# AW-IHT-1270

**8-port 10/100/1000Base-T w/PoE + 4 SFP Gigabit ports**
**Managed Industrial Switch**

# User Manual

## 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.

## HOT & COLD WARNING

The Switch surface will getting very hot or cold depend on the operating environment. Please take special care when touch to the working switch.

# Table of Content

# 1. About this Guide

## 1.1. Welcome

The AW-IHT-1270 is a Managed Industrial PoE+ Switch perfectly suited for industrial network applications which require managed devices that offer hassle-free fiber deployment and an ideal solution to deploy in automation as well as surveillance systems. The switch is designed to meet the requirements of both power and data transmission over single Ethernet cable to PoE appliances and devices without the need for power outlets, eliminating additional cost of electrical cabling and circuits. The switch's rugged IP30 aluminum case and hardened components withstand in operating temperatures from from -40℃ to 70℃.

The AW-IHT-1270 features with 4-slot Gigabit SFP which immune to moisture, static electricity, power surges and short circuits, plus 8 10/100/1000Base-T PoE ports. Each of the PoE ports complies with the IEEE 802.3at standard allowing them to supply up to 30W to satisfy the growing demand of high power consuming network devices such as WLAN AP, VoIP phones and IP surveillance cameras, and other powered devices in longer distances up to 100 meters with Cat 5e cables.

## 1.1. Purpose

This guide discusses how to install and configure your Managed Industrial Switch.

## 1.2. Terms/ Usage

In this guide, the term "Switch" (first letter upper case) refers to the AW-IHT-1270 Switch, and "switch" (first letter lower case) refers to other switches.

# 2. About the AW-IHT-1270

## 2.1. Features

**Network Functions**
Port-based Mirroring
GARP/GVRP Support
4K Active VLAN
IGMP Snooping v1/v2/v3
IGMP Querier
MVR
DHCP Relay/Option 82
Link Aggregation
Link Layer Discovery Protocol
Loop Detection, Auto Recovery Timer
STP/RSTP/MSTP
Xpress Ring
SFP DDMI Support
RMON Statistics
Static Route

**Network Security**
Access Control List (L2/L3/L4)
MAC Limitation
Port Security
802.1x Port Authentication

**Traffic management & QoS**
Port Priority
Rate Limitation
Storm Control
Port Isolation
802.1Q Tag-based VLAN
Auto MDI/MDI-X

**Network Management**
Command Line Interface, Telnet
Web GUI
SNMP v1/v2c/v3
Management VLAN
System log
Firmware Upgradable
Configuration Upload/Download
LED, SNMP trap, and email alarm

## 2.2. Specifications

**IEEE Standards**

| | |
|---|---|
| IEEE 802.3 | 10Base-T |
| IEEE 802.3u | 100Base-TX |
| IEEE 802.3ab | 1000Base-T |
| IEEE 802.3z | 1000Base-SX/LX |
| IEEE 802.3x | Flow Control |
| IEEE 802.1d | Spanning Tree Protocol |
| IEEE 802.1w | Rapid Spanning Tree Protocol |
| IEEE 802.1s | Multiple Spanning Tree Protocol |
| IEEE 802.1q | VLAN Tagging |
| IEEE 802.1p | Class of Service |
| IEEE 802.1x | Port Authentication |
| IEEE 802.1ab | Link Layer Discovery Protocol |

| | |
|---|---|
| IEEE 802.3ad | Port Trunk with LACP |
| IEEE 802.3af | Power over Ethernet (PoE) |
| IEEE 802.3at | High Power over Ethernet (PoE+) |

**Performance**

| | |
|---|---|
| Switching fabric | 24Gbps |
| L2 forwarding | 17.86Mpps |
| MAC Entries | 16 K |
| Jumbo frame | 10 K |

**Physical Ports**

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

4 Gigabit SFP slots

1 x Console port (RJ-45 to RS-232)

**Mechanical & Environmental**

| | |
|---|---|
| Dimension (WxHxD) | 50x161.5x122.2mm (1.97x6.36x4.81 inch) |
| Weight | 860g |
| Mounting | DIN-Rail |
| Housing | IP30 protection |
| Wide Operating temperature | -40 to 70℃ |
| Storage temperature | -40 to 85℃ |
| Operating humidity | 10% to 95% RH (Non Condensing) |
| Storage humidity | 5% to 95% RH (Non Condensing) |

**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

Output capacity for PoE: 240 W

PoE supported mode: Mode A

***Notice:*** *PoE Power at PDs (Powered Devices) for 100 meters deployment distance*

| DC Power Input | 48~52V DC | 54~57V DC |
|---|---|---|
| RJ-45 Distance (Cat5e or above) | 100m | 100m |
| PoE Power at PDs | 802.3af | 802.3at |

**Power**

Input Voltage:

- Primary inputs: 48~57V DC (or 24~57V DC for AW-IHT-1270-24V model)
- Redundant inputs:48~57V DC (or 24~57V DC for AW-IHT-1270-24V model)

Connection: One removable 6-pin terminal block

Support Overload current protection

Support Reverse Polarity Protection

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

Self-power consumption: 18W (Maximum)

# 3. Hardware Description

**AW-IHT-1270 Front Panel**

8-port 10/100/1000Base-T w/PoE + 4 SFP Gigabit
Managed Industrial Switch

## 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.

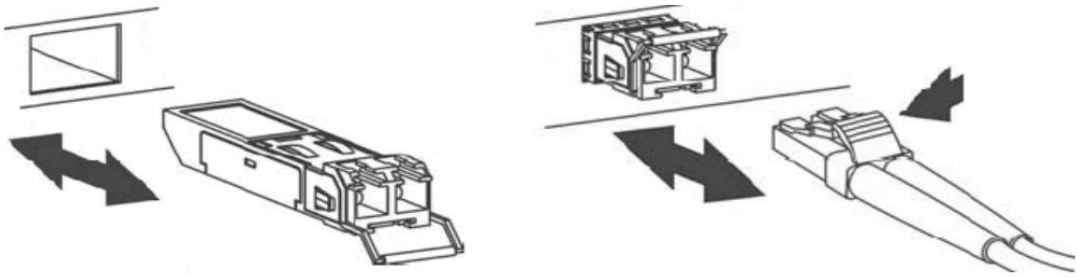
### 3.1.2. SFP Slots for SFP modules

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

**Installing the SFP modules and Fiber Cable**

1. Slide the selected SFP module into the selected SFP slot (Make sure the SFP module is aligned correctly with the inside of the slot)
2. Insert and slide the module into the SFP slot until it clicks into place
3. Remove any rubber plugs that may be present in the SFP module's mouth

4. Align the fiber cable's connector with the SFP module's mouth and insert the connector
5. Slide the connector in until a click is heard
6. If you want to pull the connector out, first push down the release clip on top of the connector to release the connector from the SFP module.



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

**Note:** When inserting the cable, be sure the tab on the plug clicks into position to ensure that it is properly seated.

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

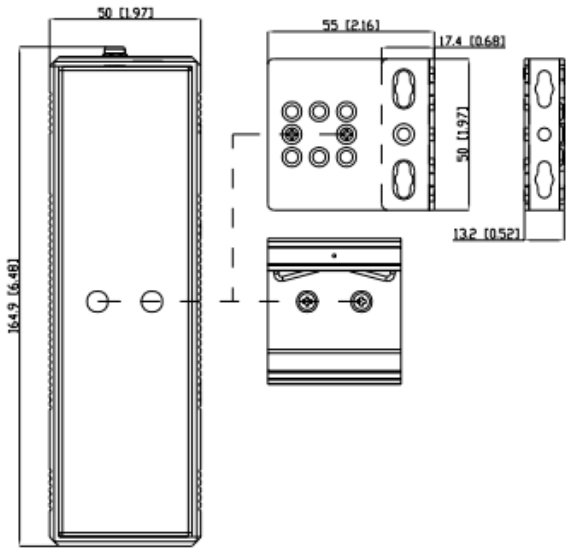
### 3.2. Installation

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

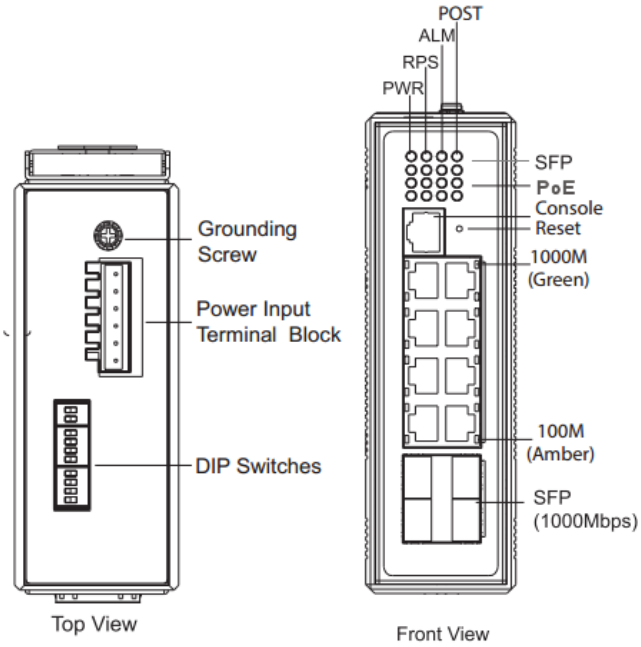
- ✓ Install the Switch in an appropriate place. See Technical Specifications for the acceptable temperature and humidity ranges.
- ✓ Install the Switch in a location that is not affected by strong electromagnetic field generators (such as motors), vibration, dust, and direct sunlight.
- ✓ Leave at least 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 AW-IHT-1270




✓ **Step 3:** Connect the 48~57V DC (or 24~57V DC for AW-IHT-1270-24V) power to the PWR & RPS terminal block.




✓ **Step 4**: Connect the Ethernet (RJ-45) port to the networking device and check the LED status to confirm the connection is established.

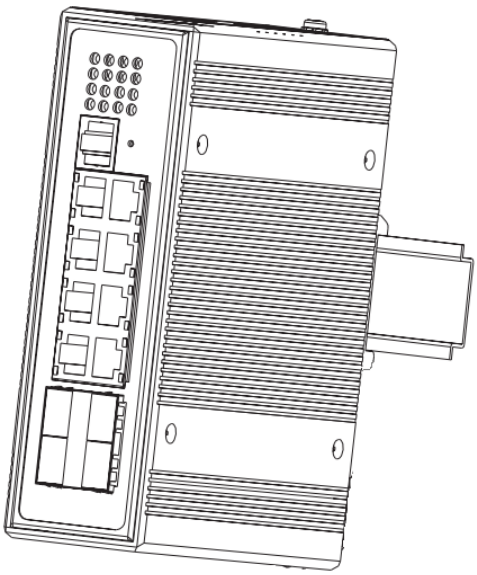
### 3.2.2. DIN rail Installation

The AW-IHT-1270 has a DIN rail bracket on the back of the Switch.

**Location:** The AW-IHT-1270 can be DIN-Rail-mounted in cabinet or enclosure.

**Mounting the switch**

Place the AW-IHT-1270 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 AW-IHT-1270 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

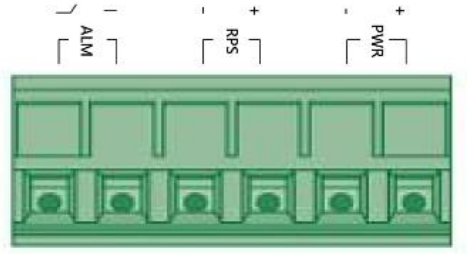
### 3.2.4. Wiring Redundant Power Inputs

You can use "Terminal Block (PWR)" for Primary Power input and "Terminal Block (RPS)" for secondary power source for Redundant Power Input.

To insert power wire and connect the 48~57V DC (or 24~57V DC for AW-IHT-1270-24V) power to the power terminal block, follow the steps below:

- ✓ Use -at-head screw driver to loosen the wire-clamp screws.
- ✓ Insert the corresponding wires into contacts.
- ✓ Tighten the wire-clamp screws to prevent the wires from loosening.

Top view of Terminal Block is shown as picture:




### 3.2.5. Powering On the Unit

The Switch accepts the power input voltage from 48~57V DC (or 24~57V DC for AW-IHT-1270-24V).

- ✓ Insert the power cables into the terminal block located on the top of the device.
- ✓ 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.*

**Reset Button**

There has "Reset" button in front of Switch which can help to manually hardware reboot.

### 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:

| Unit LEDs | | |
|---|---|---|
| **LED** | **Condition** | **Status** |
| **PWR** (Green) | Illuminated | Switch uses primary power |
| | Off | Primary power off or failure |
| **RPS** (Green) | Illuminated | Switch uses redundant power |
| | Off | Redundant power off or failure |
| **ALM** (Red) | Illuminated | External signal device will be activated through terminal block ALM when any of all port links fails |
| | Off | No alarm to report |
| **POST** (Green) | Illuminated | Switch is ready or running |
| | Off | Switch is not ready |
| **SFP** (Green) (9~12) | Illuminated | SFP port link-up |
| | Blinking | Activity (receiving or transmitting data) |
| | Off | Port disconnected or link failed |
| **PoE** (Green) (1~8) | Off | No power is feeding |
| | Illuminated | Power feeding on PoE port |
| **1000Mbps** (Green) | Illuminated | Ethernet link-up |
| | Blinking | Activity (receiving or transmitting data) |
| | Off | Port disconnected or link failed |
| | Illuminated | Ethernet link-up |

| | | |
|---|---|---|
| **10/100Mbps** (Amber) | Blinking | Activity (receiving or transmitting data) |
| | Off | Port disconnected or link failed |

### 3.4. DIP Switches

- Power: DIP 1 and DIP 2 is for primary power and redundant power supply.
- Alarm Relay output: DIP 3 to DIP 14 control each of ports to trigger the external alarm device.

| No | Name | Description |
|---|---|---|
| 1 | PWR | ON: Master power alarm reporting is enabled<br>OFF: Master power alarm reporting is disabled |
| 2 | RPS | ON: Redundant power alarm reporting is enabled<br>OFF: Redundant power alarm reporting is disabled |
| 3 | P1 | ON: port 1 link alarm reporting is enabled.<br>OFF: port 1 link alarm reporting is disabled. |
| 4 | P2 | ON: port 2 link alarm reporting is enabled.<br>OFF: port 2 link alarm reporting is disabled. |
| 5 | P3 | ON: port 3 link alarm reporting is enabled.<br>OFF: port 3 link alarm reporting is disabled. |
| 6 | P4 | ON: port 4 link alarm reporting is enabled.<br>OFF: port 4 link alarm reporting is disabled. |
| 7 | P5 | ON: port 5 link alarm reporting is enabled.<br>OFF: port 5 link alarm reporting is disabled. |
| 8 | P6 | ON: port 6 link alarm reporting is enabled.<br>OFF: port 6 link alarm reporting is disabled. |
| 9 | P7 | ON: port 7 link alarm reporting is enabled.<br>OFF: port 7 link alarm reporting is disabled. |
| 10 | P8 | ON: port 8 link alarm reporting is enabled.<br>OFF: port 8 link alarm reporting is disabled. |
| 11 | P9 | ON: port 9 (SFP) link alarm reporting is enabled.<br>OFF: port 9 (SFP) link alarm reporting is disabled. |
| 12 | P10 | ON: port 10 (SFP) link alarm reporting is enabled.<br>OFF: port 10 (SFP) link alarm reporting is disabled. |
| 13 | P11 | ON: port 11 (SFP) link alarm reporting is enabled.<br>OFF: port 11 (SFP) link alarm reporting is disabled. |
| 14 | P12 | ON: port 12 (SFP) link alarm reporting is enabled.<br>OFF: port 12 (SFP) link alarm reporting is disabled. |

# 4. System Status

## 4.1. Console Port

- 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 | 192.168.1.1 |
| 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***

***L2SWITCH#***

### 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)#***

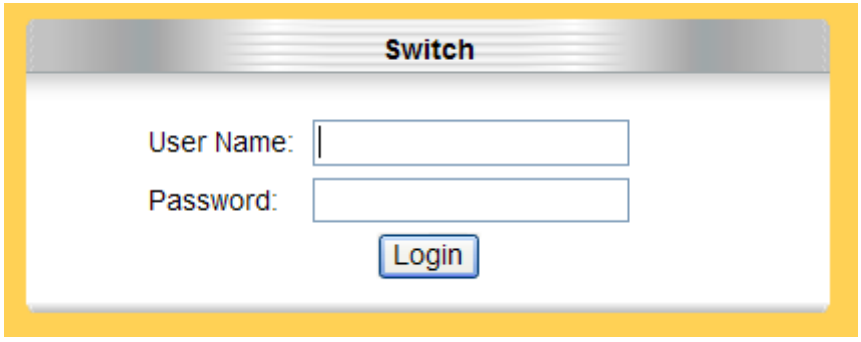
- vlan
  Its command prompt is "***L2SWITCH(config-vlan)#".***
  It means these commands can be executed in this command prompt.
  In ***Configure*** code, executing command "***vlan 2***" enter the vlan 2 node.
  Note: where the "2" is the vlan ID.

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

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

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

### 4.5. GUI Login




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

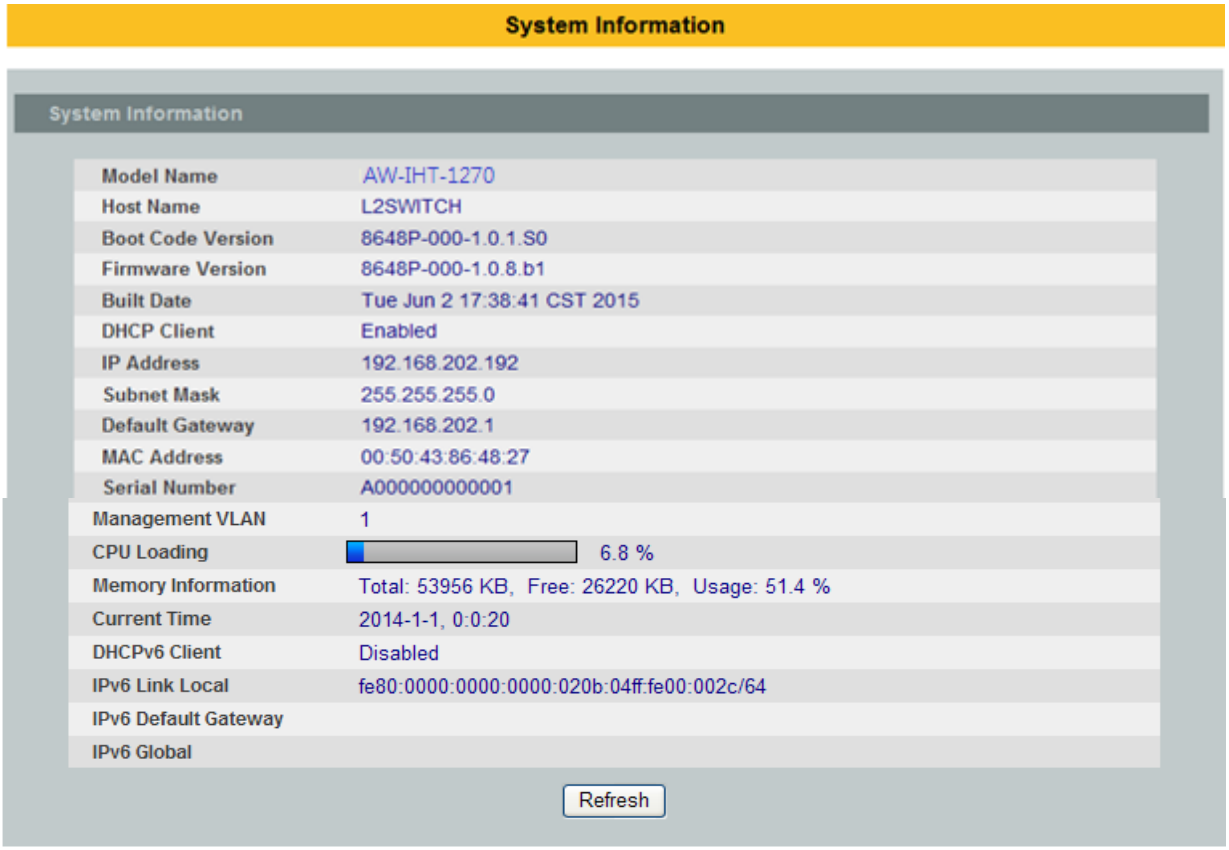
**Default:**
User name: admin,

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). |
| DHCPv6 Client | This field displays whether the DHCPv6 client is enabled on the Switch. |
| IPv6 Link Local | This field displays the Switch's link local IP address for IPv6. |
| IPv6 Default Gateway | This field displays the default gateway for IPv6. |
| IPv6 Global | This field displays the Switch's global IP address for IPv6. |
| 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**

To specify a VLAN group which can access the Switch.

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

**Host Name**

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

**Default Settings**

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

#### 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.<br>Disable: Use a static IP address on the switch.<br>Enable & Renew: Use DHCP client to get an IP address from DHCP server. |
| eth0 | management vlan VLANID | This command configures the management vlan. |
| eth0 | ip ipv6-address AAAA:BBBB:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH/M | This command configures a global scope of IPv6 address and subnet mask for the system. |
| eth0 | ip ipv6-address default-gateway AAAA:BBBB:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH | This command configures a default gateway for the system. |
| eth0 | ip ipv6-dhcp client (disable\|enable\|renew) | This command configures a DHCPv6 client function for the system.<br>Disable: Use a static IP address on the switch.<br>Enable & Renew: Use DHCPv6 client to get an IP address from DHCPv6 server. |

**Example**: 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

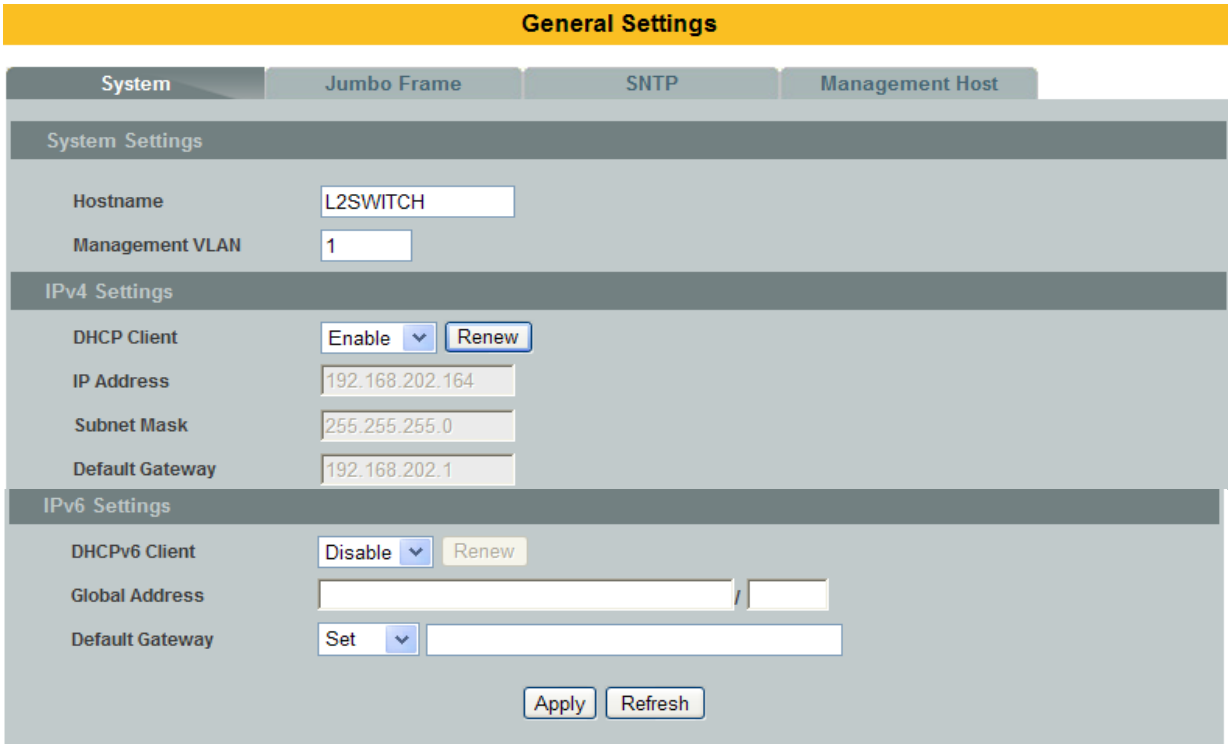
✓ To configure a static IP address and a gateway for the Switch.
L2SWITCH(config-if)#ip address 192.168.202.111/24
L2SWITCH(config-if)#ip address default-gateway 192.168.202.1

✓ To configure a static global IPv6 address and a gateway for the Switch.

■ Please set the static global IPv6 address first.
L2SWITCH(config-if)#ip ipv6-address 3ffe::1235/64

■ And the set the IPv6 default gateway address.
L2SWITCH(config-if)#ip ipv6-address default-gateway 3ffe::1234

### 5.1.1.3. Web Configuration




| | |
|---|---|
| IP Address | Configures a IPv4 address for 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. |
| IPv6 Settings | |
| DHCPv6 Client | Select **Enable** to allow the Switch to automatically get an IP address from a DHCPv6 server. Click **Renew** to have the Switch re-get an IP address from the DHCP server.<br>Select **Disable** if you want to configure the Switch's IP address manually. |
| Global Address | Configure a global IPv6 address for the Switch. |
| Default Gateway | Set – Set an IPv6 default gateway for the Switch.<br>Unset – Unset the IPv6 default gateway for the Switch. |

| | |
|---|---|
| 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 1522, 1536, 1552, 9010, 9216, 10240.

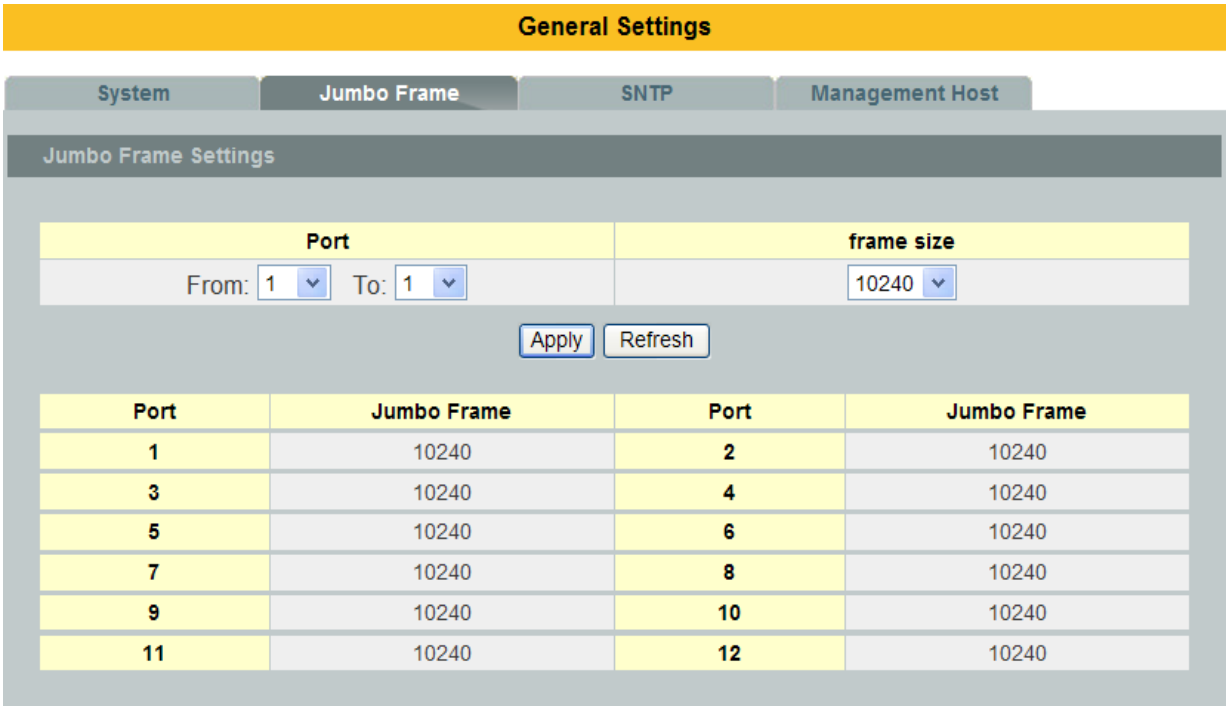
**Default Settings**

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\|1522\|1536\|1552\|9010\|9216) | This command configures the maximum number of bytes of frame size for all ports. |
| configure | interface IFNAME | This command enters the interface configure node. |
| interface | jumboframe (10240\|1522\|1536\|1552\|9010\|9216) | This command configures the maximum number of bytes of frame size. |
| configure | interface range gigabitethernet1/0/PORTLISTS | This command enters the interface configure node. |
| if-range | jumboframe (10240\|1522\|1536\|1552\|9010\|9216) | This command configures the maximum number of bytes of frame size. |

### 5.1.2.3. Web Configuration




| Parameter | Description |
|---|---|
| Port | This field specifies a port or a range of ports for configuration. |
| Frame Size | This field configures the maximum number of bytes of frame size for specified port(s). |
| 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

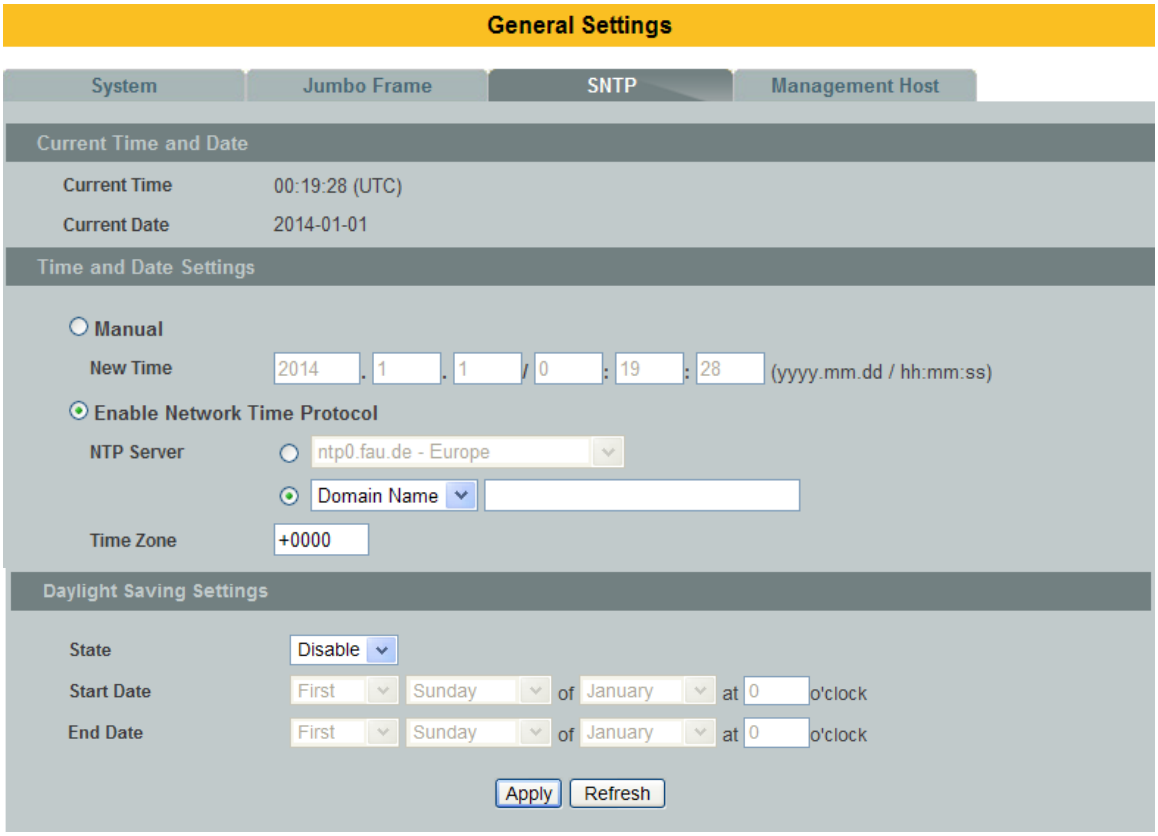
| Node | Command | Description |
|---|---|---|
| enable | show time | This command displays current time and time configurations. |
| configure | time HOUR:MINUTE:SECOND | Sets the current time on the Switch.<br>*hour*: 0-23<br>*min*: 0-59<br>*sec*: 0-59<br>Note: If you configure Daylight Saving Time 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.<br>*year*: 1970-<br>*month*: 1-12<br>*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 ntp-server domain-name STRING | This command sets a domain name of your time server. |
| configure | time timezone STRING | Configures the time difference between UTC (formerly known as GMT) and your time zone. Valid Range: -1200 ~ +1200. |

**Example:**

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

### 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 or type the domain name 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 |

| | |
|---|---|
| | from the drop-down list box. |
| **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:<br>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**, **March** and **2:00**.<br>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**, **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:<br>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**, **November** and **2:00**.<br>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**, **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 Apply to take effect the settings. |
| Refresh | Click Refresh to begin configuring this screen afresh. |

### 5.1.4. Management Host

#### 5.1.4.1. Introduction

The feature limits the hosts which can manage the Switch. That is, any hosts can manage the Switch via **telnet** or **web browser**. If user has configured one or more management host, the Switch can be managed by these hosts only. The feature allow user to configure management IP up to 3 entries.

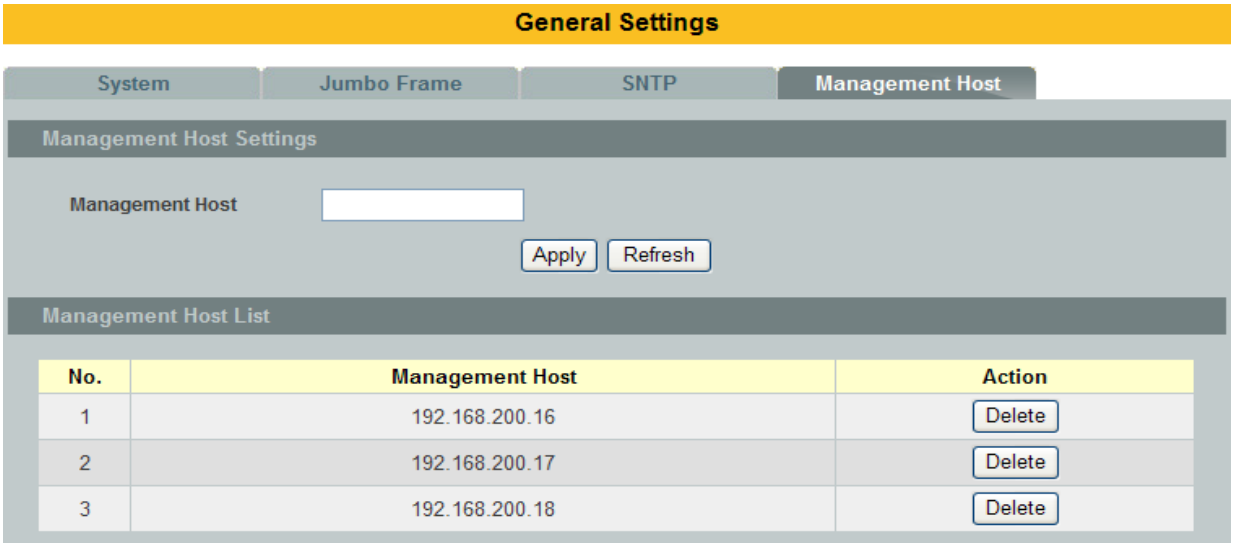
**Default Settings**
The default is none, any host can manage the Switch via telnet or web browser.

### 5.1.4.2. 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 | no management host A.B.C.D | The command deletes a management host address. |

**Example:**
L2SWITCH#configure terminal
L2SWITCH(config)#interface eth0
L2SWITCH(config-if)#management host 192.168.200.106

### 5.1.4.3. Web Configuration




| Parameter | Description |
|---|---|
| Management Host | This field configures the management host. |
| 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. |
| 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; it can be removed by user only. The maximum static address entry is up to 256.

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 the 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. If too much port flooding, it may lead 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.

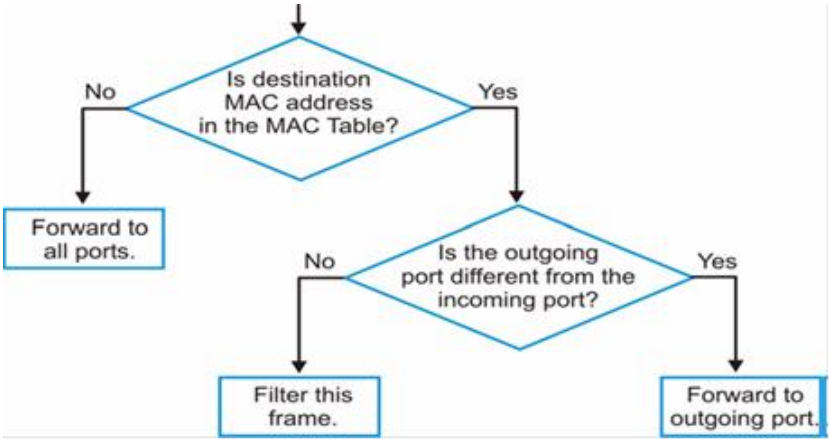



**Figure** MAC Table Flowchart

**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 mac MACADDR | This command displays information of a 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 VLANID port PORT_ID | This command configures a static unicast entry. |
| configure | no mac-address-table static MACADDR vlan VLANID | This command removes a static unicast entry from the address table. |
| configure | mac-address-table aging-time VALUE | This command configures the mac table aging time. |
| configure | clear mac address-table dynamic | This command clears the dynamic address entries. |

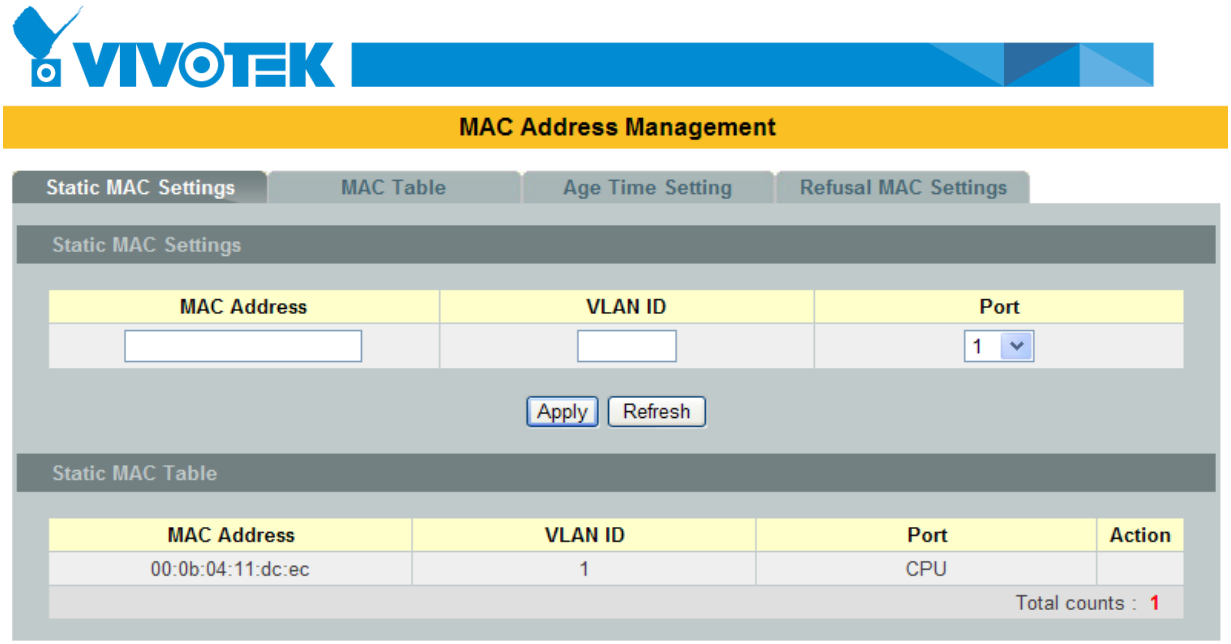
**Example:**

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

### 5.2.3. Web Configuration

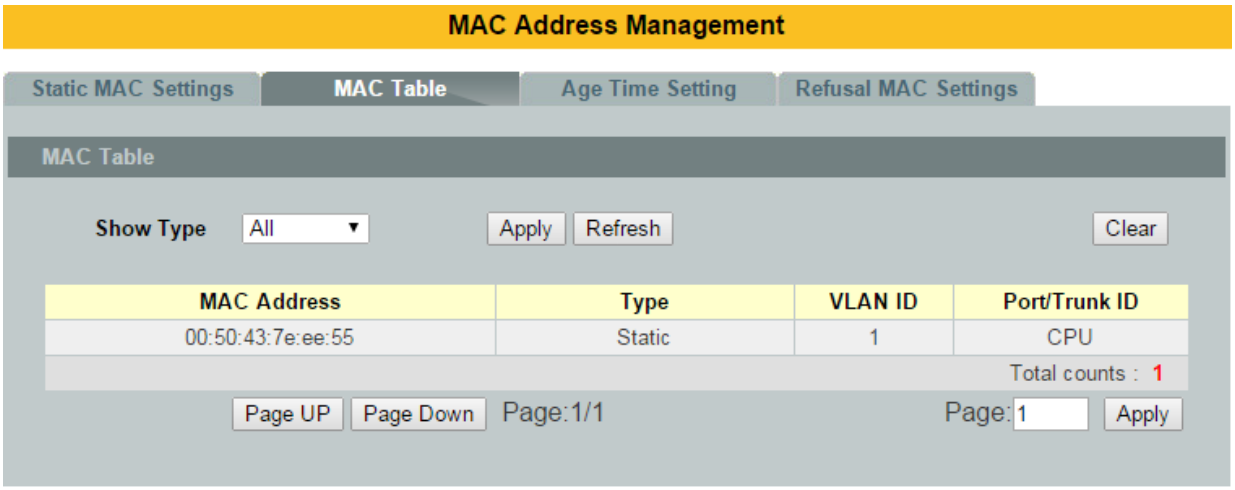
**Static MAC**

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



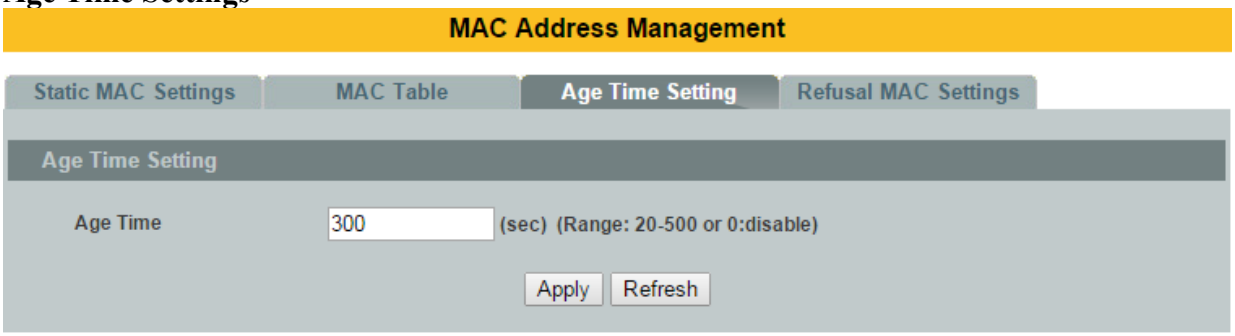

| Parameter | Description |
|---|---|
| Static MAC Settings | |
| MAC Address | Enter the MAC address of a computer or device that you want to add to the MAC address table.<br>Valid format is hh:hh:hh:hh:hh:hh. |
| VLAN ID | Enter the VLAN ID to apply to the computer or device. |
| Port | Enter the port 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<br>Apply | Select **All, Static**, **Dynamic or Port** and then click **Apply** to display the corresponding MAC address entries on this screen. |
| Refresh | Click this to update the information in the MAC table. |
| MAC Address | This field displays a MAC address. |
| Type | This field displays whether this entry was entered manually (Static) or whether it was learned by the Switch (Dynamic). |
| VLAN ID | This field displays the VLAN ID of the MAC address entry. |
| Port | This field displays the port number the MAC address entry is associated. It displays CPU if it is the entry for the Switch itself.<br>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. |

### 5.2.4. Refusal (Black-hole MAC)

#### 5.2.4.1. Introduction

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

**Notice:** User can configure up to 20 entries.

#### 5.2.4.2. CLI Configuration

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

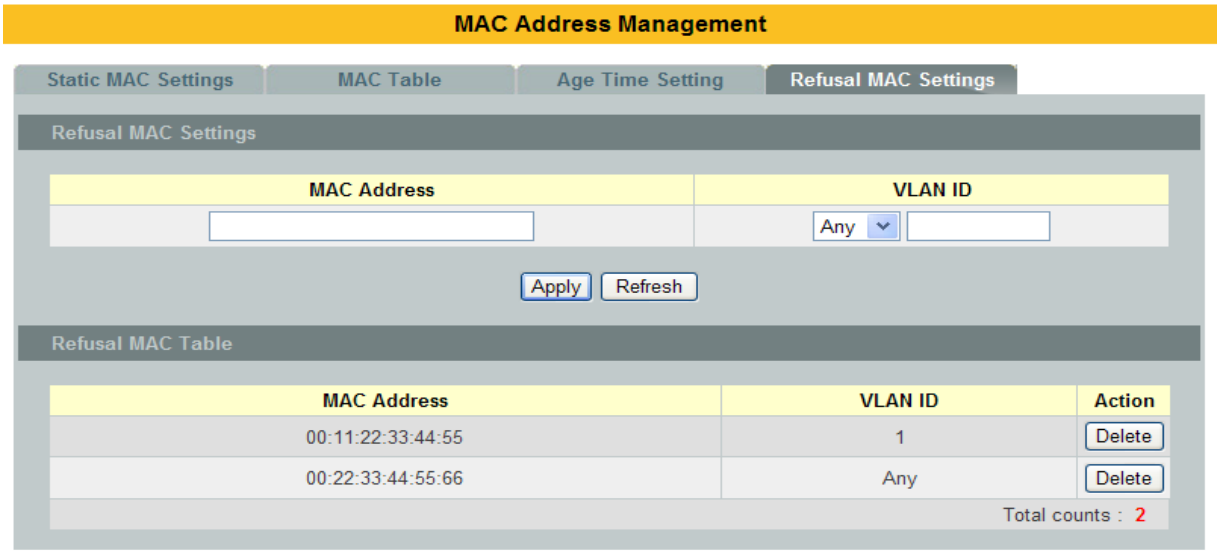
**Example:** The procedures to configure a refusal MAC address

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

✓ To configure a refusal MAC address for all ports and all vlans.
L2SWITCH(config)#mac-address-table refusal 00:11:22:33:44:55

✓ To configure a refusal MAC address for all ports on a specific vlan.
L2SWITCH(config)#mac-address-table refusal 00:11:22:33:44:55 vlan 1.

### 5.2.4.3. Web Configuration




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

## 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

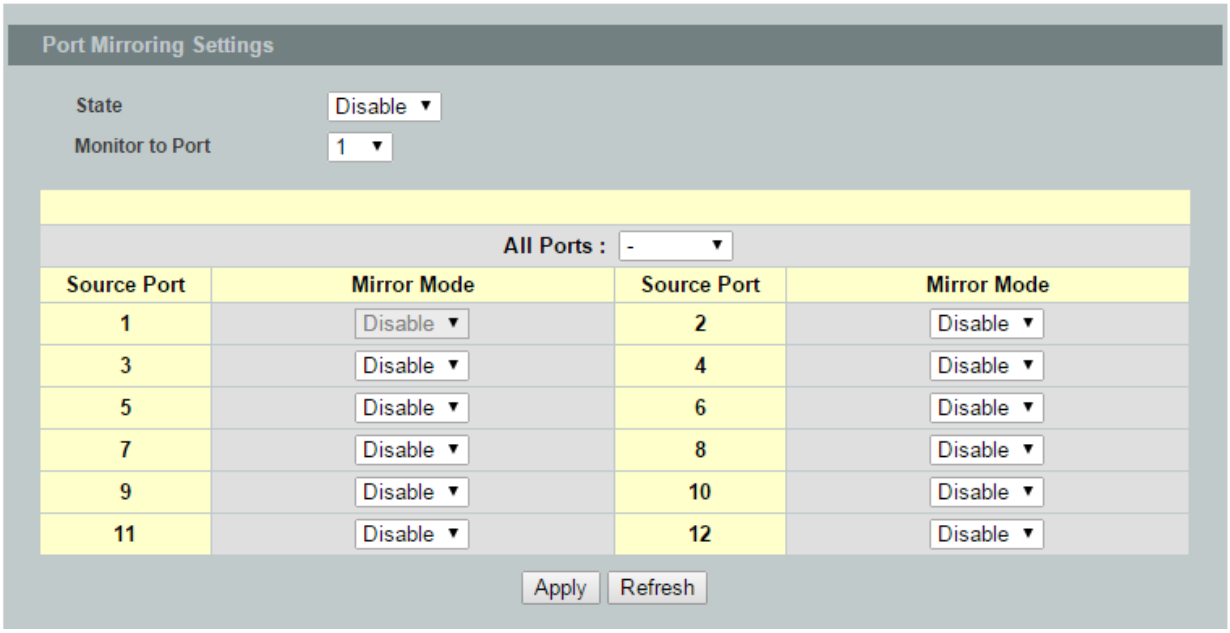
| Node | Command | Description |
|---|---|---|
| enable | show mirror | This command displays the current port mirroring configurations. |
| configure | mirror (disable\|enable) | This command disables / enables the port mirroring on the switch. |
| configure | mirror destination port PORT_ID | This 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 3-11 mode both

### 5.3.3. Web Configuration

**Port Mirroring**




| 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.<br>Use this field only if you want to make some settings the same for all ports.<br>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. |

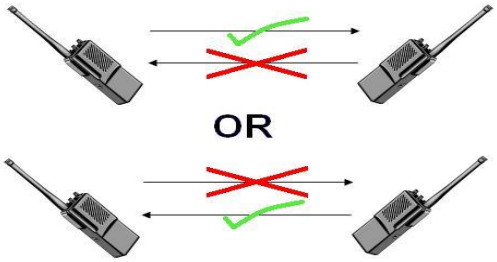
## 5.4. Port Settings

### 5.4.1. Introduction

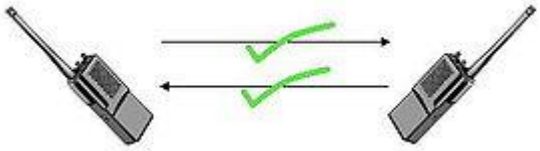
- Duplex mode

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 or the interface automatically corrects any incorrect cabling. For Auto-MDIX to operate correctly, the speed on the interface and duplex setting must be set to "auto". Auto-MDIX was developed by HP engineers Dan Dove and Bruce Melvin.

- 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.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 and resend later.

The Switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.

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

- 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.

### 5.4.2. CLI Configuration

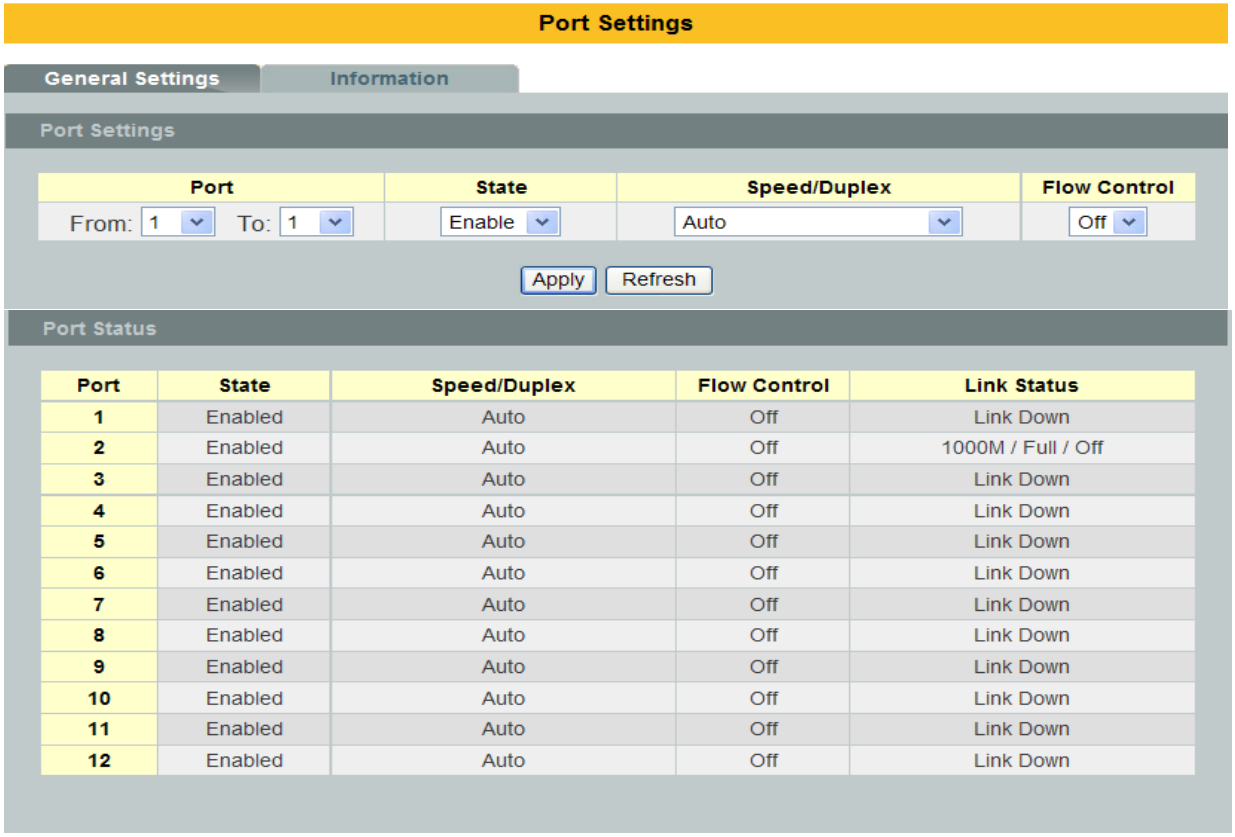
| Node | Command | Description |
|---|---|---|
| enable | show interface IFNAME | This command displays the current port configurations. |
| configure | interface IFNAME | This command enters the interface configure node. |
| interface | show | This command displays the current port configurations. |
| 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-half\| 100-full\|100-half\|1000-full) | 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 STRINGs | This command configures a description for the specific port. |
| interface | no description | This command configures the default port description. |
| interface | cable test | This command diagnostics the Ethernet cable and shows the broken distance. |
| interface | clean cable-test result | This command cleans the test result of the Ethernet cable test. |
| 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-half\| 100-full\|100-half\|1000-full) | This command configures the speed and duplex for the port. |

**Example:**

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

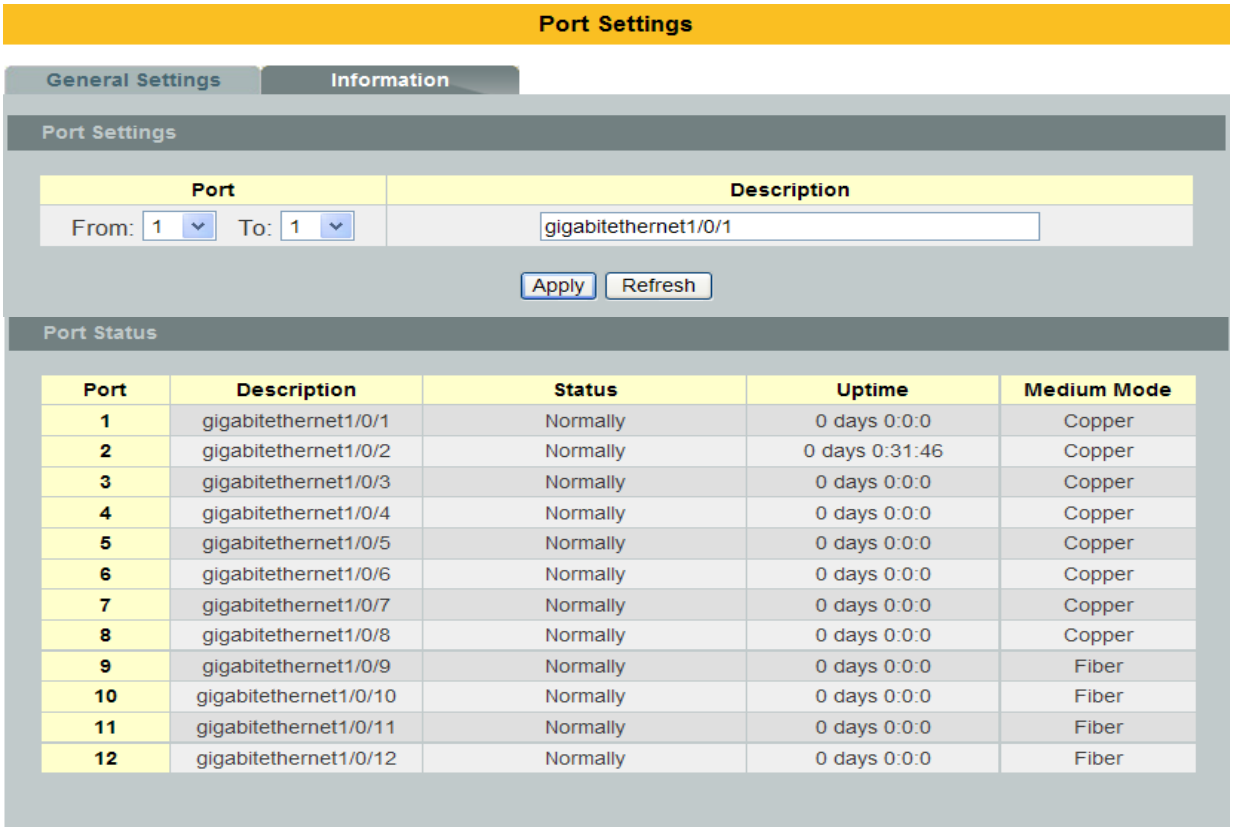
### 5.4.3. Web Configuration




| 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:<br>• **Auto**<br>• **10 Mbps / Full Duplex**<br>• **10 Mbps / Half Duplex**<br>• **100 Mbps / Full Duplex**<br>• **100 Mbps / Half Duplex**<br>• **1000 Mbps / Full Duplex** |
| Flow Control | Select **On** to enable access to buffering resources for the port thus ensuring lossless operation across network switches. Otherwise, select **Off** to disable it. |
| Apply | Click Apply to take effect the settings. |
| Refresh | Click Refresh to begin configuring this screen afresh. |
| Port | This field displays the port number. |
| State | This field displays whether the port is enabled or disabled. |

| | |
|---|---|
| Speed/Duplex | This field displays the speed either **10M**, **100M** or **1000M** and the duplex mode **Full** or **Half**. |
| Flow Control | This field displays whether the port's flow control is **On** or **Off**. |
| Link Status | This field displays the link status of the port. If the port is up, it displays the port's speed, duplex and flow control setting. Otherwise, it displays **Link Down** if the port is disabled or not connected to any device. |

**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="3">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td colspan="2">Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="3">Header Checksum</td></tr>
<tr><td colspan="6">Source Address</td></tr>
<tr><td colspan="6">Destination Address</td></tr>
<tr><td colspan="5">Options</td><td>Padding</td></tr>
</table>

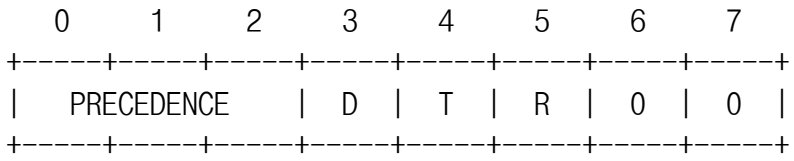
Example Internet Datagram Header

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)**
  The packets on the high priority queue are always service firstly.

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

The DiffServ is disabled on the switch.

| DSCP | Priority | DSCP | Priority | DSCP | Priority | DSCP | Priority |
|---|---|---|---|---|---|---|---|
| 00 | 0 | 01 | 0 | 02 | 0 | 03 | 0 |
| 04 | 0 | 05 | 0 | 06 | 0 | 07 | 0 |
| 08 | 0 | 09 | 0 | 10 | 0 | 11 | 0 |
| 12 | 0 | 13 | 0 | 14 | 0 | 15 | 0 |
| 16 | 0 | 17 | 0 | 18 | 0 | 19 | 0 |
| 20 | 0 | 21 | 0 | 22 | 0 | 23 | 0 |
| 24 | 0 | 25 | 0 | 26 | 0 | 27 | 0 |
| 28 | 0 | 29 | 0 | 30 | 0 | 31 | 0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 32 | 0 | 33 | 0 | 34 | 0 | 35 | 0 |
| 36 | 0 | 37 | 0 | 38 | 0 | 39 | 0 |
| 40 | 0 | 41 | 0 | 42 | 0 | 43 | 0 |
| 44 | 0 | 45 | 0 | 46 | 0 | 47 | 0 |
| 48 | 0 | 49 | 0 | 50 | 0 | 51 | 0 |
| 52 | 0 | 53 | 0 | 54 | 0 | 55 | 0 |
| 56 | 0 | 57 | 0 | 58 | 0 | 59 | 0 |
| 60 | 0 | 61 | 0 | 62 | 0 | 63 | 0 |

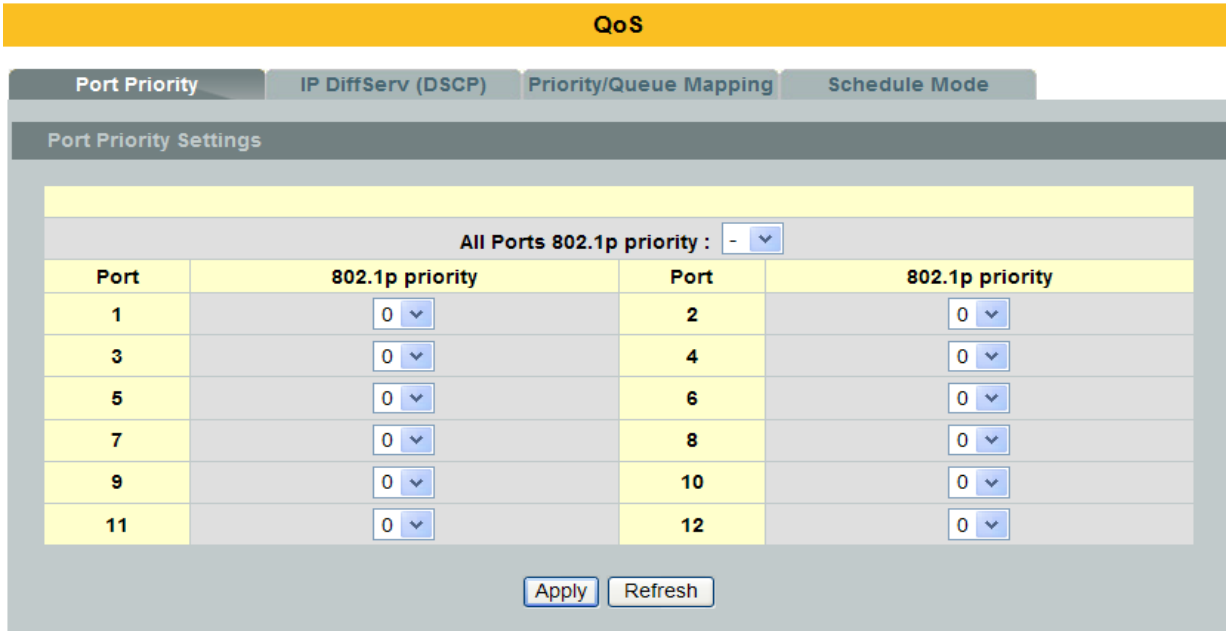
**Note:** If the DiffServ is disabled, the 802.1p tag priority will be used.

#### 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 PRIORITY QUEUE_ID | This command configures the 802.1p priority mapping to the service queue. |
| configure | no queue cos-map | This command configures the 802.1p priority mapping to the service queue to default. |
| configure | qos mode high-first | This command configures the QoS scheduling mode to high_first, each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets. |
| configure | qos mode wrr-queue weights VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE | This command configures the QoS scheduling mode to Weighted Round Robin. |
| interface | default-priority | This command allows the user to specify a default priority handling of untagged packets received by the Switch. The priority value entered with this command will be used to determine which of the hardware priority queues the packet is forwarded to. Default: 0. |
| interface | no default-priority | This command configures the default priority for the specific port to default (0). |
| enable | show diffserv | This command displays DiffServ configurations. |
| configure | diffserv (disable\|enable) | This command disables / enables the DiffServ function. |
| configure | diffserv dscp VALUE priority VALUE | This command sets the DSCP-to-IEEE 802.1q mappings. |

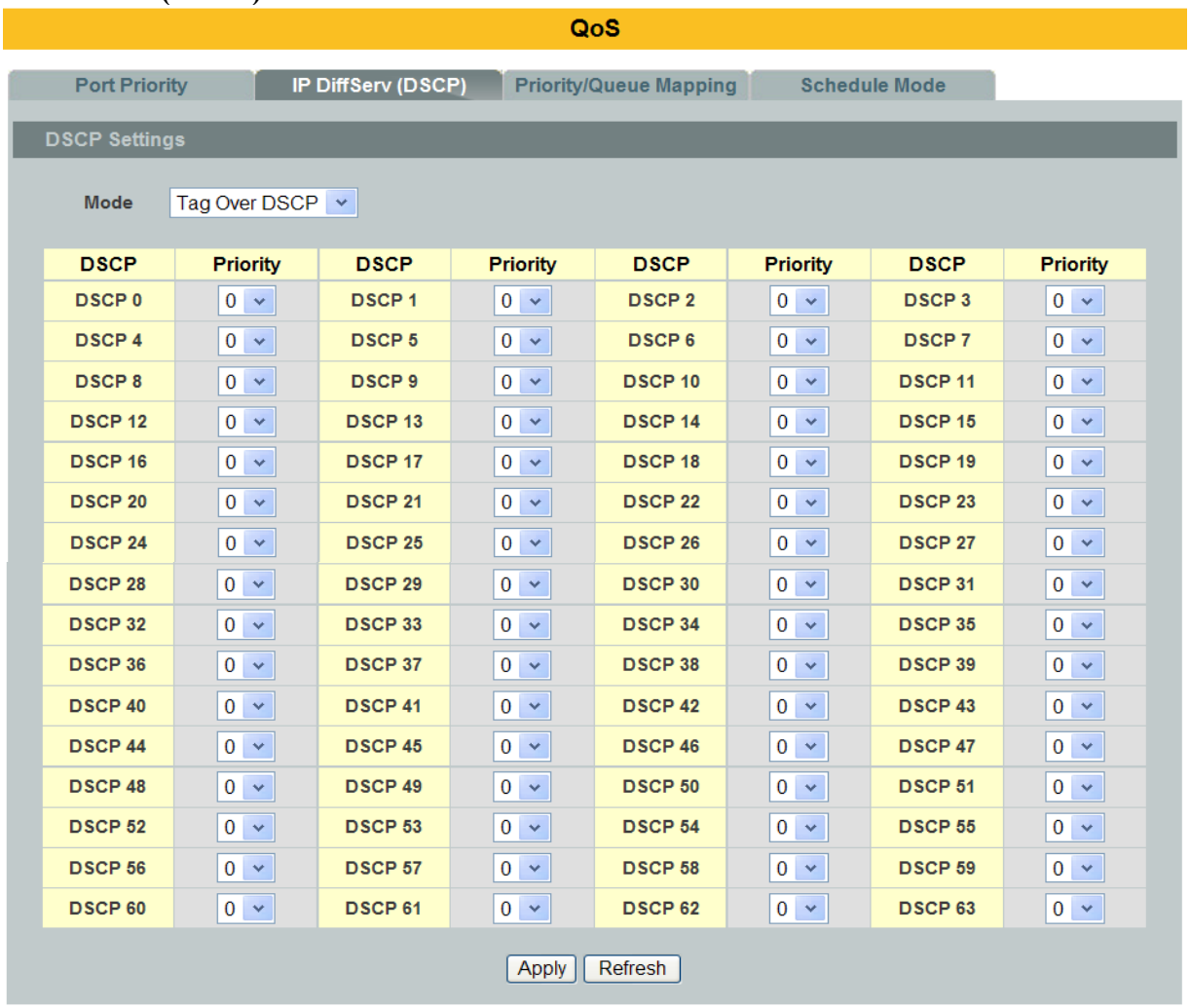
### 6.1.1.3. Web Configuration

**Port Priority**



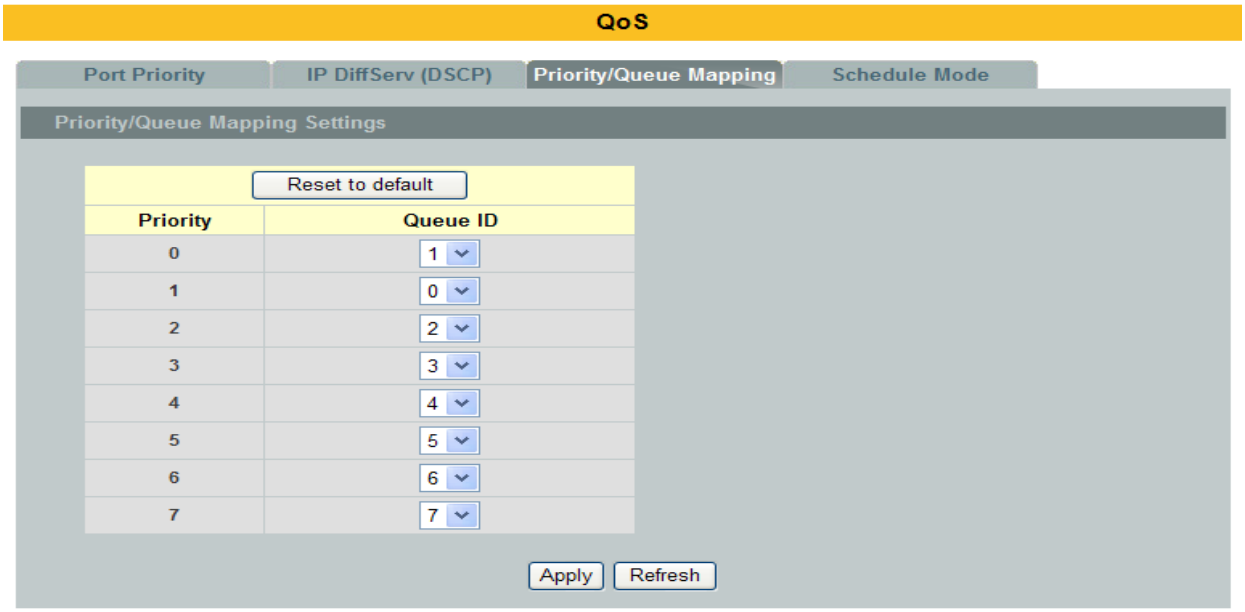

| Parameter | Description |
|---|---|
| All Ports 802.1p priority | Use this field to set a priority for all ports.<br>The value indicates packet priority and is added to the priority tag field of incoming packets. The values range from 0 (lowest priority) to 7 (highest priority). |
| Port | This field 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)



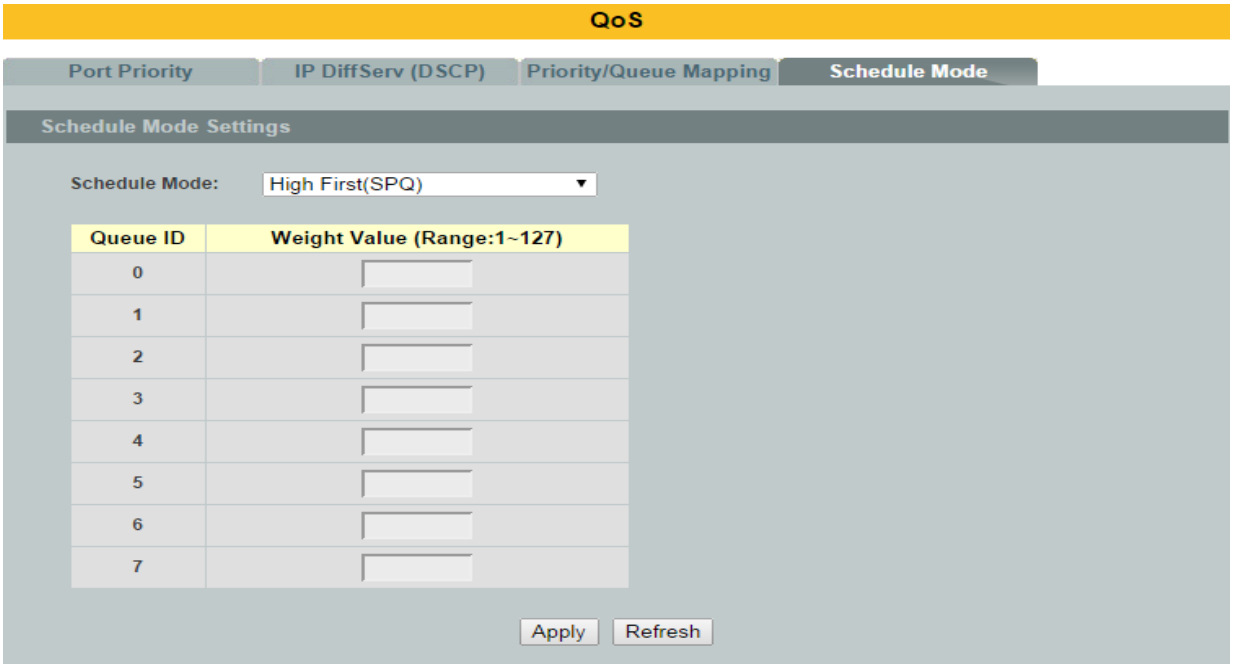

| Parameter | Description |
|---|---|
| Mode | "Tag Over DSCP" or "DSCP Over Tag". "Tag Over DSCP" means the 802.1p tag has higher priority than DSCP. |
| Priority | This field displays each priority level. The values range from 0 (lowest priority) to 7 (highest priority). |
| Apply<br>Refresh | Click Apply to take effect the settings.<br>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**).<br>Note: Queue weights can only be changed when **Weighted Round Robin** is selected.<br>**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. |
| 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: 652pps.

**Default Settings**

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

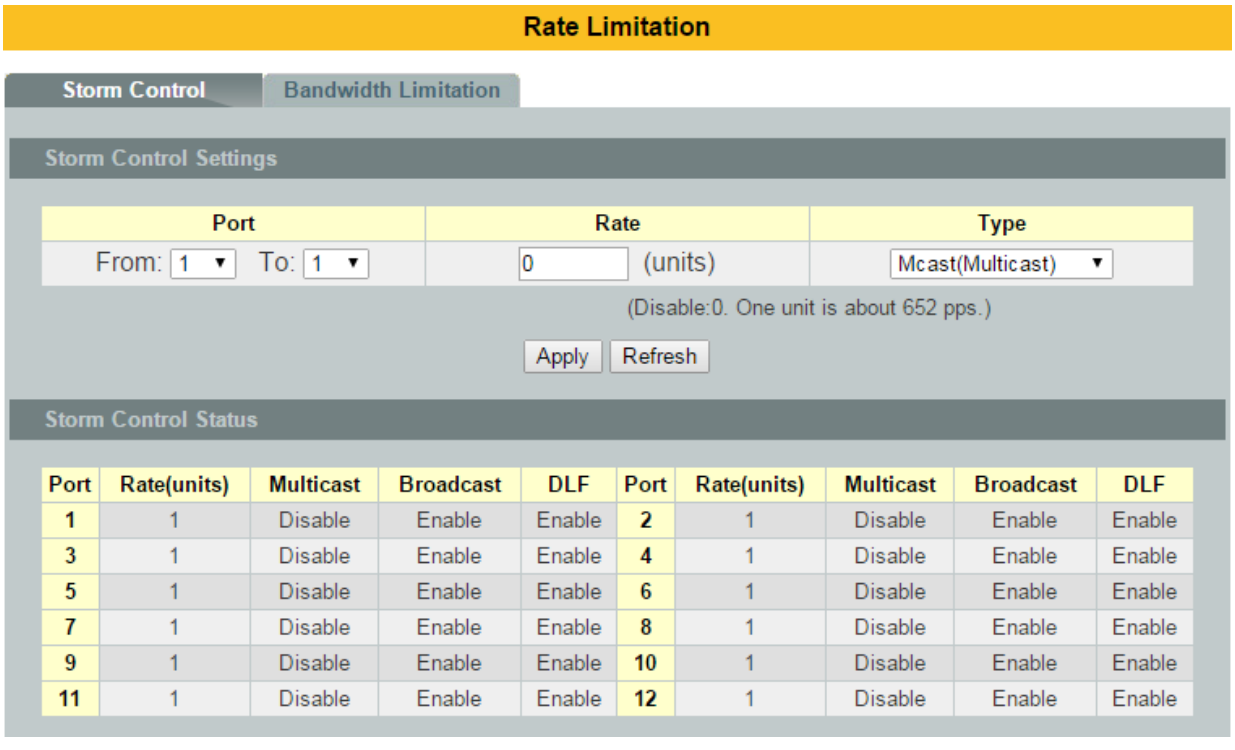
#### 6.1.2.1.2. CLI Configuration

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

#### 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.<br>**Multicast** - to specify a limit for the amount of multicast packets received per second.<br>**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: Mbs.

**Default Settings**
All ports' Ingress and Egress rate limitation are disabled.

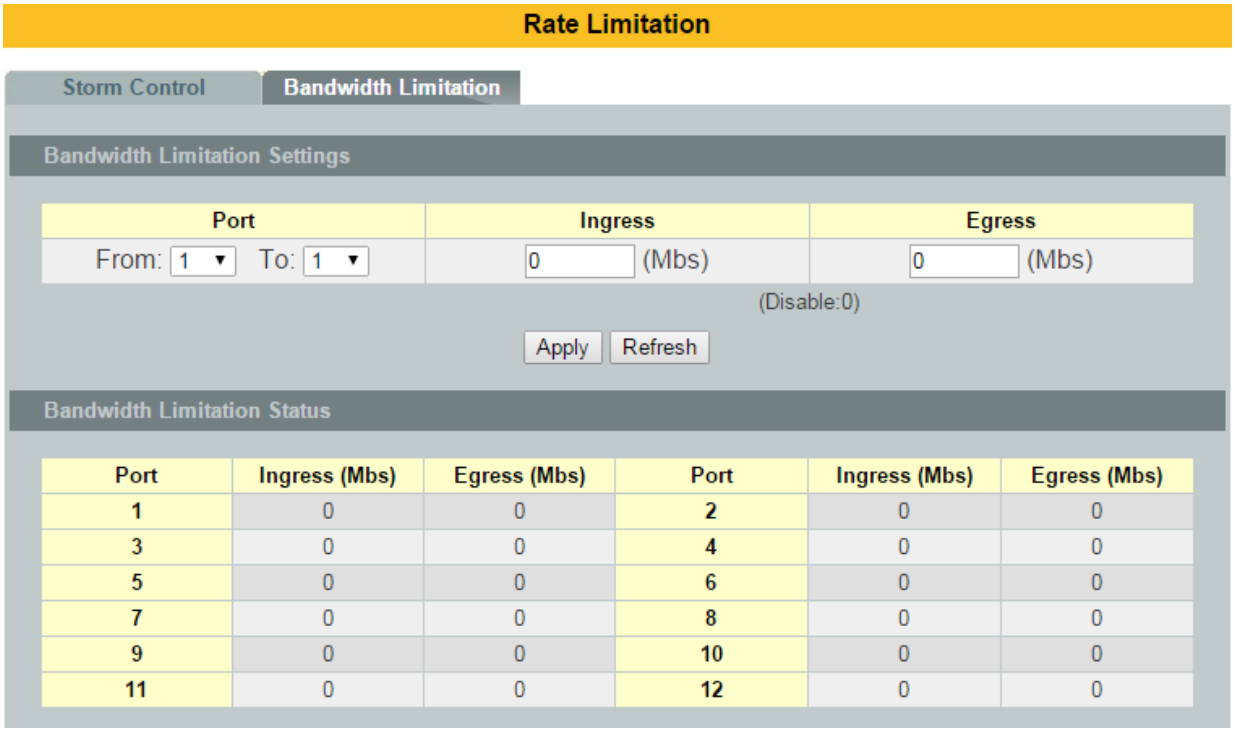
##### 6.1.2.2.2. CLI Configuration

| 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 1-8
L2SWITCH(config)#bandwidth-limit ingress 1 ports 1-8
```

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

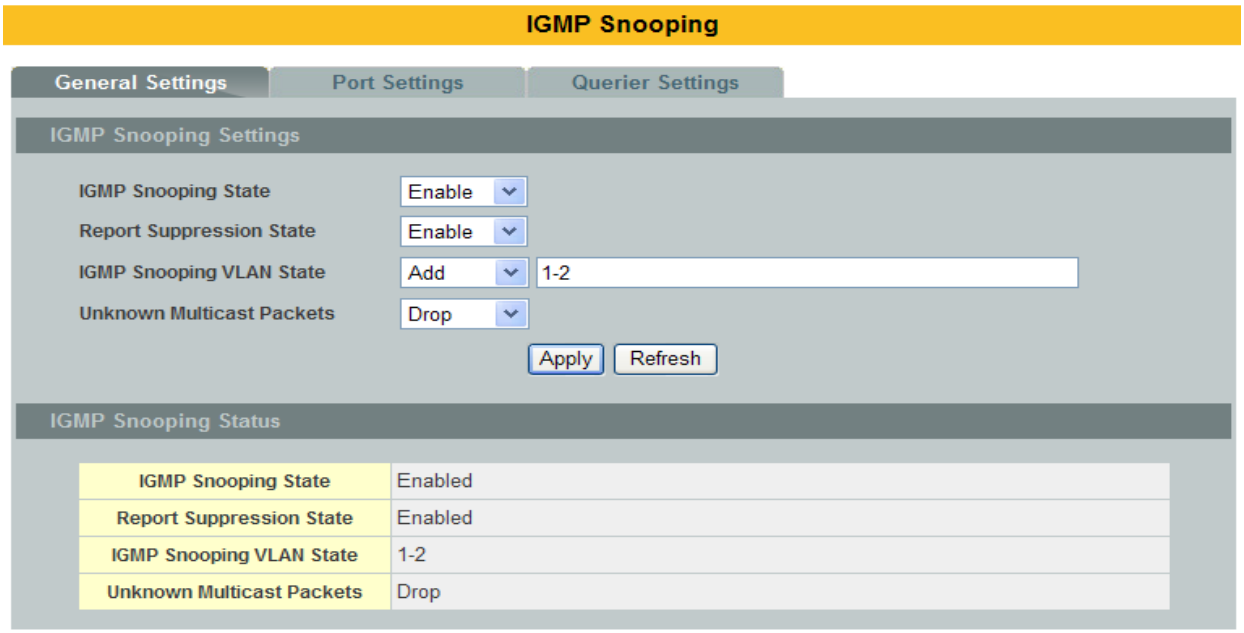
| | | |
|---|---|---|
| if-range | igmp-snooping group-limit VALUE | This command configures the maximum groups for the specific ports. |
| if-range | no igmp-snooping group-limit | This command removes the limitation of the maximum groups for the specific ports. |
| if-range | igmp-querier-mode (auto\|fixed\|edge) | 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)#*igmp-snooping* querier *enable*
L2SWITCH(config)#*igmp-snooping* querier *vlan 1*
L2SWITCH(config)#*interface 1/0/1*
L2SWITCH(config-if)#*igmp-immediate-leave*
L2SWITCH(config-if)#igmp-querier-mode fixed
L2SWITCH(config-if)#igmp-snooping group-limit 20

### 6.2.1.3. Web Configuration

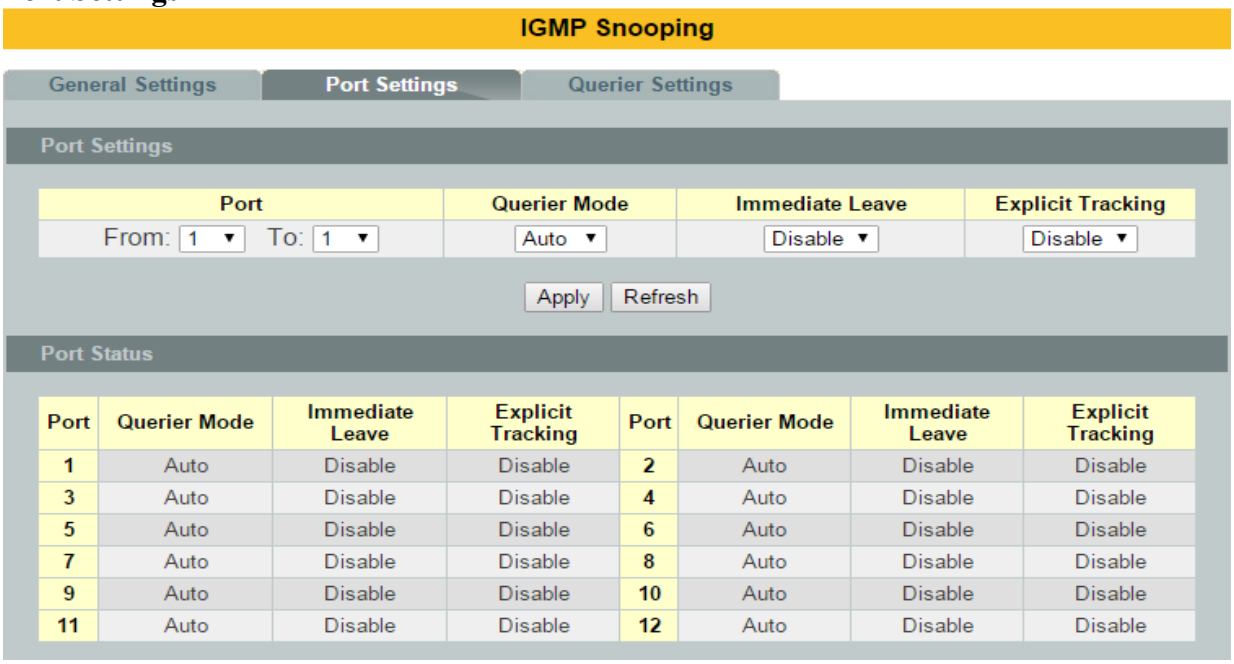
**General Settings**




| 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. |

| | |
|---|---|
| Report Suppression State | Select **Enable/Disable** to activate/deactivate IGMP Snooping report suppression function. |
| IGMP Snooping VLAN State | Select **Add** and enter VLANs upon which the Switch is to perform IGMP snooping. The valid range of VLAN IDs is between 1 and 4094. Use a comma (,) or hyphen (-) to specify more than one VLANs. Select **Delete** and enter VLANs on which to have the Switch not perform IGMP snooping. |
| Unknown Multicast Packets | Specify the action to perform when the Switch receives an unknown multicast frame. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports. |
| Apply | Click Apply to configure the settings. |
| Refresh | Click this to reset the fields to the last setting. |
| IGMP Snooping State | This field displays whether IGMP snooping is globally enabled or disabled. |
| Report Suppression State | This field displays whether IGMP snooping report suppression is enabled or disabled. |
| IGMP Snooping VLAN State | This field displays VLANs on which the Switch is to perform IGMP snooping. None displays if you have not enabled IGMP snooping on any port yet. |
| Unknown Multicast Packets | This field displays whether the Switch is set to discard or flood unknown multicast packets. |

**Port Settings**




| 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 |

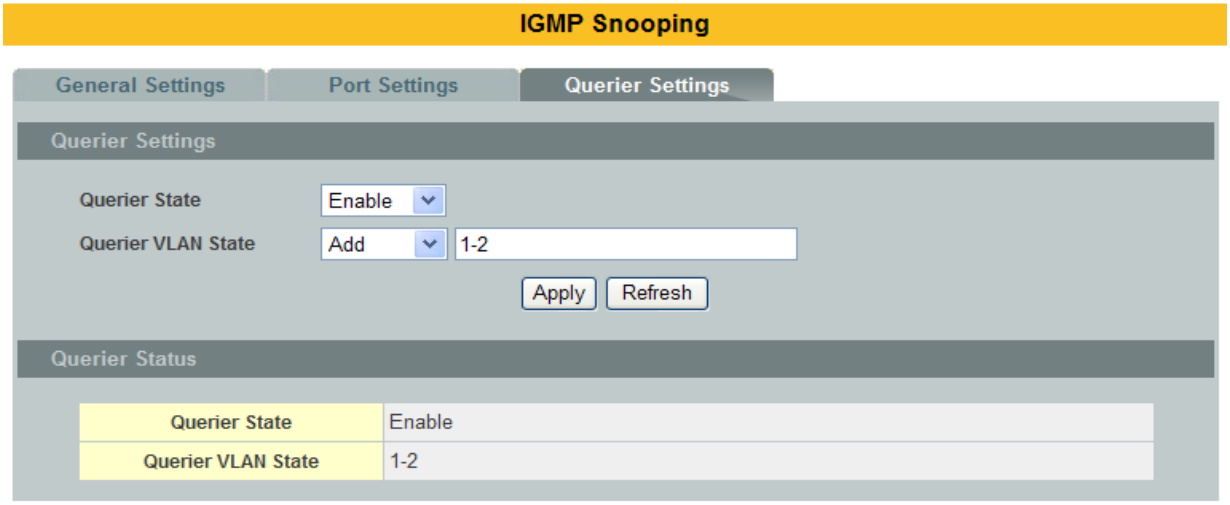
| | |
|---|---|
| | query packets. **Fixed** means the Switch always treats the port(s) as IGMP query port(s). This is for when connecting an IGMP multicast server to the port(s). **Edge** means the Switch does not use the port as an IGMP query port. In this case, the Switch does not keep a record of 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. IGMP Snooping Querier

#### 6.2.2.1. CLI Configurations

| Node | Command | Description |
|---|---|---|
| configure | igmp-snooping querier (disable \| enable) | This command disables / enables the IGMP snooping querier on the Switch. |
| configure | igmp-snooping querier vlan VLANIDs | This command enables the IGMP snooping querier function on a VLAN or range of VLANs. |
| configure | no igmp-snooping querier vlan VLANIDs | This command disables the IGMP snooping querier function on a VLAN or range of VLANs. |

#### 6.2.2.2. Web Configurations




| Parameter | Description |
|---|---|
| Querier State | This field configures the global Querier state. |
| Querier VLAN State | This field enables the Querier state in a vlan or a range of vlan. |
| Apply | Click Apply to apply the settings. |
| Refresh | Click this to reset the fields to the last setting. |
| Querier State | This filed indicates the current global Querier status. |
| Querier VLAN State | This field indicates the Querier status in vlan. |

### 6.2.3. IGMP Snooping Filtering

The IGMP Snooping Filter allows users to configure one or some of range or multicast address to drop or to forward them.

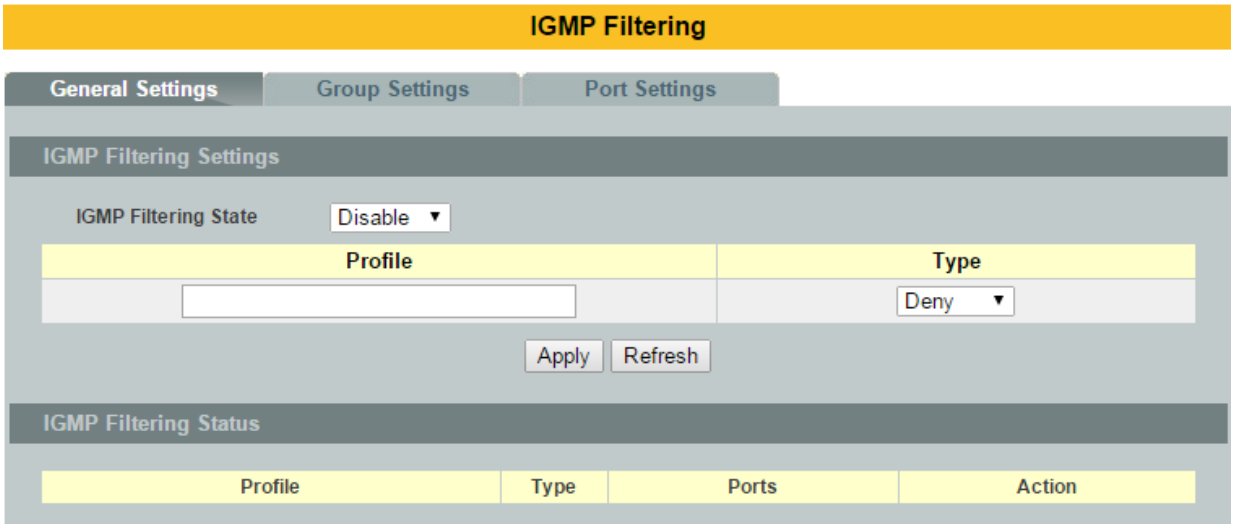
#### 6.2.3.1. CLI Configurations

| Node | Command | Description |
|---|---|---|
| enable | show igmp-snooping filtering | This command displays the IGMP snooping filtering configurations. |
| configure | igmp-snooping filtering (enable\|disable) | This command enables/disables the IGMP snooping filtering profiles on the Switch. |
| configure | igmp-snooping filtering profile | This command enters the IGMP snooping filtering profiles configuration node. |
| configure | no igmp-snooping | This command removes all of the IGMP snooping |

| | | |
|---|---|---|
| | filtering all | filtering profiles from the Switch. |
| configure | no igmp-snooping filtering STRINGS | This command removes the IGMP snooping filtering profiles by name from the Switch. |
| config-igmp | Group GROUP_ID start-address START-ADDR end-address END-ADDR | This command configures the group configurations, including group index and start multicast address and end multicast address. |
| config-igmp | type (deny\|permit) | This command configures the type of deny or permit for the group. |
| config-igmp | no group GROUP-ID | This command removes the group configurations. |
| config-igmp | no group all | This command removes all of the group configurations. |
| config-igmp | type (deny\|permit) | This command configures the type of deny or permit for the group. |
| interface | igmp-snooping filtering profile STRING | This command enables the IGMP snooping filtering profiles on the specific port. |
| interface | no igmp-snooping filtering profile STRINGS | This command disables the IGMP snooping filtering profiles on the specific port. |
| configure | interface range gigabitethernet1/0/ PORTLISTS | This command enters the interface configure node. |
| if-config | igmp-snooping filtering profile STRING | This command enables the IGMP snooping filtering profiles on the range of ports. |
| if-config | no igmp-snooping filtering profile STRINGS | This command disables the IGMP snooping filtering profiles on the range of ports. |

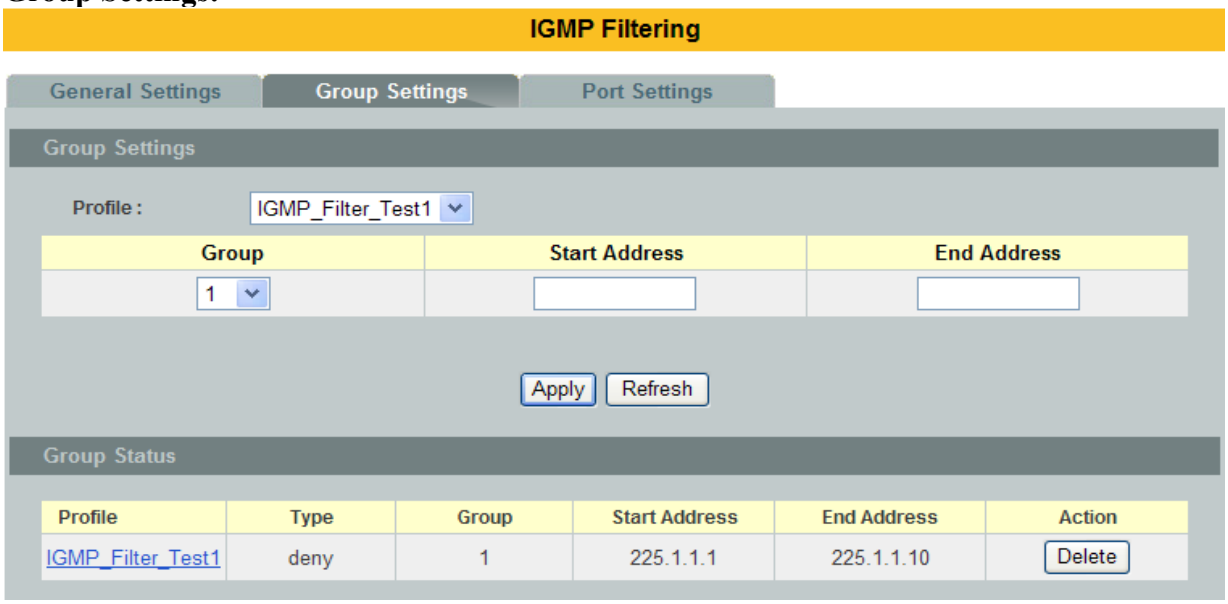
#### 6.2.3.2. Web Configurations

**General Settings:**



| Parameter | Description |
|---|---|
| IGMP Filtering State | This field configures the global IGMP Filtering state. |
| Profile | This field creates the IGMP Filtering profile. |
| Type | The field configures the type of action for the profile. |
| Apply | Click Apply to apply the settings. |
| Refresh | Click this to reset the fields to the last setting. |
| IGMP Filtering Status | |
| Profile | The profile name. |
| Type | The type of action. |
| Ports | The field indicates the ports that the IGMP Filtering profile is activated. |
| Action | Click the “Delete” button to delete the profile. |

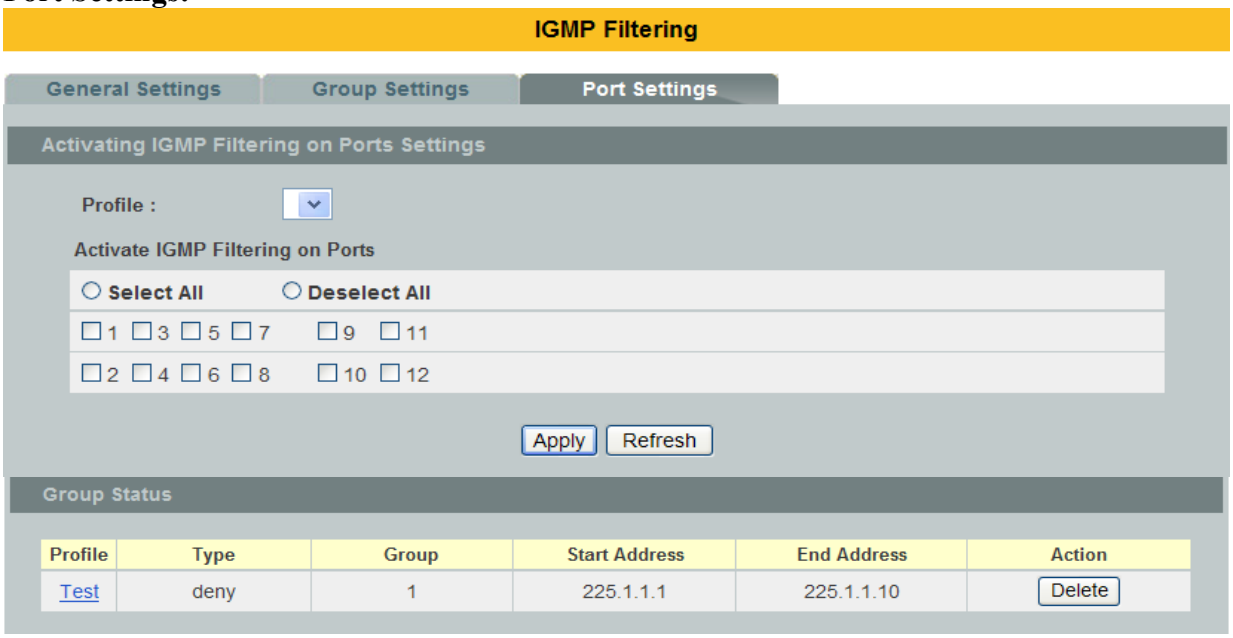
**Group Settings:**




| Parameter | Description |
|---|---|
| Profile | This field selects the profile which you want to configure the group. |
| Group | This field selects the group index. |
| Start Address | The field configures the first multicast address of the group. |
| End Address | The field configures the last multicast address of the group. |

| | |
|---|---|
| Apply | Click Apply to apply the settings. |
| Refresh | Click this to reset the fields to the last setting. |

**Port Settings:**




| Parameter | Description |
|---|---|
| Profile | This field selects the profile which you want to activate on the ports. |
| Activate IGMP Filtering on Ports | Selects the ports which you want to activate the IGMP Filtering profile. |
| Apply | Click Apply to apply the settings. |
| Refresh | Click this to reset the fields to the last setting. |

### 6.2.4. MVR

#### 6.2.4.1. Introduction

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

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

**MVR Mode**

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

**Operation Mode**

- **Join Operation:**
  A subscriber sends an IGMP report message to the switch to join the appropriate multicast. The next depends on whether the IGMP report matches the switch configured multicast MAC address. If it matches, the switch CPU modifies the hardware address table to include this receiver port and VLAN as a forwarding destination of MVLAN.

- **Leave Operation:**
  Subscriber sends an IGMP leave message to the switch to leave the multicast. The switch CPU sends an IGMP group-specific query through the receiver port VLAN. If there is another subscriber in the VLAN, subscriber must respond within the max response time. If there is no subscriber, the switch would eliminate this receiver port.

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

**Figure-1:**

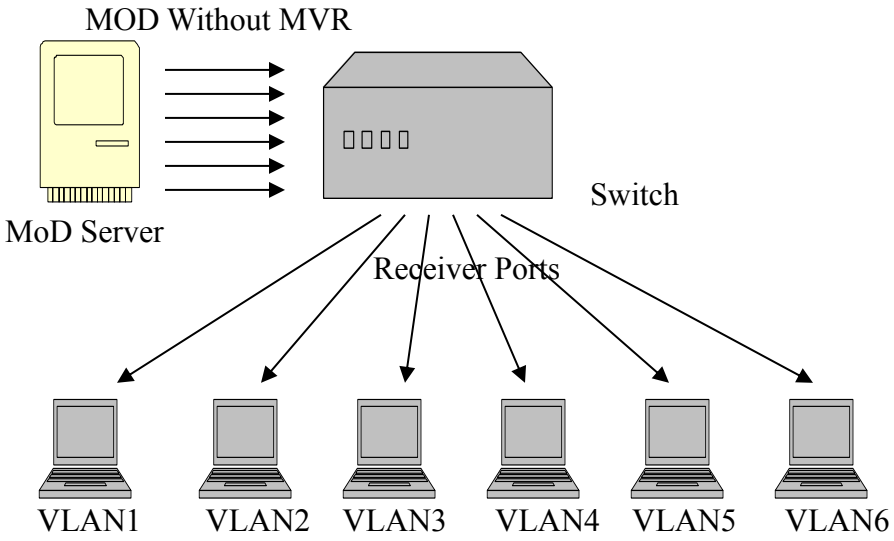
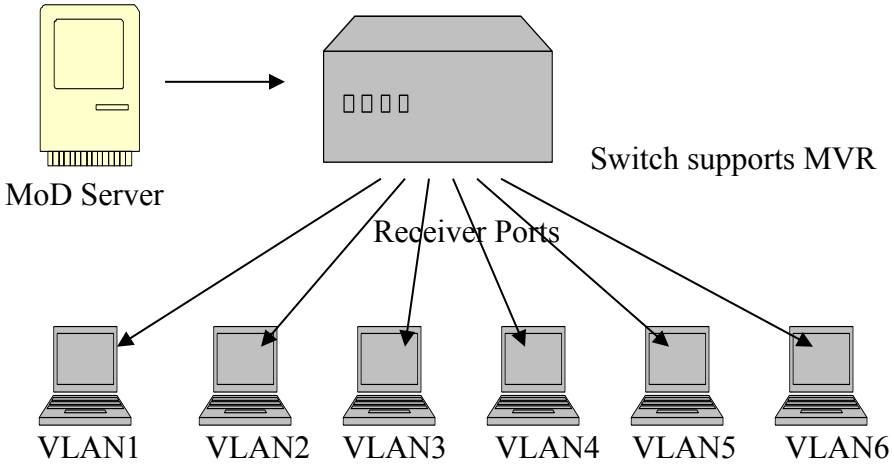



**Figure-2:**

MOD Support MVR




**Default Settings**

There is no MVR vlan.

Default configuration for a new MVR:

MVR VLAN Information

| | |
|---|---|
| VLAN ID | : 2 |
| Name | : MVR2 |
| Active | : Enabled |
| Mode | : Dynamic |
| Source Port(s) | : None |
| Receiver Port(s) | : None |
| Tagged Port(s) | : None |

The Switch allows user to create up to 250 groups.

The Switch allows user to create up to 16 MVRs.

**Notices**

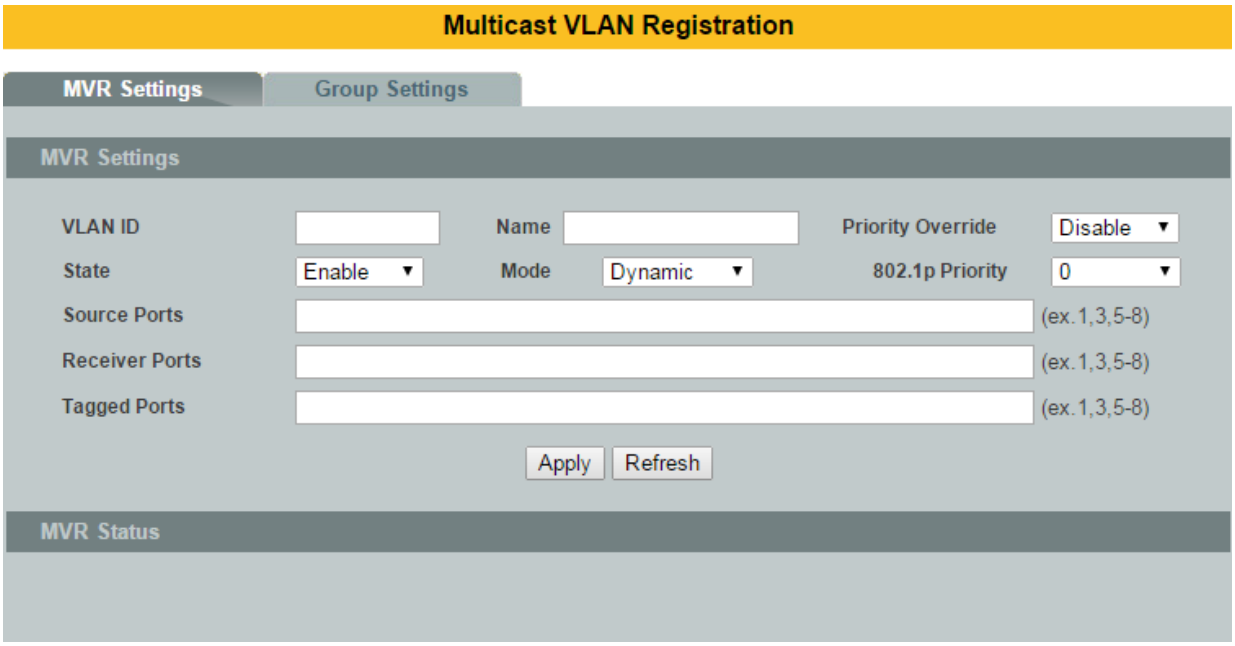
- IGMP snooping and MVR can be independently enabled.
- IGMP snooping and MVR use the same IGMP timers.
- MVR can recognize IGMPv3 reports.
- About the IGMPv3 report, switch doesn't treat those group records with the following group record types as membership reports. Those group record types are MODE_IS_INCLUDE,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

### 6.2.4.2. CLI Configuration

| Node | Command | Description |
|---|---|---|
| enable | show mvr | This command displays the current MVR configurations. |
| enable | show mvr vlan VLANID | This command displays the current MVR configurations of the specific VLAN. |
| enable | show igmp-snooping | This command displays the current IGMP snooping configurations. |
| configure | mvr VLANID | This command configures the MVR configurations for the specific VLAN. |
| configure | no mvr VLANID | This command disables the MVR configurations for the specific VLAN. |
| MVR | group NAME | This command configures a group configuration for the MVR. |
| MVR | no group NAME | This command removes the group configurations from the MVR. |
| MVR | inactive | This command disables the MVR settings. |
| MVR | no inactive | This command enables the MVR settings. |
| MVR | mode (dynamic\|compatible) | This command configures the mode for the MVR.<br>● Dynamic : Sends IGMP report to all MVR source ports in the multicast VLAN.<br>● Compatible : Sets the Switch not to send IGMP report. |
| MVR | name STRING | This command configures the name for the MVR. |
| MVR | no name | This command configures the default name for the MVR. |
| MVR | receiver-port PORTLIST | This command sets the receiver port(s). Normally the source ports are connected to the streaming client. |
| MVR | no receiver-port PORTLIST | This command removes a port or range of ports from the receiver port(s). |
| MVR | source-port PORTLIST | This command sets the source port(s). Normally the source ports are connected to the streaming server. |
| MVR | no source-port PORTLIST | This command removes a port or range of ports from the source port(s). |
| MVR | tagged PORTLIST | This command sets the tagged port(s). Same as the VLAN tagged port. |
| MVR | no tagged PORTLIST | This command removes a port or range of ports from the tagged port(s). |
| MVR | priority-override (disable\|enable) | This command enables/disables the multicast priority override. |

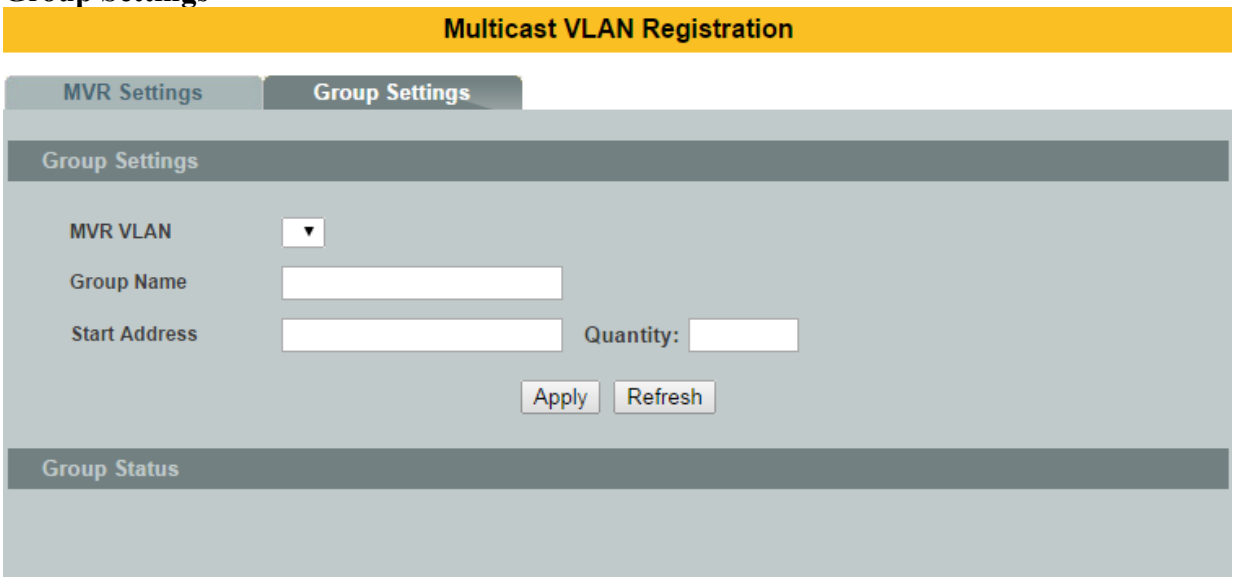
### 6.2.4.3. Web Configuration

**MVR Settings**




| Parameter | Description |
|---|---|
| VLAN ID | Configures a VLAN. |
| NAME | Configures a name for the MVR. |
| Priority Override | Enable / Disable for the priority override. |
| State | Enables / Disables the MVR. |
| Mode | Configures the mode for the MVR. |
| 802.1p Priority | The priority for these multicast group packets. |
| Source Ports | Configures the source port(s) for the MVR. Normally the source ports are connected to the streaming server. |
| Receive Ports | Configures the receive port(s) for the MVR. Normally the source ports are connected to the streaming client |
| Tagged Ports | Configures the tagged port(s) for the MVR. Same as the VLAN tagged port. |

**Group Settings**




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

### 6.2.5. Multicast Address

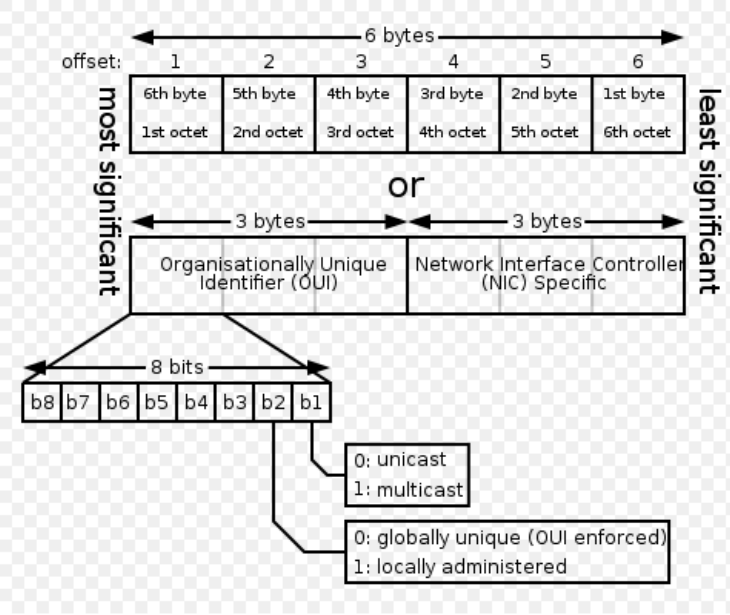
#### 6.2.5.1. Introduction

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. |



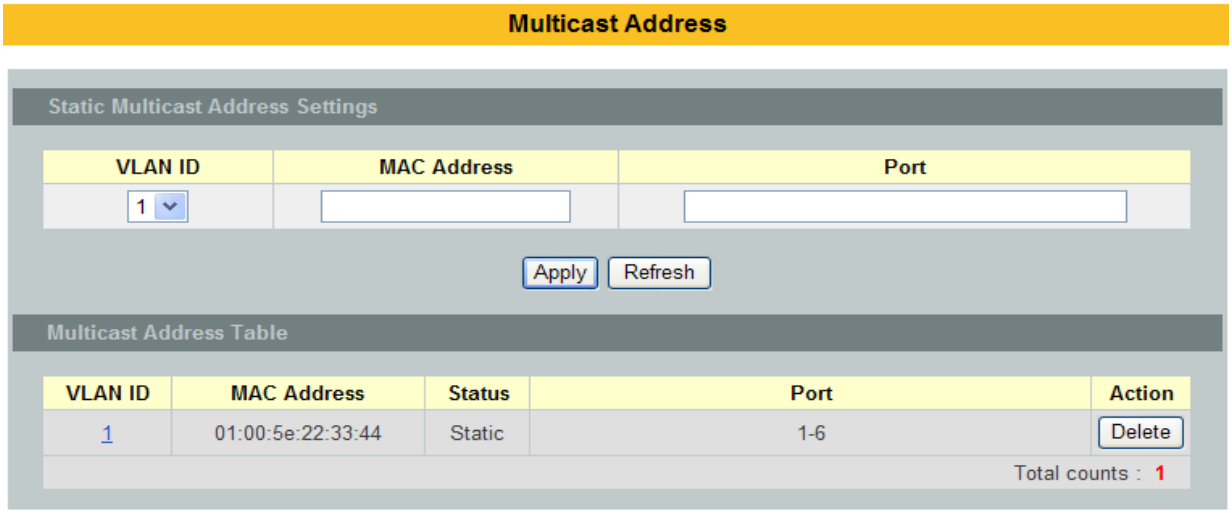

| IP multicast address | Description |
|---|---|
| 224.0.0.0 | Base address (reserved) |
| 224.0.0.1 | The All Hosts multicast group that contains all systems on the same network segment |
| 224.0.0.2 | The All Routers multicast group that contains all routers on the same network segment |
| 224.0.0.5 | 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 |

### 6.2.5.2. 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 VLANID | This command displays the current static/dynamic multicast address entries with a specific vlan. |
| configure | mac-address-table multicast MACADDR vlan VLANID 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. |

### 6.2.5.3. Web Configuration




| Parameter | Description |
|---|---|

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

### 6.2.6. Explicit Host Tracking

This capability enables the Switch to track each individual host that is joined to a particular group or channel and to achieve minimal leave latencies when hosts leave a multicast group or channel.

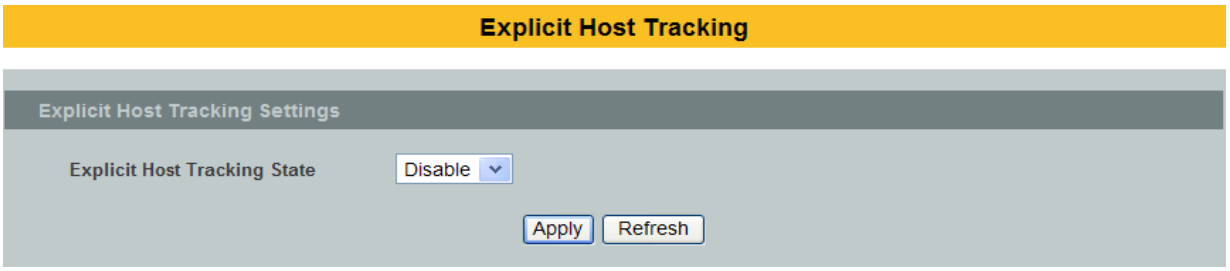
**Notice:**

- ✓ Before configuring the ip igmp explicit-tracking command, IGMP must be enabled.
- ✓ When explicit host tracking is enabled, the router uses more memory than if explicit tracking is disabled because the router must store the membership state of all hosts on the interface.

#### 6.2.6.1. CLI Configurations

| Node | Command | Description |
|---|---|---|
| enable | show ip multicast | This command shows the IGMP snooping membership information. |
| enable | show igmp-snooping membership | This command shows the IGMP snooping host membership information. |
| configure | igmp-snooping explicit-tracking | This command enables the IGMP snooping explicit host tracking on the Switch. |
| configure | no igmp-snooping explicit-tracking | This command disables the IGMP snooping explicit host tracking on the Switch. |

#### 6.2.6.2. Web Configurations




| Parameter | Description |
|---|---|
| Explicit Tracking state | The filed enables/disables the IGMP Snooping explicit host tracking state on the Switch. |
| IGMP Snooping Membership Table | |

| | |
|---|---|
| Index | This field indicates the index of the entry. |
| Port | This field indicates the port of the entry. |
| Multicast Group | This field indicates the multicast address of the entry. |
| VID | This field indicates the vlan of the entry. |
| Timeout | This field indicates the remaining time in the table of the entry. |
| Host IP | This field indicates the host IP which joins the 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
```

#### 6.3.1.2. CLI Configuration

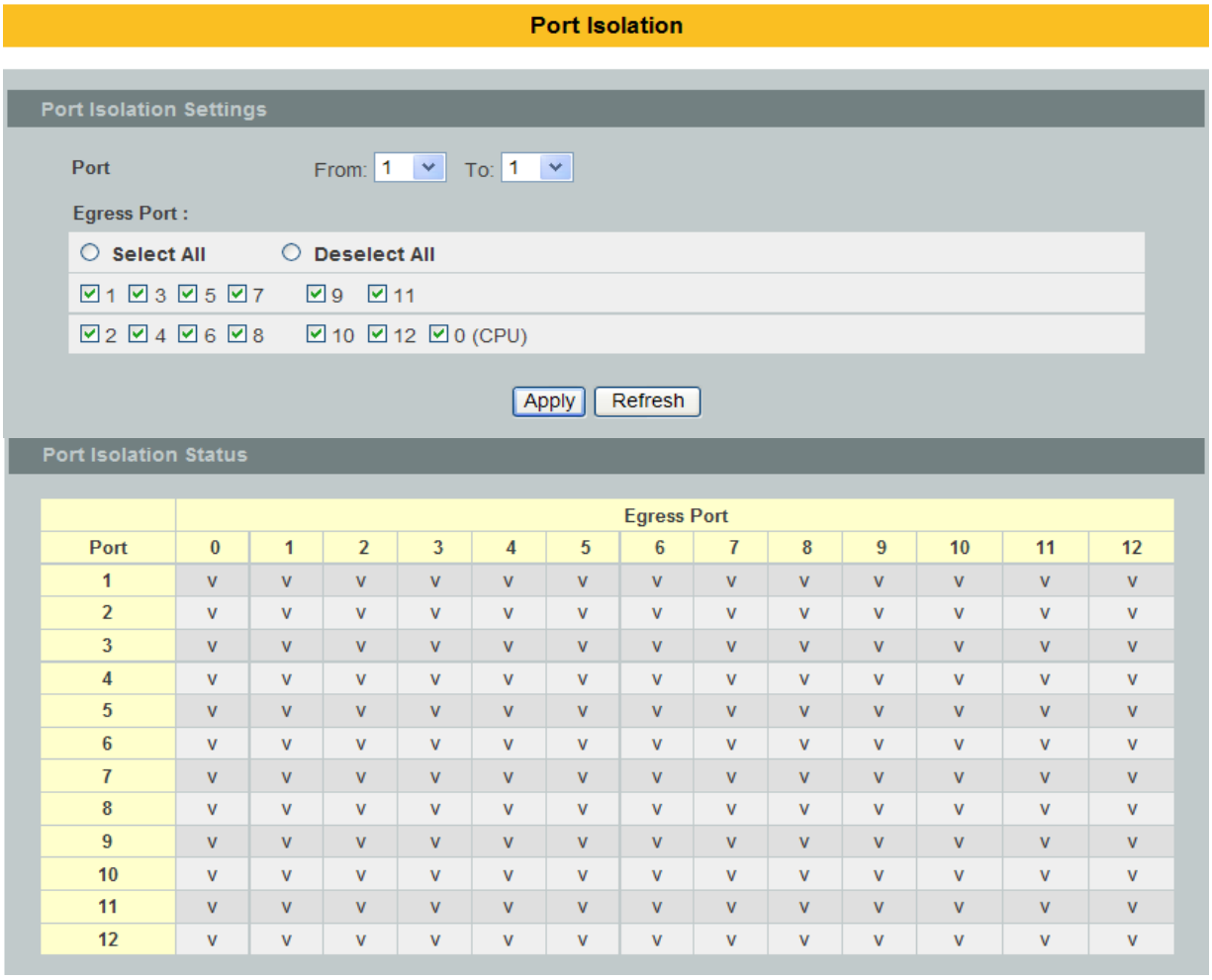
| Node | Command | Description |
|---|---|---|
| enable | show port-isolation | This command displays the current port isolation configurations.<br>"V" indicates the port's packets can be sent to that port. |

| | | |
|---|---|---|
| | | "-" indicates the port's packets cannot be sent to that port. |
| interface | port-isolation ports PORTLISTS | This command configures a port or a range of ports to egress traffic from the specific port. |
| interface | no port-isolation | This command configures all ports to egress traffic from the specific port. |

**Example:**

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

### 6.3.1.3. Web Configuration




| Parameter | Description |
|---|---|
| Port | Select a port number to configure its port isolation settings.<br>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.<br>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.<br>Click **Deselect All** to unmark all ports and isolate them.<br>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.<br>"-" 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.

**Notice:** The maximum VLAN group is 4094.

#### 6.3.2.2. CLI Configuration

| Node | Command | Description |
|---|---|---|
| enable | show vlan VLANID | This command displays the VLAN configurations. |

| | | |
|---|---|---|
| configure | vlan <1~4094> | This command enables a VLAN and enters the VLAN node. |
| configure | no vlan <1~4094> | This command deletes a VLAN. |
| vlan | show | This command displays the current VLAN configurations. |
| vlan | 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 adds 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.<br>all - acceptable all frame types.<br>tagged - acceptable tagged frame only.<br>untagged – acceptable untagged frame only. |
| interface | pvid VLANID | 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 VLANID | 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. |

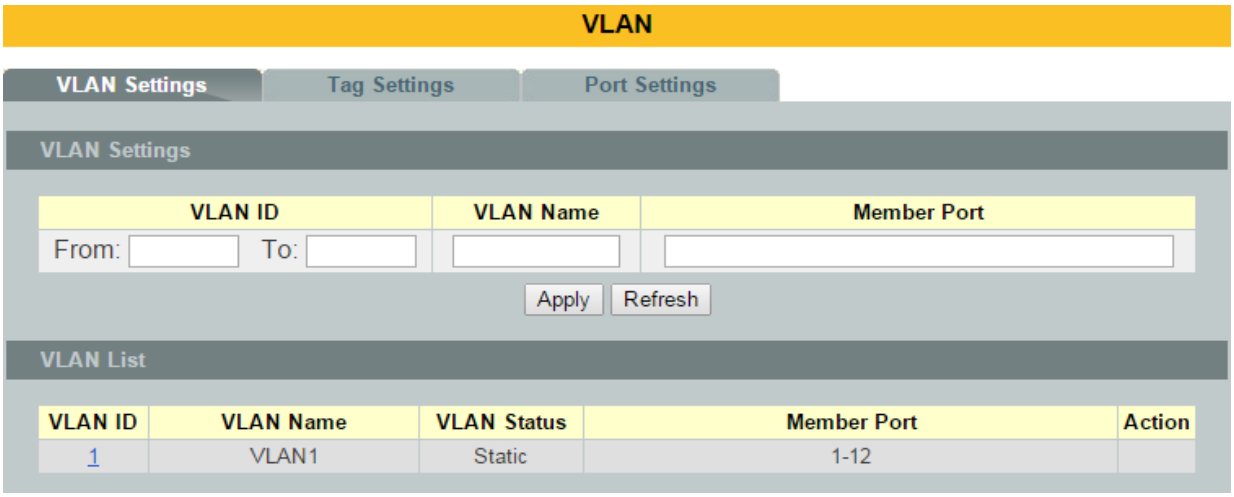
| | | |
|---|---|---|
| vlan-range | add PORTLISTS | This command adds a port or a range of ports to the vlans. |
| vlan-range | fixed PORTLISTS | This command assigns ports for permanent member of the VLAN group. |
| vlan-range | no fixed PORTLISTS | This command removes all fixed member from the vlans. |
| 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 1-6
L2SWITCH(config-vlan)#untagged 1-3
```

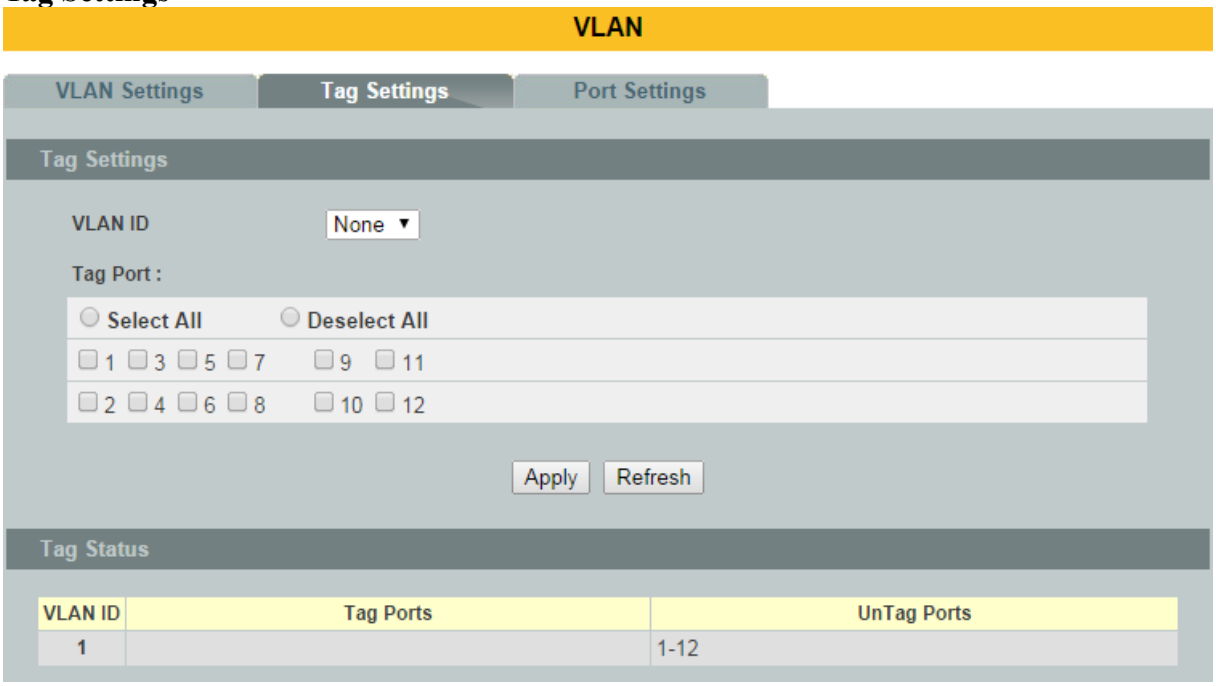
### 6.3.2.3. Web Configuration

**VLAN Settings**



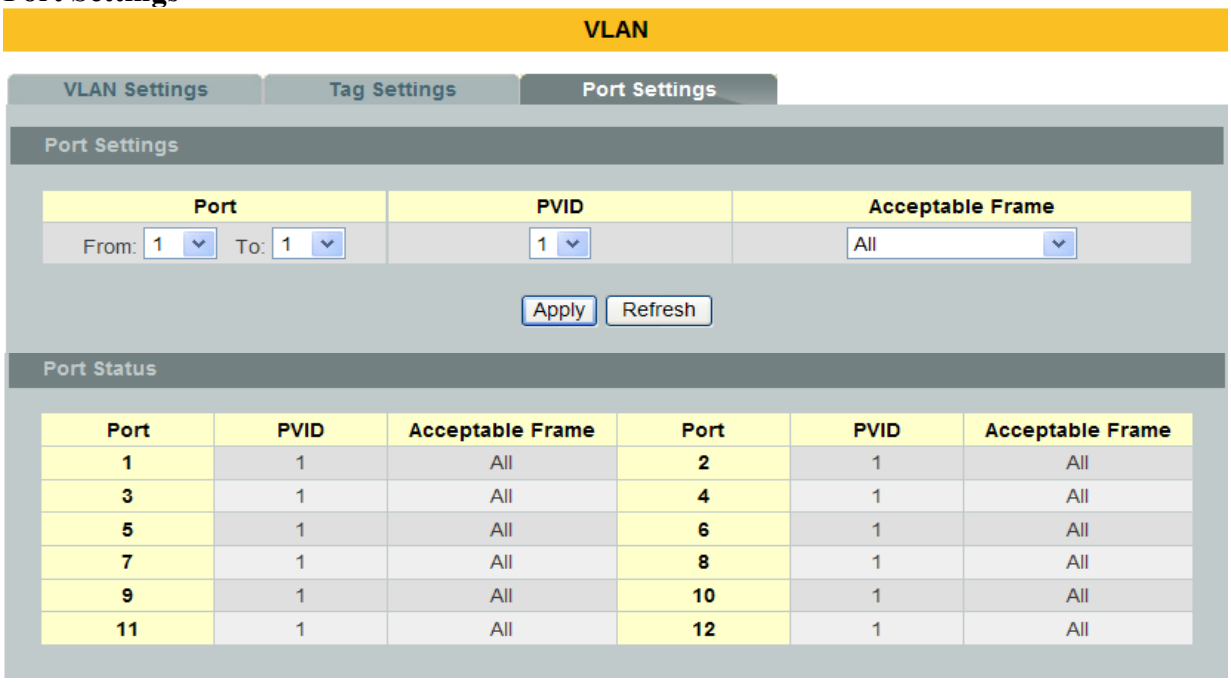

| Parameter | Description |
|---|---|
| VLAN ID | Enter the VLAN ID for this entry; the valid range is between 1 and 4094. |
| VLAN Name | Enter a descriptive name for the VLAN for identification purposes. The VLAN name should be the combination of the digit or the alphabet or hyphens (-) or underscores (_).<br>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.<br>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**.<br>- Select **All** from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting.<br>- Select **VLAN Tagged Only** to accept only tagged frames on this port. All untagged frames will be dropped.<br>- 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. GARP/GVRP

#### 6.3.3.1. Introduction

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

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

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

In other words, GVRP allows the propagation of VLAN information from device to device. With GVRP, a single switch is manually configured with all the desired VLANs for the network, and all other switches on the network learn those VLANs dynamically. An end-node can be plugged into any switch and be connected to that end-node's desired VLAN. For end-nodes to make use of GVRP, they need GVRP-aware Network Interface Cards (NICs). The GVRP-aware NIC is configured with the desired VLAN or VLANs, then connected to a GVRP-enabled switch. The NIC communicates with the switch, and VLAN connectivity is established between the NIC and switch.

**Registration Mode:**

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

**GVRP Timer:**

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

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

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

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

**Default Settings**

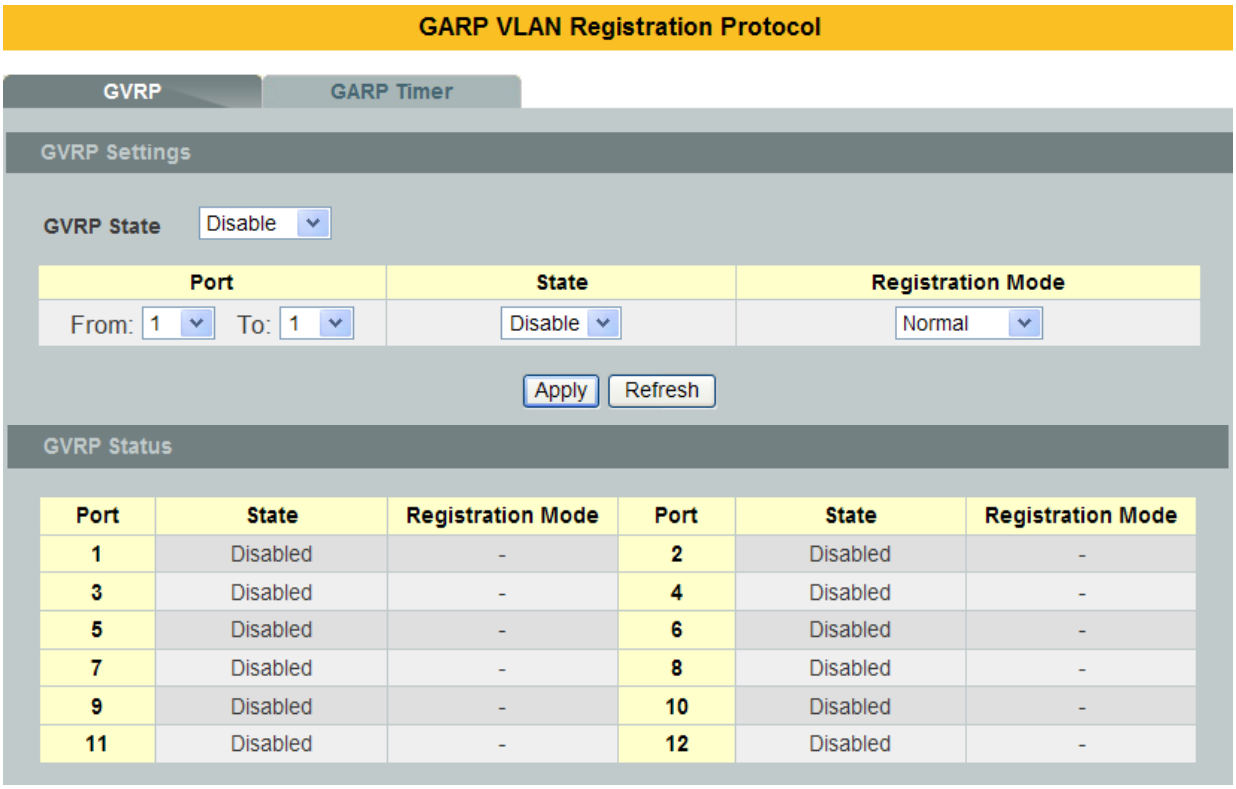
The default port Join Time is 20 for all ports.
The default port Leave Time is 60 for all ports.
The default port Leaveall Time is 1000 for all ports.
The default port Hold Time is 10 for all ports.

#### 6.3.3.2. CLI Configuration

| Node | Command | Description |
|---|---|---|
| enable | show gvrp configuration | This command displays the GVRP configurations. |
| enable | show gvrp statistics | This command displays the GVRP configurations on a port or all ports. |
| enable | show garp timer | This command displays the timers for the GARP. |
| configure | gvrp (disable \| enable) | This command disables / enables the GVRP on the switch. |
| configure | no gvrp configuration | This command set GVRP configuration to its defaults. |
| interface | gvrp (disable \| enable) | This command disables / enables the GVRP on the specific port. |
| interface | gvrp registration (normal\|forbidden) | This command configures the registration mode for the GVRP on the specific port. |
| interface | no gvrp configuration | This command set GVRP configuration to its defaults for the specific port. |
| interface | garp join-time VALUE leave-time VALUE leaveall-time VALUE | This command configures the join time / leaves time / leave all time for the GARP on the specific port. |
| interface | no garp time | This command configures the join time / leaves time / leaves all time to default for the GARP on the specific port. |

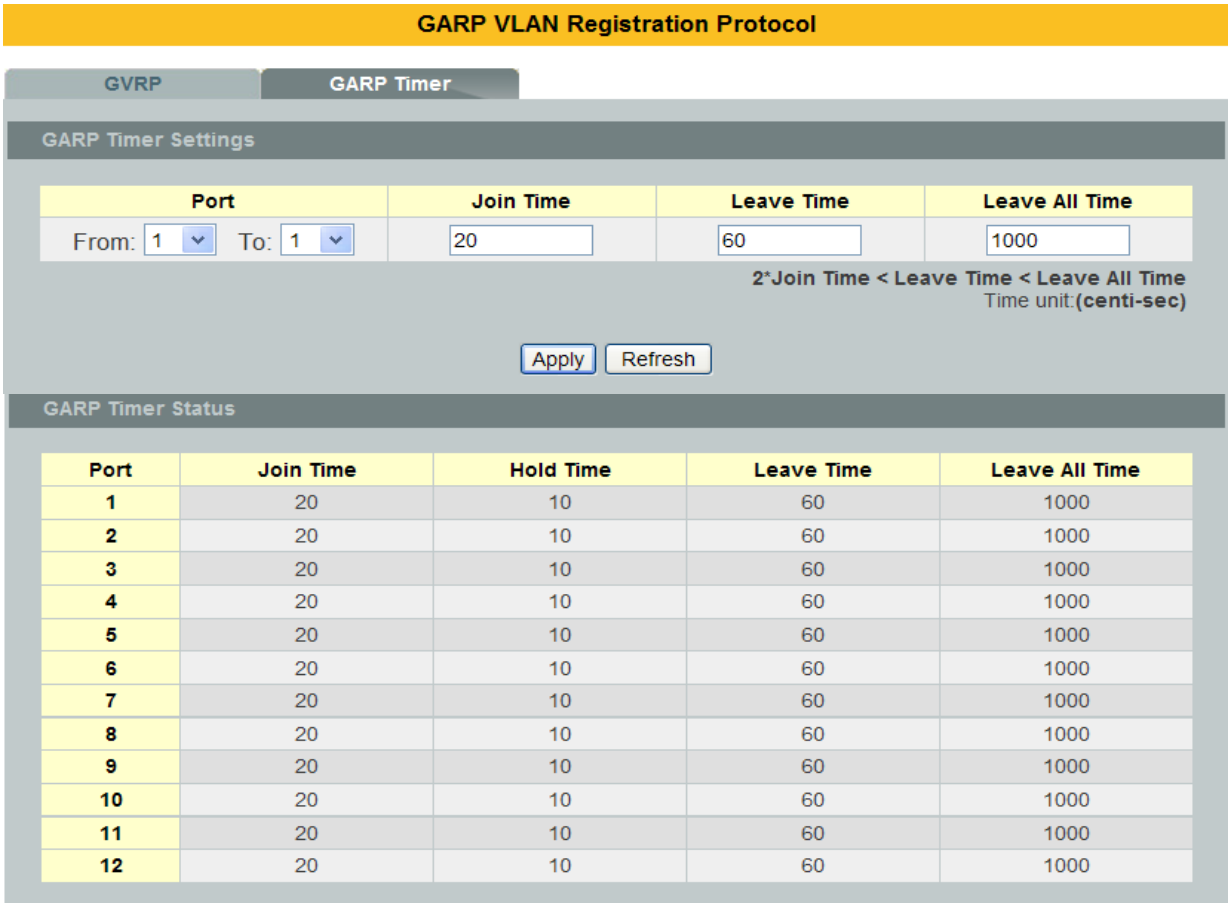
### 6.3.3.3. Web Configuration

**GVRP Settings**




| Parameter | Description |
|---|---|
| GVRP State | Select **Enable** to activate GVRP function to exchange VLAN configuration information with other GVRP switches. Select **Disable** to deactivate the feature. |
| Port | Select the port that you want to configure the GVRP settings. |
| State | Select **Enable** to activate the port GVRP function. Select **Disable** to deactivate the port GVRP function. |
| Registration Mode | Select **Normal** to allows dynamic creation (if dynamic VLAN creation is enabled), registration, and deregistration of VLANs on the trunk port. Select **Forbidden** to deregister all VLANs (except VLAN 1) and prevents any further VLAN creation or registration on the trunk port. |

**GARP Timer**




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

### 6.3.4. MAC-based VLAN

#### 6.3.4.1. 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.

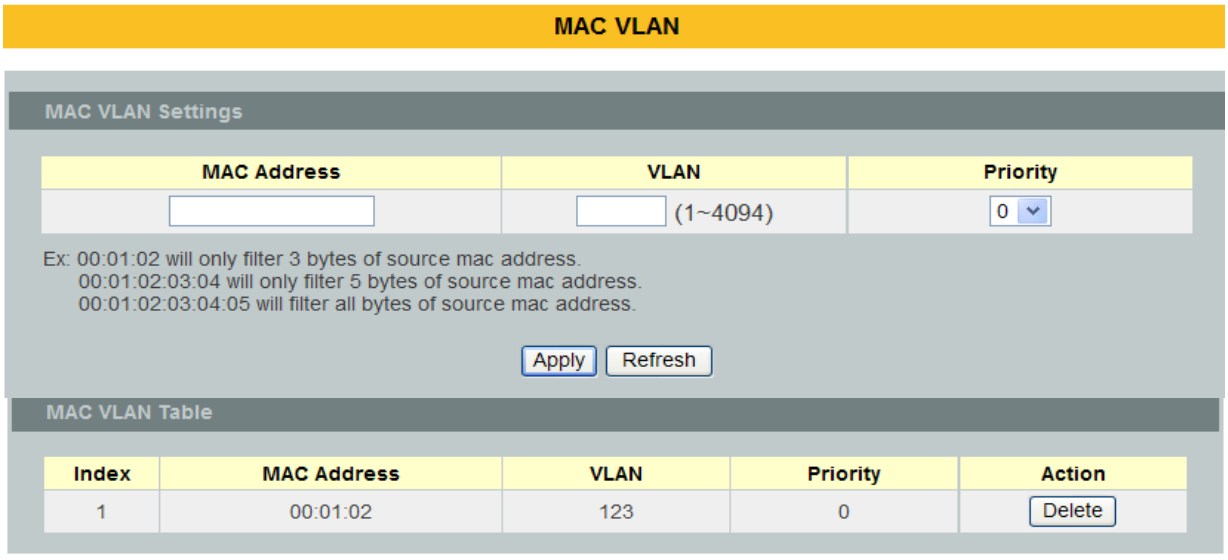
#### 6.3.4.2. CLI Configuration

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

**Example:**

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

#### 6.3.4.3. 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. |

### 6.3.5. Protocol-based VLAN

#### 6.3.5.1. Introduction

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

When the user configures the protocol VLAN as LLC-SNAP, VLAN:22, ports list: 1-3.
If the Switch receives packets with LLC-SNAP frame type from port 1 to 3, the packets’ VLAN will be replaced with VLAN 22 and be forwarded to VLAN 22 member ports.

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

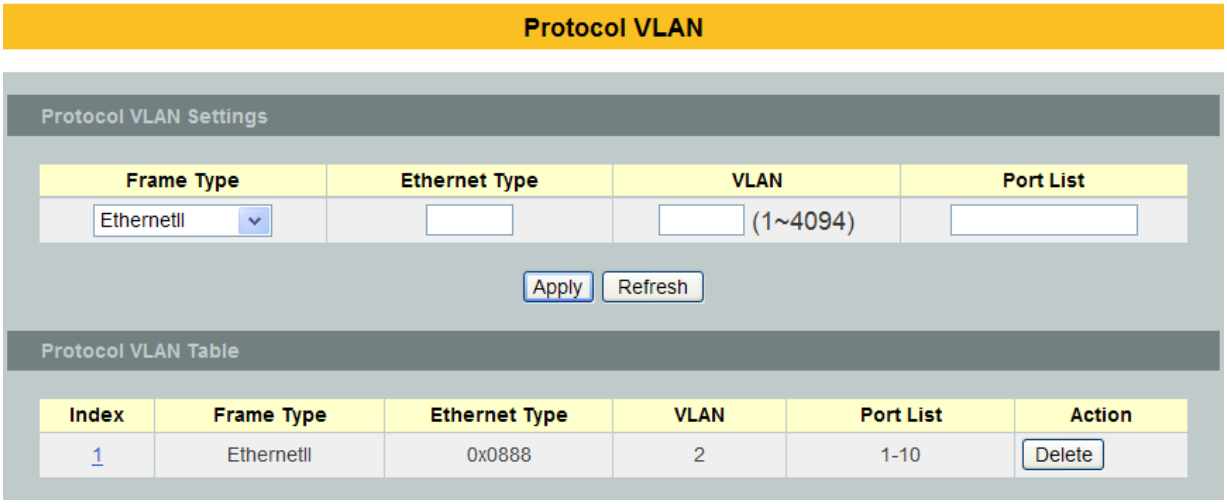
#### 6.3.5.2. CLI Configuration

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

**Example:**
L2SWITCH(config)#protocol-vlan frame-type LLC-SNAP vlan 12 ports 1-2

L2SWITCH(config)#protocol-vlan frame-type nonLLC-SNAP vlan 13 ports 3-4
L2SWITCH(config)#protocol-vlan frame-type ethernetII ether-type 0800 vlan 14 ports 1-2

#### 6.3.5.3. Web Configuration




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

### 6.3.6.Q-in-Q VLAN (VLAN Stacking)

#### 6.3.6.1. Introduction

Q-in-Q tunneling is also known as VLAN stacking. Both of them use 802.1q double tagging technology. Q-in-Q is required by ISPs (Internet Service Provider) that need Transparent LAN services (TLS), and the service provider has their own set of VLAN, independent of customer VLANs. Typically, each service provider VLAN interconnects a group of sites belonging to a customer. However, a service provider VLAN could also be shared by a set of customers sharing the same end points and quality of service requirements of the VLAN. Double tagging is considered to be a relatively simpler way of implementing transparent LAN. This is accomplished by encapsulating Ethernet Frame. A second or outer VLAN tag is inserted in Ethernet frames sent over the ingress PE (Provider Edge). This VLAN tag corresponds to the VLAN of the Service Provider (SP). When the frame reaches the destination PE, the SP VLAN is stripped off. The DA of the encapsulated frame and the VLAN ID are used to take further L2

decisions, similar to an Ethernet frame arriving from a physical Ethernet port. The SP VLAN tag determines the VPLS (Virtual Private LAN Service) membership. Double tagging aggregates multiple VLANs within another VLAN and provides a private, dedicated Ethernet connection between customers to reach their subnet transparently across multiple networks. Thus service providers can create their own VLANs without interfering with customer VLANs by using double tagging. This allows them to connect customers to ISPs and ASPs (Application Service Provider).

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

**Double Tagging Format**

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

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

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

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

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

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

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

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

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| tagged frame | | | l TPID | | | | | | Etype | a | |

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

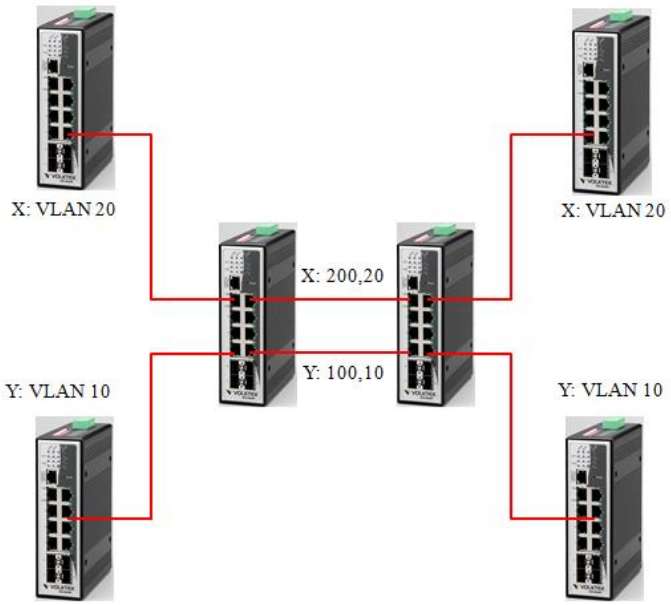
**VLAN Stacking Port Roles**
Each port can have three VLAN stacking "roles", Normal, Access Port and Tunnel Port.

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

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

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

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



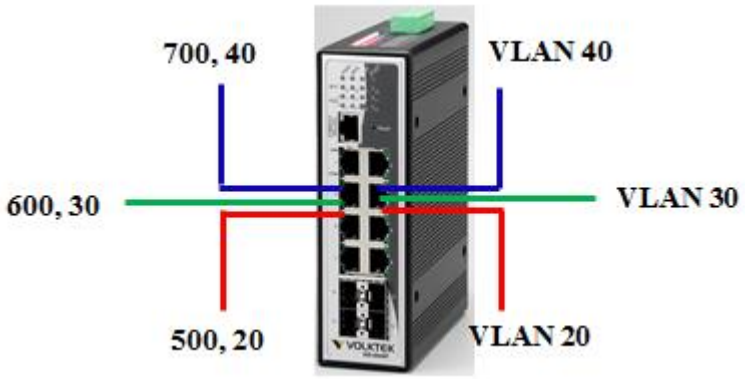

This example shows how to configure switch A with ports 1 on the Switch to tag incoming frames with the service provider's VID of 200 (ports are connected to customer X network) and configure port 7 to service provider's VID of 100 (ports are connected to customer Y network). This example also shows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

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

```
L2SWITCH(config-if)# vlan-stacking port-based role tunnel
L2SWITCH(config-if)# vlan-stacking tunnel-tpid index 2
L2SWITCH(config)# interface gigaethernet1/0/7
L2SWITCH(config-if)# vlan-stacking port-based role access
L2SWITCH(config-if)# vlan-stacking spvid 100
L2SWITCH(config-if)# vlan-stacking priority 4
L2SWITCH(config)# interface gigaethernet1/0/8
L2SWITCH(config-if)# vlan-stacking port-based role tunnel
L2SWITCH(config-if)# vlan-stacking tunnel-tpid index 2
L2SWITCH(config-if)# exite
L2SWITCH(config)# exit
L2SWITCH# show vlan-stacking
L2SWITCH# show vlan-stacking tpid-table
L2SWITCH# show vlan-stacking portbased-qinq
```

**Selective Q-in-Q**

The traffic based Q-in-Q is also called Selective Q-in-Q. Selective Q-in-Q allows the Switch to add different outer VLAN tags to the incoming frames received on one port according to their inner VLAN tags. In the Selective Q-in-Q mode, switch performs traffic classification for the traffic incoming to a port based on the VLAN ID. When a user uses different VLAN IDs for different services, traffic can be classified according to the VLAN ID. For example, the VLAN ID 20 for surfing on the internet by PC, VLAN ID 30 for IPTV and VLAN ID 40 for VIP customers. After receiving user data, the switch labels the traffic of surfing on the Internet by PC with 500 as a SPVID outer tag, IPTV with 600, and VIP customers with 700.




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

```
L2SWITCH(config)# vlan-stacking selective
L2SWITCH(config)# vlan-stacking tpid-table index 6 value 9100
L2SWITCH(config)# vlan 20
L2SWITCH(config-vlan)# fixed 3,4
L2SWITCH(config-vlan)# tagged 3
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan 30
L2SWITCH(config-vlan)# fixed 3,4
```

```
L2SWITCH(config-vlan)# tagged 3
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan 40
L2SWITCH(config-vlan)# fixed 3,4
L2SWITCH(config-vlan)# tagged 3
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan 500
L2SWITCH(config-vlan)# fixed 3,4
L2SWITCH(config-vlan)# tagged 4
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan 600
L2SWITCH(config-vlan)# fixed 3,4
L2SWITCH(config-vlan)# tagged 4
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan 700
L2SWITCH(config-vlan)# fixed 3,4
L2SWITCH(config-vlan)# tagged 4
L2SWITCH(config-vlan)# exit
L2SWITCH(config)# vlan-stacking selective-qinq rule1
L2SWITCH(config-qinq)# cvids 20
L2SWITCH(config-qinq)# priority 2
L2SWITCH(config-qinq)# spvid 500
L2SWITCH(config-qinq)# access-ports 3
L2SWITCH(config-qinq)# tunnel-ports 4
L2SWITCH(config-qinq)# active
L2SWITCH(config-qinq)# show
L2SWITCH(config-qinq)# exit
L2SWITCH(config)# vlan-stacking selective-qinq rule2
L2SWITCH(config-qinq)# cvids 30
L2SWITCH(config-qinq)# priority 5
L2SWITCH(config-qinq)# spvid 600
L2SWITCH(config-qinq)# access-ports 3
L2SWITCH(config-qinq)# tunnel-ports 4
L2SWITCH(config-qinq)# active
L2SWITCH(config-qinq)# show
L2SWITCH(config-qinq)# exit
L2SWITCH(config)# vlan-stacking selective-qinq rule3
L2SWITCH(config-qinq)# cvids 40
L2SWITCH(config-qinq)# priority 7
L2SWITCH(config-qinq)# spvid 700
L2SWITCH(config-qinq)# access-ports 3
L2SWITCH(config-qinq)# tunnel-ports 4
L2SWITCH(config-qinq)# active
L2SWITCH(config-qinq)# show
L2SWITCH(config-qinq)# exit
L2SWITCH(config)# interface interface 1/0/4
L2SWITCH(config-if)# vlan-stacking tunnel-tpid index 6
```

L2SWITCH(config-if)# exit
L2SWITCH(config)# exit
L2SWITCH# show vlan-stacking
L2SWITCH# show vlan-stacking tpid-table
L2SWITCH# show vlan-stacking selective-qinq

**Default Setting:** VLAN Stacking is disabled.

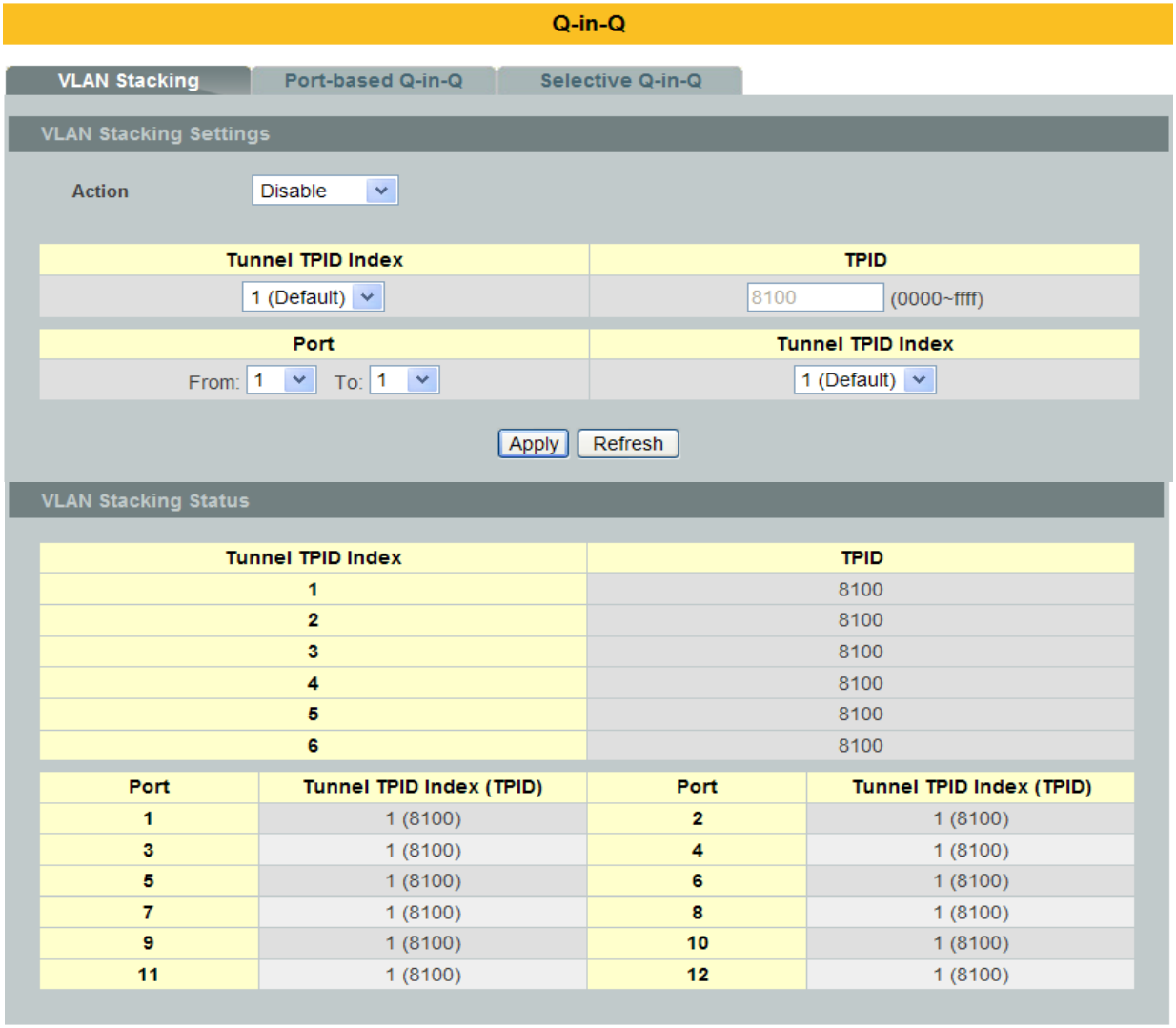
#### 6.3.6.2. CLI Configuration

| Node | Command | Description |
|---|---|---|
| enable | show vlan-stacking | This command displays the current vlan-stacking type. |
| enable | show vlan-stacking selective-qinq | This command displays the selective Q-in-Q configurations. |
| enable | show vlan-stacking portbased-qinq | This command displays the port-based q-in-Q configurations. |
| enable | show vlan-stacking tpid-inform | This command displays the TPID configurations. |
| configure | vlan-stacking (disable\|port-based\|selective) | This command disable the vlan stacking or enable the vlan-stacking with port-based or selective on the switch. |
| configure | vlan-stacking selective-qinq STRINGS | This command creates a selective Q-in-Q profile with the name. |
| configure | no vlan-stacking selective-qinq STRINGS | This command removes the selective Q-in-Q profile with the name. |
| configure | vlan-stacking tpid-table index <2-6> value STRINGS | This command configures TPID table. |
| interface | vlan-stacking port-based priority <0~7> | This command sets the priority in port based Q-in-Q. |
| interface | vlan-stacking port-based role (tunnel\|access\|normal) | This command sets VLAN stacking port role. |
| interface | vlan-stacking port-based spvid <1~4096> | This command sets the service provider's VID of the specified port. |
| interface | vlan-stacking tunnel-tpid index <1-6> | This command sets TPID for a Q-in-Q tunnel port. |
| configure | interface range gigabitethernet1/0/ ORTLISTS | This command enters the interface configure node. |
| if-range | vlan-stacking port-based priority <0~7> | This command sets the priority in port based Q-in-Q. |
| if-range | vlan-stacking port-based role (tunnel\|access\|normal) | This command sets VLAN stacking port role. |
| if-range | vlan-stacking port-based spvid <1~4096> | This command sets the service provider's VID of the specified port. |
| if-range | vlan-stacking tunnel-tpid | This command sets TPID for a Q-in-Q tunnel |

| | | |
|---|---|---|
| | index <1-6> | port. |
| qinq | active | This command enables the selective Q-in-Q profile. |
| qinq | inactive | This command disables the selective Q-in-Q profile. |
| qinq | cvid VLANID | This command specifies the customer's VLAN range on the incoming packets. |
| qinq | spvid VLANID | This command sets the service provider's VLAN ID for outgoing packets in selective Q-in-Q. |
| qinq | priority <0-7> | This command sets priority in selective Q-in-Q. |
| qinq | access-ports PORTLISTS | This command specifies the access ports to apply the rule. |
| qinq | tunnel-ports PORTLISTS | This command specifies the tunnel ports to apply the rule. |
| qinq | end | The command exits the CLI Q-in-Q node and enters the CLI enable node. |
| qinq | exit | The command exits the CLI Q-in-Q node and enter the CLI configure node. |
| qinq | show | The command shows the current selective Q-in-Q profile configurations. |
| configure | interface range gigabitethernet1/0/ PORTLISTS | This command enters the interface configure node. |
| if-range | vlan-stacking port-based priority <0~7> | This command sets the priority in port based Q-in-Q. |
| if-range | vlan-stacking port-based role (tunnel\|access\|normal) | This command sets VLAN stacking port role. |
| if-range | vlan-stacking port-based spvid <1~4096> | This command sets the service provider's VID of the specified port. |
| if-range | vlan-stacking tunnel-tpid index <1-6> | This command sets TPID for a Q-in-Q tunnel port. |

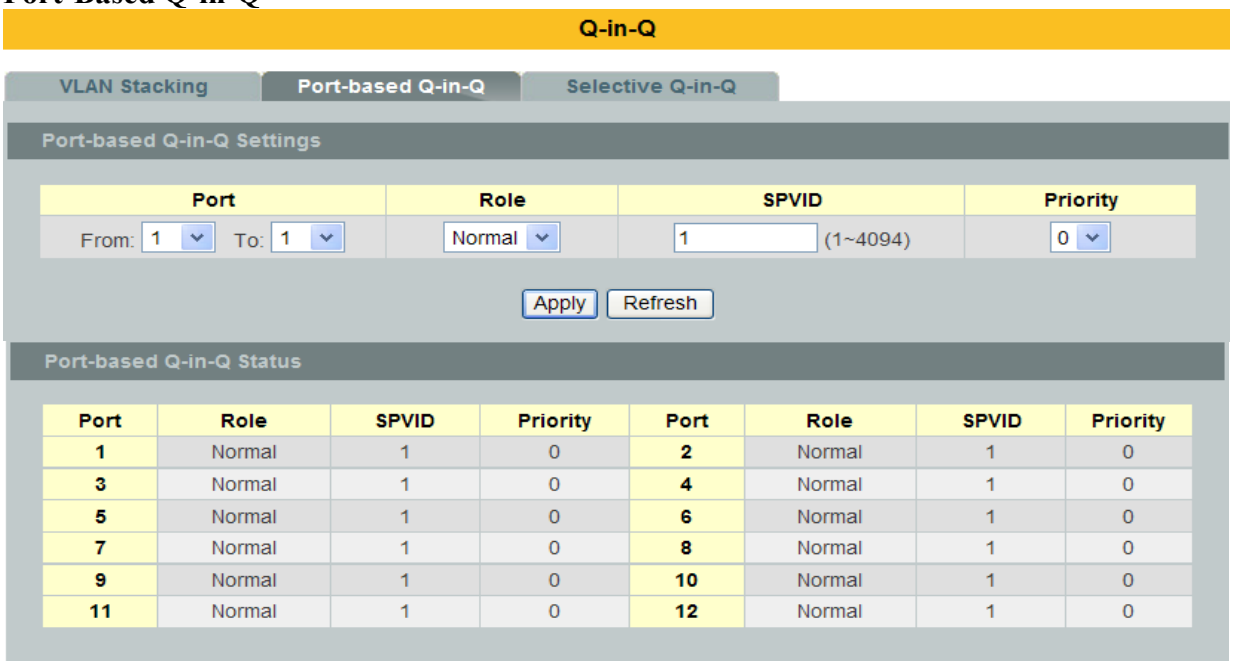
### 6.3.6.3. Web Configuration

## VLAN Stacking



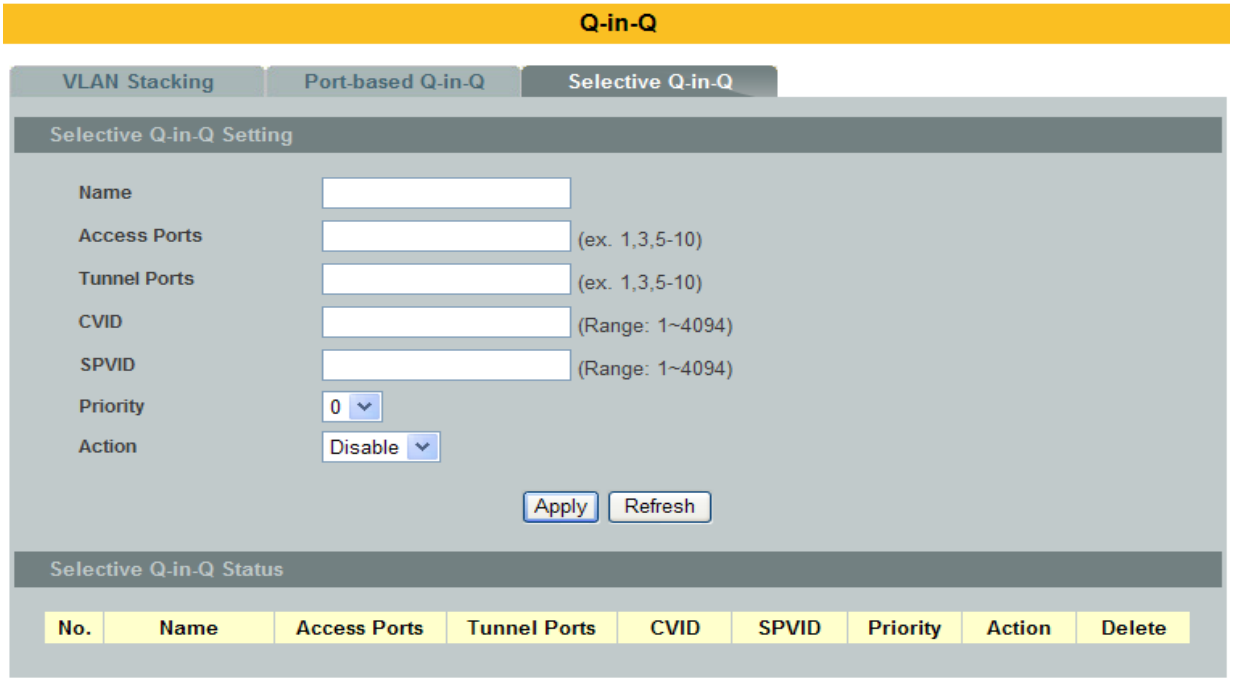

| Parameter | Description |
|---|---|
| Action | Select one of the three modes, **Disable or Port-Based** or **Selective** for the VLAN stacking. |
| Configures the TPID Table: The TPID table has 6 entries. | |
| Tunnel TPID Index | Selects the table index. |
| TPID | Configures the TPID. |
| Configures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

## Port-Based Q-in-Q




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

## Selective Q-in-Q



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

## 6.4. DHCP Option 82

### 6.4.1. Introduction

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

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

The maximum length of the information is 32 characters.

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

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

- The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- When the switch receives the DHCP request, it adds the option-82 information in the packet. The option-82 information contains the switch MAC address (the remote-ID suboption) and the port identifier, vlan-mod-port, from which the packet is received (the circuit-ID suboption).
- If the IP address of the relay agent is configured, the switch adds the IP address in the DHCP packet.

- The switch forwards the DHCP request that includes the option-82 field to the DHCP server.
- The DHCP server receives the packet. If the server is option-82 capable, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server **echoes** the option-82 field in the DHCP reply.
- The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. When the client and server are on the same subnet, the server broadcasts the reply. The switch verifies that it originally inserted the option-82 data by inspecting the remote ID and possibly the circuit ID fields. The switch **removes** the option-82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request**.**

**Option Frame Format:**

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

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

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

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

Circuit ID Sub-option Format:

| Suboption Type | Length | Information |
|---|---|---|
| 0x01 | | Circuit Form |

Remote ID Suboption Frame Format:

| Suboption Type | Length | Type | Length | MAC Address |
|---|---|---|---|---|
| 0x02 | 8 | 0 | 6 | 6 |

**Circuit Form:**

The circuit form is a flexible architecture. It allows user to combine any information or the system configurations into the circuit sub-option.

The Circuit Form is a string format. And its maximum length is 100 characters.

The keyword, %SPACE, will be replaced with a space character.

The other keywords get system configurations from the system and then replace the keyword and its leading code in the Circuit form. Eventually, the content of the circuit form is part of the payload on the DHCP option 82 packet.

**Rules:**

- The keyword must have a leading code '%'. For example: *%HOSTNAME*.
- If there are any characters following the keywords, you must add '+' between the keyword and character. For example: *%HOSTNAME+/*.
- If there are any characters before the keyword, you must add '+' between the character and the keyword. For example: *Test+%HOSTNAME*.

**Keyword:**

HOSTNAME - Add the system name into the Circuit sub-option..
SPACE - Add a space character.
SVLAN - Add the service provider VLAN ID into the Circuit sub-option.
If the service provider VLAN is not defined, the system will return PVLAN.
CVLAN - Add the customer VLAN ID into the Circuit sub-option.
If the CVLAN is not defined, the system returns 0.
PORT - Add the transmit port ID into the Circuit sub-option.
FRAME - Add the frame ID into the Circuit sub-option.
The frame ID is configured with the CLI command, "dhcp-options option82 circuit_frame VALUE". Or GUI Circuit Frame.
SHELF - Add the shelf ID into the Circuit sub-option.
The shelf ID is configured with the CLI command, "dhcp-options option82 circuit_shelf VALUE". Or GUI Circuit Shelf.
SLOT - Add the slot ID into the Circuit sub-option.
The slot ID is configured with the CLI command, "dhcp-options option82 circuit_slot VALUE". Or GUI Circuit Slot.

**For Example:**

HOSTNAME=L2SWITCH.
SVLAN=44.
CVLAN=32.
Circuit Form=RD+%SPACE+Department+%SPACE+%HOSTNAME+%SPACE+%PORT+_+%SVLAN+.+%CVLAN
The circuit sub-option result is: RD Department L2SWITCH 1_44.32

**Default Settings**

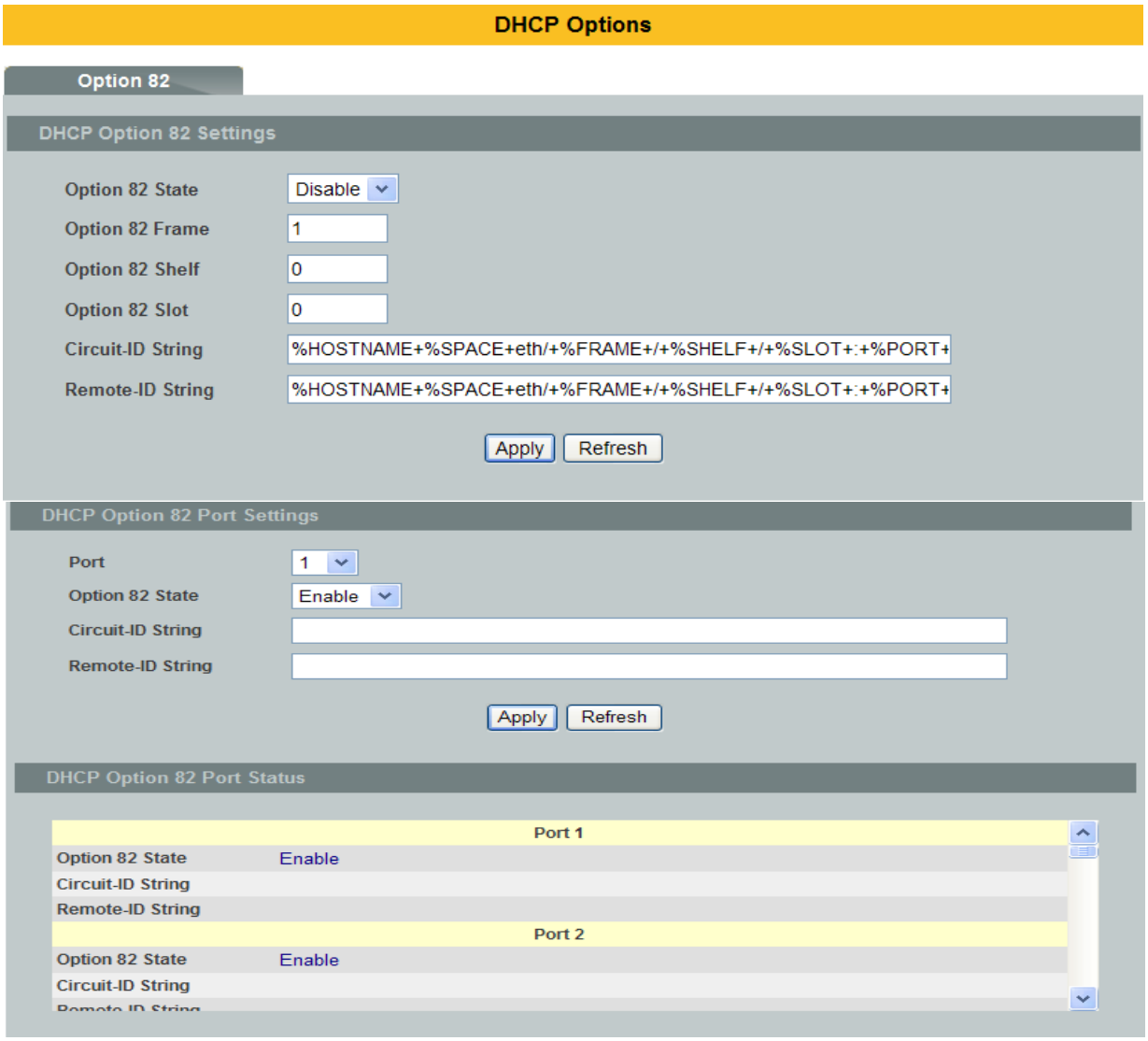
DHCP Option 82 state : disabled.
Circuit Frame : 1.
Circuit Shelf : 0.
Circuit Slot : 0.
Circuit ID String: %HOSTNAME+%SPACE+eth/+%FRAME+/+%SHELF+/+%SLOT+:+%PORT+_+%SVLAN+:+%CVLAN
Remote ID String: %HOSTNAME+%SPACE+eth/+%FRAME+/+%SHELF+/+%SLOT+:+%PORT+_+%SVLAN+:+%CVLAN

### 6.4.2. CLI Configuration

| Node | Command | Description |
|---|---|---|
| enable | show dhcp-options | This command displays the DHCP options |

| | | |
|---|---|---|
| | | configurations. |
| configure | dhcp-options option82 (disable \| enable) | This command disables / enables the DHCP option 82 on the Switch. |
| configure | dhcp-options option82 circuit_id | This command configures the information of the circuit ID sub-option. |
| configure | dhcp-options option82 remote_id | This command configures the information of the remote ID sub-option. |
| configure | dhcp-options option82 circuit_frame VALUE | This command configures the frame ID for the circuit sub-option. |
| configure | dhcp-options option82 circuit_shelf VALUE | This command configures the shelf ID for the circuit sub-option. |
| configure | dhcp-options option82 circuit_slot VALUE | This command configures the slot ID for the circuit sub-option. |

### 6.4.3. Web Configuration



| Parameter | Description |
|---|---|
| State | Select this option to enable / disable the DHCP option 82 on the Switch. |
| Circuit Frame | The frame ID for the circuit sub-option. |
| Circuit Shelf | The shelf ID for the circuit sub-option. |
| Circuit Slot | The slot ID for the circuit sub-option. |
| Circuit-ID String | The String of the circuit ID sub-option information. |
| Remote-ID String | The String of the remote ID sub-option information. |
| Apply | Click **Apply** to save your changes to the Switch. |
| Refresh | Click **Refresh** to begin configuring this screen afresh. |
| DHCP Option 82 Port Settings | |
| Port | The port ID. |
| Circuit-ID String | The String of the circuit ID sub-option information for the specific port. |
| Remote-ID String | The String of the remote ID sub-option information for the specific port. |
| DHCP Option 82 Port Status | |
| | The field displays all of the ports' configurations. |

## 6.5. DHCP Relay

### 6.5.1. Introduction

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

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

Most of the time in small networks DHCP uses broadcasts however there are some circumstances where unicast addresses will be used. A router for such a subnet receives the DHCP broadcasts,

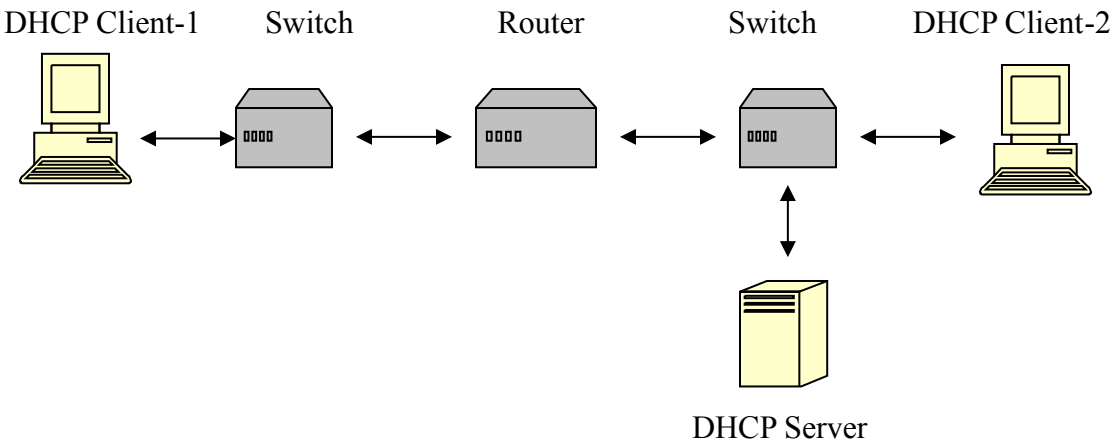
converts them to unicast (with a destination MAC/IP address of the configured DHCP server, source MAC/IP of the router itself). The field identified as the GIADDR in the main DHCP page is populated with the IP address of the interface on the router it received the DHCP request on. The DHCP server uses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

**Configurations:**

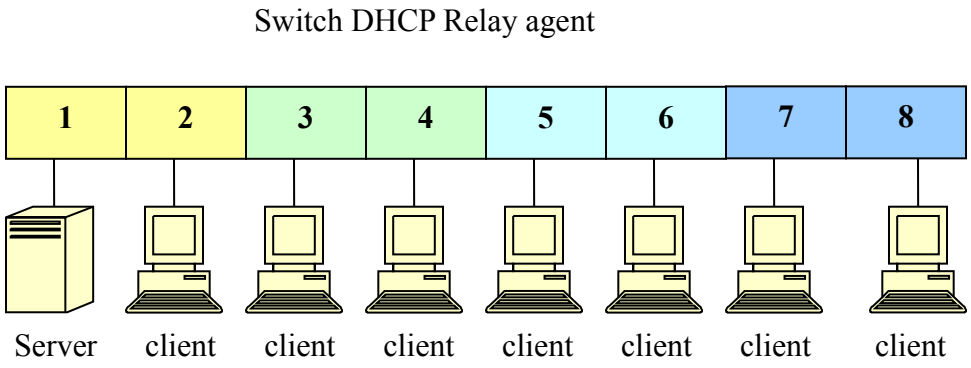
Users can enable/disable the DHCP Relay on the Switch. Users also can enable/disable the DHCP Relay on a specific VLAN. If the DHCP Relay on the Switch is disabled, the DHCP Relay is disabled on all VLANs even some of the VLAN DHCP Relay are enabled.

**Applications**

- Application-1 (Over a Router)
  The DHCP cleint-1 and DHCP client-2 are located in different IP segments. But they allocate IP address from the same DHCP server.




- Application-2 (Local in different VLANs)
  The DHCP cleint-1 and DHCP client-2 are located in different VLAN. But they allocate IP address from the same DHCP server.




VLAN 1: port 1, 2 (Management VLAN)
VLAN 2: port 3, 4

VLAN 3: port 5, 6
VLAN 4: port 7, 8

DHCP Server ➔ Port 1.
DHCP Client ➔ Port 2, 3, 4, 5, 6, 7, 8.

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

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

**Default Settings**

The default global DHCP relay state is disabled.
The default VLAN DHCP relay state is disabled for all VLANs.
The default DHCP server is 0.0.0.0

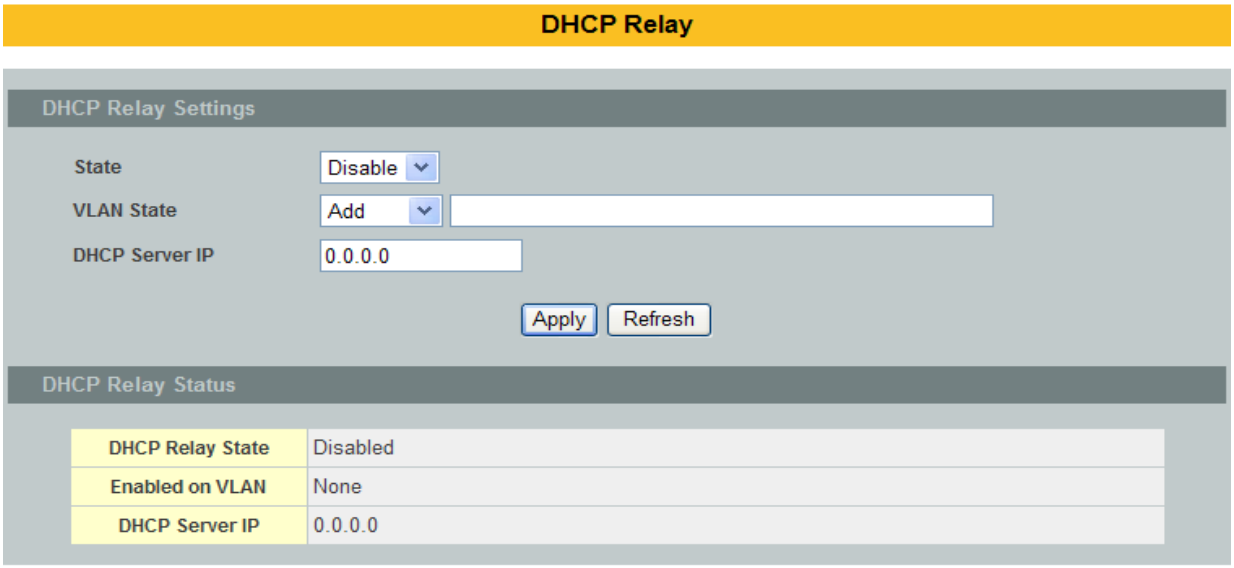
### 6.5.2. CLI Configuration

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

**Example:**

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

### 6.5.3. Web Configuration




| Parameter | Description |
|---|---|
| State | Enables / disables the DHCP relay for the Switch. |
| VLAN State | Enables / disables the DHCP relay on the specific VLAN(s). |
| DHCP Server IP | Configures the DHCP server's IP address. |

## 6.6. DHCP Server

### 6.6.1. Introduction

Dynamic Host Configuration Protocol (DHCP) uses Boot Strap protocol (BOOTP) for automatically configuring DHCP clients. DHCP server's responsibility is to assign TCP/IP parameters including private IP addresses to DHCP clients automatically.

DHCP server maintains address pools, TCP/IP parameter options are attached per pool.
DHCP server can work irrespective of routing feature in the Switch, but if router is running along with the DHCP server then administrator should take care about the address pool configurations in DHCP server and address assignments to the VLAN interface in router as below.

1. Multiple VLANs bindings to an address pool in DHCP server are not allowed when router is enabled in the switch.
2. Router's specified VLAN IP address/Mask (SubNet) should be greater than DHCP server's VLAN binding address pool IP/Mask.
   Example: Router assigned VLAN 10's IP address as 1.2.3.4/24 then
   a. DHCP server VLAN 10's following address pools are allowed.
      i. 1.2.3.0/28
      ii. 1.2.3.4/30
   b. Following address pools are not allowed

i. 1.2.0.0/16
ii. 1.2.3.0/20

And DHCP Server's VLAN 10 host address should be same as interface address in router. As per above example, host address should 1.2.3.4.

Better way is administrator has to configure Router before DHCP server configurations.

### 6.6.2. CLI Configuration

| Node | Command | Description |
|---|---|---|
| enable | show dhcp-server bindings | This command displays the current hosts static and dynamic bindings in the DHCP server. |
| enable | Show dhcp-server pools | This command displays all configured address pools information. |
| enable | Show dhcp-server statistics | This command displays DHCP server statistics including packets send and received counts. |
| enable | Show dhcp-server information | This command displays DHCP server details, including global configurations, host bindings; address pools information and packet counters. |
| configure | dhcp-server enable | This command enables DHCP server. |
| configure | no dhcp-server enable | This command disables DHCP server. |
| configure | dhcp-server icmp enable | This command enables ICMP module in DHCP server for periodical checking. |
| configure | no dhcp-server icmp enable | This command disabled ICMP module in DHCP server. |
| configure | dhcp-server offer-reuse <seconds> | This command configures offer reuse time in seconds. |
| configure | no dhcp-server offer-reuse <seconds> | This command disables existing offer reuse time and configures default time as 5 seconds. |
| configure | dhcp-server boot-file <file_name> | This command configures boot file in DHCP server |
| configure | no dhcp-server boot-file <file_name> | This command disables already configured boot file in DHCP server. |
| configure | dhcp-server next-server <IP_ADDR> | This command configures next server in DHCP server. |
| configure | no dhcp-server next-server <IP_ADDR> | This command disables already configured next server in DHCP server. |
| configure | dhcp-server option ascii [OPTION] [OPTION_VALUE] | This command configures global option in DHCP server and it will be applicable for all existing address pools. |
| configure | dhcp-server option ip-addr [OPTION] [IPADDR] | This command configures global option in DHCP server and it will be applicable for all existing address pools. |
| configure | no dhcp-server option <0-255> | This command disables already configured |

| | | |
|---|---|---|
| | | global option in DHCP server. |
| configure | dhcp-server pool <POOL_ID> | This command creates new address pool, if it is not already exist. |
| configure | no dhcp-server pool <POOL_ID> | This command disables all existing configurations on specifed address pool and deletes the pool from DHCP server pool list. |
| dhcp-server | network <IPADDR_MASK> | This command configures specified address pool with all allotted IP address in the subnet. |
| dhcp-server | no network <IPADDR_MASK> | This command disables already configured IP address from pool. |
| dhcp-server | vlan <VLAN_LIST> | This command binds specified VLAN list to pool. |
| dhcp-server | no vlan <VLAN_LIST> | This command deletes specified VLAN list from pool. |
| dhcp-server | host address <IPADDR> | This command configures specified IP address as Host address of the pool; and this address will used as source IP address while sending packets. |
| dhcp-server | no host address <IPADDR> | This command deletes host address from pool and Switch CPU IP address will be used as source IP address in sending out packets. |
| dhcp-server | excluded-address <IPADDR> <IPADDR> | This command configures to exclude specified range of IP addresses from assigning to client. This will be useful for blocking few IP addresses. |
| dhcp-server | no excluded-address <IPADDR> <IPADDR> | This command disables already configured exclude IP addresses. |
| dhcp-server | lease infinity | This command configures leased IP address binds forever. Always same MAC address machine will get same IP address. |
| dhcp-server | lease [days [hours [minutes]]] | This command configures lease for specified days, hours and minutes. |
| dhcp-server | no lease | This command configures lease to default 1 day lease. |
| dhcp-server | default-router <IPADDR> | This command configures pool with specified address as default route parameter. This option allowed up to 8 address. |
| dhcp-server | no default-router <IPADDR> | This command disables already configured IP address from default route parameter. |
| dhcp-server | dns-server <IPADDR> | This command configures pool with specified address as DNS server parameter. This option allowed up to 8 addresses. |
| dhcp-server | no dns-server <IPADDR> | This command disables already configured IP address from DNS server parameter. |
| dhcp-server | netbios-name-server <IPADDR> | This command configures pool with specified address as NetBios Server |

| | | |
|---|---|---|
| | | parameter. This option allowed up to 8 addresses. |
| dhcp-server | no netbios-name-server <IPADDR> | This command disables already configured IP address from NetBios server parameter. |
| dhcp-server | netbios-node-type (b-node\|h-node\|m-node\|p-node) | This command configures pool with NetBios node type parameter. |
| dhcp-server | no netbios-node-type (b-node\|h-node\|m-node\|p-node) | This command disables already configured NetBios node type parameter from pool. |
| dhcp-server | domain-name <DOMAIN_NAME> | This command configures pool with specified string as DNS domain name parameter. |
| dhcp-server | no domain-name <DOMAIN_NAME> | This command disables already configured DNS domain name parameter from pool. |
| dhcp-server | host client-id ascii [HEX-STRING] [OPTION][OPTION_VALUE] | This command binds option parameter with specified client_id in pool. |
| dhcp-server | no host client-id ascii [HEX-STRING] [OPTION][OPTION_VALUE] | This command deletes option parameter with specified client_id from pool. |
| dhcp-server | host client-id ip-addr [HEX-STRING] [OPTION][IPADDR] | This command binds specified IP address option parameter with specified client_id in pool. |
| dhcp-server | no host client-id ip-addr [HEX-STRING] [OPTION][IPADDR] | This command deletes specified IP address option parameter with specified client_id from pool. |

## 6.7. Link Aggregation

### 6.7.1. Static Trunk

#### 6.7.1.1. Introduction

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 : 6.
Maximum port in link aggregation group : 8.

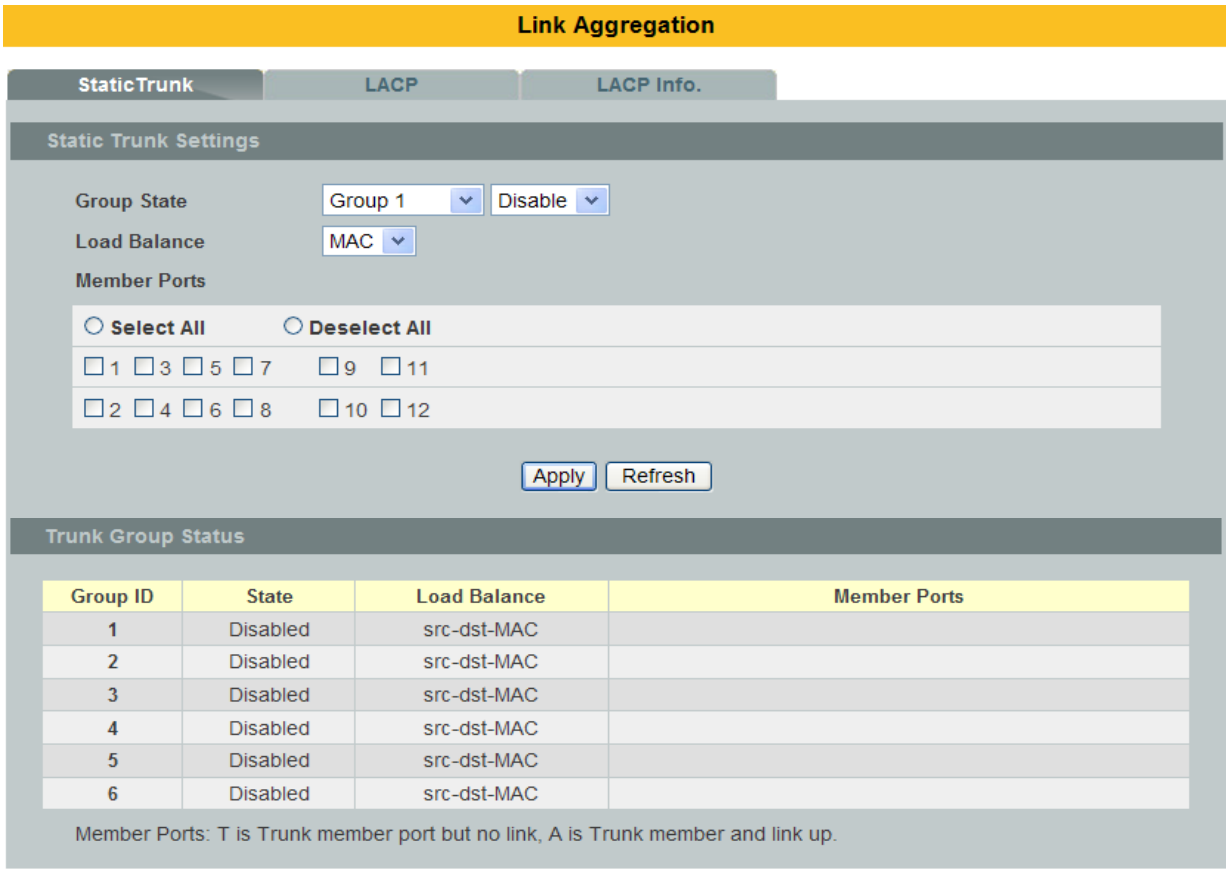
### 6.7.1.2. CLI Configuration

| 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*

### 6.7.1.3. Web Configuration




| Parameter | Description |
|---|---|

| | |
|---|---|
| Group State | Select the group ID to use for this trunk group, that is, one logical link containing multiple ports.<br>Select **Enable** to use this static trunk group. |
| Load Balance | Configures the load balance algorithm for the specific trunk group. |
| Member Ports | Select the ports to be added to the static trunk group. |
| Apply | Click Apply to configure the settings. |
| Refresh | Click this to reset the fields to the last setting. |
| Trunk Group Status | |
| Group ID | This field displays the group ID to identify a trunk group, that is, one logical link containing multiple ports. |
| State | This field displays if the trunk group is enabled or disabled. |
| Load Balance | This field displays the load balance policy for the trunk group. |
| Member Ports | This field displays the assigned ports that comprise the static trunk group. |

### 6.7.2. LACP

#### 6.7.2.1. Introduction

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.

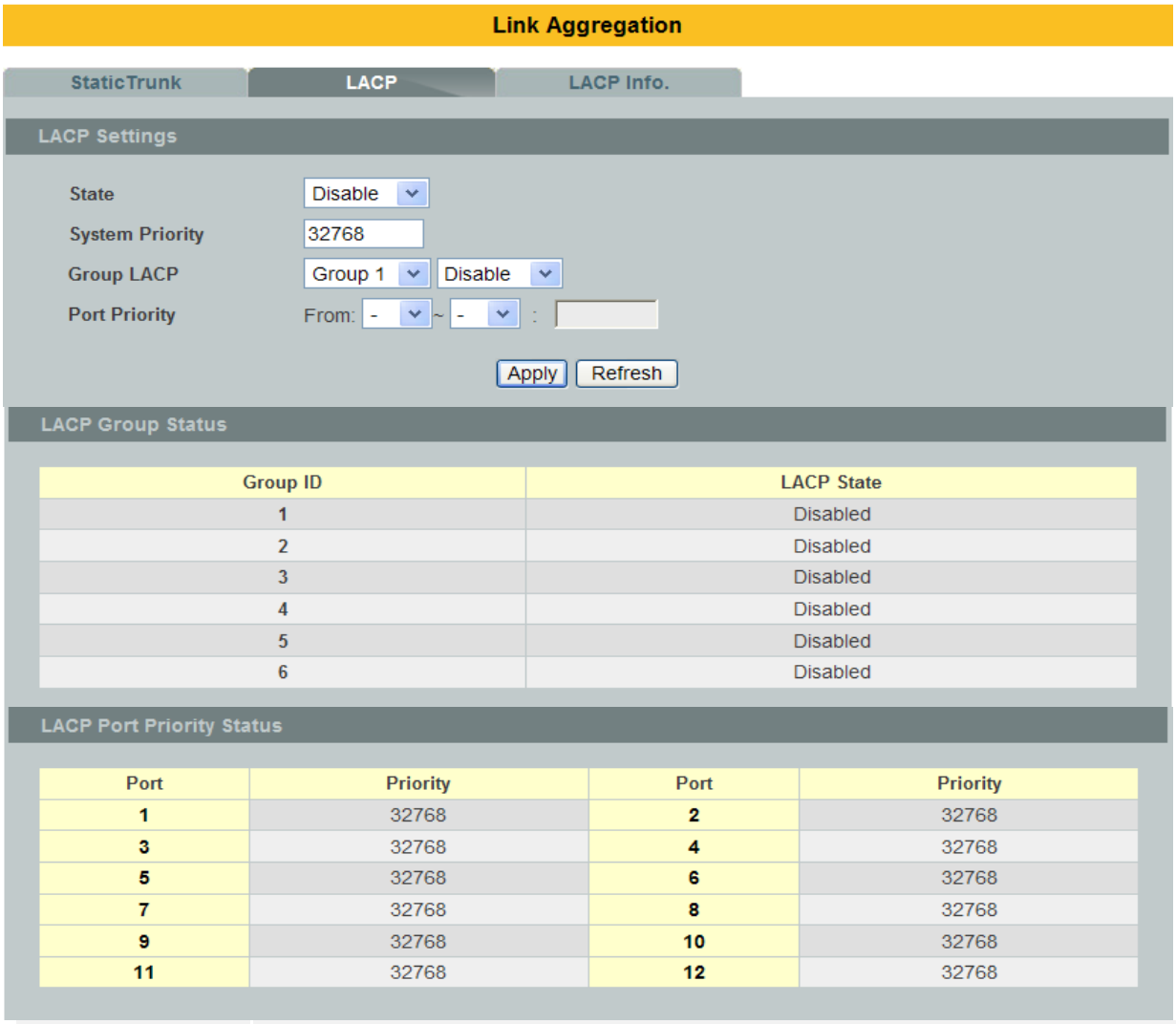
### 6.7.2.2. CLI Configuration

| 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.<br>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.<br>Note: The default value is 32768. |
| if-range | no lacp port_priority | This command configures the default for the priority for the specific ports. |

### 6.7.2.3. Web Configuration

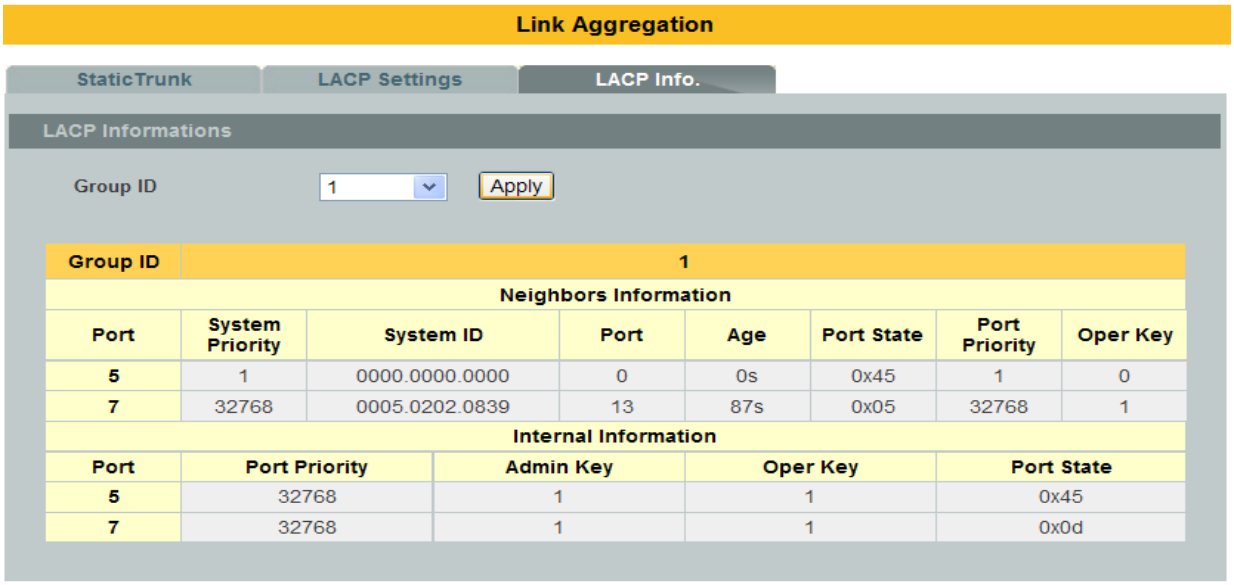
**LACP Settings**




| Parameter | Description |
|---|---|
| State | Select **Enable** from the drop down box to enable Link Aggregation Control Protocol (LACP).<br>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. |

## 6.8. Link Layer Discovery Protocol (LLDP)

### 6.8.1. 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.

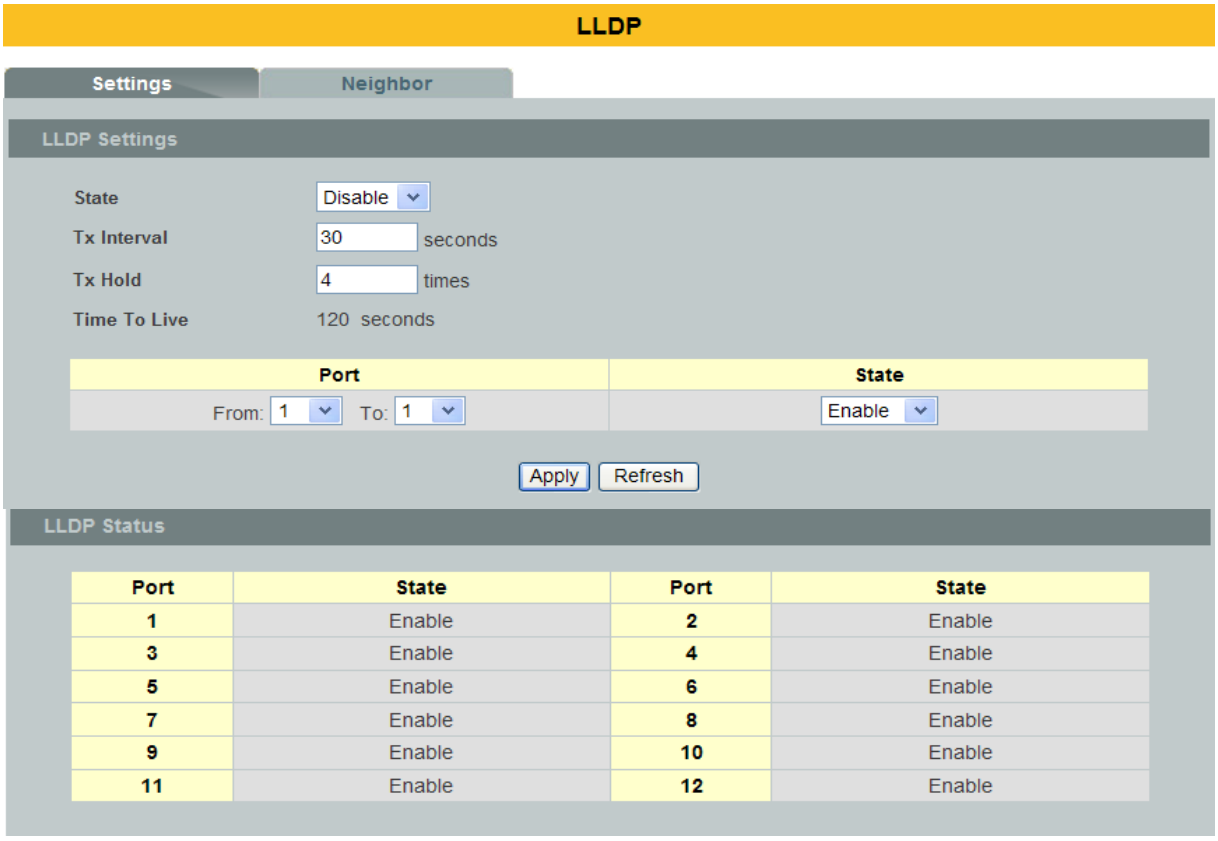
| Port | Status | Port | Status |
|---|---|---|---|
| 1 | Enable | 2 | Enable |
| 3 | Enable | 4 | Enable |
| 5 | Enable | 6 | Enable |
| 7 | Enable | 8 | Enable |
| 9 | Enable | 10 | Enable |
| 11 | Enable | 12 | Enable |

### 6.8.2. 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 | This command configures the interval to transmit the LLDP packets. |
| configure | lldp tx-hold | This command configures the tx-hold time which |

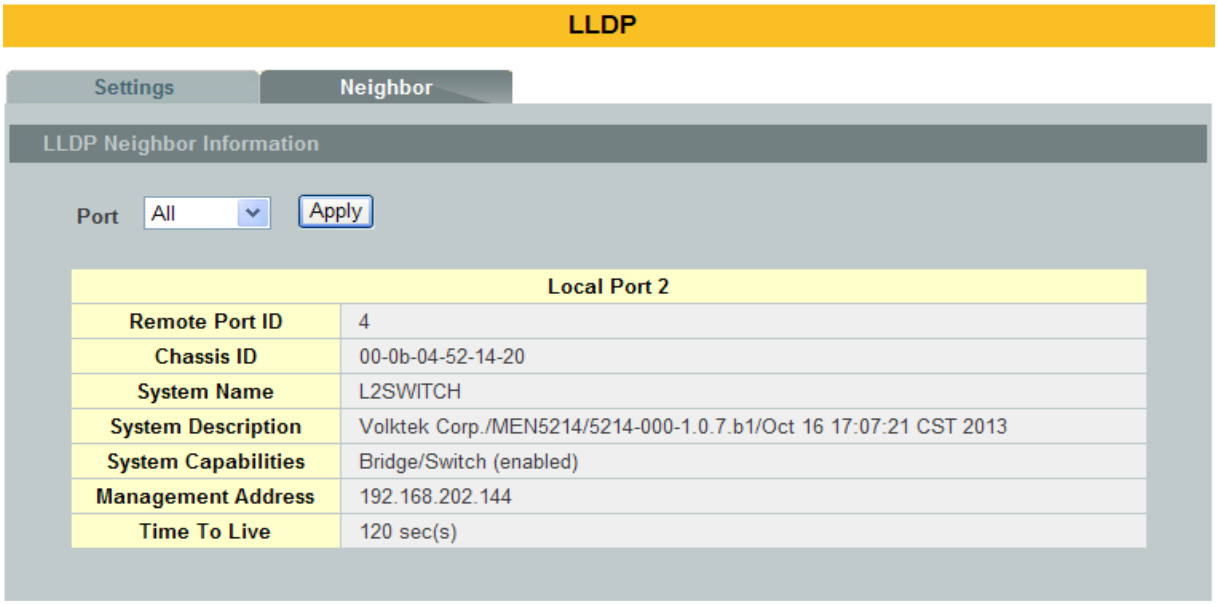
| | | |
|---|---|---|
| | | determines the TTL of the Switch's message. (TTL=tx-hold * tx-interval) |
| interface | lldp-agent (disable\|enable\|rx-only\|tx-only) | This command configures the LLDP agent function.<br>disable – Disable the LLDP on the specific port.<br>enable – Transmit and Receive the LLDP packet on the specific port.<br>tx-only – Transmit the LLDP packet on the specific port only.<br>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.<br>disable – Disable the LLDP on the specific port.<br>enable – Transmit and Receive the LLDP packet on the specific port.<br>tx-only – Transmit the LLDP packet on the specific port only.<br>rx-only – Receive the LLDP packet on the specific port. |

### 6.8.3. 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. |

## 6.9. Loop Detection

### 6.9.1. Introduction

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 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.

**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

                                  Recovery                                  Recovery
Port State    Status   State     Time   Port State    Status   State     Time
---- -------- -------  --------  ----   ---- -------- -------  --------  ----
 1   Disabled Normal   Enabled   1        2  Disabled Normal   Enabled   1
 3   Disabled Normal   Enabled   1        4  Disabled Normal   Enabled   1
 5   Disabled Normal   Enabled   1        6  Disabled Normal   Enabled   1
 7   Disabled Normal   Enabled   1        8  Disabled Normal   Enabled   1
```

```
9   Disabled Normal   Enabled  1        10  Disabled Normal   Enabled  1
11  Disabled Normal   Enabled  1        12  Disabled Normal   Enabled  1
```

### 6.9.2. CLI Configuration

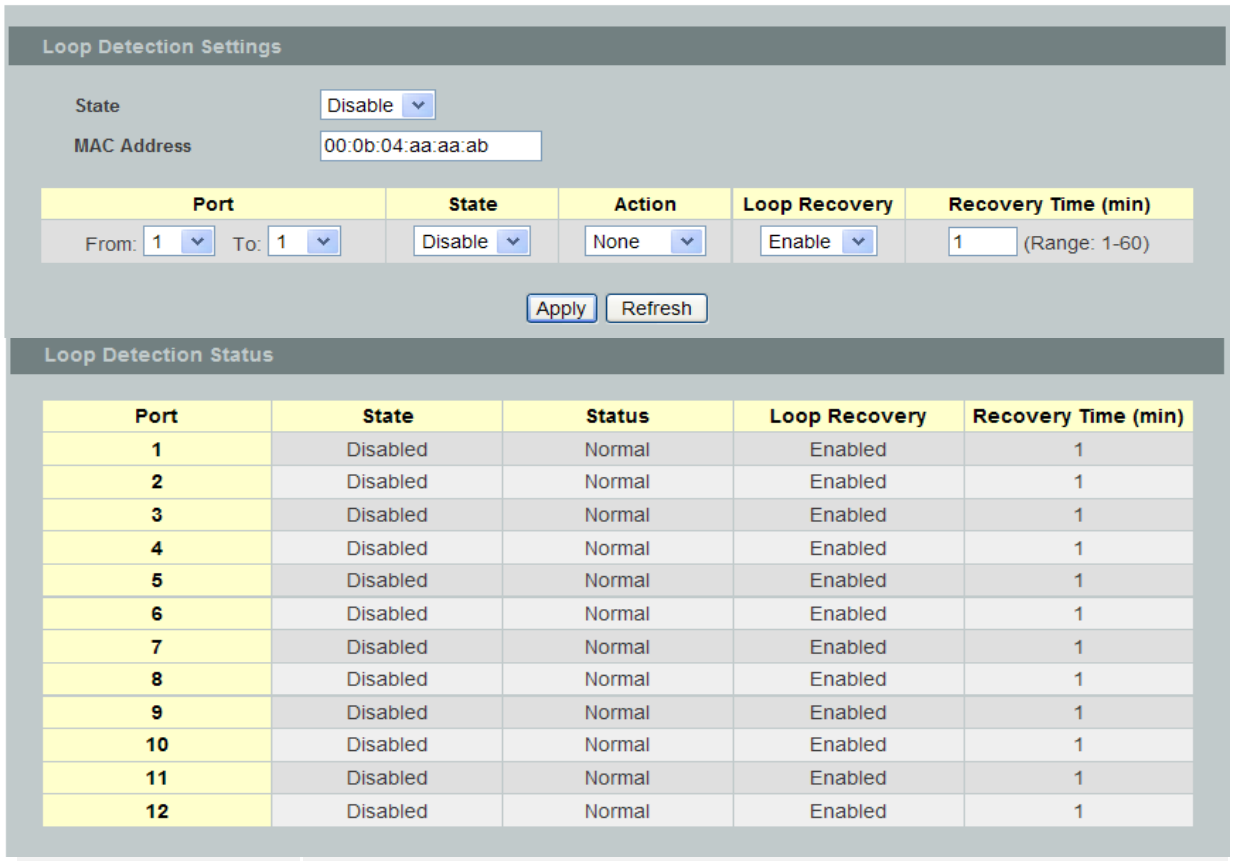
| Node | Command | Description |
|---|---|---|
| enable | show loop-detection | This command displays the current loop detection configurations. |
| configure | loop-detection (disable \| enable) | This command disables / enables the loop detection on the switch. |
| configure | loop-detection address 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 VALUE | 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 VALUE | This command configures the recovery period time. |

**Example:**

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

### 6.9.3. Web Configuration

**Loop Detection**




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

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

## 6.10. Modbus

### 6.10.1. Introduction

MODBUS TCP supports different types of data format for reading. The primary four types of them are:

| Data Access Type | | Function Code | Function Name | Note |
|---|---|---|---|---|
| Bit access | Physical Discrete Inputs | 2 | Read Discrete Inputs | Not support now |
| | Internal Bits or Physical Coils | 1 | Read Coils | Not support now |
| Word access (16-bit access) | Physical Input Registers | 4 | Read Input Registers | |
| | Physical Output Registers | 3 | Read Holding Registers | Not support now |

**MODBUS Data Map and Information Interpretation of VIVOTEK IE Switches**

MODBUS base address of VIVOTEK switches is 1001(decimal) for Function Code 4.

| Address Offset | Data Type | Interpretation | Description |
|---|---|---|---|
| **System Information** | | | |
| 0x0000 | 1 word | HEX | Vendor ID = 0x0b04 |
| 0x0001 | 16 words | ASCII | Vendor Name = “VIVOTEK Corp.”<br>Word 0 Hi byte = ‘V’<br>Word 0 Lo byte = ‘o’<br>Word 1 Hi byte = ‘l’<br>Word 1 Lo byte = ‘k’<br>Word 2 Hi byte = ‘t’<br>Word 2 Lo byte = ‘e’<br>Word 3 Hi byte = ‘k’<br>Word 3 Lo byte = ‘ ’<br>Word 4 Hi byte = ‘C’<br>Word 4 Lo byte = ‘o’<br>Word 5 Hi byte = ‘r’<br>Word 5 Lo byte = ‘p’ |

| | | | |
|---|---|---|---|
| | | | Word 6 Hi byte = '.'<br>Word 6 Lo byte = '\0' |
| 0x0020 | 16 words | ASCII | Product Name = "INS-8648"<br>Word 0 Hi byte = 'I'<br>Word 0 Lo byte = 'N'<br>Word 1 Hi byte = 'S'<br>Word 1 Lo byte = '-'<br>Word 2 Hi byte = '8'<br>Word 2 Lo byte = '6'<br>Word 3 Hi byte = '4'<br>Word 3 Lo byte = '8'<br>Word 4 Hi byte = '\0'<br>Word 4 Lo byte = '\0' |
| 0x0040 | 7 words | | Product Serial Number<br>Ex: Serial No=A000000000001 |
| 0x0050 | 12 words | ASCII | Firmware Version=" 8648-000-1.1.0.S0"<br>Word 0 Hi byte = '8'<br>Word 0 Lo byte = '6'<br>Word 1 Hi byte = '4'<br>Word 1 Lo byte = '8'<br>Word 2 Hi byte = '-'<br>Word 2 Lo byte = '0'<br>Word 3 Hi byte = '0'<br>Word 3 Lo byte = '0'<br>Word 4 Hi byte = '-'<br>Word 4 Lo byte = '1'<br>Word 5 Hi byte = '.'<br>Word 5 Lo byte = '1'<br>Word 6 Hi byte = '.'<br>Word 6 Lo byte = '0'<br>Word 7 Hi byte = '.'<br>Word 7 Lo byte = 'S'<br>Word 8 Hi byte = '0'<br>Word 8 Lo byte = '\0' |
| 0x0060 | 16 words | ASCII | Firmware Release Date=" Mon Sep 30 18:51:45 2013" |
| 0x0070 | 3 words | HEX | Ethernet MAC Address<br>Ex: MAC = 00-01-02-03-04-05<br>Word 0 Hi byte = 0 x 00<br>Word 0 Lo byte = 0 x 01<br>Word 1 Hi byte = 0 x 02<br>Word 1 Lo byte = 0 x 03<br>Word 2 Hi byte = 0 x 04<br>Word 2 Lo byte = 0 x 05 |
| 0x0080 | 1 word | HEX | Power 1(PWR) Alarm, DIP switch 1 need ON<br>0x0000: no alarm<br>0x0001: input voltage < 44V<br>0x0002: input voltage > 57V<br>0x0003: No PWR input |
| 0x0081 | 1 word | HEX | Power 2(RPS) Alarm, DIP switch 1 need ON<br>0x0000: no alarm<br>0x0001: input voltage < 44V<br>0x0002: input voltage > 57V<br>0x0003: No RPSinput |
| 0x0090 | 1 word | HEX | Fault LED Status<br>0x0000: No<br>0x0001: Yes |

| | | | |
|---|---|---|---|
| **Port Information** | | | |
| 0x0100 to 0x0109 | 1 word | HEX | Port 1 to 10 Link Status<br>0x0000: Link down<br>0x0001: 10M-Full-FC_ON (FC: Flow Control)<br>0x0002: 10M-Full-FC_OFF<br>0x0003: 10M-Half-FC_ON<br>0x0004: 10M-Half-FC_OFF<br>0x0005: 100M-Full-FC_ON<br>0x0006: 100M-Full-FC_OFF<br>0x0007: 100M-Half-FC_ON<br>0x0008: 100M-Half-FC_OFF<br>0x0009: 1000M-Full-FC_ON<br>0x000A: 1000M-Full-FC_OFF<br>0x000B: 1000M-Half-FC_ON<br>0x000C: 1000M-Half-FC_OFF<br>0xFFFF: No port |
| 0x0200 to 0x0213 (port 1)<br>0x0220 to 0x0233 (port 2)<br>…<br>0x0320 to 0x0333 (port 10) | 20 words | ASCII | Port 1 to 10 Description<br>Port Description = “100TX,RJ45.” Or “1000TX,SFP.”<br>Word 0 Hi byte = ‘1’<br>Word 0 Lo byte = ‘0’<br>Word 1 Hi byte = ‘0’<br>Word 1 Lo byte = ‘T’<br>…<br>Word 4 Hi byte = ‘4’<br>Word 4 Lo byte = ‘5’<br>Word 5 Hi byte = ‘.’<br>Word 5 Lo byte = ‘\0’ |
| 0x0400 to 0x0413 (port 1 to 10) | 2 words | HEX | Port 1 to 10 Tx Packets<br>Ex: port 1 Tx Packet Amount = 0x87654321<br>Word 0 =8765<br>Word 1 = 4321 |
| 0x0440 to 0x0453 (port 1 to 10) | 2 words | HEX | Port 1 to 10 Rx Packets<br>Ex: port 1 Rx Packet Amount = 0x123456<br>Word 0 = 0012<br>Word 1 = 3456 |
| 0x0480 to 0x0493 (port 1 to 10) | 2 words | HEX | Port 1 to 10 Tx Error Packets<br>Ex: port 1 Tx Error Packet Amount = 0x87654321<br>Word 0 =8765<br>Word 1 = 4321 |
| 0x04C0 to 0x04D3 (port 1 to 10) | 2 words | HEX | Port 1 to 10 Rx Error Packets<br>Ex: port 1 Rx Error Packet Amount = 0x123456<br>Word 0 = 0012<br>Word 1 = 3456 |
| **STP Information** | | | |
| 0x0500 | 1 word | HEX | STP Status:<br>0x0000 : STP is disabled.<br>0x0001 : STP<br>0x0002 : RSTP<br>0x0003 : MSTP |
| **Xpress Ring Information** | | | |
| 0x0501 | 1 word | HEX | Xpress Ring Status on the Switch:<br>0x0000 : Disabled.<br>0x0001 : Enabled |
| 0x0510 | 1 word | HEX | Status of Xpress-ring1 of the Switch<br>0x0000 : Disabled<br>0x0001 : Enabled |

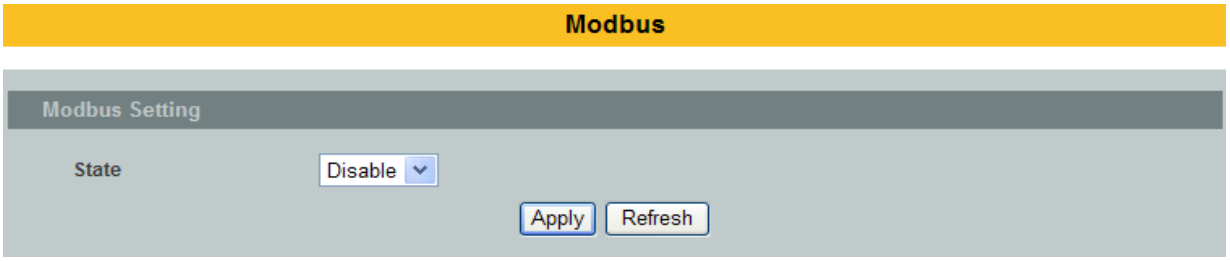
| | | | |
|---|---|---|---|
| 0x0511 | 1 word | HEX | Status of Xpress-ring2 of the Switch<br>0x0000 : Disabled<br>0x0001 : Enabled |
| 0x0512 | 3 word | HEX | Destination MAC of the Xpress-ring1<br>Word 0 Lo byte = MAC0<br>Word 0 Hi byte = MAC1<br>Word 1 Lo byte = MAC2<br>Word 1 Hi byte = MAC3<br>Word 2 Lo byte = MAC4<br>Word 2 Hi byte = MAC5 |
| 0x0515 | 3 word | HEX | Destination MAC of the Xpress-ring2<br>Word 0 Lo byte = MAC0<br>Word 0 Hi byte = MAC1<br>Word 1 Lo byte = MAC2<br>Word 1 Hi byte = MAC3<br>Word 2 Lo byte = MAC4<br>Word 2 Hi byte = MAC5 |
| 0x0518 | 1 word | HEX | Primary Port of the Xpress-ring1<br>Word 0 Hi byte = Port ID. |
| 0x0519 | 1 word | HEX | Secondary Port of the Xpress-ring1<br>Word 0 Hi byte = Port ID. |
| 0x051a | 1 word | HEX | Primary Port of the Xpress-ring2<br>Word 0 Hi byte = Port ID. |
| 0x051b | 1 word | HEX | Secondary Port of the Xpress-ring2<br>Word 0 Hi byte = Port ID. |
| 0x051c | 1 word | HEX | Role of Xpress-ring1<br>0x0000 : Forwarder<br>0x0001 : Arbiter |
| 0x051d | 1 word | HEX | Role of Xpress-ring2<br>0x0000 : Forwarder<br>0x0001 : Arbiter |
| 0x051e | 1 word | HEX | Primary Port Status of Xpress-ring1<br>0x0000 : link down<br>0x0001 : forwarding<br>0x0002 : blocking |
| 0x051f | 1 word | HEX | Secondary Port Status of Xpress-ring1<br>0x0000 : link down<br>0x0001 : forwarding<br>0x0002 : blocking |
| 0x0520 | 1 word | HEX | Primary Port Status of Xpress-ring2<br>0x0000 : link down<br>0x0001 : forwarding<br>0x0002 : blocking |
| 0x0521 | 1 word | HEX | Secondary Port Status of Xpress-ring2<br>0x0000 : link down<br>0x0001 : forwarding<br>0x0002 : blocking |

### 6.10.2. CLI Configuration

| Node | Command | Description |
|---|---|---|
| enable | show modbus | This command displays the current Modbus configurations. |

| | | |
|---|---|---|
| configure | modbus (disable\|enable) | This command disables / enables the Modbus on the switch. |

### 6.10.3. Web Configuration




| Parameter | Description |
|---|---|
| State | Select this option to enable / disable the Modbus on the Switch. |
| Apply | Click Apply to save your changes to the Switch. |
| Refresh | Click Refresh to begin configuring this screen afresh. |

## 6.11. PoE (Power over Ethernet)

### 6.11.1. PoE

#### 6.11.1.1. 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 V DC 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 10/100 Mbps

Ethernet port.

**Standard PoE parameters and comparison**

| Property | 802.3af (802.3at Type 1) | 802.3at Type 2 |
|---|---|---|
| Power available at PD | 12.95 W | 25.50 W per mode |
| Maximum power delivered by PSE | 15.40 W | 30.00 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 0.1 W steps negotiated continuously |
| Dreading of maximum cable ambient operating temperature | None | 5°C with one mode (two pairs) active, 10°C with two modes (four pairs) simultaneously 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**

| | | Power levels available | | |
|---|---|---|---|---|
| **Class** | **Usage** | **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**

- ✓ The port 1 ~ 8 supports the PoE function.
- ✓ Total-power: The maximum power which the switch can support to the PDs.
  *Notice: You must reserve about 18 W for the system. That is, if you connect an external power supported 240W. The total power should be 222W only.*
- ✓ 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 |
| 5 | Disabled | Disabled | High |
| 6 | Disabled | Disabled | High |
| 7 | Disabled | Disabled | High |
| 8 | Disabled | Disabled | High |

### 6.11.1.2. 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.<br>● critical : The highest priority.<br>● high : The middle priority.<br>● low : The lowest priority. |

### 6.11.1.3. Web Configuration

**PoE**

Configuration | Schedule | PD Alive Check | Power Delay

**PoE Settings**

State: Enable

Total Power: 240 (0~240)

Total Power(P) = Current of adaptor(I) * Voltage of adaptor(V)

| Port | State | Priority | Max Power Limit |
|---|---|---|---|
| From: 1 To: 1 | Enable | Critical | 0 (0~30) |

Apply Refresh

**PoE Status**

| | |
|---|---|
| State | Enabled |
| Total Power (W) | 240 |
| Total Power Consumption(W) | 0 |

| Port | State | Status | Priority | Class | Max Power Limit(W) | Power Consumption(W) |
|---|---|---|---|---|---|---|
| 1 | Enabled | Searching | High | None | 30 | 0 |
| 2 | Enabled | Searching | High | None | 30 | 0 |
| 3 | Enabled | Searching | High | None | 30 | 0 |
| 4 | Enabled | Searching | High | None | 30 | 0 |
| 5 | Enabled | Searching | High | None | 30 | 0 |
| 6 | Enabled | Searching | High | None | 30 | 0 |
| 7 | Enabled | Searching | High | None | 30 | 0 |
| 8 | Enabled | Searching | High | None | 30 | 0 |

| Parameter | Description |
|---|---|
| PoE Mode | Selects the PoE mode, classification or consumption.<br>**Classification** - Allocated power according to class (0 to 4).<br>**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.<br>Selects **Disable** to disable the PoE function on the specific port. |
| Priority | Selects **Critical / High / Low** priority for the specific port. |
| Apply | Click **Apply** to take effect the settings. |
| Refresh | Click **Refresh** to begin configuring this screen afresh. |
| PoE Mode | Displays the current PoE mode. |

| | |
|---|---|
| Total Power | Displays the total power that the Switch supports. |
| Total Consuming Power | Displays the total consuming power for all of the PDs. |
| External Power Module | Displays the status of the external power module. |
| Port | Display the Port No. |
| State | Displays the PoE state for the specific port. |
| PD Priority | Displays the PoE priority for the specific port. |
| Class | The field displays the class mode which the PSE negotiate with the PD on the specific port. |
| Consuming Power(mW) | Displays the consuming power for the specific port. |
| Power Allocated(mW) | Displays the power allocated for the specific port. |
| Current Status(mA) | Displays the current status for the specific port. |

### 6.11.2. PoE Schedule

#### 6.11.2.1.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.

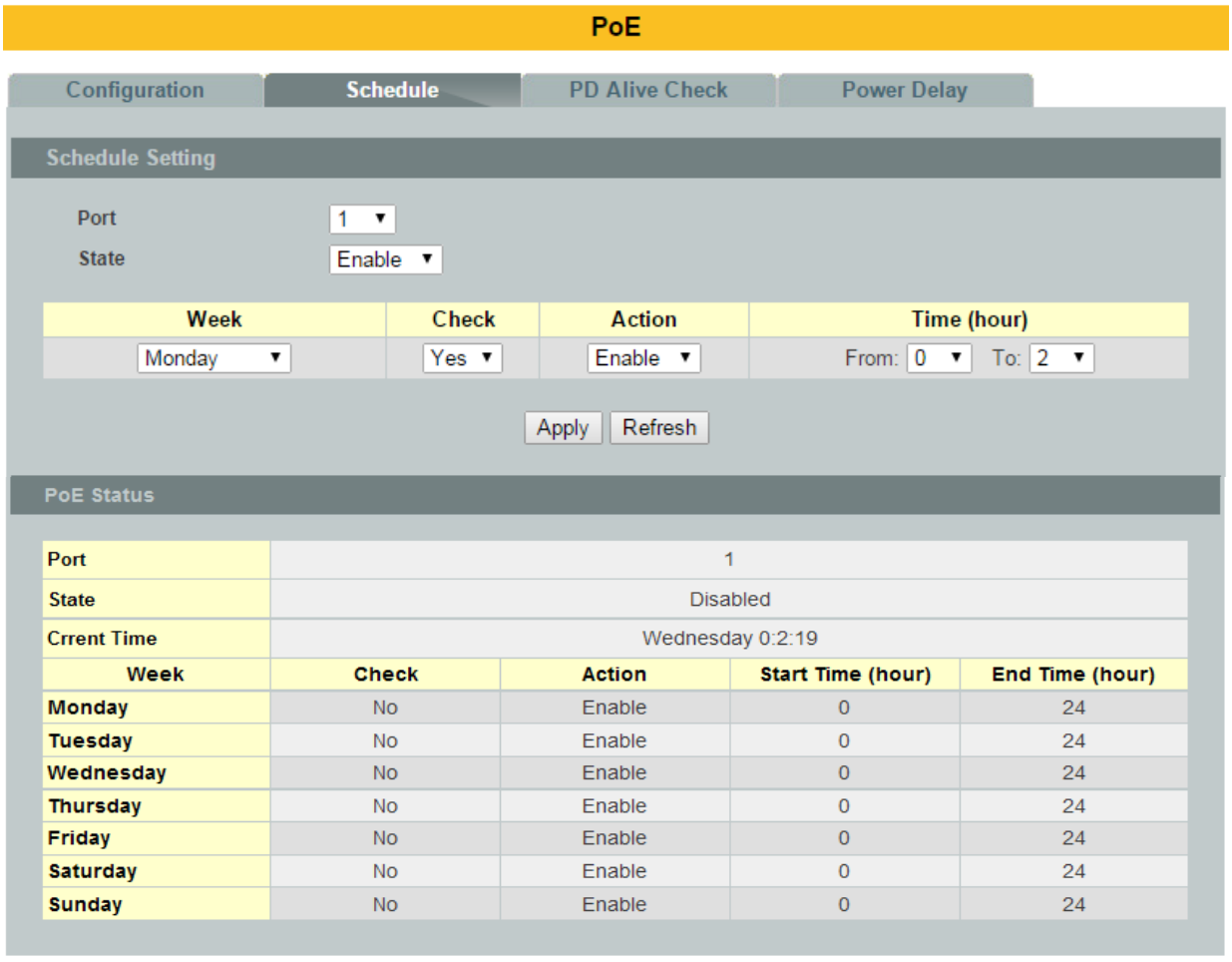
Port:
Schedule State: Disabled

| 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 |

### 6.11.2.2. 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. |

### 6.11.2.3. Web Configuration




| Parameter | Description |
|---|---|
| Port | Selects a port that you want to configure the PoE schedule function. |

| | |
|---|---|
| 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. |
| Time (Hour) | |

### 6.11.3. PD Alive Check

#### 6.11.3.1. 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.

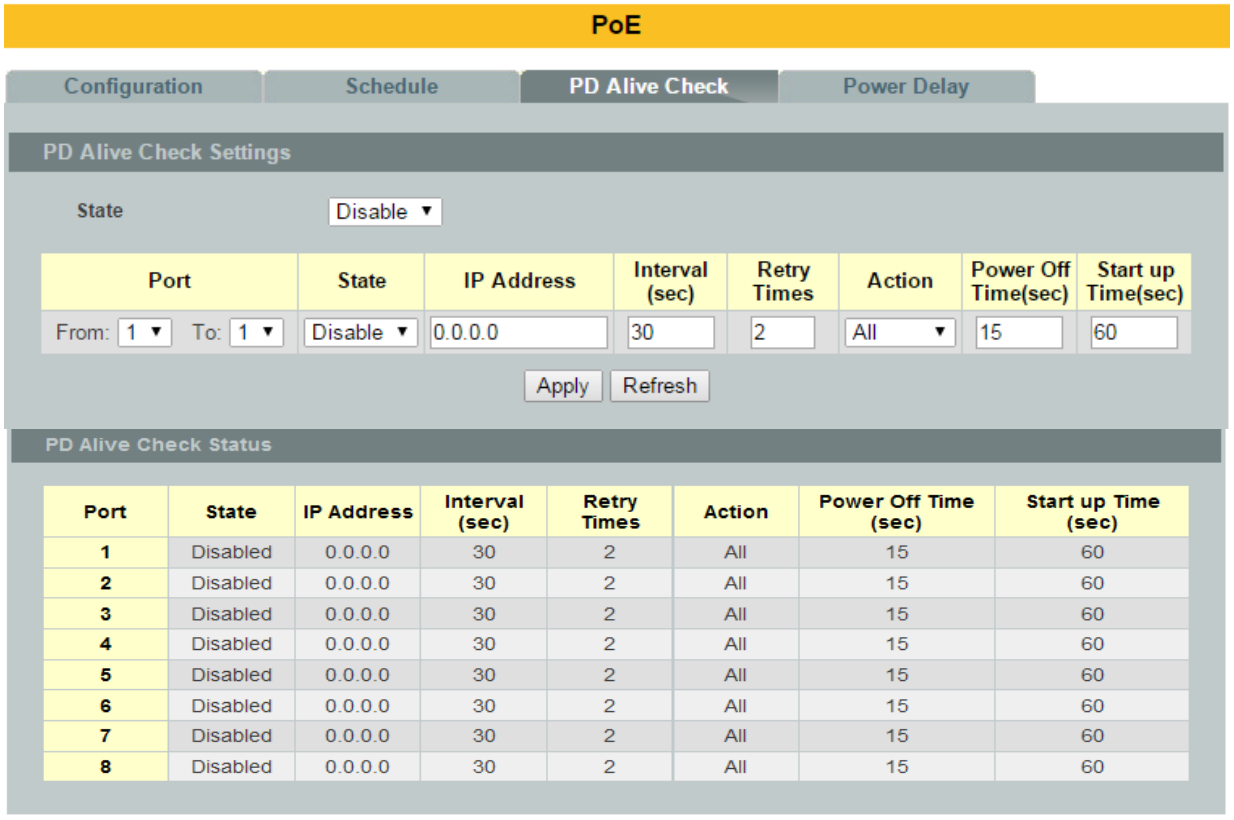
**Action:**
The action when the failure detection.
**All: S**end an alarm message to inform the administrator and then reboot the PD.
**Alarm**: Just send an alarm message to inform the administrator.
**None**: Keep Ping the remote PD but does nothing further.
**Reboot**: Cut off the power of the PoE port, make PD rebooted.

#### 6.11.3.2. 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\|none) | 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 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. |
| Interface | pd-alive power-off-time VALUE startup-time VALUE | This command configures the power-off time and startup time. |

### 6.11.3.3. 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 Time | 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 /None. |
| Power Off Time | When PD has been rebooted, the PoE port restored power after the Power Off Time time. |
| Start Up Time | The Switch waits the Start Up Time to do PoE Auto Checking when the PD is rebooting. |
| Apply | Click **Apply** to take effect the settings. |
| Refresh | Click **Refresh** to begin configuring this screen afresh. |

### 6.11.4. Power Delay

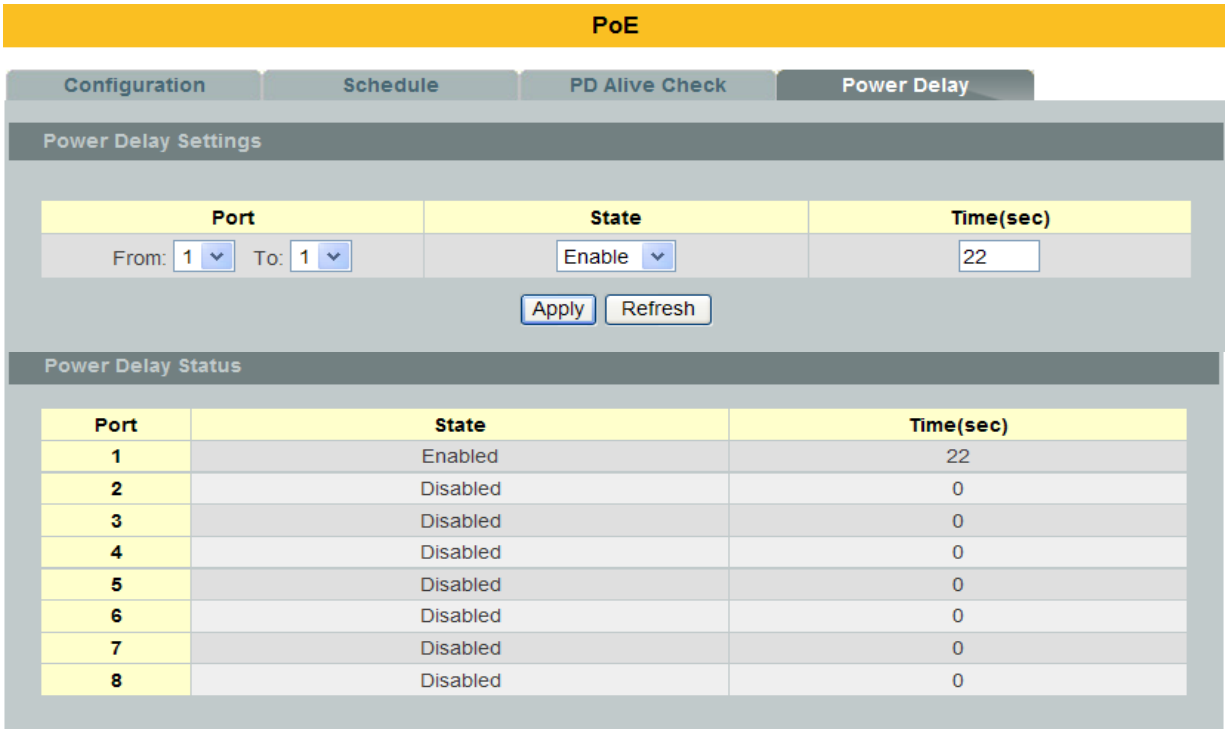
#### 6.11.4.1. Introduction

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

#### 6.11.4.2. 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. |

### 6.11.4.3. 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. |

**Notice**: The high priority port should have low value for power delay.

## 6.12. Static Route

### 6.12.1. Introduction

**Static routes**, which define explicit paths between two routers, cannot be automatically updated; you must manually reconfigure static routes when network changes occur. Static routes use less bandwidth than dynamic routes. No CPU cycles are used to calculate and analyze routing updates.

**IP forwarding**

IP forwarding provides on end to end delivery of IP packet between hosts with help of routers. Routing database plays import role in forwarding the packets. Routers populate its routing database either by manual configurations or by using dynamic routing protocols.
IP forwarding works as router as well as Inter VLAN routing with trunk stick.
Manual routing configurations are called as Static routes. Static routes are permanent routes; we can delete those routes with manual configurations only.

Whenever an IP packet received by a router then it fetches destination IP address and it will do the lookup in routing table to find the longest prefix match route. Packet is forwarded on the assigned next-hop in the route.

### 6.12.2. CLI configuration

| Node | Command | Description |
|---|---|---|
| enable | show ip forwarding status | This command displays the current configuration of the ip forwarding status. |
| enable | show ip routes (all\|ipv4\|ipv6) | This command displays the configurations of IPv4 or IPv6 or both routes from routing table. |
| enable | show ip arp (all\|ipv4\|ipv6) | This command displays dynamic and static IPv4 or IPv6 or both ARP entries in ARP table. |
| enable | show ip hosts (all\|ipv4\|ipv6) | This command displays assigned IPv4 or IPv6 or both addresses for interfaces in router. |
| configure | ip forwarding enable | This command enables layer 3 IPv4 and IPv6 forwarding/routing globally. |
| configure | no ip forwarding enable | This command disables layer 3 IPv4 and IPv6 forwarding/routing globally.<br>This will delete all assigned IP addresses and static routes from interfaces. |
| configure | ip arp proxy enable | This command enables route to act as an ARP proxy globally; It will be useful in InterVLAN routing. |
| configure | no ip arp proxy enable | This command disables route to act as an ARP proxy. |
| configure | ipv4 arp <IPv4_ADDR> <MAC_ADDR> | This command allows adding static IPv4 ARP entry in ARP table. |
| configure | ip6 arp <IPv6_ADDR> <MAC_ADDR> | This command allows adding static IPv6 ARP entry in ARP table. |
| configure | no ipv4 arp | This command deletes a static IPv4 ARP entry from |

| | | |
|---|---|---|
| | <IPv4_ADDR> <MAC_ADDR> | ARP table. |
| configure | no ipv6 arp <IPv6_ADDR> <MAC_ADDR> | This command deletes a static IPv6 ARP entry from ARP table. |
| configure | interface vlan VLAN-ID | This command enters the L3 interface node. |
| L3 interface | ipv4 address A.B.C.D/M | This command assigns a specified IPv4 interface route to the interface.<br>We can assign multiple IPv4 interface route to a single interface with different IP segment.<br>If this configuration is a first IP assigning to the interface then automatically interface is enabled for routing. |
| L3 interface | ipv6 address <IPv6_ADDR>/M | This command assigns a specified IPv6 interface route to the interface.<br>We can assign only one IPv6 interface route for an interface vlan.<br>If this configuration is a first IP assigning to the interface then it automatically enables the interface with routing. |
| L3 interface | no ipv4 address A.B.C.D/M | This command deletes a specified IPv4 interface route from the interface vlan.<br>This command deletes all dependent static routes on the specified IPv4 interface route.<br>If there is no assigned IP addresses for the specified interface after deleting then it will automatically disables routing in interface. |
| L3 interface | no ipv4 address <IPv6_ADDR>/M | This command deletes a specified IPv6 interface route from the interface.<br>This command deletes all dependent static routes on the specified IPv6 interface route.<br>If there is no assigned IP addresses for the specified interface after deleting then it will automatically disables routing in interface vlan. |
| L3 interface | ipv4 route A.B.C.D/M A.B.C.D | This command configures an IPv4 static route onto the specified interface vlan. |
| L3 interface | ipv6 route <IPv6_ADDR>/M <IPv6_ADDR> | This command configures an IPv6 static route onto the specified interface vlan. |
| L3 interface | no ipv4 route A.B.C.D/M A.B.C.D | This command deletes a specified IPv4 static route from an interface vlan. |
| L3 interface | no ipv6 route <IPv6_ADDR>/M <IPv6_ADDR> | This command deletes a specified IPv6 static route from an interface vlan. |

**Example:**

- IP Forwarding Enable: This command is used to enable ip forwarding (routing).
  L2SWITCH(config)#ip forwarding enable

- IP Forwarding Disable: This command is used to disable ip forwarding.
  L2SWITCH(config)#no ip forwarding enable

- ARP proxy enable: This command is used to enable ARP proxy.
  L2SWITCH(config)#ip arp proxy enable

- ARP proxy disable: This command is used to disable ARP proxy.
  L2SWITCH(config)#no ip arp proxy enable

- Add a static IPv4/IPv6 ARP entry: This command is used to add a static IPv4/IPv6 ARP entries.
  L2SWITCH(config)#ipv4 arp 192.168.20.1 00:11:22:33:44:55
  L2SWITCH(config)#ipv6 arp 1234:ab::ccdd 00:11:22:33:44:55

- Deletes a static IPv4/IPv6 ARP entry: This command is used to delete static IPv4/IPv6 ARP entries
  L2SWITCH(config)#no ipv4 arp 192.168.20.1 00:11:22:33:44:55
  L2SWITCH(config)#no ipv6 arp 1234:ab::ccdd 00:11:22:33:44:55

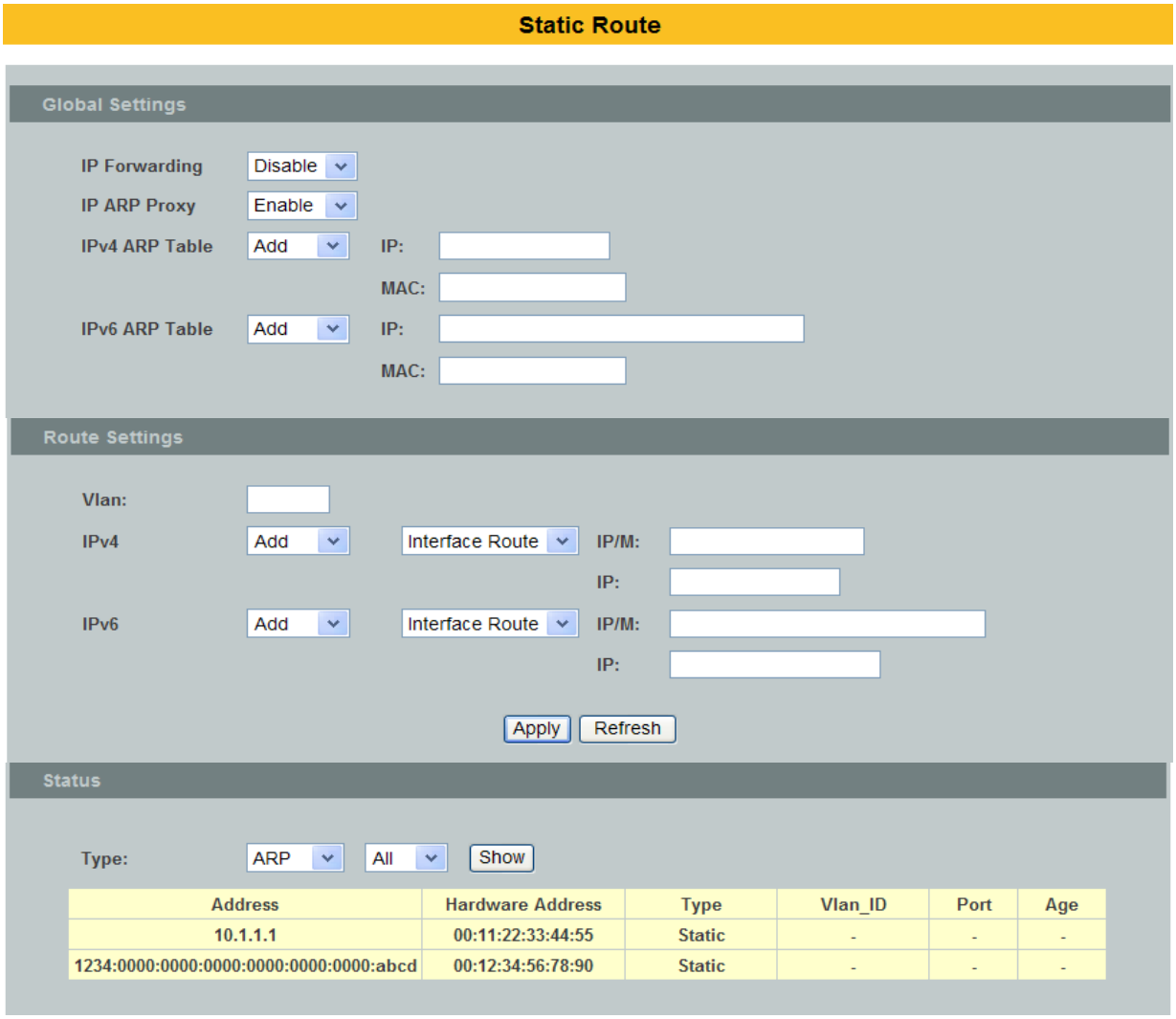
- Assigning a IPv4/IPv6 interface router: This command is used to add an IPv4/IPv6 interface route to a interface vlan.
  L2SWITCH(config)#interface vlan 1
  L2SWITCH(config-if-vlan-l3)#
  L2SWITCH(config-if-vlan-l3)#ipv4 address 192.168.20.1/24
  L2SWITCH(config-if-vlan-l3)#ipv6 address 1234:ab::ccdd/120

- Deleting IPv4/IPv6 address: This command is used to delete an IPv4/IPv6 interface route from a interface vlan.
  L2SWITCH(config-if-vlan-l3)#no ipv4 address 192.168.20.1/24
  L2SWITCH(config-if-vlan-l3)#no ipv6 address 1234:ab::ccdd/120

- Adding static IPv4/IPv6 route: This command is used to add an IPv4/IPv6 static route to a interface vlan.
  L2SWITCH(config-if-vlan-l3)#ipv4 address 192.168.20.1/24 192.168.20.1
  L2SWITCH(config-if-vlan-l3)#ipv6 address 1234:ab::ccdd/120 1234:ab::ccdd

- Deleting static IPv4/IPv6 route: This command is used to delete an IPv4/IPv6 static route form an interface vlan.
  L2SWITCH(config-if-vlan-l3)#no ipv4 address 192.168.20.1/24 192.168.20.1
  L2SWITCH(config-if-vlan-l3)#no ipv6 address 1234:ab::ccdd/120 1234:ab::ccdd

### 6.12.3. Web configuration




| Parameter | Description |
|---|---|
| Global Settings | |
| IP Forwarding | Enables / disables the IP forwarding globally. |
| IP ARP Proxy | Enables / disables the route to act as an ARP proxy globally. |
| IPv4 ARP Table | Adds a static IPv4 ARP entry in the ARP table.<br>/ Deletes a static IPv4 ARP entry from the ARP table. |
| IP: | The IP address for the entry. |
| MAC: | The MAC address for the entry. |
| IPv6 ARP Table | Adds a static IPv6 ARP entry in the ARP table.<br>/ Deletes a static IPv6 ARP entry from the ARP table. |

| | |
|---|---|
| IP: | The IP address for the entry. |
| MAC: | The MAC address for the entry. |
| Route Settings | |
| vlan | Specifics an interface vlan. |
| IPv4 | Adds an IPv4 Interface Route / Static Route onto the interface vlan. / Deletes an IPv4 Interface Route / Static Route from the interface vlan.<br>Selects the route type, Interface Route or Static Route. |
| IP/M: | The IP address and the netmask for the entry. |
| IP: | The static route address for the Static Route type only. |
| IPv6 | Adds an IPv6 Interface Route / Static Route onto the interface vlan. / Deletes an IPv6 Interface Route / Static Route from the interface vlan.<br>Selects the route type, Interface Route or Static Route. |
| IP/M: | The IP address and the netmask for the entry. |
| IP: | The static route address for the Static Route type only. |
| Status | |
| | Shows the ARP table / Host table / Route configurations. |

## 6.13. STP

### 6.13.1. STP/RSTP

#### 6.13.1.1. Introduction

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

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

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

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

notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database.
In STP, the port states are Blocking, Listening, Learning, Forwarding.
In RSTP, the port states are Discarding, Learning, and Forwarding.

**Note**: In this document, "STP" refers to both STP and RSTP.

**STP Terminology**

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

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

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

**Forward Time (Forward Delay):**

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

**Max Age:**

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

**Hello Time:**

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

**PathCost:**

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

**How STP Works?**

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

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

**802.1D STP**

The Spanning Tree Protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN. It is based on an algorithm invented by Radia Perlman while working for Digital Equipment Corporation. In the OSI model for computer networking, STP falls under the OSI layer-2. Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links. Bridge loops must be avoided because they result in flooding the network.

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

STP switch port states

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

- Disabled - Not strictly part of STP, a network administrator can manually disable a port

**802.1w RSTP**

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

RSTP bridge port roles:

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

**Edge Port:**

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

**Forward Delay**:

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

**Transmission Limit:**

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

**Hello Time:**

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

**Bridge priority:**

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

**Port Priority:**

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

value is from 0 to 240.

**Path Cost:**

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

**BPDU Guard**

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

**BPDU Filter**

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

***Notice:***

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

**Root Guard**

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

**Default Settings**

STP/RSTP : disabled.
STP/RSTP mode : RSTP.
Forward Time : 15 seconds.
Hello Time : 2 seconds.
Maximum Age : 20 seconds.
System Priority : 32768.
Transmission Limit : 3 seconds.
Per port STP state : enabled.
Per port Priority : 128.
Per port Edge port : disabled.
Per port BPDU filter : disabled.
Per port BPDU guard : disabled.
Per port BPDU Root guard: disabled.
Per port Path Cost : depend on port link speed.
Example: Bandwidth -> STP Port Cost Value
10 Mbps -> 100
100 Mbps-> 19
1 Gbps -> 4
10 Gbps -> 2

### 6.13.1.2.CLI Configuration

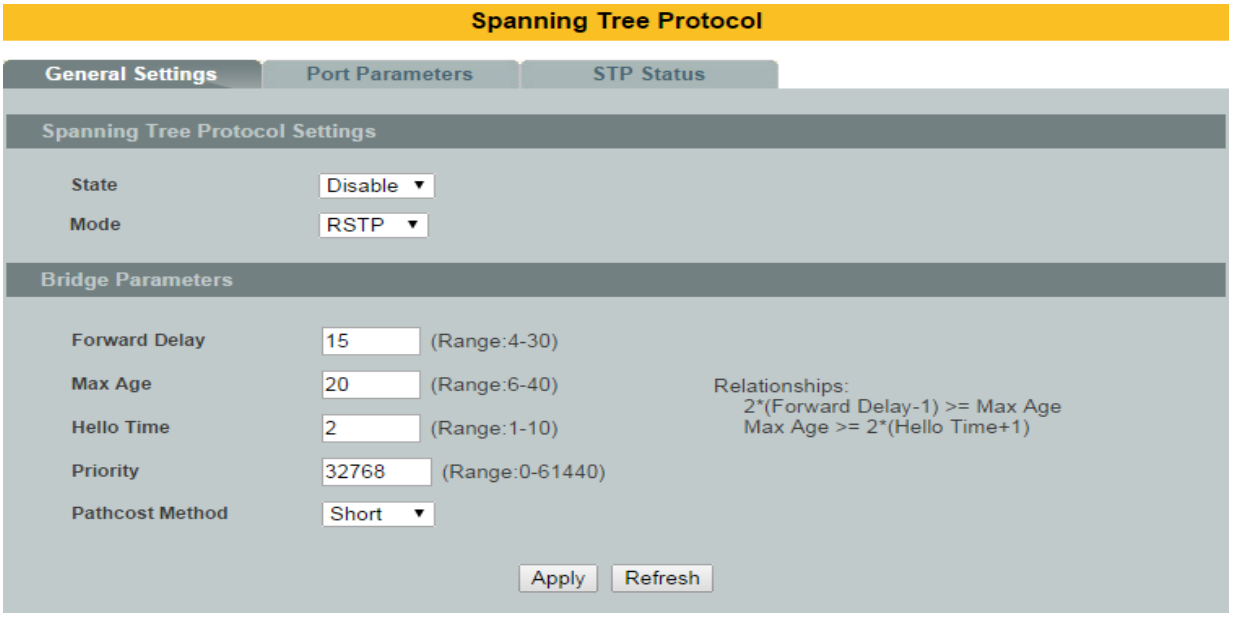
| Node | Command | Description |
|---|---|---|
| enable | show spanning-tree active | This command displays the spanning tree information for only active port(s) |
| enable | show spanning-tree blockedports | This command displays the spanning tree information for only blocked port(s) |
| enable | show spanning-tree port detail PORT_ID | This command displays the spanning tree information for the interface port. |
| enable | show spanning-tree statistics PORT_ID | This command displays the spanning tree information for the interface port. |
| enable | show spanning-tree summary | This command displays the summary of port states and configurations |
| enable | clear spanning-tree counters | This command clears spanning-tree statistics for all ports. |
| enable | clear spanning-tree counters PORT_ID | This command clears spanning-tree statistics for a specific port. |
| configure | spanning-tree (disable \| enable) | This command disables / enables the spanning tree function for the system. |
| configure | spanning-tree algorithm-timer forward-time TIME max-age TIME hello-time TIME | This command configures the bridge times (forward-delay,max-age,hello-time). |
| configure | no spanning-tree algorithm-timer | This command configures the default values for forward-time & max-age & hello-time. |
| configure | spanning-tree forward-time <4-30> | This command configures the bridge forward delay time (sec). |
| configure | no spanning-tree forward-time | This command configures the default values for forward-time. |
| configure | spanning-tree hello-time <1-10> | This command configures the bridge hello time(sec). |
| configure | no spanning-tree hello-time | This command configures the default values for hello-time. |
| configure | spanning-tree max-age <6-40> | This command configures the bridge message max-age time(sec). |
| configure | no spanning-tree max-age | This command configures the default values for max-age time. |
| configure | spanning-tree mode (rstp\|stp) | This command configures the spanning mode. |
| configure | spanning-tree pathcost method (short\|long) | This command configures the pathcost method. |
| configure | spanning-tree priority <0-61440> | This command configures the priority for the system. |
| configure | no spanning-tree priority | This command configures the default values for the system priority. |

| | | |
|---|---|---|
| interface | spanning-tree (disable\|enable) | This command configures enables/disables the STP function for the specific port. |
| interface | spanning-tree bpdufilter (disable\|enable) | This command configures enables/disables the bpdufilter function for the specific port. |
| interface | spanning-tree bpduguard (disable\|enable) | This command configures enables/disables the bpduguard function for the specific port. |
| interface | spanning-tree rootguard (disable\|enable) | This command enables/disables the BPDU Root guard port setting for the specific port. |
| interface | spanning-tree edge-port (disable\|enable) | This command enables/disables the edge port setting for the specific port. |
| interface | spanning-tree cost VALUE | This command configures the cost for the specific port.<br>Cost range:<br>16-bit based value range 1-65535,<br>32-bit based value range 1-200000000. |
| interface | no spanning-tree cost | This command configures the path cost to default for the specific port. |
| interface | spanning-tree port-priority <0-240> | This command configures the port priority for the specific port.<br>Default: 128. |
| interface | no spanning-tree port-priority | This command configures the port priority to default for the specific port. |
| configure | interface range gigabitethernet1/0/ PORTLISTS | This command enters the interface configure node. |
| if-range | spanning-tree (disable\|enable) | This command configures enables/disables the STP function for the specific port. |
| if-range | spanning-tree bpdufilter (disable\|enable) | This command configures enables/disables the bpdufilter function for the specific port. |
| if-range | spanning-tree bpduguard (disable\|enable) | This command configures enables/disables the bpduguard function for the specific port. |
| if-range | spanning-tree rootguard (disable\|enable) | This command enables/disables the BPDU Root guard port setting for the specific port. |
| if-range | spanning-tree edge-port (disable\|enable) | This command enables/disables the edge port setting for the specific port. |
| if-range | spanning-tree cost VALUE | This command configures the cost for the specific port.<br>Cost range:<br>16-bit based value range 1-65535,<br>32-bit based value range 1-200000000. |
| if-range | no spanning-tree cost | This command configures the path cost to default for the specific port. |

| | | |
|---|---|---|
| if-range | spanning-tree port-priority <0-240> | This command configures the port priority for the specific port.<br>Default: 128. |
| if-range | no spanning-tree port-priority | This command configures the port priority to default for the specific port. |

#### 6.13.1.3. Web Configuration

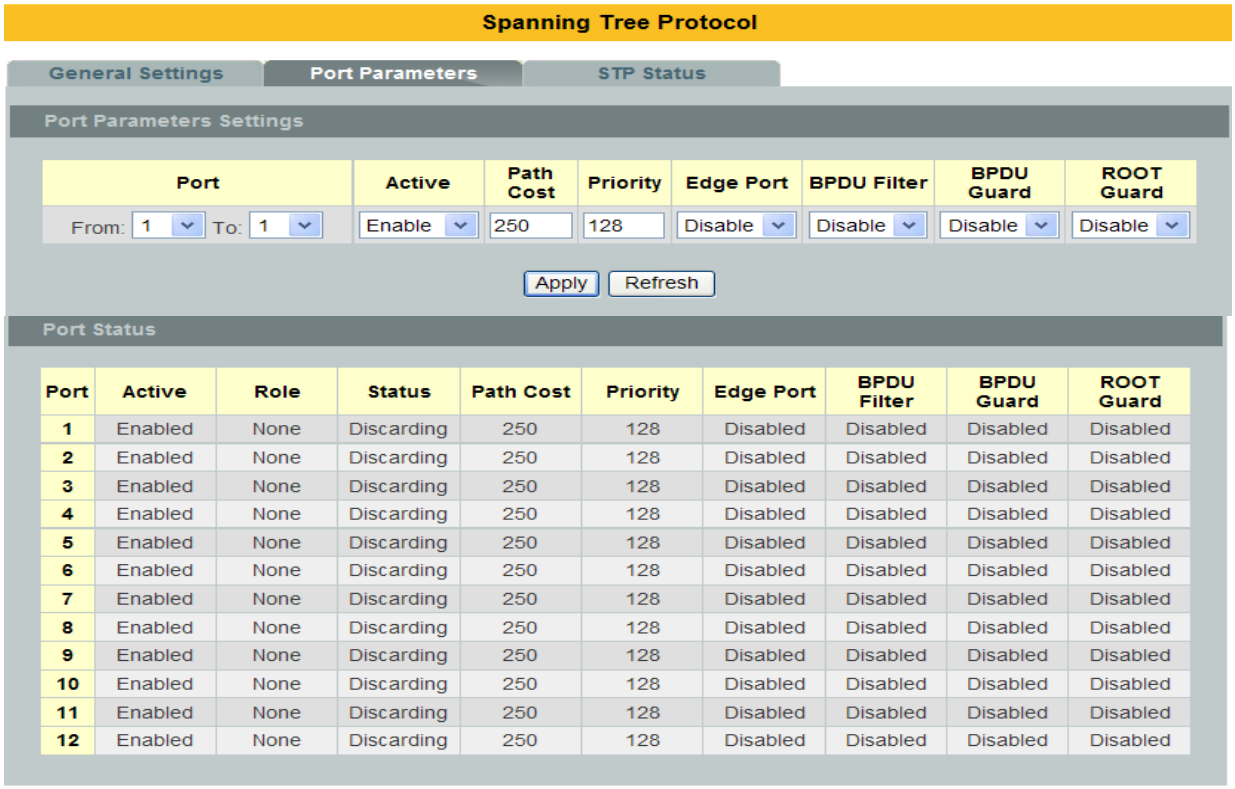
**General Settings**




| Parameter | Description |
|---|---|
| State | Select **Enabled** to use Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP). |
| Mode | Select to use either Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP). |
| Forward Time | This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. |
| Max Age | This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals.<br>Any port that age out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds. |
| Hello Time | This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 |

| | |
|---|---|
| | to 10 seconds. |
| Priority | Priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch.<br>Enter a value from 0~61440.<br>The lower the numeric value you assign, the higher the priority for this bridge. Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay. |
| Pathcost | Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost. |

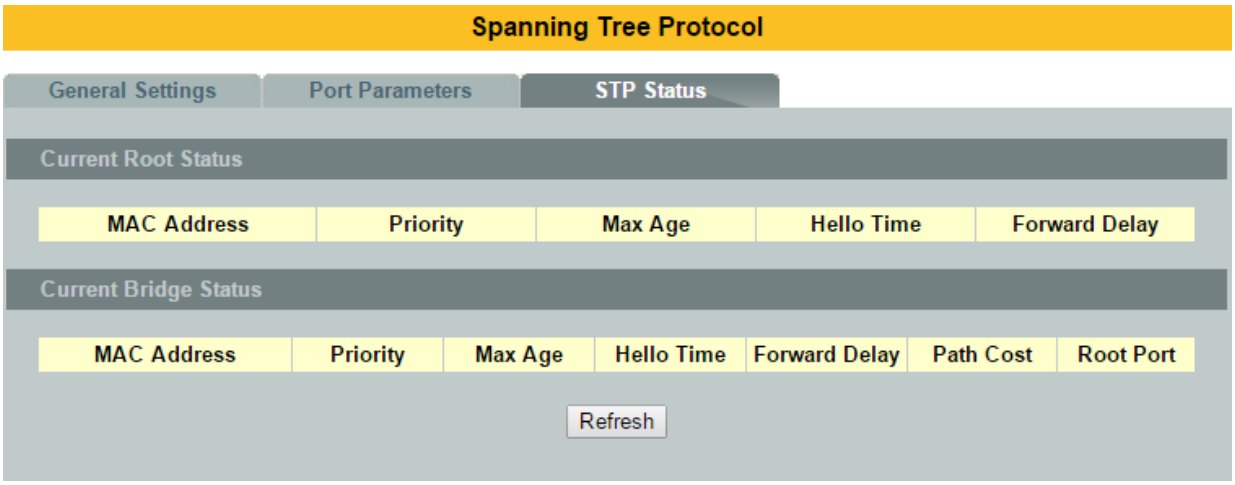
**Port Parameters**




| Parameter | Description |
|---|---|
| Port | Selects a port that you want to configure. |
| Active | Enables/Disables the spanning tree function for the specific port. |
| Path Cost | Configures the path cost for the specific port. |
| Priority | Configures the priority for the specific port. |
| Edge Port | Configures the port type for the specific port. Edge or Non-Edge. |

| | |
|---|---|
| BPDU Filter | Enables/Disables the BPDU filter function for the specific port. |
| BPDU Guard | Enables/Disables the BPDU guard function for the specific port. |
| ROOT Guard | Enables/Disables the BPDU root guard function for the specific port. |
| Port Status | |
| Active | The state of the STP function. |
| Role | The port role. Should be one of the Alternated / Designated / Root / Backup / None. |
| Status | The port's status. Should be one of the Discarding / Blocking / Listening / Learning / Forwarding / Disabled. |
| Path Cost | The port's path cost. |
| Priority | The port's priority. |
| Edge Port | The state of the edge function. |
| BPDU Filter | The state of the BPDU filter function. |
| BPDU Guard | The state of the BPDU guard function. |
| ROOT Guard | The state of the BPDU Root guard function. |

## STP Status




| Parameter | Description |
|---|---|
| Current Root Status | |
| MAC address | This is the MAC address of the root bridge. |
| Priority | **Root** refers to the base of the spanning tree (the root bridge). This field displays the root bridge's priority. This Switch may also be the root bridge. |
| MAX Age | This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure. |
| Hello Time | This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay. |
| Forward Delay | This is the time (in seconds) the root switch will wait before changing states. |
| Current Bridge Status | |
| MAC address | This is the MAC address of the current bridge. |
| Priority | Priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay. |
| MAX Age | This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that age out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. |

| | |
|---|---|
| Hello Time | This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. |
| Forward Delay | This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. |
| Path Cost | Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost. |
| Root Cost | This is the number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree. |

### 6.13.2. MSTP

#### 6.13.2.1.Introduction

MSTP (IEEE 802.1S Multiple STP), which uses RSTP for rapid convergence, enables VLANs to be grouped into a spanning-tree instance, with each instance having a spanning-tree topology independent of other spanning-tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning-tree instances required to support a large number of VLANs.

**Multiple Spanning-Tree Regions:**
For switches to participate in multiple spanning-tree (MST) instances, you must consistently configure the switches with the same MST configuration information. A collection of interconnected switches that have the same MST configuration comprises an MST region. The MST configuration determines to which MST region each switch belongs. The configuration includes the name of the region, the revision number, and the MST instance-to-VLAN assignment map. You configure the switch for a region by using the spanning-tree mst configuration global configuration command, after which the switch enters the MST configuration mode. From this mode, you can map VLANs to an MST instance by using the instance MST configuration command, specify the region name by using the name MST configuration command, and set the revision number by using the revision MST configuration command.

A region can have one member or multiple members with the same MST configuration; each member must be capable of processing RSTP BPDUs. There is no limit to the number of MST regions in a network, but each region can support up to 16 spanning-tree instances. You can assign a VLAN to only one spanning-tree instance at a time.

**Boundary Ports**
A boundary port is a port that connects an MST region to a single spanning-tree region running RSTP, or to a single spanning-tree region running 802.1D, or to another MST region with a

different MST configuration. A boundary port also connects to a LAN, the designated switch of which is either a single spanning-tree switch or a switch with a different MST configuration.

At the boundary, the roles of the MST ports do not matter, and their state is forced to be the same as the IST port state (MST ports at the boundary are in the forwarding state only when the IST port is forwarding). An IST port at the boundary can have any port role except a backup port role.

On a shared boundary link, the MST ports wait in the blocking state for the forward-delay time to expire before transitioning to the learning state. The MST ports wait another forward-delay time before transitioning to the forwarding state.

- ✓ If the boundary port is on a point-to-point link and it is the IST root port, the MST ports transition to the forwarding state as soon as the IST port transitions to the forwarding state.
- ✓ If the IST port is a designated port on a point-to-point link and if the IST port transitions to the forwarding state because of an agreement received from its peer port, the MST ports also immediately transition to the forwarding state.
- ✓ If a boundary port transitions to the forwarding state in an IST instance, it is forwarding in all MST instances, and a topology change is triggered. If a boundary port with the IST root or designated port role receives a topology change notice external to the MST cloud, the MSTP switch triggers a topology change in the IST instance and in all the MST instances active on that port.

**Interoperability with 802.1D STP:**
A switch running MSTP supports a built-in protocol migration mechanism that enables it to interoperate with legacy 802.1D switches. If this switch receives a legacy 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only 802.1D BPDUs on that port. An MSTP switch can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MSTP BPDU (version 3) associated with a different region, or an RSTP BPDU (version 2).

However, the switch does not automatically revert to the MSTP mode if it no longer receives 802.1D BPDUs because it cannot determine whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. Also, a switch might continue to assign a boundary role to a port when the switch to which this switch is connected has joined the region. To restart the protocol migration process (force the renegotiation with neighboring switches), you can use the clear spanning-tree detected-protocols privileged EXEC command.

If all the legacy switches on the link are RSTP switches, they can process MSTP BPDUs as if they are RSTP BPDUs. Therefore, MSTP switches send either a version 0 configuration and TCN BPDUs or version 3 MSTP BPDUs on a boundary port. A boundary port connects to a LAN, the designated switch of which is either a single spanning-tree switch or a switch with a different MST configuration.

#### 6.13.2.2. CLI Configurations

| Node | Command | Description |
|---|---|---|
| enable | show spanning-tree mst configuration | This command displays the MSTP configurations. |

| | | |
|---|---|---|
| enable | show spanning-tree mst instance | This command displays all of the instance configurations of the MSTP. |
| enable | show spanning-tree mst instance <0-63> | This command displays specific instance configurations of the MSTP. |
| enable | show spanning-tree mst instance <0-63> interface IFNAME | This command displays specific instance configurations on an interface of the MSTP. |
| enable | show spanning-tree mst interface IFNAME | This command displays the configurations on an interface of the MSTP. |
| enable | show spanning-tree mst root | This command displays the root bridge configurations. |
| configure | spanning-tree (disable\|enable) | This command enables / disables the spanning tree. |
| configure | spanning-tree mode mst | This command configures the mode of the spanning tree. (one of the three modes STP/RSTP/MSTP.) |
| configure | spanning-tree mst forward-time | This command configures the forward time for the MSTP. |
| configure | no spanning-tree mst forward-time | This command resets the forward time for the MSTP. The default forward delay time is 15 seconds. |
| configure | spanning-tree mst hello-time | This command configures the hello time for the MSTP. |
| configure | no spanning-tree mst hello-time | This command resets the hello time for the MSTP. The default hello time is 2 seconds. |
| configure | spanning-tree mst max-age | This command configures the maximum age time for the MSTP. |
| configure | no spanning-tree mst max-age | This command resets the maximum age time for the MSTP. The default maximum age time is 20 seconds. |
| configure | spanning-tree mst max-hops | This command configures the maximum hop count. |
| configure | no spanning-tree mst max-hops | This command resets the maximum hop count. The default maximum hop count is 20. |
| configure | spanning-tree mst instance STRING priority <0-61440> | This command resets the maximum hop count. The default maximum hop count is 20. |
| configure | no spanning-tree mst instance STRING priority | This command resets the priority for the specific instance. |
| interface | spanning-tree mst instance STRING cost <1-200000000> | This command configures a cost on the specific port for the MSTP. |
| interface | no spanning-tree mst instance STRING cost | This command resets the cost on the specific port for the MSTP. |
| interface | spanning-tree mst | This command configures a priority on the specific port |

| | | |
|---|---|---|
| | instance STRING port-priority <0-240> | for the MSTP. |
| interface | no spanning-tree mst instance STRING port-priority | This command resets the priority on the specific port for the MSTP. |
| configure | spanning-tree mst configuration | This command enters the MSTP configure node. |
| configure | no spanning-tree mst configuration | This command resets all of configurations for the MSTP. |
| mst | apply | This command applies configurations to current instant. |
| mst | instance | This command configures the instance and vlan map. |
| mst | name | This command configures a region name for the MSTP. |
| mst | no name | This command reset the region name for the MSTP. |
| mst | revision | This command configures the revision for the MSTP. |
| mst | no revision | This command resets the revision for the MSTP. |
| mst | show (current \| pending) | This command shows the MSTP configures.<br>Current – the working configurations.<br>Pending – the not applied configurations. |

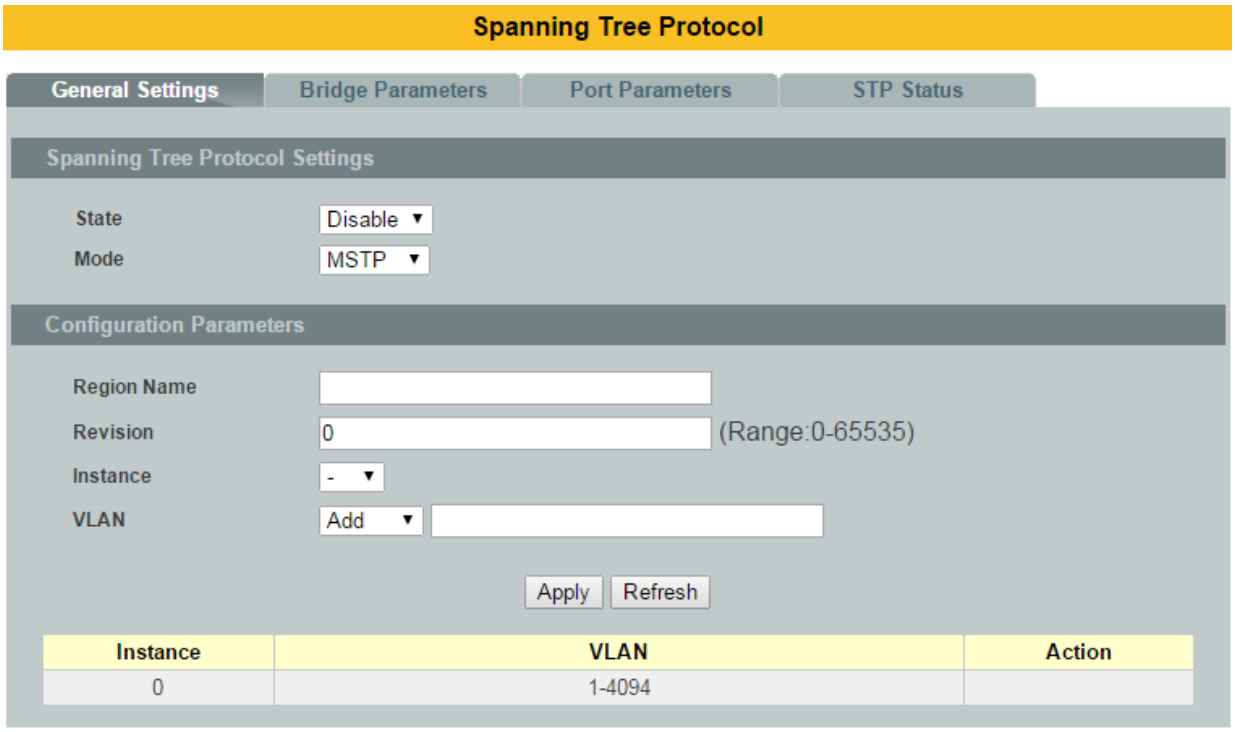
**Specifying the MST Region Configuration and Enabling MSTP**

For two or more switches to be in the same MST region, they must have the same VLAN-to-instance mapping, the same configuration revision number, and the same name. A region can have one member or multiple members with the same MST configuration; each member must be capable of processing RSTP BPDUs. There is no limit to the number of MST regions in a network, but each region can support up to 16 spanning-tree instances. You can assign a VLAN to only one spanning-tree instance at a time.

```
L2SWITCH(config)#spanning-tree mst configuration
L2SWITCH(config-mst)#name MSTP
L2SWITCH(config-mst)#revision 1
L2SWITCH(config-mst)#instance 1 vlan 1-10
```

### 6.13.2.3. Web Configurations

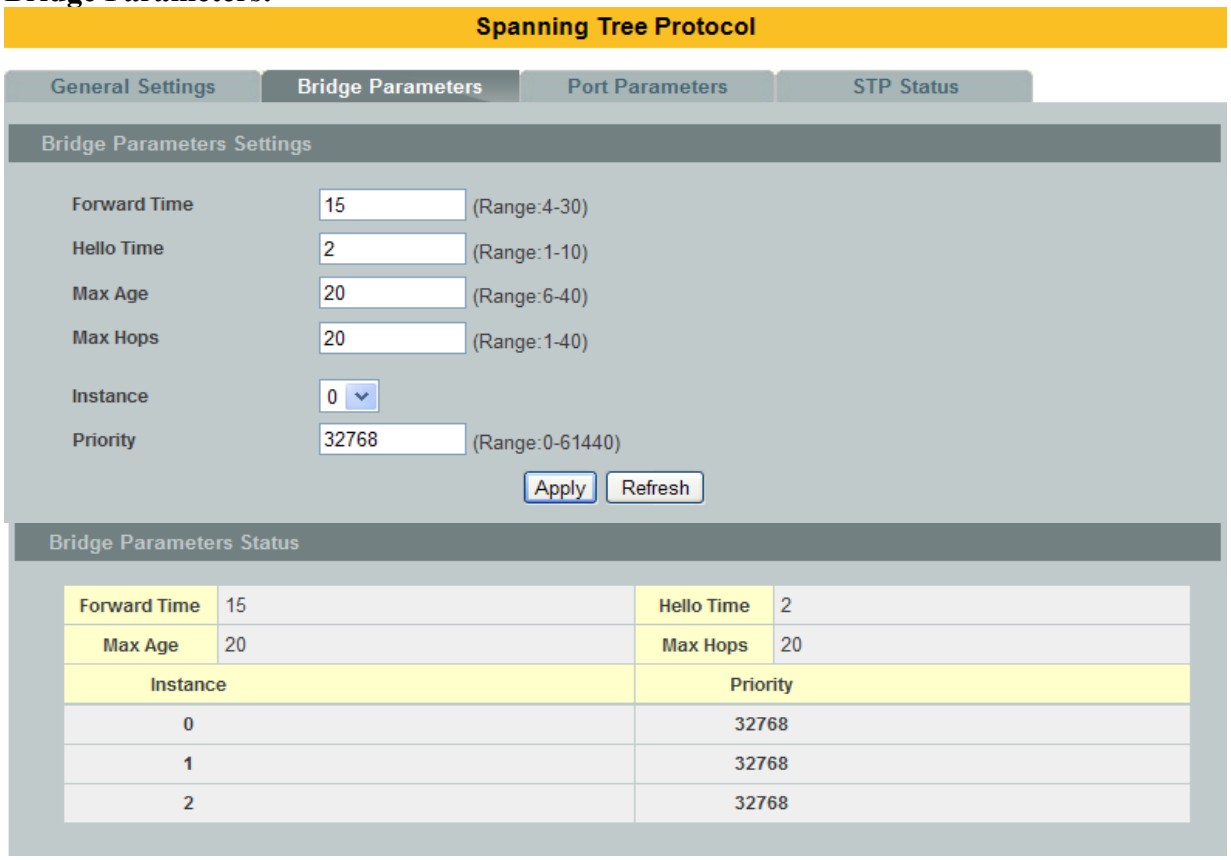
**General Settings:**




| Parameter | Description |
|---|---|
| State | Select **Enabled** to use Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) or Multiple Spanning Tree Protocol (MSTP). |
| Mode | Selects the Spanning Tree running mode.<br>STP - Spanning Tree Protocol.<br>RSTP - Rapid Spanning Tree Protocol.<br>MSTP - Multiple Spanning Tree Protocol. |
| Configuration Parameters | |
| Region Name | Configures the region name for the Switch. |
| Revision | Configures the revision for the Switch. |
| Instance | Selects an instance which you want to configure. |
| VLAN | Select one or more vlans which will join the instance.<br>Note: the vlan will be removed from instance 0 automatically. |
| **Instance and vlan map table** | |
| Instance | The instance. |
| VLAN | The vlan in the instance. |

| | |
|---|---|
| Action | Click Delete button to delete this instance. |

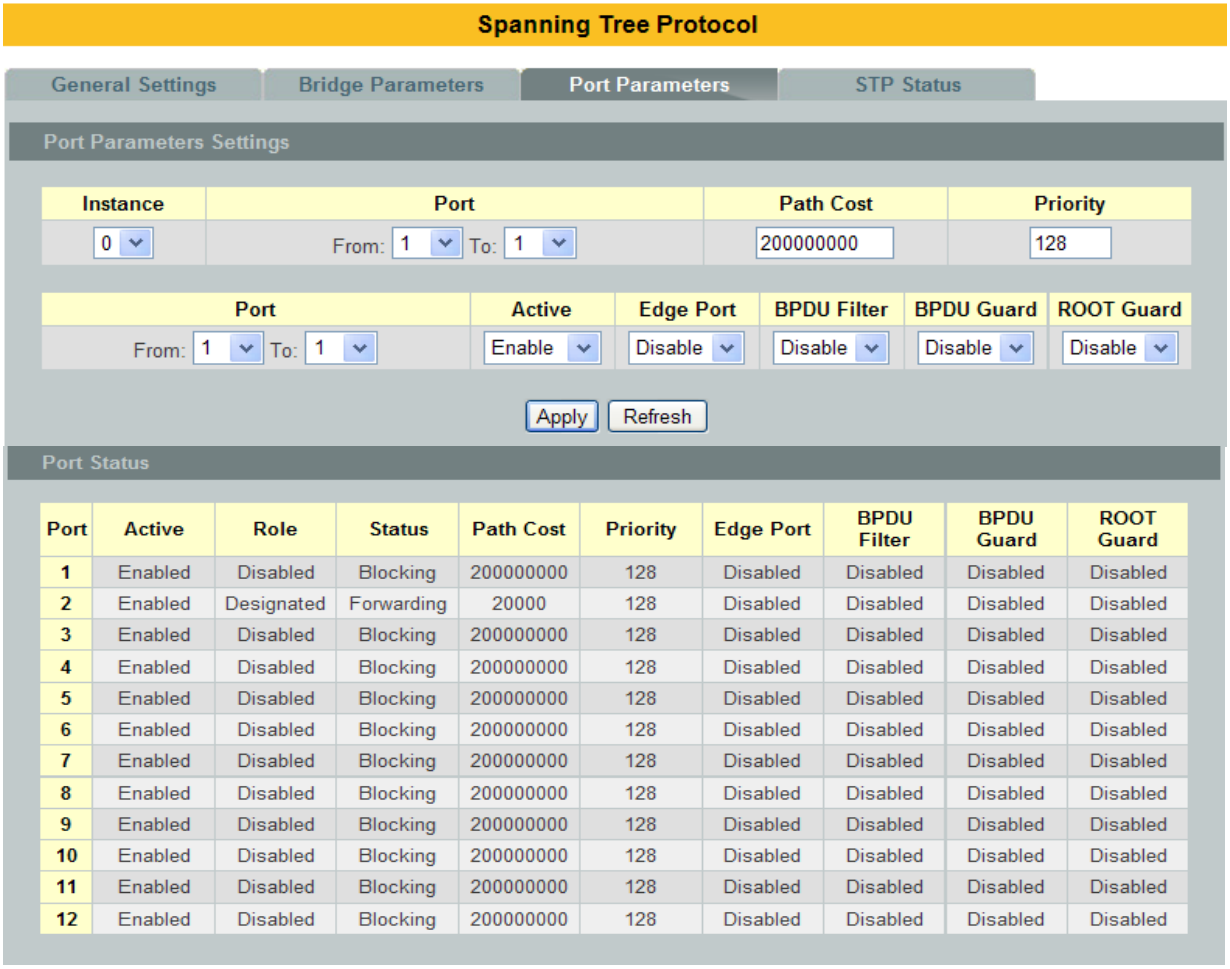
**Bridge Parameters:**




| Parameter | Description |
|---|---|
| Forward Time | This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. |
| Hello Time | This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds. |
| Max Age | This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals.<br>Any port that age out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the |

| | |
|---|---|
| | network. The allowed range is 6 to 40 seconds. |
| Max Hops | |
| Instance | Selects an instance which you want to configure. |
| Priority | Configures the priority for the instance.<br>Priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch.<br>Enter a value from 0~61440.<br>The lower the numeric value you assign, the higher the priority for this bridge.<br>Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay. |

**Port Parameters:**

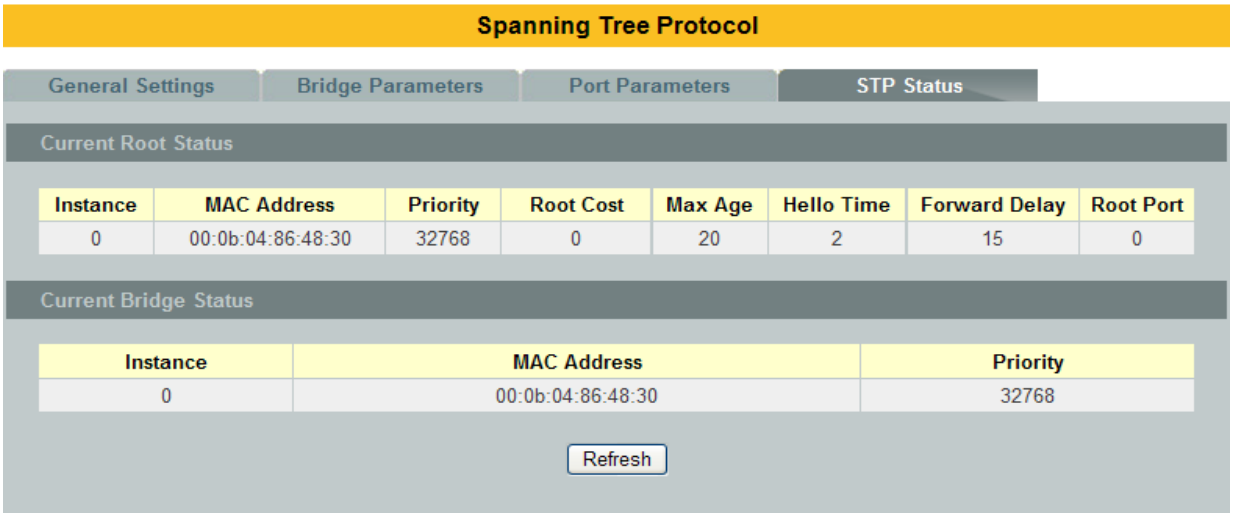



| Port | Active | Role | Status | Path Cost | Priority | Edge Port | BPDU Filter | BPDU Guard | ROOT Guard |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Enabled | Disabled | Blocking | 200000000 | 128 | Disabled | Disabled | Disabled | Disabled |
| 2 | Enabled | Designated | Forwarding | 20000 | 128 | Disabled | Disabled | Disabled | Disabled |
| 3 | Enabled | Disabled | Blocking | 200000000 | 128 | Disabled | Disabled | Disabled | Disabled |
| 4 | Enabled | Disabled | Blocking | 200000000 | 128 | Disabled | Disabled | Disabled | Disabled |
| 5 | Enabled | Disabled | Blocking | 200000000 | 128 | Disabled | Disabled | Disabled | Disabled |
| 6 | Enabled | Disabled | Blocking | 200000000 | 128 | Disabled | Disabled | Disabled | Disabled |
| 7 | Enabled | Disabled | Blocking | 200000000 | 128 | Disabled | Disabled | Disabled | Disabled |
| 8 | Enabled | Disabled | Blocking | 200000000 | 128 | Disabled | Disabled | Disabled | Disabled |
| 9 | Enabled | Disabled | Blocking | 200000000 | 128 | Disabled | Disabled | Disabled | Disabled |
| 10 | Enabled | Disabled | Blocking | 200000000 | 128 | Disabled | Disabled | Disabled | Disabled |
| 11 | Enabled | Disabled | Blocking | 200000000 | 128 | Disabled | Disabled | Disabled | Disabled |
| 12 | Enabled | Disabled | Blocking | 200000000 | 128 | Disabled | Disabled | Disabled | Disabled |

| Parameter | Description |
|---|---|

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

**STP Status:**




| Parameter | Description |
|---|---|
| Current Root Status | |
| Instance | The Instance ID. |
| MAC address | This is the MAC address of the root bridge. |
| Priority | **Root** refers to the base of the spanning tree (the root bridge). This field displays the root bridge's priority. This Switch may also be the root bridge. |
| Root Cost | This is the path cost to the root bridge. |
| MAX Age | This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure. |
| Hello Time | This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay. |
| Forward Delay | This is the time (in seconds) the root switch will wait before changing states. |
| Root Port | This is the port to the root bridge. |
| Current Bridge Status | |
| Instance | This is the MAC address of the current bridge. |
| MAC address | This is the MAC address of the bridge. |
| Priority | This is the priority of the Switch. |

## 6.14. Xpress Ring

### 6.14.1. Introduction

The Xpress-Ring is a fast-acting, self-healing ring recovery technology that enables networks to recover from link failure within 10ms.

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

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

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

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

**Default Settings**

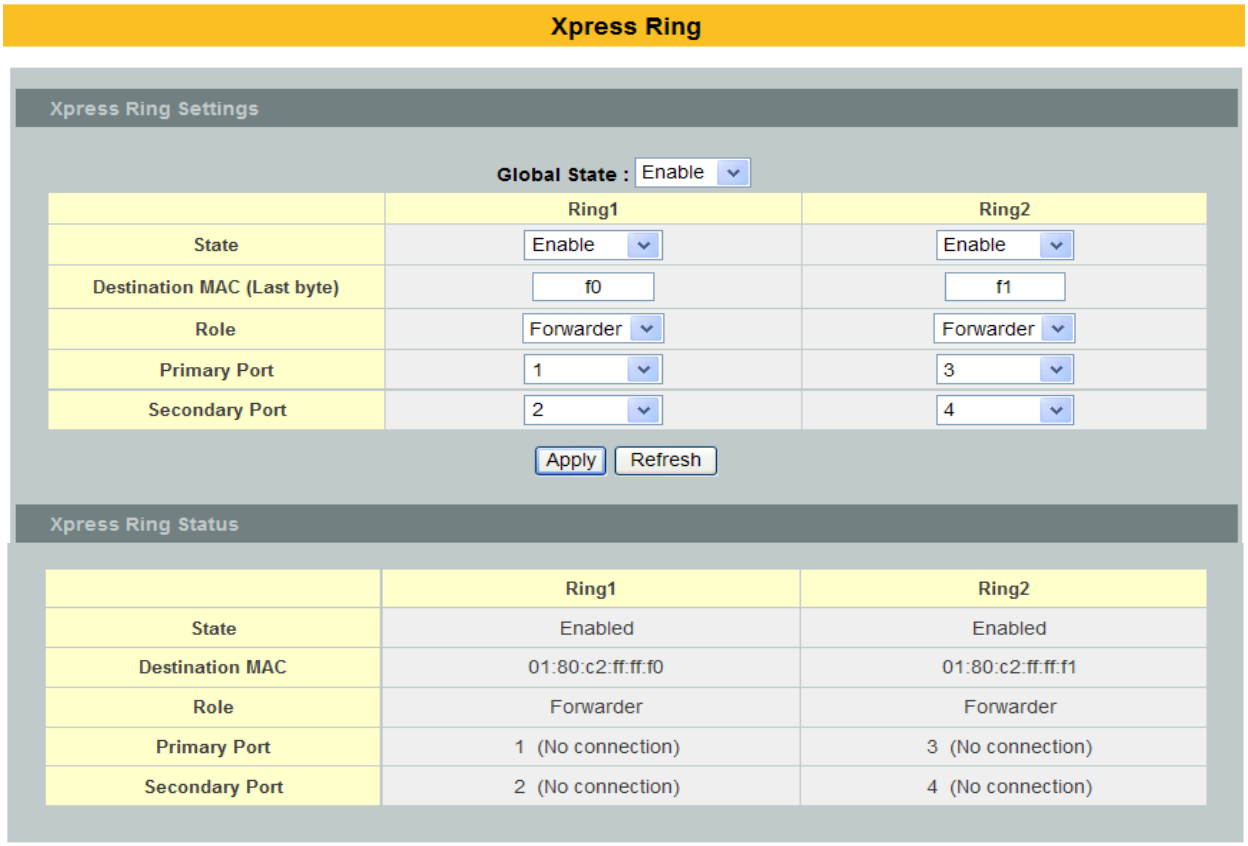
Xpress-Ring Configurations:
The global Xpress Ring state is:Disabled.
Ring 1: State : Disabled.
Destination MAC : 01:80:c2:ff:ff:f0.
Role : Forwarder.
Primary Port : None.
Secondary Port : None.
Ring 2: State : Disabled.
Destination MAC : 01:80:c2:ff:ff:f1.
Role : Forwarder.
Primary Port : None.
Secondary Port : None.

### 6.14.2. CLI Configuration

| Node | Command | Description |
|---|---|---|
| enable | show xpress-ring | This command displays the current Xpress-Ring configurations. |
| configure | xpress-ring (disable\|enable) | This command enables/disables the Xpress-Ring on the Switch. |
| configure | xpress-ring ring (RING1\|RING2) state (disable\|enable) | This command enables/disables the ring on the Switch. |
| configure | xpress-ring ring (RING1\|RING2) last-byte-destination-mac VALUE | This command configures the last byte of the destination MAC for the ring on the Switch. |
| configure | xpress-ring ring | This command configures the role (forwarder/arbiter) |

| | | |
|---|---|---|
| | (RING1\|RING2) role (forwarder\|arbiter) | for the ring on the Switch. |
| configure | xpress-ring ring (RING1\|RING2) primary-port PORTID | This command configures the primary port for the ring on the Switch.<br>***Notice**: If the global xpress ring is disabled or ring state is disabled, you can input 0 to reset the primary port.* |
| configure | xpress-ring ring (RING1\|RING2) secondary-port PORTID | This command configures the secondary port for the ring on the Switch.<br>***Notice**: If the global xpress ring is disabled or ring state is disabled, you can input 0 to reset the primary port.* |

### 6.14.3. Web Configuration




| Parameter | Description |
|---|---|
| Current Root Status | |
| Global State | Enables/Disable the global Xpress ring function. |
| State | Enables / Disables the ring state. |
| Destination MAC(Last byte) | Configures the last byte of the destination MAC for the ring. |

| | |
|---|---|
| Role | Configures the role for the ring. |
| Primary Port | Configures the primary port for the ring. |
| Secondary Port | Configure the secondary port for the ring. |
| Xpress Ring Status | |
| State | The current state of the ring. |
| Destination MAC | The destination MAC for the ring. |
| Role | The current role of the ring. |
| Primary Port | The current primary port and its status. |
| Secondary Port | The current secondary port and its status. |

**Notices**

- An Xpress Ring can have one Arbiter only.
- A Switch can join one or two Xpress Ring.
- Every Switch can be a Forwarder or Arbiter in an Xpress Ring.
- The two adjacent Xpress Rings should not use a same destination multicast MAC.
- If you want to enable the STP(RSTP) and Xpress Ring on a Switch, you should disable the STP (RSTP) on the Xpress Ring's member ports.
- If you want to enable the Loop Detection and Xpress Ring on a Switch, you should disable the Loop Detection on the Xpress Ring's member ports.
- If you want to enable the Broadcast Storm and Xpress Ring on a Switch, you should disable the Broadcast Storm on the Xpress Ring's member ports.
- If there are old devices (for example: INS-803A) to join the Xpress-Ring, they can join as a forwarder only.

# 7. Security

## 7.1. IP Source Guard

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

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

The IP Source Guard features include below functions:

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

### 7.1.1. DHCP Snooping

#### 7.1.1.1. Introduction

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

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

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

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

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

- ✓ A packet from a DHCP server, such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet, is received from the untrusted port.
- ✓ A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match any of the current bindings.

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

**Trusted vs. Untrusted Ports**

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

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

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

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

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

**DHCP Snooping Database**

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

**Configuring DHCP Snooping**

Follow these steps to configure DHCP snooping on the Switch.

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

**Note:**

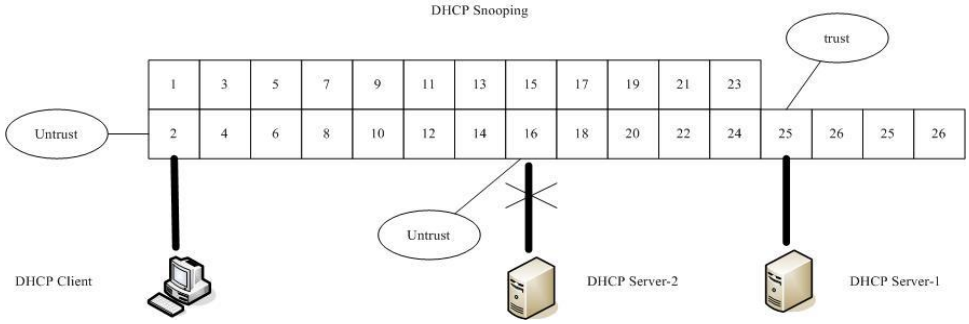
The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.

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

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

The main purposes of the DHCP Snooping are:

1. Create and maintain binding table for ARP Inspection function.
2. Filter the DHCP server's packets that the DHCP server connects to an untrusted port.




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

**Default Settings**

The DHCP snooping on the Switch is disabled.
The DHCP snooping is enabled in VLAN(s): None.

| Port | Trusted | Maximum Host Count | Port | Trusted | Maximum Host Count |
|---|---|---|---|---|---|
| 1 | no | 32 | 2 | no | 32 |
| 3 | no | 32 | 4 | no | 32 |
| 5 | no | 32 | 6 | no | 32 |
| 7 | no | 32 | 8 | no | 32 |
| 9 | no | 32 | 10 | no | 32 |
| 11 | no | 32 | 12 | no | 32 |

***Notices***

- There are a global state and per VLAN states.

When the global state is disabled, the DHCP Snooping on the Switch is disabled even per VLAN states are enabled.
When the global state is enabled, user must enable per VLAN states to enable the DHCP Snooping on the specific VLAN.

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

Procedures:

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

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

➔ DHCP Client-1 can get an IP address.

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

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

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

#### 7.1.1.2. CLI Configuration

| Node | Command | Description |
|---|---|---|
| enable | show dhcp-snooping | This command displays the current DHCP snooping configurations. |
| configure | dhcp-snooping (disable\|enable) | This command disables/enables the DHCP snooping on the switch. |
| configure | dhcp-snooping vlan VLANID | This command enables the DHCP snooping function on a VLAN or range of VLANs. |
| configure | no dhcp-snooping vlan VLANID | This command disables the DHCP snooping function on a VLAN or range of VLANs. |
| configure | dhcp-snooping server IPADDR | This command configures a valid DHCP server. |
| interface | dhcp-snooping host | This command configures the maximum host count for the specific port. |
| interface | no dhcp-snooping host | This command configures the maximum host count to default for the specific port. |
| interface | dhcp-snooping trust | This command configures the trust port for the specific port. |
| interface | no dhcp-snooping trust | This command configures the un-trust port for the specific port. |
| configure | interface range gigabitethernet1/0/ PORTLISTS | This command enters the interface configure node. |

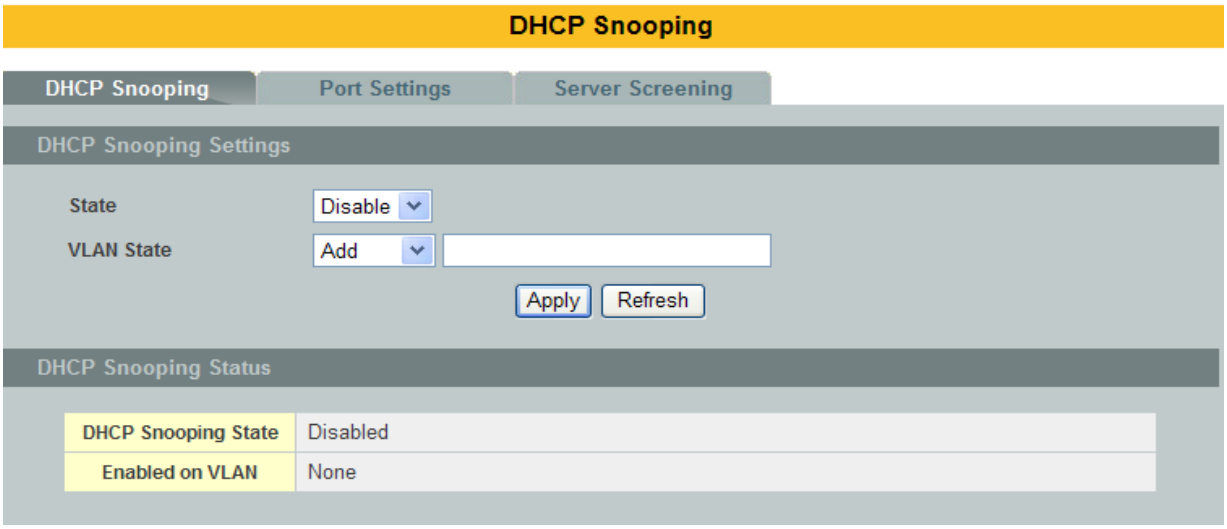
| | | |
|---|---|---|
| if-range | dhcp-snooping host | This command configures the maximum host count for the specific ports. |
| if-range | no dhcp-snooping host | This command configures the maximum host count to default for the specific ports. |
| if-range | dhcp-snooping trust | This command configures the trust port for the specific ports. |
| if-range | no dhcp-snooping trust | This command configures the un-trust port for the specific ports. |

**Example:**

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

### 7.1.1.3. Web Configuration

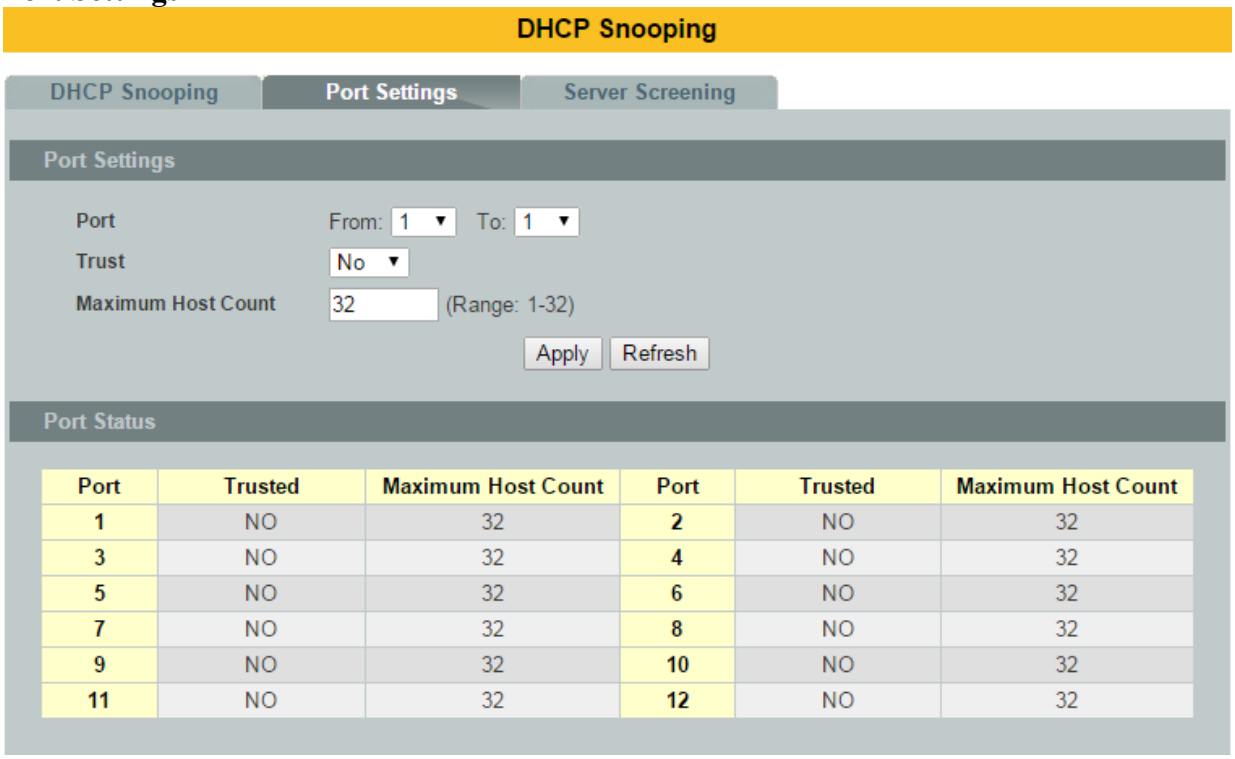
**DHCP Snooping**




| Parameter | Description |
|---|---|
| State | Select **Enable** to use DHCP snooping on the Switch. You still have to enable DHCP snooping on specific VLANs and specify trusted ports.<br>Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.<br>Select **Disable** to not use DHCP snooping. |
| VLAN State | Select **Add** and enter the VLAN IDs you want the Switch to enable DHCP snooping on. You can designate multiple VLANs individually by using a comma (,) and by range with a hyphen (-).<br>Select **Delete** and enter the VLAN IDs you no longer want the Switch to use DHCP snooping on. |

| | |
|---|---|
| Apply | Click **Apply** to take effect the settings. |
| Refresh | Click **Refresh** to begin configuring this screen afresh. |
| DHCP Snooping Status | |
| DHCP Snooping State | This field displays the current status of the DHCP snooping feature, **Enabled** or **Disabled**. |
| Enabled on VLAN | This field displays the VLAN IDs that have DHCP snooping enabled on them. This will display **None** if no VLANs have been set. |

**Port Settings**




| **Parameter** | **Description** |
|---|---|
| Port | Select a port number to modify its maximum host count. |
| Trust | Configures the specific port if it is a trust port. |
| Maximum Host Count | Enter the maximum number of hosts (1-32) that are permitted to simultaneously connect to a port. |
| Apply | Click Apply to take effect the settings. |
| Refresh | Click Refresh to begin configuring this screen afresh. |

### 7.1.1.4. DHCP Server Screening

#### 7.1.1.4.1. Introduction

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

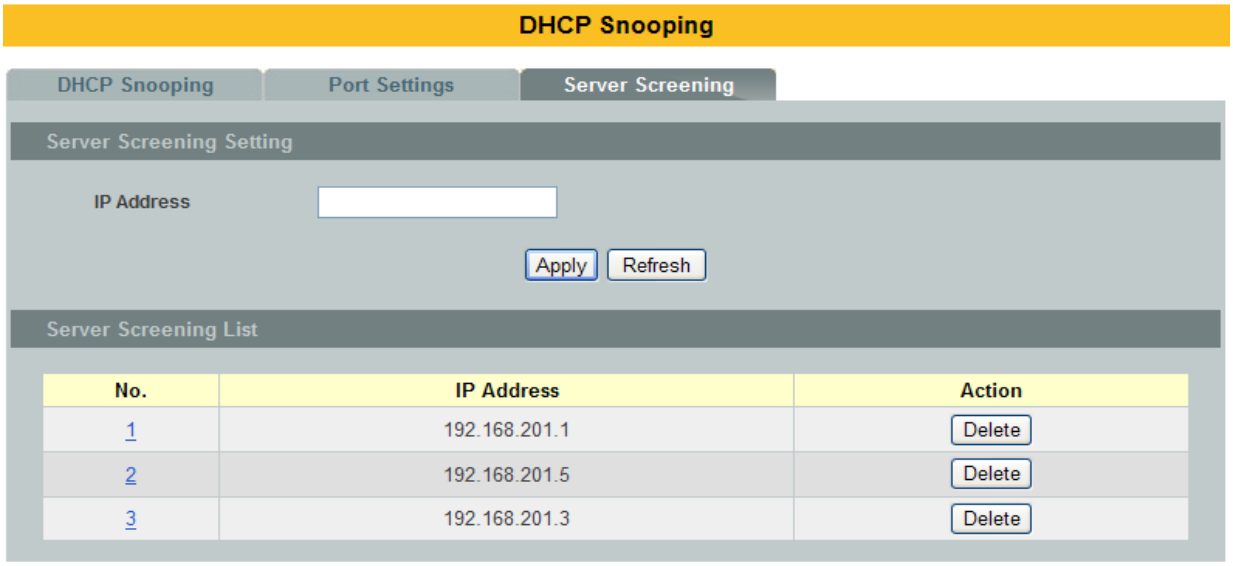
If you want to enable this feature, you must enable the DHCP Snooping function first. The Switch allows users to configure up to three valid DHCP servers.

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

#### 7.1.1.4.2. CLI Configuration

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

#### 7.1.1.4.3. Web Configuration




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

| Server Screening List | |
|---|---|
| No. | This field displays the index number of the DHCP server entry. Click the number to modify the entry. |
| IP Address | This field displays the IP address of the DHCP server. |
| Action | Click **Delete** to remove a configured DHCP server. |

### 7.1.2. Binding Table

#### 7.1.2.1. Introduction

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

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

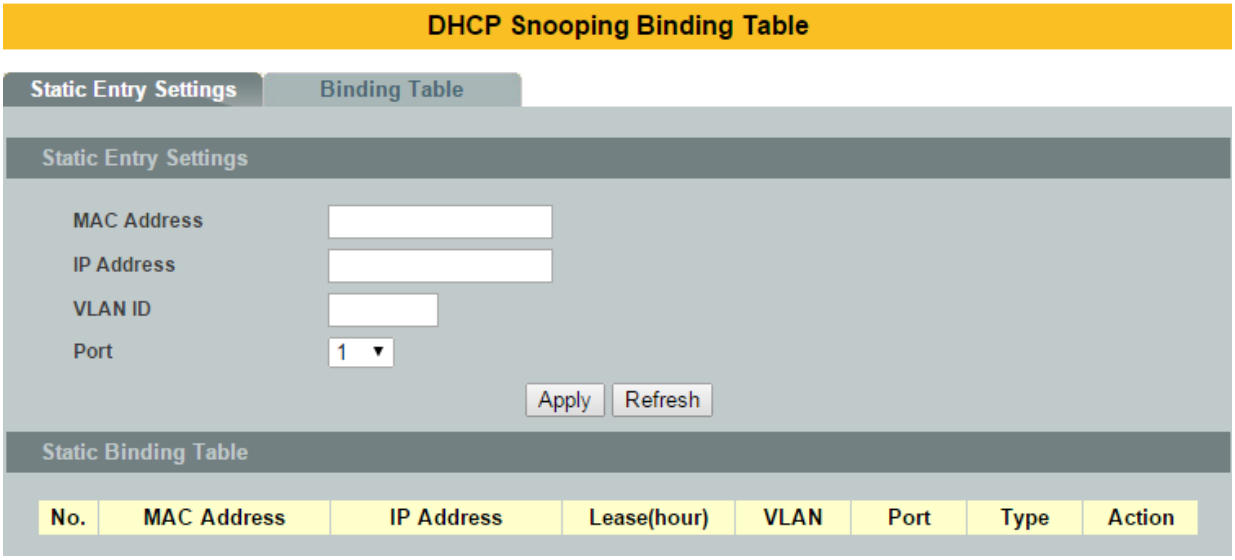
#### 7.1.2.2. CLI Configuration

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

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

### 7.1.2.3. Web Configuration

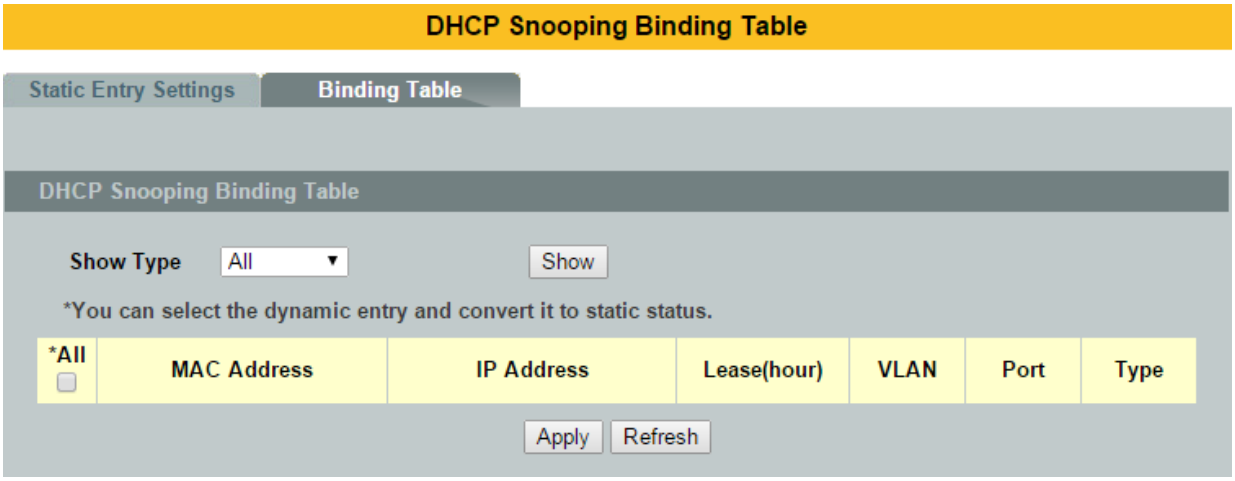
**Static Entry Settings**




| Parameter | Description |
|---|---|
| MAC Address | Enter the source MAC address in the binding. |
| IP Address | Enter the IP address assigned to the MAC address in the binding. |
| VLAN ID | Enter the source VLAN ID in the binding. |
| Port | Specify the port in the binding. |
| Static Binding Table | |
| No. | This field displays a sequential number for each binding. Click it to update an existing entry. |
| MAC Address | This field displays the source MAC address in the binding. |
| IP Address | This field displays the IP address assigned to the MAC address in the binding. |
| Lease (Hour) | This field displays how long the binding is valid. |
| VLAN | This field displays the source VLAN ID in the binding. |
| Port | This field displays the port number in the binding. |
| Type | This field displays how the Switch learned the binding.<br>**Static**: This binding was learned from information provided manually by an administrator.<br>**Dynamic**: This binding was learned by snooping DHCP packets. |
| Action | Click **Delete** to remove the specified entry. |

**Binding Table**

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




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

### 7.1.3. ARP Inspection

#### 7.1.3.1. ARP Inspection

##### 7.1.3.1.1. Introduction

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

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

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

**Trusted and untrusted port**

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

**Configurations:**

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

**Default Settings**

The ARP Inspection on the Switch is disabled.
The age time for the MAC filter is 5 minutes.
ARP Inspection is enabled in VLAN(s): None.

| Port | Trusted | Port | Trusted |
|---|---|---|---|
| 1 | no | 2 | no |
| 3 | no | 4 | no |
| 5 | no | 6 | no |
| 7 | no | 8 | no |
| 9 | no | 10 | no |
| 11 | no | 12 | no |

***Notices***

There are a global state and per VLAN states.

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

#### 7.1.3.1.2. CLI Configuration

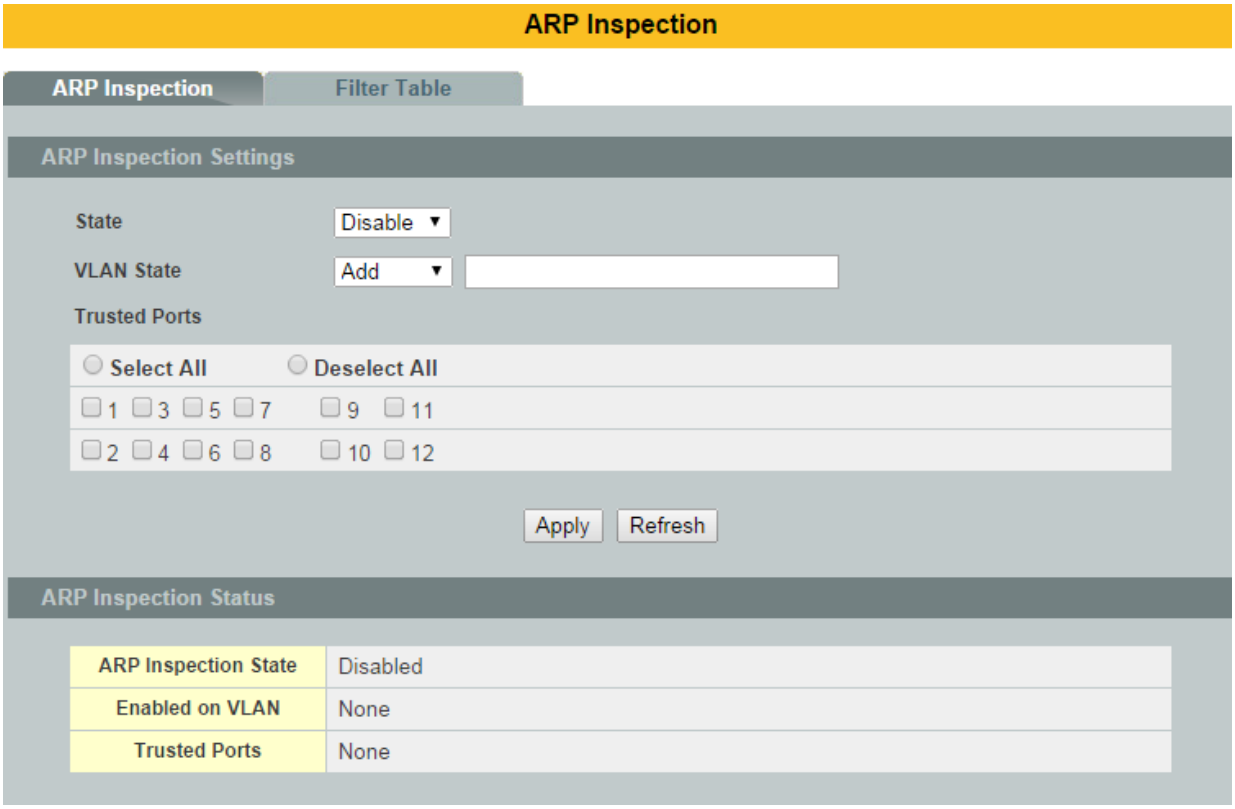
| Node | Command | Description |
|---|---|---|
| enable | show arp-inspection | This command displays the current ARP Inspection |

| | | |
|---|---|---|
| | | configurations. |
| configure | arp-inspection (disable \| enable) | This command disables/enables the ARP Inspection function on the switch. |
| configure | arp-inspection vlan VLANID | This command enables the ARP Inspection function on a VLAN or range of VLANs. |
| configure | no arp-inspection vlan VLANID | This command disables the ARP Inspection function on a VLAN or range of VLANs. |
| interface | arp-inspection trust | This command configures the trust port for the specific port. |
| interface | no arp-inspection trust | This command configures the un-trust port for the specific port. |

**Example:**

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

#### 7.1.3.1.3. Web Configuration




| Parameter | Description |
|---|---|
| State | Use this to **Enable** or **Disable** ARP inspection on the Switch. |

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

#### 7.1.3.2. Filter Table

##### 7.1.3.2.1. Introduction

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

- If the ARP Inspection is enabled and the system detects invalid hosts, the system will create a filtered entry in the MAC address table.
- When Port link down and ARP Inspection was disabled, Switch will remove the MAC-filter entries learned by this port.
- When Port link down and ARP Inspection was enabled, Switch will remove the MAC-filter entries learned by this port.
- The maximum entry of the MAC address filter table is 256.

- When MAC address filter table of ARP Inspection is full, the Switch receives unauthorized ARP packet, and it automatically creates a SYSLOG and drop this ARP packet. The SYSLOG event happens on the first time.

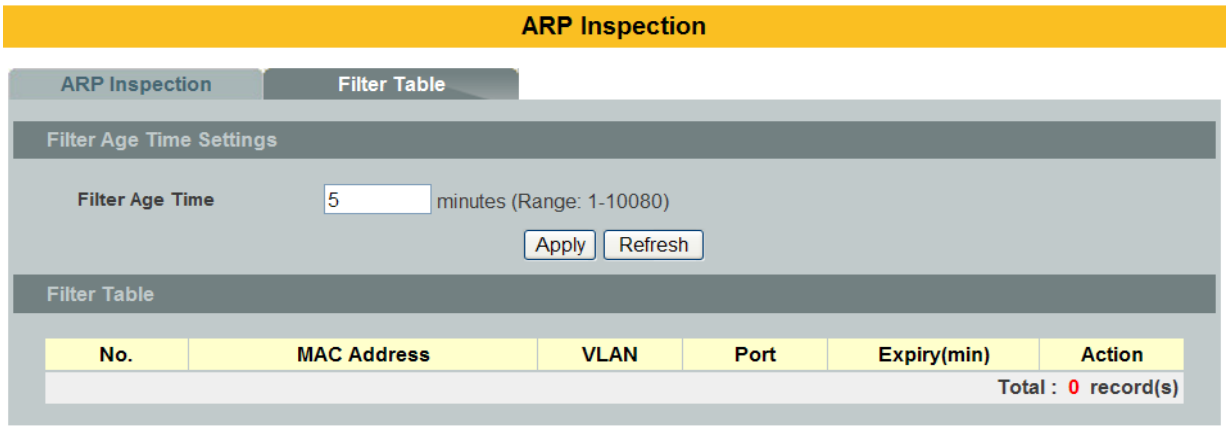
**Default Settings**

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

#### 7.1.3.2.2. CLI Configuration

| Node | Command | Description |
|---|---|---|
| enable | show arp-inspection mac-filter | This command displays the current ARP Inspection filtered MAC. |
| configure | arp-inspection mac-filter age VALUE | This command configures the age time for the ARP inspection MAC filter entry. |
| configure | clear arp-inspection mac-filter | This command clears all of entries in the filter table. |
| configure | no arp-inspection mac-filter mac MACADDR vlan VLANID | This command removes an entry from the ARP inspection MAC filter table. |

#### 7.1.3.2.3. Web Configuration




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

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

## 7.2. ACL

### 7.2.1. Introduction

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

L2 ACL function allows user to configure a few rules to reject packets from the specific ingress ports or all ports. These rules will check the packets' source MAC address and destination MAC address. If packets match these rules, the system will do the actions "deny". "deny" means rejecting these packets.
The Action Resolution engine collects the information (action and metering results) from the hit entries: if more than one rule matches, the actions and meter/counters are taken from the policy associated with the matched rule with highest priority.

L2 ACL Support:

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

L3 ACL Support:

1. Filter a specific source IP address.
   Command: *source ip host IPADDR*
2. Filter a specific destination IP address.

Command: *destination ip host IPADDR*

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

L4 ACL Support:

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

**Default Settings**

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

***Notices***

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

### 7.2.2. CLI Configuration

| Node | Command | Description |
|---|---|---|
| enable | show access-list | This command displays all of the access control profiles. |
| configure | access-list STRING ip-type (ipv4\|ipv6) | This command creates a new access control profile. Where the STRING is the profile name. And you can specify the type, ipv4 or ipv6. |
| 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.<br>disable – disable the profile.<br>drop – If packets match the profile, the packets will be dropped.<br>permit – If packets match the profile, the packets will be forwarded. |
| acl | action dscp remarking <0-63> | This command actives this profile and specify that it is for DSCP remark. And configures the new DSCP value which will be override to all packets matched this profile. |
| acl | action 802.1p remarking <0-7> | This command actives this profile and specify that it is for 802.1p remark. And configures the new 802.1p value which will be override to all packets matched this profile. |
| acl | 802.1p VALUE | This command configures the 802.1p value for the profile. |
| acl | dscp VALUE | This command configures the DSCP value for the |

| | | |
|---|---|---|
| | | profile. |
| 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 VLANID | This command configures the VLAN for the profile. |
| acl | no vlan | This command removes the limitation of the VLAN from the profile. |
| acl | source interface | This command configures the source interface for the |

| | | |
|---|---|---|
| | PORT_ID | 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

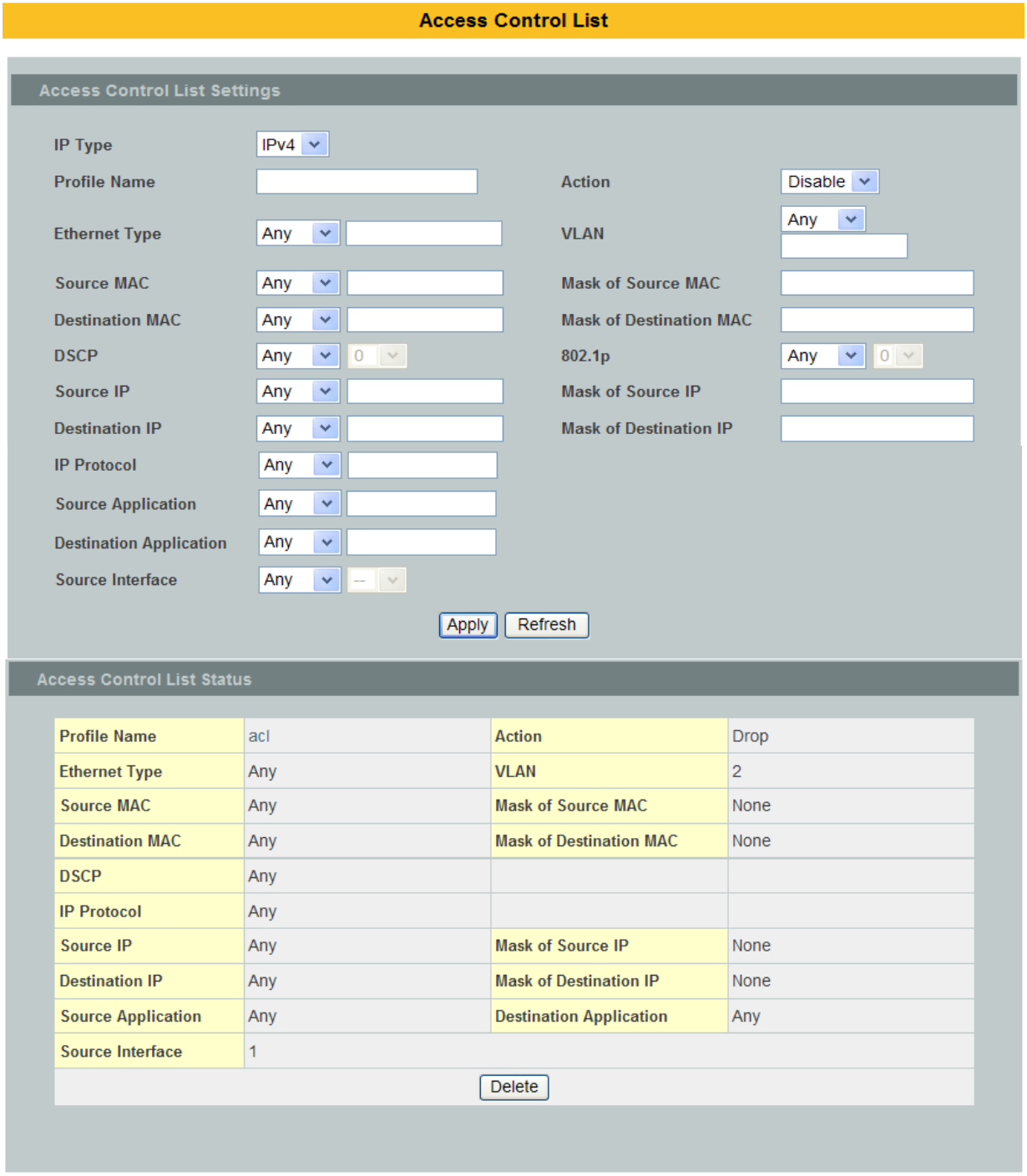
➔ The command will filter source IP range from 172.20.0.0 to 172.20.255.255

**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

Note: Any: Don't care.

### 7.2.3. Web Configuration




| Parameter | Description |
|---|---|
| IP Type | Selects IPv4 / IPv6 type for the profile. |
| Profile Name | The access control profile name. |

| | |
|---|---|
| Action | Selects Disables / Drop / Permits / DSCP action for the profile. |
| 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.<br>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.<br>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. |
| DSCP | Configure the DSCP for the profile. |
| 802.1p | Configures the 802.1p for the profile. |
| 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.<br>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.<br>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. |
| IP Protocol | Configures the IP protocol type. The setting will be used for Source Application and Destination Application.<br>TCP:0x06. UDP:0x11. |
| 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. |

## 7.3. 802.1x

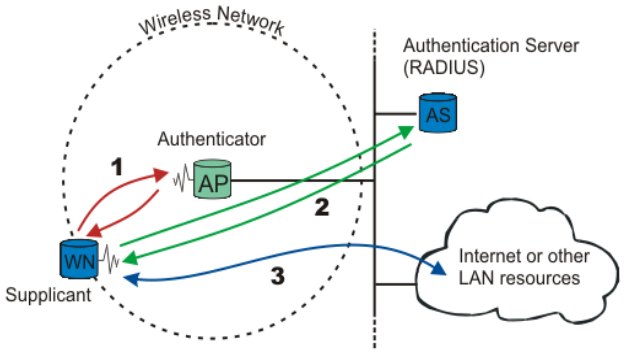
### 7.3.1. Introduction

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

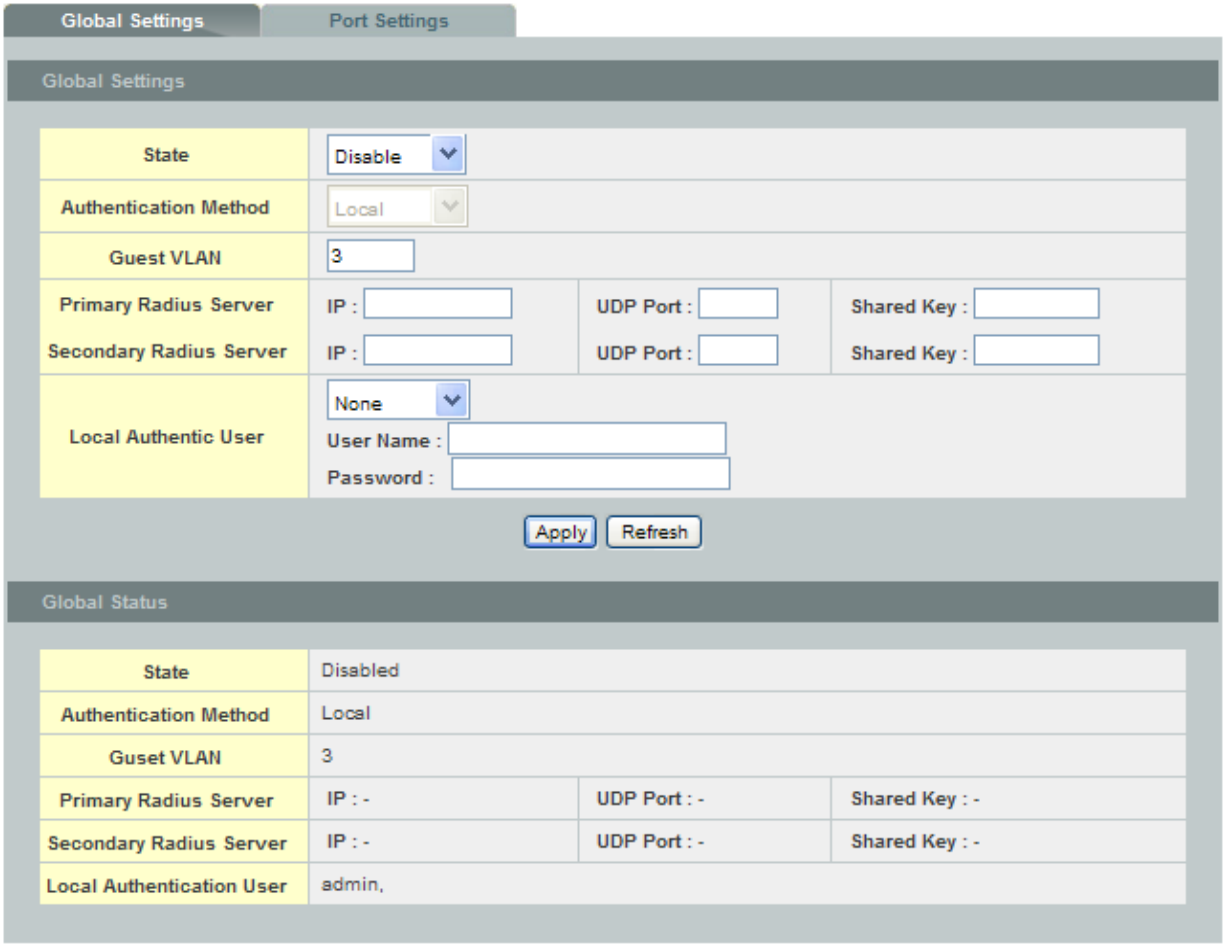
### 7.3.2. CLI Configuration

| 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- | This command configures the primary radius server. |

| | | |
|---|---|---|
| | server-ip <IP> port PORTID key KEY | |
| 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 re-auth-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. |

### 7.3.3. Web Configuration

**Global Settings**

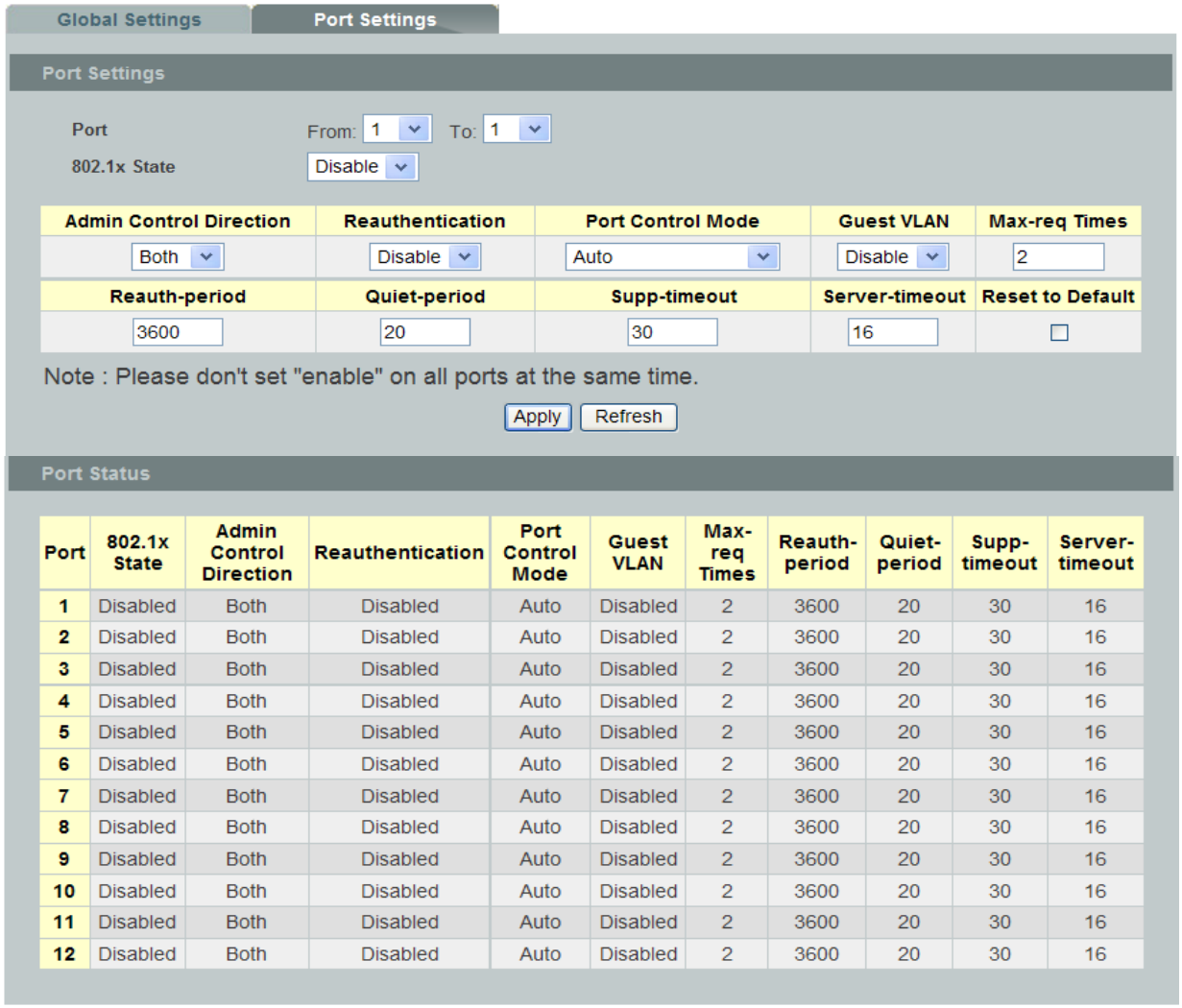



| Parameter | Description |
|---|---|
| State | Select **Enable** to permit 802.1x authentication on the Switch.<br>Note: You must first enable 802.1x authentication on the Switch before configuring it on each port. |
| Authentication Method | Select whether to use **Local** or **RADIUS** as the authentication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

**802.1x**




| Port | 802.1x State | Admin Control Direction | Reauthentication | Port Control Mode | Guest VLAN | Max-req Times | Reauth-period | Quiet-period | Supp-timeout | Server-timeout |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Disabled | Both | Disabled | Auto | Disabled | 2 | 3600 | 20 | 30 | 16 |
| 2 | Disabled | Both | Disabled | Auto | Disabled | 2 | 3600 | 20 | 30 | 16 |
| 3 | Disabled | Both | Disabled | Auto | Disabled | 2 | 3600 | 20 | 30 | 16 |
| 4 | Disabled | Both | Disabled | Auto | Disabled | 2 | 3600 | 20 | 30 | 16 |
| 5 | Disabled | Both | Disabled | Auto | Disabled | 2 | 3600 | 20 | 30 | 16 |
| 6 | Disabled | Both | Disabled | Auto | Disabled | 2 | 3600 | 20 | 30 | 16 |
| 7 | Disabled | Both | Disabled | Auto | Disabled | 2 | 3600 | 20 | 30 | 16 |
| 8 | Disabled | Both | Disabled | Auto | Disabled | 2 | 3600 | 20 | 30 | 16 |
| 9 | Disabled | Both | Disabled | Auto | Disabled | 2 | 3600 | 20 | 30 | 16 |
| 10 | Disabled | Both | Disabled | Auto | Disabled | 2 | 3600 | 20 | 30 | 16 |
| 11 | Disabled | Both | Disabled | Auto | Disabled | 2 | 3600 | 20 | 30 | 16 |
| 12 | Disabled | Both | Disabled | Auto | Disabled | 2 | 3600 | 20 | 30 | 16 |

| Parameter | Description |
|---|---|
| Port | Select a port number to configure. |
| 802.1x State | Select **Enable** to permit 802.1x authentication on the port.<br>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.<br>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.<br>Select **Force Authorized** to always force this port to be authorized.<br>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.<br>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.<br>**Both** will drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication.<br>**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.<br>**Auto** requires authentication on the port.<br>**Force Authorized** forces the port to be authorized.<br>**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. |

## 7.4. Port Security

### 7.4.1. Introduction

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

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

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

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

**Default Settings**

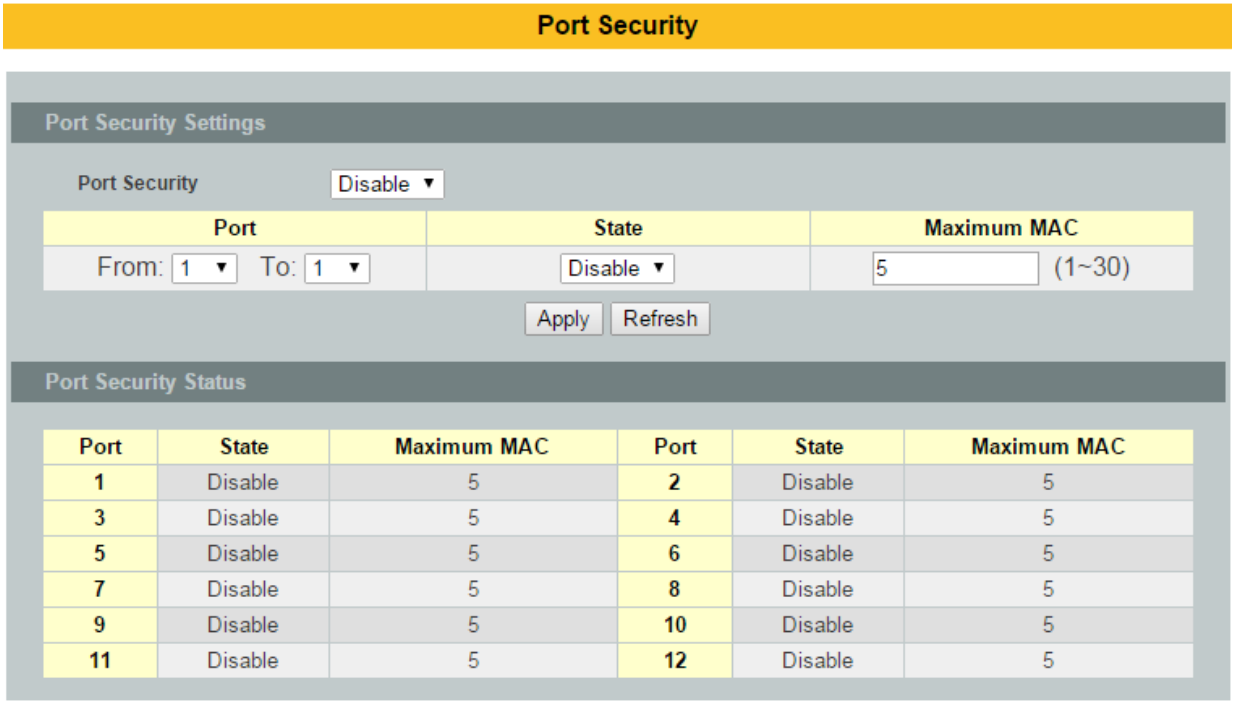
The port security on the Switch is disabled.
The Maximum MAC per port is 5.
The port state of the port security is disabled.

### 7.4.2. 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 | This command enables / disables the port security |

| | | |
|---|---|---|
| | (disable\|enable) | function on the specific port. |
| interface | port-security limit VALUE | 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 VALUE | This command configures the maximum MAC entries for the specified ports. |

### 7.4.3. 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. |
| 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:**

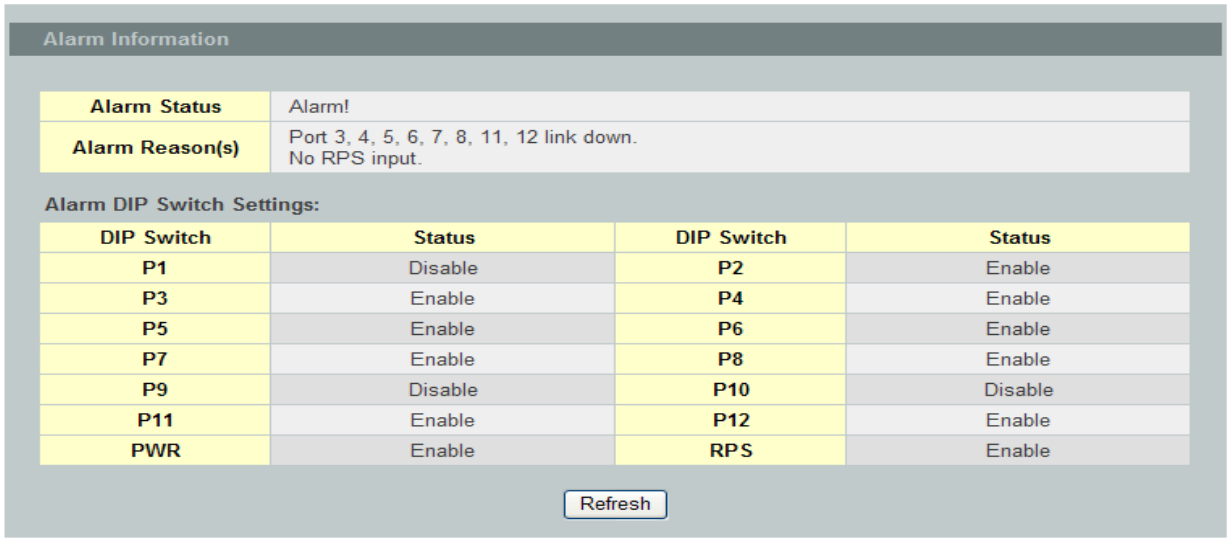
P1: ON, The Switch will send alarm message when port 1 is link down.
PWR: ON, The Switch will send alarm message when the main power supply disconnect.
RPS: ON, The Switch will send alarm message when the redundant power supply disconnect.

### 8.1.2. CLI Configuration

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

### 8.1.3. Web Configuration

**Alarm Information**




| 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. Hardware Information

### 8.2.1. Introduction

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

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

### 8.2.2. CLI Configuration

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

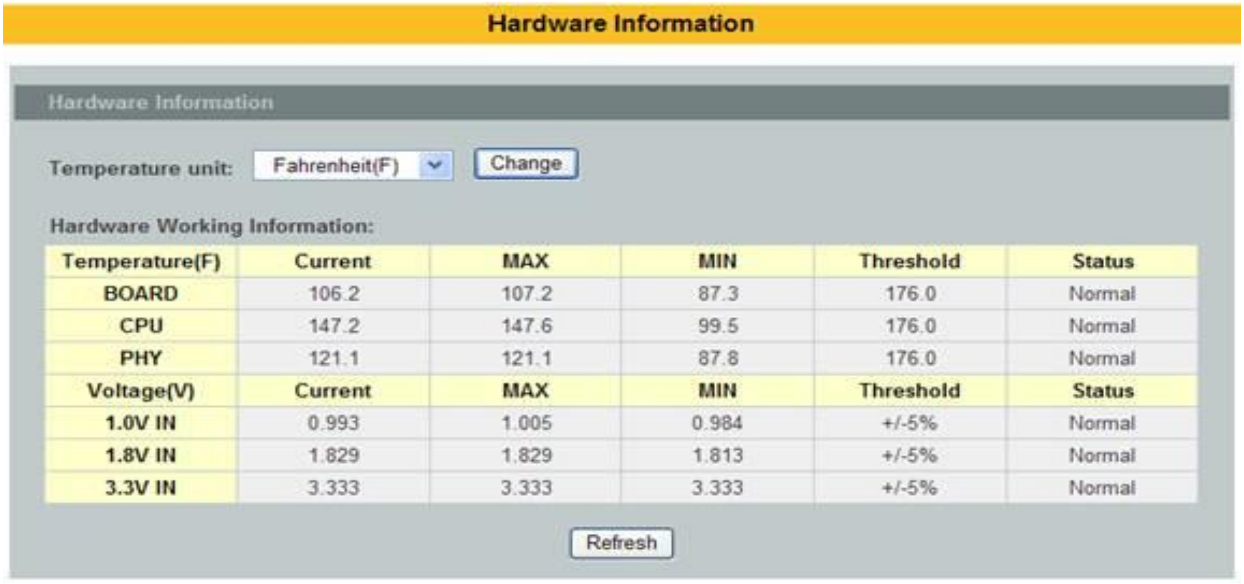
**Example:**

L2SWITCH#show hardware-monitor C

| Temperature(C) | Crent | MAX | MIN | Threshold | Status |
|---|---|---|---|---|---|
| BOARD | 44.0 | 44.2 | 24.0 | 80.0 | Normal |
| CPU | 49.2 | 49.2 | 26.5 | 80.0 | Normal |
| PHY | 57.5 | 57.5 | 30.0 | 80.0 | Normal |

| Voltage(V) | Current | MAX | MIN | Threshold | Status |
|---|---|---|---|---|---|
| 1.0V IN | 1.009 | 1.009 | 1.009 | +/-5% | Normal |
| 1.8V IN | 1.768 | 1.778 | 1.755 | +/-5% | Normal |
| 3.3V IN | 3.264 | 3.264 | 3.259 | +/-5% | Normal |

### 8.2.3. Web Configuration



## 8.3. Port Statistics

### 8.3.1. Introduction

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

### 8.3.2. CLI Configuration

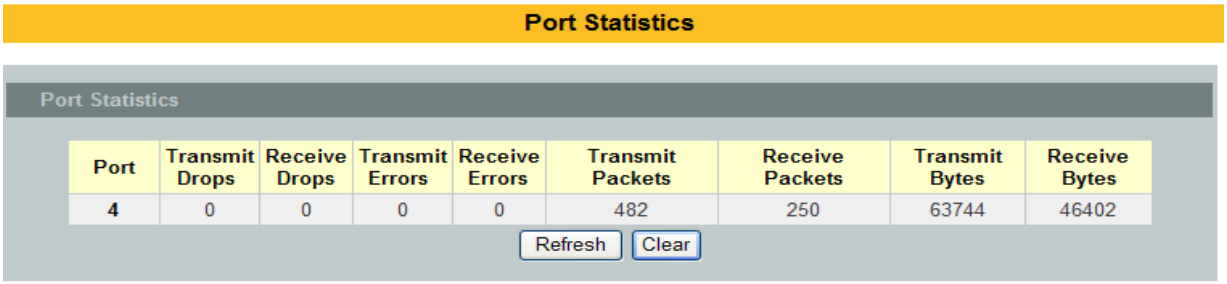
| Node | Command | Description |
|---|---|---|
| enable | show port-statistics | This command displays the link up ports' statistics. |

**Example:**

```
L2SWITCH#show port-statistics

          Packets                 Bytes                   Errors                  Drops
Port      Rx          Tx          Rx          Tx          Rx          Tx          Rx          Tx
----  --------    --------    --------    --------    --------    --------    --------    --------
 7    1154        2           108519      1188        0           0           0           0
```

### 8.3.3. 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. |

## 8.4. Port Utilization

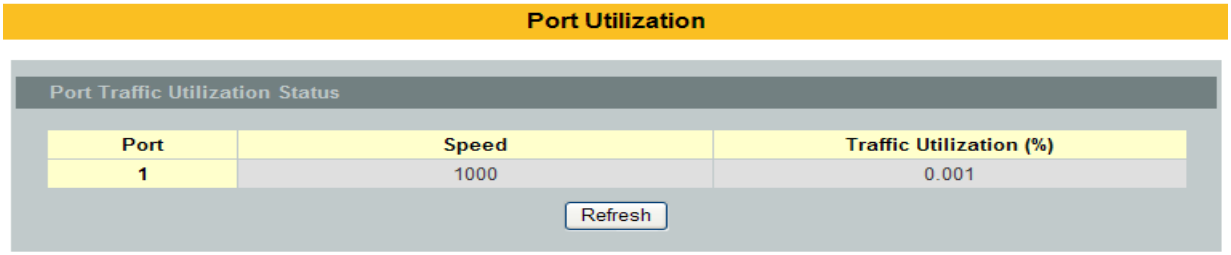
### 8.4.1. Introduction

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

### 8.4.2. CLI Configuration

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

### 8.4.3. 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. |

## 8.5. RMON Statistics

### 8.5.1. Introduction

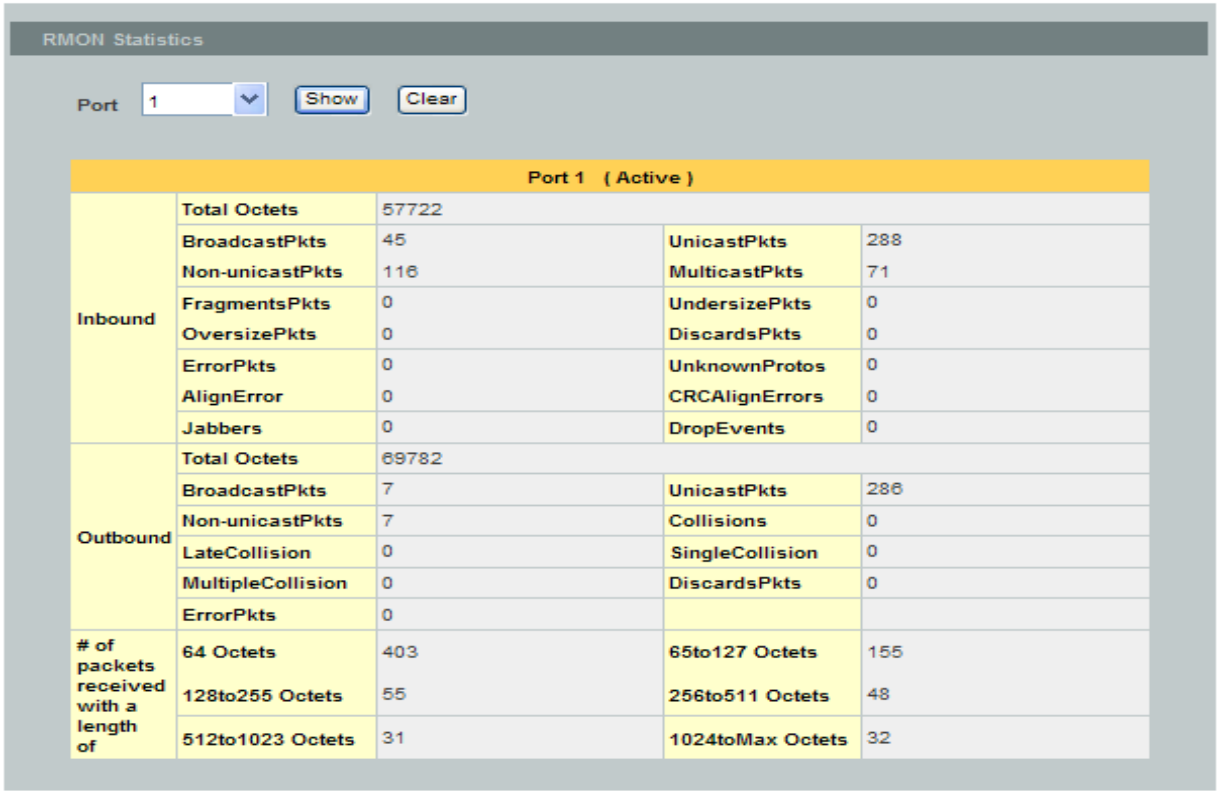
This feature helps users to monitor or clear the port's RMON statistics.

### 8.5.2. 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. |

### 8.5.3. Web Configuration

**RMON Statistics**




| Port 1 ( Active ) | | | | |
|---|---|---|---|---|
| Inbound | Total Octets | 57722 | | |
| | BroadcastPkts | 45 | UnicastPkts | 288 |
| | Non-unicastPkts | 116 | MulticastPkts | 71 |
| | FragmentsPkts | 0 | UndersizePkts | 0 |
| | OversizePkts | 0 | DiscardsPkts | 0 |
| | ErrorPkts | 0 | UnknownProtos | 0 |
| | AlignError | 0 | CRCAlignErrors | 0 |
| | Jabbers | 0 | DropEvents | 0 |
| Outbound | Total Octets | 69782 | | |
| | BroadcastPkts | 7 | UnicastPkts | 286 |
| | Non-unicastPkts | 7 | Collisions | 0 |
| | LateCollision | 0 | SingleCollision | 0 |
| | MultipleCollision | 0 | DiscardsPkts | 0 |
| | ErrorPkts | 0 | | |
| # of packets received with a length of | 64 Octets | 403 | 65to127 Octets | 155 |
| | 128to255 Octets | 55 | 256to511 Octets | 48 |
| | 512to1023 Octets | 31 | 1024toMax Octets | 32 |

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

## 8.6. SFP Information

### 8.6.1. Introduction

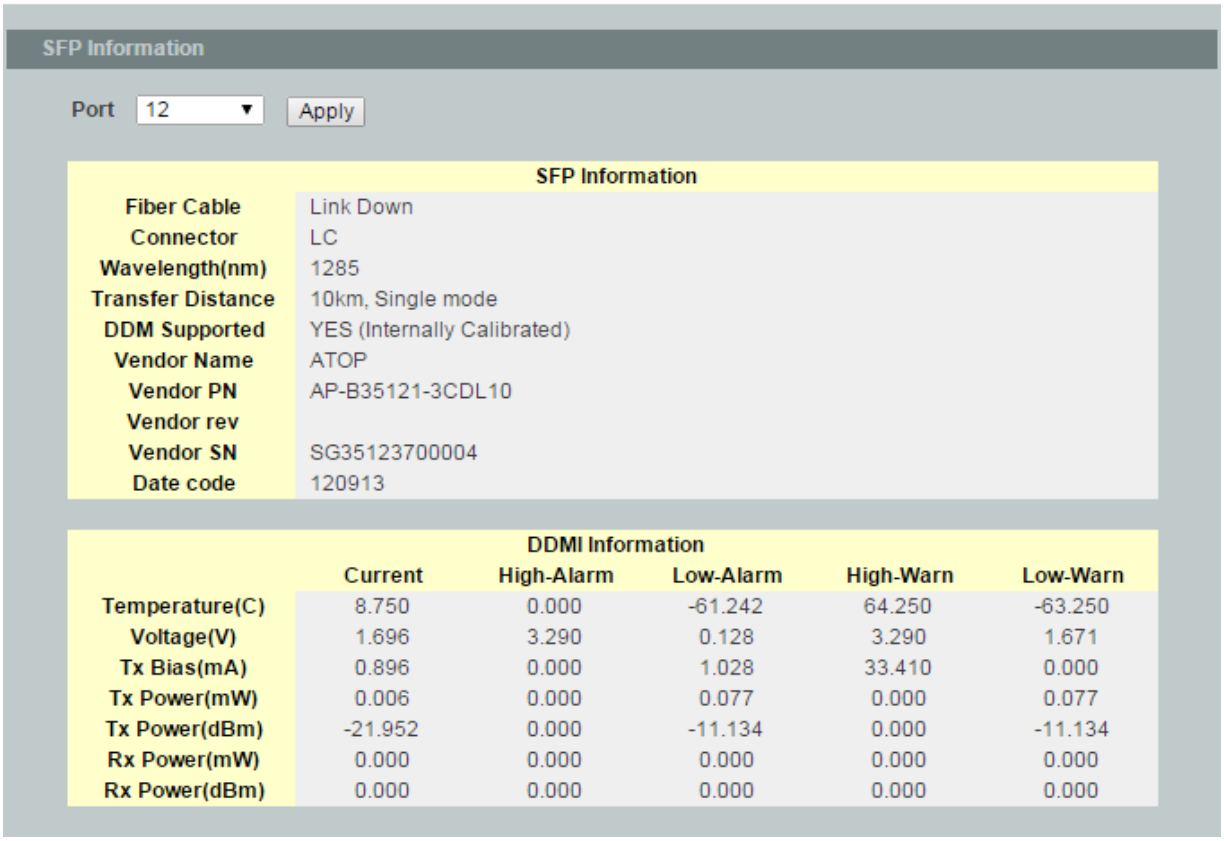
The SFP information allows user to know the SFP module's information, such as vendor name, connector type, revision, serial number, manufacture date, and to know the DDMI information if the SFP modules have supported the DDMI function.

### 8.6.2. 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. |

### 8.6.3. Web Configuration

**SFP Information**




| 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. |

Notice: If the fiber cable is not connected, the Rx Power fields are not available.

## 8.7. Traffic Monitor

### 8.7.1. 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**

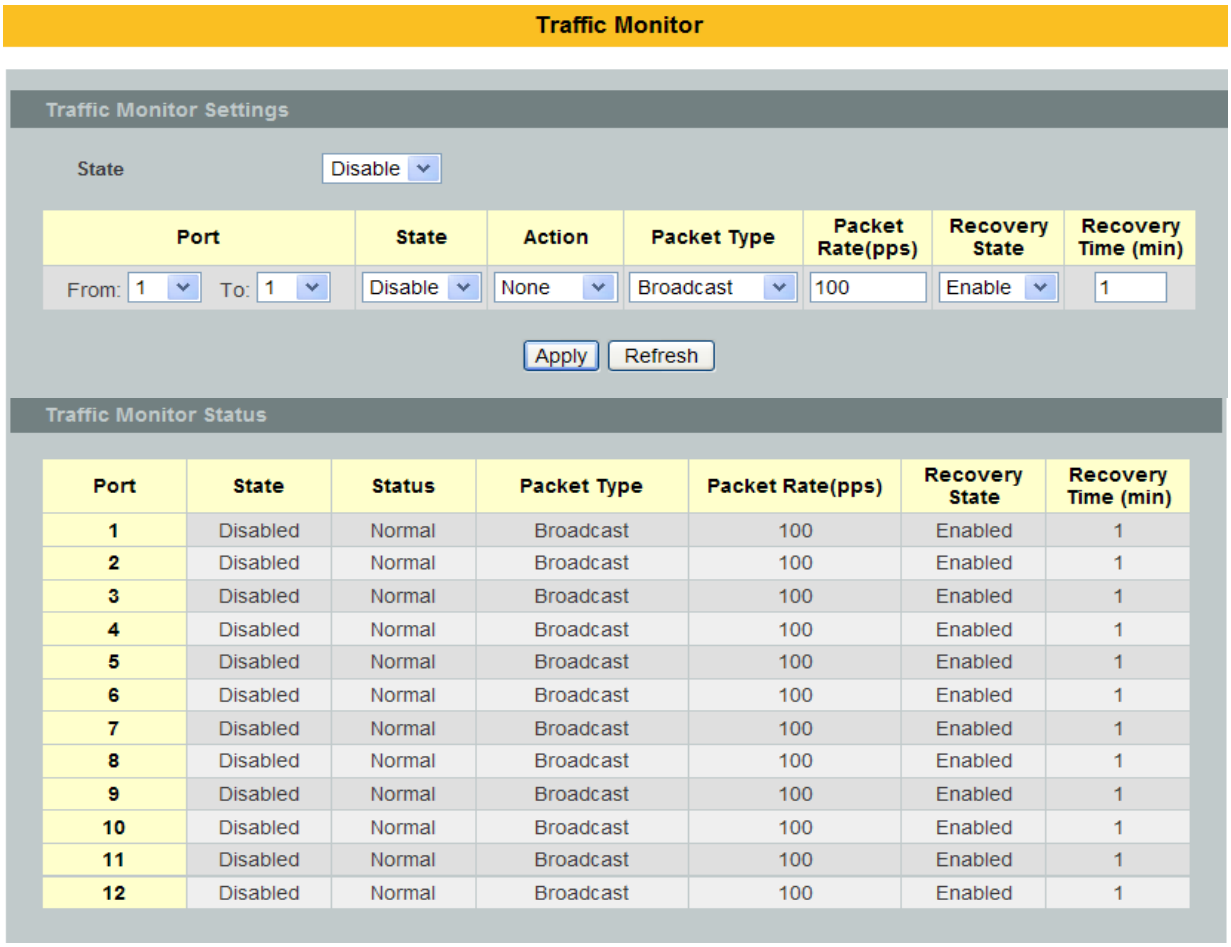
| Port | State | Status | Packet Type | Packet Rate(pps) | Recovery State | Recovery Time(min) |
|---|---|---|---|---|---|---|
| 1 | Disabled | Normal | Bcast | 1000 | Enabled | 1 |
| 2 | Disabled | Normal | Bcast | 1000 | Enabled | 1 |
| 3 | Disabled | Normal | Bcast | 1000 | Enabled | 1 |
| 4 | Disabled | Normal | Bcast | 1000 | Enabled | 1 |
| 5 | Disabled | Normal | Bcast | 1000 | Enabled | 1 |
| 6 | Disabled | Normal | Bcast | 1000 | Enabled | 1 |
| 7 | Disabled | Normal | Bcast | 1000 | Enabled | 1 |
| 8 | Disabled | Normal | Bcast | 1000 | Enabled | 1 |
| 9 | Disabled | Normal | Bcast | 1000 | Enabled | 1 |
| 10 | Disabled | Normal | Bcast | 1000 | Enabled | 1 |
| 11 | Disabled | Normal | Bcast | 1000 | Enabled | 1 |
| 12 | Disabled | Normal | Bcast | 1000 | Enabled | 1 |

### 8.7.2. 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.<br>bcast – Broadcast packet.<br>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 VALUE | 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+mcast) | This command configures the packet rate and packet type for the traffic monitor on the port.<br>bcast – Broadcast packet.<br>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 VALUE | This command configures the recovery time for the traffic monitor on the port. |

### 8.7.3. 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

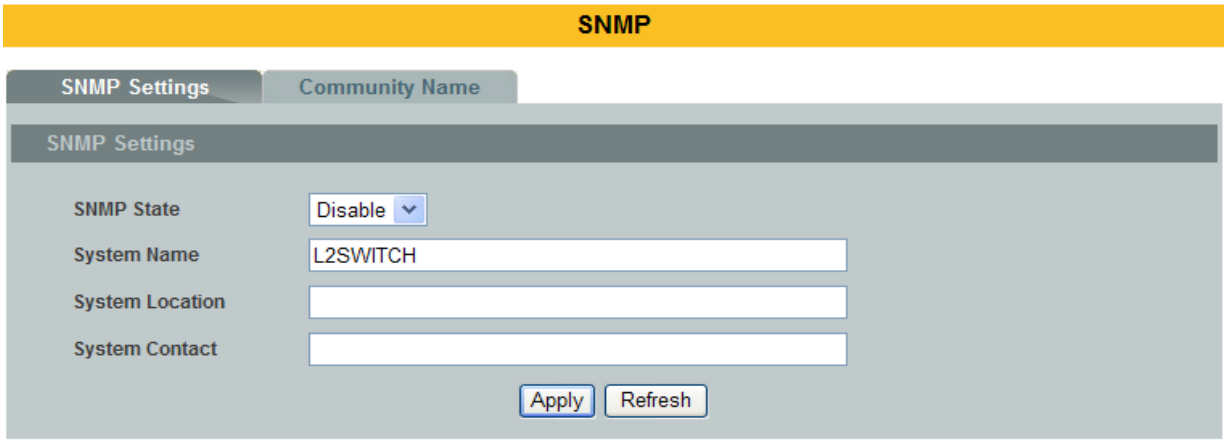
| Node | Command | Description |
|---|---|---|
| enable | show snmp | This command displays the SNMP configurations. |
| configure | snmp community STRING (ro\|rw) trusted-host IPADDR | This command configures the SNMP community name. |
| configure | snmp (disable\|enable) | This command disables/enables 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

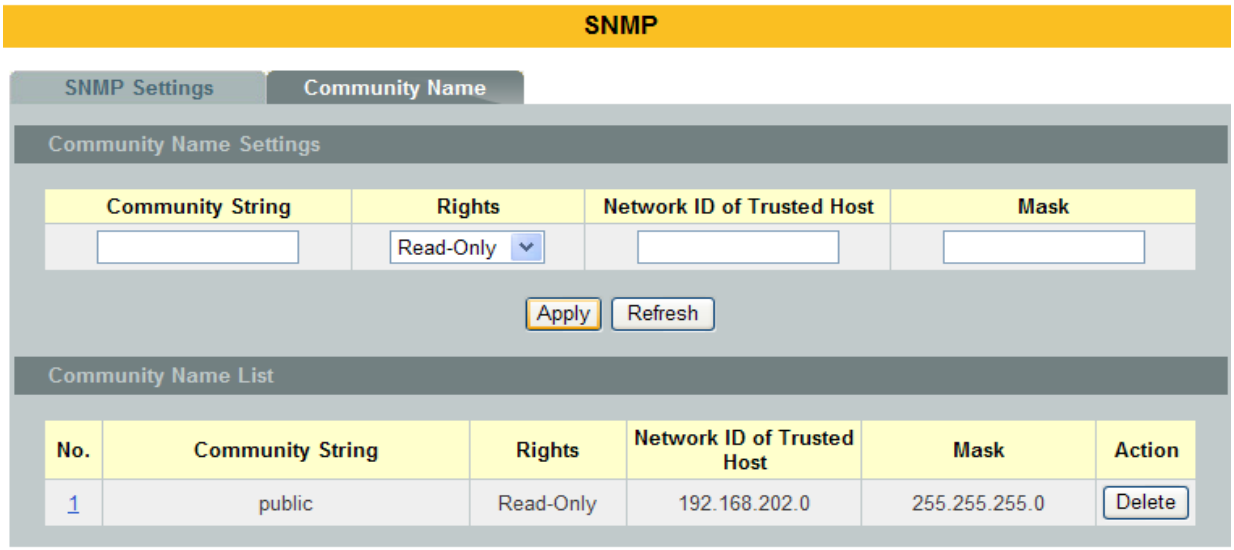
**SNMP Setting:**




| Parameter | Description |
|---|---|

| | |
|---|---|
| SNMP State | Select **Enable** to activate SNMP on the Switch.<br>Select **Disable** to not use SNMP on the Switch. |
| System Name | Type a System Name for the Switch.<br>(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:**

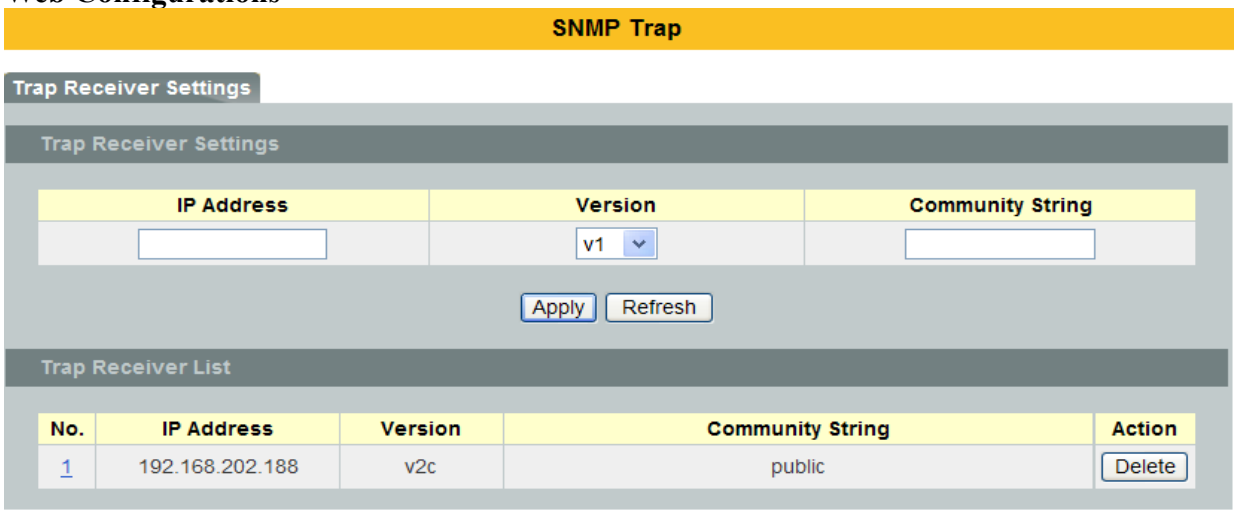



| Parameter | Description |
|---|---|
| Community String | Enter a Community string, this will act as a password for requests from the management station.<br>An SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (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.<br>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<br><br>Mask | Type the IP address of the remote SNMP management station in dotted decimal notation, for example 192.168.1.0.<br><br>Type the subnet mask for the IP address of the remote SNMP |

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

### 9.1.2. SNMP Trap

**Web Configurations**




| 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. |

### 9.1.3. SNMPv3

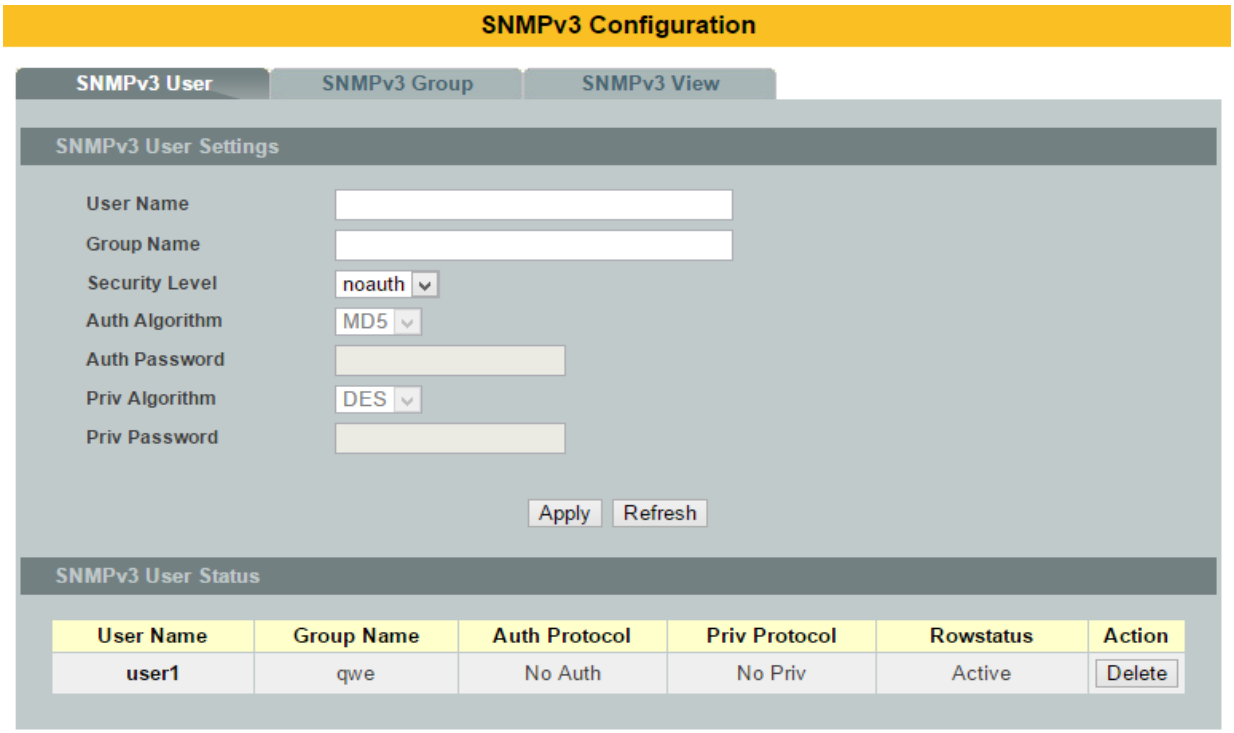
#### 9.1.3.1. CLI Configuration

| Node | Command | Description |
|---|---|---|
| enable | show snmp user | This command displays all snmp v3 users. |
| enable | show snmp group | This command displays all snmp v3 groups. |
| enable | show snmp view | This command displays all snmp v3 view. |
| configure | snmp user USERNAME GROUPNAME noauth | Configures v3 user of non- authentication. |
| configure | snmp user USERNAME GROUPNAME auth (MD5\|SHA) STRINGS | Configures v3 user of authentication. |
| configure | snmp user USERNAME GROUPNAME priv (MD5\|SHA) STRINGS des STRINGS | Configures v3 user osnmf authentication and encryption. |
| configure | snmp group GROUPNAME noauth (read STRINGS write STRINGS notify STRINGS) | Configures v3 group of non- authentication. |
| configure | snmp group GROUPNAME auth (read STRINGS write STRINGS notify STRINGS) | Configures v3 group of authentication. |
| configure | snmp group GROUPNAME priv (read STRINGS write STRINGS notify STRINGS) | Configures v3 group of authentication and encryption. |

| | | |
|---|---|---|
| configure | snmp view VIEWNAME STRINGS (included\|excluded) | To identify the subtree. |
| configure | no snmp user USERNAME GROUPNAME | This command removes a v3 user from switch. |
| configure | no snmp group GROUPNAME | This command removes a v3 group from switch. |
| configure | no snmp view VIEWNAME STRINGS | This command removes a v3 view from switch. |

### 9.1.3.2. Web Configuration

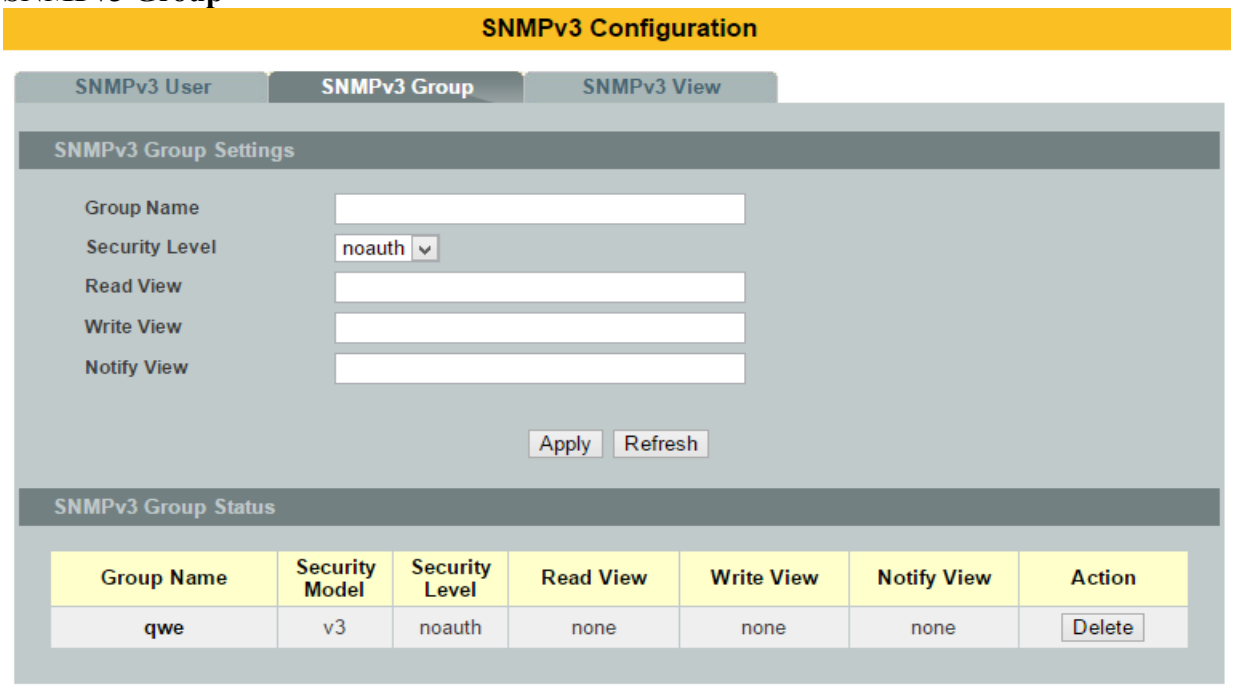
**SNMPv3 User**




| Parameter | Description |
|---|---|
| User Name | Enter the v3 user name. |
| Group Name | Map the v3 user name into a group name. |
| Security Level | Select the security level of the v3 user to use.<br>**noauth** means no authentication and no encryption.<br>**auth** means messages are authenticated but not encrypted.<br>**priv** means messages are authenticated and encrypted. |
| Auth Algorithm | Select **MD5** or **SHA** Algorithm when security level is **auth** or **priv.** |
| Auth Password | Set the password for this user when security level is **auth** or **priv.** |

| | |
|---|---|
| | (pass phrases must be at least 8 characters long!) |
| Priv Algorithm | Select **DES** encryption when security level is **priv.** |
| Priv Password | Set the password for this user when security level is **priv.** (pass phrases must be at least 8 characters long!) |
| Apply | Click **Apply** to configure the settings. |
| Refresh | Click **Refresh** to begin configuring this screen afresh. |
| **SNMPv3 User Status** | |
| User Name | This field displays the v3 user name. |
| Group Name | This field displays the group name which the v3 user mapping. |
| Auth Protocol | These fields display the security level to this v3 user. |
| Priv Protocol | |
| Rowstatus | This field displays the v3 user rowstatus. |
| Action | Click **Delete** to remove a v3 user. |

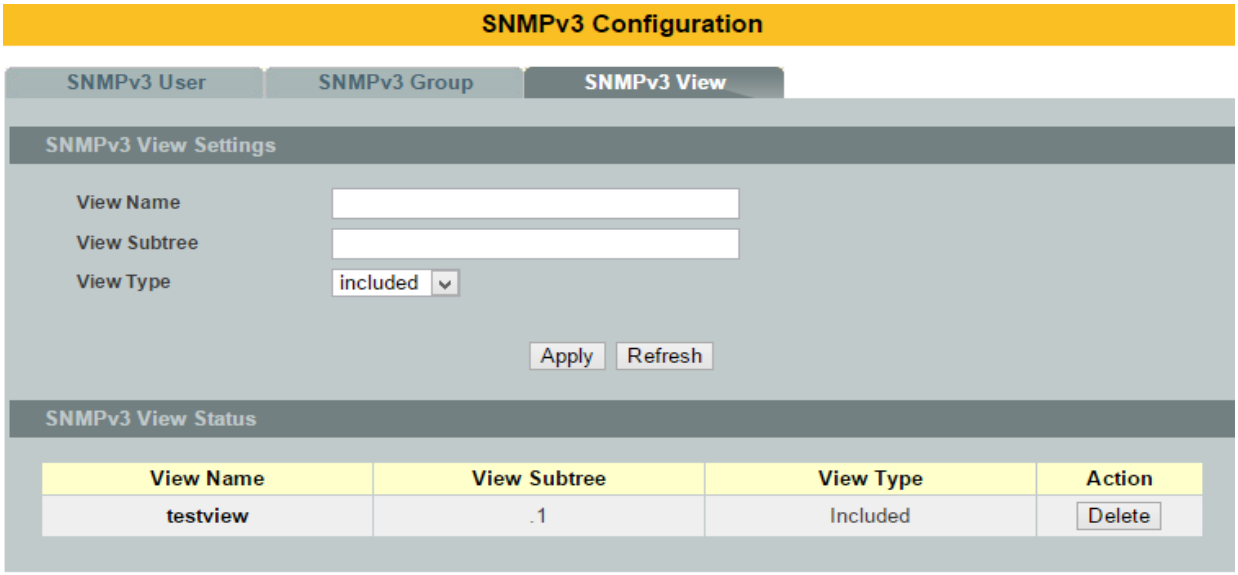
## SNMPv3 Group




| Parameter | Description |
|---|---|
| Group Name | Enter the v3 user name. |

| | |
|---|---|
| Security Level | Select the security level of the v3 group to use. |
| Read View | Note that if a group is defined without a read view than all objects are available to read. (default value is **none**.) |
| Write View | if no write or notify view is defined, no write access is granted and no objects can send notifications to members of the group. (default value is **none**.) |
| Notify View | By using a notify view, a group determines the list of notifications its users can receive. (default value is **none**.) |
| Apply | Click **Apply** to configure the settings. |
| Refresh | Click **Refresh** to begin configuring this screen afresh. |
| **SNMPv3 Group Status** | |
| Group Name | This field displays the v3 user name. |
| Security Model | This field displays the security model of the group.<br>Always displayed **v3**: User-based Security Model (USM) |
| Security Level | This field displays the security level to this group. |
| Read View | These fields display the View list of this group. |
| Write View | |
| Notify View | |
| Action | Click **Delete** to remove a v3 group. |

**SNMPv3 View**



| Parameter | Description |
|---|---|
| View Name | Enter the v3 view name for creating an entry in the SNMPv3 MIB view table. |
| View Subtree | The OID defining the root of the subtree to add to (or exclude from) the named view. |
| View Type | Select **included** or **excluded** to define subtree adding to the view or not. |
| Apply | Click **Apply** to configure the settings. |
| Refresh | Click **Refresh** to begin configuring this screen afresh. |
| **SNMPv3 View Status** | |
| View Name | This field displays the v3 view name. |
| View Subtree | This field displays the subtree. |
| View Type | This field displays the subtree adding to the view or not. |
| Action | Click **Delete** to remove a v3 view. |

## 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: **INS-8648_*Autoprovision.txt***

The contents of the file are listed below:

```
AUTO_PROVISION_VER=1
Firmware_Upgrade_State=1
Firmware_Version=8648P-000-1.1.0.S0
Firmware_Image_File=8648P-000-1.1.0.S0.fw
Firmware_Reboot=1
Global_Configuration_State=0
Global_Configuration_File=8648P-000-1.1.0.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 "AW-IHT-1270_***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:

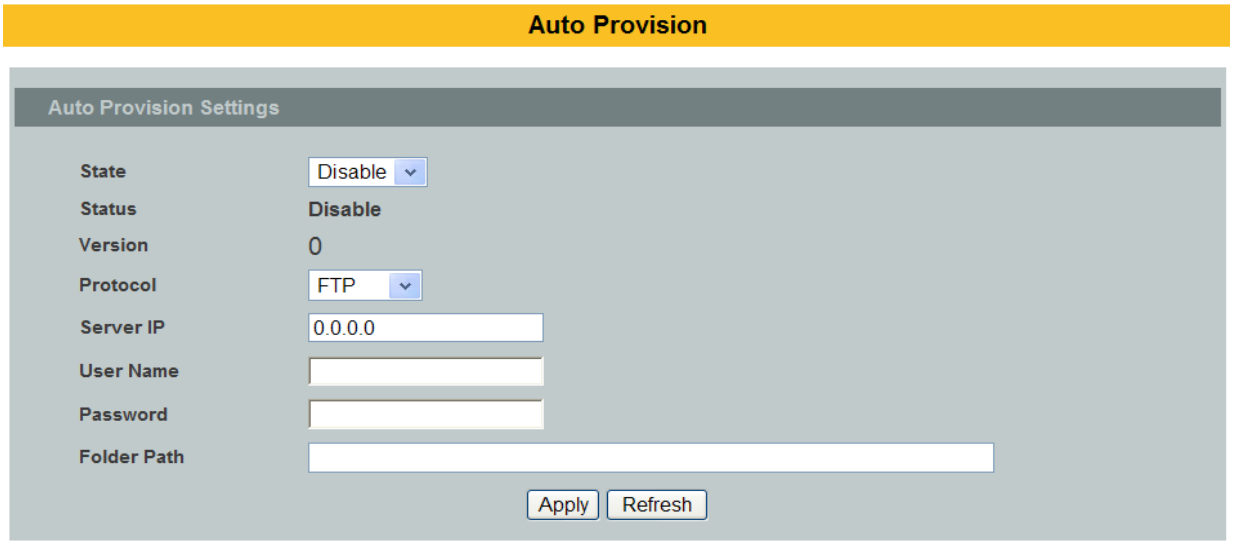
| | |
|---|---|
| Active | : Disable |
| Version | : 0 |
| Protocol | : FTP |
| FTP user/pwd | : / |
| Folder | : |
| Server address | : |

### 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 | This command configures the auto provision |

| | | |
|---|---|---|
| | IPADDR | 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.

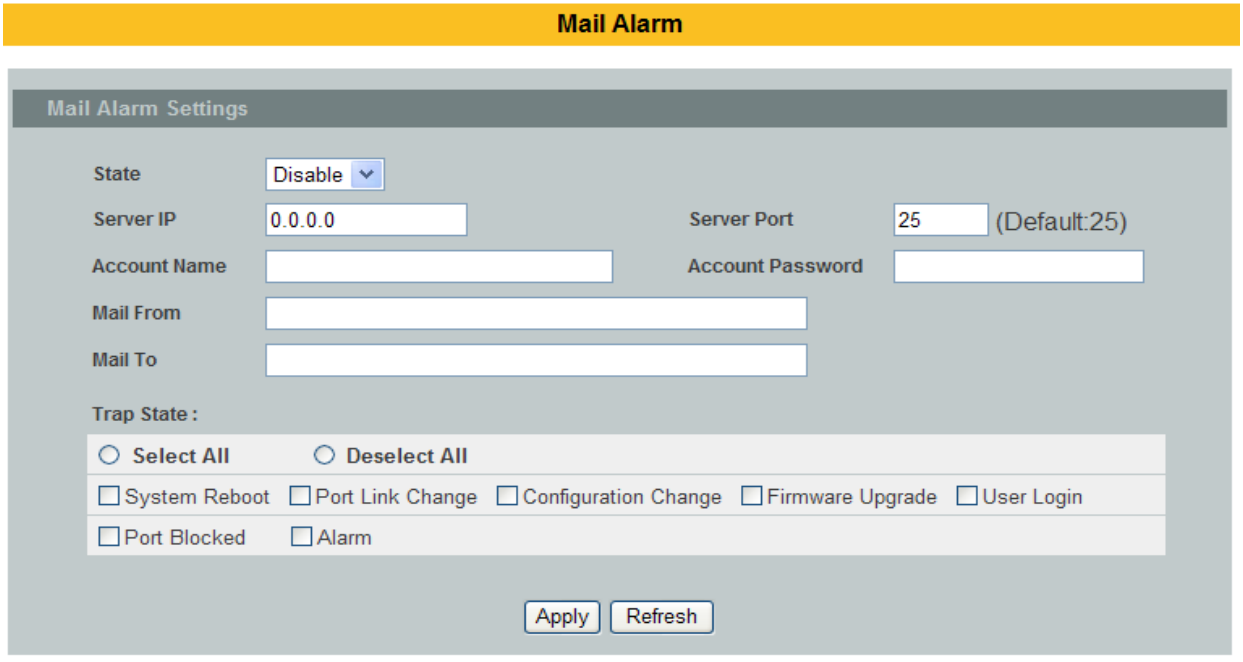
### 9.3.2. Reference

| **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. CLI Configuration

| Node | Command | Description |
|---|---|---|
| enable | show config-change-status | This command displays the configurations status if there are default values. |
| configure | reboot | This command reboots the system. |
| configure | reload default-config | This command copies a default-config file to replace the current one.<br>**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.<br>Where <URL PATH> can be:<br>ftp://user:pass@192.168.1.1/file<br>http://192.168.1.1/file<br>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.<br>Where <URL PATH> can be:<br>ftp://user:pass@192.168.1.1/file<br>http://192.168.1.1/file<br>tftp://192.168.1.1/file |

**Example:**

L2SWITCH#*configure terminal*
L2SWITCH(config)#*interface eth0*
L2SWITCH(config-if)#*ip address 172.20.1.101/24*

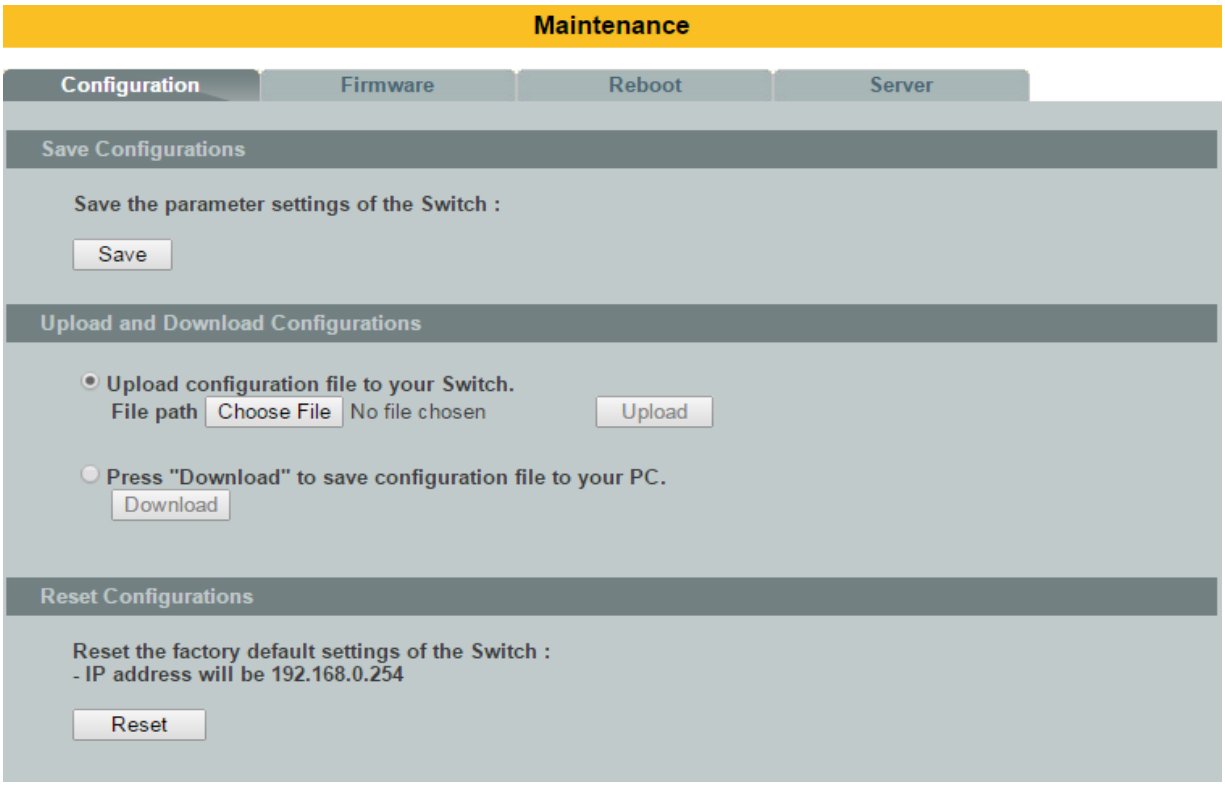
L2SWITCH(config-if)#*ip address default-gateway 172.20.1.1*
L2SWITCH(config-if)#*management vlan 1*

Enable the DHCP client function for the switch.

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

L2SWITCH#show config-change-status
The user configuration file is default.
The configurations have been modified.

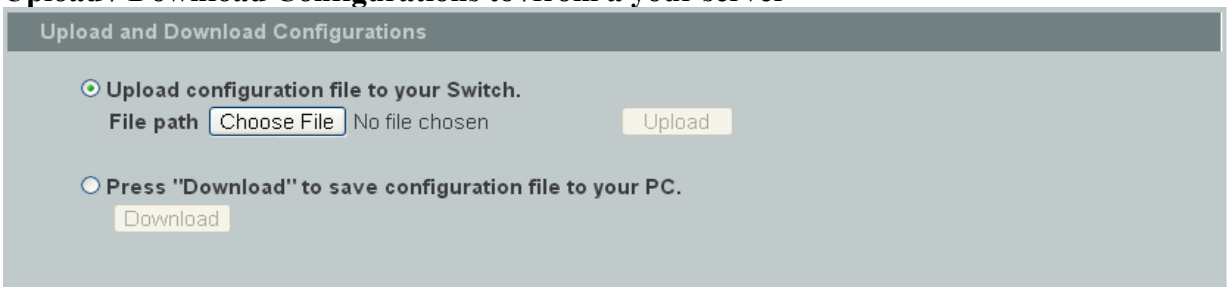
### 9.4.2. Web Configuration




**Save Configurations**


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

**Upload / Download Configurations to /from a your server**



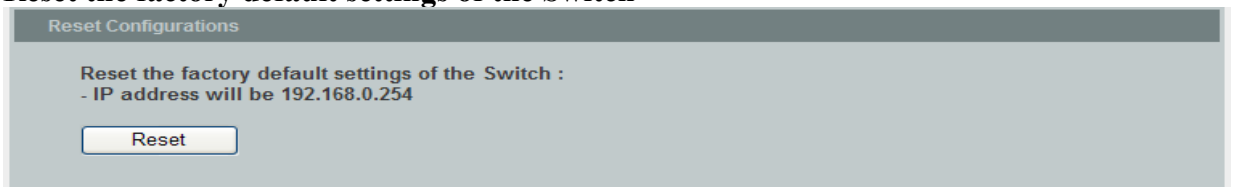

Follow the steps below to save the configuration file to your PC.

- 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:**

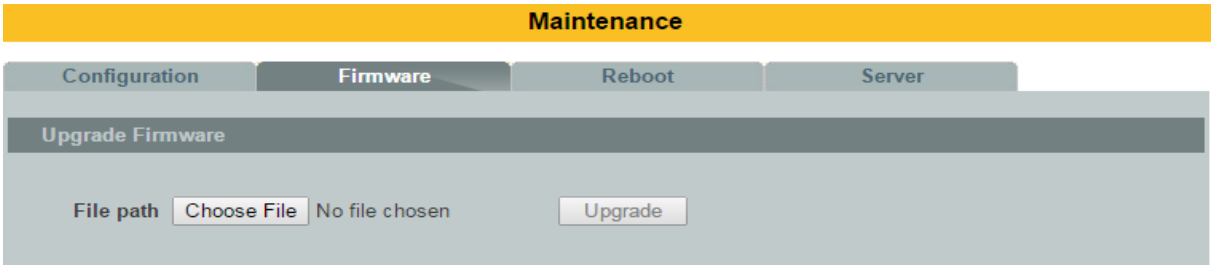
If the user has changed any configurations, the message displays "The configurations have been modified!" Otherwise, the message "The configurations are default values."

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".

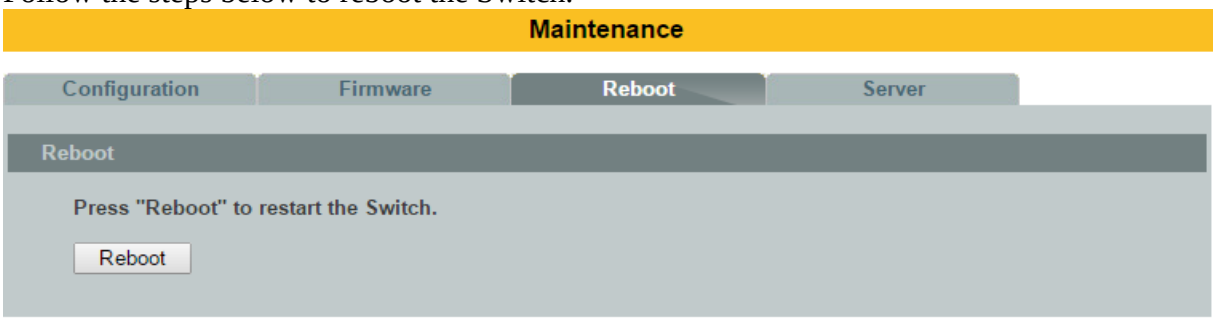
**Firmware**

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.

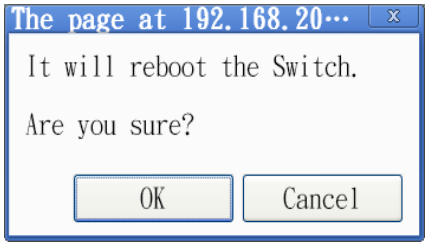



**Reboot**

**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.

### 9.4.3. Server Control

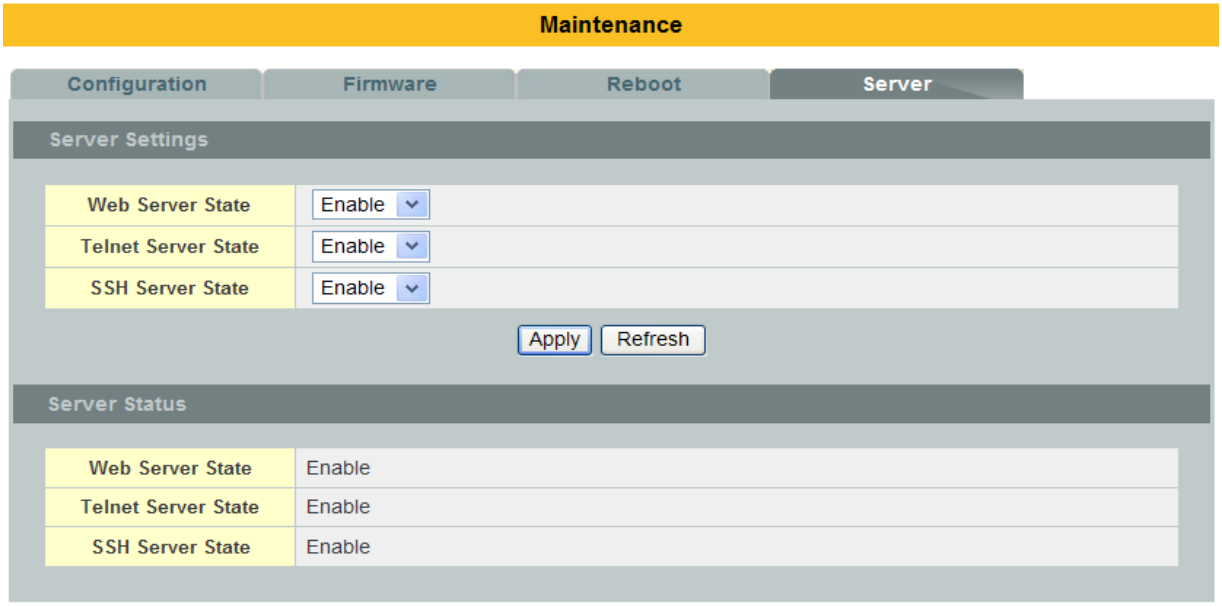
The function allows users to enable or disable the SSH or Telnet or Web service individual using the CLI or GUI.

#### 9.4.3.1. CLI Configuration

| Node | Command | Description |
|---|---|---|
| enable | show server status | This command displays the current server status. |
| 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 | web server | This command enables the web on the Switch. |

| | | |
|---|---|---|
| configure | no web server | This command disables the web on the Switch. |

### 9.4.3.2. Web Configuration




| Parameter | Description |
|---|---|
| Server Settings | |
| Web Server State | Selects Enable or Disable to enable or disable the Web service. |
| Telnet Server State | Selects Enable or Disable to enable or disable the Telnet service. |
| SSH Server State | Selects Enable or Disable to enable or disable the SSH service. |
| Apply | Click Apply to configure the settings. |
| Refresh | Click this button to reset the fields to the last setting. |
| Server Status | |
| Web Server Status | Displays the current Web service status. |
| Telnet Server Status | Displays the current Telnet service status. |
| SSH Server Status | Displays the current SSH service status. |

## 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.

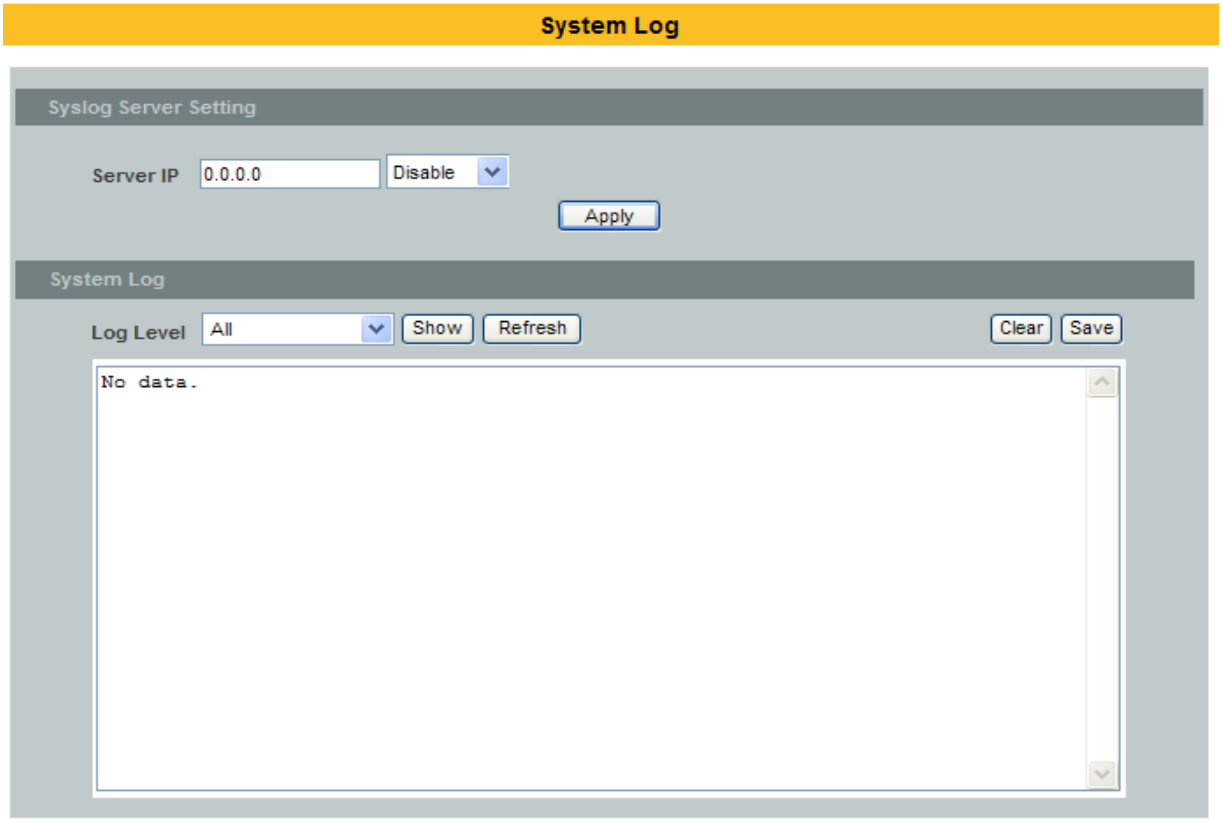
### 9.5.2. CLI Configuration

| Node | Command | Description |
|---|---|---|
| enable | show syslog | The command displays the entire log message recorded in the Switch. |
| enable | show syslog level LEVEL | The command displays the log message with the LEVEL recorded in the Switch. |
| enable | show syslog server | The command displays the syslog server configurations. |
| configure | clear syslog | The command clears the syslog message. |
| configure | syslog-server (disable\|enable) | The command disables / enables the syslog server function. |
| configure | syslog-server ipv4-ip IPADDR | The command configures the syslog server's IP address in IPv4 format. |
| configure | syslog-server ipv6-ip IPADDR | The command configures the syslog server's IP address in IPv6 format. |
| configure | syslog-server facility | The command configures the syslog facility level. |

**Example:**

```
L2SWITCH#configure terminal
L2SWITCH(config)#syslog-server ipv4-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. |
| Log Level | Select **Alert/Critical/Error/Warning/Notice/Information** to choose which log message to want see. |
| Apply | Click Apply to add/modify the settings. |
| Refresh | Click Refresh to begin configuring this screen afresh. |

## 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** user's 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.

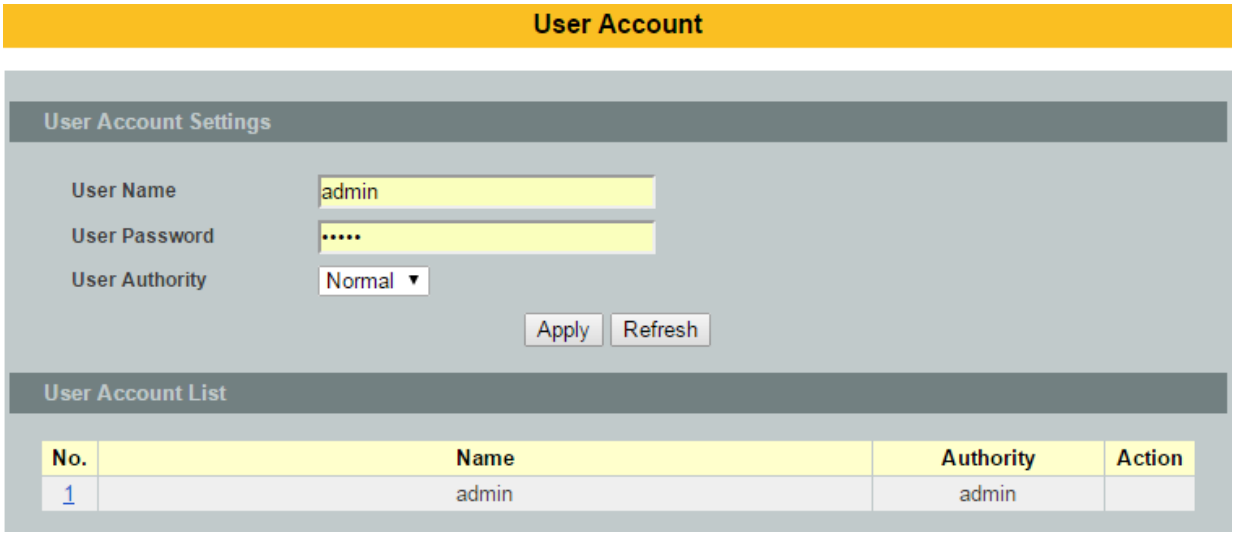
### 9.6.2. CLI Configuration

| 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. |

**Example:**

```
L2SWITCH#configure terminal
L2SWITCH(config)#add user q q admin
L2SWITCH(config)#add user 1 1 normal
```

### 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.<br>Note: You cannot delete the last admin accounts. |