MEN-5314

12-slot 100FX SFP + 2-slot Gigabit SFP Multi-rate
(100/1000Mbps) Managed L2+ Switch

User Manual

VOLKTEK
Connecting Communities

Version 1.0 22nd Aug 2014

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.

CAUTION

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

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

Warning

Table of Content

1. About this Manual

1.1. Welcome

The MEN-5314 Managed Layer 2 Aggregation switch is an industry-first small form-factor fiber switch specifically designed considering the size constraints involved in on-field network deployments. Where time and space are constraints, and broadband competition is high, the MEN-5314 is a much quicker deployment solution that reduces time-to-deploy across large number of locations. Easily deploy the MEN-5314 along with your existing access switch cabinet and avoid unnecessary CAPEX by preventing additional cables and cabinet installation costs.

Equipped with 12-slot 100Mbps SFP downlinks plus 2 Gigabit Multi-rate SFP uplinks, the MEN-5314 is capable of connecting up to 14 network devices for Fast Ethernet and Gigabit Ethernet. Extensive software features of the switch deliver high-quality, reliable yet simple-to-use experience to its users. The MEN-5314 is a high performance and time-saving solution for service providers who want to increase the bandwidths, reduce transmission bottlenecks and offer highly flexible packages to low density subscriber base with medium ARPU.

1.2. Purpose

This manual discusses how to install and configure your Managed Layer 2 Aggregation Switch.

1.3. Terms/ Usage

In this manual, the term “Switch” (first letter upper case) refers to the MEN-5314 Switch, and “switch” (first letter lower case) refers to other switches.

2. About the MEN-5314

2.1. Features

Network Function

Static trunk / LACP

STP/RSTP

Loop Detection with Auto-recovery timer

IGMP snooping (v1/v2, v3)

MVR

User Security

DHCP Snooping

Access Control List (L2/L3/L4)

Static MAC Forwarding

MAC Limitation

ARP Inspection

Port Authentication

Port Security

Abnormal Traffic Detection

Network Management

SNMP v1/v2c

SNMP Trap

Port-based Mirroring

SNTP

RS-232 console port

CLI through console

Telnet

Web-based GUI

Status display and event report

Auto-logout timer

Firmware upgrade by TFTP/HTTP/FTP

Configuration backup/restore

User self-defined default configuration

Traffic Management & QoS

802.1Q Tag-based VLAN

Port-based VLAN

Active VLAN support: 4K

Management VLAN

802.1p Priority Queues per port

Traffic Classification

Network Storm Control

Rate Limitation

2.2. Specifications

IEEE Standards

IEEE 802.3u	100Base-/FX
IEEE 802.3z	1000Base-SX/LX/LHX
IEEE 802.3ad	Link Aggregation
IEEE 802.1d	Spanning Tree Protocol
IEEE 802.1w	Rapid Spanning Tree Protocol
IEEE 802.3x	Flow Control
IEEE 802.1p	Priority Queues

IEEE 802.1x	Port Authentication
IEEE 802.1q	VLAN Tagging

Performance

Throughput	148,800 pps to 100 Mbps ports
	1,488,000 pps to 1000 Mbps ports
Switching fabric	6.4 Gbps
L2 forwarding	4.8 Mpps
MAC entries	16k

Connectors and Cabling:

Ports:	- Uplink: 2-slot Gigabit SFP Multi-rate
	- Downlink: 12-slot x 100FX SFP
Console Interface	1 x DB9 (female) console port

Mechanical & Environmental

Operating temperature	0℃ to 50℃
Storage temperature	0℃ to 70℃
Operating humidity	10% to 80% RH (non-condensing)
Storage humidity	5% to 95% RH (non-condensing)

Power

Front access AC power	100 ~ 240VAC/Max 300VAC, 50 ~ 60Hz
15VDC	Optional
12V DC battery back-up	Optional
Power consumption	21.3W (w/o Battery)

Dimensions & Weight

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

2.3. Hardware Description

MEN-5314 Front Panel

12-slot 100Base-FX SFP + 2-slot Gigabit Multi-rate SFP

2.4. Connectors

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

2.4.1. 100Base-FX Ports

The 100BASE-FX ports support network speeds of 100Mbps. These ports can gives true "plug-n-play" capability – just plug the network cables into the ports.

2.4.2. Gigabit SFP Ports

There are two Gigabit SFP ports on the MEN-5314 operate at speed of 100 or 1000Mbps.

2.5. Installation

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

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

2.5.1. Desktop Installation

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

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

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

firmly in place.

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

2.5.2. Mounting on a Rack

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

2.5.3. Getting Connected

The Switch is capable of connecting up to 14 network devices with fiber cabling paths at Fast Ethernet speed for downlink, or Gigabit Ethernet speed for uplink.

2.5.4. Powering On the Unit

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

1. Insert the power cable plug directly into the receptacle located at the front of the device.

2. Plug the power adapter into an available socket.
   Note: For international use, you may need to change the AC power adapter cord. You must use a power cord set that has been approved for the receptacle type and electrical current in your country.

3. 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.

2.5.5. 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).

2.5.6. Connecting to Computer or a LAN

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

2.5.7. Power on the Unit

Connect the AC power cord to the POWER receptacle on the front of the Switch and plug the other end of the power cord into a wall outlet or a power strip.

Check the front LED indicators with the description in the next chapter. If the LEDs light up as described, the Switch's hardware is working properly.

2.5.8. LED Indicators

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

Unit LEDs		
LED	**Condition**	**Status**
POWER (Green)	Illuminated	Power on
	Off	Power off or fail
POST (Green)	Illuminated	Switch is ready and running ok
	Blinking	Switch is booting
	Off	Switch is not ready or failed
LNK/ACT (Green) (for 1~12th Fiber ports)	Illuminated	100Mbps Ethernet link-up
	Blinking	Receiving or transmitting data
	Off	Port disconnected or link failed
LNK (Green) (for 13~14th Fiber ports)	Upper Green	1000Mbps Ethernet link-up
	Middle Green	100Mbps Ethernet link-up
	Bottom Green	Receiving or transmitting data
	Off	Port disconnected or link failed

3. Management options

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

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

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

3.1. Management via console port

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

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

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

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

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

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

3.2. Management by Telnet

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

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

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

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

3.3. How to enter the CLI?

Press [Enter] key to enter the login command prompt when below message is displayed on the screen.
Please press Enter to activate this console

Input "***admin***" to enter the CLI mode when below message is displayed on the screen.
L2SWITCH login:

You can execute a few limited commands when CLI prompt is displayed as below.
L2SWITCH>

If you want to execute more powerful commands, you must enter the privileged mode.
Input command "***enable***"
L2SWITCH>enable

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

L2SWITCH#

3.4. CLI command concept

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

The Node type:

- enable
  Its command prompt is "***L2SWITCH#".***
  It means these commands can be executed in this command prompt.

- configure
  Its command prompt is "***L2SWITCH(config)#".***
  It means these commands can be executed in this command prompt.
  In ***Enable*** code, executing command "***configure terminal***" enter the configure node.
  L2SWITCH# configure terminal

- eth0
  Its command prompt is "***L2SWITCH(config-if)#".***
  It means these commands can be executed in this command prompt.
  In ***Configure*** code, executing command "***interface eth0***" enter the eth0 interface node.
  L2SWITCH(config)#interface eth0
  L2SWITCH(config-if)#

- interface
  Its command prompt is "***L2SWITCH(config-if)#".***
  It means these commands can be executed in this command prompt.
  In ***Configure*** code, executing command "***interface 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.

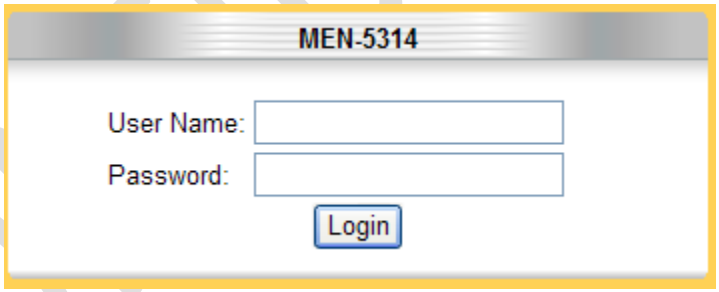
  L2SWITCH(config)#vlan 2
  L2SWITCH(config-vlan)#

- 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)#

3.5. Management via Internet Browser Interface

From a PC, open your Web browser, type the following in the Web address (or location) box: http://192.168.0.254 and then press <Enter>.
This is the factory default IP address for the switch. A login dialog is displayed, as shown in the figure:



Enter your user name and password, and then click OK.
Use the defaults the first time you log into the program. You can change the password at any time through CLI interface.

Default:
User name: admin,
Password: admin.

3.6. System Information

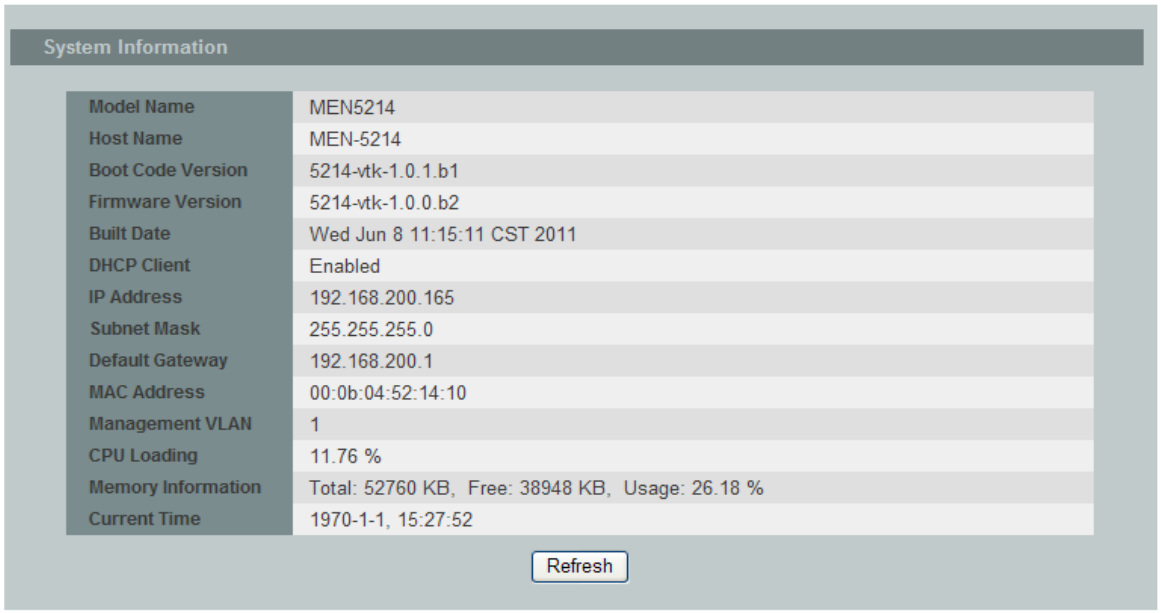
The System Information window appears each time you log into the program. Alternatively, this window can be accessed by clicking System Status > System Information

3.6.1. CLI Configuration

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

3.6.2. Web Configuration

System Information



Parameter	Description
Model Name	This field displays the model name of your Switch.
Host name	This field displays the name of your Switch.
Boot Code Version	This field displays the boot code version.
Firmware Version	This field displays the version number of the currently installed firmware.
Built Date	This field displays the built date of the currently installed firmware.
DHCP Client	This field displays whether the DHCP client feature is enabled.
IP Address	This field indicates the IP address of the Switch.
Subnet Mask	This field indicates the subnet mask of the Switch.

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

4. Basic Settings

4.1. General Settings

4.1.1. System

Management VLAN

To specify a VLAN group which can access the Switch.

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

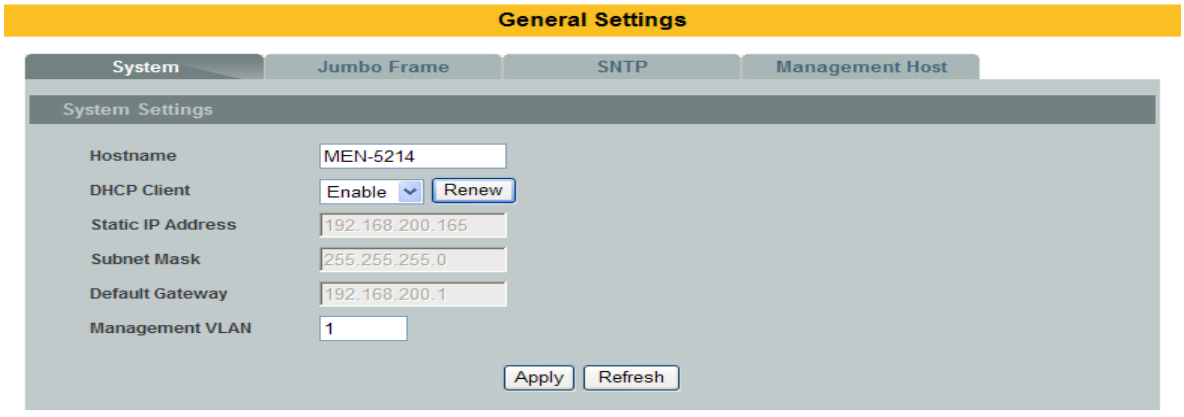
Host Name

The **hostname** is 16 alphanumeric characters for the name of your Switch. The hostname should be the combination of the digit or the alphabet or hyphens (-) or underscores (_).

4.1.1.1. CLI Configuration

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

4.1.1.2. Web Configuration



Parameter	Description
Hostname	Enter up to 16 alphanumeric characters for the name of your Switch. The hostname should be the combination of the digit or the alphabet or hyphens (-) or underscores (_).
DHCP Client	Select **Enable** to allow the Switch to automatically get an IP address from a DHCP server. Click **Renew** to have the Switch re-get an IP address from the DHCP server. Select **Disable** if you want to configure the Switch's IP address manually.
Static IP Address	Enter the IP address of your Switch in dotted decimal notation. For example, 192.168.0.254.
Subnet Mask	Enter the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.1.
Management VLAN	Enter a VLAN ID used for Switch management purposes.
Apply	Click **Apply** to take effect the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.

Default Settings

The default Hostname is L2SWITCH
The default Jumbo frame size is 2048 bytes.
The default DHCP client is disabled.
The default Static IP is 192.168.0.254
Subnet Mask is 255.255.255.0
Default Gateway is 0.0.0.0
Management VLAN is 1.

4.1.2. Jumbo Frame

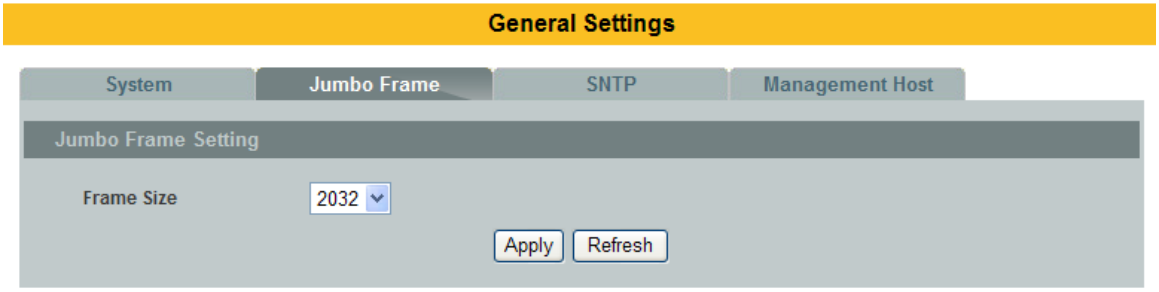
Jumbo frames are Ethernet frames with a payload greater than 1500 bytes. Jumbo frames can enhance data transmission efficiency in a network. The jumbo frame settings will apply to all ports.

The available values are 2032, 2000, 9712.

4.1.2.1. CLI Configuration

Node	Command	Description
configure	jumboframe (2032|2000|9712)	This command configures the maximum number of bytes of a jumbo frame for all ports. The bigger the frame size, the better the performance.

4.1.2.2. Web Configuration



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

Default Setting: The default jumbo frame is 2032 bytes.

4.1.3. SNTP

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

UDP Port: 123.

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

Note:

1. The SNTP server always replies the UTC current time.
2. When the Switch receives the SNTP reply time, the Switch will adjust the time with the time zone configuration and then configure the time to the Switch.
3. If the time server's IP address is not configured, the Switch will not send any SNTP request packets.
4. If no SNTP reply packets, the Switch will retry every 10 seconds forever.
5. If the Switch has received SNTP reply, the Switch will re-get the time from NTP server every one hour.
6. If the time zone and time NTP server have been changed, the Switch will repeat the query process.
7. No default SNTP server.

4.1.3.1. CLI Configuration

Node	Command	Description
enable	show time	This command displays current time and time configurations.
configure	time HOUR:MINUTE:SECOND	Sets the current time on the Switch. *hour*: 0-23 *min*: 0-59 *sec*: 0-59 Note: If you configure Daylight Saving Time after you configure the time, the Switch will apply Daylight Saving Time.
configure	time date YEAR/MONTH/DAY	Sets the current date on the Switch. *year*: 1970- *month*: 1-12 *day*: 1-31
configure	time daylight-saving-time	This command enables the daylight saving time.
configure	time daylight-saving-time start-date <month> <*day*> <hour>	This command sets the start time of the Daylight Saving Time.
configure	time daylight-saving-time end-date <month> <*day*> <hour>	This command sets the end time of the Daylight Saving Time.
configure	no time daylight-saving-time	This command disables daylight saving on the Switch.
configure	time ntp-server IP_ADDRESS	This command sets the IP address of your time server.
configure	no time ntp-server	This command disables the NTP server settings.
configure	time timezone operator (+|-) hour (VALUE 0~14) min (VALUE 00 or 30)	Selects the time difference between UTC (formerly known as GMT) and your time zone.

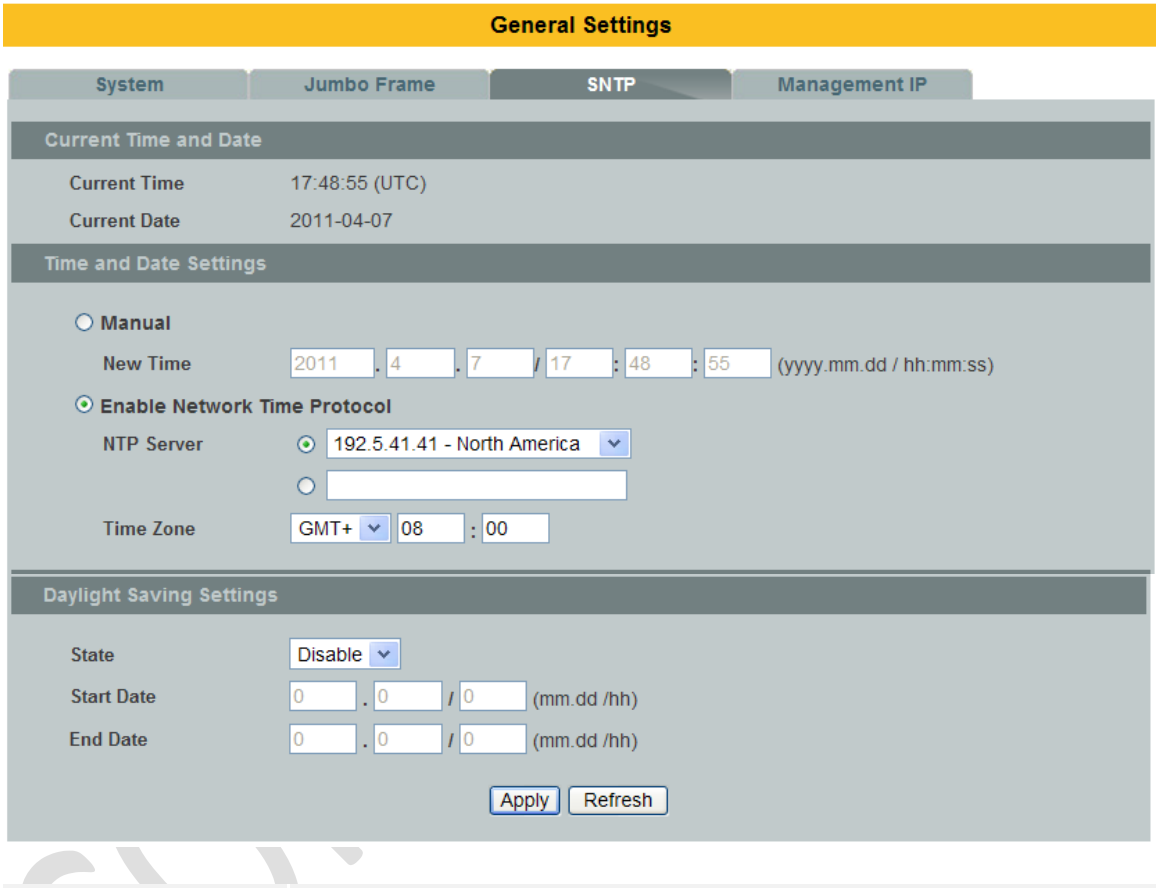
Example:

L2SWITCH(config)#*time ntp-server 192.5.41.41*
L2SWITCH(config)#*time timezone operator + hour 8 min 0*
L2SWITCH#show time

```
Current Time:
-----------------------------------------------

  Time: 13:46:54 (UTC)
  Date: 2011-4-8

Time Server Configuration:
-----------------------------------------------

  Time Zone : +0800
```

```
IP Address: 192.5.41.41

DayLight Saving Time Configuration:
-------------------------------------------
  State     : disabled
  Start Date: None.
  End Date  : None.
```

4.1.3.2. Web Configuration



Parameter	Description
Current Time and Date	
Current Time	This field displays the time you open / refresh this menu.
Current Date	This field displays the date you open / refresh this menu.
Time and Date Setting	
Manual	Select this option if you want to enter the system date and time manually.
New Time	Enter the new date in year, month and day format and time in hour, minute and second format. The new date and time then

	appear in the **Current Date** and **Current Time** fields after you click **Apply**.
Enable Network Time Protocol	Select this option to use Network Time Protocol (NTP) for the time service.
NTP Server	Select a pre-designated time server or type the IP address of your time server. The Switch searches for the timeserver for up to 60 seconds.
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone 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: 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**. 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: 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**. 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.

Default Settings

```
L2SWITCH#show time
Current Time:
-----------------------------------------------
   Time    : 0:1:4 (UTC)
   Date    : 2000-1-1

Time Server Configuration:
-----------------------------------------------
   Time Zone  : +0000
   IP Address  : 0.0.0.0

DayLight Saving Time Configuration:
-----------------------------------------------
   State          : disabled
   Start Date     : None.
   End Date       : None.
```

4.1.4. Management Host

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

4.1.4.1. CLI Configuration

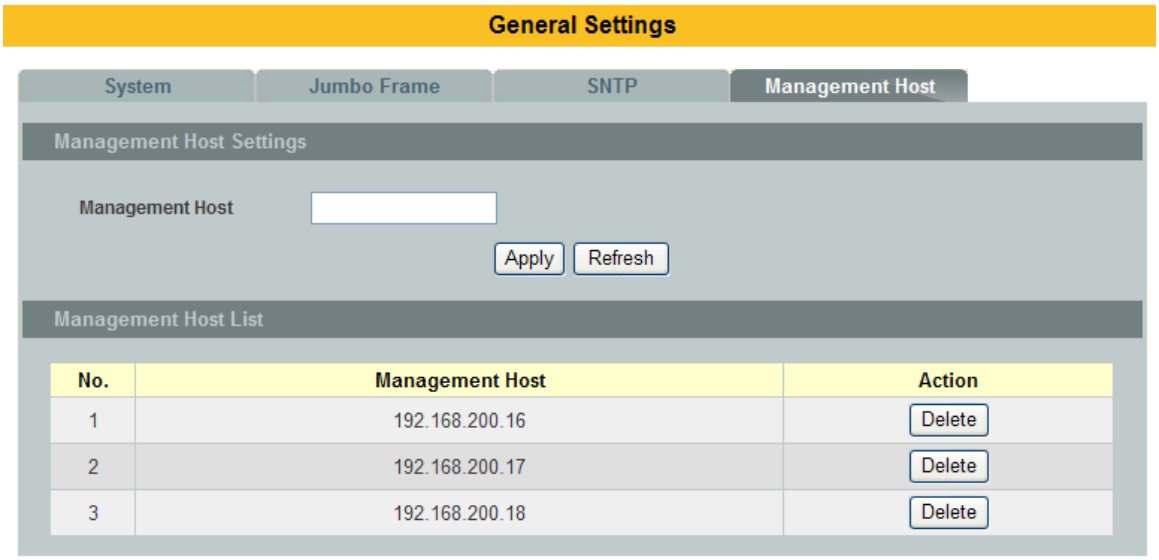
Node	Command	Description
enable	show interface eth0	The command displays the all of the interface *eth0* configurations.
eth0	show	The command displays the all of the interface *eth0* configurations.
eth0	management host A.B.C.D	The command adds a management host address.
eth0	no management host A.B.C.D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

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#interface eth0
```

```
L2SWITCH(config-if)#management host 192.168.200.106
L2SWITCH(config-if)#show
Eth0    DHCP client: Enable
        Management vlan: 1
        Management Host: 192.168.200.106
        Default gateway: 192.168.200.1
        Link encap:Ethernet    HWaddr 00:02:09:02:06:17
        inet addr:192.168.200.120    Bcast:192.168.200.255    Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST    MTU:1500    Metric:1 ASYMMTU:0
        RX packets:262 errors:0 dropped:0 overruns:0 frame:0
        TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:23630 (23.0 kb)    TX bytes:2492 (2.4 kb)
        Interrupt:24
```

4.1.4.2. Web Configuration



Parameter	Description
Management Host	This field configures the management host.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
No.	This field displays a sequential number for each management host.
Management Host	This field displays the management host.
Action	Click **Delete** to remove the specified entry.

4.2. MAC Management

Dynamic Address:
When the switch receives frames, it will record source MAC, 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 static addresses will not be aged out by the switch. The static address can be removed by user only.

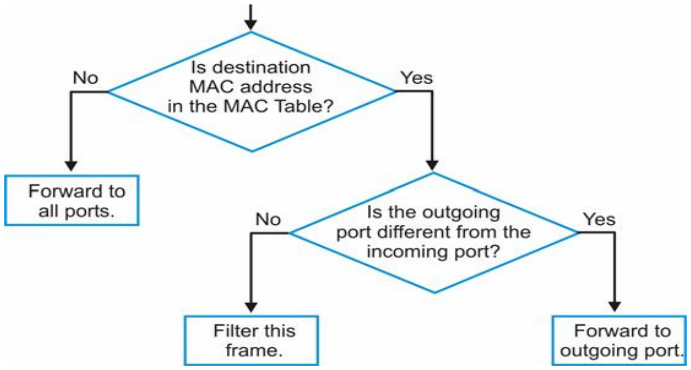
The switch supports up to 16K address table. The static address and the dynamic address share the same table.

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

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

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



4.2.1. CLI Configuration

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

Example:

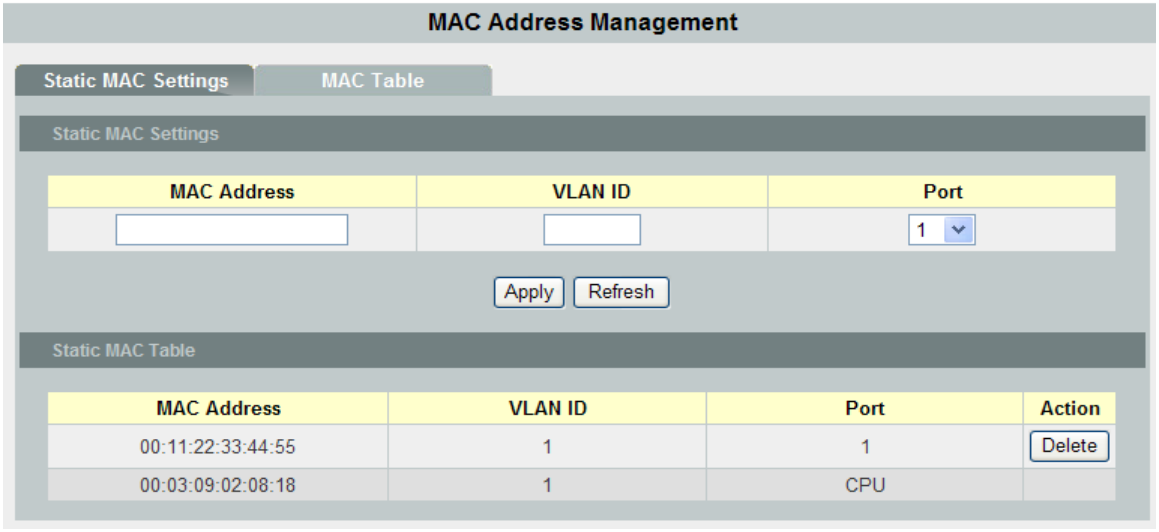
L2SWITCH(config)#mac-address-table static 00:11:22:33:44:55 vlan 1 port 1
L2SWITCH#show mac-address-table static

```
MAC Address        Type      VLAN  Port
-----------------  --------  ----  ----
00:02:09:02:06:17  Static    1     CPU
00:11:22:33:44:55  Static    1     1
```

4.2.2. Web Configuration

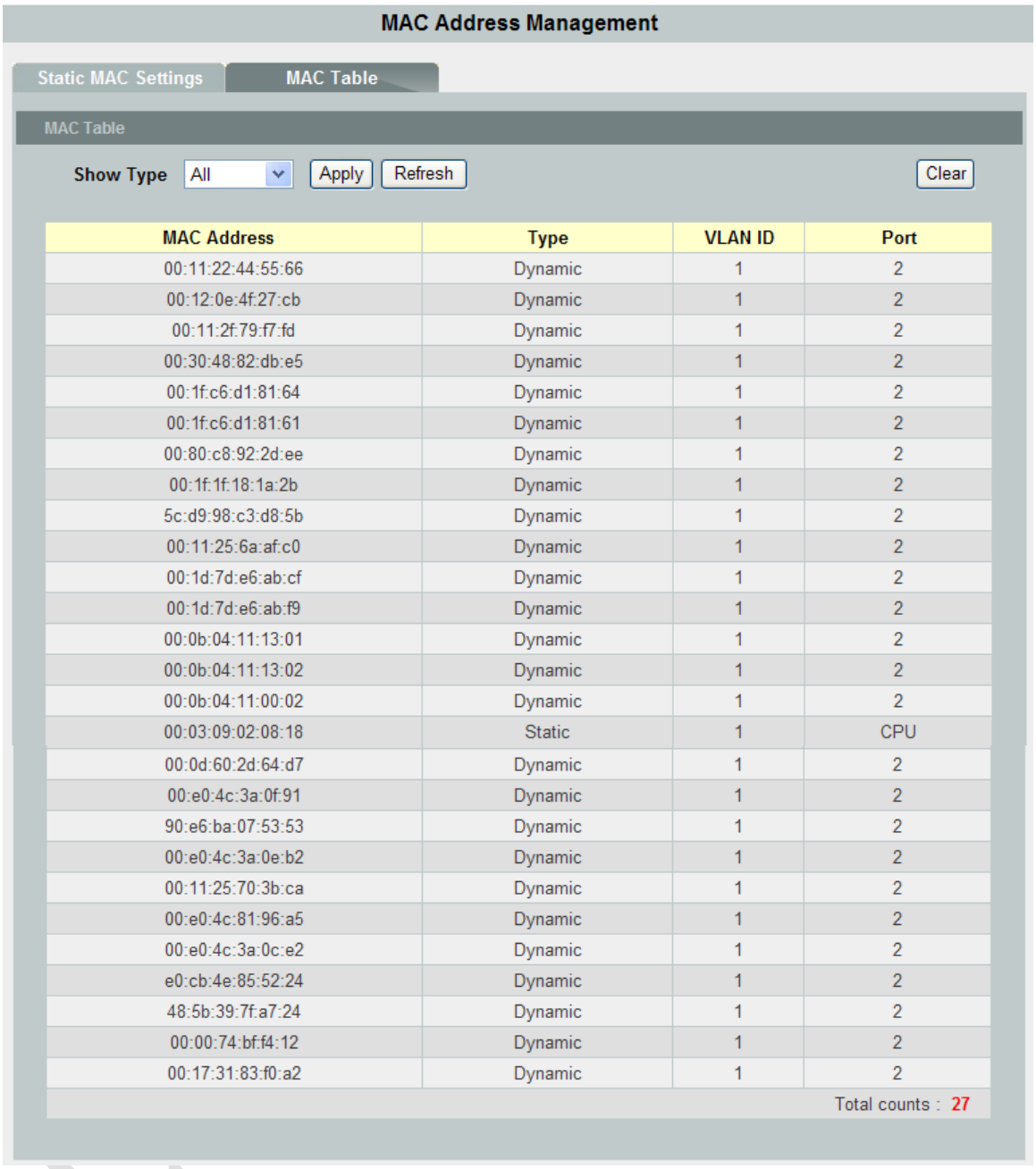
4.2.2.1. Static MAC

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



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

4.2.2.2. MAC Table



Parameter	Description
Show Type Apply	Select **Static**, **Dynamic**, or **All** and then click **Apply** to display the corresponding MAC address entries on this screen.
Refresh	Click this to update the information in the MAC table.
MAC Address	This field displays a MAC address.
Type	This field displays whether this entry was entered manually (Static) or whether it was learned by the Switch (Dynamic).

VLAN ID	This field displays the VLAN ID of the MAC address entry.
Port	This field displays the port number the MAC address entry is associated. It displays CPU if it is the entry for the Switch itself. The CPU means that it is the Switch's MAC.
Total Counts	This field displays the total entries in the MAC table.

4.3. Port Mirror

The Port Mirroring is used on a network switch to send a copy of network packets sent/received on one or a range of switch port 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 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.

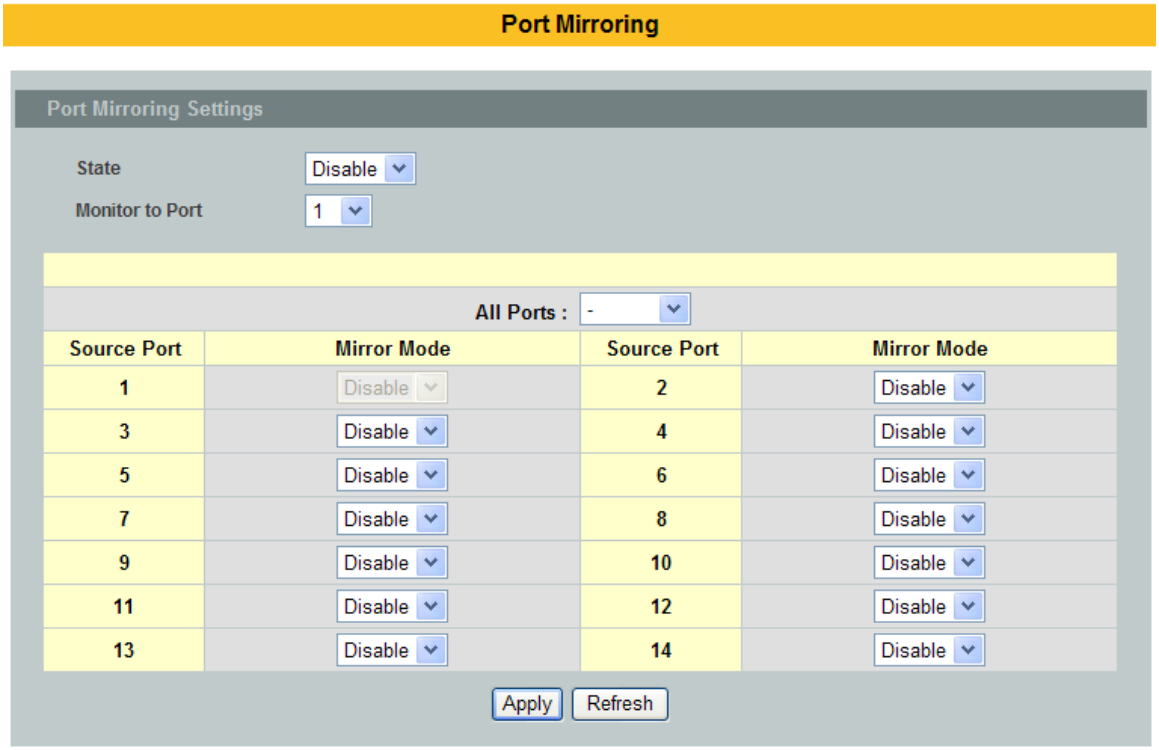
4.3.1. CLI Configuration

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

Example:

L2SWITCH#*configure terminal*
L2SWITCH(config)#mirror enable
L2SWITCH(config)#mirror destination port 2
L2SWITCH(config)#mirror source ports 3-11 mode both
L2SWITCH#show mirror
Mirror Configurations:
State : Enable
Monitor port : 2
Ingress port(s) : 3-11
Egress port(s) : 3-11

4.3.2. Web Configuration



Parameter	Description
State	Select **Enable** to turn on port mirroring or select **Disable** to turn it off.
Monitor to Port	Select the port which connects to a network traffic analyzer.
All Ports	Settings in this field apply to all ports. Use this field only if you want to make some settings the same for all ports. Use this field first to set the common settings and then make adjustments on a port-by-port basis.
Source Port	This field displays the number of a port.

Mirror Mode	Select **Ingress**, **Egress** or **Both** to only copy the ingress (incoming), egress (outgoing) or both (incoming and outgoing) traffic from the specified source ports to the monitor port. Select **Disable** to not copy any traffic from the specified source ports to the monitor port.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

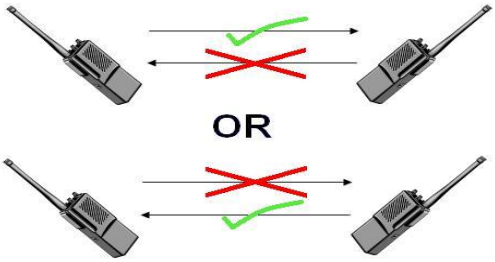
4.4. Port Settings

- Duplex mode

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

Half Duplex:

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



Full Duplex:

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

- Loopback Test

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

- Auto MDI-MDIX

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

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

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

- Auto Negotiation

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

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

- Flow Control

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

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

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

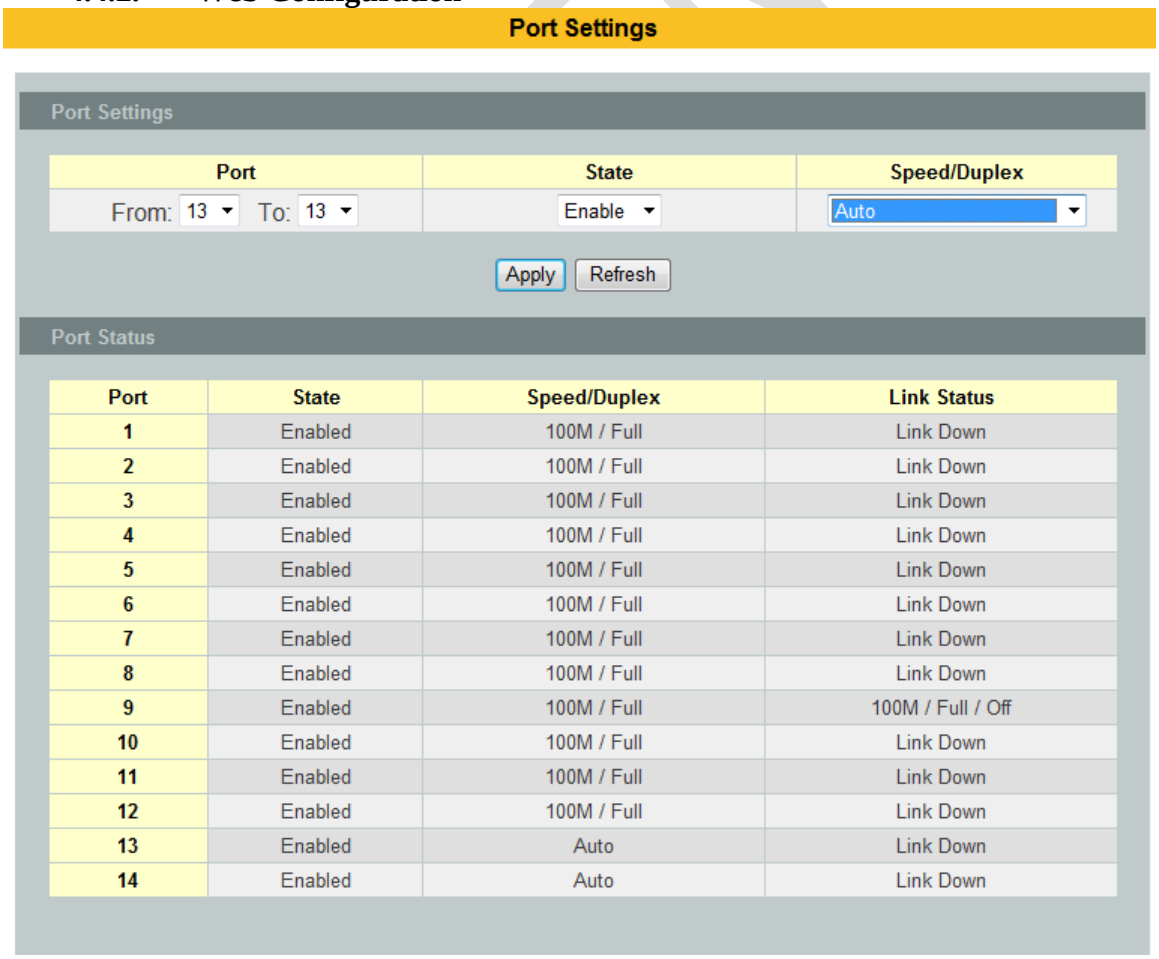
4.4.1. CLI Configuration

Node	Command	Description
enable	show interface IFNAME	This command displays the curent port configurations.
interface	show	This command displays the current port configurations.
interface	loopback (none | phy)	This command specifies the loopback mode of operation for the specific port.
interface	speed (auto|100-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.

Example:

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

4.4.2. Web Configuration



Parameter	Description
Port	Select a port number you want to configure on this screen.
State	Select **Enable** to activate the port or **Disable** to deactivate the port.
Speed/Duplex	Select the speed and duplex mode of the port. The choices are: • **Auto** • **100 Mbps / Full Duplex**
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 **100M** or **1000M** and the duplex mode **Full**.
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.

5. Advanced Settings

5.1. Bandwidth Control

5.1.1. QoS

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

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

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

The Switch supports 802.1p priority queuing. The Switch has 8 priority queues. These priority queues are numbered from 3 (Class 3) — 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, 3, to the lowest priority queue, 0. Each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue will begin transmitting any packets it may have received.

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.

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

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

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

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

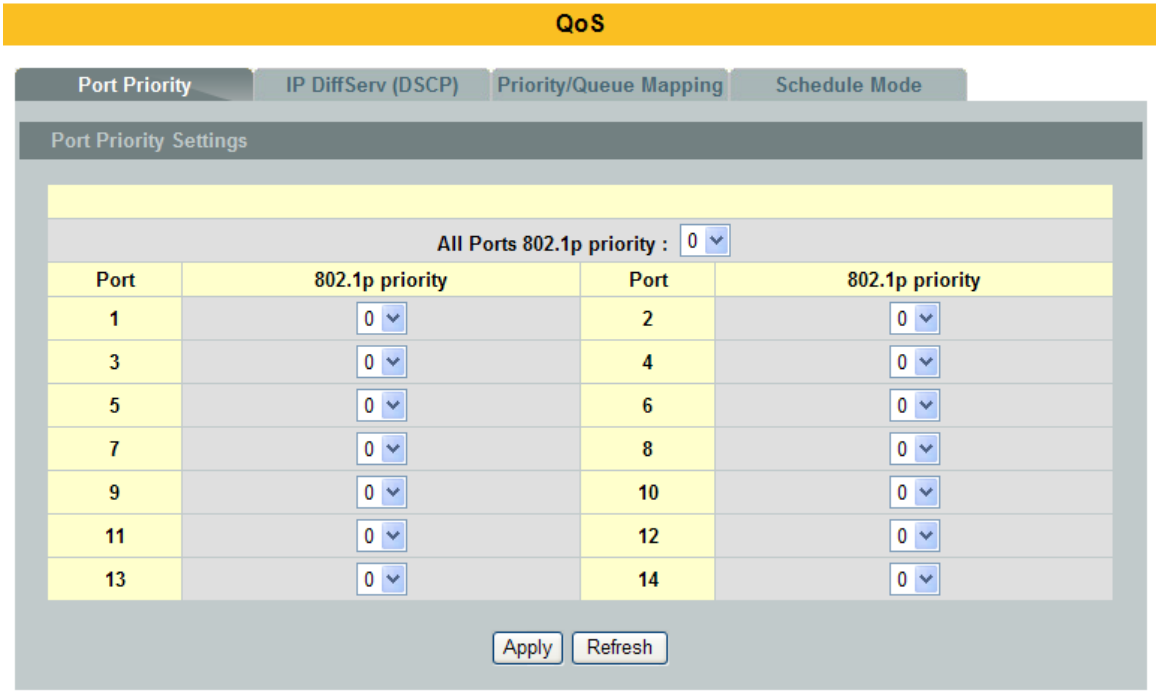
5.1.1.1. CLI Configuration

Node	Command	Description
enable	show queue cos-map	This command displays the current 802.1p priority mapping to the service queue.
enable	show qos mode	This command displays the current QoS scheduling mode of IEEE 802.1p.
enable	show diffserv	This command displays the Displays general DiffServ settings.
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. Default: Priority: 0 1 2 3 4 5 6 7 Queue : 1 0 0 1 2 2 3 3
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 VALUE	This command configures the QoS scheduling mode to Weighted Round Robin.
interface	default-priority	This command allows the user to specify a default priority handling of untagged packets received by the Switch. The priority value entered with this command will be used to determine which of the hardware priority queues the packet is forwarded to. Default: 0.
interface	no default-priority	This command configures the default priority for the specific port to default (0).

5.1.1.2. Web Configuration

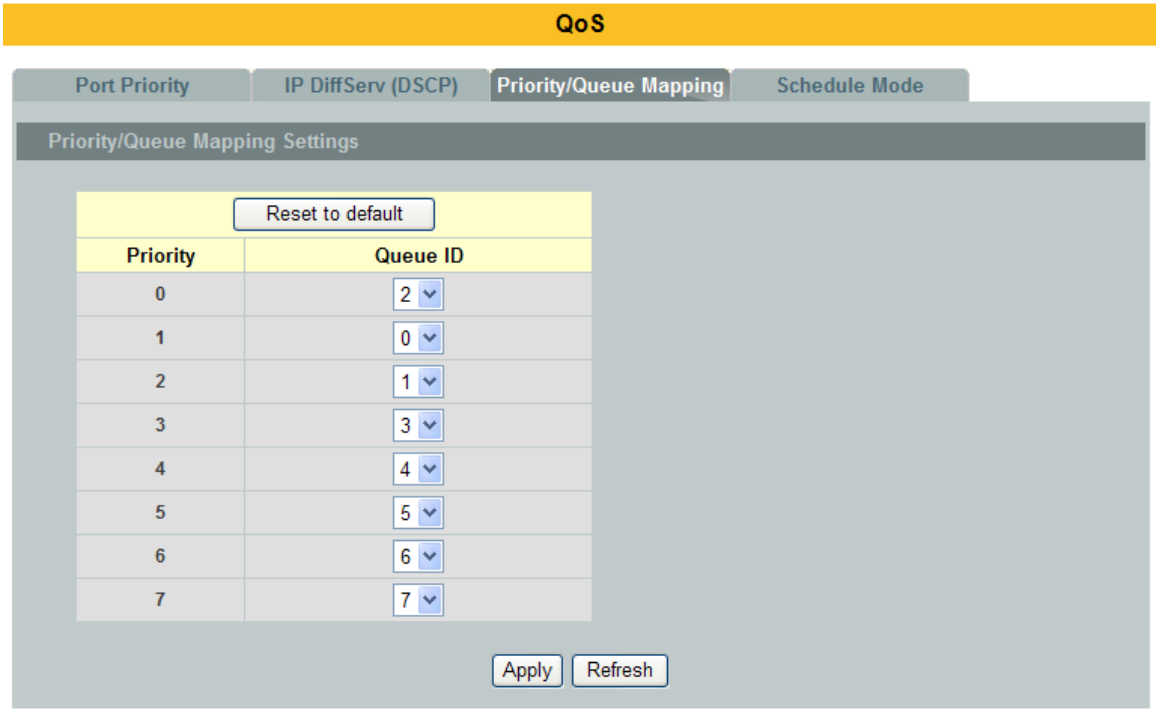
Port Priority



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

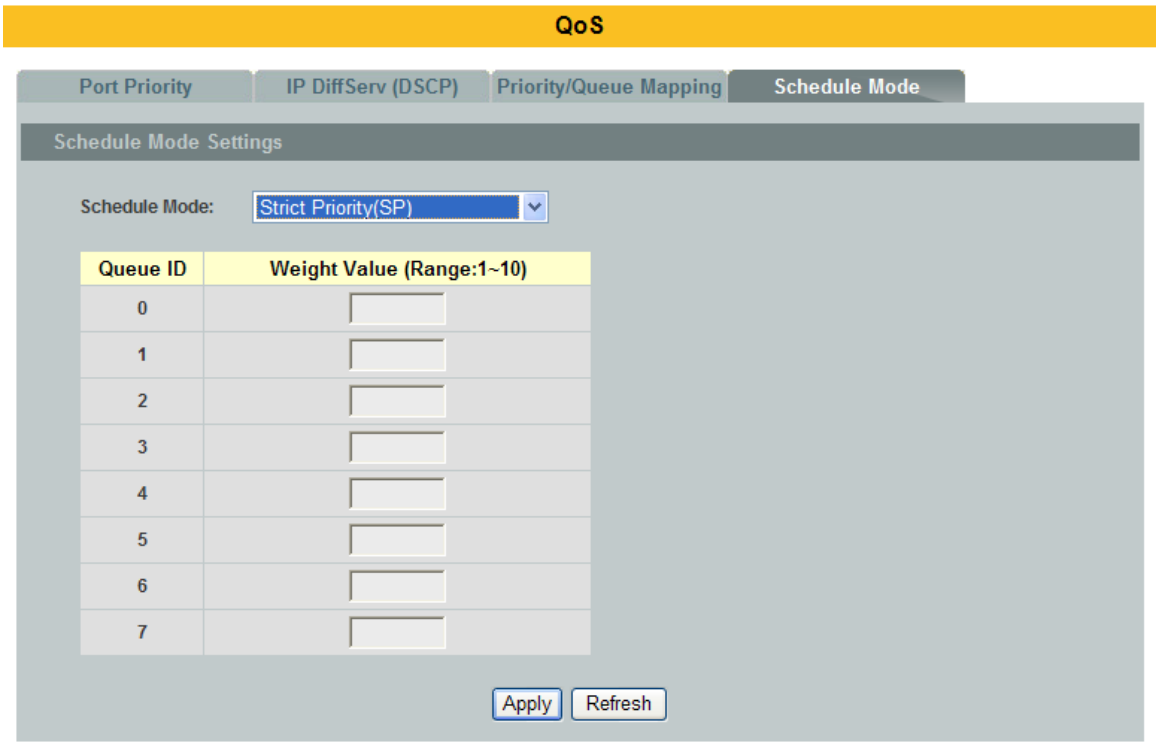
Port	This field displays the number of a port.
802.1p Priority	Select a priority for packets received by the port. Only packets without 802.1p priority tagged will be applied the priority you set here.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

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

5.1.2. Rate Limitation

5.1.2.1. Storm Control

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

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

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

Storm Control unit ：125 pps.

5.1.2.1.1. CLI Configuration

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

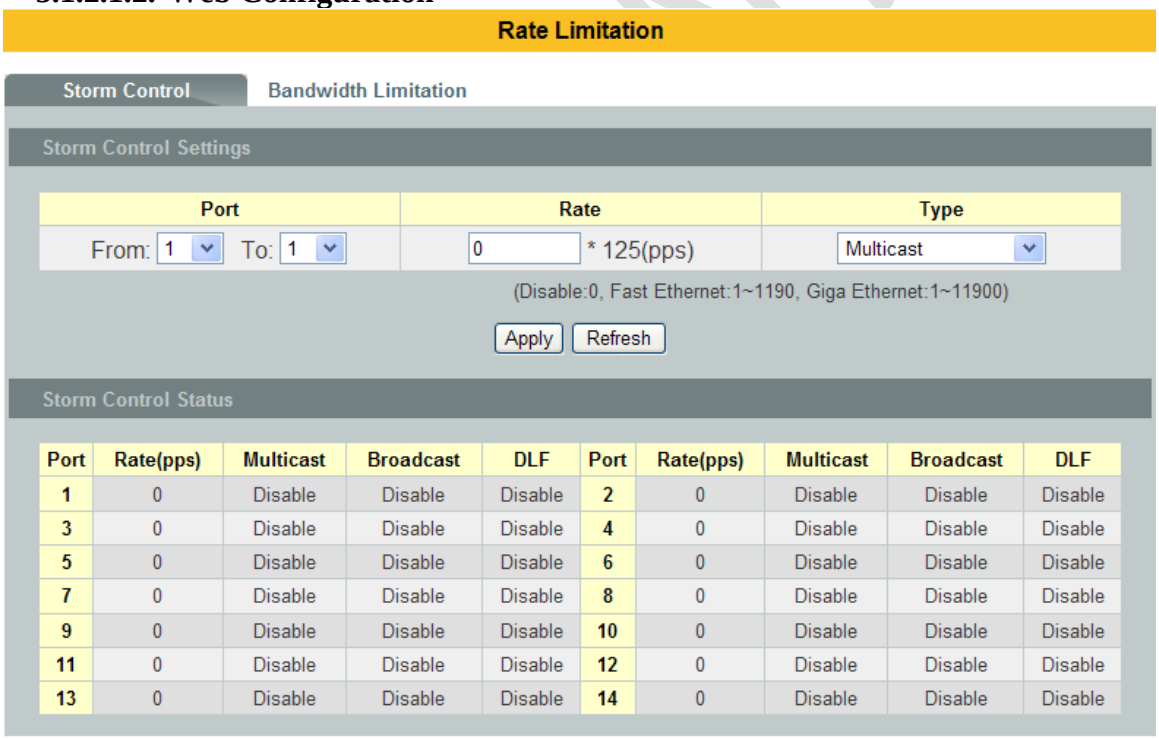
Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#storm-control rate 1 type broadcast ports 1-14
L2SWITCH(config)#storm-control rate 1 type multicast ports 1-14
```

L2SWITCH(config)#storm-control rate 1 type DLF ports 1-14
L2SWITCH#show storm-control

Port	Rate(pps)	Multicast	Broadcast	DLF
1	220	Disabled	Enabled	Enabled
2	220	Disabled	Enabled	Enabled
3	220	Disabled	Enabled	Enabled
4	220	Disabled	Enabled	Enabled
5	220	Disabled	Enabled	Enabled
6	220	Disabled	Enabled	Enabled
7	220	Disabled	Enabled	Enabled
8	220	Disabled	Enabled	Enabled
9	220	Disabled	Enabled	Enabled
10	220	Disabled	Enabled	Enabled
11	220	Disabled	Enabled	Enabled
12	220	Disabled	Enabled	Enabled
13	220	Disabled	Enabled	Enabled
14	220	Disabled	Enabled	Enabled

5.1.2.1.2. Web Configuration



Parameter	Description
Port	Select the port number for which you want to configure storm control settings.
Rate	Select the number of packets (of the type specified in the **Type** field) per second the Switch can receive per second.
Type	Select **Broadcast** - to specify a limit for the amount of broadcast

	packets received per second. **Multicast** - to specify a limit for the amount of multicast packets received per second. **DLF** - to specify a limit for the amount of DLF packets received per second.
Apply	Click Apply to take effect the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

5.1.2.2. Rate Limitation

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

Rate Limitation unit: 32 Kbits.

5.1.2.2.1. CLI Configuration

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

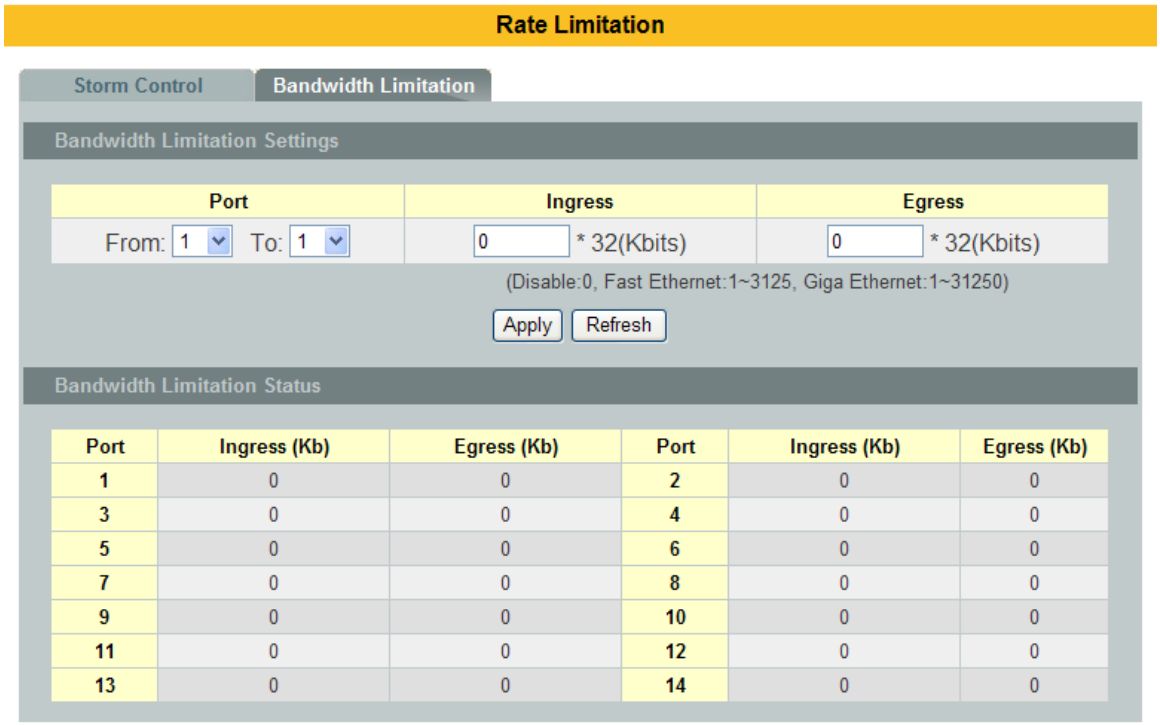
Example:

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

Port ID	Ingress rate(Kb)	Egress rate(Kb)	Port ID	Ingress rate(Kb)	Egress rate(Kb)
1	16	16	2	16	16
3	16	16	4	16	16
5	16	16	6	16	16
7	16	16	8	16	16

9	16	16	10	16	16
11	16	16	12	16	16
13	16	16	14	16	16

5.1.2.2.2. 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.

5.2. VLAN

5.2.1. Port Isolation

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

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

port, the host connected to the specific port cannot manage the Switch.

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

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

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

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

L2SWITCH#show port-isolation
          Egress Port                              Egress Port
                   1         2                              1         2
Port  01234567890123456789012345 6        Port  01234567890123456789012345 6
----  -------------------------          ----  -------------------------
 1    ---V---------------------          2     VVVVVVVVVVVVVVVVVVVVVVVVV
 3    -V----------------------           4     VVVVVVVVVVVVVVVVVVVVVVVVV
 5    VVVVVVVVVVVVVVVVVVVVVVVVV          6     VVVVVVVVVVVVVVVVVVVVVVVVV
 7    VVVVVVVVVVVVVVVVVVVVVVVVV          8     VVVVVVVVVVVVVVVVVVVVVVVVV
 9    VVVVVVVVVVVVVVVVVVVVVVVVV          10    VVVVVVVVVVVVVVVVVVVVVVVVV
 11   VVVVVVVVVVVVVVVVVVVVVVVVV          12    VVVVVVVVVVVVVVVVVVVVVVVVV
 13   VVVVVVVVVVVVVVVVVVVVVVVVV          14    VVVVVVVVVVVVVVVVVVVVVVVVV
```

5.2.1.1. CLI Configuration

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

Example:

L2SWITCH(config)#interface 1/0/2
L2SWITCH(config-if)#port-isolation ports 3-10
L2SWITCH#show port-isolation
(Port-0=CPU).

```
                Egress Port                                  Egress Port
                      1         2                                  1         2
Port  01234567890123456789012345 6    Port  01234567890123456789012345 6
----  -------------------------      ----  -------------------------
 1    VVVVVVVVVVVVVVVVVVVVV            2    ---VVVVV-----------------
 3    VVVVVVVVVVVVVVVVVVVVV            4    VVVVVVVVVVVVVVVVVVVVV
 5    VVVVVVVVVVVVVVVVVVVVV            6    VVVVVVVVVVVVVVVVVVVVV
 7    VVVVVVVVVVVVVVVVVVVVV            8    VVVVVVVVVVVVVVVVVVVVV
 9    VVVVVVVVVVVVVVVVVVVVV           10    VVVVVVVVVVVVVVVVVVVVV
11    VVVVVVVVVVVVVVVVVVVVV           12    VVVVVVVVVVVVVVVVVVVVV
13    VVVVVVVVVVVVVVVVVVVVV           14    VVVVVVVVVVVVVVVVVVVVV
```

5.2.1.2. Web Configuration

Port Isolation

Port Isolation Settings

Port From: 1 To: 1

Egress Port:

Select All Deselect All

1 3 5 7 9 11 0 (CPU)

2 4 6 8 10 12 13 14

Apply Refresh

Port Isolation Status

	Egress Port														
Port	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
2	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
3	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
4	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
5	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
6	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
7	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
8	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
9	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
10	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
11	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
12	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
13	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v
14	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v

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

5.2.2. VLAN

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

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

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand. 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.

5.2.2.1. CLI Configuration

Node	Command	Description
enable	show vlan VLANID	This command displays the VLAN configurations.
configure	vlan <1~4094>	This command enables a VLAN and enters the VLAN node.
configure	no vlan <1~4094>	This command deletes a VLAN.
vlan	show	This command displays the current VLAN configurations.
vlan	fixed PORT_LIST	This command assigns ports for permanent member of the VLAN group.
vlan	forbidden PORT_LIST	This command assigns ports to prohibit the port to join in the VLAN group. The ports should be one/some of the permanent members of the vlan group.
vlan	untagged PORT_LIST	This command assigns ports for untagged member of the VLAN group. The ports should be one/some of the permanent members of the vlan group.
vlan	name STRING	This command assigns a name for the specific VLAN. The VLAN name should be the combination of the digit or the alphabet or hyphens (-) or underscores (_).
vlan	no fixed	This command removes all fixed member from the vlan.
vlan	no forbidden	This command removes all forbidden member from the vlan.
vlan	no untagged	This command removes all untagged member from the vlan.
vlan	no name	This command configures the vlan name to default. Note: The default vlan name is “VLAN”+vlan_ID, VLAN1, VLAN2,…
vlan	acceptable frame type (all|tagged|untagged)	This command configures the acceptable frame type. all – acceptable all frame types.

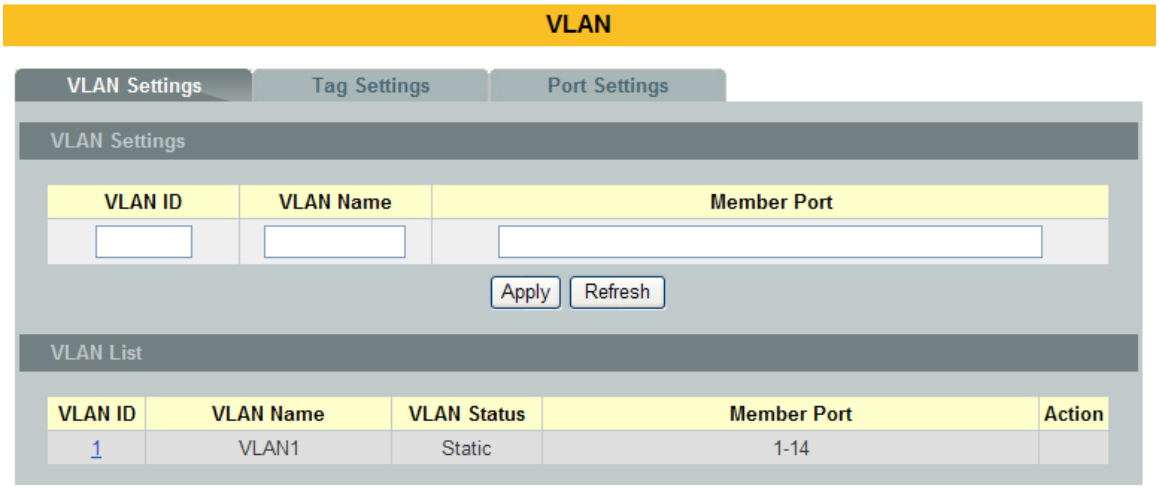
Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#vlan 2
L2SWITCH(config-vlan)#fixed 1-12
L2SWITCH(config-vlan)#untagged 1-6
L2SWITCH(config-vlan)#show
      Vlan: 2
        Name: VLAN2
        Member port(s): 1-12
        Tagged port(s): 7-12
```

Dynamic port(s): None
Untagged port(s): 1-6
Forbidden port(s): None

5.2.2.2. Web Configuration

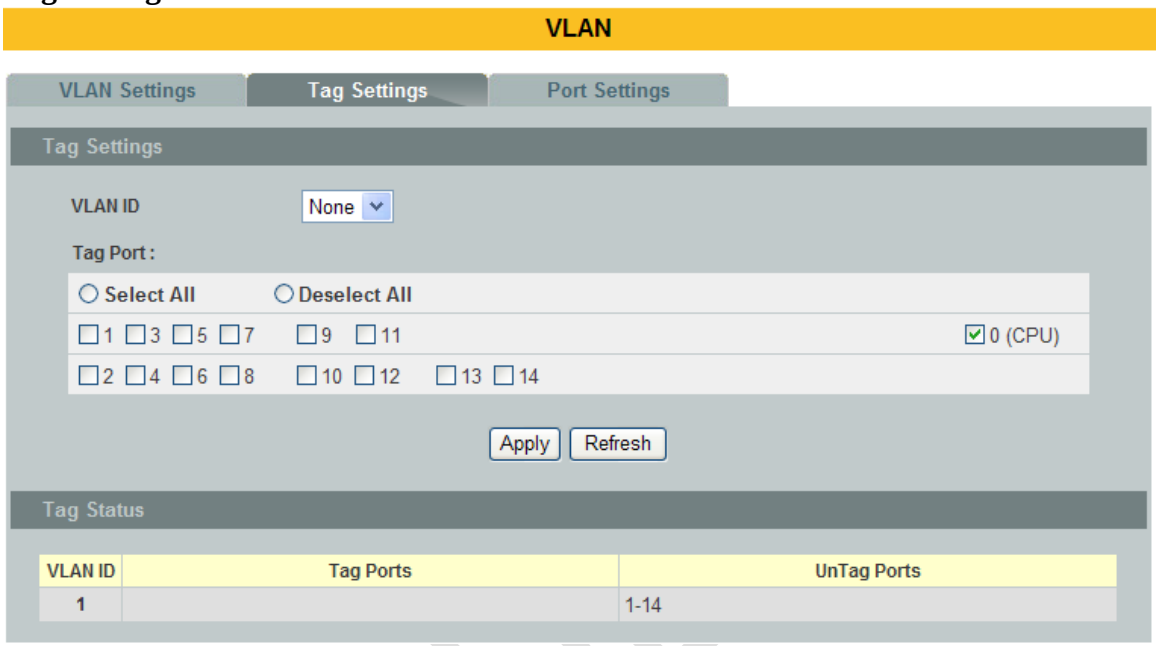
VLAN Settings



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 (_).
Member Port	Enter the port numbers you want the Switch to assign to the VLAN as members. You can designate multiple port numbers individually by using a comma (,) and by range with a hyphen (-).
Apply	Click Apply to save your changes back to the Switch.
Refresh	Click Refresh to begin configuring this screen afresh.
VLAN List	
VLAN ID	This field displays the index number of the VLAN entry. Click the number to modify the VLAN.
VLAN Name	This field displays the name of the VLAN.
VLAN Status	This field displays the status of the VLAN. **Static** or **Dynamic** (802.1Q VLAN).
Member Port	This field displays which ports have been assigned as members of the VLAN. This will display **None** if no ports have been

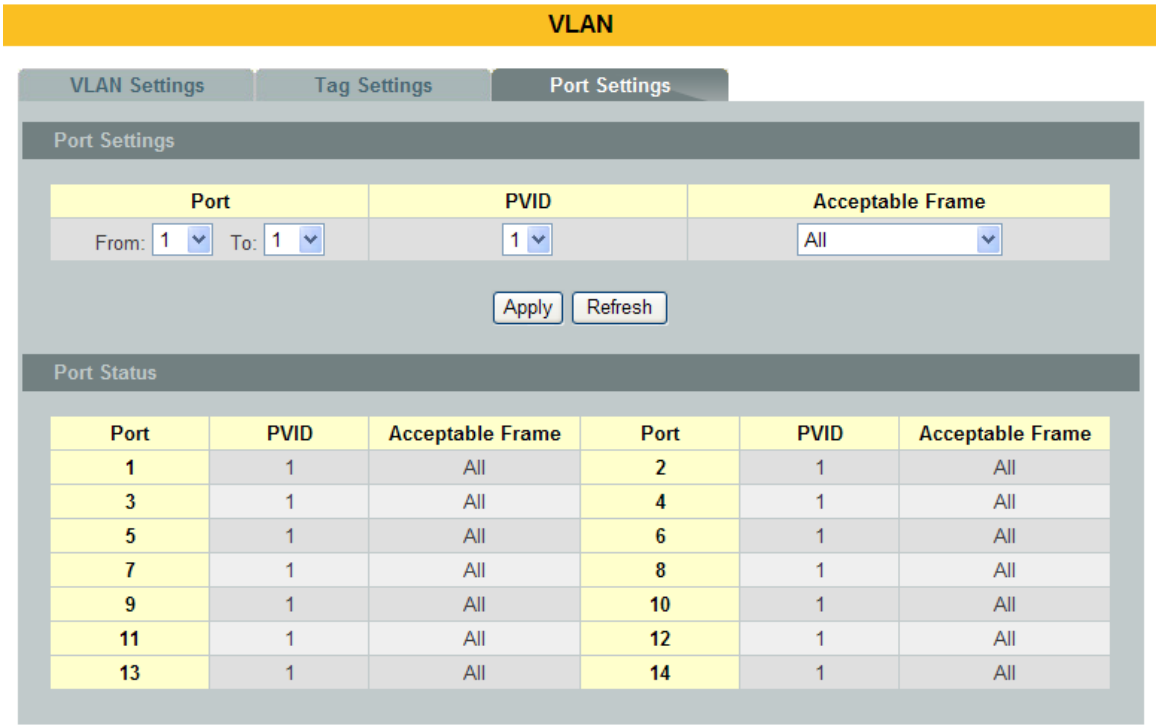
	assigned.
Action	Click **Delete** to remove the VLAN. The VLAN 1 cannot be deleted.

Tag Settings



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

Port Settings



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

5.3. IGMP Snooping

5.3.1. IGMP Snooping

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

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

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

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

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

Immediate Leave

When you enable IGMP Immediate-Leave processing, the switch immediately removes 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.

5.3.1.1. CLI Configuration

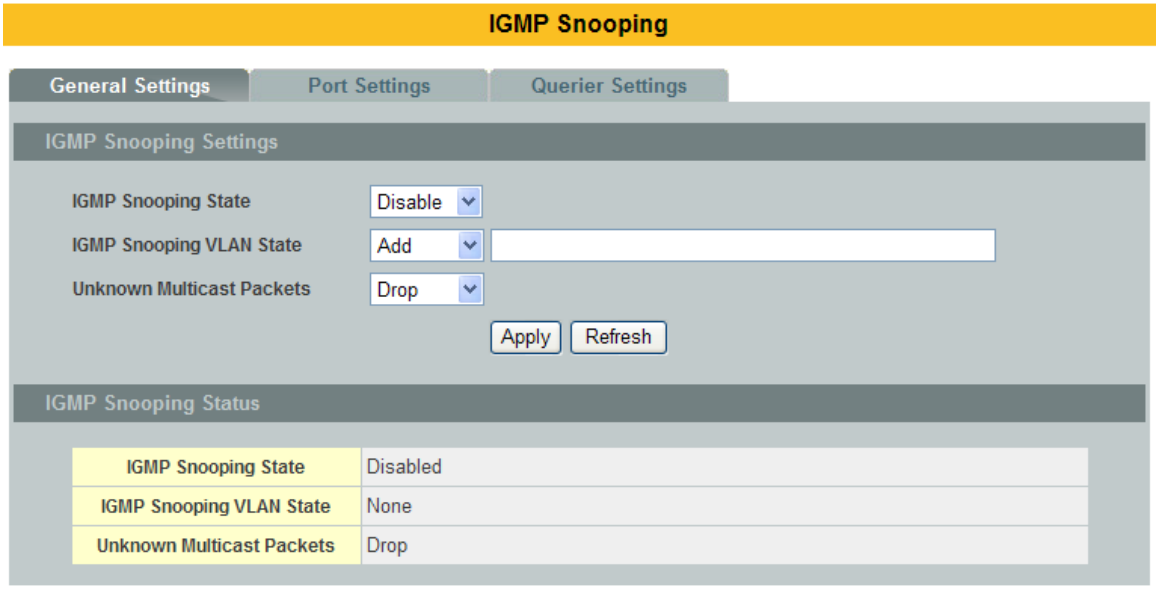
Node	Command	Description
enable	show igmp-snooping	This command displays the current IGMP snooping configurations.
configure	igmp-snooping (disable | enable)	This command disables / enables the IGMP snooping on the switch.
configure	igmp-snooping vlan VLAN_ID	This command enables the IGMP snooping function on a VLAN or range of VLANs.
configure	no igmp-snooping vlan VLAN_ID	This command disables the IGMP snooping function on a VLAN or range of VLANs.
configure	igmp-snooping querier (disable | enable)	This command disables / enables the IGMP snooping querier on the switch.
configure	igmp-snooping querier vlan VLAN_ID	This command enables the IGMP snooping querier function on a VLAN or range of VLANs.
configure	no igmp-snooping querier vlan VLAN_ID	This command disables the IGMP snooping querier function on a VLAN or range of VLANs.
configure	igmp-snooping unknown-multicast (drop|flooding)	This command configures the process for unknown multicast packets when the IGMP snooping function is enabled. *drop:* Drop all of the unknown multicast packets.
interface	igmp-querier-mode (auto|fixed|edge)	This command specifies whether or not and under what conditions the port(s) is (are) IGMP query port(s). The Switch forwards IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well. (Default:auto)
interface	igmp-immediate-leave	This command enables the IGMP Snooping immediate leave function for the specific interface.
interface	no igmp-immediate-leave	This command disables the IGMP Snooping immediate leave function for the specific interface.

Example:

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

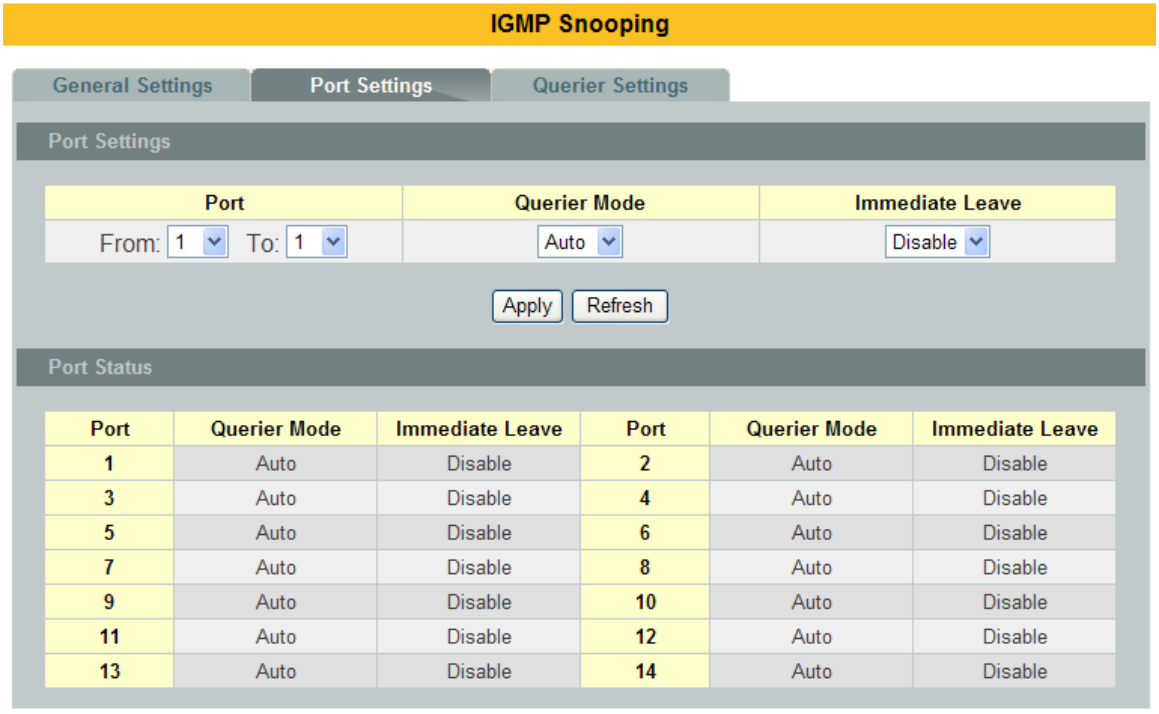
5.3.1.2. Web Configuration

General Settings



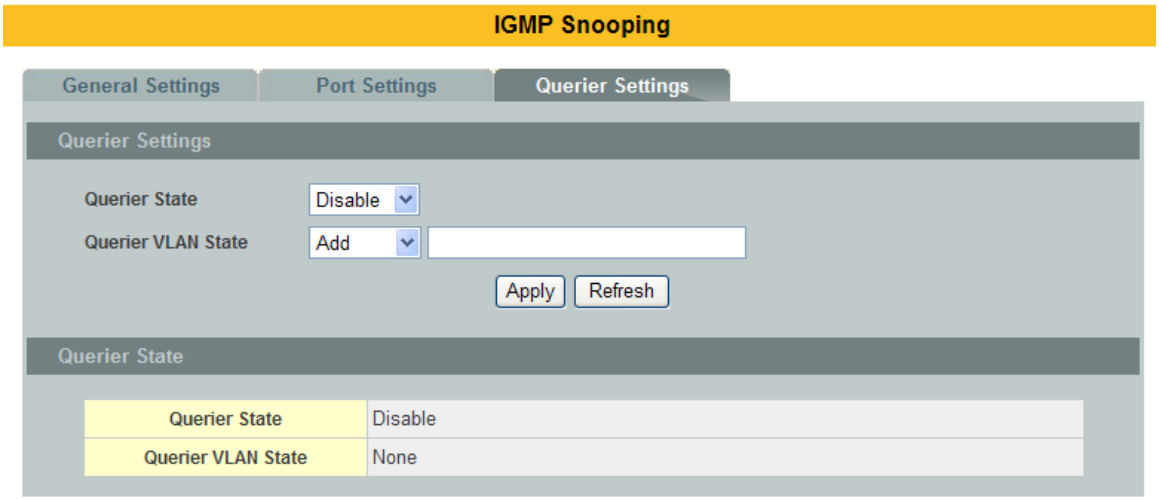
Parameter	Description
IGMP Snooping State	Select **Enable** to activate IGMP Snooping to forward group multicast traffic only to ports that are members of that group. Select **Disable** to deactivate the feature.
IGMP Snooping VLAN State	Select **Add** and enter VLANs upon which the Switch is to perform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

Port Settings



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

Querier Settings



Parameter	Description
Querier State	Enables / disables the querier function on the switch.
Querier VLAN State	Enable / disable the querier function on the specific VLAN.

5.3.2. MVR

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

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

MVR Mode

Dynamic Mode:

If we select the dynamic mode in MVR setting, IGMP report message transmitted from the receiver port will be forwarded to a multicast router through its source port. Multicast router knows which multicast groups exist on which interface dynamically.

Compatible mode:

If we select the dynamic mode in MVR setting, IGMP report message transmitted from the receiver port will not be transmitted to a multicast router.

Multicast router must be statically configured.

Operation Mode

Join Operation:

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

Leave Operation:

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

Immediate Leave Operation:

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

Figure-1:

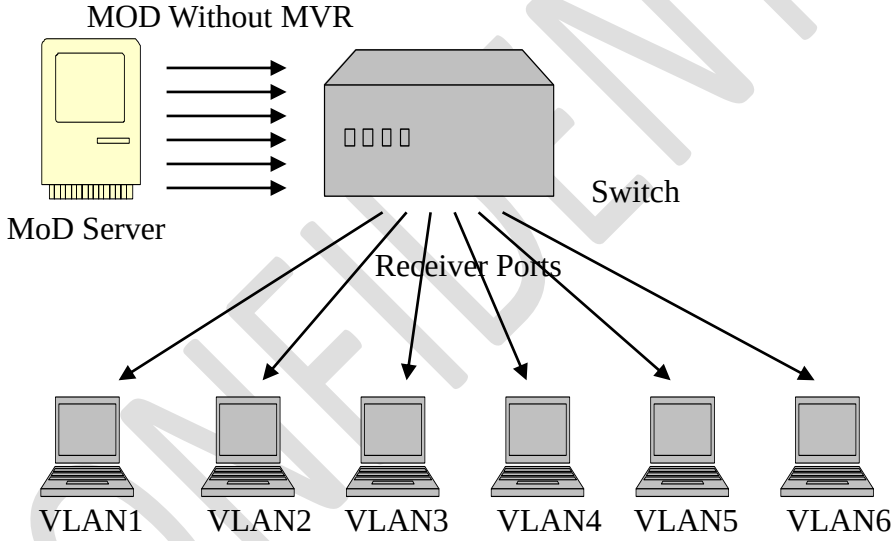
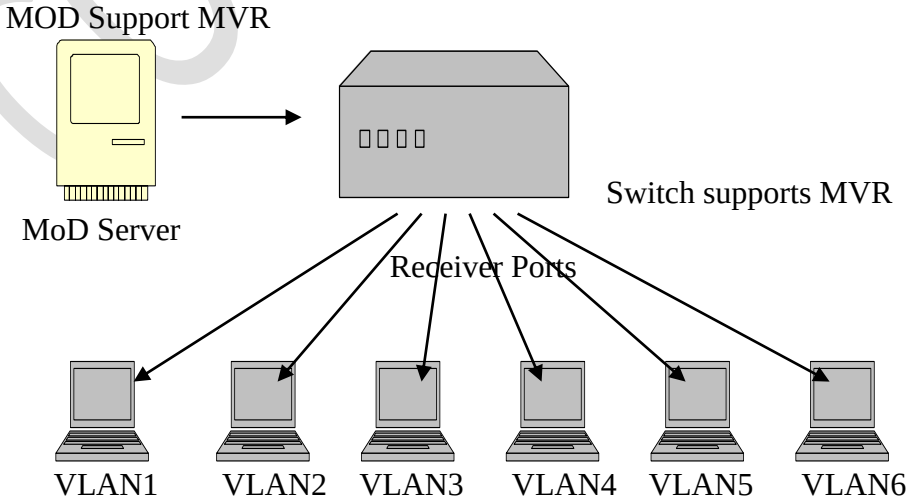


Figure-2:

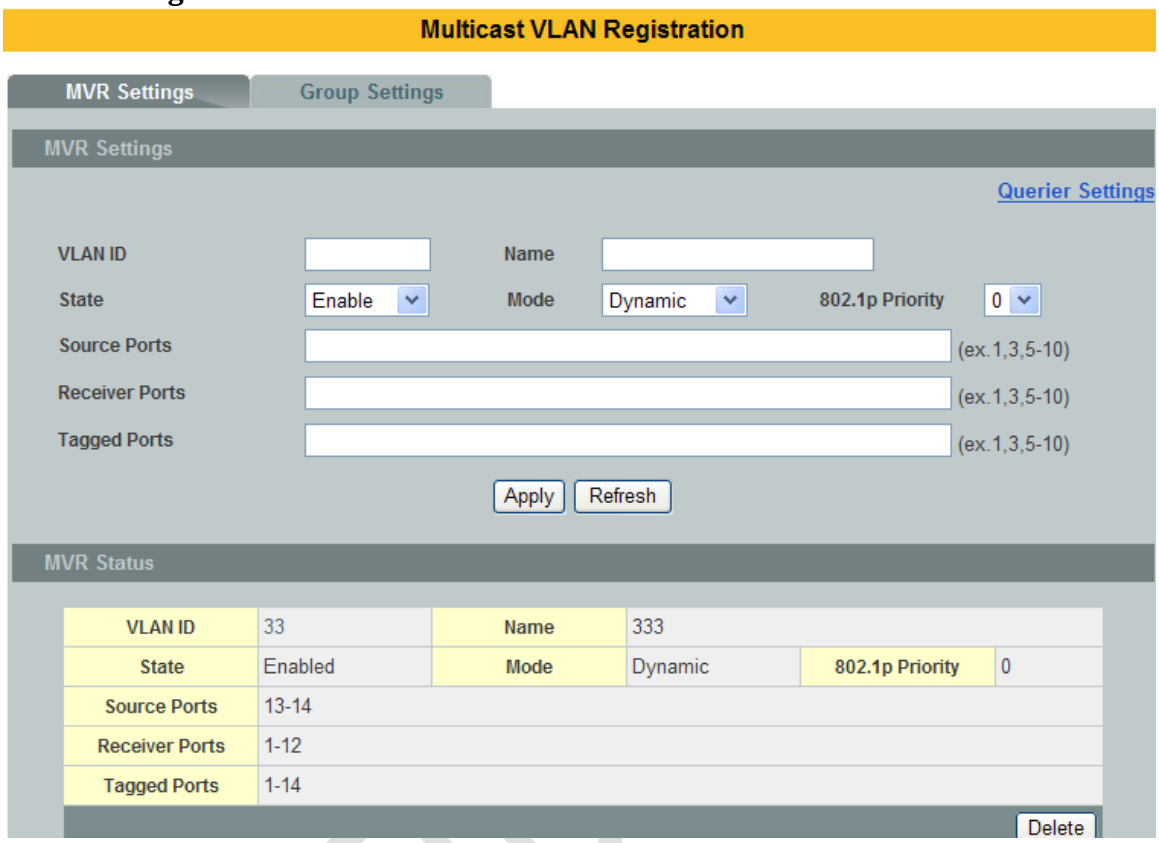


5.3.2.1. CLI Configuration

Node	Command	Description
enable	show mvr	This command displays the current MVR configurations.
enable	show mvr vlan VLAN_ID	This command displays the current MVR configurations of the specific VLAN.
enable	show igmp-snooping	This command displays the current IGMP snooping configurations.
configure	mvr VLAN_ID	This command configures the MVR configurations for the specific VLAN.
configure	no mvr VLAN_ID	This command disables the MVR configurations for the specific VLAN.
MVR	8021p-priority PRIORITY	This command sets the IEEE 802.1p priority of outgoing MVR packets. The priority range is 0~7.
MVR	group NAME	This command configures group configurations for the MVR.
MVR	no group NAME	This command removes the group configurations from the MVR.
MVR	inactive	This command disables the MVR settings.
MVR	no inactive	This command enables the MVR settings.
MVR	mode (dynamic|compatible)	This command configures the mode for the MVR. ● Dynamic: Sends IGMP report to all MVR source ports in the multicast VLAN. ● Compatible: Sets the Switch not to send IGMP report.
MVR	name STRING	This command configures the name for the MVR.
MVR	no name	This command configures the default name for the MVR.
MVR	receiver-port PORTLIST	This command sets the receiver port(s). Normally the source ports are connected to the streaming client.
MVR	no receiver-port PORTLIST	This command removes a port or range of ports from the receiver port(s).
MVR	source-port PORTLIST	This command sets the source port(s). Normally the source ports are connected to the streaming server.
MVR	no source-port PORTLIST	This command removes a port or range of ports from the source port(s).
MVR	tagged PORTLIST	This command sets the tagged port(s). Same as the VLAN tagged port.
MVR	no tagged PORTLIST	This command removes a port or range of ports from the tagged port(s).

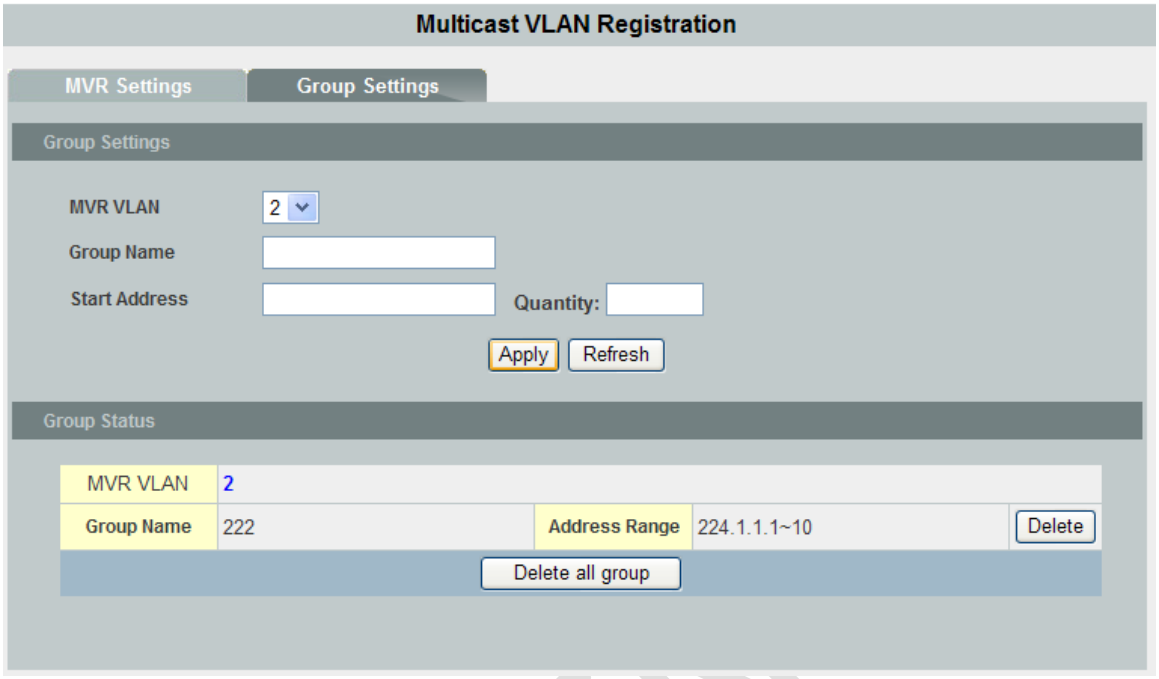
5.3.2.2. Web Configuration

MVR Settings



Parameter	Description
VLAN ID	Configures a VLAN.
NAME	Configures a name for the MVR.
Action	Enables / Disables the MVR.
Mode	Configures the mode for the MVR.
802.1p Priority	Configures the priority for the outgoing MVR 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.

MVR 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.

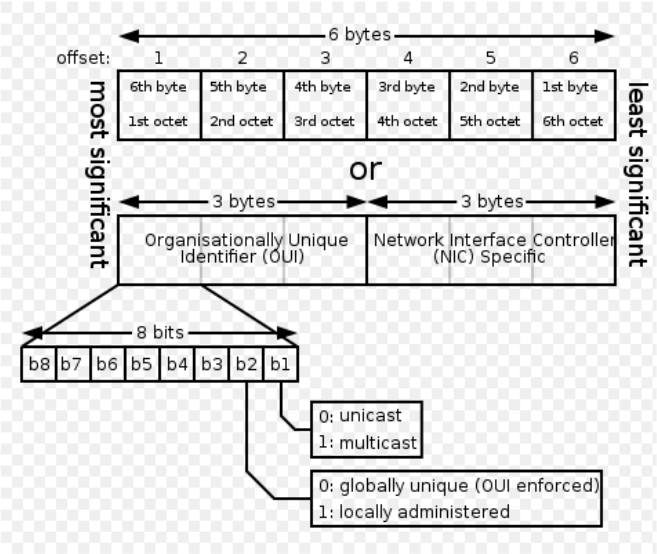
5.3.3. Multicast Address

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

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

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

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



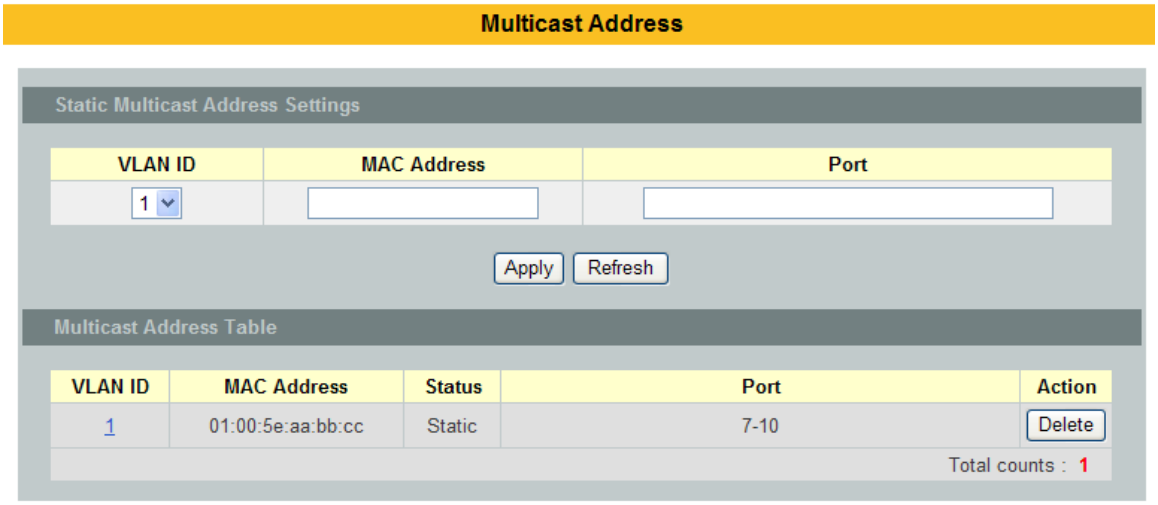
IP multicast address	Description
224.0.0.0	Base address (reserved)
224.0.0.1	The All Hosts multicast group that contains all systems on the same network segment
224.0.0.2	The All Routers multicast group that contains all routers on the same network segment
224.0.0.5	The Open Shortest Path First (OSPF) AllSPFRouters address. Used to send Hello packets to all OSPF routers on a network segment
224.0.0.6	The OSPF AllDRouters address. Used to send OSPF routing information to OSPF designated routers on a network segment
224.0.0.9	The 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

5.3.3.1. CLI Configuration

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

5.3.3.2. Web Configuration



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

5.4. DHCP Relay

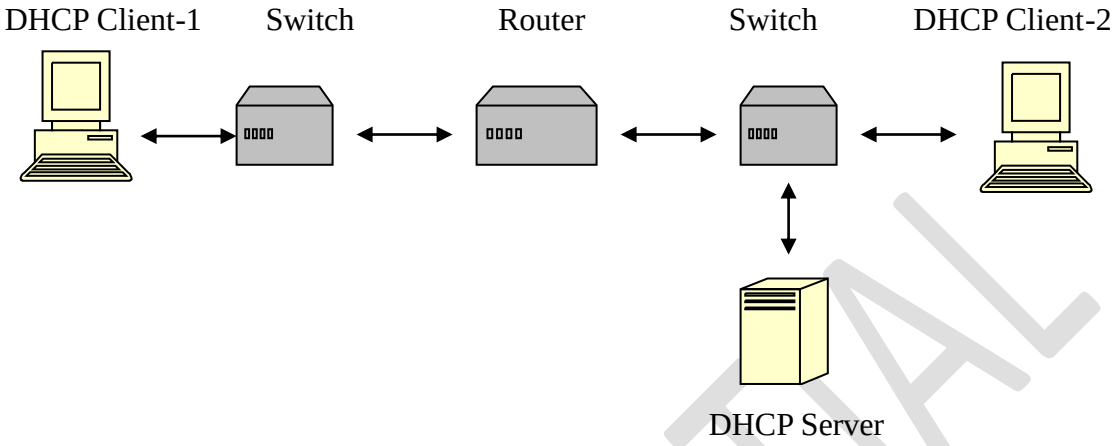
Because the *DHCPDISCOVER message is a broadcast message*, and broadcasts only cross other segments when they are explicitly routed, you might have to configure a DHCP Relay Agent on the router interface so that all DHCPDISCOVER messages can be forwarded to your DHCP server. Alternatively, you can configure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

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

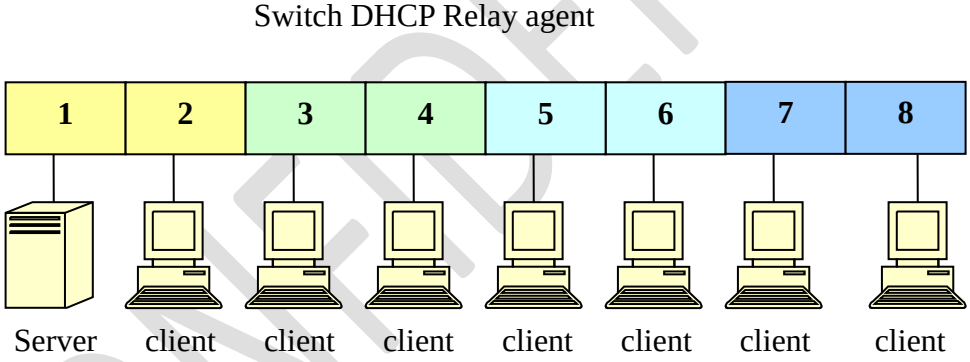
Most of the time in small networks DHCP uses broadcasts however there are some circumstances where unicast addresses will be used. When networks have a single DHCP server that provides IP addresses for multiple subnets. A router for such a subnet receives the DHCP broadcasts, converts them to unicast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

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

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.

DHCP Relay Option 82

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

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

The maximum length of the information is 32 characters.

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

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

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

Option Frame Format:

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

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

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

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

Circuit ID Suboption Frame Format:

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

Remote ID Suboption Frame Format:

Suboption Type	Length	Circuit ID Type	Length	MAC Address
2	8	0	6	6

Volktek Format:
Circuit ID Sub-option Format:

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

5.4.1. CLI Configuration

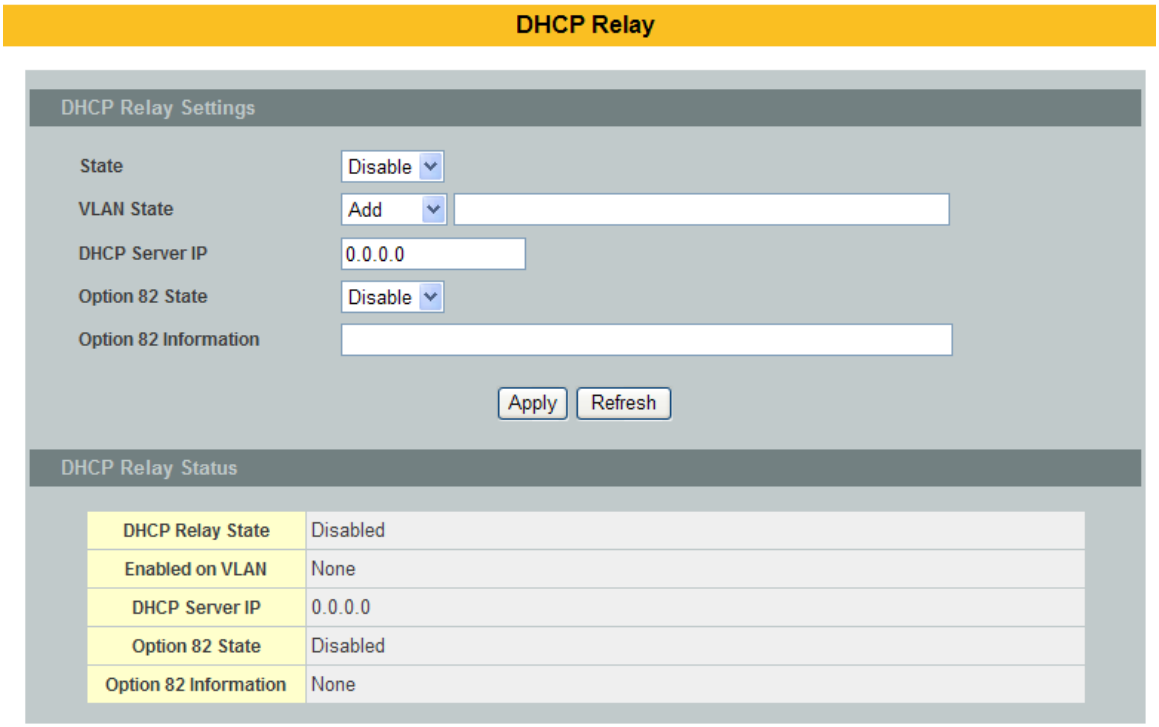
Node	Command	Description
enable	show dhcp relay	This command displays the current configurations for the DHCP relay.
configure	dhcp relay (disable | enable)	This command disables / enables the DHCP relay on the switch.
configure	dhcp relay vlan VLAN_RANGE	This command enables the DHCP relay function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

	helper-address	address.
configure	dhcp option82 (disable | enable)	This command disables / enables the DHCP relay option 82 on the switch.
configure	dhcp option82 information STRING	This command configures the information for the DHCP relay option 82.
configure	no dhcp option82 information	This command removes the information for the DHCP relay option 82.

Example:

L2SWITCH#*configure terminal*
L2SWITCH(config)# *interface eth0*
L2SWITCH(config-if)# *ip address 172.20.1.101/24*
L2SWITCH(config-if)# *ip address default-gateway 172.20.1.1*
L2SWITCH(config)#*dhcp relay enable*
L2SWITCH(config)# *dhcp relay vlan 1*
L2SWITCH(config)# *dhcp helper-address 172.20.1.1*
L2SWITCH(config)#*dhcp option82 enable*
L2SWITCH(config)#*dhcp option82 information Justin*

5.4.2. Web Configuration



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

Option 82 State	Enables / disables the DHCP Relay Option 82 for the Switch.
Option 82 Information	The information for the DHCP Relay Option 82. If the DHCP Option 82 is enabled, the Switch will append the Information into the DHCP discover and request packets.

5.5. Link Aggregation

5.5.1. Static Trunk

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

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

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

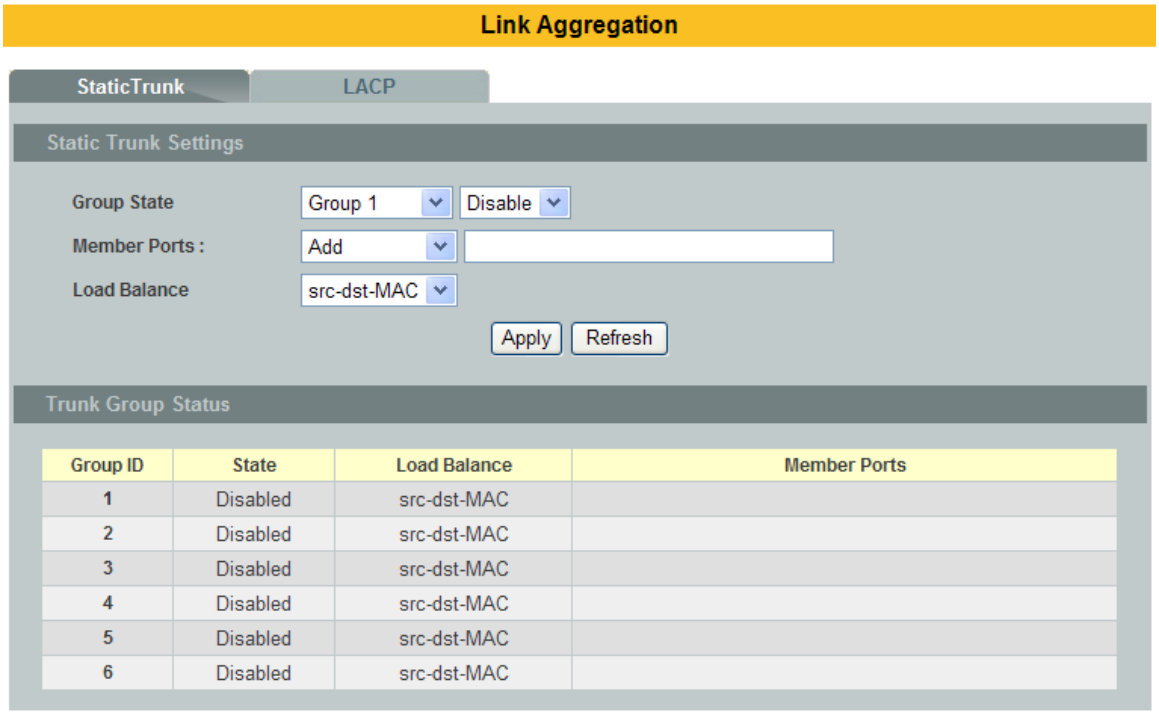
5.5.1.1. CLI Configuration

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

Example:

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

5.5.1.2. Web Configuration



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

Load Balance	This field displays the load balance policy for the trunk group.
Member Ports	This field displays the assigned ports that comprise the static trunk group.

5.5.2. LACP

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

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups.

LACP also allows port redundancy, that is, if an operational port fails, then one of the "standby" ports become operational without user intervention.

Please note that:

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

System Priority:

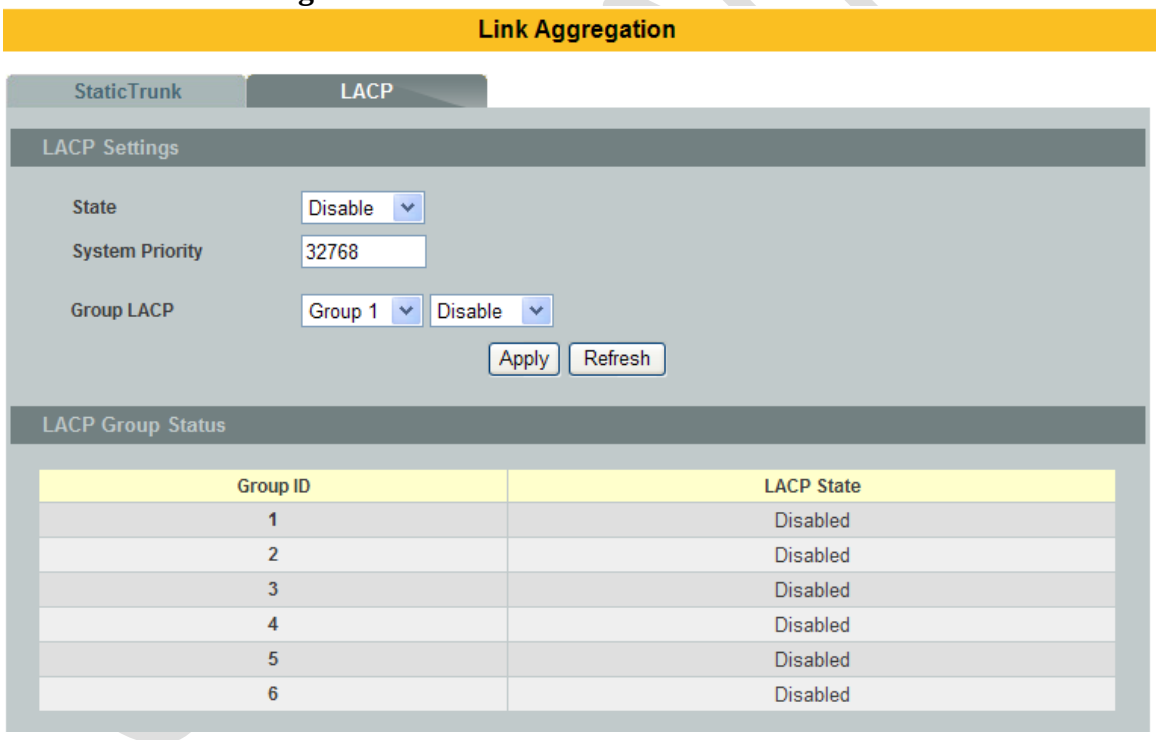
The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number,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

5.5.2.1. CLI Configuration

Node	Command	Description
enable	show trunk	This command displays the current trunk configurations.
enable	show lacp counters [GROUP_ID]	This command displays the LACP counters for the specific group or all groups.
enable	show lacp internal [GROUP_ID]	This command displays the LACP internal information for the specific group or all groups.
enable	show lacp neighbor [GROUP_ID]	This command displays the LACP neighbor's information for the specific group or all groups.
enable	show lacp port_priority	This command c displays the port priority for the LACP.
enable	show lacp sys_id	This command displays the actor's and partner's

		system ID.
configure	Lacp (disable | enable)	This command disables / enables the LACP on the switch.
configure	Lacp GROUP_ID (disable | enable)	This command disables / enables the LACP on the specific trunk group.
configure	clear lacp counters [PORT_ID]	This command clears the LACP statistics for the specific port or all ports.
configure	lacp system-priority <1-65535>	This command configures the system priority for the LACP. Note: The default value is 32768.
configure	no lacp system-priority	This command configures the default for the system priority for the LACP.
interface	lacp port_priority <1-65535>	This command configures the priority for the specific port. Note: The default value is 32768.
interface	no lacp port_priority	This command configures the default for the priority for the specific port.

5.5.2.2. Web Configuration



Parameter	Description
State	Select **Enable** from the drop down box to enable Link Aggregation Control Protocol (LACP). Select **Disable** to not use LACP.
System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The

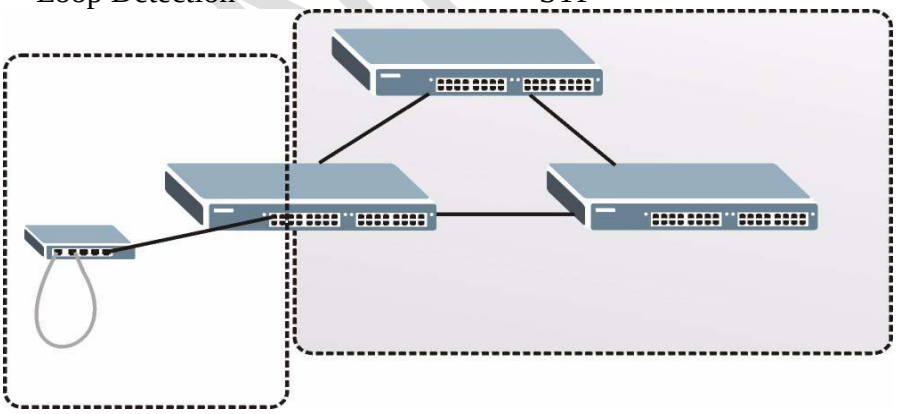
	LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Group LACP	Select a trunk group ID and then select whether to **Enable** or **Disable** Group Link Aggregation Control Protocol for that trunk group.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last saved setting.
LACP Group Status	
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
LACP State	This field displays if the group has LACP enabled.

5.6. Loop Detection

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

The difference between the Loop Detection and STP:

Loop Detection STP



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

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

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

5.6.1. CLI Configuration

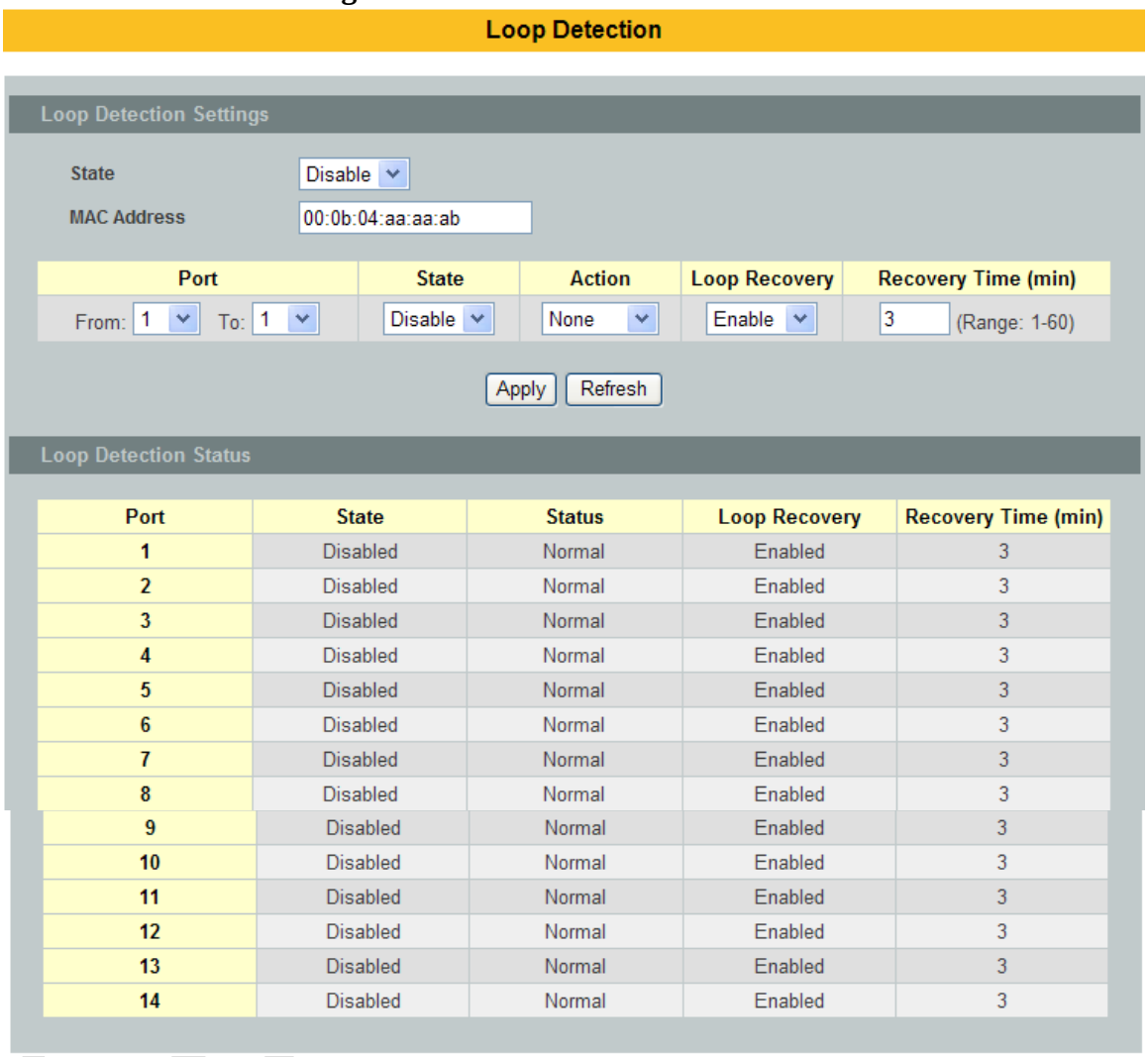
Node	Command	Description
enable	show loop-detection	This command displays the current loop detection configurations.
configure	loop-detection (disable | enable)	This command disables / enables the loop detection on the switch.
configure	loop-detection address MACADDR	This command configures the destination MAC for the loop detection special packets.
configure	no loop-detection address	This command configures the destination MAC to default (00:F0:F0:00:00:00).
interface	loop-detection (disable | enable)	This command disables / enables the loop detection on the specific port.
interface	no shutdown	This command enables the specific port. It can unblock port blocked by loop detection.
interface	loop-detection recovery (disable | enable)	This command enables / disables the recovery function on the port.
interface	loop-detection recovery time VALUE	This command configures the recovery period time.

Example:

```
L2SWITCH(config)#loop-detection enable
L2SWITCH(config)#interface 1/0/1
L2SWITCH(config-if)#loop-detection enable
L2SWITCH(config-if)#loop-detection recovery enable
L2SWITCH(config-if)#loop-detection recovery time 10
L2SWITCH#show loop-detection

The loop detection on the Switch is disabled.
Loop Detection Destination MAC=01:a0:c5:21:22:23

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

7	Disabled	Normal	Enabled	3	8	Disabled	Normal	Enabled	3
9	Disabled	Normal	Enabled	3	10	Disabled	Normal	Enabled	3
11	Disabled	Normal	Enabled	3	12	Disabled	Normal	Enabled	3
13	Disabled	Normal	Enabled	3	14	Disabled	Normal	Enabled	3

5.6.2. Web Configuration



Parameter	Description
State	Select this option to enable loop guard on the Switch.
MAC Address	Enter the destination MAC address the probe packets will be sent to. If the port receives these same packets the port will be shut down.
Port	Select a port on which to configure loop guard protection.
State	Select **Enable** to use the loop guard feature on the Switch.
Loop Recovery	Select **Enable** to reactivate the port automatically after the

	designated recovery time has passed.
Recovery Time	Specify the recovery time in minutes that the Switch will wait before reactivating the port. This can be between 1 to 60 minutes.
Apply	Click **Apply** to save your changes to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Loop Guard Status	
Port	This field displays a port number.
State	This field displays if the loop guard feature is enabled.
Status	This field displays if the port is blocked.
Loop Recovery	This field displays if the loop recovery feature is enabled.
Recovery Time (min)	This field displays the recovery time for the loop recovery feature.

5.7. STP

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

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

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

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

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

STP Terminology

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

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

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

Forward Time (Forward Delay):

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

Max Age:

This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port 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.

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

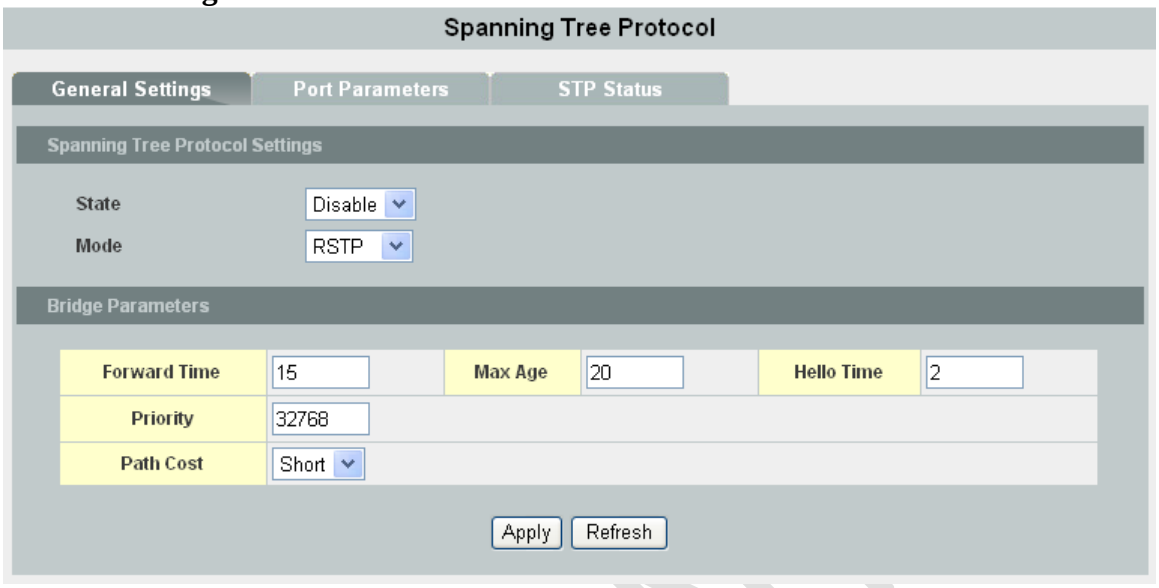
5.7.1. CLI Configuration

Node	Command	Description
enable	show spanning-tree active	This command displays the spanning tree information for only active port(s)
enable	show spanning-tree blockedports	This command displays the spanning tree information for only blocked port(s)
enable	show spanning-tree port detail PORT_ID	This command displays the spanning tree information for the interface port.
enable	show spanning-tree statistics PORT_ID	This command displays the spanning tree information for the intrerface 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 bpdufilter (disable|enable)	This command configures enables/disables the bpdufilter function.
interface	spanning-tree bpduguard (disable|enable)	This command configures enables/disables the bpduguard function.
interface	spanning-tree edge-port (disable|enable)	This command enables/disables the edge port setting.
interface	spanning-tree cost VALUE	This command configures the cost for the specific port. Cost range: 16-bit based value range 1-65535, 32-bit based value range 1-200000000.
interface	no spanning-tree cost	This command configures the path cost to default for the specific port.
interface	spanning-tree port-priority <0-240>	This command configures the port priority for the specific port. Default: 128.
interface	no spanning-tree port-priority	This command configures the port priority to default for the specific port.

5.7.2. Web Configuration

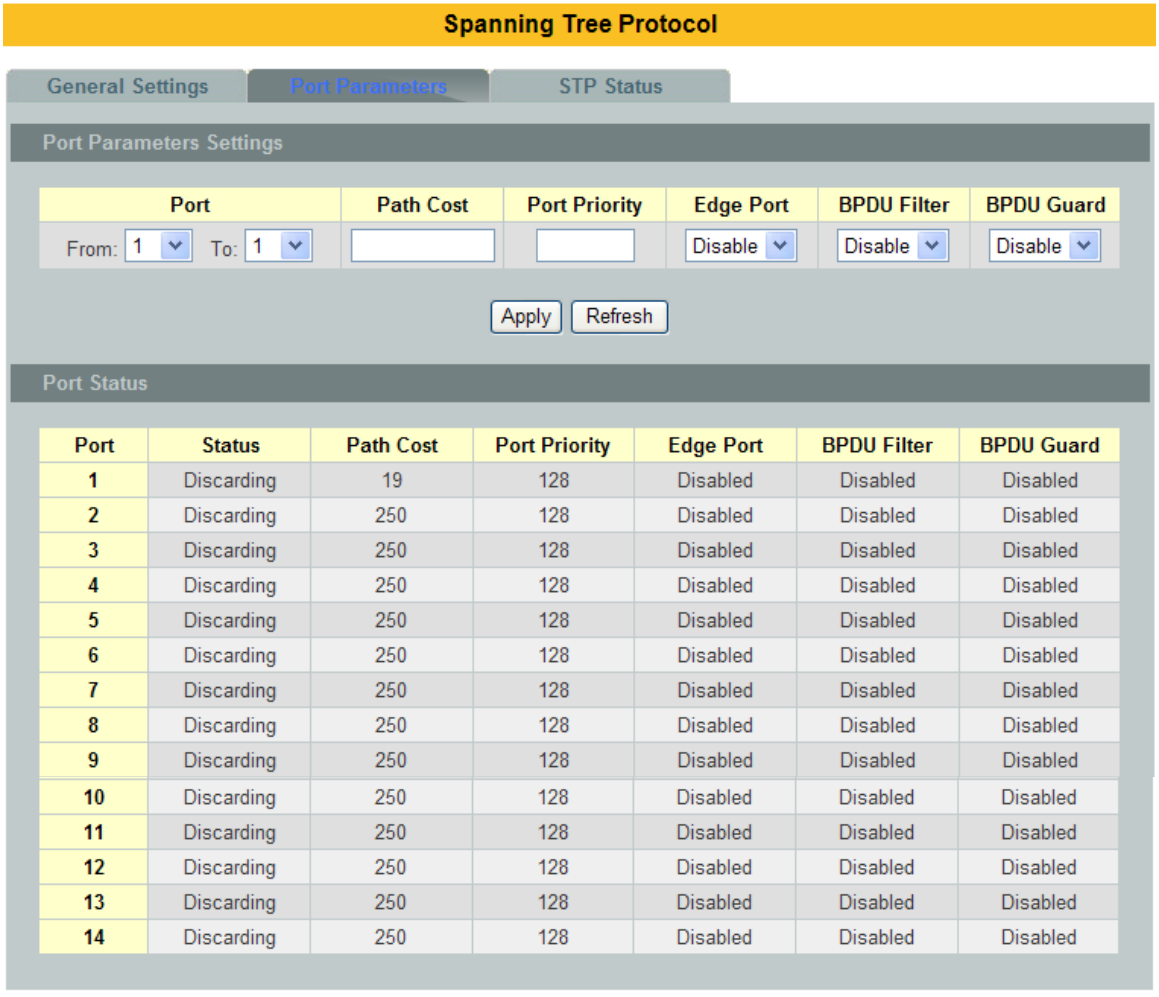
General Settings



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. 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. Enter a value from 0~61440. 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.

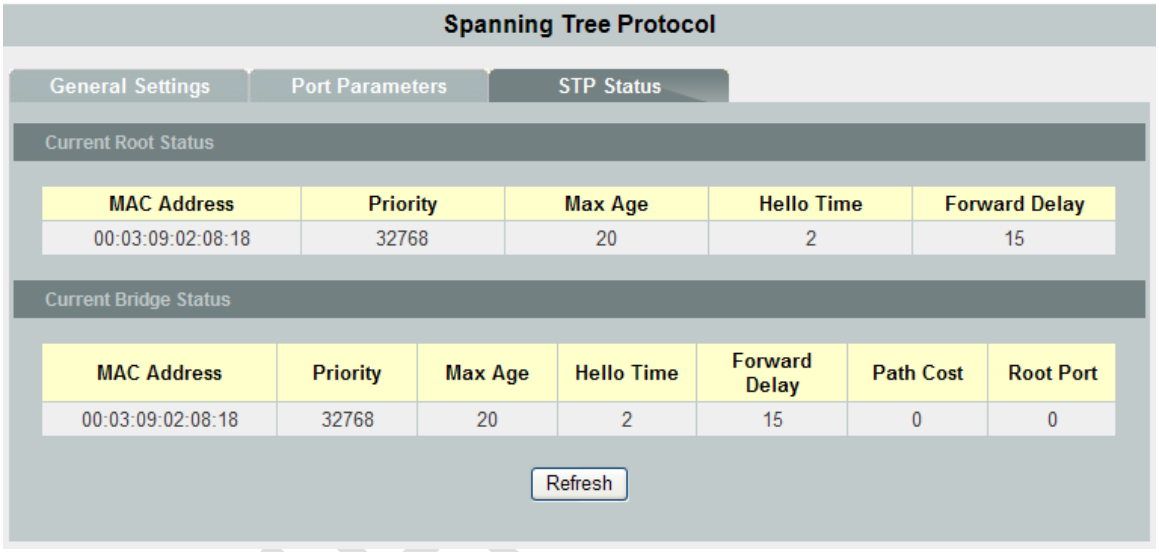
Port Parameters



Parameter	Description

Port	Selects a port that you want to configure.
Path Cost	Configures the path cost for the specific port.
Port Priority	Configures the priority for the specific port.
Edge Port	Configures the port type for the specific port. Edge or Non-Edge.
Bpdufilter	Enables / Disables the BPDU filter function for the specific port.
Bpdugard	Enables / Disables the BPDU guard function for the specific port.

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. Security

6.1. IP Source Guard

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

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

The IP Source Guard features include below functions:

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

6.1.1. DHCP Snooping

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

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

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

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

The switch drops a DHCP packet when one of these situations occurs:
A packet from a DHCP server, such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet, is received from the un-trusted port.
A packet is received on an un-trusted interface, and the source MAC address and the DHCP client hardware address do not match any of the current bindings.

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

Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted/untrusted setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.
Trusted ports are connected to DHCP servers or other switches. The Switch discards

DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The Switch learns dynamic bindings from trusted ports.

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

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

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

DHCP Snooping Database

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

Configuring DHCP Snooping

Follow these steps to configure DHCP snooping on the Switch.

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

Note:

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

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

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

The main purposes of the DHCP Snooping are:

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

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

6.1.1.1. CLI Configuration

Node	Command	Description
enable	show dhcp-snooping	This command displays the current DHCP snooping configurations.
configure	dhcp-snooping	This command disables/enables the DHCP snooping

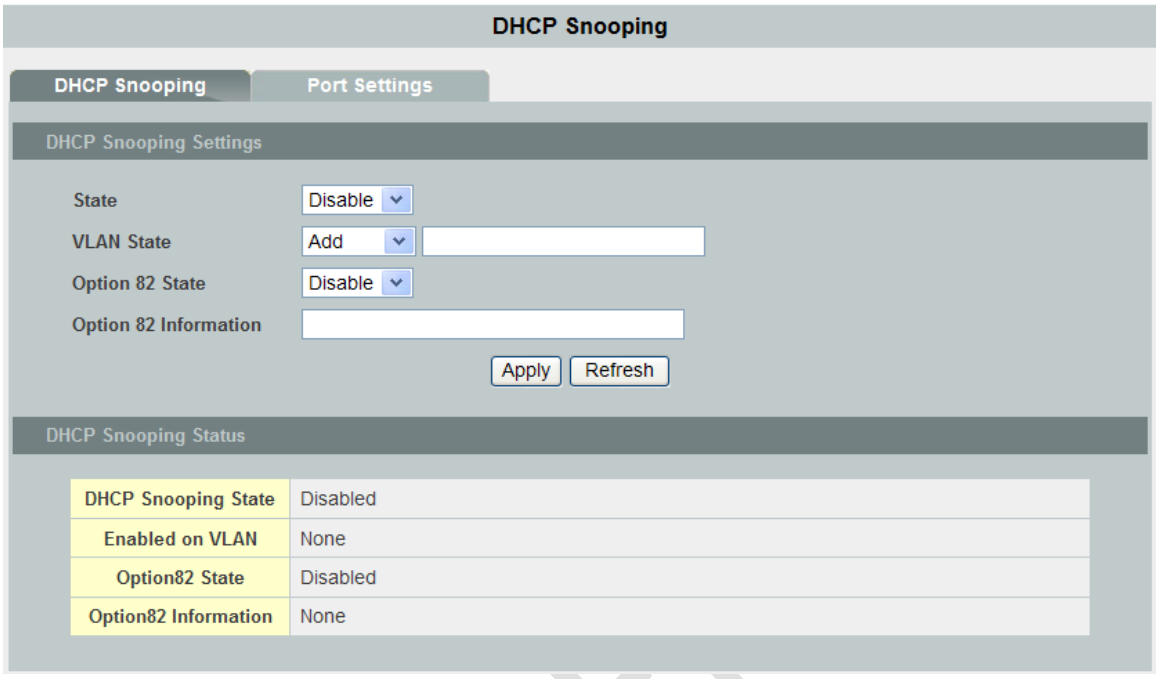
	(disable|enable)	on the switch.
configure	dhcp-snooping vlan VLAN_ID	This command enables the DHCP snooping function on a VLAN or range of VLANs.
configure	no dhcp-snooping vlan VLANID	This command disables the DHCP snooping function on a VLAN or range of VLANs.
configure	dhcp option82 (disable | enable)	This command disables / enables the DHCP relay option 82.
configure	dhcp option82 information STRING	This command configures the information for the DHCP relay option 82.
configure	no dhcp option82 information	This command removes the information for the DHCP relay option 82.
interface	dhcp-snooping host	This command configures the maximum host count for the specific port.
interface	no dhcp-snooping host	This command configures the maximum host count to default for the specific port.
interface	dhcp-snooping trust	This command configures the trust port for the specific port.
interface	no dhcp-snooping trust	This command configures the un-trust port for the specific port.

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#dhcp-snooping enable
L2SWITCH(config)#dhcp-snooping vlan 1
L2SWITCH(config)#interface 1/0/1
L2SWITCH(config-if)#dhcp-snooping trust
L2SWITCH(config)#dhcp option82 enable
L2SWITCH(config)#dhcp option82 information Justin
L2SWITCH#show dhcp-snooping
    The DHCP snooping on the Switch is enabled.
    The DHCP snooping is enabled in VLAN(s): 1
    The DHCP option 82 on the Switch is enabled.
    The information of the DHCP option 82 is Justin.

                        Maximum                          Maximum
    Port  Trusted  Host Count        Port  Trusted  Host Count
    ----  -------  ----------       ----  -------  ----------
     1       yes       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
     13      no        32            14      no        32
```

6.1.1.2. Web Configuration

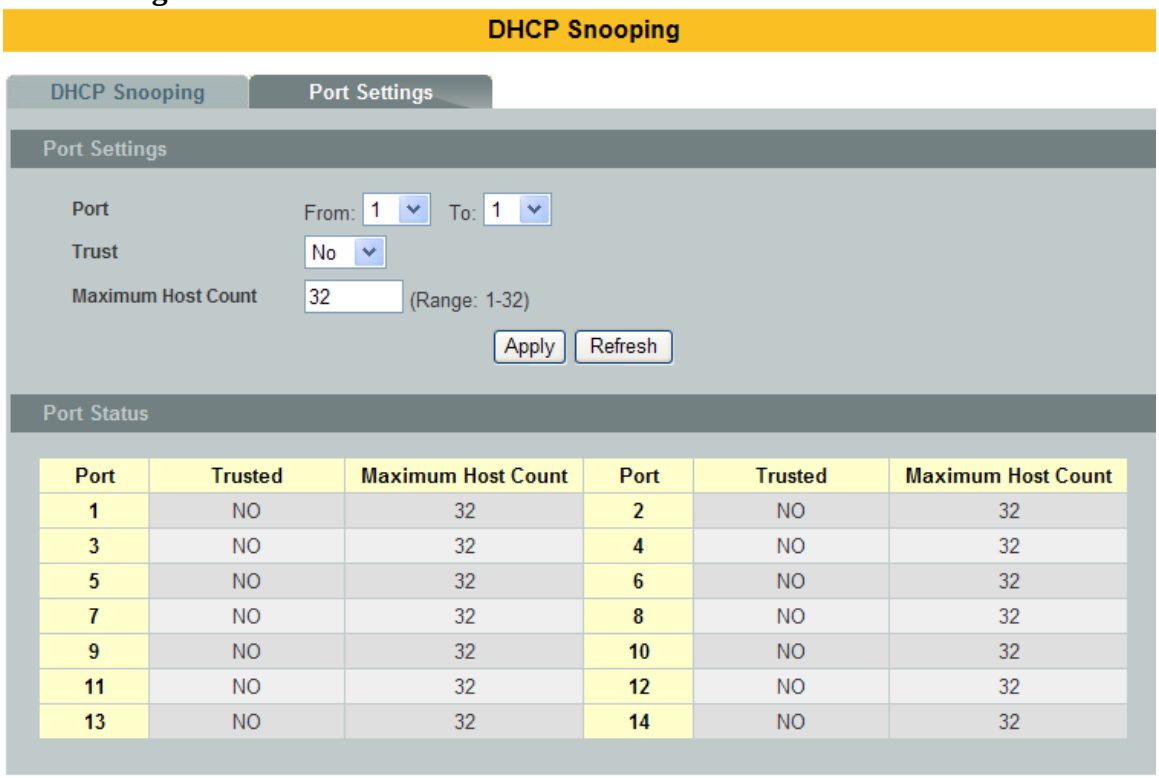
DHCP Snooping



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. Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports. Select **Disable** to not use DHCP snooping..
VLAN State	Select **Add** and enter the VLAN IDs you want the Switch to enable DHCP snooping on. You can designate multiple VLANs individually by using a comma (,) and by range with a hyphen (-). Select **Delete** and enter the VLAN IDs you no longer want the Switch to use DHCP snooping on.
Option 82 State	Enables or disables the DHCP Option 82 for the Switch.
Option 82 Information	The information for the DHCP Option 82. If the DHCP Option 82 is enabled, the Switch will append the Information into the DHCP discover and request packets. The maximum length of the information is 32 characters.
DHCP Snooping Status	
DHCP Snooping State	This field displays the current status of the DHCP snooping feature, **Enabled** or **Disabled**.

Enabled 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.

6.1.2. ARP Inspection

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

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

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

Trusted and un-trusted port

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

Configurations:

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

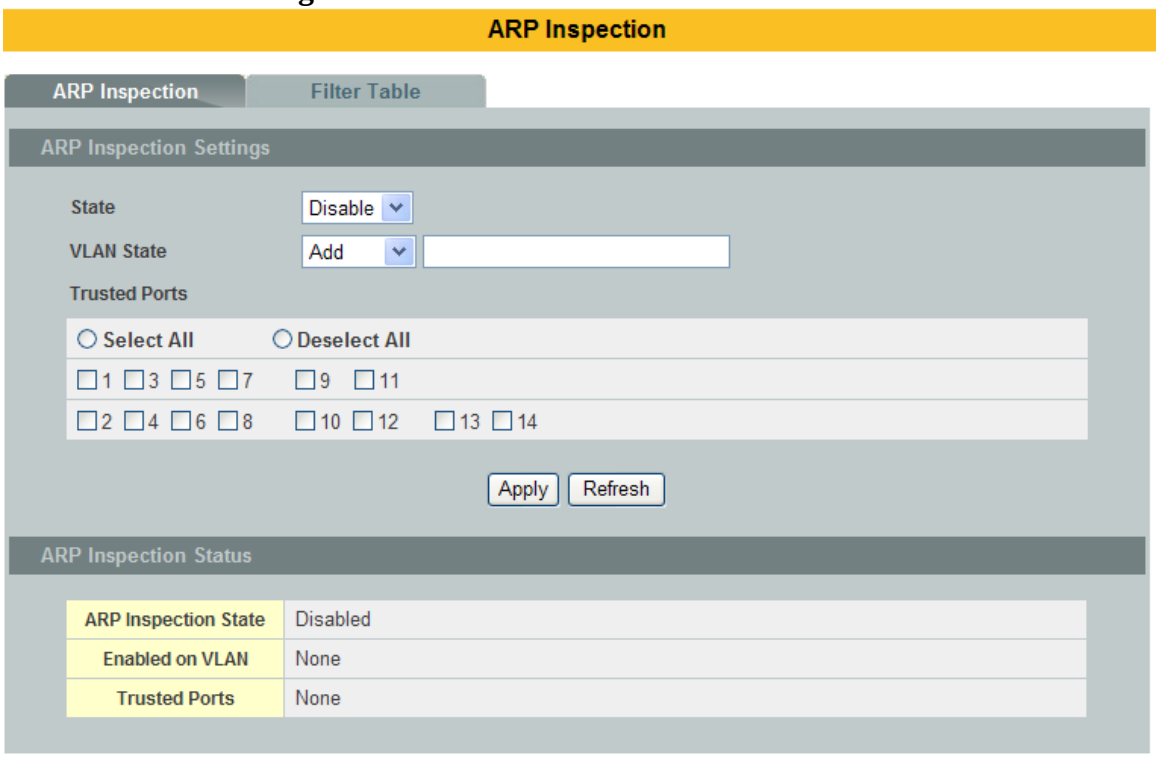
6.1.2.1. CLI Configuration

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

Example:

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

6.1.2.2. Web Configuration



Parameter	Description
State	Use this to **Enable** or **Disable** ARP inspection on the Switch.
VLAN State	Enter the VLAN IDs you want the Switch to enable ARP Inspection for. You can designate multiple VLANs individually by using a comma (,) and by range with a hyphen (-).
Trusted Ports	Select the ports which are trusted and deselect the ports which are untrusted. The Switch does not discard ARP packets on trusted ports for any reason. The Switch discards ARP packets on untrusted ports in the following situations: • The sender's information in the ARP packet does not match any of the current bindings. • The rate at which ARP packets arrive is too high. You can specify the maximum rate at which ARP packets can arrive on untrusted ports.
Select All	Click this to set all ports to trusted.
Deselect All	Click this to set all ports to untrusted.
Apply	Click **Apply** to add/modify the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.

ARP Inspection Status	
ARP Inspection State	This field displays the current status of the ARP Inspection feature, **Enabled** or **Disabled**.
Enabled on VLAN	This field displays the VLAN IDs that have ARP Inspection enabled on them. This will display **None** if no VLANs have been set.
Trusted Ports	This field displays the ports which are trusted. This will display **None** if no ports are trusted.

6.1.3. Filter Table

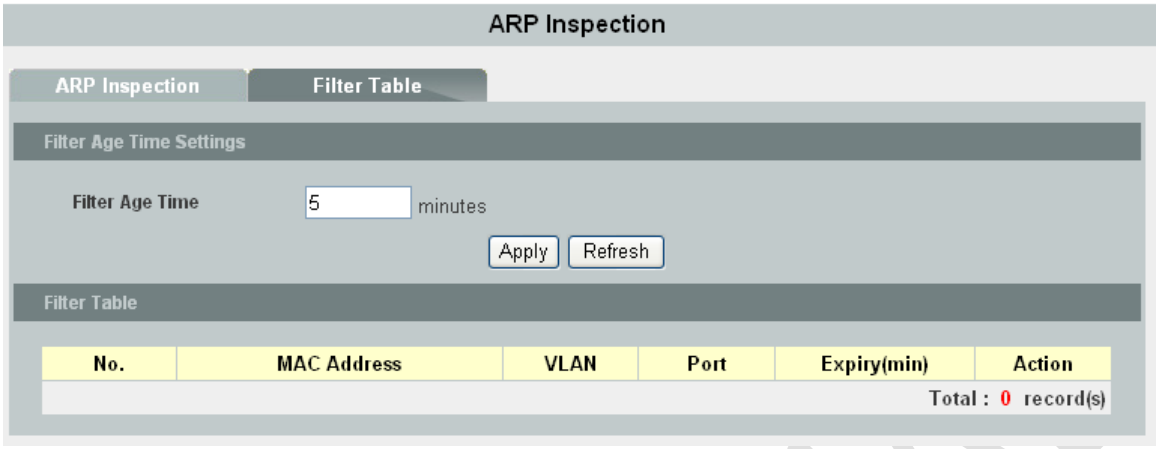
Dynamic ARP inspections validates the packet by performing IP to MAC address binding inspection stored in a trusted database (the DHCP snooping database) before forwarding the packet. When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic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

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

6.1.3.1. CLI Configuration

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

6.1.3.2. Web Configuration



Parameter	Description
Filter Age Time	This setting has no effect on existing MAC address filters. Enter how long (1-10080 minutes) the MAC address filter remains in the Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Filter Table	
No.	This field displays a sequential number for each MAC address filter.
MAC Address	This field displays the source MAC address in the MAC address filter.
VLAN	This field displays the source VLAN ID in the MAC address filter.
Port	This field displays the source port of the discarded ARP packet.
Expiry (min)	This field displays how long (in minutes) the MAC address filter remains in the Switch.
Action	Click **Delete** to remove the record manually.
Total	This field displays the current number of MAC address filters that were created because the Switch identified unauthorized ARP packets.

6.1.4. Binding Table

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

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

6.1.4.1. CLI Configuration

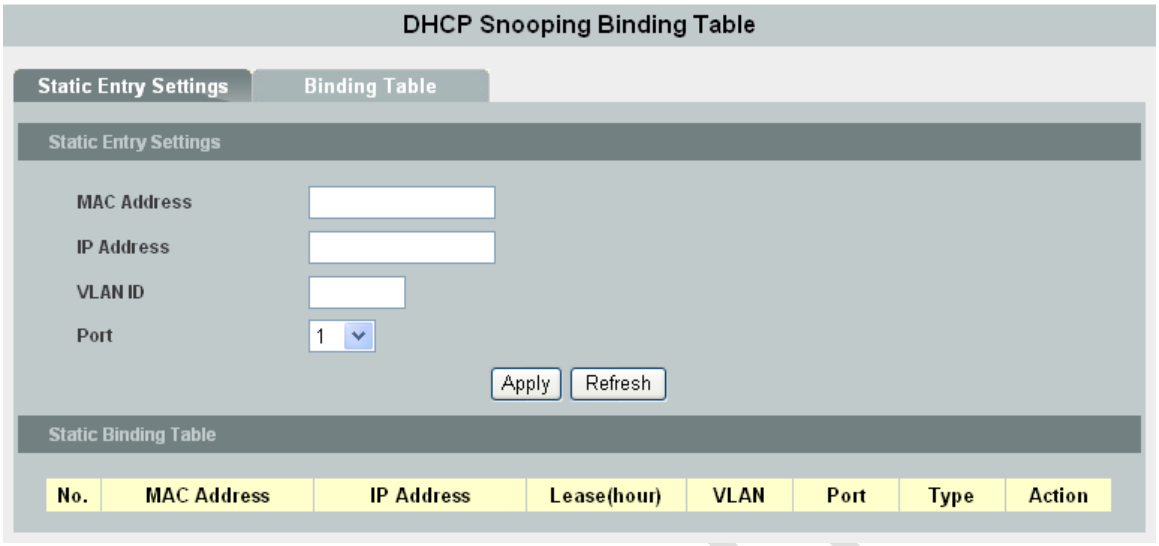
Node	Command	Description
enable	show dhcp-snooping binding	This command displays the current DHCP snooping binding table.
configure	dhcp-snooping binding mac MAC_ADDR ip IP_ADDR vlan VLAN_ID port PORT_NO	This command configures a static host into the DHCP snooping binding table.
configure	no dhcp-snooping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

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#dhcp-snooping binding mac 00:11:22:33:44:55 ip 1.1.1.1 vlan 1
port 2
L2SWITCH(config)#no dhcp-snooping binding mac 00:11:22:33:44:55
L2SWITCH#show dhcp-snooping binding
MAC Address         IP Address     Lease(hour)  VLAN  Port  Type
------------------- -------------- -----------  ----  ----  -------
00:11:22:33:44:55   1.1.1.1        0            1     2     Static
```

6.1.4.2. Web Configuration

Static Entry Settings

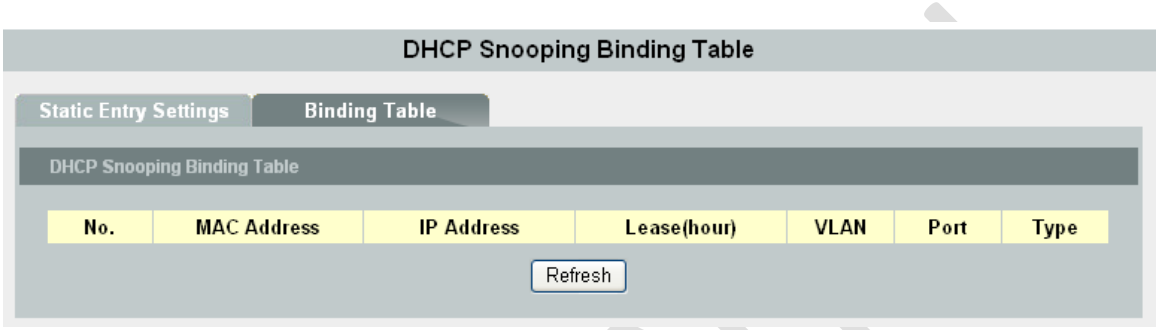


Parameter	Description
MAC Address	Enter the source MAC address in the binding.
IP Address	Enter the IP address assigned to the MAC address in the binding.
VLAN ID	Enter the source VLAN ID in the binding.
Port	Specify the port in the binding.
Static Binding Table	
No.	This field displays a sequential 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. **Static**: This binding was learned from information provided manually by an administrator. **Dynamic**: This binding was learned by snooping DHCP packets.

Action	Click **Delete** to remove the specified entry.

6.1.4.2.1. 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. **Static**: This binding was learned from information provided manually by an administrator. **Dynamic**: This binding was learned by snooping DHCP packets.

6.2. ACL

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

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

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

Actions:

Broadcom Support:
PERMITRULE,
DENYRULE,
DIRECTCPU,
DIRECTTO,
RealTek Support:
Permit, Drop, Redirect, Copy to CPU.

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.

6.2.1. CLI Configuration

Node	Command	Description
enable	show access-list	This command displays all of the access control profiles.
configure	access-list STRING	This command creates a new access control profile. Where the STRING is the profile name.

configure	no access-list STRING	This command deletes an access control profile.
acl	show	This command displays the current access control profile.
acl	activate	This command actives this profile.
acl	no activate	This command disables 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 interfaces PORTLIST	This command configures the source interfaces for the profile.
acl	no source interfaces PORTLIST	This command removes the source interfaces 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:

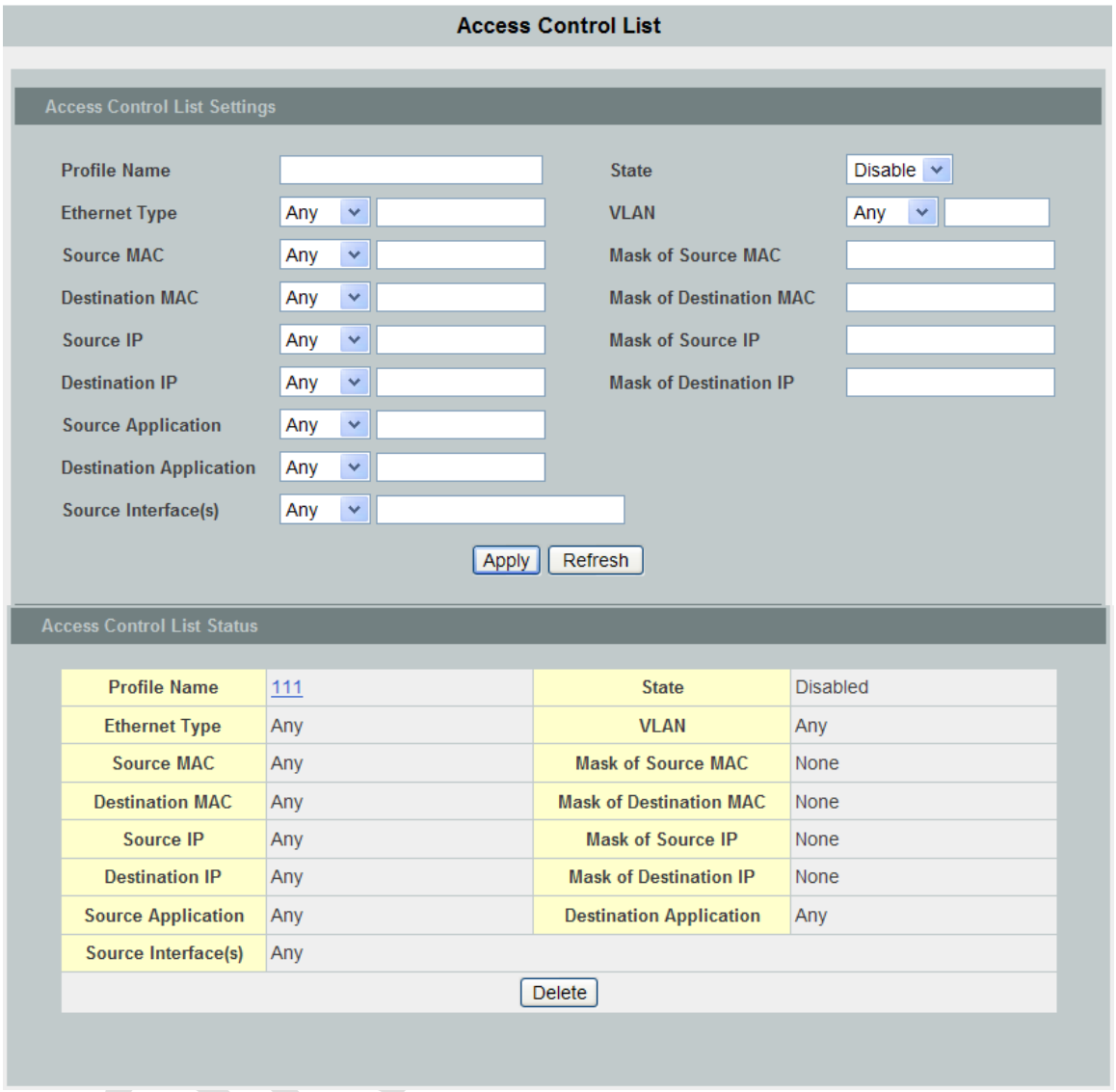
source ip 172.20.1.1 255.255.0.0

➔ 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 interfaces 1-10
L2SWITCH(config-acl)#show
Profile Name: 111
Activate: disabled
VLAN: 2
Source Interface(s): 1-10
Destination MAC Address: any
Source MAC Address: any
Ethernet Type: any
Source IP Address: any
Destination IP Address: any
Source Application: any
Destination Application: any

6.2.2. Web Configuration



Parameter	Description
Profile Name	The access control profile name.
State	Enables / Disables the access control on the Switch.
Ethernet Type	Configures the Ethernet type of the packets that you want to filter.
VLAN	Configures the VLAN of the packets that you want to filter.
Source MAC	Configures the source MAC of the packets that you want to filter.
Mask of Source MAC	Configures the bitmap mask of the source MAC of the packets that you want to filter. If the Source MAC field has been configured and this field is

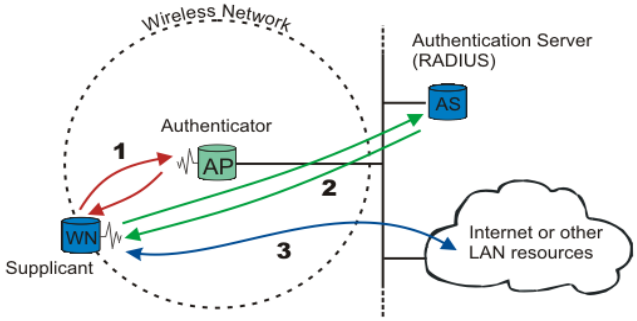
	empty, it means the profile will filter the one MAC configured in Source MAC field.
Destination MAC	Configures the destination MAC of the packets that you want to filter.
Mask of Destination MAC	Configures the bitmap mask of the destination MAC of the packets that you want to filter. If the Destination MAC field has been configured and this field is empty, it means the profile will filter the one MAC configured in Destination MAC field.
Source IP	Configures the source IP of the packets that you want to filter.
Mask of Source IP	Configures the bitmap mask of the source IP of the packets that you want to filter. If the Source IP field has been configured and this field is empty, it means the profile will filter the one IP configured in Source IP field.
Destination IP	Configures the destination IP of the packets that you want to filter.
Mask of Destination IP	Configures the bitmap mask of the destination IP of the packets that you want to filter. If the Destination IP field has been configured and this field is empty, it means the profile will filter the one IP configured in Destination IP field.
Source Application	Configures the source UDP/TCP ports of the packets that you want to filter.
Destination Application	Configures the destination UDP/TCP ports of the packets that you want to filter.
Source Interface(s)	Configures one or a rage of the source interfaces of the packets that you want to filter.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.

6.3. 802.1x

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

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

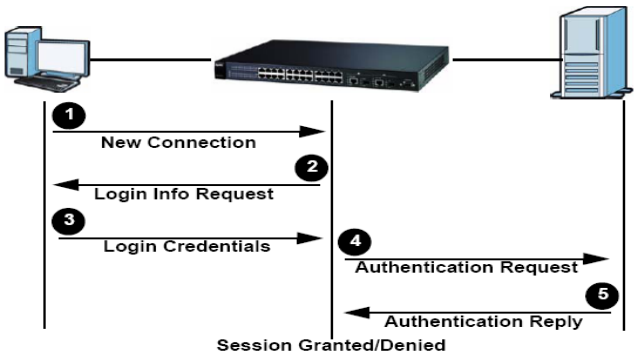
Upon detection of the new client (supplicant), the port on the switch (authenticator) is enabled and set to the "**unauthorized**" state. In this state, only 802.1X traffic is allowed; other traffic, such as DHCP and HTTP, is blocked at the network layer (Layer 3). The authenticator sends out the EAP-Request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



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

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

Figure 62 IEEE 802.1x Authentication Process



Local User Accounts

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

Guest VLAN:

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

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

Port Parameters:

Admin Control Direction:

both - drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication.

in - drop only incoming packets on the port when a user has not passed 802.1x port authentication.

Re-authentication:

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

Reauth-period:

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

Port Control Mode:

auto : Users can access network after authenticating.

force-authorized : Users can access network without authentication.

force-unauthorized : Users cannot access network.

Quiet Period:

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

Server Timeout:

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

Supp-Timeout:

The supp-timeout value is the initialization value used for timing out a Supplicant.

Max-req Time:

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

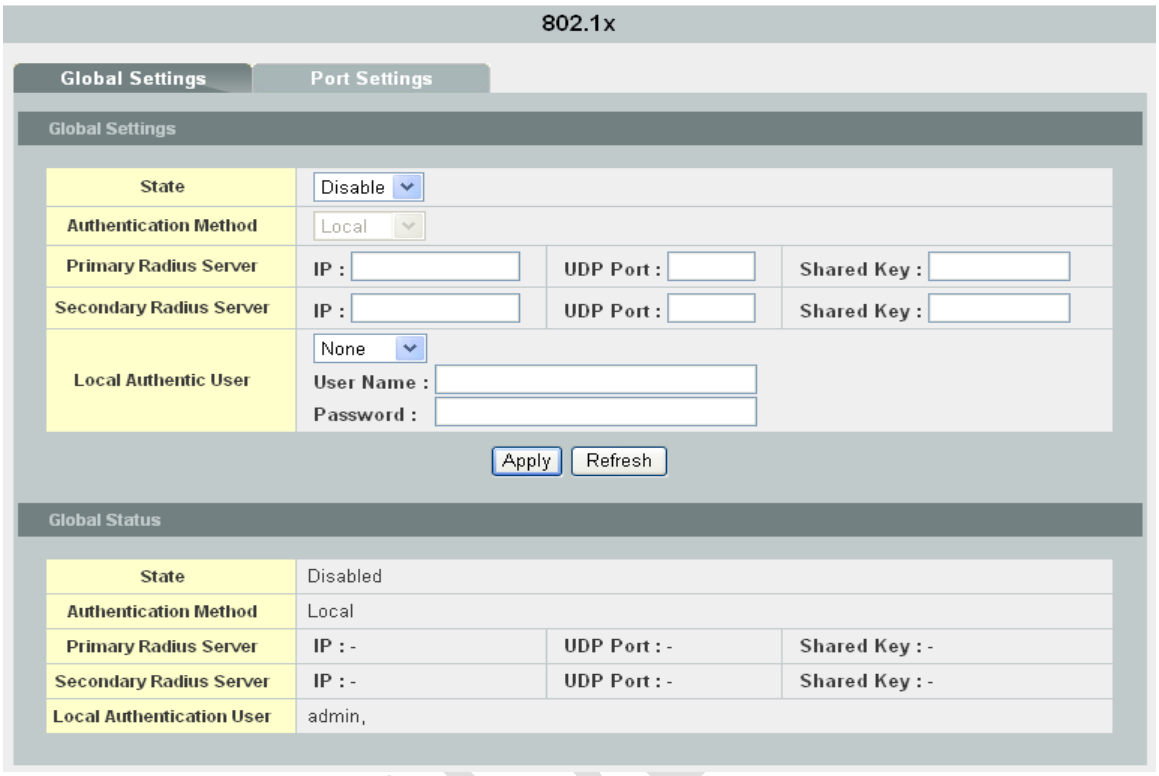
6.3.1. CLI Configuration

Node	Command	Description
enable	show dot1x	This command displays the current 802.1x configurations.
enable	show dot1x username	This command displays the current user accounts for the local authentication.
enable	show dot1x accounting-record	This command displays the local accounting records.
configure	dot1x authentication (disable|enable)	This command enables/disables the 802.1x authentication on the switch.
configure	dot1x authentic-method (local|radius)	This command configures the authentic method of 802.1x.
configure	no dot1x authentic-method	This command configures the authentic method of 802.1x to default.
configure	dot1x radius primary-server-ip <IP> port PORTID	This command configures the primary radius server.
configure	dot1x radius primary-server-ip <IP> port PORTID key KEY	This command configures the primary radius server.
configure	dot1x radius secondary-server-ip <IP> port PORTID	This command configures the secondary radius server.
configure	dot1x radius secondary-server-ip <IP> port PORTID key KEY	This command configures the secondary radius server.
configure	no dot1x radius secondary-server-ip	This command removes the secondary radius server.

configure	dot1x username <STRING> passwd <STRING>	This command configures the user account for local authentication.
configure	no dot1x username <STRING>	This command deletes the user account for local authentication.
configure	dot1x accounting (disable|enable)	This command enables/disables the dot1x local accounting records.
interface	dot1x admin-control-direction (both|in)	This command configures the control direction for blocking packets.
interface	dot1x default	This command sets the port configuration to default settings.
interface	dot1x max-req <1-10>	This command sets the max-req times of a port. (1~10).
interface	dot1x port-control (auto | force-authorized | force-unauthorized)	This command configures the port control mode on the port.
interface	dot1x authentication (disable|enable)	This command enables/disables the 802.1x on the port.
interface	dot1x reauthentication (disable|enable)	This command enables/disables re-authentication on the port.
interface	dot1x timeout quiet-period	This command configures the quiet-period value on the port.
interface	dot1x timeout server-timeout	This command configures the server-timeout value on the port.
interface	dot1x timeout reauth-period	This command configures the reauth-period value on the port.
interface	dot1x timeout supp-timeout	This command configures the supp-timeout value on the port.
interface	dot1x guest-vlan VLAN_ID	This command configures the guest vlan on the port.
interface	no dot1x guest-vlan	This command deletes the guest vlan on the port.

6.3.2. Web Configuration

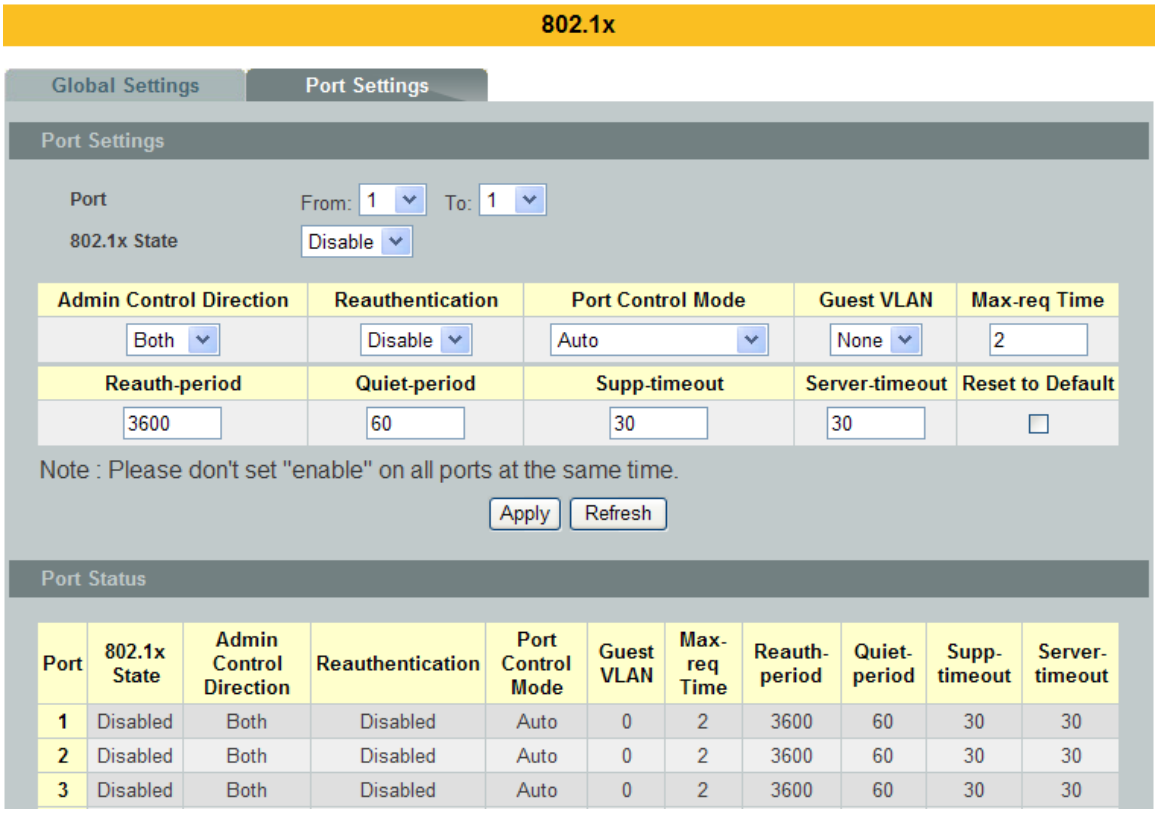
Global Settings



Parameter	Description
State	Select **Enable** to permit 802.1x authentication on the Switch. Note: You must first enable 802.1x authentication on the Switch before configuring it on each port.
Authentication Method	Select whether to use **Local** or **RADIUS** as the authentication method. The **Local** method of authentication uses the "guest" and "user" user groups of the user account database on the Switch itself to authenticate. However, only a certain number of accounts can exist at one time. **RADIUS** is a security protocol used to authenticate users by means of an external server instead of an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS allows you to validate an unlimited number of users from a central location.
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**.
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



4	Disabled	Both	Disabled	Auto	0	2	3600	60	30	30
5	Disabled	Both	Disabled	Auto	0	2	3600	60	30	30
6	Disabled	Both	Disabled	Auto	0	2	3600	60	30	30
7	Disabled	Both	Disabled	Auto	0	2	3600	60	30	30
8	Disabled	Both	Disabled	Auto	0	2	3600	60	30	30
9	Disabled	Both	Disabled	Auto	0	2	3600	60	30	30
10	Disabled	Both	Disabled	Auto	0	2	3600	60	30	30
11	Disabled	Both	Disabled	Auto	0	2	3600	60	30	30
12	Disabled	Both	Disabled	Auto	0	2	3600	60	30	30
13	Disabled	Both	Disabled	Auto	0	2	3600	60	30	30
14	Disabled	Both	Disabled	Auto	0	2	3600	60	30	30

Parameter	Description
Port	Select a port number to configure.
802.1x State	Select **Enable** to permit 802.1x authentication on the port. You must first enable 802.1x authentication on the Switch before configuring it on each port.
Admin Control Direction	Select **Both** to drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication. Select **In** to drop only incoming packets on the port when a user has not passed 802.1x port authentication.
Reauthentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Port Control Mode	Select **Auto** to require authentication on the port. Select **Force Authorized** to always force this port to be authorized. Select **Force Unauthorized** to always force this port to be unauthorized. No packets can pass through this port.
Guest VLAN	Select **None** to disable Guest VLAN. Select **1** to use VLAN 1 for traffic from hosts that have not passed authentication. Use this to limit the permissions of hosts which have not passed authentication.
Max-req Time	Specify the amount of times the Switch will try to connect to the authentication server before determining the server is down. The acceptable range for this field is 1 to 10 times.
Reauth period	Specify how often a client has to re-enter his or her username and password to stay connected to the port. The acceptable range for this field is 0 to 65535 seconds.
Quiet period	Specify a period of the time the client has to wait before the next re-authentication attempt. This will prevent the Switch from becoming overloaded with continuous re-authentication attempts from the client. The acceptable range for this field is

	0 to 65535 seconds.
Supp timeout	Specify how long the Switch will wait before communicating with the server. The acceptable range for this field is 0 to 65535 seconds.
Server timeout	Specify how long the Switch to time out the Authentication Server. The acceptable range for this field is 0 to 65535 seconds.
Reset to Default	Select this and click **Apply** to reset the custom 802.1x port authentication settings back to default.
Apply	Click Apply to add/modify the settings.
Refresh	Click Refresh to begin configuring this screen afresh.
Port Status	
Port	This field displays the port number.
802.1x State	This field displays if 802.1x authentication is **Enabled** or **Disabled** on the port.
Admin Control Direction	This field displays the Admin Control Direction. **Both** will drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication. **In** will drop only incoming packets on the port when a user has not passed 802.1x port authentication.
Reauthentication	This field displays if the subscriber must periodically re-enter his or her username and password to stay connected to the port.
Port Control Mode	This field displays the port control mode. **Auto** requires authentication on the port. **Force Authorized** forces the port to be authorized. **Force Unauthorized** forces the port to be unauthorized. No packets can Pass through the port.
Guest VLAN	This field displays the Guest VLAN setting for hosts that have not passed authentication. **None** or **1**.
Max-req Time	This field displays the amount of times the Switch will try to connect to the authentication server before determining the server is down.
Reauth period	This field displays how often a client has to re-enter his or her username and password to stay connected to the port.
Quiet period	This field displays the period of the time the client has to wait before the next re-authentication attempt.

Supp timeout	This field displays how long the Switch will wait before communicating with the server.
Server timeout	This field displays how long the Switch will wait before communicating with the client.

6.4. Port Security

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

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

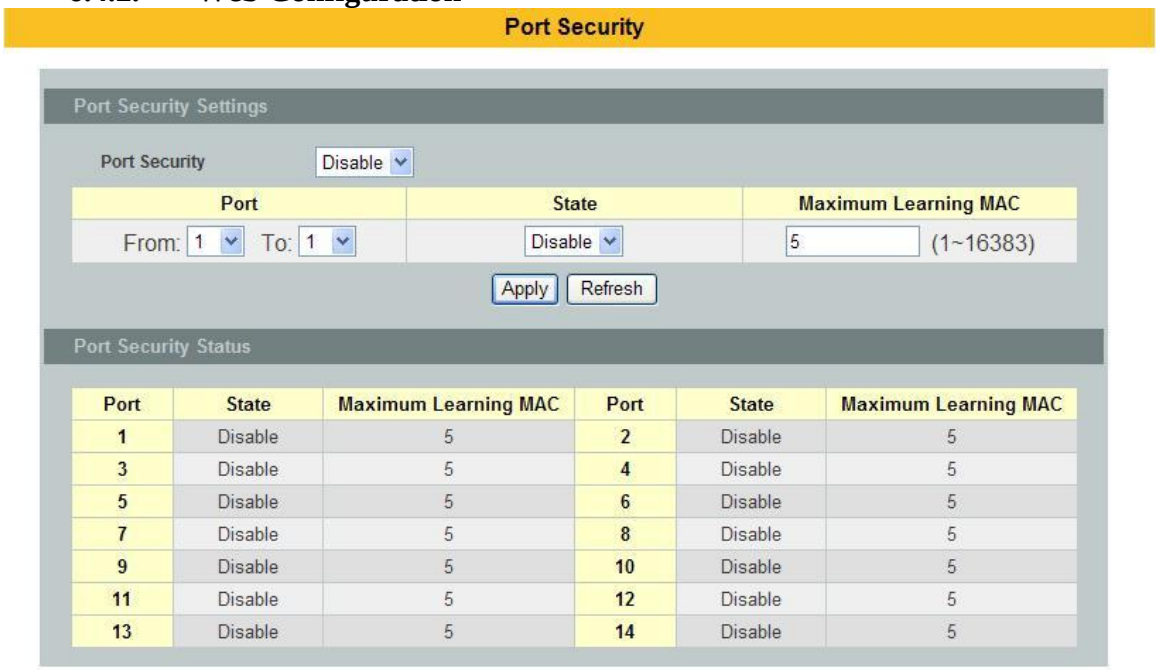
Port security can sets maximum number of dynamic MAC addresses allowed per interface. When the limit is exceeded, incoming packets with new MAC addresses are dropped. It can be use MAC table to check it. The static MAC addresses are not included for the limit.

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

6.4.1. CLI Configuration

Node	Command	Description
enable	show port-security	This command displays the port-security configurations.
configure	port-security (disable|enable)	This command enables/disables the port-security on the switch.
interface	port-security (disable|enable)	This command enables/disables the port-security on the port.
interface	port-security limit<1-16383>	The maximum number of dynamic MAC addresses.

6.4.2. Web Configuration



Parameter	Description
Port Security Settings	
Port Security	Select **Enable/Disable** to permit Port Security on the Switch.
Port	Select a port number to configure.
State	Select **Enable/Disable** to permit Port Security on the port.
Maximum Learning MAC	The maximum number of dynamic MAC addresses allowed per interface. The acceptable range is 1 to 16383 .
Port Security Status	
Port	This field displays a port number.
State	This field displays if Port Security is **Enabled** or **Disabled**
Maximum Learning MAC	This field displays the maximum number of dynamic MAC addresses

7. Management

7.1. Maintenance

7.1.1. Configuration

7.1.1.1. CLI Configuration

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

Example:

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

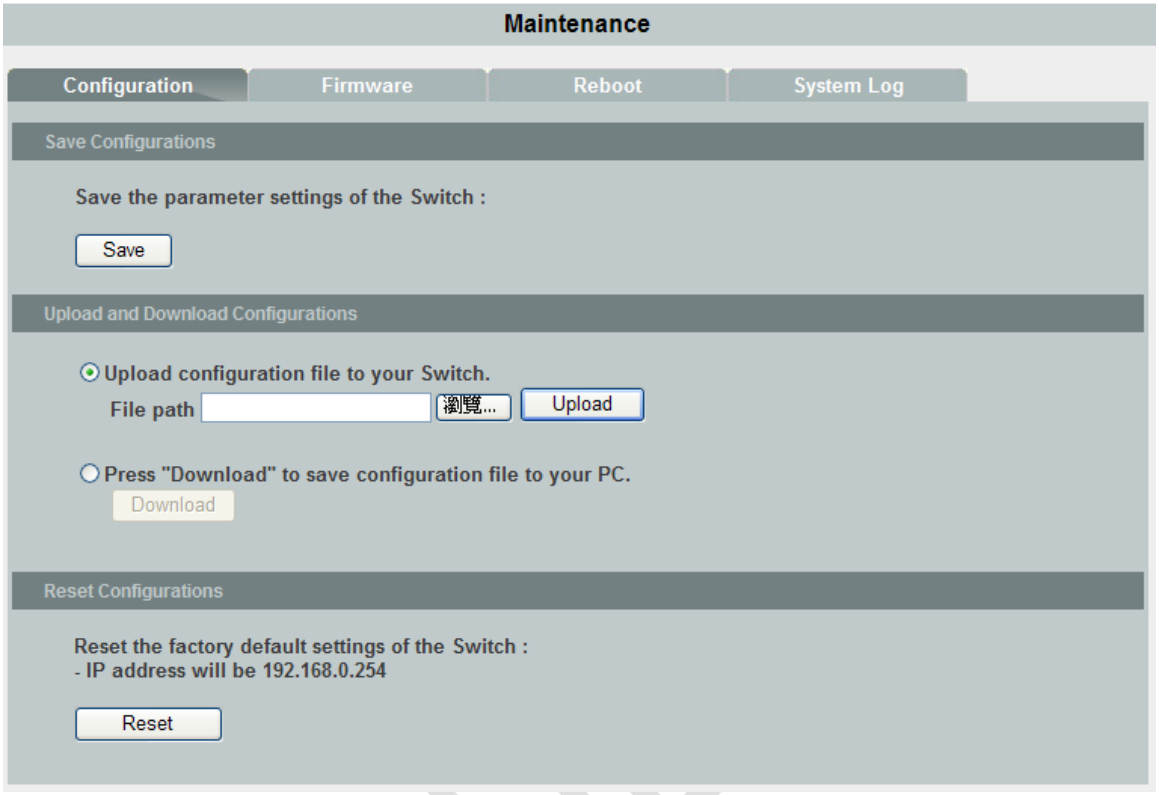
Enable the DHCP client function for the switch.

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

Upgrade new firmware:

- L2SWITCH#*configure terminal*
- L2SWITCH#archive download-fw http://172.20.1.34/3928p-vtk-1.1.0.b1.fw

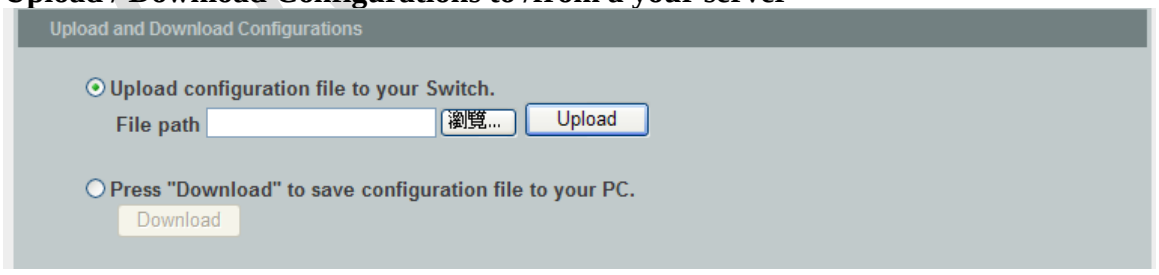
7.1.1.2. Web Configuration



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.

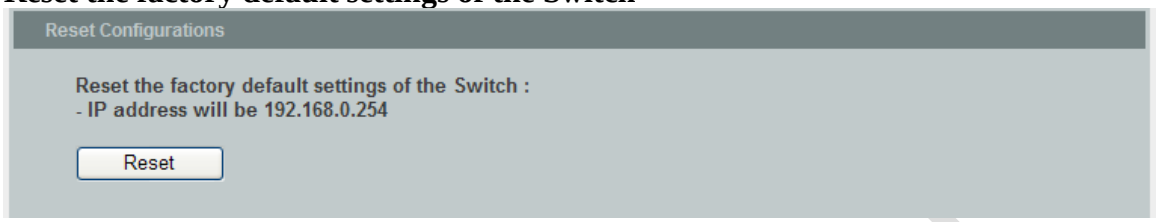
- Select the “Press “Download” to save configurations file to your PC”.
- Click the “Download” button to start the process.

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.

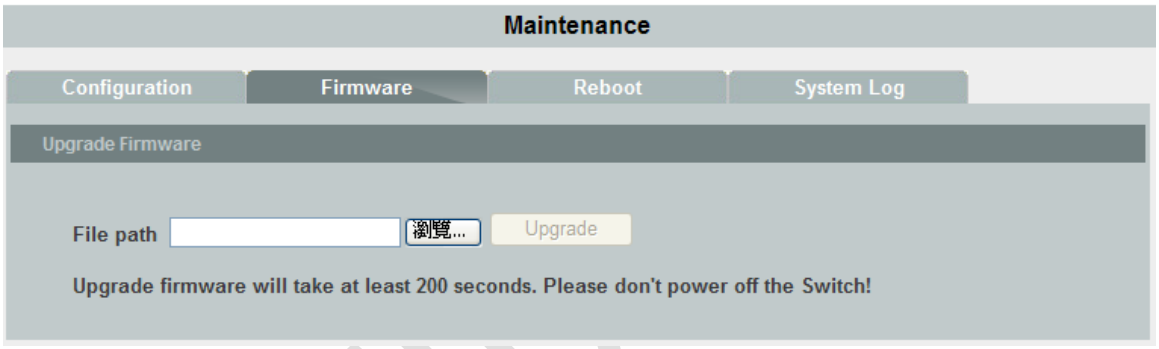
Reset the factory default settings of the Switch



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

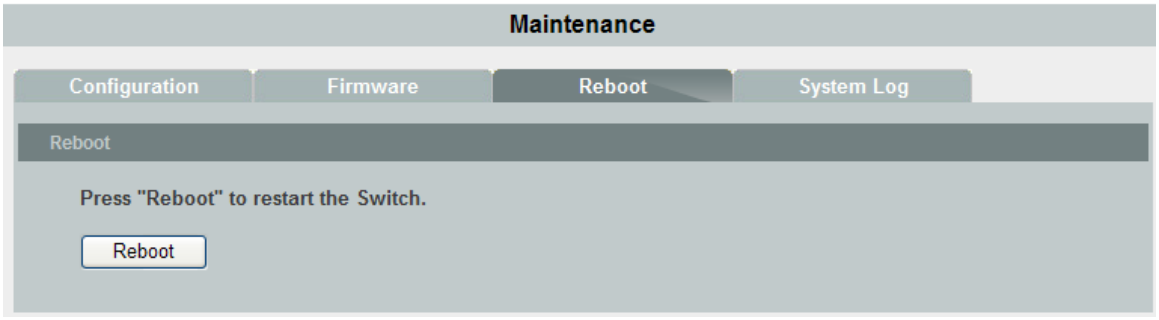
7.1.2. Firmware

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

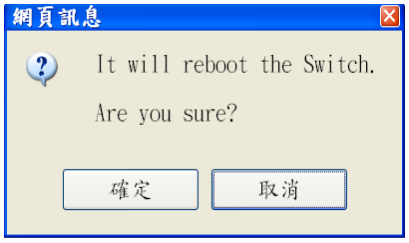


7.1.3. Reboot

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



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



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

7.1.4. Syslog

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.

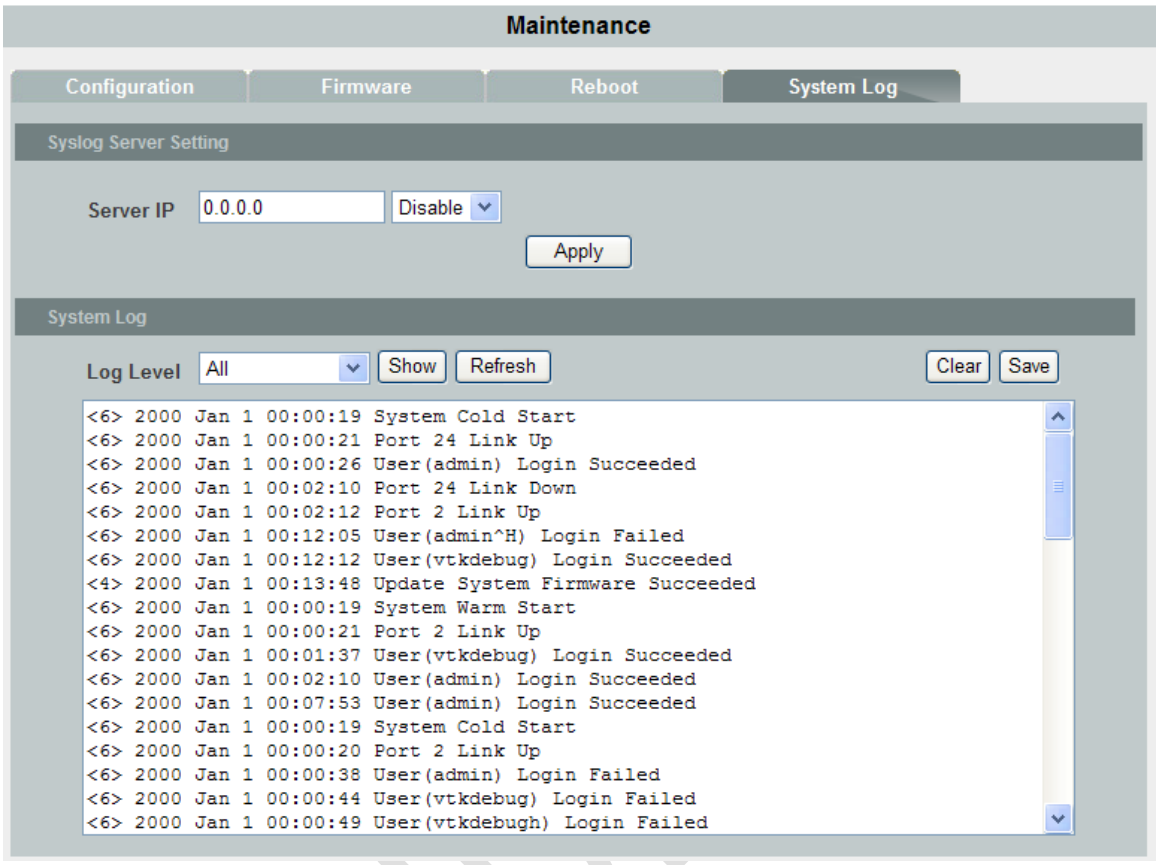
7.1.4.1. CLI Configuration

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

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#syslog-server ip 192.168.200.106
L2SWITCH(config)#syslog-server enable
L2SWITCH#show syslog server
      Syslog Server Configurations:
        State       : Enabled
        Server IP: 192.168.200.106
```

7.1.4.2. 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.

7.2. SNMP

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

SNMP exposes management data in the form of variables on the managed systems, which

describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

Support below MIBs:

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

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

Network ID of Trusted Host:

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

Network ID = (Host IP & Mask).

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

Note: Allow user to configure the community string and rights only.
User configures the Community String and the Rights and the Network ID of Trusted Host=0.0.0.0, Subnet Mask=0.0.0.0. It means that all hosts with the community string can access the Switch.

7.2.1. CLI Configuration

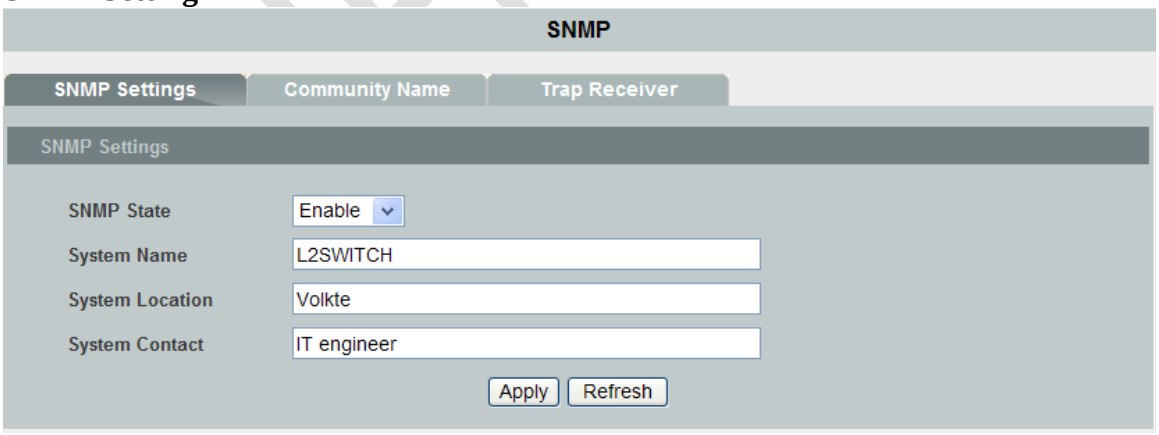
Node	Command	Description
enable	show snmp	This command displays the SNMP configurations.
configure	snmp community STRING (ro|rw) trusted-host IPADDR	This command configures the SNMP community name.
configure	snmp (disable|enable)	This command disables/enables the SNMP on the switch.
configure	snmp system-contact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

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#snmp enable
L2SWITCH(config)#snmp community public rw trusted-host 192.168.200.106/24
L2SWITCH(config)#snmp trap-receiver 192.168.200.106 v2c public
L2SWITCH(config)#snmp system-contact IT engineer
L2SWITCH(config)#snmp system-location Volkte
L2SWITCH#show snmp
  SNMP State      : Enabled
  System Name     : L2SWITCH
  System Location: Volkte
  System Contact : IT engineer

  Community Name:
  IP Address        Mask              Rights     Community String
  ---------------   ---------------   ---------  ----------------
  192.168.200.0     255.255.255.0     Read/Write  public

  Trap Receiver:
  IP Address        Version     Community String
  ---------------   ---------   ----------------
  192.168.200.106   2           public
```

7.2.2. Web Configuration

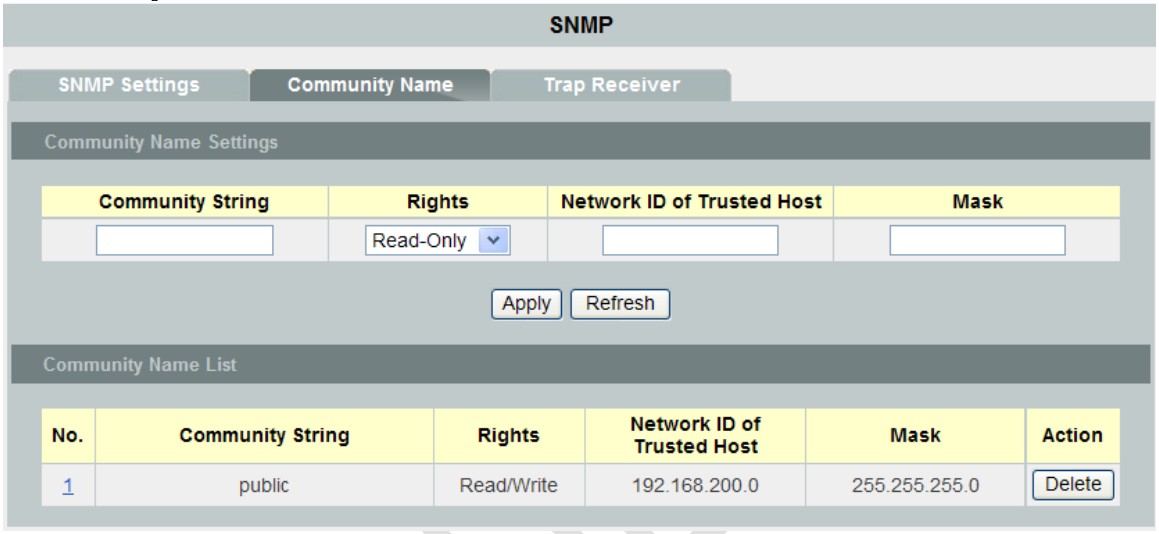
SNMP Setting



Parameter	Description
SNMP State	Select **Enable** to activate SNMP on the Switch. Select **Disable** to not use SNMP on the Switch.
System Name	Type a System Name for the Switch. (The System Name is same as the host name)

System Location	Type a System Location for the Switch.
System Contact	Type a System Contact for the Switch.
Apply	Click Apply to configure the settings.
Refresh	Click this to reset the fields to the last saved setting.

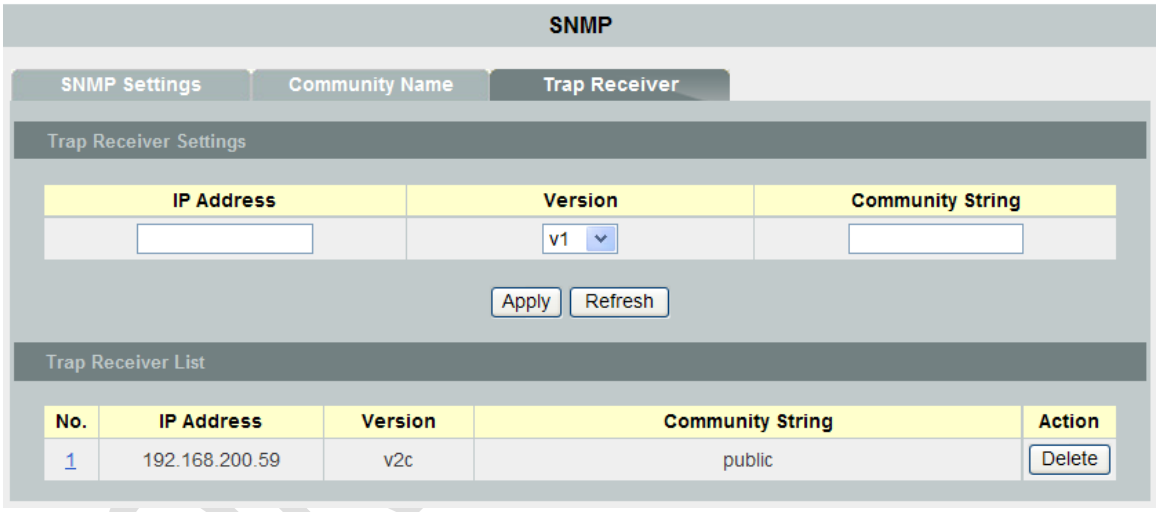
Community Name



Parameter	Description
Community String	Enter a Community string; this will act as a password for requests from the management station. An SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (the SNMP manager) and the device (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.
Rights	Select Read-Only to allow the SNMP manager using this string to collect information from the Switch. Select Read-Write to allow the SNMP manager using this string to create or edit MIBs (configure settings on the Switch).
Network ID of Trusted Host	Type the IP address of the remote SNMP management station in dotted decimal notation, for example 192.168.1.0.
Mask	Type the subnet mask for the IP address of the remote SNMP management station in dotted decimal notation, for example 255.255.255.0.
Apply	Click **Apply** to configure the settings.
Refresh	Click **Refresh** to begin configuring this screen afresh.

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

Trap Receiver



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.

7.3. User Account

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

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

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

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

7.3.1. CLI Configuration

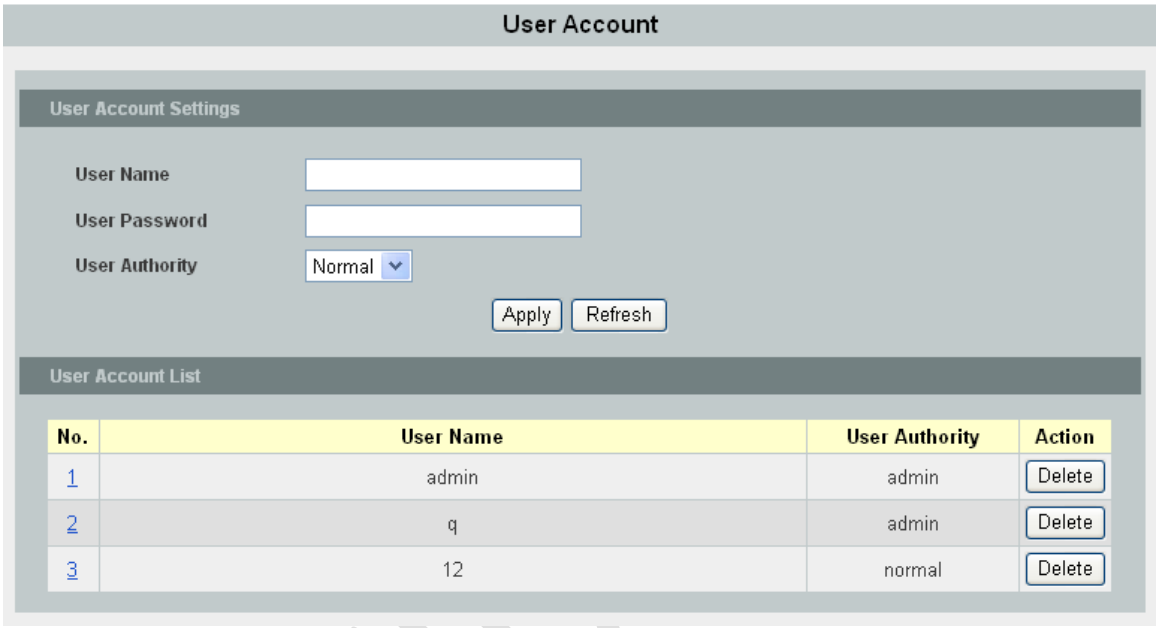
Node	Command	Description
enable	show user account	This command displays the current user accounts.
configure	add user USER_ACCOUNT PASSWORD (normal|admin)	This command adds a new user account.
configure	delete user USER_ACCOUNT	This command deletes a present user account.

Example:

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

```
L2SWITCH#show user account
        Authority    User
        -----------  --------------------------------
         admin       admin
         admin       q
         normal      1
```

7.3.2. Web Configuration



Parameter	Description
User Name	Type a new username or modify an existing one.
User Password	Type a new password or modify an existing one. Enter up to 32 alphanumeric or digit characters.
User Authority	Select with which group the user associates. **admin** (read and write) or **normal** (read only) for this user account.
Apply	Click **Apply** to add/modify the user account.
Refresh	Click **Refresh** to begin configuring this screen afresh.
User Account List	
No.	This field displays the index number of an entry.
User Name	This field displays the name of a user account.
User Password	This field displays the password.
User Authority	This field displays the associated group.
Action	Click the **Delete** button to remove the user account. Note: You cannot delete the last admin accounts.

Customer support

For all questions related to the MEN-5314 or any other Volktek product, please feel free to contact Volktek customer support:

Address	Volktek Customer Support 4F, 192 Liancheng Road, Zhonghe District, New Taipei City 23553, Taiwan
Phone	+886-2-8242-1000
Fax	+886-2-8242-3333
E-mail	*support@volktek.com.tw*
Website	www.volktek.com

ISO 9001 Certified