

VOLKTEK

User Manual

INS-8615

5-port 10/100/1000Base-T + 1-slot Gigabit SFP
Managed Industrial Gigabit Ethernet Switch

COPYRIGHT

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

FCC WARNING



This equipment has been tested and found to comply with the limits for a class A device, pursuant to part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. Operation of this equipment in a residential area is likely to cause harmful interference, in which case, the user will be required to correct the interference at the user's own expense.

CE



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



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

Warning



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

Warning



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

Warning



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

Warning



Warning

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



Warning

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



Warning

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



Warning

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



Warning

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



Warning

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



Warning

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

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



Warning

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



Warning

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



Warning

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



Warning

No user-serviceable parts inside. Do not open.



Warning

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

Table of Content

| | |
|---|-----------|
| <u>1. ABOUT THIS MANUAL</u> | 1 |
| 1.1. WELCOME | 1 |
| 1.2. PURPOSE | 1 |
| 1.3. TERMS/ USAGE | 1 |
| <u>2. ABOUT THE INS-8615</u> | 2 |
| 2.1. FEATURES | 2 |
| 2.2. SPECIFICATIONS..... | 2 |
| <u>3. HARDWARE DESCRIPTION</u> | 5 |
| 3.1. CONNECTORS | 5 |
| 3.1.1. 10/100/1000BASE-T PORTS..... | 5 |
| 3.1.2. SFP SLOTS FOR SFP MODULES | 5 |
| 3.2. INSTALLATION..... | 6 |
| 3.2.1. HARDWARE INSTALLATION..... | 6 |
| 3.2.2. DIN RAIL INSTALLATION..... | 6 |
| 3.2.3. WALL MOUNT INSTALLATION..... | 7 |
| 3.2.4. WIRING REDUNDANT POWER INPUTS | 7 |
| 3.2.5. POWER ON THE UNIT | 7 |
| 3.2.6. MANUAL REBOOT / RESET SWITCH | 8 |
| 3.3. LED INDICATORS..... | 8 |
| <u>4. SYSTEM STATUS</u> | 9 |
| 4.1. CONSOLE PORT (ONBOARD PIN HEADER CONNECTOR)..... | 9 |
| 4.2. TELNET | 9 |
| 4.3. HOW TO ENTER THE CLI? | 9 |
| 4.4. CLI COMMAND CONCEPT | 10 |
| 4.5. GUI LOGIN | 11 |
| 4.6. CLI CONFIGURATION | 11 |
| 4.7. SYSTEM INFORMATION..... | 12 |
| <u>5. BASIC SETTINGS</u> | 14 |
| 5.1. GENERAL SETTINGS..... | 14 |
| 5.1.1. SYSTEM..... | 14 |
| 5.1.1.1. INTRODUCTION | 14 |
| 5.1.1.2. CLI CONFIGURATION..... | 14 |
| 5.1.1.3. WEB CONFIGURATION | 15 |
| 5.1.2. JUMBO FRAME | 15 |
| 5.1.2.1. INTRODUCTION | 15 |
| 5.1.2.2. CLI CONFIGURATION | 16 |
| 5.1.2.3. WEB CONFIGURATION..... | 16 |
| 5.1.3. SNTP | 16 |
| 5.1.3.1. INTRODUCTION | 16 |

| | | |
|-------------|---------------------------------------|------------------|
| 5.1.3.2. | CLI CONFIGURATION | 17 |
| 5.1.3.3. | WEB CONFIGURATION | 19 |
| 5.1.4. | MANAGEMENT HOST | 21 |
| 5.1.4.1. | INTRODUCTION | 21 |
| 5.1.4.2. | CLI CONFIGURATION | 21 |
| 5.1.4.3. | WEB CONFIGURATION | 21 |
| 5.2. | MAC MANAGEMENT | 22 |
| 5.2.1. | INTRODUCTION | 22 |
| 5.2.2. | CLI CONFIGURATION | 23 |
| 5.2.3. | WEB CONFIGURATION | 23 |
| 5.3. | PORT MIRROR | 26 |
| 5.3.1. | INTRODUCTION | 26 |
| 5.3.2. | CLI CONFIGURATION | 26 |
| 5.3.3. | WEB CONFIGURATION | 27 |
| 5.4. | PORT SETTINGS | 28 |
| 5.4.1. | INTRODUCTION | 28 |
| 5.4.2. | CLI CONFIGURATION | 29 |
| 5.4.3. | WEB CONFIGURATION | 30 |
| 6. | <u>ADVANCED SETTINGS</u> | <u>33</u> |
| 6.1. | BANDWIDTH CONTROL | 33 |
| 6.1.1. | QoS..... | 33 |
| 6.1.1.1. | INTRODUCTION | 33 |
| 6.1.1.2. | CLI CONFIGURATION | 38 |
| 6.1.1.3. | WEB CONFIGURATION | 39 |
| 6.1.2. | RATE LIMITATION | 42 |
| 6.1.2.1. | STORM CONTROL..... | 42 |
| 6.1.2.1.1. | INTRODUCTION | 42 |
| 6.1.2.1.2. | CLI CONFIGURATION | 43 |
| 6.1.2.1.3. | WEB CONFIGURATION | 44 |
| 6.1.2.2. | BANDWIDTH LIMITATION..... | 44 |
| 6.1.2.2.1. | INTRODUCTION | 44 |
| 6.1.2.2.2. | CLI CONFIGURATION | 45 |
| 6.1.2.2.3. | WEB CONFIGURATION | 45 |
| 6.2. | IGMP SNOOPING..... | 46 |
| 6.2.1. | IGMP SNOOPING | 46 |
| 6.2.1.1. | INTRODUCTION | 46 |
| 6.2.1.2. | CLI CONFIGURATION | 48 |
| 6.2.1.3. | WEB CONFIGURATION | 49 |
| 6.2.2. | MULTICAST ADDRESS | 51 |
| 6.2.2.1. | INTRODUCTION | 51 |
| 6.2.2.2. | CLI CONFIGURATION | 53 |
| 6.2.2.3. | WEB CONFIGURATION | 53 |
| 6.3. | VLAN..... | 54 |
| 6.3.1. | PORT ISOLATION | 54 |
| 6.3.1.1. | INTRODUCTION | 54 |
| 6.3.1.2. | CLI CONFIGURATION | 55 |
| 6.3.1.3. | WEB CONFIGURATION | 55 |
| 6.3.2. | 802.1Q VLAN | 56 |
| 6.3.2.1. | INTRODUCTION | 56 |

| | | |
|-----------------|---|------------------|
| 6.3.2.2. | CLI CONFIGURATION | 58 |
| 6.3.2.3. | WEB CONFIGURATION | 59 |
| 6.3.3. | MAC-BASED VLAN | 62 |
| 6.3.3.1. | INTRODUCTION | 62 |
| 6.3.3.2. | CLI CONFIGURATION | 62 |
| 6.3.3.3. | WEB CONFIGURATION | 63 |
| 6.4. | EEE (ENERGY EFFICIENT ETHERNET) | 63 |
| 6.4.1. | INTRODUCTION | 63 |
| 6.4.2. | CLI CONFIGURATION | 64 |
| 6.4.3. | WEB CONFIGURATION | 64 |
| 6.5. | LINK LAYER DISCOVERY PROTOCOL (LLDP) | 65 |
| 6.5.1. | INTRODUCTION | 65 |
| 6.5.2. | CLI CONFIGURATION | 65 |
| 6.5.1. | WEB CONFIGURATION | 66 |
| 6.6. | SPANNING TREE PROTOCOL (STP/RSTP) | 67 |
| 6.6.1. | INTRODUCTION | 67 |
| 6.6.2. | CLI CONFIGURATION | 72 |
| 6.6.3. | WEB CONFIGURATION | 75 |
| 7. | <u>MONITOR</u> | <u>79</u> |
| 7.1. | ALARM | 79 |
| 7.1.1. | INTRODUCTION | 79 |
| 7.1.2. | CLI CONFIGURATION | 79 |
| 7.1.3. | WEB CONFIGURATION | 79 |
| 7.2. | PORT STATISTIC | 80 |
| 7.2.1. | INTRODUCTION | 80 |
| 7.2.2. | CLI CONFIGURATION | 80 |
| 7.2.3. | WEB CONFIGURATION | 80 |
| 7.3. | PORT UTILIZATION | 81 |
| 7.3.1. | INTRODUCTION | 81 |
| 7.3.2. | CLI CONFIGURATION | 81 |
| 7.3.3. | WEB CONFIGURATION | 81 |
| 7.4. | RMON STATISTICS | 81 |
| 7.4.1. | INTRODUCTION | 81 |
| 7.4.2. | CLI CONFIGURATION | 81 |
| 7.4.3. | WEB CONFIGURATION | 82 |
| 7.5. | TRAFFIC MONITOR | 82 |
| 7.5.1. | INTRODUCTION | 82 |
| 7.5.2. | CLI CONFIGURATION | 83 |
| 7.5.3. | WEB CONFIGURATION | 84 |
| 8. | <u>MANAGEMENT</u> | <u>85</u> |
| 8.1. | SNMP | 85 |
| 8.1.1. | SNMP | 85 |
| 8.1.1.1. | INTRODUCTION | 85 |
| 8.1.1.2. | CLI CONFIGURATION | 86 |
| 8.1.1.3. | WEB CONFIGURATION | 86 |
| 8.1.2. | SNMP TRAP RECEIVER | 88 |
| 8.2. | MAIL ALARM | 89 |

| | |
|--------------------------------------|------------------|
| 8.2.1. INTRODUCTION | 89 |
| 8.2.2. REFERENCE..... | 90 |
| 8.2.3. CLI CONFIGURATION..... | 90 |
| 8.2.4. WEB CONFIGURATION | 91 |
| 8.3. MAINTENANCE | 92 |
| 8.3.1. CONFIGURATION | 92 |
| 8.3.1.1. CLI CONFIGURATION..... | 92 |
| 8.3.1.2. WEB CONFIGURATION | 93 |
| 8.3.2. FIRMWARE | 94 |
| 8.3.3. REBOOT | 94 |
| 8.4. SYSTEM LOG | 95 |
| 8.4.1. INTRODUCTION | 95 |
| 8.4.2. CLI CONFIGURATION..... | 95 |
| 8.4.3. WEB CONFIGURATION | 96 |
| 8.5. USER ACCOUNT | 96 |
| 8.5.1. INTRODUCTION | 96 |
| 8.5.2. CLI CONFIGURATION..... | 97 |
| 8.5.3. WEB CONFIGURATION | 98 |
| <u>CUSTOMER SUPPORT</u> | <u>99</u> |

CONFIDENTIAL

1. About this Manual

1.1. Welcome

The INS-8615 is a Managed Industrial Switch specifically designed to suit your heavy industrial environments and contains all necessary standard features to deploy in automation systems. Engineered with hardened components and enclosed in a rugged IP40 metal case, the INS-8615 can operate in regular operating temperature -40°C to 75°C . Addition to this, the switch has excellent tolerance capability to high vibration and shock.

Despite the fact that the INS-8615 is perfectly designed to operate in extreme industrial conditions; the switch is also equipped with a variety of management functions that let you configure communication parameters as you desire and monitor the network behavior in number of different simple ways. In addition, the switch is built with dual redundant power inputs to ensure reliability and maximize network up time. Other integrated features of the switch such as Auto-negotiation, Rate limitation and Port Isolation optimizes your network performance and provide a secure network, offering a cost-effective solution in a small but powerful package.

1.2. Purpose

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

1.3. Terms/ Usage

In this manual, the term “Switch” (first letter upper case) refers to the INS-8615 Switch, and “switch” (first letter lower case) refers to other switches.

2. About the INS-8615

2.1. Features

Configuration

Command Line Interface
Telnet, Web GUI,
SNMP v1/v2c
Management VLAN
System log
Firmware Upgradable
Configuration Upload/Download
Spanning Tree Protocol
Rapid Spanning Tree Protocol

VLAN

802.1Q Tag-based VLAN
MAC-based VLAN
256 Active VLAN

Traffic Control

IGMP snooping v1/v2/v3
802.1p Priority Queues per port
Rate Limitation
Storm Control
Port Isolation

Diagnostic

LED status
SNMP trap
E-mail alarm
Port Mirroring
SNTP
RMON
Port Statistic

2.2. Specifications

IEEE Standards

| | |
|--------------|-------------------------------|
| IEEE 802.3 | 10Base-T |
| IEEE 802.3u | 100Base-TX |
| IEEE 802.3ab | 1000Base-T |
| IEEE 802.3z | 1000Base-SX/LX |
| IEEE 802.3x | Flow Control |
| IEEE 802.1p | Class of service |
| IEEE 802.1q | VLAN Tagging |
| IEEE 802.1d | Spanning Tree Protocol |
| IEEE 802.1w | Rapid STP |
| IEEE 802.1ab | Link Layer Discovery Protocol |
| IEEE 802.3az | Energy Efficient Ethernet |

Performance

| | |
|--------------------|----------|
| Switching fabric | 12Gbps |
| L2 forwarding | 8.93Mpps |
| Packet buffer size | 4.1Mbit |
| MAC table size | 8k |
| Jumbo Frame Size | 10k |

Physical ports

1 x Gigabit SFP
4 x 10/100/1000Base-T

Maximum Distances

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

Power

Input Voltage:

- Primary inputs : 20~57VDC
- Redundant inputs : 20~57VDC

Connection:

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

Support Overload current protection

Support Power Reverse Polarity Protection

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

Self-power Consumption: 10W

Mechanical

| | |
|-------------------|-------------------------------------|
| Dimension (WxHxD) | 31x136x109.5 mm (1.22x5.36x4.31 in) |
| Housing | IP40 metal protection |
| Weight | 395g |
| Installation | DIN-Rail or Wall Mount (Optional) |

Operating Requirement

Operating Temperature -40°C to 75°C

VOLKTEK

| | |
|---------------------|-------------------------------|
| Storage Temperature | -40 to 85°C |
| Operating Humidity | 10 to 95% RH (non-condensing) |
| Storage Humidity | 5 to 95% RH (non-condensing) |

CONFIDENTIAL

3. Hardware Description

3.1. Connectors

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

3.1.1. 10/100/1000Base-T Ports

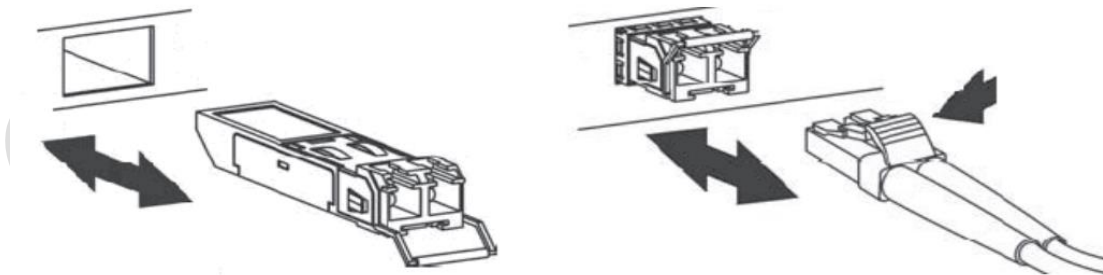
The 10/100/1000Base-T ports support network speeds of 10Mbps, 100Mbps or 1000Mbps, and can operate in half- and full-duplex transfer modes. These ports also offer automatic MDI/MDI-X crossover detection that gives true “plug-n-play” capability – just plug the network cables into the ports and the ports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

3.1.2. SFP Slots for SFP modules

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

Installing the SFP modules and Fiber Cable

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



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

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

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

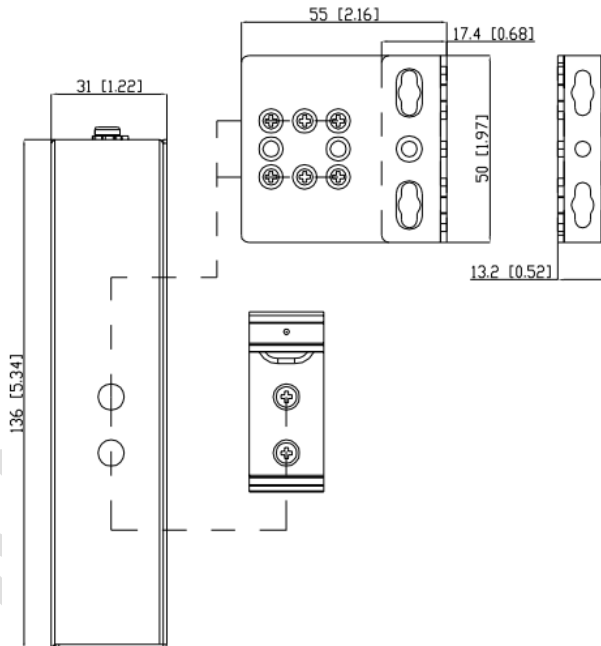
3.2. Installation

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

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

3.2.1. Hardware Installation

- ✓ **Step 1:** Unpack the device and other contents of the package.
- ✓ **Step 2:** Fasten DIN-Rail or Wall-mount kit on the rear of the INS-8615



- ✓ **Step 3:** Connect the 20~57V DC power supply to the PWR & RPS terminal block or 4-pin power adapter to DC jack receiver on the top of the Switch (Refer to “Wiring Redundant Power Inputs”)
- ✓ **Step 4:** Connect the Ethernet (RJ-45) port to the networking device and check the LED status to confirm the connection is established.

3.2.2. DIN rail Installation

The INS-8615 has a DIN rail bracket on the back of the Switch to satisfy the mounting installation.

Location: The INS-8615 can be DIN-Rail-mounted in cabinet or enclosure.

Mounting the switch

Place the INS-8615 on the DIN rail from above using the slot. Push the front of the switch toward the mounting surface until it snaps into place with a click sound.

Dismounting the switch

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

3.2.3. Wall mount Installation

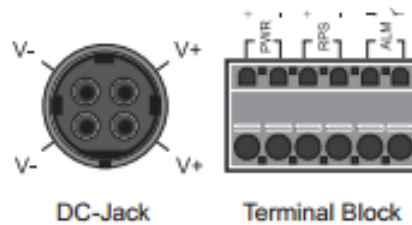
Location: The INS-8615 can be placed on a horizontal surface through wall-mounted kit

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

3.2.4. Wiring Redundant Power Inputs

You can use either “DC-Jack” or “Terminal Block (PWR)” for primary power and “Terminal Block (RPS)” for secondary power source, to be a Redundant Power Input.

Top views of DC-Jack and Terminal Block are shown as pictures:



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

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

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

3.2.5. Power On the Unit

The Switch accepts the power input voltage from 20~57V DC.

- ✓ Wiring appropriate power source as above guideline before turn on the power.
- ✓ Check the front-panel LEDs as the device is powered on to verify that the Power LED is lit. If not, check that the power cable is correctly and securely plugged in.

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

- *The correct power supply voltage is listed on the product label. Check the voltage of your power source to make sure that you are using the correct voltage. Do NOT use a voltage greater than what is specified on the product label.*
- *Calculate the maximum possible current in each power wire and common wire.*

Observe all electrical codes dictating the maximum current allowable for each wire size. If current go above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.

3.2.6. Manual Reboot / Reset Switch

There has “Reset” function in the Switch’s bottom which can help to manually reboot or reload to factory default setting.

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



3.3. LED Indicators

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

| | | |
|-----------------------------|-------------|--|
| PWR (Green) | Illuminated | Power On by terminal block PWR or DC-Jack |
| | Off | Terminal block PWR/DC-Jack fails or is not available |
| RPS (Green) | Illuminated | Power On by terminal block RPS |
| | Off | Terminal block RPS fails or is not available |
| ALM (Red) | Illuminated | PWR/RPS fails or not available |
| | Off | No power lost or DIP function is disabled |
| 10/100/1000 Mbps (Green) | Illuminated | Copper port speeds at 1000Mbps |
| | Off | Copper port speeds at 10/100Mbps |
| LNK/ACT (Green) | Illuminated | Copper port link-up |
| | Blinking | Data is transmitting / receiving |
| | Off | Port disconnected or link failed |
| SFP (Green) | Illuminated | SFP port speeds at 1000Mbps |
| | Blinking | Data is transmitting / receiving |
| | Off | Port disconnected or link failed |

Notice:

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

4. System Status

4.1. Console Port (Onboard Pin header connector)

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

Default Settings for the Console Port

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

- Press [ENTER] to open the login screen.

| Setting | Default Value |
|------------------|---------------|
| Default Username | admin |
| Default Password | admin |

4.2. Telnet

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

Default Management IP Address

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

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

4.3. How to enter the CLI?

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

Please press Enter to activate this console

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

L2SWITCH login:

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

L2SWITCH>

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

Input command “*enable*”

L2SWITCH>enable

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

user: admin

password: admin

4.4. CLI command concept

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

The Node type:

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

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

```
L2SWITCH(config)#interface gigaethernet1/0/5
L2SWITCH(config-if)#
```

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

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

4.5. GUI Login

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

Default:

User name: admin
 Password: admin

4.6. CLI Configuration

| Node | Command | Description |
|--------|---------------|--|
| enable | show hostname | This command displays the system's network name. |

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

4.7. System Information

System Information

System Information

| | |
|--------------------|--|
| Model Name | INS-8615 |
| Host Name | L2SWITCH |
| Boot Code Version | 8615-000-1.0.1.S0 |
| Firmware Version | 8615-000-1.0.4.b1 |
| Built Date | Mon Jun 15 11:25:30 CST 2015 |
| DHCP Client | Enabled |
| IP Address | 192.168.202.140 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.202.1 |
| MAC Address | 00:02:01:02:01:06 |
| Serial Number | A0000000000001 |
| Management VLAN | 1 |
| CPU Loading | <div style="width: 100px; height: 15px; background-color: #ccc; display: inline-block;"></div> 0 % |
| Memory Information | Total: 127780 KB, Free: 120988 KB, Usage: 5.32 % |
| Current Time | 2014-1-1, 0:21:22 |

| Parameter | Description |
|-------------------|---|
| Model Name | This field displays the model name of the Switch. |
| Host name | This field displays the name of the Switch. |
| Boot Code Version | This field displays the boot code version. |
| Firmware Version | This field displays the firmware version. |
| Built Date | This field displays the built date of the firmware. |
| DHCP Client | This field displays whether the DHCP client is enabled on the Switch. |
| IP Address | This field indicates the IP address of the Switch. |
| Subnet Mask | This field indicates the subnet mask of the Switch. |
| Default Gateway | This field indicates the default gateway of the Switch. |

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

CONFIDENTIAL

5. Basic Settings

5.1. General Settings

5.1.1. System

5.1.1.1. Introduction

Management VLAN

If you want to configure a management VLAN, the management VLAN should be created first and the management VLAN should have at least one member port.

Host Name

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

Default Settings

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

5.1.1.2. CLI Configuration

| Node | Command | Description |
|-----------|---------------------------------------|---|
| 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 | Show | This command displays the eth0 configurations. |
| eth0 | ip address A.B.C.D/M | This command configures a static IP and subnet mask for the system. |
| eth0 | ip address default-gateway A.B.C.D | This command configures the system default gateway. |
| eth0 | ip dhcp client (disable enable renew) | This command configures a DHCP client function for the system. Disable: Use a static IP address on the switch. Enable & Renew: Use DHCP client to get an IP address from DHCP server. |
| eth0 | management vlan VLANID | This command configures the management vlan. |

5.1.1.3. Web Configuration

General Settings

System
Jumbo Frame
SNTP
Management Host

System Settings

Hostname

DHCP Client Enable ▾ Renew

Static IP Address

Subnet Mask

Default Gateway

Management VLAN

Apply
Refresh

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

5.1.2. Jumbo Frame

5.1.2.1. Introduction

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

Notice:

- ✓ The jumbo frame settings will apply to all ports.
- ✓ If the size of a packet exceeds the jumbo frame size, the packet will be dropped.
- ✓ The available values are 10240, 9216, 1522, 1536, 1552.

Default Setting: The default jumbo frame is 10240 bytes.

5.1.2.2. CLI Configuration

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

5.1.2.3. Web Configuration

General Settings

System
Jumbo Frame
SNTP
Management Host

Jumbo Frame Setting

Frame Size

10240 ▼

1522

1536

1552

9216

10240

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

5.1.3. SNTP

5.1.3.1. Introduction

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

UDP Port: 123.

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

Note:

1. The SNTP server always replies the UTC current time.
2. When the Switch receives the SNTP reply time, the Switch will adjust the time with the time zone configuration and then configure the time to the Switch.
3. If the time server's IP address is not configured, the Switch will not send any SNTP request packets.
4. If no SNTP reply packets, the Switch will retry every 10 seconds forever.
5. If the Switch has received SNTP reply, the Switch will re-get the time from NTP server every 24 hours.
6. If the time zone and time NTP server have been changed, the Switch will repeat the query process.
7. No default SNTP server.

Default Settings

Current Time:

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

Time Server Configuration:

 Time Zone : +00:00
 IP Address: 0.0.0.0

DayLight Saving Time Configuration:

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

5.1.3.2. CLI Configuration

| Node | Command | Description |
|-----------|-----------------------------|--|
| enable | show time | This command displays current time and time configurations. |
| configure | time HOUR:MINUTE:SECOND | Sets the current time on the Switch. <i>hour:</i> 0-23 <i>min:</i> 0-59 <i>sec:</i> 0-59 Note: If you configure Daylight Saving Time after you configure the time, the Switch will apply Daylight Saving Time. |
| configure | time date YEAR/MONTH/DAY | Sets the current date on the Switch. <i>year:</i> 1970- <i>month:</i> 1-12 |

| | | |
|-----------|---|---|
| | | <i>day: 1-31</i> |
| configure | time daylight-saving-time | This command enables the daylight saving time. |
| configure | time daylight-saving-time start-date (first second third fourth last) (Sunday Monday Tuesday Wednesday Thursday Friday Saturday) MONTH OCLOCK | This command sets the start date for the Daylight Saving Time. For Example: first Sunday 4 0 (AM:0 1st Sunday in April) |
| configure | time daylight-saving-time end-date (first second third fourth last) (Sunday Monday Tuesday Wednesday Thursday Friday Saturday) MONTH OCLOCK | This command sets the end date for the Daylight Saving Time. For Example: Last Sunday 10 18 (PM: 6 Last Sunday in October) |
| 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 VALUE | Selects the time difference between UTC (formerly known as GMT) and your time zone. Valid value: -1200 to 1200. |

Example:

L2SWITCH(config)#time ntp-server 192.5.41.41

L2SWITCH(config)#time timezone +800

5.1.3.3. Web Configuration

General Settings

System
Jumbo Frame
SNTP
Management Host

Current Time and Date

Current Time 00:04:54 (UTC)
Current Date 2014-01-01

Time and Date Settings

Manual
New Time . . / : : (yyyy.mm.dd / hh:mm:ss)

Enable Network Time Protocol
NTP Server 192.5.41.41 - North America

Time Zone

Daylight Saving Settings

State
Start Date o'clock
End Date o'clock

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

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

5.1.4. Management Host

5.1.4.1. Introduction

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

Default Settings

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

5.1.4.2. CLI Configuration

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

Example:

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

5.1.4.3. Web Configuration

General Settings

System
Jumbo Frame
SNTP
Management Host

Management Host Settings

Management Host

Management Host List

| No. | Management Host | Action |
|-----|-----------------|--------|
| | | |

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

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

5.2. MAC Management

5.2.1. Introduction

Dynamic Address:

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

Static Address:

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

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

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

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

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

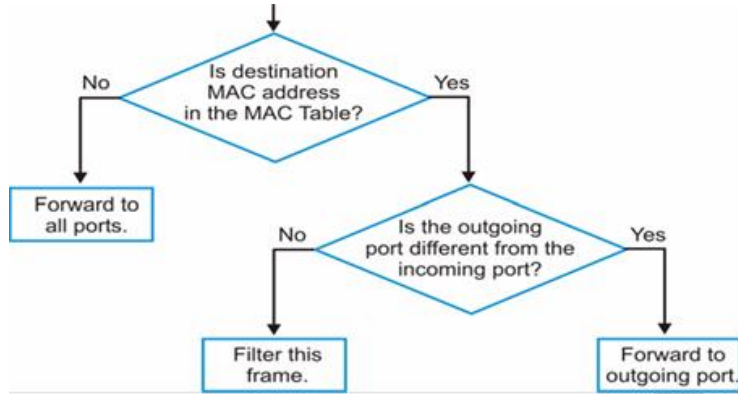


Figure MAC Table Flowchart

Default Settings

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

5.2.2. CLI Configuration

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

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

5.2.3. Web Configuration

Static MAC

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

MAC Address Management

Static MAC Settings
MAC Table
Age Time Setting

Static MAC Settings

| MAC Address | VLAN ID | Port |
|----------------------|----------------------|--|
| <input type="text"/> | <input type="text"/> | 1 ▼ |

Static MAC Table

| MAC Address | VLAN ID | Port | Action |
|-------------------|---------|------|--------|
| 00:02:01:02:01:06 | 1 | CPU | |

Total counts : 1

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

MAC Table

MAC Address Management

Static MAC Settings
MAC Table
Age Time Setting

MAC Table

Show Type: All Apply Refresh Clear

| MAC | Type | VLAN ID | Port |
|-------------------|---------|---------|------|
| 00:02:00:00:00:00 | Static | 1 | CPU |
| 00:1d:70:00:00:00 | Dynamic | 1 | 1 |
| 00:17:c5:66:48:cc | Dynamic | 1 | 1 |

Total counts : **3**

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

Age Time Settings

MAC Address Management

Static MAC Settings
MAC Table
Age Time Setting

Age Time Setting

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

Apply Refresh

| Parameter | Description |
|-----------|--|
| Age Time | Configure the age time; the valid range is from 20 to 500 seconds. The default value is 300 seconds. |
| Apply | Click Apply to take effect the settings. |

Refresh

Click this to update the information in the MAC table.

5.3. Port Mirror

5.3.1. Introduction

Port-based Mirroring

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

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

Source Mode:

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

Note:

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

Default Settings

Mirror Configurations:

- State : Disable
- Monitor port : 1
- Ingress port(s) : None
- Egress port(s) : None

5.3.2. CLI Configuration

| Node | Command | Description |
|-----------|------------------------------------|--|
| enable | show mirror | This command displays the current port mirroring configurations. |
| configure | mirror (disable enable) | This command disables / enables the port mirroring on the switch. |
| configure | mirror destination port PORT_ID | This command specifies the monitor port for the port mirroring. |
| configure | mirror source ports PORT_LIST mode | This command adds a port or a range of ports as the source ports of the port mirroring. |

| | | |
|-----------|-------------------------------------|---|
| | <i>(both/ingress/egress)</i> | |
| 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 3-5 mode both
```

5.3.3. Web Configuration

Port Mirroring

Port Mirroring Settings

State: Disable ▾

Monitor to Port: 1 ▾

All Ports: - ▾

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

Apply
Refresh

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

5.4. Port Settings

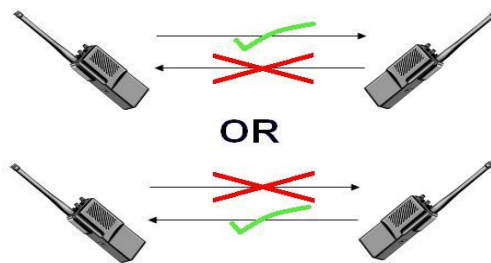
5.4.1. Introduction

- Duplex mode

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

Half Duplex:

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



Full Duplex:

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



- Loopback Test

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

- Auto MDI-MDIX

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

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

- **Auto Negotiation**

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

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

- **Flow Control**

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

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

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

- **Cable Test.**

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

Default Settings

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

The default port Flow Control is Off for all ports.

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

5.4.2. CLI Configuration

| Node | Command | Description |
|-------------|-----------------------|--|
| enable | show interface IFNAME | This command displays the current port configurations. |
| interface | show | This command displays the current port configurations. |
| interface | loopback (none mac) | This command tests the loopback |

| | | |
|-----------|---|---|
| | | mode of operation for the specific port. |
| interface | flowcontrol (off on) | This command disables / enables the flow control for the port. |
| interface | speed (auto 10-full 10-half 100-full 100-half 1000-full) | This command configures the speed and duplex for the port. |
| interface | shutdown | This command disables the specific port. |
| interface | no shutdown | This command enables the specific port. |
| interface | description STRING | This command configures a description for the specific port. |
| interface | no description | This command configures the default port description. |
| interface | cable-test start | This command starts to diagnostics the Ethernet cable. |
| interface | show cable-test result | This command displays the test result of the Ethernet cable test. |

5.4.3. Web Configuration

General Settings:

Port Settings

General Settings
Information

Port Settings

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

Port Status

| Port | State | Speed/Duplex | Flow Control | Link Status |
|------|---------|--------------|--------------|-------------------|
| 1 | Enabled | Auto | Off | 100M / Full / Off |
| 2 | Enabled | Auto | Off | Link Down |
| 3 | Enabled | Auto | Off | Link Down |
| 4 | Enabled | Auto | Off | Link Down |
| 5 | Enabled | Auto | Off | Link Down |
| 6 | Enabled | N/A | Off | Link Down |

| Parameter | Description |
|--------------|---|
| Port | Select a port or a range ports you want to configure on this screen. |
| State | Select Enable to activate the port or Disable to deactivate the port. |
| Speed/Duplex | Select the speed and duplex mode of the port. The choices are: • Auto |

| | |
|--------------|--|
| | <ul style="list-style-type: none"> • 10 Mbps / Full Duplex • 10 Mbps / Half Duplex • 100 Mbps / Full Duplex • 100 Mbps / Half Duplex • 1000 Mbps / Full Duplex |
| Flow Control | Select On to enable access to buffering resources for the port thus ensuring lossless operation across network switches. Otherwise, select Off to disable it. |
| Apply | Click Apply to take effect the settings. |
| Refresh | Click Refresh to begin configuring this screen afresh. |
| Port | This field displays the port number. |
| State | This field displays whether the port is enabled or disabled. |
| Speed/Duplex | This field displays the speed either 10M , 100M or 1000M and the duplex mode Full or Half . |
| Flow Control | This field displays whether the port's flow control is On or Off . |
| Link Status | This field displays the link status of the port. If the port is up, it displays the port's speed, duplex and flow control setting. Otherwise, it displays Link Down if the port is disabled or not connected to any device. |

CONFIDENTIAL

Information:

Port Settings

General Settings
Information

Port Settings

| Port | Description |
|---|---|
| From: <input type="text" value="1"/> To: <input type="text" value="1"/> | <input type="text" value="gigabitethernet1/0/1"/> |

Port Status

| Port | Description | Status | Uptime | Medium Mode |
|------|----------------------|----------|----------------|-------------|
| 1 | gigabitethernet1/0/1 | Normally | 0 days 2:43:16 | Copper |
| 2 | gigabitethernet1/0/2 | Normally | 0 days 0:0:0 | Copper |
| 3 | gigabitethernet1/0/3 | Normally | 0 days 0:0:0 | Copper |
| 4 | gigabitethernet1/0/4 | Normally | 0 days 0:0:0 | Copper |
| 5 | gigabitethernet1/0/5 | Normally | 0 days 0:0:0 | Copper |
| 6 | gigabitethernet1/0/6 | Normally | 0 days 0:0:0 | Fiber |

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

6. Advanced Settings

6.1. Bandwidth Control

6.1.1. QoS

6.1.1.1. Introduction

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

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

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

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

The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues as follows:

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

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

QoS Enhancement

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

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

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

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

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

802.1p Priority

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

Ethernet Packet:

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

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

802.1Q Tag:

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

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

Priority Levels:

PCP: Priority Code Point.

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

DiffServ (DSCP)

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

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

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

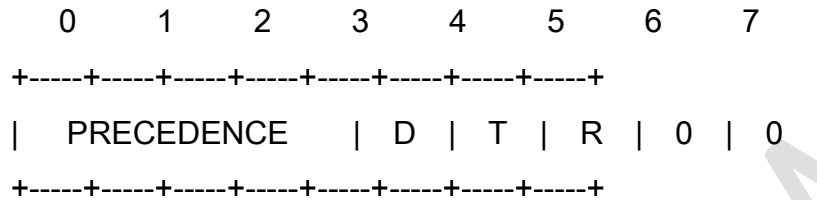
| Version | IHL | Type of Service | Total Length | |
|---------------------|----------|-----------------|-----------------|--|
| Identification | | Flags | Fragment Offset | |
| Time to Live | Protocol | Header Checksum | | |
| Source Address | | | | |
| Destination Address | | | | |
| Options | | |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

Example Internet Datagram Header

IP Header Type of Service: 8 bits

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

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



Precedence

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

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

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

The Network Control precedence designation is intended to be used within a network only. The actual use and control of that designation is up to each network. The Internetwork Control designation is intended for use by gateway control originators only. If the actual use of these precedence designations is of concern to a particular network, it is the responsibility of that network to control the access to, and use of, those precedence designations.

| DSCP | Priority | DSCP | Priority | DSCP | Priority |
|------|----------|------|----------|------|----------|
| 0 | 0 | 1 | 0 | 2 | 0 |
| ... | | | | | |
| 60 | 0 | 61 | 0 | 62 | 0 |
| 63 | 0 | | | | |

Example:

IP Header

DSCP=50 → 45 C8 . . .

Queuing Algorithms

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

- **Strict-Priority (SPQ)**
The packets on the high priority queue are always service firstly.
- **Weighted Fair Queuing (WFQ)**
WFQ is a data packet scheduling technique allowing different scheduling priorities to statistically multiplexed data flows. It provides traffic priority management that automatically sorts among individual traffic streams without requiring an access list. WFQ decides which queue is selected in one slot time to guarantee the minimal packet rate of one queue. Thus, WFQ allows Internet operators to define traffic classes and then assign different bandwidth proportions.
- **Weighted round robin (WRR)**
Round Robin scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

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

Default Settings

Qos mode : High First (SPQ)

The mappings of the Priority to Queue are:

PRI0 0 ==> COSQ 2
PRI0 1 ==> COSQ 0
PRI0 2 ==> COSQ 1
PRI0 3 ==> COSQ 3
PRI0 4 ==> COSQ 4
PRI0 5 ==> COSQ 5
PRI0 6 ==> COSQ 6
PRI0 7 ==> COSQ 7

6.1.1.2. CLI Configuration

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

6.1.1.3. Web Configuration

Port Priority

QoS

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

Port Priority Settings

All Ports 802.1p priority : - ▾

| Port | 802.1p priority | Port | 802.1p priority |
|------|-----------------|------|-----------------|
| 1 | 0 ▾ | 2 | 0 ▾ |
| 3 | 0 ▾ | 4 | 0 ▾ |
| 5 | 0 ▾ | 6 | 0 ▾ |

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

IP DiffServ(DSCP)

QoS

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

DSCP Settings

Mode Tag Over DSCP

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

Apply
Refresh

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

Priority/Queue Mapping

QoS

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

Priority/Queue Mapping Settings

Reset to default

| Priority | Queue ID |
|----------|----------|
| 0 | 1 |
| 1 | 0 |
| 2 | 2 |
| 3 | 3 |
| 4 | 4 |
| 5 | 5 |
| 6 | 6 |
| 7 | 7 |

Apply Refresh

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

Schedule Mode

QoS

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

Schedule Mode Settings

Schedule Mode: Strict Priority(SP) ▼

| Queue ID | Weight Value (Range:1~127) |
|----------|----------------------------|
| 0 | <input type="text"/> |
| 1 | <input type="text"/> |
| 2 | <input type="text"/> |
| 3 | <input type="text"/> |
| 4 | <input type="text"/> |
| 5 | <input type="text"/> |
| 6 | <input type="text"/> |
| 7 | <input type="text"/> |

Apply
Refresh

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

6.1.2. Rate Limitation

6.1.2.1. Storm Control

6.1.2.1.1. Introduction

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

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

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

Storm Control unit : pps.

Default Settings

Broadcast Storm Control : 300pps.

Multicast Storm Control : None.

DLF Storm Control : 300pps.

6.1.2.1.2. CLI Configuration

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

Example:

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

6.1.2.1.3. Web Configuration

Rate Limitation

Storm Control
Bandwidth Limitation

Storm Control Settings

| Port | Rate | Type |
|---|--|--|
| From: 1 To: 1 | <input style="width: 80%;" type="text" value="0"/> (pps) | Multicast |
| (Disable 0, Range 1~262143) | | |
| <input type="button" value="Apply"/> <input type="button" value="Refresh"/> | | |

Storm Control Status

| Port | Multicast Rate (pps) | Broadcast Rate (pps) | DLF Rate (pps) | Port | Multicast Rate (pps) | Broadcast Rate (pps) | DLF Rate (pps) |
|------|----------------------|----------------------|----------------|------|----------------------|----------------------|----------------|
| 1 | 0 | 300 | 300 | 2 | 0 | 300 | 300 |
| 3 | 0 | 300 | 300 | 4 | 0 | 300 | 300 |
| 5 | 0 | 300 | 300 | 6 | 0 | 300 | 300 |

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

6.1.2.2. Bandwidth Limitation

6.1.2.2.1. Introduction

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

Rate Limitation unit: Kbs.

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

6.1.2.2.2. CLI Configuration

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

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#bandwidth-limit egress 1 ports 1-6
L2SWITCH(config)#bandwidth-limit ingress 1 ports 1-6
```

6.1.2.2.3. Web Configuration

| Parameter | Description |
|-----------|---|
| Port | Selects a port that you want to configure. |
| Ingress | Configures the rate limitation for the ingress packets. |
| Egress | Configures the rate limitation for the egress packets. |

| | |
|---------|--|
| Apply | Click Apply to take effect the settings. |
| Refresh | Click Refresh to begin configuring this screen afresh. |

6.2. IGMP Snooping

6.2.1. IGMP Snooping

6.2.1.1. Introduction

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

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

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

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

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

Immediate Leave

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

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

Fast Leave

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

Last Member Query Interval

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

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

IGMP Querier

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

Port IGMP Querier Mode

- **Auto:**

The Switch uses the port as an IGMP query port if the port receives IGMP query packets.
- **Fixed:**

The Switch always treats the port(s) as IGMP query port(s). This is for when connecting an IGMP multicast server to the port(s).
The Switch always forwards the client's **report/leave** packets to the port.
Normally, the port is connected to an IGMP server.
- **Edge:**

The Switch does not use the port as an IGMP query port.
The IGMP query packets received by this port will be dropped.
Normally, the port is connected to an IGMP client.

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

Configurations:

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

Default Settings

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

Notices

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

6.2.1.2. CLI Configuration

| Node | Command | Description |
|-----------|---|---|
| enable | show igmp-snooping | This command displays the current IGMP snooping configurations. |
| enable | show igmp-counters | This command displays the current IGMP snooping counters. |
| enable | show igmp-counters (port vlan) | This command displays the current IGMP snooping counters per port or per vlan. |
| configure | igmp-snooping (disable enable) | This command disables / enables the IGMP snooping on the switch. |
| configure | igmp-snooping vlan VLANID | This command enables the IGMP snooping function on a VLAN or range of VLANs. |
| configure | no igmp-snooping vlan VLANID | This command disables the IGMP snooping function on a VLAN or range of VLANs. |
| configure | igmp-snooping unknown-multicast (drop flooding) | This command configures the process for unknown multicast packets when the IGMP snooping function is enabled. <i>drop</i> : 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)#interface 1/0/1
L2SWITCH(config-if)#igmp-immediate-leave
L2SWITCH(config-if)#igmp-querier-mode fixed
L2SWITCH(config-if)#igmp-snooping group-limit 20
```

6.2.1.3. Web Configuration

General Settings

IGMP Snooping

General Settings
Port Settings

IGMP Snooping Settings

IGMP Snooping State: Disable

IGMP Snooping VLAN State: Add

Unknown Multicast Packets: Drop

Apply Refresh

IGMP Snooping Status

| | |
|---------------------------|----------|
| IGMP Snooping State | Disabled |
| IGMP Snooping VLAN State | None |
| Unknown Multicast Packets | Drop |

| Parameter | Description |
|---------------------------|---|
| IGMP Snooping State | Select Enable to activate IGMP Snooping to forward group multicast traffic only to ports that are members of that group. Select Disable to deactivate the feature. |
| IGMP Snooping VLAN State | Select Add and enter VLANs upon which the Switch is to perform IGMP snooping. The valid range of VLAN IDs is between 1 and 4094. Use a comma (,) or hyphen (-) to specify more than one VLANs. Select Delete and enter VLANs on which to have the Switch not perform IGMP snooping. |
| Unknown Multicast Packets | Specify the action to perform when the Switch receives an unknown multicast frame. Select Drop to discard the frame(s). |

| | |
|---------------------------|---|
| | Select Flooding to send the frame(s) to all ports. |
| Apply | Click Apply to configure the settings. |
| Refresh | Click this to reset the fields to the last setting. |
| IGMP Snooping State | This field displays whether IGMP snooping is globally enabled or disabled. |
| IGMP Snooping VLAN State | This field displays VLANs on which the Switch is to perform IGMP snooping. None displays if you have not enabled IGMP snooping on any port yet. |
| Unknown Multicast Packets | This field displays whether the Switch is set to discard or flood unknown multicast packets. |

Port Settings



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

| | |
|-----------------|--|
| Apply | Click Apply to apply the settings. |
| Refresh | Click this to reset the fields. |
| Port | The port ID. |
| Querier Mode | The Querier mode setting for the specific port. |
| Immediate Leave | The Immediate Leave setting for the specific port. |
| Group Counts | The current joining group count and the maximum group count. |

6.2.2. Multicast Address

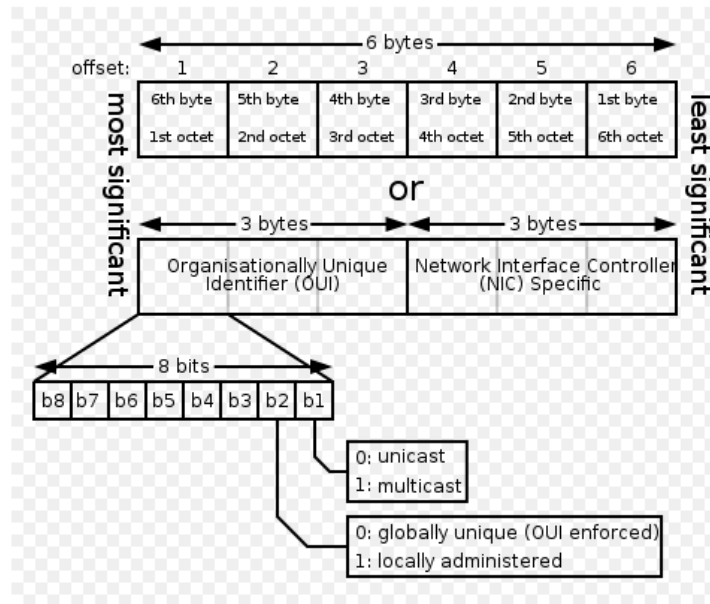
6.2.2.1. Introduction

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

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

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

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



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

| | |
|------------|------------------------------------|
| 224.0.1.39 | Cisco Auto-RP-Announce address |
| 224.0.1.40 | Cisco Auto-RP-Discovery address |
| 224.0.1.41 | H.323 Gatekeeper discovery address |

6.2.2.2. CLI Configuration

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

6.2.2.3. Web Configuration

Multicast Address

Static Multicast Address Settings

| VLAN ID | Group IP | Source IP | Port |
|------------------------------------|----------------------|----------------------|----------------------|
| 1 <input type="button" value="v"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

Multicast Address Table

| VLAN ID | Group IP | Source IP | Status | Port | Action |
|------------------|----------|-----------|--------|------|--------|
| Total counts : 0 | | | | | |

| Parameter | Description |
|-------------------------|--|
| VLAN ID | Configures the VLAN that you want to configure. |
| Group IP | Configures the multicast group IP. |
| Source IP | Configures the multicast server IP. |
| Port | Configures the member port for the multicast group. |
| Apply | Click Apply to save your changes back to the Switch. |
| Refresh | Click Refresh to begin configuring this screen afresh. |
| Multicast Address Table | |
| VLAN ID | The VLAN ID for the multicast group. |

| | |
|-----------|---|
| Group IP | The multicast group IP. |
| Source IP | The multicast server IP. |
| Status | The status of the multicast group. |
| Port | The member ports for the multicast group. |
| Action | Click the Delete button to delete this multicast group. |

6.3. VLAN

6.3.1. Port Isolation

6.3.1.1. Introduction

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

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

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

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

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

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

Default Settings

(Port-0=CPU).

| Port | Egress Port | Port | Egress Port |
|------|-------------|-------|-------------|
| ---- | ----- | ----- | ----- |
| 1 | VVVVVVV | 2 | VVVVVVV |

```

3      VVVVVVVV      4      VVVVVVVV
5      VVVVVVVV      6      VVVVVVVV
    
```

6.3.1.2. CLI Configuration

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

Example:

```

L2SWITCH(config)#interface 1/0/2
L2SWITCH(config-if)#port-isolation ports 3-5
    
```

6.3.1.3. Web Configuration

Port Isolation

Port Isolation Settings

Port From: To:

Egress Port:

Select All Deselect All

1 2 3 4 5 6 0 (CPU)

Port Isolation Status

| Port | Egress Port | | | | | | |
|------|-------------|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | v | v | v | v | v | v | v |
| 2 | v | v | v | v | v | v | v |
| 3 | v | v | v | v | v | v | v |
| 4 | v | v | v | v | v | v | v |
| 5 | v | v | v | v | v | v | v |
| 6 | 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 setting. |
| Port Isolation Status | “V” indicates the port’s packets can be sent to that port. “-” indicates the port’s packets cannot be sent to that port. |

6.3.2. 802.1Q VLAN

6.3.2.1. Introduction

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

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

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

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

VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

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

- **Forwarding Tagged and Untagged Frames**

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

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

- **802.1Q Port base VLAN**

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

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

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

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

Default Settings

The default PVID is 1 for all ports.

The default Acceptable Frame is All for all ports.

All ports join in the VLAN 1.

6.3.2.2. CLI Configuration

| Node | Command | Description |
|-----------|---|---|
| enable | show vlan VLANID | This command displays the VLAN configurations. |
| configure | vlan <1~4094> | This command enables a VLAN and enters the VLAN node. |
| configure | no vlan <1~4094> | This command deletes a VLAN. |
| vlan | show | This command displays the current VLAN configurations. |
| vlan | name STRING | This command assigns a name for the specific VLAN. The VLAN name should be the combination of the digit or the alphabet or hyphens (-) or underscores (_). The maximum length of the name is 16 characters. |
| vlan | no name | This command configures the vlan name to default. Note: The default vlan name is "VLAN"+vlan_ID, VLAN1, VLAN2,... |
| vlan | fixed PORT_LIST | This command assigns ports for permanent member of the VLAN group. |
| vlan | no fixed | This command removes all fixed member from the vlan. |
| vlan | tagged PORT_LIST | This command assigns ports for tagged member of the VLAN group. The ports should be one/some of the permanent members of the vlan group. |
| vlan | no tagged | This command removes all tagged member from the vlan. |
| 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 | no untagged | This command removes all untagged member from the vlan. |
| vlan | acceptable frame type (all tagged untagged) | This command configures the acceptable frame type. all – acceptable all frame types. |
| interface | pvid VLANID | This command configures a VLAN ID for the port default VLAN ID. |
| interface | no pvid | This command configures 1 for the port default VLAN ID. |

Example:

```
L2SWITCH#configure terminal
L2SWITCH(config)#vlan 2
L2SWITCH(config-vlan)#fixed 1-5
L2SWITCH(config-vlan)#untagged 1-3
```

6.3.2.3. Web Configuration

VLAN Settings

VLAN

VLAN Settings
Tag Settings
Port Settings

VLAN Settings

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

VLAN List

| VLAN ID | VLAN Name | VLAN Status | Member Port | Action |
|---------|-----------|-------------|-------------|--------|
| 1 | VLAN1 | Static | 1-6 | |

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

Tag Settings

VLAN

VLAN Settings
Tag Settings
Port Settings

Tag Settings

VLAN ID None ▼

Tag Port :

Select All Deselect All

1 2 3 4 5 6

Tag Status

| VLAN ID | Tag Ports | UnTag Ports |
|---------|-----------|-------------|
| 1 | | 1-6 |

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

Port Settings

VLAN

VLAN Settings
Tag Settings
Port Settings

Port Settings

| Port | PVID | Acceptable Frame |
|---|---|---|
| From: <input style="width: 30px;" type="text" value="1"/> To: <input style="width: 30px;" type="text" value="1"/> | <input style="width: 30px;" type="text" value="1"/> | <input style="width: 60px;" type="text" value="All"/> |
| <input type="button" value="Apply"/> <input type="button" value="Refresh"/> | | |

Port Status

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

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

6.3.3. MAC-based VLAN

6.3.3.1. Introduction

The MAC base VLAN allows users to create VLAN with MAC address. The MAC address can be the leading three or more bytes of the MAC address.

For example, 00:0b:04 or 00:03:04:05 or 00:01:02:03:04:05.

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

For example:

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

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

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

6.3.3.2. CLI Configuration

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

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

For example:

00:0B:04

00:0B:04:11

00:0B:04:11:22

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

Example:

```
L2SWITCH(config)#vlan 22
```

```
L2SWITCH(config-vlan)#fixed 1-4
```

```
L2SWITCH(config-vlan)#exit
```

```
L2SWITCH(config)#mac-vlan 00:0B:04:11:22 vlan 22 priority 1
```

6.3.3.3. Web Configuration

MAC VLAN

MAC VLAN Settings

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

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

MAC VLAN Table

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

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

6.4. EEE (Energy Efficient Ethernet)

6.4.1. Introduction

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

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

Notice: This feature is for Ethernet copper ports only.

Default Settings

All ports' EEE states are disabled.

6.4.2. CLI Configuration

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

Example:

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

6.4.3. Web Configuration

Energy Efficient Ethernet

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

6.5. Link Layer Discovery Protocol (LLDP)

6.5.1. Introduction

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

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

Default Settings

The LLDP on the Switch is disabled.

Tx Interval : 30 seconds.
 Tx Hold : 4 times.
 Time To Live : 120 seconds.

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

6.5.2. CLI Configuration

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

| | | |
|--|--|-------|
| | | port. |
|--|--|-------|

6.5.1. Web Configuration

LLDP

Settings
Neighbor

LLDP Settings

State Disable ▾

Tx Interval 30 seconds

Tx Hold 4 times

Time To Live 120 seconds

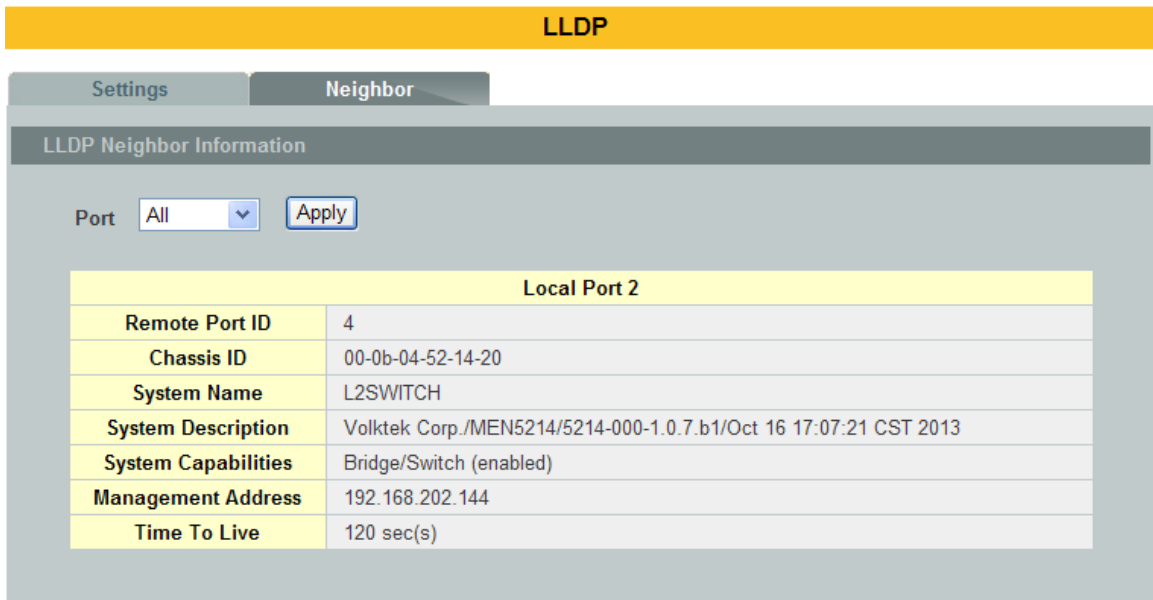
| Port | State |
|-------------------|----------|
| From: 1 ▾ To: 1 ▾ | Enable ▾ |

Apply
Refresh

LLDP Status

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

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



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

6.6. Spanning Tree Protocol (STP/RSTP)

6.6.1. Introduction

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

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

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

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

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

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

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

STP Terminology

- The root bridge is the base of the spanning tree.
- Path cost is the cost of transmitting a frame onto a LAN through that port. There commended 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 30seconds.

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.

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.

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 IEEEStandard802.1D. 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 Non root-bridge to Root bridge
- Designated - A forwarding port for every LAN segment
- Alternate - An alternate path to the root bridge. This path is different than using the root port.
- Backup - A backup/redundant path to a segment where another bridge port already connects.
- Disabled - Not strictly part of STP, a network administrator can manually disable a port

Edge Port:

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

Forward Delay:

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

Transmission Limit:

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

Hello Time:

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

Bridge priority:

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

Port Priority:

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

Path Cost:

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

BPDU Guard

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

BPDU Filter

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

Notice:

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

Root Guard

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

Default Settings

| | |
|---------------|---------------|
| STP/RSTP | : disabled. |
| STP/RSTP mode | : RSTP. |
| Forward Time | : 15 seconds. |
| Hello Time | : 2 seconds. |

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

6.6.2. CLI Configuration

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

| | | |
|-----------|--|--|
| configure | no spanning-tree hello-time | This command configures the default values for hello-time. |
| configure | spanning-tree max-age <6-40> | This command configures the bridge message max-age time (sec). |
| configure | no spanning-tree max-age | This command configures the default values for max-age time. |
| configure | spanning-tree mode (rstp stp) | This command configures the spanning mode. |
| configure | spanning-tree pathcost method (short long) | This command configures the path cost method. |
| configure | spanning-tree priority<0-61440> | This command configures the priority for the system. |
| configure | no spanning-tree priority | This command configures the default values for the system priority. |
| interface | spanning-tree (disable enable) | This command configures enables/disables the STP functions for the specific port. |
| interface | spanning-tree bpdudfilter(disable enable) | This command configures enables/disables the bpdudfilter function for the specific port. |
| interface | spanning-tree bpduguard (disable enable) | This command configures enables/disables the bpduguard functions for the specific port. |
| interface | spanning-tree rootguard (disable enable) | This command enables/disables the BPDU Root guard port setting for the specific port. |
| interface | spanning-tree edge-port (disable enable) | This command enables/disables the edge port setting for the specific port. |
| interface | spanning-tree cost VALUE | This command configures the cost for the specific port. 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. |
| configure | interface range gigabitethernet1/0/ PORTLISTS | This command enters the interface configure node. |
| if-range | spanning-tree (disable enable) | This command configures enables/disables the STP functions for |

| | | |
|----------|---|--|
| | | the specific port. |
| if-range | spanning-tree bpdupfilter (disable enable) | This command configures enables/disables the bpdu filter function for the specific port. |
| if-range | spanning-tree bpduguard (disable enable) | This command configures enables/disables the bpdu guard functions for the specific port. |
| if-range | spanning-tree rootguard (disable enable) | This command enables/disables the BPDU Root guard port setting for the specific port. |
| if-range | spanning-tree edge-port (disable enable) | This command enables/disables the edge port setting for the specific port. |
| if-range | spanning-tree cost VALUE | This command configures the cost for the specific port. Cost range: 16-bit based value range 1-65535, 32-bit based value range 1-200000000. |
| if-range | no spanning-tree cost | This command configures the path cost to default for the specific port. |
| if-range | spanning-tree port-priority<0-240> | This command configures the port priority for the specific port. Default: 128. |
| if-range | no spanning-tree port-priority | This command configures the port priority to default for the specific port. |

6.6.3. Web Configuration

General Settings

Spanning Tree Protocol

General Settings
Port Parameters
STP Status

Spanning Tree Protocol Settings

State

Mode

Bridge Parameters

Forward Delay (Range:4-30)

Max Age (Range:6-40) Relationships:
 $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$
 $\text{Max Age} \geq 2 * (\text{Hello Time} + 1)$

Hello Time (Range:1-10)

Priority (Range:0-61440)

Pathcost Method

| 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 30seconds. |
| 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, anew 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 |

| | |
|-----------|---|
| | <p>switch with the lowest MAC address will then become the root switch. Enter a value from 0~61440.</p> <p>The lower the numeric value you assign, the higher the priority for this bridge.</p> <p>Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay.</p> |
| Path cost | <p>Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost.</p> |

Port Parameters

Spanning Tree Protocol

General Settings
Port Parameters
STP Status

Port Parameters Settings

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

Port Status

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

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

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

STP Status

Spanning Tree Protocol

General Settings
Port Parameters
STP Status

Current Root Status

| MAC Address | Priority | Max Age | Hello Time | Forward Delay |
|-------------------|----------|---------|------------|---------------|
| 00:03:09:02:08:18 | 32768 | 20 | 2 | 15 |

Current Bridge Status

| MAC Address | Priority | Max Age | Hello Time | Forward Delay | Path Cost | Root Port |
|-------------------|----------|---------|------------|---------------|-----------|-----------|
| 00:03:09:02:08:18 | 32768 | 20 | 2 | 15 | 0 | 0 |

| 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 | <p>Priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch.</p> <p>Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay.</p> |
| MAX Age | <p>This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals.</p> <p>Any port 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.</p> |
| 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. |

7. Monitor

7.1. Alarm

7.1.1. Introduction

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

Notice:

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

For Example:

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

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

7.1.2. CLI Configuration

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

7.1.3. Web Configuration

Alarm Information

Alarm Information

| | |
|------------------------|---------------|
| Alarm Status | Alarm! |
| Alarm Reason(s) | No PWR input. |

Alarm DIP Switch Settings:

| DIP Switch | Status | DIP Switch | Status |
|------------|--------|------------|---------|
| PWR | Enable | RPS | Disable |

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

7.2. Port Statistic

7.2.1. Introduction

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

7.2.2. CLI Configuration

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

Example:

```
L2SWITCH#show port-statistics
```

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

7.2.3. Web Configuration

Port Statistics

Port Statistics

| Port | Transmit Drops | Receive Drops | Transmit Errors | Receive Errors | Transmit Packets | Receive Packets | Transmit Bytes | Receive Bytes |
|------|----------------|---------------|-----------------|----------------|------------------|-----------------|----------------|---------------|
| 4 | 0 | 0 | 0 | 0 | 482 | 250 | 63744 | 46402 |

| Parameter | Description |
|------------|--|
| Port | Select a port or a range of ports to display their statistics. |
| Rx Packets | The field displays the received packet count. |
| Tx Packets | The field displays the transmitted packet count. |
| Rx Bytes | The field displays the received byte count. |
| Tx Bytes | The field displays the transmitted byte count. |
| Rx Errors | The field displays the received error count. |
| Tx Errors | The field displays the transmitted error count. |
| Rx Drops | The field displays the received drop count. |
| Tx Drops | The field displays the transmitted drop count. |
| Refresh | Click this button to refresh the screen quickly. |

7.3. Port Utilization

7.3.1. Introduction

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

7.3.2. CLI Configuration

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

7.3.3. Web Configuration

Port Utilization

Port Traffic Utilization Status

| Port | Speed | Traffic Utilization (%) |
|------|-------|-------------------------|
| 1 | 1000 | 0.001 |

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

7.4. RMON Statistics

7.4.1. Introduction

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

7.4.2. CLI Configuration

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

7.4.3. Web Configuration

RMON Statistics

RMON Statistics

Port

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

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

7.5. Traffic Monitor

7.5.1. Introduction

The function can be enabled / disabled on a specific port or globally be enabled disabled on the Switch. The function will monitor the broadcast / multicast / broadcast and multicast packets rate. If the packet rate is over the user's specification, the port will be blocked. And if the recovery function is enabled, the port will be enabled after recovery time.

Default Settings

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

7.5.2. CLI Configuration

| Node | Command | Description |
|-----------|--|---|
| enable | show traffic-monitor | This command displays the traffic monitor configurations and current status. |
| configure | traffic-monitor (disable enable) | This command enables / disables the traffic monitor on the Switch. |
| interface | traffic-monitor rate RATE_LIMIT type (bcast mcast bcast+mcast) | This command configures the packet rate and packet type for the traffic monitor on the specific port. bcast – Broadcast packet. mcast – Multicast packet. |
| interface | traffic-monitor (disable enable) | This command enables / disables the traffic monitor on the specific port. |
| interface | traffic-monitor recovery (disable enable) | This command enables / disables the recovery function for the traffic monitor on the specific port. |
| interface | traffic-monitor recovery time VALUE | This command configures the recovery time for the traffic monitor on the specific port. |

7.5.3. Web Configuration

Traffic Monitor

Traffic Monitor Settings

State: Disable ▾

| Port | State | Action | Packet Type | Packet Rate(pps) | Recovery State | Recovery Time (min) | |
|---|---|---|--|---|---|--|---|
| From: 1 ▾ | To: 1 ▾ | Disable ▾ | None ▾ | Broadcast ▾ | 100 | Enable ▾ | 1 |

Apply
Refresh

Traffic Monitor Status

| Port | State | Status | Packet Type | Packet Rate(pps) | Recovery State | Recovery Time (min) |
|------|----------|--------|-------------|------------------|----------------|---------------------|
| 1 | Disabled | Normal | Broadcast | 100 | Enabled | 1 |
| 2 | Disabled | Normal | Broadcast | 100 | Enabled | 1 |
| 3 | Disabled | Normal | Broadcast | 100 | Enabled | 1 |
| 4 | Disabled | Normal | Broadcast | 100 | Enabled | 1 |
| 5 | Disabled | Normal | Broadcast | 100 | Enabled | 1 |
| 6 | Disabled | Normal | Broadcast | 100 | Enabled | 1 |

| Parameter | Description |
|---------------|--|
| State | Globally enables / disables the traffic monitor function. |
| Port | The port range which you want to configure. |
| State | Enables / disables the traffic monitor function on these ports. |
| Action | Unblock these ports. |
| Packet Type | Specify the packet type which you want to monitor. |
| Packet Rate | Specify the packet rate which you want to monitor. |
| Recover State | Enables / disables the recovery function for the traffic monitor function on these ports. |
| Recovery Time | Configures the recovery time for the traffic monitor function on these ports.(Range: 1 – 60 minutes) |

8. Management

8.1. SNMP

8.1.1. SNMP

8.1.1.1. Introduction

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

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

Support below MIBs:

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

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

Network ID of Trusted Host:

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

Network ID = (Host IP & Mask).

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

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

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

Default Settings

- SNMP : disabled.
- System Location : L2SWITCH. (Maximum length 64 characters)
- System Contact : None. (Maximum length 64 characters)
- System Name : None. (Maximum length 64characters)
- Trap Receiver : None.

- Community Name : None.
- The maximum entry for community : 3.
- The maximum entry for trap receiver : 5.

8.1.1.2. CLI Configuration

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

Example:

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

8.1.1.3. Web Configuration

SNMP Setting:

SNMP

SNMP Settings
Community Name

SNMP Settings

SNMP State:

System Name:

System Location:

System Contact:

| Parameter | Description |
|-----------------|--|
| SNMP State | Select Enable to activate SNMP on the Switch. Select Disable to not use SNMP on the Switch. |
| System Name | Type a System Name for the Switch. (The System Name is same as the host name) |
| System Location | Type a System Location for the Switch. |
| System Contact | Type a System Contact for the Switch. |
| Apply | Click Apply to configure the settings. |
| Refresh | Click this button to reset the fields to the last setting. |

Community Name:

SNMP

SNMP Settings
Community Name

Community Name Settings

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

Community Name List

| No. | Community String | Rights | Network ID of Trusted Host | Mask | Action |
|-----|------------------|-----------|----------------------------|---------------|---------------------------------------|
| 1 | public | Read-Only | 192.168.202.0 | 255.255.255.0 | <input type="button" value="Delete"/> |

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

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

8.1.2. SNMP Trap Receiver

SNMP

Trap Receiver Settings

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

Trap Receiver List

| No. | IP Address | Version | Community String | Action |
|-------------------|-----------------|---------|------------------|---------------------------------------|
| 1 | 192.168.202.188 | v2c | public | <input type="button" value="Delete"/> |

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

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

8.2. Mail Alarm

8.2.1. Introduction

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

The events are listed below:

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

Default Settings

Mail-Alarm Configuration:

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

Trap Event Status:

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

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

8.2.2. Reference

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

8.2.3. CLI Configuration

| Node | Command | Description |
|-----------|-----------------------------|--|
| enable | show mail-alarm | This command displays the Mail Alarm configurations. |
| configure | mail-alarm (disable enable) | This command disables / enables the Mail Alarm function. |

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

8.2.4. Web Configuration

Mail Alarm

Mail Alarm Settings

State: ▾

Server IP: Server Port: (Default:25)

Account Name: Account Password:

Mail From:

Mail To:

Trap State :

Select All Deselect All

System Reboot Port Link Change Configuration Change Firmware Upgrade User Login

Port Blocked Alarm

| Parameter | Description |
|------------------|---|
| State | Enable / disable the Mail Alarm function. |
| Server IP | Specifies the mail server's IP address. |
| Server Port | Specifies the TCP port for the SMTP. |
| Account Name | Specifies the mail account name. |
| Account Password | Specifies the mail account password. |
| Mail From | Specifies the mail sender. |

| | |
|------------|--|
| Mail To | Specifies the mail receiver. |
| Trap State | Enables / disables the mail trap event states. |

8.3. Maintenance

8.3.1. Configuration

8.3.1.1. CLI Configuration

| Node | Command | Description |
|-----------|--|---|
| enable | show config-change-status | This command displays the configurations status if there are default values. |
| configure | reboot | This command reboots the system. |
| configure | reload default-config | This command copies a default-config file to replace the current one. 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 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 |
| configure | archive upload-config <URL PATH> | This command uploads the current configurations file to a TFTP server. |

Example:

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

Enable the DHCP client function for the switch.

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

8.3.1.2. Web Configuration

Maintenance

Configuration **Firmware** **Reboot**

Save Configurations

Save the parameter settings of the Switch :

Upload and Download Configurations

Upload configuration file to your Switch.
File path No file chosen

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

Reset Configurations

Reset the factory default settings of the Switch :
- IP address will be 192.168.0.254

Save Configurations

Save Configurations

Save the parameter settings of the Switch :

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

Upload / Download Configurations to /from a your server

Upload and Download Configurations

Upload configuration file to your Switch.
File path No file chosen

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

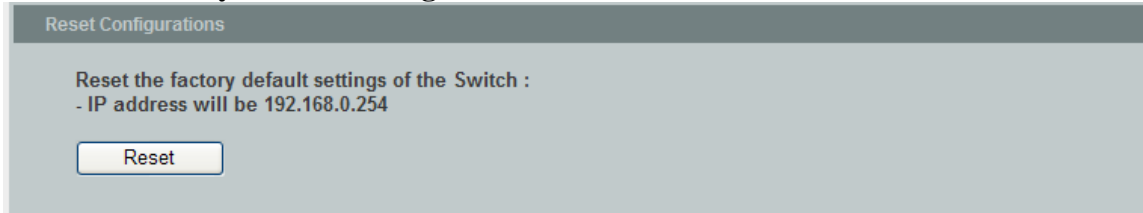
Follow the steps below to save the configuration file to your PC.

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

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

- Select the “Upload configurations file to your Switch”.
- Select the full path to your configuration file.
- Click the Upload button to start the process.

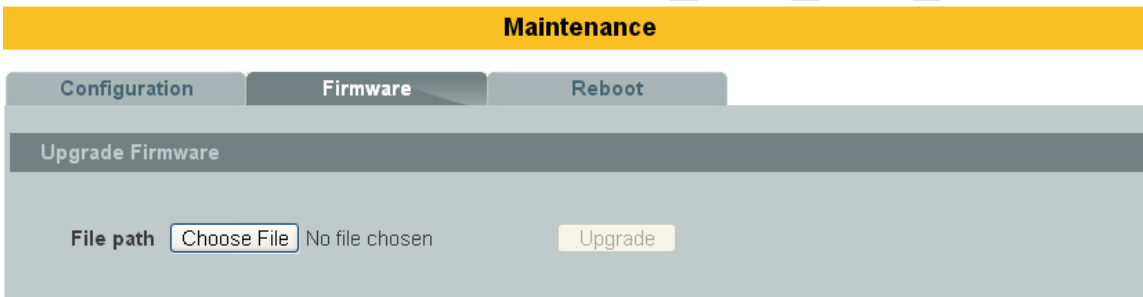
Reset the factory default settings of the Switch



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

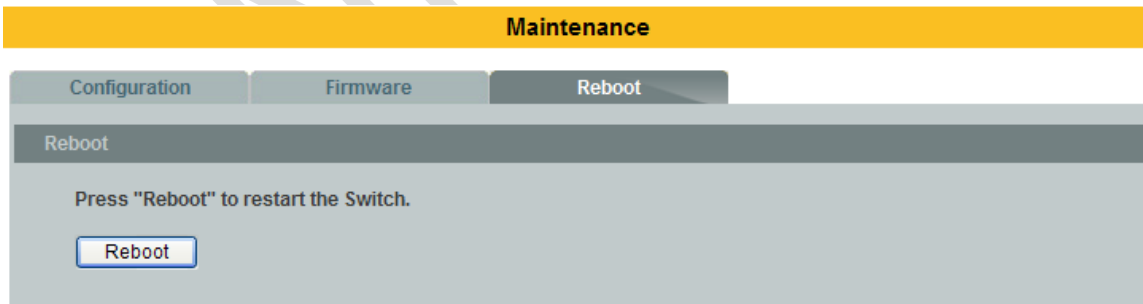
8.3.2. Firmware

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

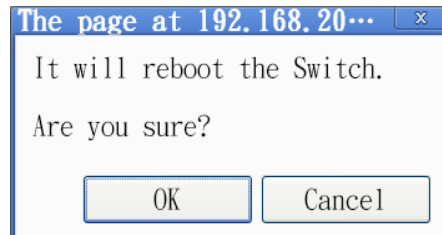


8.3.3. Reboot

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



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



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

8.4. System log

8.4.1. Introduction

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

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

8.4.2. CLI Configuration

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

Example:

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

8.4.3. Web Configuration

System Log

Syslog Server Setting

Server IP

System Log

Log Level

No data.

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

8.5. User Account

8.5.1. Introduction

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

User Authority:

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

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

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

Default Settings

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

Notices

The Switch allows users to create up to 6 user account.
The user name and the password should be the combination of the digit or the alphabet.
The last admin user account cannot be deleted.
The maximum length of the username and password is 32 characters.

8.5.2. CLI Configuration

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

Example:

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

8.5.3. Web Configuration

User Account

User Account Settings

User Name

User Password

User Authority Normal ▾

User Account List

| No. | Name | Authority | Action |
|-----|-------|-----------|--------|
| 1 | admin | admin | |

| 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 relate to the INS-8615 or any other Volktek product, please contact Volktek customer support:

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

ISO 9001 Certified

CONFIDENTIAL