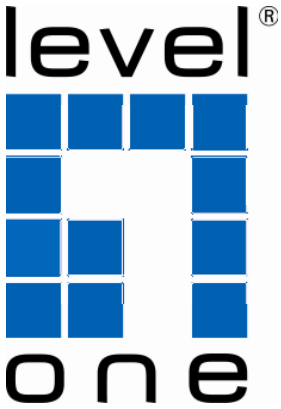


MSL-3S79

3-Slot Gigabit Modular L2 Managed Switch

User Manual

V1.0

FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential 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 communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

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.

Content

Chapter 1 Introduction

The MSL-3S79 is a modular switch that can be used to build high-performance switched workgroup networks. This switch is a store-and-forward device that offers low latency for high-speed networking. The Switch is targeted at workgroup, department or backbone computing environment.

The MSL-3S79 features a “store-and-forward” switching scheme. This allows the switch to auto-learn and store source address in an 16K-entry MAC address table.

MDI (Medium Dependent Interface) Port is also called an "uplink port". The MDI port does not cross transmit and receive lines, which is done by the regular ports (MDI-X ports) that connect to end stations. In general, MDI means connecting to another Hub or Switch while MDIX means connecting to a workstation or PC. Therefore, Auto MDI/MDIX means that you can connect to another Switch or workstation without changing non-crossover or crossover cabling.

The MSL-3S79 has 3-module slot. User can purchase the modules in accordance with their needs as well as giving elasticity on network application.

1.1 Hardware Features

Standards	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3z Gigabit fiber IEEE 802.3ab 1000Base-T IEEE 802.3x Flow control and Back pressure IEEE 802.3ad Port trunk with LACP IEEE 802.1d Spanning tree protocol IEEE 802.1w Rapid spanning tree IEEE 802.1p Class of service IEEE 802.1q VLAN Tagging IEEE 802.1x User authentication IEEE 802.1ab LLDP
LED Indicators	System Power 10/100/1000TX module: Link/Activity, 1000/100/10Mbps speed 8 Port Gigabit Fiber module: Link/Activity 8 Port MINI GBIC: Link/Activity 4 Port Gigabit copper + 4 Port MINI GBIC module: RJ-45 (Link/Activity, 1000/100/10Mbps speed), MINI GBIC (Link/Activity)
Connector	RS-232 console: Female DB-9 Gigabit copper module: 8 x RJ-45 MINI GBIC module: 8 x MINI GBIC socket Gigabit Fiber module: 8 x SC for Gigabit SX or LX 4 Gigabit Copper & 4 MINI GBIC module: 4 x RJ-45 + 4 x 3.3v MINI GBIC Socket
Switch architecture	Store and forward switch architecture with Back-plane up to

	48Gbps.
Packet buffer	6Mbits
Dimensions	440mm(W) x 280mm(D) x 44mm(H)
MAC Address	16K
Storage Temp.	-40℃~70℃, 5%~95%RH
Operational Temp.	0℃~45℃, 5%~95%RH
Power Supply	AC 100~240V 50/60Hz, Redundant Power: DC 12~48V
Power Consumption	35 Watts
Ventilation	2 fan at the rear
EMI	Compliance with FCC Class A, CE
Safety	Compliance with UL, cUL, CE/EN60950-1

1.2 Software Feature

Management	SNMP v1/v2c, Telnet, RMON1, CLI and Web management.
MIB	RFC 2863 Interface Group MIB, RFC 1213 MIBII, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC 1643 Ethernet Like MIB, RFC 1215 Trap MIB, RFC 1757 RMON MIB, Private MIB
SNMP Trap	Cold start/Warm start trap, Link down/Link up trap, Authentication fail trap,
Firmware Upgrade	TFTP
Configuration upload and download	System quick installation and backup by TFTP
Port Trunk	Support IEEE802.3ad with LACP function. Up to 7 trunk groups with failover feature and the member up to 8 ports.
Spanning Tree	IEEE802.1w Rapid spanning tree (Compatible with STP)

VLAN	Port based VLAN, up to 24 groups IEEE802.1Q Tag VLAN Static VLAN groups up to 256 entries and dynamic VLAN groups up to 2048, the VLAN ID can be assigned from 1 to 4094. GVRP
Class of Service	Per port 8 priority queues and support strict and WRR priority rule. Weight round ratio (WRR):1:2:3:4:5:6:7:8 Weight round ratio (WRR):1:1:2:2:3:3:4:4 Weight round ratio (WRR):1:1:2:2:4:4:8:8
Quality of service	Port based, Tag based, IPv4 Type of service, IPv4 Different service.
IGMP	IGMP v1, v2 Supports 256 multicast groups and IGMP query
Port Security	Support 128 entries of MAC address for static MAC and another 128 for MAC filter
Port Mirror	Supports 3 mirroring types: “RX, TX and Both packet”.
Bandwidth Control	Per port support ingress rate limiting and egress rate shaping control.
Access security	IP Management Security: Support IP addresses security to prevent unauthorized intruder.
802.1x Authentication	Support IEEE802.1x User-Authentication and can report to RADIUS server. ● Reject ● Accept ● Authorize

	● Disable
Access Control List	The system provides control list on Source IP & Destination IP.
DHCP	DHCP Client and DHCP Server
DNS	Provide DNS client feature and support Primary and Secondary DNS server.
System log	1000 records (Maximum) Provide remote storage ability and also can view the log by Web/Telnet/SNMP interface.
SNTP	Support RFC 2030 SNTP client.
SMTP	System supports 5 mail accounts and 2 Mail servers for Primary and Secondary. The SMTP will auto send event message to supervisor whom is pre-defined in the SMTP system through the pre-defined mail server.
Packet filter	Broadcast storm control
LLDP	Support IEEE 802.1ab Link Layer Discovery Protocol

1.3 Package Contents

Unpack the contents of the MSL-3S79 and verify them against the checklist below.

- ■ One MSL-3S79
- ■ Four Rubber Feet

- Power Cord
- Rack-mounted kit
- RS-232 Cable
- CD Manual

Compare the contents of your MSL-3S79 package with the standard checklist above. IF any item is missing or damaged, please contact your local dealer for service.

Chapter 2 Hardware Description

This section mainly describes the hardware of the MSL-3S79.

2.1 Physical Dimension

The physical dimensions of the MSL-3S79 is 440mm(W) x 280mm(D) x 44mm(H)

2.2 LED Indicators

The LED Indicators gives real-time information of systematic operation status. The LED indicators are located in every module. The LED indicators will be different for different module. The following table provides descriptions of LED status and their meaning.

- **8-port 1000Base-T module**

LED	Status	Meaning
1000/100	Green	Link on 1000Mbps speed mode
	Amber	Link on 100Mbps speed mode
	Off	Link on 10Mbps speed mode or No device attached

LK/ACT	Green	Ethernet Link connected
	Blink	The port is receiving or transmitting data.
	Off	No device attached or Link is disconnected

■ **4-port 1000Base-T + 4-port Mini GBIC module**

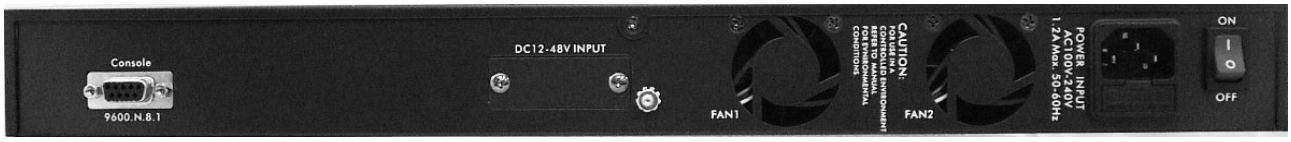
LED	Status	Meaning
Gigabit Copper		
1000/100	Green	Link on 1000Mbps mode
	Amber	Link on 100Mbps speed mode
	Off	Link on 10Mbps speed mode or No device attached
LK/ACT	Green	Ethernet Link is connected
	Blink	The port is receiving or transmitting data.
	Off	No device attached or Link is disconnected
Mini GBIC		
LK/ACT	Green	Link is connected
	Blink	The port is receiving or transmitting data.
	Off	No device attached or Link is disconnected

- **8-port Mini GBIC module**

LED	Status	Meaning
LNK/ACT	Green	Link connected
	Blink	The port is receiving or transmitting data.
	Off	No device attached or Link is disconnected

2.3 Rear Panel

The 3-pronged power plug is located at the Rear Panel of the MSL-3S79 as shown in figure. The Switches will work with AC in the range 100-240V AC, 50-60Hz. The DC redundant power jack is optional.



Rear Panel of the MSL-3S79

Chapter 3 Hardware Installation

3.1 Desktop Installation

Set the switch on a sufficiently large flat space with a power outlet nearby. The surface where you put your Switch should be clean, smooth, level, and sturdy. Make sure there is enough clearance around the Switch to allow attachment of cables, power cord and air circulation.

Attaching Rubber Feet

1. Make sure mounting surface on the bottom of the Switch is grease and dust free.
2. Remove adhesive backing from your Rubber Feet.
3. Apply the Rubber Feet to each corner on the bottom of the Switch. These footpads can prevent the Switch from shock/vibration.

3.2 Rack-mounted Installation

The switch come with a rack-mounted kid and can be mounted in an EIA standard size, 19-inch Rack. The Switch can be placed in a wiring closet with other equipment.

Perform the following steps to rack mount the switch:

A. Position one bracket to align with the holes on one side of the switch and secure it with the smaller bracket screws. Then attach the remaining bracket to the other side of the Switch.

B. After attaching both mounting brackets, position the switch in the rack by lining up the holes in the brackets with the appropriate holes on the rack. Secure the Switch to the rack with a screwdriver and the rack-mounting screws.

   Note: For proper ventilation, allow about at least 4 inches (10 cm) of clearance on the front and 3.4 inches (8 cm) on the back of the Switch. This is especially important for enclosed rack installation.

3.3 Power On

Connect the power cord to the power socket at the rear panel of the Switch. The other side of power cord connects to the power outlet. The internal power can work with AC in the voltage range of 100-240VAC/ frequency 50~60Hz or 12-48VDC (It’s optional). Besides, The AC and DC input can be used for redundant power supply. When one fails, another one is able to keep providing power to the switch. Check the power indicator on the front panel to see if power is properly supplied.

Chapter 4 Network Application

This section provides you a few samples of network topology in which the switch is used. In general, the MSL-3S79 is designed as a segment switch. That is, with its large address table (16K MAC address) and high performance, it is ideal for interconnecting networking segments.

PC, workstations, and servers can communicate each other by directly connecting with MSL-3S79. The switch automatically learns nodes address, which are subsequently used to filter and forward all traffic based on the destination address.

.

By using Gigabit or Gigabit Fiber, the switch can connect with another switch or hub to interconnect other small-switched workgroups to form a larger switched network. Meanwhile, you can also use Ethernet or Gigabit fiber ports to connect switches.

4.1 Desktop Application

The MSL-3S79 is designed to be a switch that is an ideal solution for small workgroup. The Switch can be used as a standalone switch to which personal computers, server, printer server are directly connected to form small workgroup.

4.2 Segment Application

For enterprise networks where large data broadcast are constantly processed, this switch is suitable for department user to connect to the corporate backbone.

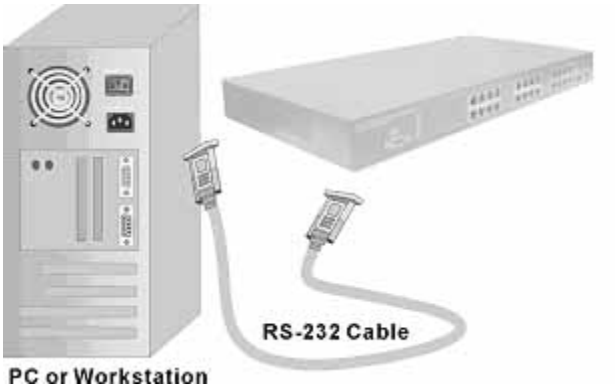
You can use the MSL-3S79 to connect PCs, workstations, and servers to each other. All the devices in this network can communicate with each other by connecting directly to the Switch. Connecting servers to the backbone switch allow other users to access the server’s data.

The switch automatically learns node address, which are subsequently used to filter and forward all traffic based on the destination address. You can use any of the RJ-45 port of the MSL-3S79 to connect with another Switch or Hub to interconnect each of your small-switched workgroups to form a larger switched network.

Chapter 5 Console Management

5.1 Connecting to the Console Port

The Console port is a female DB-9 connector that enables a connection to a PC or terminal for monitoring and configuring the Switch. Use the supplied RS-232 cable with a male DB-9 connector to connect a terminal or PC to the Console port.

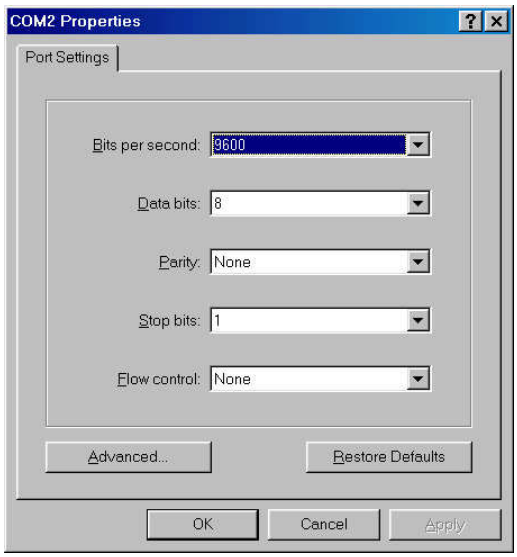


Connecting the switch to a terminal via RS-232 cable

5.2 Login in the Console Interface

When the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program or **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

Baud Rate: 9600 bps
Data Bits: 8
Parity: none
Stop Bit: 1
Flow control: None

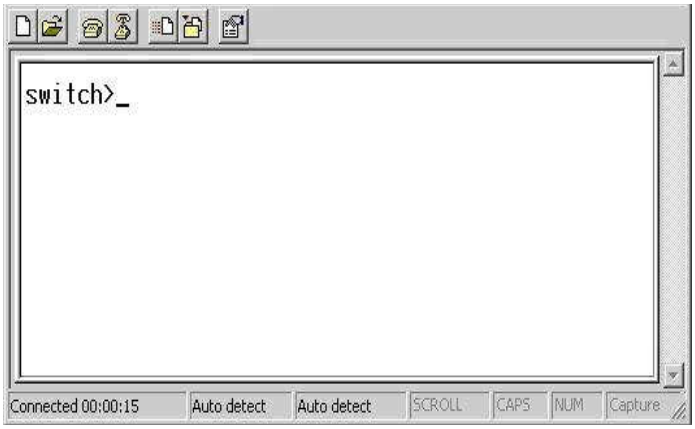


The settings of communication parameters

After finishing the parameter settings, click "**OK**". When the blank screen shows up, press **Enter** key to get into command line mode. Please see below figure for login screen.

5.3 CLI Management

The system supports console management (CLI command). After you login to the system, you will see a command prompt. To enter CLI management interface, enter "**enable**" or "**e**" command.



CLI command interface

Chapter 6 Web-Based Management

This section introduces the configuration and functions of the Web-Based management.

6.1 About Web-based Management

On CPU board of the switch there is an embedded HTML web site residing in flash memory, which offers advanced management features and allow users to manage the switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 5.0 or later. And, it is applied for Java Applets for reducing network bandwidth consumption, enhance access speed and present an easy viewing screen.

[NOTE] By default, IE5.0 or later version does not allow Java Applets to activate sockets. In fact, the user has to explicitly modify the browser setting to enable Java Applets to operate network ports.

6.2 Preparing for Web Management

Before using web management, install the industrial switch on the network and make sure that any one of PC on the network can connect with the industrial switch through the web browser. The switch default value of IP, subnet mask, username and password is as below:

- IP Address: **192.168.1.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.1.254**
- User Name: **admin**
- Password: **admin**

6.3 System Login

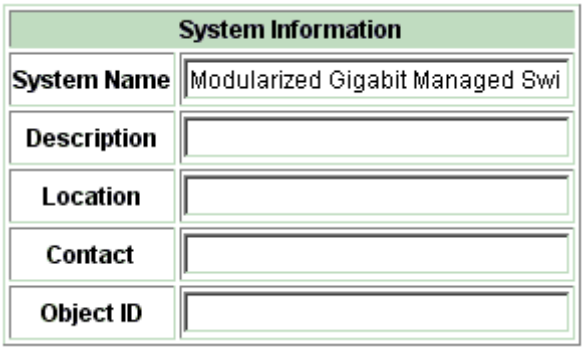
1. Launch the Internet Explorer on the PC
2. Key in “http:// “+” the IP address of the switch”, and then Press “**Enter**”.
3. The login screen will appear right after
4. Key in the user name and password. The default user name and password are the same as “**admin**”
5. Press “**Enter**” or ”**OK**”, and then the home screen of the Web-based management appears

6.4 System

6.4.1 System Information

Assigning the system name, location and view the system information

- **System Name:** Assign the name of switch. The maximum length is 31 bytes
- **Description:** Display the description of switch. The maximum length is 31 bytes
- **Location:** Assign the switch physical location. The maximum length is 31 bytes
- **Contact:** Enter the name of contact person or organization
- **Object ID:** object ID. The most common OIDs seen "in the wild" usually belong to the private enterprise numbers allocated by IANA under the 1.3.6.1.4.1 (iso.org.dod.internet.private.enterprise) arc. In computer networking, an **OID**, in the context of the Simple Network Management Protocol (SNMP), consists of the object identifier for an object in a Management Information Base (MIB).



System information interface

6.4.2 Switch Information

6.4.2.1 Main Board

- **Hardware Version:** display the hardware version
- **Fan 1 Status:** display the status of Fan 1
- **Fan 2 Status:** display the status of Fan 2

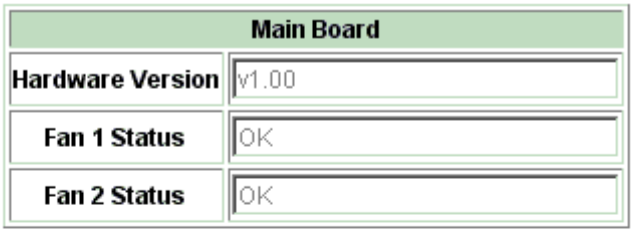
6.4.2.2 Management Software

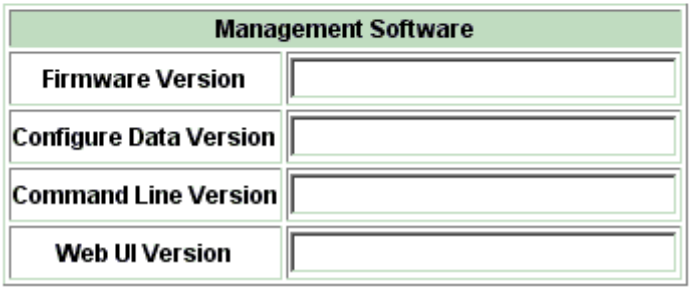
Firmware Version: display the firmware version

Configure Data version: display the configure data version

Command Line Version: display the command line version

Web UI Version: display the Web UI version





Switch information interface

6.4.3 IP Configuration

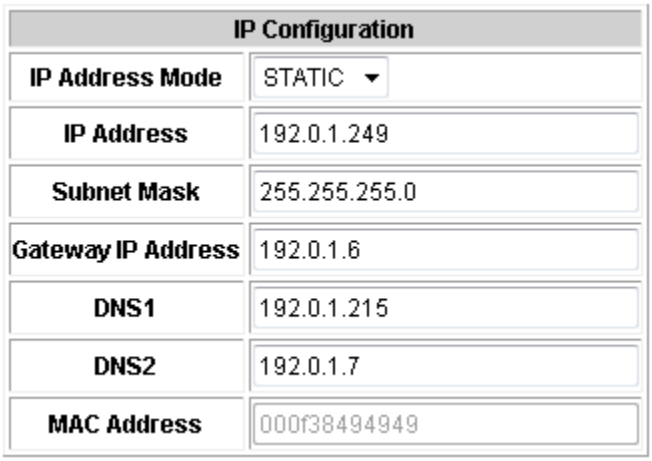
User can configure the IP Settings.

- **IP Address Mode:**

  Static: It means the IP address of this switch will be assigned by user.

  DHCP: It means the IP address of this switch will be assigned by the network DHCP server.

- **IP Address:** Assign the IP address that the network is using. If **IP Address Mode** function is set in DHCP mode, user needn't assign the IP address manually. And, the network DHCP server will assign the IP address which is going to be displayed in this column for the switch. The default IP is 192.168.1.1
- **Subnet Mask:** Assign the subnet mask of the IP address. If **IP Address Mode** function is in DHCP mode, user need not assign the subnet mask manually.
- **Gateway IP Address:** Assign the network gateway for the switch. The default gateway is 192.168.1.254
- **DNS1:** Assign the IP address of DNS server1 that the network is using.
- **DNS2:** Assign the IP address of DNS server2 that the network is using.
- **MAC Address:** Display the unique hardware address assigned by manufacturer (default)
- And then, click Apply



IP configuration interface

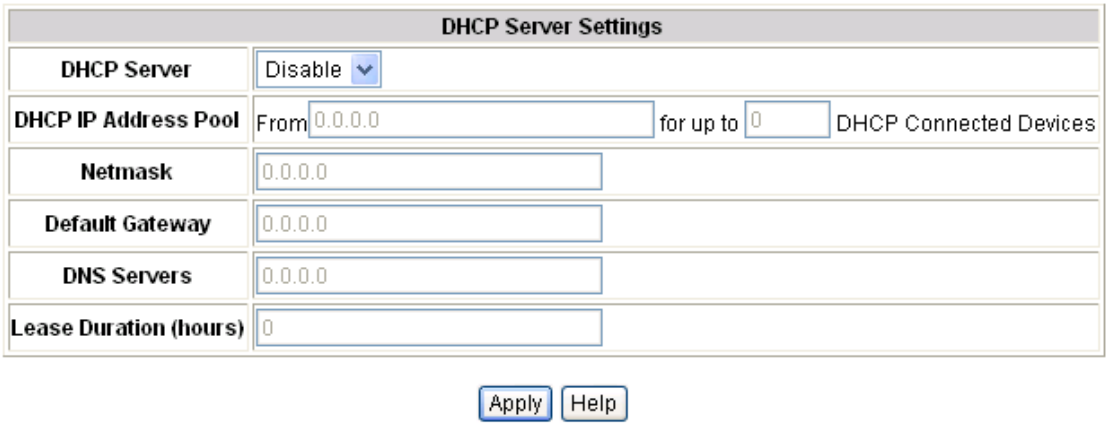
6.4.4 DHCP Configuration

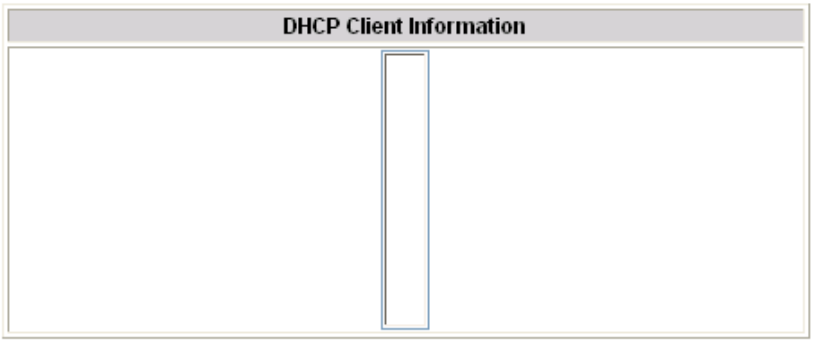
The system provides the DHCP server function. Enable the DHCP server function, the

switch system will be a DHCP server.

- **DHCP Server Settings**

1. **DHCP Server:** Enable or disable the DHCP Server function. Enable – the switch will be a DHCP server on your local network.
2. **DHCP IP Address Pool:** User has to set a range of IP addresses for the DHCP server assigning an IP address to the DHCP client by giving the starting IP address and how many IP addresses within this address pool. For instance, user can set 192.168.1.100 to be the beginning IP address and 50 (can't be greater than 253) to be the maximum number. The range of the address pool should be from 192.168.1.100 to 192.168.1.49.
3. **Netmask:** the dynamic IP assign range subnet mask.
4. **Default Gateway:** the gateway in your network.
5. **DNS Servers:** Domain Name Server IP Address in your network.
6. **Lease Duration(hours):** Assign the lease duration time in hours
7. And then, click Apply





DHCP Server Configuration interface

- **DHCP Client Information**

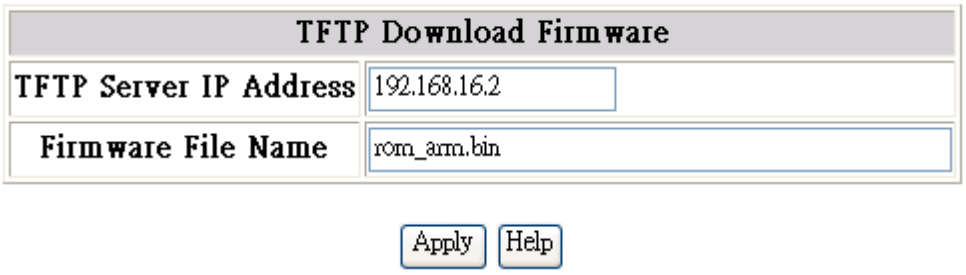
  Display the DHCP Client information which has gotten an IP address from the DHCP server.

6.4.5 Firmware Update

6.4.5.1 TFTP Download Firmware

It provides the functions to allow a user to update the switch firmware. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server.

1. **TFTP Server IP Address:** Fill in your TFTP server IP.
2. **Firmware File Name:** The name of firmware image.
3. Click Apply.

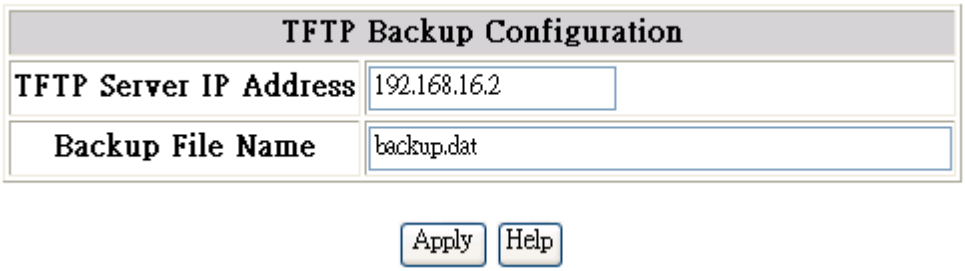


TFTP-Update Firmware interface

6.4.5.2 TFTP Backup Configuration

User can save current EEPROM value from the switch to TFTP server, then go to the TFTP restore configuration page to restore the EEPROM value.

1. **TFTP Server IP Address:** Fill in the TFTP server IP
2. **Backup File Name:** Fill in the file name
3. Click Apply.



TFTP-Configuration Backup interface

6.4.5.3 TFTP Restore Configuration

User can restore EEPROM value from TFTP server, but user must put back the backup file in TFTP server, switch will download it back.

1. **TFTP Server IP Address:** Fill in the TFTP server IP.
2. **Restore File Name:** Fill in the correct restore file name.
3. Click Apply.

TFTP-Configuration Restore interface

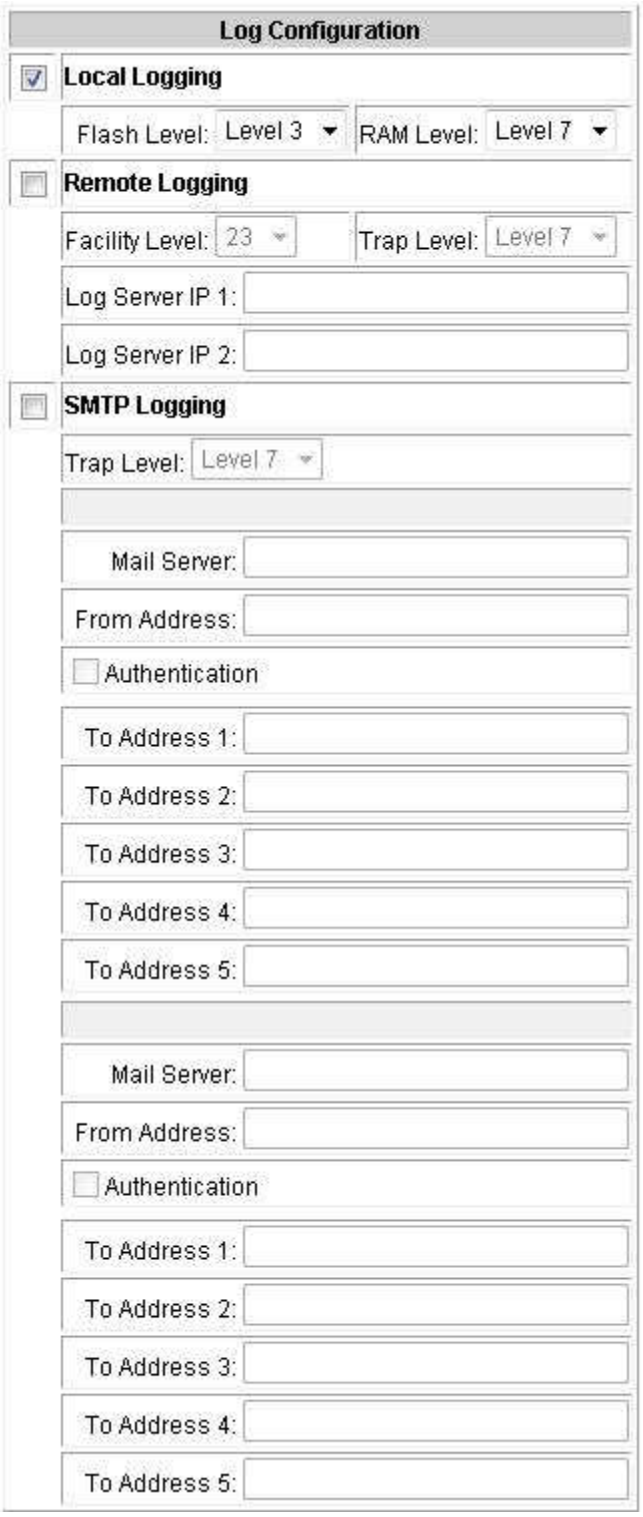
6.4.6 System Event Log

6.4.6.1 LOG Configuration

You can mark the check box of Local Logging, Remote Logging, and SMTP Logging to enable the functions of LOG Configuration.

- **Local Logging:** Mark this check box for enabling to set Flash Level and RAM Level. Set Flash Level to send event log to flash ROM or RAM by assigning the level.
  - **Flash Level:** Set the level range of 0 to 7.
  - **RAM Level:** Set the level range of 0 to 7.

- **Remote Logging:** Mark this check box for enabling to set Facility Level, Trap Level, Log Server IP 1, and Log Server IP 2.
  - **Facility Level:** Set the level range of 16 to 23.
  - **Trap Level:** Set the level range of 0 to 7.
  - **Log Server IP 1:** Assign a remote log server IP address.
  - **Log Server IP 2:** Assign a remote log server IP address.



LOG Configuration interface

6.4.6.2 Logging Events Level

User can select the system log events and SMTP events. When selected events occur, the system will send out the log information. The range of Logging Event Level is from level 0 to level 7. When the level value is the same as the one among Local Logging,

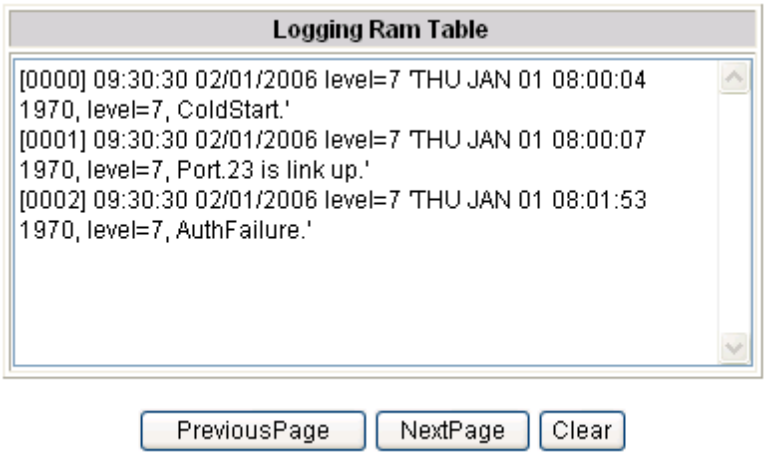
Remote Logging, and SMTP Logging, the system will issue a log record to location where user has designated. After configuring, click Apply.

- **Logging Event Level:** 4 events – Cold Start Event, Warm Start Event, Auth Failure Event, and Port Link Change Event. Pull down the right side item menu to select the event level. When selected events occur, the system will issue the logs.
  - **Cold Start Event:** when the device executes cold start action, the system will issue a log event.
  - **Warm Start Event:** when the device executes warm start, the system will issue a log event.
  - **Auth Failure Event:** You get this trap if a network management system (NMS) polls the device with the wrong community string.
  - **Port Link Change Event:** when the port link has changed, the system will issue a log event.

Logging Events Level interface

6.4.6.3 Logging RAM Table

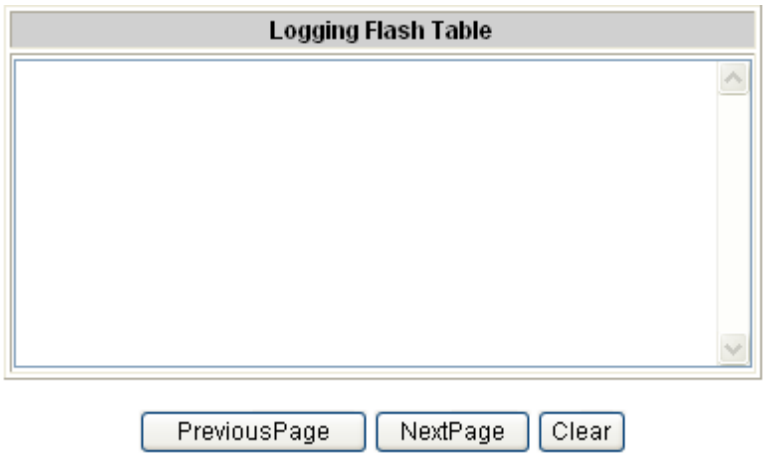
Logging RAM Table displays the logs which have been sent to RAM.



Logging RAM Table interface.

6.4.6.4 Logging Flash Table

Logging Flash Table displays the logs which have been sent to Flash ROM.



Logging ROM Table interface

6.4.7 Security Manager

Change login user name and password for the management security issue

- **User Name:** Key in the new user name (The default is “admin”)
- **New Password:** Key in the new password (The default is “admin”)
- **Confirm Password:** Re-type the new password
- And then, click Apply

6.5 Port

6.5.1 Port Statistics

Display the port statistic information.

Port Statistic interface

6.5.2 Port Information

The following information provides the current port statistic information

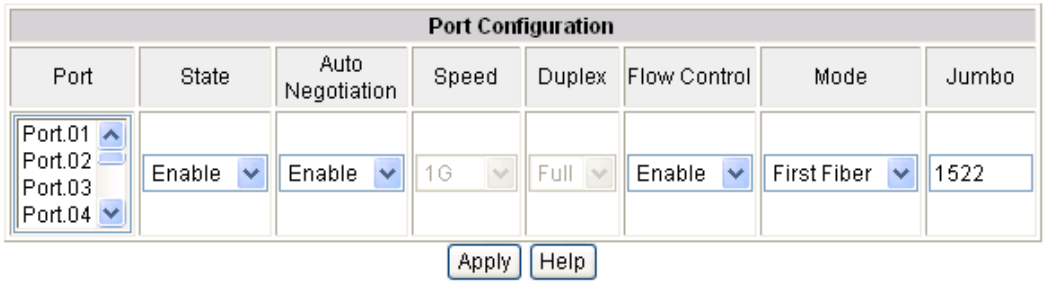
Port Infomation												
Port	Type	Link	State	Auto Negotiation		Speed		Duplex		Flow Control		Jumbo
				Config	Actual	Config	Actual	Config	Actual	Config	Actual	
Port.01	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.02	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.03	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.04	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.05	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.06	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.07	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.08	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.09	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.10	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.11	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.12	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.13	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.14	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.15	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.16	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.17	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.18	GIGA_COPPER	Up	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.19	GIGA_COPPER	Down	Enable	Enable	Enable	1000	1000	full	full	Enable	Enable	1522
Port.20	GIGA_COPPER	Up	Enable	Enable	Enable	1000	100	full	full	Enable	Enable	1522

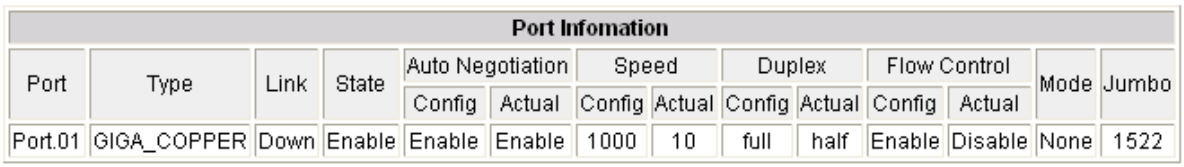
Port Information interface

6.5.3 Port Control

In Port configuration, user can view every port status that depended on user setting and the negotiation result.

1. **Port:** select the port that user wants to configure.
2. **State:** Current port status. The port can be set to disable or enable mode. If the port setting is disabled, it will not receive or transmit any packet.
3. **Auto Negotiation:** enable or disable auto negotiation
4. **Speed:** when Auto Negotiation is disabled, user can select the port link speed.
5. **Duplex:** set full-duplex or half-duplex mode of the port.
6. **Flow Control:** set flow control function is Enable or Disable. The default value is Enable.
7. **Jumbo:** Assign the Jumbo frame size. The maximum is 10K bytes.
8. Click Apply.





Port Configuration interface

6.5.4 Port Trunk

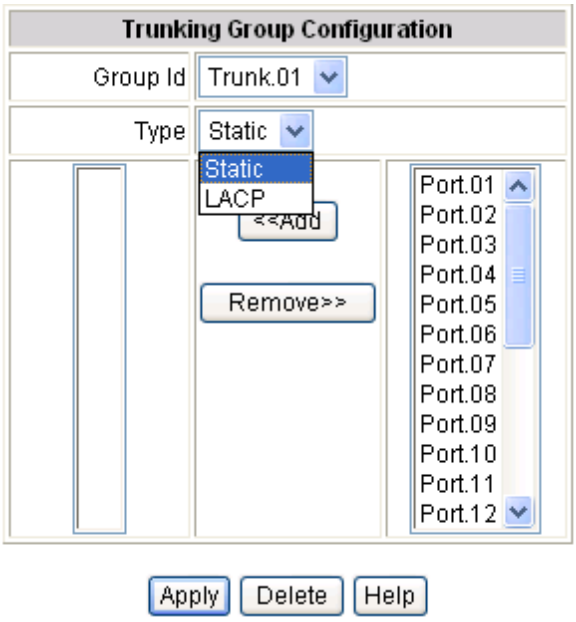
The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to eight ports into two dedicated connections. This feature can expand bandwidth between 2 (or more) devices. LACP operation requires full-duplex mode, more detail information refers to IEEE 802.3ad.

6.5.4.1 Trunk Configuration

1. **Group ID:** list the Trunk group ID.
2. **Type:** Static and LACP for selecting
3. select the port number from the right column list and then click Add button to add the port into a trunk group

4. Click Remove button to remove the port from a trunk group

5. To delete Trunk Group, select the Group Id and click Delete button.



Trunk Configuration interface

6.5.4.2 Trunk Information

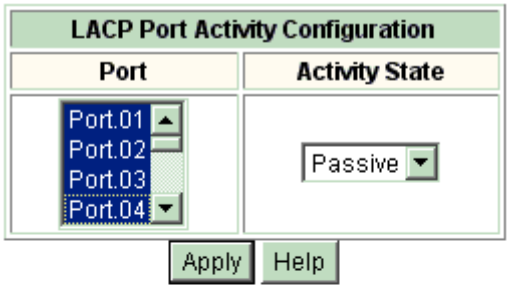
After setting up the trunk group, user will see the related information as below.

Static Trunking Group Information	
Group Id	1
Port Member	Port.23,Port.24

Trunk Information interface

6.5.4.3 Port Activity

User will see the related information of LACP Port Activity State as below.

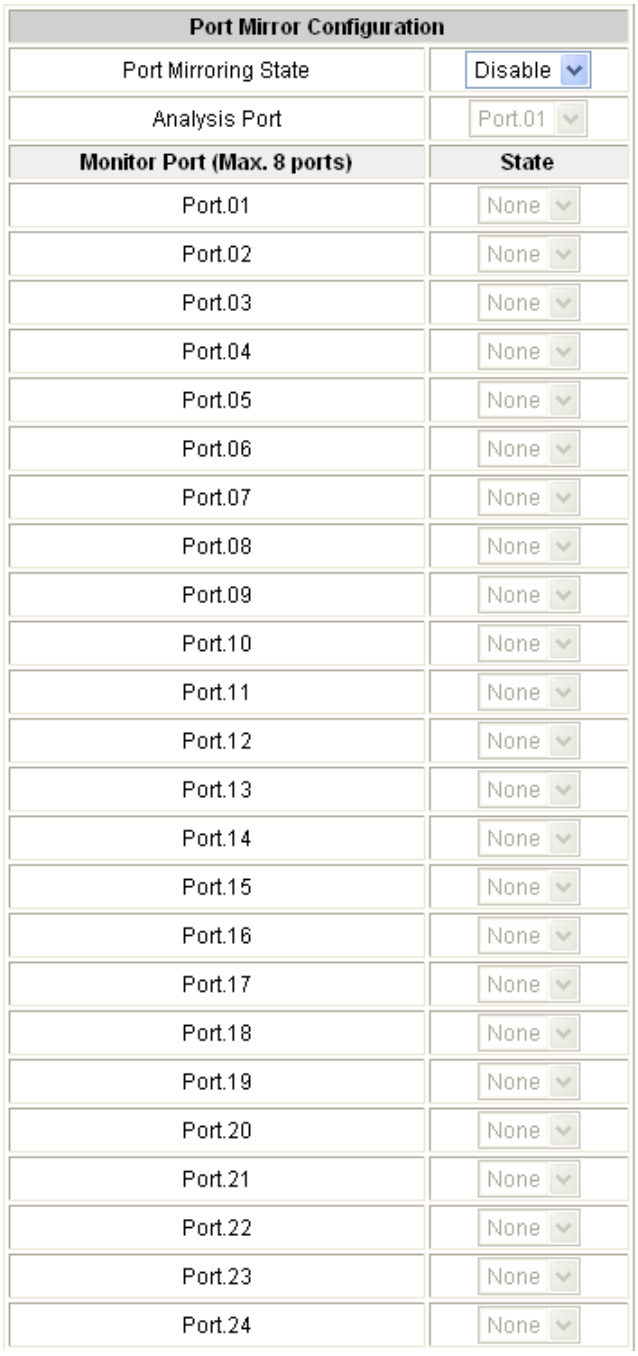


Port	State
Port.01	Active
Port.02	Active
Port.03	Active
Port.04	Active

Port Activity interface

6.5.5 Port Mirror

The port mirror is a method for monitor traffic in switched networks. Traffic through ports can be monitored by specific port. That means traffic goes in or out monitored ports will be duplicated into analysis port.



Port Mirror Configuration interface

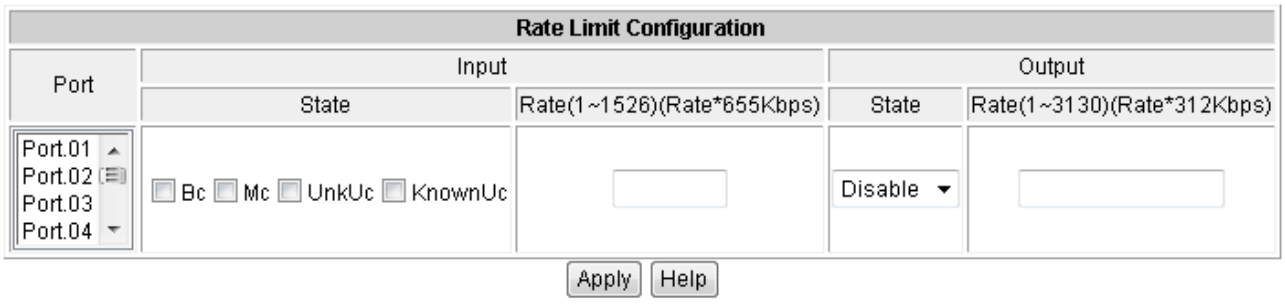
1. **Port Mirroring State:** enable or disable the port mirror function
2. **Analysis Port:** Select a port for analyzing all monitor port traffic. User can connect mirror port to LAN analyzer or Netxray.
3. **Monitor Port:** The ports which user wants to monitor. All monitored port traffic will be copied to analysis port. (UP to 8 ports)
4. **State:** User can choose the monitored port packet in RX, TX or Both state by pulling down the pull-down menu.

5. Click Apply.

6.5.6 Rate Limiting

User can set up the bandwidth rate and packet limitation type of each port.

- **Input**
  - **State:** There are 4 check boxes of Bc, Mc, UnkUc, KnownUc for selecting.
  - **Rate (1~1526)(Rate*655Kbps):** Type in the input rate limit in number between 1~1526.
- **Output**
  - **State:** Enable or disable the output rate limit.
  - **Rate (Rate*312Kbps):** Type in the output rate limit which is a multiple of 312.



Port Configuration interface

6.6 Protocol

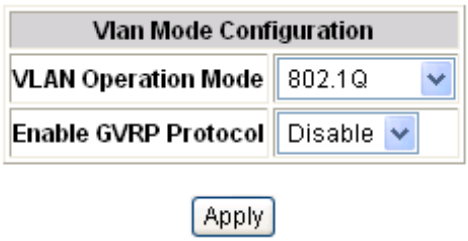
6.6.1 VLAN

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allow you to isolate network traffic, so only the members of the VLAN will receive traffic from the same members of VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch

physically.

6.6.1.1 VLAN Mode Configuration

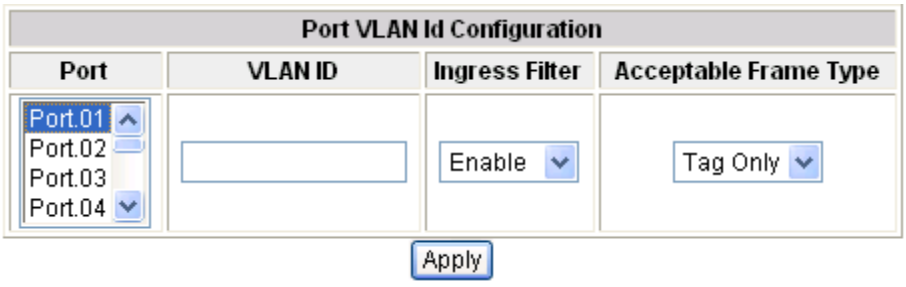
The switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration of VLAN operation mode is “**802.1Q**”.



VLAN Mode Configuration interface

6.6.1.2 Port VLAN Id Configuration

1. **Port:** Select the port number in the table list.
2. **VLAN ID:** Key in the VLAN ID.
3. **Ingress Filter**: Enable or Disable the ingress filter.
4. **Acceptable Frame Type:** Choose **Tag only** or **All type**.
5. Click Apply

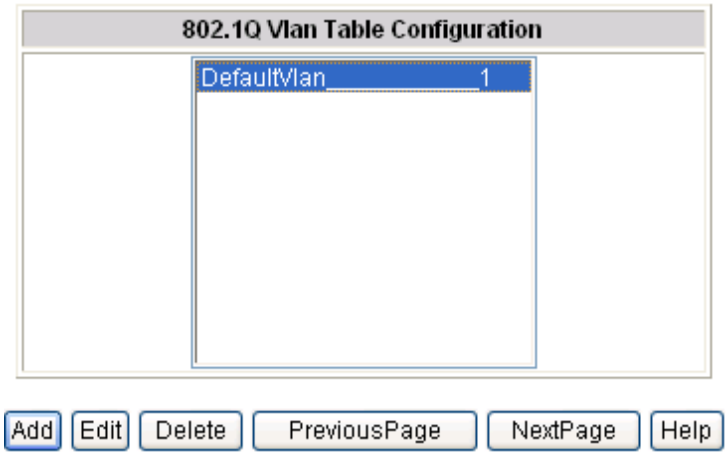


Port VLAN Id Configuration interface

6.6.1.3 VLAN Entry

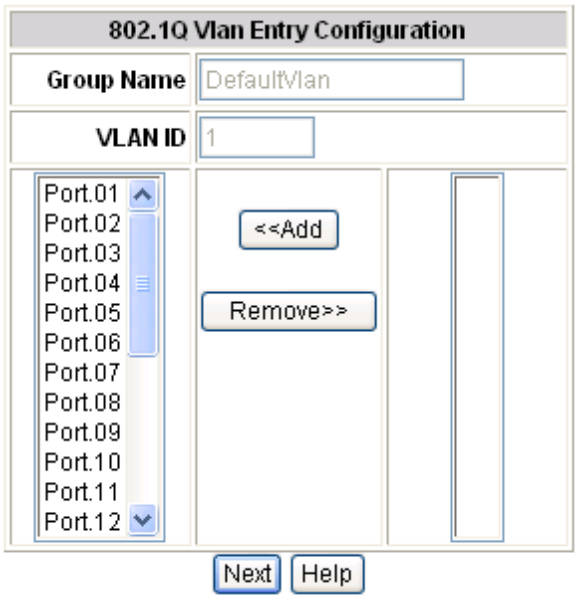
Edit the existing VLAN Group.

1. Select the VLAN group in the table list.
2. Click Edit



VLAN Table Configuration interface

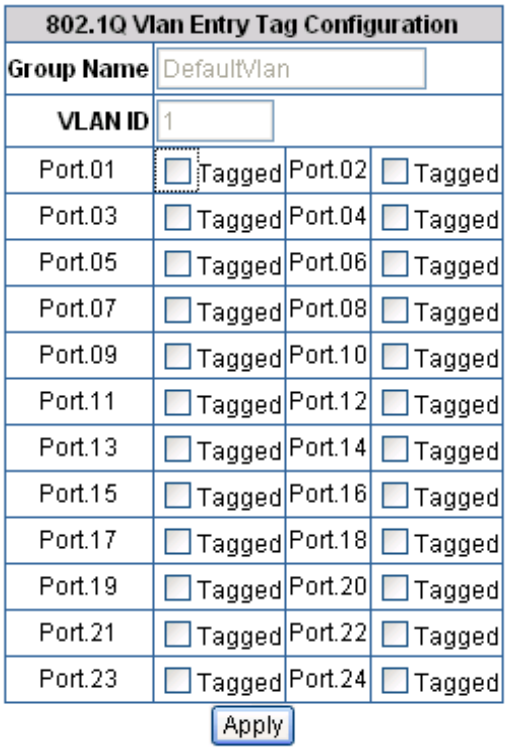
3. User can add/ remove the ports from a VLAN group.
4. Click Next.



VLAN Table Configuration - Edit interface

5. Mark the check box to tag the ports of a VLAN group.

6. Click Apply.



VLAN Table Configuration - Edit interface

6.6.2 Rapid Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will auto detect the connected device that is running STP or RSTP protocol.

6.6.2.1 STP System Configuration

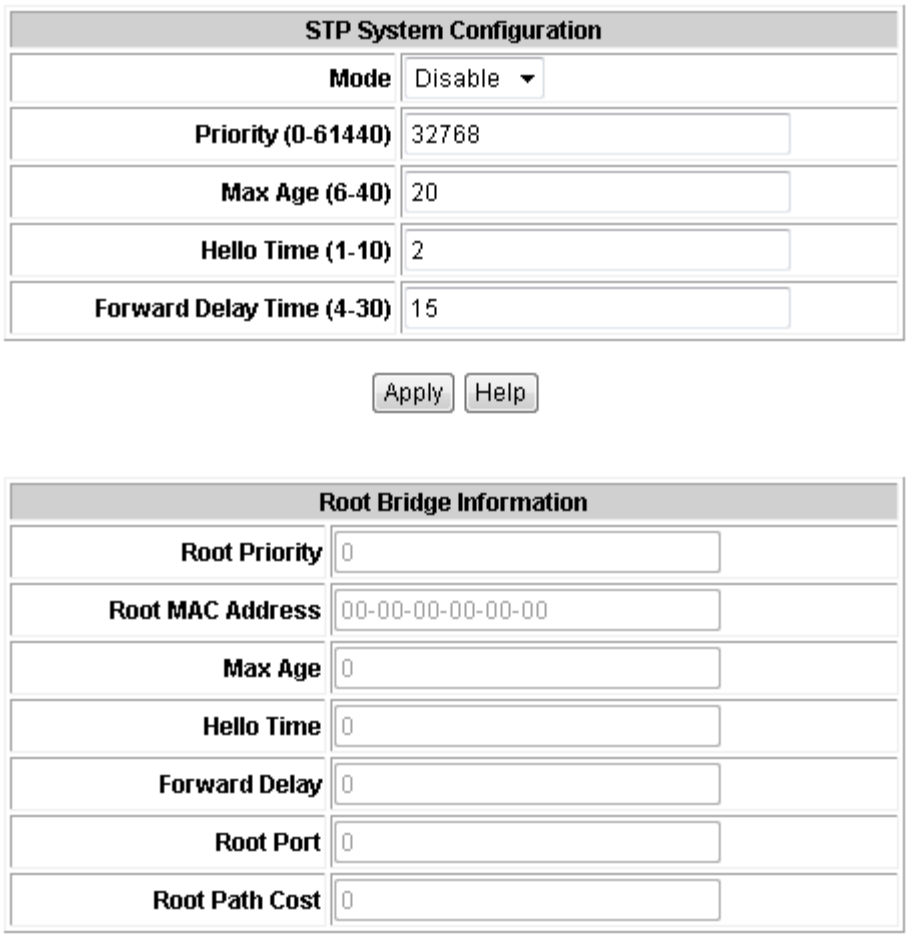
- User can view spanning tree information about the Root Bridge
- User can modify RSTP state. After modification, click Apply button
  - **Mode:** user must enable or disable RSTP function before configure the related parameters
  - **Priority (0-61440):** a value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root.
  - **Max Age (6-40):** the number of seconds a bridge waits without receiving

Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40

- **Hello Time (1-10):** the time that controls switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10
- **Forward Delay Time (4-30):** the number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30

[NOTE] Follow the rule to configure the MAX Age, Hello Time, and Forward Delay Time.

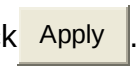
2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)



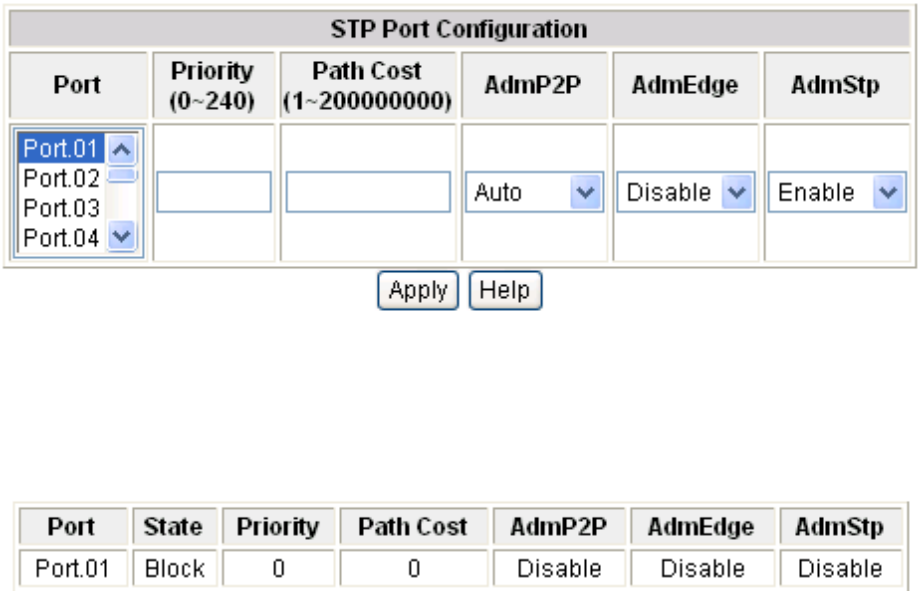
RSTP System Configuration interface

6.6.2.2 STP Port Configuration

User can configure path cost and priority of every port.

1. Select the port in Port column.
1. **Priority:** Decide which port should be blocked by priority in LAN. Enter a number 0 through 240.
2. **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
3. **AdmP2P:** Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. Enable is P2P enabled; disable is P2P disabled; and auto means auto-sense.
4. **AdmEdge:** The port directly connected to end stations which cannot create bridging loop in the network. To configure the port as an edge port, set the port to "**Enable**" status.
5. **AdmStp:** The port includes the STP mathematic calculation. **Enable** is including STP mathematic calculation. **Disable** is not including the STP mathematic calculation.
6. Click 

.



RSTP Port Configuration interface

6.6.3 SNMP

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

■ **SNMP Information**

Enter the system name, contact and location information.

- **Name:** Assign a name for the switch.
- **Location:** Type the location of the switch.
- **Contact:** Type the name of contact person or organization.

■ **SNMP Community String**

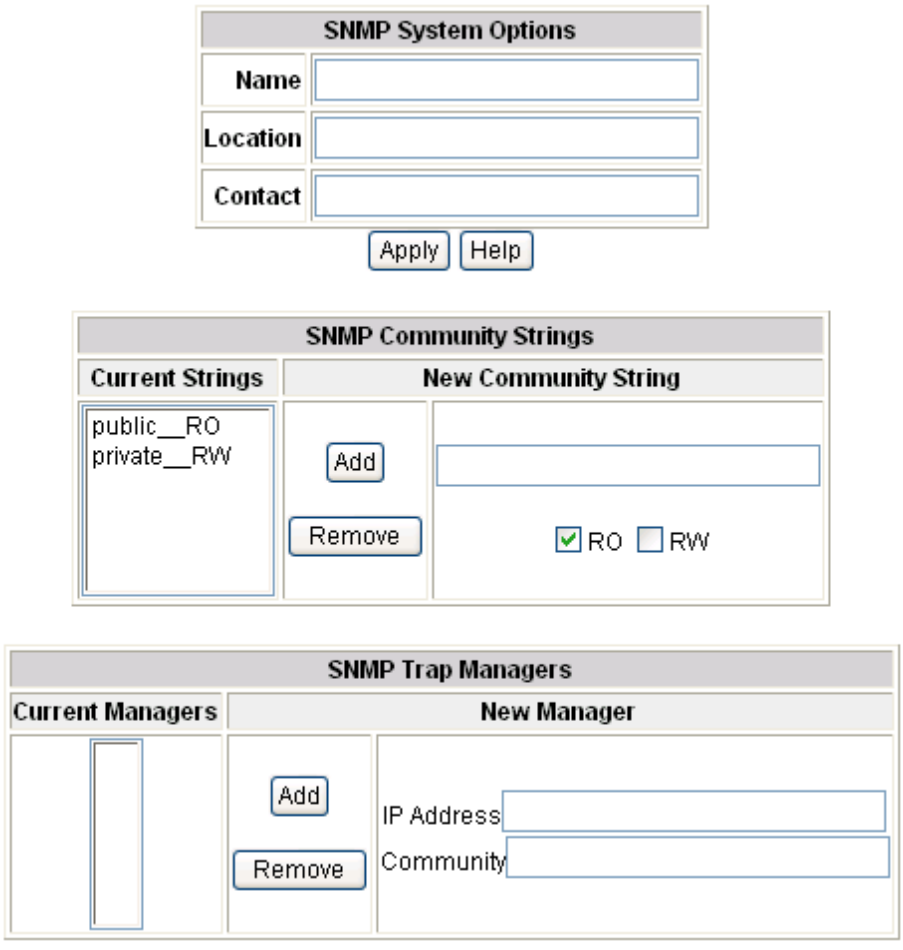
User can define new community string set and remove unwanted community string.

- **RO:** Read only. Enable requests accompanied by this string to display MIB-object information.
- **RW:** Read write. Enable requests accompanied by this string to display MIB-object information and to set MIB objects.

- **SNMP Trap managers**

  A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will issue. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager and enter SNMP community strings and selects the SNMP version.

  - **IP Address:** enter the IP address of trap manager.
  - **Community:** enter the community string.
  - Click Add.



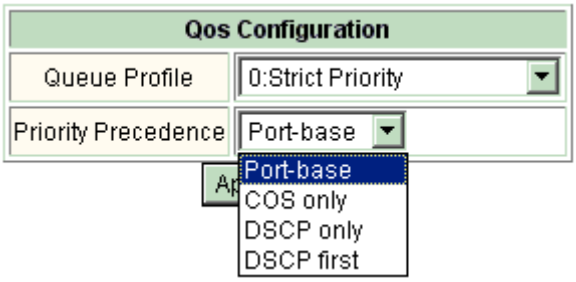
SNMP Configuration interface

6.6.4 QoS

User can configure QoS policy and priority setting, per port priority setting, COS and DSCP setting.

6.6.4.1 QoS Configuration

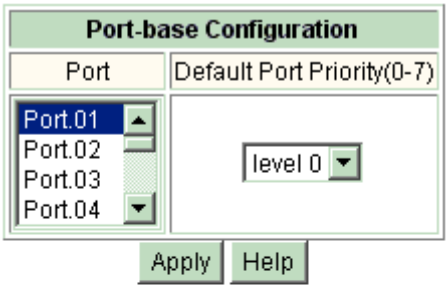
- **Queue Profile:** Select the queue profile from the column list.
- **Priority Precedence:** There are 4 priority precedence selections available.
- Click Adpply.



QoS Configuration interface

6.6.4.2 Port-bace Configuration

- **Port:** Select the number port from the column list.
- **Default Port Priority (0-7):** Assign the priority level.
- Click Adpply.

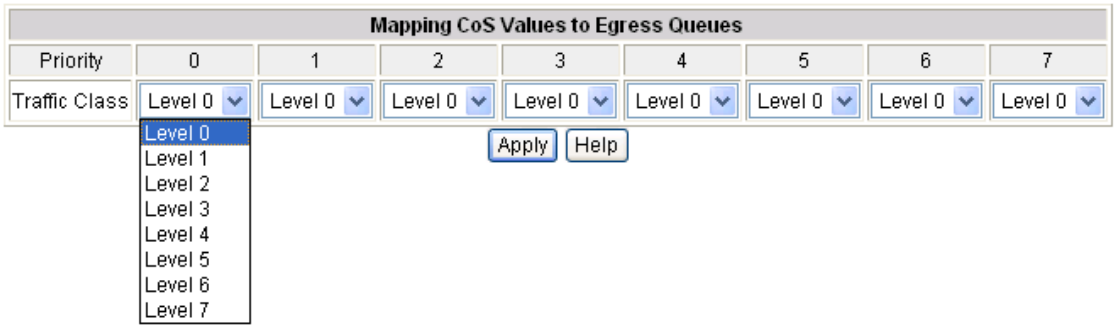


Port-base Configuration interface

6.6.4.3 COS Configuration

Set up the COS priority level.

- **COS priority:** Set up the COS priority level 0~7, 7 is the highest priority.
- Click Apply.

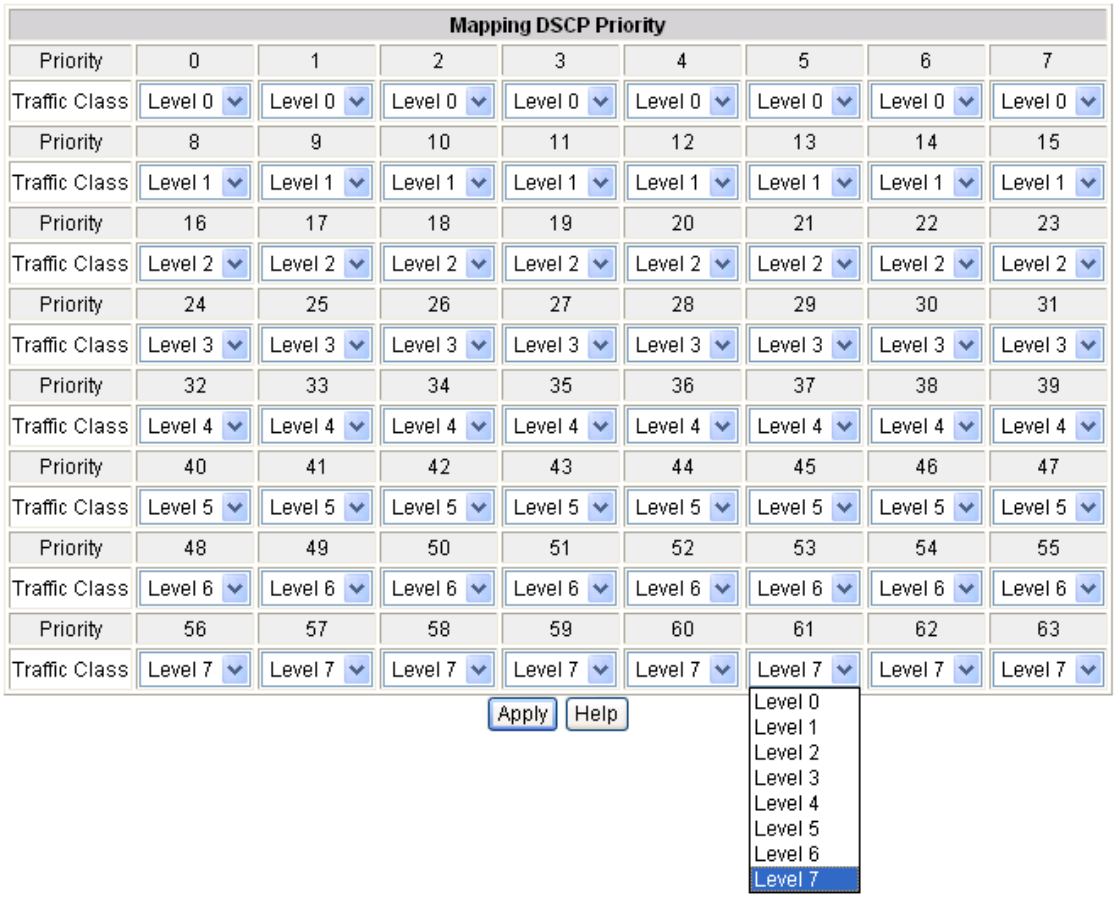


COS Configuration interface

6.6.4.4 DSCP Configuration

Set up the DSCP priority.

- **Mapping DSCP priority:** The system provides 0~63 DSCP priority level. Each level has 8 types of priority – 0~7, 7 is the highest priority. When the IP packet is received, the system will check the DSCP level value in the IP packet that has been received. For example: user set the DSCP level 25 as high. When the packet received, the system will check the DSCP value of the received IP packet. If the DSCP value of received IP packet is 25(priority = high), and then the packet priority will have highest priority.
- Click Apply.

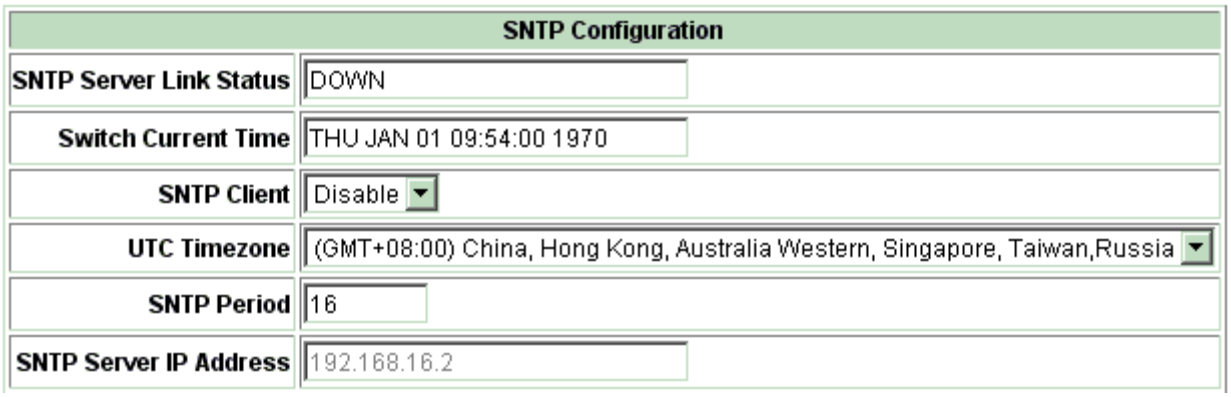


DSCP Configuration interface

6.6.5 SNTP

User can configure the SNTP (Simple Network Time Protocol) settings. The SNTP allows user to synchronize switch clocks in the Internet.

1. **SNTP Server Link Status:** Display the link status of SNTP server.
2. **Switch Current Time:** Display the current time of the switch.
3. **SNTP Client:** Enable or disable SNTP function. When it is enabled, user can assign the domain name or IP address of SNTP server for getting the time from SNTP server.
4. **UTC Timezone:** Set the switch location time zone.
5. **SNTP Period:** The SNTP period is used for sending synchronizing packets periodically.
6. **SNTP Sever IP Address:** Assign the SNTP server IP address.
7. Click Apply.



SNTP Configuration interface

6.6.6 IGMP

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP have three fundamental types of message as follows:

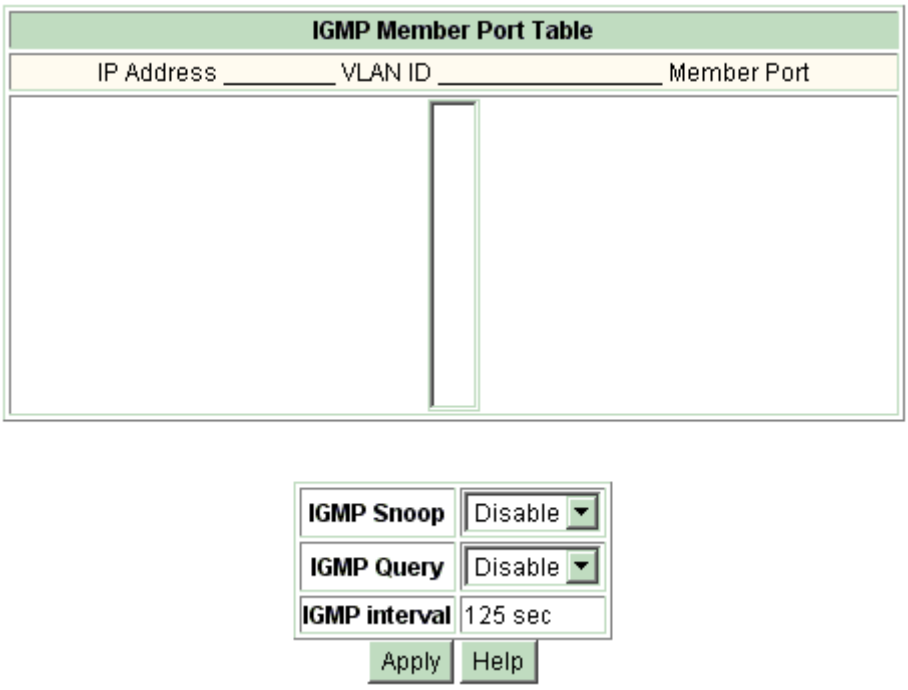
Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Join Group	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

6.6.6.1 IGMP Configuration

The switch support IP multicast, user can enable IGMP protocol on web management's switch setting advanced page, then display the IGMP snooping

information. IP multicast addresses range from 224.0.0.0 through 239.255.255.255.

- **IGMP Snoop:** Enable or disable the IGMP snoop.
- **IGMP Query:** The IGMP query function has 3 modes - Enable, Disable or Auto - for selection. The IGMP query information will be displayed in IGMP status section.
- **IGMP interval**: The interval of General Query being sent. (Read Only)
- Click Apply.



IGMP Configuration interface

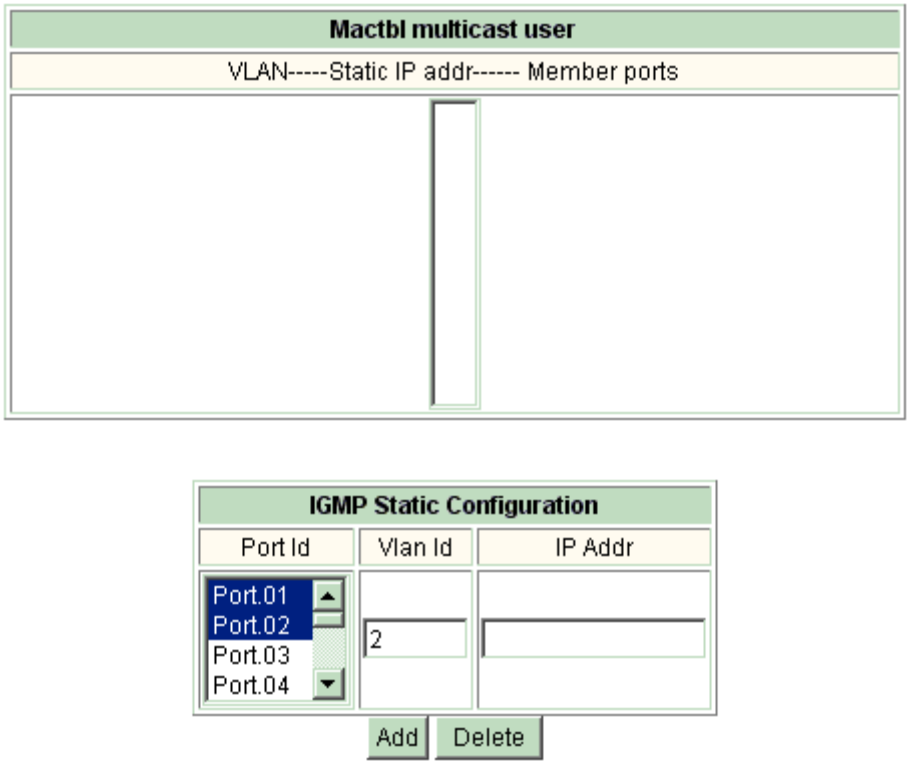
6.6.6.2 IGMP Static Configuration

Multicasts are similar to broadcasts, they are sent to all end stations on a LAN or VLAN. Multicast filtering is the system by which end stations only receive multicast traffic if they register to join specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the end stations that are connected to registered ports.

This function action when **IGMP Configuration** disable.

- **Port ID:** Select the port number in the specific multicast group IP address.
- **VLAN ID:** Input the value of VLAN ID.
- **IP Address:** Assign a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255.
- Click "Add".

If you want to delete an entry from table, select the entry and click "Delete".



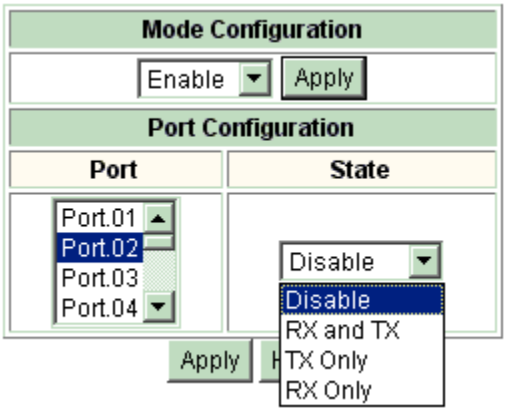
IGMP Static Configuration interface

6.6.7 LLDP

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

6.6.7.1 LLDP Configuration

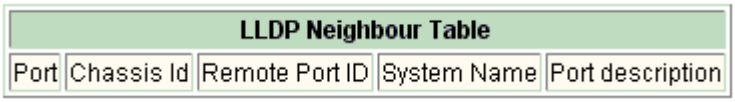
- Mode Configuration: Enable or disable the LLDP function.
- Port Configuration: Enable or disable the LLDP state of the number port.



LLDP Configuration interface

6.6.7.2 LLDP Neighbor Table

User will see all information of port by LLDP enable.



LLDP Neighbor Table interface

6.7 Security

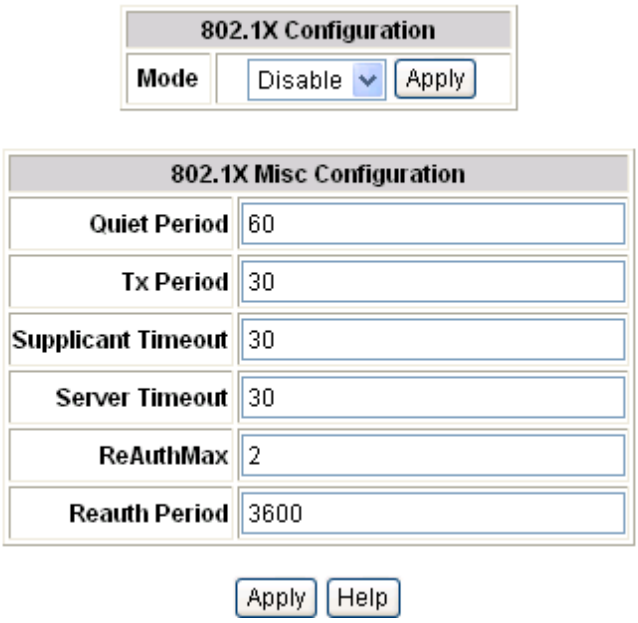
6.7.1 802.1x/ RADIAS

802.1x is an IEEE authentication specification that allows a client to connect to a wireless access point or wired switch but prevents the client from gaining access to the port until it provides authority, like a user name and password that are verified by a separate server.

6.7.1.1Misc Configuration

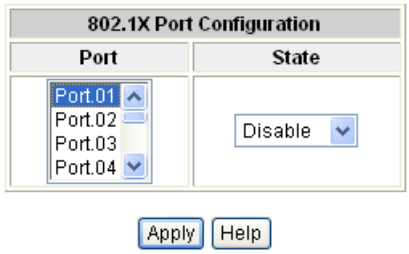
1. **Mode:** Enable or disable 802.1 x protocols.
2. **Quiet Period:** Set the period during which the port doesn't try to acquire a supplicant.
3. **TX Period:** Set the period the port waits for retransmit next EAPOL PDU during an authentication session.

4. **Supplicant Timeout:** Set the period of time the switch waits for a supplicant response to an EAP request.
5. **Server Timeout:** Set the period of time the switch waits for a server response to an authentication request.
6. **ReAuthMax:** Set the number of authentication that must time-out before authentication fails and the authentication session ends.
7. **Reauth period:** set the period of time after which clients connected must be re-authenticated.
8. Click Apply.



MISC Configuration interface

6.7.1.2 Port Configuration



Port Configuration interface

You can configure 802.1x authentication state for each port. The State provides Disable, Authorize, Accept and Reject.

- **Disable:** This function is disabled.
- **Authorize:** The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the supplicant and the authenticator.
- **Accept:** The specified port will allow the client accessing in any case.
- **Reject:** The specified port rejects the client accessing regardless of whether the authentication passed or not.
- Click Apply.

6.7.1.3Radius Client Configuration

After having enabled the IEEE 802.1X function, user can configure the parameters of this function.

1. **Radius Server IP:** Set the Radius Server IP address.
2. **Server Port:** Set the UDP destination port for authentication requests to the specified Radius Server.
3. **Accounting Port:** Set the UDP destination port for accounting requests to the

specified Radius Server.

4. **Shared Key:** Set an encryption key for using during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
5. **NAS Identifier:** A string used to identify this switch.
6. Click Apply.

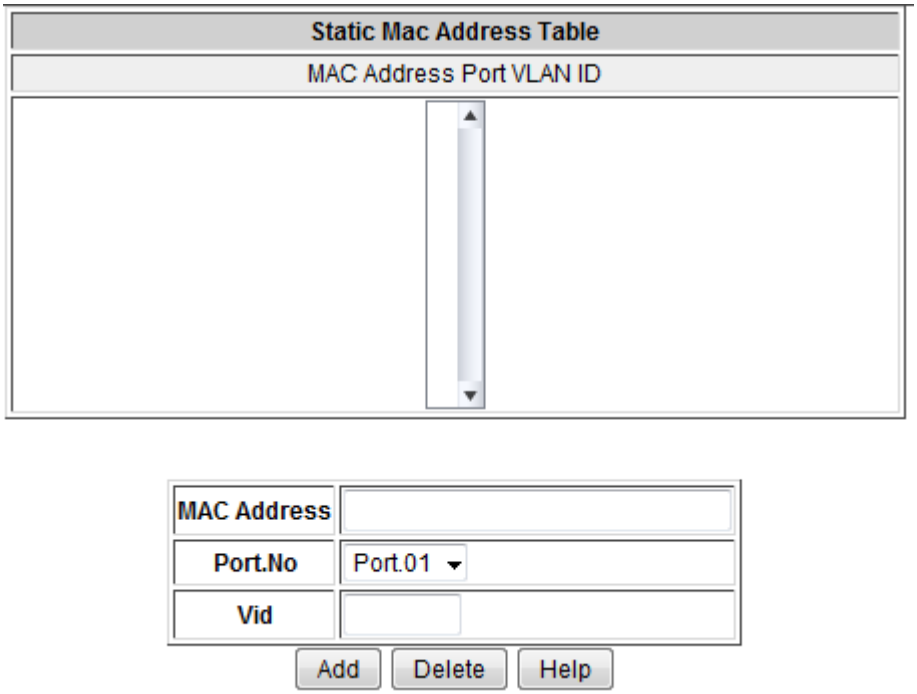
6.7.2 Port Security

Use the MAC address table to ensure the port security.

6.7.2.1 Static MAC Address Table

User can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. User can add / modify / delete a static MAC address.

Packets with the specified destination address received in the specified VLAN are forwarded to the specified interface.



Static MAC Addresses interface

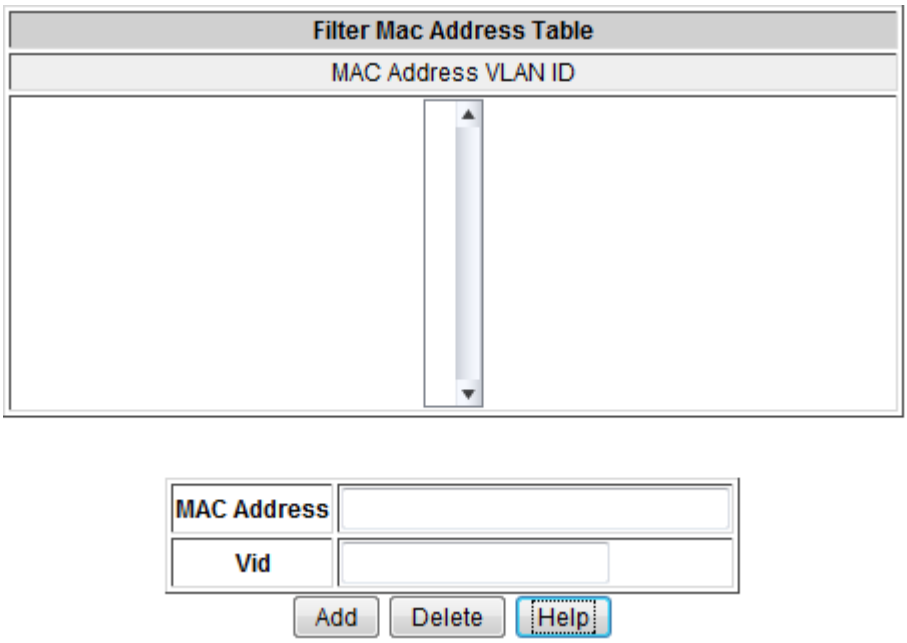
Add the Static MAC Address

User can add static MAC address in switch MAC table.

1. **MAC Address Port VLAN ID:** list the MAC Address Port. VLAN ID
2. **MAC Address:** Specify the destination MAC address to add to the address table.
3. **Port.No:** pull down the selection menu to select the port number.
4. **Vid:** enter the Vid of the MAC address, it has to be between 1 to 4094.
5. Click Add.
6. If user wants to delete the MAC address from filtering table, select the MAC address and click Delete.

6.7.2.2 Filter MAC Address Table

MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination addresses. For example, if your network is congested because of high utilization from one MAC address, you can filter all traffic transmitted to that MAC address, restoring network flow while you troubleshoot the problem.



MAC Filtering interface

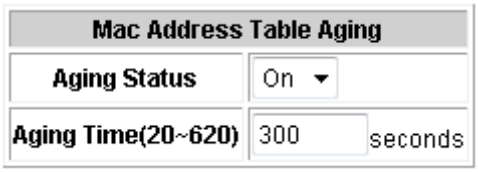
1. **MAC Address:** Enter the MAC address that user wants to filter.
2. **Vid:** enter the Vid of the MAC address, it has to be between 1 to 4094.
3. Click Add.

4. If user wants to delete the MAC address from filtering table, select the MAC address and click Delete.

6.7.2.3 MAC Address Table Aging

Aging Status: Pull-down menu to enable MAC address table aging function.

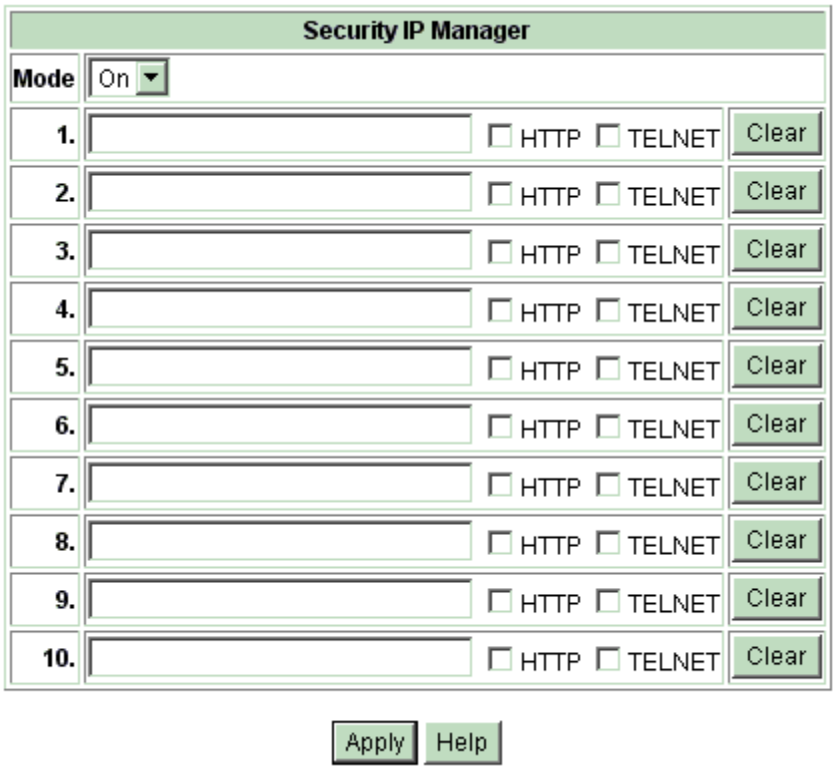
Aging Time (20~620): Assign the aging time in second.



Address Aging interface

6.7.3 IP Security

User can assign up to 10 security IP addresses for accessing the switch via HTTP, TELNET or both, any other IPs which are not included will be restricted.



IP Security interface

1. **Mode:** When mode is set at **ON**, user can assign up to 10 Security IP addresses.

2. **HTTP:** mark the check box to enable the access via HTTP for the assigned IP
3. **TELNET:** mark the check box to enable the access via TELNET for the assigned IP.
4. Click Clear button to clear IP address and all the check box.
5. And then, click Apply

6.7.4 ACL

An ACL is a sequential list of permit or deny conditions that apply to IP addresses. This switch tests ingress or egress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match for a list of all permit rules, the packet is dropped; and if no rules matches for a list of all deny rules, the packet is accepted.

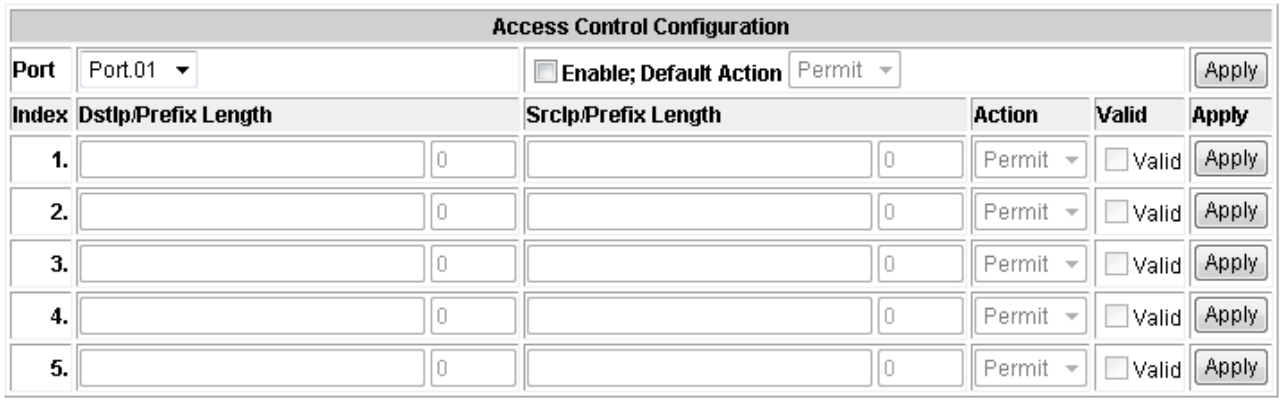
The following restrictions apply to ACLs:

- The ACL only support single port and not support trunk group.
- The maximum number of ACLs is also 5 for each port.

Command Attributes

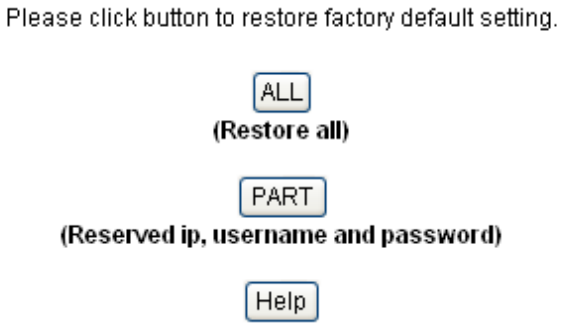
- **Enable:** An ACL can be enable per port.
- **Default Action:** The action if no rules matched.
- **Action:** An ACL can be permit or deny rule.
- **IP Address and Prefix Length:** Include destination and source IP address.

Ex: source 192.168.16.1/24 means all frames that source IP address is 192.168.16.x matched.



6.8 Factory Default

Reset switch to default configuration. Click ALL to reset all configurations to the default value or PART to reset all configuration except reserved IP, user name and password.



Factory Default interface

6.9 Save Configuration

Save all configurations that user has made in the system. To ensure the all configuration will be saved. Click Save Flash to save the all configuration to the flash memory.

Please be noted, it is recommend to do the “save configuration” once changes has been made on system.

Save Configuration interface

6.10 System Reboot

Reboot the switch in software reset. Click Reboot to reboot the system.

System Reboot interface

Troubleshooting

This section is intended to help you solve the most common problems on MSL-3S79.

- **Incorrect connections**

The switch port can automatically detect straight or crossover cable when you link switch with other Ethernet device. As for RJ-45 connection, you should use correct UTP or STP cable that 10/100/1000Mbps port uses 2-pairs twisted cable and Gigabit 1000T port uses 4 pairs twisted cable. If the RJ-45 connector is not correctly pinned on right position then the link will fail. As for fiber connection, please notice the fiber cable mode and fiber module should match.

- **Faulty or loose cables**

Look for loose or obviously faulty connections. If they appear to be OK, make sure the connections are snug. If that does not correct the problem, try a different cable.

- **Non-standard cables**

Non-standard and miss-wired cables may cause numerous network collisions and other network problem, and can seriously impair network performance. A category 5-cable tester is a recommended tool for every 100Base-T network installation.

RJ-45 ports: Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections: 100Ω Category 3, 4 or 5 cable for 10Mbps connections, 100Ω Category 5 cable for 100Mbps connections or Category-5e / Category-6 for above 1000Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet). Gigabit port should use Cat-5 or cat-5e cable for 1000Mbps connections. The length does not exceed 100 meters.

- **Improper Network Topologies**

It is important to make sure that you have a valid network topology. Common topology faults include excessive cable length and too many repeaters (hubs) between end

nodes. In addition, you should make sure that your network topology contains no data path loops. Between any two ends nodes, there should be only one active cabling path at any time. Data path loops will cause broadcast storms that will severely impact your network performance.

- **Diagnosing LED Indicators**

The Switch can be easily monitored through panel indicators, which describes common problems you may encounter and where you can find possible solutions to assist in identifying problems.

If the power indicator is not lighted when the power cord is plugged in, you may have a problem with power outlet, or power cord. However, if the switch powers off after running for a while check for loose power connections, power losses or surges at power outlet. If you still cannot resolve the problem, contact your local dealer for assistance.

Appendix A- Command Sets

Commands Set List

Modes	Access Method	Prompt	Exit Method	About This Model
User EXEC	Begin a session with your switch.	switch>	Enter logout or quit.	The user commands available at the user level are a subset of those available at the privileged level. Use this mode to • Perform basic tests. • Display system information.
Privileged EXEC	Enter the enable command while in user EXEC mode.	switch#	Enter disable to exit.	The privileged command is advance mode Privileged this mode to • Display advance function status • save configures
Global configuration	Enter the configure command while in privileged EXEC mode.	switch(config)#	To exit to privileged EXEC mode, enter exit or end	Use this mode to configure Parameters that apply to your switch as a whole.
VLAN database	Enter the vlan database command while in privileged EXEC mode.	switch(vlan)#	To exit to user EXEC mode, enter Exit.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the interface command (with a specific interface) while in global configuration mode	switch(config-if)#	To exit to global Configuration mode, enter exit. To exist to privileged EXEC mode or end.	Use this mode to configure Parameters for the switch and Ethernet ports.

System Commands Set

Commands	Command Level	Description	Defaults	Example
system name [system name]	**Global configuration mode**	Set switch system name string		switch(config)# **system name xxx**
system location [system Location]	**Global configuration mode**	Set switch system location string		switch(config)# **system location xxx**
system description [description]	**Global configuration mode**	Set switch system description string		switch(config)# **system description xxx**
system contact [contact]	**Global configuration mode**	Set switch system contact window string		switch(config)# **system contact xxx**
ip address [ip-address] [subnet-mask] [gateway]	**Global configuration mode**	Use the **ip address** interface configuration command to set an IP address for a switch. Use the **no** form of this command to remove an IP address or to disable IP processing.		switch(config)# **ip address 192.168.1.1 255.255.255.0 192.168.1.254**
write memory	**Privileged EXEC**	Save user configuration into permanent memory(flash rom)		switch#**write memory**
reload	**Global configuration mode**	Halt and perform a cold restart		switch(config)# **reload**
default	**Global configuration mode**	Restore to default **no**: restore all to default. **yes**: reserved ip, username and password.		switch(config)#**default**
admin username [Username]	**Global configuration mode**	Changes a login username. (maximum 32 words)		switch(config)#**admin username xxxxxx**
admin password [Username]	**Global configuration**	Specifies a password (maximum 32 words)		switch(config)#**admin password xxxxxx**

	mode			
console-timeout [time(sec)]	**Global configuration mode**	Set console timeout. The range of timeout is 30 sec ~ 600 sec.	180 sec	switch(config)#**console-timeout 30**
show system-info	**Privileged EXEC**	Show system information		switch#**show system-info**
show ip	**Privileged EXEC**	Show ip information of switch		switch#**show ip**
show admin	**Privileged EXEC**	Show username & password		switch#**show admin**
show version	**Privileged EXEC**	Use the **show version** user EXEC command to display version information for the hardware and firmware.		switch# **show version**
show terminal	**Privileged EXEC**	Use the **show terminal** command to display console information for the switch		switch#**show terminal**
show fan-status	**Privileged EXEC**	Use the show fan-status command to display fan status		switch(config)# **show fan-status**

Port Commands Set

Commands	Command Level	Description	Default	Example
interface gigaethernet [port ID]	**Interface configuration mode**	Use the **Ethernet** interface configuration command		switch(config)#**interface gigaethernet 1**
		Use the **module Ethernet** interface configuration command		switch(config)#**interface gigaethernet 1**
duplex [full | half]	**Interface configuration mode**	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	Auto	switch(config)#**interface gigaethernet 1** switch(config-if)#**duplex full** or switch(config-if)#**duplex half**
speed [10|100|1000|auto]	**Interface configuration mode**	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet.		switch(config)#**interface gigaethernet 1** switch(config-if)#**speed 1000** or

				switch(config-if)#**speed 100** or switch(config-if)#**speed 10** or switch(config-if)#**speed auto**
flowcontrol [enable|disable]	**Interface configuration mode**	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion. Use the no form of this command to disable security on the port. Configure flow control Disable flow control of interface	Off	switch(config)#**interface gigaethernet 1** switch(config-if)#**flowcontrol enable** or switch(config-if)#**flowcontrol disable**
jumbo [size]	**Interface configuration mode**	Set jumbo frame size. Use the **no** form of this command to default value. [Jumbo size must be even and between 1522~10240]	1522	switch(config)#**interface gigaethernet 1** switch(config-if)# **jumbo 1524** or switch(config-if)# **jumbo 10240**
rate-limit input-mode {bc|mc|unkuc|knownuc} or **no rate-limit input-mode {bc|mc|unkuc|knownuc}**	**Interface configuration mode**	Set **rate-limit input** mode. You can enable rate-limit for specific packets such as broadcast, multicast, unknown unicast and known unicast. Use the **no** form of this command to disable for that packets	Disable	switch(config)#**interface gigaethernet 1** switch(config-if)# **rate-limit input-mode bc** or switch(config-if)# **no rate-limit input-mode bc** or switch(config-if)# **rate-limit input-mode mc** or switch(config-if)# **no rate-limit input-mode mc**
rate-limit input-rate [value]	**Interface configuration mode**	Set **rate-limit input** rate value. Input rate limit must be between 1~1526	Disable	switch(config)#**interface gigaethernet 1** switch(config-if)# **rate-limit input-rate 1000**
rate-limit output-mode or **no rate-limit output-mode**	**Interface configuration mode**	Set **rate-limit output** mode. You can enable output rate-limit. Use the **no** form of this command to disable output rate	Disable	switch(config)#**interface gigaethernet 1** switch (config-if)# **rate-limit output-mode** switch (config-if)#

		limit.		**no rate-limit output-mode**
rate-limit output-rate [value]	**Interface configuration mode**	Set **rate-limit output** rate value. Range is 1~3130 for 312Kbps unit on the port. Output rate limit must be between 1~3130	Disable	switch (config)#**interface gigaethernet 1** switch (config-if)# **rate-limit output-rate 1000**
shutdown or **no shutdown**	**Interface configuration mode**	Use the **shutdown** Interface configuration command to disable the port. Use the **no shutdown** form of this command to enable the port.	Enable	switch (config)#**interface gigaethernet 1** switch(config-if)# **shutdown** switch(config-if)# **no shutdown**
show interfaces status [gigaethernet|port-channel|vlan] [if-num]	**Privileged EXEC**	Show interface configuration status and configuration.		switch # **show interfaces status gigaethernet 1** or switch # **show interfaces status port-channel 1** or switch # **show interfaces status vlan 1**
show interfaces counters [gigaethernet|port-channel] [if-num]	**Privileged EXEC**	Show interface statistic counter.		switch # **show interfaces counters gigaethernet 1** or switch # **show interfaces counters port-channel 1**

Mac / Filter Table Commands Set

Commands	Command Level	Description	Default	Example
mac-address-table aging-time [sec.] or	**Global configuration mode**	Use the **mactbl aging-time** global configuration command to set the length of time that a	300 secs	(Enable) switch(config)# **mac-address-table aging-time**

no mac-address-table aging-time		dynamic entry remains in the MAC address table after the entry is used or updated. Range: 0-300 seconds; 0 to disable aging) Use the **no** form of this command to use the default aging-time interval. The aging time applies to all VLANs. time must be 20~620 and in steps of 20 seconds		**150** (Disable) switch(config)# **mac-address-table aging-time 0** (Default) switch(config)# **no mac-address-table aging-time**
mac-address-table static hwaddr [MAC] vlan [VLAN-ID] or **no mac-address-table static hwaddr [MAC] vlan [VLAN-ID]**	**Interface configuration mode**	Configure MAC address table of interface (static) Remove an entry of MAC address table of interface (static)		config)#**interface gigaethernet 1** switch(config-if)#**mac-address-table static hwaddr 000012345678 vlan 1** or config)#**interface gigaethernet 1** switch(config-if)#**no mac-address-table static hwaddr 000012345678 vlan 1**
mac-address-table filter hwaddr [MAC] vlan [VLAN-ID] or **no mac-address-table filter hwaddr [MAC] vlan [VLAN-ID]**	**Global configuration mode**	Configure MAC address table(filter) Remove an entry of MAC address table (filter)		switch(config)#**mac-address-table filter hwaddr 000012348678 vlan 1** or switch(config)#**no mac-address-table filter hwaddr 000012348678 vlan 1**
show mac-address-table [static|filter|all] or **show mac-address-table static** or **show**	**Privileged EXEC mode**	Show static MAC address table Show filter MAC address table. Show all MAC address table		switch#**show mac-address-table static** or switch#**show mac-address-table filter** or

mac-address-table filter or **show mac-address-table all**				switch#**show mac-address-table all**
show mac-address-table aging-time	**Privileged EXEC mode**	Show current aging time setup		switch#**show mac-address-table aging-time**

Port Mirroring Commands Set

Commands	Command Level	Description	Default	Example
monitor [port number] [rx | tx | both] or **no monitor [port number| all]**	**Interface configuration mode**	Use the port monitor interface configuration command to enable Switch Port Analyzer (SPAN) port monitoring on a port. Use the **no** form of this command to return the port to its default value.		switch(config)#interface gigaethernet 1 switch(config-if)#monitor 3 both or switch(config-if)#no monitor 3 or (Disable) switch(config-if)# no monitor all
show monitor	**Privileged EXEC**	Show port monitor information		switch#show monitor

TFTP Commands Set

Commands	Command Level	Description	Default	Example
backup flash:backup_cfg	**Global configuration mode**	Save configuration to TFTP server and need to specify the IP of TFTP server and the file name of image.		switch(config)#**backup flash:backup_cfg**
restore flash:restore_cfg	**Global configuration mode**	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.		switch(config)#**restore flash:restore_cfg** TFTP server ip address [192.168.16.2]: Restore file name [restore.dat]: *config success.*

upgrade flash:upgrade_fw	**Global configuration mode**	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.		switch(config)#**upgrade lash:upgrade_fw**

QOS Commands Set

Commands	Command Level	Description	Default	Example
show qos	**Privileged EXEC**	Show QoS settings		switch#**show qos**
qos priority cos [Cos] [Qid] or **no qos priority cos**	**Global configuration mode**	Configure COS Priority	Qid = Traffic Class	switch(config)#**qos priority cos 0 2** or (Default) switch(config)# **no qos priority cos**
qos priority dscp [dscp] [Qid] or **no qos priority dscp**	**Global configuration mode**	Set DSCP Map		switch(config)# **qos priority dscp 61 5** or (Default) switch(config)# **no qos priority dscp**
qos priority profile [profile]	**Global configuration mode**	Set Qos Port Profile [0~3]	0	switch(config)# **qos priority profile 3**
qos priority portbased[Qid] or **no qos priority portbased**	**Interface configuration mode**	Set Qos Port Priority [0~7]	0	onfig)#**interface gigaethernet 1** switch(config-if)# **qos priority portbased 3** or (Default) switch(config-if)# **no qos priority portbased**
qos priority precedence [port-base| cos-only| dscp-only| dscp-first]	**Global configuration mode**	Set Priority Precedence	Port-base	switch(config)# **qos priority precedence port-base** or switch(config)# **qos priority precedence cos-only** or

or **no qos priority precedence**				switch(config)# **qos priority precedence dscp-only** or switch(config)# **qos priority precedence dscp-first** or (Default) switch(config)# **no qos priority precedence**

Spanning Tree Commands Set

Commands	Command Level	Description	Default	Example
show spanning-tree	**Privileged EXEC**	Display a summary of the spanning-tree states.		switch#**show spanning-tree**
spanning-tree enable or **no spanning-tree**	**Global configuration mode**	Enable/disable spanning tree	Disable	switch(config)#**spanning-tree enable** or switch(config)#**no spanning-tree**
spanning-tree priority [0~61440]	**Global configuration mode**	Use the spanning-tree priority global configuration command to change the priority. Priority must be a multiple of 4096	32768	switch(config)#**spanning-tree priority 4096**
spanning-tree max-age [6~40seconds]	**Global configuration mode**	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	20 sec	switch(config)#**spanning-tree max-age 15**
spanning-tree hello-time [1~10seconds]	**Global configuration mode**	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol	2 sec.	switch(config)#**spanning-tree hello-time 3**

		data units (BPDUs).		
spanning-tree forward-time [4~30seconds]	**Global configuration mode**	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	15 sec.	switch(config)#**spanning-tree forward-time 20**
stp-port priority [port priority] pathcost [path cost]	**Interface configuration mode**	Use the **stp-port** interface configuration command to configure a port priority and path cost that is used when two switches tie for position as the root switch.	128	switch(config)#**interface gigaethernet 1** switch(config-if)# **stp-port priority 16 pathcost 200000**
stp-admin-p2p [disable|enable|auto]	**Interface configuration mode**	Use the stp-admp2p interface configuration command to configure a port AdmP2P variable.	Enable	switch (config)#**interface gigaethernet 1** switch(config-if)# **stp-admin-p2p auto** or switch(config-if)# **stp-admin-p2p enable** or switch(config-if)# **stp-admin-p2p disable**
stp-admin-edge [disable|enable]	**Interface configuration mode**	Use the stp-admedge interface configuration command to configure a port AdmEdge variable.	Enable	switch (config)#**interface gigaethernet 1** switch(config-if)# **stp-admin-edge enable** or switch(config-if)# **stp-admin-edge disable**

stp-admin- stp [disable|enable]	**Interface configuration mode**	Use the stp-admstp interface configuration command to configure a port controlled by stp protocol.	Enable	switch (config)#**interface gigaethernet 1** switch(config-if)# **stp-admin stp enable**

VLAN Commands Set

Commands	Command Level	Description	Default	Example
vlan database	**Privileged EXEC**	Enter VLAN configure mode		switch#**vlan database** switch(vlan)#
vlanmode [portbase| 802.1q| gvrp]	**VLAN database mode**	To set switch VLAN mode.	**8021q**	switch(vlan)#**vlanmode portbase** or switch(vlan)#**vlanmode 802.1q** or switch(vlan)#**vlanmode gvrp**
show vlan **or** **show vlan [GroupName| VLAN ID]**	**VLAN database mode**	Show VLAN information		switch(vlan)#**show vlan** or switch(vlan)#**show vlan 2**
Port Base VLAN mode				
no vlan group [VLAN ID]	**VLAN database mode**	Delete port base group ID		switch(vlan)#**no vlan group 2**
vlan port-based grpname [Group Name] grpid [VLAN ID] port [PortNumbers]	**VLAN database mode**	Add new port based VALN		switch(vlan)#**vlan port-based grpname test grpid 2 port 2-4** or switch(vlan)#**vlan port-based grpname test grpid 2 port 2,3,4**
802.1Q | 802.1Q with GVRP VLAN mode*				
vlan 8021q name [GroupName] vid [VLAN ID] media	**VLAN database mode**	Change the name of VLAN group, if the group didn't exist, this command can't be applied.		switch(vlan)# **vlan 8021q name RD vid 2 media gigaethernet state**

gigaethernet state active or **no vlan 8021q [VLAN ID]**		or Delete port base group ID		**active** or switch(vlan)#**no vlan 8021q 2**
switchport allowed vlan 8021q add [VLAN ID] [tagged|untagged] or **switchport allowed vlan 8021q remove [VLAN ID]** or **no switchport allowed vlan8021q**	**Interface configuration mode**	Add port to the VLAN Remove port to the VLAN Remove port from all VLAN except default VLAN		onfig)#**interface gigaethernet 1** switch(config-if)# **switchport allowed vlan 8021q add 2 tagged** or switch(config-if)# **switchport allowed vlan 8021q remove 2** or switch(config-if)# **no switchport allowed vlan 8021q**
switchport native vlan [PVID] or **no switchport native vlan**	**Interface configuration mode**	Set Port PVID	**1**	switch(config)# **interface gigaethernet 1** switch(config-if)# **switchport native vlan 2** or switch(config-if)# **no switchport native vlan**
switchport acceptable-frame-types [all|tagged] or **no switchport acceptable-frame-types**	**Interface configuration mode**	Set accept frame type	**all**	switch(config)# **interface gigaethernet 1** switch(config-if)# **switchport acceptable-frame-types all** or switch(config-if)# **no switchport acceptable-frame-types**
switchport ingress-filtering or **no switchport ingress-filtering**	**Interface configuration mode**	Set ingress filter	**disable**	switch(config)# **interface gigaethernet 1** switch(config-if)# **switchport ingress-filtering** or switch(config-if)# **no switchport ingress-filtering**

show vlan [id|name] [VLAN ID | Name]	**Privileged EXEC**	Show VLAN of Group Name or VLAN ID information **vlanid:** 1 ~ 4094		switch#**show vlan id**
show interfaces switchport [gigaethernet|port-channel] [port]	**Privileged EXEC**	show Port PVID and ingress filter & accept frame type		switch# **show interfaces switchport gigaethernet 1**

*Future Release

System log Commands Set

Commands	Command Level	Description	Default	Example
show logging [flash | ram | sendmail | trap| map]	**Privileged EXEC**	Show system log information		switch# **show logging flash**
logging-mode {local|remote|smtp} or **no logging-mode {local|remote|smtp}**	**Global configuration mode**	Enable logging mode for local, remote and smtp		Switch(config)# **logging-mode local** Switch(config)# **no logging-mode local** Switch(config)# **logging-mode remote**
logging-local history [flash | ram] [level] or **no logging-local history [flash | ram]**	**Global configuration mode**	Set system log level	Flash:3(level 3-0) RAM:7(level 7-0)	Switch(config)# **logging-local history flash 3**

logging-events [coldstart | warmstart | authfailure | portlinkchange] [level] or **no logging-events [coldstart | warmstart | authfailure | portlinkchange]**	**Global configuration mode**	Set the level of each logging events.	Level 7	Switch(config)# **logging-events coldstart 3** Switch(config)# **no logging-events coldstart**
Logging-host [server] or **no logging-host [server]**	**Global configuration mode**	Add or delete the remote server address		Switch(config)# **logging-host 192.168.16.5** Switch(config)# **no logging-host 192.168.16.5**
logging facility [value] or **no logging facility**	**Global configuration mode**	Set system log facility	23	Switch(config)# **logging facility 19** Switch(config)# **no logging facility**
logging trap [value] or **no logging trap**	**Global configuration mode**	Set system log trap	7	Switch(config)# **logging trap 4** Switch(config)# **no logging trap 4**
clear logging-local [flash | ram]	**Global configuration mode**	Clear system log buffer		Switch(config)# **clear logging-local flash**
logging sendmail {host-0|host-1} [server] or **no logging**	**Global configuration mode**	Set the SMTP server address		Switch(config)# **logging sendmail host-0 192.168.16.5** Switch(config)# **no logging**

sendmail {host-0|host-1}				**sendmail host-0 192.168.16.5**
logging sendmail level [value] or **no logging sendmail level**	**Global configuration mode**	Set system log SMTP level	7	Switch(config)# **logging sendmail level 4** Switch(config)# **no logging sendmail level 4**
logging sendmail {src-0|src-1} [email addr] or **no logging sendmail {src-0|src-1}**	**Global configuration mode**	Set system log SMTP source-email address		Switch(config)# **logging sendmail src-0 bill@this-company.com** Switch(config)# **no logging sendmail src-0 bill@this-company.com**
logging sendmail {dst-0|dst-1} [email addr] or **no logging sendmail {dst-0|dst-1} [email addr]**	**Global configuration mode**	Add or delete system log SMTP destination-email address		Switch(config)# **logging sendmail dst-0 bill@this-company.com** Switch(config)# **no logging sendmail dst-0 bill@this-company.com**
logging sendmail service or **no logging sendmail service**	**Global configuration mode**	Enable or disable system log SMTP	Disable	Switch(config)# **logging sendmail service** Switch(config)# **No logging sendmail service**

SNTP Commands Set

Commands	Command Level	Description	Default	Example

calendar set [hour] [min] [sec] [day] [mon] [year]	**Global configuration mode**	Set system time		switch(config)# **calendar set 15 03 30 29 4 2006**
sntp timezone hours [hours] minute [min] [after-UTC|before-UTC]	**Global configuration mode**	Set timezone index, use “show sntp timezone” command to get more information of index number		switch(config)# **sntp timezone hours 9 minute 0 after-UTC**
show sntp timezone	**Privileged EXEC**	Show index number of time zone list		switch#**show sntp timezone**
no sntp timezone	**Global configuration mode**	Set system time zone to default	(GMT+08:00)	switch(config)# **no sntp timezone**
show sntp	**Privileged EXEC**	Show system time configuration.		switch# **show sntp**
sntp server [ipaddr]	**Global configuration mode**	Set SNTP server IP address.		switch(config)# sntp server 192.168.16.5
no sntp server	**Global configuration mode**	Set SNTP server IP address to default.	NULL	switch(config)# no sntp server
sntp enable	**Global configuration mode**	Enable SNTP Client.		switch(config)#**sntp enable**
no sntp	**Global configuration mode**	Disable SNTP Client.		switch(config)#**no sntp**
sntp poll [sec]	**Global configuration mode**	Set SNTP client polling interval seconds.	16	switch(config)# sntp poll 60
no sntp poll	**Global configuration mode**	Set SNTP client polling interval seconds to default.		switch(config)# no sntp poll

IGMP Commands Set

Commands	Command Level	Description	Default	Example
igmp enable	**Global**	Enable IP IGMP Snooping	disable	switch(config)#**igmp enable**

	configuration mode	service.		
no igmp	**Global configuration mode**	Disable IP IGMP Snooping service to default disable.		switch(config)#**no igmp**
igmp-query {enable |disable |auto}	**Global configuration mode**	Set IP IGMP query mode.	disable	switch(config)#**igmp-query auto**
igmp vlan [vid] static [ipaddr] [gigaethernet|port-channel] [port]	**Global configuration mode**	Adds a static multicast group and its member port.		switch(config)# **igmp vlan 1 static 224.0.0.251 gigaethernet 1**
no igmp vlan [vid] static [ipaddr] [gigaethernet|port-channel] [port]	**Global configuration mode**	Remove a static multicast group and its member port.		switch(config)# **no igmp vlan 1 static 224.0.0.251 gigaethernet 1**
show igmp configuration	**Privileged EXEC**	Displays the details of an IGMP configuration		switch#**show igmp configuration**
show mactbl multicast vlan [vid]	**Privileged EXEC**	Shows known multicast addresses for specific VLAN Id.		switch#show mactbl multicast vlan 1
show mactbl multicast [user | igmp-snooping]	**Privileged EXEC**	Shows known multicast addresses only the user-configured multicast entries or only entries learned through IGMP snooping.		switch#show mactbl multicast user

TRUNK Commands Set

Commands	Command Level	Description		Example
interface port-channel [group id]	**Global configuration mode**	Configures a trunk and enters interface configuration mode for the trunk. If the trunk group isn't exist, you should create it by add a member port		switch(config)# **interface port-channel 1**
no interface port-channel	**Global configuration**	Delete the trucking group.		switch(config)# **no interface port-channel 1**

[group id]	**mode**			
trunk mode [lacp|static] or **no trunk mode**	**Interface configuration mode**	Configure the mode of the trunk group.	static	switch(config)# **interface port-channel 1** switch(config-if)# **trunk mode static** **or** switch(config-if)# **no trunk mode**
channel-group [group id]	**Interface configuration mode**	Adds a port to a trunk. If the trunk group doesn't exist, it will create the group.		switch(config)# **interface gigaethernet 1** switch(config-if)# **channel-group 1**
no channel-group	**Interface configuration mode**	Remove a port from a trunk.		switch(config)# **interface gigaethernet 1** switch(config-if)# **no channel-group 1**
show interfaces status port-channel [group id]	**Privileged EXEC**	Shows trunk information		switch# **show interfaces status port-channel 1**
show port activity	**Privileged EXEC**	Show lacp port activity information	active	switch#**show port activity**
port {active|passive}	**Interface configuration mode**	Set port active|passive		switch(config)# **interface gigaethernet 1** switch(config-if)# **port passive**

SNMP Commands Set

Commands	Command Level	Description	Default	Example
snmp name [station name]	**Global configuration mode**	Configure station name.		switch(config)# **snmp name station1**
snmp location [station location]	**Global configuration mode**	Configure station location.		switch(config)# **snmp location Taiwan**
snmp contact [station contact]	**Global configuration mode**	Configure station contact.		switch(config)# **snmp contact support@level1.com**

snmp community-strings [Community] right [RO/RW]	**Global configuration mode**	Add SNMP community string.	**public, private**	switch(config)#**snmp community-strings public right rw**
no snmp community-strings [Community]	**Global configuration mode**	Remove the specified community.		switch(config)#**no snmp community-strings public**
snmp-server host [IP address] community [Community-string]	**Global configuration mode**	Configure SNMP trap manager information and community string		switch(config)#**snmp-server host 192.168.1.50 community public**
no snmp-server host [Host-address]	**Global configuration mode**	Remove the SNMP server host.		switch(config)#**no snmp-server host 192.168.1.50**
show snmp	**Privileged EXEC**	Show snmp configuration		switch#**show snmp**

DHCP Server Commands Set

Commands	Command Level	Description		Example
dhcpserver [ip start] [ip number]	**Global configuration mode**	Enable dhcp server and add lease entry.		switch(config)#**dhcpserver 192.168.1.5 5** Netmask [255.255.255.0]: **255.255.255.0** Gateway [192.168.16.254]: **192.168.16.254** DNS [192.168.16.254]: **192.168.16.254** Lease Duration [24](hours) **24**
no dhcpserver	**Global configuration mode**	Disable dhcp server.		switch(config)#**no dhcpserver**
show dhcpserver	**Privileged EXEC**	Show configuration of dhcp server and client status.		switch#**show dhcpserver**

Security IP Commands Set

Commands	Command Level	Description	Default	Example
security [entry id] ip [ip address] http [on/off] telnet [on/off]	**Global configuration mode**	Enable and add security ip. Entry id: 1 - 10		switch(config)# **security 1 ip 192.168.16.5 http on telnet on**
no security	**Global configuration mode**	Disable IP security function		switch(config)#**no security**
show security	**Privileged EXEC**	Show the information of IP security		switch#**show security**

802.1X Commands Set

Commands	Command Level	Description		Example
8021x enable	**Global configuration mode**	Use the 802.1x global configuration command to enable 802.1x protocols.	Disable	switch(config)# **8021x enable**
8021x misc quietperiod [sec.]	**Global configuration mode**	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	60	switch(config)# **8021x misc quietperiod 10**
8021x misc txperiod [sec.]	**Global configuration mode**	Use the 802.1x misc TX period global configuration command to set the TX period.	30	switch(config)# **8021x misc txperiod 5**
8021x misc supportimeout [sec.]	**Global configuration mode**	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	30	switch(config)# **8021x misc supportimeout 20**
8021x misc servertimeout [sec.]	**Global configuration mode**	Use the 802.1x misc server timeout global configuration command to set the server timeout.	30	switch(config)#**8021x misc servertimeout 20**
8021x misc maxrequest [number]	**Global configuration mode**	Use the 802.1x misc max request global configuration command to set the MAX	2	switch(config)# **8021x misc maxrequest 3**

		requests.		
8021x misc reauthperiod [sec.]	**Global configuration mode**	Use the 802.1x misc reauth period global configuration command to set the reauth period.	3600	switch(config)# **8021x misc reauthperiod 3000**
8021x portstate [disable | reject | accept | authorize]	**Interface configuration mode**	Use the 802.1x port state interface configuration command to set the state of the selected port.	Disable	switch(config)# **interface gigaethernet 1** switch(config-if)#**8021x portstate accept**
show 8021x	**Privileged EXEC**	Displays a summary of the 802.1x properties and also the port status.		switch#**show 8021x**
8021x system radiusip [IP address]	**Global configuration mode**	Use the 802.1x system radius IP global configuration command to change the radius server IP.		switch(config)# **8021x system radiusip 192.168.1.1**
8021x system serverport [port ID]	**Global configuration mode**	Use the 802.1x system server port global configuration command to change the radius server port		switch(config)# **8021x system serverport 1815**
8021x system accountport [port ID]	**Global configuration mode**	Use the 802.1x system account port global configuration command to change the accounting port		switch(config)# **8021x system accountport 816**
8021x system sharekey [ID]	**Global configuration mode**	Use the 802.1x system share key global configuration command to change the shared key value.		switch(config)# **8021x system sharekey 123456**

LLDP Commands Set

Commands	Command Level	Description	Default	Example
lldp [enable] or **no lldp**	**Global configuration mode**	Enable or disable LLDP protocol.	Disable	switch(config)# **lldp enable** or switch(config)# **no lldp**
show lldp status	**Privileged EXEC**	Show LLDP status.		switch# **show lldp status**

show lldp remote	**Privileged EXEC**	Show LLDP remote table.		switch# **show lldp remote**
lldp-port [disable |rx|tx|both]	**Interface configuration mode**	Use those commands to set lldp port tx and rx mode.	Disable	switch(config)# **interface gigaethernet 1** switch(config-if)# **lldp-port disable** or switch(config-if)# **lldp-port rx**

ACL Commands Set

Commands	Command Level	Description	Defaults	Example
acl-port [deny|permit] or **no acl-port**	**Interface configuration mode**	Use the acl-port interface configuration command to enable Access Control on a port. The default action can be Deny or Permit. Use the no form of this command to return the port to its default value (disable).	Disable	switch(config)# **interface gigaethernet 1** switch(config-if)# **acl-port deny** or switch(config-if)# **no acl-port**
acl-rule [index] dst [dstIp/prefix] src [srcIp/prefix] {deny|permit} or **no acl-rule [index]**	**Interface configuration mode**	Use those commands to add or delete the acl rules of the port. [index] range= 0~4	**N/A**	switch(config)# **interface gigaethernet 1** switch(config-if)# **acl-rule 0 dst 192.168.16.1/32 src 192.168.16.2/32 permit** or switch(config-if)# **no acl-rule 0**
show acl [gigaethernet|port-channel][port]	**Privileged EXEC**	Show acl configuration of the port.	**N/A**	switch# **show acl gigaethernet 1**