OPTICAL
SYSTEMS
DESIGN

# OPERATOR MANUAL

## OSD2700SFP SERIES

## MANAGED 24-PORT 100BASE SFP AND 4-COMBO PORT GIGABIT ETHERNET SWITCH

# INDEX 1

# 1 QUICK START GUIDE

This quick start guide describes how to install and use the Managed Ethernet Switch.

## 1.1 FUNCTIONAL DESCRIPTION

- RS-232 console, Telnet, SNMP v1 & v2c & v3, RMON, Web Browser, and TFTP management.
- Supports Command Line Interface in RS-232 console.
- Supports 8192 MAC addresses. Provides 3M bits memory buffer.
- Supports IEEE802.3i/802.3u/802.3ab/802.3z/802.3x. Auto-negotiation: 1000Mbps-full-duplex; 10/100Mbps-full/half-duplex; Auto MDI/MDIX.
- 100Base-FX: Multi mode LC type, Single mode LC type; 100Base-BX: WDM Single mode LC type.
- 1000Base-SX/LX: Multi mode LC type, Single mode LC type; 1000Base-BX: WDM Single mode LC type.
- 10/100Base-T available on 24-Ports only if copper SFP used.
- SFP socket for Gigabit fiber optic expansion.
- Store-and-forward mechanism.
- Full wire-speed forwarding rate.
- AC inlet power socket: 90~264VAC, 50~60Hz internal universal PSU.
- Supports redundant power supplies for flexible application.
- -10℃ to 60℃ operating temperature range.
- Metal case.
- Supports Rack Mounting installation.

## 1.2 PHYSICAL DESCRIPTION

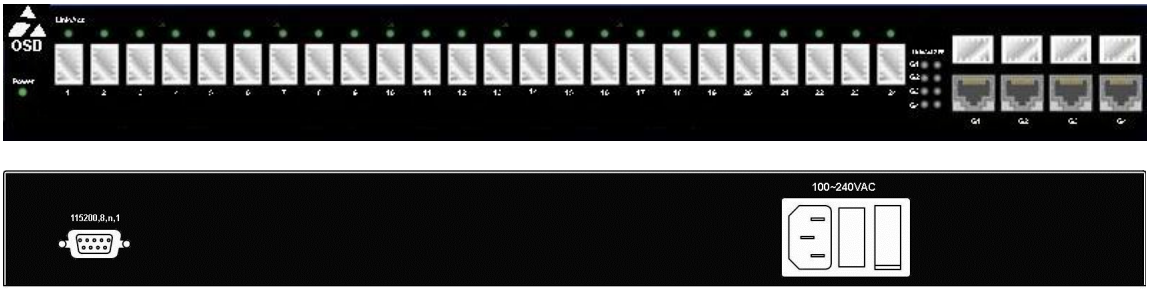



FIGURE 1: OSD2700SFP FRONT AND REAR PANELS

TABLE 1: OSD2700SFP LED FUNCTIONS

| LED | State | Indication |
|---|---|---|
| Power | Green | Power On |
| | Off | Power Off |
| 10/100Base-TX, 100Base-FX/BX | | |
| Link/ACT x 24 | Steady | A valid network connection established |
| | Flashing | Transmitting or receiving data<br>ACT stands for ACTIVITY |
| 10/100/1000Base-TX, SFP, 1000Base-SX/LX/BX | | |
| Link/ACT x 4 | Steady | A valid network connection established |
| | Flashing | Transmitting or receiving data<br>ACT stands for ACTIVITY |
| SFP | | |
| SFP | Steady | A valid SFP connection established |
| | Off | SFP not fitted |

## 1.3 CONSOLE CONFIGURATION

### 1.3.1 CONNECT TO THE SWITCH CONSOLE:

Connect the DB9 straight cable to the RS-232 serial port of the device and the RS-232 serial port of the terminal or computer running the terminal emulation application. Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as HyperTerminal) to the switch console port.

### 1.3.2 CONFIGURATION SETTINGS OF THE TERMINAL-EMULATION PROGRAM:

Baud rate: 115,200bps
Data bits: 8
Parity: none
Stop bit: 1
Flow control: none
Press the “Enter” key. The Command Line Interface (CLI) screen should appear as below:
Logon to Exec Mode (View Mode):
At the “switch_a login:” prompt just type in “root” and press <Enter> to logon to Exec Mode (or View Mode). And the “switch_a>” prompt will show on the screen.

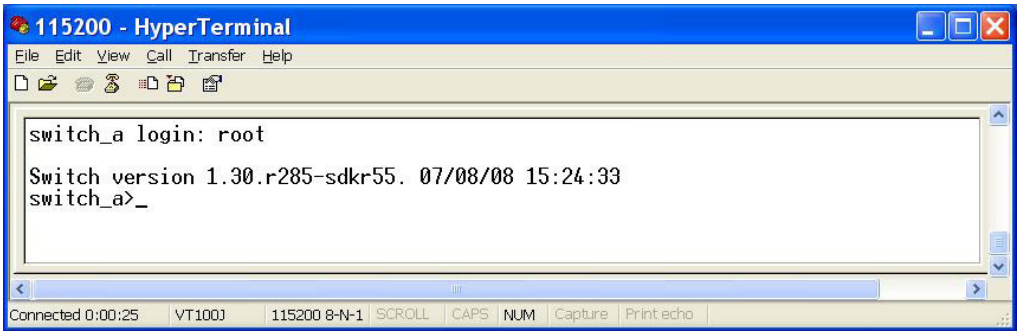



FIGURE 2: CLI LOGIN

- Logon to Privileged Exec Mode (Enable Mode):
  At the “switch_a>” prompt just type in “enable” and press <Enter> to logon to Privileged Exec Mode (or Enable Mode). And the “switch_a#” prompt will show on the screen.
- Logon to Configure Mode (Configure Terminal Mode):
  At the “switch_a#” prompt just type in “configure terminal” and press <Enter> to logon to Configure Mode (or Configure Terminal Mode). And the “switch_a(config)#” prompt will show on the screen.
- Set new IP address and subnet mask for Switch:
  At the “switch_a(config)#” prompt just type in “interface vlan1.1” and press <Enter> to logon to vlan 1 (vlan1.1 means vlan 1). And the “switch_a(config-if)#” prompt will show on the screen.

Command Syntax: “ip address A.B.C.D/M”. “A.B.C.D” specifies IP address. “M” specifies IP subnet mask. “M”= 8: 255.0.0.0, 16:255.255.0.0, or 24: 255.255.255.0.
For example, At the “switch_a(config-if)#” prompt just type in “ip address 192.168.1.10/24” and press <Enter> to set new IP address (192.168.1.10) and new IP subnet mask (255.255.255.0) for Switch.

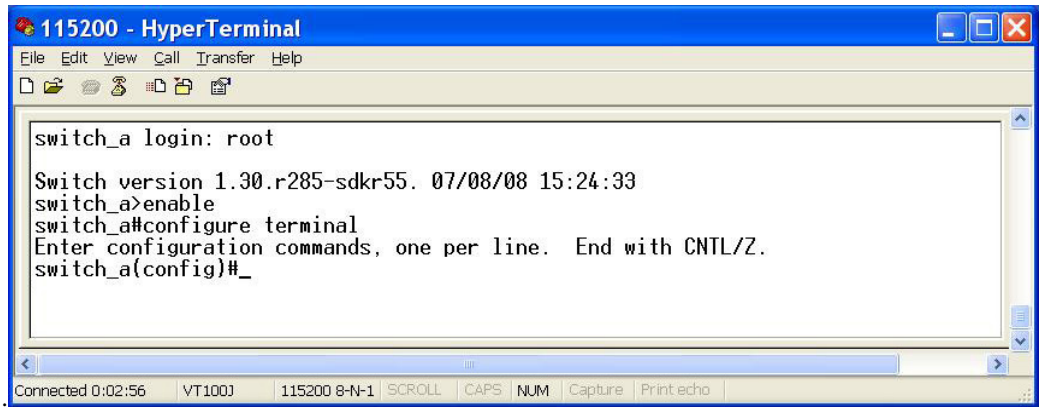



FIGURE 3: CLI CONFIG

## 1.4 WEB CONFIGURATION

- Login the switch:
  Specify the default IP address (192.168.1.10) of the switch in the web browser. A login window will be shown as below:

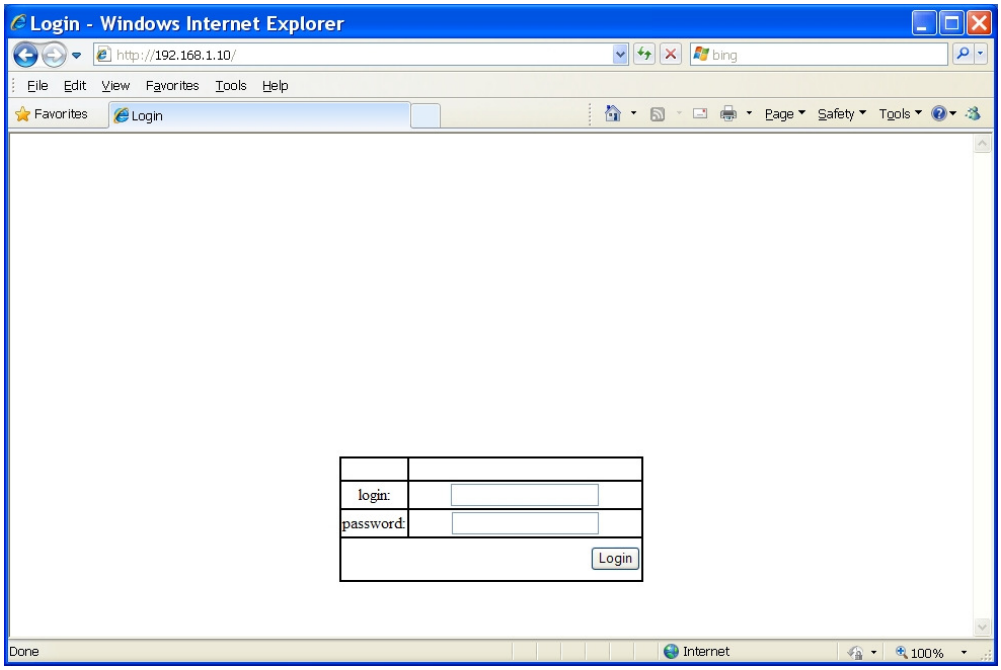



FIGURE 4: WEB LOGIN

- Enter the factory default login ID: root.
  Enter the factory default password (no password).
  Then click on the “Login” button to log on to the switch.

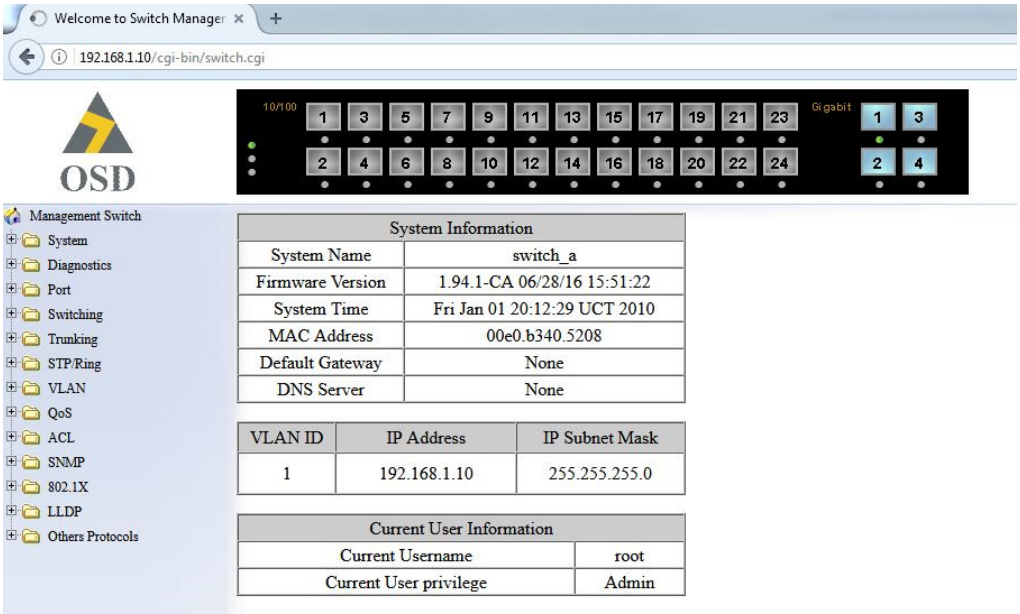



FIGURE 5: WEB CONFIG

# 2 TECHNICAL SUMMARY

## 2.1 BRIEF DESCRIPTION

### 2.1.1 PREFACE

This manual describes how to install and use the OSD2700SFP Managed Ethernet Switch. The OSD2700SFP switch is designed to deliver full scalability with SNMP/RMON web-based management functions. To get the most out of this manual, you should have an understanding of Ethernet networking concepts.

### 2.1.2 OVERVIEW

The OSD2700SFP is a managed 24-port 100BASE-SFP and 4-port Gigabit Ethernet switch designed to operate in tough industrial applications providing real-time redundant performance. The four 1000Base RJ45 copper ports and four Gigabit SFP ports are combo ports - It is possible to use either the RJ45 port of the SFP port per channel (G1, G2, G3, G4). ie It is not possible to use both at the same time. SFPs are sold separately.

The unit will operate on either 1310nm and/or 1550nm singlemode. Operation over at least 40km of singlemode fiber is possible by use of the appropriate SFP optical devices. It normally requires two fibers per SFP port but is optionally available for one fiber operation.

A major benefit of the OSD2700SFP is its reliable and consistent performance over the -10°C to +60°C temperature range that allows it to be used in uncontrolled environments such as roadside cabinets, mine sites and factories.

### 2.1.3 APPLICATIONS

- Any network utilising a mix of copper and fiber
- Industrial IP communications
- Self-healing Gigabit Ethernet backbone networks
- Gigabit Combo ports: copper (RJ45) or fiber (SFP)

### 2.1.4 FEATURES AND BENEFITS

- Complies with IEC61850-3/IEEE1613 for power substations & EN50121-4 for railway applications.
- Complies with IEEE802.3i/802.3u/ 802.3ab 10/100/1000Base-T, IEEE802.3z 1000Base-LX standards on the four combo ports.
- Supports RSTP/MSTP/STP for Ethernet redundancy IP Multicast Filtering through IGMP Snooping V1, V2 & V3
- Supports port-based VLAN and IEEE802.1Q VLAN Tagging and GVRP
- IEEE802.1p QoS with four priority queues
- MAC-based trunking with automatic link fail-over
- Port mirroring
- Per-port programmable MAC address locking
- RS232 console, Telnet, SNMP V1, V2c & V3, RMON, Web Browser, and TFTP Management
- Full wire-speed forwarding rate
- Supports IEEE802.1x Security
- Bandwidth Rate Control
- Up to 24 Static Secure MAC addresses per port
- Supports NTP
- SFP modules sold separately
- 1000Mbps-Full-duplex, 10/100Mbps-Full/Half-duplex, Auto-Negotiation, Auto-MDI/MDIX
- Operates over the temperature range of -10°C to +60°C

## 2.2 TYPICAL CONFIGURATION

Figure 6 below indicates a possible set-up for an OSD2700 system.

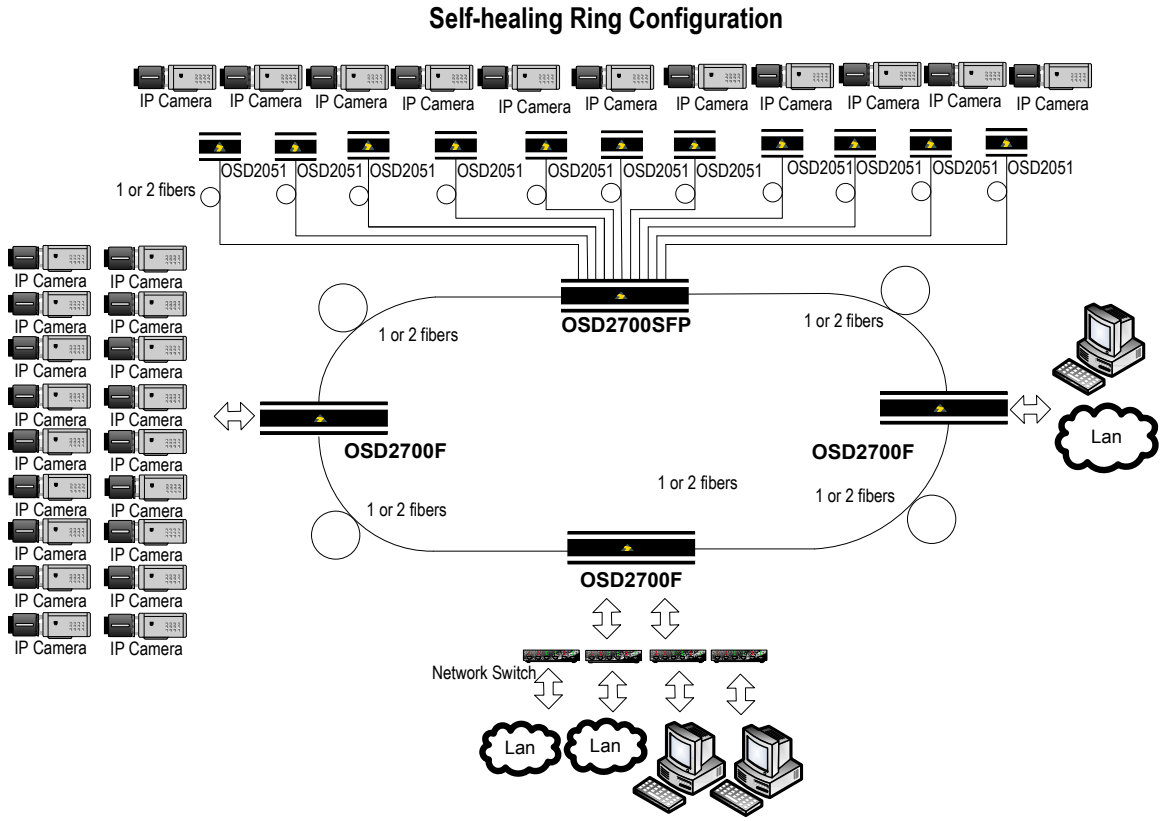



FIGURE 6: OSD2700SFP TYPICAL CONFIGURATION

## 2.3 TECHNICAL SPECIFICATIONS

TABLE 2: TECHNICAL SPECIFICATIONS

| SPECIFICATION | PERFORMANCE |
|---|---|
| **24 x SFP Ports** | |
| Standards | IEEE802.3u |
| Optical connector | LC Standard |
| SFP Port Options | 100Base-SFP (Contact OSD for SFP options) |
| **4 x RJ45/SFP Combo Ports** | |
| Standards | IEEE802.3i, IEEE802.3ab for 10, 100 or 1000Base-T Ethernet |
| Optical Connector | LC Standard |
| Electrical Connector | RJ45 |
| SFP Port Options | 1000Base-Lx, 10/100/1000Base-T (Contact OSD for SFP options) |
| Optical Data Interface | IEEE802.3z, 100Base-Lx, 1000Base-Sx, IEEE802.3u, 100Base-Fx |
| Transmitter Wavelength | Refer to OSD SFP datasheets or contact OSD sales for options |
| Transmit Optical Power | |
| Receiver Sensitivity | |
| Standard Optical Link Budget | Optical link budgets are SFP dependant. Refer to OSD SFP data sheets or contact OSD sales for options/details. |
| Optional Optical Link Budget | |
| Operating Mode | Half or full duplex for 10/100<br>Full duplex for 1000<br>Store-and-Forward<br>Half-duplex back-pressure and IEEE802.3x full-duplex flow control |
| **Common** | |
| Standards | IEC61850-3/IEEE1613 for power substations & EN50121-4 for railway applications |
| Indicators | 1x Power<br>24x 100Base-T, 100BaseFx: Link/Activity<br>4x 10/100/1000Base-T, 100Base-Sx, 1000Base-Lx: Link/Activity |
| Configuration Connector | DB9 |
| Dimensions (mm) | 442W x 250D x 44H |
| Weight | 4.1kg |
| Power Requirements | 90-264$V_{AC}$ @ 45VA Max |
| Operating Temperature | -10°C to +60°C |
| Relative Humidity | 5 to 95% non-condensing |

## 2.4 OSD2700 FRONT AND REAR PANELS

There are 24 fixed 100M SFP ports, four fixed Gigabit copper ports and four optional Gigabit SFP ports which can be either copper or fiber on the front panel. The rear panel consists of a DB9 configuration connector and an IEC power. Each section will be described further throughout this manual.

*Note: The 4 SFP ports and 4 fixed Copper ports are Gigabit combo ports. It is possible to use either the RJ45 port or the SFP port per channel (G1, G2, G3, G4). ie It is not possible to use both at the same time.

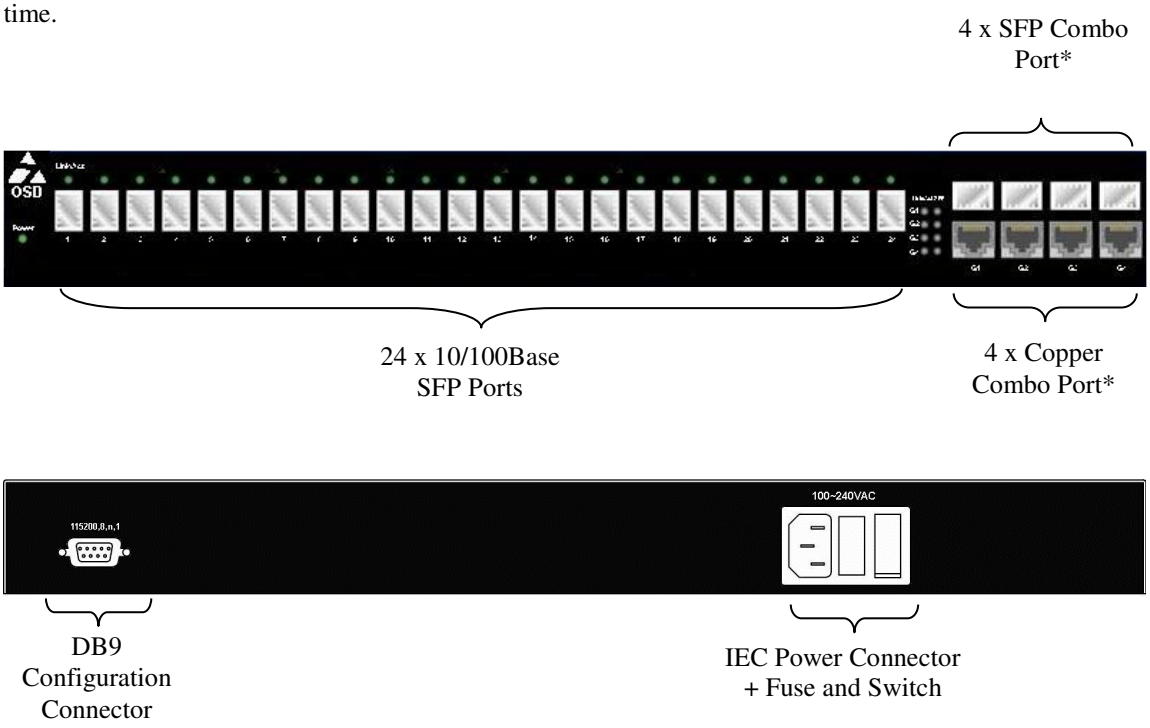
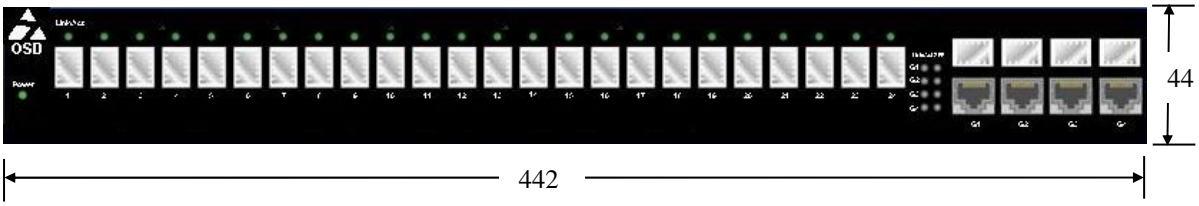



FIGURE 7: OSD2700SFP FRONT AND REAR PANELS

### 2.4.1 OSD2700SFP DIMENSIONS

The OSD2700SFP is designed to be mounted onto a 19” rack unit occupying 1RU space or can be free standing on an even surface.



# 3 INSTALLATION AND OPERATION

## 3.1 INTRODUCTION

This section outlines the methods required to install and operate the OSD2700SFP successfully. It should be studied carefully if damage to the equipment or poor results are to be avoided.

This equipment has been fully tested prior to dispatch and is ready for immediate operation. However it is advisable to check for external transportation damage before operation. If damage is evident, return the unit with the packaging to your supplier immediately.

## 3.2 INSTALLATION

### 3.2.1 WARNING AND PRECAUTIONS

▲ **ELECTROMAGNETIC COMPATIBILITY**

**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.

▲ **OPTICAL OUTPUT OPERATION**

**WARNING**: **Laser Safety:** Class 1 Laser Product per IEC/EN 60825-1:20011 standard.

| **Class 1** |
| --- |
| The OSD2700SFP is a **Class 1 laser product.** |
|  |



**PRECAUTIONS**

- ▲ All service personnel should be provided training as to the hazards of direct viewing of laser radiation and of the precautionary measures during servicing of equipment
- ▲ Areas where laser products are installed should be restricted in access to trained service personnel only and appropriate warning signs posted in the work area.
- ▲ All laser apertures should be covered by protective covers when not connected to optical fibers. Never leave outputs uncovered.
- ▲ Laser equipment should be positioned above or below eye level where possible. Apertures should be positioned away from personnel.
- ▲ Protective eyewear should be worn in the vicinity of laser equipment.

### 3.2.2 POWER SUPPLY CONNECTIONS

The OSD2700SFP requires external 90 to 264$V_{AC}$ @ 45VA Max power. Power should be connected to the power socket located at the back of the unit using standard IEC plug (supplied). Always ensure that the power is off before any installation.

### 3.2.3 DB9 CONFIGURATION CONNECTIONS

The OSD2700SFP has a DB9 DCE connector located on the rear of the unit. Table 3 outlines the pin assignments.

TABLE 3: DB9 CONFIGURATION CONNECTOR

| Pin no. | Name | RS232 Signal name |
|---|---|---|
| 1 | DCD | Data Carrier detect |
| 2 | RxD | Received data |
| 3 | TxD | Transmit data |
| 4 | --- | N/C |
| 5 | GND | Signal ground |
| 6 | DSR | Data set Ready |
| 7 | --- | N/C |
| 8 | CTS | Clear to send |
| 9 | --- | N/C |

### 3.2.4 LED INDICATORS

TABLE 4: OSD2700SFP LED INDICATORS

| LED | State | Indication |
|---|---|---|
| Power | Green | Power on |
| | Off | Power off |
| 10/100Base-TX, 100Base-FX/BX | | |
| Link/ACT x 24 | Steady | A valid network connection established |
| | Flashing | Transmitting or receiving data<br>ACT stands for ACTIVITY |
| 10/100/1000Base-TX, SFP, 1000Base-SX/LX/BX | | |
| Link/ACT x 4 | Steady | A valid network connection established |
| | Flashing | Transmitting or receiving data<br>ACT stands for ACTIVITY |
| SFP | | |
| SFP | Steady | A valid SFP connection established |
| | Off | SFP not installed |

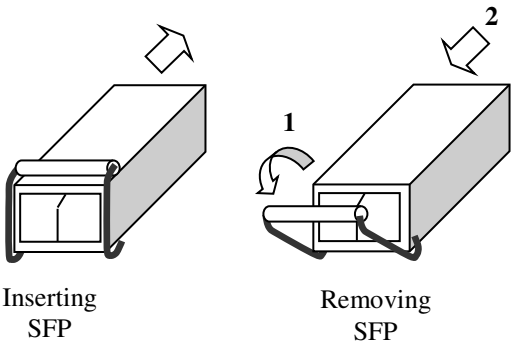
### 3.2.5 FITTING SFP CONNECTORS

Care should be taken when inserting/removing the SFP connectors from SFP ports as SFP modules are Electrostatic (ES) sensitive and Electrostatic Discharge (ESD) precautions should be taken when installing. Ensure that the SFP is fully engaged and latched into position.

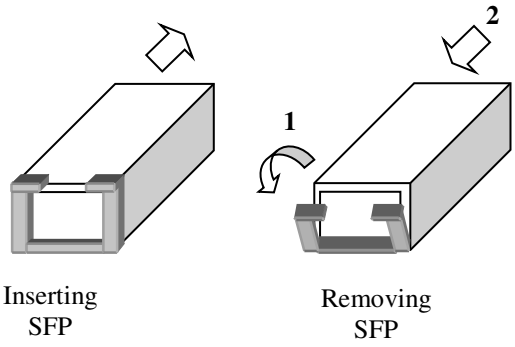
**Inserting SFP** – Ensure that the SFP lever is in the locked position and insert into appropriate SFP port. Gently push the SFP until it locks into place. Remove plastic/rubber dust cap and fit fiber cable or RJ45 plug.

**Removing SFP** – Remove fiber connector or RJ45 plug. Pull the SFP lever down to unlock SFP from housing. Using the lever, gently pull the SFP out.

**Fiber SFP**




**Copper SFP**




Note: The 24 x 10/100BASE SFPs are mounted sideways. SFP handle/Latch must be inserted facing left side as shown below.

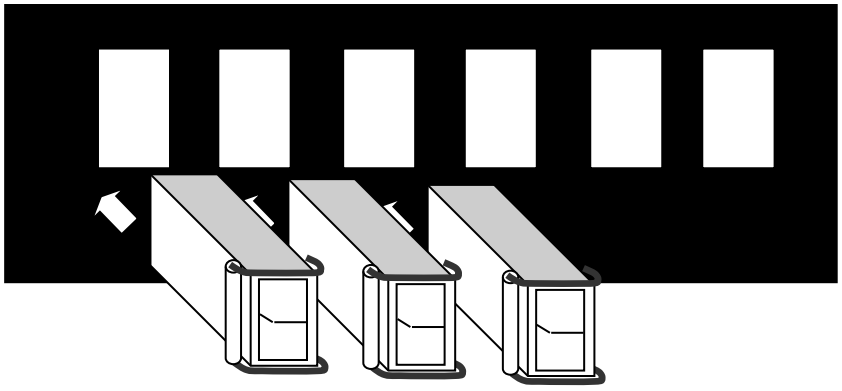


FIGURE 8: FITTING/REMOVING SFP CONNECTORS

## 3.3 OSD2700SFP OPERATION

When using the OSD2700SFP for the first time, check that the unit is in good condition with no visible damage.

Connect the unit to an appropriate power source and check that the indicators illuminate accordingly on power up (see Table 4) after all other connections have been made.

### 3.3.1 CABLE CONNECTIONS

It is necessary to follow the cable specifications below when connecting the switch to your network. Use appropriate cables that meet your speed and cabling requirements.

TABLE 5: CABLE SPECIFICATIONS

| Speed | Connector | Port Speed Half/Full Duplex | Cable | Max. Distance |
|---|---|---|---|---|
| 100Base-TX | RJ-45 | 100/200 Mbps | 2-pair UTP/STP Cat. 5 | 100m |
| 1000Base-T | RJ-45 | 2000 Mbps | 4-pair UTP/STP Cat. 5 | 100m |
| 100Base-FX | LC | 200 Mbps | MMF (62.5µm) | 2km |
| 100Base-FX | LC | 200 Mbps | SMF (10µm) | 20, 40, 75, 100km |
| 100Base-BX | LC | 200 Mbps | MMF (62.5µm) | 2, 5km |
| 100Base-BX | LC | 200 Mbps | SMF (10µm) | 20, 40km |
| SFP | | | | |
| 1000Base-SX | Duplex LC | 2000 Mbps | MMF (62.5µm) | 550m<br>2km |
| 1000Base-LX | Duplex LC | 2000 Mbps | SMF (10µm) | 10, 40, 60km |
| 1000Base-BX | Duplex LC | 2000 Mbps | SMF (10µm) | 70km |

Step 1: First, ensure the power of the switch and end devices are turned off.

Step 2: Prepare cable with corresponding connectors for each type of port in use.

Step 3: Consult Cable Specifications Table on previous page for cabling requirements based on connectors and speed.

Step 4: Connect one end of the cable to the switch and the other end to a desired device.

Step 5: Once the connections between two end devices are made successfully, turn on the power and the switch is operational.

*Note: The 4 Gigabit SFP ports and 4 fixed Copper Ports are combo ports. It is possible to use either the RJ45 port of the SFP port per channel (G1, G2, G3, G4). Ie It is not possible to use both at the same time

# 4 SWITCH MANAGEMENT

This chapter explains the methods that can be used to configure management access to the switch. It describes the types of management applications and the communication and management protocols that deliver data between your management device (workstation or personal computer) and the system. It also contains information about port connection options.

This chapter covers the following topics:

- Management Access Overview
- Key Concepts
- Key Guidelines for Implementation
- Web Management Access
- Administration Console Access
- SNMP Access
- Standards, Protocols, and Related Reading

## 4.1 MANAGEMENT ACCESS OVERVIEW

The switch gives you the flexibility to access and manage the switch using any or all of the following methods.

The web browser interface and administration console (CLI) support are embedded in the switch software and are available for immediate use.

## 4.2 ADMINISTRATION CONSOLE (CLI)

The administration console is an internal, character-oriented, Command Line Interface (CLI) for performing system administration such as displaying statistics or changing option settings.

Using this method, you can view the administration console from a terminal, personal computer, Apple Macintosh, or workstation connected to the switch's console port.

There are two ways to use this management method: direct access or modem access. The following sections describe these methods.

### 4.2.1 DIRECT ACCESS

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as HyperTerminal) to the switch console port.

When using the management method, configure the terminal-emulation program to use the following parameters (you can change these settings after login):

[Default parameters]

- 115,200bps
- 8 data bits
- No parity
- 1 stop bit

This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use any terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator such as TIP.

### 4.2.2 MODEM ACCESS

You can access the switch's administration console from a PC or Macintosh using an external modem attached to the console port. The switch management program provides **Console Port** screen, accessible from the **Basic Management** screen that lets you configure parameters for modem access.

When you have configured the external modem from the administration console, the switch transmits characters that you have entered as output on the modem port. The switch echoes characters that it receives as input on the modem port to the current administration console session. The console appears to be directly connected to the external modem.

## 4.3 WEB MANAGEMENT

The switch provides a browser interface that lets you configure and manage the switch remotely.

After you set up your IP address for the switch, you can access the switch's web interface applications directly in your web browser by entering the IP address of the switch. You can then use your web browser to list and manage switch configuration parameters from one central location, just as if you were directly connected to the switch's console port.

## 4.4 SNMP-BASED NETWORK MANAGEMENT

You can use an external SNMP-based application to configure and manage the switch. This management method requires the SNMP agent on the switch and the SNMP Network Management Station to use the same community string. This management method, in fact, uses two community strings: the get community string and the set community string. If the SNMP Network management station only knows the set community string, it can read and write to the MIBs. However, if it only knows the get community string, it can only read MIBs. **The default get and set community strings for the switch are public.**

## 4.5 PROTOCOLS

The switch supports the following protocols:

**Virtual terminal protocols, such as Telnet**

A virtual terminal protocol is a software program, such as Telnet, that allows you to establish a management session from a Macintosh, a PC, or a UNIX workstation. Because Telnet runs over TCP/IP, you must have at least one IP address configured on the switch before you can establish access to it with a virtual terminal protocol.

**<Note>** Terminal emulation is different from a virtual terminal protocol in that you must connect a terminal directly to the console port.

**Simple Network Management Protocol (SNMP)**

SNMP is the standard management protocol for multivendor IP networks. SNMP supports transaction-based queries that allow the protocol to format messages and to transmit information between reporting devices and data-collection programs. SNMP runs on top of the User Datagram Protocol (UDP), offering a connectionless-mode service.

## 4.6 MANAGEMENT ARCHITECTURE

All of the management application modules use the same Messaging Application Programming Interface (MAPI). By unifying management methods with a single MAPI, configuration parameters set using one method (e.g. console port) are immediately displayed the other management methods (e.g. SNMP agent of web browser).

The management architecture of the switch adheres to the IEEE open standard. This compliance assures customers that the switch is compatible with, and will interoperate with other solutions that adhere to the same open standard.

# 5 SNMP & RMON MANAGEMENT

This chapter describes the switch's Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON) capabilities. The following documentation applies to both the OSD2700F and to the OSD2700SFP

## 5.1 OVERVIEW

RMON is an abbreviation for the Remote Monitoring MIB (Management Information Base). RMON is a system defined by the Internet Engineering Task Force (IETF) document RFC 2819, which defines how networks can be monitored remotely.

RMONs typically consist of two components: an RMON probe and a management workstation:

- *The RMON probe is an intelligent device or software agent that continually collects statistics about a LAN segment or VLAN. The RMON probe transfers the collected data to a management workstation on request or when a pre-defined threshold is reached.*

- *The management workstation collects the statistics that the RMON probe gathers. The workstation can reside on the same network as the probe, or it can have an in-band or out-of-band connection to the probe.*

The switch provides RMON capabilities that allow network administrators to set parameters and view statistical counters defined in MIB-II, Bridge MIB, and RMON MIB. RMON activities are performed at a Network Management Station running an SNMP network management application with graphical user interface.

## 5.2 SNMP AGENT AND MIB-2 (RFC 1213)

The SNMP Agent running on the switch manager CPU is responsible for:

- *Retrieving MIB counters from various layers of software modules according to the SNMP GET/GET NEXT frame messages.*

- *Setting MIB variables according to the SNMP SET frame message.*

- *Generating an SNMP TRAP frame message to the Network Management Station if the threshold of a certain MIB counter is reached or if other trap conditions (such as the following) are met:*

    - Warm start
    - Cold start
    - Link up
    - Link down
    - Authentication failure
    - Rising alarm
    - Falling alarm
    - Topology Alarm

MIB-II defines a set of manageable objects in various layers of the TCP/IP protocol suites. MIB-II covers all manageable objects from layer 1 to layer 4, and, as a result, is the major SNMP MIB supported by all vendors in the networking industry. The switch supports a complete implementation of SNMP Agent and MIB-II.

## 5.3 RMON MIB (RFC 2819) AND BRIDGE MIB (RFC 1493)

The switch provides hardware-based RMON counters in the switch chipset. The switch manager CPU polls these counters periodically to collect the statistics in a format that complies with the RMON MIB definition.

### 5.3.1 RMON GROUPS SUPPORTED

The switch supports the following RMON MIB groups defined in RFC 2819:

- *RMON Statistics Group – maintains utilization and error statistics for the switch port being monitored.*
- *RMON History Group – gathers and stores periodic statistical samples from the previous Statistics Group.*
- *RMON Alarm Group – allows a network administrator to define alarm thresholds for any MIB variable. An alarm can be associated with Low Threshold, High Threshold, or both. A trigger can trigger an alarm when the value of a specific MIB variable exceeds a threshold, falls below a threshold, or exceeds or falls below a threshold.*
- *RMON Event Group – allows a network administrator to define actions based on alarms. SNMP Traps are generated when RMON Alarms are triggered. The action taken in the Network Management Station depends on the specific network management application*

### 5.3.2 BRIDGE GROUPS SUPPORTED

The switch supports the following four groups of Bridge MIB (RFC 1493):

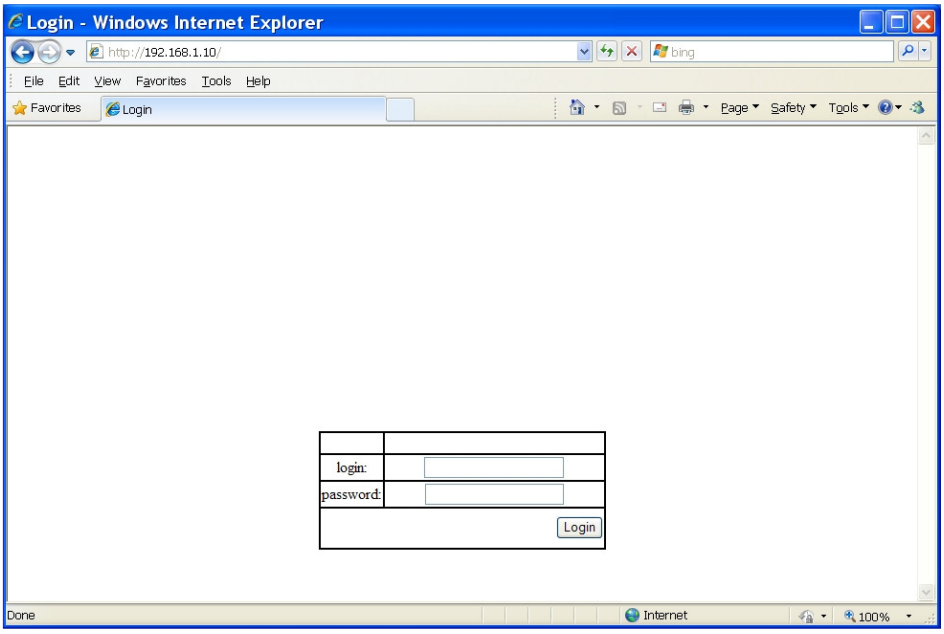
- *The dot1dBase Group – a mandatory group that contains the objects applicable to all types of bridges.*
- *The dot1dStp Group – contains objects that denote the bridge's state with respect to the Spanning Tree Protocol. If a node does not implement the Spanning Tree Protocol, this group will not be implemented. This group is applicable to any transparent only, source route, or SRT bridge that implements the Spanning Tree Protocol.*
- *The dot1dTp Group – contains objects that describe the entity's transparent bridging status. This group is applicable to transparent operation only and SRT bridges.*
- *The dot1dStatic Group – contains objects that describe the entity's destination-address filtering status. This group is applicable to any type of bridge which performs destination-address filtering.*

# 6 WEB-BASED BROWSER MANAGEMENT

The switch provides a web-based browser interface for configuring and managing the switch. This interface allows you to access the switch using a preferred web browser.

This chapter describes how to configure the switch using its web-based browser interface.

## 6.1 LOGGING ON TO THE SWITCH



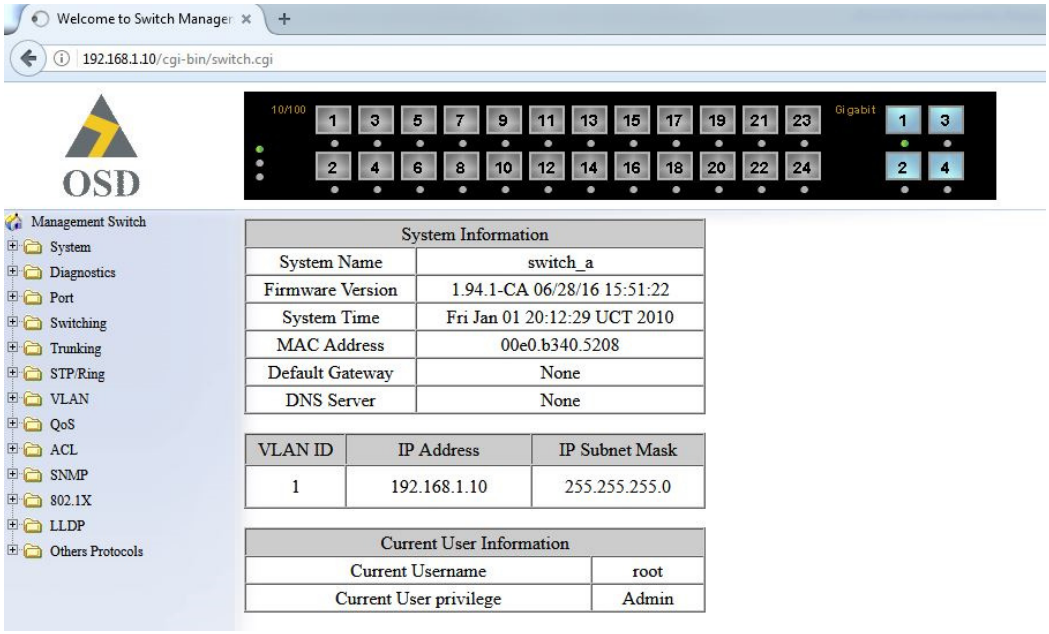

**SWITCH IP ADDRESS**
In your web browser, specify the IP address of the switch. Default IP address is 192.168.1.10.

**LOGIN**
Enter the factory default login ID: root.

**PASSWORD**
Enter the factory default password (no password).
Or enter a user-defined password if you followed the instructions later and changed the factory default password.
Then click on the “Login” button to log on to the switch.

## 6.2 UNDERSTANDING THE BROWSER INTERFACE

The web browser interface provides groups of point-and-click buttons at the left field of the screen for configuring and managing the switch.




**SYSTEM**
System Information, System Name/Password, IP Address, Save Configuration, Firmware Upgrade, Reboot, Logout

**DIAGNOSTICS**
Utilization, System Log, Remote Logging, ARP Table, Route Table, Alarm Setting

**PORT**
Configuration, Port Status, Rate Control, RMON Statistics, Per Port VLAN Activities

**SWITCHING**
Bridging, Static MAC Entry, Port Mirroring

**TRUNKING**
Port Trunking

**STP / RING**
Global Configuration, RSTP Port Setting, MSTP Properties, MSTP Instance Setting, MSTP Port Setting, Ring Setting

**VLAN**
VLAN Mode Setting, 802.1Q VLAN Setting, 802.1Q Port Setting, Port Based VLAN

**QOS**
Global Configuration, 802.1p Priority, DSCP

**ACL**
ACL Information, ACL Configuration

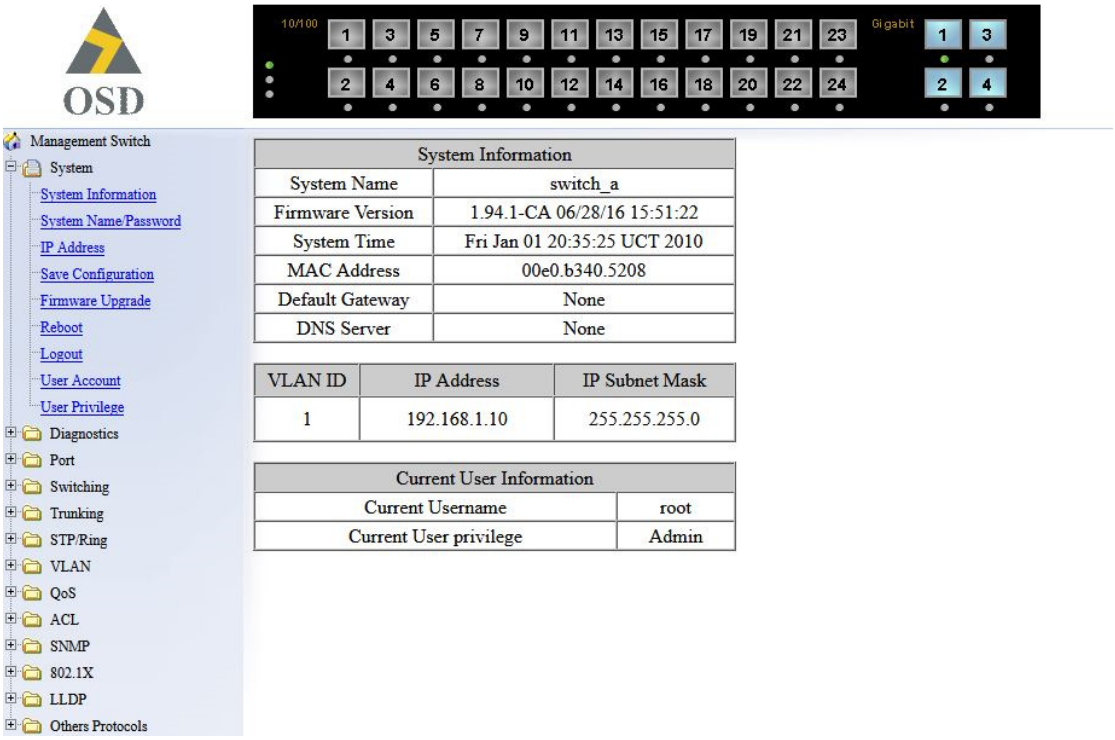
**SNMP**
SNMP General Setting, SNMP v1/v2c, SNMP v3

**802.1X**
Radius Configuration, Port Authentication

**LLPD**
LLDP General Settings, LLDP Ports Settings, LLDP Neighbors, LLDP Statistics

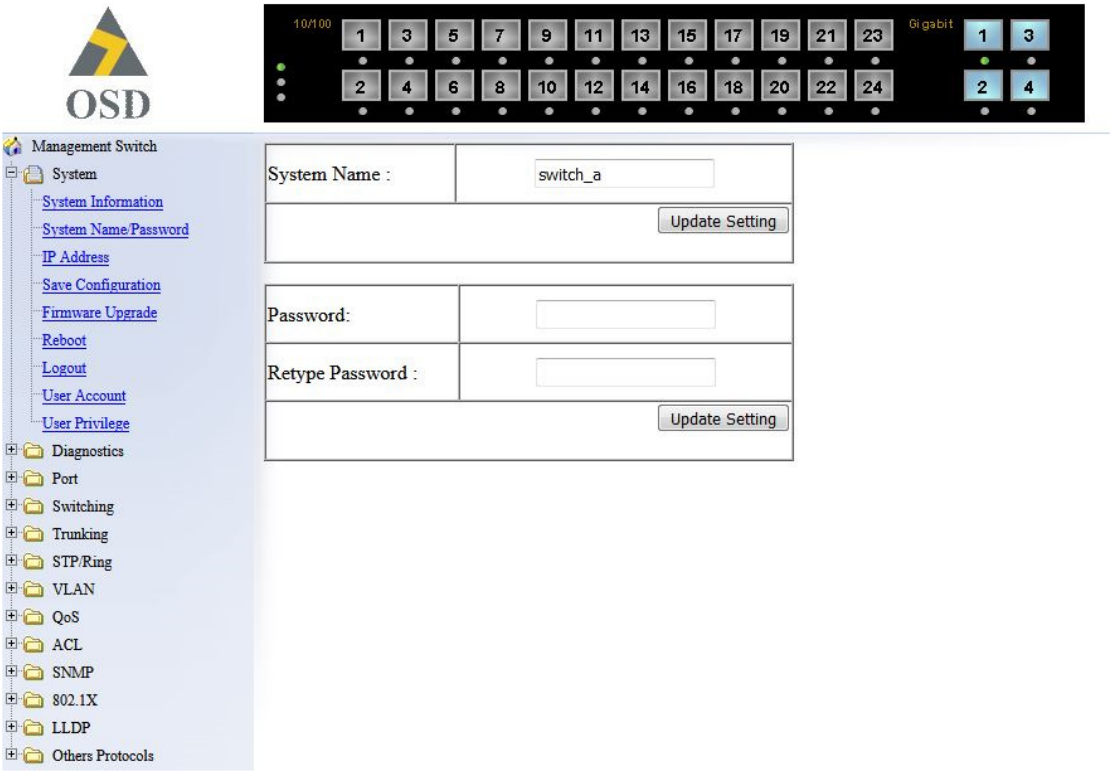
**OTHER PROTOCOLS**
GVRP, IGMP Snooping, NTP

## 6.3 SYSTEM



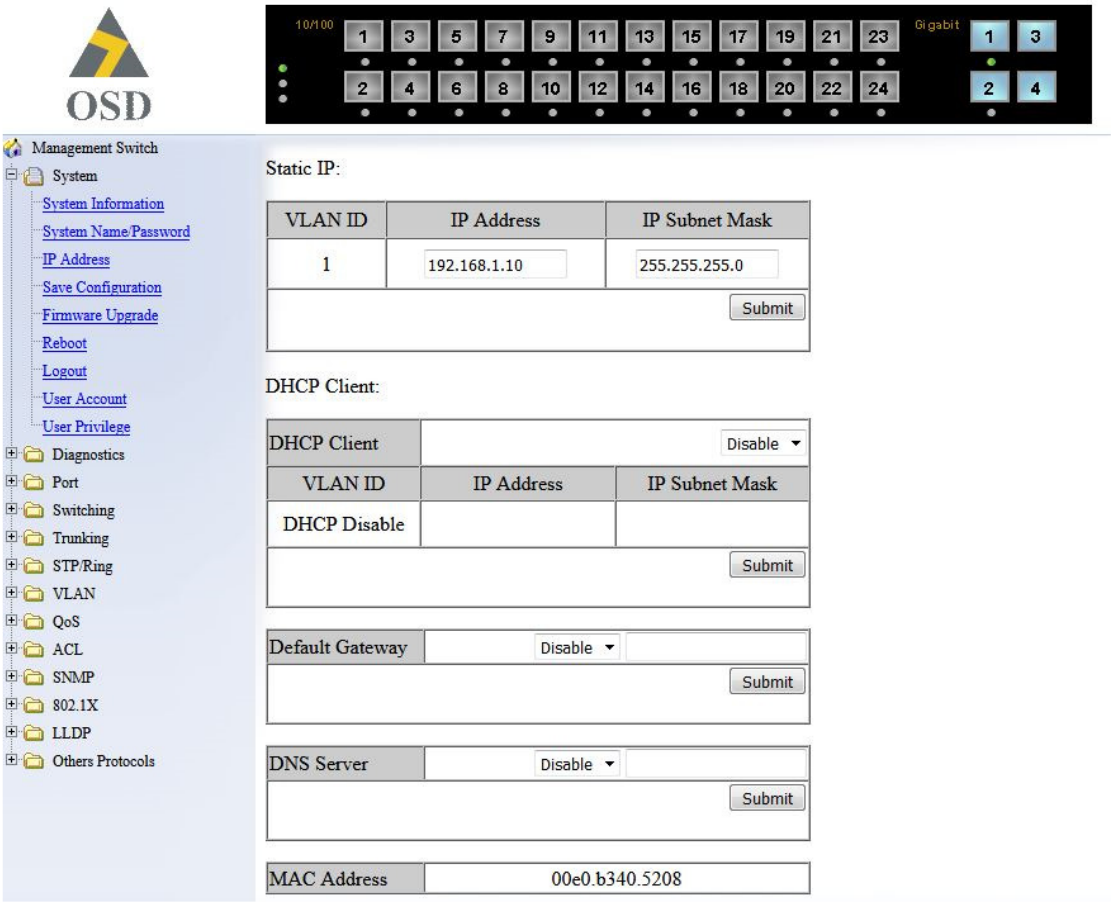

**SYSTEM INFORMATION**

The System name, Firmware version, MAC address, Default gateway, VLAN ID, IP Address, and IP Subnet Mask of Switch.



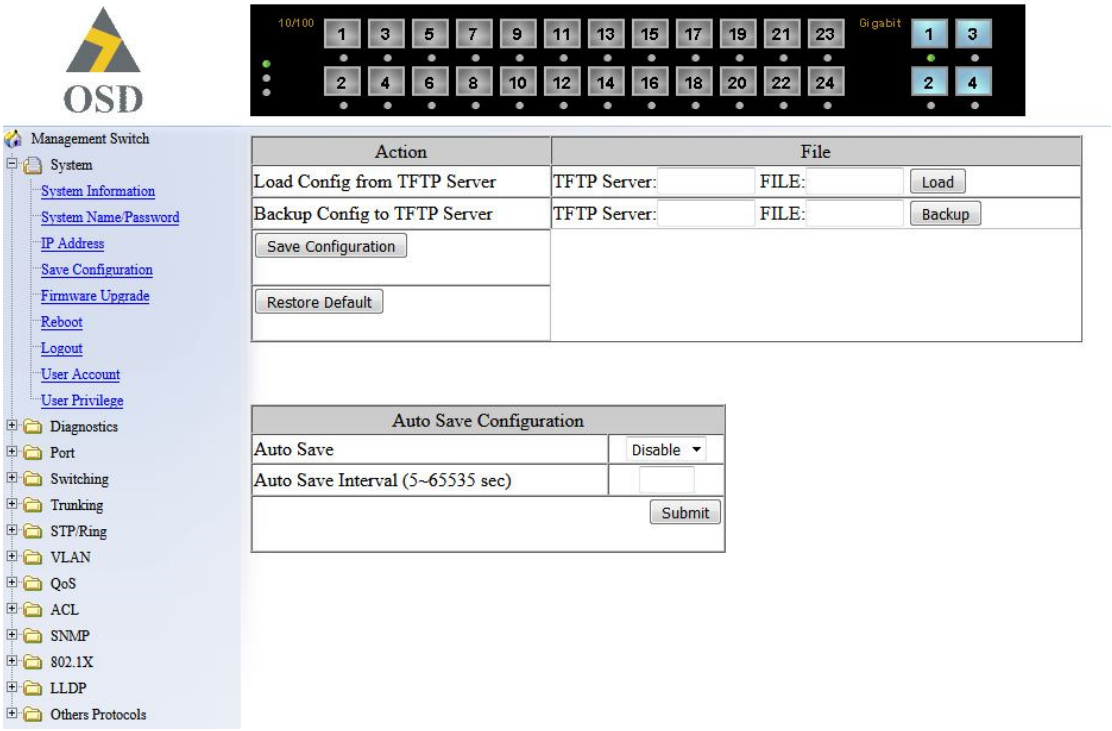

**SYSTEM NAME/PASSWORD**

1. System Name: Click in “System Name” text box. Type a system name if it is blank, or replace the current system name with a new one.
2. Updating setting: Click “Updating setting” button to update your settings.
3. Password: Click in “Password” text box. Type a password.
4. Retype Password: Click in “Retype Password” text box. Type the same password in “Password” text box again to verify it.
5. Updating setting: Click “Updating setting” button to update your settings



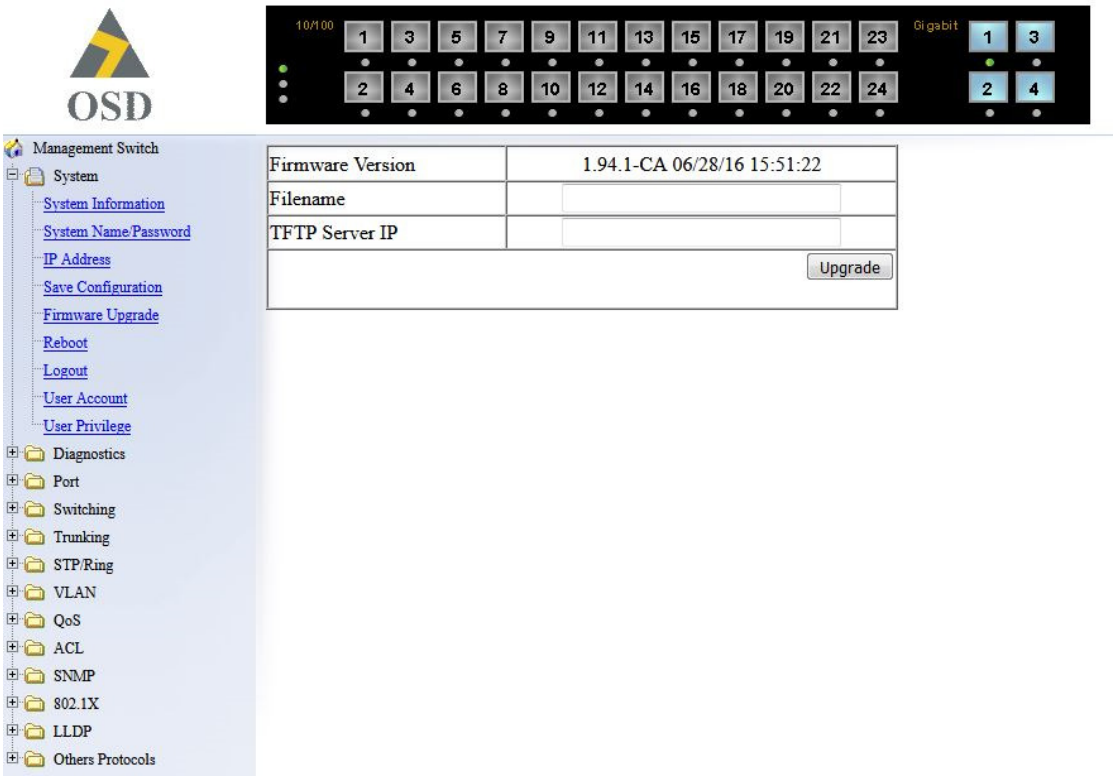

**IP ADDRESS**

1. IP Address: Click in “IP Address” text box and type a new address to change the IP Address.
2. IP Subnet Mask: Click in “IP Subnet Mask” text box and type a new address to change the IP Subnet Mask.
3. Submit: Click “Submit” button when you finished these selections.
4. You need to enter the new IP address on the browser and reconnect to the switch after IP or subnet mask are changed.
5. Default Gateway: Click “Default Gateway” drop-down menu to choose “Disable” or “Enable” from the “Default Gateway” drop-down list to disable or enable Default Gateway Setting for the switch.
6. Click the text box and type a new address to change the Default Gateway. (Need to choose “Enable” from the “Default Gateway” drop-down menu.)
7. Submit: Click “Submit” button when you finished Default Gateway.




**SAVE CONFIGURATION**

1. Load config from TFTP server:
2. Click in “TFTP Server” text box and type the TFTP server IP address from where the file will be obtained.
3. Click in “FILE” text box and type the name of the file that will be obtained.
4. Click “Load” button to load the file from the TFTP server.
5. Backup config to TFTP server:
6. Click in “TFTP Server” text box and type the TFTP server IP address to where the file will be backupped.
7. Click in “FILE” text box and type the name of the file that will be backupped.
8. Click “Backup” button to backup the file to the TFTP server.
9. Save Configuration: Click “Save Configuration” button to save your configuration settings.
10. Restore Default: Click “Restore Default” button to restore the default settings of the switch.
11. Auto save: Click “Auto save” drop-down menu to choose “Disable” or “Enable” from the “Auto save” drop-down list to disable or enable Auto save for the switch.
12. Auto save interval (5~65536 sec): Click in “Auto save interval” text box and type a decimal number between 5 and 65536.
13. Submit: Click “Submit” button when you finished Auto save configuration.

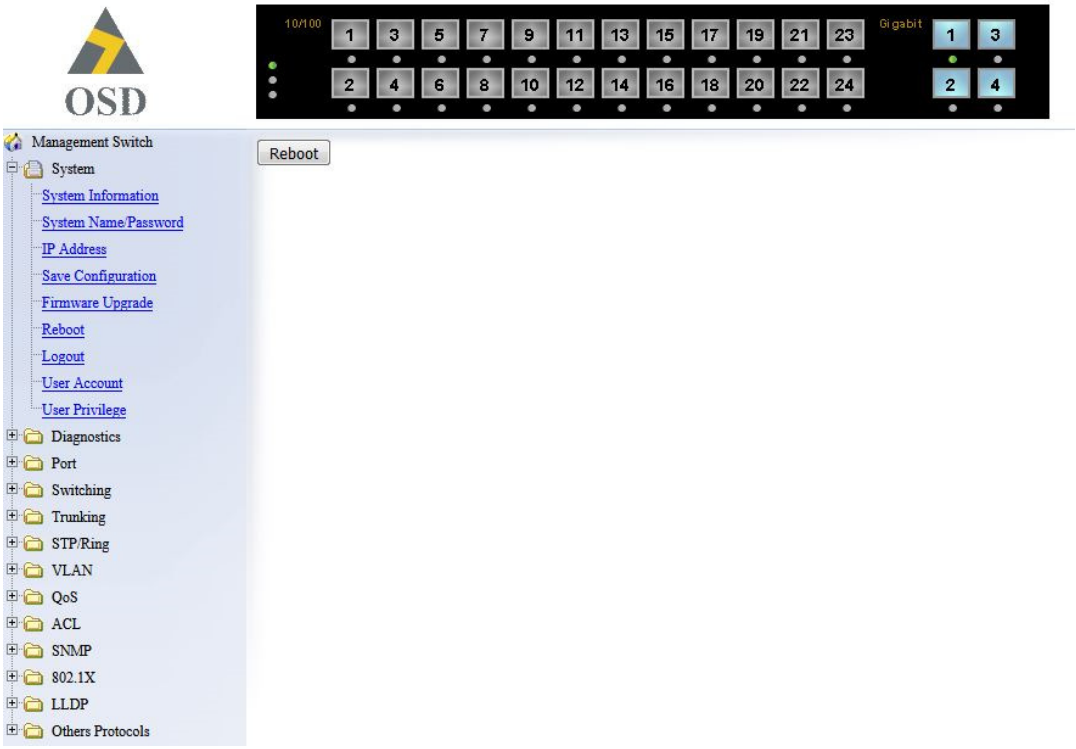



**FIRMWARE UPGRADE**

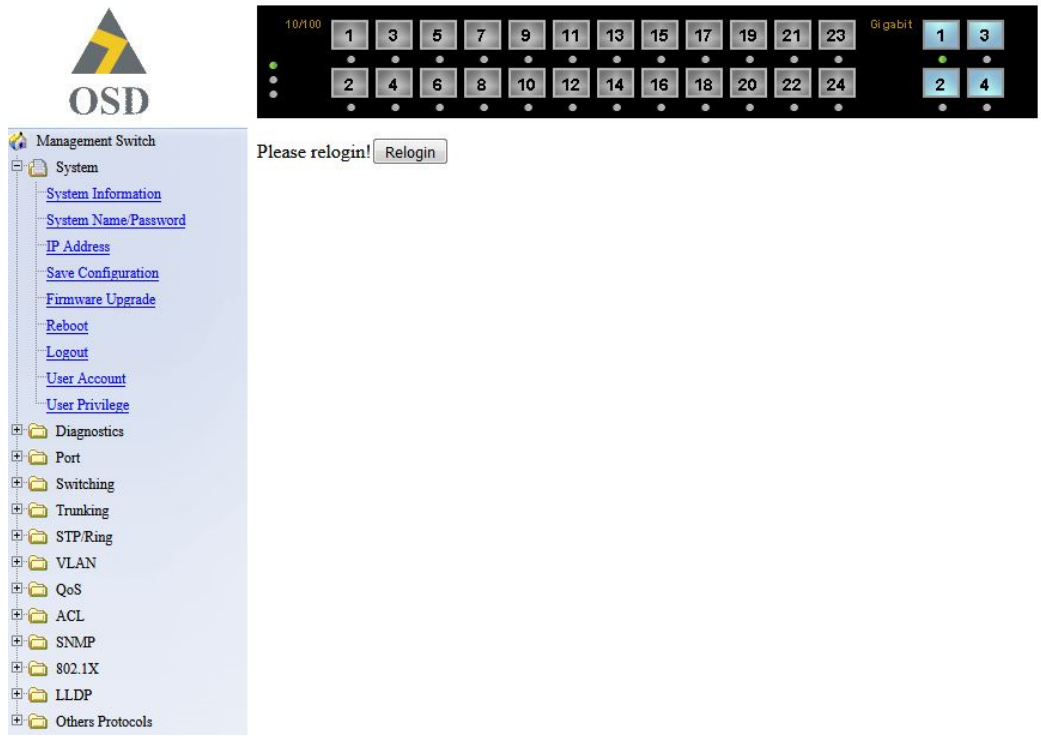
1. Filename: Click in “Filename” text box and type the name of the file that you intend to upgrade it to the switch.
2. TFTP server IP: Click in “TFTP server IP” text box and type the TFTP server IP address from where the file will be obtained.
3. Upgrade: Click “upgrade” button to upgrade firmware to the switch. Please follow the message on the screen during the firmware upgrade process. Do not turn off the power or perform other functions during this period of time. Reboot the switch after completing the upgrade process.

Please follow the message on the screen during the firmware upgrade process. Do not turn off the power or perform other functions during this period of time.

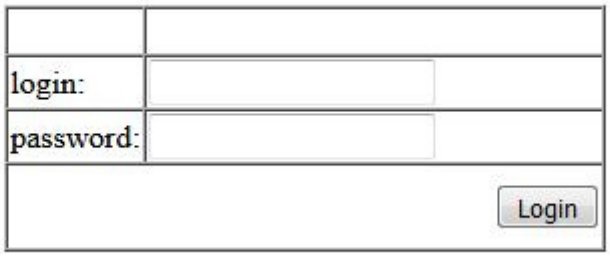
Firmware has been upgraded successfully to the switch. Reboot the switch after completing the upgrade process.




**REBOOT**
Reboot: Click “Reboot” button to restart the switch.




**LOGOUT**
Logout: Click “Logout” button to logout of the switch.




**USER ACCOUNT**

Multi-User Mode:

1. User Account: Click “Mode” drop-down menu to choose “Single-User” or “Multi-User” from the “Mode” drop-down list to choose single user or multi user mode.
2. Update Setting: Click “Update Setting” button to update settings to the switch.

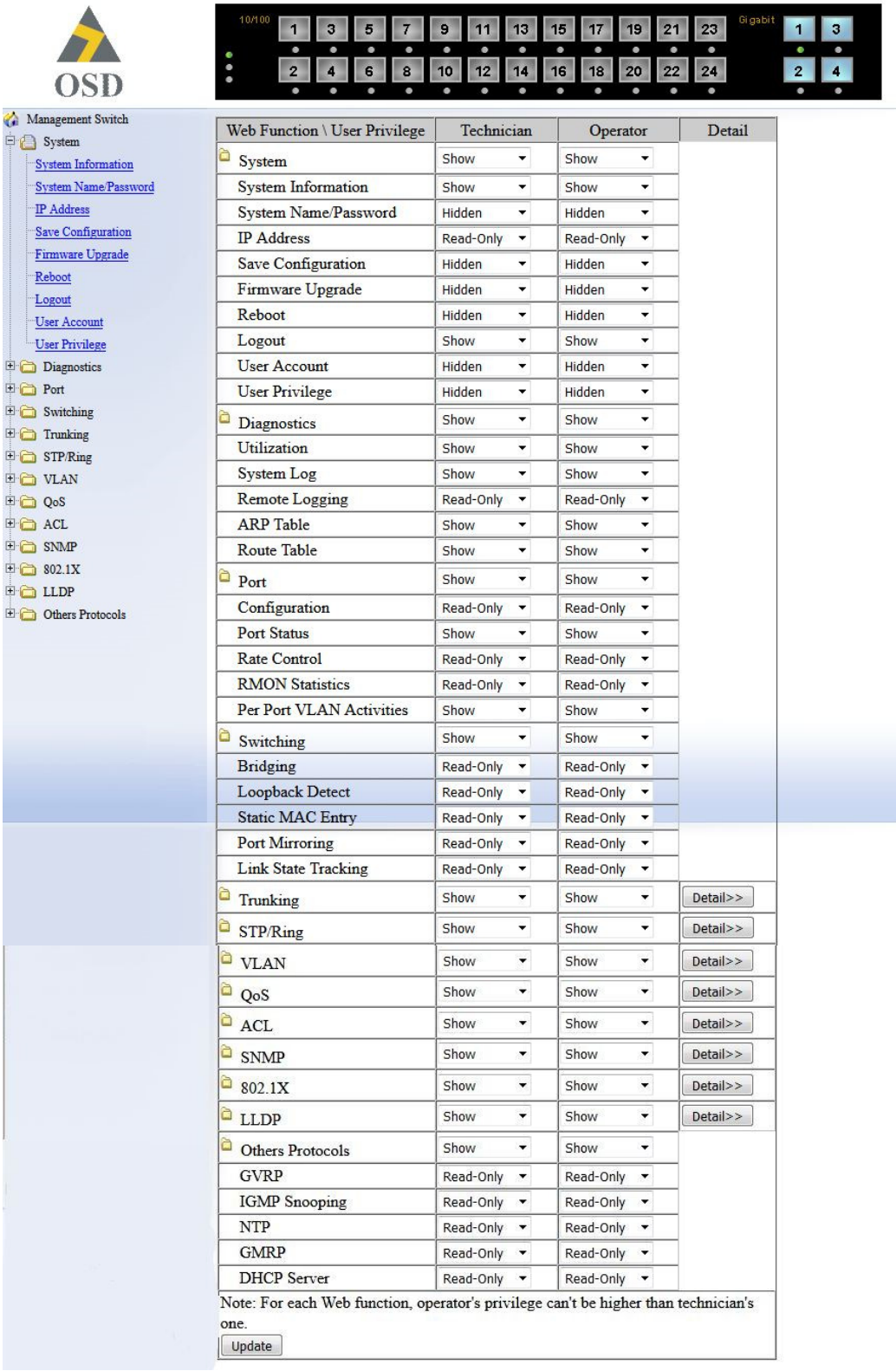
Create:

1. User Account: Click “User Account” drop-down menu to choose “Create” from the “User Account” drop-down list to create new user account or choose “User” from the “User Account” drop-down list to modify user account.
2. User Name: Click in “User Name” text box and create a user name for new user account.
3. Password: Click in “Password” text box and create a password for new user account.
4. Confirm Password: Click in “Confirm Password” text box. Type the same password in “Password” text box again to verify it.
5. Privilege Level: Click “Privilege Level” drop-down menu to choose “Admin”, “Operator”, or “Technician” from the “Privilege Level” drop-down list to choose privilege level for new user account.
6. Update: Click “Update” button to update settings to the switch.

Delete:

1. User Account: Click “User Account” drop-down menu to choose “User” from the “User Account” drop-down list to delete user account.

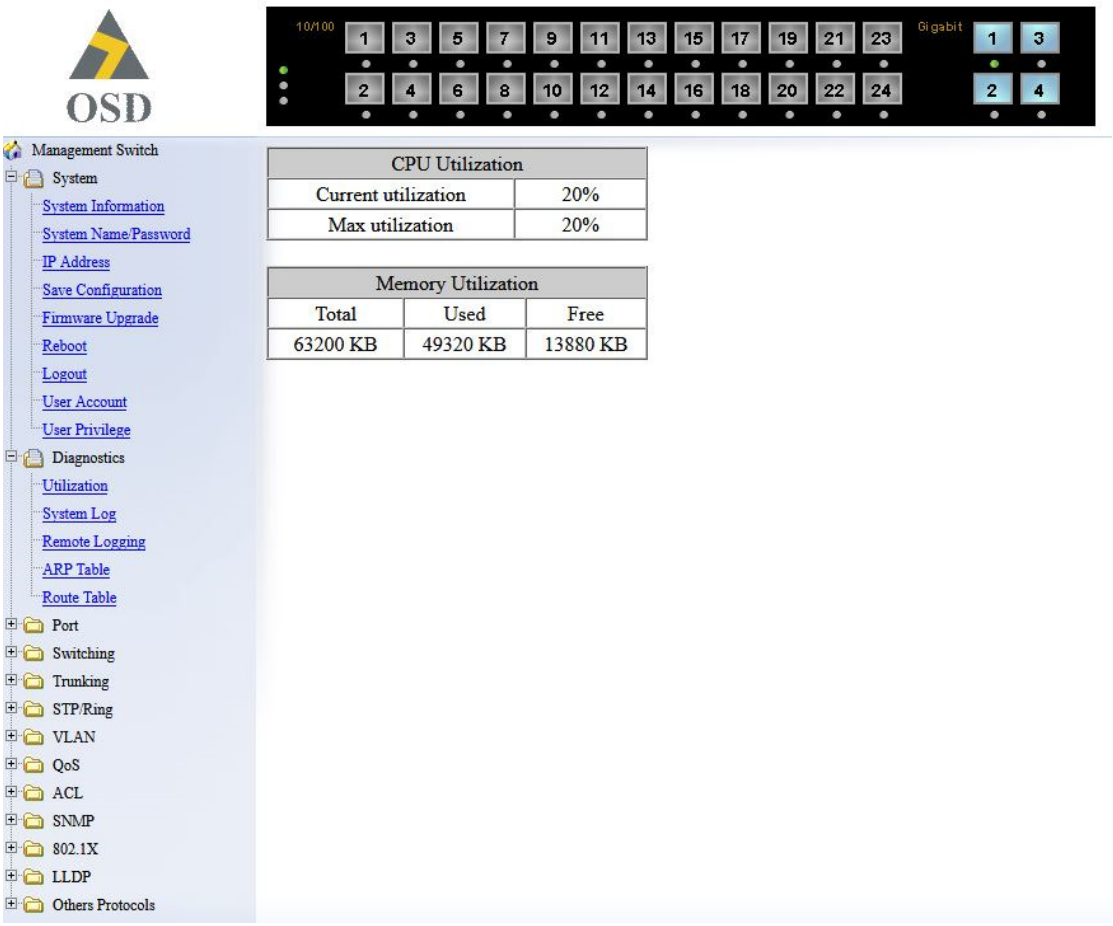
Delete: Click “Delete” button to delete user account.



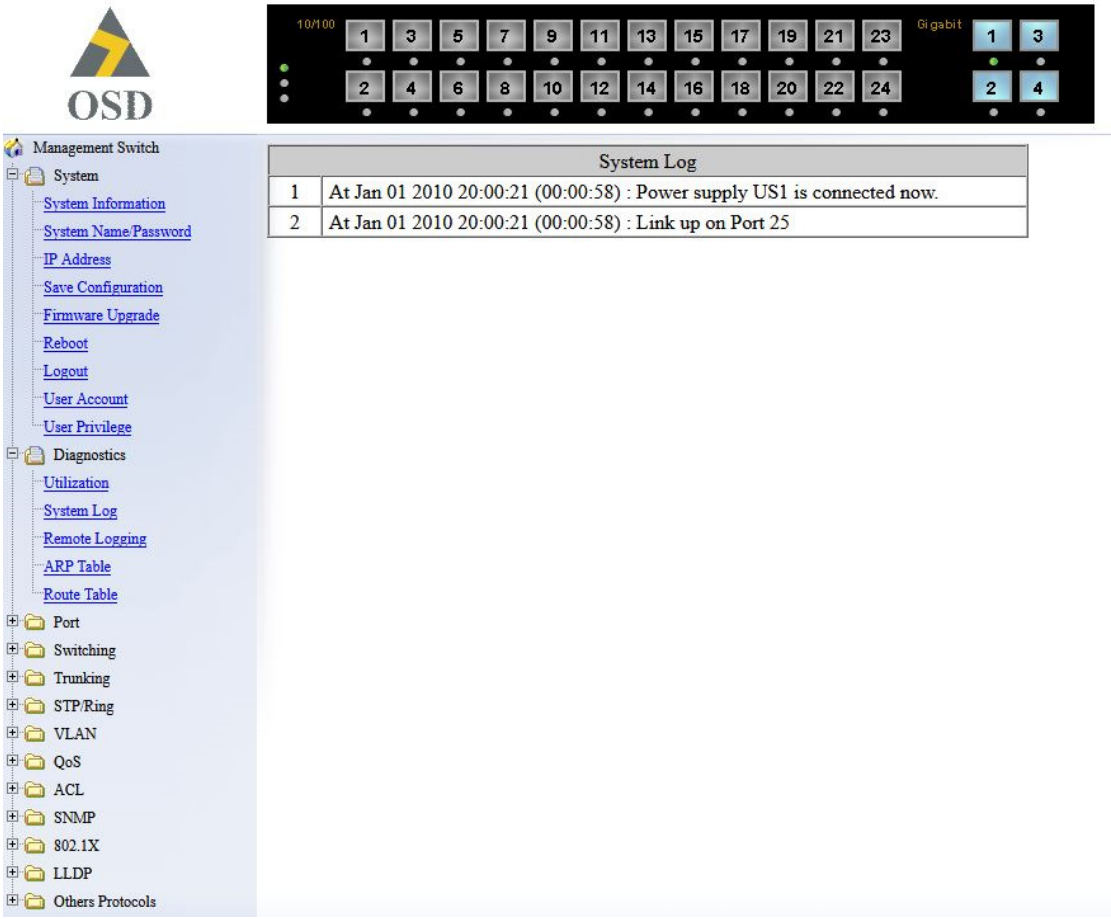

**USER PRIVILEGE**

Update: Click “Update” button when you finished user mode configuration.

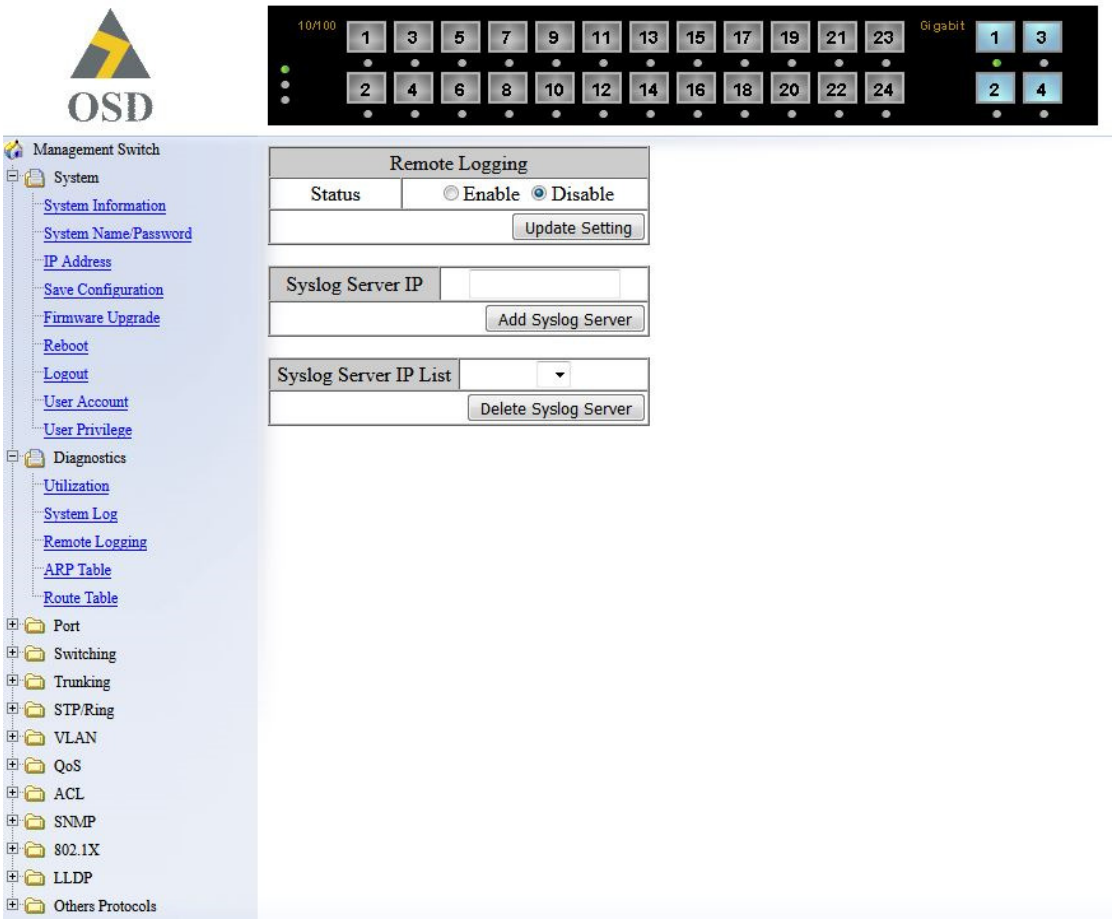
## 6.4 DIAGNOSTICS




**UTILIZATION**
Click **Utilization** to view CPU Utilization and Memory Utilization.

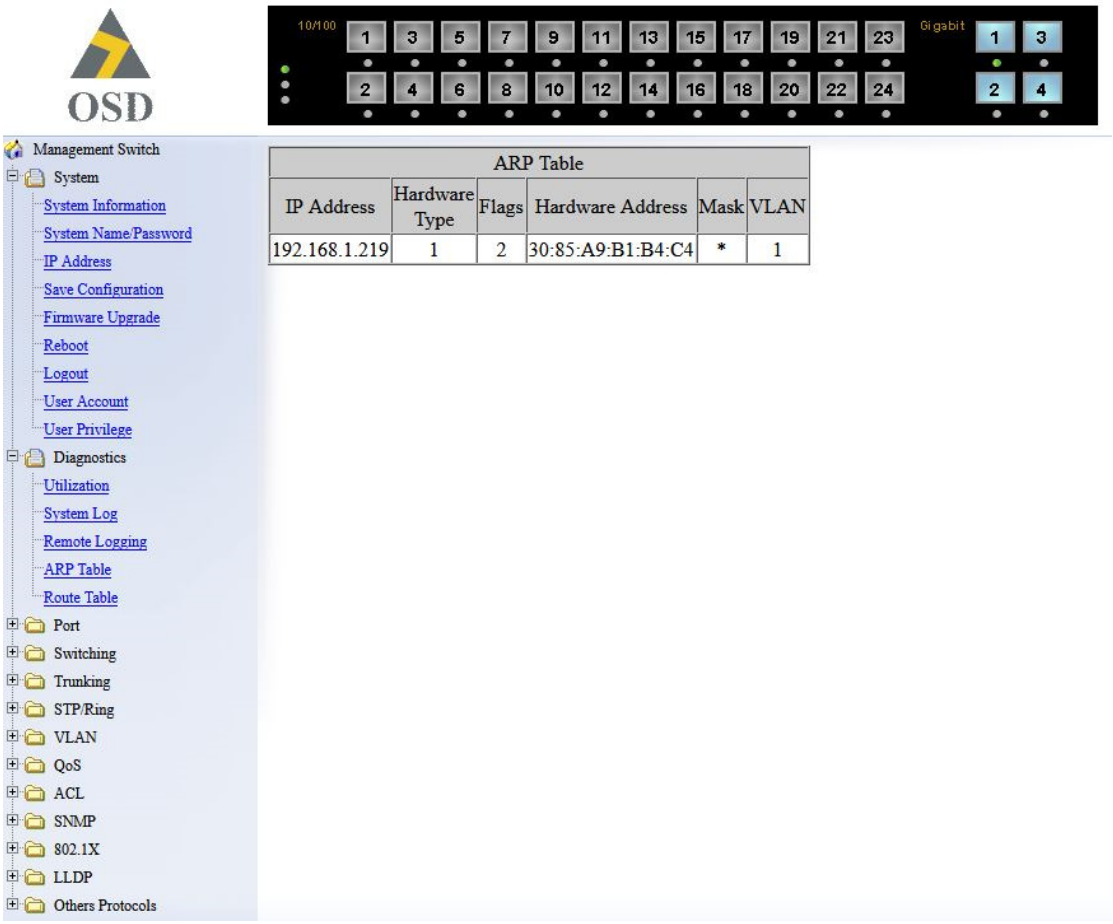



**SYSTEM LOG**
Click **System Log** to view system log.




**REMOTE LOGGING**

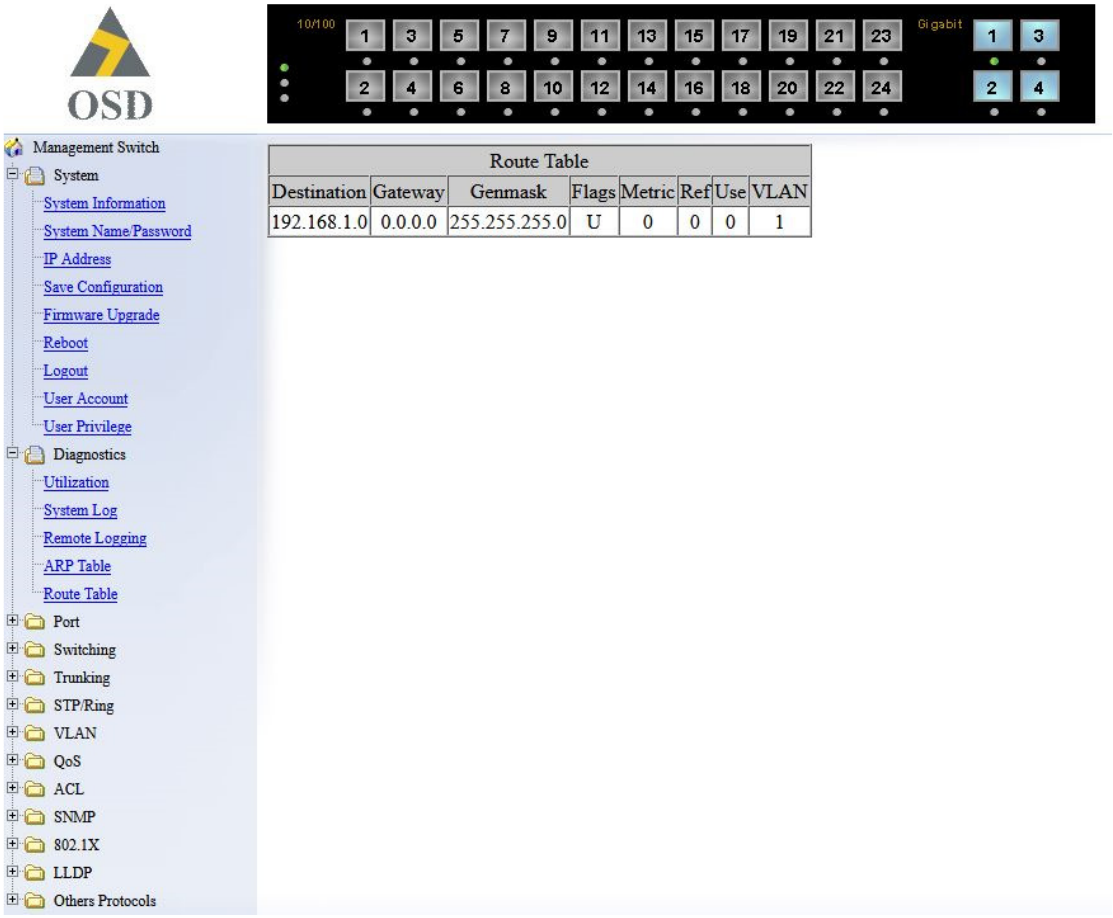
1. Status: Click and choose “Enable” or “Disable” to enable or disable the logging of messages that are sent to syslog servers.
2. Update Setting: Click “Update Setting” button to update your settings.
3. Syslog Server IP: Click in “Syslog Server IP” text box and type a syslog server IP address.
4. Add Syslog Server: Click “Add Syslog Server” button to add a syslog server.
5. Syslog Server IP List: Click “Syslog Server IP List” drop-down menu and choose a syslog server IP address from the “Syslog Server IP List” drop-down list to be deleted.
6. Delete Syslog Server: Click “Delete Syslog Server” button to delete a syslog server.




**ARP TABLE**

Click **ARP Table** to view ARP Table.

The ARP Table is learned by Switch CPU, not learned by Switch MAC. The MAC Address of PC that have accessed Switch user interface will be recorded in the ARP Table.




**ROUTE TABLE**

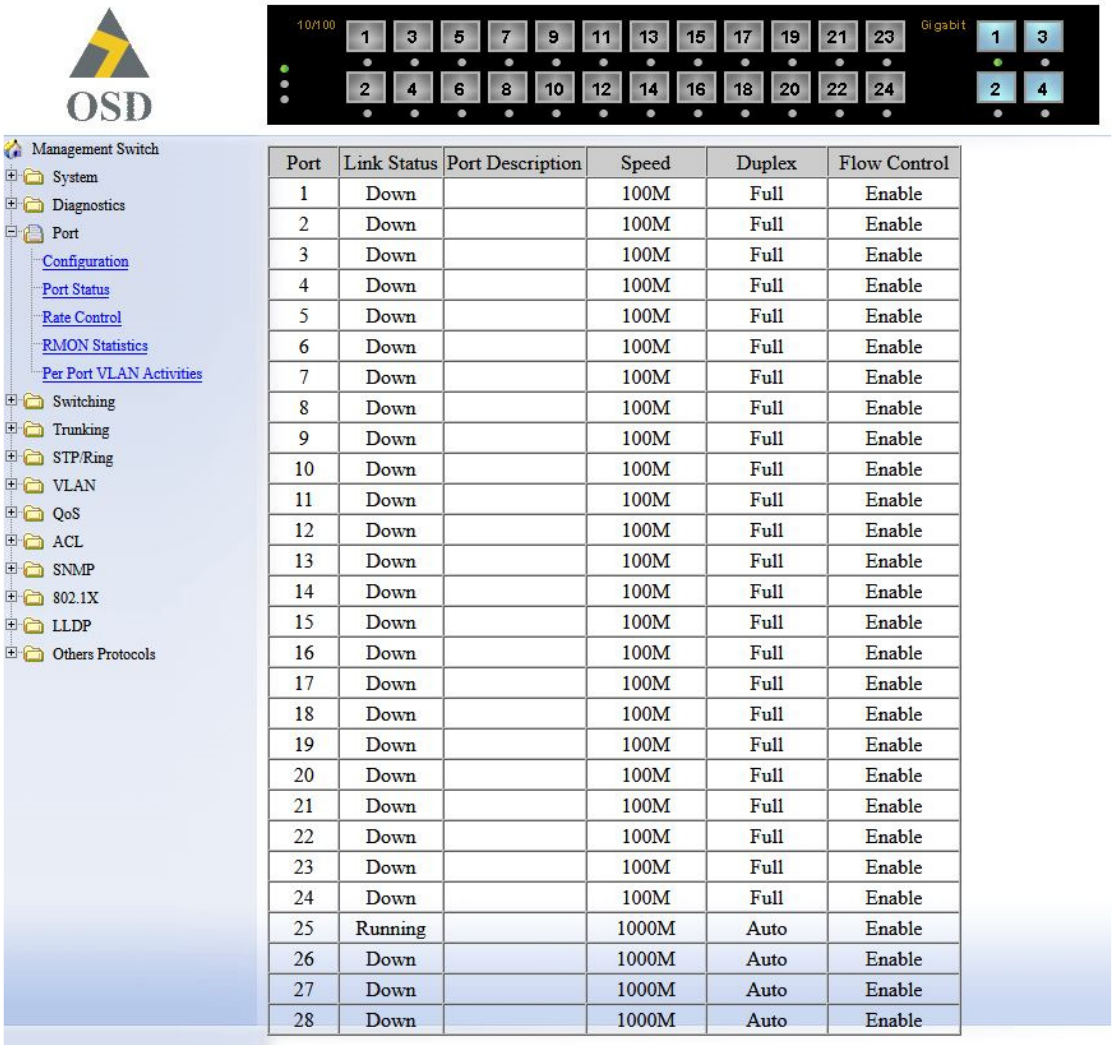
Click **Route Table** to view Route Table.

Route Table lists the routes to network destinations. And metrics (distances) are associated with those routes. The Route Table contains information about the topology of the network around it.

## 6.5 PORT


**CONFIGURATION**

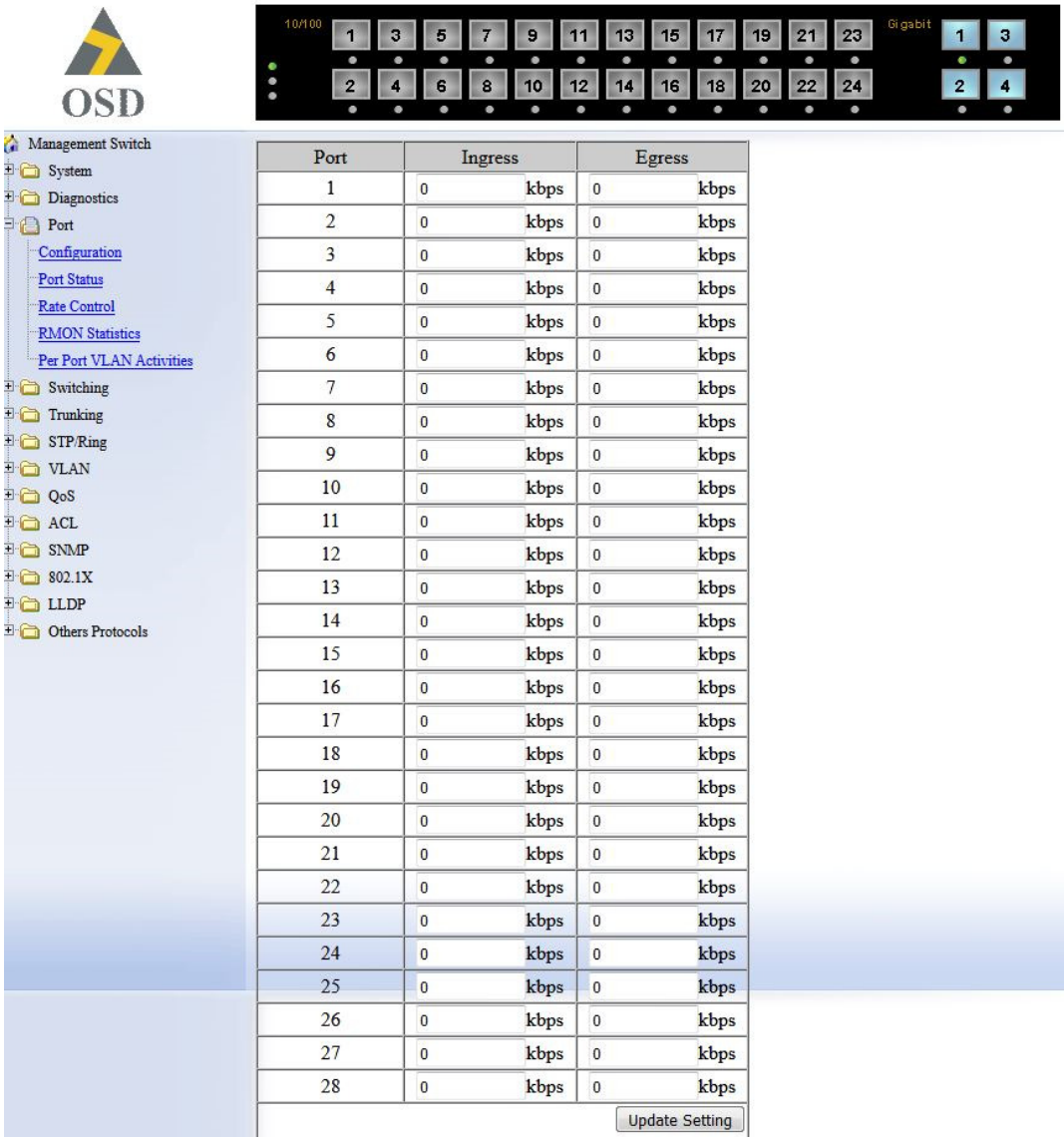
1. Port Description: Click in “Port Description” text box and type description for port.
2. Admin Setting: Click “Admin Setting” drop-down menu to choose “Link down” or “Link up” from the “Admin Setting” drop-down list to disable or enable Admin Setting for the port.
3. Speed: Click “Speed” drop-down menu to change the line speed and duplex settings from the “Speed” drop-down list for the port.
4. Flow Control: Click “Flow Control” drop-down menu to choose “Disable” or “Enable” from the “Flow Control” drop-down list to disable or enable Flow Control for the port.
5. Submit: Click “Submit” button when you finished configurations.




| Port | Link Status | Port Description | Speed | Duplex | Flow Control |
|---|---|---|---|---|---|
| 1 | Down | | 100M | Full | Enable |
| 2 | Down | | 100M | Full | Enable |
| 3 | Down | | 100M | Full | Enable |
| 4 | Down | | 100M | Full | Enable |
| 5 | Down | | 100M | Full | Enable |
| 6 | Down | | 100M | Full | Enable |
| 7 | Down | | 100M | Full | Enable |
| 8 | Down | | 100M | Full | Enable |
| 9 | Down | | 100M | Full | Enable |
| 10 | Down | | 100M | Full | Enable |
| 11 | Down | | 100M | Full | Enable |
| 12 | Down | | 100M | Full | Enable |
| 13 | Down | | 100M | Full | Enable |
| 14 | Down | | 100M | Full | Enable |
| 15 | Down | | 100M | Full | Enable |
| 16 | Down | | 100M | Full | Enable |
| 17 | Down | | 100M | Full | Enable |
| 18 | Down | | 100M | Full | Enable |
| 19 | Down | | 100M | Full | Enable |
| 20 | Down | | 100M | Full | Enable |
| 21 | Down | | 100M | Full | Enable |
| 22 | Down | | 100M | Full | Enable |
| 23 | Down | | 100M | Full | Enable |
| 24 | Down | | 100M | Full | Enable |
| 25 | Running | | 1000M | Auto | Enable |
| 26 | Down | | 1000M | Auto | Enable |
| 27 | Down | | 1000M | Auto | Enable |
| 28 | Down | | 1000M | Auto | Enable |

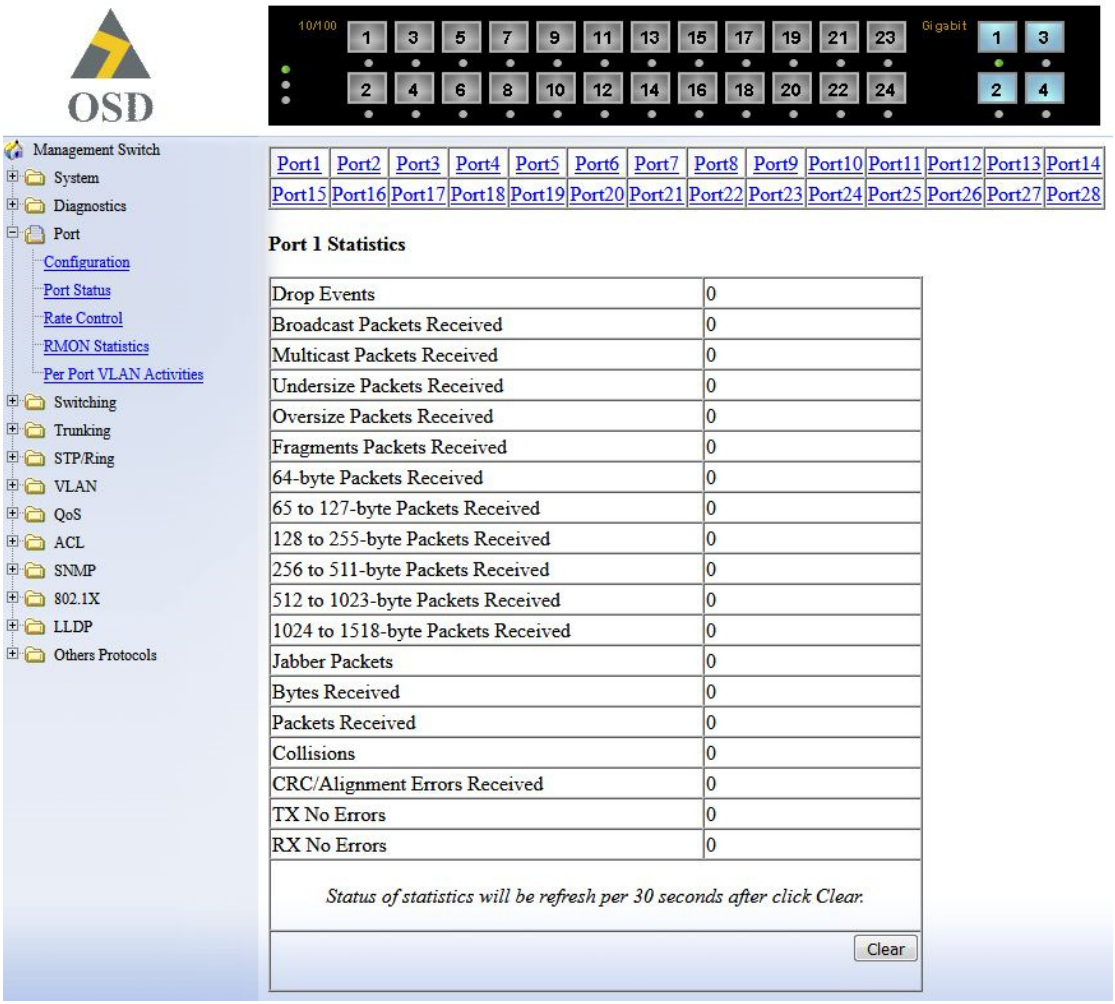
**PORT STATUS**

View the Link Status, Port Description, Speed, Duplex, and Flow Control status for all ports.

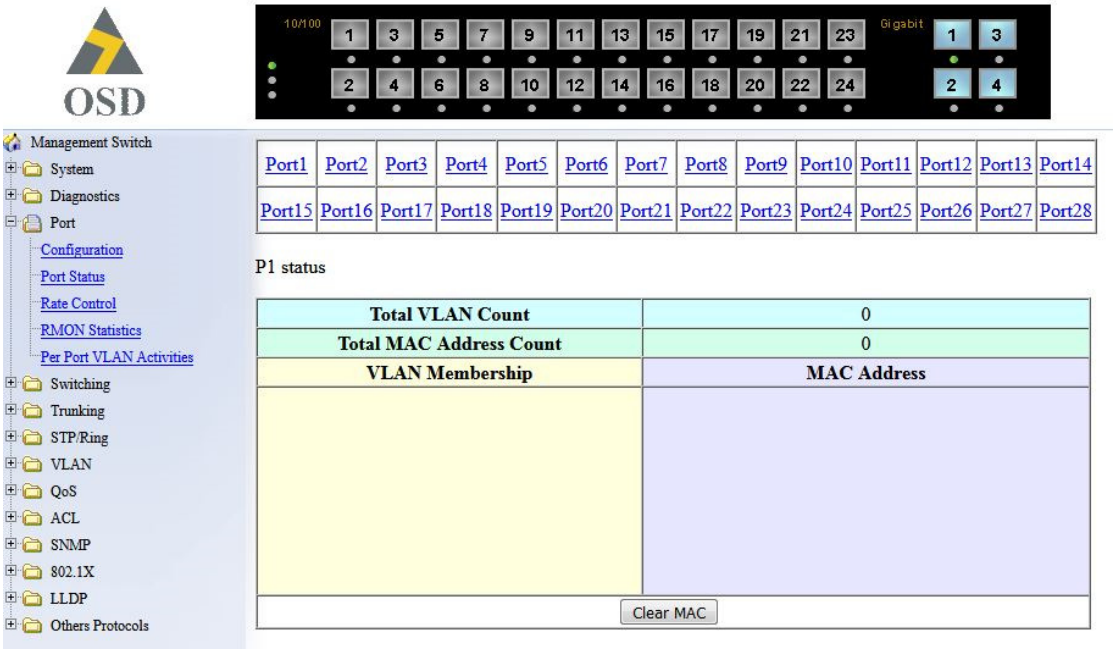



**RATE CONTROL**

1. Ingress: Click in “Ingress” text box and type a new Rate to change the Ingress Rate Control for the port.
   Rate Values: 64kbps, 128kbps, 192kbps, … , 1792kbps.
   2Mbps, 3Mbps, 4Mbps, … , 100Mbps.
   104Mbps, 112Mbps, 120Mbps, … , 1000Mbps.
   <Note>: M = 1024k.
2. Egress: Click in “Egress” text box and type a new Rate to change the Egress Rate Control for the port.
   Rate Values: 64kbps, 128kbps, 192kbps, … , 1792kbps.
   2Mbps, 3Mbps, 4Mbps, … , 100Mbps.
   104Mbps, 112Mbps, 120Mbps, … , 1000Mbps.
   <Note>: M = 1024k.
3. Update Setting: Click “Update Setting” button when you finished these Rate Control settings.

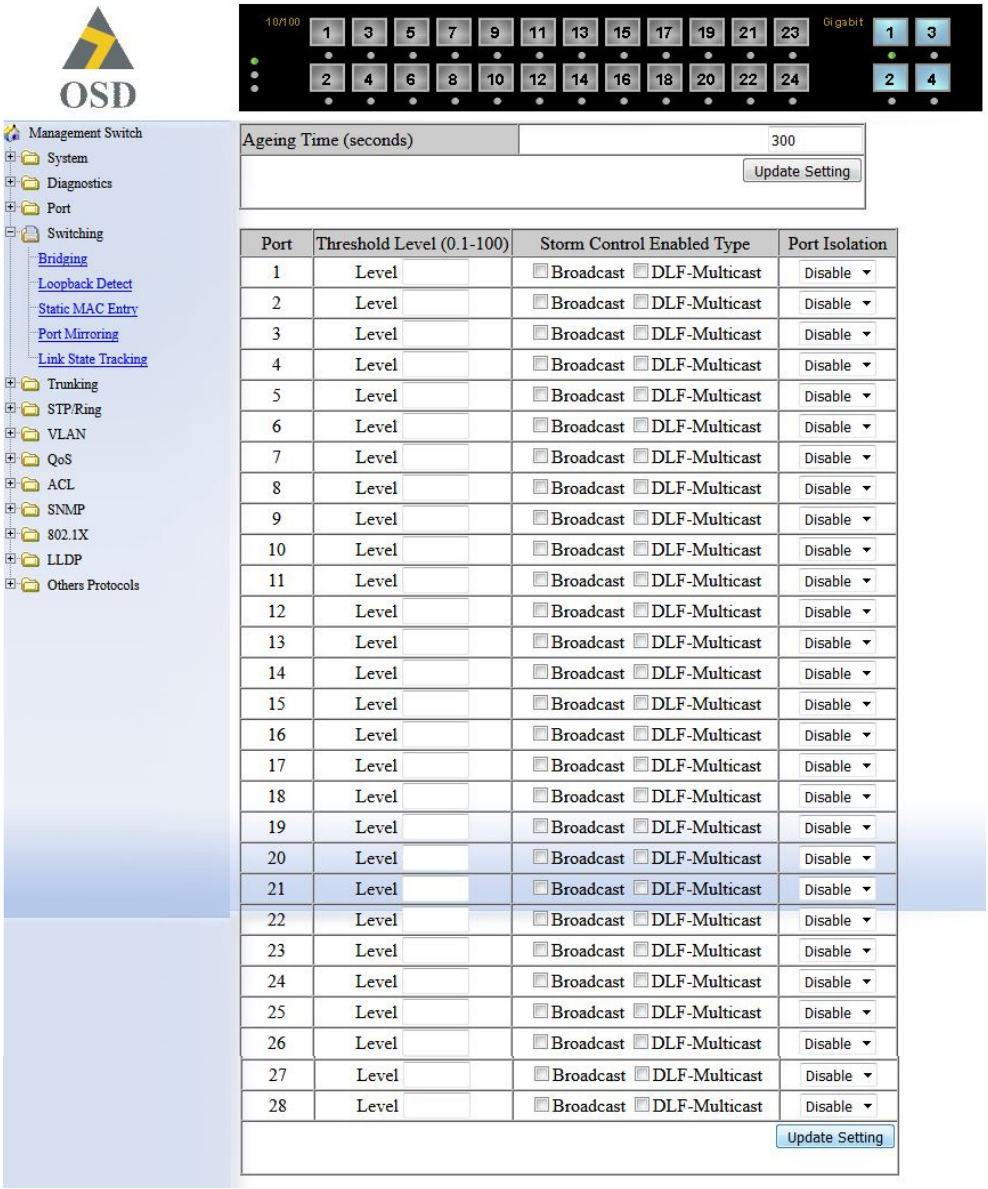



**RMON STATISTICS**
Click ports to view corresponding RMON Statistics.



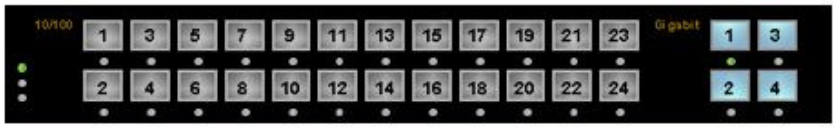

**PER PORT VLAN ACTIVITIES**
Click ports to view corresponding VLAN activities.

## 6.6 SWITCHING




**BRIDGING**

1. Aging Time (seconds): Click the text box and type a decimal number as Bridging Aging Time in seconds.
2. Update Setting: Click “Update Setting” button when you finished Aging Time settings.
3. Threshold Level (0.1-100): Click in “Level” text box and type a decimal number for the port. Need to choose “Broadcast” and/or “DFL-Multicast“ from “Storm-control enabled type” for the port. DLF (Destination Lookup Failure).
4. Storm Control Enabled Type: Choose “Broadcast” and/or “DLF-Multicast” from “Storm-control enabled type” for the port.
5. Port Isolation: Click “Port Isolation” drop-down menu to choose “Enable” or “Disable” from the “Port Isolation” drop-down list to enable or disable port isolation for the port.
6. Update Setting: Click “Update Setting” button when you finished Threshold Level, Storm Control Enabled Type, and Port Isolation settings.




- Management Switch
- System
- Diagnostics
- Port
- Switching
  - Bridging
  - Loopback Detect
  - Static MAC Entry
  - Port Mirroring
  - Link State Tracking
- Trunking
- STP/Ring
- VLAN
- QoS
- ACL
- SNMP
- 802.1X
- LLDP
- Others Protocols

| General Setting | |
|---|---|
| LoopBack Detect | Disable (default) |
| LoopBack Detect Action | None (default) |
| Error Disable Recovery (0-65535 seconds, Default:0) | 0 |
| Interval (1-30 seconds, Default:1) | 1 |

NOTE:Error Disable Recovery must over two times of Interval.

Update Setting

| Port | Mode | State |
|---|---|---|
| 1 | Disable (default) | -- |
| 2 | Disable (default) | -- |
| 3 | Disable (default) | -- |
| 4 | Disable (default) | -- |
| 5 | Disable (default) | -- |
| 6 | Disable (default) | -- |
| 7 | Disable (default) | -- |
| 8 | Disable (default) | -- |
| 9 | Disable (default) | -- |
| 10 | Disable (default) | -- |
| 11 | Disable (default) | -- |
| 12 | Disable (default) | -- |
| 13 | Disable (default) | -- |
| 14 | Disable (default) | -- |
| 15 | Disable (default) | -- |
| 16 | Disable (default) | -- |
| 17 | Disable (default) | -- |
| 18 | Disable (default) | -- |
| 19 | Disable (default) | -- |
| 20 | Disable (default) | -- |
| 21 | Disable (default) | -- |
| 22 | Disable (default) | -- |
| 23 | Disable (default) | -- |
| 24 | Disable (default) | -- |
| 25 | Disable (default) | -- |
| 26 | Disable (default) | -- |
| 27 | Disable (default) | -- |
| 28 | Disable (default) | -- |

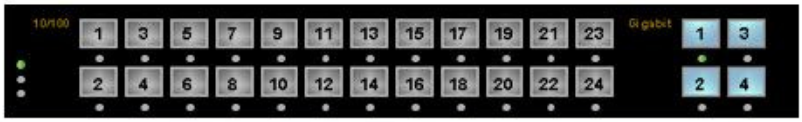
Update Setting

**Loopback Detect**

General Setting:

1. LoopBack Detect: Click “LoopBack Detect” drop-down menu to choose “Disable (default)” or “Enable” from “LoopBack Detect” drop-down list to disable or enable a loopback detection on a port interface.
2. LoopBack Detect Action: Click “LoopBack Detect Action” drop-down menu to choose “None (default)” or “Error Disable” from “LoopBack Detect Action” drop-down list to disable or enable error disable LoopBack Detect Action on a port interface.
3. Error Disable Recovery (0-65535 seconds): Click the text box and type a decimal number as error disable recovery time in seconds. The default value is 0 second (no recovery).
4. Interval (1-65535 seconds): Click the text box and type a decimal number as loopback detect interval time in seconds. The default value is 1 second.
5. Update Setting: Click “Update Setting” button when you finished General Setting.

1. Mode: Click “Mode” drop-down menu to choose “Enable” or “Disable (default)” from “Mode” drop-down list to enable or disable LoopBack Detect for port interface.
2. Update Setting: Click “Update Setting” button when you finished LoopBack Detect settings for port interface.




- Management Switch
  - System
  - Diagnostics
  - Port
  - Switching
    - Bridging
    - Loopback Detect
    - Static MAC Entry
    - Port Mirroring
    - Link State Tracking
  - Trunking
  - STP/Ring
  - VLAN
  - QoS
  - ACL
  - SNMP
  - 802.1X
  - LLDP
  - Others Protocols

Static-MAC-Entry Forward

| Port | Add MAC Address (Ex: 0000.1111.2222) | VLAN ID | Delete MAC Address |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |
| 11 | | | |
| 12 | | | |
| 13 | | | |
| 14 | | | |
| 15 | | | |
| 16 | | | |
| 17 | | | |
| 18 | | | |
| 19 | | | |
| 20 | | | |
| 21 | | | |
| 22 | | | |
| 23 | | | |
| 24 | | | |
| 25 | | | |
| 26 | | | |
| 27 | | | |
| 28 | | | |

Submit

Static-MAC-Entry Discard

| Add MAC Address (Ex: 0000.1111.2222) | VLAN ID | Delete MAC Address |
|---|---|---|
| | | |

Submit

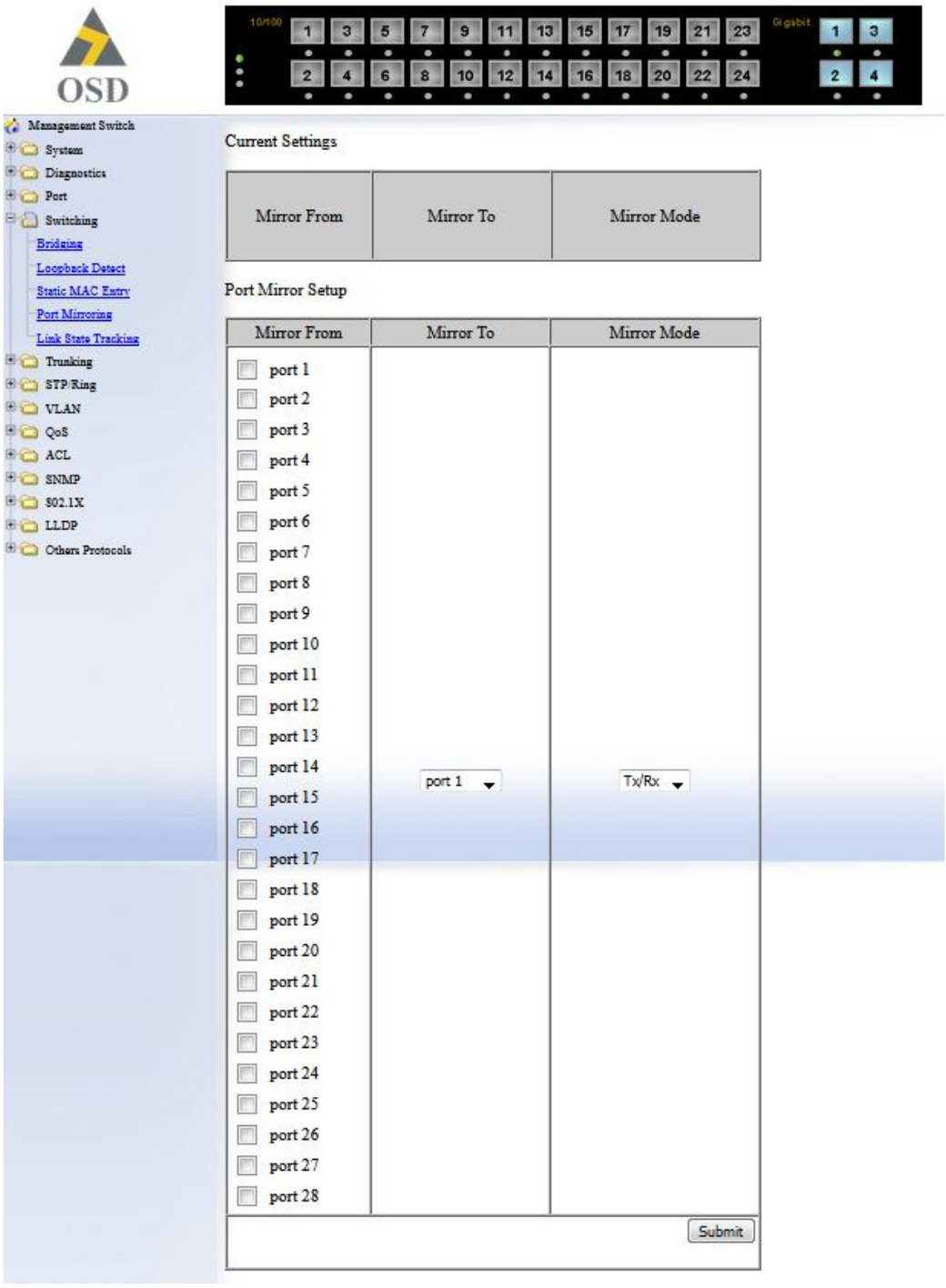
**STATIC MAC ENTRY**

Static-MAC-Entry Forward:

1. Add MAC Address: Click in “Add MAC Address” text box and type a locked forwarding MAC address for the port.
2. VLAN ID: Click “VLAN ID” drop-down menu and choose a VLAN ID from the “VLAN ID” drop-down list.
3. Delete MAC Address: Click “Delete MAC Address” drop-down menu and choose a locked forwarding MAC address from the “Delete MAC Address” drop-down list to be deleted from the port.
4. Submit: Click “Submit” button when you finished Static-MAC-Entry Forward settings.

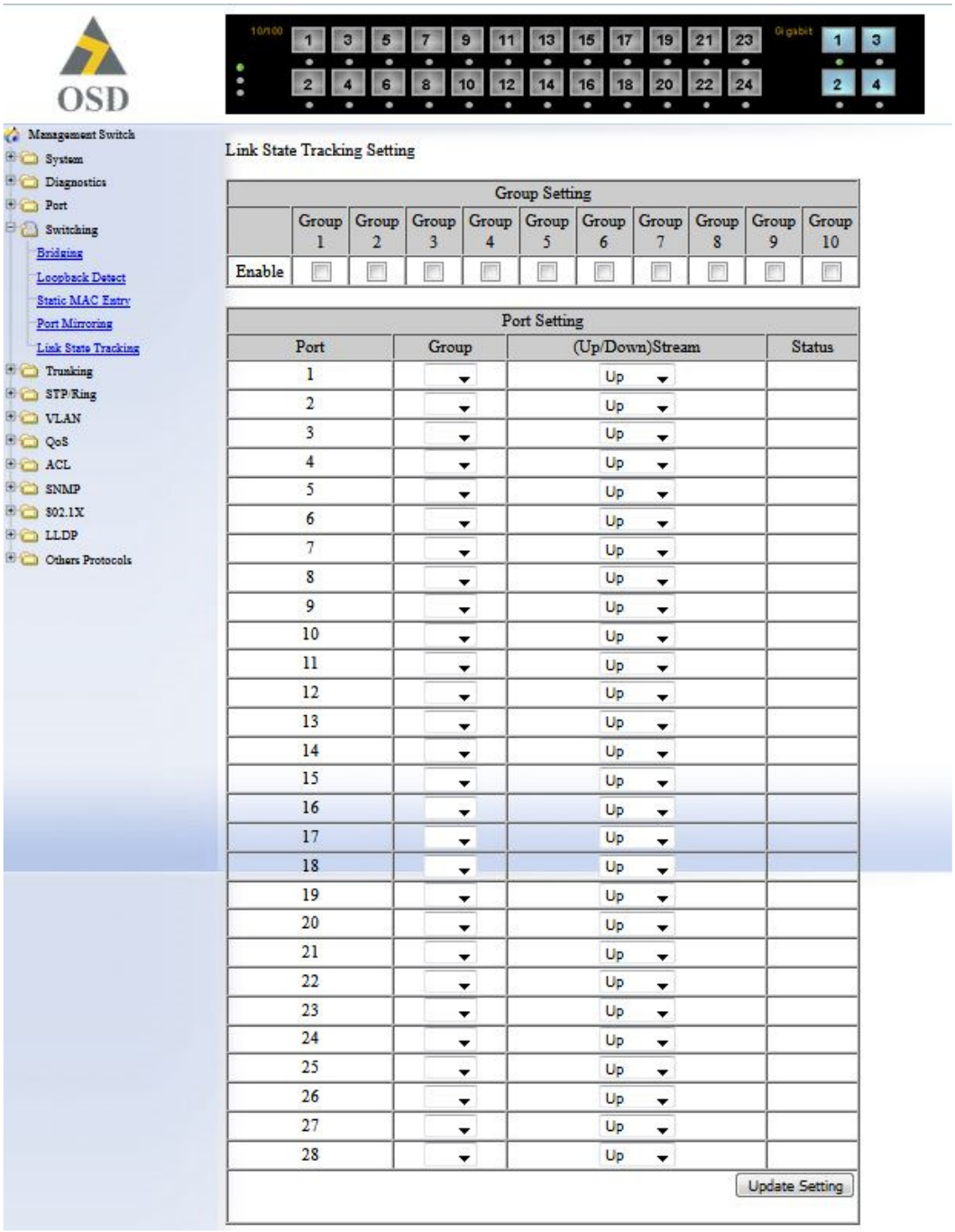
Static-MAC-Entry Discard:

1. Add MAC Address: Click in “Add MAC Address” text box and type a MAC address to be discarded for the VLAN.
2. VLAN ID: VLAN ID: Click “VLAN ID” drop-down menu and choose a VLAN ID from the “VLAN ID” drop-down list.
3. Delete MAC Address: Click “Delete MAC Address” drop-down menu and choose a MAC address from the “Delete MAC Address” drop-down list to be discarded from the VLAN.
4. Submit: Click “Submit” button when you finished Static-MAC-Entry Discard settings.




**PORT MIRRORING**

1. Mirror From: Choose Mirror From port from Port 1 ~ Port 28.
2. Mirror To: Click “Mirror To” drop-down menu to choose Mirror To port (Port 1 ~ Port 28) from “Mirror To” drop-down list.
3. Mirror Mode: Click “Mirror Mode” drop-down menu to choose “Tx/Rx”, “Tx”, or “Rx” from “Mirror Mode” drop-down list.
4. Submit: Click “Submit” button when you finished Port Mirroring settings.




### Link State Tracking

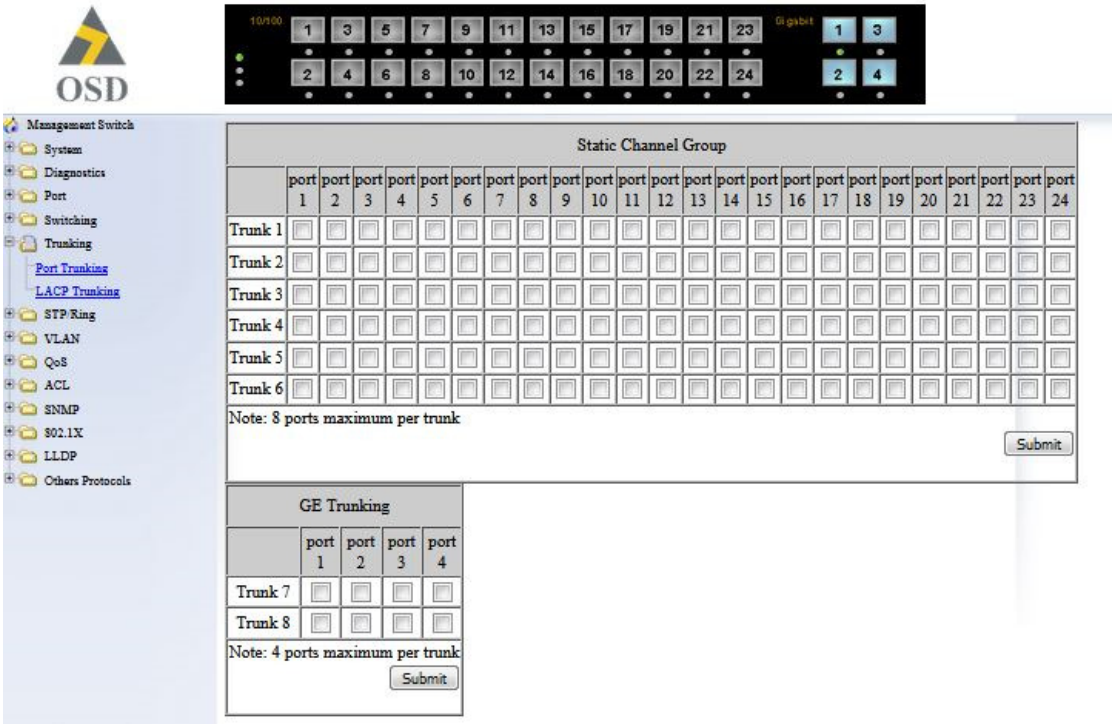
Group Setting:

1. Enable: Click check box of group to enable Link State tracking for group.

Port Setting:

1. Group: Click “Group” drop-down menu to choose group for port from “Group” drop-down list.
2. (Up/Down)Stream: Click “(Up/Down)Stream” drop-down menu to choose Up (upstream) or Down (downstream) for port from “(Up/Down)Stream” drop-down list.
3. Update Setting: Click “Update Setting” button when you finished Link State Tracking Setting.

## 6.7 TRUNKING

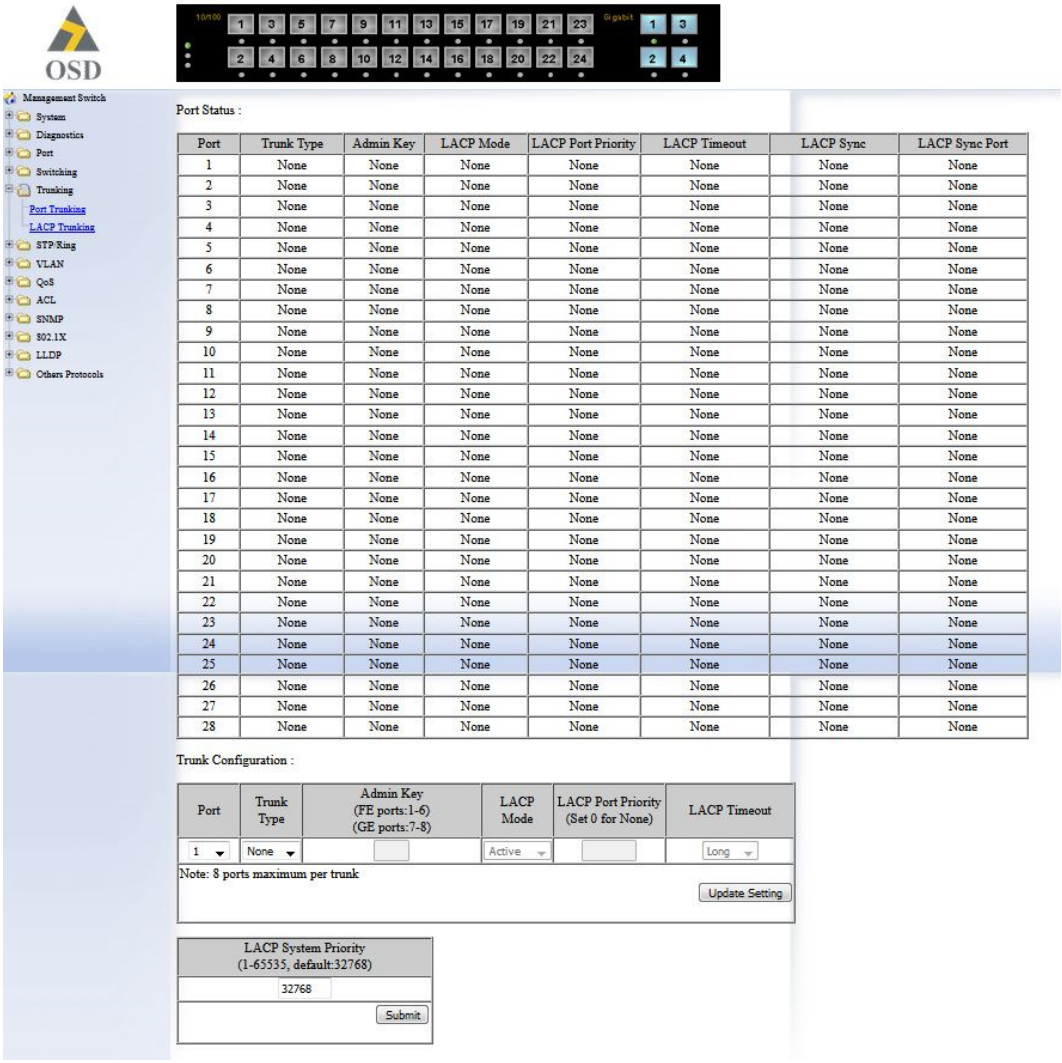



**PORT TRUNKING**
Static Channel Group:
1. Trunk 1: Click ports to assign ports to Trunk 1. (Maximum 4 ports per Trunk.)

LACP Group:
1. Trunk 1: Click ports to assign ports to Trunk 1. (Maximum 4 ports in Trunk 1.)

GE Trunking (Gigabit Ports):
1. Trunk 3: Check “Static”, “LACP”, or “Disable” to enable Static or LACP Trunk 3 or disable Trunk 3 for Gigabit Ethernet ports.

Submit: Click “Submit” button when you finished Port Trunking settings.

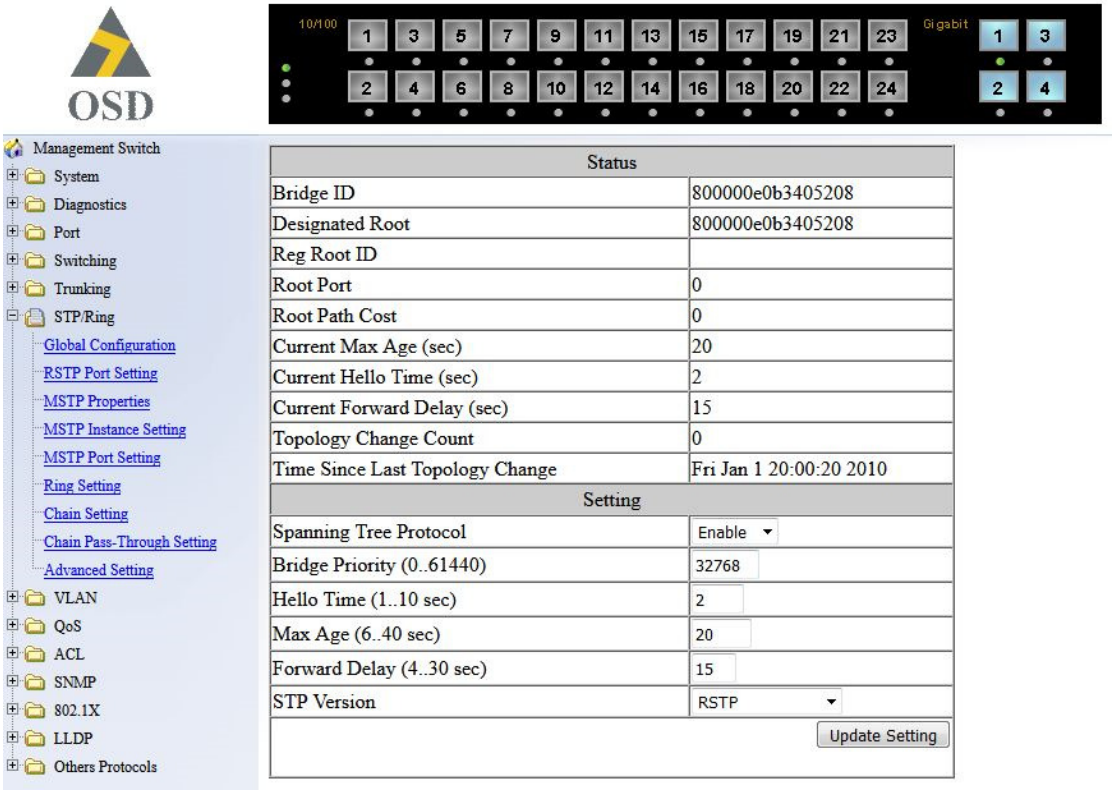



## LACP Trunking

Trunk Configuration:

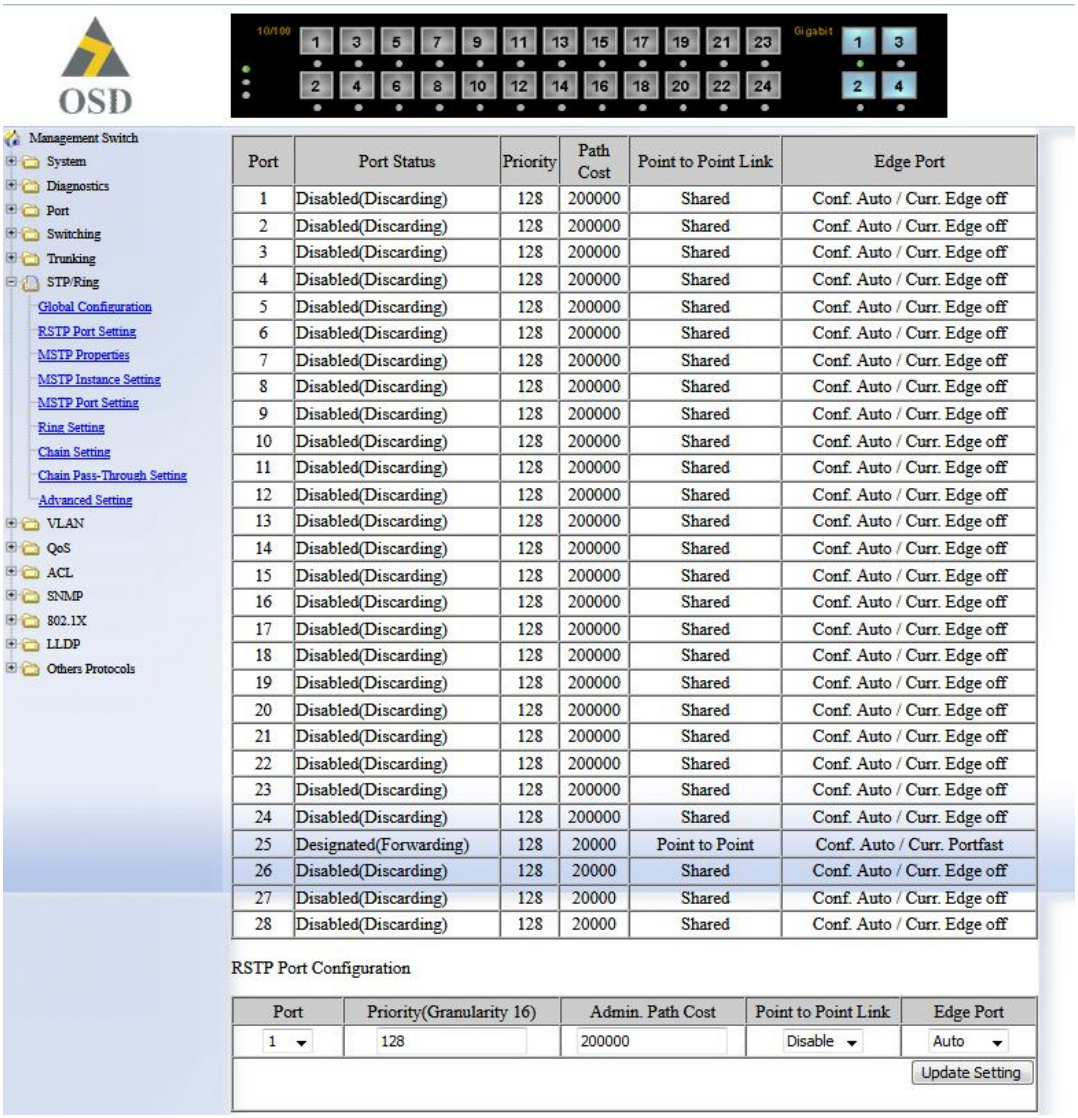
1. Port: Click “Port” drop-down menu to choose port from “Port” drop-down list.
2. Trunk Type: Click “Trunk Type” drop-down menu to choose “None”, “Static”, or “LACP” from “Trunk Type” drop-down list to disable or enable Static or LACP Trunk.
3. Admin Key: Click in “Admin Key” text box and type a decimal number 1-6 for FE ports. Type a decimal number 7-8 for GE ports.
4. LACP Mode: Click “LACP Mode” drop-down menu to choose “Active” or “Passive” from “LACP Mode” drop-down list to enable Active or Passive LACP Mode.
5. LACP Port Priority (Set 0 for None): Click in “LACP Port Priority” text box and type 1-65535 for port. Default value is 32768.
6. LACP Timeout: Click “LACP Timeout” drop-down menu to choose “Long” or “Short” from “LACP Timeout” drop-down list to enable Long or Short LACP Timeout. Long timeout value is 90 seconds. Short timeout value is 3 seconds.
7. Update Setting: Click “Update Setting” button when you finished Trunk Configuration.
8. LACP System Priority (1-65535, default 32768): Click in “LACP System Priority” text box and type 1-65535. Default value is 32768.
9. Submit: Click “Submit” button when you finished LACP System Priority settings.

## 6.8 STP / RING




**GLOBAL CONFIGURATION**

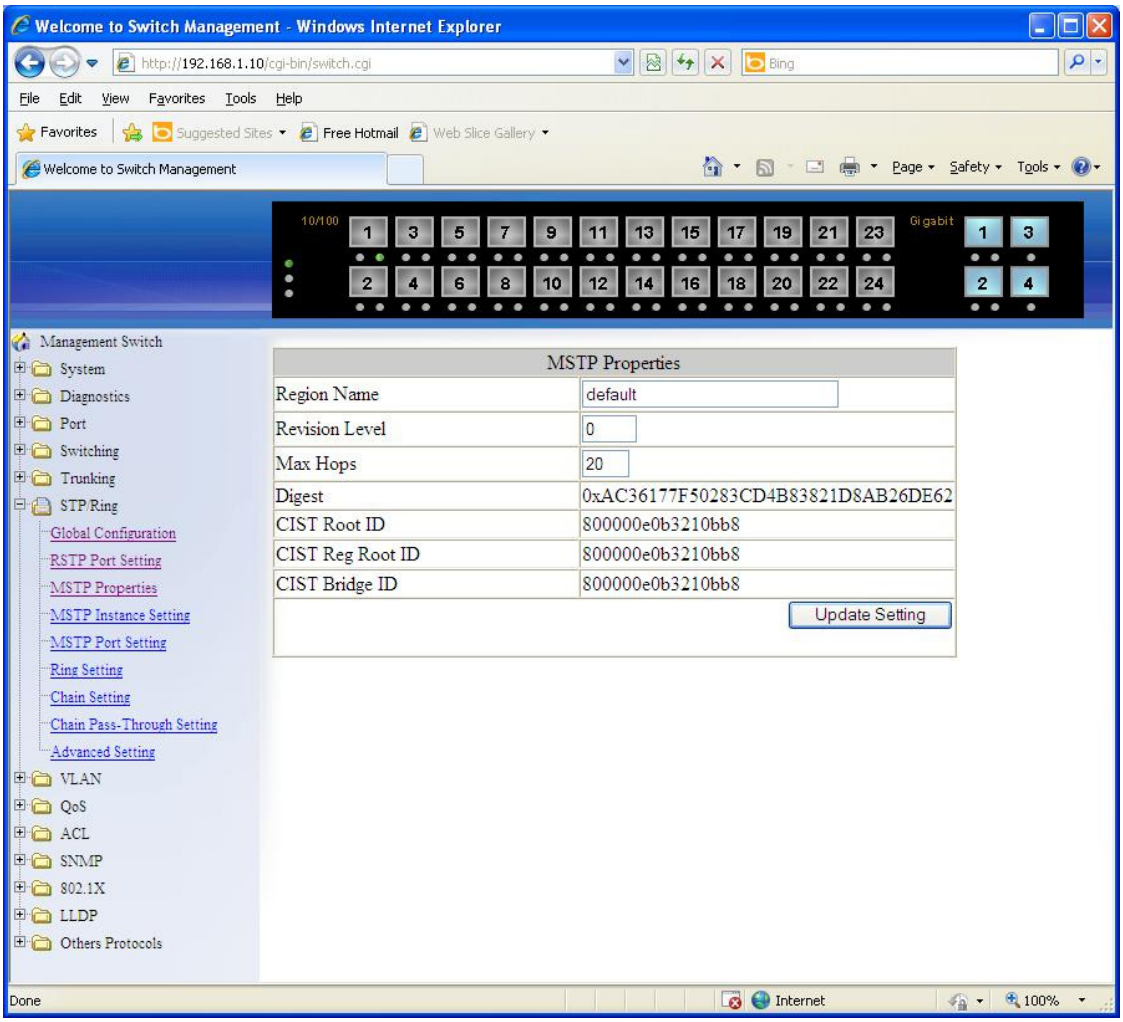
1. Spanning Tree Protocol: Click “Spanning Tree Protocol” drop-down menu to choose “Enable” or “Disable” from “Spanning Tree Protocol” drop-down list to enable or disable Spanning Tree Protocol.
2. Bridge Priority (0..61440): Click in “Bridge Priority” text box and type a decimal number between 0 and 61440.
3. Hello Time (sec) (1..9 sec): Click in “Hello Time” text box and type a decimal number between 1 and 9.
4. Max Age (sec) (6..28 sec): Click in “Max Age” text box and type a decimal number between 6 and 28.
5. Forward Delay (sec) (4..30 sec): Click in “Forward Delay” text box and type a decimal number between 4 and 30.
6. STP Version: Click “STP Version” drop-down menu to choose “MSTP”, “RSTP” or “STP compatible” from “STP Version” drop-down list.
7. Update Setting: Click “Update Setting” button when you finished Global Configuration.




| Port | Port Status | Priority | Path Cost | Point to Point Link | Edge Port |
|---|---|---|---|---|---|
| 1 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 2 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 3 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 4 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 5 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 6 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 7 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 8 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 9 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 10 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 11 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 12 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 13 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 14 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 15 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 16 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 17 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 18 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 19 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 20 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 21 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 22 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 23 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 24 | Disabled(Discarding) | 128 | 200000 | Shared | Conf. Auto / Curr. Edge off |
| 25 | Designated(Forwarding) | 128 | 20000 | Point to Point | Conf. Auto / Curr. Portfast |
| 26 | Disabled(Discarding) | 128 | 20000 | Shared | Conf. Auto / Curr. Edge off |
| 27 | Disabled(Discarding) | 128 | 20000 | Shared | Conf. Auto / Curr. Edge off |
| 28 | Disabled(Discarding) | 128 | 20000 | Shared | Conf. Auto / Curr. Edge off |

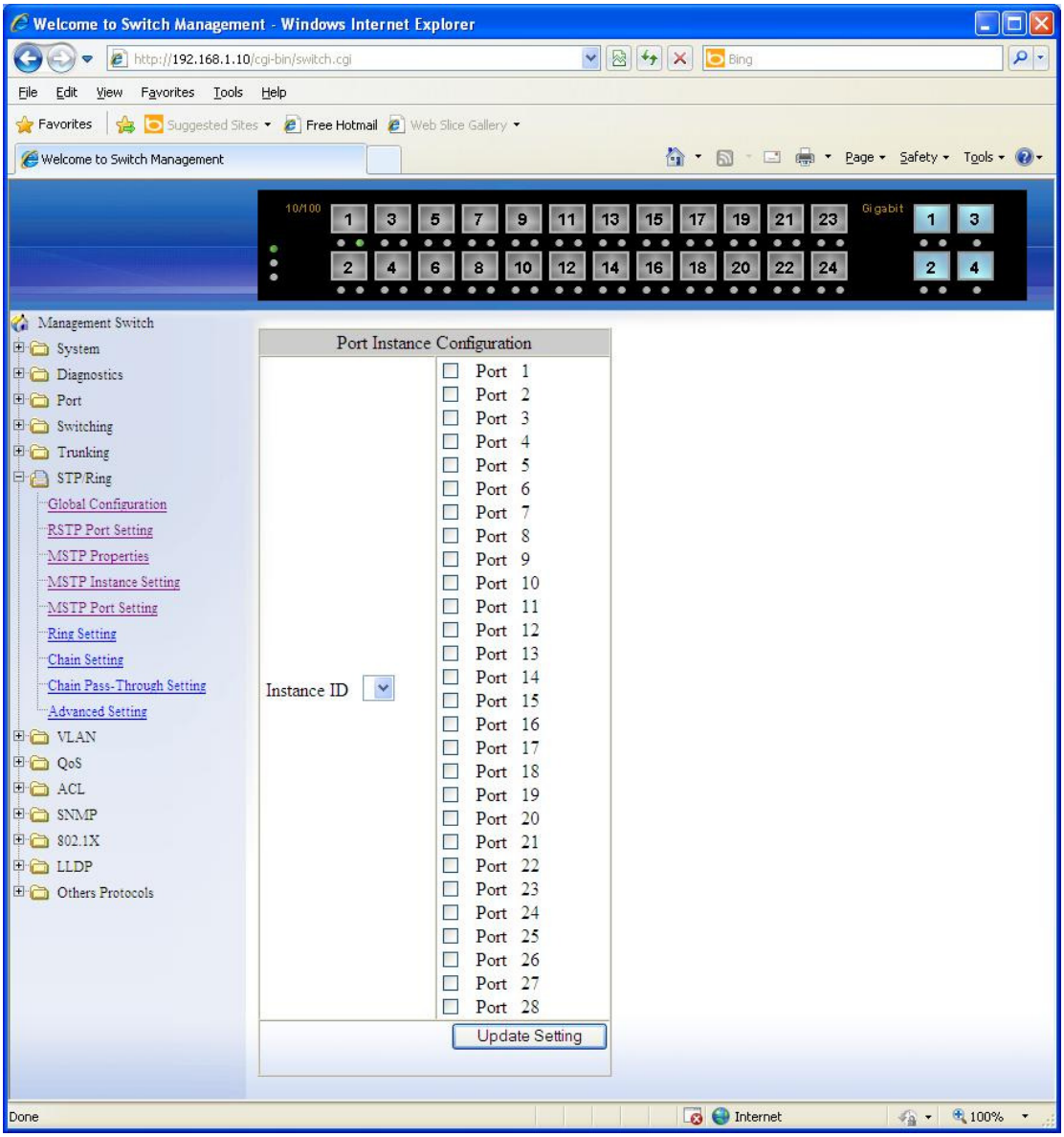
**RSTP PORT SETTING**

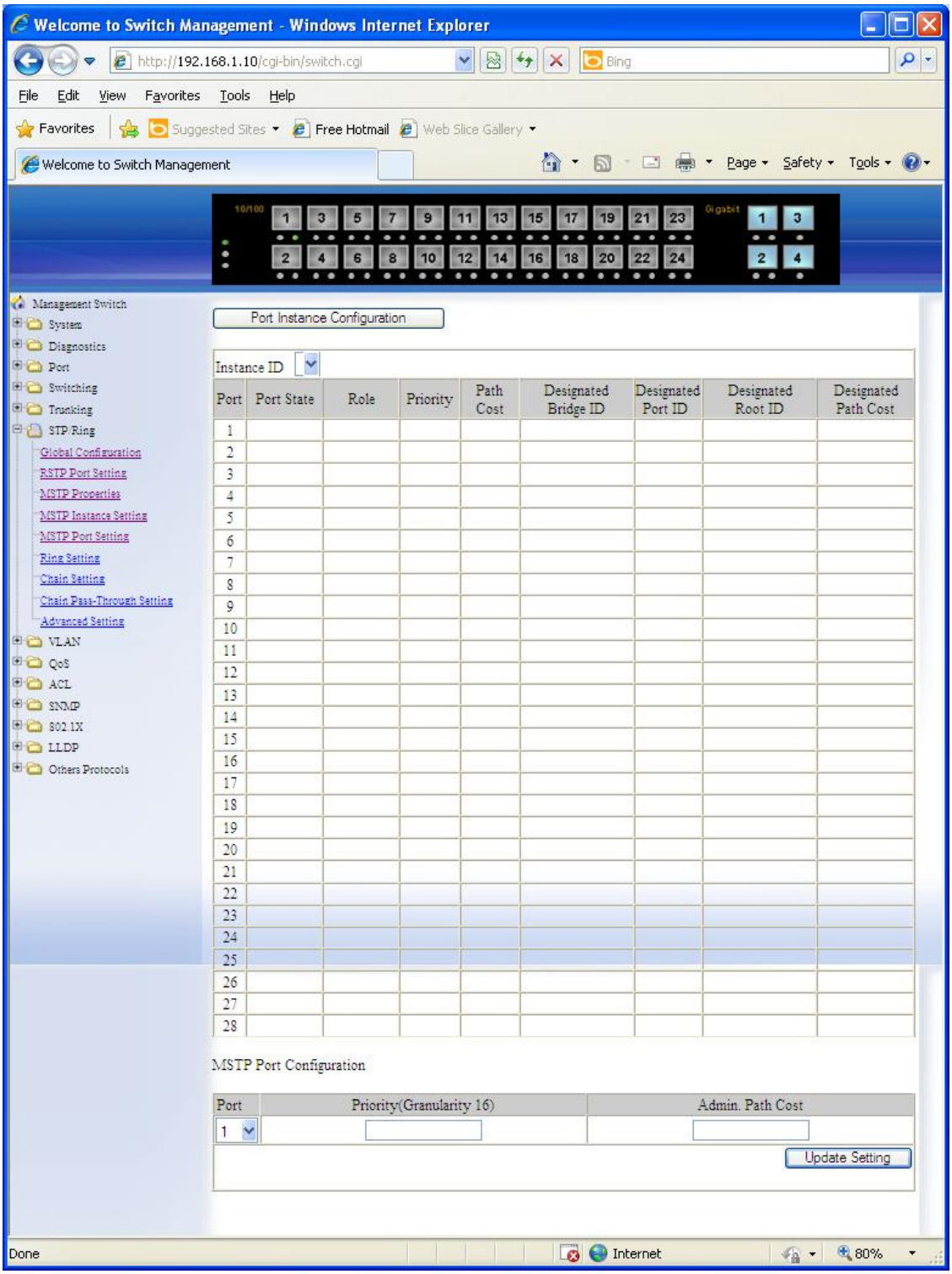
1. STP Version: Click “STP Version” drop-down menu to choose “RSTP” from “STP Version” drop-down list.
2. Port: Click “Port” drop-down menu to choose port from “Port” drop-down list.
3. Priority(Granularity 16): Click in “Priority” text box and enter a value between 0 and 240 to set the priority for the port. A higher priority will designate the port to forward packets first. A lower number denotes a higher priority. This entry must be divisible by 16. The default priority setting is 128.
4. Admin. Path Cost: Click in “Admin. Path Cost” text box and enter a value between 0 and 2000000 to set the Admin. Path Cost for the port. 0 (auto) - Setting 0 for the Admin. Path Cost will automatically set the speed for forwarding packets to the port for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000.
5. Point to Point Link: Click “Point to Point Link” drop-down menu to choose “Enable” or “Disable” from “Point to Point Link” drop-down list to enable or disable Point to Point Link for the port.
6. Edge Port: Click “Edge Port” drop-down menu to choose “Enable”, “Disable”, or “Auto” from “Edge Port” drop-down list to set Enable, Disable, or Auto Edge Port for the port.
7. Update Setting: Click “Update Setting” button when you finished RSTP Port Setting.




**MSTP PROPERTIES**

1. STP Version: Click “STP Version” drop-down menu to choose “MSTP” from “STP Version” drop-down list.
2. Region Name: Click in “Region Name” text box to create an MST region and specify a name to it. MST bridges of a region form different spanning trees for different VLANs. By default, each MST bridge starts with the region name as its bridge address. This means each MST bridge is a region by itself, unless specifically added to one.
3. Revision Level: Click in “Revision Level” text box to specify the number for configuration information. The default value of revision number is 0.
4. Max Hops: Click in “Max Hops” text box to specify the maximum allowed hops for BPDU in an MST region. This parameter is used by all the instances of the MST. Specifying the max hops for a BPDU prevents the messages from looping indefinetely in the network. When a bridge receives a MST BPDU that has exceeded the allowed max-hops, it discards the BPDU.
5. Update Setting: Click “Update Setting” button when you finished MSTP Properties setting.


Welcome to Switch Management - Windows Internet Explorer
http://192.168.1.10/cgi-bin/switch.cgi
File Edit View Favorites Tools Help
Favorites
Welcome to Switch Management
10/100
Gigabit
Management Switch
System
Diagnostics
Port
Switching
Trunking
STP/Ring
Global Configuration
RSTP Port Setting
MSTP Properties
MSTP Instance Setting
MSTP Port Setting
Ring Setting
Chain Setting
Chain Pass-Through Setting
Advanced Setting
VLAN
QoS
ACL
SNMP
802.1X
LLDP
Others Protocols
Port Instance Configuration
Instance ID
Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
Port 7
Port 8
Port 9
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15
Port 16
Port 17
Port 18
Port 19
Port 20
Port 21
Port 22
Port 23
Port 24
Port 25
Port 26
Port 27
Port 28
Update Setting
Done
Internet
100%


Welcome to Switch Management - Windows Internet Explorer
http://192.168.1.10/cgi-bin/switch.cgi
File Edit View Favorites Tools Help
Favorites Suggested Sites Free Hotmail Web Slice Gallery
Welcome to Switch Management
Page Safety Tools
10/100
Gigabit
Management Switch
System
Diagnostics
Port
Switching
Trunking
STP/Ring
Global Configuration
RSTP Port Setting
MSTP Properties
MSTP Instance Setting
MSTP Port Setting
Ring Setting
Chain Setting
Chain Pass-Through Setting
Advanced Setting
VLAN
QoS
ACL
SNMP
802.1X
LLDP
Others Protocols
Port Instance Configuration
Instance ID
Port
Port State
Role
Priority
Path Cost
Designated Bridge ID
Designated Port ID
Designated Root ID
Designated Path Cost
MSTP Port Configuration
Port
Priority(Granularity 16)
Admin. Path Cost
Update Setting
Done
Internet
80%

**MSTP INSTANCE SETTING**

VLAN Instance Configuration

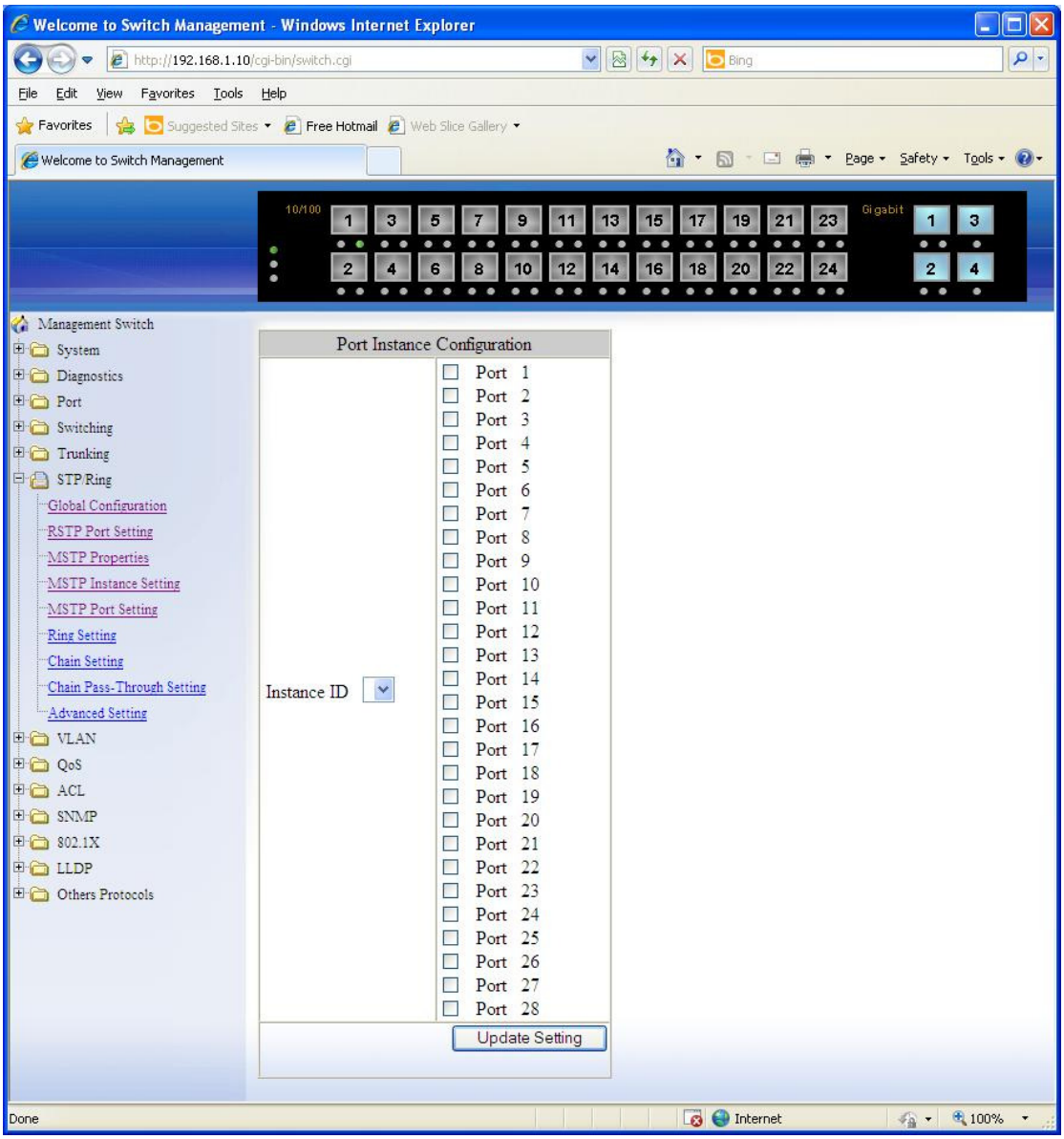
1. VLAN Instance Configuration: Click “VLAN Instance Configuration” button. The “VLAN Instance Configuration” window appears.
2. VLAN ID: Click “VLAN ID” drop-down menu to choose VLAN from “VLAN ID” drop-down list to simultaneously add multiple VLANs for the corresponding instance of a bridge.
3. Instance ID (1..15): Click in “Instance ID” text box to specify the instance ID.
4. Update Setting: Click “Update Setting” button when you finished VLAN Instance Configuration.

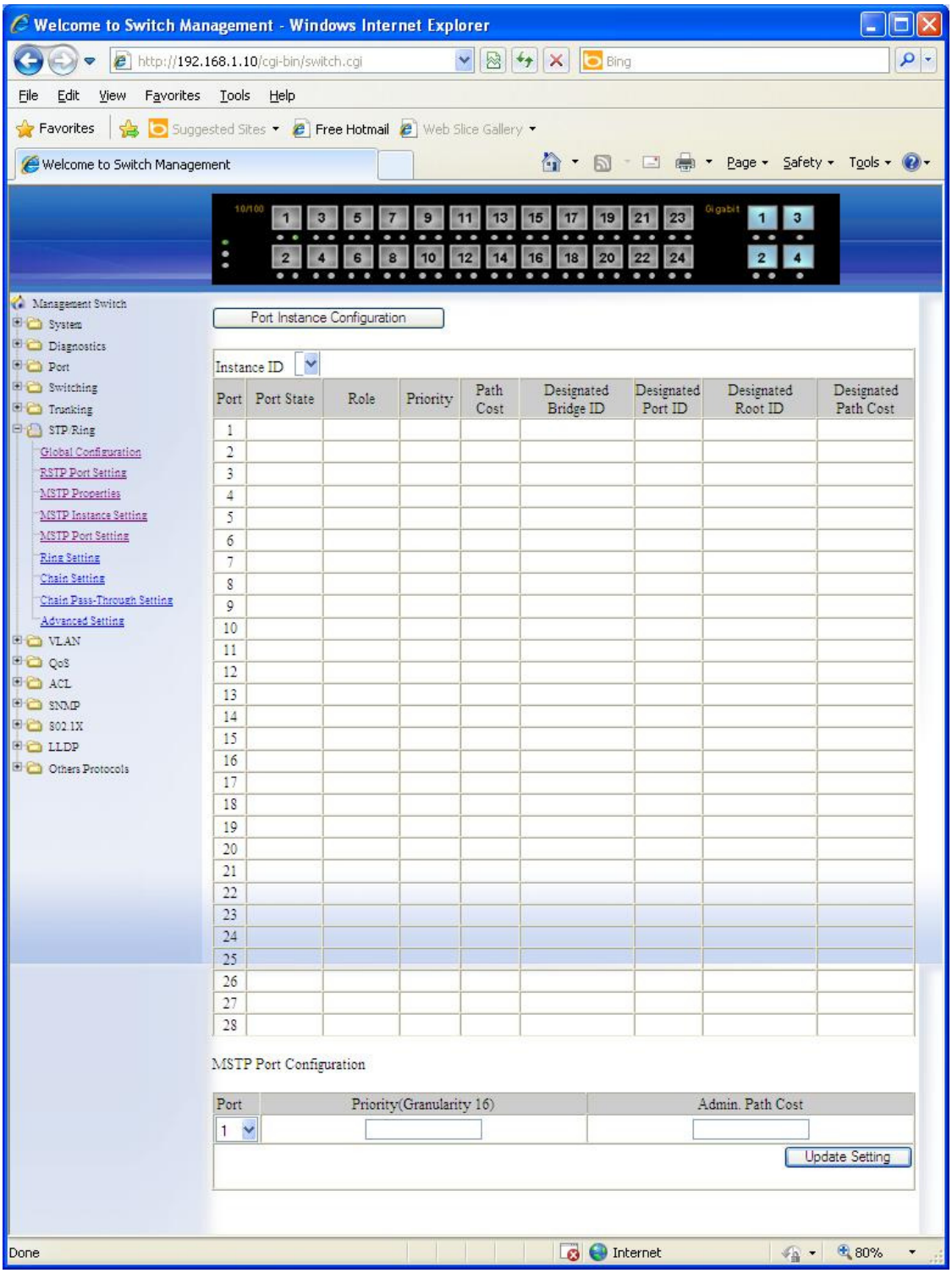
Included VLANs

1. Instance ID: Click “Instance ID” drop-down menu to choose instance ID from “Instance ID” drop-down list.
2. Included VLAN: Click “Included VLAN” drop-down menu to choose VLAN from “Included VLAN” drop-down list.

Instance Setting

1. Bridge Priority (0..61440): Click in “Bridge Priority” text box to set the bridge priority for an MST instance to the value specified. The lower the priority of the bridge, the better the chances are the bridge becoming a root bridge or a designated bridge for the LAN.
2. Update Setting: Click “Update Setting” button when you finished VLAN Instance Configuration.


Welcome to Switch Management - Windows Internet Explorer
http://192.168.1.10/cgi-bin/switch.cgi
File Edit View Favorites Tools Help
Favorites
Welcome to Switch Management
Page Safety Tools
10/100
Gigabit
Management Switch
System
Diagnostics
Port
Switching
Trunking
STP/Ring
Global Configuration
RSTP Port Setting
MSTP Properties
MSTP Instance Setting
MSTP Port Setting
Ring Setting
Chain Setting
Chain Pass-Through Setting
Advanced Setting
VLAN
QoS
ACL
SNMP
802.1X
LLDP
Others Protocols
Port Instance Configuration
Instance ID
Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
Port 7
Port 8
Port 9
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15
Port 16
Port 17
Port 18
Port 19
Port 20
Port 21
Port 22
Port 23
Port 24
Port 25
Port 26
Port 27
Port 28
Update Setting
Done
Internet
100%


Welcome to Switch Management - Windows Internet Explorer
http://192.168.1.10/cgi-bin/switch.cgi
Bing
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Free Hotmail
Web Slice Gallery
Welcome to Switch Management
Page Safety Tools
10/100
Gigabit
Management Switch
System
Diagnostics
Port
Switching
Trunking
STP/Ring
Global Configuration
RSTP Port Setting
MSTP Properties
MSTP Instance Setting
MSTP Port Setting
Ring Setting
Chain Setting
Chain Pass-Through Setting
Advanced Setting
VLAN
QoS
ACL
SNMP
802.1X
LLDP
Others Protocols
Port Instance Configuration
Instance ID
Port
Port State
Role
Priority
Path Cost
Designated Bridge ID
Designated Port ID
Designated Root ID
Designated Path Cost
MSTP Port Configuration
Port
Priority(Granularity 16)
Admin. Path Cost
Update Setting
Done
Internet
80%

**MSTP PORT SETTING**

Port Instance Configuration

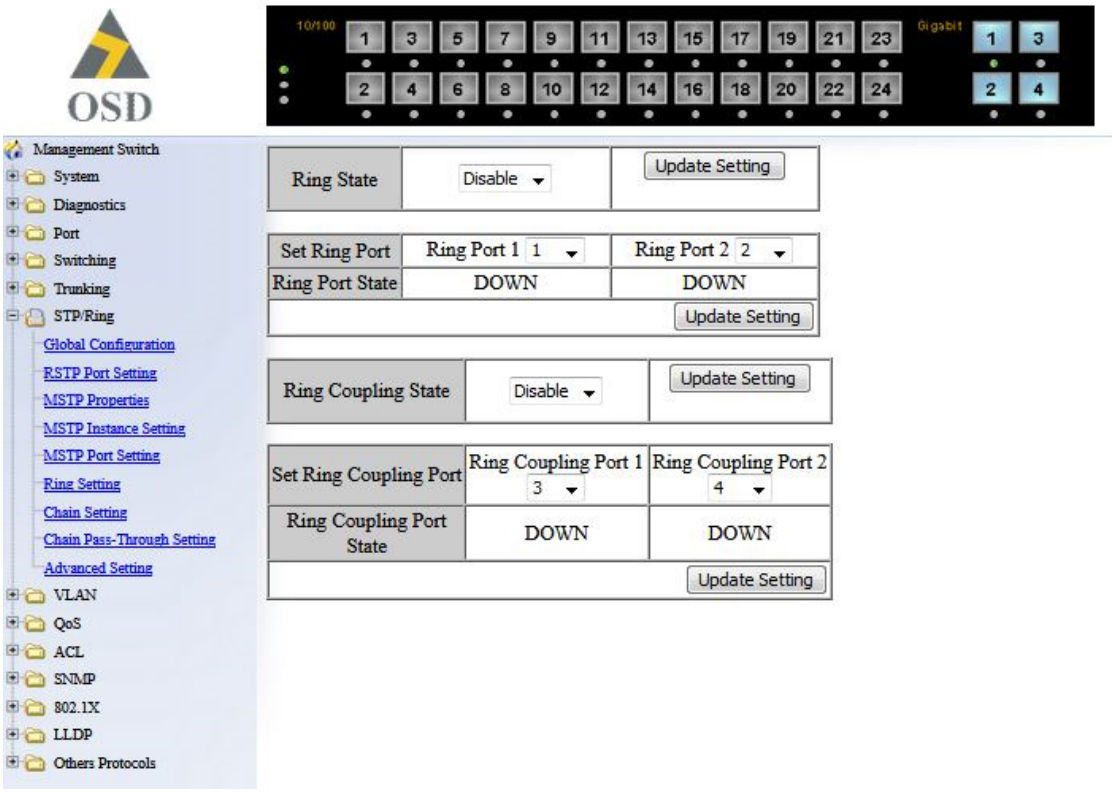
1. Instance ID: Click “Instance ID” drop-down menu to choose instance ID from “Instance ID” drop-down list.
2. Click ports to assign ports to the corresponding instance ID.
3. Update Setting: Click “Update Setting” button when you finished Port Instance Configuration.

Instance ID

1. Instance ID: Click “Instance ID” drop-down menu to choose instance ID from “Instance ID” drop-down list.

MSTP Port Configuration

1. Port: Click “Port” drop-down menu to choose port from “Port” drop-down list.
2. Priority(Granularity 16): Click in “Priority” text box to set the port priority for a bridge group. The Multiple Spanning Tree Protocol uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies a better priority. In the case of the same priority, the interface index will serve as the tiebreaker, with the lower-numbered interface being preferred over others. The permitted range is 0-240. The priority values can only be set in increments of 16.
3. Admin. Path Cost: Click in “Admin. Path Cost” text box to set the cost of a path associated with an interface.
4. Update Setting: Click “Update Setting” button when you finished MSTP Port Setting.




**RING SETTING**

Ring State:

1. Click “Ring State” drop-down menu from “Ring State” drop-down list to choose “Enable” or “Disable” to enable or disable Ring State.
2. Update Setting: Click “Update Setting” button when you finished Ring State setting.

Set Ring Port:

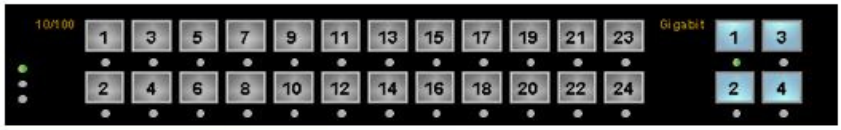
1. Ring Port 1: Click “Ring Port 1” drop-down menu to choose Ring Port 1 from “Ring Port 1” drop-down list.
2. Ring Port 2: Click “Ring Port 2” drop-down menu to choose Ring Port 2 from “Ring Port 2” drop-down list.
3. Update Setting: Click “Update Setting” button when you finished Set Ring Port.

Ring Coupling State:

1. Click “Ring Coupling State” drop-down menu from “Ring Coupling State” drop-down list to choose “Enable” or “Disable” to enable or disable Ring Coupling State.
2. Update Setting: Click “Update Setting” button when you finished Ring Coupling State setting.

Set Ring Coupling Port:

1. Ring Coupling Port 1: Click “Ring Coupling Port 1” drop-down menu to choose Ring Coupling Port 1 from “Ring Coupling Port 1” drop-down list.
2. Ring Coupling Port 2: Click “Ring Coupling Port 2” drop-down menu to choose Ring Coupling Port 2 from “Ring Coupling Port 2” drop-down list.
3. Update Setting: Click “Update Setting” button when you finished Set Ring Coupling Port.




OSD

- Management Switch
- System
- Diagnostics
- Port
- Switching
- Trunking
- STP/Ring
  - Global Configuration
  - RSTP Port Setting
  - MSTP Properties
  - MSTP Instance Setting
  - MSTP Port Setting
  - Ring Setting
  - Chain Setting
  - Chain Pass-Through Setting
  - Advanced Setting
- VLAN
- QoS
- ACL
- SNMP
- 802.1X
- LLDP
- Others Protocols

| Chain Protocol | | | |
|---|---|---|---|
| Port | Enable | Role | State |
| 1 | ☐ | None | None |
| 2 | ☐ | None | None |
| 3 | ☐ | None | None |
| 4 | ☐ | None | None |
| 5 | ☐ | None | None |
| 6 | ☐ | None | None |
| 7 | ☐ | None | None |
| 8 | ☐ | None | None |
| 9 | ☐ | None | None |
| 10 | ☐ | None | None |
| 11 | ☐ | None | None |
| 12 | ☐ | None | None |
| 13 | ☐ | None | None |
| 14 | ☐ | None | None |
| 15 | ☐ | None | None |
| 16 | ☐ | None | None |
| 17 | ☐ | None | None |
| 18 | ☐ | None | None |
| 19 | ☐ | None | None |
| 20 | ☐ | None | None |
| 21 | ☐ | None | None |
| 22 | ☐ | None | None |
| 23 | ☐ | None | None |
| 24 | ☐ | None | None |
| 25 | ☐ | None | None |
| 26 | ☐ | None | None |
| 27 | ☐ | None | None |
| 28 | ☐ | None | None |

Submit

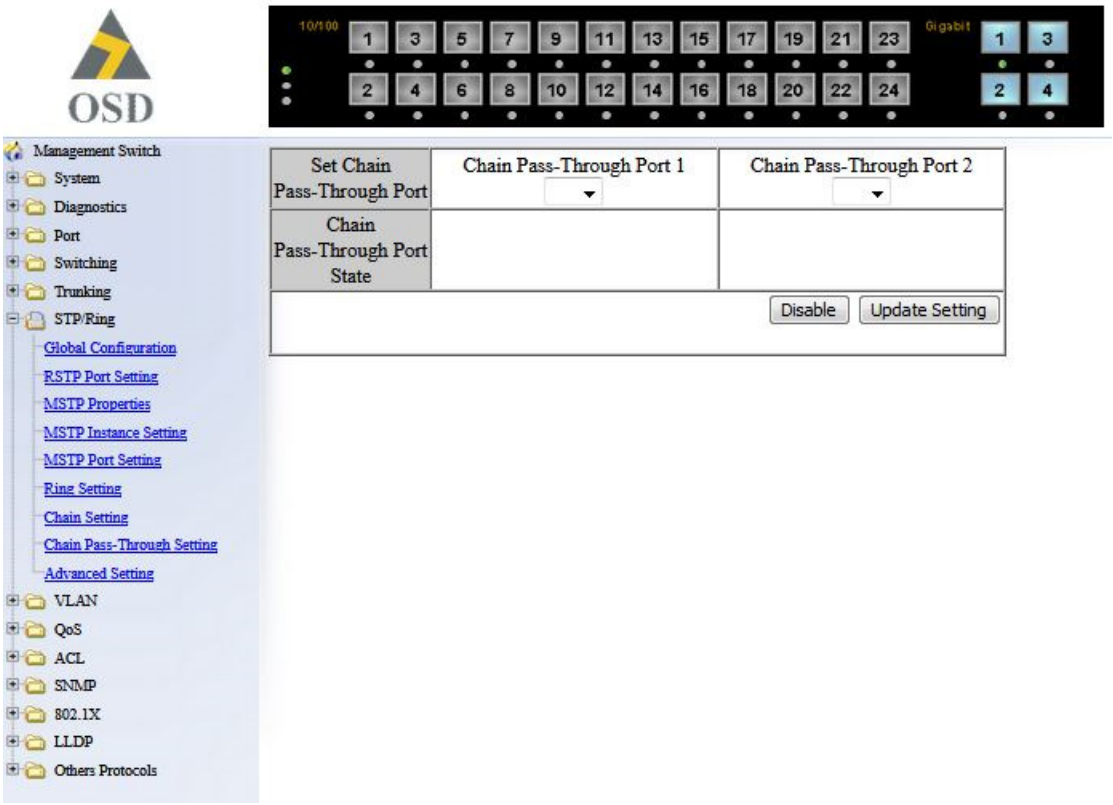
| Global Setting | |
|---|---|
| VLAN (1-4094, default:1) | 1 |
| Priority (0-255, default:128) | 128 |
| Timeout Count (3-255, default:5) | 5 |
| Storm Control (broadcast and multicast) | Enable |

Submit

**CHAIN SETTING**

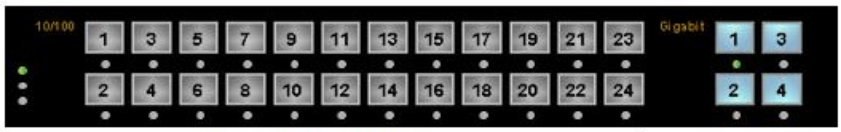
Chain Protocol:
1. Click “Enable” to enable Chain Protocol for ports.
2. Submit: Click “Submit” button when you finished Chain Protocol setting.

Global Setting:
1. VLAN (1-4094, default:1): Click in the “VLAN” textbox and specify a VLAN ID number from 1 ~ 4094.
2. Priority (1-255, default:128): Set the Switch priority for running chain protocol. Switch with lower priority will run as Master (forwarding) port.
3. Timeout Count (3-255, default:5): Set the Switch timeout count for running chain protocol.
   Chain recovery time = (Chain Timeout Count – 1) x 200ms.
   Default Chain recovery time = (5 – 1) x 200ms = 800ms.
4. Storm Control (broadcast and multicast): Click “Storm Control (broadcast and multicast)” drop-down menu to choose “Enable” or “Disable” from “Storm Control (broadcast and multicast)” drop-down list to enable or disable Storm Control (broadcast and multicast) for Chain Protocol setting.
5. Submit: Click “Submit” button when you finished Chain Protocol setting.




**CHAIN PASS-THROUGH SETTING**

1. Chain pass-through port 1: Click “Chain pass-through port 1” drop-down menu to choose Chain pass-through port 1 from “Chain pass-through port 1” drop-down list.
2. Chain pass-through port 2: Click “Chain pass-through port 2” drop-down menu to choose Chain pass-through port 2 from “Chain pass-through port 2” drop-down list.
3. Disable: Click “Disable” button to disable chain pass-through setting.
4. Update Setting: Click “Update Setting” button when you finished chain pass-through setting.




- Management Switch
  - System
  - Diagnostics
  - Port
  - Switching
  - Trunking
  - STP/Ring
    - Global Configuration
    - RSTP Port Setting
    - MSTP Properties
    - MSTP Instance Setting
    - MSTP Port Setting
    - Ring Setting
    - Chain Setting
    - Chain Pass-Through Setting
    - Advanced Setting
  - VLAN
  - QoS
  - ACL
  - SNMP
  - 802.1X
  - LLDP
  - Others Protocols

| Advnced Bridge Configuration | |
|---|---|
| Bridge BPDU-guard configuration | Disable |
| Error disable timeout configuration | Disable |
| Interval (10..1000000 sec), Default: 300 | 300 |

| Advanced Per Port Configuration | | |
|---|---|---|
| Port | Portfast configuration / status | BPDU-guard configuration |
| 1 | Disable / Enable / Curr. OFF | Default |
| 2 | Disable / Enable / Curr. OFF | Default |
| 3 | Disable / Enable / Curr. OFF | Default |
| 4 | Disable / Enable / Curr. OFF | Default |
| 5 | Disable / Enable / Curr. OFF | Default |
| 6 | Disable / Enable / Curr. OFF | Default |
| 7 | Disable / Enable / Curr. OFF | Default |
| 8 | Disable / Enable / Curr. OFF | Default |
| 9 | Disable / Enable / Curr. OFF | Default |
| 10 | Disable / Enable / Curr. OFF | Default |
| 11 | Disable / Enable / Curr. OFF | Default |
| 12 | Disable / Enable / Curr. OFF | Default |
| 13 | Disable / Enable / Curr. OFF | Default |
| 14 | Disable / Enable / Curr. OFF | Default |
| 15 | Disable / Enable / Curr. OFF | Default |
| 16 | Disable / Enable / Curr. OFF | Default |
| 17 | Disable / Enable / Curr. OFF | Default |
| 18 | Disable / Enable / Curr. OFF | Default |
| 19 | Disable / Enable / Curr. OFF | Default |
| 20 | Disable / Enable / Curr. OFF | Default |
| 21 | Disable / Enable / Curr. OFF | Default |
| 22 | Disable / Enable / Curr. OFF | Default |
| 23 | Disable / Enable / Curr. OFF | Default |
| 24 | Disable / Enable / Curr. OFF | Default |
| 25 | Disable / Enable / Curr. OFF | Default |
| 26 | Disable / Enable / Curr. OFF | Default |
| 27 | Disable / Enable / Curr. OFF | Default |
| 28 | Disable / Enable / Curr. OFF | Default |

Note: Per port BPDU-guard configuration takes precedence over bridge configuration.

Submit

## ADVANCED SETTING

Advanced Bridge Configuration:

1. Bridge bpdu-guard cofiguration: Click “Bridge bpdu-guard cofiguration” drop-down menu to choose “Enable” or “Disable” from “Bridge bpdu-guard cofiguration” drop-down list to enable or disable the portfast ports to guard against bpdu received for a bridge. When the BPDU Guard feature is set for a bridge, all portfast-enabled ports of the bridge that have bpdu-guard set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed.
2. Error disable timeout cofiguration: Click “Error disable timeout cofiguration” drop-down menu to choose “Enable” or “Disable” from “Error disable timeout cofiguration” drop-down list to enable or disable the timeout mechanism for the port to be enabled back for a bridge.
3. Interval (10..1000000 sec), Default: 300: Click the text box and type a decimal number as interval time in seconds after which port shall be enabled for a bridge.

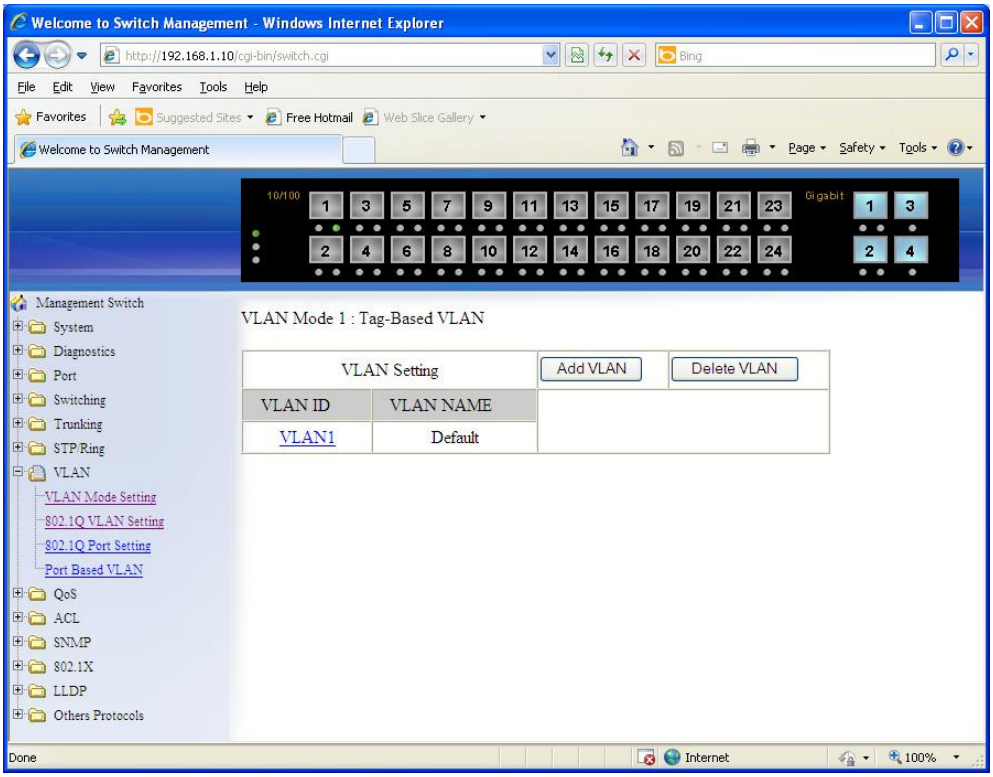
Advanced Per Port Configuration:

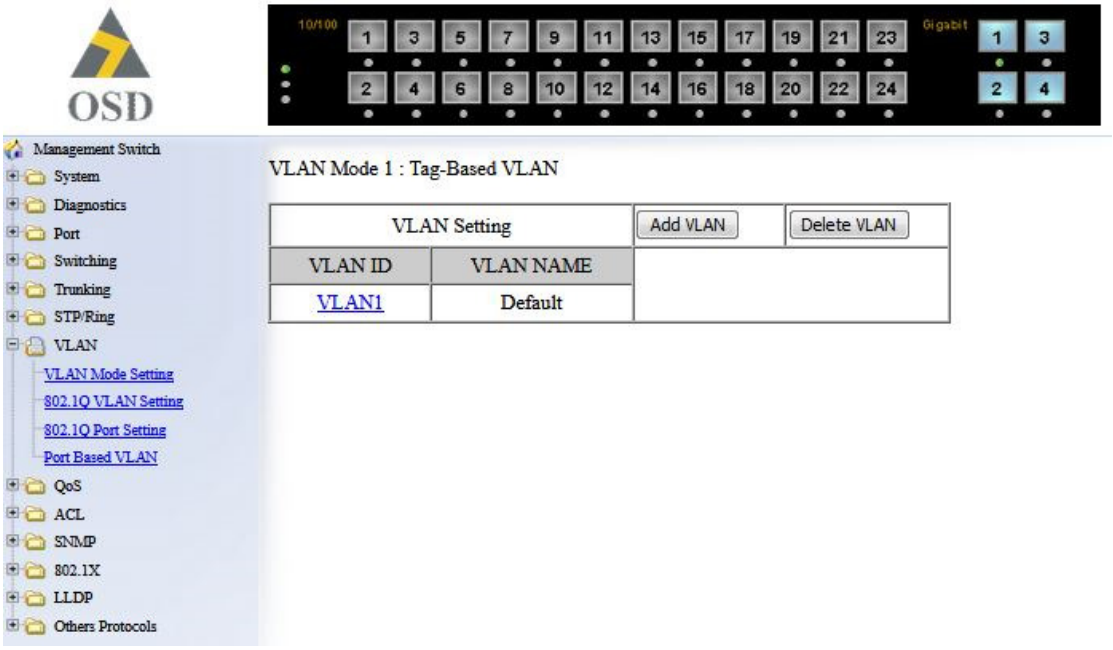
1. Portfast configuration / status: Click and choose “Disable” or “Enable” to disable or enable a port as an edge-port to enable rapid transition.
2. Bpdu-guard configuration: Click “Bpdu-guard configuration” drop-down menu to choose “Enable”, “Disable”, or “Default” from “Bpdu-guard configuration” drop-down list to enable, disable, or default the BPDU Guard feature on a port. This command supersedes the bridge level configuration for the BPDU Guard feature. When the enable or disable parameter is used with this command, this configuration takes precedence over bridge configuration. However, when the default parameter is used with this command, the bridge level BPDU-Guard configuration takes effect.
3. Submit: Click “Submit” button when you finished Advanced Setting.

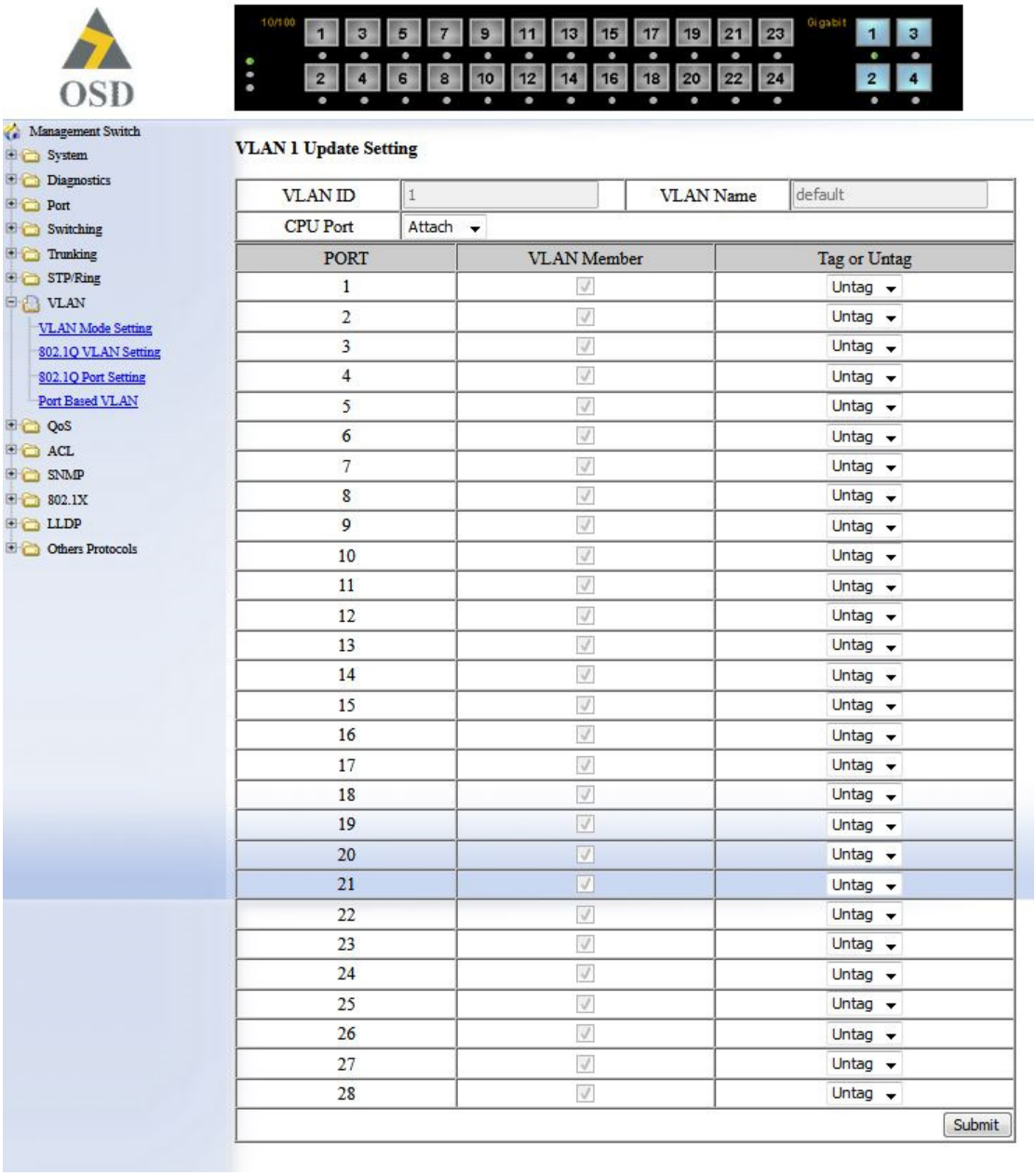
## 6.9 VLAN


**VLAN MODE SETTING**

1. VLAN Mode Setting: Click "VLAN Mode Setting" drop-down menu to choose "Tag-based VLAN" or "Port-based VLAN" from "VLAN Mode Setting" drop-down list.
2. Submit: Click "Submit" button when you finished VLAN Mode Setting.




OSD
10/100
1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24
Gigabit
1 3
2 4
Management Switch
System
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
VLAN Mode Setting
802.1Q VLAN Setting
802.1Q Port Setting
Port Based VLAN
QoS
ACL
SNMP
802.1X
LLDP
Others Protocols
VLAN Mode 1 : Tag-Based VLAN
VLAN Setting
Add VLAN
Delete VLAN
VLAN ID
VLAN NAME
VLAN1
Default



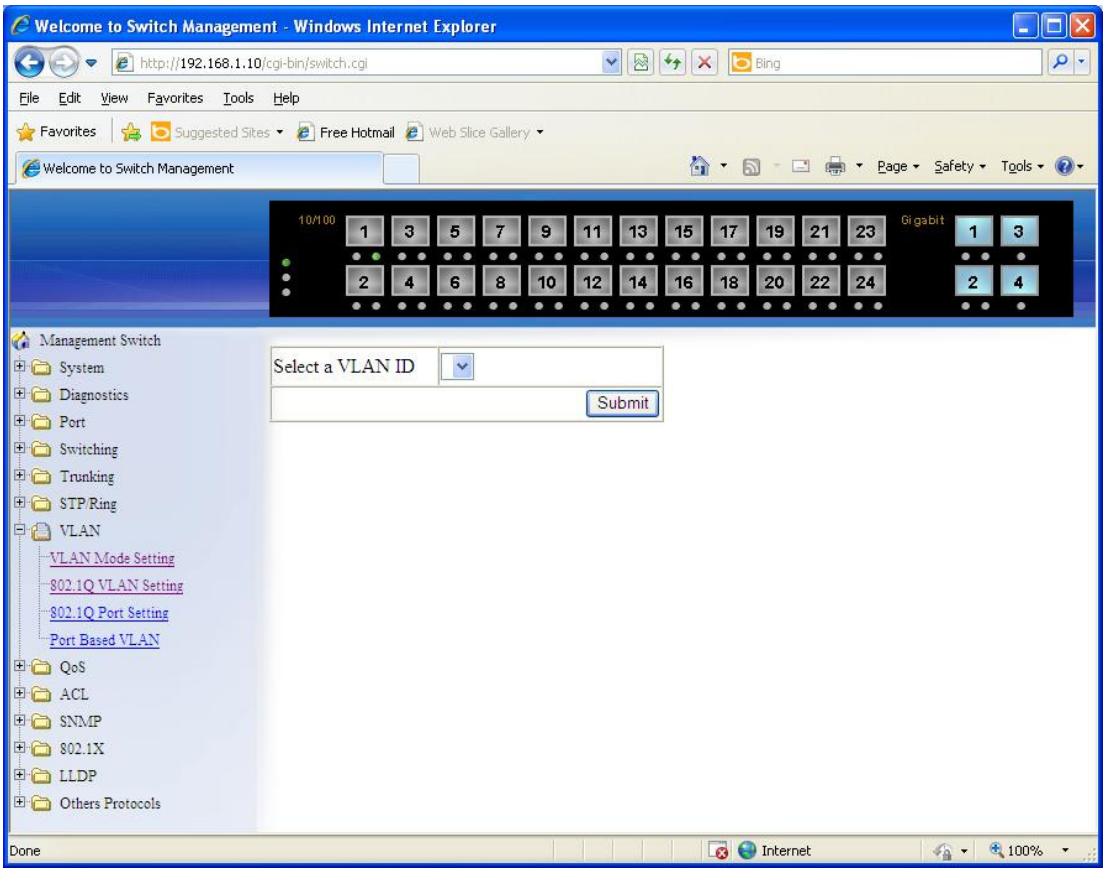

**802.1Q VLAN SETTING**

Add VLAN:

1. 802.1Q VLAN Setting: Click “802.1Q VLAN Setting”. The “VLAN Setting” window appears.
2. Add VLAN: Click “Add VLAN” button to create a new VLAN from “VLAN Setting” window.
3. VLAN ID(2-4094): Click in the “VLAN ID” textbox and specify a new VLAN ID number from 2 ~ 4094.
4. VLAN Name: Click in the “VLAN Name” textbox and type a name for this newly created VLAN.

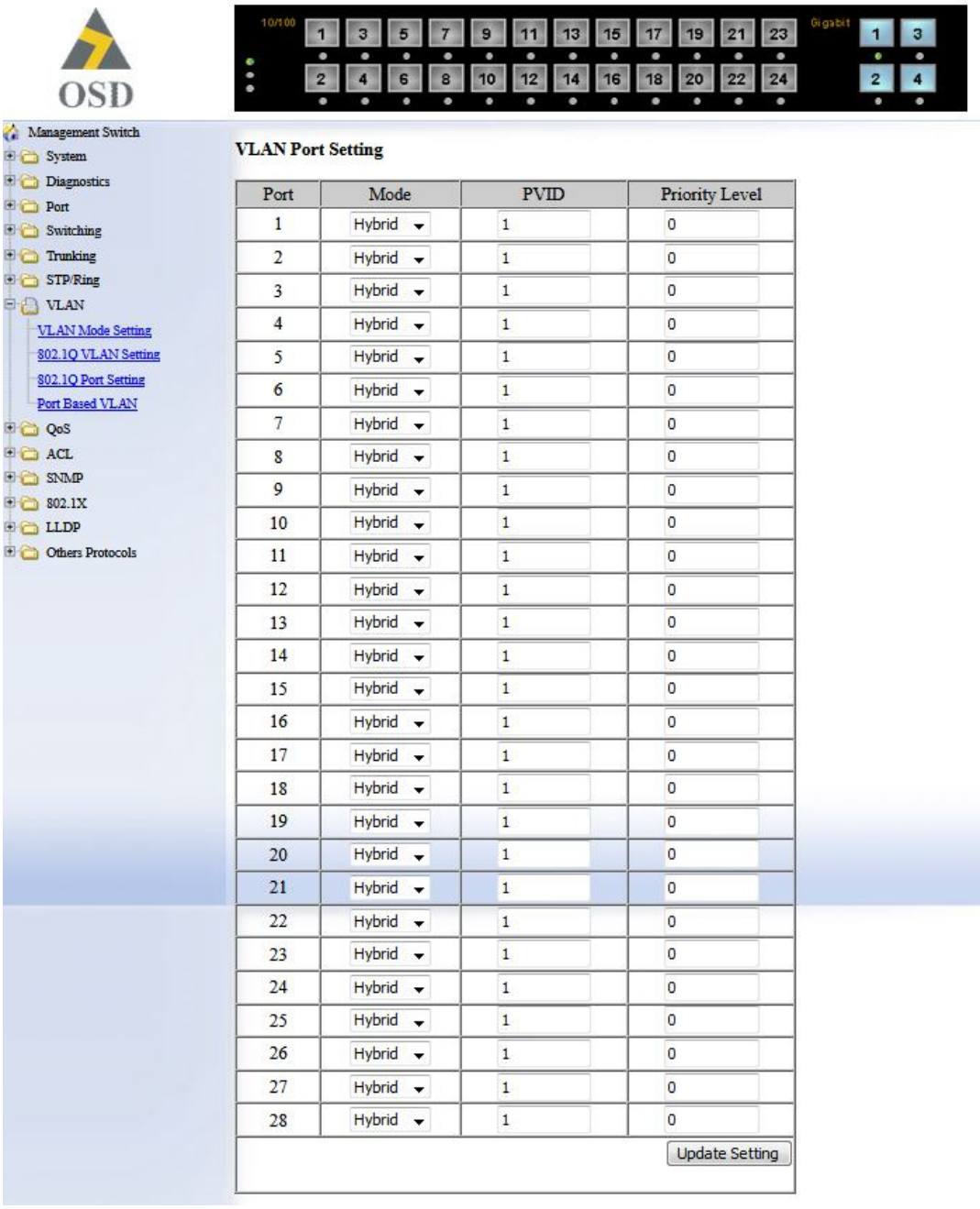
Add port to or delete port from VLAN:

1. VLAN Member: Choose the port to be added to or deleted from the VLAN.
2. Tag or Untag: Click “Tag or Untag” drop-down menu to choose “Tag” or “Untag” from “Tag or Untag” drop-down list for a “Hybrid” port.
3. Submit: Click “Submit” button when you finished VLAN setting.



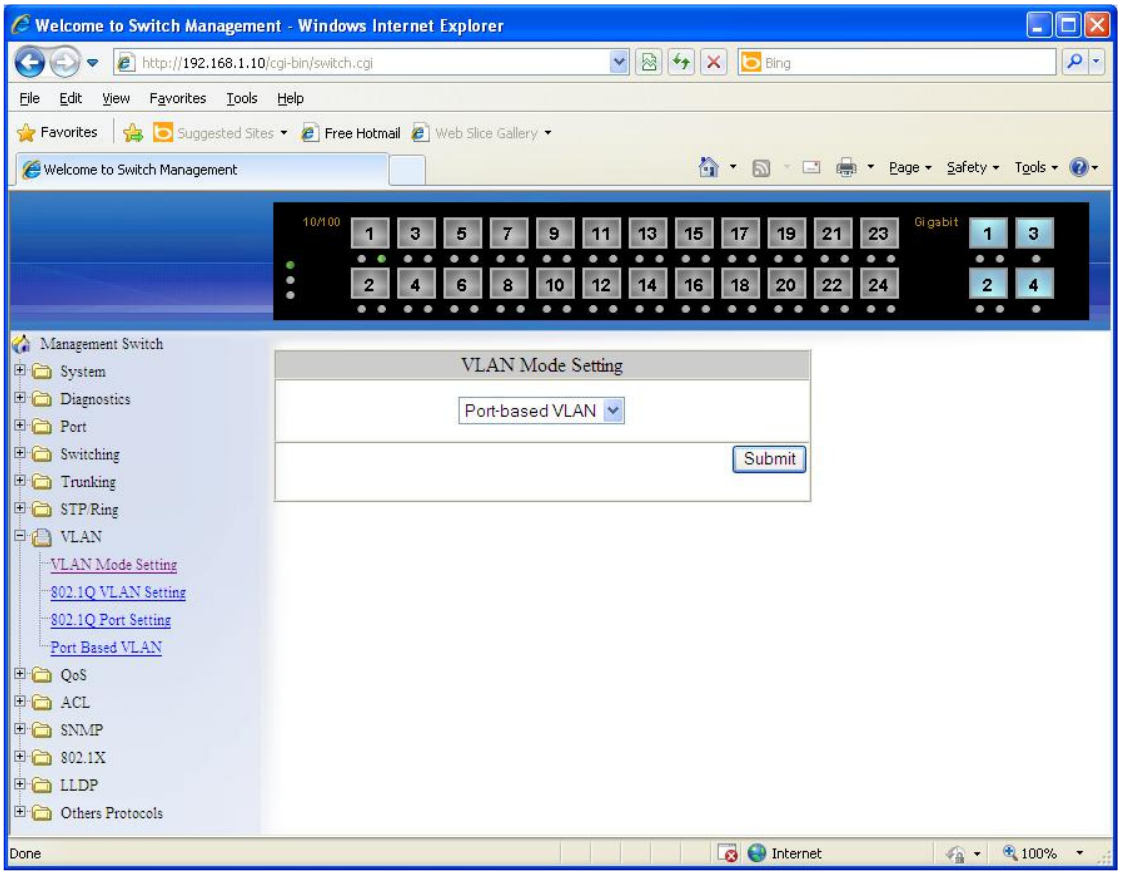

Delete VLAN:

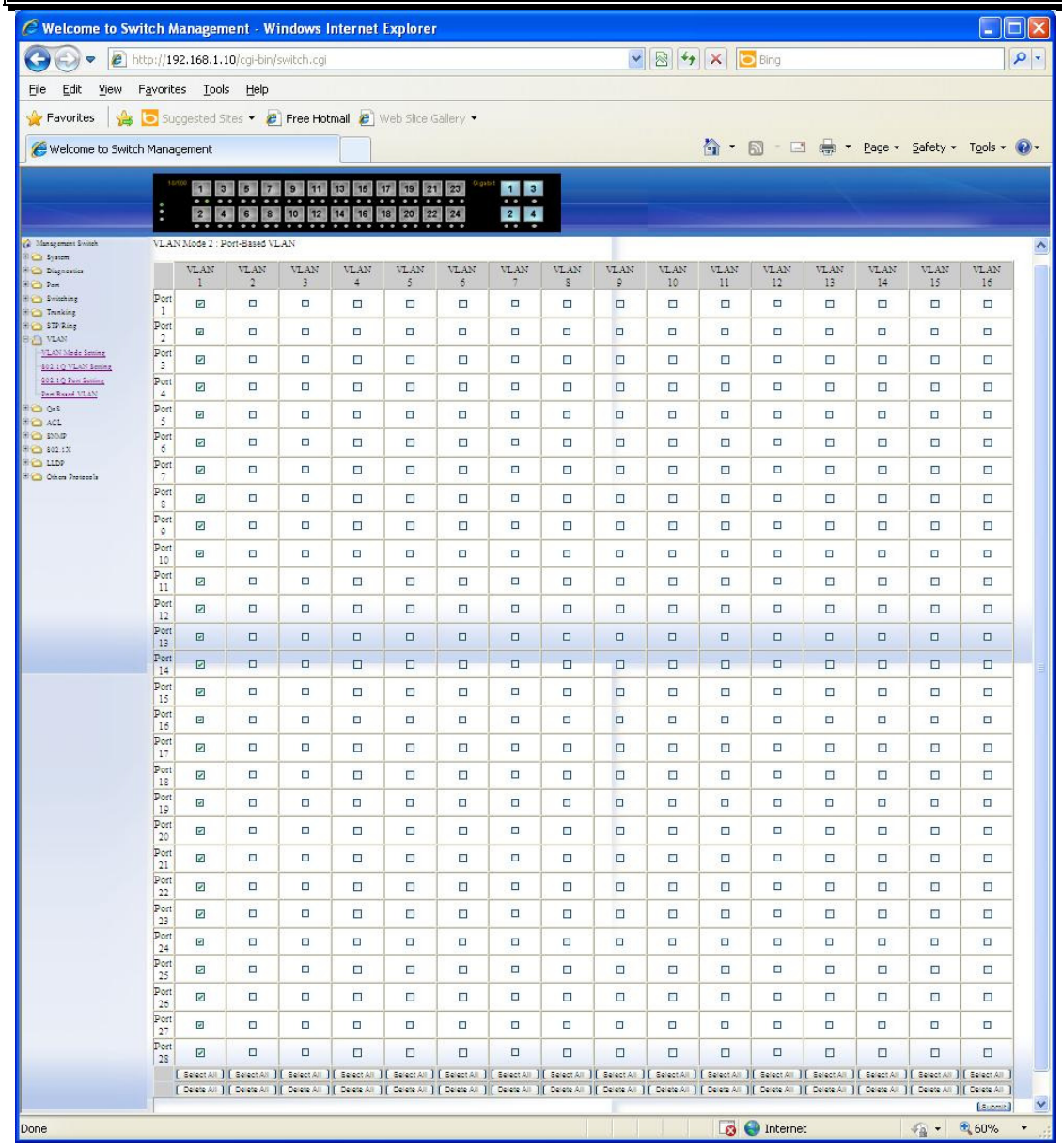
1. 802.1Q VLAN Setting: Click “802.1Q VLAN Setting”. The “VLAN Setting” window appears.
2. Delete VLAN: Click “Delete VLAN” button.
3. Select a VLAN ID: Click “Select a VLAN ID” drop-down menu from “Select a VLAN ID” drop-down list to choose the VLAN to be deleted.
4. Submit: Click “Submit” button when you finished VLAN setting.




**VLAN PORT SETTING**

1. VLAN Port Setting: Click “802.1Q Port Setting”. The “VLAN Port Setting” window appears.
2. Mode: Click “Mode” drop-down menu to choose “Access”, “Trunk”, or “Hybrid” from “Mode” drop-down list for the port. The port will be Tag port if you choose “Trunk” Mode for the port. And the port will be Tag or Untag port if you choose “Hybrid” Mode for the port.
3. PVID: Click in the “PVID” textbox and specify a new PVID number for the port.
4. Priority Level: Click in the “Priority Level” textbox and specify a new Priority Level number from 0 ~ 7 for the port. The default Priority Level number is 0.
5. Update Setting: Click “Update Setting” button when you finished VLAN Port Setting.

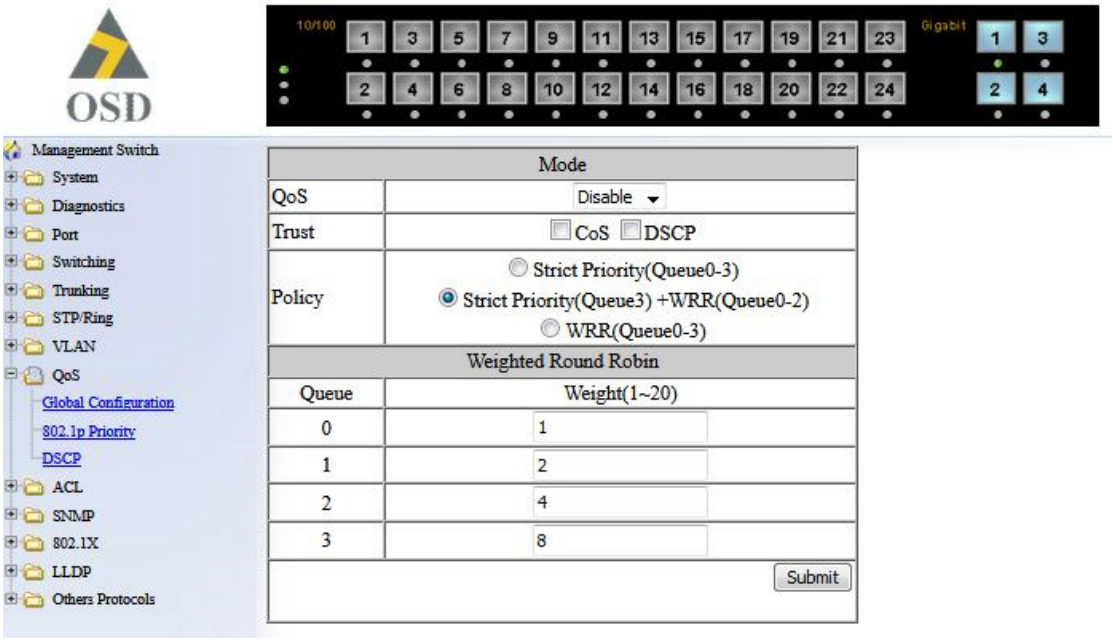

Welcome to Switch Management - Windows Internet Explorer
http://192.168.1.10/cgi-bin/switch.cgi
File Edit View Favorites Tools Help
Favorites
Welcome to Switch Management
10/100
Gigabit
Management Switch
System
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
VLAN Mode Setting
802.1Q VLAN Setting
802.1Q Port Setting
Port Based VLAN
QoS
ACL
SNMP
802.1X
LLDP
Others Protocols
VLAN Mode Setting
Port-based VLAN
Submit
Done
Internet
100%




**PORT BASED VLAN**

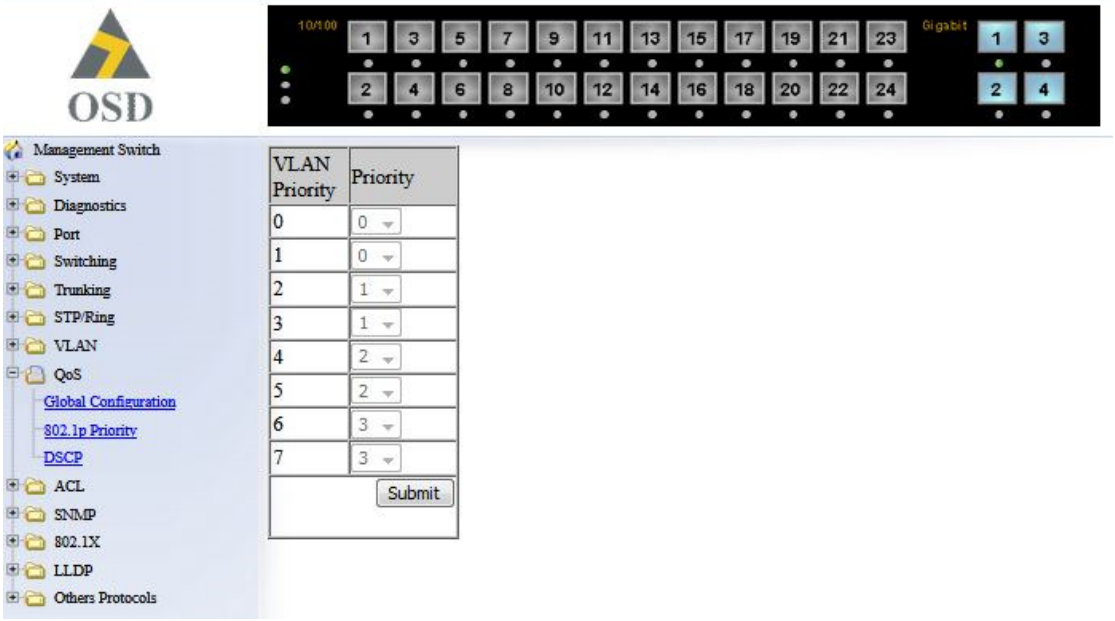
1. VLAN: Choose the port to be added to or deleted from the VLAN.
2. Select All: Click “Select All” button to choose all ports to be added to the VLAN.
3. Delete All: Click “Delete All” button to choose all ports to be deleted from the VLAN.
4. Submit: Click “Submit” button when you finished Port Based VLAN setting.

## 6.10 QOS



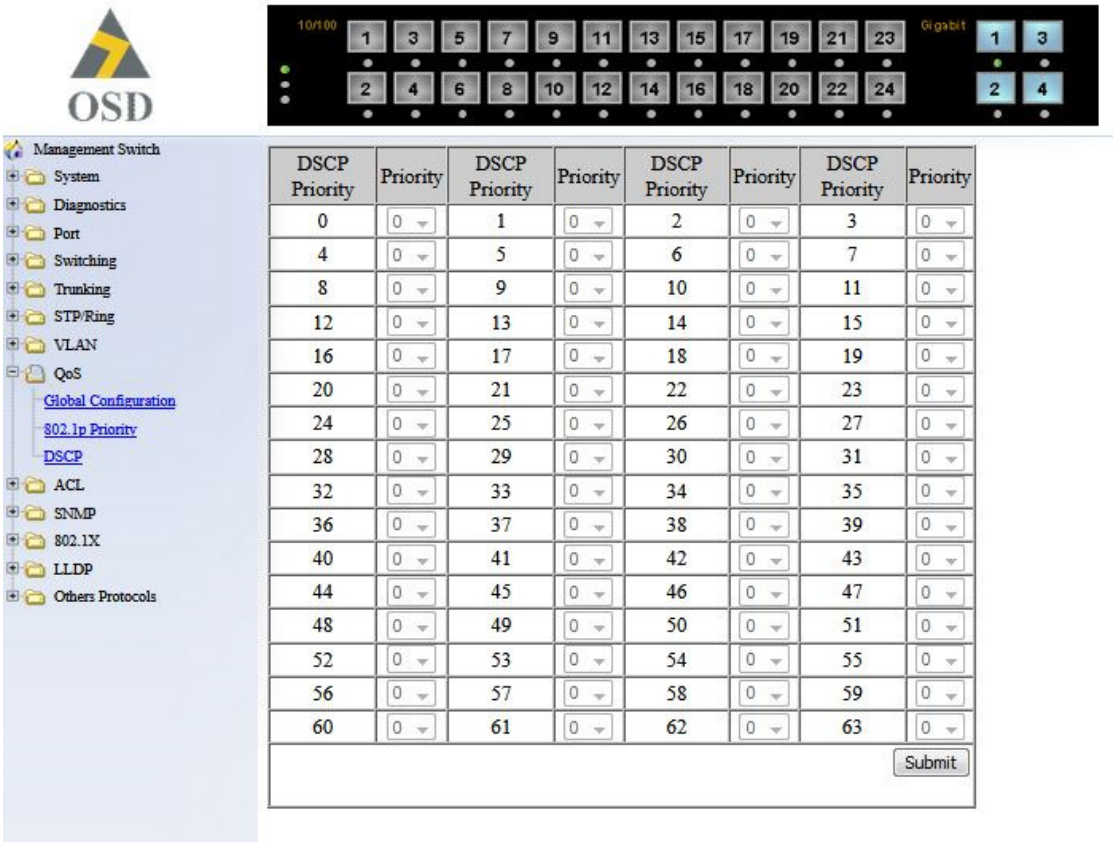

**GLOBAL CONFIGURATION**

1. QoS: Click "QoS" drop-down menu from "QoS" drop-down list to choose "Enable" or "Disable" to enable or disable QoS.
2. Trust: Enable or disable the switch port to trust the CoS (Class of Service) labels of all traffic received on that port. Enable or disable a routed port to trust the DSCP (Differentiated Service Code Point) labels of all traffic received on that port.
3. Policy: Choose "Strict Priority(Queue3) + WRR(Queue0-2)" or "WRR(Queue0-3)". A strict priority queue is always emptied first. The queues that are used in the WRR (Weighted Round Robin) are emptied in a round–robin fashion, and you can configure the weight for each queue.
4. Weighted Round Robin: Click in the "Weight(1~55)" textbox and specify a new number from 1 ~ 55 for Queue 0 ~ 3.
5. Submit: Click "Submit" button when you finished Global Configuration.




**802.1P PRIORITY**

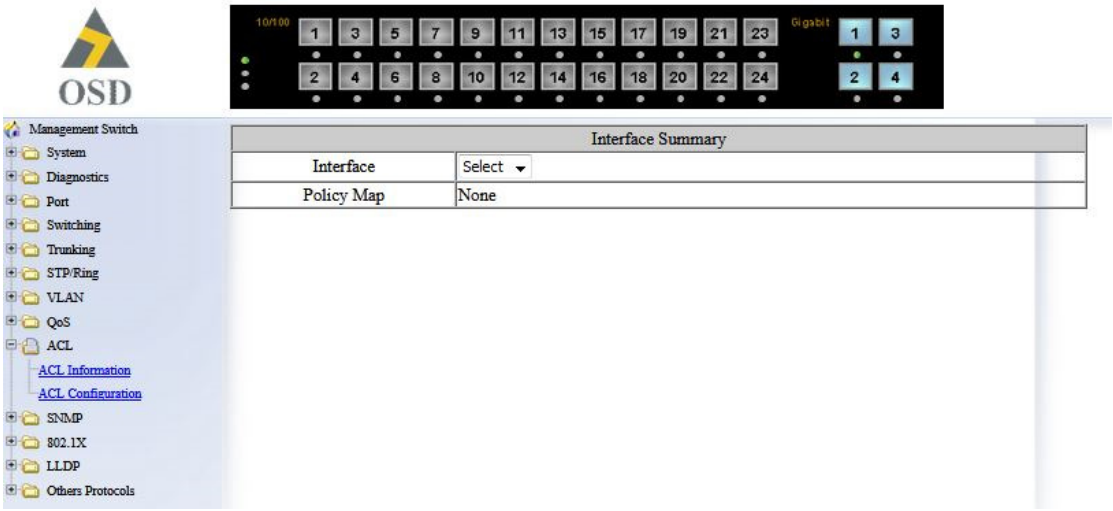
1. Priority: Click “Priority” drop-down menu from “Priority” drop-down list to choose 0 ~ 3 for VLAN Priority 0 ~ 7.
2. Submit: Click “Submit” button when you finished 802.1p priority




***DSCP***

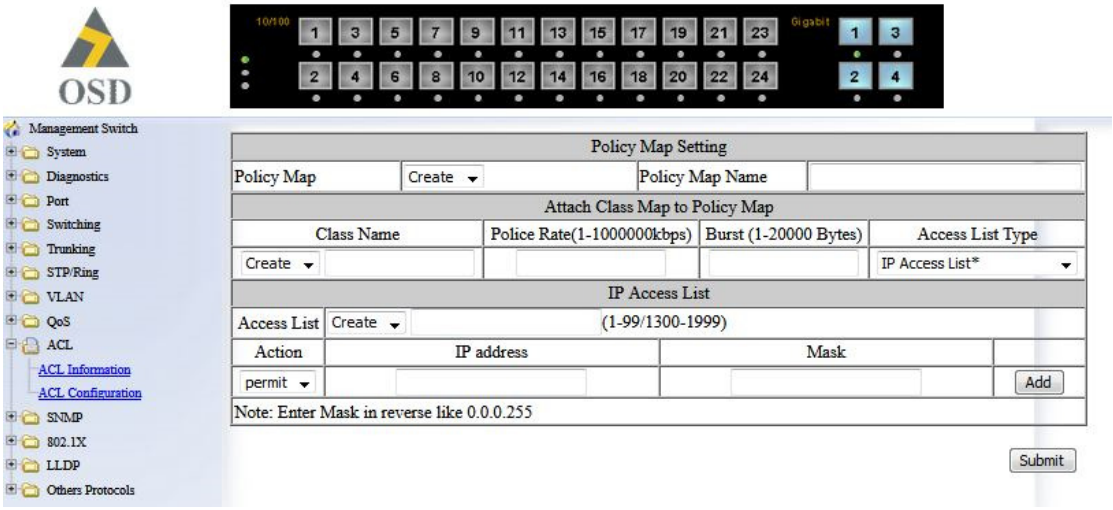
1. Priority: Click “Priority” drop-down menu from “Priority” drop-down list to choose 0 ~ 3 for DSCP Priority 0 ~ 63.
2. Submit: Click “Submit” button when you finished DSCP.

## 6.11 ACL




**ACL INFORMATION**

1. Interface: Click “Interface” drop-down menu from “Interface” drop-down list to choose port.
2. Policy Map: Choose Policy Map




**ACL CONFIGURATION**

Policy Map Setting:

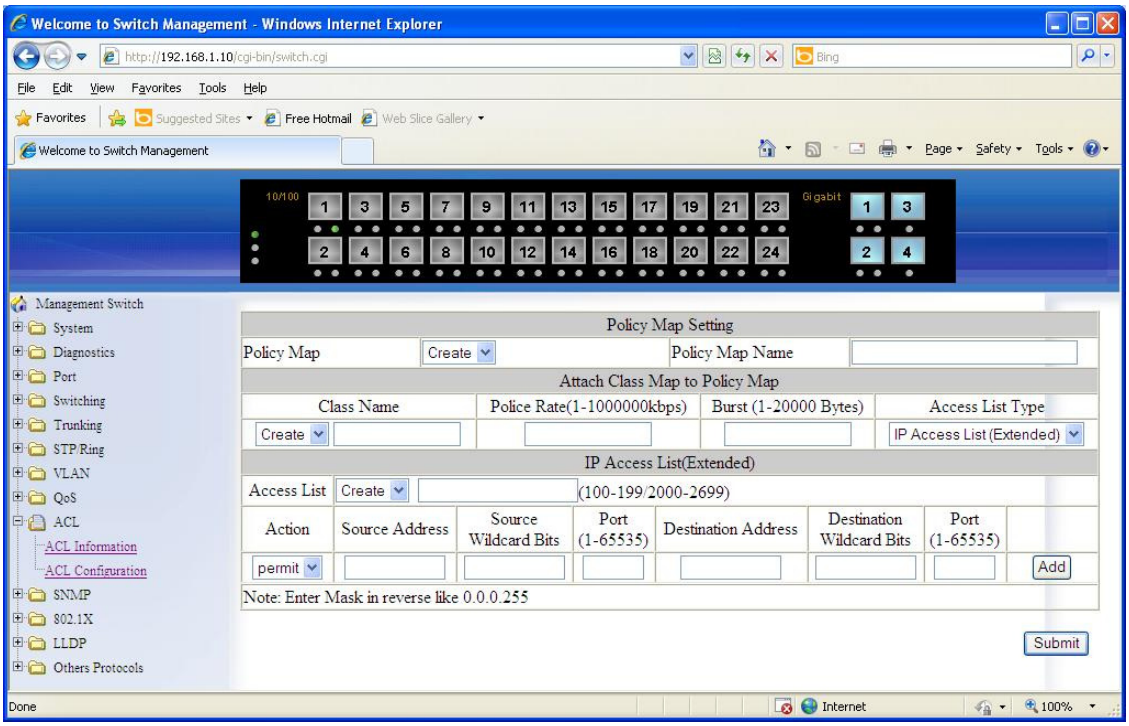
1. Policy Map: Click "Policy Map" drop-down menu to choose "Create" or "Policy Map Name" from the "Policy Map" drop-down list to create new Policy Map or modify a Policy Map.
2. Policy Map Name: Click in the "Policy Map Name" textbox and specify a Policy Map Name.

Attach Class Map to Policy Map:

1. Class Name: Click "Class Name" drop-down menu to choose "Create" or "Class Name" from the "Class Name" drop-down list to create new Class Name or modify a Class Name.
2. Police Rate (1-1000000kbps): Click in the "Police Rate" textbox and specify an average traffic rate (kbps).
3. Burst (1-20000 Bytes): Click in the "Burst" textbox and specify a normal burst size (bytes).

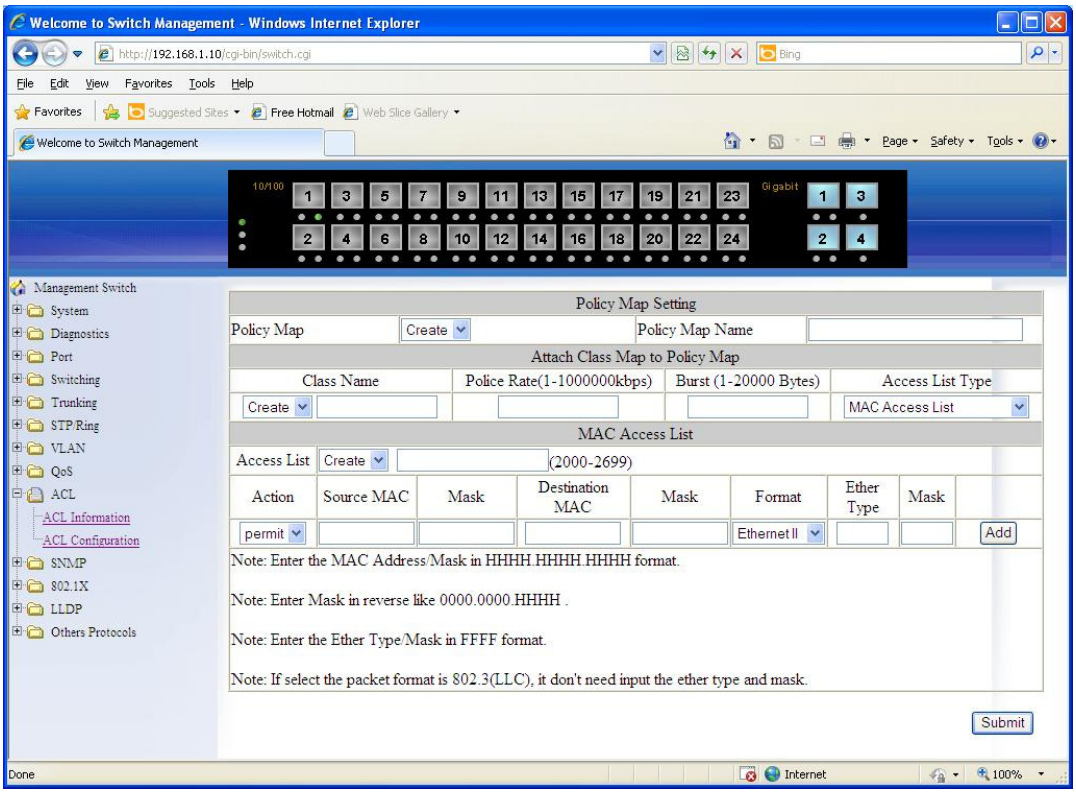
IP Access List:

1. Access List Type: Click "Access List Type" drop-down menu to choose "IP Access List" from the "Access List Type" drop-down list to create new IP Access List or modify an IP Access List.
2. Access List: Click "Access List" drop-down menu to choose "Create" or "Access List" from the "Access List" drop-down list to create new Access List or modify an Access List.
3. Access List (1-99/1300-1999): Click in the "Access List (1-99/1300-1999)" textbox and specify an IP Access List number 1 ~ 99 or 1300 ~ 1999 for Access List.
4. Action: Click "Action" drop-down menu from "Action" drop-down list to choose "permit" or "deny" to permit or deny certain traffic if conditions matched.
5. IP address: Click in the "IP address" textbox and specify the IP address of originating network or host sending packet.
6. Mask: Click in the "Mask" textbox and specify the Wildcard bits in dotted decimal notation to apply to the source. Ones go in bit positions to ignore.
   Example: IP address: 192.168.1.10. Mask: 0.0.0.3. Then IP address 192.168.1.8 ~ 192.168.1.11 would be permitted or denied.
7. Add: Click "Add" button to add IP Access List number.
8. Submit: Click "Submit" button when you finished ACL Configuration settings.



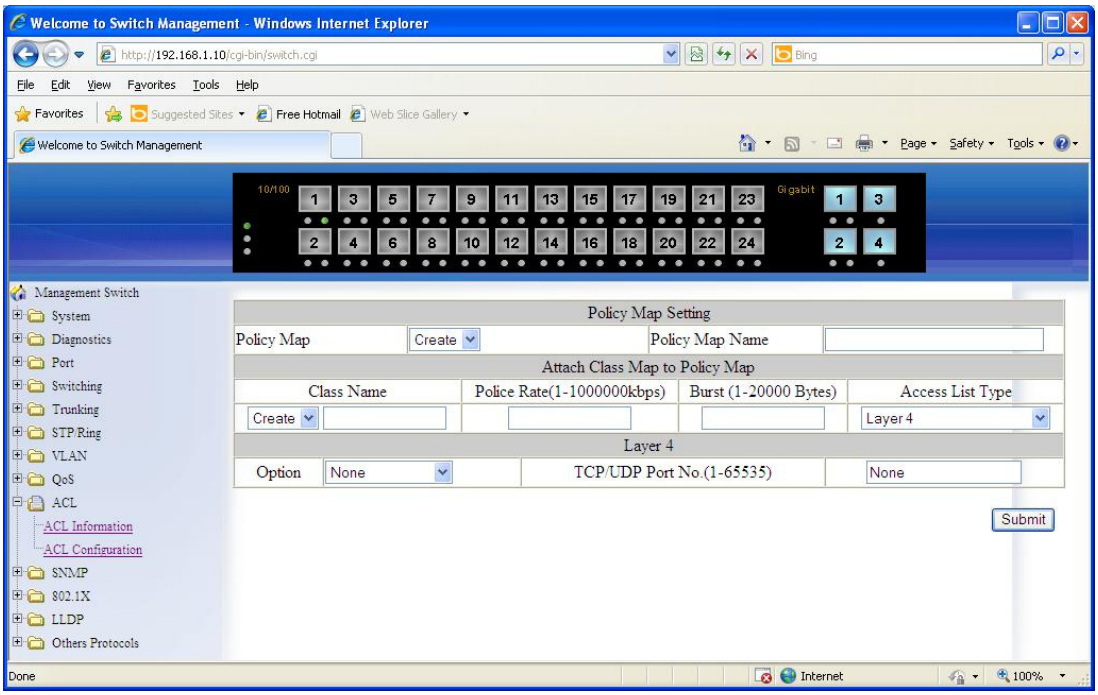

IP Access List (Extended):

1. Access List Type: Click "Access List Type" drop-down menu to choose "IP Access List (Extended)" from the "Access List Type" drop-down list to create new IP Access List (Extended) or modify an IP Access List (Extended).
2. Access List: Click "Access List" drop-down menu to choose "Create" or "Access List" from the "Access List" drop-down list to create new Access List or modify an Access List.
3. Access List (100-199/2000-2699): Click in the "Access List (100-199/2000-2699)" textbox and specify an IP Access List (Extended) number 100 ~ 199 or 2000 ~ 2699 for Access List.
4. Action: Click "Action" drop-down menu from "Action" drop-down list to choose "permit" or "deny" to permit or deny certain traffic if conditions matched.
5. Source Address: Click in the "Source Address" textbox and specify the IP address of originating network or host sending packet.
6. Source Wildcard Bits: Click in the "Source Wildcard Bits" textbox and specify the Wildcard bits in dotted decimal notation to apply to the source. Ones go in bit positions to ignore.
   Example: Source Address: 192.168.1.10. Source Wildcard Bits: 0.0.0.3. Then Source IP address 192.168.1.8 ~ 192.168.1.11 would be permitted or denied.
7. Port (1-65535): Click in the "Port (1-65535)" textbox and specify a TCP/UDP Port number 1 ~ 65535 for Access List.
8. Destination Address: Click in the "Destination Address" textbox and specify the IP address of host receiving packet.
9. Destination Wildcard Bits: Click in the "Destination Wildcard Bits" textbox and specify the Wildcard bits in dotted decimal notation to apply to the destination. Ones go in bit positions to ignore.
   Example: Destination Address: 192.168.1.20. Destination Wildcard Bits: 0.0.0.255. Then Destination IP address 192.168.1.0 ~ 192.168.1.255 would be permitted or denied.
10. Port (1-65535): Click in the "Port (1-65535)" textbox and specify a TCP/UDP Port number 1 ~ 65535 for Access List.
11. Add: Click "Add" button to add IP Access List (Extended) number.
12. Submit: Click "Submit" button when you finished ACL Configuration settings.




MAC Access List:

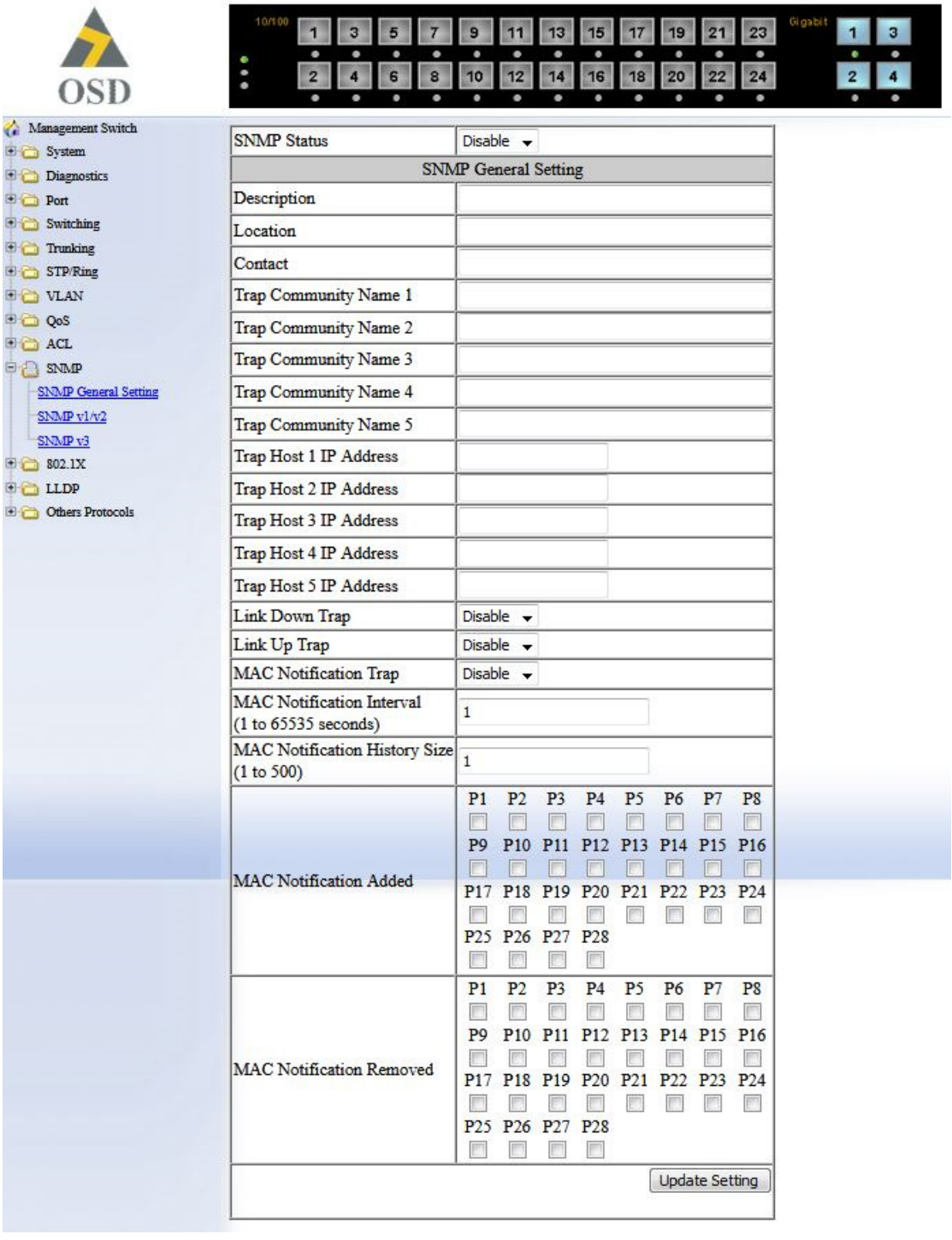
1. Access List Type: Click “Access List Type” drop-down menu to choose “MAC Access List” from the “Access List Type” drop-down list to create new MAC Access List or modify a MAC Access List.
2. Access List: Click “Access List” drop-down menu to choose “Create” or “Access List” from the “Access List” drop-down list to create new Access List or modify an Access List.
3. Access List (2000-2699): Click in the “Access List (2000-2699)” textbox and specify a MAC Access List number 2000 ~ 2699 for Access List.
4. Action: Click “Action” drop-down menu from “Action” drop-down list to choose “permit” or “deny” to permit or deny certain traffic if conditions matched.
5. Source MAC: Click in the “Source MAC” textbox and specify the MAC address of originating network or host sending packet.
6. Mask: Click in the “Mask” textbox and specify the Wildcard bits in dotted decimal notation to apply to the source. Ones go in bit positions to ignore.
   Example: MAC Address: 001a.4d9f.ab89. Mask: 0.0.ff. Then MAC address 001a.4d9f.ab00 ~ 001a.4d9f.abff would be permitted or denied.
7. Destination MAC: Click in the “Destination MAC” textbox and specify the MAC address of host receiving packet.
8. Mask: Click in the “Mask” textbox and specify the Wildcard bits in dotted decimal notation to apply to the destination. Ones go in bit positions to ignore.
   Example: Destination Address: 001b.4c94.4567. Mask: 0.0.eff. Then MAC address 001b.4c94.4000 ~ 001b.4c94.4eff would be permitted or denied.
9. Format: Click “Format” drop-down menu to choose “Ethernet II”, “SNAP”, “802.3”, or “LLC” from the “Format” drop-down list.
10. Ether type: Click in the “Ether type” textbox and specify the Ether type for packet.
11. Mask: Click in the “Mask” textbox and specify the Wildcard bits to apply to the Ether type.
12. Add: Click “Add” button to add MAC Access List number.
13. Submit: Click “Submit” button when you finished ACL Configuration settings.




Layer 4:

1. Access List Type: Click “Access List Type” drop-down menu to choose “Layer 4” from the “Access List Type” drop-down list to create new Layer 4 Access List or modify Layer 4 Access List.
2. Option: Click “Option” drop-down menu from “Option” drop-down list to choose “Source port” or “Destination port”.
3. TCP/UDP Port No. (1-65535): Click in the “TCP/UDP Port No. (1-65535)” textbox and specify a TCP/UDP Port number 1 ~ 65535 for Access List.
4. Submit: Click “Submit” button when you finished ACL Configuration settings.

## 6.12 SNMP

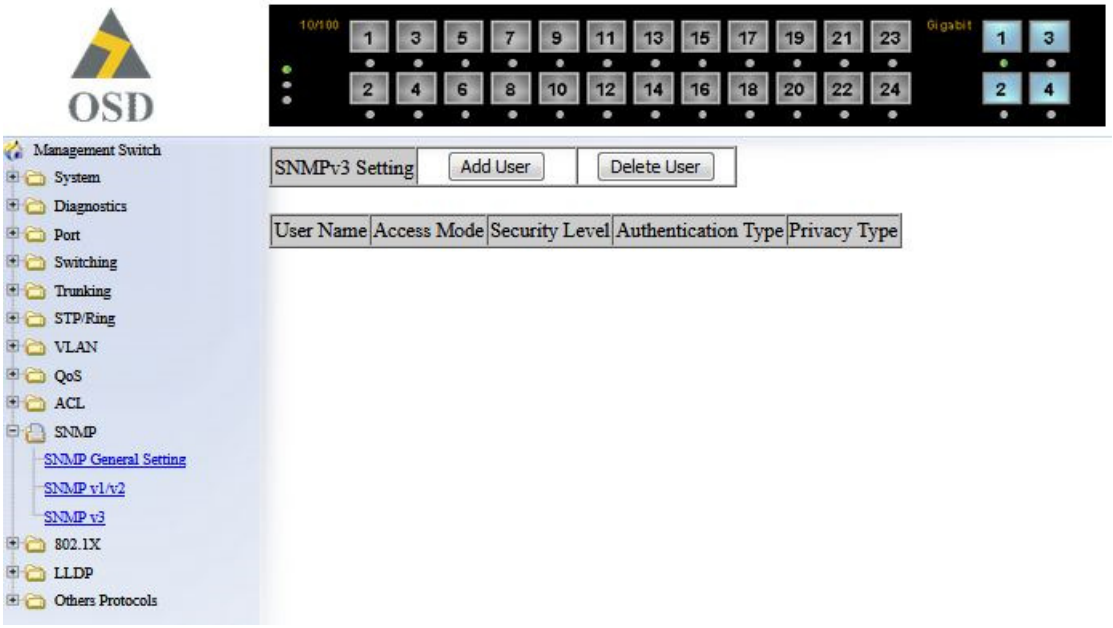

OSD
10/100
1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24
Gigabit
1 3
2 4
Management Switch
System
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
ACL
SNMP
SNMP General Setting
SNMP v1/v2
SNMP v3
802.1X
LLDP
Others Protocols
SNMP Status
Disable
SNMP General Setting
Description
Location
Contact
Trap Community Name 1
Trap Community Name 2
Trap Community Name 3
Trap Community Name 4
Trap Community Name 5
Trap Host 1 IP Address
Trap Host 2 IP Address
Trap Host 3 IP Address
Trap Host 4 IP Address
Trap Host 5 IP Address
Link Down Trap
Disable
Link Up Trap
Disable
MAC Notification Trap
Disable
MAC Notification Interval (1 to 65535 seconds)
1
MAC Notification History Size (1 to 500)
1
MAC Notification Added
P1 P2 P3 P4 P5 P6 P7 P8
P9 P10 P11 P12 P13 P14 P15 P16
P17 P18 P19 P20 P21 P22 P23 P24
P25 P26 P27 P28
MAC Notification Removed
P1 P2 P3 P4 P5 P6 P7 P8
P9 P10 P11 P12 P13 P14 P15 P16
P17 P18 P19 P20 P21 P22 P23 P24
P25 P26 P27 P28
Update Setting

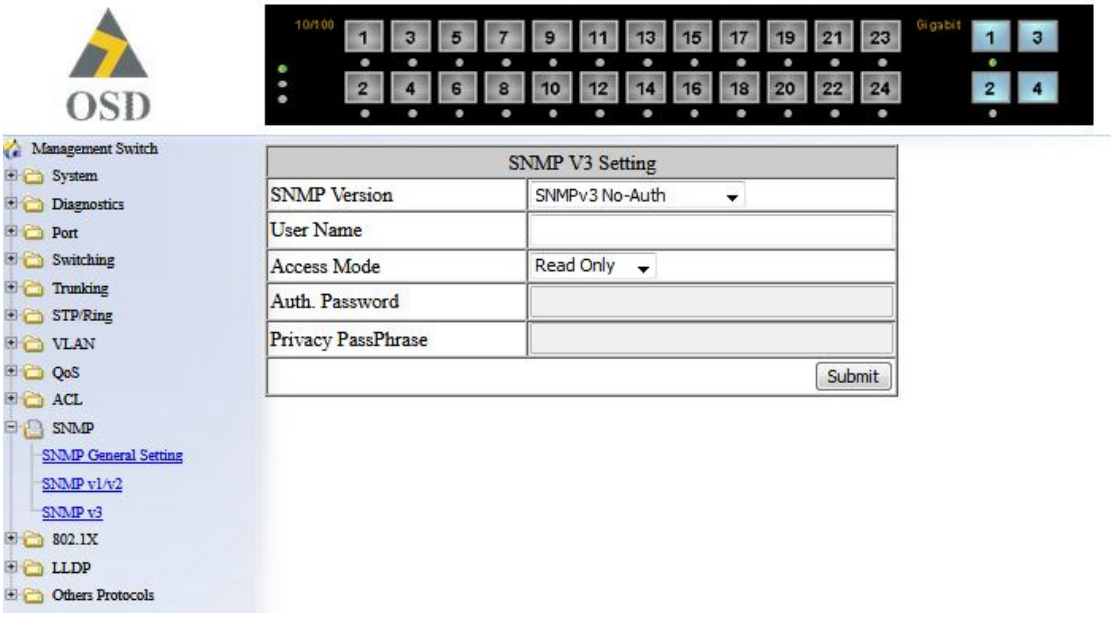
**SNMP GENERAL SETTING**

1. SNMP Status: Click “SNMP Status” drop-down menu from “SNMP Status” drop-down list to choose “Enable” or “Disable” to enable or disable SNMP.
2. Description: Click in the “Description” textbox and specify a new description for SNMP.
3. Location: Click in the “Location” textbox and specify a new location for SNMP.
4. Contact: Click in the “Contact” textbox and specify a new contact for SNMP.
5. Trap Community Name: For each “Trap Community Name”, Click in the “Trap Community Name” textbox and specify a trap community name.
6. Trap Host IP Address: For each “Trap Host IP Address”, Click in the “Trap Host IP Address” textbox and specify a trap host IP address.
7. Link Down Trap: Click “Link Down Trap” drop-down menu from “Link Down Trap” drop-down list to choose “Enable” or “Disable” to enable or disable link down trap.
8. Link Up Trap: Click “Link Up Trap” drop-down menu from “Link Up Trap” drop-down list to choose “Enable” or “Disable” to enable or disable link up trap.
9. MAC Notification Trap: Click “MAC Notification Trap” drop-down menu from “MAC Notification Trap” drop-down list to choose “Disable” or “Enable” to disable or enable the Switch to send MAC Notification Trap to the network management system (NMS).
10. MAC Notification Interval (1 to 65535 seconds): Click the text box and type a decimal number to configure the MAC notification interval in seconds. The range is 1 to 65535 seconds. The switch sends the MAC Notification Trap when this amount of time has elapsed.
11. MAC Notification History Size (1 to 500): Click the text box and type a decimal number to configure the maximum number of entries in the MAC notification history table. The range is 1 to 500.
12. MAC Notification Added: Click and choose the port to enable MAC Notification Trap on an interface port.
13. MAC Notification Removed: Click and choose the port to disable MAC Notification Trap on an interface port.
14. Update Setting: Click “Update Setting” button when you finished SNMP General Setting.


**SNMP V1/V2C**

1. Get Community Name: Click in the “Get Community Name” textbox and specify a get community name.
2. Set Community Name: Click in the “Set Community Name” textbox and specify a set community name.
3. Update Setting: Click “Update Setting” button when you finished SNMP V1/V2c Setting.



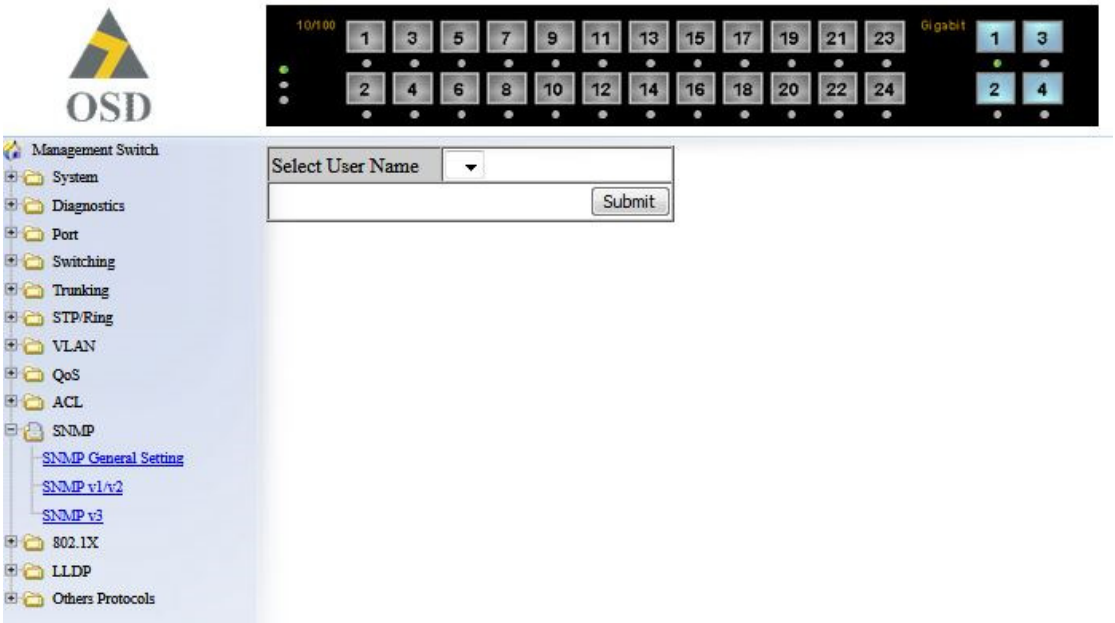

**SNMP V3**

Add User:

1. Add User: Click “Add User” button. The “SNMP V3 Setting” window appears.
2. SNMP Version: Click “SNMP Version” drop-down menu from “SNMP Version” drop-down list to choose “SNMPv3 No-Auth”, “SNMPv3 Auth-MD5”, “SNMPv3 Auth-SHA”, “SNMPv3 Priv Auth-MD5”, or “SNMPv3 Priv Auth-SHA”.
   - SNMPv3 No-Auth: Add a user using SNMP v3 without authentication.
   - SNMPv3 Auth-MD5: Add a user using SNMP v3 with authentication. Click in the “Auth. Password” textbox and specify an authentication password.
   - SNMPv3 Auth-SHA: Add a user using SNMP v3 with authentication. Click in the “Auth.

Password" textbox and specify an authentication password.
- SNMPv3 Priv Auth-MD5: Add a user using SNMP v3 with authentication and privacy. Click in the "Auth. Password" textbox and specify an authentication password. Click in the "Privacy PassPhrase" textbox and specify a privacy pass phrase.
- SNMPv3 Priv Auth-SHA: Add a user using SNMP v3 with authentication and privacy. Click in the "Auth. Password" textbox and specify an authentication password. Click in the "Privacy PassPhrase" textbox and specify a privacy pass phrase.

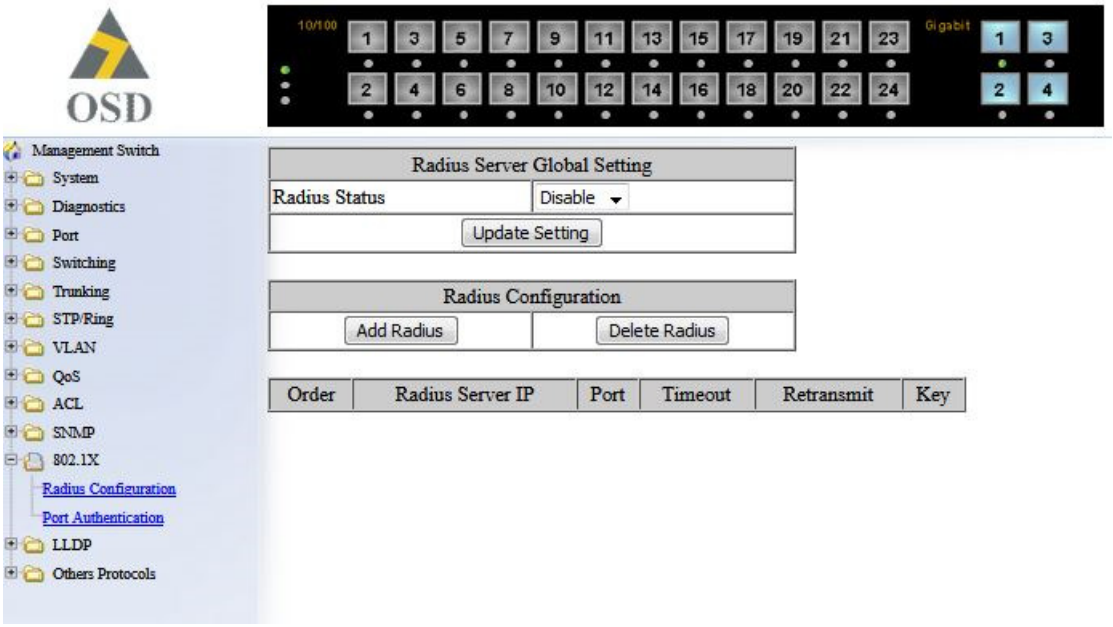
3. User Name: Click in the "User Name" textbox and specify a user name for user using SNMP v3.
4. Access Mode: Click "Access Mode" drop-down menu from "Access Mode" drop-down list to choose "Read Only" or "Read/Write".
   - Read Only: Add a user using SNMP v3 with read-only access mode.
   - Read/Write: Add an user using SNMP v3 with read-write access mode
5. Submit: Click "Submit" button when you finished SNMP V3 Setting.




Delete User:

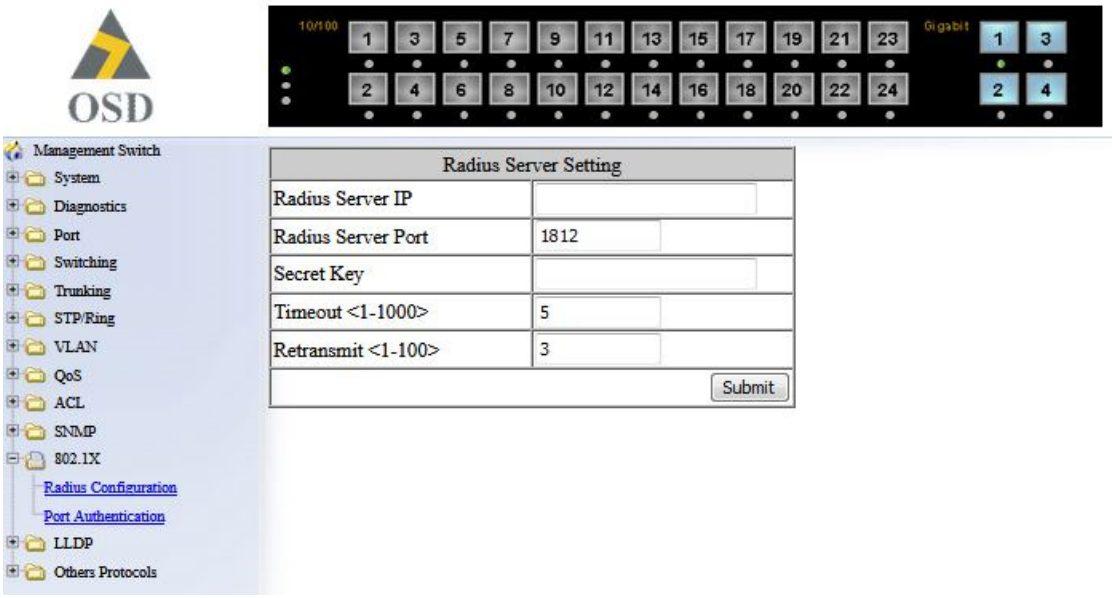
1. Delete User: Click "Delete User" button. The "Select User Name" window appears.
2. Select User Name: Click "Select User Name" drop-down menu from "Select User Name" drop-down list to choose the user to be deleted from using SNMP v3.
3. Submit: Click "Submit" button when you finished user deletion.

## 6.13 802.1X



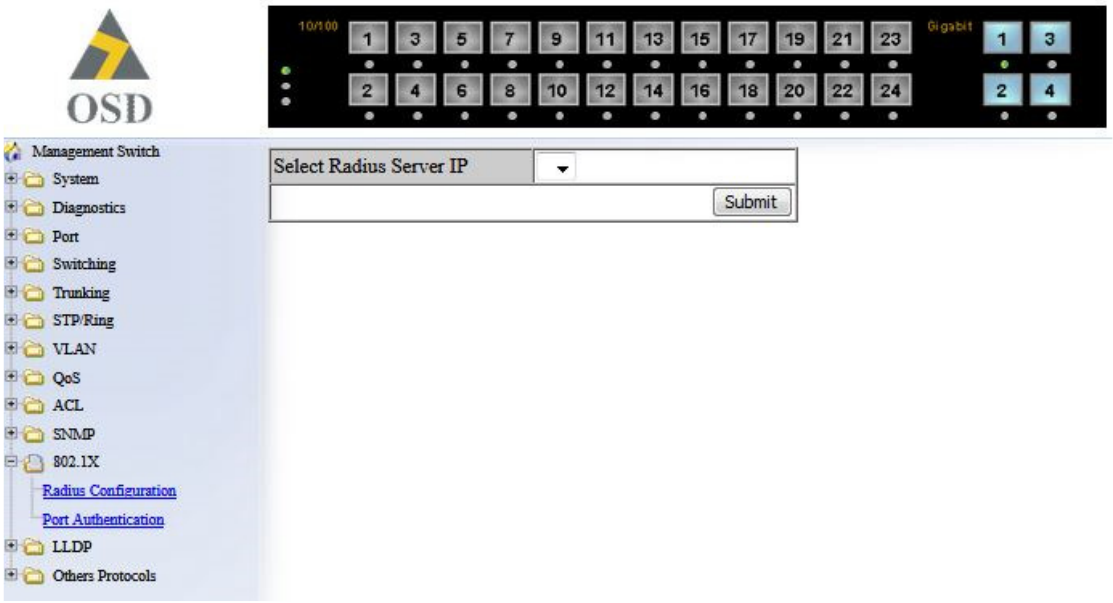

**RADIUS CONFIGURATION**

1. Radius Status: Click “Radius Status” drop-down menu from “Radius Status” drop-down list to choose “Enable” or “Disable” to globally enable or disable authentication.
2. Update Setting: Click “Update Setting” button when you finished Radius Status Setting.



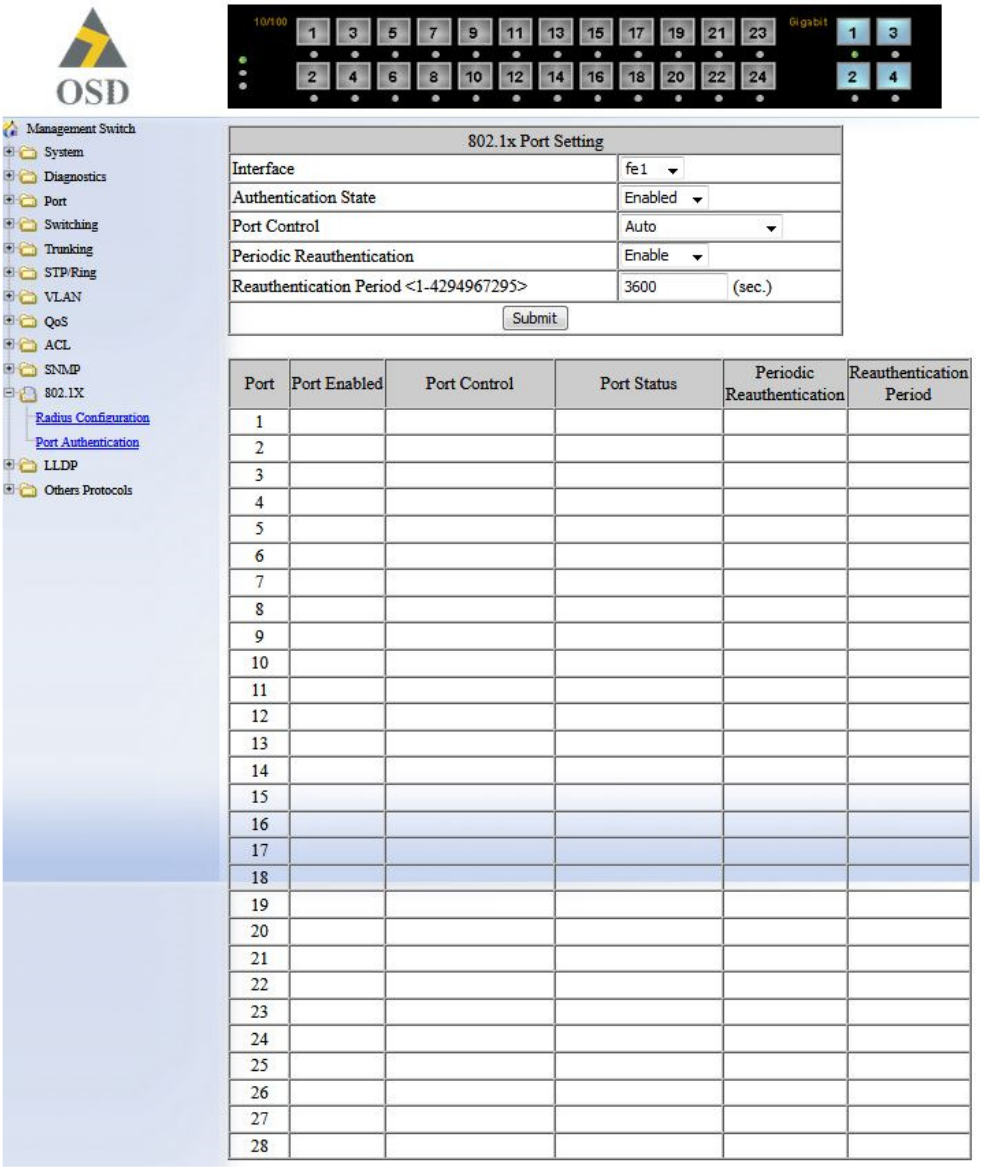

Add Radius:

1. Add Radius: Click “Add Radius” button. The “Radius Server Setting” window appears.
2. Radius Server IP: Click in the “Radius Server IP” textbox and specify the IP address of the remote radius server host.
3. Radius Server Port: Click in the “Radius Server Port” textbox and specify the UDP destination port for authentication requests. The host is not used for authentication if set to 0.
4. Secret Key: Click in the “Secret Key” textbox and specify the authentication and encryption key for all radius communications between the Switch and radius server. This key must match the encryption used on the radius daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If spaces are used in the key, do not enclose the key in quotaion marks unless the quotation marks themselves are part of the key.
5. Timeout <1-1000>: Click in the “Timeout” textbox and specify the time interval (in seconds) that the Switch waits for the radius server to reply before retransmitting. Enter a value in the range 1 to 1000.
6. Retransmit <1-100>: Click in the “Retransmit” textbox and specify the number of times a radius request is resent to a server if that server is not responding or responding slowly. Enter a value in the range 1 to 100.
7. Submit: Click “Submit” button when you finished Radius Server Setting.




Delete Radius:

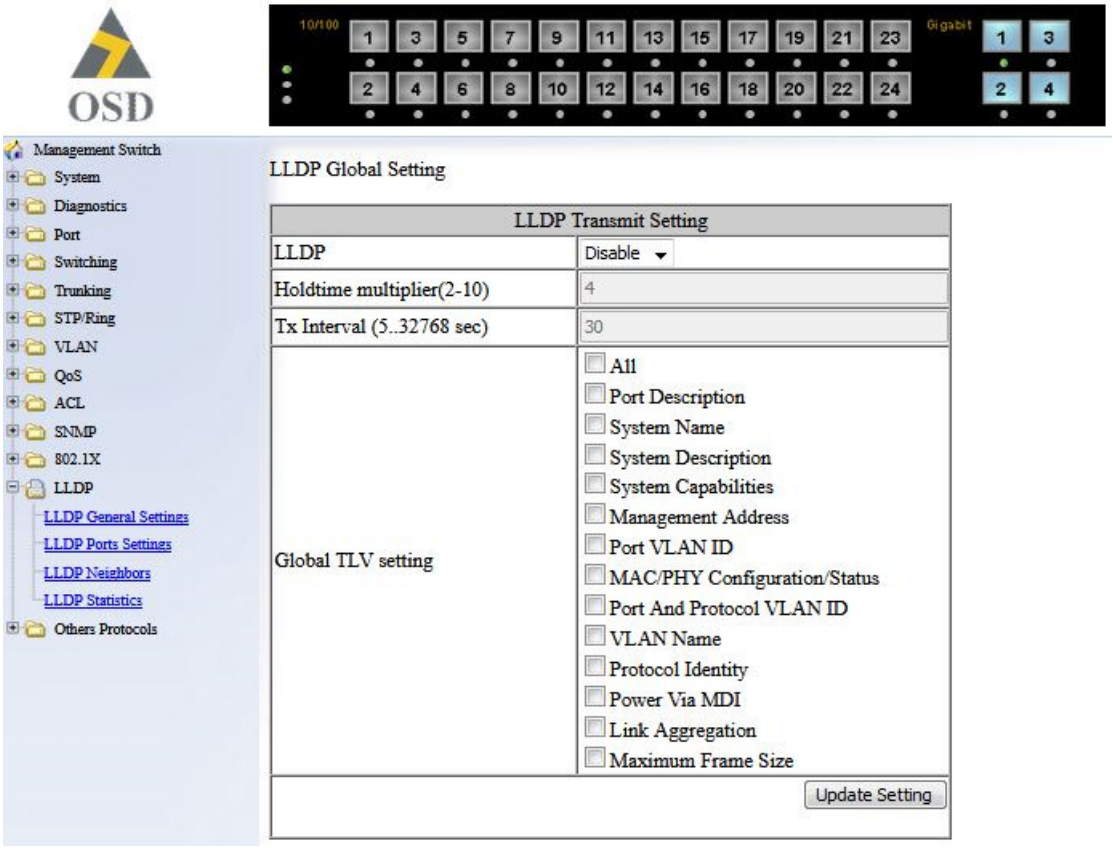
1. Delete Radius: Click “Delete Radius” button. The “Select Radius Server IP” window appears.
2. Select Radius Server IP: Click “Select Radius Server IP” drop-down menu from “Select Radius Server IP” drop-down list to choose the IP address of the remote radius server host to be deleted.
3. Submit: Click “Submit” button when you finished radius server deletion.




**PORT-BASED AUTHENTICATION**

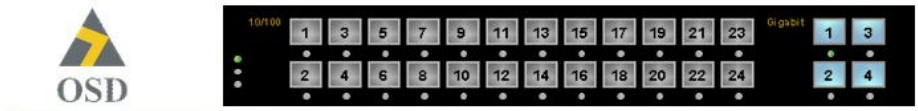
1. Interface: Click “Interface” drop-down menu from “Interface” drop-down list to choose the port to be set port-based authentication.
2. Authentication State: Click “Authentication State” drop-down menu from “Authentication State” drop-down list to choose “Enable” or “Disable” to enable or disable authentication state.
3. Port Control: Click “Port Control” drop-down menu from “Port Control” drop-down list to choose “Auto”, “Force Authorized”, or “Force Unauthorized” to force a port state. “Auto” specifies to enable authentication on port. “Force Authorized” specifies to force a port to always be in an authorized state. “Force Unauthorized” specifies to force a port to always be in an unauthorized state.
4. Periodic Reauthentication: Click “Periodic Reauthentication” drop-down menu from “Periodic Reauthentication” drop-down list to choose “Enable” or “Disable” to enable or disable periodic reauthentication.
5. Reauthentication Period <1-4294967295>: Click in the “Reauthentication Period” textbox and specify the seconds between reauthorization attempts. The default time is 3600 seconds.
6. Update Setting: Click “Update Setting” button when you finished port-based authentication setting.

## 6.14 LLDP




**LLDP GENERAL SETTINGS**

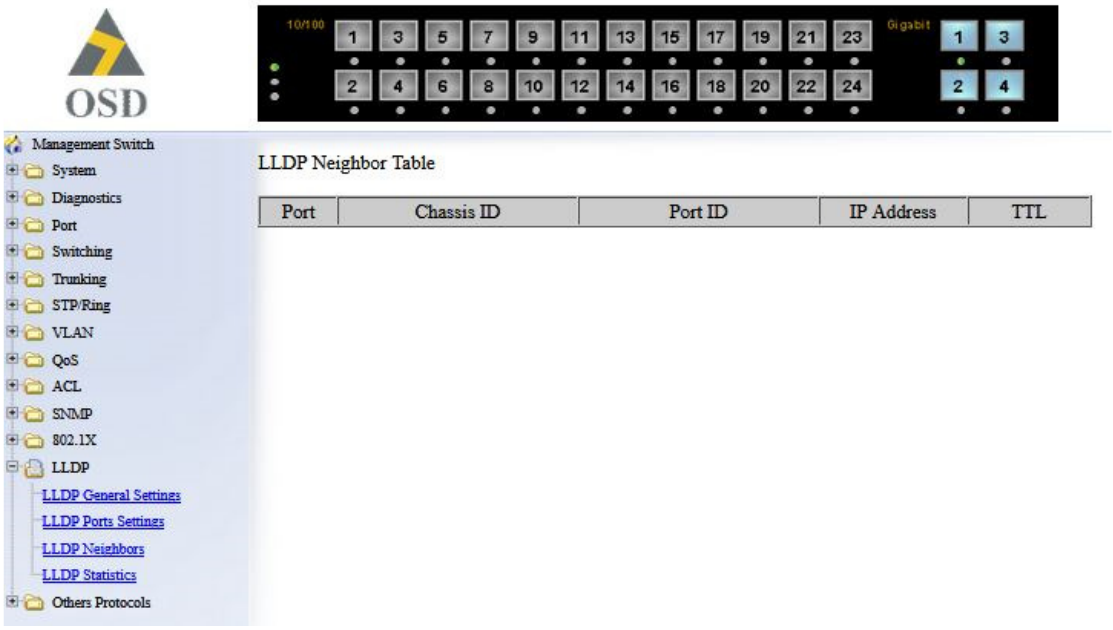
1. LLDP: Click "LLDP" drop-down menu from "LLDP" drop-down list to choose "Enable" or "Disable" to enable or disable Link Layer Discovery Protocol (LLDP) globally.
2. Holdtime multiplier(2-10): Click in the "Holdtime multiplier" textbox and set the Link Layer Discovery Protocol (LLDP) holdtime multiplier value. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) that the switch advertises to the neighbors. Enter a Holdtime multiplier value in the range from 2 to 10. Default is 4.
3. Tx Interval (5-32768 seconds): Click in the "Tx Interval" textbox and set the transmit interval. This is the interval between regular transmissions of Link Layer Discovery Protocol (LLDP) advertisements. Enter a Tx Interval value in the range from 5 to 32768. Default is 30 seconds.
4. Global TLV setting: Click and choose Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) setting.
5. Update Setting: Click "Update Setting" button when you finished LLDP General Settings.





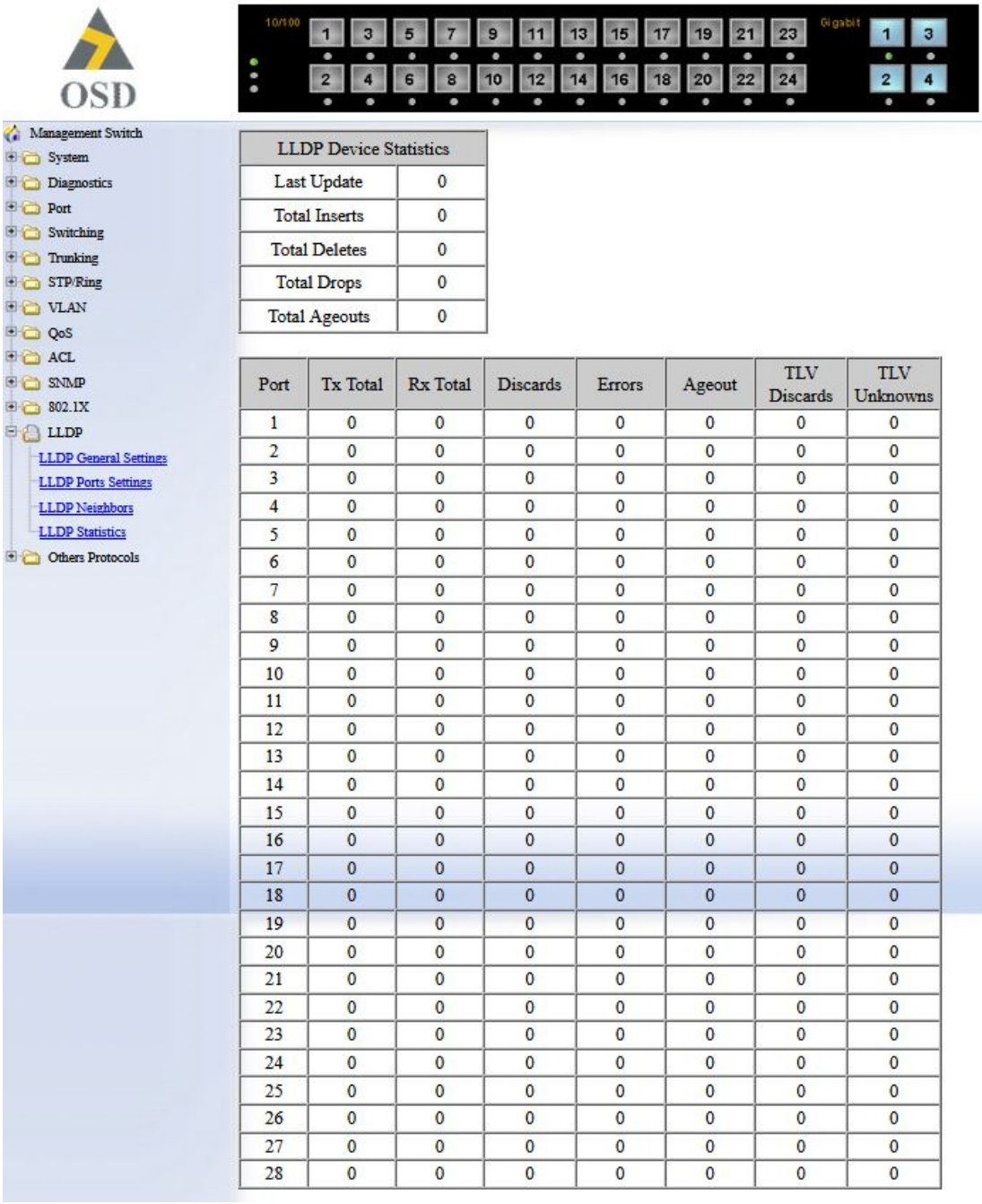
**LLDP PORT SETTINGS**

1. Transmit: Click “Transmit” drop-down menu from “Transmit” drop-down list to choose “Disable” or “Enable” to disallow or allow sending Link Layer Discovery Protocol (LLDP) packets on the interface.
2. Receive: Click “Receive” drop-down menu from “Receive” drop-down list to choose “Disable” or “Enable” to disallow or allow receiving Link Layer Discovery Protocol (LLDP) packets on the interface.
3. Notify: Click “Notify” drop-down menu from “Notify” drop-down list to choose “Disable” or “Enable” to disable or enable Link Layer Discovery Protocol (LLDP) notification on the interface.
4. TLVs: Click and choose Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) setting on the interface.
5. Submit: Click “Submit” button when you finished LLDP Ports Settings.




**LLDP NEIGHBOURS**

Click **LLDP Neighbors** to show Link Layer Discovery Protocol (LLDP) neighbors information.



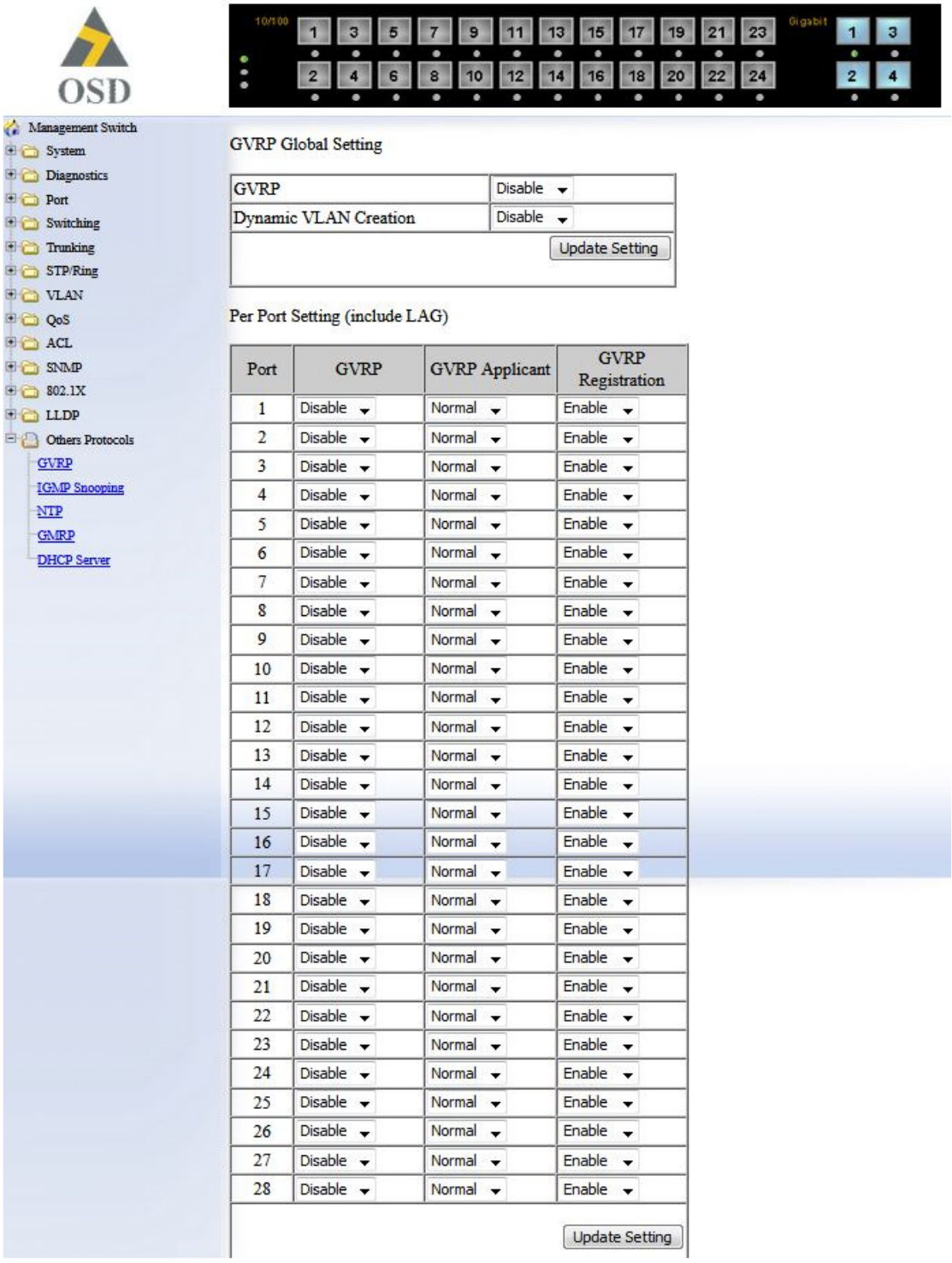

| LLDP Device Statistics | |
|---|---|
| Last Update | 0 |
| Total Inserts | 0 |
| Total Deletes | 0 |
| Total Drops | 0 |
| Total Ageouts | 0 |

| Port | Tx Total | Rx Total | Discards | Errors | Ageout | TLV Discards | TLV Unknowns |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 13 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 14 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 17 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 18 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 19 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 20 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 21 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 22 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 23 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 24 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 25 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 26 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 27 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 28 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**LLDP STATISTICS**

Click **LLDP Statistics** to show Link Layer Discovery Protocol (LLDP) statistics.

## 6.15 OTHER PTOTOCOLS



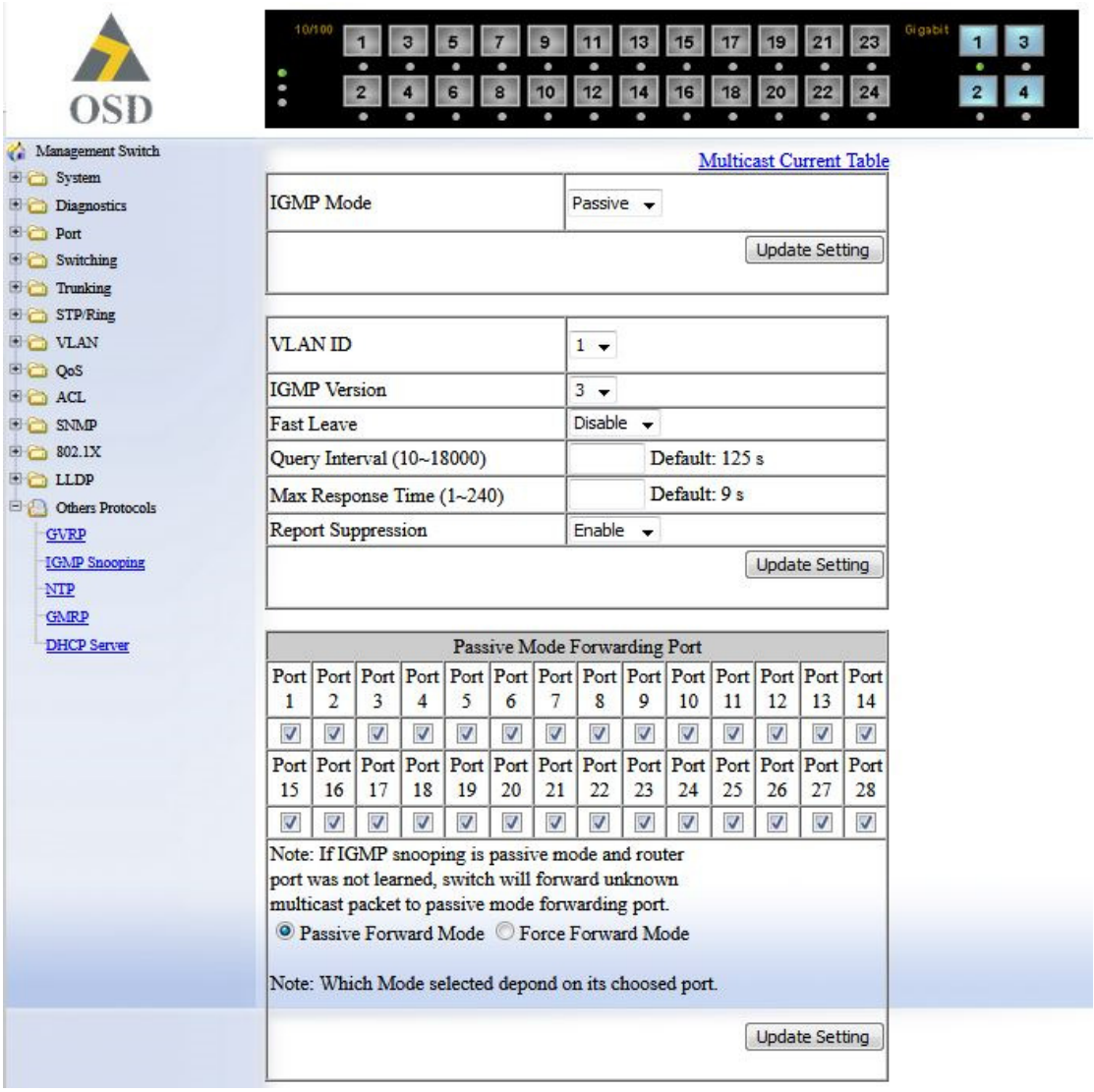
**GVRP**

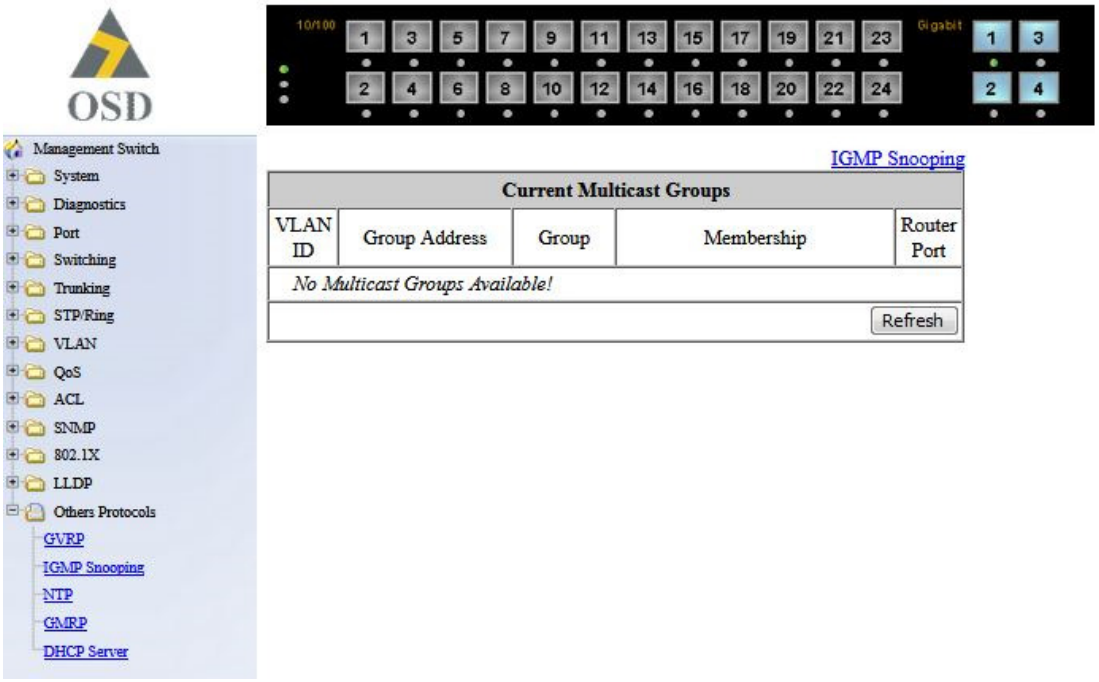
GVRP Global Setting:

1. GVRP: Click “GVRP” drop-down menu from “GVRP” drop-down list to choose “Enable” or “Disable” to enable or disable GVRP (GARP VLAN Registration Protocol).
2. Dynamic VLAN Creation: Click “Dynamic VLAN Creation” drop-down menu from “Dynamic VLAN Creation” drop-down list to choose “Enable” or “Disable” to enable or disable Dynamic VLAN Creation. GARP (Generic Attribute Registration Protocol) provides IEEE802.1Q compliant VLAN pruning and dynamic VLAN creation on IEEE802.1Q trunk ports.
3. Update Setting: Click “Update Setting” button when you finished GVRP Global Setting.

Per Port Setting (include LAG):

1. GVRP: Click “GVRP” drop-down menu from “GVRP” drop-down list to choose “Enable” or “Disable” to enable or disable GVRP for the port.
2. GVRP Applicant: Click “GVRP Applicant” drop-down menu from “GVRP Applicant” drop-down list to choose “Active” or “Normal” to the port. Ports in the GVRP active applicant state send GVRP VLAN declarations when they are in the STP (Spanning Tree Protocol) blocking state, which prevents the STP bridge protocol data units (BPDUs) from being pruned from the other port. Ports in the GVRP normal applicant state do not declare GVRP VLANs when in the STP blocking state.
3. GVRP Registration: Click “GVRP Registration” drop-down menu from “GVRP Registration” drop-down list to choose “Enable” or “Disable” to enable or disable GVRP Registration to the port. Configuring an IEEE802.1Q trunk port in registration mode allows dynamic creation (if dynamic VLAN creation is enabled), registration, and deregistration of VLANs on the trunk port.
4. Update Setting: Click “Update Setting” button when you finished Per Port Setting.


OSD
10/100
1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24
Gigabit
1 3
2 4
Management Switch
System
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
ACL
SNMP
802.1X
LLDP
Others Protocols
GVRP
IGMP Snooping
NTP
GMRP
DHCP Server
Multicast Current Table
IGMP Mode
Passive
Update Setting
VLAN ID
1
IGMP Version
3
Fast Leave
Disable
Query Interval (10~18000)
Default: 125 s
Max Response Time (1~240)
Default: 9 s
Report Suppression
Enable
Update Setting
Passive Mode Forwarding Port
Port 1 Port 2 Port 3 Port 4 Port 5 Port 6 Port 7 Port 8 Port 9 Port 10 Port 11 Port 12 Port 13 Port 14
Port 15 Port 16 Port 17 Port 18 Port 19 Port 20 Port 21 Port 22 Port 23 Port 24 Port 25 Port 26 Port 27 Port 28
Note: If IGMP snooping is passive mode and router port was not learned, switch will forward unknown multicast packet to passive mode forwarding port.
Passive Forward Mode
Force Forward Mode
Note: Which Mode selected depond on its choosed port.
Update Setting




**IGMP SNOOPING**

IGMP Snooping:

1. Click on "IGMP Snooping" to change to IGMP Snooping windows.
2. IGMP Mode: Click "IGMP Mode" drop-down menu from "IGMP Mode" drop-down list to choose "Disable", "Passive", or "querier" for the switch. Disable: Disable IGMP on the switch. Passive: The switch with only multicast-data-forwarding capability. Querier: The switch acts as the querier for the network. There is only one querier on a network at any time.
3. Update Setting: Click "Update Setting" button when you finished IGMP Mode settings.
4. VLAN ID: Click "VLAN ID" drop-down menu from "VLAN ID" drop-down list to choose the VLAN under configuration for the switch.
5. IGMP Version: Click "IGMP Version" drop-down menu from "IGMP Version" drop-down list to choose "1", "2", or "3" for the switch.
6. Fast Leave: Click "Fast Leave" drop-down menu from "Fast Leave" drop-down list to choose "Enable" or "Disable" for the switch. Enable this function will allow members of a multicast group to leave the group immediately when an IGMP Leave Report Packet is received by the Switch.

IGMP Querier:

1. Query Interval (1~18000): Click in the "Query Interval" textbox and specify a new number from 1 ~ 18000. The Query Interval field is used to set the time (in seconds) between transmitting IGMP queries. Entries between 1 and 18000 seconds are allowed. Default = 125.
2. Max Response Time (1~240): Click in the "Max Response Time" textbox and specify a new number from 1 ~ 240. This determines the maximum amount of time in seconds allowed before sending an IGMP response report. The Max Response Time field allows an entry between 1 and 240 (seconds). Default = 10.

IGMP Passive Snooping:

1. Report Suppression: Click "Report Suppression" drop-down menu from "Report Suppression" drop-down list to choose "Enable" or "Disable" for the switch. Use this command to enable report suppression for IGMP version 1 and version 2. Report suppression does not apply to IGMP version 3, and is turned off by default for IGMP version 1 and IGMP version 2 reports. The switch uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast

devices. When IGMP router suppression is enabled, the switch sends the first IGMP report from all hosts for a group to all the multicast routers. The switch does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

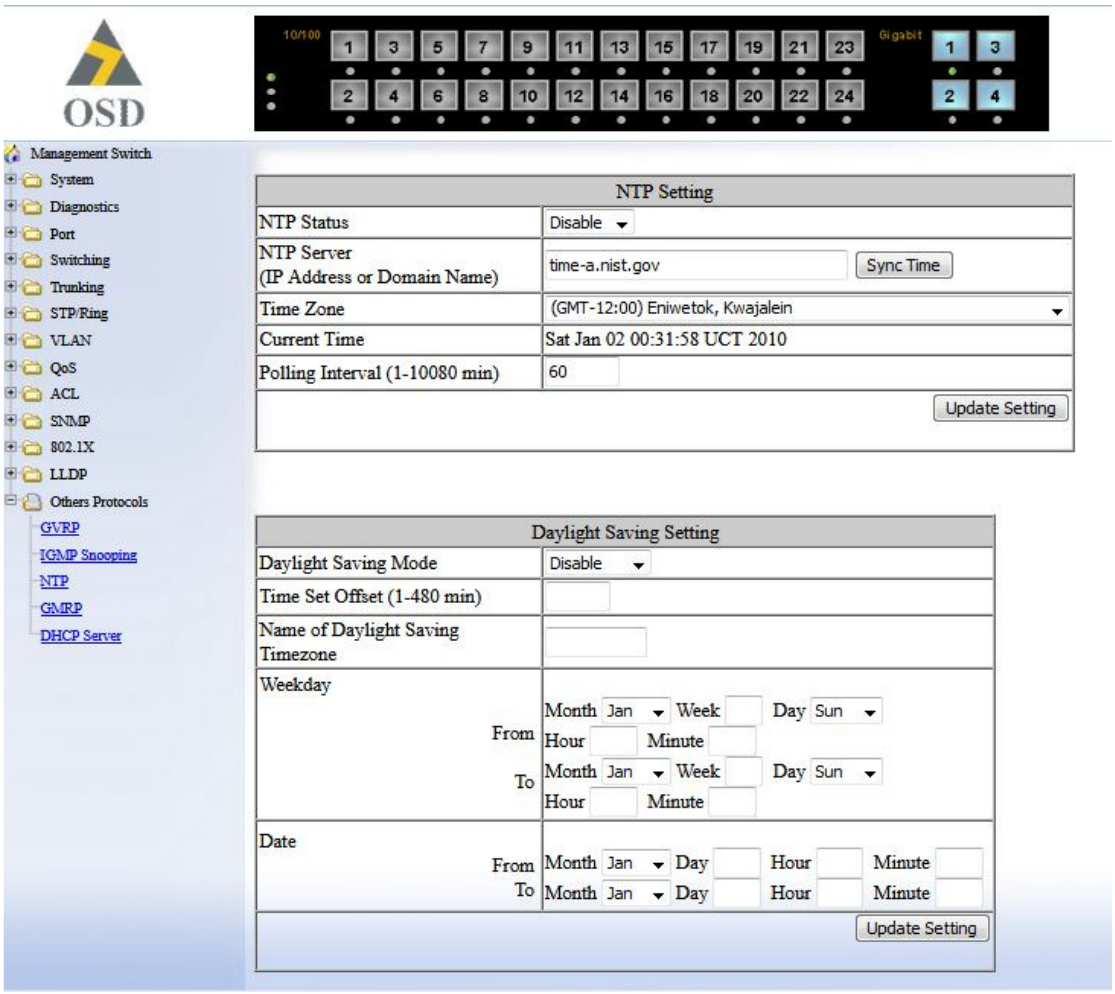
2. Update Setting: Click “Update Setting” button when you finished IGMP Snooping.

Force Forwarding Port / Passive Mode Forwarding Port:

1. Port: Choose the port to set the port as force forwarding port / passive mode forwarding port. The Switch will forward unknown multicast packets to force forwarding port / passive mode forwarding port before receiving IGMP query.
2. PassiveForwardMode / ForceForwardMode: Click and choose Passive Forward Mode or Force Forward Mode.
3. Update Setting: Click “Update Setting” button when you finished Force Forwarding Port or Passive Mode Forwarding Port setting.

Multicast Current Table:

1. Click on “Multicast Current Table” to change to Current Multicast Groups windows.
2. Refresh: Click “Refresh” button to refresh Current Multicast Groups information.




**NTP**

Adjust RTC Time:

1. Click in textbox and specify the Year, Month, Day, Hour, Minute, and Second.
2. Update Setting: Click “Update Setting” button when you finished Adjust RTC Time.

NTP Setting:

1. NTP Status: Click “NTP Status” drop-down menu from “NTP Status” drop-down list to choose “Enable” or “Disable” to enable or disable NTP for the Switch.
2. NTP Server (IP Address or Domain name): Click in the “NTP Server” textbox and specify the IP address or Domain name of NTP server.
3. Sync Time: Click “Sync Time” button to synchronize time with NTP server.
4. Time Zone: Click “Time Zone” drop-down menu from “Time Zone” drop-down list to set time zone.
5. Polling Interval (1-10080 min): Click in the “Polling Interval” textbox and specify the polling interval.
6. Update Setting: Click “Update Setting” button when you finished NTP Setting.

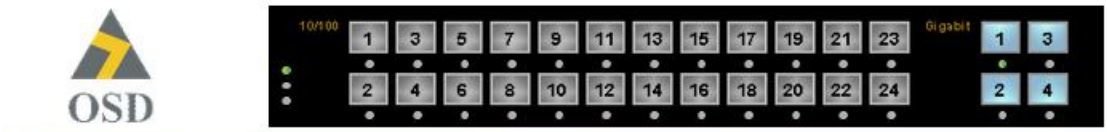
Daylight Saving Setting:

1. Daylight Saving Mode: Click "Daylight Saving Mode" drop-down menu from "Daylight Saving

Mode" drop-down list to choose "Disable", "Weekday", or "Date" to choose disable, weekday, or date daylight saving for the Switch.

2. Time Set Offset (1-1440 min): Click in the "Time Set Offset" textbox and specify the offset time of daylight saving. For example enter 60 for one hour offset.
3. Name of Daylight Saving Tmiezone: Click in the "Name of Daylight Saving Tmiezone" textbox and specify the name of daylight saving timezone. This can be any given name in 14-character alpha-numericals. Enter the name of Daylight-Saving time zone using the following example:
   EDT - East Daylight Saving Time Zone.
   CDT - Central Daylight-Saving Time Zone.
   MDT - Mountain Daylight-Saving Time Zone.
   PDT - Pacific Daylight-Saving Time Zone.
   ADT - Alaska Daylight-Saving Time Zone.
4. Weekday: Click in the textboxes and specify the daylight saving period.
   - Month: Click "Month" drop-down menu from "Month" drop-down list to choose from January to December.
   - Week: <1-5> Specifies starting/ending week of daylight savings time.
   - Day: Click "Day" drop-down menu from "Day" drop-down list to choose from Sunday to Saturday.
   - Hour: <0-23> Specifies from 0 to 23.
   - Minute: <0-59> Specifies from 0 to 59.
5. Date: Click in the textboxes and specify the daylight saving period.
   - Month: Click "Month" drop-down menu from "Month" drop-down list to choose from January to December.
   - Day: <1-31> Specifies from 1 to 31.
   - Hour: <0-23> Specifies from 0 to 23.
   - Minute: <0-59> Specifies from 0 to 59.
6. Update Setting: Click "Update Setting" button when you finished Daylight Saving Setting.

**<Note> The “Week”, “Hour”, “Minute”, and “Day” fields would not accept the alphabetic characters (Like Jan, Feb, sun, mon). They only accept the two digit numbers (0 throught 9).**




- Management Switch
  - System
  - Diagnostics
  - Port
  - Switching
  - Trunking
  - STP/Ring
  - VLAN
  - QoS
  - ACL
  - SNMP
  - 802.1X
  - LLDP
  - Others Protocols
    - GVRP
    - IGMP Snooping
    - NTP
    - GMRP
    - DHCP Server

GMRP Global Setting

| GMRP | Disable |
|---|---|

Update Setting

Per Port Setting (Include LAG)

| Port | GMRP | GMRP Registration | GMRP Forward All |
|---|---|---|---|
| 1 | Disable | Normal | Disable |
| 2 | Disable | Normal | Disable |
| 3 | Disable | Normal | Disable |
| 4 | Disable | Normal | Disable |
| 5 | Disable | Normal | Disable |
| 6 | Disable | Normal | Disable |
| 7 | Disable | Normal | Disable |
| 8 | Disable | Normal | Disable |
| 9 | Disable | Normal | Disable |
| 10 | Disable | Normal | Disable |
| 11 | Disable | Normal | Disable |
| 12 | Disable | Normal | Disable |
| 13 | Disable | Normal | Disable |
| 14 | Disable | Normal | Disable |
| 15 | Disable | Normal | Disable |
| 16 | Disable | Normal | Disable |
| 17 | Disable | Normal | Disable |
| 18 | Disable | Normal | Disable |
| 19 | Disable | Normal | Disable |
| 20 | Disable | Normal | Disable |
| 21 | Disable | Normal | Disable |
| 22 | Disable | Normal | Disable |
| 23 | Disable | Normal | Disable |
| 24 | Disable | Normal | Disable |
| 25 | Disable | Normal | Disable |
| 26 | Disable | Normal | Disable |
| 27 | Disable | Normal | Disable |
| 28 | Disable | Normal | Disable |

Update Setting

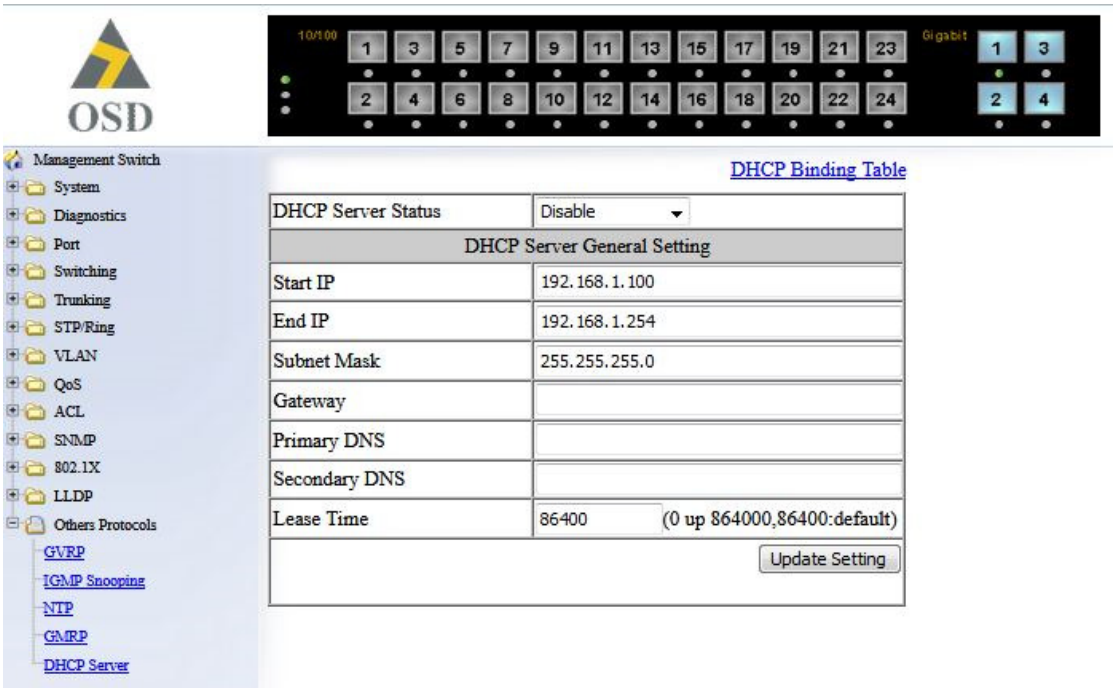
**GMRP**

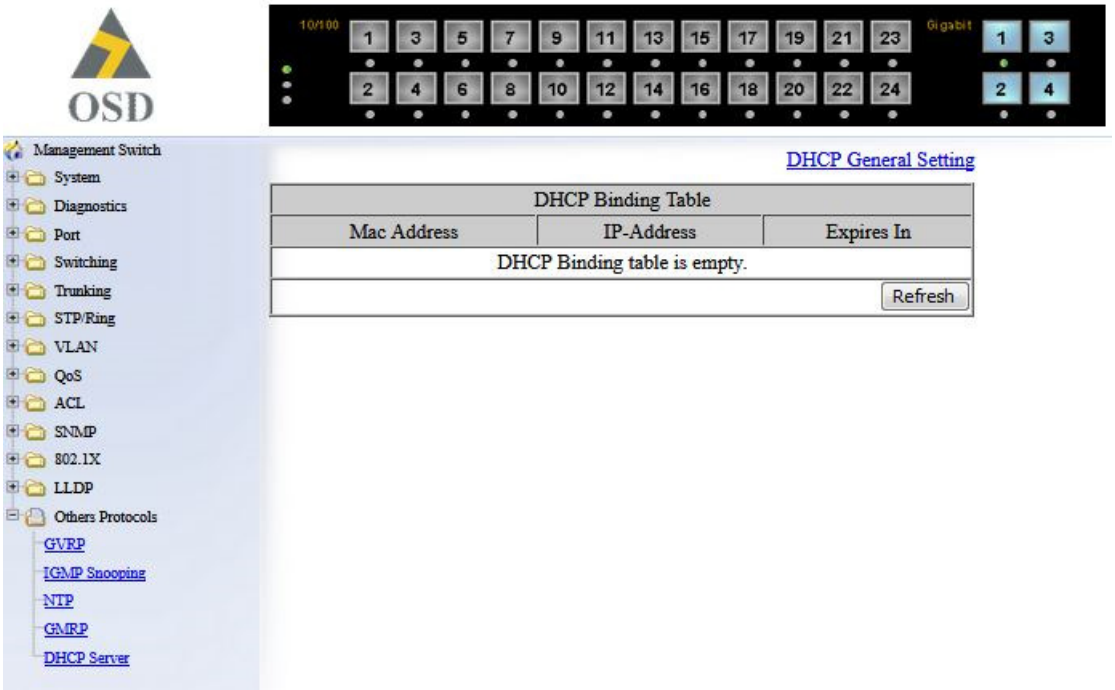
GMRP Global Setting:

1. GMRP: Click “GMRP” drop-down menu from “GMRP” drop-down list to choose “Enable” or “Disable” to enable or disable GMRP.
2. Update Setting: Click “Update Setting” button when you finished GMRP Global Setting.

Per Port Setting (Include LAG):

1. GMRP: Click “GMRP” drop-down menu from “GMRP” drop-down list to choose “Enable” or “Disable” to enable or disable GMRP for the port.
2. GMRP Registration: Click “GMRP Registration” drop-down menu from “GMRP Registration” drop-down list to choose “Normal”, “Fixed” or “Forbidden” to specify GMRP Registration to the port.
   Normal specifies dynamic GMRP multicast registration and deregistration on the port.
   Fixed specifies the multicast groups currently registered on the switch are applied to the port, but any subsequent registrations or deregistrations do not affect the port. Any registered multicast groups on the port are not deregistered based on the GARP timers.
   Forbidden specifies that all GMRP multicasts are deregistered, and prevent any further GMRP multicast registration on the port.
3. GMRP Forward All: Click “GMRP Forward All” drop-down menu from “GMRP Forward All” drop-down list to choose “Enable” or “Disable” to enable or disable GMRP forwarding to the port.
4. Update Setting: Click “Update Setting” button when you finished Per Port Setting.


OSD
10/100
1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24
Gigabit
1 3
2 4
Management Switch
System
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
ACL
SNMP
802.1X
LLDP
Others Protocols
GVRP
IGMP Snooping
NTP
GMRP
DHCP Server
DHCP Binding Table
DHCP Server Status
Disable
DHCP Server General Setting
Start IP
192.168.1.100
End IP
192.168.1.254
Subnet Mask
255.255.255.0
Gateway
Primary DNS
Secondary DNS
Lease Time
86400
(0 up 864000,86400:default)
Update Setting


OSD
10/100
1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24
Gigabit
1 3
2 4
Management Switch
System
Diagnostics
Port
Switching
Trunking
STP/Ring
VLAN
QoS
ACL
SNMP
802.1X
LLDP
Others Protocols
GVRP
IGMP Snooping
NTP
GMRP
DHCP Server
DHCP General Setting
DHCP Binding Table
Mac Address
IP-Address
Expires In
DHCP Binding table is empty.
Refresh

**DHCP Server**

1. DHCP Binding Table: Click on “DHCP Binding Table” to show DHCP Binding Table. Click “Refresh” button to refresh DHCP Binding Table. Click on “DHCP General Setting” to back to DHCP General Setting.
2. DHCP Server Status: Click “DHCP Server Status” drop-down menu from “DHCP Server Status” drop-down list to choose “Disable”, “Default VLAN 1”, or other VLAN.
3. Start IP: Click in the “Start IP” textbox and specify the default Start IP for the DHCP Server.
4. End IP: Click in the “End IP” textbox and specify the default End IP for the DHCP Server.
5. Subnet Mask: Click in the “Subnet Mask” textbox and specify the default subnet mask for the DHCP Server.
6. Gateway: Click in the “Gateway” textbox and specify the default gateway for the DHCP Server.
7. Primary DNS: Click in the “Primary DNS” textbox and specify the default primary DNS for the DHCP Server.
8. Secondary DNS: Click in the “Secondary DNS” textbox and specify the default secondary DNS for the DHCP Server.
9. Lease Time: Click in the “Lease Time” textbox and specify the default lease time for the DHCP Server.
10. Update Setting: Click “Update Setting” button when you finished DHCP Server General Setting.

# 7 COMMAND LINE CONSOLE MANAGEMENT

The switch provides a command line console interface for configuration purposes. The switch can be configured either locally through its RS-232 port or remotely via a Telnet session. For the later, you must specify an IP address for the switch first.

This chapter describes how to configure the switch using its console by Command Line.

## 7.1 ADMINISTRATION CONSOLE

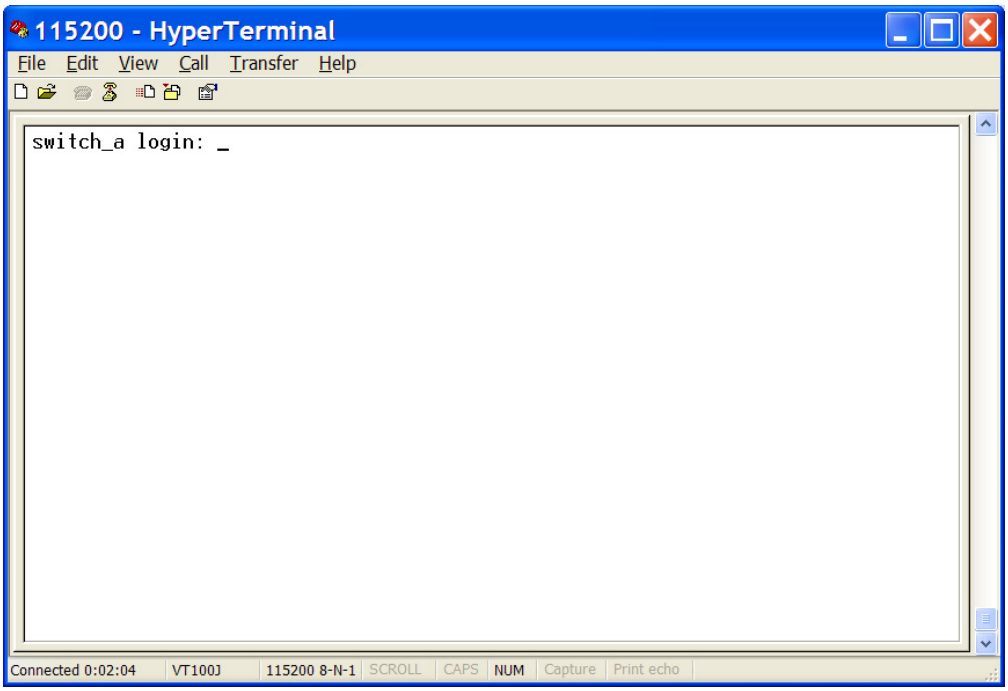
Connect the DB9 straight cable to the RS-232 serial port of the device to the RS-232 serial port of the terminal or computer running the terminal emulation application.

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as HyperTerminal) to the switch console port.

When using the management method, configure the terminal-emulation program to use the following parameters (you can change these settings after login):

[Default parameters]
115,200bps
8 data bits
No parity
1 stop bit

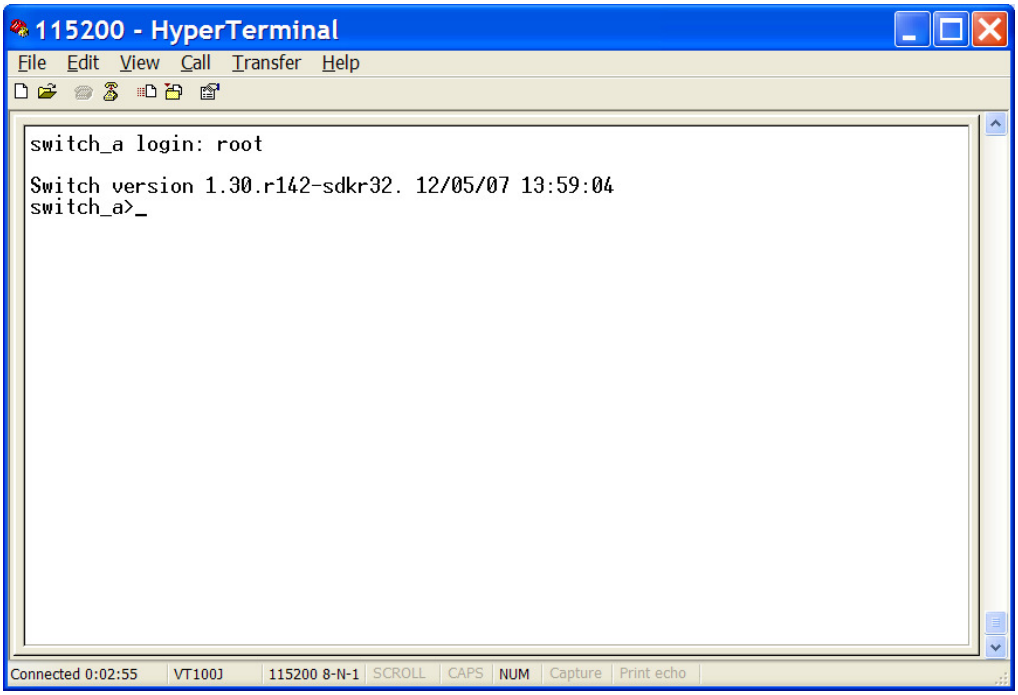
### 7.1.1 EXEC MODE (VIEW MODE)




**LOGON TO EXEC MODE (VIEW MODE)**

At the **switch_a login:** prompt just type in “root” and press <Enter> to logon to Exec Mode (or View Mode).

```
switch_a login: root
```

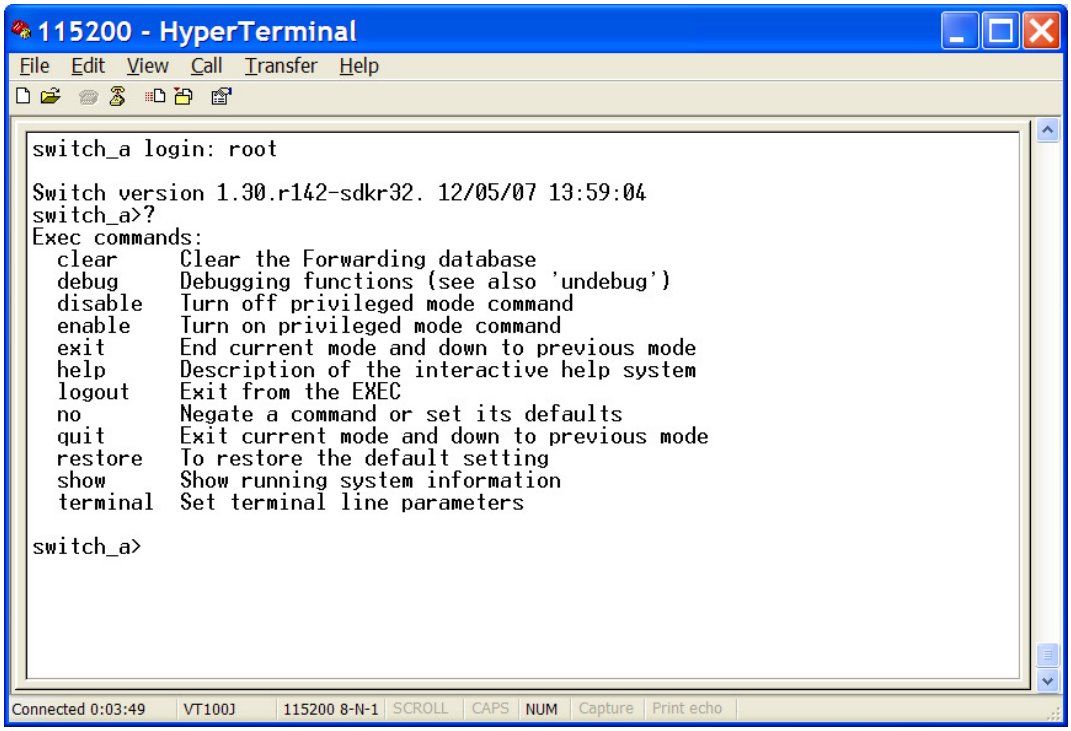


**BASIC COMMANDS**

Exec Mode (or View Mode) is the base mode from where users can perform basic commands like: clear, debug, disable, enable, exit, help, logout, no, quit, show, terminal
The CLI contains a text-based help facility. Access this help by typing in the full or partial command string then typing a question mark "?". The CLI displays the command keywords or parameters along with a short description.

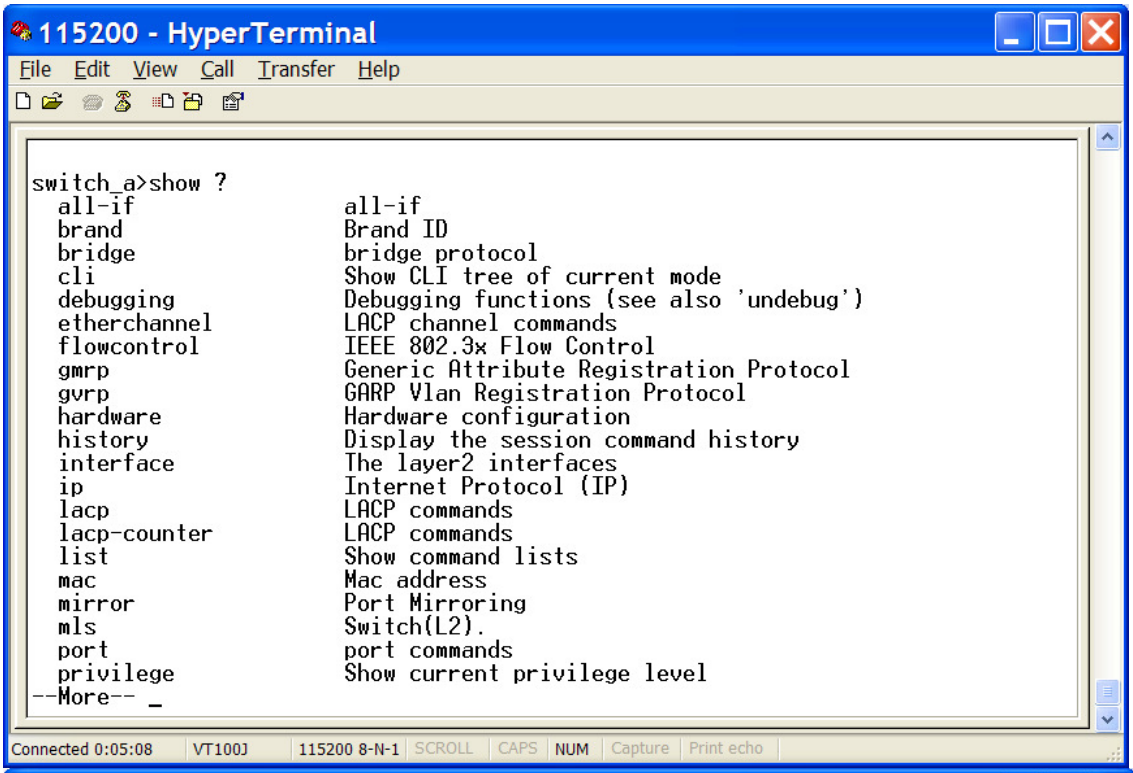
At the **switch_a>** prompt just press <?> to list the above basic commands.

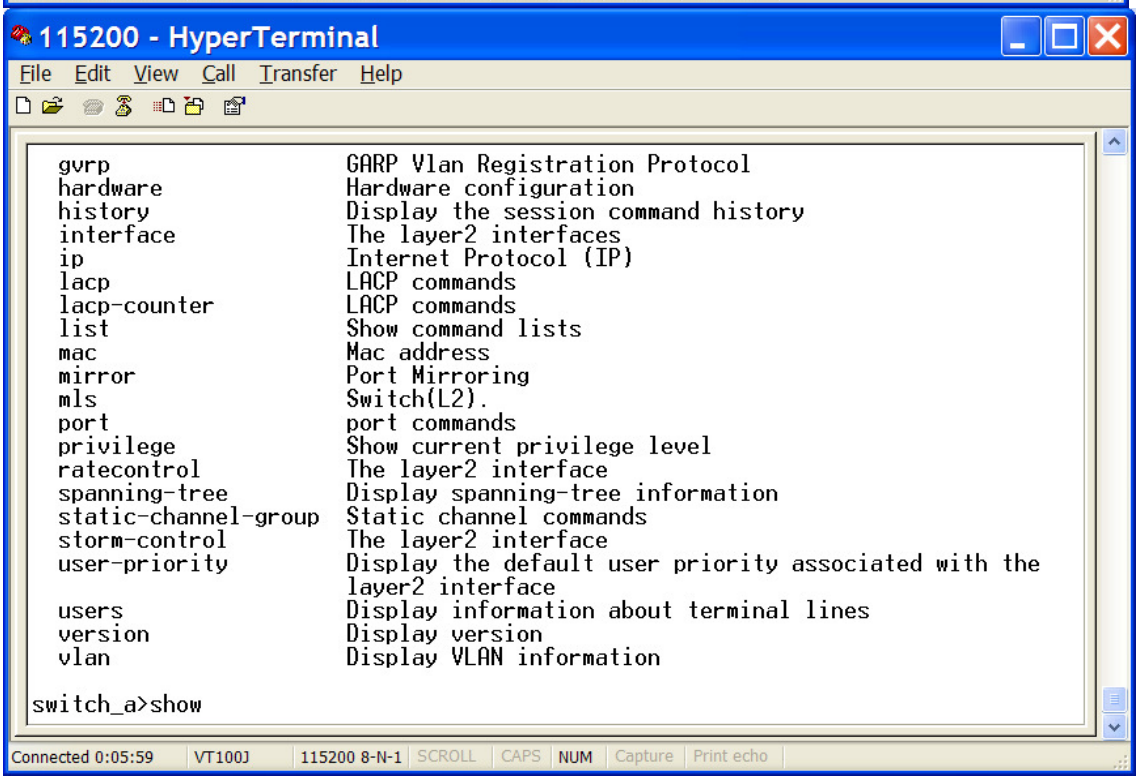
```
switch_a>?
```



At the **switch_a>** prompt just type in the full or partial command string then typing a question mark "?" to display the command keywords or parameters along with a short description.

```
switch_a>show ?
```



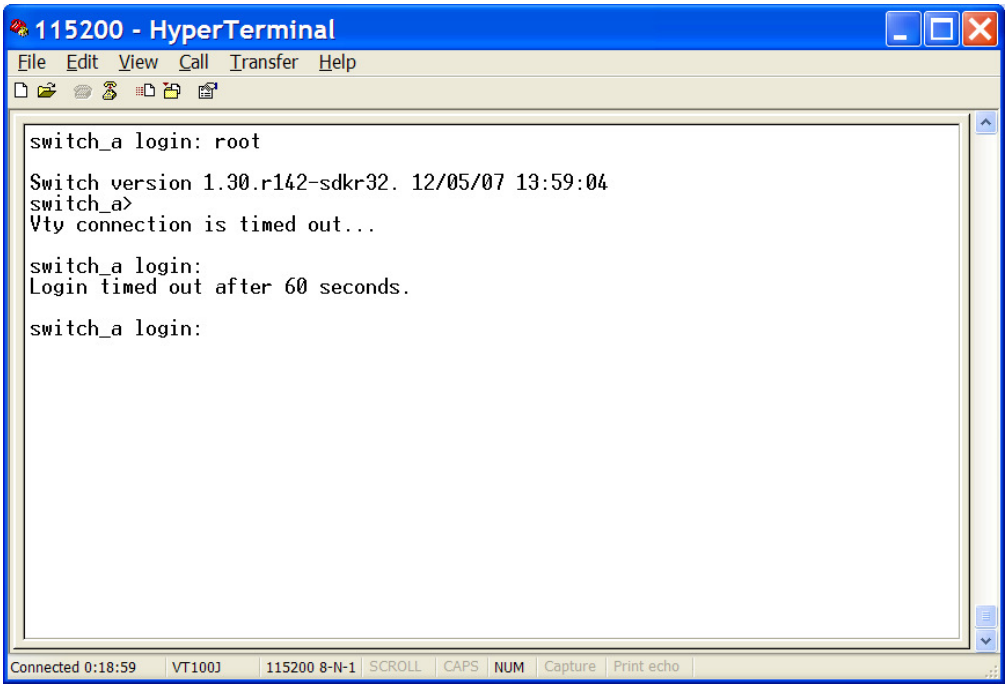
**LOGIN TIMED OUT**

The login session to Exec Mode (or View Mode) has timed out due to an extended period of inactivity (60 seconds) to indicate authentication attempt timed out. And the **switch_a login:** prompt will show on the screen.

**LOGON BACK TO EXEC MODE (VIEW MODE)**

At the **switch_a login:** prompt just type in "root" and press <Enter> to logon back to Exec Mode (or View Mode).

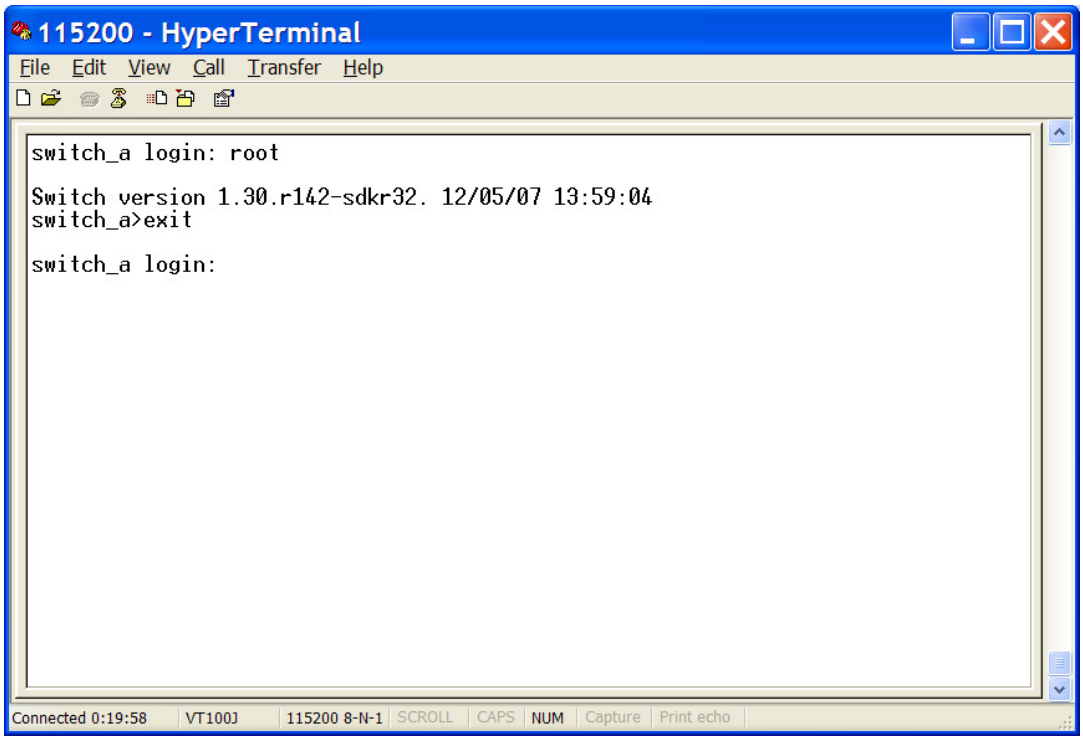
```
switch_a login: root
```



**EXIT FROM EXEC MODE (VIEW MODE)**

At the **switch_a>** prompt just type in “exit” and press <Enter> to exit from Exec Mode (or View Mode).

```
switch_a>exit
```

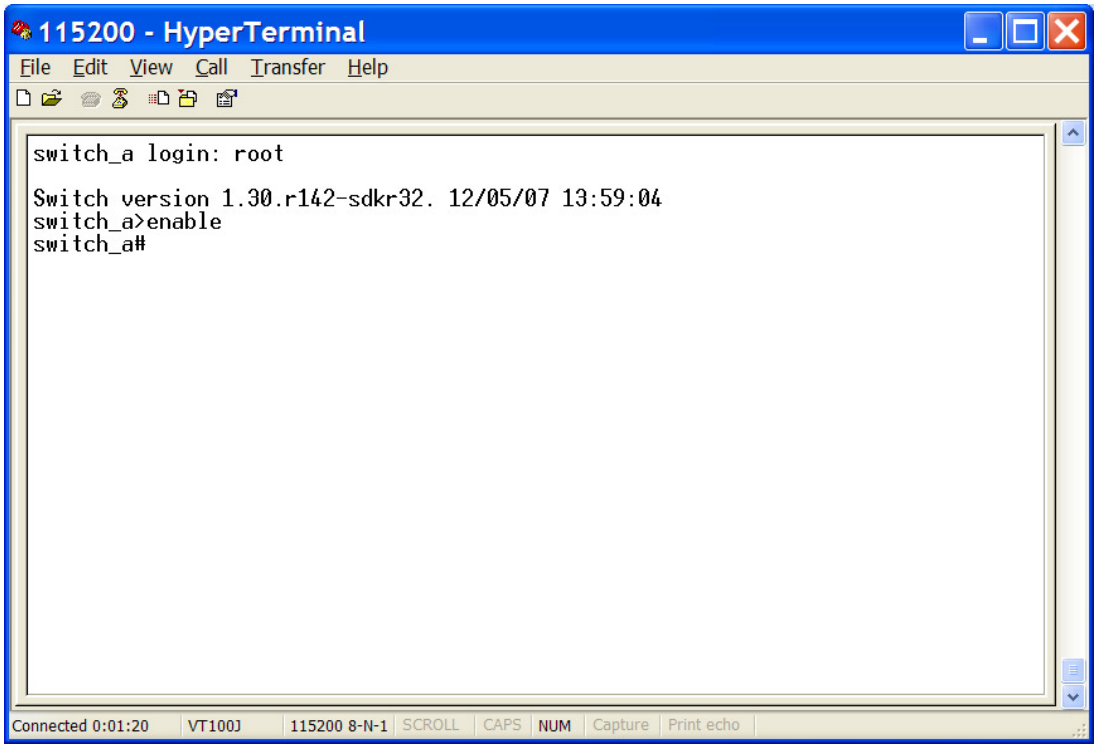


### 7.1.2 PRIVILEGED EXEC MODE (ENABLE MODE)

**LOGON TO PRIVILEGED EXEC MODE (ENABLE MODE)**

At the **switch_a>** prompt just type in “enable” and press <Enter> to logon to Privileged Exec Mode (or Enable Mode). And the **switch_a#** prompt will show on the screen.

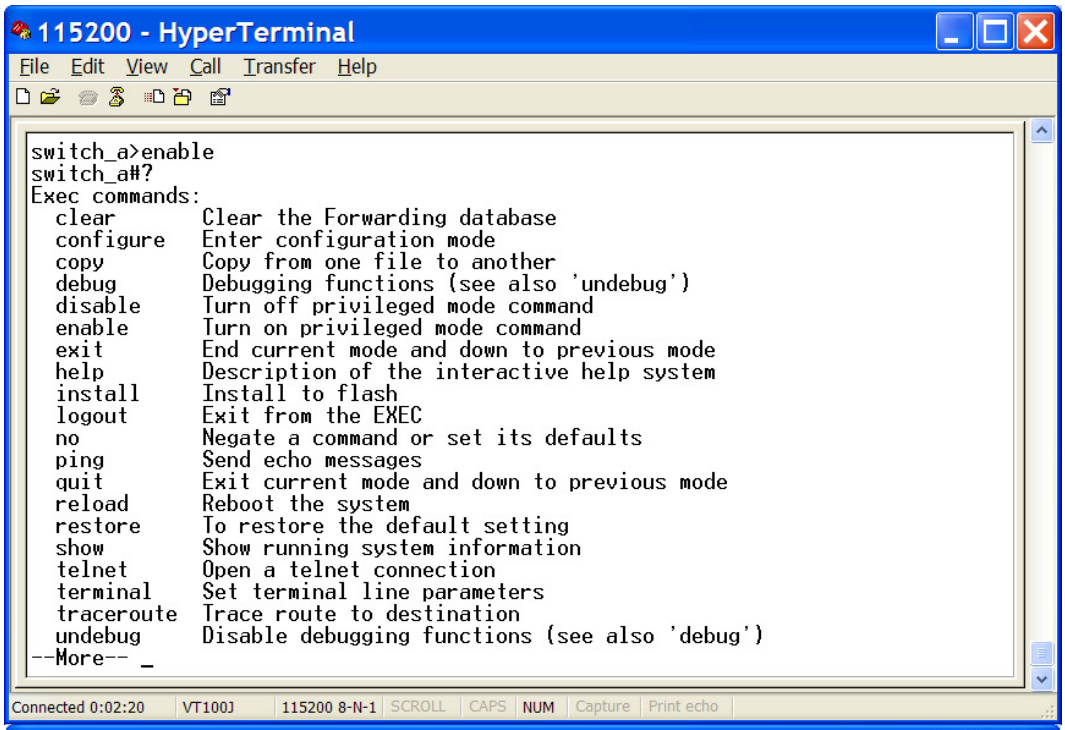
```
switch_a>enable
```

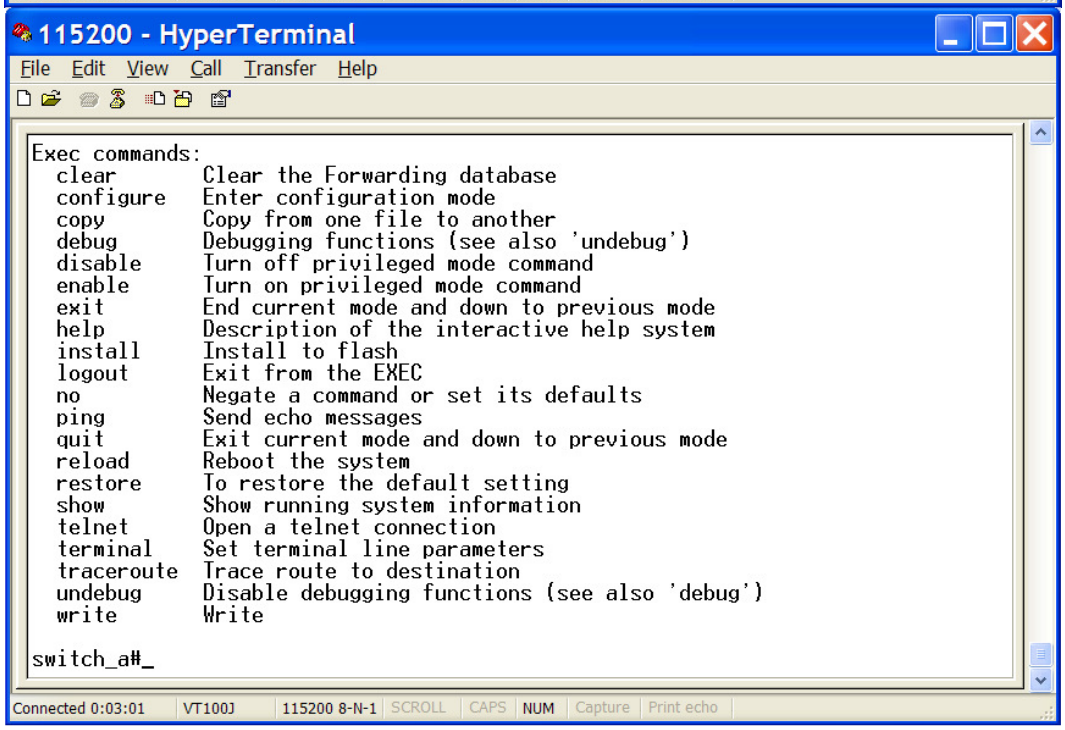


**COMMANDS**

Privileged Exec Mode (or Enable Mode) allows users to run commands as following.
At the **switch_a#** prompt just press <?> to list the commands.

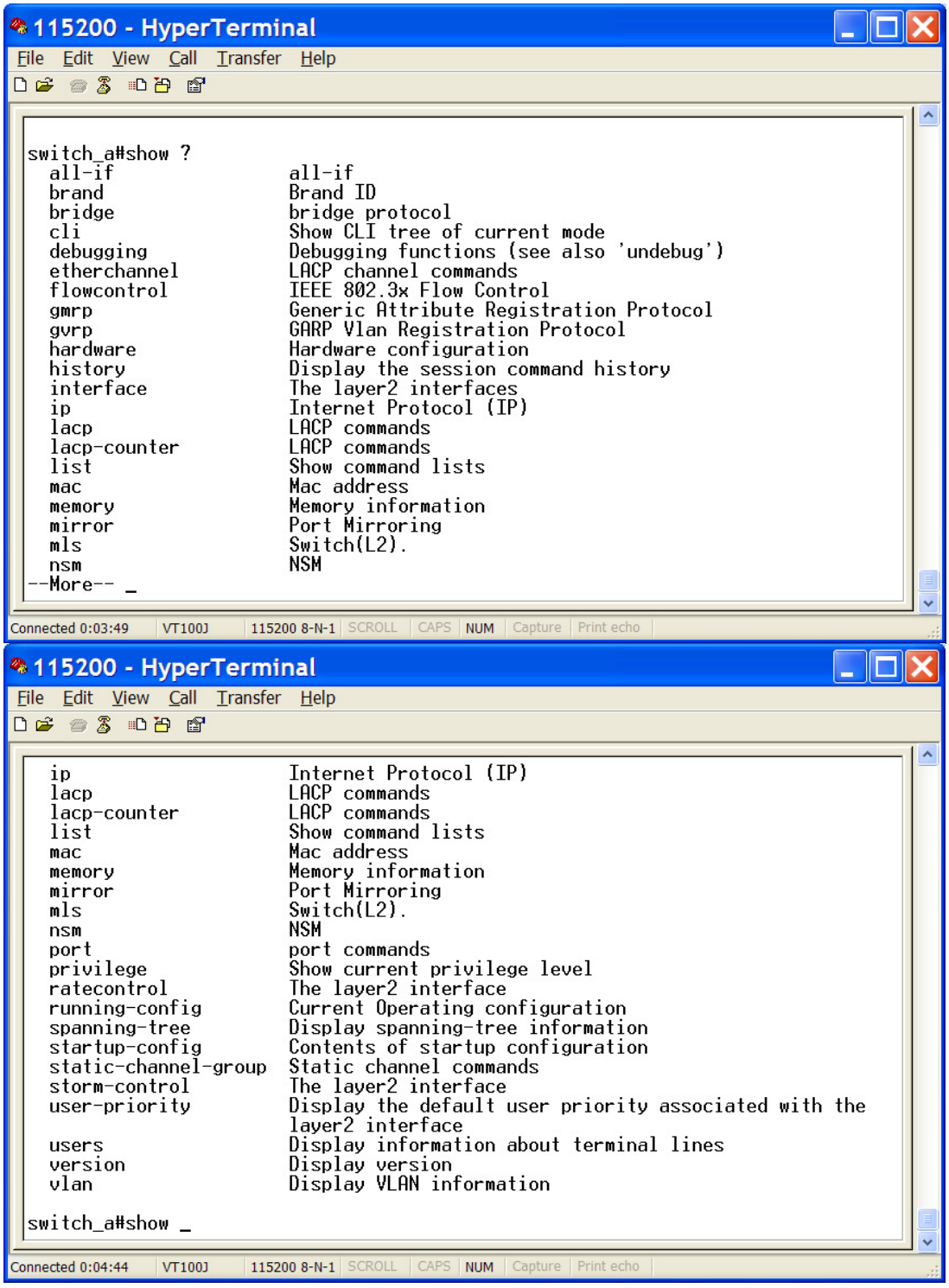
```
switch_a#?
```



At the **switch_a#** prompt just type in the full or partial command string then typing a question mark "?" to display the command keywords or parameters along with a short description.

```
switch_a#show ?
```



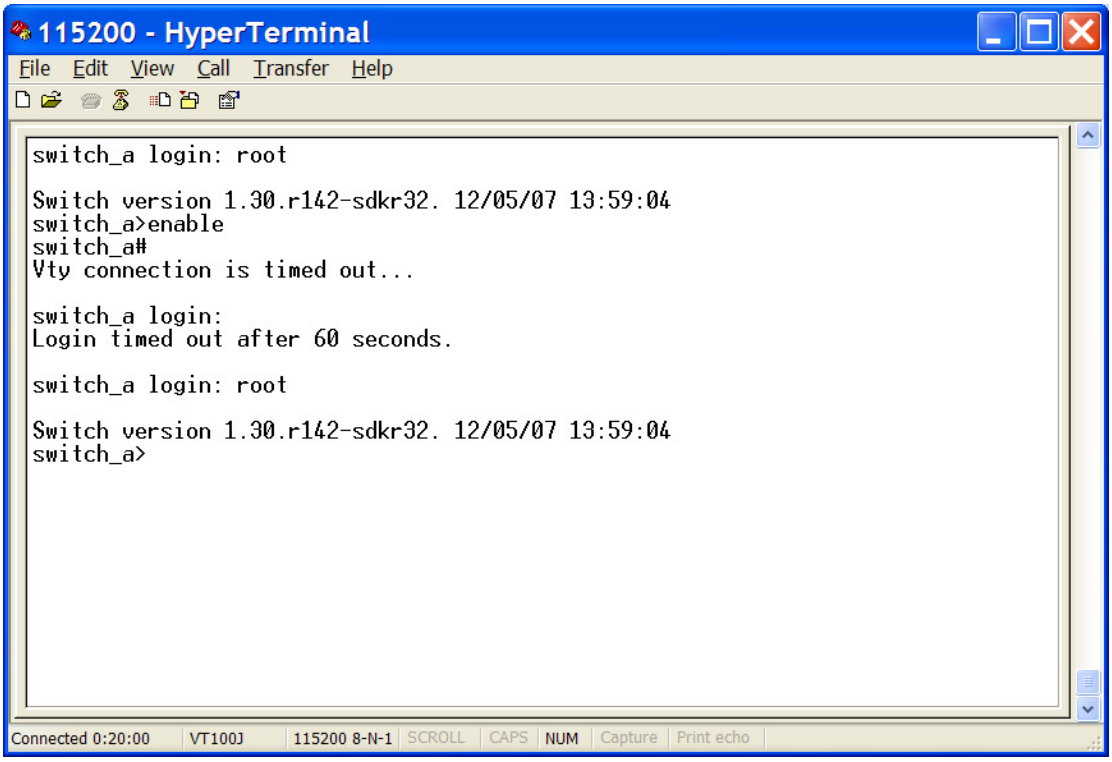
**LOGIN TIMED OUT**

The login session to Privileged Exec Mode (or Enable Mode) has timed out due to an extended period of inactivity (60 seconds) to indicate authentication attempt timed out. And the **switch_a login:** prompt will show on the screen.

**LOGON BACK TO EXEC MODE (VIEW MODE)**

At the **switch_a login:** prompt just type in "root" and press <Enter> to logon back to Exec Mode (or View Mode).

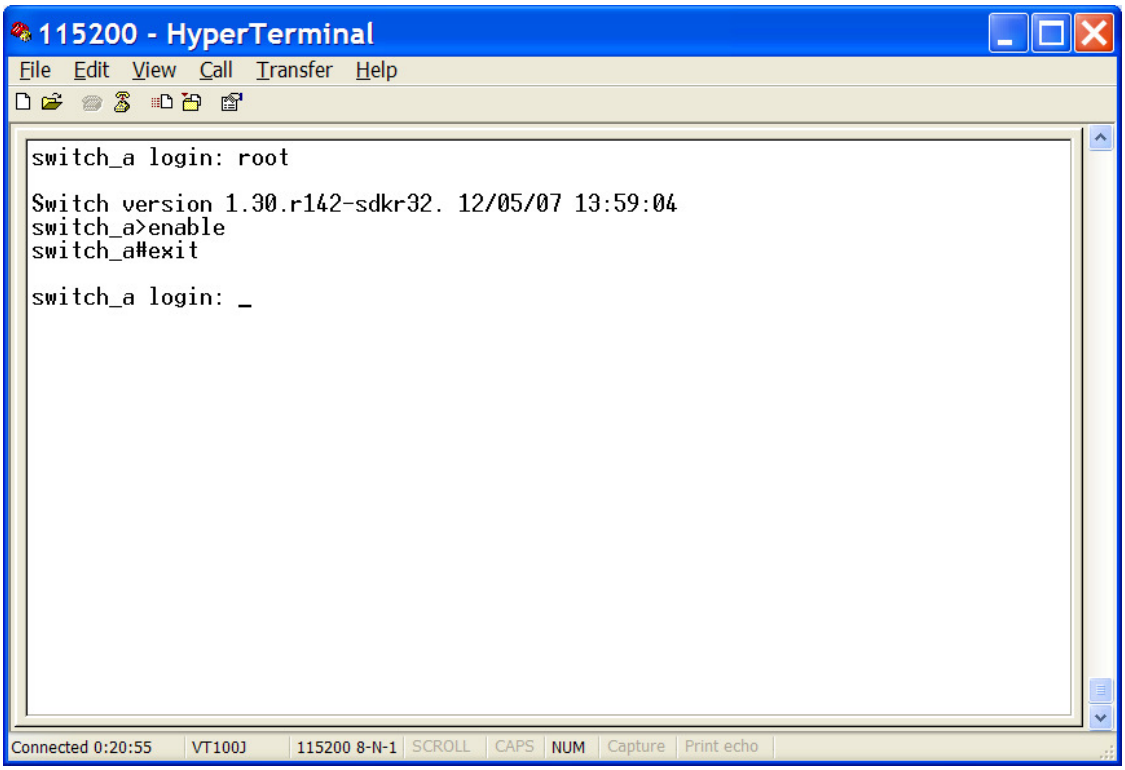
```
switch_a login: root
```



**EXIT FROM PRIVILEGED EXEC MODE (OR ENABLE MODE)**

At the **switch_a#** prompt just type in “exit” and press <Enter> to exit from Privileged Exec Mode (or Enable Mode).

```
switch_a#exit
```

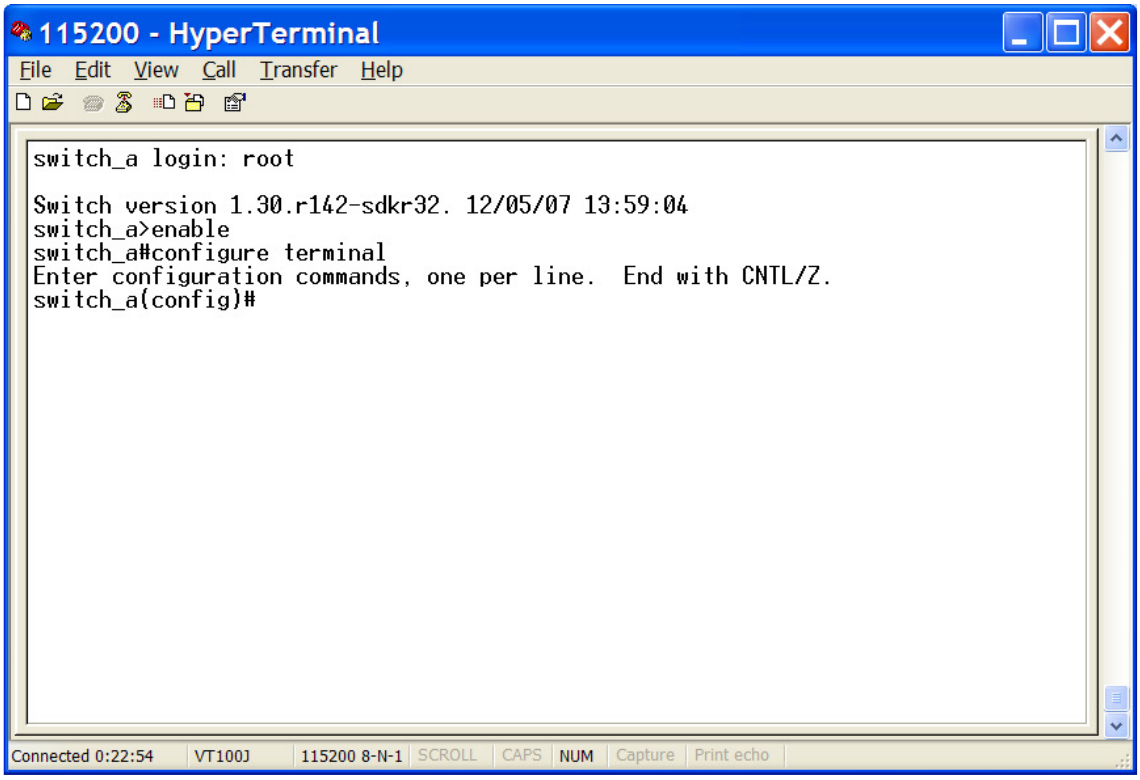


### 7.1.3 CONFIGURE MODE (CONFIGURE TERMINAL MODE)

**LOGON TO CONFIGURE MODE (CONFIGURE TERMINAL MODE)**

At the **switch_a#** prompt just type in "configure terminal" and press <Enter> to logon to Configure Mode (or Configure Terminal Mode). And the **switch_a(config)#** prompt will show on the screen.

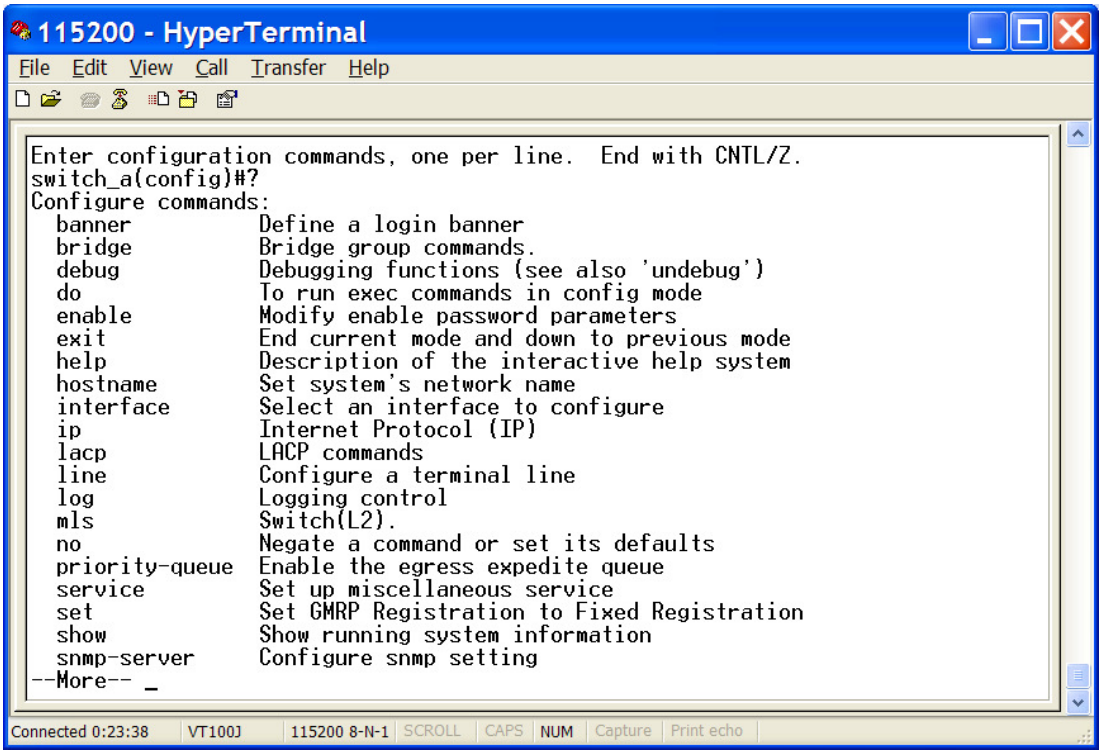
```
switch_a#configure terminal
```

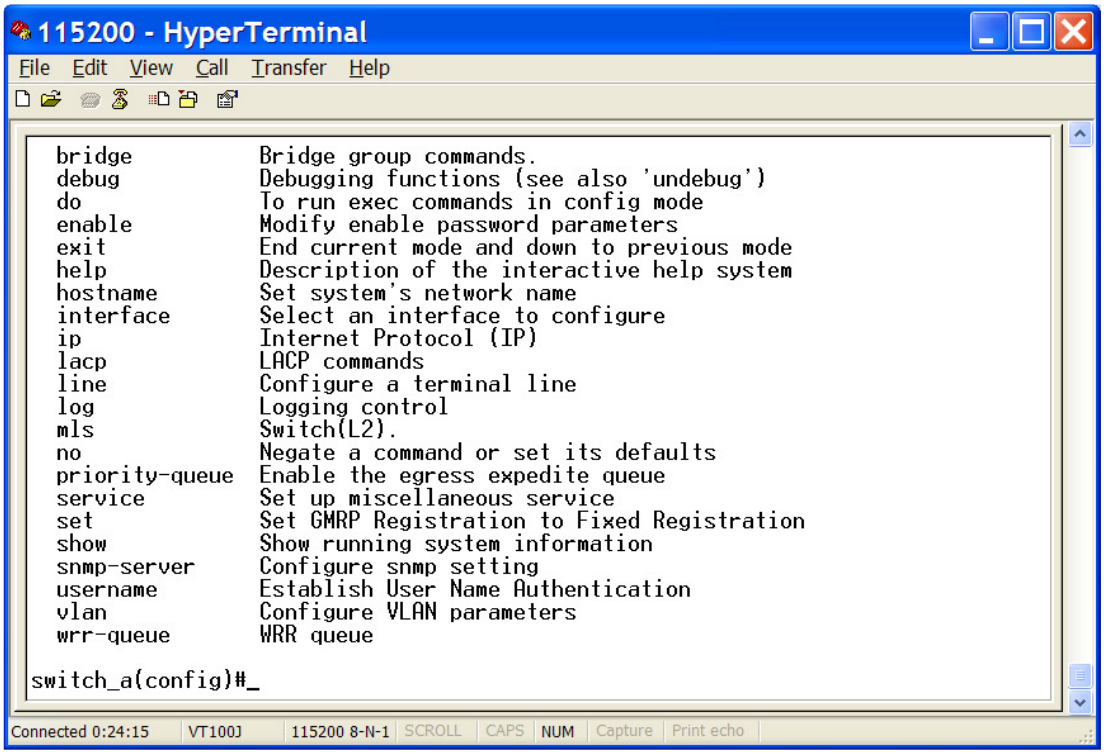


**COMMANDS**

Configure Mode (or Configure Terminal Mode) serves as a gateway into the modes as following.
At the **switch_a(config)#** prompt just press <?> to list the commands.

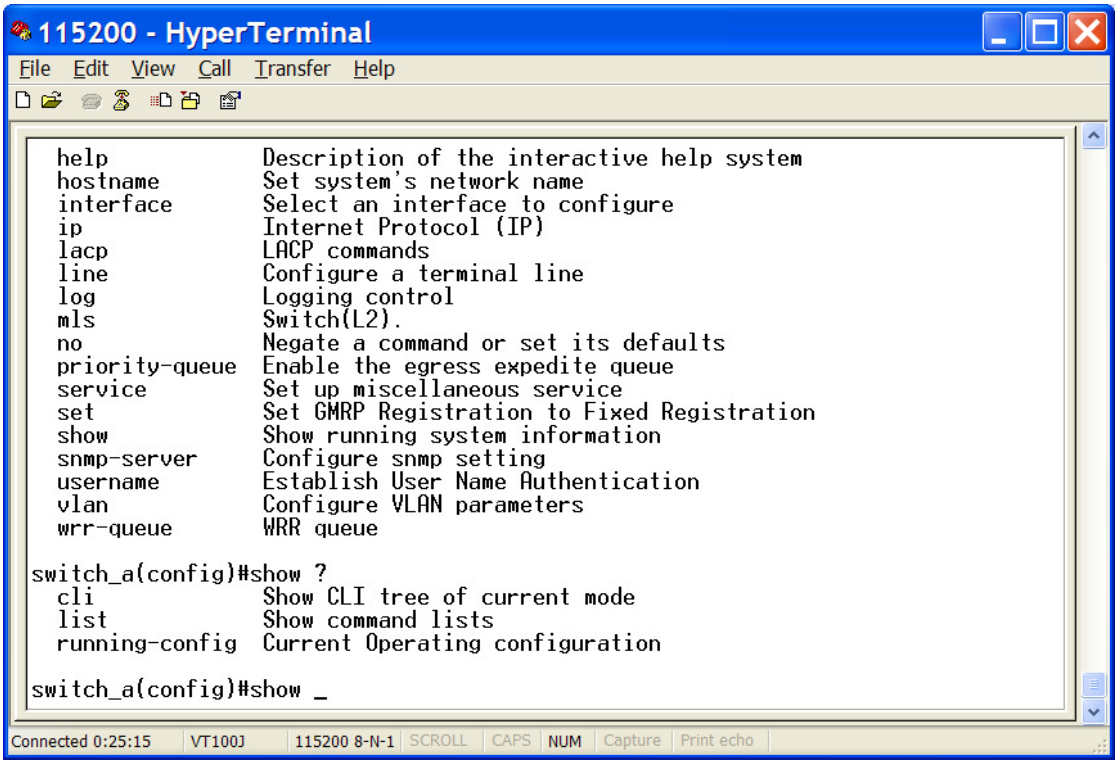
```
switch_a(config)#?
```



At the **switch_a(config)#** prompt just type in the full or partial command string then typing a question mark "?" to display the command keywords or parameters along with a short description.

switch_a(config)#show ?



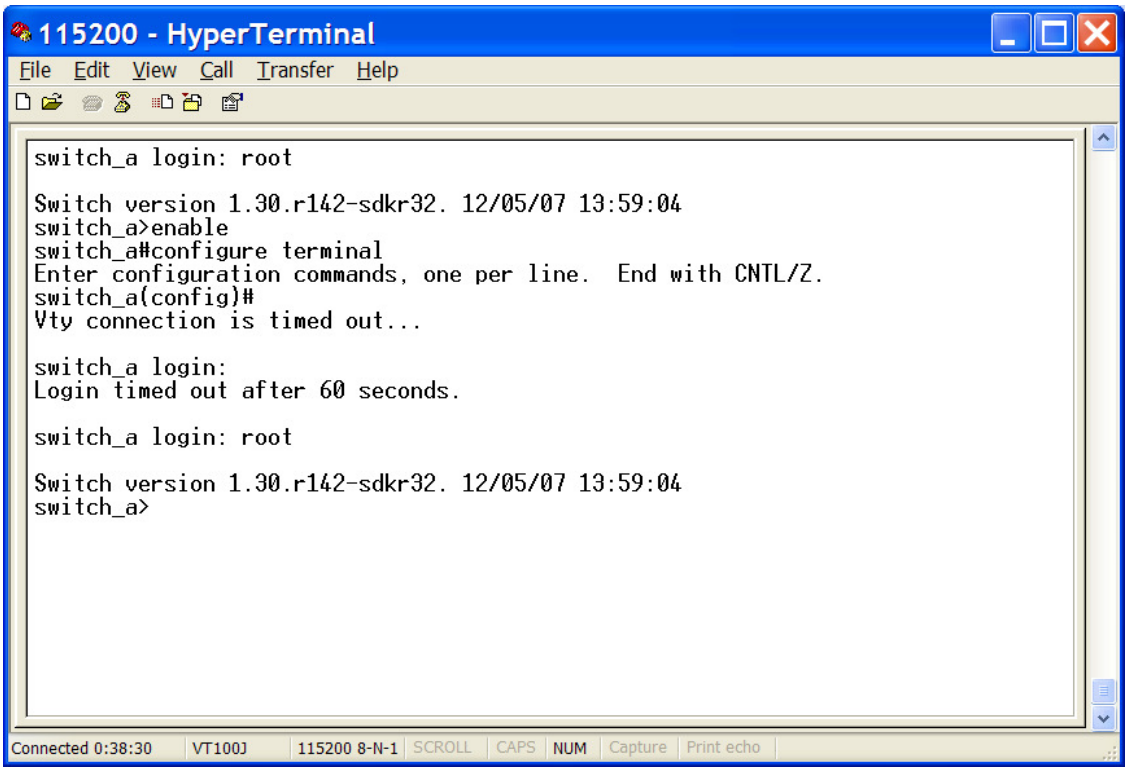
**LOGIN TIMED OUT**

The login session to Configure Mode (or Configure Terminal Mode) has timed out due to an extended period of inactivity (60 seconds) to indicate authentication attempt timed out. And the **switch_a login:** prompt will show on the screen.

**LOGON BACK TO EXEC MODE (VIEW MODE)**

At the **switch_a login:** prompt just type in "root" and press <Enter> to logon back to Exec Mode (or View Mode).

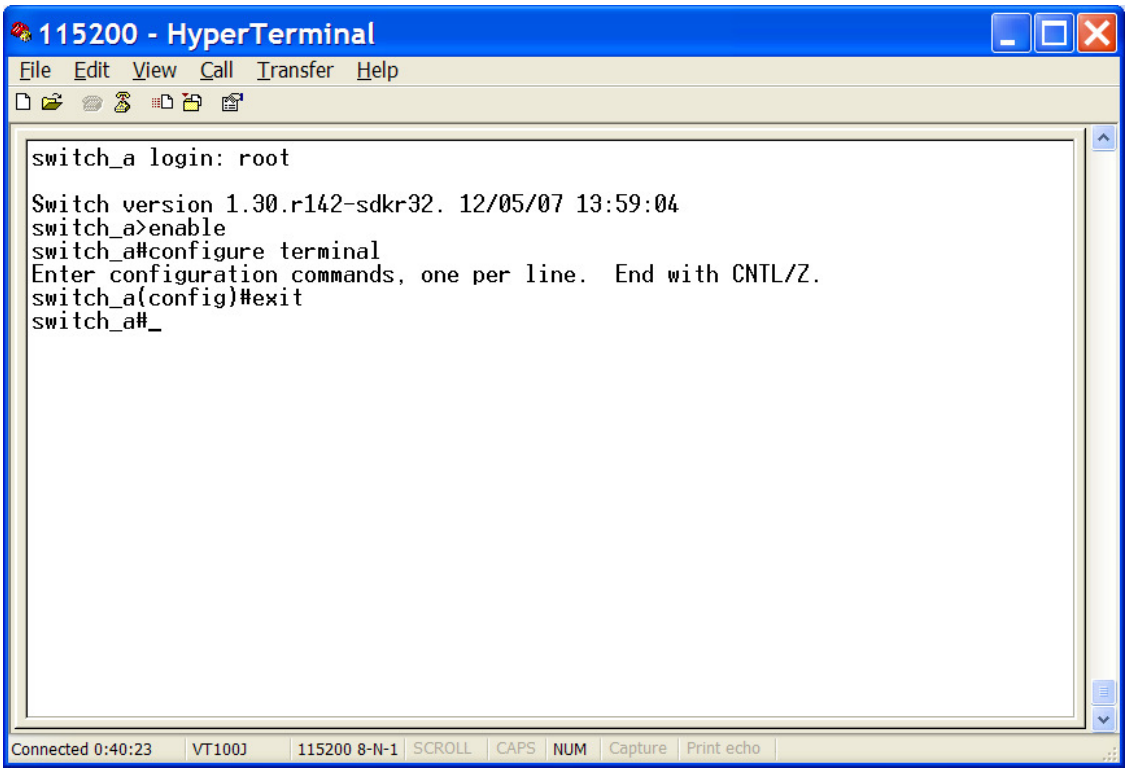
```
switch_a login: root
```



**EXIT FROM CONFIGURE MODE (OR CONFIGURE TERMINAL MODE)**

At the **switch_a(config)#** prompt just type in “exit” and press <Enter> to exit from Configure Mode (or Configure Terminal Mode).

```
switch_a(config)#exit
```



## 7.2 SYSTEM

System Information, System Name/Password, IP Address, Save Configuration, Firmware Upgrade, Reboot, Logout, User Account, User Privilege

**SYSTEM NAME/PASSWORD**
System Name:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **hostname** command to set or change the network server name.
Use the **no hostname** command to disable this function.

3. Command Syntax:
(no) hostname HOSTNAME
HOSTNAME specifies the network name of the system.

4. Example:
The following example sets the hostname to **switch**, and shows the change in the prompt:

```
switch_a(config)#hostname switch
switch(config)#
```

---

Password:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **enable password** command to modify or create a password to be used when entering the Enable mode.

3. Command Syntax:
enable password PASSWORD
PASSWORD specifies the new password of the system.

4. Example:
The following example sets the new password **mypasswd** to switch:

```
switch_a(config)#enable password mypasswd
switch_a(config)#
```

---

**IP ADDRESS**
IP Address/IP Subnet Mask:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
vlan1.1 means vlan 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:
Use **ip address** command to set the IP address of an interface.
Use the **no ip address** command to remove the IP address from an interface.

3. Command Syntax:
ip address IP-ADDRESS
no ip address IP-ADDRESS
no ip address
IP-ADDRESS A.B.C.D/M specifies the IP address and prefix length of an interface.
M specifies IP subnet mask, 8: 255.0.0.0, 16:255.255.0.0, 24: 255.255.255.0.

4. Example:
The following example sets the new IP address **192.168.1.10** and new IP subnet mask **255.255.255.0** to switch:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip address 192.168.1.10/24
switch_a(config-if)#
```

---

**DHCP CLIENT:**
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
vlan1.1 means vlan 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:
Use **get ip dhcp enable** command to get IP address through DHCP server.
Use the **no get ip dhcp enable** command to cancel the IP address which got through DHCP server.

3. Command Syntax:
(no) get ip dhcp enable

4. Example:
The following example gets IP address through DHCP server:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#get ip dhcp enable
switch_a(config-if)#
```

---

Default Gateway:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **ip default-gateway** command to set the IP address of the default gateway.
Use the **no ip default-gateway** command to remove the IP address of the default gateway.

3. Command Syntax:
ip default-gateway IP-ADDRESS
no ip default-gateway
IP-ADDRESS A.B.C.D specifies the IP address of the default gateway.

4. Example:
The following example sets the default gateway **192.168.1.254** to switch:

```
switch_a(config)#ip default-gateway 192.168.1.254
switch_a(config)#
```

---

**DNS SERVER:**
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **ip dns** command to set the IP address of the DNS server.
Use the **no ip dns** command to remove the IP address of the DNS server.

3. Command Syntax:
ip dns IP-ADDRESS
no ip dns
IP-ADDRESS A.B.C.D specifies the IP address of the DNS server.

4. Example:
The following example sets the DNS server **192.168.1.100** to switch:

```
switch_a(config)#ip dns 192.168.1.100
switch_a(config)#
```

---

**SAVE CONFIGURATION**
Load config from TFTP server:
1. Command Mode: Privileged Exec mode
Logon to Privileged Exec Mode (Enable Mode).
The **switch_a#** prompt will show on the screen.

```
switch_a#
```

2. Usage:
Use **install image** command to load configuration file from tftp server to switch.

3. Command Syntax:
install image IP-ADDRESS WORD
IP-ADDRESS specifies the IP address of tftp server.
WORD specifies the file name to be loaded to switch.

4. Example:
The following example specifies upgrading firmware (file name: **flash.tgz**) from tftp server (IP address: **192.168.1.100)** to switch:

```
switch_a#install image 192.168.1.100 flash.tgz
switch_a#
```

---

**LOAD CONFIG TO TFTP SERVER:**

1. Command Mode: Privileged Exec mode
Logon to Privileged Exec Mode (Enable Mode).
The **switch_a#** prompt will show on the screen.

```
switch_a#
```

2. Usage:
Use **write config-file** command to backup configuration file to tftp server.

3. Command Syntax:
write config-file IP-ADDRESS
IP-ADDRESS specifies the IP address of tftp server.

4. Example:
The following example backups configuration file to tftp server (IP address: **192.168.1.20)**:

```
switch_a#write config-file 192.168.1.20
switch_a#
```

---

**SAVE CONFIGURATION:**

1. Command Mode: Privileged Exec mode
Logon to Privileged Exec Mode (Enable Mode).
The **switch_a#** prompt will show on the screen.

```
switch_a#
```

2. Usage:
Use **copy running-config startup-config** command to write configurations to the file to be used at startup. This is the same as the **write memory** command.

3. Command Syntax:
copy running-config startup-config

4. Example:
The following example specifies writing configurations to the file to be used at startup to switch:

```
switch_a#copy running-config startup-config
switch_a#
```

---

Restore Default:
1. Command Mode: Privileged Exec mode
Logon to Privileged Exec Mode (Enable Mode).
The **switch_a#** prompt will show on the screen.

```
switch_a#
```

2. Usage:
Use **restore default** command to restore default setting of the switch.

3. Command Syntax:
restore default

4. Example:
The following example restores default setting of the switch:

```
switch_a#restore default
switch_a#
```

---

Auto Save:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to enable auto save configuration function. The configuration will be automatically saved at every configured interval while this command is enabled. Use the no form of this command to disable this feature.

3. Command Syntax:
service auto-config enable
no service auto-config enable

4. Example:
The following example enables or disables auto save configuration to switch:

```
switch_a(config)#service auto-config enable
switch_a(config)#no service auto-config enable
switch_a(config)#
```

---

Auto Save Interval (5~65536 sec):
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set the interval when the configuration would be automatically saved. The range of interval value is from 5 to 65535. And the default value is 30 seconds.

3. Command Syntax:
service auto-config interval WORD
WORD specifies the interval value.

4. Example:
The following example sets the interval WORD (**10**) when the configuration would be automatically saved to switch:

```
switch_a(config)#service auto-config interval 10
switch_a(config)#
```

**FIRMWARE UPGRADE**

1. Command Mode: Privileged Exec mode
Logon to Privileged Exec Mode (Enable Mode).
The **switch_a#** prompt will show on the screen.

```
switch_a#
```

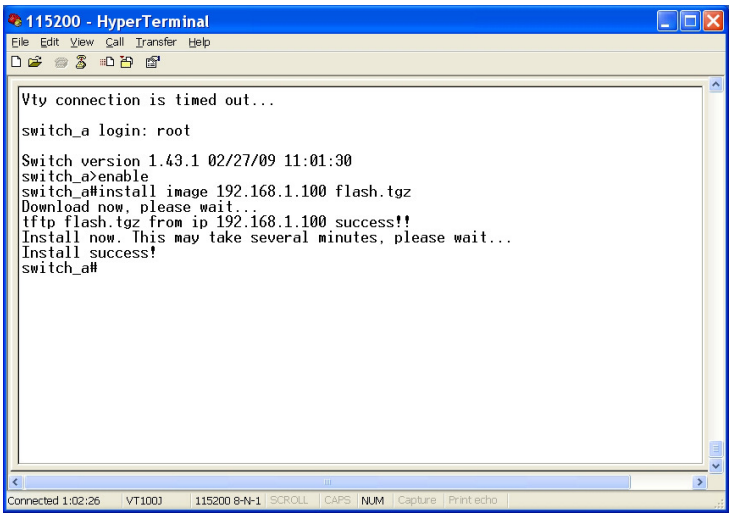
2. Usage:
Use **install image** command to upgrade firmware from tftp server to switch.

3. Command Syntax:
install image IP-ADDRESS WORD
IP-ADDRESS specifies the IP address of tftp server.
WORD specifies the file name to be upgraded to switch.

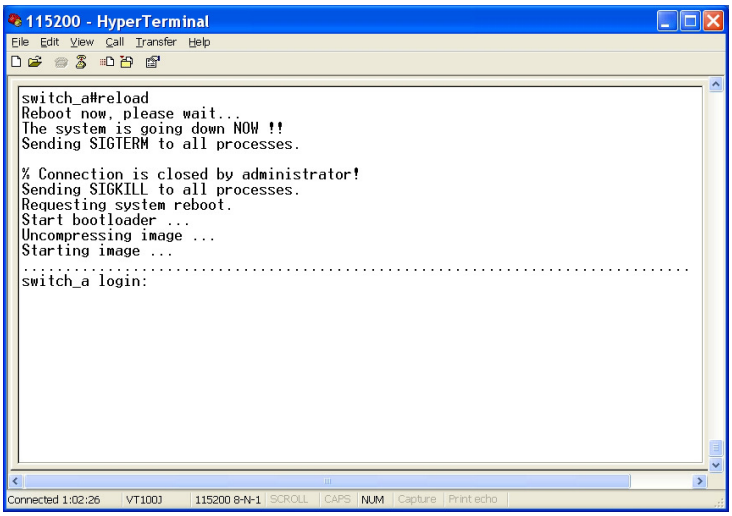
4. Example:
The following example specifies upgrading firmware (file name: **flash.tgz**) from tftp server (IP address: **192.168.1.100**) to switch:

```
switch_a#install image 192.168.1.100 flash.tgz
switch_a#
```

Please follow the message on the screen during the firmware upgrade process. Do not turn off the power or perform other functions during this period of time.




At the "switch_a#" prompt just type in "reload" and press <Enter> to reboot the switch after completing the upgrade process.




**REBOOT**

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).
The **switch_a#** prompt will show on the screen.

```
switch_a#
```

2. Usage:

Use **reload** command to restart switch.

3. Command Syntax:

reload

4. Example:

The following example specifies restarting switch:

```
switch_a#reload
switch_a login:
```

**LOGOUT**

1. Command Mode: Exec mode or Privileged Exec mode

Logon to Exec Mode (View Mode) or Privileged Exec Mode (Enable Mode).
The **switch_a>** or **switch_a#** prompt will show on the screen.

```
switch_a>
```

```
switch_a#
```

2. Usage:

Use **logout** command to exit from the Exec mode or Privileged Exec mode.

3. Command Syntax:

logout

4. Example:

The following example specifies to exit from the Exec mode or Privileged Exec mode.

```
switch_a>logout
switch_a login:
```

---

**USER ACCOUNT**

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to specify the privilege level and set a password to user who needs to access the Switch at this level.

Use the **no username** command to disable this function.

3. Command Syntax:

username WORD privilege (admin | operator | technician) password LINE

username WORD privilege (admin | operator | technician) password 8 LINE

no username WORD

WORD User name.

8 Specifies the password will be hidden.

LINE User password string.

4. Example:

The following example sets the privilege level operator and password **111111111111** for user **operator**:

```
switch_a(config)#username operator operator password 111111111111
switch(config)#
```

## 7.3 DIAGNOSTICS

Utilization, System Log, Remote Logging, ARP Table, Route Table, Alarm Setting

**UTILIZATION**
CPU Utilization:
1. Command Mode: Exec mode
Logon to Exec Mode (View Mode).
The **switch_a>** prompt will show on the screen.

```
switch_a>
```

2. Usage:
Use the **show cpu-usage** command to show the CPU usage.

3. Command Syntax:
show cpu-usage

4. Example:
The following example shows the CPU usage:

```
switch_a>show cpu-usage
```

---

Memory Utilization:
1. Command Mode: Exec mode
Logon to Exec Mode (View Mode).
The **switch_a>** prompt will show on the screen.

```
switch_a>
```

2. Usage:
Use the **show memory-usage** command to show the memory usage.

3. Command Syntax:
show memory-usage

4. Example:
The following example shows the memory usage:

```
switch_a>show memory-usage
```

---

***System Log***
1. Command Mode: Exec mode or Privileged Exec mode
Logon to Exec Mode (View Mode) or Privileged Exec Mode (Enable Mode).
The **switch_a>** or **switch_a#** prompt will show on the screen.

```
switch_a>
```

```
switch_a#
```

2. Usage:
Use the **show system-log** command to show system log.

3. Command Syntax:
show system-log

4. Example:
The following example shows system log of the switch:

```
switch_a>show system-log
```

---

**REMOTE LOGGING**
Remote Logging:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to enable the logging of messages that are sent to syslog servers.
Use the no parameter with this command to disable the logging of messages that are sent to syslog servers.

3. Command Syntax:
(no) remote-log enable

4. Example:
The following example enables remote logging:

```
switch_a(config)#remote-log enable
switch_a(config)#
```

---

Add Syslog Server:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to enable the logging of messages that are sent to remote syslog servers.

3. Command Syntax:
remote-log add A.B.C.D
A.B.C.D Specifies the IP address of the remote syslog server.

4. Example:
The following example adds a remote syslog server (IP address: **192.168.1.100**) for the switch:

```
switch_a(config)#remote-log add 192.168.1.100
switch_a(config)#
```

---

Delete Syslog Server:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to delete the logging of messages that are sent to remote syslog servers.

3. Command Syntax:

remote-log del A.B.C.D
A.B.C.D Specifies the IP address of the remote syslog server.

4. Example:

The following example deletes a remote syslog server (IP address: **192.168.1.100**) for the switch:

```
switch_a(config)#remote-log del 192.168.1.100
switch_a(config)#
```

---

**ARP TABLE**

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).
The **switch_a#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use **show arp-table** command to view ARP Table.

3. Command Syntax:

show arp-table

4. Example:

The following example shows the ARP Table of switch:

```
switch_a#show arp-table
```

---

**ROUTE TABLE**

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).
The **switch_a#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use **show route-table** command to view Route Table.

3. Command Syntax:

show route-table

4. Example:

The following example shows the Route Table of switch:

```
switch_a#show route-table
```

---

**ALARM SETTING**

Alarm-trigger if:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable or disable alarm trigger on interface.

3. Command Syntax:

(no) alarm-trigger if INTERFACE
INTERFACE specifies the interface.

4. Example:

The following example enables alarm trigger on interface "**fe1**" to switch:

```
switch_a(config)#alarm-trigger if fe1
switch_a(config)#
```

---

Alarm-trigger power:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable or disable alarm trigger of power source.

3. Command Syntax:

(no) alarm-trigger power POWER
POWER specifies the power source.

4. Example:

The following example enables alarm trigger of power "**1**" to switch:

```
switch_a(config)#alarm-trigger power 1
switch_a(config)#
```

## 7.4 PORT

Configuration, Port Status, Rate Control, RMON Statistics, Per Port VLAN Activities

**CONFIGURATION**
Port Name:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use the **portname** command to specify the ascii name of port.
Use the **no portname** to cancel the ascii name of port.

3. Command Syntax:
portname LINE
(no) portname
LINE specifies the ascii name of port.

4. Example:
The following example shows the use of the **portname** command to specify the ascii name **fe1** for the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#portname fe1
switch_a(config-if)#
```

---

Admin Setting:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use the **shutdown** command to shut down the selected interface.
Use the **no shutdown** to disable this function.

3. Command Syntax:
(no) shutdown

4. Example:
The following example shows the use of the **shutdown** command to shut down the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#shutdown
switch_a(config-if)#
```

Duplex:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **duplex** command to specify the duplex mode to be used for each interface.
Use the **no duplex** to disable this function.

3. Command Syntax:
(no) duplex MODE
MODE specifies the duplex mode: auto, full, half.

4. Example:
The following example shows the use of **duplex** MODE (**full**) to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#duplex full
switch_a(config-if)#
```

Flow control:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **flowcontrol on** command to enable flow control, and configure the flow control mode for the port.
Use the **no flowcontrol** to disable this function.

3. Command Syntax:
flowcontrol on
no flowcontrol

4. Example:
The following example shows the use of **flowcontrol on** to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#flowcontrol on
switch_a(config-if)#
```

**PORT STATUS**

Port Status:

1. Command Mode: Exec mode or Privileged Exec mode

Logon to Exec Mode (View Mode) or Privileged Exec Mode (Enable Mode).

The **switch_a>** or **switch_a#** prompt will show on the screen.

```
switch_a>
```

```
switch_a#
```

2. Usage:

Use the **show interface** command to display interface configuration and status.

3. Command Syntax:

show interface IFNAME

IFNAME specifies the name of the interface for which status and configuration information is desired.

4. Example:

The following example shows the use of **show interface** to display interface configuration and status of the interface fe1 (port 1):

```
switch_a>show interface fe1
```

---

Alarm Situation:

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).

The **switch_a#** prompt will show on the screen.

```
switch_a#
```

2. Usage:

Use the **show sfp-alarm-trigger** command to show the information of SFP alarm trigger including temperature, Vcc, Tx_bias, Tx_pow and Rx_pow.

3. Command Syntax:

show sfp-alarm-trigger IFNAME

IFNAME specifies the name of the interface for which status and configuration information is desired.

4. Example:

The following example shows the use of **show sfp-alarm-trigger** to display the information of SFP alarm trigger of the interface ge1 (port G1):

```
switch_a#show sfp-alarm-trigger ge1
```

---

Temperature Alarm (Warning) Threshold:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set temperature alarm (warning) threshold for SFP transceiver.

3. Command Syntax:
sfp set-temp IFNAME high-alarm | high-warning | low alarm | low warning LEVEL
IFNAME specifies the name of the interface for which status and configuration information is desired.
LEVEL Threshold value -128 ~ 128℃.

4. Example:
The following example sets high temperature alarm threshold 100℃ for SFP transceiver of interface ge1 (port G1):

```
switch_a(config)#sfp set-temp ge1 high-alarm 100
switch_a(config)#
```

---

Voltage Alarm (Warning) Threshold:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set voltage alarm (warning) threshold for SFP transceiver.

3. Command Syntax:
sfp set-vcc IFNAME high-alarm | high-warning | low alarm | low warning LEVEL
IFNAME specifies the name of the interface for which status and configuration information is desired.
LEVEL Threshold value 0 ~ 6.55 volts.

4. Example:
The following example sets high voltage alarm threshold 6 volts for SFP transceiver of interface ge1 (port G1):

```
switch_a(config)#sfp set-vcc ge1 high-alarm 6
switch_a(config)#
```

---

Tx-bias Alarm (Warning) Threshold:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set transmitter laser bias alarm (warning) threshold for SFP transceiver.

3. Command Syntax:
sfp set-tx-bias IFNAME high-alarm | high-warning | low alarm | low warning LEVEL
IFNAME specifies the name of the interface for which status and configuration information is desired.
LEVEL Threshold value 0 ~ 131 mA.

4. Example:
The following example sets high transmitter laser bias alarm threshold 131 mA for SFP transceiver of interface ge1 (port G1):

```
switch_a(config)#sfp set-tx-bias ge1 high-alarm 131
switch_a(config)#
```

---

Tx-pow Alarm (Warning) Threshold:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set transmitted output power alarm (warning) threshold for SFP transceiver.

3. Command Syntax:
sfp set-tx-pow IFNAME high-alarm | high-warning | low alarm | low warning LEVEL
IFNAME specifies the name of the interface for which status and configuration information is desired.
LEVEL Threshold value -30 ~ 8.16 dbm.

4. Example:
The following example sets high transmitted output power alarm threshold 8.16 dbm for SFP transceiver of interface ge1 (port G1):

```
switch_a(config)#sfp set-tx-pow ge1 high-alarm 8.16
switch_a(config)#
```

---

Rx-pow Alarm (Warning) Threshold:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set received optical power alarm (warning) threshold for SFP transceiver.

3. Command Syntax:
sfp set-rx-pow IFNAME high-alarm | high-warning | low alarm | low warning LEVEL
IFNAME specifies the name of the interface for which status and configuration information is desired.
LEVEL Threshold value -30 ~ 8.16 dbm.

4. Example:
The following example sets high received optical power alarm threshold 8.16 dbm for SFP transceiver of interface ge1 (port G1):

```
switch_a(config)#sfp set-rx-pow ge1 high-alarm 8.16
switch_a(config)#
```

---

**RATE CONTROL**

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to specify the ingress/egress rate to be used for each interface. The bandwidth value is in bits.
Use the no parameter with this command to remove the ingress/egress rate to be used for each interface.

3. Command Syntax:

(no) rate-control ingress/egress VALUE
VALUE
<1-10000000000 bits> (usable units: k, m, g)
<1-999>klm for 1 to 999 kilo bits or mega bits.
1g for 1 giga bits.

4. Example:

The following example shows the use of rate-control ingress VALUE (**10 mega bits**) to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#rate-control ingress 10m
switch_a(config-if)#
```

---

**RMON STATISTICS**

1. Command Mode: Exec mode or Privileged Exec mode

Logon to Exec Mode (View Mode) or Privileged Exec Mode (Enable Mode).
The **switch_a>** or **switch_a#** prompt will show on the screen.

```
switch_a>
```

```
switch_a#
```

2. Usage:

Use the **show interface statistics** command to display RMON statistics of interface.

3. Command Syntax:

show interface statistics IFNAME
IFNAME specifies the name of the interface for which RMON statistics is desired.

4. Example:

The following example shows the use of **show interface statistics** to display RMON statistics of the interface fe1 (port 1):

```
switch_a>show interface statistics fe1
```

---

**PER PORT VLAN ACTIVITIES**

1. Command Mode: Exec mode or Privileged Exec mode

Logon to Exec Mode (View Mode) or Privileged Exec Mode (Enable Mode).
The **switch_a>** or **switch_a#** prompt will show on the screen.

```
switch_a>
```

```
switch_a#
```

2. Usage:

Use **show vlan** command to display information about a particular VLAN by specifying the VLAN ID.

3. Command Syntax:

show vlan <2-4094>
<2-4094> VLAN ID.

4. Example:

The following is an output of **show vlan** command displaying information about VLAN 2:

```
switch_a>show vlan 2
```

## 7.5 SWITCHING

Bridging, Static MAC Entry, Port Mirroring

**BRIDGING**
Aging Time (seconds):
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to specify an ageing-out time for a learned MAC address. The learned MAC address will persist till this specified time.

3. Command Syntax:
Bridge GROUP ageing-time AGEINGTIME
no bridge GROUP ageing-time
Group = <1-1> The ID of the bridge-group that this ageing time is for.
AGEINGTIME = <10-1000000> The number of seconds of persistence.

4. Example:
The following example sets the new AGEINGTIME (**1000**) to bridge GROUP (**1**):

```
switch_a(config)#bridge 1 ageing-time 1000
switch_a(config)#
```

---

Threshold level (0-100):
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **storm-control level** command to specify the rising threshold level for broadcasting, multicast, or destination lookup failure traffic. The storm control action occurs when traffic utilization reaches this level.

3. Command Syntax:
storm-control level LEVEL
LEVEL <0-100> specifies the percentage of the threshold; percentage of the maximum speed (pps) of the interface.

4. Example:
The following example shows setting **storm-control level** LEVEL (**30**) to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#storm-control level 30
switch_a(config-if)#
```

---

Broadcast:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **storm-control broadcast enable** command to enable broadcast traffic.
Use **no storm-control broadcast** command to disable broadcast traffic.

3. Command Syntax:
storm-control broadcast enable
no storm-control broadcast

4. Example:
The following example shows setting **storm-control broadcast enable** to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#storm-control broadcast enable
switch_a(config-if)#
```

---

Multicast:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **storm-control multicast enable** command to enable multicast traffic.
Use **no storm-control multicast** command to disable multicast traffic.

3. Command Syntax:
storm-control multicast enable
no storm-control multicast

4. Example:
The following example shows setting **storm-control multicast enable** to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#storm-control multicast enable
switch_a(config-if)#
```

---

DLF:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.

fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **storm-control dlf enable** command to enable destination lookup failure traffic.
Use **no storm-control dlf** command to disable destination lookup failure traffic.

3. Command Syntax:
storm-control dlf enable
no storm-control dlf
dlf destination lookup failure

4. Example:
The following example shows setting **storm-control dlf enable** to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#storm-control dlf enable
switch_a(config-if)#
```

---

Port isolation:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **port-isolation enable** command to enable port isolation.
Use **port-isolation disable** command to disable port isolation.

3. Command Syntax:
port-isolation (enable | disable)

4. Example:
The following example enables port-isolation to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#port-isolation enable
switch_a(config-if)#
```

---

**LOOPBACK DETECT**
LoopBack Detect:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable or disable a loopback detection on a port interface.

3. Command Syntax:
bridge GROUP loopback-detect (enable | disable)
GROUP <1-1> Bridge-group ID used for bridging.
enable Enables a loopback detection on a port interface.
disable Disables a loopback detection on a port interface.

4. Example:
The following example enables a loopback detection for bridge GROUP (**1**):

```
switch_a(config)#bridge 1 loopback-detect enable
switch_a(config)#
```

---

LoopBack Detect Action:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to configure action while loopback detected.

3. Command Syntax:
bridge GROUP loopback-detect action (errdisable | none (default))
GROUP <1-1> Bridge-group ID used for bridging.
errdisableEnable error disable LoopBack Detect Action on a port interface.
none Disable error disable LoopBack Detect Action on a port interface.

4. Example:
The following example enables error disable LoopBack Detect Action for bridge GROUP (**1**):

```
switch_a(config)#bridge 1 loopback-detect action errdisable
switch_a(config)#
```

---

Error Disable Recovery:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set the error disable recovery time interval. The range of interval value is from 0 to 65535. And the default value is 0 second (no recovery).

3. Command Syntax:
bridge GROUP loopback-detect errdisable-recovery <0-65535>
GROUP <1-1> Bridge-group ID used for bridging.
<0-65535> The error disable recovery time in seconds.

4. Example:
The following example sets error disable recovery time 1 second for bridge GROUP (**1**):

```
switch_a(config)#bridge 1 loopback-detect errdisable-recovery 1
switch_a(config)#
```

---

Interval:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set the loopback detect interval time. The range of interval value is from 1 to 65535. And the default value is 1 second.

3. Command Syntax:
bridge GROUP loopback-detect interval <1-65535>
GROUP <1-1> Bridge-group ID used for bridging.
<1-65535> The loopback detect interval time in seconds.

4. Example:
The following example sets loopback detect interval time 10 seconds for bridge GROUP (**1**):

```
switch_a(config)#bridge 1 loopback-detect interval 10
switch_a(config)#
```

---

Loopback Detect (Port Interface):
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to enable loopback detect for port interface.
Use the no parameter with this command to disable loopback detect for port interface.

3. Command Syntax:
loopback-detect port enable
no loopback-detect port enable

4. Example:
The following example enables loopback detect for port fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#loopback-detect port enable
switch_a(config-if)#
```

---

**STATIC MAC ENTRY**

Static-MAC-Entry Forward:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to statically configure a bridge entry to forward matching frames.

3. Command Syntax:

bridge GROUP address MAC forward IFNAME VLANID

no bridge GROUP address MAC forward IFNAME VLANID

GROUP <1-1> Bridge-group ID used for bridging.

MAC the Media Access Control (MAC) address in the HHHH.HHHH.HHHH format.

IFNAME the interface on which the frame comes in.

VLANID The VID of the VLAN that will be enabled or disabled on the bridge <2-4094>.

4. Example:

The following example configures a bridge GROUP (**1**) to forward matching frames (MAC address **2222.2222.2222**) to the interface fe1 (port 1) in vlan VLANID (**2**):

```
switch_a(config)#bridge 1 address 2222.2222.2222 forward fe1 vlan 2
switch_a(config)#
```

---

Static-MAC-Entry Discard:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to statically configure a bridge entry to discard matching frames in a particular VLAN.

3. Command Syntax:

bridge GROUP address MAC discard vlan VLANID

no bridge GROUP address MAC discard vlan VLANID

GROUP <1-1> Bridge-group ID used for bridging.

MAC the Media Access Control (MAC) address in the HHHH.HHHH.HHHH format.

VLANID The VID of the VLAN on the bridge <1-4094>.

4. Example:

The following example configures a bridge GROUP (**1**) to discard matching frames (MAC address **2222.2222.2222**) in vlan VLANID (**1**):

```
switch_a(config)#bridge 1 address 2222.2222.2222 discard vlan 1
switch_a(config)#
```

---

**PORT MIRRORING**

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to define a mirror source port and its direction.
Use the no parameter with this command to disable port mirroring by the destination port on the specified source port.

3. Command Syntax:

mirror interface SOURCEPORT direction SNOOPDIRECTION
no mirror interface SOURCEPORT
SOURCEPORT Name of the Source interface to be used.
SNOOPDIRECTION [both|receive|transmit]
both Specifies mirroring of traffic in both directions.
receive Specifies mirroring of received traffic.
transmit Specifies mirroring of transmitted traffic.

4. Example:

The following example enables port mirroring by the destination port fe1 (port 1) on the specified source port fe2 (port 2):

```
switch_a(config)#interface fe1
switch_a(config-if)#mirror interface fe2 direction both
switch_a(config-if)#
```

**LINK STATE TRACKING**

Group Setting:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable link state tracking for the group.
Use the no parameter with this command to disable link state tracking for the group.

3. Command Syntax:

(no) link state track <1-10>
<1-10> Link state group number.

4. Example:

The following example enables link state tracking for the group 1:

```
switch_a(config)#link state track 1
switch_a(config)#
```

Port Setting:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to enable link state tracking for the port.
Use the no parameter with this command to disable link state tracking for the port.

3. Command Syntax:
(no) link state group <1-10> (downstream | upstream)
<1-10> Link state group number.

4. Example:
The following example enables downstream link state tracking of port fe1 (port 1) for the group 1:

```
switch_a(config)#interface fe1
switch_a(config-if)# link state group 1 downstream
switch_a(config-if)#
```

---

**POE (FOR POE MODEL)**
System Power Budget:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to specify the power budget (Watts) to be set to Switch.

3. Command Syntax:
poe system-power-budget LEVEL
LEVEL <1-800> specifies the power budget (Watts) to be set to Switch.

4. Example:
The following example sets new power budget 246 Watts to Switch:

```
switch_a(config)#poe system-power-budget 246
switch_a(config)#
```

---

Enable Mode:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **poe enable** command to enable this port to discover Powered Device (PD) connected to this port.
Use the **no poe enable** to disable this function.

3. Command Syntax:
(no) poe enable

4. Example:
The following example shows the use of **poe enable** to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#poe enable
switch_a(config-if)#
```

---

Power Limit by Classification:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **poe power-classification enable** command to enable this port to provide power to PD according to classification of maximum power range used by PD.
Use the **no poe power-classification enable** to disable this function.

3. Command Syntax:
(no) poe power-classification enable

4. Example:
The following example shows the use of **poe power-classification enable** to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#poe power-classification enable
switch_a(config-if)#
```

---

Fixed Power Limit (W):
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to specify the fixed power limit for this port to provide power to PD.

3. Command Syntax:
poe fixed-power-limit LEVEL
LEVEL <1-15.4> specifies the fixed power limit (Watts) for this port to provide power to PD.

4. Example:
The following example sets new fixed power limit 15 Watts to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#poe fixed-power-limit 15
switch_a(config-if)#
```

Power Priority:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to specify the power priority to this port.

3. Command Syntax:
poe power-priority PRIORITY
PRIORITY specifies high, medium, low power priority for this port.

4. Example:
The following example sets **high** power priority to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#poe power-priority high
switch_a(config-if)#
```

Power Down Alarm:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **poe power-down-alarm enable** command to enable power down alarm to this port.
Use the **no poe power-classification enable** to disable this function.

3. Command Syntax:
(no) poe power-down-alarm enable

4. Example:
The following example shows the use of **poe power-down-alarm enable** to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#poe power-down-alarm enable
switch_a(config-if)#
```

**POE SCHEDULING (FOR POE MODEL)**

PoE Schedule:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to enble PoE scheduling to this port.

3. Command Syntax:

poe scheduling enable

4. Example:

The following example enables PoE scheduling to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#poe scheduling enable
switch_a(config-if)#
```

---

PoE Schedule:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to set PoE scheduling to this port.

3. Command Syntax:

poe schedule-time DAY HOUR
DAY <0-6> specifies Sunday ~ Saturday to Switch.
HOUR <0-23> specifies hours to Switch.
no poe schedule-time DAY

4. Example:

The following example sets PoE scheduling to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#poe schedule-time 3 0-10,12,14-20, 22-23
switch_a(config-if)#
```

## 7.6 TRUNKING

Port Trunking, LACP Trunking

**PORT TRUNKING**

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use **static-channel-group** command to create a static aggregator, or add a member port to an already-existing static aggregator.
Use the **no static-channel-group** command to detach the port from the static aggregator.

3. Command Syntax:

static-channel-group <1-8>
no static-channel-group
<1-8> Channel group number.
Maximum 8 ports in static-channel-group 1 to 6.
Maximum 4 ports in static-channel-group 7 and 8.

4. Example:

The following example adding the interface fe1 (port 1) to **static-channel-group 1**:

```
switch_a(config)#interface fe1
switch_a(config-if)#static-channel-group 1
switch_a(config-if)#
```

---

**LACP TRUNKING**

Static Channel Group:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use **static-channel-group** command to create a static aggregator, or add a member port to an already-existing static aggregator.
Use the **no static-channel-group** command to detach the port from the static aggregator.

3. Command Syntax:

static-channel-group <1-8>
no static-channel-group
<1-8> Channel group number.
Maximum 8 ports in static-channel-group 1 to 6.
Maximum 4 ports in static-channel-group 7 and 8.

4. Example:
The following example adding the interface fe1 (port 1) to **static-channel-group 1**:

```
switch_a(config)#interface fe1
switch_a(config-if)#static-channel-group 1
switch_a(config-if)#
```

---

Channel Group:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **channel-group** command to add a port to a channel group specified by the channel group number (<1 | 3>). This command enables link aggregation on a port, so that it may be selected for aggregation by the local system.
Use the **no channel-group** command to turn off link aggregation on a port.

3. Command Syntax:
channel-group <1 | 3> mode MODE
no channel-group
<1 | 3> Channel group number.
1 Channel group number 1 for FE ports.
3 Channel group number 3 for GE ports.
Maximum 4 ports in channel-group 1.
Maximum 4 ports in channel-group 3.
MODE
active Enable initiation of LACP negotiation on a port.
passive Disable initiation of LACP negotiation on a port.

4. Example:
The following example enalbes initiation of LACP negotiation on the interface fe1 (port 1) to **channel-group 1**:

```
switch_a(config)#interface fe1
switch_a(config-if)#channel-group 1 mode active
switch_a(config-if)#
```

---

Clear LACP Counters:
1. Command Mode: Privileged Exec mode
Logon to Privileged Exec Mode (Enable Mode).
The **switch_a#** prompt will show on the screen.

```
switch_a#
```

2. Usage:
Use this command to clear all counters of all present LACP aggregators or a given LACP aggregator.

3. Command Syntax:

clear lacp (<1-65535>) counters
<1-65535> Channel-group number.

4. Example:
The following example clears all counters of LACP channel group 1:

```
switch_a#clear lacp 1 counters
switch_a#
```

---

LACP Port Priority:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **lacp port-priority** command to set the priority of a channel. Channels are selected for aggregation based on their priority with the higher priority (numerically lower) channels selected first.
Use the **no lacp port-priority** command to reset the priority of port to the default value (32768).

3. Command Syntax:
lacp port-priority <1-65535>
no lacp port-priority
<1-65535> Specify the LACP port priority.

4. Example:
The following example sets the LACP port priority **34** of interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#lacp port-priority 34
switch_a(config-if)#
```

---

LACP Timeout:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **lacp timeout** command to set the short or long timeout on a port. The default is long timeout

3. Command Syntax:
lacp timeout shor | long
timeout Number of seconds before invalidating a received LACP data unit (DU).
short LACP short timeout. Short timeout value is 3 seconds.
long LACP long timeout. Long timeout value is 90 seconds.

4. Example:
The following example sets the LACP short timeout on interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#lacp timeout short
switch_a(config-if)#
```

---

LACP System Priority:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **lacp system-priority** command to set the system priority of a local system. This is used in determining the system responsible for resolving conflicts in the choice of aggregation groups. Note: Lower numerical values have higher priorities.
Use **no lacp system-priority** command to reset the system priority of the local system to the default value (32768).

3. Command Syntax:
lacp system-priority <1-65535>
no lacp system-priority
<1-65535> LACP system priority. The default system priority is 32768.

4. Example:
The following example sets the LACP system priority **6700**:

```
switch_a(config)#lacp system-priority 6700
switch_a(config)#
```

## 7.7 STP / RING

Global Configuration, RSTP Port Setting, MSTP Properties, MSTP Instance Setting, MSTP Port Setting, Ring Setting, Chain Setting, Chain Pass-Through Setting, Advanced Setting

**GLOBAL CONFIGURATION**

STP Version:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to choose the Spanning Tree protocol, Rapid Spanning Tree protocol, or Multiple Spanning Tree protocol on a bridge.

3. Command Syntax:

bridge GROUP protocol PROTOCOL vlan-bridge
GROUP <1-1> Bridge group name used for bridging.
PROTOCOL
ieee IEEE 802.1Q spanning-tree protocol.
mstp IEEE 802.1s multiple spanning-tree protocol.
rstp IEEE 802.1w rapid spanning-tree protocol.

4. Example:

The following example chooses the PROTOCOL (**rstp**) on bridge GROUP (**1**):

```
switch_a(config)#bridge 1 protocol rstp vlan-bridge
switch_a(config)#
```

---

Multiple Spanning Tree Protocol:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable the Multiple Spanning Tree protocol on a bridge.
Use the no form of the command to disable the Multiple Spanning Tree protocol on a bridge.

3. Command Syntax:

bridge GROUP multiple-spanning-tree enable
no bridge GROUP multiple-spanning-tree enable BRIDGE-FORWARD
GROUP <1-1> Bridge group name used for bridging.
BRIDGE-FORWARD Puts all ports of the specified bridge into the forwarding state.

4. Example:

The following example enables or disables the **multiple-spanning-tree** on bridge GROUP (**1**):

```
switch_a(config)#bridge 1 multiple-spanning-tree enable
switch_a(config)#no bridge 1 multiple-spanning-tree enable bridge-forward
switch_a(config)#
```

---

Rapid Spanning Tree Protocol:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to enable the Rapid Spanning Tree protocol on a bridge.
Use the no form of the command to disable the Rapid Spanning Tree protocol on a bridge.

3. Command Syntax:
bridge GROUP rapid-spanning-tree enable
no bridge GROUP rapid-spanning-tree enable BRIDGE-FORWARD
GROUP <1-1> Bridge group name used for bridging.
BRIDGE-FORWARD Puts all ports of the specified bridge into the forwarding state.

4. Example:
The following example enables or disables the **rapid-spanning-tree** on bridge GROUP (**1**):

```
switch_a(config)#bridge 1 rapid-spanning-tree enable
switch_a(config)#no bridge 1 rapid-spanning-tree enable bridge-forward
switch_a(config)#
```

---

Spanning Tree Protocol:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to enable the Spanning Tree protocol on a bridge.
Use the no form of the command to disable the Spanning Tree protocol on a bridge.

3. Command Syntax:
bridge GROUP spanning-tree enable
no bridge GROUP spanning-tree enable BRIDGE-FORWARD
GROUP <1-1> Bridge group name used for bridging.
BRIDGE-FORWARD Puts all ports of the specified bridge into the forwarding state.

4. Example:
The following example enables or disables the **spanning-tree** on bridge GROUP (**1**):

```
switch_a(config)#bridge 1 spanning-tree enable
switch_a(config)#no bridge 1 spanning-tree enable bridge-forward
switch_a(config)#
```

---

Bridge Priority (0..61440):
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set bridge priority for the common instance. Using a lower priority indicates a greater likelihood of the bridge becoming root.

3. Command Syntax:
bridge GROUP priority PRIORITY
no bridge GROUP priority
GROUP <1-1> The ID of the bridge group for which the priority is set.
PRIORITY <0-61440> The bridge priority.

4. Example:
The following example sets the **priority** PRIORITY (**4096**) of bridge GROUP (**1**):

```
switch_a(config)#bridge 1 priority 4096
switch_a(config)#
```

---

Hello Time (sec) (1..9):
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set the hello-time, the time in seconds after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs).

3. Command Syntax:
bridge GROUP hello-time HELLOTIME
no bridge GROUP hello-time
GROUP <1-1> The ID of the bridge group to which this hello time is assigned.
HELLOTIME <1-9> The hello BPDU interval in seconds.

4. Example:
The following example sets the **hello-time** HELLOTIME (**9**) of bridge GROUP (**1**):

```
switch_a(config)#bridge 1 hello-time 9
switch_a(config)#
```

---

Max Age (sec) (6..28):
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set the max-age for a bridge.
Use the no parameter with this command to restore the default value of max-age.

3. Command Syntax:
bridge GROUP max-age MAXAGE
no bridge GROUP max-age
GROUP <1-1> The ID of the bridge group to which this maximum age time is assigned.
MAXAGE <6-28> The maximum time, in seconds, to listen for the root bridge.

4. Example:
The following example sets the **max-age** MAXAGE (**28**) of bridge GROUP (**1**):

```
switch_a(config)#bridge 1 max-age 28
switch_a(config)#
```

---

Forward Delay (sec) (4..30):
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding.
Use the no parameter with this command to restore the default value.

3. Command Syntax:
bridge GROUP forward-time FORWARD_DELAY
no bridge GROUP forward-time
GROUP <1-1> The ID of the bridge group to which this delay time is assigned.
FORWARD_DELAY <4-30> the forwarding time delay in seconds.

4. Example:
The following example sets the **forward-time** FORWARD_DELAY (**30**) of bridge GROUP (**1**):

```
switch_a(config)#bridge 1 forward-time 30
switch_a(config)#
```

---

**RSTP PORT SETTING**
Priority(Granularity 16):
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to set the port priority for a bridge. The lower priority indicates a greater likelihood of the bridge becoming root.

3. Command Syntax:
bridge GROUP priority PRIORITY
GROUP <1-1> the ID of the bridge group.
PRIORITY <0-240> The priority to be assigned to the group.

4. Example:
The following example sets the priority PRIORITY (**100**) of the interface fe1 (port 1) of bridge GROUP (**1**):

```
switch_a(config)#interface fe1
switch_a(config-if)#bridge 1 priority 100
switch_a(config-if)#
```

Admin. Path Cost:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to set the cost of a path associated with a bridge-group.
Use the no parameter with this command to restore the default cost of a path associated with a bridge-group.

3. Command Syntax:
bridge GROUP path-cost PATHCOST
no bridge GROUP path-cost
GROUP <1-1> the ID of the bridge group.
PATHCOST <1-200000000> The cost to be assigned to the group.

4. Example:
The following example sets the cost (**123**) of the interface fe1 (port 1) of bridge GROUP (**1**):

```
switch_a(config)#interface fe1
switch_a(config-if)#bridge 1 path-cost 123
switch_a(config-if)#
```

Point to Point Link:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **spanning-tree link-type** command to set the link type of a port to enable or disable rapid transition.
Use the **no spanning-tree link-type** command to set a port to its default state and to disable rapid transition.

3. Command Syntax:
(no) spanning-tree link-type LINKTYPE
LINKTYPE The link type to be assigned to the port.
point-to-point Enable rapid transition.
shared Disable rapid transition.

4. Example:
The following example sets the link-type LINKTYPE (**point-to-point**) of the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#spanning-tree link-type point-to-point
switch_a(config-if)#
```

Autoedge:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **spanning-tree autoedge** command to assist in automatic identification of the edge port.
Use the **no spanning-tree autoedge** command to disable this feature.

3. Command Syntax:
(no) spanning-tree autoedge

4. Example:
The following example enables the **spanning-tree autoedge** of the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#spanning-tree autoedge
switch_a(config-if)#
```

Edgeport:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **spanning-tree edgeport** command to set a port as an edge-port and to enable rapid transitions.
Use the **no spanning-tree edgeport** command to set a port to its default state (not an edge-port) and to disable rapid transitions.

3. Command Syntax:
(no) spanning-tree edgeport

4. Example:
The following example enables the **spanning-tree edgeport** of the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#spanning-tree edgeport
switch_a(config-if)#
```

**MSTP PROPERTIES**
Region Name:
1. Command Mode: MST Configuration mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to MST Configuration mode.
The **switch_a(config-mst)#** prompt will show on the screen.

```
switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#
```

2. Usage:
Use this command to create an MST region and specify a name to it. MST bridges of a region form different spanning trees for different VLANs. By default, each MST bridge starts with the region name as its bridge address. This means each MST bridge is a region by itself, unless specifically added to one.

3. Command Syntax:
bridge GROUP region REGION_NAME
no bridge GROUP region
GROUP <1-1> Specify the bridge-group ID.
REGION_NAME Specify the name of the region.

4. Example:
The following example creates an MST region and specifies a name (**regionname**) to it in bridge GROUP (**1**):

```
Switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#bridge 1 region regionname
switch_a(config-mst)#
```

---

Revision Level:
1. Command Mode: MST Configuration mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to MST Configuration mode.
The **switch_a(config-mst)#** prompt will show on the screen.

```
switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#
```

2. Usage:
Use this command to specify the number for configuration information. The default value of revision number is 0.

3. Command Syntax:
bridge GROUP revision REVISION_NUM
GROUP <1-1> Specify the bridge-group ID.
REVISION_NUM <0-255> Revision number.

4. Example:
The following example specifies a revision number (**25**) of MST configuration in bridge GROUP (**1**):

```
switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#bridge 1 revision 25
switch_a(config-mst)#
```

---

Max Hops:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to specify the maximum allowed hops for BPDU in an MST region. This parameter is used by all the instances of the MST. Specifying the max hops for a BPDU prevents the messages from looping indefinetely in the network. When a bridge receives a MST BPDU that has exceeded the allowed max-hops, it discards the BPDU.

3. Command Syntax:
bridge GROUP max-hops HOP_COUNT
no bridge GROUP max-hops
GROUP <1-1> Specify the bridge-group ID.
HOP_COUNT Maximum hops the BPDU will be valid for.

4. Example:
The following example specifies the maximum allowed hops (**25**) for BPDU in bridge GROUP (**1**):

```
switch_a(config)#bridge 1 max-hops 25
switch_a(config)#
```

---

**MSTP INSTANCE SETTING**
Bridge Instance VLAN:
1. Command Mode: MST Configuration mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to MST Configuration mode.
The **switch_a(config-mst)#** prompt will show on the screen.

```
switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#
```

2. Usage:
Use this command to simultaneously add multiple VLANs for the corresponding instance of a bridge. This command can be used only after the VLANs are defined. Use the no parameter with this command to simultaneously remove multiple VLANs for the corresponding instance of a bridge.

3. Command Syntax:
bridge GROUP instance INSTANCE_ID vlan VLAN_ID
no bridge GROUP instance INSTANCE_ID vlan VLAN_ID
GROUP <1-1> Specify the bridge-group ID.
INSTANCE_ID <1-15> Specify the instance ID.
VLAN_ID <1-4094> Specify multiple VLAN IDs corresponding to the bridge instance

4. Example:
The following example associates multiple VLANs (**10**) and (**20**) to instance (**1**) of bridge GROUP (**1**):

```
switch_a(config)#bridge 1 protocol mstp
switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#bridge 1 instance 1 vlan 10, 20
switch_a(config-mst)#
```

---

Bridge Instance Priority:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the bridge priority for an MST instance to the value specified. Use the no parameter with this command to restore the default value of the bridge priority. The lower the priority of the bridge, the better the chances are the bridge becoming a root bridge or a designated bridge for the LAN. The priority values can be set only in increments of 4096.

3. Command Syntax:
bridge GROUP instance INSTANCE_ID priority BRIDGE_PRIORITY
no bridge GROUP instance INSTANCE_ID priority
GROUP <1-1> Specify the bridge-group ID.
INSTANCE_ID Specify the instance ID.
BRIDGE_PRIORITY <0-61440> Specify the bridge priority.

4. Example:
The following example sets the bridge priority (**0**) for an MST instance (**3**) in bridge GROUP (**1**):

```
switch_a(config)#bridge 1 instance 3 priority 0
switch_a(config)#
```

---

**MSTP PORT SETTING**
Bridge-Group Instance:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to assign a Multiple Spanning Tree instance to a port. Use the no parameter with this command to remove the instance.

3. Command Syntax:
bridge GROUP instance INSTANCE_ID
no bridge GROUP instance INSTANCE_ID
GROUP <1-1> Specify the bridge-group ID.
INSTANCE_ID Specify the instance ID.

4. Example:
The following example assigns a Multiple Spanning Tree instance (**3**) to a port (**fe1**) in bridge GROUP (**1**):

```
switch_a(config)#interface fe1
switch_a(config-if)#bridge-group 1 instance 3
switch_a(config-if)#
```

---

Bridge-Group Instance Priority:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to set the port priority for a bridge group. The Multiple Spanning Tree Protocol uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies a better priority. In the case of the same priority, the interface index will serve as the tiebreaker, with the lower-numbered interface being preferred over others. The permitted range is 0-240. The priority values can only be set in increments of 16.

3. Command Syntax:
bridge GROUP instance INSTANCE_ID priority PRIORITY
GROUP <1-1> Specify the bridge-group ID.
INSTANCE_ID <1-15> Specify the instance ID.
PRIORITY <0-240> Specify the port priority in a range of <0-240>.

4. Example:
The following example sets the port priority (**121**) for Multiple Spanning Tree instance (**3**) to a port (**fe1**) in bridge GROUP (**1**):

```
switch_a(config)#interface fe1
switch_a(config-if)#bridge-group 1 instance 3 priority 121
switch_a(config-if)#
```

---

Bridge-Group Instance Path-Cost:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to set the cost of a path associated with an interface. Use the no parameter with this command to restore the default cost value of the path. A lower path-cost indicates a greater likelihood of the specific interface becoming a root.

3. Command Syntax:
bridge GROUP instance INSTANCE_ID path-cost PATH_COST
GROUP <1-1> Specify the bridge-group ID.
INSTANCE_ID <1-15> Specify the instance ID.
PATH_COST <1-200000000> Specify the cost of path in the range of <1-200000000>.

4. Example:
The following example sets the path cost (**1000**) for Multiple Spanning Tree instance (**3**) to a port (**fe1**) in bridge GROUP (**1**):

```
switch_a(config)#interface fe1
switch_a(config-if)#bridge-group 1 instance 3 path-cost 1000
switch_a(config-if)#
```

---

**RING SETTING**

Ring state:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable Ring state. Use the no parameter with this command to disable Ring state.

3. Command Syntax:

bridge GROUP protocol ring

no bridge GROUP ring enable BRIDGE-FORWARD

GROUP <1-1> Specify the bridge-group ID.

BRIDGE-FORWARD Puts all ports of the specified bridge into the forwarding state.

4. Example:

The following example enables Ring state in bridge GROUP (**1**):

```
switch_a(config)#bridge 1 protocol ring
switch_a(config)#
```

---

Set ring port:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set Ring port 1 and Ring port 2.

3. Command Syntax:

ring set-port RING_PORT_1 RING_PORT_2

RING_PORT_1 Specify the Ring port 1.

RING_PORT_2 Specify the Ring port 2.

4. Example:

The following example sets the fe1 and fe2 as Ring port 1 and Ring port 2:

```
switch_a(config)#ring set-port fe1 fe2
switch_a(config)#
```

---

Ring-coupling state:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).

The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable Ring-coupling state. Use the no parameter with this command to disable Ring-coupling state.

3. Command Syntax:
(no) ring-coupling enable

4. Example:
The following example enables Ring-coupling state:

```
switch_a(config)#ring-coupling enable
switch_a(config)#
```

---

Set ring-coupling port:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set Ring-coupling port 1 and Ring-coupling port 2.

3. Command Syntax:
ring set-coupling-port COUPLING_PORT_1 COUPLING_PORT_2
COUPLING_PORT_1 Specify the Ring-coupling port 1.
COUPLING_PORT_2 Specify the Ring-coupling port 2.

4. Example:
The following example sets the fe3 and fe4 as Ring-coupling port 1 and Ring-coupling port 2:

```
switch_a(config)#ring set-coupling-port fe3 fe4
switch_a(config)#
```

---

**CHAIN SETTING**
Chain Protocol:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to set Chain Protocol to an interface. Use the no parameter with this command to revoke Chain Protocol from an interface.

3. Command Syntax:
chain port enable
no chain port

4. Example:
The following example sets Chain Protocol to the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#chain port enable
switch_a(config-if)#
```

VLAN:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set the Switch priority for running chain protocol. Switch with lower priority will run as Master (forwarding) port. Use the no form of the command to restore default value (1).

3. Command Syntax:
bridge <1-1> chain-vlan <1-4094>
no bridge <1-1> chain-vlan
<1-1> Bridge Group name for bridging.
<1-4094> The VID of the VLAN for chain on the bridge <1-4094>.

4. Example:
The following example sets VLAN ID (**1**) for chain on bridge GROUP (**1**):

```
switch_a(config)#bridge 1 chain-vlan 1
switch_a(config)#
```

Chain Priority:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set the Switch priority for running chain protocol. Switch with lower priority will run as Master (forwarding) port. Use the no form of the command to restore default value (128).

3. Command Syntax:
bridge GROUP chain-priority <0-255>
no bridge GROUP chain-priority
Group = <1-1> Bridge Group name for bridging.
<0-255> The Switch priority for running chain protocol.

4. Example:
The following example sets the new Switch priority (**10**) to bridge GROUP (**1**):

```
switch_a(config)#bridge 1 chain-priority 10
switch_a(config)#
```

Chain Timeout:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set the Switch timeout count for running chain protocol. Chain recovery time = (Chain Timeout Count – 1) x 200ms.
Use the no form of the command to restore default value (5).
Default Chain recovery time = (5 – 1) x 200ms = 800ms.

3. Command Syntax:
bridge GROUP chain-timeout <3-255>
no bridge GROUP chain-timeout
Group = <1-1> Bridge Group name for bridging.
<3-255> The Switch timeout count for running chain protocol.

4. Example:
The following example sets the new Switch timeout (**10**) to bridge GROUP (**1**):

```
switch_a(config)#bridge 1 chain-timeout 10
switch_a(config)#
```

---

Storm Control:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to enable Storm Control (broadcast and multicast) for Chain Protocol setting. Use the no form of the command to disable Storm Control (broadcast and multicast) for Chain Protocol setting.

3. Command Syntax:
bridge GROUP chain-storm enable
no bridge GROUP chain-storm
Group = <1-1> Bridge Group name for bridging.

4. Example:
The following example enables chain storm control for bridge GROUP (**1**):

```
switch_a(config)#bridge 1 chain-storm enable
switch_a(config)#
```

---

Chain Pass-Through Setting
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set chain pass-through port 1 and chain pass-through port 2.

3. Command Syntax:
chain pass-through IFNAME IFNAME
no chain pass-through
IFNAME Chain pass-through port number 1.

IFNAME Chain pass-through port number 2.

4. Example:
The following example enables the fe3 and fe4 as chain pass-through port 1 and chain pass-through port 2:

```
switch_a(config)#chain pass-through fe3 fe4
switch_a(config)#
```

---

**ADVANCED SETTING**
Advanced Bridge Configuration:
Bridge bpdu-guard configuration:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to enable the BPDU (Bridge Protocol Data Unit) Guard feature on a bridge.
Use the no parameter with this command to disable the BPDU Guard feature on a bridge.
When the BPDU Guard feature is set for a bridge, all portfast-enabled ports of the bridge that have bpdu-guard set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed.

3. Command Syntax:
bridge GROUP spanning-tree portfast bpdu-guard
no bridge GROUP spanning-tree portfast bpdu-guard
GROUP <1-1> Bridge-group ID used for bridging.

4. Example:
The following example enables the BPDU Guard feature on bridge GROUP (**1**):

```
switch_a(config)#bridge 1 spanning-tree portfast bpdu-guard
switch_a(config)#
```

---

Error disable timeout configuration:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to enable the timeout mechanism for the port to be enabled back for a bridge.
Use the no parameter with this command to disable the timeout mechanism for the port to be enabled back for a bridge.

3. Command Syntax:
bridge GROUP spanning-tree errdisable-timeout enable
no bridge GROUP spanning-tree errdisable-timeout enable
GROUP <1-1> Bridge-group ID used for bridging.

4. Example:

The following example enables the timeout mechanism for the port to be enabled back for bridge GROUP (**1**):

```
switch_a(config)#bridge 1 spanning-tree errdisable-timeout enable
switch_a(config)#
```

---

Interval:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to specify the time interval after which a port is brought back up. The range of interval value is from 10 to 1000000. And the default value is 300 seconds.

3. Command Syntax:

bridge GROUP spanning-tree errdisable-timeout interval <10-1000000>
no bridge GROUP spanning-tree errdisable-timeout interval
GROUP <1-1> Bridge-group ID used for bridging.
<10-1000000> The error disable timeout interval in seconds.

4. Example:

The following example sets error disable timeout interval time 100 seconds for bridge GROUP (**1**):

```
switch_a(config)#bridge 1 spanning-tree errdisable-timeout interval 100
switch_a(config)#
```

---

Advanced Per Port Configuration:
Portfast configuration / status:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to set a port as an edge-port and to enable rapid transitions.
Use the no parameter with this command to set a port to its default state (not an edge-port) and to disable rapid transitions.

3. Command Syntax:

spanning-tree portfast
no spanning-tree portfast

4. Example:

The following example sets the interface fe1 (port 1) as an edge-port and to enable rapid transitions:

```
switch_a(config)#interface fe1
switch_a(config-if)# spanning-tree portfast
switch_a(config-if)#
```

Bpdu-guard configuration:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to enable or disable the BPDU Guard feature on a port.
Use the no parameter with this command to set the BPDU Guard feature on a port to default.
This command supersedes the bridge level configuration for the BPDU Guard feature. When the enable or disable parameter is used with this command, this configuration takes precedence over bridge configuration. However, when the default parameter is used with this command, the bridge level BPDU-Guard configuration takes effect.

3. Command Syntax:

spanning-tree portfast bpdu-guard (enable | disable | default)
no spanning-tree portfast bpdu-guard

4. Example:

The following example enables the BPDU Guard feature on the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)# spanning-tree portfast bpdu-guard enable
switch_a(config-if)#
```

## 7.8 VLAN

VLAN Mode Setting, 802.1Q VLAN Setting, 802.1Q Port Setting, Port Based VLAN

**802.1Q VLAN SETTING**

VLAN Database:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use **vlan database** command to enter the VLAN configuration mode.

3. Command Syntax:

vlan database

4. Example:

The following example changes to VLAN configuration mode from Configure mode:

```
switch_a(config)#vlan database
switch_a(config-vlan)#
```

---

Add VLAN/Delete VLAN:

1. Command Mode: VLAN Configure mode

Logon to Configure Mode (Configure Terminal Mode).
Logon to VLAN Configure Mode.
The **switch_a(config-vlan)#** prompt will show on the screen.

```
switch_a(config)#vlan database
switch_a(config-vlan)#
```

2. Usage:

This command enables or disables the state of a particular VLAN on a bridge basis. Specifying the disable state causes all forwarding over the specified VLAN ID on the specified bridge to cease. Specifying the enable state allows forwarding of frames on the specified VLAN-aware bridge.

3. Command Syntax:

vlan VLANID bridge GROUP name VLAN_NAME state enable/disable
no vlan VLANID bridge GROUP
VLANID The VID of the VLAN that will be enabled or disabled on the bridge <2-4094>.
GROUP <1-1> The ID of the bridge-group on which the VLAN will be affected.
VLAN_NAME The ASCII name of the VLAN. Maximum length: 16 characters.
enable Sets VLAN into an enable state.
disable Sets VLAN into a disable state.

4. Example:

The following example enables the vlan VLANID (**2**) and name VLAN_NAME (**vlan2**) of bridge GROUP (**1**):

```
switch_a(config-vlan)#vlan 2 bridge 1 name vlan2 state enable
switch_a(config-vlan)#
```

---

**802.1Q PORT SETTING**

Switchport mode access:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use **switchport mode access** command to set the switching characteristics of the Layer-2 interface to access mode, and classify untagged frames only.
Use the **no switchport access** command to reset the mode of the Layer-2 interface to access (default).

3. Command Syntax:

switchport mode access
no switchport access

4. Example:

The following example sets the **switchport mode access** of the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#switchport mode access
switch_a(config-if)#
```

---

Switchport mode hybrid:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use **switchport mode hybrid** command to set the switching characteristics of the Layer-2 interface as hybrid, and classify both tagged and untagged frames.
Use the **no switchport hybrid** command to reset the mode of the Layer-2 interface to access (default).

3. Command Syntax:

switchport mode hybrid
switchport mode hybrid acceptable-frame-type all/vlan-tagged
no switchport hybrid
all Set all frames can be received.
vlan-tagged Set vlan-tagged frames can only be received.

4. Example:

The following example sets the **switchport mode hybrid** of the interface fe1 (port 1) and all frames to be received on interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#switchport mode hybrid acceptable-frame-type all
switch_a(config-if)#
```

Switchport mode trunk:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **switchport mode trunk** command to set the switching characteristics of the Layer-2 interface as trunk, and specify only tagged frames.
Use the **no switchport trunk** command to reset the mode of the Layer-2 interface to access (default).

3. Command Syntax:
switchport mode trunk
no switchport trunk

4. Example:
The following example sets the **switchport mode trunk** of the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#switchport mode trunk
switch_a(config-if)#
```

Switchport hybrid allowed vlan:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to set the switching characteristics of the Layer-2 interface to hybrid. Both tagged and untagged frames will be classified over hybrid interfaces.
Use the no parameter to turn off allowed hybrid switching.

3. Command Syntax:
switchport hybrid allowed vlan all
switchport hybrid allowed vlan none
switchport hybrid allowed vlan add VLANID egress-tagged enable/disable
switchport hybrid allowed vlan remove VLANID
no switchport hybrid vlan
all Allow all VLANs to transmit and receive through the Layer-2 interface.
none Allow no VLANs to transmit and receive through the Layer-2 interface.
add Add a VLAN to the member set.
remove Remove a VLAN from the member set.
VLANID <2-4094> The ID of the VLAN or VLANs that will be added to, or removed from, the Layer-2 interface.

For a VLAN range, specify two VLAN numbers: lowest, then highest number in the range, separated by a hyphen.
For a VLAN list, specify the VLAN numbers separated by commas.
egress-tagged
enable Enable the egress tagging for the outgoing frames.
disable Disable the egress tagging for the outgoing frames.

4. Example:
The following example specifies to **add** the interface fe1 (port 1) to VLANID (**2**) and **enable** the **egress-tagged** for the outgoing frames on interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#switchport hybrid allowed vlan add 2 egress-tagged enable
switch_a(config-if)#
```

---

Switchport trunk allowed vlan:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to set the switching characteristics of the Layer-2 interface to trunk. The all parameter indicates that any VLAN ID is part of its port's member set. The none parameter indicates that no VLAN ID is configured on this port. The add and remove parameters will add and remove VLAN IDs to/from the port's member set.
Use the no parameter to remove all VLAN IDs configured on this port.

3. Command Syntax:
switchport trunk allowed vlan all
switchport trunk allowed vlan none
switchport trunk allowed vlan add VLANID
switchport trunk allowed vlan remove VLANID
switchport trunk allowed vlan except VLANID
no switchport trunk vlan
all Allow all VLANs to transmit and receive through the Layer-2 interface.
none Allow no VLANs to transmit and receive through the Layer-2 interface.
add Add a VLAN to transmit and receive through the Layer-2 interface.
remove Remove a VLAN from transmit and receive through the Layer-2 interface.
except All VLANs, except the VLAN for which the ID is specified, are part of its ports member set.
VLANID <2-4094> The ID of the VLAN or VLANs that will be added to, or removed from, the Layer-2 interface. A single VLAN, VLAN range, or VLAN list can be set.
For a VLAN range, specify two VLAN numbers: lowest, then highest number in the range, separated by a hyphen.
For a VLAN list, specify the VLAN numbers separated by commas.

4. Example:
The following example specifies to **add** the interface fe1 (port 1) to VLANID (**2**):

```
switch_a(config)#interface fe1
switch_a(config-if)#switchport trunk allowed vlan add 2
switch_a(config-if)#
```

Priority Level:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to set user priority for port.

3. Command Syntax:
user-priority <0-7>
<0-7> User priority value.

4. Example:
The following example sets user priority (**0**) for the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#user-priority 0
switch_a(config-if)#
```

**PORT BASED VLAN**
Switchport portbase add/remove vlan:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to set or remove the default VLAN for the interface.

3. Command Syntax:
switchport portbase add | remove vlan VLANID
VLANID The ID of the VLAN will be added to or removed from the Layer-2 interface.

4. Example:
The following example specifies to **add** the interface fe1 (port 1) to VLANID (**2**):

```
switch_a(config)#interface fe1
switch_a(config-if)#switchport portbase add vlan 2
switch_a(config-if)#
```

## 7.9 QOS

Global Configuration, 802.1p Priority, DSCP

**GLOBAL CONFIGURATION**
QoS:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **mls qos enable** command to globally enable QoS.
Use the **no mls qos** command to globally disable QoS.

3. Command Syntax:
mls qos enable
(no) mls qos

4. Example:
The following example globally enables QoS on the switch:

```
switch_a(config)#mls qos enable
switch_a(config)#
```

---

Trust:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **mls qos trust** command to turn on QoS trust CoS or DSCP.
Use the **no mls qos trust** command to turn off QoS trust CoS or DSCP.

3. Command Syntax:
(no) mls qos trust cos/dscp
cos Class of Service.
dscp Differentiated Service Code Point.

4. Example:
The following example turns on QoS trust CoS on the switch:

```
switch_a(config)#mls qos trust cos
switch_a(config)#
```

---

Strict Priority:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **priority-queue out** command to enable the egress expedite queue.
Use the **no priority-queue out** command to disable the egress expedite queue.

3. Command Syntax:
(no) priority-queue out

4. Example:
The following example enables the egress expedite queue on the switch:

```
switch_a(config)#priority-queue out
switch_a(config)#
```

---

Weighted Round Robin:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **wrr-queue bandwidth** command to specify the bandwidth ratios of the transmit queues.

3. Command Syntax:
wrr-queue bandwidth WRR_WTS
WRR_WTS Weighted Round Robin (WRR) weights for the 4 queues (4 values separated by spaces). Range is 1-55.

4. Example:
The following example specifies the bandwidth ratios of the transmit queues on the switch:

```
switch_a(config)#wrr-queue bandwidth 1 2 4 8
switch_a(config)#
```

---

**802.1P PRIORITY**
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **wrr-queue cos-map** command to specify CoS values for a queue.

3. Command Syntax:
wrr-queue cos-map QUEUE_ID COS_VALUE
QUEUE_ID Queue ID. Range is 0-3.
COS_VALUE CoS values. Up to 8 values (separated by spaces). Range is 0-7.

4. Example:
The following example shows mapping CoS values 0 and 1 to queue 1 on the switch:

```
switch_a(config)#wrr-queue cos-map 1 0 1
switch_a(config)#
```

---

**DSCP**

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use **mls qos map dscp-queue** command to map the DSCP values to a queue.

3. Command Syntax:

mls qos map dscp-queue DSCP_VALUE to QUEUE_ID
DSCP_VALUE DSCP values. Up to 8 values (separated by spaces). Range is 0-63.
QUEUE_ID Queue ID. Range is 0-3.

4. Example:

The following example shows mapping DSCP values 0 to 3 to queue 1 on the switch:

```
switch_a(config)#mls qos map dscp-queue 0 1 2 3 to 1
switch_a(config)#
```

## 7.10 ACL

ACL Information, ACL Configuration

ACL is supported by EX27/77/87/29/89000 product series.

**ACL CONFIGURATION**
Policy Map:
Create New Policy Map:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **policy-map** command to create a policy map and **no policy-map** command to delete a policy map.

3. Command Syntax:
(no) policy-map NAME
NAME Policy map name.

4. Example:
Create a policy map p1.

```
switch_a(config)#policy-map p1
switch_a(config-pmap)#
```

---

Attach Policy Map to Interface:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **service-policy input** command to attach a policy map to an interface and **no service-policy input** command to remove a policy map from an interface.

3. Command Syntax:
(no) service-policy input NAME
NAME Policy map name.

4. Example:
Attach a policy map p1 to interface fe1.

```
switch_a(config)#interface fe1
switch_a(config-if)#service-policy input p1
switch_a(config-if)#
```

---

Class Map:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use **class-map** command to create a class map and **no class-map** command to delete a class map.

3. Command Syntax:

(no) class-map NAME
NAME Class map name.

4. Example:

Create a class map c1.

```
switch_a(config)#class-map c1
switch_a(config-cmap)#
```

---

Attach Class Map to Policy Map:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use **class** command to match a class map to a policy map and **no class** command to dismiss a class map from a policy map.

3. Command Syntax:

(no) class NAME
NAME Class map name.

4. Example:

Match a class map c1 to a policy map p1.

```
switch_a(config)#policy-map p1
switch_a(config-pmap)#class c1
switch_a(config-pmap-c)#
```

---

Set Traffic Rate and Burst Size:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set average traffic rate and normal burst size in an access group.

3. Command Syntax:

police RATE BURST exceed-action drop
RATE <1-1000000> Specify an average traffic rate (kbps).
BURST <1-20000> Specify a normal burst size (bytes).

4. Example:
Set average traffic rate 1000000kbps and normal burst size 20000 bytes.

```
switch_a(config)#policy-map p1
switch_a(config-pmap)#class c1
switch_a(config-pmap-c)#police 1000000 20000 exceed-action drop
switch_a(config-pmap-c)#
```

---

Attach Access Group to Class Map:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **match access-group** command to match an access group to a class map and **no match access-group** command to dismiss an access group from a class map.

3. Command Syntax:
(no) match access-group NAME
NAME ACL list name.

4. Example:
Match an access group 1 to a class map c1.

```
switch_a(config)#class-map c1
switch_a(config-cmap)#match access-group 1
switch_a(config-cmap)#
```

---

IP Access List:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **ip-access-list** command to create an IP access list and **no ip-access-list** command to delete an IP access list.

3. Command Syntax:
(no) ip-access-list ACCESS-LIST NUMBER (deny | permit) SOURCE ( | SOURCE WILDCARD)
ACCESS-LIST NUMBER Range is 1-99 and 1300-1999.
deny Deny certain traffic if conditions matched.
permit Permit certain traffic if conditions matched.
SOURCE Originating network or host sending packet. The word, any, can be used in place of 0.0.0.0 255.255.255.255.
SOURCE WILDCARD Optional. Wildcard bits in dotted decimal notation to apply to the source. Ones go in bit positions to ignore.

4. Example:
IP address: 192.168.1.10. Mask: 0.0.0.3. Then IP address 192.168.1.8 ~ 192.168.1.11 would be permitted.

```
switch_a(config)#ip-access-list 1 permit 192.168.1.10 0.0.0.3
switch_a(config)#
```

IP Access List (Extended):

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to create an Extended IP access list and no with this command to delete an Extended IP access list.

3. Command Syntax:

(no) ip-access-list ACCESS-LIST NUMBER (deny | permit) ip ( | host) SOURCE ( | SOURCE_WILDCARD) ( | tcp TCP_SOURCE) ( | host) DESTINATION ( | DESTINATION_WILDCARD) ) ( | tcp TCP_ DESTINATION)

ACCESS-LIST NUMBER Range is 100-199 and 2000-2699.
deny Deny certain traffic if conditions matched.
permit Permit certain traffic if conditions matched.
( | host) Optional. If this parameter is set, it means this access list has a single source (or destination) host. This parameter equals to setting SOURCE_WILDCARD to 0.0.0.0.
SOURCE Originating network or host sending packet. The word, any, can be used in place of 0.0.0.0 255.255.255.255.
( | SOURCE WILDCARD) Optional. Wildcard bits in dotted decimal notation to apply to the source. Ones go in bit positions to ignore. If parameter "host" was set, this parameter can not be set.
( | tcp TCP_SOURCE) Optional. Set L4 port value.
DESTINATION Host receiving packet. The word, any, can be used in place of 0.0.0.0 255.255.255.255.
( | DESTINATION WILDCARD) Optional. Wildcard bits in dotted decimal notation to apply to the destination. Ones go in bit positions to ignore. If parameter "host" was set, this parameter can not be set.
( | tcp TCP_ DESTINATION) Optional. Set L4 port value.

4. Example:

Source Address: any. Destination Address: 192.168.1.20. Destination Wildcard Bits: 0.0.0.255. Then Destination IP address 192.168.1.0 ~ 192.168.1.255 would be permitted.

```
switch_a(config)#ip-access-list 100 permit ip any 192.168.1.20 0.0.0.255
switch_a(config)#
```

MAC Access List:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use **mac-access-list** command to create a MAC access list and **no mac-access-list** command to delete a MAC access list.

3. Command Syntax:

(no) mac-access-list ACCESS-LIST NUMBER (deny | permit) SOURCE ( | SOURCE_WILDCARD) DESTINATION ( | DESTINATION_WILDCARD) <1-8> ( | ether-type (any | (ETHER_TYPE ETHER_TYPE_WILDCARD))

ACCESS-LIST NUMBER Range is 2000-2699.
deny Deny certain traffic if conditions matched.
permit Permit certain traffic if conditions matched.
SOURCE Originating network or host sending packet. The word, any, can be used in place of 0.0.0 ffff.ffff.ffff.
( | SOURCE WILDCARD) Optional. Wildcard bits in dotted decimal notation to apply to the source. Ones go in bit positions to ignore.
DESTINATION Host receiving packet. The word, any, can be used in place of 0.0.0 ffff.ffff.ffff.
( | DESTINATION WILDCARD) Optional. Wildcard bits in dotted decimal notation to apply to the destination. Ones go in bit positions to ignore.
<1-8> Specify packet format: Ethernet II, 802.3, SNMP, LLC.
( | ether-type (any | (ETHER_TYPE ETHER_TYPE_WILDCARD)) Optional. Set ether type value. The word, any, can be used in place of 00.

4. Example:
Source MAC Address: any. Destination MAC Address: 001a.4d9f.ab89. Destination Wildcard Bits: 0.0.ff. Then Destination MAC address 001a.4d9f.ab00 ~ 001a.4d9f.abff would be permitted.

```
switch_a(config)#mac-access-list 2000 permit any 001a.4d9f.ab89 0.0.ff
switch_a(config)#
```

---

Attach Layer 4 Access List to Class Map:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to match a layer 4 access list to a class map and no form of the command to dismiss a layer 4 access list from a class map.

3. Command Syntax:
(no) match layer4 (source-port | destination-port) <1-65535>

source-port Specify source TCP/UDP port.
destination-port Specify destination TCP/UDP port.
<1-65535> TCP/UDP port value.

4. Example:
Match a layer 4 access list (source TCP/UDP port 1) to a class map c1.

```
switch_a(config)#class-map c1
switch_a(config-cmap)#match layer4 source-port 1
switch_a(config-cmap)#
```

## 7.11 SNMP

SNMP General Setting, SNMP v1/v2c, SNMP v3

**SNMP GENERAL SETTING**
SNMP Status:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **snmp-server enable** command to enable and **no snmp-server enable** command to disable SNMP to the switch.

3. Command Syntax:
(no) snmp-server enable

4. Example:
The following example enables SNMP to the switch:

```
switch_a(config)#snmp-server enable
switch_a(config)#
```

---

Description:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **snmp-server description** command to specify and **no snmp-server description** command to remove description for SNMP.

3. Command Syntax:
snmp-server description DESCRIPTION
no snmp-server description
DESCRIPTION The description for SNMP.

4. Example:
The following example specifies description (**description**) for SNMP:

```
switch_a(config)#snmp-server description description
switch_a(config)#
```

---

Location:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **snmp-server location** command to specify and **no snmp-server location** command to remove location for SNMP.

3. Command Syntax:
snmp-server location LOCATION
no snmp-server location
LOCATION The location for SNMP.

4. Example:
The following example specifies location (**location**) for SNMP:

```
switch_a(config)#snmp-server location location
switch_a(config)#
```

---

Contact:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **snmp-server contact** command to specify and **no snmp-server contact** command to remove contact for SNMP.

3. Command Syntax:
snmp-server contact CONTACT
no snmp-server contact
CONTACT The contact for SNMP.

4. Example:
The following example specifies contact (**contact**) for SNMP:

```
switch_a(config)#snmp-server contact contact
switch_a(config)#
```

---

Trap Community Name:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to specify trap community name for SNMP.
Use the no parameter with this command to remove trap community name for SNMP.

3. Command Syntax:
snmp-server trap-community <1-5> NAME
no snmp-server trap-community <1-5>
<1-5> The trap community 1-5.
NAME The trap community name for SNMP.

4. Example:

The following example specifies trap community name 1 (**name**) for SNMP:

```
switch_a(config)#snmp-server trap-community 1 name
switch_a(config)#
```

---

Trap Host IP Address:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to specify trap host IP address for SNMP.
Use the no parameter with this command to remove trap host IP address for SNMP.

3. Command Syntax:

snmp-server trap-ipaddress <1-5> IP-ADDRESS
no snmp-server trap-ipaddress <1-5>
<1-5> The trap host IP address 1-5.
IP-ADDRESS The trap host IP address for SNMP. A.B.C.D specifies the IP address.

4. Example:

The following example specifies trap host 1 IP address (**192.168.1.20**) for SNMP:

```
switch_a(config)#snmp-server trap-ipaddress 1 192.168.1.20
switch_a(config)#
```

---

Link Down Trap:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use **snmp-server trap-type enable linkDown** command to enable link down trap for SNMP.
Use the **no snmp-server trap-type enable linkDown** command to disable link down trap for SNMP.

3. Command Syntax:

(no) snmp-server trap-type enable linkDown

4. Example:

The following example enables link down trap for SNMP:

```
switch_a(config)#snmp-server trap-type enable linkDown
switch_a(config)#
```

---

Link Up Trap:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **snmp-server trap-type enable linkUp** command to enable link up trap for SNMP.
Use the **no snmp-server trap-type enable linkUp** command to disable link up trap for SNMP.

3. Command Syntax:
(no) snmp-server trap-type enable linkUp

4. Example:
The following example enables link up trap for SNMP:

```
switch_a(config)#snmp-server trap-type enable linkUp
switch_a(config)#
```

---

MAC Notification Trap:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to enable the Switch to send MAC Notification Trap to the network management system (NMS).
Use the no parameter with this command to disable the Switch to send MAC Notification Trap to the network management system (NMS).

3. Command Syntax:
snmp-server trap-type enable mac-notification
no snmp-server trap-type enable mac-notification

4. Example:
The following example enables the Switch to send MAC Notification Trap to the network management system (NMS):

```
switch_a(config)#snmp-server trap-type enable mac-notification
switch_a(config)#
```

---

MAC Notification Interval:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to specify the MAC notification trap interval in seconds between each set of traps that are generated.

3. Command Syntax:
snmp-server mac-notification interval <1-65535>
<1-65535> The MAC notification trap interval in seconds.

4. Example:
The following example sets MAC notification trap interval time 10 seconds:

```
switch_a(config)# snmp-server mac-notification interval 10
switch_a(config)#
```

MAC Notification History Size:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to specify the maximum number of entries in the MAC notification history table.

3. Command Syntax:
snmp-server mac-notification history-size <1-500>
<1-500> The range is 1 to 500.

4. Example:
The following example sets the maximum 500 entries in the MAC notification history table:

```
switch_a(config)# snmp-server mac-notification history-size 500
switch_a(config)#
```

MAC Notification Added/Removed:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to add or remove MAC Notification Trap on an interface port.

3. Command Syntax:
snmp-server trap mac-notification (added | removed)
no snmp-server trap mac-notification (added | removed)

4. Example:
The following example specifies to add MAC Notification Trap on the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)# snmp-server trap mac-notification added
switch_a(config-if)#
```

**SNMP V1/V2C**
Get Community Name:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use **snmp-server community get** command to specify and **no snmp-server community get** command to remove get community name for SNMP.

3. Command Syntax:
snmp-server community get NAME
no snmp-server community get
NAME The get community name for SNMP.

4. Example:
The following example specifies get community name (**name**) for SNMP:

```
switch_a(config)#snmp-server community get name
switch_a(config)#
```

---

Set Community Name:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **snmp-server community set** command to specify and **no snmp-server community set** command to remove set community name for SNMP.

3. Command Syntax:
snmp-server community set NAME
no snmp-server community set
NAME The set community name for SNMP.

4. Example:
The following example specifies set community name (**name**) for SNMP:

```
switch_a(config)#snmp-server community set name
switch_a(config)#
```

---

**SNMP V3**
SNMPv3 No-Auth:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Add a user using snmp v3 with read-only or read-write access mode and without authentication. Use the no form of the command to delete this user.

3. Command Syntax:
(no) snmp-server v3-user USERNAME (ro | rw) noauth
USERNAME Specify a user name.
ro read-only access mode
rw read-write access mode

4. Example:
The following example adds a user (**myuser**) using snmp v3 with read-only access mode and without authentication:

```
switch_a(config)#snmp-server v3-user myuser ro noauth
switch_a(config)#
```

---

SNMPv3 Auth-MD5, SNMPv3 Auth-SHA:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Add a user using snmp v3 with read-only or read-write access mode and with MD5 or SHA authentication. Use the no form of the command to delete this user.

3. Command Syntax:
(no) snmp-server v3-user USERNAME (ro | rw) auth (md5 | sha) AUTH_PASSWORD
USERNAME Specify a user name.
ro read-only access mode
rw read-write access mode
md5 authentication method
sha authentication method
AUTH_PASSWORD authentication password

4. Example:
The following example adds a user (**myuser**) using snmp v3 with read-write access mode and MD5 authentication (**mypassword**):

```
switch_a(config)#snmp-server v3-user myuser rw auth md5 mypassword
switch_a(config)#
```

---

SNMPv3 Priv Auth-MD5, SNMPv3 Priv Auth-SHA:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Add a user using snmp v3 with read-only or read-write access mode, MD5 or SHA authentication, and privacy. Use the no form of the command to delete this user.

3. Command Syntax:
(no) snmp-server v3-user USERNAME (ro | rw) priv auth (md5 | sha) AUTH_PASSWORD des PRIV_PASS_PHRASE
USERNAME Specify a user name.
ro read-only access mode
rw read-write access mode
md5 authentication method
sha authentication method
AUTH_PASSWORD authentication password
PRIV_PASS_PHRASE encryption pass phrase

4. Example:

The following example adds a user (**myuser**) using snmp v3 with read-write access mode, MD5 authentication (**mypassword**), and encryption pass phrase (**mypassphrase**):

```
switch_a(config)#snmp-server v3-user myuser rw priv md5 mypassword des mypassphrase
switch_a(config)#
```

## 7.12 802.1X

Radius Configuration, Port Authentication

**RADIUS CONFIGURATION**

Radius Status:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use **dot1x system-auth-ctrl** command to globally enable authentication.
Use **no dot1x system-auth-ctrl** command to globally disable authentication.

3. Command Syntax:

(no) dot1x system-auth-ctrl

4. Example:

The following example globally enables authentication:

```
switch_a(config)#dot1x system-auth-ctrl
switch_a(config)#
```

---

Radius Server IP:
Radius Server Port:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to specify the IP address of the remote radius server host and assign authentication and accounting destination port number.

3. Command Syntax:

(no) radius-server host IP-ADDRESS auth-port PORT
IP-ADDRESS A.B.C.D specifies the IP address of the radius server host.
PORT specifies the UDP destination port for authentication requests. The host is not used for authentication if set to 0.

4. Example:

The following example specifies the IP address (**192.168.1.100**) of the remote radius server host and assigns authentication and accounting destination port number (**1812**):

```
switch_a(config)#radius-server host 192.168.1.100 auth-port 1812
switch_a(config)#
```

---

Secret Key:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set the shared secret key between a Radius server and a client.

3. Command Syntax:
(no) radius-server host IP-ADDRESS key KEY
IP-ADDRESS A.B.C.D specifies the IP address of the radius server host.
KEY specifies the secret key shared among the radius server and the 802.1x client.

4. Example:
The following example specifies the IP address (**192.168.1.100**) of the remote radius server host and set the secret key **(ipi**) shared among the radius server and the 802.1x client:

```
switch_a(config)#radius-server host 192.168.1.100 key ipi
switch_a(config)#
```

---

Timeout:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to specify the number of seconds a Switch waits for a reply to a radius request before retransmitting the request.

3. Command Syntax:
radius-server timeout SEC
no radius-server timeout
SEC <1-1000> The number of seconds for a Switch to wait for a server host to reply before timing out. Enter a value in the range 1 to 1000.

4. Example:
The following example specifies **20** seconds for the Switch to wait for a server host to reply before timing out:

```
switch_a(config)#radius-server timeout 20
switch_a(config)#
```

---

Retransmit:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to specify the number of times the Switch transmits each radius request to the server before giving up.

3. Command Syntax:
radius-server retransmit RETRIES
no radius-server retransmit
RETRIES <1-100> Specifies the retransmit value. Enter a value in the range 1 to 100.

4. Example:
The following example specifies the retransmit value **12**:

```
switch_a(config)#radius-server retransmit 12
switch_a(config)#
```

---

**PORT AUTHENTICATION**
Authentication State:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use **dot1x reauthetication** command to enable reauthentication on a port.
Use **no dot1x reauthetication** command to disable reauthentication on a port.

3. Command Syntax:
(no) dot1x reauthentication

4. Example:
The following example specifies to enable reauthetication on the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#dot1x reauthentication
switch_a(config-if)#
```

---

Port Control:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to force a port state.
Use **no dot1x port-control** command to remove a port from the 802.1x management.

3. Command Syntax:
dot1x port-control auto | force-authorized | force-unauthorized
no dot1x port-control
auto Specify to enable authentication on port.
force-authorized Specify to force a port to always be in an authorized state.
force-unauthorized Specify to force a port to always be in an unauthorized state.

4. Example:
The following example specifies to enable authetication on the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#dot1x port-control auto
switch_a(config-if)#
```

---

Periodic Reauthentication:
Reauthentication Period:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to set the interval between reauthorization attempts.
Use **no dot1x timeout re-authperiod** command to delete the interval between reauthorization attempts.

3. Command Syntax:
dot1x timeout re-authperiod SECS
no dot1x timeout re-authperiod
SECS <1-4294967295> Specify the seconds between reauthorization attempts. The default time is 3600 seconds.

4. Example:
The following example specifies to set the interval **25** seconds between reauthorization attempts:

```
switch_a(config)#interface fe1
switch_a(config-if)#dot1x timeout re-authperiod 25
switch_a(config-if)#
```

## 7.13 LLDP

LLDP General Settings, LLDP Ports Settings, LLDP Neighbors, LLDP Statistics

**LLDP GENERAL SETTING**
LLDP:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to enable Link Layer Discovery Protocol (LLDP) globally.
Use the no parameter with this command to disable Link Layer Discovery Protocol (LLDP) globally.

3. Command Syntax:
(no) lldp enable

4. Example:
The following example enables Link Layer Discovery Protocol (LLDP) globally:

```
switch_a(config)#lldp enable
switch_a(config)#
```

---

Holdtime Multiplier (2-10):
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set the Link Layer Discovery Protocol (LLDP) holdtime multiplier value. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) that the switch advertises to the neighbors.

3. Command Syntax:
lldp holdtime multiplier <2-10>
<2-10> Holdtime multiplier 2-10, default is 4.

4. Example:
The following example sets Link Layer Discovery Protocol (LLDP) holdtime multiplier to 5:

```
switch_a(config)#lldp holdtime multiplier 5
switch_a(config)#
```

---

Tx Interval (5-32768 seconds):
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the transmit interval. This is the interval between regular transmissions of Link Layer Discovery Protocol (LLDP) advertisements.

3. Command Syntax:
lldp txinterval <5-32768>
<5-32768> TxInterval 5-32768 seconds, default is 30 seconds.

4. Example:
The following example sets Link Layer Discovery Protocol (LLDP) transmit interval to 60 seconds:

```
switch_a(config)#lldp txinterval 60
switch_a(config)#
```

---

Global TLV Setting:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to configure Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) setting.
Use the no parameter with this command to disable Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) setting.

3. Command Syntax:
(no) lldp tlv-global port-descr |sys-name |sys-descr |sys-cap |mgmt-addrs |port-vlan-id |mac-phy |protocol-identity |vlan-name |port-and-protocol |power-mdi |link-aggregation |max-frame
port-descr Port Description TLV.
sys-name System Name TLV.
sys-descr System Description TLV.
sys-cap System Capabilities TLV.
mgmt-addrs Management Address TLV.
port-vlan-id Port VLAN ID TLV.
mac-phy MAC/PHY Configuration/Status TLV.
protocol-identity Protocol Identity TLV.
vlan-name VLAN Name TLV.
port-and-protocol Port And Protocol VLAN ID TLV.
power-mdi Power Via MDI TLV.
link-aggregation Link Aggregation TLV.
max-frame Maximum Frame Size TLV.

4. Example:
The following example sets Link Layer Discovery Protocol (LLDP) Link Aggregation Type Length Value (TLV):

```
switch_a(config)#lldp tlv-global link-aggregation
switch_a(config)#
```

---

**LLDP PORTS SETTINGS**

Transmit:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to send Link Layer Discovery Protocol (LLDP) packets on the interface.
Use the no parameter with this command to disallow sending Link Layer Discovery Protocol (LLDP) packets on the interface.

3. Command Syntax:

(no) lldp tx-pkt

4. Example:

The following example sends Link Layer Discovery Protocol (LLDP) packets on the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#lldp tx-pkt
switch_a(config-if)#
```

---

Receive:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:

Use this command to receive Link Layer Discovery Protocol (LLDP) packets on the interface.
Use the no parameter with this command to disallow receiving Link Layer Discovery Protocol (LLDP) packets on the interface.

3. Command Syntax:

(no) lldp rcv-pkt

4. Example:

The following example receives Link Layer Discovery Protocol (LLDP) packets on the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#lldp rcv-pkt
switch_a(config-if)#
```

---

Notify:

1. Command Mode: Interface mode

Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to enable Link Layer Discovery Protocol (LLDP) notification on the interface.
Use the no parameter with this command to disable Link Layer Discovery Protocol (LLDP) notification on the interface.

3. Command Syntax:
(no) lldp notification

4. Example:
The following example enables Link Layer Discovery Protocol (LLDP) notification on the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#lldp notification
switch_a(config-if)#
```

---

TLVs:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
fe1 means port 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface fe1
switch_a(config-if)#
```

2. Usage:
Use this command to configure Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) setting on the interface.
Use the no parameter with this command to disable Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) setting on the interface.

3. Command Syntax:
(no) lldp tlv-global port-descr |sys-name |sys-descr |sys-cap |mgmt-addrs |port-vlan-id |mac-phy |protocol-identity |vlan-name |port-and-protocol |power-mdi |link-aggregation |max-frame
port-descr Port Description TLV.
sys-name System Name TLV.
sys-descr System Description TLV.
sys-cap System Capabilities TLV.
mgmt-addrs Management Address TLV.
port-vlan-id Port VLAN ID TLV.
mac-phy MAC/PHY Configuration/Status TLV.
protocol-identity Protocol Identity TLV.
vlan-name VLAN Name TLV.
port-and-protocol Port And Protocol VLAN ID TLV.
power-mdi Power Via MDI TLV.
link-aggregation Link Aggregation TLV.
max-frame Maximum Frame Size TLV.

4. Example:
The following example sets Link Layer Discovery Protocol (LLDP) Link Aggregation Type Length Value (TLV) on the interface fe1 (port 1):

```
switch_a(config)#interface fe1
switch_a(config-if)#lldp tlv-global link-aggregation
switch_a(config-if)#
```

**LLDP NEIGHBORS**

1. Command Mode: Exec mode or Privileged Exec mode
Logon to Exec Mode (View Mode) or Privileged Exec Mode (Enable Mode).
The **switch_a>** or **switch_a#** prompt will show on the screen.

```
switch_a>
```

```
switch_a#
```

2. Usage:
Use the **show lldp neighbors** command to show Link Layer Discovery Protocol (LLDP) neighbors information.

3. Command Syntax:
show lldp neighbors

4. Example:
The following example shows Link Layer Discovery Protocol (LLDP) neighbors information:

```
switch_a> show lldp neighbors
```

**LLDP STATISTICS**

1. Command Mode: Exec mode or Privileged Exec mode
Logon to Exec Mode (View Mode) or Privileged Exec Mode (Enable Mode).
The **switch_a>** or **switch_a#** prompt will show on the screen.

```
switch_a>
```

```
switch_a#
```

2. Usage:
Use this command to show Link Layer Discovery Protocol (LLDP) statistics.

3. Command Syntax:
show lldp statistics
show lldp statistics IFNAME
IFNAME Interface name.

4. Example:
The following example shows Link Layer Discovery Protocol (LLDP) statistics:

```
switch_a> show lldp statistics
```

## 7.14 OTHER PROTOCOLS

GVRP, IGMP Snooping, NTP, GMRP, DHCP Server

**GVRP**
GVRP:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **set gvrp enable bridge** command to enable (set) and **set gvrp disable bridge** command to disable (reset) GVRP globally for the bridge instance. This command does not enable/disable GVRP in all ports of the bridge. After enabling GVRP globally, use the **set port gvrp enable** command to enable GVRP on individual ports of the bridge.

3. Command Syntax:
set gvrp enable bridge GROUP
set gvrp disable bridge GROUP
GROUP Bridge-group ID used for bridging.

4. Example:
The following example globally enables GVRP to bridge GROUP (**1**):

```
switch_a(config)#set gvrp enable bridge 1
switch_a(config)#
```

---

Dynamic VLAN creation:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **set gvrp dynamic-vlan-creation enable bridge** command to enable and **set gvrp dynamic-vlan-creation disable bridge** command to disable dynamic VLAN creation for a specific bridge instance.

3. Command Syntax:
set gvrp dynamic-vlan-creation enable bridge GROUP
set gvrp dynamic-vlan-creation disable bridge GROUP
GROUP Bridge-group ID used for bridging.

4. Example:
The following example enables dynamic VLAN creation for bridge GROUP (**1**):

```
switch_a(config)#set gvrp dynamic-vlan-creation enable bridge 1
switch_a(config)#
```

---

Per port setting:
GVRP:

1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **set port gvrp enable** command to enable and **set port gvrp disable** command to disable GVRP on a port or all ports in a bridge.

3. Command Syntax:
set port gvrp enable all/IFNAME
set port gvrp disable all/IFNAME
all All ports added to recently configured bridge.
IFNAME The name of the interface.

4. Example:
The following example enables GVRP on the interface fe1 (port 1):

```
switch_a(config)#set port gvrp enable fe1
switch_a(config)#
```

---

Per port setting:
GVRP applicant:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set the GVRP applicant state to normal or active.

3. Command Syntax:
set gvrp applicant state active/normal IFNAME
active Active state
normal Normal state
IFNAME Name of the interface.

4. Example:
The following example sets GVRP applicant state to active on the interface fe1 (port 1):

```
switch_a(config)#set gvrp applicant state active fe1
switch_a(config)#
```

---

Per port setting:
GVRP registration:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set GVRP registration to normal, fixed, and forbidden registration mode for a given port.

3. Command Syntax:
set gvrp registration normal IF_NAME
set gvrp registration fixed IF_NAME
set gvrp registration forbidden IF_NAME
normal Specify dynamic GVRP multicast registration and deregistration on the port.
fixed Specify the multicast groups currently registered on the switch are applied to the port, but any subsequent registrations or deregistrations do not affect the port. Any registered multicast groups on the port are not deregistered based on the GARP timers.
forbidden Specify that all GVRP multicasts are deregistered, and prevent any further GVRP multicast registration on the port.
IF_NAME The name of the interface.

4. Example:
The following example sets GVRP registration to fixed registration mode on the interface fe1 (port 1):

```
switch_a(config)#set gvrp registration fixed fe1
switch_a(config)#
```

---

**IGMP SNOOPING**
IGMP mode:
Querier:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **ip igmp snooping querier** command to enable IGMP querier operation on a subnet (VLAN) when no multicast routing protocol is configured in the subnet (VLAN). When enabled, the IGMP Snooping querier sends out periodic IGMP queries for all interfaces on that VLAN.
Use the **no ip igmp snooping querier** command to disable IGMP querier configuration.

3. Command Syntax:
(no) ip igmp snooping querier

4. Example:
The following example enables IGMP snooping querier:

```
switch_a(config)# ip igmp snooping querier
switch_a(config)#
```

---

IGMP mode:
Passive:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **ip igmp snooping** command to enable IGMP Snooping. This command is given in the Global Config mode. IGMP Snooping is enabled at the switch level.
Use the **no ip igmp snooping** command to globally disable IGMP Snooping.

3. Command Syntax:
(no) ip igmp snooping enable

4. Example:
The following example enables IGMP snooping on the switch:

```
switch_a(config)# ip igmp snooping enable
switch_a(config)#
```

---

IGMP version:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
vlan1.1 means vlan 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:
Use **ip igmp version** command to set the current IGMP protocol version on an interface.
To return to the default version, use the **no ip igmp version** command.

3. Command Syntax:
ip igmp version VERSION
no ip igmp version
VERSION IGMP protocol version number.

4. Example:
The following example sets the IGMP protocol version 3 on **vlan1.1**:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip igmp version 3
switch_a(config-if)#
```

---

Fast-leave:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
vlan1.1 means vlan 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:
Use **ip igmp snooping fast-leave** command to enable IGMP Snooping fast-leave processing. Fast-leave processing is analogous to immediate leave processing; the IGMP group-membership is removed, as soon as an IGMP leave group message is received without sending out a group-specific query.
Use the **no ip igmp snooping fast-leave** command to disable fast-leave processing.

3. Command Syntax:
(no) ip igmp snooping fast-leave

4. Example:
The following example enables IGMP snooping fast-leave on **vlan1.1**:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip igmp snooping fast-leave
switch_a(config-if)#
```

---

IGMP querier:
Query-interval:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
vlan1.1 means vlan 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:
Use **ip igmp query-interval** command to configure the frequency of sending IGMP host query messages.
To return to the default frequency, use the **no ip igmp query-interval** command.

3. Command Syntax:
ip igmp query-interval INTERVAL
no ip igmp query-interval
INTERVAL <1-18000> Frequency (in seconds) at which IGMP host query messages are sent. Default: 125 seconds.

4. Example:
The following example changes the frequency of sending IGMP host-query messages to 2 minutes on **vlan1.1**:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip igmp query-interval 120
switch_a(config-if)#
```

---

IGMP querier:
Max-response-time:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
vlan1.1 means vlan 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:
Use **ip igmp query-max-response-time** command to configure the maximum response time advertised in IGMP queries.

To restore to the default value, use the **no ip igmp query-max-response-time** command.

3. Command Syntax:

ip igmp query-max-response-time RESPONSETIME
no ip igmp query-max-response-time
RESPONSETIME <1-240> Maximum response time (in seconds) advertised in IGMP queries. Default: 10 seconds.

4. Example:
The following example configures a maximum response time of 8 seconds on **vlan1.1**:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip igmp query-max-response-time 8
switch_a(config-if)#
```

---

IGMP passive snooping:
Static mc router port:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
vlan1.1 means vlan 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:
Use **ip igmp snooping mrouter interface** command to statically configure the specified VLAN constituent interface as a multicast router interface for IGMP Snooping in that VLAN.
Use the **no ip igmp snooping mrouter interface** command to remove the static configuration of the interface as a multicast router interface.

3. Command Syntax:
(no) ip igmp snooping mrouter interface IFNAME
IFNAME Specify the name of the interface

4. Example:
The following example shows interface fe1 (port 1) statically configured to be a multicast router interface on **vlan1.1**:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip igmp snooping mrouter interface fe1
switch_a(config-if)#
```

---

IGMP passive snooping:
Report suppression:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
vlan1.1 means vlan 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:
Use **ip igmp snooping report-suppression** command to enable report suppression for IGMP versions 1 and 2.

Use the **no ip igmp snooping report-suppression** command to disable report suppression.

3. Command Syntax:
(no) ip igmp snooping report-suppression

4. Example:
The following example enables report suppression for IGMPv2 reports on **vlan1.1**:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip igmp version 2
switch_a(config-if)#ip igmp snooping report-suppression
switch_a(config-if)#
```

---

Force Forwarding Port:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to force forward multicast packet to interface before the interface receiving IGMP query.

3. Command Syntax:
ip igmp snooping force-forward LINE | none | all
LINE Interface name list, ex: fe1-fe3, fe5.
none Not forward multicast packet to any interface.
all Forward multicast packet to all interfaces.

4. Example:
The following example force forwards multicast packet to interfaces fe1-fe3 and fe5:

```
switch_a(config)# ip igmp snooping force-forward fe1-fe3, fe5
switch_a(config)#
```

---

Passive Mode Forwarding Port:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to forward multicast packet to interface before the interface receiving IGMP query in passive mode.

3. Command Syntax:
ip igmp snooping passive-forward LINE | none | all
LINE Interface name list, ex: fe1-fe3, fe5.
none Not forward multicast packet to any interface.
all Forward multicast packet to all interfaces.

4. Example:
The following example forwards multicast packet to interfaces fe1-fe3 and fe5:

```
switch_a(config)# ip igmp snooping passive-forward fe1-fe3, fe5
switch_a(config)#
```

**NTP**

RTC Time:

1. Command Mode: Exec mode or Privileged Exec mode

Logon to Exec Mode (View Mode) or Privileged Exec Mode (Enable Mode).
The **switch_a>** or **switch_a#** prompt will show on the screen.

```
switch_a>
```

```
switch_a#
```

2. Usage:

Use the **show rtc time** command to show RTC time.

3. Command Syntax:

show rtc time

4. Example:

The following example shows the use of **show rtc time** to show RTC time:

```
switch_a>show rtc time
```

---

Adjust RTC Time:

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).
The **switch_a#** prompt will show on the screen.

```
switch_a#
```

2. Usage:

Use this command to configure the time of RTC.

3. Command Syntax:

set clock YEAR MONTH DAY HOUR MINUTE SECOND
YEAR Specifies year from 2000 to 2037.
MONTH <1-12> Specifies from 1 to 12.
DAY <1-31> Specifies from 1 to 31.
HOUR <0-23> Specifies from 0 to 23.
MINUTE <0-59> Specifies from 0 to 59.
SECOND <0-59> Specifies from 0 to 59.

4. Example:

The following example sets the time of RTC as July/20/2015 12:30:50:

```
switch_a#set clock 2015 7 20 12 30 50
switch_a#
```

---

NTP Status:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **ntp enable** command to enable NTP for the Switch.
Use **no ntp enable** command to disable NTP for the Switch.

3. Command Syntax:
(no) ntp enable

4. Example:
The following example enables NTP for the Switch:

```
switch_a(config)#ntp enable
switch_a(config)#
```

---

NTP Server:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to specify the IP address or Domain name of NTP server.

3. Command Syntax:
ntp server IP-ADDRESS | DOMAIN-NAME
IP-ADDRESS A.B.C.D specifies the IP address of NTP server.
DOMAIN-NAME Specifies the Domain name of NTP server.

4. Example:
The following example specifies the IP address (**192.168.1.100**) of NTP server:

```
switch_a(config)#ntp server 192.168.1.100
switch_a(config)#
```

---

Sync Time:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use **ntp sync-time** command to synchronize time with NTP server.

3. Command Syntax:
ntp sync-time

4. Example:
The following example synchronizes time with NTP server:

```
switch_a(config)#ntp sync-time
switch_a(config)#
```

---

Time Zone:
1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to to set time zone.

3. Command Syntax:
clock timezone TIMEZONE
TIMEZONE Specifies the time zone. (Please refer the Appendix B)

4. Example:
The following example sets time zone (Canada/Yukon):

```
switch_a(config)#clock timezone YST9YDT
switch_a(config)#
```

---

Polling Interval:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to specify the polling interval.

3. Command Syntax:
ntp polling-interval MINUTE
MINUTE <1-10080> The polling interval. Enter a value in the range 1 to 10080 minutes.

4. Example:
The following example specifies the polling interval **60** minutes:

```
switch_a(config)#ntp polling interval 60
switch_a(config)#
```

---

Daylight Saving Mode:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to enable daylight saving.
Use **no clock summer-time** command to disable daylight saving.

3. Command Syntax:
clock summer-time TIMEZONE weekday WEEK DAY MONTH HOUR MINUTE WEEK DAY MONTH HOUR MINUTE OFFSET
TIMEZONE Specifies the daylight saving timezone.
WEEK <1-5> Specifies starting/ending week of daylight savings time.
DAY <0-6> Specifies from Sunday to Saturday.
MONTH <1-12> Specifies from January to December.
HOUR <0-23> Specifies from 0 to 23.

MINUTE <0-59> Specifies from 0 to 59.
OFFSET <1-1440> Specifies from 1 to 1440 minutes.
clock summer-time TIMEZONE date DAY MONTH HOUR MINUTE DAY MONTH HOUR MINUTE OFFSET
TIMEZONE Specifies the daylight saving timezone.
DAY <1-31> Specifies from 1 to 31.
MONTH <1-12> Specifies from January to December.
HOUR <0-23> Specifies from 0 to 23.
MINUTE <0-59> Specifies from 0 to 59.
OFFSET <1-1440> Specifies from 1 to 1440 minutes.
no clock summer-time

4. Example:
The following example sets clock summer-time TIMEZONE (**onehour**) as daylight saving offset 60 minutes from 4 April AM0:00 to 31 October AM0:00:

```
switch_a(config)#clock summer-time onehour date 4 4 0 0 31 10 0 0 60
switch_a(config)#
```

---

**GMRP**

Clear GMRP Statistics:

1. Command Mode: Privileged Exec mode

Logon to Privileged Exec Mode (Enable Mode).
The **switch_a#** prompt will show on the screen.

```
switch_a#
```

2. Usage:

Use this command to clear GMRP statistics for a given VLAN or all the VLANs configured on the Layer-2 switch. This default clearing is for all the configured VLANs.

3. Command Syntax:

clear gmrp statistics [all | vlanid VLANID] bridge BRIDGE_NAME
all Clear GMRP statistics for all the VLANs.
VLANID vlanid <1 to 4094> Clear GMRP statistics for the particular VLAN ID**.**
BRIDGE_NAME Bridge instance name.

4. Example:

The following example clears the GMRP statistics for VLAN 12 on bridge 1:

```
switch_a#clear gmrp statistics vlanid 12 bridge 1
switch_a#
```

The following example clears the GMRP statistics for all the configured VLANs on bridge 1:

```
switch_a#clear gmrp statistics all bridge 1
switch_a#
```

---

Set GMRP:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable/disable GMRP globally on a particular bridge. This command does not enable/disable GMRP in all ports of the bridge. After enabling GMRP globally, use the **set port gmrp** command to enable GMRP on individual ports of the bridge. GMRP cannot be enabled if IGMP Snooping is enabled, or if GMRP has already been configured for a particular VLAN.

3. Command Syntax:

set gmrp enable | disable bridge BRIDGE_NAME
enable Enable GMRP on Layer-2 switch.
disable Disable GMRP on Layer-2 switch
BRIDGE_NAME The text string to use for the name of the bridge.

4. Example:

The following example enables GMRP on a Layer-2 switch for bridge 1:

```
switch_a(config)#set gmrp enable bridge 1
switch_a(config)#
```

---

Set Port GMRP:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to enable/disable GMRP on a particular port in all VLANs or all ports in a bridge. GMRP on a port cannot be enabled for all VLANs if GMRP has already been configured for a particular VLAN for the port.

3. Command Syntax:

set port gmrp enable | disable all | IF_NAME
enable Enable GMRP on Layer-2 switch port
disable Disable GMRP on Layer-2 switch port
all All ports added to recently configured bridge
IF_NAME Specify the name of the interface.

4. Example:

The following example enables GMRP on interface fe1 (port 1):

```
switch_a(config)#set port gmrp enable fe1
switch_a(config)#
```

The following example enables GMRP on all ports:

```
switch_a(config)#set port gmrp enable all
switch_a(config)#
```

---

GMRP Registration:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set GMRP registration type for all ports for a given bridge.

3. Command Syntax:
set gmrp registration normal | fixed | forbidden IF_NAME
normal Specify dynamic GMRP multicast registration and deregistration on the port.
fixed Specify the multicast groups currently registered on the switch are applied to the port, but any subsequent registrations or deregistrations do not affect the port. Any registered multicast groups on the port are not deregistered based on the GARP timers.
forbidden Specify that all GMRP multicasts are deregistered, and prevent any further GMRP multicast registration on the port.
IF_NAME Defines a text string used as the name of the interface; ASCII string from 1 to 16 characters.

4. Example:
The following example sets interface fe1 (port 1) to normal registration:

```
switch_a(config)#set gmrp registration normal fe1
switch_a(config)#
```

---

GMRP Forward All:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set the GMRP forward all option for an interface.

3. Command Syntax:
set gmrp fwdall enable | disable IF_NAME
IF_NAME Interface name.

4. Example:
The following example enables GMRP forwarding on a Layer-2 switch for interface fe1 (port 1):

```
switch_a(config)#set gmrp fwdall enable fe1
switch_a(config)#
```

---

Set GMRP Timer:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set the values for the GMRP Join, Leave, and Leaveall timers for a specified bridge. The default is the join timer (200 milliseconds); the leave timer is 600 milliseconds (ms); and the leaveall timer is 10000 milliseconds (ms).

3. Command Syntax:
set gmrp timer [join | leave | leaveall] TIMER_VALUE IF_NAME
join Type of timer

leave Type of timer
leaveall Type of timer
TIMER_VALUE Timervalue in centiseconds.
IF_NAME Specify the name of the interface.

4. Example:
The following example sets the join timers 100 centiseconds for interface fe1 (port 1):

```
switch_a(config)#set gmrp join timer 100 fe1
switch_a(config)#
```

---

**DHCP SERVER**
DHCP Binding Table:
1. Command Mode: Privileged Exec mode
Logon to Privileged Exec Mode (Enable Mode).
The **switch_a#** prompt will show on the screen.

```
switch_a#
```

2. Usage:
Use **show dhcp-server binding** command to display DHCP Server information.

3. Command Syntax:
show dhcp-server binding

4. Example:
The following example displays DHCP Server information:

```
switch_a#show dhcp-server binding
```

---

DHCP Server Status:
1. Command Mode: Interface mode
Logon to Configure Mode (Configure Terminal Mode).
Then logon to Interface mode.
vlan1.1 means vlan 1.
The **switch_a(config-if)#** prompt will show on the screen.

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#
```

2. Usage:
Use **dhcp-server enable** command to start the DHCP Server.
Use **no dhcp-server enable** command to disable DHCP Server.

3. Command Syntax:
(no) dhcp-server enable

4. Example:
The following example starts the DHCP Server:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#dhcp-server enable
switch_a(config-if)#
```

---

DHCP Server Range:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).

The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set the default IP lease block for the DHCP Server.

3. Command Syntax:
dhcp-server range A.B.C.D A.B.C.D
A.B.C.D The default Start IP for the DHCP Server.
A.B.C.D The default End IP for the DHCP Server.

4. Example:
The following example sets the default IP lease block for the DHCP Server:

```
switch_a(config)#dhcp-server range 192.168.1.100 192.168.1.250
switch_a(config)#
```

---

DHCP Server Subnet-mask:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set the default subnet mask for the DHCP Server.
Use the no form of this command to remove this setting.

3. Command Syntax:
dhcp-server subnet-mask A.B.C.D
no dhcp-server subnet-mask
A.B.C.D The default subnet mask for the DHCP Server.

4. Example:
The following example sets the default subnet mask for the DHCP Server:

```
switch_a(config)#dhcp-server subnet-mask 255.255.255.0
switch_a(config)#
```

---

DHCP Server Gateway:
1. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:
Use this command to set the default gateway for the DHCP Server.
Use the no form of this command to remove this setting.

3. Command Syntax:
dhcp-server gateway A.B.C.D
no dhcp-server gateway
A.B.C.D The default gateway for the DHCP Server.

4. Example:
The following example sets the default gateway for the DHCP Server:

```
switch_a(config)#dhcp-server gateway 192.168.1.254
switch_a(config)#
```

---

DHCP Server DNS:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the default DNS for the DHCP Server.
Use the no form of this command to remove this setting.

3. Command Syntax:

dhcp-server dns 1 | 2 A.B.C.D
no dhcp-server dns 1 | 2
A.B.C.D The default DNS for the DHCP Server.

4. Example:

The following example sets the default DNS for the DHCP Server:

```
switch_a(config)#dhcp-server dns 1 192.168.1.20
switch_a(config)#
```

---

DHCP Server Lease Time:

1. Command Mode: Configure mode

Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

2. Usage:

Use this command to set the default lease time for the DHCP Server. Use the value 0 to reset this setting.

3. Command Syntax:

dhcp-server lease-time <0-86400>
<0-86400> The default lease time for the DHCP Server (default: 86400).

4. Example:

The following example sets the default lease time for the DHCP Server:

```
switch_a(config)#dhcp-server lease-time 86400
switch_a(config)#
```

# 8 APPENDIX

| OSD Systems Managed switches firmware release notes | | |
|---|---|---|
| **Switch Series Affected** | **Protocols/ Functions Involved** | **Release notes** |
| | | **Ver 1.94.1** |
| | | **Add New protocol or commands** |
| All | Chain protocol | Add Chain-Pass-through protocol |
| All | LLDP | Add LLDP protocol |
| All | CLI | Add CLI command - web UI can be disabled |
| All | CLI | Add CLI command -detach CPU |
| All | User Account | Add Multi user (Admin / Technician / Operator ) |
| All | System log | Add System log(Local /remote ) |
| All | VLAN | Add Port priority |
| All | Web interface | Add Clear button for RMON statistics to reset counter information and auto refresh per 10 sec |
| | | **Enhancement or changes** |
| All | VLAN | Modify :The Maxium Vlan-Number from 128 to 64. |
| All | IGMP Snooping | Modify :IGMP snooping force-forward/passive CLI and GUI for trunking port |
| All | Ring coupling | Modify :Ring Coupling Port 2 unused options string. |
| All | Web interface | Modify :SNMPv3 account limit to 20 on webpage |
| All | Loopback-Detect | Change :The max value of loopback-detect interval to 30 |
| All | NTP | Change :Limit the timezone name not to over 6 characters |
| All | NTP | Change :NTP server to [time-a.nist.gov] |
| All | Web interface | Change: web banner of the switch interface to generic interface |
| | | |

# 9 MAINTENANCE

## 9.1 INTRODUCTION

The following section outlines the fault-finding procedure for the OSD2700 modems. Please take note of the following:

- Personnel without appropriate training should not attempt any maintenance except that outlined below.
- If further maintenance is attempted you are warned that every care should be taken to ensure that internal measurements made while the equipment is operational are taken carefully as some components within the unit are expensive and may be damaged by failure of any portion of their support circuitry.
- Some components within the unit are Electrostatic (ES) sensitive and Electrostatic Discharge (ESD) precautions should be taken when performing maintenance upon the unit.

## 9.2 EXTERNAL INSPECTION

Visually check for the following:

- Check that the correct power source is connected to the power socket.
- Check that the Ethernet cables are connected to the modem correctly and that distant modem(s) have been connected correctly to any external equipment.
- Inspect the optical connectors (for fiber SFP option) for any contamination and clean using isopropyl alcohol and a lint free tissue if any contamination is detected.

## 9.3 ROUTINE MAINTENANCE

- There is no routine maintenance required with the OSD2700.

# 10 WARRANTY

Thank you for purchasing equipment designed, manufactured and serviced by Optical Systems Design (OSD). OSD warrants that at the time of shipment, its products are free from defects in material and workmanship and conforms to specifications. Our Warranty conditions are outlined below:

## 10.1 WARRANTY PERIOD

For warranty period, please contact your local OSD distributor.

## 10.2 REPAIRS

Optical Systems Design reserves the right to repair or replace faulty modules/units. Please obtain a "Return Material Authorisation" (RMA) form and number before returning goods.
Goods must be returned in adequate packing material to Optical Systems Design, Warriewood or its nominated authorised representative, for all repairs.

### 10.2.1 WARRANTY REPAIRS

Return shipments to OSD shall be at customer's expense and freight back to the customer will be at OSD expense.

### 10.2.2 OUT-OF-WARRANTY REPAIRS

OSD reserves the right to repair or replace any faulty goods. Freight costs and insurance for both journeys are met by the user. All equipment repaired by OSD will have a 3-Month Warranty from the date of dispatch.

### 10.2.3 SITE REPAIRS

By agreement site repairs may be undertaken for which out of pocket, hotel and travel expenses will be charged.

### 10.2.4 EXCLUSIONS

This warranty does not apply to defects caused by unauthorized modifications, misuse, abuse or transport damage to the equipment. All modifications to OSD's standard product will need written authorization and will be charged at normal repair rates. All modifications are to be carried out by OSD Technicians. Warranty is void if unauthorized removal and/or tampering with serial number and/or repair labels is evident.

Optical Systems Design Pty. Ltd.
7/1 Vuko Pl. Warriewood 2102
P.O. Box 891 Mona Vale
N.S.W. Australia 2103
Telephone: +61 2 9913 8540
Facsimile: +61 2 9913 8735
Email: sales@osd.com.au
Web Site: www.osd.com.au

OPTICAL
SYSTEMS
DESIGN
PTY LTD A.B.N. 83 003 020 504

Printed in Australia