IES-1081

8 FE + 2 GE SFP Managed Switch -40 to 75C, DIN-rail

User Manual

v1.00 - 1206

Preface

This manual describes how to install and use the Hardened Managed Ethernet Switch. This switch introduced here is designed to deliver full scalability with SNMP/RMON web-based management functions by providing:

To get the most out of this manual, you should have an understanding of Ethernet networking concepts.

In this manual, you will find:

Features on the Hardened Managed Ethernet Switch
- Illustrative LED functions
- Installation instructions
- Management Configuration
- SNMP, IGMP…
- Specifications

Table of Contents

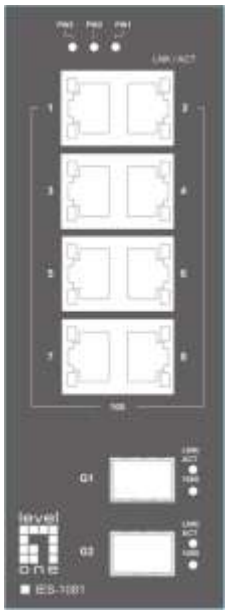
Quick Start Guide

This quick start guide describes how to install and use the Hardened Managed Ethernet Switch. This is the switch of choice for harsh environments constrained by space.

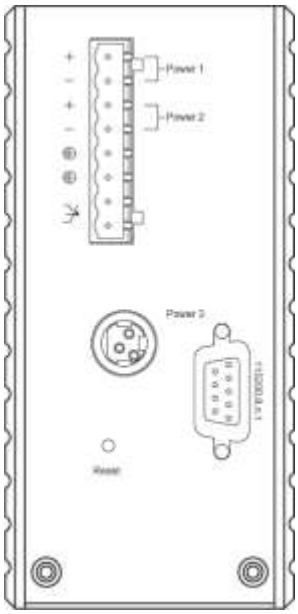
Physical Description

The Port Status LEDs and Power Inputs

Front Panel



Rear Panel



Terminal Block	PW1	+	12 – 48VDC
		–	Power Ground
	PW2	+	12 – 48VDC
		–	Power Ground
	⏚	**Earth Ground**	
		Relay Output	1A @ 24VDC
	Relay Alarm warning signal disable for following: 1. The relay contact closes if Power1 and Power2 are both failed but Power3 on 2. The relay contact closes if Power3 is failed but Power1 and Power2 are both on		

- **The relay output is normal open position when there is no power to the switch. Please do not connect any power source to this terminal to prevent shorting your power supply.**
- **There are three power inputs can be used. Redundant power function is supported**

PW3 is DC Jack type with 12VDC input

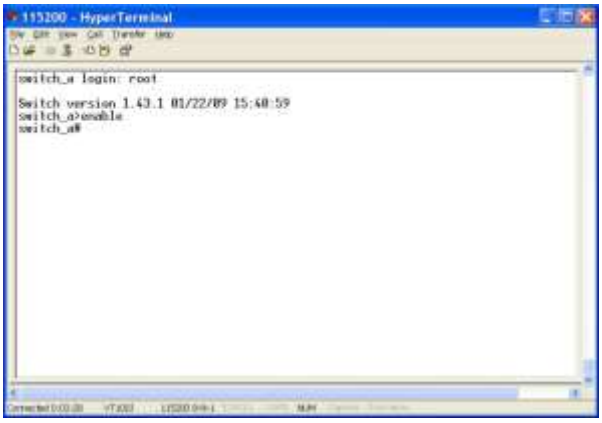
LED	Status	Description
PW 1,2,3	Steady	Power On
	Off	Power Off
10/100Base-TX & 100Base-FX		
LNK/ACT	Steady	Network connection established
	Flashing	Transmitting or Receiving data
100	Steady	Connection at 100Mbps
10/100/1000Base-TX & 1000Base-FX & SFP		
LNK/ACT	Steady	Network connection established
	Flashing	Transmitting or Receiving data
1000	Steady	Connection at 1000Mbps

Functional Description

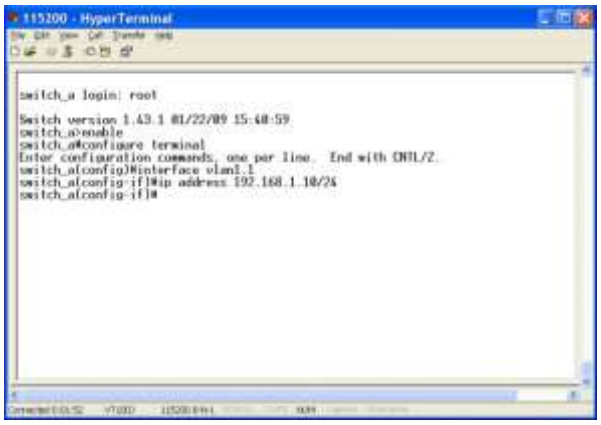
- Complies with EN50121-4 environmental requirements for railway applications.
- Meets NEMA TS1/TS2 Environmental requirements such as temperature, shock, and vibration for traffic control equipment.
- Meets EN61000-6-2 & EN61000-6-4 EMC Generic Standard Immunity for industrial environment.
- Manageable via SNMP, Web-based, Telnet, and RS-232 console port.
- Supports IEEE802.3/802.3u/802.3ab/802.3z/802.3x. Auto-negotiation: 1000Mbps-full-duplex; 10/100Mbps-full/half-duplex; Auto MDI/MDIX.
- 100Base-FX: Multi mode SC or ST type, Single mode SC or ST type. 100Base-BX: WDM Single mode SC type.
- 1000Base-SX/LX: Multi mode SC type, Single mode SC type. 1000Base-BX: WDM Single mode SC type.
- Supports 8192 MAC addresses. Provides 2M bits memory buffer.
- Store-and-forward mechanism.
- Full wire-speed forwarding rate.
- Alarms for power and port link failure by relay output.
- Power Supply: Redundant DC Terminal Block power inputs and 12VDC DC JACK with 100-240VAC external power supply.
- Operating voltage and Max. current consumption: 0.92A @ 12VDC, 0.46A @ 24VDC, 0.23A @ 48VDC. Power consumption: 11W Max.
- -40°C to 75°C (-40°F to 167°F) operating temperature range. Tested for functional operation @ -40°C to 85°C (-40°F to 185°F).
- Supports DIN-Rail and Panel Mounting installation.

Console Configuration

- 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.
- 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.



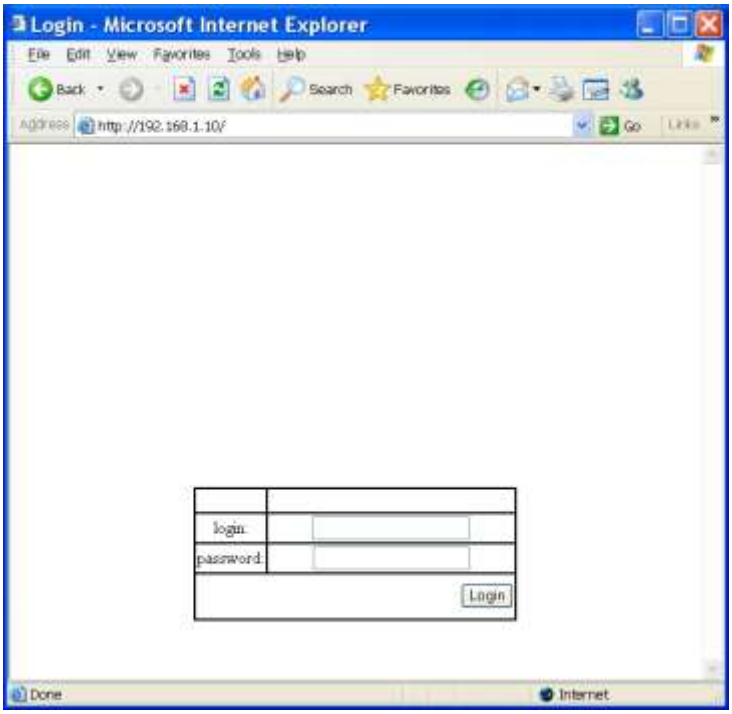
- Logon to Privileged Exec Mode (Enable Mode):
  At the "switch_a>" prompt just type in "enable" and press <Enter> to logon to Privileged Exec Mode (or Enable Mode). And the "switch_a#" prompt will show on the screen.
- Logon to Configure Mode (Configure Terminal Mode):
  At the "switch_a#" prompt just 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.



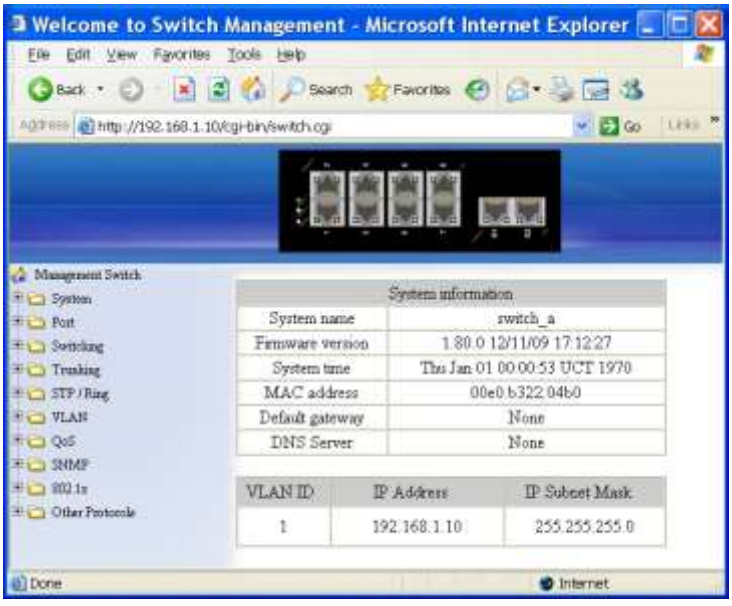
Web Configuration

- 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:

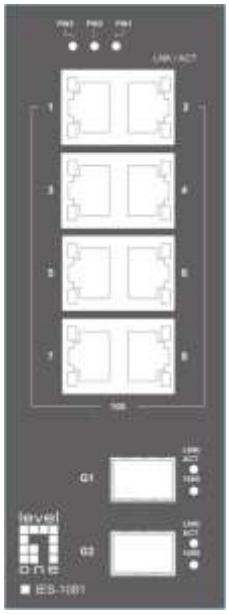


- Enter the factory default login ID: root.
  Enter the factory default password (no password).
  Then click on the "Login" button to log on to the switch.



Overview

Hardened Managed Ethernet Switch



Front View

Package Contents

When you unpack the product package, you shall find the items listed below. Please inspect the contents, and report any apparent damage or missing items immediately to your authorized reseller.

- IES-1081
- Quick Installation Guide
- CD User Manual
- RS232 cable

Product Highlights

Basic Features

- Complies with EN50121-4 environmental requirements for railway applications.
- Meets NEMA TS1/TS2 Environmental requirements such as temperature, shock, and vibration for traffic control equipment.
- Meets EN61000-6-2 & EN61000-6-4 EMC Generic Standard Immunity for industrial environment.
- Manageable via SNMP, Web-based, Telnet, and RS-232 console port.
- Supports IEEE802.3/802.3u/802.3ab/802.3z/802.3x. Auto-negotiation: 1000Mbps-full-duplex; 10/100Mbps-full/half-duplex; Auto MDI/MDIX.
- 100Base-FX: Multi mode SC or ST type, Single mode SC or ST type. 100Base-BX: WDM Single mode SC type.
- 1000Base-SX/LX: Multi mode SC type, Single mode SC type. 1000Base-BX: WDM Single mode SC type.
- Supports 8192 MAC addresses. Provides 2M bits memory buffer.
- Store-and-forward mechanism.
- Full wire-speed forwarding rate.
- Alarms for power and port link failure by relay output.
- Power Supply: Redundant DC Terminal Block power inputs and 12VDC DC JACK with 100-240VAC external power supply.
- Operating voltage and Max. current consumption: 0.92A @ 12VDC, 0.46A @ 24VDC, 0.23A @ 48VDC. Power consumption: 11W Max.
- -40°C to 75°C (-40°F to 167°F) operating temperature range. Tested for functional operation @ -40°C to 85°C (-40°F to 185°F).
- Supports DIN-Rail and Panel Mounting installation.

Management Support

VLAN

- Port-based VLAN
- IEEE802.1Q tagged VLAN

TRUNKING

- MAC-based Trunking with automatic link fail-over

PORT-SECURITY

- Per-port programmable MAC address locking
- Up to 24 Static Secure MAC addresses per port
- IEEE802.1x Port-based Network Access Control

PORT-MIRRORING

- Port-mirroring

QOS (IEEE802.1p Quality of Service)

- 4 priority queues

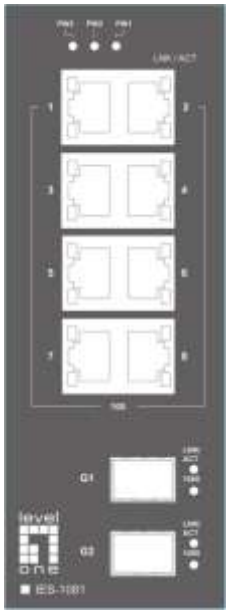
INTERNETWORKING PROTOCOLS

- Bridging:
  - IEEE802.1s Multiple Spanning Tree
  - IEEE802.1w Rapid Spanning Tree
  - IEEE802.1D Spanning Tree compatible
  - IEEE802.1Q – GVRP
  - Ring
- IP Multicast:
  - IGMP Snooping
- Rate Control
- NTP

NETWORK MANAGEMENT METHODS

- Console port access via RS-232 cable (CLI, Command Line Interface)
- Telnet remote access
- SNMP agent:
  - MIB-2 (RFC1213)
  - Bridge MIB (RFC1493)
  - RMON MIB (RFC2819) – statistics, history, alarm and events
  - VLAN MIB (IEEE802.1Q/RFC2674)
  - Private MIB
- Web browser
- TFTP software-upgrade capability

Front Panel Display



- POWER

This LED comes on when the switch is properly connected to power and turned on.

- Port Status LEDs

The LEDs are located on the front panel, displaying status for each respective port. Please refer to the following table for more details.

LED	Status	Description
PW 1,2,3	Steady	Power On
	Off	Power Off
10/100Base-TX & 100Base-FX		
LNK/ACT	Steady	Network connection established
	Flashing	Transmitting or Receiving data
100	Steady	Connection at 100Mbps
10/100/1000Base-TX & 1000Base-FX & SFP		
LNK/ACT	Steady	Network connection established
	Flashing	Transmitting or Receiving data
1000	Steady	Connection at 1000Mbps

Physical Ports

The Hardened Managed Ethernet Switch provides:

Number of ports		
10/100Base-TX	100Base-FX/BX 100Base SFP	Gigabit: 10/100/1000Base-TX 1000Base-SX/LX/BX 1000Base SFP
8	0	0, 1, 2
6	2	0, 1, 2
4	2	0, 1, 2
4	4	0

CONNECTIVITY

- RJ-45 connectors on TX ports
- ST or SC connector on 100Base-FX fiber port
- SC connector on 100Base-BX fiber port
- Duplex LC connector on SFP 100Base-FX/BX fiber transceiver
- SC connector on 1000Base-SX/LX/BX fiber port
- Duplex LC connector on SFP 1000Base-SX/LX/BX fiber transceiver

MODE SELECTION

- 10Base-T full-duplex mode
- 10Base-T half-duplex mode
- 100Base-TX full-duplex mode
- 100Base-TX half-duplex mode
- 100Base-FX full-duplex mode
- 1000Base-T/SX/LX full-duplex mode
- Auto-negotiating mode

Switch Management

Web-based browser interface

The switch also boasts a point-and-click browser-based interface that lets user access full switch configuration and functionality from a Netscape or Internet Explorer browser.

Administration console via RS-232 serial port (CLI)

The switch provides an onboard serial port, which allows the switch to be configured via a directly connected terminal.

External SNMP-based network management application

The switch can also be configured via SNMP.

Installation

This chapter gives step-by-step instructions about how to install the switch:

Selecting a Site for the Switch

As with any electric device, you should place the switch where it will not be subjected to extreme temperatures, humidity, or electromagnetic interference. Specifically, the site you select should meet the following requirements:

-The ambient temperature should be between -40°C to 75°C (-40°F to 167°F).

-The relative humidity should be less than 95 percent, non-condensing.

-Surrounding electrical devices should not exceed the electromagnetic field (RFC) standards.

-Make sure that the switch receives adequate ventilation. Do not block the ventilation holes on each side of the switch.

Connecting to Power

Redundant DC Terminal Block Power Inputs or 12VDC DC Jack:

12VDC DC Jack

Step 1: Connect the supplied AC to DC power adapter to the receptacle on the topside of the switch.

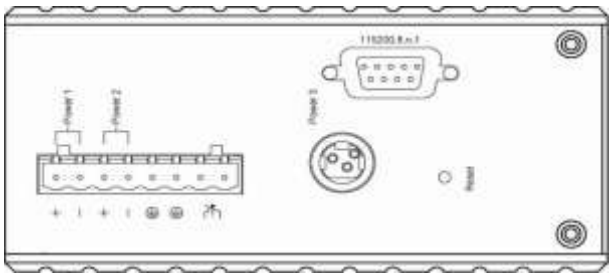
Step 2: Connect the power cord to the AC to DC power adapter and attach the plug into a standard AC outlet with the appropriate AC voltage.

Redundant DC Terminal Block Power Inputs

There are two pairs of power inputs for use with redundant power sources. You only need to have one power input connected to run the switch.

Step 1: Connect the DC power cord to the plug-able terminal block on the switch, and then plug it into a standard DC outlet.

Step 2: Disconnect the power cord if you want to shut down the switch.



Top View

Alarms for Power Failure

Step 1: There are two pins on the terminal block used for power failure detection. It provides the normally closed output when the power source is active. Use this as a dry contact application to send a signal for power failure detection.

Terminal Block	PW1	+	12 – 48VDC
		–	Power Ground
	PW2	+	12 – 48VDC
		–	Power Ground
	⏚	**Earth Ground**	
		Relay Output	1A @ 24VDC
	Relay Alarm warning signal disable for following: 3. The relay contact closes if Power1 and Power2 are both failed but Power3 on 4. The relay contact closes if Power3 is failed but Power1 and Power2 are both on		

DC Jack	PW3	**DC Jack**	12VDC

Special note:
The relay output is normal open position when there is no power to the switch. Please do not connect any power source to this terminal to prevent shorting your power supply.

Connecting to Your Network

Cable Type & Length

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.

Cable Specifications

Speed	Connector	Port Speed Half/Full Duplex	Cable	Max. Distance
10Base-T	RJ-45	10/20 Mbps	2-pair UTP/STP Cat. 3, 4, 5	100 m
100Base-TX	RJ-45	100/200 Mbps	2-pair UTP/STP Cat. 5	100 m
1000Base-T	RJ-45	2000 Mbps	4-pair UTP/STP Cat. 5	100 m
100Base-FX	ST, SC	200 Mbps	MMF (62.5µm)	2 km
100Base-FX	ST, SC	200 Mbps	SMF (10µm)	20, 40, 75, 100 km
100Base-BX	SC	200 Mbps	MMF (62.5µm)	2, 5 km
100Base-BX	SC	200 Mbps	SMF (10µm)	20, 40 km
1000Base-SX	SC	2000 Mbps	MMF (62.5µm)	220 m, 2 km
1000Base-SX	SC	2000 Mbps	MMF (50µm)	550 m
1000Base-LX	SC	2000 Mbps	SMF (10µm)	10, 20, 50 km
1000Base-BX	SC	2000 Mbps	SMF (10µm)	20, 40 km
SFP				
1000Base-SX	Duplex LC	2000 Mbps	MMF (62.5µm)	550 m, 2 km
1000Base-LX	Duplex LC	2000 Mbps	SMF (9µm)	10, 40, 60 km
1000Base-BX	Duplex LC	2000 Mbps	SMF (9µm)	70 km

Cabling

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

<Note> Always ensure that the power is off before any installation.

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.

Switch Management

This chapter explains the methods that you can use 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

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.

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.

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.

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.

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.

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.**

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.

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.

SNMP & RMON Management

This chapter describes the switch's Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON) capabilities.

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.

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.

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.

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.

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.

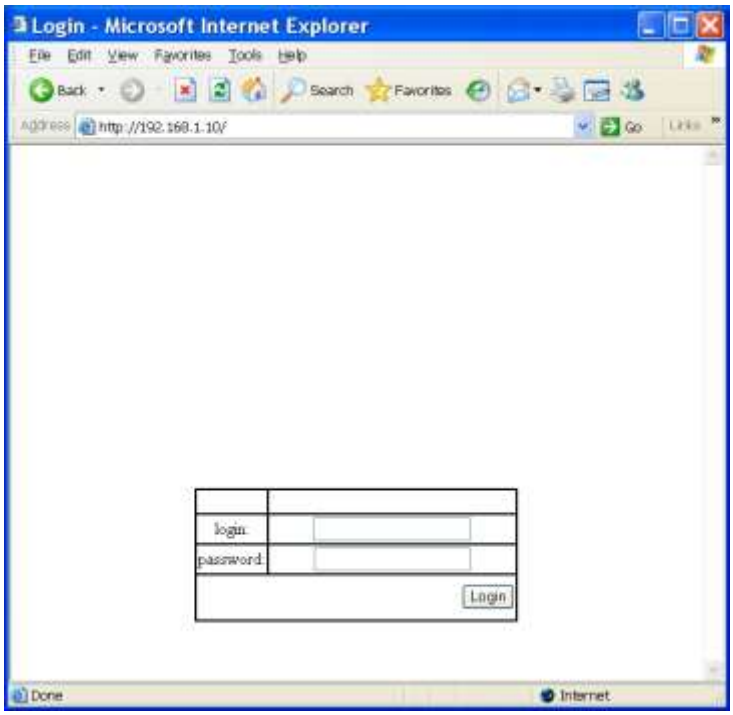
- The dot1dStatic Group – contains objects that describe the entity's destination-address filtering status. This group is applicable to any type of bridge which performs destination-address filtering.

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.

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.

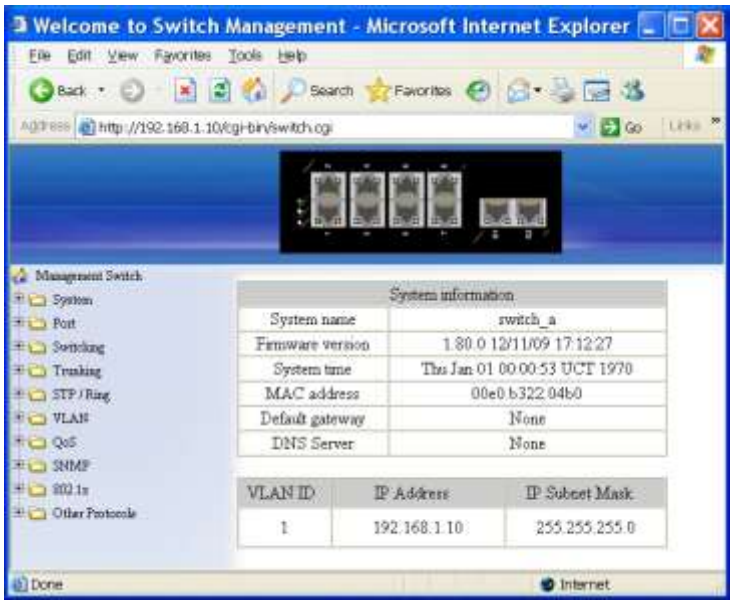
PASSWORD

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.

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, Alarm Setting, Reboot, Logout

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

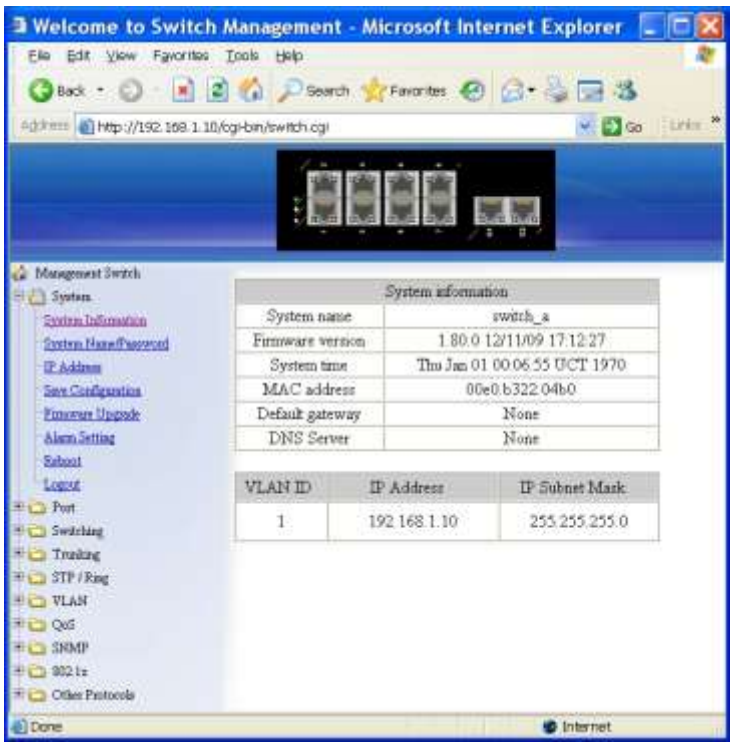
QOS
Global Configuration, 802.1p Priority, DSCP

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

802.1X
Radius Configuration, Port-Based Authentication

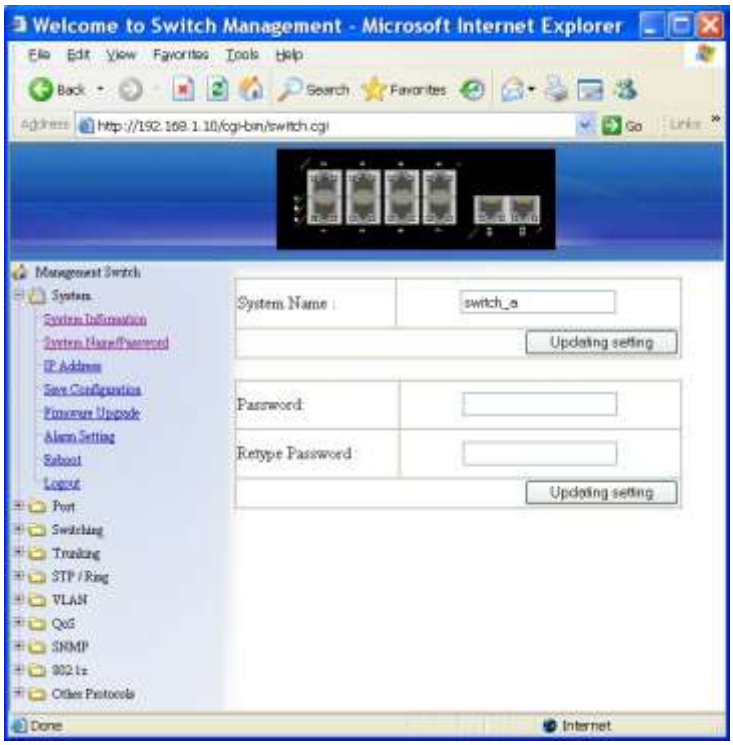
OTHER PROTOCOLS
GVRP, IGMP Snooping, NTP

System



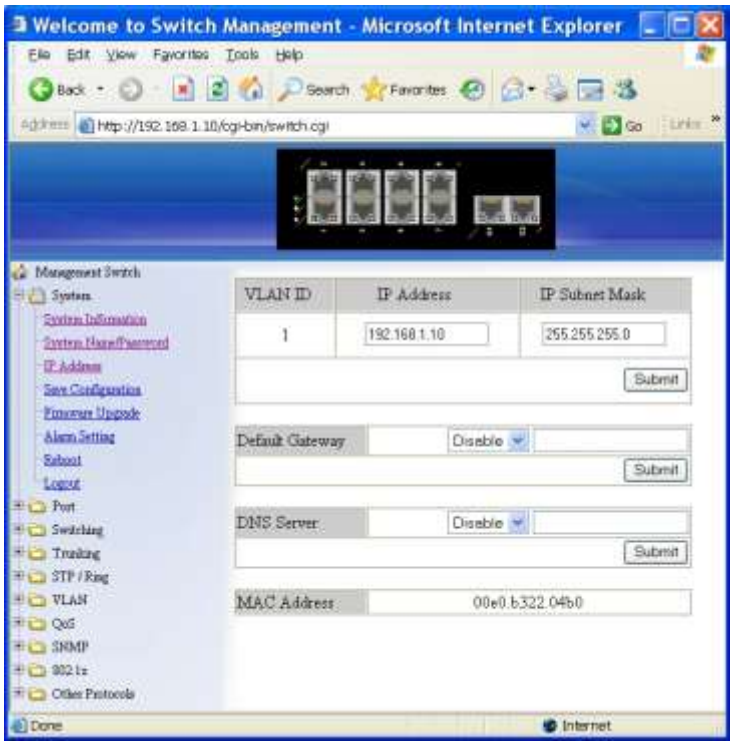
System Information

View System information, VLAN ID, IP Address, and IP Subnet Mask of the 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.



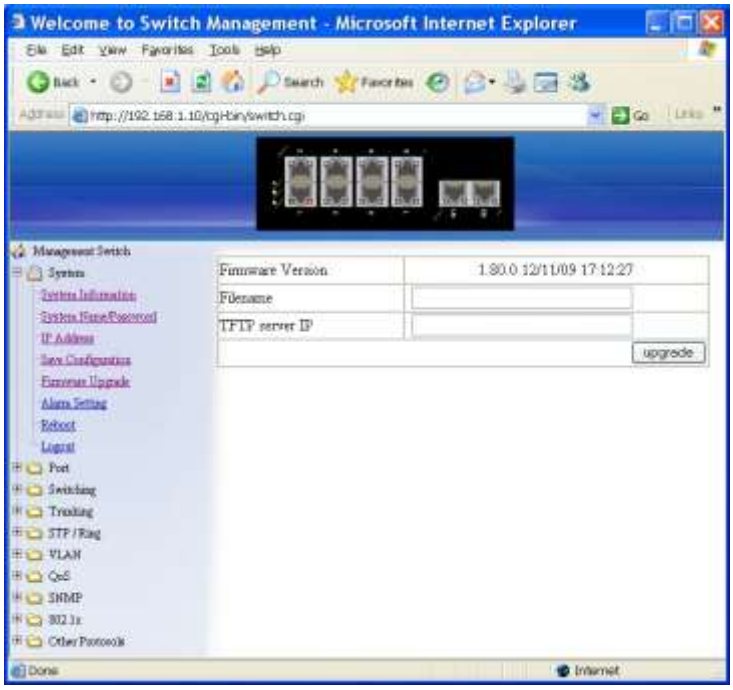
IP Address

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.
   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.)
6. Submit: Click "Submit" button when you finished Default Gateway.
7. DNS Server: Click "DNS Server" drop-down menu to choose "Disable" or "Enable" from the "DNS Server" drop-down list to disable or enable DNS Server Setting for the switch.
   Click the text box and type a new address to change the DNS Server. (Need to choose "Enable" from the "DNS Server" drop-down menu.)

8. Submit: Click "Submit" button when you finished DNS Server.

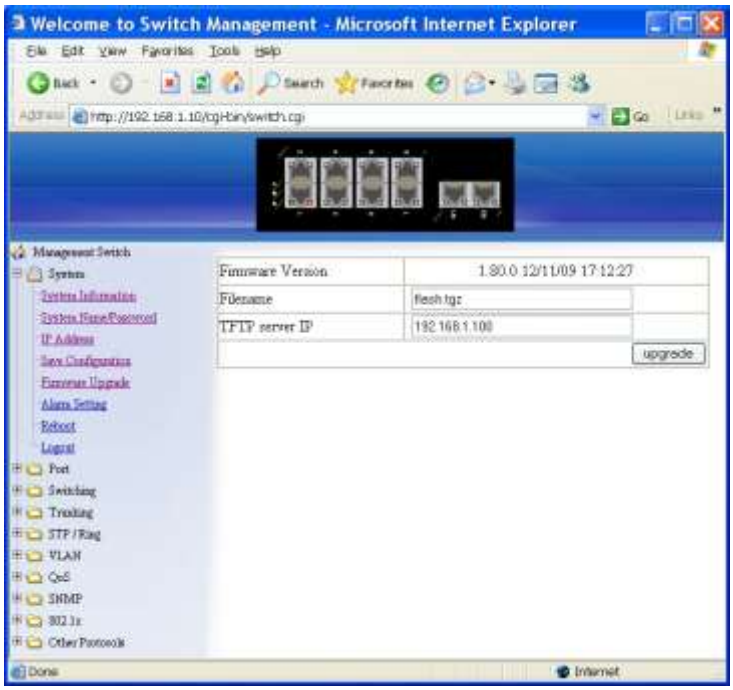
Save Configuration

1. Load config from TFTP server:
   Click in "TFTP Server" text box and type the TFTP server IP address from where the file will be obtained.
   Click in "FILE" text box and type the name of the file that will be obtained.
   Click "Load" button to load the file from the TFTP server.
2. Backup config to TFTP server:
   Click in "TFTP Server" text box and type the TFTP server IP address to where the file will be back upped.
   Click in "FILE" text box and type the name of the file that will be back upped.
   Click "Backup" button to backup the file to the TFTP server.
3. Save Configuration: Click "Save Configuration" button to save your configuration settings.
4. Restore Default: Click "Restore Default" button to restore the default settings of the switch.
5. 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.
6. Auto save interval (5~65536 sec): Click in "Auto save interval" text box and type a decimal number between 5 and 65536.
7. Submit: Click "Submit" button when you finished Auto save configuration.

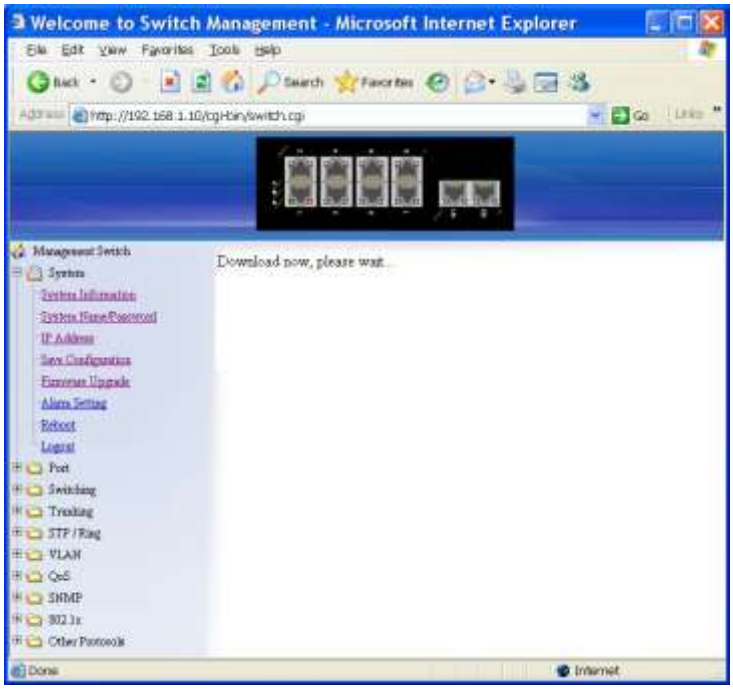


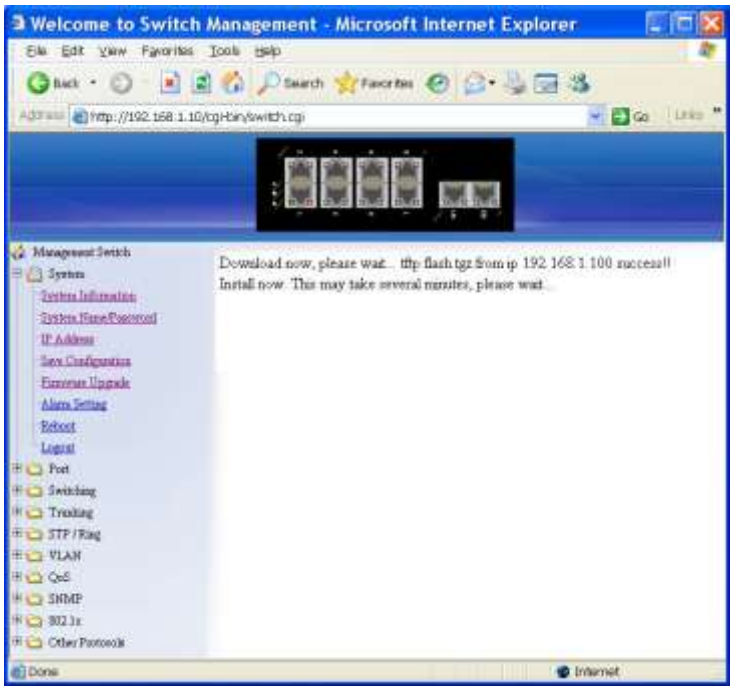
Firmware Upgrade

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.

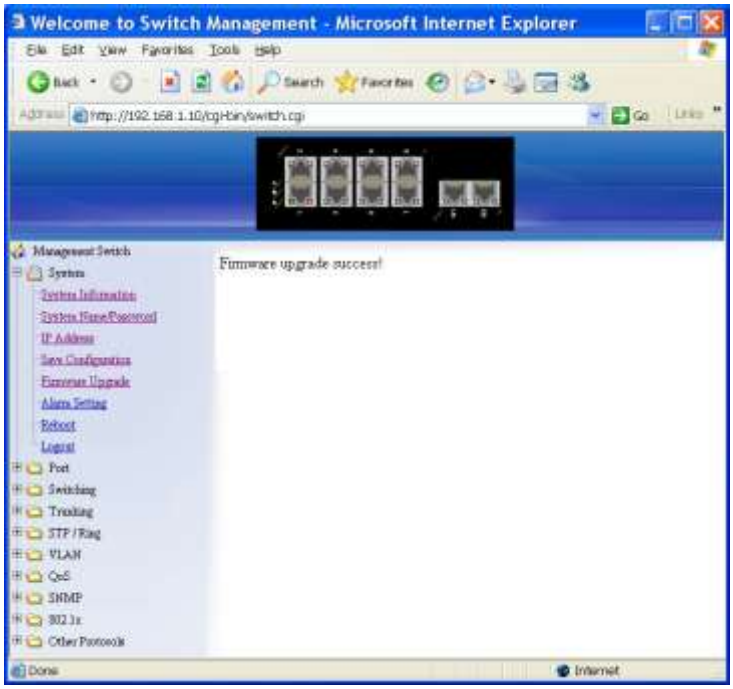


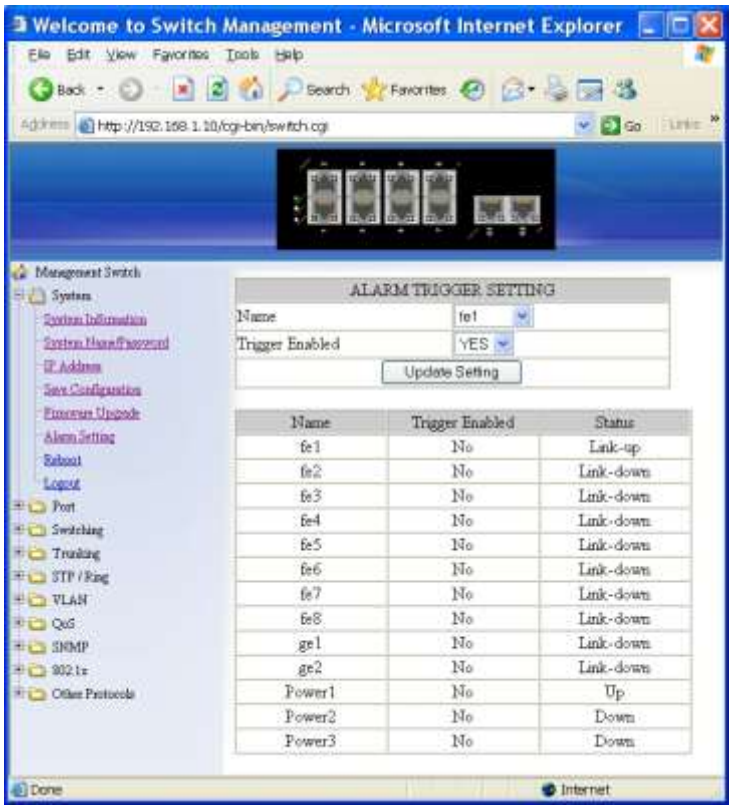
Please follow the message on the screen during the firmware upgrade process. Do not turn off the power or perform other functions during this period of time.





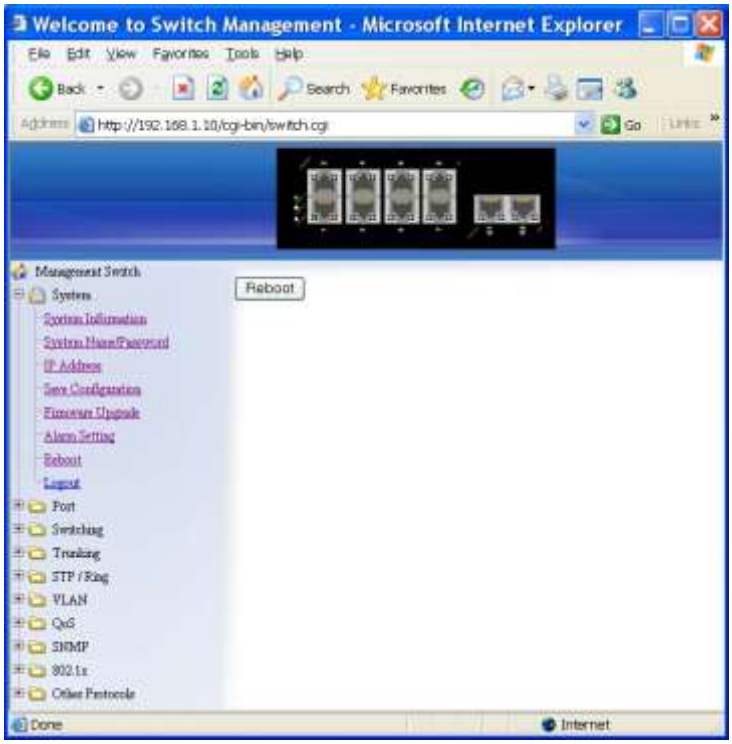
Firmware has been upgraded successfully to the switch. Reboot the switch after completing the upgrade process.





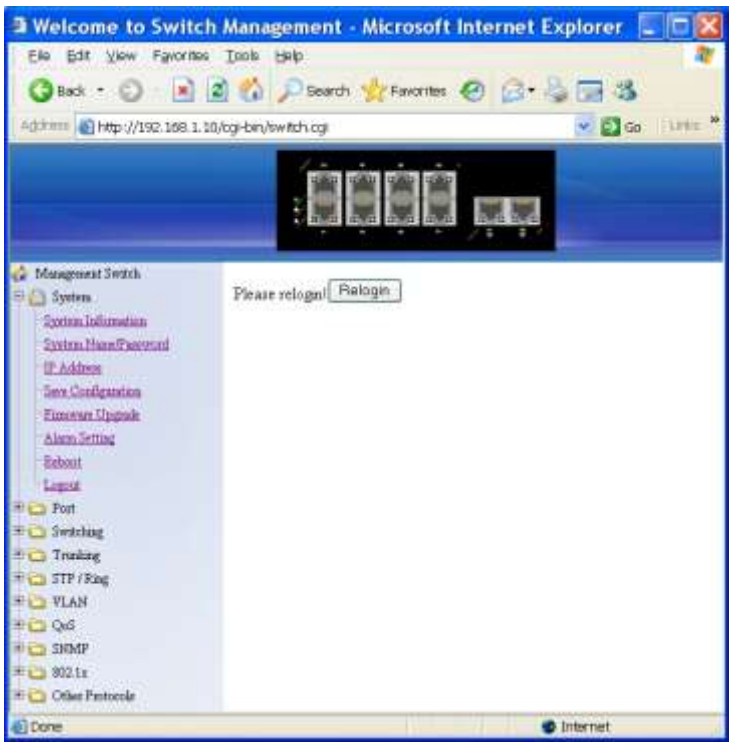
Alarm Setting

1. Name: Click "Name" drop-down menu to choose "fe1~fe8", "ge1~ge2", or "Power1~Power3" from the "Name" drop-down list.
2. Trigger Enabled: Click "Trigger Enabled" drop-down menu to choose "YES" or "NO" from the "Trigger Enabled" drop-down list to enable or disable Trigger.
3. Update Setting: Click "Update Setting" button to update settings to the switch.



Reboot

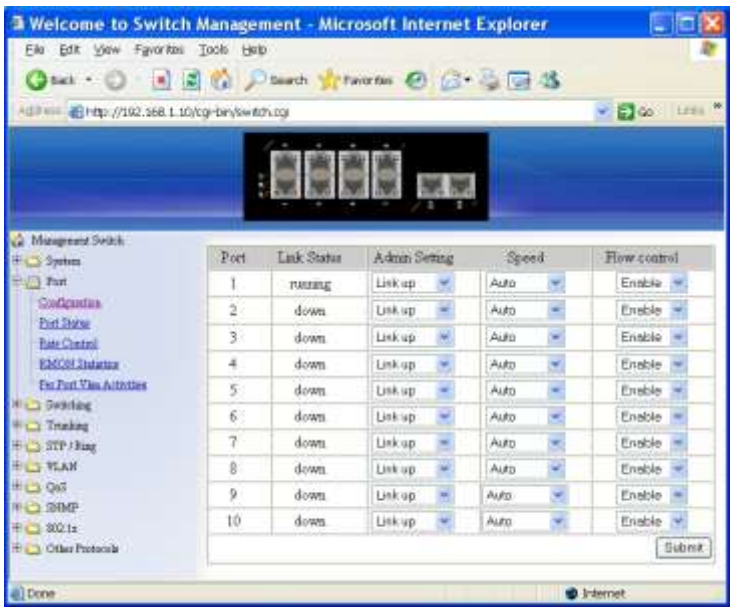
Reboot: Click "Reboot" button to restart the switch.



Logout

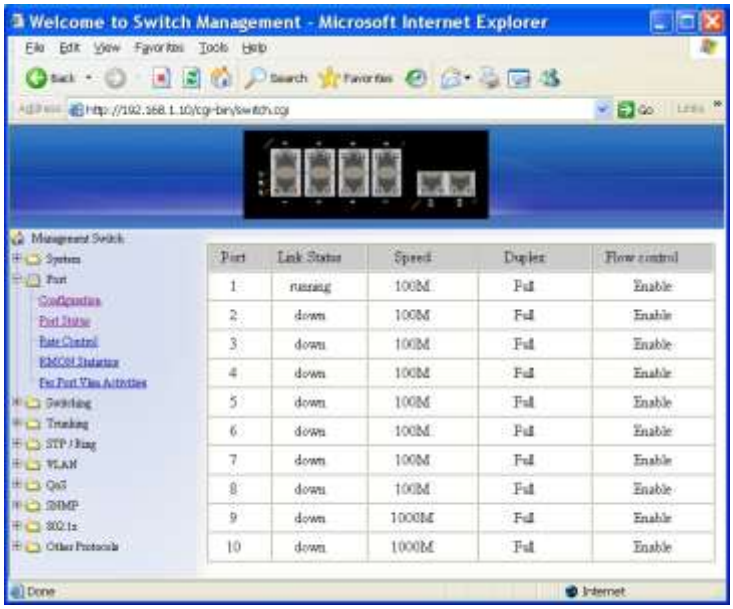
Logout: Click "Logout" button to logout of the switch.

Port



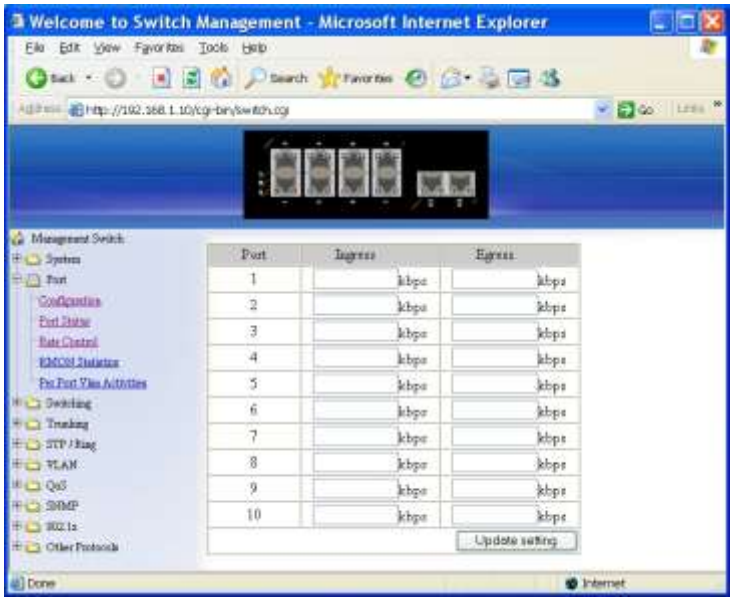
Configuration

1. 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.
2. Speed: Click "Speed" drop-down menu to change the line speed and duplex settings from the "Speed" drop-down list for the port.
3. 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.
4. Submit: Click "Submit" button when you finished configurations.



Port Status

View the Link Status, Speed, Duplex, and Flow control status for all ports.

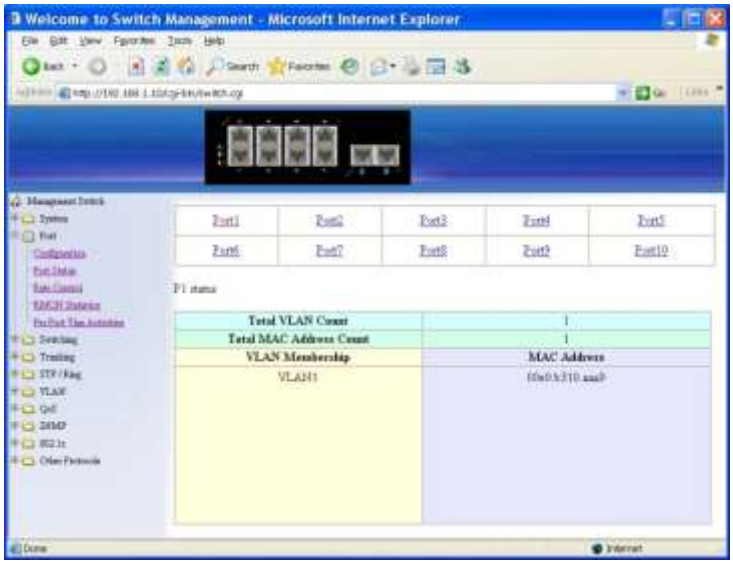


Rate Control

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

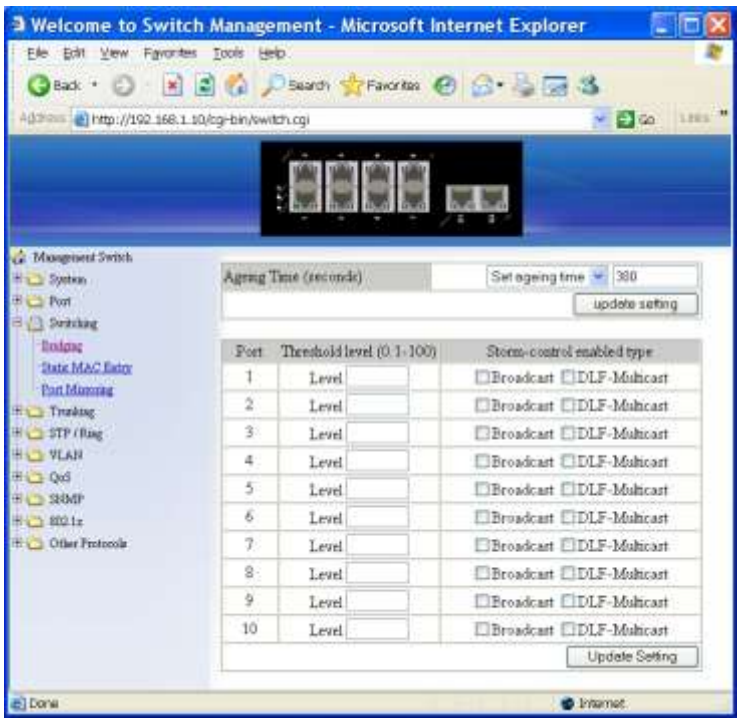
Click Port 1 ~ Port 10 to view corresponding RMON Statistics.



Per port vlan activities

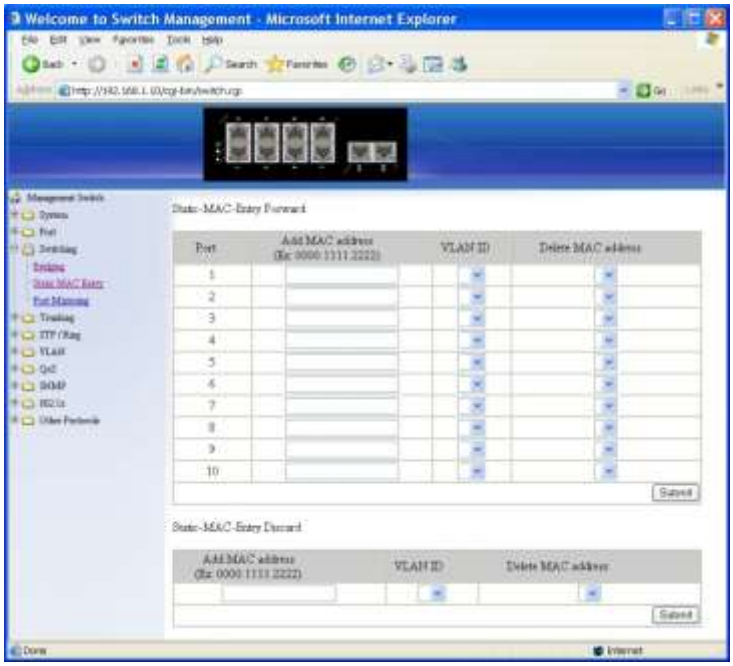
Click Port 1 ~ Port 10 to view corresponding vlan activities.

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 (0-100): 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. Update Setting: Click "Update Setting" button when you finished Threshold level and Storm-control enabled type settings.



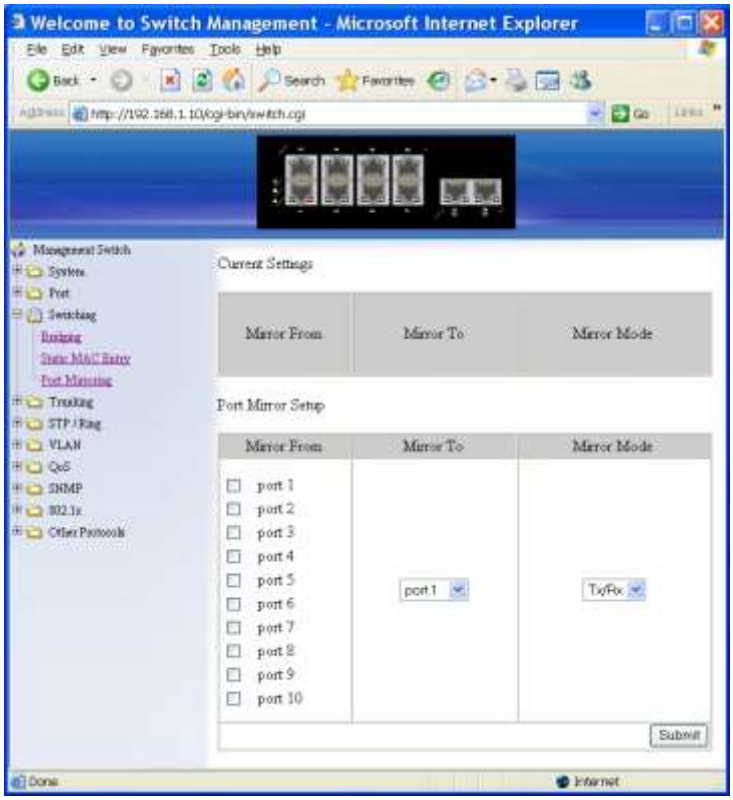
Static MAC Entry

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:

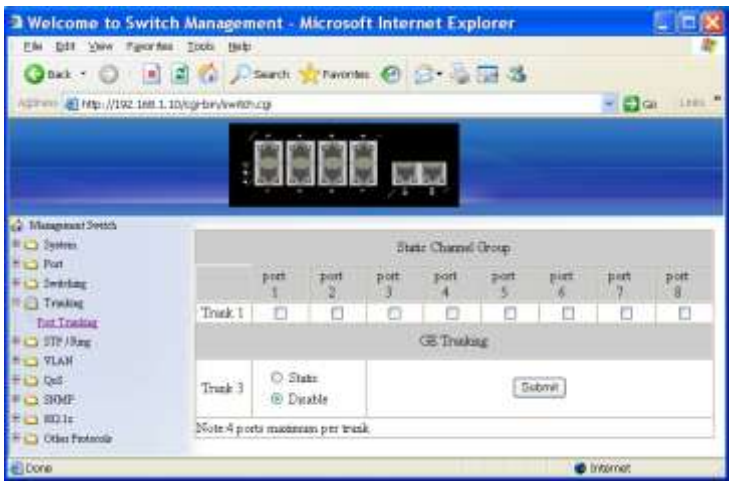
1. Add MAC address: Click in "Add MAC address" text box and type a MAC address to be discarded for the VLAN.
2. VLAN ID: VLAN ID: Click "VLAN ID" drop-down menu and choose a VLAN ID from the "VLAN ID" drop-down list.
3. Delete MAC address: Click "Delete MAC address" drop-down menu and choose a MAC address 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 10.
2. Mirror To: Click "Mirror To" drop-down menu to Choose Mirror To port (Port 1 ~ Port 10) 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.

Trunking



Port Trunking

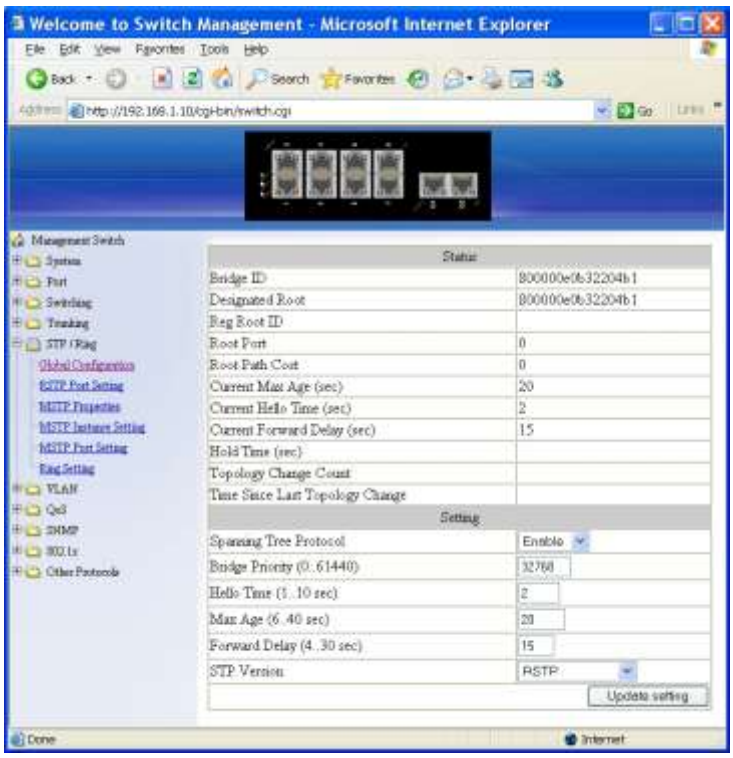
Static Channel Group:

1. Trunk 1: Click Port 1 ~ Port 8 to assign ports to Trunk 1. (Maximum 4 ports in Trunk 1.)

GE Trunking:

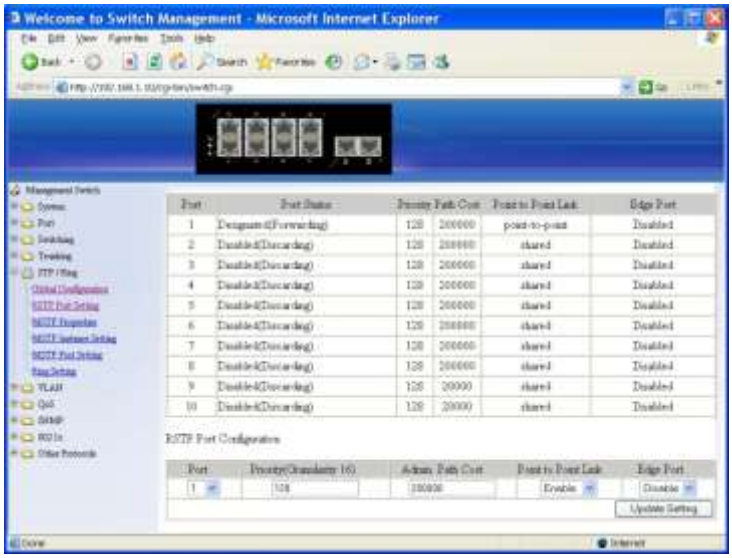
1. Trunk 3: Click "Static" or "Disable" for Trunk 3.
2. Submit: Click "Submit" button when you finished Port Trunking settings.

STP / Ring



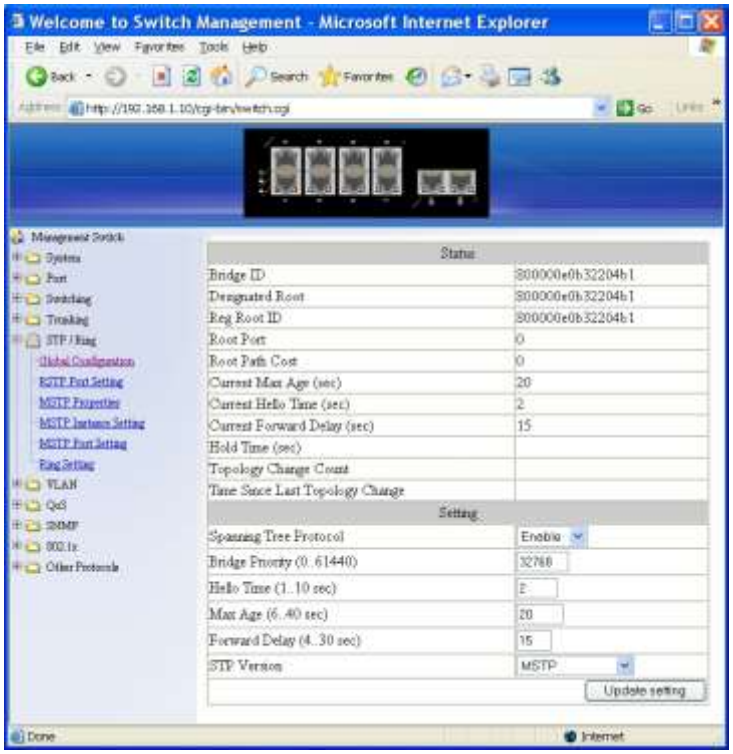
Global Configuration

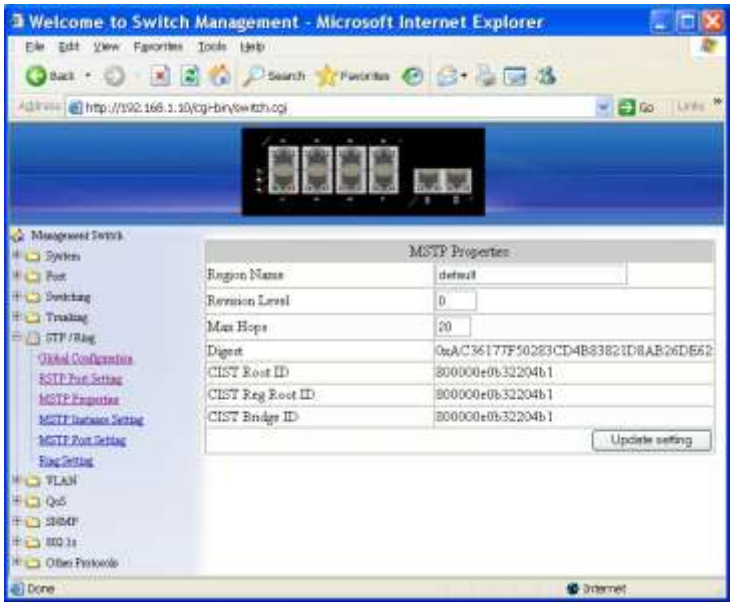
1. Spanning Tree Protocol: Click "Spanning Tree Protocol" drop-down menu to Choose "Enable" or "Disable" from "Spanning Tree Protocol" drop-down list to enable or disable Spanning Tree Protocol.
2. Bridge Priority (0..61440): Click in "Bridge Priority" text box and type a decimal number between 0 and 61440.
3. Hello Time (sec) (1..9): Click in "Hello Time" text box and type a decimal number between 1 and 9.
4. Max Age (sec) (6..28): Click in "Max Age" text box and type a decimal number between 6 and 28.
5. Forward Delay (sec) (4..30): 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.



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 1 ~ Port 10 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.



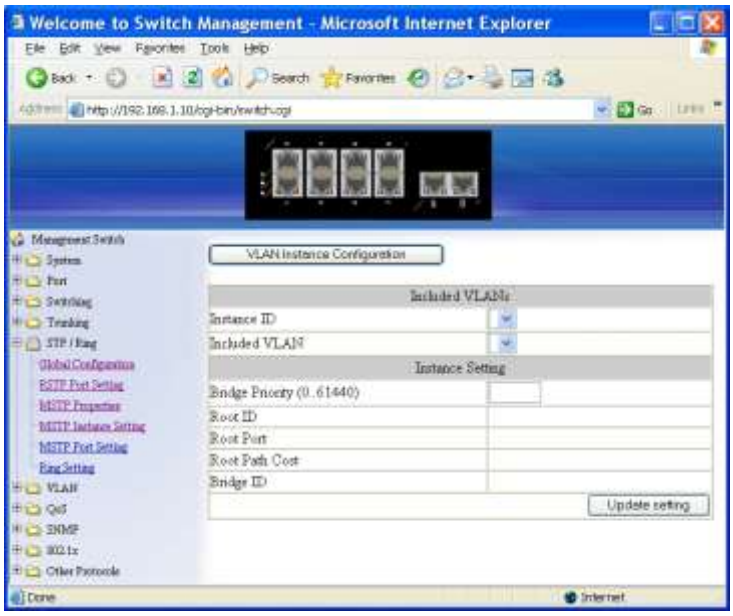


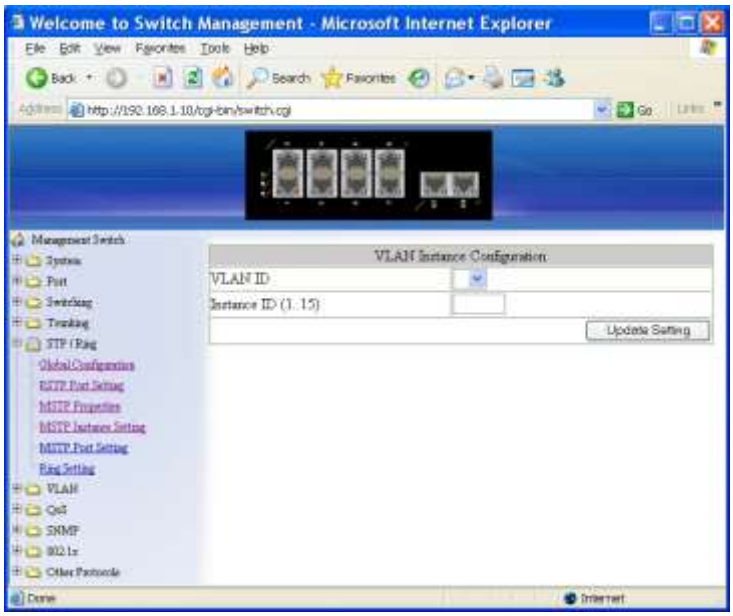
MSTP Properties

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 indefinitely 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.





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

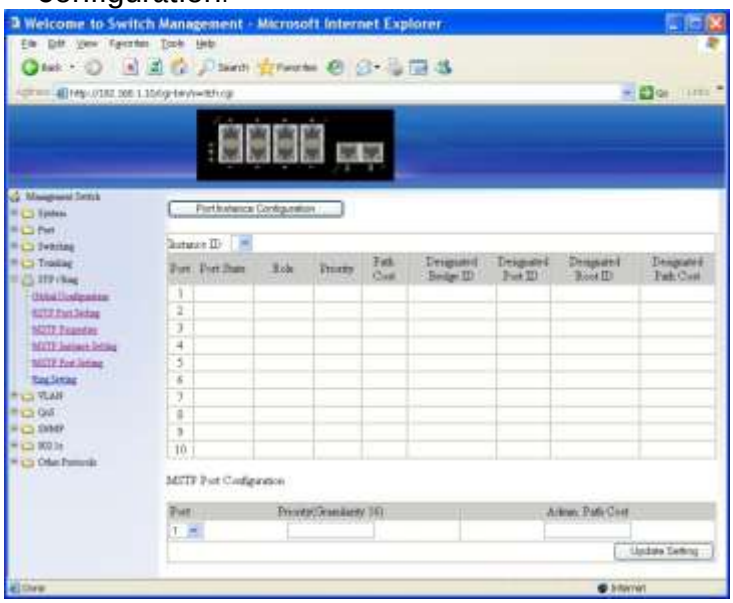
Configuration.

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.



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 Port 1 ~ Port 10 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

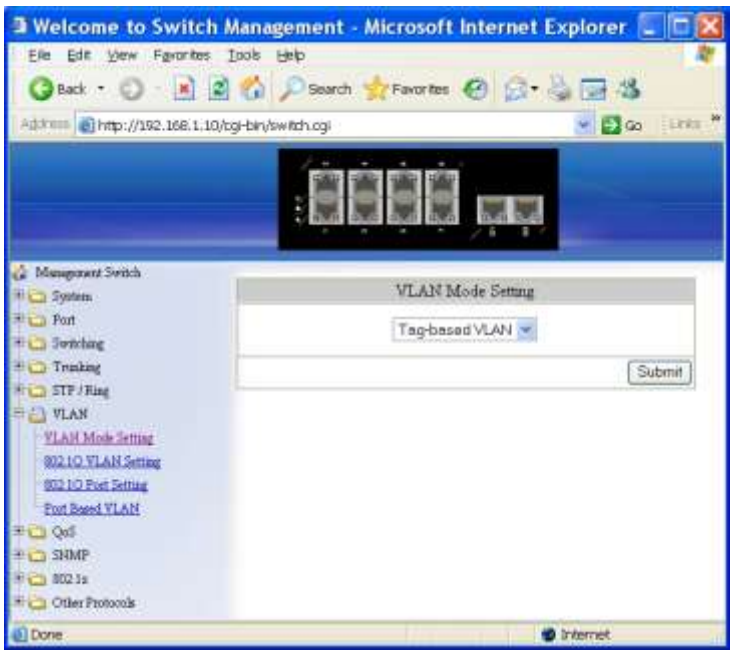
Ring state

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

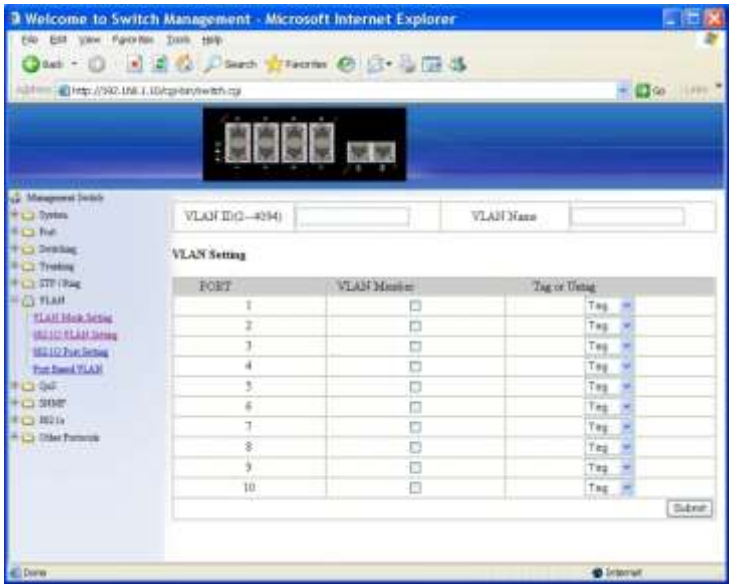
1. Ring port 1: Click "Ring port 1" drop-down menu to choose Ring port 1 from "Ring port 1" drop-down list.
2. Ring port 2: Click "Ring port 2" drop-down menu to choose Ring port 2 from "Ring port 2" drop-down list.
3. Update setting: Click "Update setting" button when you finished Set ring port.

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. Update Setting: Click "Update Setting" button when you finished VLAN Mode Setting.



802.1Q VLAN setting

Add VLAN:

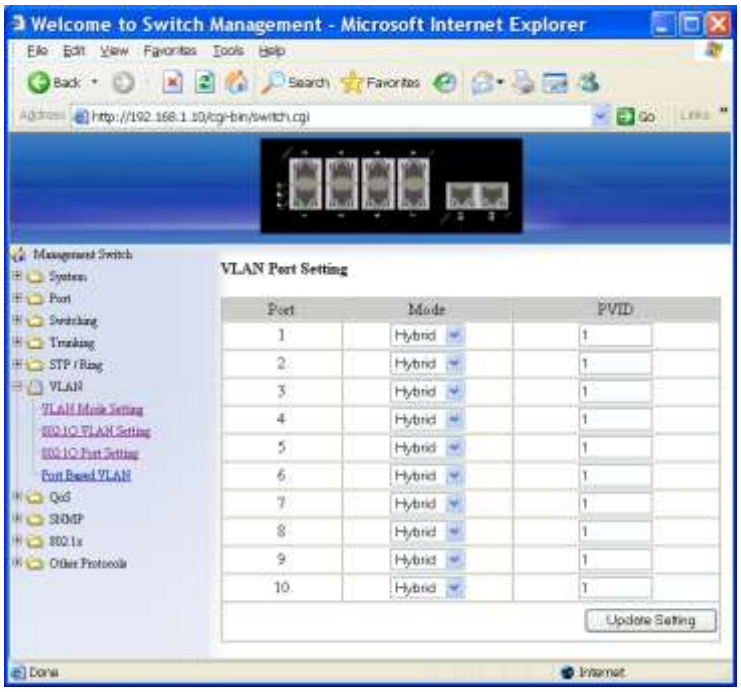
1. VLAN setting: Click "VLAN setting". The "VLAN Setting" window appears.
2. Add VLAN: Click "Add VLAN" button to create a new VLAN from "VLAN Setting" window.
3. VLAN ID(2-4094): Click in the "VLAN ID" textbox and specify a new VLAN ID number from 2 ~ 4094.
4. VLAN Name: Click in the "VLAN Name" textbox 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.

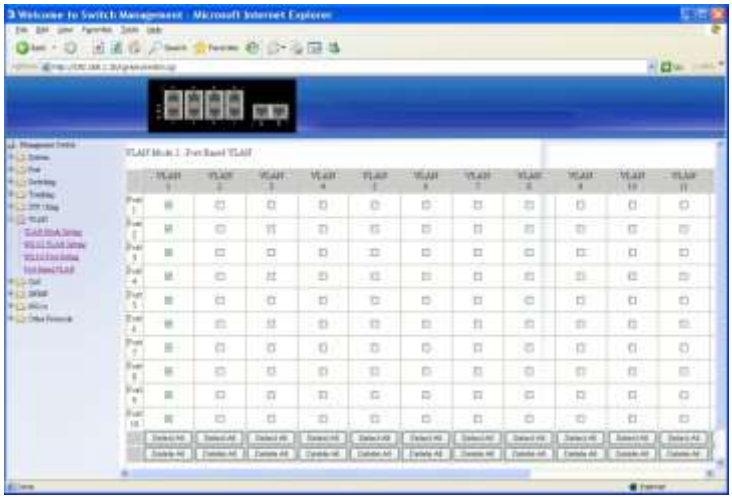
Delete VLAN:

1. VLAN setting: Click "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.



802.1Q Port Setting

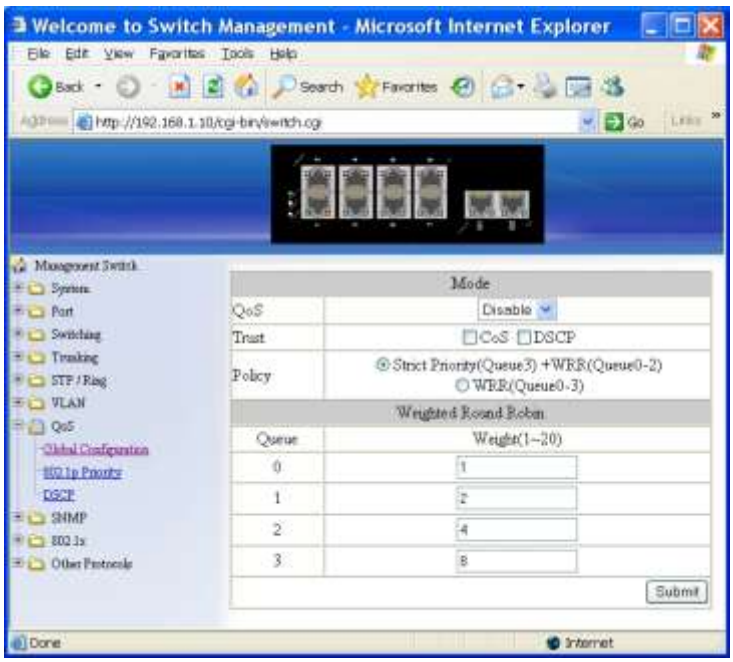
1. VLAN Port Setting: Click "VLAN Port Setting". The "VLAN Port Setting" window appears.
2. Mode: Click "Mode" drop-down menu to choose "Access", "Trunk", or "Hybrid" from "Mode" drop-down list for the port. The port will be Tag port if you choose "Trunk" Mode for the port. And the port will be Tag or 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. Update Setting: Click "Update Setting" button when you finished VLAN Port Setting.



Port Based VLAN

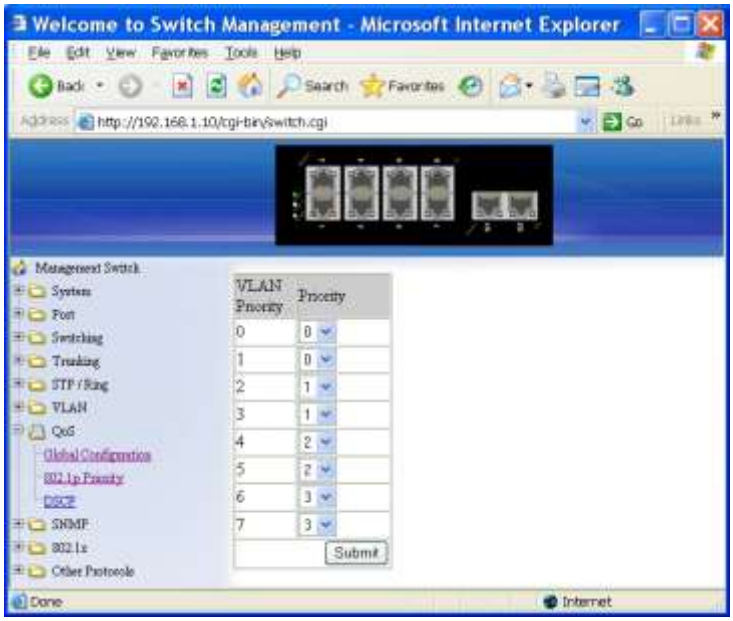
1. VLAN: Choose the port to be added to or deleted from the VLAN.
2. Select all: Click "select all" button to choose Port 1 ~ Port 10 all to be added to the VLAN.
3. Delete all: Click "delete all" button to choose Port 1 ~ Port 10 all to be deleted from the VLAN.
4. Submit: Click "Submit" button when you finished Port Based VLAN setting.

QoS



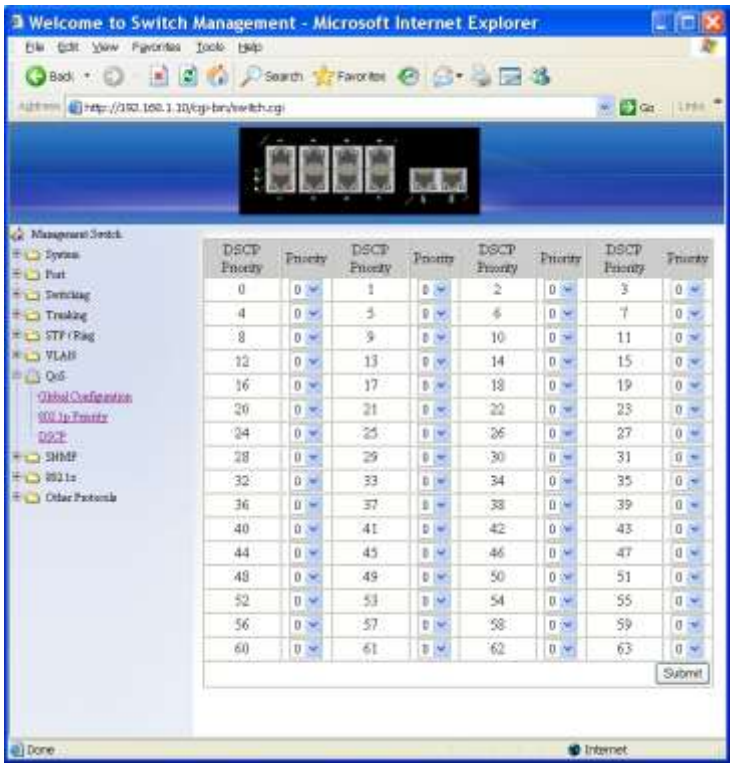
Global Configuration

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

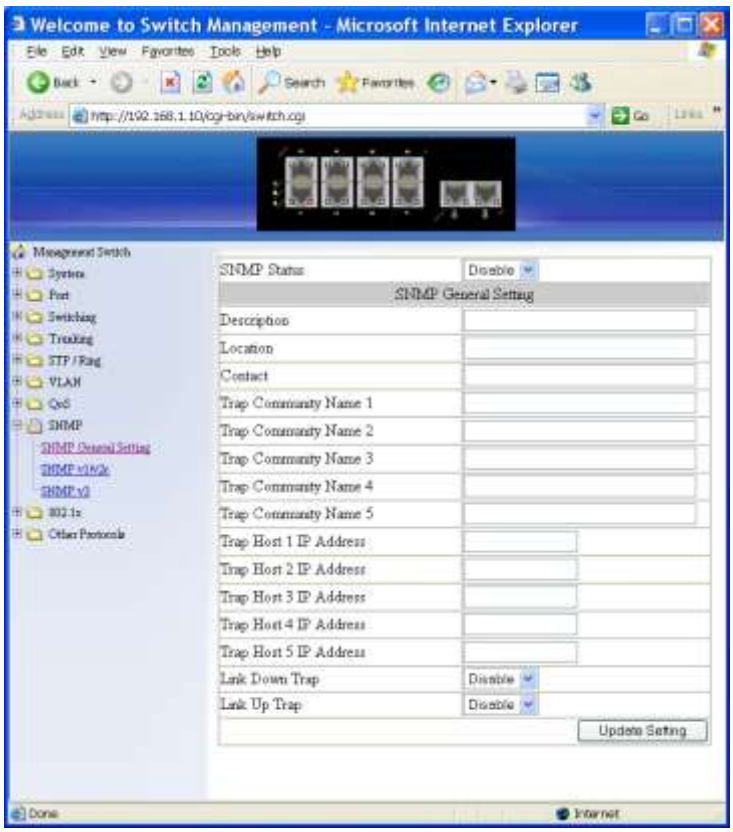
1. Priority: Click "Priority" drop-down menu from "Priority" drop-down list to choose 0 ~ 3 for VLAN Priority 0 ~ 7.
2. Submit: Click "Submit" button when you finished 802.1p priority.



DSCP

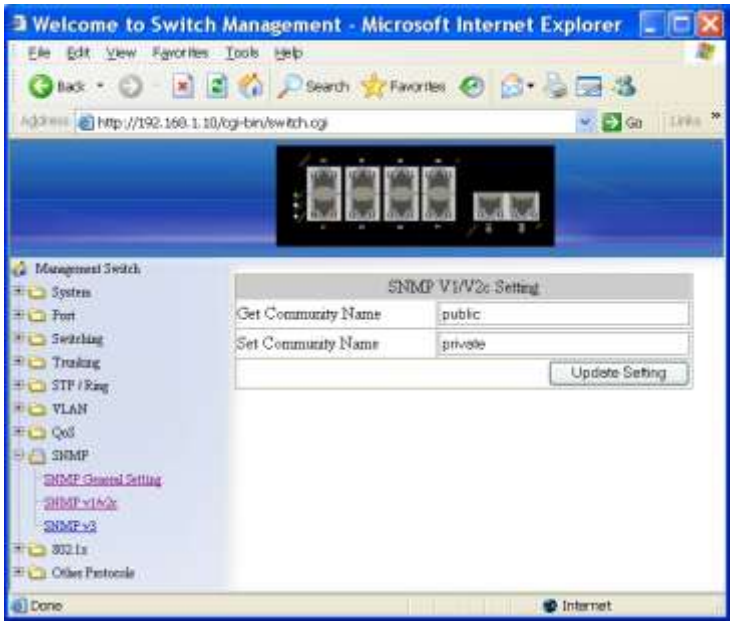
1. Priority: Click "Priority" drop-down menu from "Priority" drop-down list to choose 0 ~ 3 for DSCP Priority 0 ~ 63.
2. Submit: Click "Submit" button when you finished DSCP.

SNMP



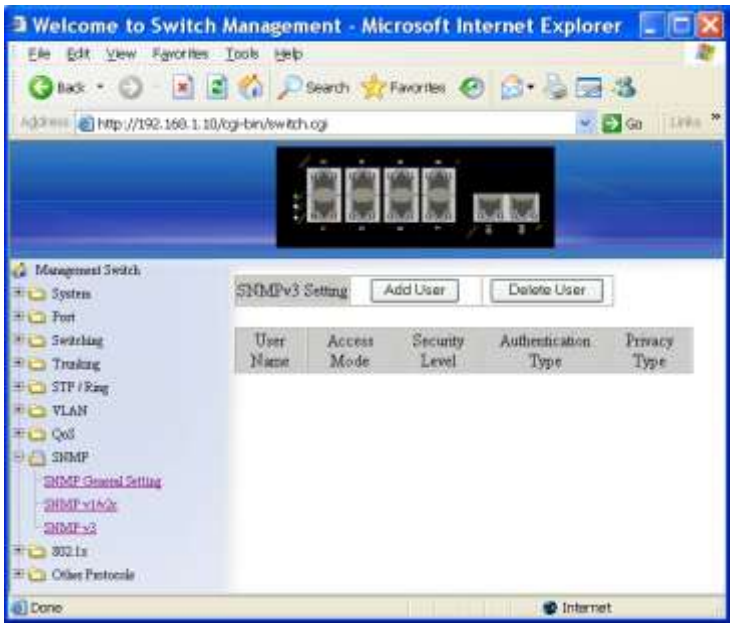
SNMP General Setting

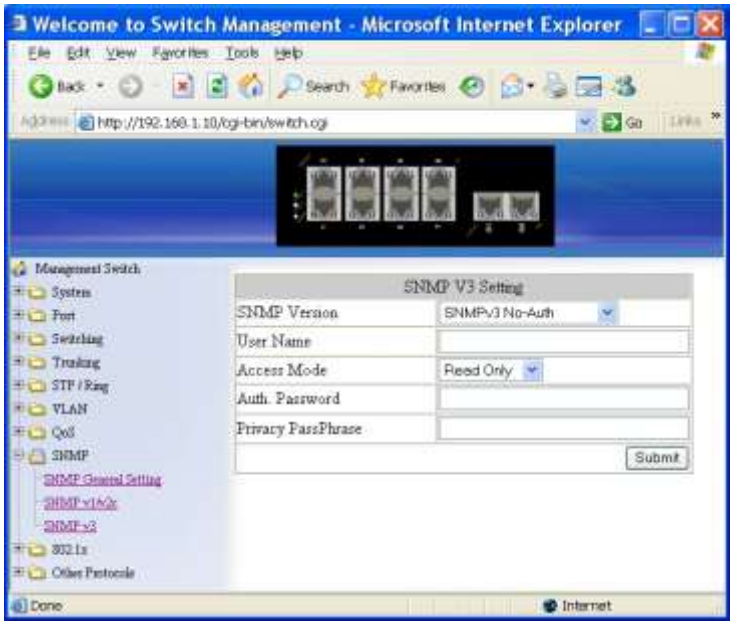
1. SNMP Status: Click "SNMP Status" drop-down menu from "SNMP Status" drop-down list to choose "Enable" or "Disable" to enable or disable SNMP.
2. Description: Click in the "Description" textbox and specify a new description for SNMP.
3. Location: Click in the "Location" textbox and specify a new location 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. 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.

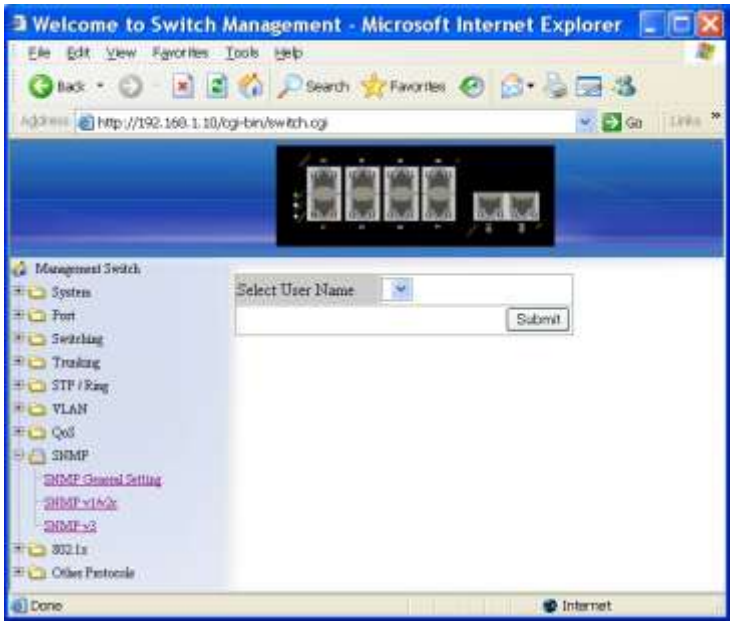




SNMP v3

Add User:

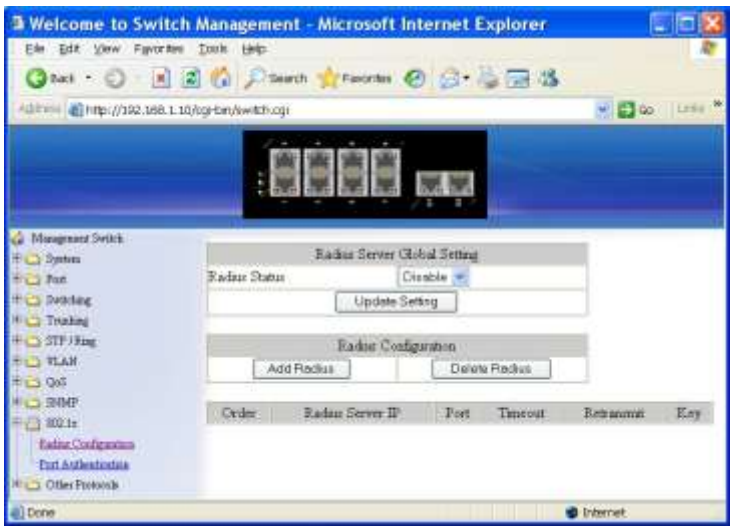
1. Add User: Click "Add User" button. The "SNMP V3 Setting" window appears.
2. SNMP Version: Click "SNMP Version" drop-down menu from "SNMP Version" drop-down list to choose "SNMPv3 No-Auth", "SNMPv3 Auth-MD5", "SNMPv3 Auth-SHA", "SNMPv3 Priv Auth-MD5", or "SNMPv3 Priv Auth-SHA".
   - SNMPv3 No-Auth: 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:

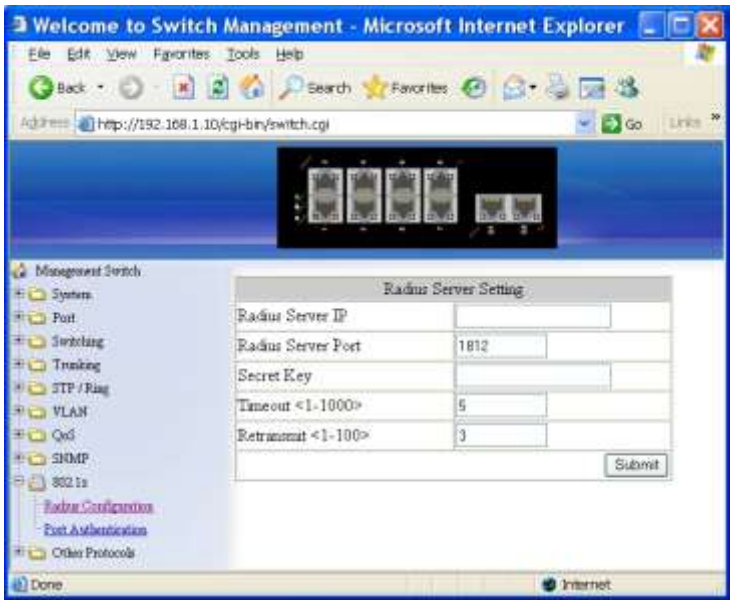
1. Delete User: Click "Delete User" button. The "Select User Name" window appears.
2. Select User Name: Click "Select User Name" drop-down menu from "Select User Name" drop-down list to choose the user to be deleted from using SNMP v3.
3. Submit: Click "Submit" button when you finished user deletion.

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:

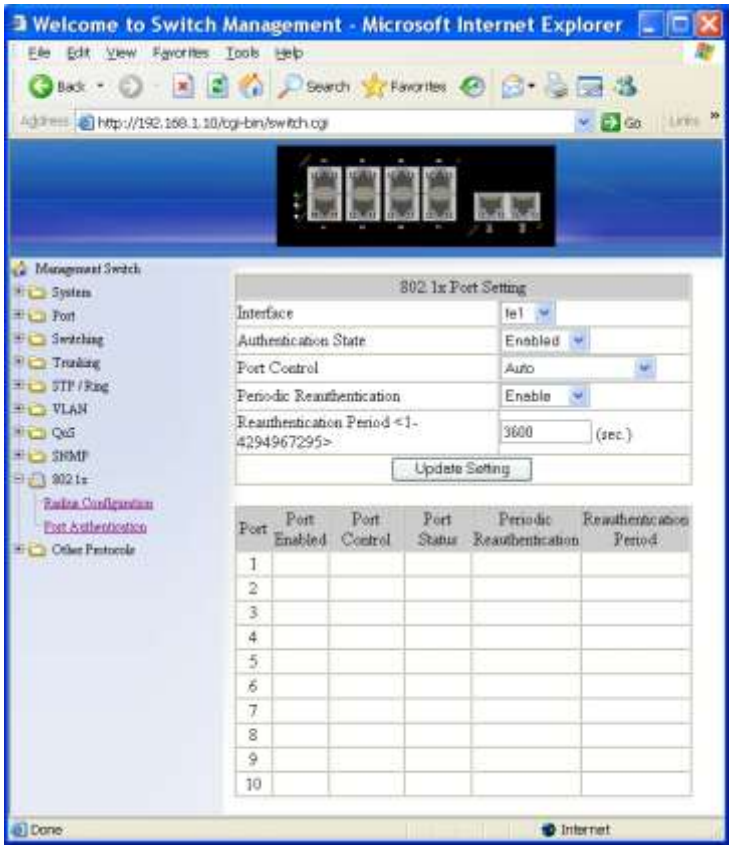
1. Add Radius: Click "Add Radius" button. The "Radius Server Setting" window appears.
2. Radius Server IP: Click in the "Radius Server IP" textbox and specify the IP address of the remote radius server host.
3. Radius Server Port: Click in the "Radius Server Port" textbox and specify the UDP destination 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 quotation 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:

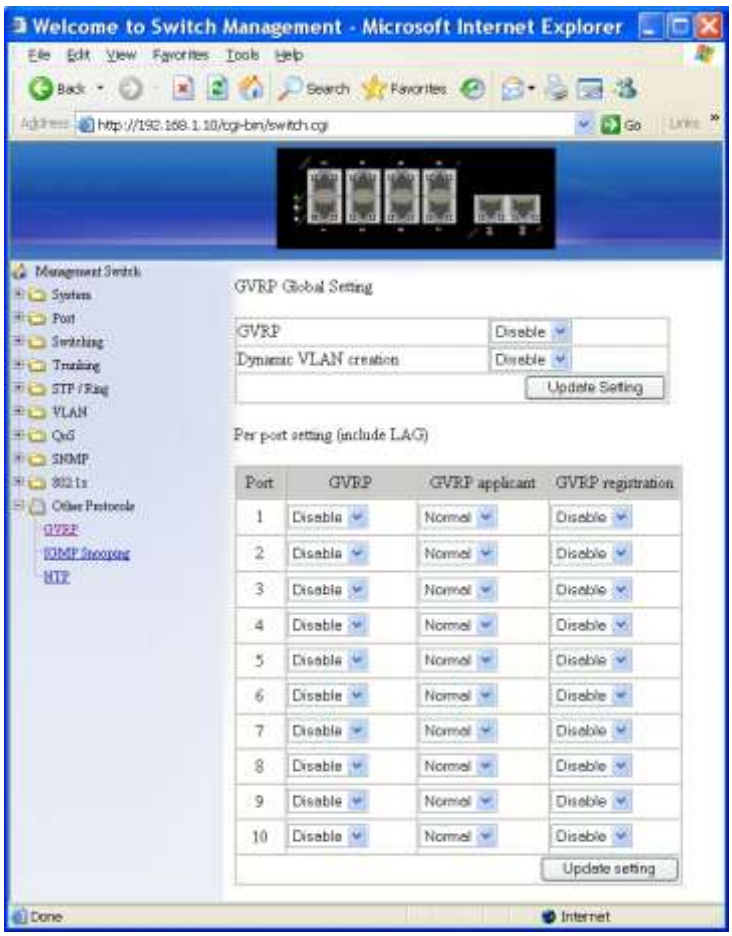
1. Delete Radius: Click "Delete Radius" button. The "Select Radius Server IP" window appears.
2. Select Radius Server IP: Click "Select Radius Server IP" drop-down menu from "Select Radius Server IP" drop-down list to choose the IP address of the remote radius server host to be deleted.
3. Submit: Click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



Port 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.

Other Protocols



GVRP

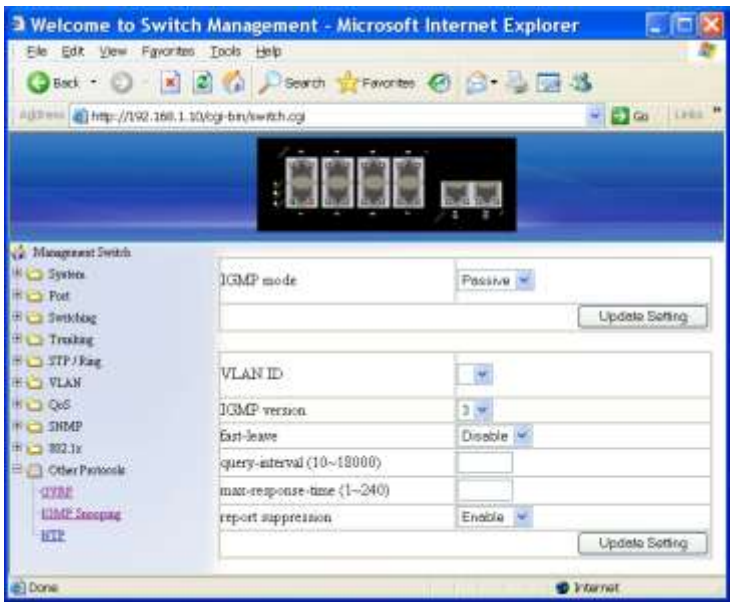
GVRP Global Setting:

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.



IGMP Snooping

1. 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.
2. Update Setting: Click "Update Setting" button when you finished IGMP mode settings.
3. VLAN ID: Click "VLAN ID" drop-down menu from "VLAN ID" drop-down list to choose the VLAN under configuration for the switch.
4. IGMP version: Click "IGMP version" drop-down menu from "IGMP version" drop-down list to choose "1", "2", or "3" for the switch.
5. 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.

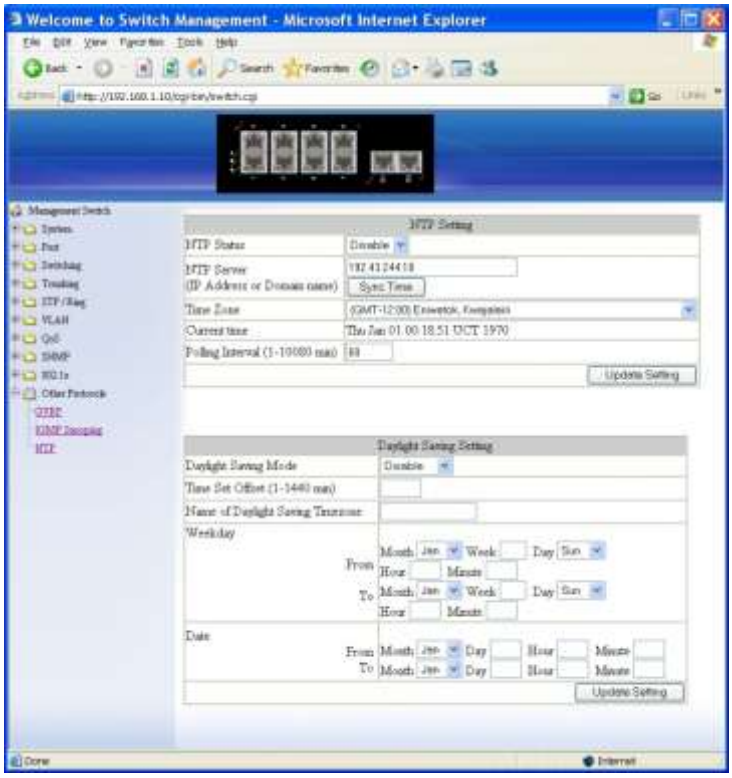
IGMP querier:

1. Query-interval: 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: Click in the "max-response-time" textbox and specify a new number from 1 ~ 124. 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 124 (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.



NTP

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. Daylight Saving Timezone: Click in the "Daylight Saving Timezone" textbox and specify the daylight saving timezone. This can be any given name in 14-character alpha-numerical. Enter the 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 weekdays from Monday to Friday.
   - 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 through 9).

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 Commend Line.

Administration Console

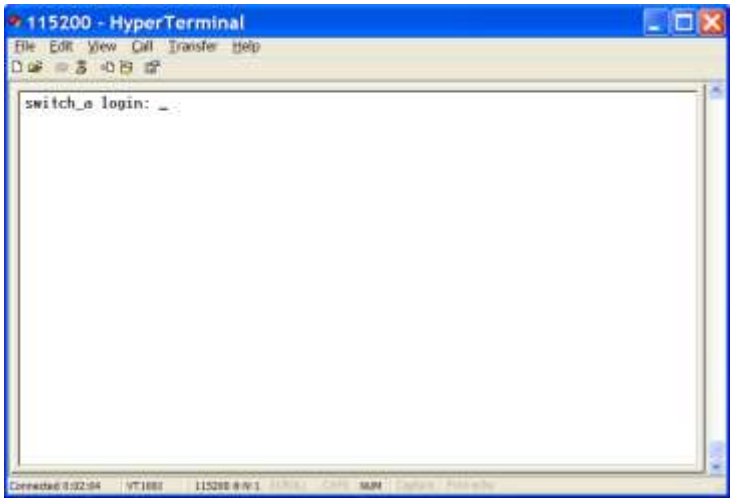
Connect the DB9 straight cable to the RS-232 serial port of the device to the RS-232 serial port of the terminal or computer running the terminal emulation application.

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

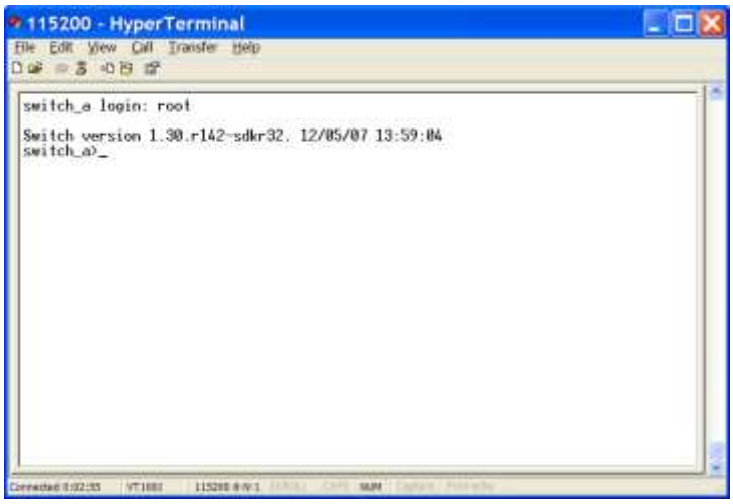
Exec Mode (View Mode)



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

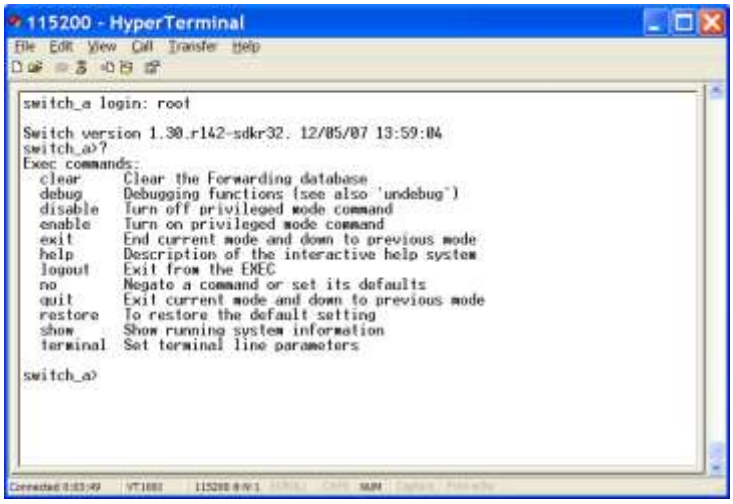
Exec Mode (or View Mode) is the base mode from where users can perform basic commands like:

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.

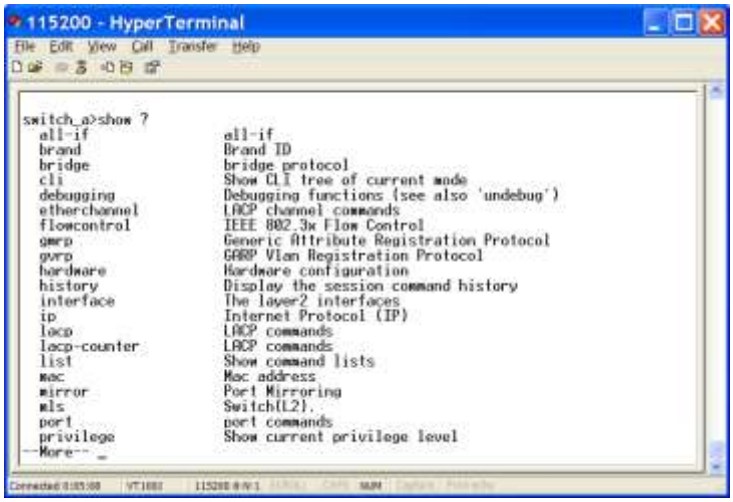
At the **switch_a>** prompt just press <?> to list the above basic commands.

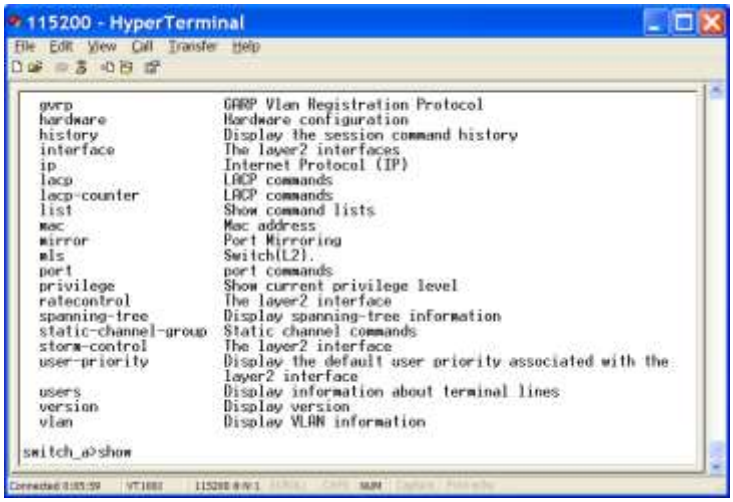
```
switch_a>?
```



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 ?
```





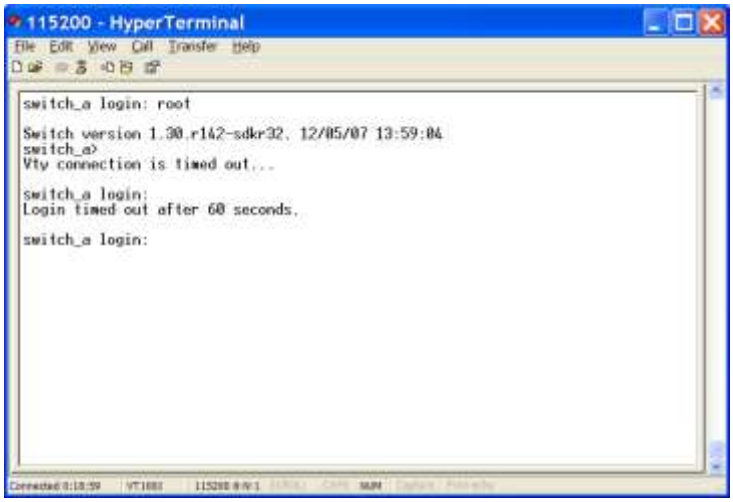
Login timed out

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).

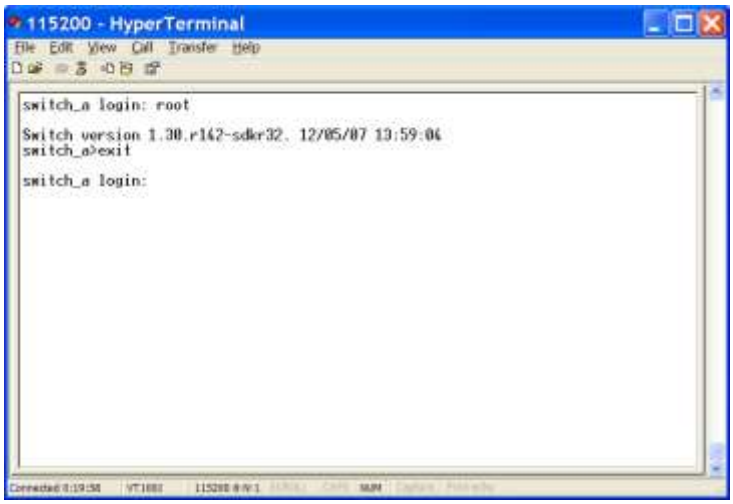
```
switch_a login: root
```



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
```

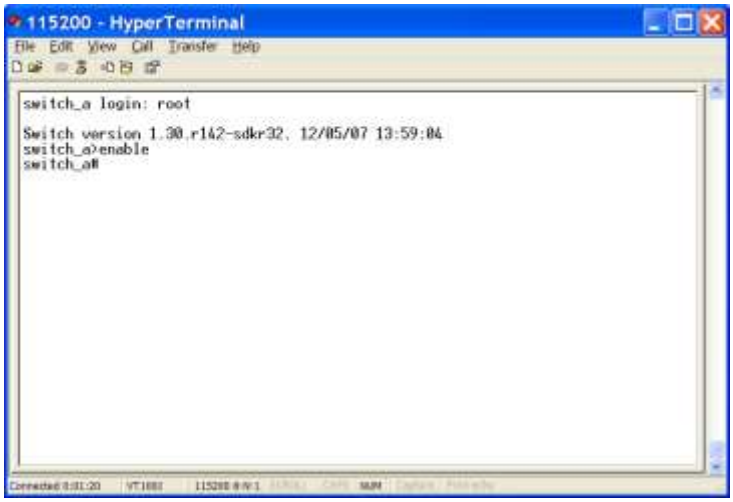


Privileged Exec Mode (Enable Mode)

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
```

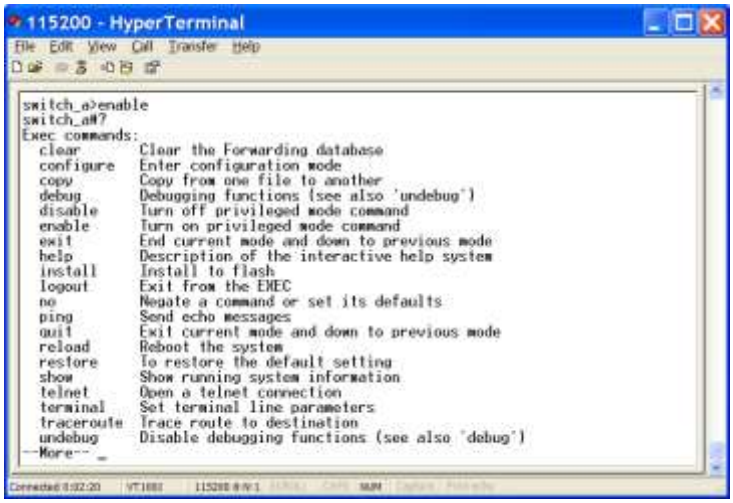


Commands

Privileged Exec Mode (or Enable Mode) allows users to run commands as following.

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

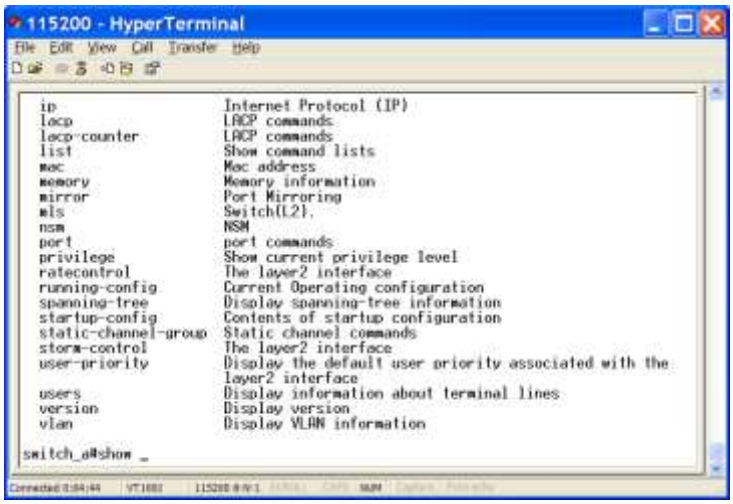
```
switch_a#?
```



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 ?
```



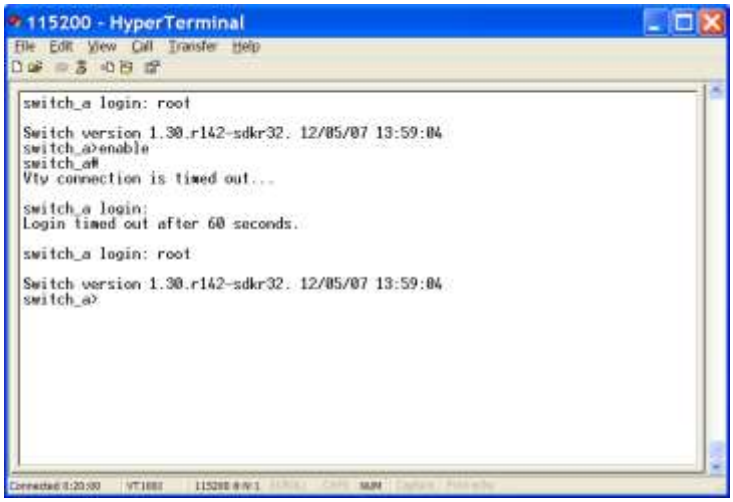
Login timed out

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).

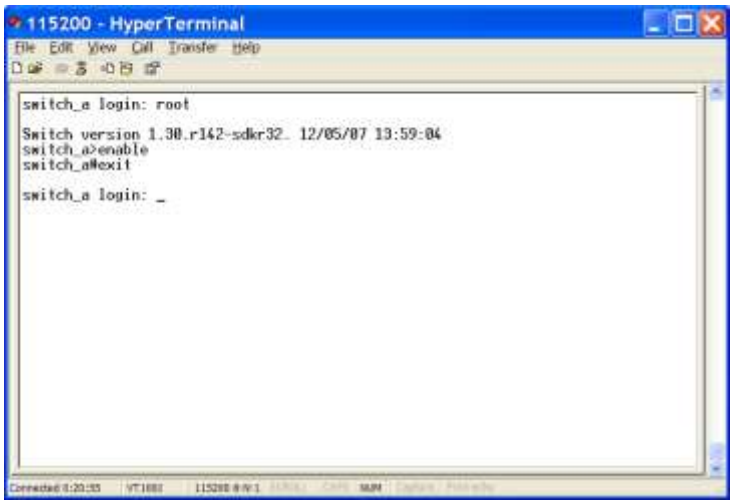
```
switch_a login: root
```



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
```

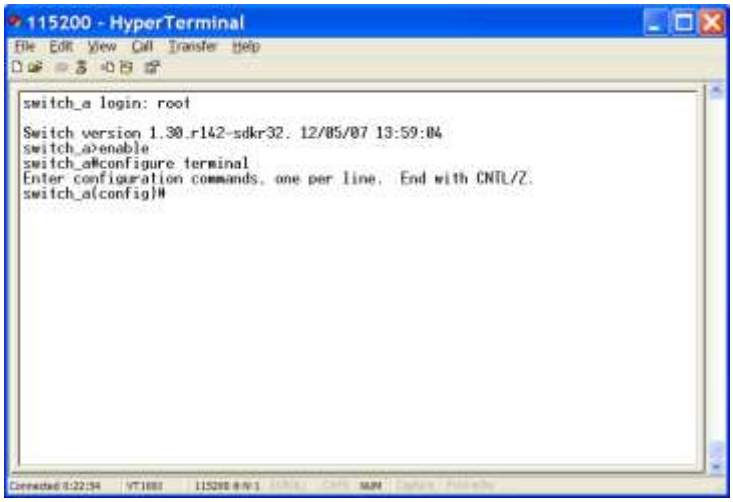


Configure Mode (Configure Terminal Mode)

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
```

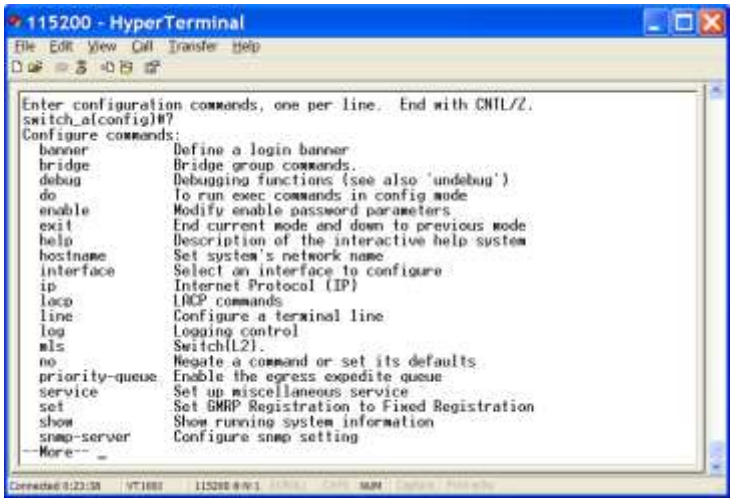


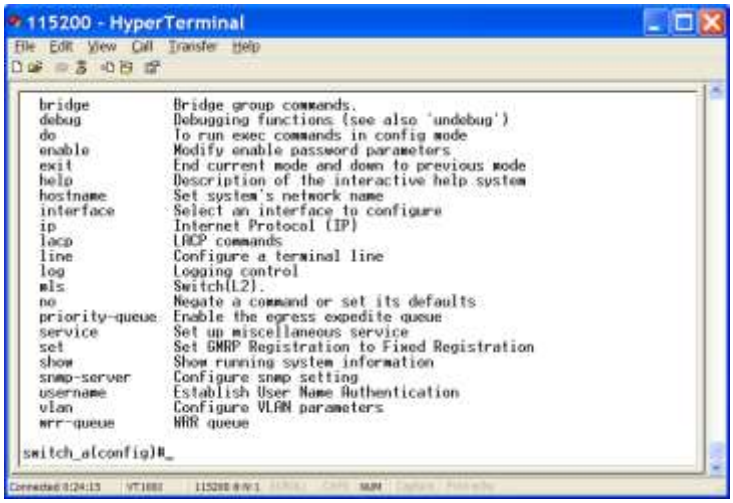
Commands

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.

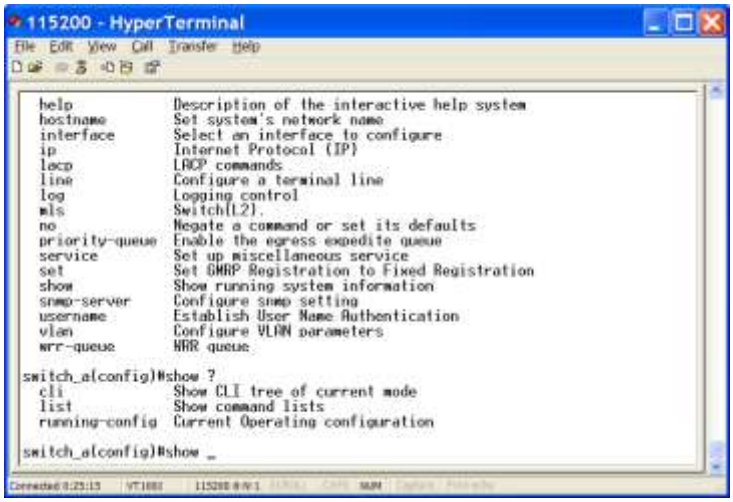
```
switch_a(config)#?
```





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 ?
```



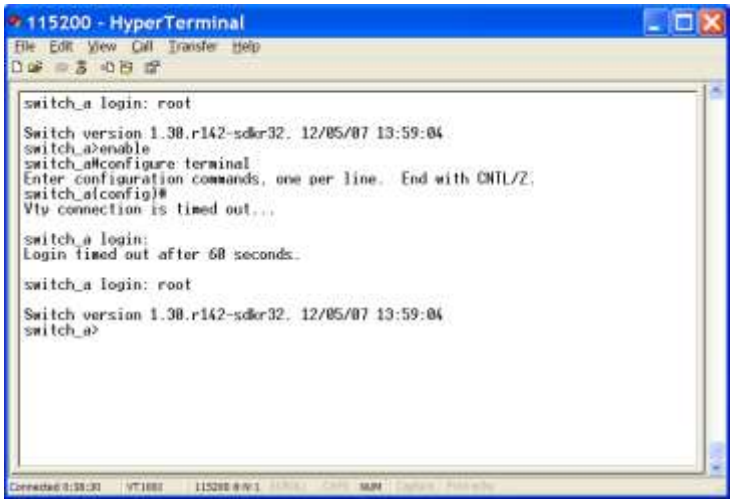
Login timed out

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).

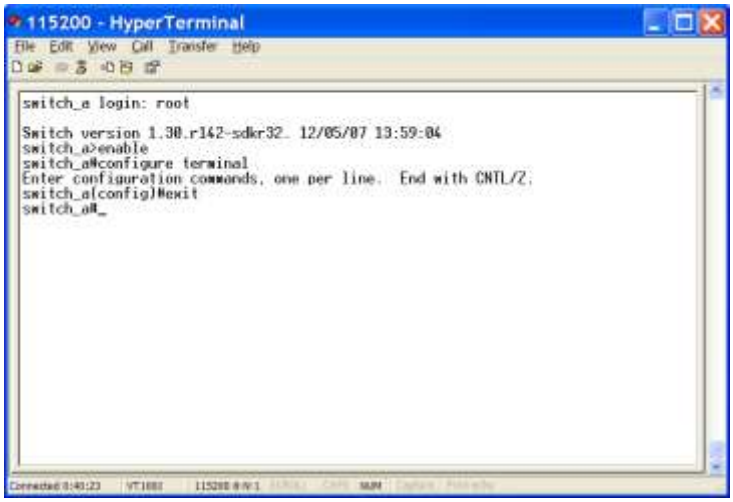
```
switch_a login: root
```



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
```



System

System Information, System Name/Password, IP Address, Save Configuration, Firmware Upgrade, Alarm Setting, Reboot, Logout

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)#
```

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: **192.168.1.100)**:

```
switch_a#write config-file 192.168.1.100
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#
```

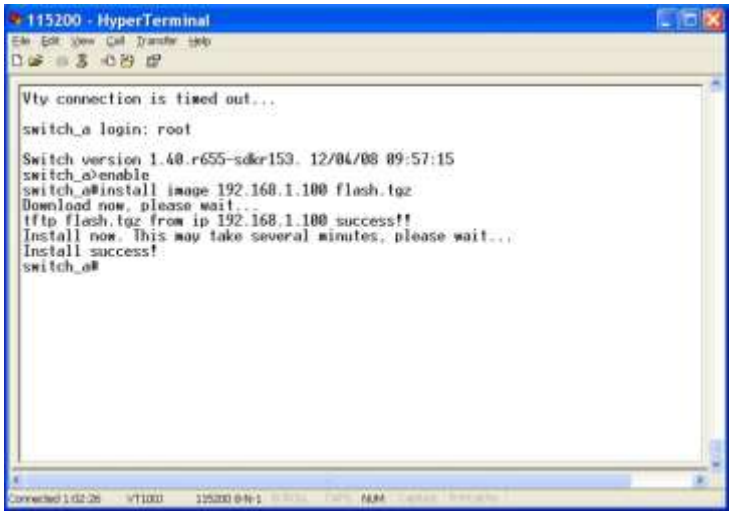
2. Usage:
Use **install image** command to upgrade firmware from tftp server to switch.

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.

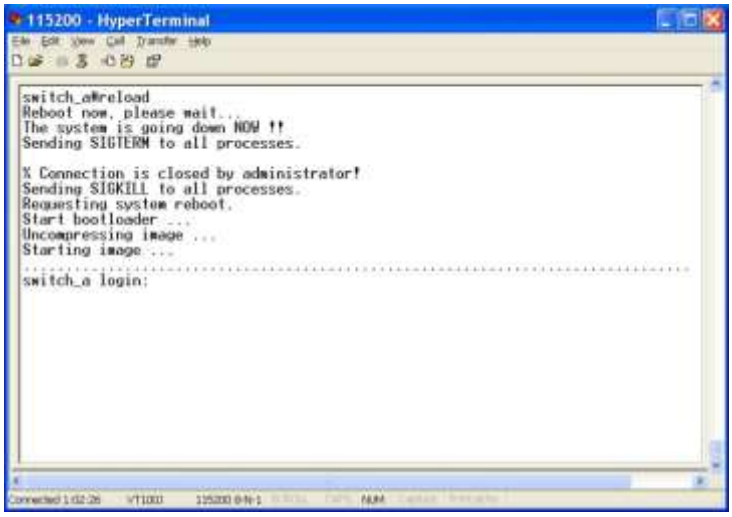
4. Example:
The following example specifies upgrading firmware (file name: **flash.tgz**) from tftp server (IP address: **192.168.1.100)** to switch:

```
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.



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)#
```

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:
```

Port

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

Configuration

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

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
```

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>k|m 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
```

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)#
```

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)#
```

Trunking

Port 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 <1-3>
no static-channel-group
<1-3> Channel group number.
Maximum 4 ports in static-channel-group 1 and static-channel-group 2.
Maximum 2 ports in static-channel-group 3

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)#
```

STP / Ring

Global Configuration, RSTP Port Setting, MSTP Properties, MSTP Instance Setting, MSTP Port Setting, Ring 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:
5. Command Mode: Configure mode
Logon to Configure Mode (Configure Terminal Mode).
The **switch_a(config)#** prompt will show on the screen.

```
switch_a(config)#
```

6. 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.

7. 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.

8. 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)#
```

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)#
```

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)#
```

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)#
```

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)#
```

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)#
```

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)#
```

Other Protocols

GVRP, IGMP Snooping, NTP

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)#
```

NTP

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 weekdays from Monday to Friday.
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)#
```

Specifications

Applicable Standards	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX, 100Base-FX IEEE 802.3ab 1000Base-T IEEE 802.3z 1000Base-SX/LX
Switching Method	Store-and-Forward
Forwarding Rate	
10Base-T	10 / 20Mbps half / full-duplex
100Base-TX	100 / 200Mbps half / full-duplex
100Base-FX	200Mbps full-duplex
1000Base-T/SX/LX	2000Mbps full-duplex
Performance	14,880pps for 10Mbps 148,810pps for 100Mbps 1,488,100pps for 1000Mbps
Cable	
10Base-T	2-pair UTP/STP Cat. 3, 4, 5 Up to 100m (328ft)
100Base-TX	2-pair UTP/STP Cat. 5 Up to 100m (328ft)
1000Base-T	4-pair UTP/STP Cat. 5 Up to 100m (328ft)
100Base-FX	MMF (50 or 62.5µm), SMF (9 or 10µm)
1000Base-SX/LX	MMF (50 or 62.5µm), SMF (9 or 10µm)
LED Indicators	Per unit – Power status (Power 1, Power 2, Power 3) Per port – 10/100TX, 100FX: LINK/ACT 10/100/1000TX, 1000SX/LX: LINK/ACT
Dimensions	65mm (W) x 125mm (D) x 145mm (H) (2.56″ (W) x 4.92″ (D) x 5.71″ (H))
Net Weight	1Kg (2.2lbs.)
Power Input	DC Jack: 12VDC, External AC/DC required Terminal Block: 12-48VDC
Operating Voltage & Max. Current Consumption	0.92A @ 12VDC, 0.46A @ 24VDC, 0.23A @ 48VDC
Power Consumption	11W Max.
Operating Temperature	-40°C to 75°C (-40°F to 167°F) Tested for functional operation @ -40°C to 85°C (-40°F to 185°F)
Storage Temperature	-40°C to 85°C (-40°F to 185°F)
Humidity	5%-95% non-condensing
Safety	UL508
EMI	FCC Part 15, Class A EN61000-6-4: EN55022, EN61000-3-2, EN61000-3-3
EMS	EN61000-6-2: EN61000-4-2 (ESD Standard) EN61000-4-3 (Radiated RFI Standards) EN61000-4-4 (Burst Standards) EN61000-4-5 (Surge Standards) EN61000-4-6 (Induced RFI Standards) EN61000-4-8 (Magnetic Field Standards)
Environmental Test Compliance	IEC60068-2-6 Fc (Vibration Resistance) IEC60068-2-27 Ea (Shock) IEC60068-2-32 Ed (Free Fall)
EN50121-4 environmental requirements for railway applications	
NEMA TS1/2 Environmental requirements for traffic control equipment	

Appendix A

DB9 DCE pin assignment

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

Appendix B

Time Zone	Country and City Lists
Europe	
MEZ-1MESZ	Europe/Vienna, Europe/Berlin, Europe/Zurich
MET-1METDST	Africa/Tunis, CET, MET, Europe/Tirane, Europe/Andorra, Europe/Brussels, Europe/Prague, Europe/Copenhagen, Europe/Paris, Europe/Gibraltar, Europe/Budapest, Europe/Rome, Europe/Vaduz, Europe/Luxembourg, Europe/Malta, Europe/Monaco, Europe/Amsterdam, Europe/Oslo, Europe/Warsaw, Europe/Belgrade, Europe/Madrid, Africa/Ceuta, Europe/Stockholm, Europe/Vatican, Europe/San_Marino, Arctic/Longyearbyen, Atlantic/Jan_Mayen, Europe/Ljubljana, Europe/Sarajevo, Europe/Skopje, Europe/Zagreb, Europe/Bratislava, Poland
EET-2EETDST	Asia/Nicosia, EET, Europe/Minsk, Europe/Sofia, Europe/Athens, Europe/Vilnius, Europe/Chisinau, Europe/Istanbul, Europe/Kiev, Europe/Uzhgorod, Europe/Zaporozhye, Europe/Nicosia, Asia/Istanbul, Europe/Tiraspol, Turkey
GMT0BST	Europe/London, Europe/Dublin, Eire, Europe/Belfast, GB, GB-Eire
WET0WETDST	WET, Atlantic/Faeroe, Atlantic/Madeira, Atlantic/Canary
PWT0PST	Europe/Lisbon, Portugal
MST-3MDT	Europe/Moscow, W-SU
EUT-1EUTDST	America/Scoresbysund, Atlantic/Azores
EUT-2EUTDST	Asia/Beirut, Europe/Simferopol
EUT-3EUTDST	Asia/Tbilisi
EUT-4EUTDST	Europe/Samara
EUT-6EUTDST	Asia/Almaty, Asia/Qyzylorda
EUT-8EUTDST	Asia/Ulaanbaatar
Russian Federation	
RFT-2RFTDST	Europe/Kaliningrad
RFT-3RFTDST	Europe/Moscow
RFT-4RFTDST	Asia/Yerevan, Asia/Baku, Asia/Oral, Asia/Ashkhabad
RFT-5RFTDST	Asia/Aqtobe, Asia/Aqtau, Asia/Bishkek, Asia/Yekaterinburg
RFT-6RFTDST	Asia/Omsk, Asia/Novosibirsk
RFT-7RFTDST	Asia/Hovd, Asia/Krasnoyarsk
RFT-8RFTDST	Asia/Irkutsk, Asia/Chungking, Asia/Ulan_Bator
RFT-9RFTDST	Asia/Choibalsan, Asia/Yakutsk
RFT-10RFTDST	Asia/Vladivostok

RFT-11RFTDST	Asia/Sakhalin, Asia/Magadan
RFT-12RFTDST	Asia/Kamchatka, Asia/Anadyr
North America	
PST8PDT	America/Los_Angeles, US/Pacific-New, PST8PDT, US/Pacific, SystemV/PST8PDT
MST7MDT	America/Denver, America/Boise, America/Cambridge_Bay, America/Shiprock, MST7MDT, Navajo, US/Mountain, SystemV/MST7MDT
MST7	America/Phoenix, MST, US/Arizona, SystemV/MST7
CST6CDT	America/Chicago, America/North_Dakota/Center, America/Menominee, America/Costa_Rica, America/Managua, CST6CDT, US/Central, SystemV/CST6CDT
EST5EDT	America/New_York, America/Kentucky/Louisville, America/Kentucky/Monticello, America/Detroit, America/Pangnirtung, America/Louisville, EST5EDT, US/Eastern, US/Michigan, SystemV/EST5EDT
AST4ADT	America/Thule, Atlantic/Bermuda, SystemV/AST4ADT
EST5	America/Coral_Harbour, America/Cayman, America/Jamaica, America/Panama, EST, Jamaica, SystemV/EST5
AST10ADT	America/Adak, America/Atka, US/Aleutian
YST9YDT	Canada/Yukon
NST3:30NDT	America/St_Johns, Canada/Newfoundland
NAST3NADT	America/Godthab, America/Miquelon
NAST9NADT	Pacific/Pitcairn, America/Juneau, America/Yakutat, America/Anchorage, America/Nome, US/Alaska, SystemV/YST9YDT, SystemV/PST8
South America & Central America	
TTST4	America/Port_of_Spain
SAT3	America/Argentina/Buenos_Aires, America/Argentina/Cordoba, America/Argentina/Tucuman, America/Argentina/La_Rioja, America/Argentina/San_Juan, America/Argentina/Jujuy, America/Argentina/Catamarca, America/Argentina/Mendoza, America/Argentina/Rio_Gallegos, America/Argentina/Ushuaia, America/Argentina/ComodRivadavia, America/Buenos_Aires, America/Cordoba, America/Jujuy, America/Mendoza
EBST3EBDT	America/Fortaleza, America/Recife, America/Araguaina, America/Maceio,

	America/Bahia, America/Sao_Paulo, America/Cuiaba, America/Montevideo, America/Catamarca, America/Rosario, Brazil/East
WBST4WBDT	America/Campo_Grande, America/Boa_Vista, America/Manaus, Atlantic/Stanley, America/Asuncion, Brazil/West
ACRE5	America/Rio_Branco, America/Porto_Acre, Brazil/Acre
NORO2	America/Noronha, Brazil/DeNoronha
CST4CDT	Antarctica/Palmer, America/Santiago, Chile/Continental
EIST6EIDT	Pacific/Easter, Chile/EasterIsland
Asia	
MST-8	Asia/Kuala_Lumpur, Asia/Kuching
CST-8	Asia/Harbin, Asia/Shanghai, Asia/Chongqing, Asia/Urumqi, Asia/Kashgar, Asia/Hong_Kong, Asia/Macau, Asia/Macao, Hongkong, PRC, ROC
Oceania	
CST-9:30CDT	Australia/Adelaide, Australia/Broken_Hill, Australia/South, Australia/Yancowinna
EST-10EDT	Australia/Brisbane, Australia/Lindeman, Australia/Currie, Australia/Melbourne, Australia/Sydney, Australia/ACT, Australia/Canberra, Australia/NSW, Australia/Queensland, Australia/Tasmania, Australia/Victoria
LHT-10:30LHDT	Australia/Lord_Howe, Australia/LHI
TST-10TDT	Australia/Hobart
NZST-12NZDT	Antarctica/McMurdo, Pacific/Auckland, Antarctica/South_Pole, NZ
CIST-12:45CIDT	Pacific/Chatham, NZ-CHAT
Africa	
SAST-2	Africa/Maseru, Africa/Johannesburg, Africa/Mbabane
EST-2EDT	Africa/Cairo, Egypt
UAEST-4	Asia/Dubai
IST-3IDT	Asia/Baghdad
JST-2JDT	Asia/Amman
SST-2SDT	Asia/Damascus
Universal	
UCT	Africa/Ouagadougou, Africa/Abidjan, Africa/Banjul, Africa/Accra, Africa/Conakry, Africa/Bissau, Africa/Monrovia, Africa/Bamako, Africa/Nouakchott, Africa/Casablanca, Africa/El_Aaiun, Atlantic/St_Helena, Africa/Sao_Tome, Africa/Dakar, Africa/Freetown, Africa/Lome, America/Danmarkshavn, Atlantic/Reykjavik, Etc/GMT, Etc/UTC, Etc/UCT, GMT, Etc/Universal,

	Etc/Zulu, Etc/Greenwich, Etc/GMT-0, Etc/GMT+0, Etc/GMT0, Africa/Timbuktu, GMT+0, GMT-0, GMT0, Greenwich, Iceland, UCT, UTC, Universal, Zulu
UCT1	Atlantic/Cape_Verde, Etc/GMT+1
UCT2	Atlantic/South_Georgia, Etc/GMT+2
UCT3	Antarctica/Rothera, America/Belem, America/Cayenne, America/Paramaribo, Etc/GMT+3
UCT4	America/Anguilla, America/Antigua, America/Barbados, America/Dominica, America/Grenada, America/Guadeloupe, America/Martinique, America/Montserrat, America/Puerto_Rico, America/St_Kitts, America/St_Lucia, America/St_Vincent, America/Tortola, America/St_Thomas, America/Aruba, America/La_Paz, America/Porto_Velho, America/Curacao, America/Caracas, America/Guyana, Etc/GMT+4, America/Virgin, SystemV/AST4
UCT5	America/Guayaquil, America/Eirunepe, America/Lima, Etc/GMT+5
UCT6	America/Belize, America/El_Salvador, America/Tegucigalpa, Pacific/Galapagos, Etc/GMT+6
UCT7	Etc/GMT+7
UCT8	Etc/GMT+8
UCT9	Pacific/Gambier, Etc/GMT+9, SystemV/YST9
UCT10	Pacific/Rarotonga, Pacific/Tahiti, Pacific/Fakaofo, Pacific/Johnston, Pacific/Honolulu, Etc/GMT+10, HST, US/Hawaii, SystemV/HST10
UCT11	Pacific/Niue, Pacific/Pago_Pago, Pacific/Apia, Pacific/Midway, Etc/GMT+11, Pacific/Samoa, US/Samoa
UCT-1	Africa/Algiers, Africa/Luanda, Africa/Porto-Novo, Africa/Douala, Africa/Bangui, Africa/Ndjamena, Africa/Kinshasa, Africa/Brazzaville, Africa/Malabo, Africa/Libreville, Africa/Windhoek, Africa/Niamey, Africa/Lagos, Etc/GMT-1
UCT-2	Africa/Gaborone, Africa/Bujumbura, Africa/Lubumbashi, Africa/Tripoli, Africa/Blantyre, Africa/Maputo, Africa/Kigali, Africa/Lusaka, Africa/Harare, Etc/GMT-2, Libya
UCT-3	Indian/Comoro, Africa/Djibouti, Africa/Asmera, Africa/Addis_Ababa, Africa/Nairobi, Indian/Antananarivo, Indian/Mayotte, Africa/Mogadishu, Africa/Khartoum, Africa/Dar_es_Salaam, Africa/Kampala, Antarctica/Syowa, Asia/Bahrain, Asia/Kuwait,

	Asia/Qatar, Asia/Riyadh, Asia/Aden, Etc/GMT-3
UCT-4	Indian/Mauritius, Indian/Reunion, Indian/Mahe, Asia/Muscat, Etc/GMT-4
UCT-5	Indian/Kerguelen, Indian/Maldives, Asia/Karachi, Asia/Dushanbe, Asia/Ashgabat, Asia/Samarkand, Asia/Tashkent, Etc/GMT-5
UCT-5:45	Asia/Katmandu
UCT-6	Antarctica/Mawson, Antarctica/Vostok, Asia/Dhaka, Asia/Thimphu, Indian/Chagos, Asia/Colombo, Etc/GMT-6, Asia/Dacca, Asia/Thimbu
UCT-6:30	Asia/Rangoon, Indian/Cocos
UCT-7	Antarctica/Davis, Asia/Phnom_Penh, Asia/Jakarta, Asia/Pontianak, Asia/Vientiane, Asia/Bangkok, Asia/Saigon, Indian/Christmas, Etc/GMT-7
UCT-8	Antarctica/Casey, Asia/Brunei, Asia/Taipei, Asia/Makassar, Asia/Manila, Asia/Singapore, Etc/GMT-8, Asia/Ujung_Pandang, Singapore
UCT-9	Asia/Dili, Asia/Jayapura, Pacific/Palau, Etc/GMT-9
UCT-9:30	Australia/Darwin, Australia/North
UCT-10	Antarctica/DumontDUrville, Pacific/Guam, Pacific/Saipan, Pacific/Truk, Pacific/Noumea, Pacific/Port_Moresby, Etc/GMT-10, Pacific/Yap
UCT-11	Pacific/Ponape, Pacific/Kosrae, Pacific/Guadalcanal, Etc/GMT-11
UCT-11:30	Pacific/Norfolk
UCT-12	Pacific/Fiji, Pacific/Tarawa, Pacific/Enderbury, Pacific/Majuro, Pacific/Kwajalein, Pacific/Nauru, Pacific/Tongatapu, Pacific/Funafuti, Pacific/Wake, Pacific/Efate, Pacific/Wallis, Etc/GMT-12, Kwajalein
UCT-13	Etc/GMT-13
JST	Asia/Tokyo, Japan
KST	Asia/Seoul, Asia/Pyongyang, ROK
UCT-3:30	Asia/Tehran, Iran
UCT-4:30	Asia/Kabul
IST-2IDT	Asia/Jerusalem, Asia/Gaza, Asia/Tel_Aviv, Israel
CST6MEX	America/Cancun, America/Merida, America/Monterrey, America/Mexico_City, America/Lima, Mexico/General
CST6	America/Regina, America/Swift_Current, Canada/East-Saskatchewan, Canada/Saskatchewan, SystemV/CST6
EET-2EETDST2	Europe/Bucharest
EET-2EETDST3	Europe/Tallinn, Europe/Helsinki, Europe/Riga, Europe/Mariehamn
EET-2EETDST2W2K	Europe/Istanbul
UCT-14	Pacific/Kiritimati, Etc/GMT-14
UCT9:30	Pacific/Marquesas

UCT12	Etc/GMT+12
North America (Canada)	
PST8PDT_CA	America/Vancouver, America/Dawson_Creek, America/Whitehorse, America/Dawson, Canada/Pacific
MST7MDT_CA	America/Edmonton, America/Yellowknife, America/Inuvik, Canada/Mountain
CST6CDT_CA	America/Rainy_River, America/Winnipeg, America/Rankin_Inlet, Canada/Central
EST5EDT_CA	America/Montreal, America/Toronto, America/Thunder_Bay, America/Nipigon, America/Iqaluit, Canada/Eastern
AST4ADT_CA	America/Goose_Bay, America/Halifax, America/Glace_Bay, Canada/Atlantic
North America (Cuba)	
EST5EDT_CU	America/Havana, Cuba
North America (Haiti)	
EST5EDT_HT	America/Nassau, America/Santo_Domingo, America/Port-au-Prince, America/Bogota
North America (Mexico)	
PST8PDT_MX	America/Tijuana, America/Ensenada, Mexico/BajaNorte
MST7MDT_MX	America/Chihuahua, America/Hermosillo, America/Mazatlan, Mexico/BajaSur
CST6CDT_MX	America/Guatemala
North America (Turks and Caicos)	
EST5EDT_TC	America/Grand_Turk
Additions Since 10g RTM	
EST5EDT_INDIANA	America/Indiana/Indianapolis, America/Indiana/Marengo, America/Indiana/Vevay, America/Fort_Wayne, America/Indianapolis, America/Indiana/Knox, America/Knox_IN, US/Indiana-Starke, US/East-Indiana
UCT-8_WA	Australia/Perth, Australia/West