COBRA

CME-822(E)

Industrial 8 10/100Base-T(X) + 2 Copper/SFP Gigabit Managed PoE Ethernet Switch (Embedded 8 PoE Injectors) User's Manual

V2.0
10-21-2009

COMPATIBLE IntraVUE

RoHS

WEEE

POWER OVER ETHERNET

EXTENDED TEMP 80℃+ 40℃−

GLOBAL WARRANTY

Cobra Series Industrial Power over Ethernet Switch Solutions
CME-822(E) Industrial Gigabit Managed PoE Ethernet Switch
User's Manual

Copyright Notice

Table of Contents

Chapter 1

Introduction

Welcome to Cobra Series CME-822(E) Industrial Gigabit Managed PoE Ethernet Switch. This chapter includes the following topics:

- Overview
- Product Features
- Package Checklist

1-1 Overview

The Cobra CME-822(E) is a highly reliable and fault-tolerant Industrial 10-port Managed Power over Ethernet Switch. It supports eight PoE injector ports classified as power source equipment (PSE). CME-822(E) offers state of the art design with eight 10/100 Mbps Ethernet ports and two small form pluggable (SFP) ports that supports Gigabit SX or LC depending on your existing network structure. The innovative SFP fiber slot design provides user the flexibility to insert different fiber modules, either multi-mode or single-mode at various distances, whether you require typical 10km or overhaul 40 km, 80 km and 120 km distances. With its high performance switching device, CME-822(E) provides redundant self-recovery mechanism in less than 10ms on full load which allows you to establish a redundant Ethernet network to build a back-up ring topology. Dual Homing and Ring Coupling are supported to add reliability by allowing a device to be connected to be network by way of two independent connection points. CME-822(E) offers powerful network management functions including SNMP, SMTP, SNTP, QoS, Class of Service, IGMP, Snooping, LACP, DHCP, VLAN, RMON, Port Trunk, Port Mirror, User Authentication (Radius) and IP Security. The CME-822(E) is equipped with a terminal block to provide dual power inputs with reverse polarity protection. Its IP-30 housing protection, wide operating temperature of -10 to 70℃, the E version has wider temperature range of -40 to 80℃ and DIN-Rail mounting is suitable for an industrial environment. The CME-822(E) is a plug-and-play solution for your Power over Ethernet applications.

1-2 Product Features

CME-822(E) has the following features:

High Performance Network Switching Technology

- Complies with IEEE 802.3af, IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3x, IEEE 802.3ad, IEEE 802.1D, IEEE 802.1w, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1X, IEEE 802.1AB,
- Provides 8 x 10/100Base-T(X) Ethernet ports with RJ-45 connector
- Provides 2 combo ports
- Embedded 8 ports PoE injector function classified as PSE
- Supplies 15.4 watts of power per port full load with PoE
- RJ-45 ports support auto MDI/MDI-X crossover
- Provides broadcast storm protection
- Redundant X-Ring recovery time < 10ms on full load
- Supports Dual Homing - RSTP over X-Ring
- Supports Ring Coupling
- SNMP for network management
- IGMP Snooping for multicast traffic
- QoS/ToS to increase network packet determinism
- VLAN for easy network planning
- Event notification by email, SNMP trap, syslog & relay output
- Online Port Mirroring for online debugging
- Supports IP security
- Configurable by web browser
- IntraVUE™ network management software compatible

Robust Industrial Design

- Robust aluminum case complying to IP-30 housing standard

- Supports operating temperature -10 to 70℃ & extended temperature -40 to 80℃
- DIN-Rail, panel mount or desktop installation
- High level of immunity to electromagnetic interference & power supply surges typically found in industrial plant environments or external curb side enclosures

Reliable Power Design

- Supports 6000VDC Ethernet ESD protection
- Provides surge (EFT) protection 3000VDC for power line
- Equipped with redundant power inputs
- Supports 48VDC redundant power with polarity reverse protection
- Removable terminal block

1-3 Package Checklist

CME-822(E) is shipped with the following items:

- 1 x Cobra Series CME-822(E) Industrial Gigabit Managed PoE Ethernet Switch
- 1 x User's manual
- 1 x RS-232/RJ-45 cable
- 2 x wall-mounting plates and 6 x screws
- 1 x DIN-Rail mounting kit (attached to the CME-822(E)'s back panel by default)

1-4 Software Version

This manual content is based on the software version listed in the table below. If your CME-822(E) functions differently from the descriptions in this manual, please contact Ethernet Direct local partner for more information.

Firmware Version	V1.11
Kernel Version	V1.58
MAC Address	----------

Chapter 2

Hardware Installation

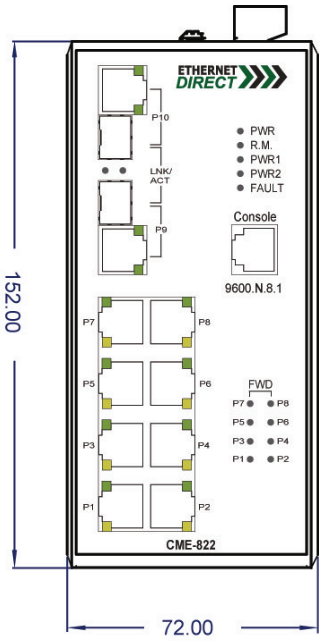
This chapter contains information on CME-822(E)'s dimensions and hardware installation. Topics include:

- Dimensions and Panel Layout
- LED Indicators
- RJ-45 Ports
- SFP Ports
- Installing Your Ethernet Direct Switch

2-1 Dimensions and Panel Layout

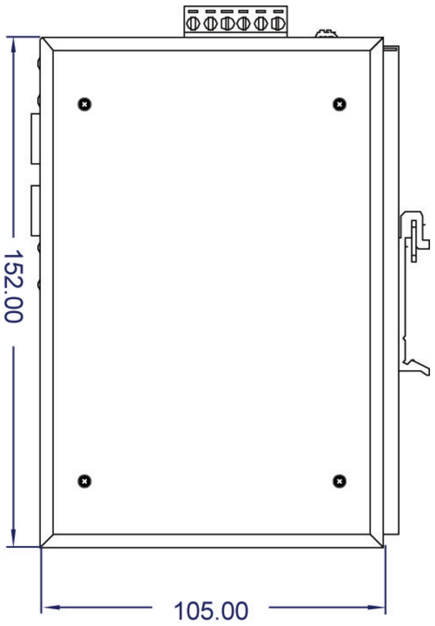
Dimensions of CME-822(E) Industrial Gigabit Managed Switch are 72mm (W) x 102mm (D) x 152mm (H).

Front Panel

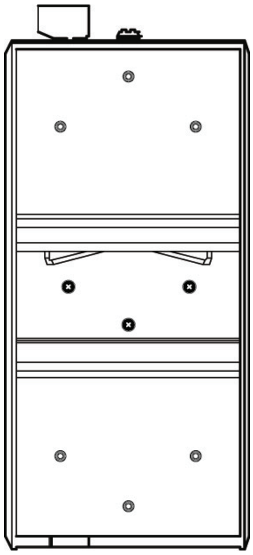


Side Panel

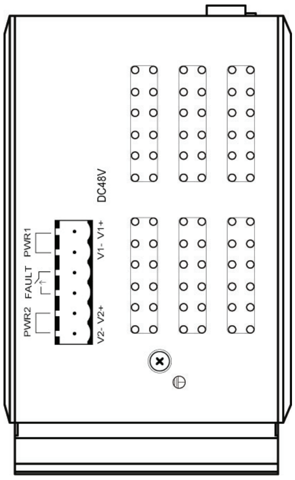
Unit: mm



Back Panel



Top Panel



2-2 LED Indicators

There are 7 diagnostic LEDs located on the front panel of CME-822(E). They provide primary information on switch status as described in the table below.

LED Name	LED Color	LED Function
PWR	Green	Power is on.
	Off	Power is off or no power is being supplied to the switch.
PWR1	Green	Power is on.
	Off	Power is off or no power is being supplied to the switch.
PWR2	Green	Power is on.
	Off	Power is off or no power is being supplied to the switch.
Fault	Orange	One of the following errors occur: ● Power failure ● UTP port failure ● Fiber port failure
	Off	None of the above mentioned errors occurs.
R.M.	Green	This switch unit is the Ring Master.
	Off	This switch unit is NOT the Ring Master.
FWD (P1-P8)	Green	The port is supplying power to the powered device (PD)
	Off	No powered-device (PD) attached or power supplying fails
Link/Active (P9-P10, SFP)	Green	The fiber port is linked.
	Blinking	The port is transmitting or receiving packets from a TX device.
	Off	No device is attached.
RJ-45 Ports (P1-P10)	Orange	The port is operating in full-duplex mode.
	Blinking Orange	Collision of packets occurs.
	Off	The port is in half-duplex mode or no device is attached.
	Green	A network device is detected.
	Blinking Green	The port is transmitting or receiving packets from a TX device.
	Off	No device is attached.

2-3 RJ-45 Ports

CME-822(E) has 8 10/100Mbps auto-sensing ports for 10Base-T or 100Base-TX devices connection. The UTP ports can auto-sense for 10Base-T or 100Base-TX connections. Auto MDI/MDIX function allows CME-822(E) to connect to another switch or workstation without changing straight through or crossover cabling. See **Cabling** section for straight through and crossover cable schematic.

2-3.1 RJ-45 Pin Assignments

RJ-45 pin assignments as described in the table below:

Pin Number	Assignment
1	Tx+
2	Tx-

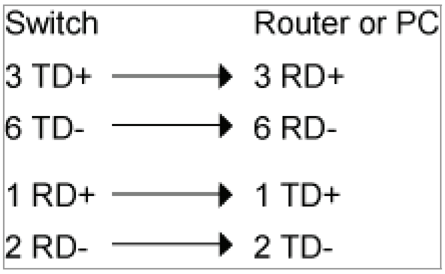
3	Rx+
6	Rx-

"+" and "-" signs represent the polarity of the wires that make up each wire pair.

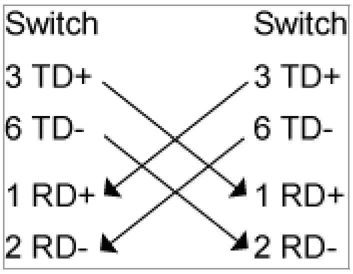
All ports on CME-822(E) support automatic MDI/MDI-X function, users can use straight-through cables (see figure below) for all network connections to PCs or servers, or to other switches or hubs. When auto MDI/MDI-X is enabled, either type of cable can be used and the interface automatically corrects any incorrect cabling. The table below shows the 10Base-T/100Base-TX MDI and MDI-X port pinouts.

Pin	MDI	MDI-X
1	TD+	RD+
2	TD+	RD-
3	RD+	TD+
6	RD-	TD-

Below are the illustrations of straight through connection and cross over connection.



Straight Through Cable Schematic



Cross Over Cable Schematic

2-3.2 RJ-45 PoE Pin Assignments

RJ-45 PoE pin assignments as described in the table below:

Pin Number	Assignment
1	VCC+
2	VCC+
3	VCC-
6	VCC-

CME-822(E) supports PoE function and it has classified as PSE (Power Sourcing Equipment) where the power can be supplied to the Powered-device (PD) via RJ-45 ports with Type-A (Alternative A) PoE pin assignment, with its PoE capability, the CME-822(E) is a perfect solution for the PoE End-point application in your industrial environment.

2-4 Gigabit Copper/SFP Combo Ports

CME-822(E) has 2 gigabit copper/SFP combo ports. SFP design gives users more flexibility in choosing fiber modules to fit the existing network structure on the plant floor. The 2 combo ports will automatically detect UTP or fiber connection.

ℹ	If both copper port and SFP port are cabled, CME-822(E) has auto-detecting mechanism that will prioritize the fiber connection and disable the copper port connection.

2-5 Installing Your Ethernet Direct Switch

Unpack the CME-822(E) from the packing box. Please refer to **Package Checklist** section to see if any item is missing or damaged. The installation steps include **Mounting The Switch**, **Wiring The Power Inputs**, **Wiring The Fault Alarm Contact**, and **Cabling**.

2-5.1 Mounting The Switch

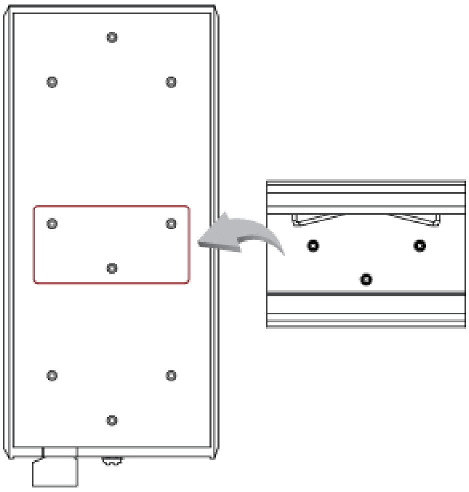
The are two types of mounting options: DIN-Rail mounting, and wall mounting. Users can choose the most suitable mounting installation for your own onsite applications.

2-5.1.1 DIN-Rail Mounting

The DIN-Rail mounting kit is attached to the back panel of CME-822(E) by default. If not, or users want to disassemble the DIN-Rail mounting kit from the CME-822(E), follow the steps below.

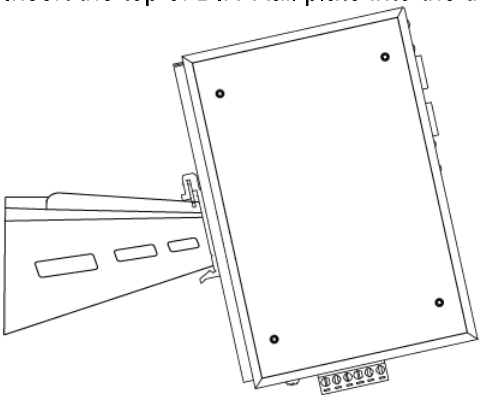
To attach the DIN-Rail mounting kit:

1. Screw the DIN-Rail kit to the position shown in the figure below.
2. To detach DIN-Rail kit from the switch, reverse the step 1.

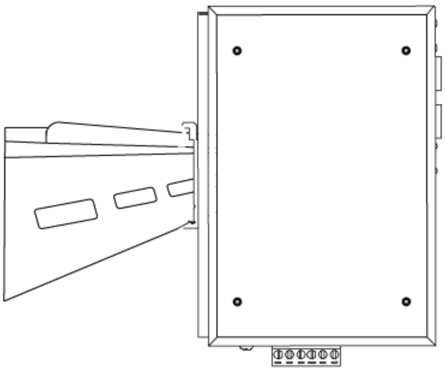


Follow the steps below for mount the switch onto the track.

1. Insert the top of DIN-Rail plate into the track.



2. Lightly push the DIN-Rail plate into the track.

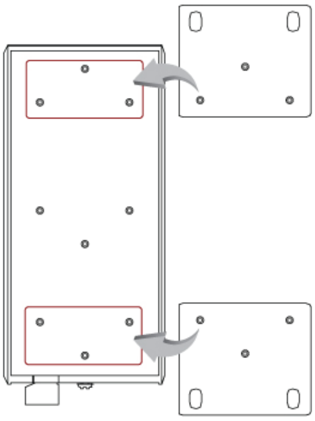


3. Check if the DIN-Rail is tightened on the track or not.
4. To remove the switch from the track, reverse steps above.

2-5.1.2 Wall Mounting

Follow the steps below for wall-mounting installation.

1. Remove the DIN-Rail plate from the switch; loosen the screws to remove the DIN-Rail plate.
2. Place the wall mounting plate on the back panel of the switch.
3. Use the screws to screw the wall mounting plates on the switch.
4. Use the hook holes at the corners of the wall mounting plates to place the switch on the wall.
5. To remove the wall mounting plate, reverse the steps above.

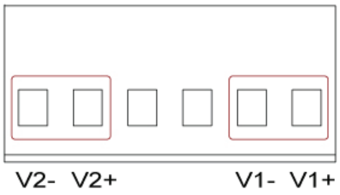


2-5.2 Wiring The Power Inputs

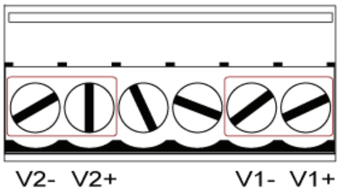
Follow the steps below to wire the power inputs.

⚠	Be sure to disconnect the power cord before installing and/or wiring your switch. Be sure of the maximum possible current when wiring connections. If the current goes above the maximum ratings, the wire could overheat and result in serious damage to your switch.

1. Insert the positive and negative wires of your DC supply into the corresponding V+ and V- contacts of the terminal block.



2. Tighten the screws to prevent the DC wires from coming detached.



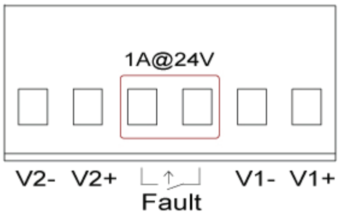
The acceptable wire range is 12 to 24 AWG.

After the wiring the power inputs, the PWR LED will light up. Please refer to LED Indicators section for more information.

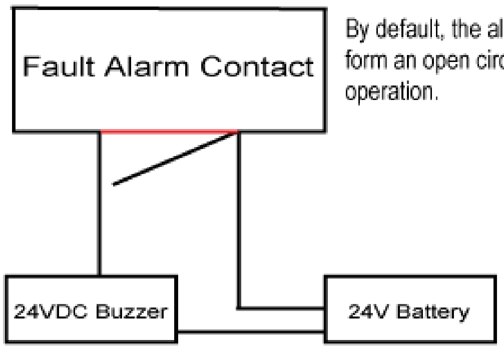
2-5.3 Wiring The Fault Alarm Contact

The fault alarm contacts are the two middle terminals located on the terminal block as show in the figure below. It detects errors such as power failure or port break and sends an alarm signal when faults occur. By default, the fault alarm contacts will form an open circuit under normal operation. The contacts will close when power failures or port breaks are detected. See below steps for wiring the fault alarm contact, and the illustration of how fault alarm contact function works.

1. Insert the wires into the two middle terminals. Tighten the screws to prevent the wires from coming detached.



How Fault Alarm Contact Works



When power failures or port breaks occur, the contact will form a closed circuit, and the fault alarm device will send a warning signal.

By default, the alarm contact will form an open circuit under normal operation.

The acceptable wire range is 12 to 24 AWG.

2-5.4 Cabling

For RJ-45 port connection, prepare twisted-paired, straight through Category 5 or above cables for Ethernet connection. The linking distance between the switch and the network device must be less than 100 meters (328 ft.).

For single-mode fiber connection, a 9/125µm single-mode fiber cables must be used. The maximum linking distance can be up to 30km.

For multi-mode fiber connection, a 50 or 62.5/125µm multi-mode fiber cable must be used. The maximum linking distance can be up to 2km.

The UTP port (RJ-45) LED(s) on the switch will light up when the cable is connected with the network device. Please refer to the LED Indicators section for more information.

⚠	Before connecting any network device, make sure network devices support auto MDI/MDI-X. If not support, use the cross over Category 5 or above cables.

After all wiring and connection are done and the LED lights on the switch’s front panel show normal status, the hardware installation is complete.

Chapter 3

Configuration Using Console Interface

This chapter describes how to configure CME-822(E) using the console interface. The topics include:

- Connecting Console Port
- Login the Console Interface
- CLI Management

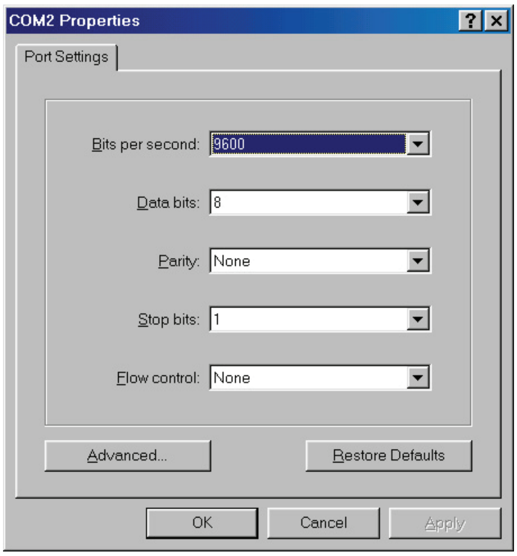
3-1 Connecting Console Port

Take out the RS-232/RJ-45 cable that comes with the CME-822(E) package, connect the RS-232 end to a PC or a terminal, and connect the RJ-45 end to the console port of CME-822(E). The linked PC or terminal must support the terminal emulation program.

3-2 Login The Console Interface

After the connection between the PC/terminal and the CME-822(E) is successfully established, turn on the PC/terminal and run a terminal emulation program or Hyper Terminal to configure its communication parameters to match the following default settings of the console port:

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



Bits per second: 9600

Data bits: 8

Parity: None

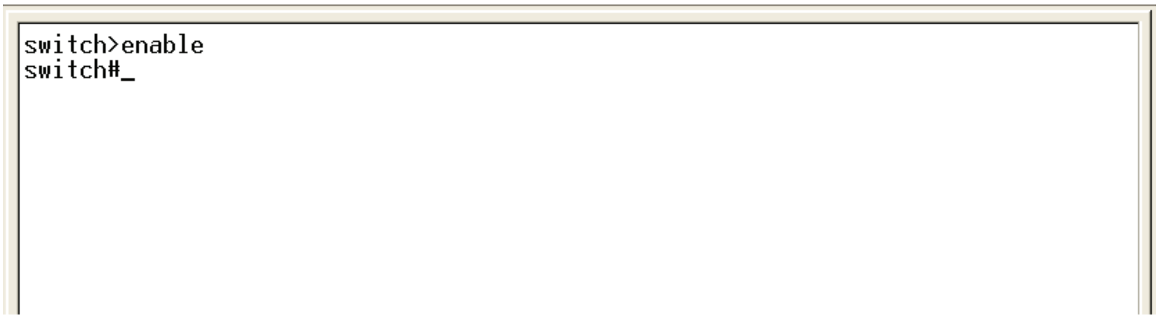
Stop bits: 1

Flow control: None

After finishing the parameter settings, click **OK**. When the blank screen shows up, press **Enter** key to bring out the login prompt. Key in **root** (default value) for the both User name and Password (use **Enter** key to switch), then press **Enter** key and the Main Menu of console management will appear.

3-3 CLI Management

The system supports the console management – CLI command. After logging into the system, you will see a command prompt. To enter CLI management interface, type in **enable** command. Please see below figure for CLI command interface.



```
switch>enable
switch#_
```

For Command Levels, and Command Set Lists, please refer to **Appendix C**.

3-4 Command Levels

The table below lists the command levels. For Command Set Lists, please refer to **Appendix C**.

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

Chapter 4

Configuration Using a Web Browser

This chapter contains information on how to configure your CME-822(E) via a web browser. The topics include:

- About Web-based Management Interface
- Preparing for Web-based Management
- System Login
- Management Main Screen
- Basic Settings
- Advanced Management Settings

4-1 About Web-based Management Interface

CME-822(E) offers an easy-to-use management interface, which allows users to manage the CME-822(E) via a standard web browser such as IE from anywhere on the network.

This web-based management interface supports Internet Explorer 6.0 or later version. Java Applets is also applied for reducing network bandwidth consumption, enhancing access speed and presenting an easy-viewing screen.

4-2 Preparing for Web-based Management

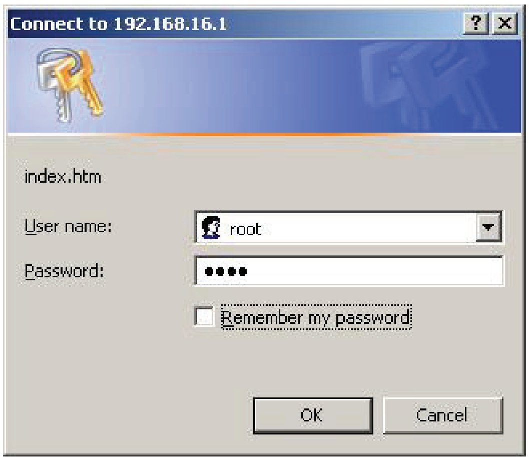
Before using web-based management interface, install the CME-822(E) onto the network and make sure that any one of PC on the network can access the CME-822(E) through a web browser. The default settings of IP address, subnet mask, username, and password of the CME-822(E) are as follows:

IP Address	192.168.16.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.16.254
User Name	root
Password	root

4-3 System Login

Follow the steps below to login into the web-based management interface.

1. Launch the web browser.
2. Key in the default IP address in the web address box and press **Enter**.
3. The login window will appear.
4. Key in the user name and the password. The default username and password is **root**.



Connect to 192.168.16.1

index.htm

User name: root

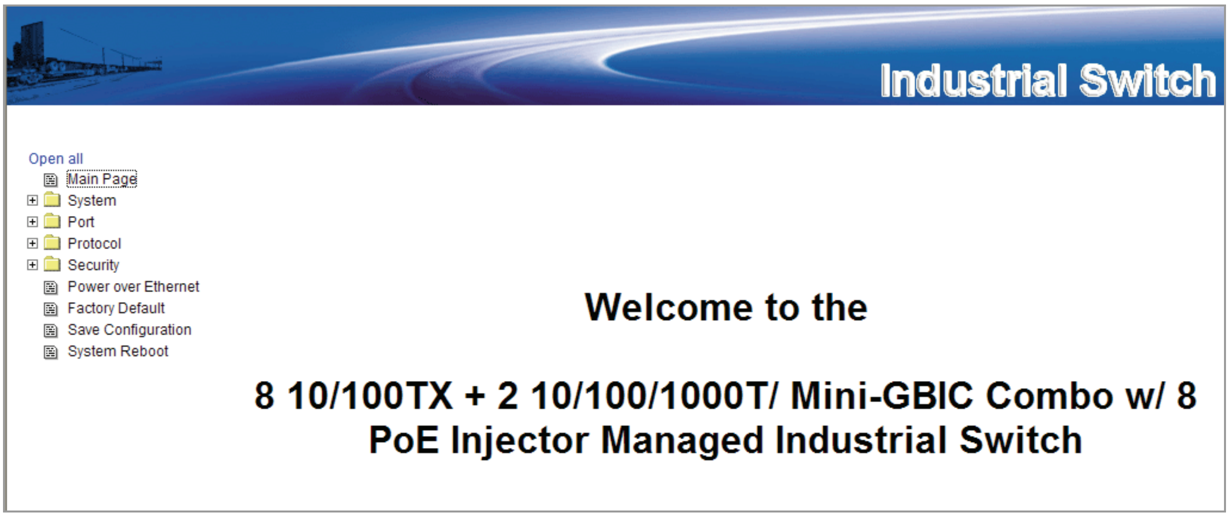
Password: ••••

5. Press **Enter** or click **OK**, the main screen of web-based management interface will then appear. Please

refer to the **Management Main Screen** section for more information.

4-4 Management Main Screen

See below for the web-based management interface main screen. The function menu is located on the left hand side of this entrance page.



Welcome to the

8 10/100TX + 2 10/100/1000T/ Mini-GBIC Combo w/ 8 PoE Injector Managed Industrial Switch

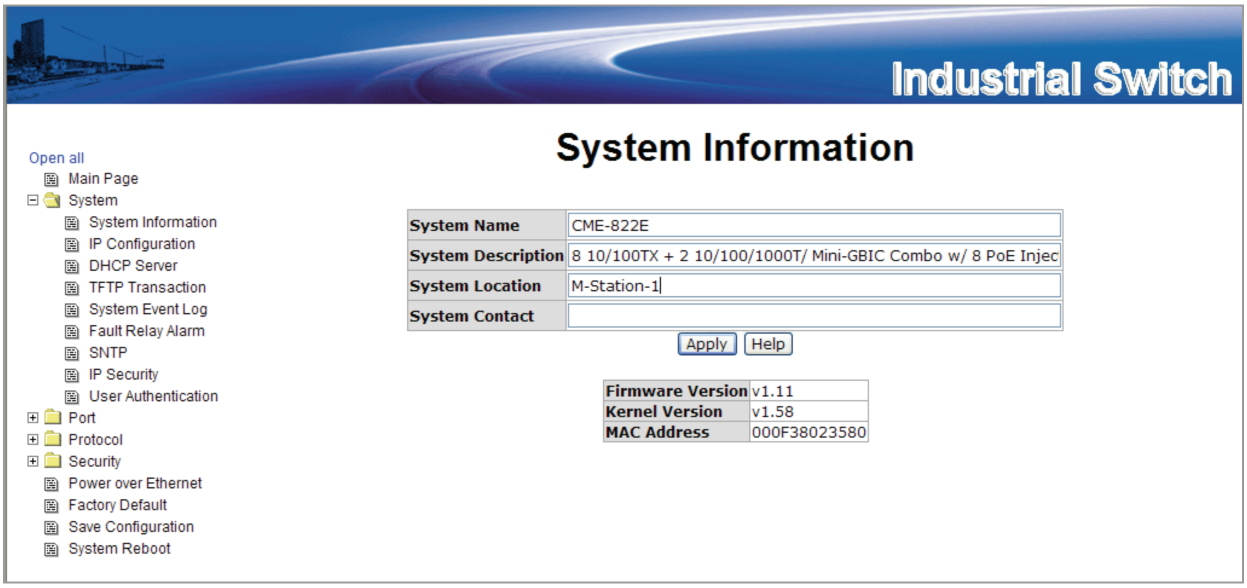
4-5 Basic Settings

This section covers the most commonly used configurations for maintain and control CME-822(E).

4-5.1 System Information

This feature allows you to assign the system name and location, and to view the system information.

System Name	Use this feature to assign a name for the switch. The maximum length is 64 bytes.
System Description	To display the description of the switch. This is READ ONLY information. It cannot be modified.
System Location	Use this feature to specify the physical location of the switch. The maximum length is 64 bytes.
System Contact	To provide the information of the contact person in case of problems. Use this feature to enter the contact person info responsible for maintain this switch.
Firmware Version	To display the switch's firmware version.
Kernel Version	To display the switch's kernel software version.
MAC Address	To display the unique hardware address assigned by Ethernet Direct (default).



System Information

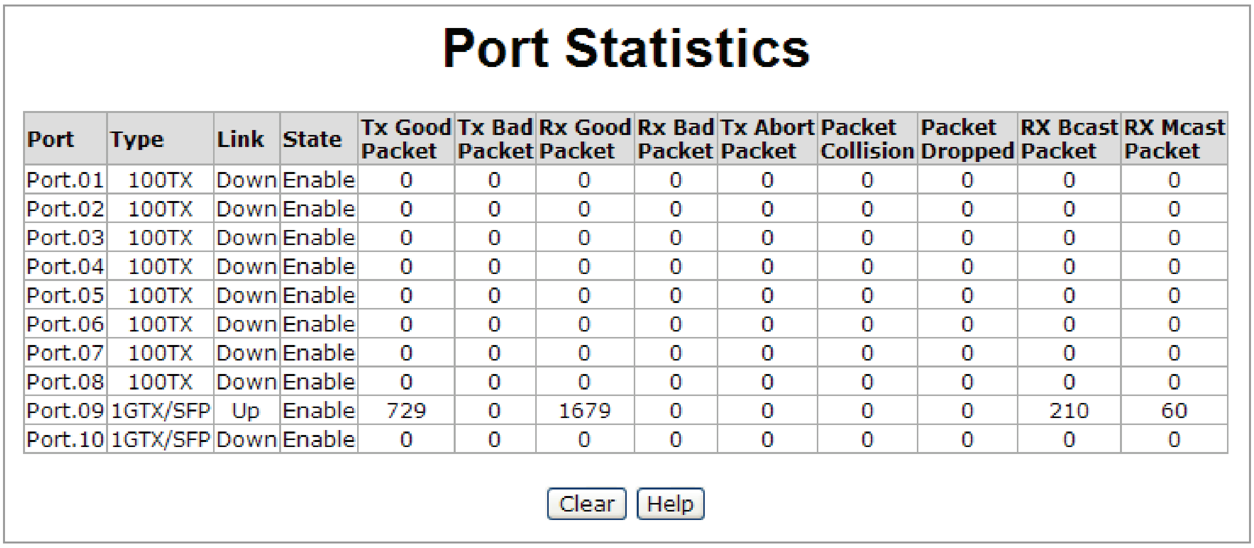
System Name	CME-822E
System Description	8 10/100TX + 2 10/100/1000T/ Mini-GBIC Combo w/ 8 PoE Injec
System Location	M-Station-1
System Contact	

Firmware Version	v1.11
Kernel Version	v1.58
MAC Address	000F38023580

4-5.2 Port Statistics

The feature allows users to view the information of the port statistics.

Port	This column shows port number.
Type	This column shows the current connection speed of the port.
Link	This column shows the link status, either **Up** or **Down**.
State	This column shows whether the port is enabled or disabled. When the port is disabled, no packet will be transmitted or received by this port. To enable or disable ports, please refer to **Port Control** section for more information.
Tx Good Packet	This column shows the number of good packets transmitted by this port.
Tx Bad Packet	This column shows the number of bad packets transmitted by this port, including undersized packets (less than 64 octets), oversized packets, CRC Align errors, fragmented and jabber packets.
Rx Good Packet	This column shows the number of good packets received by this port.
Rx Bad Packet	This column shows the number of bad packets received by this port, including undersized packets (less than 64 octets), oversized packets, CRC Align errors, fragmented and jabber packets.
Tx Abort Packet	This column shows the number of aborted packets while transmitting.
Packet Collision	This column shows the number of collision packets.
Packet Dropped	The column shows the number of dropped packets.
RX Bcast Packet	The column shows the number of broadcast packets.
RX Mcast Packet	The column shows the number of multicast packets.



Port Statistics

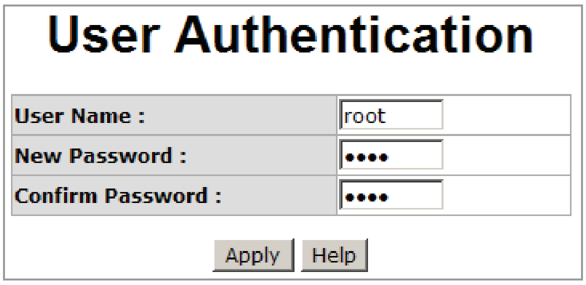
Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision	Packet Dropped	RX Bcast Packet	RX Mcast Packet
Port.01	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.07	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.08	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.09	1GTX/SFP	Up	Enable	729	0	1679	0	0	0	0	210	60
Port.10	1GTX/SFP	Down	Enable	0	0	0	0	0	0	0	0	0

Click on **Clear** to remove the current values.

4-5.3 User Authentication

This feature allows the administrator to change the web management login user name and password for security reason.

User name	Key in the new user name (the default username is root).
Password	Key in the new password (the default username is root).
Confirm password	Re-type the new password.



User Authentication

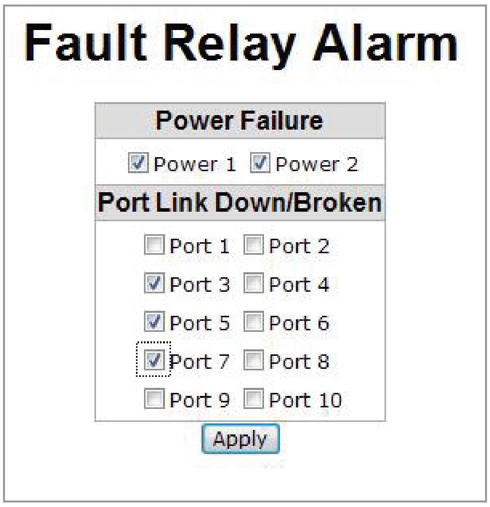
User Name :	root
New Password :	••••
Confirm Password :	••••

After finishing necessary configurations, click on **Apply** to save the settings.

4-5.4 Fault Relay Alarm

The Fault Relay Alarm function provides the Power Failure and Port Link Down/Broken detection. With both power input 1 and power input 2 installed and the check boxes of power 1/power 2 marked, the FAULT LED indicator will then be possible to light up when any one of the power failures occurs. As for the Port Link Down/Broken detection, the FAULT LED indicator will light up when the port failure occurs if the check box beside the port is marked. Please refer to the segment of ‘Wiring the Fault Alarm Contact’ for the failure detection.

Power Failure	The FAULT LED on the front panel of the CME-822(E) will light up when a power failure occurs if this box is checked.
Port Link Down/Broken	The FAULT LED on the front panel of the CME-822(E) will light up when a port link is down or broken if this box is checked.



Fault Relay Alarm

Power Failure

☑ Power 1 ☑ Power 2

Port Link Down/Broken

☐ Port 1 ☐ Port 2

☑ Port 3 ☐ Port 4

☑ Port 5 ☐ Port 6

☑ Port 7 ☐ Port 8

☐ Port 9 ☐ Port 10

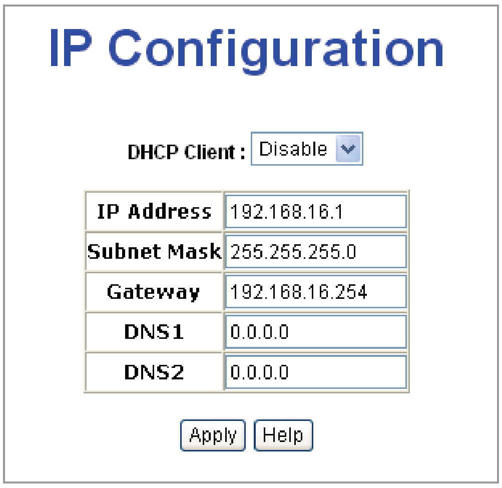
After finishing necessary configurations, click on **Apply** to save the settings.

4-5.5 IP Configuration

This feature allows users to configure the IP settings and DHCP client function of the CME-822(E).

DHCP Client	Use this feature to enable or disable the DHCP Client function. When DHCP Client is enabled, the CME-822(E) will be assigned with an IP address from the network DHCP server. The default IP address will be replaced by the DHCP server-assigned IP address. After clicking on **Apply** button, a popup window will show up. It is to inform the administrator that when the DHCP Client is enabled, the current IP will no longer exist, and new one will be assigned by the DHCP server.
IP Address	Use this feature to assign an IP address to the CME-822(E). The administrator will not need to assign an IP address to the CME-822(E) if the DHCP Client function is enabled, and this column will show the IP address assigned by the DHCP server. The default IP is 192.168.16.1.
Subnet Mask	Use this feature to assign the subnet mask of the IP address. The administrator will not need to assign the subnet mask if the DHCP Client function is enabled.
Gateway	Use this feature to assign the network gateway for the industrial switch. The default gateway is 192.168.16.254.
DNS1	Use this feature to assign the primary DNS IP address.
DNS2	Use this feature to assign the secondary DNS IP address.

After finishing necessary configurations, click on **Apply** to save the settings.



IP Configuration

DHCP Client : Disable

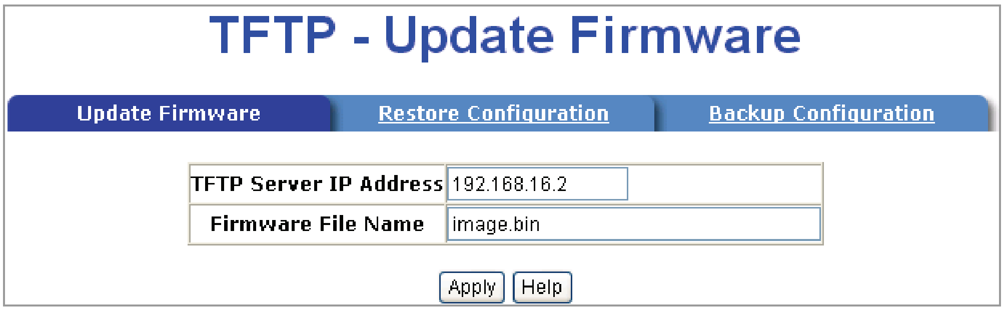
IP Address	192.168.16.1
Subnet Mask	255.255.255.0
Gateway	192.168.16.254
DNS1	0.0.0.0
DNS2	0.0.0.0

4-5.6 Updating Firmware by TFTP

This feature allows the administrator to update the switch firmware. Before updating, make sure the TFTP server is ready and the firmware image is on the TFTP server.

TFTP Server IP Address	Use this feature to fill in your TFTP server IP.
Firmware File Name	Use this feature to fill in the name of the firmware image.

After finishing necessary configurations, click on **Apply** to save the settings.



TFTP - Update Firmware

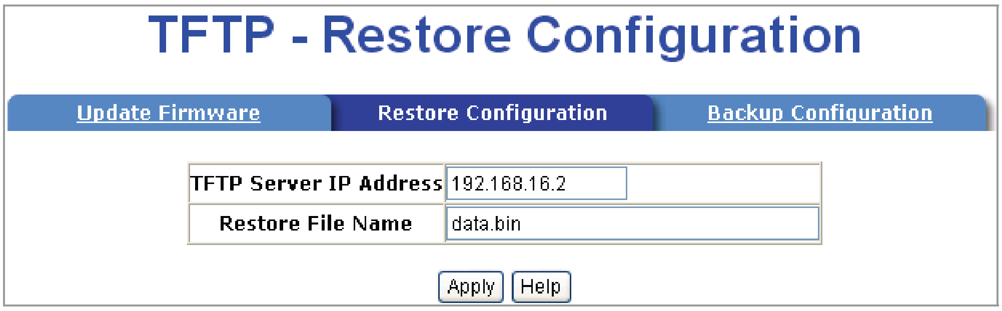
TFTP Server IP Address	192.168.16.2
Firmware File Name	image.bin

4-5.7 Restoring Configurations by TFTP

You can restore EEPROM value from the TFTP server. Before doing so, make sure the image file is already placed on TFTP server. The CME-822(E) will download the flash image.

TFTP Server IP Address	Use this feature to fill in your TFTP server IP.
Firmware File Name	Use this feature to fill in the correct file name to restore.

After finishing necessary configurations, click on **Apply** to save the settings.



TFTP - Restore Configuration

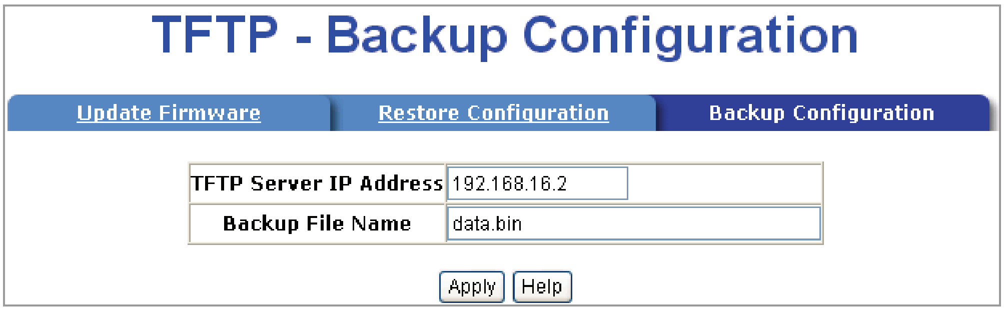
TFTP Server IP Address	192.168.16.2
Restore File Name	data.bin

4-5.8 Backing up Configurations by TFTP

With this feature, the administrator can save the current EEPROM configurations from the CME-822(E) to the TFTP server, and then go to the TFTP restore configuration page to restore the EEPROM settings.

TFTP Server IP Address	Use this feature to fill in your TFTP server IP.
Firmware File Name	Use this feature to fill in the file name.

After finishing necessary configurations, click on **Apply** to save the settings.

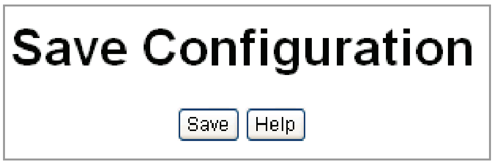


TFTP - Backup Configuration

TFTP Server IP Address	192.168.16.2
Backup File Name	data.bin

4-5.9 Saving Configuration Files

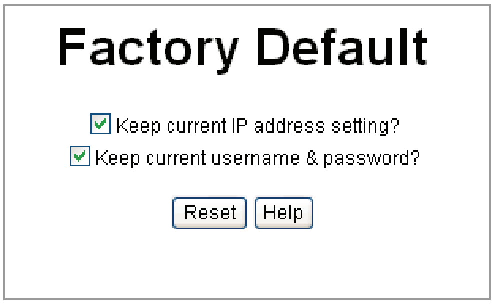
This feature allows the administrator to save all configurations made for the CME-822(E). Click **Save** to save all of the CME-822(E)'s settings to the flash memory.



Save Configuration

4-5.10 Factory Default

This feature allows the administrator to reset the CME-822(E) to the default settings. Click **Reset** to reset all configurations to the default value.



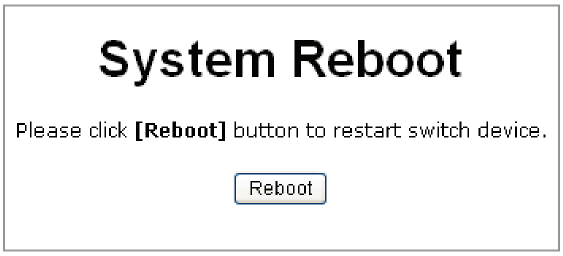
Factory Default

☑ Keep current IP address setting?

☑ Keep current username & password?

4-5.11 Rebooting System

This feature allows the administrator to reboot the CME-822(E). Click **Reboot** to restart the switch.



System Reboot

Please click **[Reboot]** button to restart switch device.

4-6 Advanced Management Settings

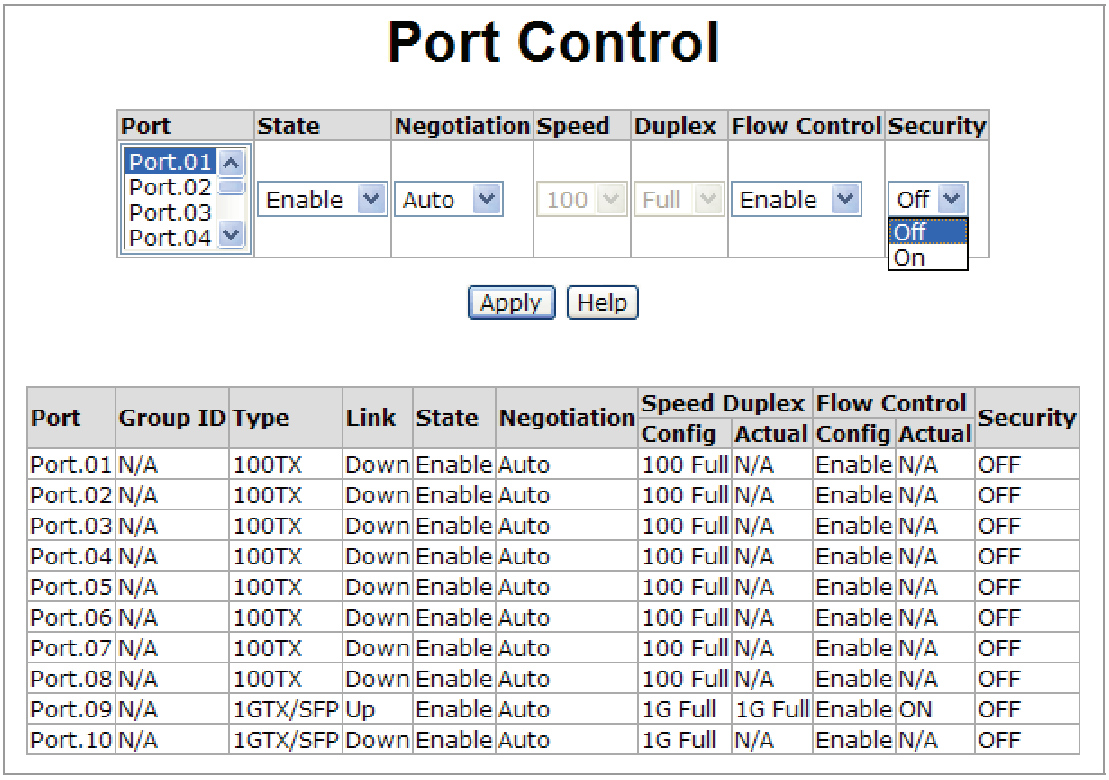
This section covers the instructions on how to configure CME-822(E)'s advanced management functions.

4-6.1 Port Control

This feature allows the administrator to configure each port's settings and view the port status.

Port	This column is for you to select the port that you want to configure.
State	This column shows the current port status, and also allows you to enable or disable the port. If the port is disabled, no packet will be transmitted or received by this port.
Negotiation	This feature allows you to configure the negotiation function to be **Auto** or **Force**. When **Auto**, the switch will auto-negotiate the speed and the duplex mode with the connected port. When **Force**, the administrator will have to manually configure the speed in the **Speed** column and the duplex mode in **Duplex** column to match with the connected port.
Speed	When **Negotiation** column is configured as **Force**, this column will be available for you to choose the port link speed.
Duplex	When **Negotiation** column is configured as **Force**, this column will be available for you to choose the duplex mode of the port.
Flow Control	This feature allows the administrator to select flow control options. When **Disable**, the receiving device will drop the packet if there is too much to process. When **Enable**, once the device exceeds the input data rate of another device, the receiving device will send a PAUSE frame which halts the transmission of the sender for a specified period of time.
Security	This feature allows the administrator to configure the security level for managing this switch. If the security column is configured as **On**, the port will accept only the first MAC address entry in **Static MAC Address** table to access this switch and change the switch settings. If the security

	column is configured as **Off**, any MAC address can access the switch and change the switch settings.



Port Control

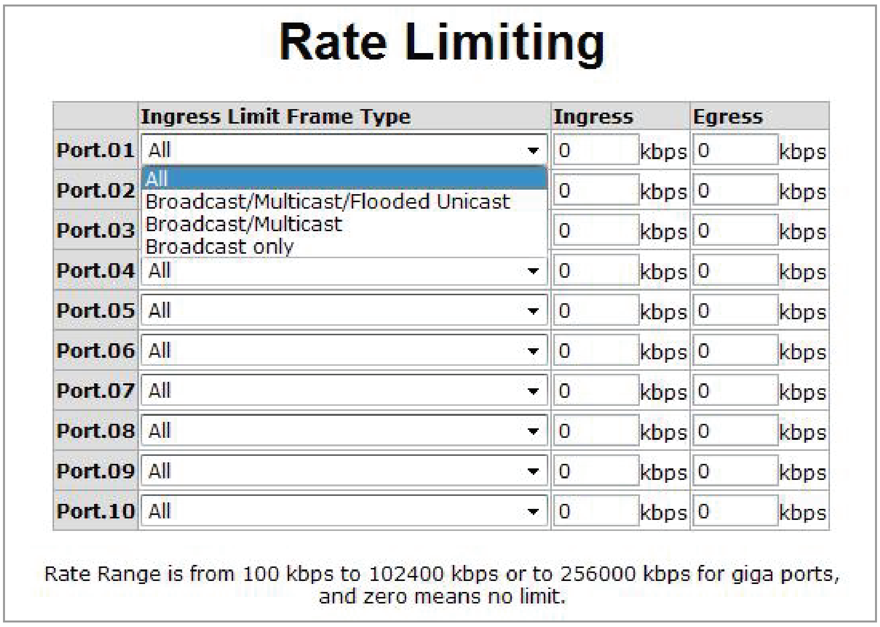
Port	State	Negotiation	Speed	Duplex	Flow Control	Security
Port.01 Port.02 Port.03 Port.04	Enable	Auto	100	Full	Enable	Off Off On

Port	Group ID	Type	Link	State	Negotiation	Speed Duplex		Flow Control		Security
						Config	Actual	Config	Actual	
Port.01	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.02	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.03	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.04	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.05	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.06	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.07	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.08	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.09	N/A	1GTX/SFP	Up	Enable	Auto	1G Full	1G Full	Enable	ON	OFF
Port.10	N/A	1GTX/SFP	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF

4-6.2 Rate Limiting

This feature allows the administrator to set up every port's bandwidth rate and packet limitation type.

Ingress Limit Frame Type	This feature allows the administrator to select the packet type that needs to be filtered for a certain port. The packet types available for selecting include: ➢ **All** ➢ **Broadcast/Multicast/Flooded Unicast** ➢ **Broadcast/Multicast** ➢ **Broadcast only** **Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast**, and **Broadcast only** are only for ingress packets. The egress rate only supports **All** type.
Bandwidth	All ports support port ingress and egress rate control. For example, if port 1 runs at 10Mbps, the administrator can set its effective egress rate as 1Mbps, and ingress rate is 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate. ➢ **Ingress:** Enter the port effective ingress rate (The default value is 0). ➢ **Egress for All**: Enter the port effective egress rate (The default value is 0).



Rate Limiting

	Ingress Limit Frame Type	Ingress		Egress	
Port.01	All ▾ All Broadcast/Multicast/Flooded Unicast Broadcast/Multicast Broadcast only	0	kbps	0	kbps
Port.02		0	kbps	0	kbps
Port.03		0	kbps	0	kbps
Port.04	All ▾	0	kbps	0	kbps
Port.05	All ▾	0	kbps	0	kbps
Port.06	All ▾	0	kbps	0	kbps
Port.07	All ▾	0	kbps	0	kbps
Port.08	All ▾	0	kbps	0	kbps
Port.09	All ▾	0	kbps	0	kbps
Port.10	All ▾	0	kbps	0	kbps

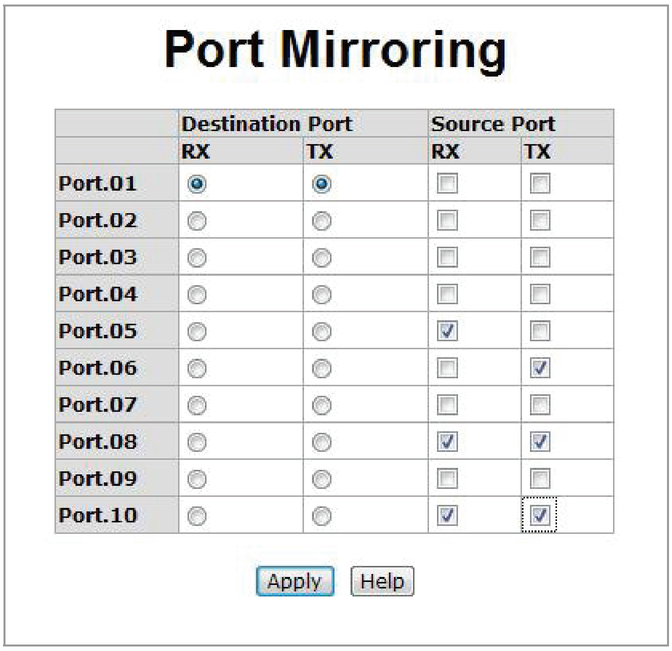
Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.

After finishing necessary configurations, click on **Apply** to save the settings.

4-6.3 Port Mirroring

The feature allows the administrator to monitor and record the traffic of a specific port. The traffic goes in or out of the monitored ports will be duplicated into the mirror port.

Destination Port	There is only one port can be selected to be destination (mirror) port for monitoring both RX and TX traffic which come from source ports. Or, use one of two ports for monitoring RX traffic only and the other one for TX traffic only. The administrator can connect the mirror port to LAN analyzer.
Source Port	The port(s) the administrator wants to monitor. All source port(s) traffic will be copied to the destination (mirror) port. The administrator can select up to 7 monitor ports in the switch. The administrator can select multiple source ports by checking the RX or TX boxes.



Port Mirroring

	Destination Port		Source Port	
	RX	TX	RX	TX
Port.01	●	●	□	□
Port.02	○	○	□	□
Port.03	○	○	□	□
Port.04	○	○	□	□
Port.05	○	○	☑	□
Port.06	○	○	□	☑
Port.07	○	○	□	□
Port.08	○	○	☑	☑
Port.09	○	○	□	□
Port.10	○	○	☑	☑

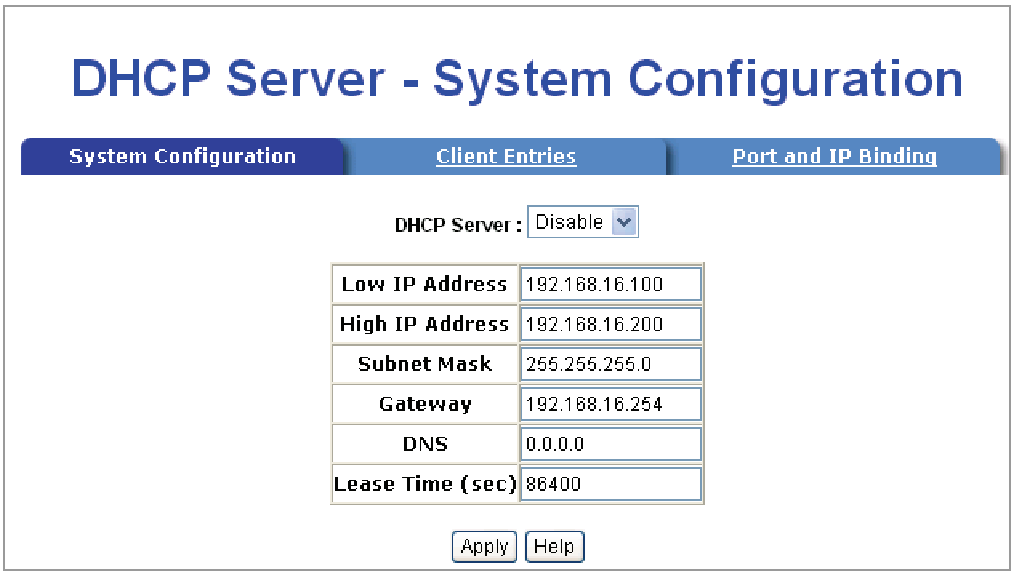
After finishing necessary configurations, click on **Apply** to save the settings.

4-6.4 DHCP Server

CME-822(E) offers the DHCP server function. CME-822(E) will be a DHCP server if the DHCP server function is enabled.

DHCP Server	This feature allows the administrator to enable or disable the CME-822(E) to be a DHCP server on the local network.
Low IP Address	This feature allows the administrator to define the low boundary of the IP address range that the DHCP server will assign to devices that request them.
High IP Address	This feature allows the administrator to define the high boundary of the IP address range that the DHCP server will assign to devices that request them.
Subnet Mask	This feature is to define the subnet mask for the dynamic IP assign range.
Gateway	This feature is to define the gateway in your network.
DNS	This feature is to define the Domain Name Server IP Address in your network.
Lease Time (sec)	It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not be occupied for a long time or the server doesn't know that the dynamic IP is idle.

After finishing necessary configurations, click on **Apply** to save the settings.



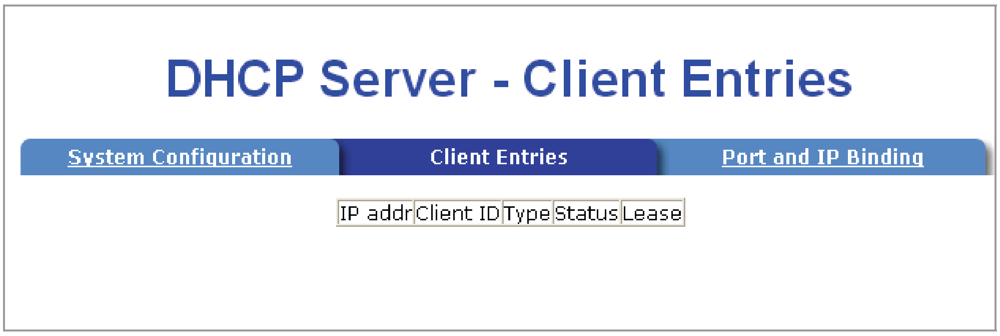
DHCP Server - System Configuration

DHCP Server : Disable

Low IP Address	192.168.16.100
High IP Address	192.168.16.200
Subnet Mask	255.255.255.0
Gateway	192.168.16.254
DNS	0.0.0.0
Lease Time (sec)	86400

4-6.5 DHCP Client

When the DHCP server function is active, the CME-822(E) will collect the DHCP client information and display it here.



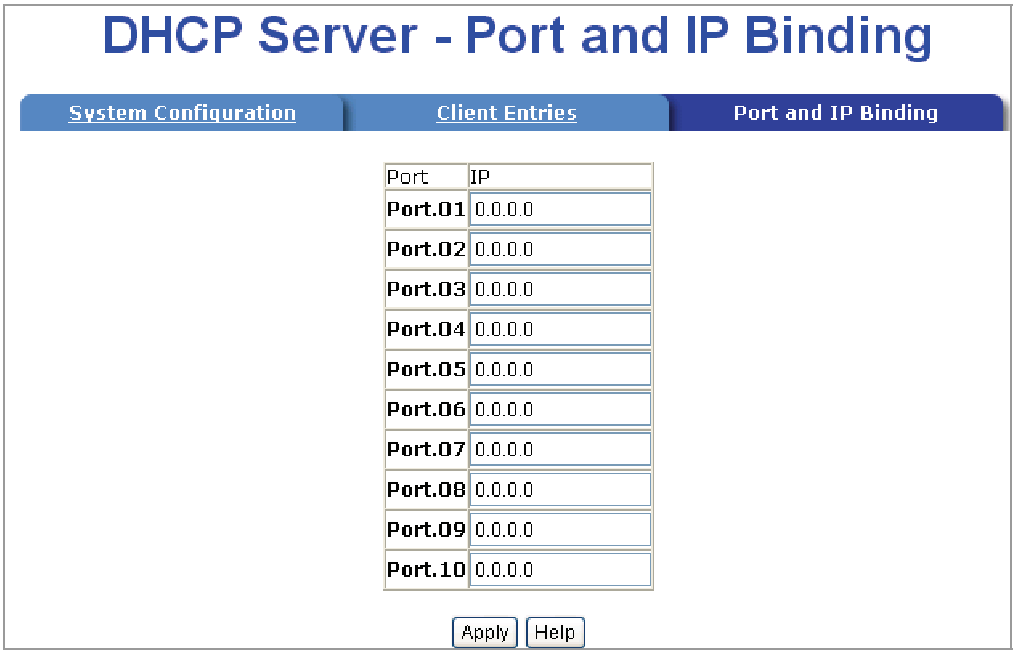
DHCP Server - Client Entries

IP addr	Client ID	Type	Status	Lease

4-6.6 Port and IP Bindings by DHCP Server

This feature allows the administrator to pre-define a specific IP address within the dynamic IP range to a certain port. When a device connected to this certain port requests for an IP address, this pre-defined IP address will then be assigned to this connected device.

After finishing necessary configurations, click on **Apply** to save the settings.



DHCP Server - Port and IP Binding

Port	IP
Port.01	0.0.0.0
Port.02	0.0.0.0
Port.03	0.0.0.0
Port.04	0.0.0.0
Port.05	0.0.0.0
Port.06	0.0.0.0
Port.07	0.0.0.0
Port.08	0.0.0.0
Port.09	0.0.0.0
Port.10	0.0.0.0

4-6.7 System Event Log

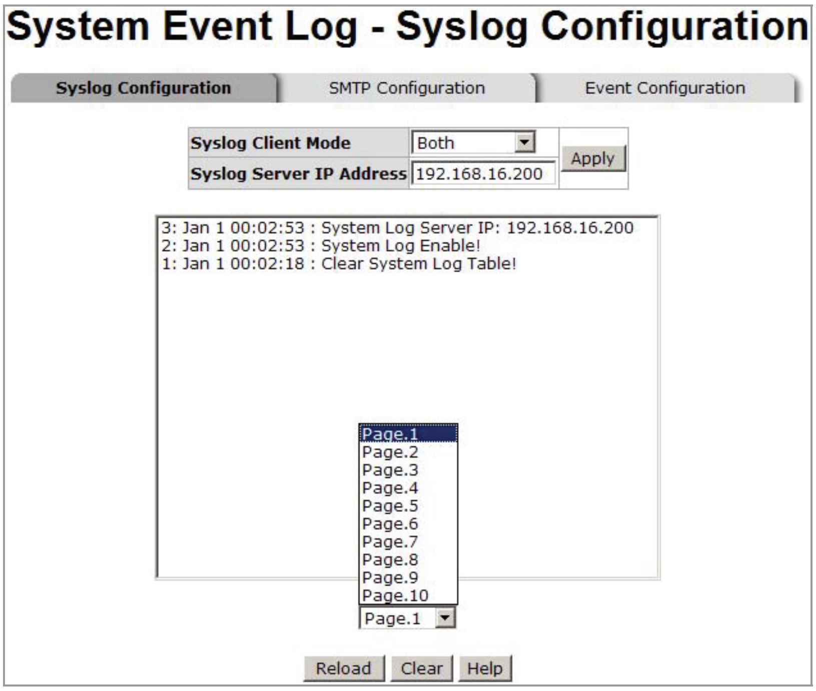
4-6.7.1 Syslog Configuration

This feature allows the administrator to configure the ways of keeping the system log files, and define the system log server IP.

Syslog Client Mode	This feature allows the administrator to select the system log mode – client only, server only, or both S/C. **Client only**: it means the system log will only be saved in the switch. **Server only**: it means the system log will only be saved in a connected PC or server. **Both S/C**: it means the system log will be saved in both the switch and the PC.
System Log Server IP Address	This feature allows the administrator to assign the system log server IP.

After finishing necessary configurations, click on **Reload** to refresh the event log, or click on **Clear** to erase all current event logs. And then click on **Apply** to save the settings.

⚠	The system log saved in the switch when the **Client only** mode is selected will be lost once the switch is restarted.



Syslog Client Mode	Both
Syslog Server IP Address	192.168.16.200

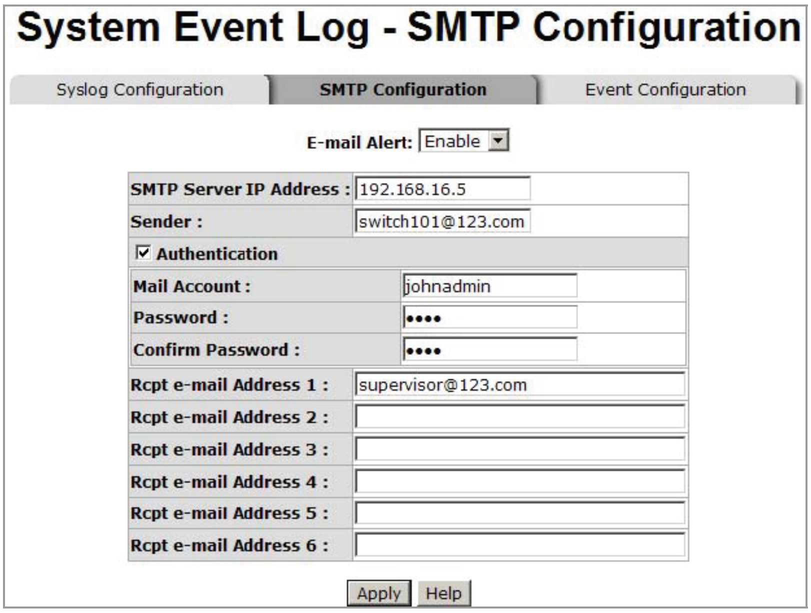
```
3: Jan 1 00:02:53 : System Log Server IP: 192.168.16.200
2: Jan 1 00:02:53 : System Log Enable!
1: Jan 1 00:02:18 : Clear System Log Table!
```

4-6.7.2 SMTP Configuration

This feature allows the administrator to set up the mail server IP, mail account, account password, and forwarding email account for receiving the event alert.

Email Alert	This feature is to enable or disable the email alert function.
SMTP Server IP	This feature is to set up the mail server IP address (when Email Alert enabled, this function will then be available).
Sender	Type in an alias of the switch in complete email address format, e.g. switch101@123.com, to identify where the e-mail alert comes from.
Authentication	Check the box to enable and configure the email account and password for authentication (when Email Alert is enabled, this function will then be available).
Mail Account	This feature is to set up the email account, e.g. johnadmin@123.com, to receive the alert. It must be an existing email account on the mail server, which you set up in SMTP Server IP Address column.
Password	Use this feature to set up the email account password.
Confirm Password	To reconfirm the password.
Rcpt e-mail Address 1-6	This feature is to assign up to 6 e-mail accounts which will also receive the alert.

After finishing necessary configurations, click on **Apply** to save the settings.



System Event Log - SMTP Configuration

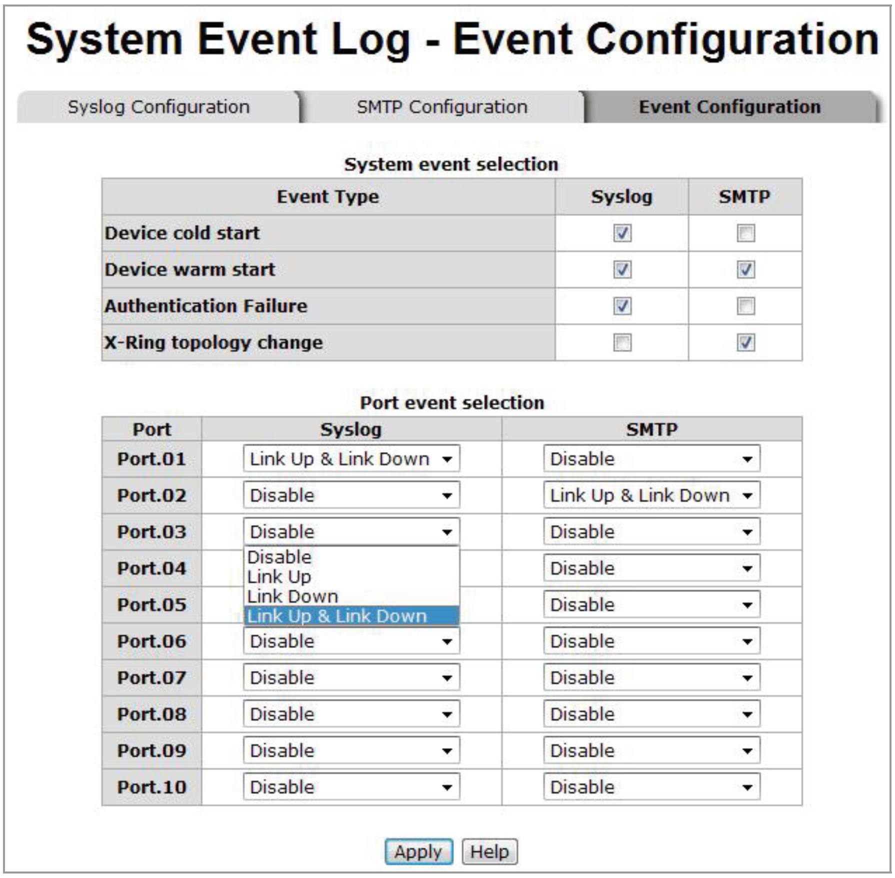
E-mail Alert: Enable

SMTP Server IP Address :	192.168.16.5
Sender :	switch101@123.com
☑ Authentication	
Mail Account :	johnadmin
Password :	••••
Confirm Password :	••••
Rcpt e-mail Address 1 :	supervisor@123.com
Rcpt e-mail Address 2 :	
Rcpt e-mail Address 3 :	
Rcpt e-mail Address 4 :	
Rcpt e-mail Address 5 :	
Rcpt e-mail Address 6 :	

4-6.7.3 Event Configuration

This feature allows the administrator to pre-define the events which will trigger the system log to document errors occurred and send out alert messages. The administrator can select system log events and SMTP events. In addition, per port log and SMTP events can be selected too.

System event selection	This feature allows the administrator to select events that will trigger the system to issue logs. Check the box to select the events. There are four events available to pre-define: **Device cold start**: when the device has a cold start action, the system will issue a log event. **Device warm start**: when the device has a warm start action, the system will issue a log event. **Authentication Failure**: when the SNMP authentication fails, the system will issue a log event. **X-Ring topology change**: when the Redundant-Ring topology changes, the system will issue a log event.
Port event selection	This feature allows the administrator to select per port events and per port SMTP events. There are 3 events available to pre-define: **Link Up**: the system will issue a log message when port connection is up. **Link Down**: the system will issue a log message when port connection is down. **Link Up & Link Down**: the system will issue a log message when port connection is up or down. **Disable**: it means no event is selected.



System event selection

Event Type	Syslog	SMTP
Device cold start	☑	□
Device warm start	☑	☑
Authentication Failure	☑	□
X-Ring topology change	□	☑

Port event selection

Port	Syslog	SMTP
Port.01	Link Up & Link Down	Disable
Port.02	Disable	Link Up & Link Down
Port.03	Disable	Disable
Port.04		Disable
Port.05		Disable
Port.06	Disable	Disable
Port.07	Disable	Disable
Port.08	Disable	Disable
Port.09	Disable	Disable
Port.10	Disable	Disable

After finishing necessary configurations, click on **Apply** to save the settings.

4-6.8 SNTP Configuration

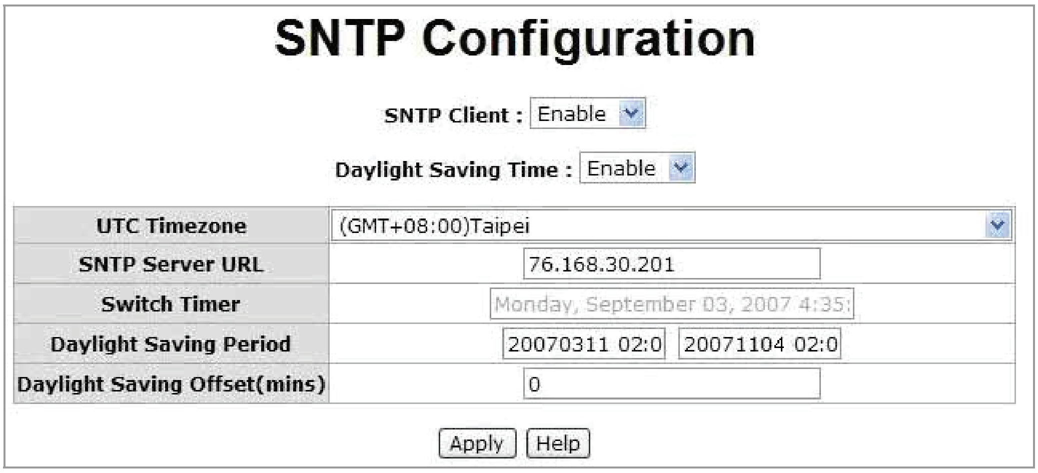
This feature allows the administrator to configure the SNTP (Simple Network Time Protocol) settings. The SNTP enables users to synchronize the switch clock in the Internet.

SNTP Client	This feature is to enable or disable SNTP function to acquire the time from the SNTP server.
Daylight Saving Time	This feature is to enable or disable daylight saving time function. When daylight saving time function is enabled, it is required to configure the daylight saving time period.
UTC Timezone	This feature is to set the switch location time zone. The following table lists the different location time zones for reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC	Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11 am	CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
Oscar Time Zone	-2 hours	10 am	EET - Eastern European, USSR Zone 1	+2 hours	2 pm
ADT - Atlantic Daylight	-3 hours	9 am	BT - Baghdad, USSR Zone 2	+3 hours	3 pm
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am	ZP4 - USSR Zone 3	+4 hours	4 pm
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am	ZP5 - USSR Zone 4	+5 hours	5 pm
CST - Central Standard	-6 hours	6 am	ZP6 - USSR Zone 5	+6 hours	6 pm

MDT - Mountain Daylight					
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am	WAST - West Australian Standard	+7 hours	7 pm
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am	CCT - China Coast, USSR Zone 7	+8 hours	8 pm
ALA - Alaskan Standard	-9 hours	3 am	JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
HAW - Hawaiian Standard	-10 hours	2 am	EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
Nome, Alaska	-11 hours	1 am	IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

SNTP Sever URL	This feature is to define the SNTP server IP address.
Daylight Saving Period	This feature is to set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different every year.
Daylight Saving Offset (mins)	This feature is to set up the offset time.
Switch Timer	This feature displays the switch current time.



SNTP Configuration

SNTP Client : Enable

Daylight Saving Time : Enable

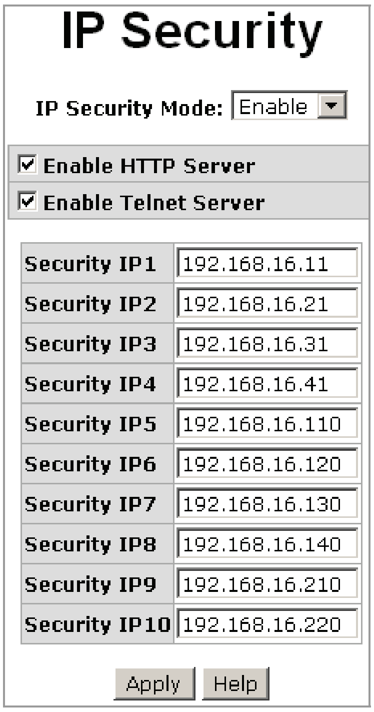
UTC Timezone	(GMT+08:00)Taipei
SNTP Server URL	76.168.30.201
Switch Timer	Monday, September 03, 2007 4:35:
Daylight Saving Period	20070311 02:0 20071104 02:0
Daylight Saving Offset(mins)	0

After finishing necessary configurations, click on **Apply** to save the settings.

4-6.9 IP Security

IP security function allows the administrator to grant 10 specific IP addresses the access to the switches through a web browser.

IP Security Mode	When this option is enabled, the **Enable HTTP Server** and **Enable Telnet Server** check boxes will then be available.
Enable HTTP Server	When this option is checked, the IP addresses among Security IP1- IP10 will be allowed to access via HTTP service.
Enable Telnet Server	When this option is checked, the IP addresses among Security IP1-IP10 will be allowed to access via telnet service.
Security IP 1-10	This feature allows the administrator to assign up to 10 specific IP addresses. Only these 10 IP addresses can access and manage the switch through a Web browser.



IP Security

IP Security Mode: Enable

☑ Enable HTTP Server

☑ Enable Telnet Server

Security IP1	192.168.16.11
Security IP2	192.168.16.21
Security IP3	192.168.16.31
Security IP4	192.168.16.41
Security IP5	192.168.16.110
Security IP6	192.168.16.120
Security IP7	192.168.16.130
Security IP8	192.168.16.140
Security IP9	192.168.16.210
Security IP10	192.168.16.220

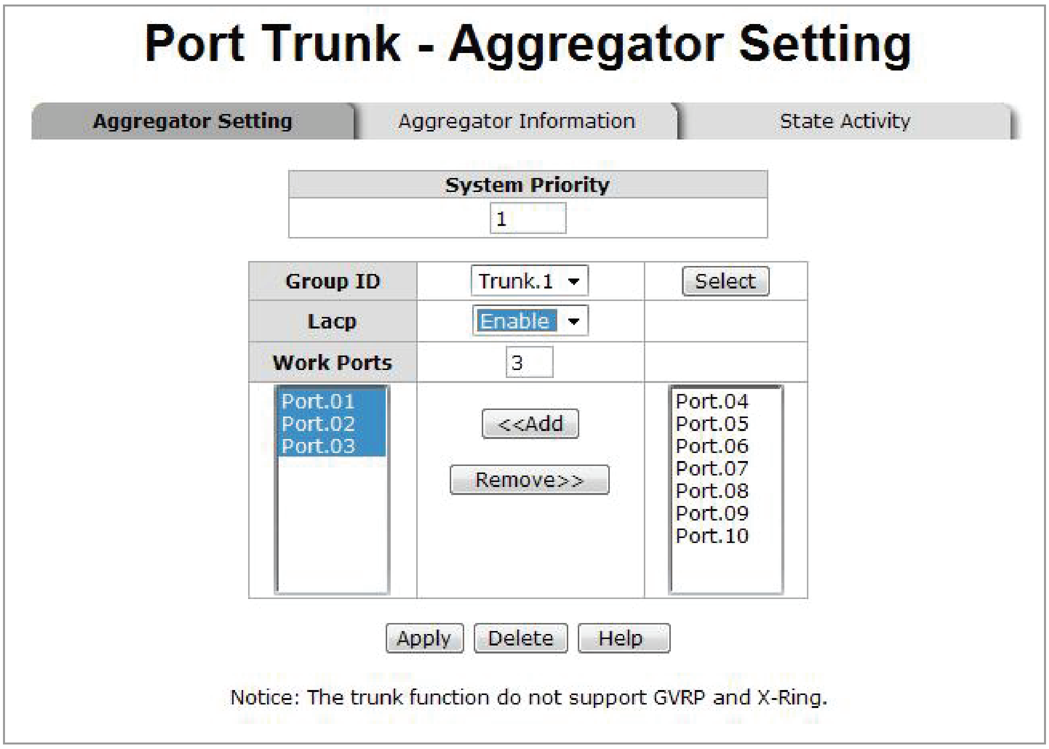
After finishing necessary configurations, click on **Apply** to save the settings.

4-6.10 Port Trunking

Port trunking is the combination of several ports or network cables to expand the connection speed beyond the limits of any one single port or network cable. Link Aggregation Control Protocol (LACP), which is a protocol running on layer 2, provides a standardized means in accordance with IEEE 802.3ad to bundle several physical ports together to form a single logical channel. All the ports within the logical channel or so-called logical aggregator work at the same connection speed and LACP operation requires full-duplex mode.

4-6.10.1 Aggregator Settings

System Priority	This value is used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP peer of the trunk group.
Group ID	There are 4 trunk groups available for configuration. The administrator can assign the **Group ID** to the trunk group.
LACP	When enabled, the trunk group is using LACP. A port which joins an LACP trunk group has to make an agreement with its member ports first. Please notice that a trunk group, including member ports distributed between two switches, has to enable the LACP function of the two switches. When disabled, the trunk group is a static trunk group. The advantage of having the LACP disabled is that a port joins the trunk group without any handshaking with its member ports; but member ports won't know that they should be aggregated together to form a logic trunk group.
Work Ports	This column field allows the administrator to type in the total number of active ports up to four. With LACP trunk group, e.g. you assign four ports to be the members of a trunk group whose work ports column field is set as two; the exceed ports are standby/redundant ports and can be aggregated if working ports fail. If it is a static trunk group (non-LACP), the number of work ports must equal the total number of group member ports.



Port Trunk - Aggregator Setting

System Priority: 1

Group ID: Trunk.1

Lacp: Enable

Work Ports: 3

Port.01
Port.02
Port.03

Port.04
Port.05
Port.06
Port.07
Port.08
Port.09
Port.10

Notice: The trunk function do not support GVRP and X-Ring.

To add ports to a trunk group, select the wanted ports on the right hand side column, and click on **Add**.

To remove ports from a trunk group, selection the wanted ports on the left hand side column, and click on **Remove**.

After finishing necessary configurations, click on **Apply** to save the settings.

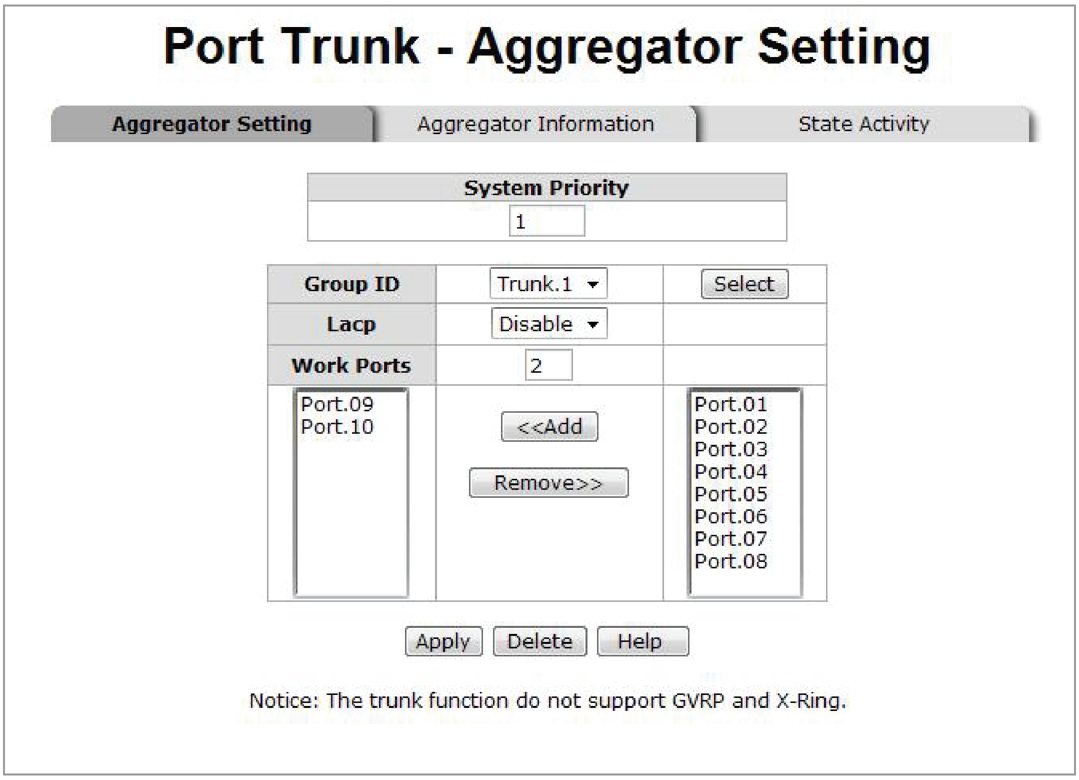
4-6.10.2 Aggregator Information

The settings in this feature will be different depending on whether LACP is enabled or disabled.

LACP Disabled

When LACP function is disabled in **Aggregator Setting**, the administrator will see the local static trunk group information here.

Group Key	This is a read-only column field that displays the trunk group ID.
Port Member	This is a read-only column field that displays the members of this static trunk group.

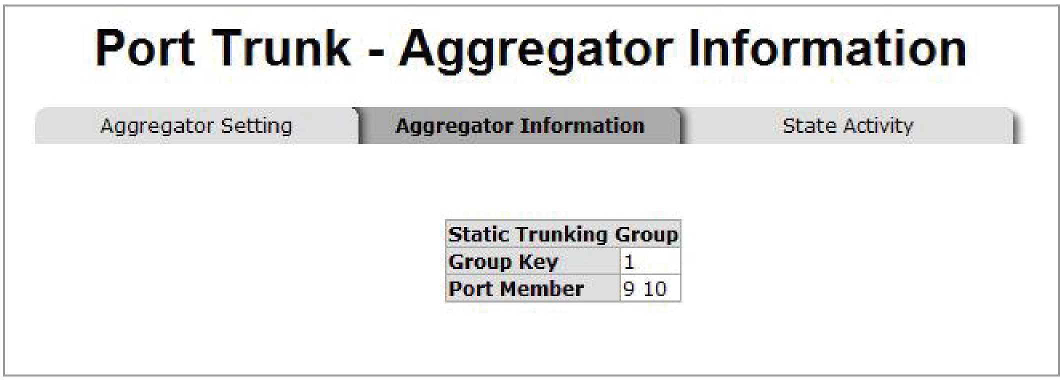


Port Trunk - Aggregator Setting

System Priority
1

Group ID	Trunk.1	Select
Lacp	Disable	
Work Ports	2	
Port.09 Port.10	<<Add Remove>>	Port.01 Port.02 Port.03 Port.04 Port.05 Port.06 Port.07 Port.08

Notice: The trunk function do not support GVRP and X-Ring.

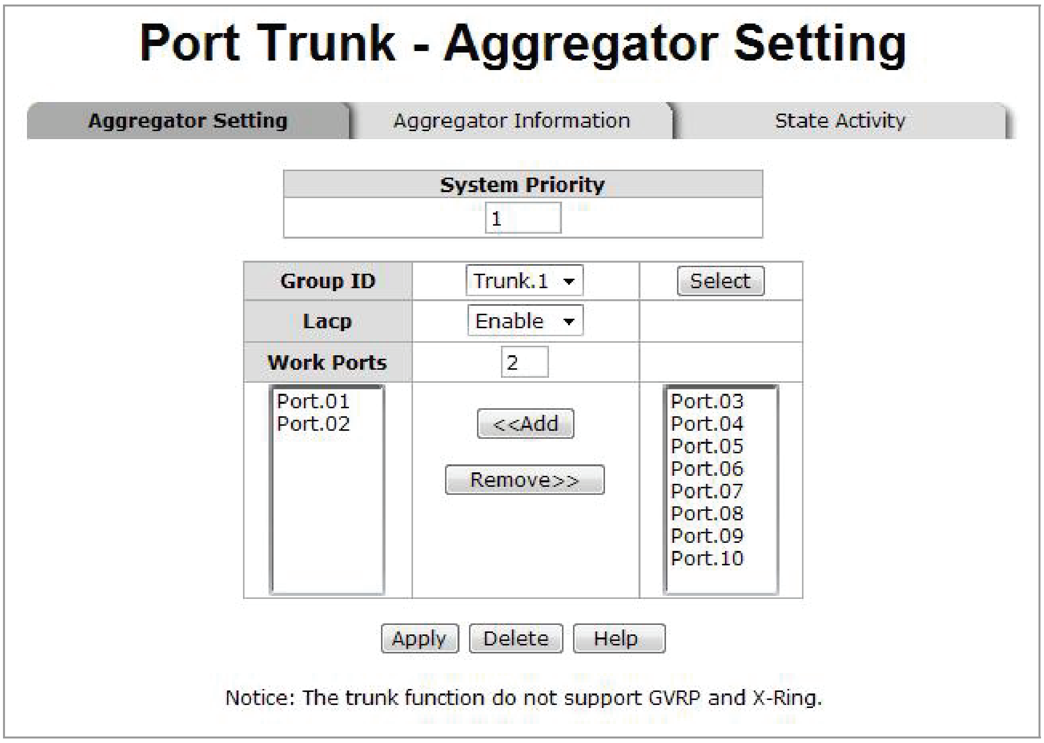


Port Trunk - Aggregator Information

Static Trunking Group	
Group Key	1
Port Member	9 10

LACP Enabled

When LACP function is enabled in **Aggregator Setting**, the administrator will see the trunk group information here.



Port Trunk - Aggregator Setting

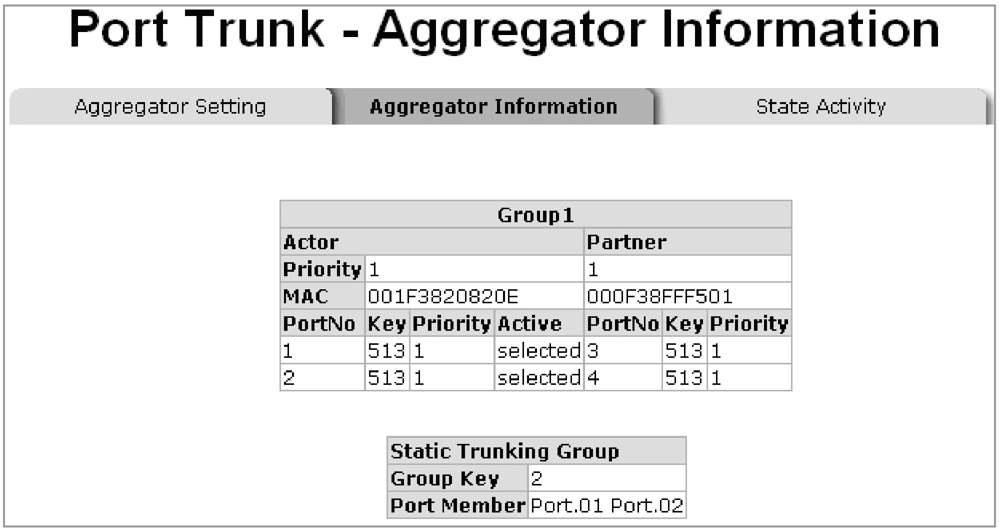
System Priority: 1

Group ID	Trunk.1
Lacp	Enable
Work Ports	2

Port.01
Port.02

Port.03
Port.04
Port.05
Port.06
Port.07
Port.08
Port.09
Port.10

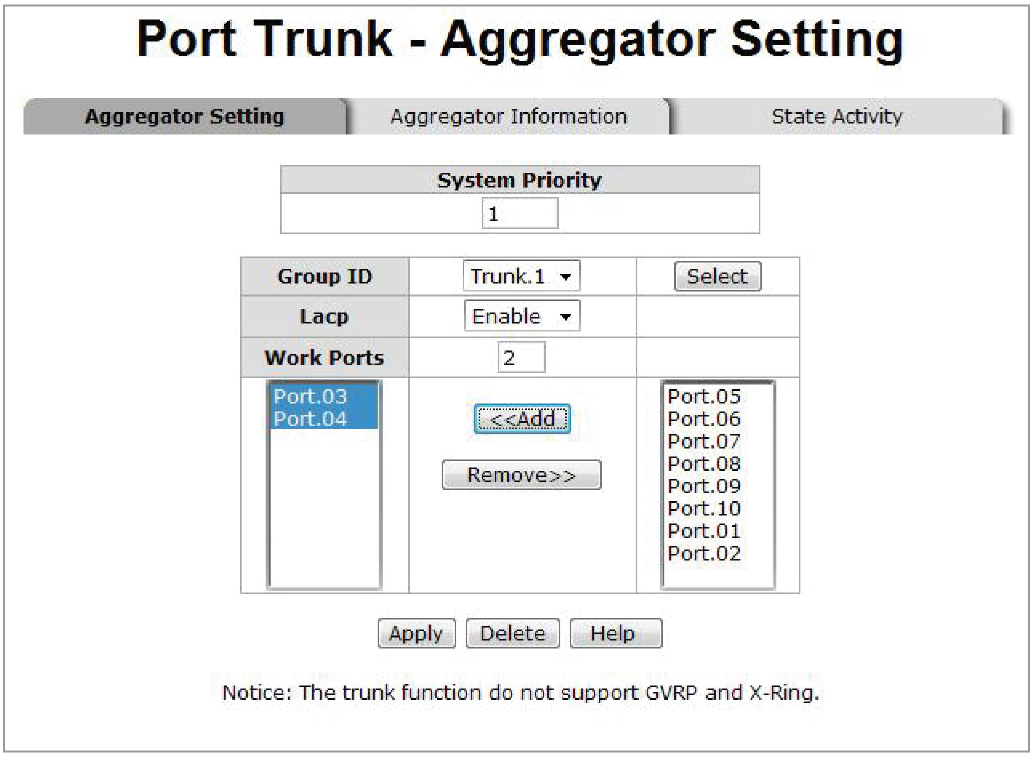
Notice: The trunk function do not support GVRP and X-Ring.



Port Trunk - Aggregator Information

Group1						
Actor				Partner		
Priority	1			1		
MAC	001F3820820E			000F38FFF501		
PortNo	Key	Priority	Active	PortNo	Key	Priority
1	513	1	selected	3	513	1
2	513	1	selected	4	513	1

Static Trunking Group	
Group Key	2
Port Member	Port.01 Port.02

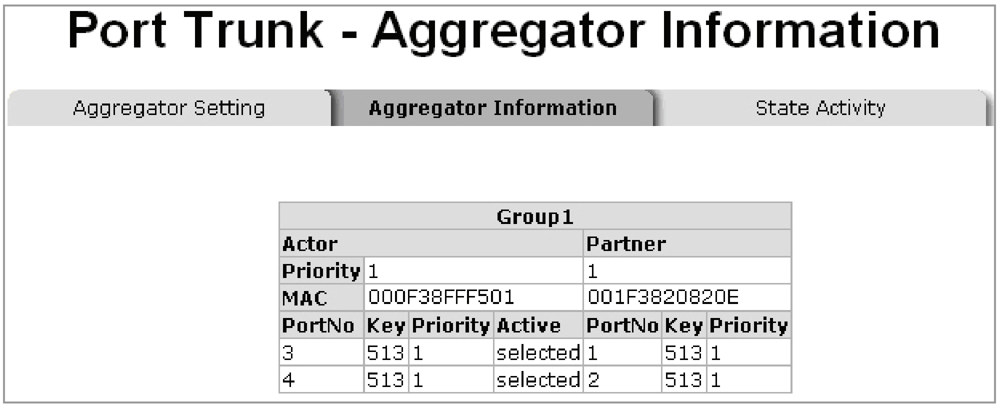


Port Trunk - Aggregator Setting

System Priority
1

Group ID	Trunk.1	Select
Lacp	Enable	
Work Ports	2	
Port.03 Port.04	<<Add Remove>>	Port.05 Port.06 Port.07 Port.08 Port.09 Port.10 Port.01 Port.02

Notice: The trunk function do not support GVRP and X-Ring.



Port Trunk - Aggregator Information

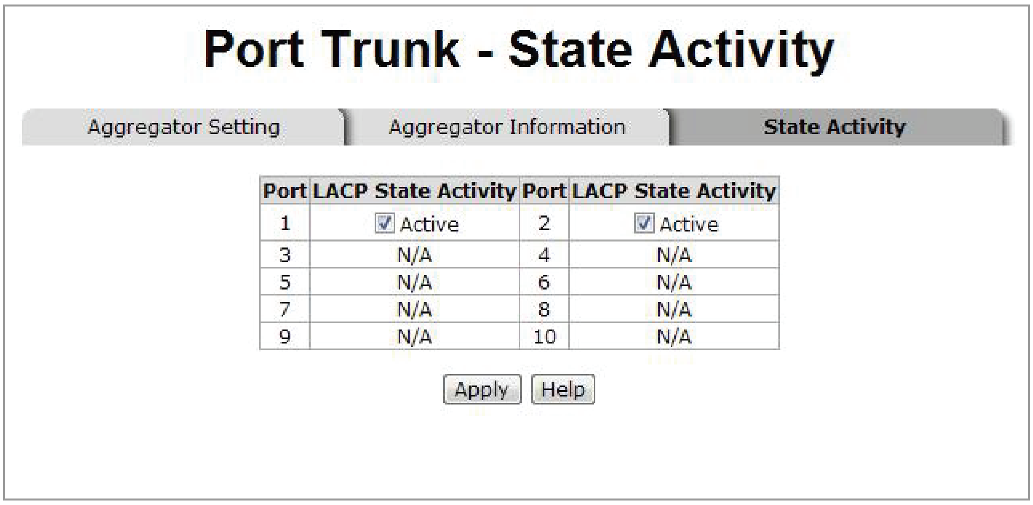
Group1						
Actor				Partner		
Priority	1			1		
MAC	000F38FFF501			001F3820820E		
PortNo	Key	Priority	Active	PortNo	Key	Priority
3	513	1	selected	1	513	1
4	513	1	selected	2	513	1

4-6.10.3 State Activity

When LACP is enabled, the State Activity feature will be available for configuration. The administrator can mark or unmark the check boxes next to the trunk group member ports to make the port state activity to be active or passive.

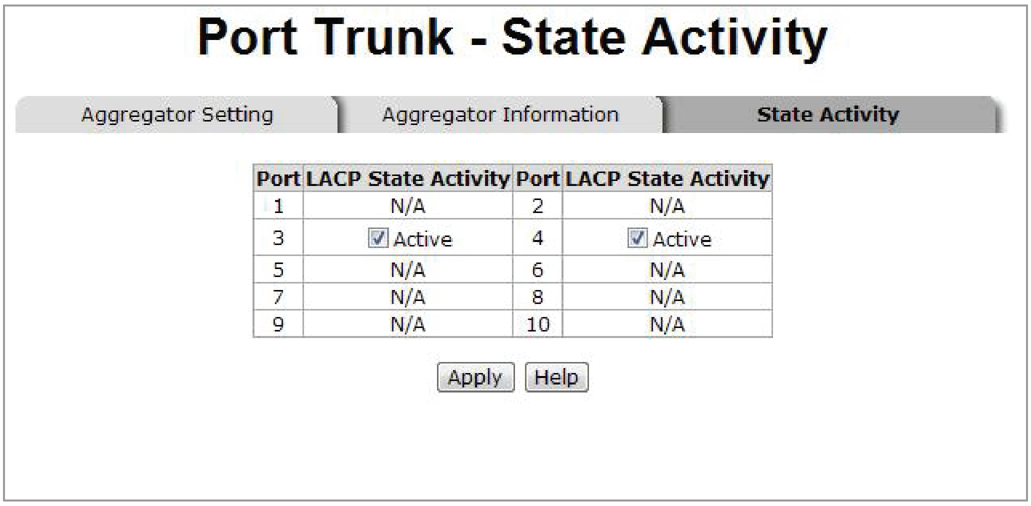
Active	The port automatically sends LACP protocol packets.
Passive	The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

A link having two passive LACP nodes will not perform dynamic LACP trunk since both ports are waiting for an LACP protocol packet from the opposite device.



Port Trunk - State Activity

Port	LACP State Activity	Port	LACP State Activity
1	☑ Active	2	☑ Active
3	N/A	4	N/A
5	N/A	6	N/A
7	N/A	8	N/A
9	N/A	10	N/A



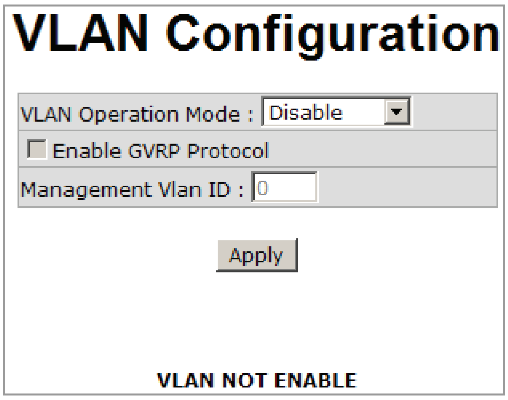
Port Trunk - State Activity

Port	LACP State Activity	Port	LACP State Activity
1	N/A	2	N/A
3	☑ Active	4	☑ Active
5	N/A	6	N/A
7	N/A	8	N/A
9	N/A	10	N/A

4-6.11 VLAN Configuration

A Virtual LAN (VLAN) is a logic networking group consisting of hosts with a common set of requirements that communicate as if they were attached to the broadcast domain, regardless of their physical location. VLAN allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be realized through software instead of physically relocating devices.

CME-822(E) supports both port-based VLAN and IEEE 802.1Q (Tag-based) VLAN. CME-822(E) VLAN operation mode if **Disable** by default.



VLAN Configuration

VLAN Operation Mode : Disable

□ Enable GVRP Protocol

Management Vlan ID : 0

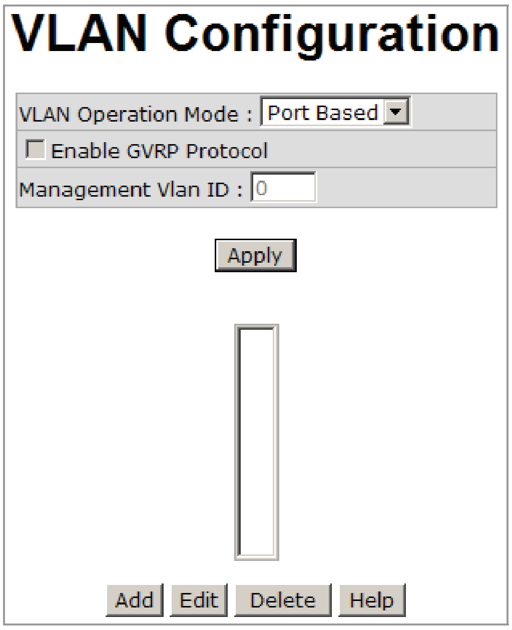
VLAN NOT ENABLE

4-6.11.1 Port-based VLAN

A port-based VLAN is formed by a group of switch ports which are not necessary located on the same switch. A four-byte field in the header is used to identify the VLAN. Packets can go among only members of the same VLAN group. All unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging will be ignored.

In order for an end station to send packets to different VLAN groups, it has to be either capable of tagging packets it sends with VLAN tags, or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.

Add	To add a new VLAN group.
Edit	To modify a certain VLAN's settings.
Delete	To delete a VLAN group.
Next Page	To view another VLAN group settings.
Group Name	To enter the name for this VLAN group.

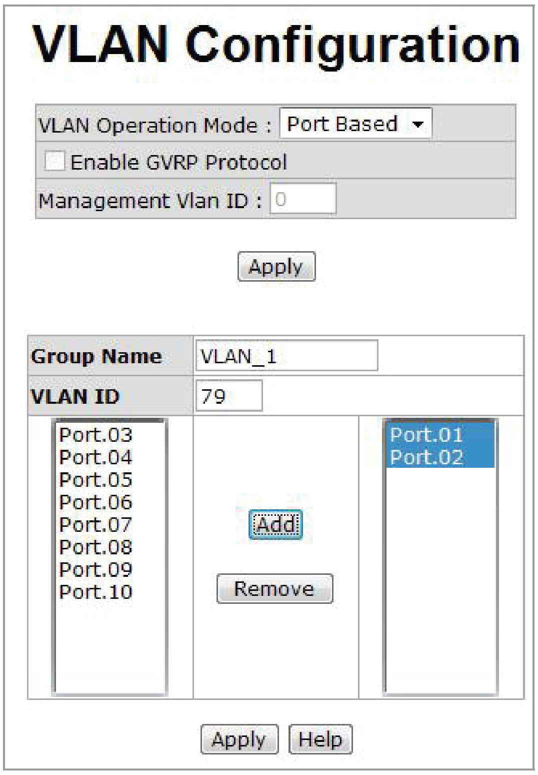


VLAN Configuration

VLAN Operation Mode : Port Based

□ Enable GVRP Protocol

Management Vlan ID : 0



VLAN Configuration

VLAN Operation Mode : Port Based

□ Enable GVRP Protocol

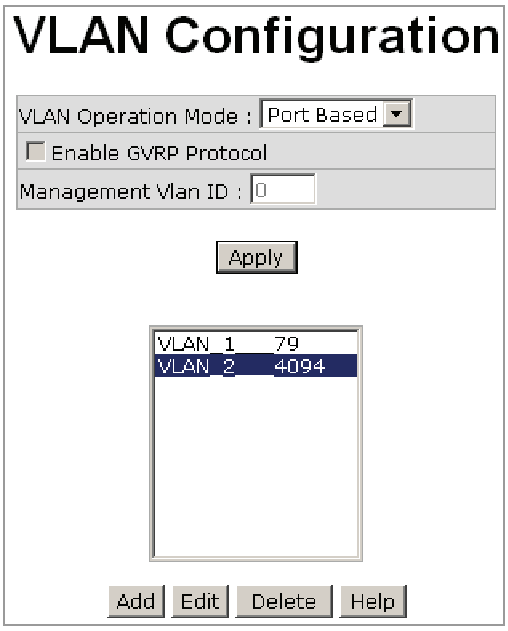
Management Vlan ID : 0

Group Name: VLAN_1

VLAN ID: 79

Port.03
Port.04
Port.05
Port.06
Port.07
Port.08
Port.09
Port.10

Port.01
Port.02



VLAN Configuration

VLAN Operation Mode : Port Based

□ Enable GVRP Protocol

Management Vlan ID : 0

After finishing necessary configurations, click on **Apply** to save the settings.

4-6.11.2 IEEE 802.1Q Tag-based VLAN

Tag-based VLAN is an IEEE 802.1Q standard which allows to create a VLAN across devices from different switch venders. IEEE 802.1Q VLAN uses a technique to insert a “tag” into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

All ports on the switch belong to default VLAN, VID is 1. The default VLAN can’t be deleted. The maximum VLAN group is up to 256.

Virtual Local Area Network (VLAN) can be implemented on the switch to logically create different broadcast domain.

When the 802.1Q VLAN function is enabled, all ports on the switch belong to default VLAN of VID 1, which means they logically are considered as members of the same broadcast domain. The valid VLAN ID number ranges from 1 to 4094. The amount of VLAN groups is up to 256 including default VLAN that cannot be deleted.

Each member port of an 802.1Q VLAN group is on either an Access Link (non VLAN-tagged) or a Trunk Link (VLAN-tagged). All frames on an Access Link carry no VLAN identification, while all frames on a Trunk Link are VLAN-tagged. In addition to above-mentioned 2 types, there is the third mode—Hybrid. A Hybrid Link can carry both VLAN-tagged frames and untagged frames. A single port is supposed to belong to one VLAN group, except it is on a Trunk/Hybrid Link.

The technique of 802.1Q tagging inserts a 4-byte tag, including VLAN ID of the destination port—PVID, in the frame. With the combination of Access/Trunk/Hybrid Links, the communication across switches also can make the packet sent through tagged and untagged ports.

4-6.11.2.1 802.1Q Configuration

VLAN Operation Mode	Select 802.1Q from the drop down list to configure Tag-based VLAN settings.
Management VLAN ID	Only when the VLAN members, whose Untagged VID (PVID) equals to the value in this column, will have the permission to access the switch. The default value is **0**, meaning this limit is not enabled (all members in different VLANs can access this switch).
Enable GVRP	GVRP (GARP VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration

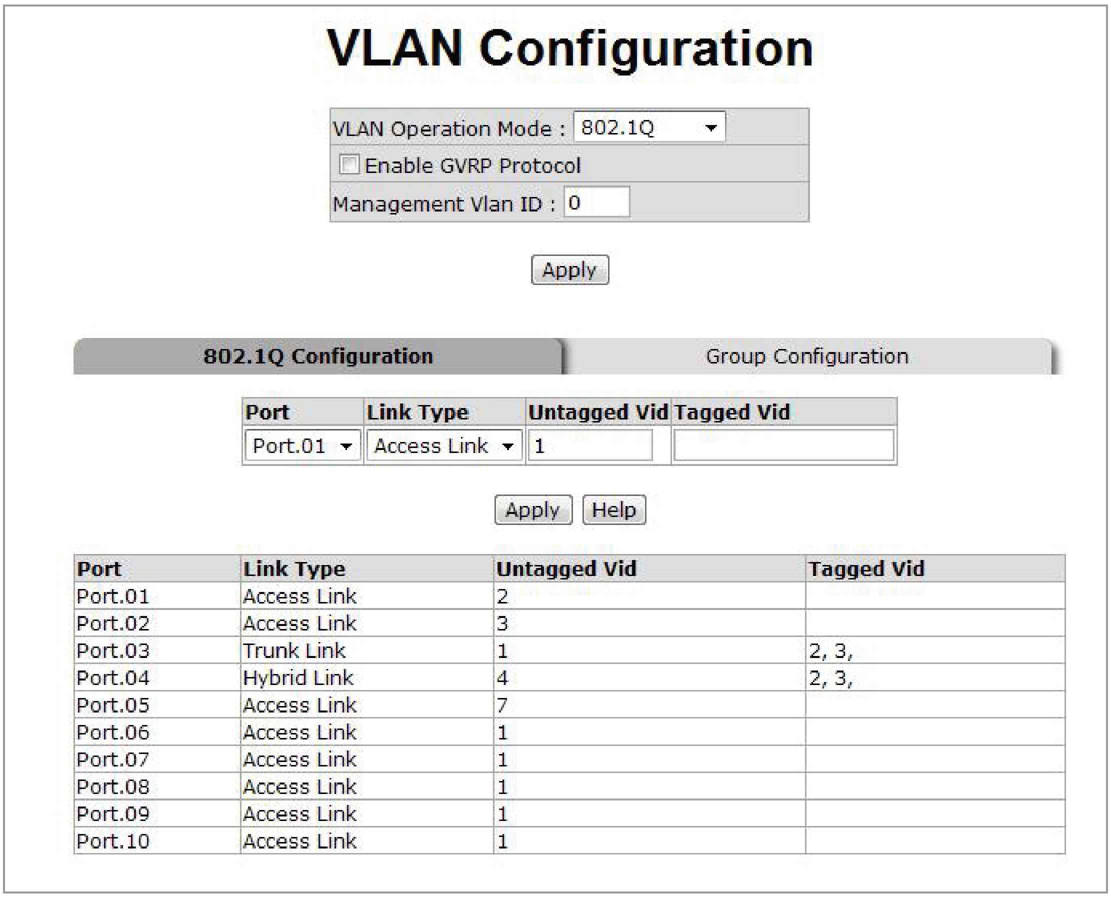
	information with other devices. For example, with GVRP function enabled on two switches, the switches are able to automatically exchange the information of their VLAN database. Therefore, the administrator doesn’t need to manually configure whether the link is trunk or hybrid, the packets belonging to the same VLAN can communicate across switches. Mark this checkbox to enable GVRP protocol. This checkbox is available while the VLAN Operation Mode is in 802.1Q mode.
Port	To select the port you want to configure
Link Type	This feature allows the administrator to decide a certain port to be an Access Link, a Trunk Link, or a Hybrid Link. ➢ Access Link: A segment which provides the link path for one or more stations to the VLAN-aware device. An Access Port (untagged port), connected to the access link, has an untagged VID (also called PVID). After an untagged frame gets into the access port, the switch will insert a four-byte tag in the frame. The contents of the last 12-bit of the tag is untagged VID. When this frame is sent out through any of the access port of the same PVID, the switch will remove the tag from the frame to recover it to what it was. Those ports of the same untagged VID are considered as the same VLAN group members. ➢ Trunk Link: A segment which provides the link path for one or more VLAN-aware devices (switches). A Trunk Port, connected to the trunk link, has an understanding of tagged frame, which is used for the communication among VLANs across switches. Which frames of the specified VIDs will be forwarded depend on the values filled in the Tagged VID column field. Please insert a comma between two VIDs. ➢ Hybrid Link: A segment which consists of Access and Trunk links. The hybrid port has both the features of access and trunk ports. A hybrid port has a PVID belonging to a particular VLAN, and it also forwards the specified tagged-frames for the purpose of VLAN communication across switches.
Untagged VID	This column field is available when Link Type is set as Access Link or Hybrid Link. Assign a number ranging from 1 to 4094.
Tagged VID	This column field is available when Link Type is set as Trunk Link or Hybrid Link. Assign a number ranging from 1 to 4094.

After finishing necessary configurations, click on **Apply** to save the settings.

ℹ	Since the access port doesn’t have an understanding of tagged frames, the column field of Tagged VID will not be available when the port is configured as an Access Link.

ℹ	1. A trunk port doesn’t insert tag into an untagged frame, and therefore the untagged VID column field is not available when the port is configured as a Trunk Link. 2. It’s not necessary to type ‘1’ in the tagged VID. The trunk port will forward the frames of VLAN 1. 3. The trunk port has to be connected to a trunk/hybrid port of the other switch. Both the tagged VID of the two ports have to be the same.

ℹ	1. It’s not necessary to type ‘1’ in the tagged VID. The hybrid port will forward the frames of VLAN 1. 2. The hybrid port has to be connected to a trunk/hybrid port of the other switch. Both the tagged VID of the two ports have to be the same.



VLAN Configuration

VLAN Operation Mode : 802.1Q

□ Enable GVRP Protocol

Management Vlan ID : 0

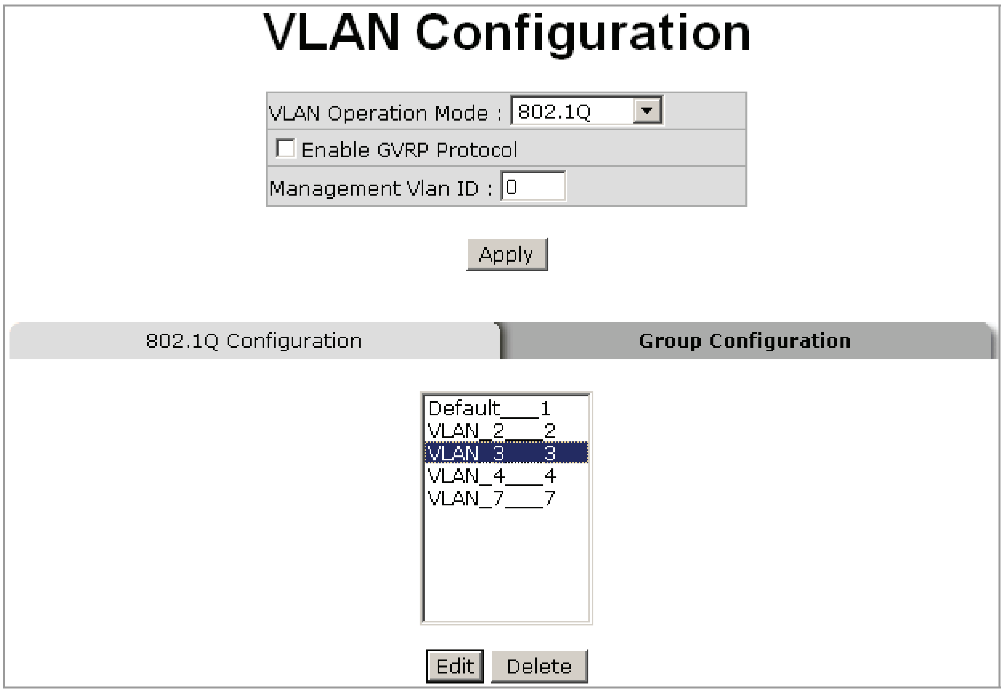
Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	2	
Port.02	Access Link	3	
Port.03	Trunk Link	1	2, 3,
Port.04	Hybrid Link	4	2, 3,
Port.05	Access Link	7	
Port.06	Access Link	1	
Port.07	Access Link	1	
Port.08	Access Link	1	
Port.09	Access Link	1	
Port.10	Access Link	1	

4-6.11.2.2 Group Configuration

This feature allows the administrator to edit the existing VLAN groups.

Select the VLAN group that you want to modify, and click on **Edit**. You can modify the VLAN Group Name, and VLAN ID.



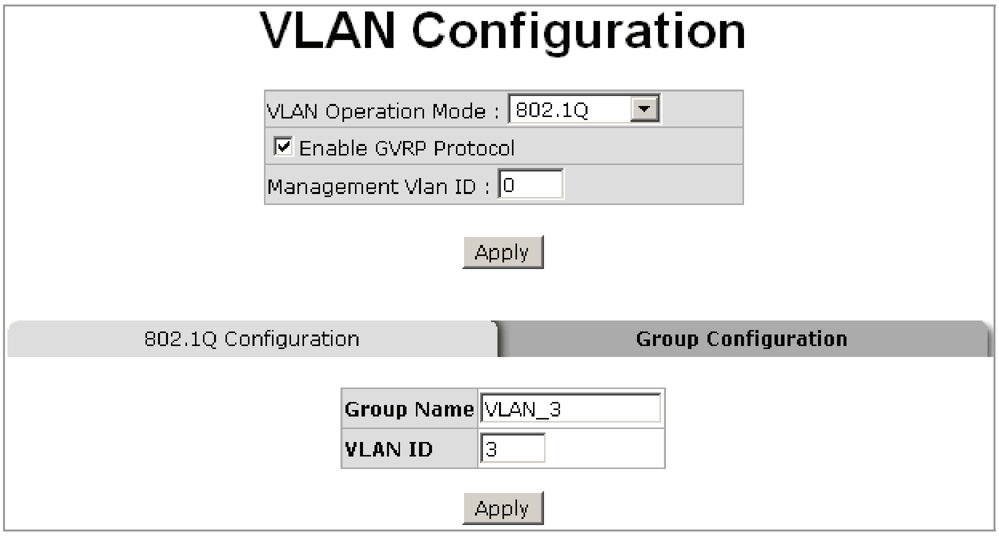
VLAN Configuration

VLAN Operation Mode : 802.1Q

□ Enable GVRP Protocol

Management Vlan ID : 0

Default___1
VLAN_2___2
VLAN_3___3
VLAN_4___4
VLAN_7___7



VLAN Configuration

VLAN Operation Mode : 802.1Q

☑ Enable GVRP Protocol

Management Vlan ID : 0

Group Name	VLAN_3
VLAN ID	3

After finishing necessary configurations, click on **Apply** to save the settings.

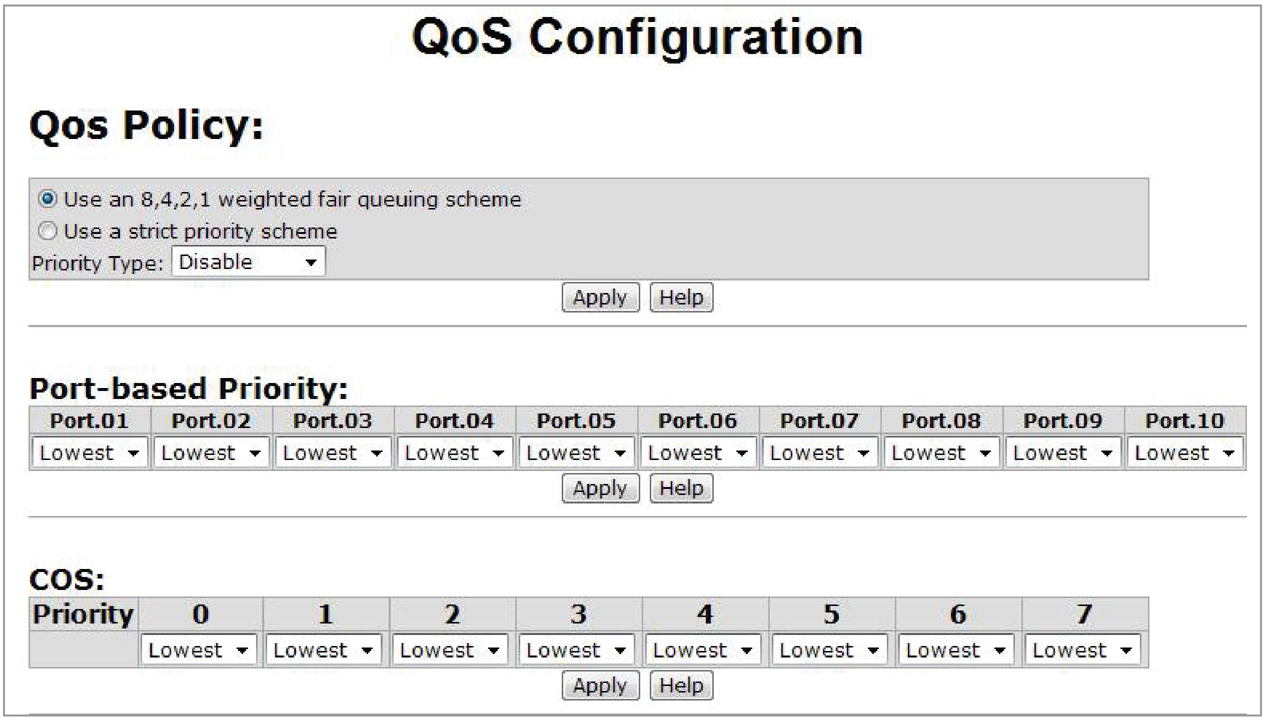
4-6.12 QoS Configuration

Quality of Service (QoS) helps prioritizing traffic. High priority packets will be transmitted or processed first, making sure your network reliability and stability.

QoS Policy	This feature allows the administrator to select QoS policy. **Use an 8, 4, 2, 1 weighted fair queuing scheme**: The switch will follow 8:4:2:1 proportion to process priority queue from the highest to the lowest. For example: the switch will process 8 highest priority packets first, and then 4 second highest priority packets, and then 2 low priority packets, and then the 1 lowest priority packets. **Use the strict priority scheme**: The switch will process the packets with the highest priority first. The switch won't continue to process the second highest priority packets until the highest priority ones have been all processed.
Priority Type	This feature allows the administrator to configure each port's priority type. There are 5 types available: ➢ Port-based: this port priority will follow the default port priority that administrator has configured: High, middle, low, or lowest ➢ COS only: this port priority will only follow the COS priority rules that administrator has configured. ➢ TOS only: this port priority will only follow the TOS priority rules that administrator has configured. ➢ COS first: this port priority will follow the COS priority rules that administrator has configured first, and then follow other priority rules. ➢ TOS first: this port priority will follow the TOS priority rules that administrator has configured first, and then follow other priority rules.
Port-based Priority	This feature allows the administrator to configure each port's default port priority. There 4 types of priority available: High, Middle, Low, Lowest.
COS Priority	This feature allows the administrator to configure the COS priority level 0 to 7.
TOS Priority	The switch provides 0 to 63 TOS priority levels. Each level has 4 types of priority – high, mid, low, and lowest. The default priority value is "Lowest" for each level. When an IP packet is received, the switch will check the TOS level value in the IP packet received. For example: the administrator

	set the TOS level 25 to be high. The port 1 is following the TOS priority policy only. When the packet received by port 1, the switch will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25 (priority = high), and then the packet priority will have the highest priority.

QoS and Rate Limiting function cannot be enabled at the same time.



QoS Configuration

Qos Policy:

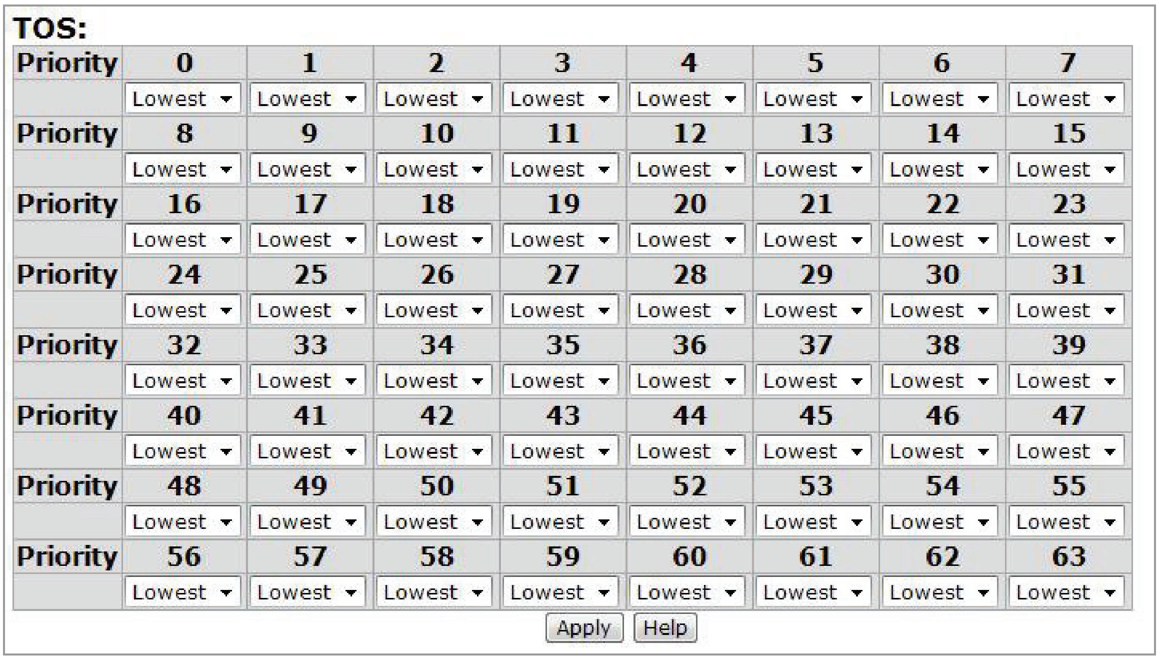
● Use an 8,4,2,1 weighted fair queuing scheme
○ Use a strict priority scheme
Priority Type: Disable

Port-based Priority:

Port.01	Port.02	Port.03	Port.04	Port.05	Port.06	Port.07	Port.08	Port.09	Port.10
Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

COS:

Priority	0	1	2	3	4	5	6	7
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest



TOS:

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

After finishing necessary configurations, click on **Apply** to save the settings.

4-6.13 IGMP Configuration

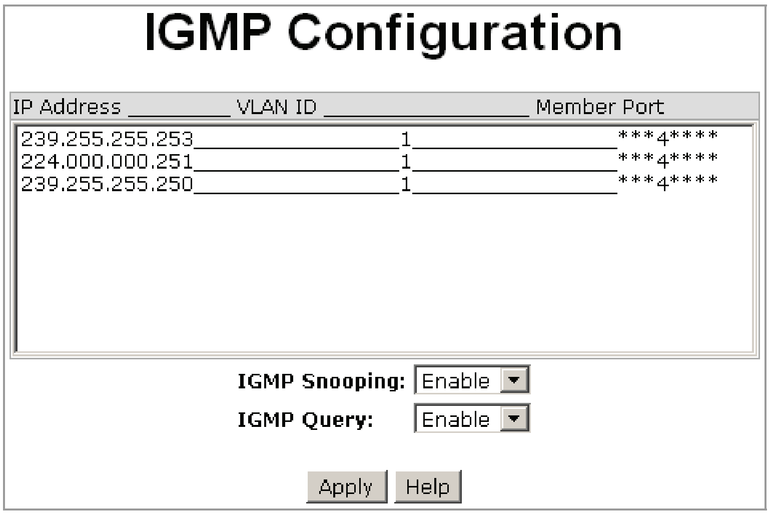
The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP). IGMP

Snooping mode allows the switch to forward multicast packets to appropriate ports. The switch will detect IGMP queries when multicast packets come in and then report back with packets indicating which port is willing to accept the multicast packets. With this function, network traffic can be limited without unwanted packets being sent to certain ports. IGMP has three fundamental types of messages as follows:

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

This feature allows the administrator to enable IGMP protocol and IGMP Query function. The administrator will see the IGMP snooping information in this section -- different multicast group VIDs and member ports, and IP multicast addresses range from 224.0.0.0 through 239.255.255.255.

After finishing necessary configurations, click on **Apply** to save the settings.



IGMP Configuration

```
IP Address _________ VLAN ID _________________ Member Port
239.255.255.253_________________1_________________***4****
224.000.000.251_________________1_________________***4****
239.255.255.250_________________1_________________***4****
```

IGMP Snooping: Enable

IGMP Query: Enable

4-6.14 SNMP Configuration

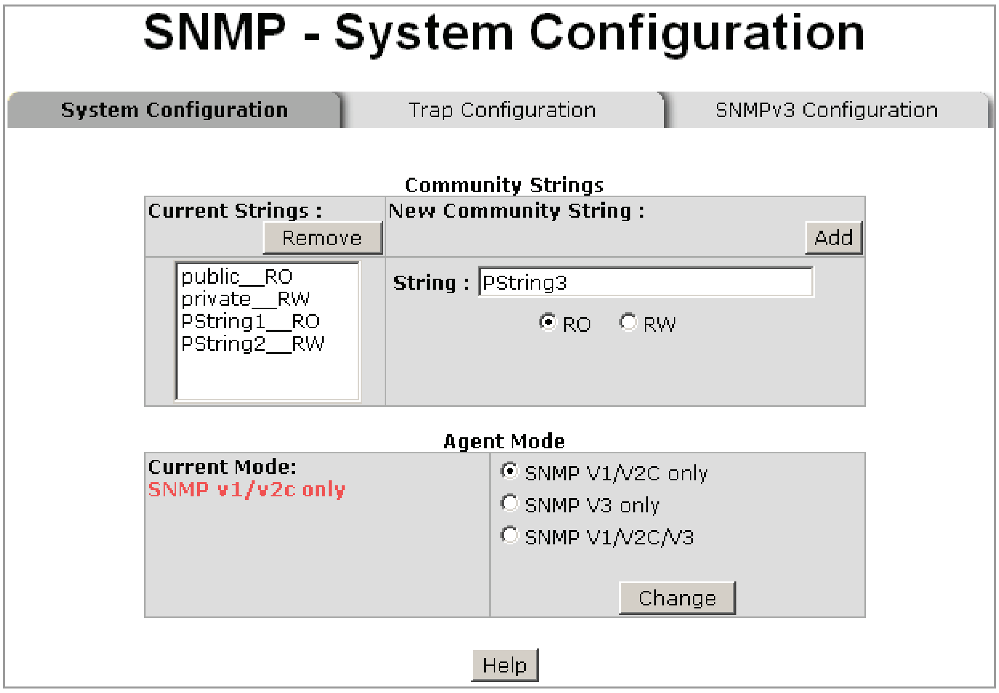
Simple Network Management Protocol (SNMP) is used to monitor exchange of information among devices in a network system. CME-822(E) supports SNMP v1/v2c/v3.

4-6.14.1 Community Strings

This function is to use community strings for authentication.

Strings	This feature allows the administrator to enter a name for the string.
RO	RO means Read Only. This feature allows the requests accompanied by this string to display MIB-object information.
RW	RW means Read & Write. This feature allows the requests accompanied by this string to display MIB-object information and to set MIB object.
Agent Mode	This feature allows the administrator to select the SNMP version for necessary configuration. Click on the version option required, and then click on **Change** to validate the settings.

After finishing necessary configurations, click on **Apply** to save the settings.



SNMP - System Configuration

Community Strings

Current Strings :

public__RO
private__RW
PString1__RO
PString2__RW

New Community String :

String : PString3

● RO ○ RW

Agent Mode

Current Mode:
SNMP v1/v2c only

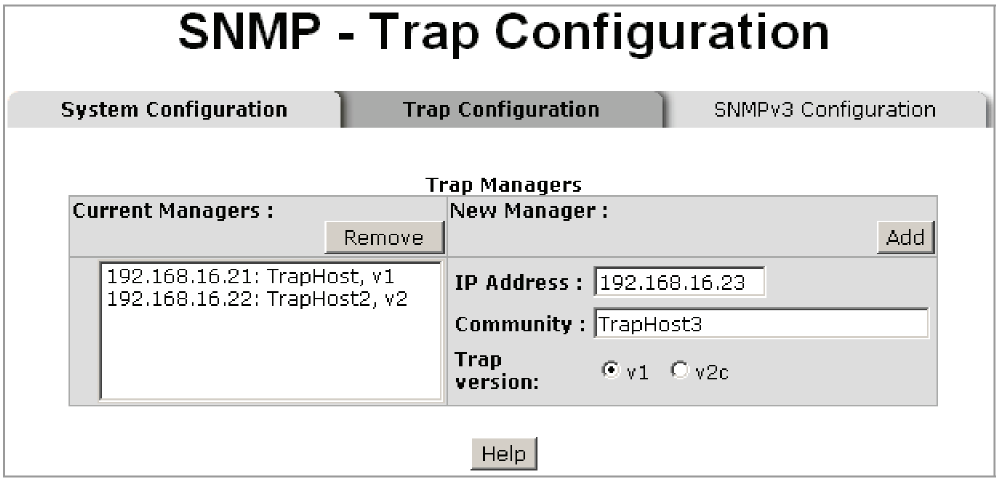
● SNMP V1/V2C only
○ SNMP V3 only
○ SNMP V1/V2C/V3

4-6.14.2 Trap Configuration

A trap manager is a management station that receives the trap messages generated by the switch. If no trap manager is defined, no traps will be issued. To define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version.

IP Address	This feature allows the administrator to enter the IP address of the trap manager.
Community	This feature allows the administrator to enter the community strings for trap stations.
Trap Version	This feature allows the administrator to select the SNMP version.

After finishing necessary configurations, click on **Apply** to save the settings.



SNMP - Trap Configuration

Trap Managers

Current Managers :

192.168.16.21: TrapHost, v1
192.168.16.22: TrapHost2, v2

New Manager :

IP Address : 192.168.16.23

Community : TrapHost3

Trap version: ● v1 ○ v2c

4-6.14.3 SNMP v3 Configuration

SNMPv3 primarily added security and remote configuration enhancements to SNMP, including:

- Message integrity to ensure that a packet has not been tampered with in transit.
- Authentication to verify that the message is from a valid source.
- Encryption of packets to prevent snooping by an unauthorized source.

Please follow the steps below to configure SNMP v3 settings.

Context Table

Context Name	This feature allows the administrator to enter a name for this context table.

After finishing necessary configurations, click on **Apply** to save the settings.

User Table

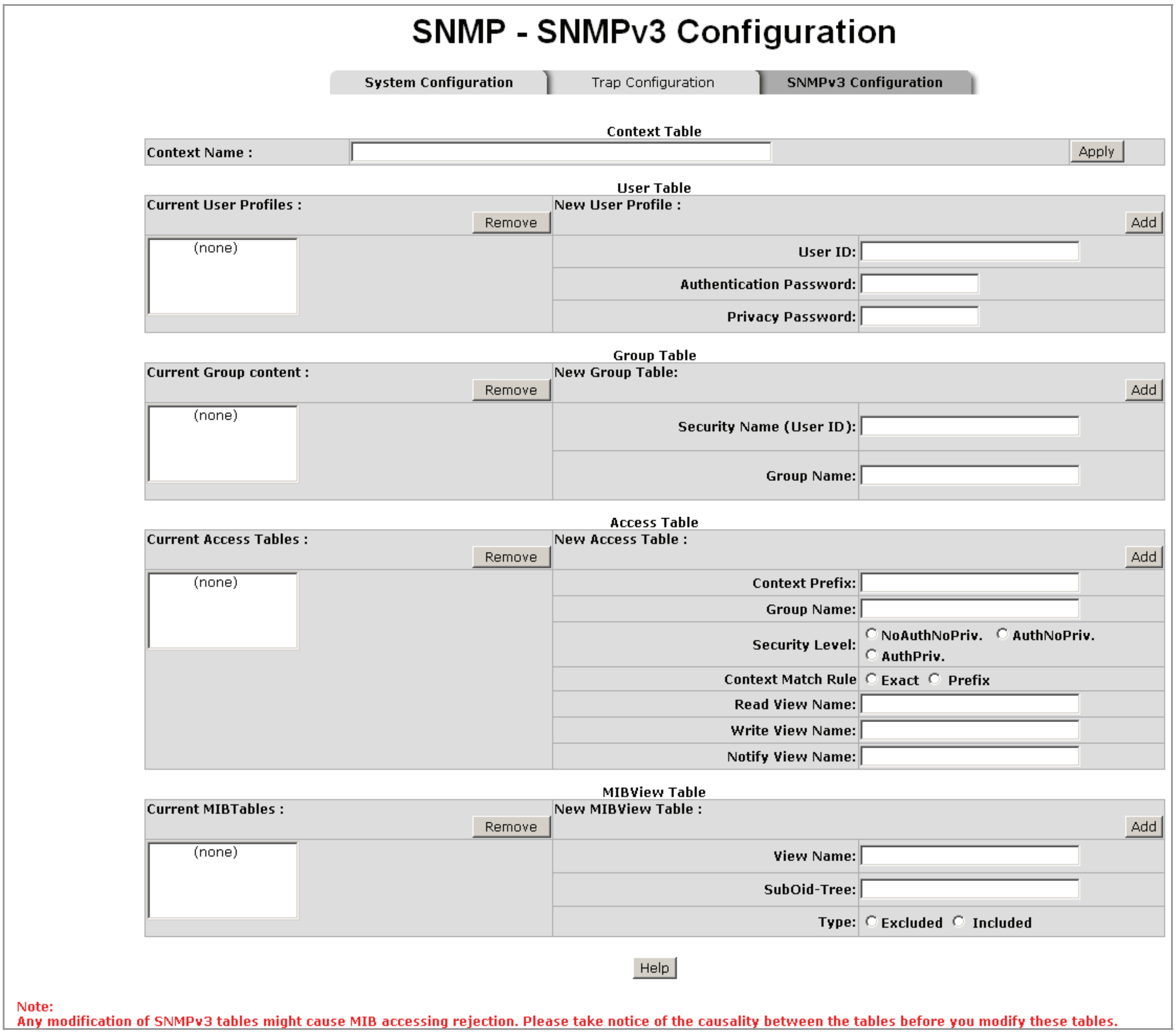
User ID	This feature allows the administrator to enter the user name.
Authentication Password	This feature allows the administrator to set up the authentication password.
Privacy Password	This feature allows the administrator to set up the privacy password.

After finishing necessary configurations, click on **Apply** to save the settings.

Group Table

Security Name (User ID)	This feature allows the administrator to assign the user name that was just set up in the **User Table**.
Group Name	This feature allows the administrator to set up the group name.

After finishing necessary configurations, click on **Apply** to save the settings.



SNMP - SNMPv3 Configuration

System Configuration | Trap Configuration | SNMPv3 Configuration

Context Table

Context Name : [ ] Apply

User Table

Current User Profiles : Remove
(none)

New User Profile : Add
User ID: [ ]
Authentication Password: [ ]
Privacy Password: [ ]

Group Table

Current Group content : Remove
(none)

New Group Table: Add
Security Name (User ID): [ ]
Group Name: [ ]

Access Table

Current Access Tables : Remove
(none)

New Access Table : Add
Context Prefix: [ ]
Group Name: [ ]
Security Level: ○ NoAuthNoPriv. ○ AuthNoPriv. ○ AuthPriv.
Context Match Rule ○ Exact ○ Prefix
Read View Name: [ ]
Write View Name: [ ]
Notify View Name: [ ]

MIBView Table

Current MIBTables : Remove
(none)

New MIBView Table : Add
View Name: [ ]
SubOid-Tree: [ ]
Type: ○ Excluded ○ Included

Help

Note:
Any modification of SNMPv3 tables might cause MIB accessing rejection. Please take notice of the causality between the tables before you modify these tables.

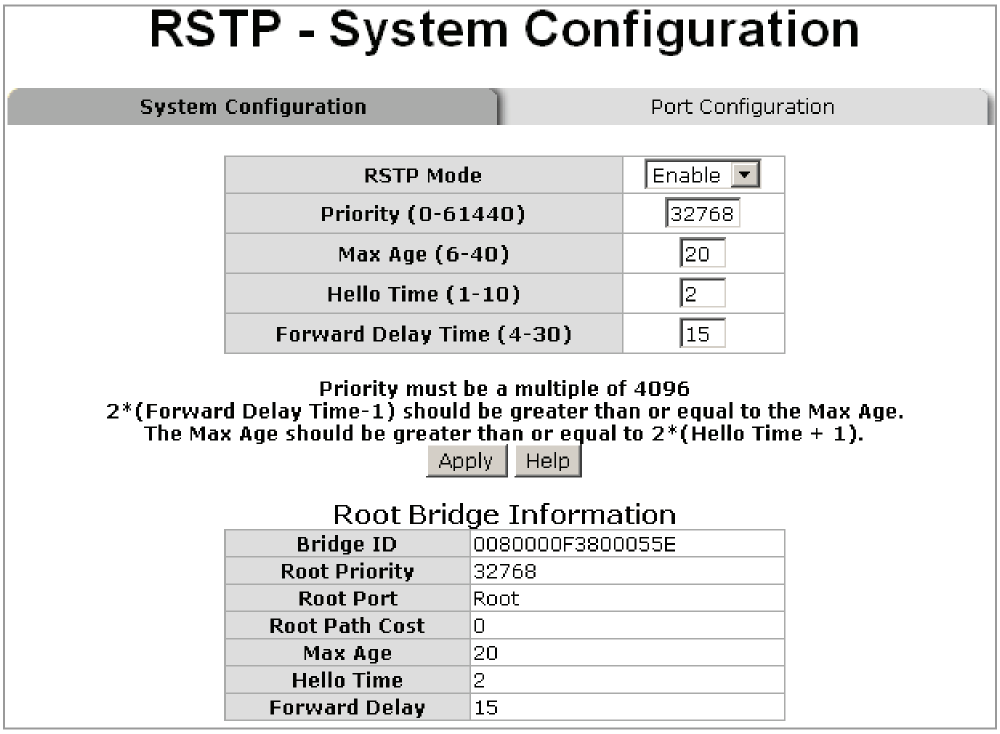
4-6.15 Rapid Spanning Tree Protocol

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. CME-822(E) also supports STP and will auto detect the connected device whether it is running STP or RSTP protocol.

4-6.15.1 System Configuration

The administrator can view the spanning tree information from the Root Bridge Information column.

RSTP Mode	This feature allows the administrator to enable or disable the RSTP function. The parameters will be available for configuration after the RSTP function is enabled.
Priority (0-61440)	This is the value used to identify the root bridge. The bridge with the lowest value has the highest priority and will be selected as the root. If this value has been changed, the switch must be rebooted for the new settings to be in effect. The value must be multiple of 4096 according to the protocol standard.
Max Age (6-40)	This value is the seconds a bridge waits for without receiving spanning tree messages before attempting to reconfigure. Enter a value between 6 and 40.
Hello Time (1-10)	This value is the time in seconds that controls when the switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 and 10.
Forward Delay Time (4-30)	This value is the time in seconds a port waits for before changing its Rapid Spanning Tree protocol learning and listening state to the forwarding state. Enter a value between 4 and 30.



RSTP - System Configuration

RSTP Mode	Enable
Priority (0-61440)	32768
Max Age (6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15

Priority must be a multiple of 4096
2*(Forward Delay Time-1) should be greater than or equal to the Max Age.
The Max Age should be greater than or equal to 2*(Hello Time + 1).

Root Bridge Information

Bridge ID	0080000F3800055E
Root Priority	32768
Root Port	Root
Root Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15

After finishing necessary configurations, click on **Apply** to save the settings.

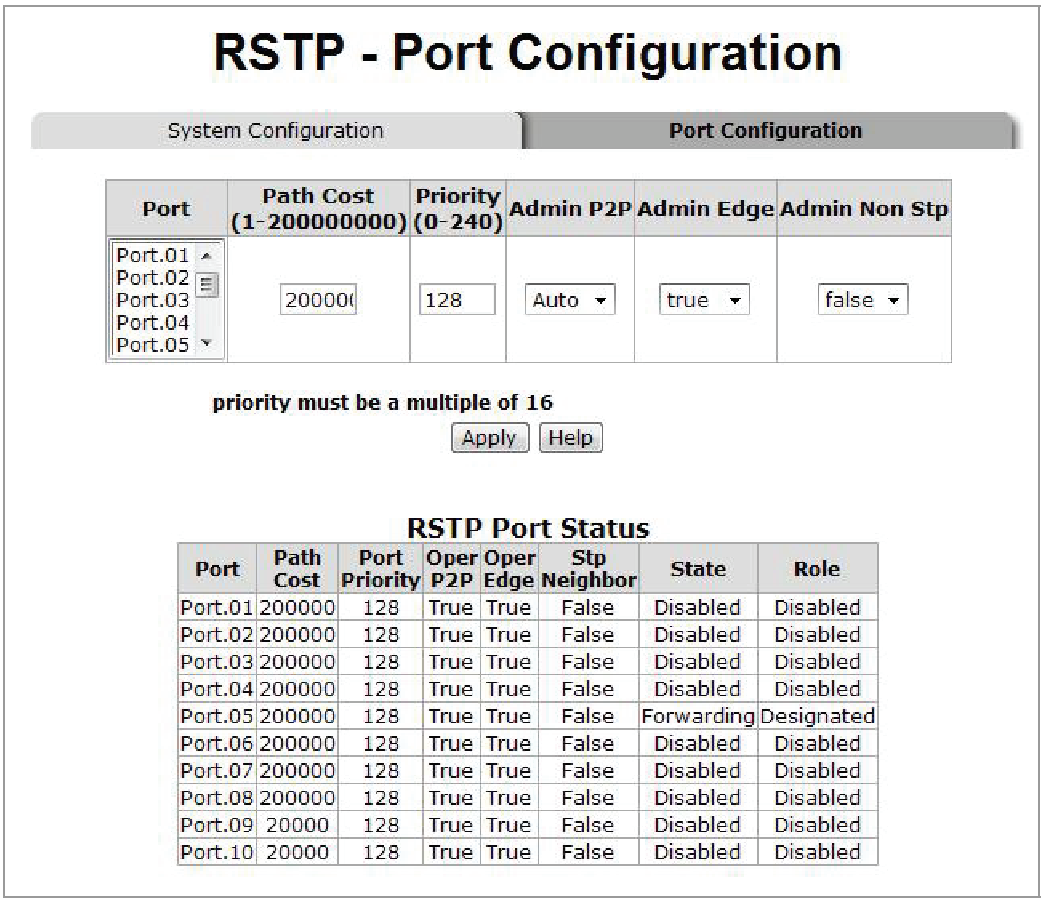
ℹ	The administrator must follow the rule to configure the MAX Age, Hello Time, and Forward Delay Time: 2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1).

4-6.15.2 Port Configuration

The administrator can use this interface to configure path cost and priority of every port.

Port	Select the port that you want to configure.
Path Cost	This feature allows the administrator to configure the cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number between 1 and 200000000.
Priority	This feature allows the administrator to configure which port should be blocked by priority in LAN. Enter a number between 0 and 240. The value of priority must be the multiple of 16.
Admin P2P	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. **True** is to enable P2P function. **False** is to disable P2P.
Admin Edge	The port directly connected to end stations cannot create bridging loop in the network. To configure the port as an edge port, set the port to **True**.
Admin Non Stp	The port includes the STP mathematic calculation. **True** is not including STP mathematic calculation. **False** is including the STP mathematic calculation.

After finishing necessary configurations, click on **Apply** to save the settings.



RSTP - Port Configuration

Port	Path Cost (1-200000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non Stp
Port.01 Port.02 Port.03 Port.04 Port.05	20000(	128	Auto	true	false

priority must be a multiple of 16

RSTP Port Status

Port	Path Cost	Port Priority	Oper P2P	Oper Edge	Stp Neighbor	State	Role
Port.01	200000	128	True	True	False	Disabled	Disabled
Port.02	200000	128	True	True	False	Disabled	Disabled
Port.03	200000	128	True	True	False	Disabled	Disabled
Port.04	200000	128	True	True	False	Disabled	Disabled
Port.05	200000	128	True	True	False	Forwarding	Designated
Port.06	200000	128	True	True	False	Disabled	Disabled
Port.07	200000	128	True	True	False	Disabled	Disabled
Port.08	200000	128	True	True	False	Disabled	Disabled
Port.09	20000	128	True	True	False	Disabled	Disabled
Port.10	20000	128	True	True	False	Disabled	Disabled

4-6.16 X-Ring Configuration

CME-822(E) provides redundant self-recovery mechanism named as X-Ring. When compared with the commercial standard redundant technologies like STP or RSTP, the X-Ring can effectively reduce the recovery time to less than 10ms. The Ring Topology must be applied to all the connected switches.

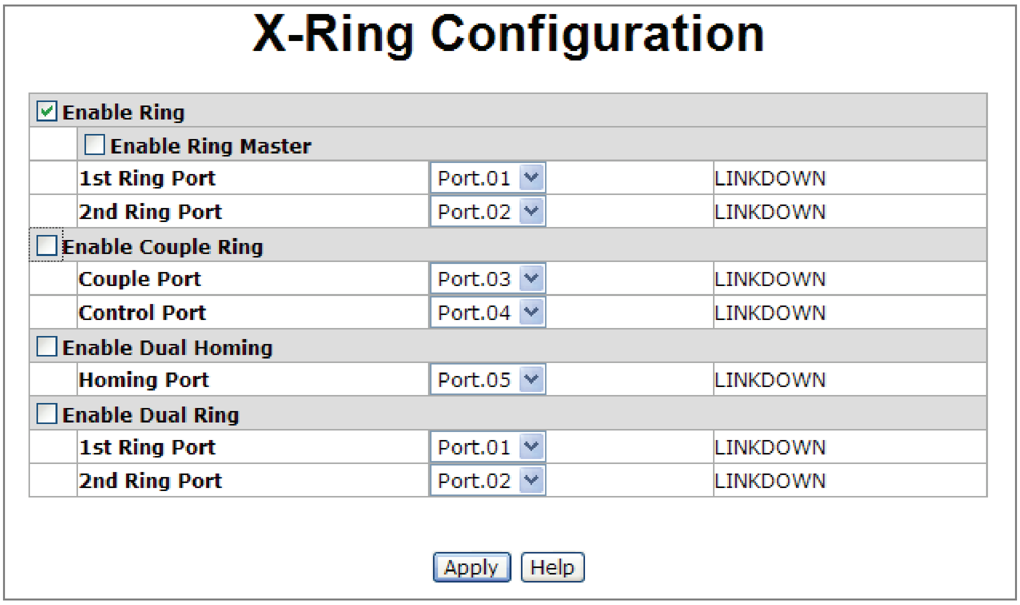
When all switches are connected in a ring topology with X-Ring function enabled, one of the switches will be appointed as "Ring Master." The ring master will monitor the ring's health to make sure the ring is working properly. Once a failure is detected by the ring master, the ring master will activate the blocked backup path within milliseconds to replace the faulty primary transmission path to make sure the ring will continue to work.

In the X-Ring topology, every switch should enable X-Ring function and assign two member ports to form the ring. Only one switch in the X-Ring group would be set as a backup switch, and one of its two member ports on this backup switch would be blocked, called the backup port, while the other member port is called a working port. Other switches are called working switches and their two member ports are called working ports. When the network connection fails, the backup port will automatically become a working port to resume the connection.

CME-822(E) also supports Couple Ring, a power management function that allows 2 or more X-Ring groups to be connected to each other to offer more advanced redundancy. Dual Homing function is another advanced management feature that CME-822(E) offers, an advanced redundancy network solution by connecting switches running in different redundant protocols such as IEEE 802.1w Rapid Spanning Tree Protocol and X-Ring to extend the network redundant coverage.

Enable Ring	This feature allows the administrator to enable the X-Ring function. Mark the check box to enable the X-Ring function.
Enable Ring Master	This feature allows the administrator to enable particular switch to be a Ring Master in an X-Ring group.
1st & 2nd Ring Ports	This feature allows the administrator to assign two ports as the X-Ring group member ports. One of the ports will be the working port and the other port will be the backup port. ■ For Ring Master: The 1st Ring port will be the primary transmission path and the 2nd Ring port will only activated while 1st Ring port is fail, usually the 2nd Ring port will be in "Blocking" status and the 1st Ring port will be in "Forwarding" status. ■ For the Member switch: Both 1st and 2nd Ring ports will all show in "Forwarding" status, the switch will decide according to the user's settings, once the 1st Ring port is fail, the 2nd Ring port will prompt become the primary transmission path for the X-Ring.
Enable Couple Ring	This feature allows the administrator to enable the Couple Ring function. Mark the check box to enable the Couple Ring function.
Coupling Port	This feature allows the administrator to assign the coupling port between two X-Ring groups.
Control Port	This feature allows the administrator to set the control port for each X-Ring group to detect the X-Ring health in a Couple Ring topology.
Enable Dual Homing	This feature allows the administrator to set up one of the ports on the switch to be the Dual Homing port. In an X-Ring group, maximum number of Dual Homing ports is one. Dual Homing will only work when the X-Ring function is enabled.
Enable Dual Ring	This feature allows the administrator to enable the Dual Ring function. Mark the check box to enable the Dual Ring function. And in order to work with Dual Ring, the central backbone switch has to be assigned as X-Ring's Ring Master too.
1st & 2nd Ring Ports	This feature allows the administrator to assign two ports as the Dual Ring group member ports. One of the ports will be the working port and the other port will be the backup port.

After finishing necessary configurations, click on **Apply** to save the settings.



X-Ring Configuration

☑ Enable Ring			
	□ Enable Ring Master		
	1st Ring Port	Port.01	LINKDOWN
	2nd Ring Port	Port.02	LINKDOWN
□ Enable Couple Ring			
	Couple Port	Port.03	LINKDOWN
	Control Port	Port.04	LINKDOWN
□ Enable Dual Homing			
	Homing Port	Port.05	LINKDOWN
□ Enable Dual Ring			
	1st Ring Port	Port.01	LINKDOWN
	2nd Ring Port	Port.02	LINKDOWN

When the X-Ring function is enabled, RSTP function must be disabled. The X-Ring function and RSTP function cannot be in operation at the same time.

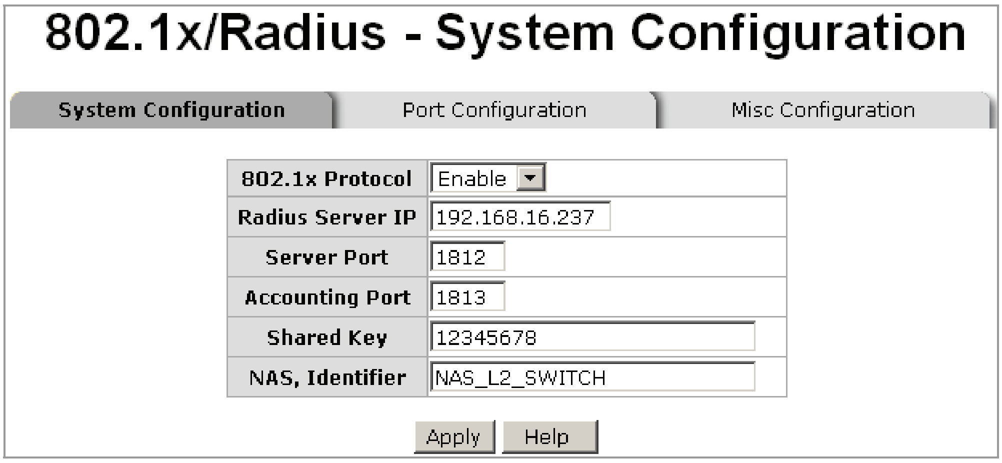
4-6.17 802.1X/Radius Configuration

802.1X is an IEEE standard, which provides port-based authentication. It involves communications between a supplicant, authenticator, and authentication server. The supplicant is often software on a client device, such as a laptop, the authenticator is a wired Ethernet switch or wireless access point, and an authentication server is generally a RADIUS database. The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity is authorized.

4-6.17.1 System Configuration

The administrator can use this interface to enable and configure 802.1X/Radius security function.

IEEE 802.1x Protocol	This feature is to enable or disable IEEE 802.1X protocol.
Radius Server IP	This feature is to assign the RADIUS Server IP address.
Server Port	This feature is to set the UDP destination port for authentication requests to the specified RADIUS Server.
Accounting Port	This feature is to set the UDP destination port for accounting requests to the specified RADIUS Server.
Shared Key	This feature is to set an encryption key for authentication with the specified RADIUS server. This key must match the encryption key used on the RADIUS Server.
NAS, Identifier	This feature is to assign the identifier for the RADIUS client.



802.1x/Radius - System Configuration

802.1x Protocol	Enable
Radius Server IP	192.168.16.237
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

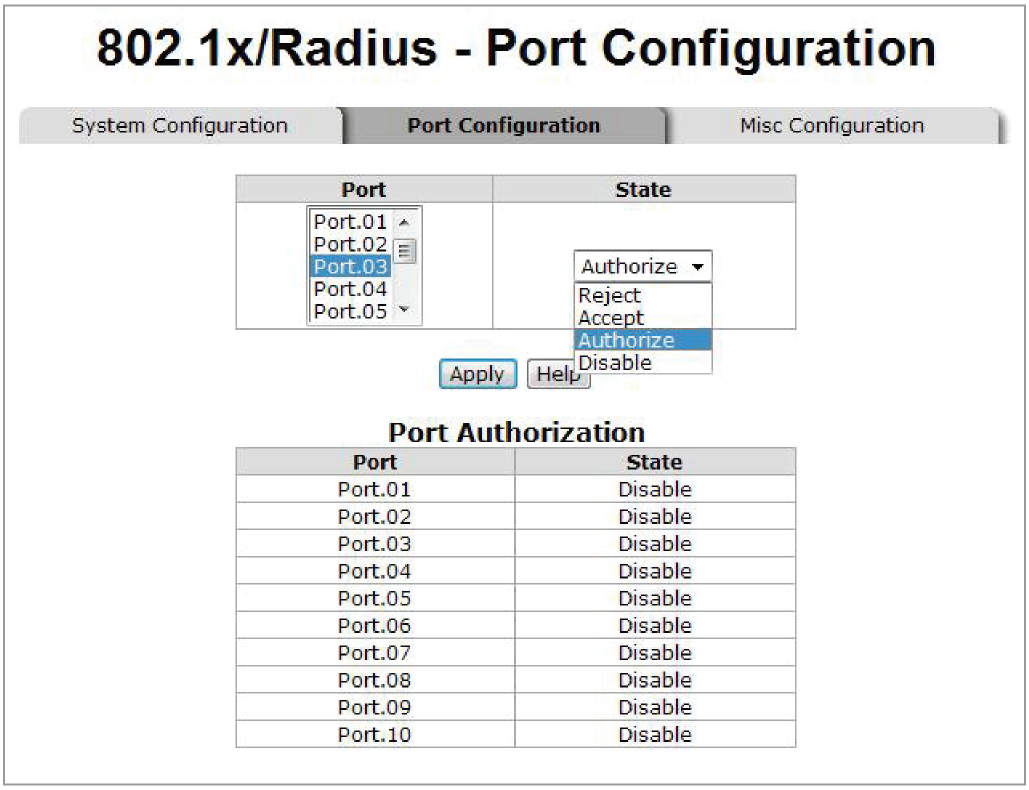
After finishing necessary configurations, click on **Apply** to save the settings.

4-6.17.2 Port Configuration

The administrator can use this interface to enable and configure 802.1X authentication state for each port. The available state options include **Disable**, **Accept**, **Reject**, and **Authorize**.

Reject	The specified port is required to be held in the unauthorized state.
Accept	The specified port is required to be held in the authorized state.
Authorize	The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the supplicant and the authentication server.
Disable	When disabled, the specified port works without complying with 802.1x protocol.

After finishing necessary configurations, click on **Apply** to save the settings.



802.1x/Radius - Port Configuration

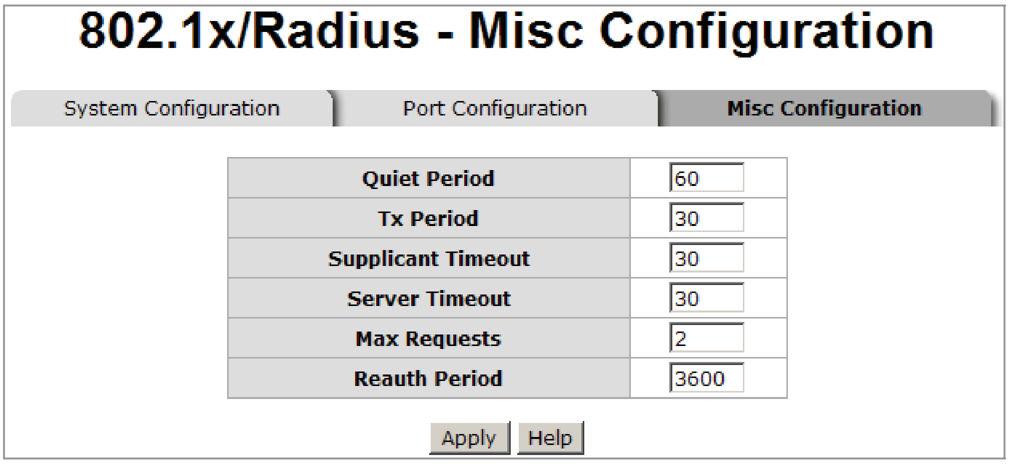
Port Authorization

Port	State
Port.01	Disable
Port.02	Disable
Port.03	Disable
Port.04	Disable
Port.05	Disable
Port.06	Disable
Port.07	Disable
Port.08	Disable
Port.09	Disable
Port.10	Disable

4-6.17.3 Misc Configuration

The administrator can use this interface to configure the Misc settings.

Quiet Period	This feature is to set the time period which the port doesn't try to acquire a supplicant.
Tx Period	This feature is to set the time period the port waits for retransmitting next EAPOL PDU during an authentication session.
Supplicant Timeout	This feature is to set the time period the switch waits for a supplicant response to an EAP request.
Server Timeout	This feature is to set the time period the switch waits for a server's response to an authentication request.
Max Requests	This feature is to set the number of authentication requests that must time out before authentication fails and the authentication session ends.
Reauth Period	This feature is to set the time period after which the connected client devices must be re-authenticated.



802.1x/Radius - Misc Configuration

Quiet Period	60
Tx Period	30
Supplicant Timeout	30
Server Timeout	30
Max Requests	2
Reauth Period	3600

After finishing necessary configurations, click on **Apply** to save the settings.

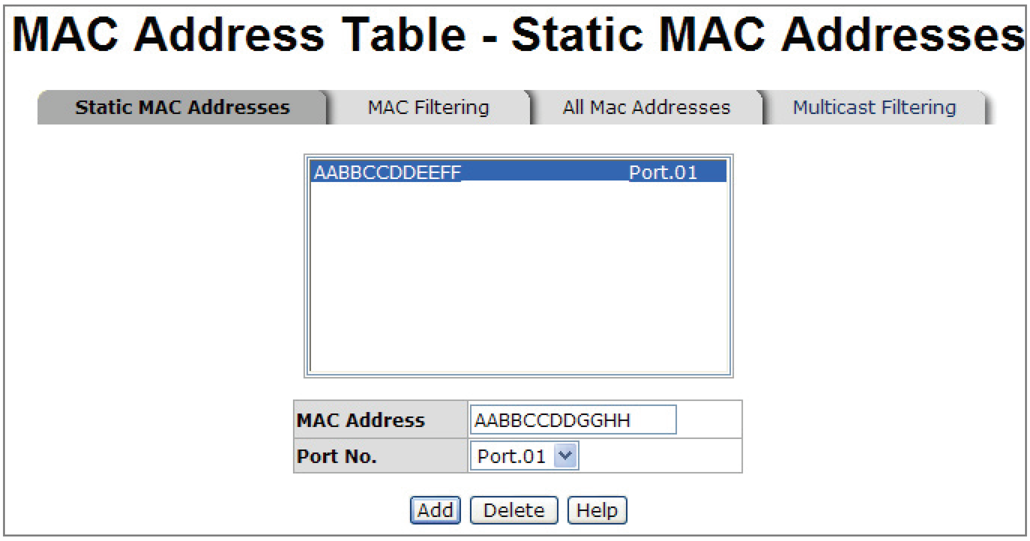
4-6.18 MAC Address Table

MAC address table can help define the authorization levels for certain devices on the network, and further secure the network integrity by preventing unauthorized access.

4-6.18.1 Static MAC Address Settings

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

MAC Address	This feature is to assign the MAC address to a certain port so that the packets destined or un-destined to this MAC address will still or will not be forwarded regardless of the physical location of the device with this MAC address.
Port No.	This feature is to select the port that the MAC address is assigned to.



MAC Address Table - Static MAC Addresses

AABBCCDDEEFF Port.01

MAC Address: AABBCCDDGGHH

Port No.: Port.01

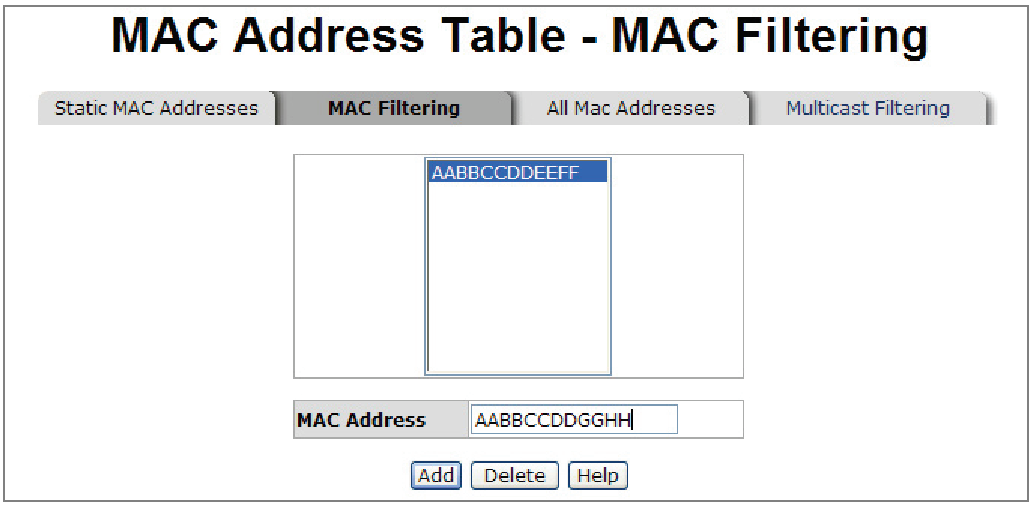
To delete a MAC address, simply select the MAC address, and then click on **Delete**.

4-6.18.2 MAC Filtering

By filtering MAC addresses, the switch can easily filter packets from unwanted MAC addresses, and further keep the network intact.

MAC Address	Enter the MAC address that you want to filter.

To delete a MAC address, simply select the MAC address, and then click on **Delete**.



MAC Address Table - MAC Filtering

AABBCCDDEEFF

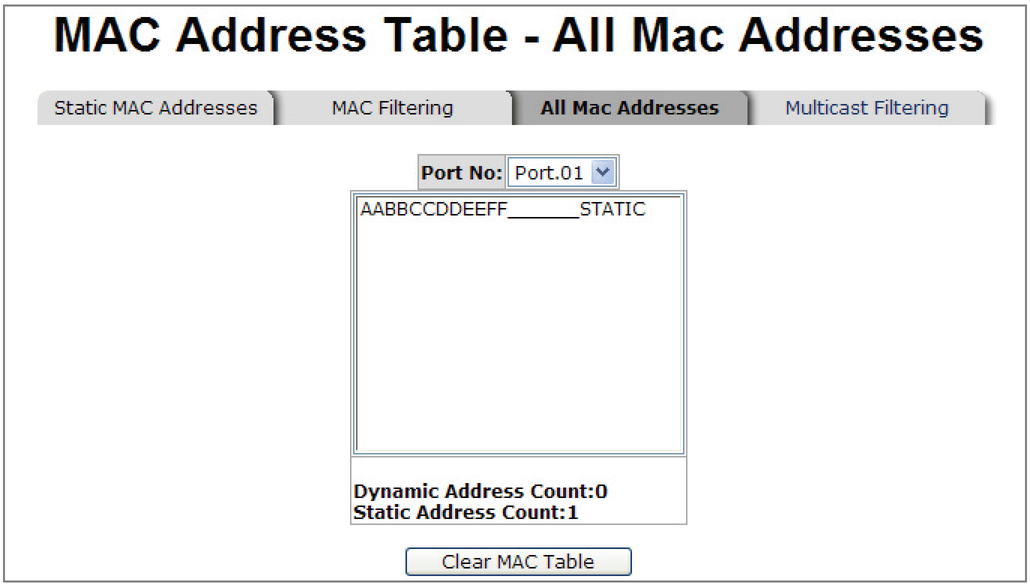
MAC Address: AABBCCDDGGHH

4-6.18.3 All MAC Addresses

You can view all of the MAC addresses learned by the selected port.

Port No.	This feature is to select the port which you would like to see the MAC addresses assigned to it. The selected port’s static & dynamic MAC address information will then be displayed in the box below.

To clear the current MAC address information on this screen, click on **Clear MAC Table**.



MAC Address Table - All Mac Addresses

Port No: Port.01

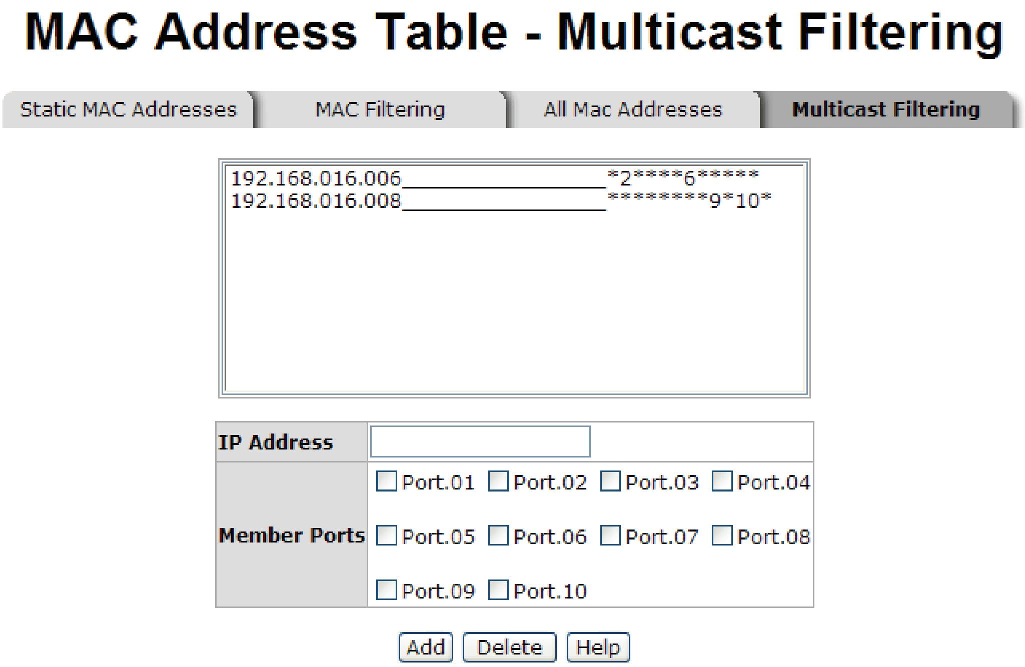
```
AABBCCDDEEFF_______STATIC
```

Dynamic Address Count:0
Static Address Count:1

4-6.18.4 Multicast Filtering

The Multicast Filtering function enables port blocking function for multicast traffic from a specified multicast server.

IP Address	This feature allows administrator to enter a specify IP address of the multicast server.
Member Ports	This feature allows administrator to specify which port to be block for the multicast traffic, tick the checkbox besides the port number to enable the blocking.



MAC Address Table - Multicast Filtering

```
192.168.016.006__________________*2****6*****
192.168.016.008__________________********9*10*
```

IP Address	
Member Ports	□ Port.01 □ Port.02 □ Port.03 □ Port.04 □ Port.05 □ Port.06 □ Port.07 □ Port.08 □ Port.09 □ Port.10

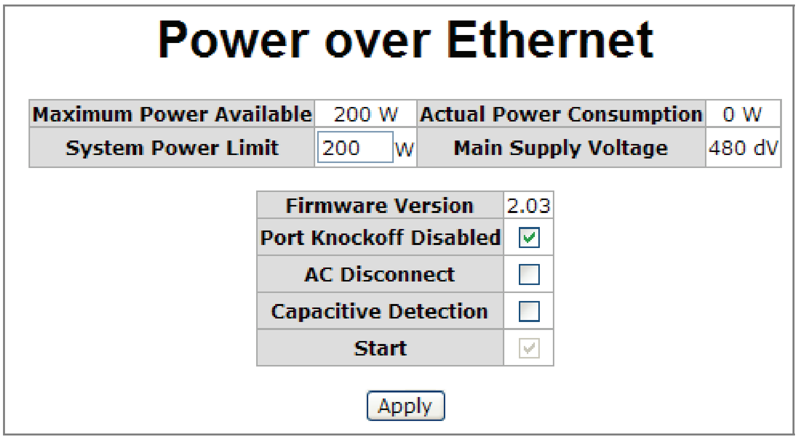
4-6.19 Power over Ethernet

The Power over Ethernet feature provides monitoring and configuration for the PoE functions.

Maximum Power Available	This column shows the maximum power supply in Watts.
Actual Power Consumption	This column shows the real-time total power consumptions.

System Power Limit	This column allows administrator to modify the value to limit the total output power for the system.
Main Supply Voltage	This column shows the output voltage of the system for PoE ports.
Firmware Version	This column shows the PoE chipset's firmware version.
Port Knockoff Disabled	The tick option allows administrator to configure the power management state where one or more PDs have been powered down so that a higher priority PD may be powered up and yet not exceed the maximum total power available for PDs.
AC Disconnect	The tick option allows administrator to monitor the AC impedance on the port terminals and removes power when the impedance rises above a certain value, for a certain period (for details, see the IEEE 802.3af specification).
Capacitive Detection	If the port and capacitive detection are enabled, the capacitances state reads in the voltage result from the constant current. This is then subtracted from the pre-capacitance voltage to get a charge rate. If this charge rate is within the window of the PD signatures, the device is considered to be discovered.
Start	This column shows the information that system initializes and resets successfully.

After finishing necessary configurations, click on **Apply** to save the settings.

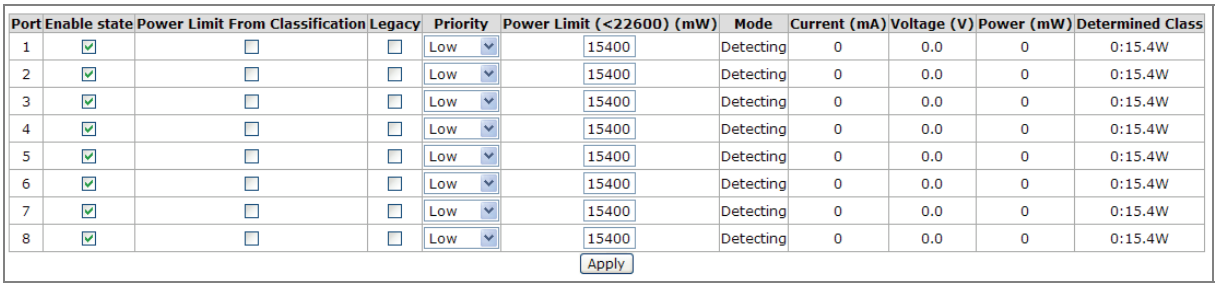


Power over Ethernet

Maximum Power Available	200 W	Actual Power Consumption	0 W
System Power Limit	200 W	Main Supply Voltage	480 dV

Firmware Version	2.03
Port Knockoff Disabled	☑
AC Disconnect	□
Capacitive Detection	□
Start	☑

Port	This column shows the index of PoE ports.
Enable State	The tick option allows administrator to enable/disable the PoE function to the port.
Power Limit From Classification	The tick option allows administrator to decide the power limit method. When this check box is ticked, the system will limit the power supply to the powered device in accordance with the related class.
Legacy	The tick option allows administrator to enable/disable the legacy powered devices support.
Priority	The pull down menu allows administrator to decide the priority of power supplying by each PoE port.
Power Limit (<22600) mW	The column allows administrator to key in the power limit value which is under 15.4 Watts.
Mode	This column shows the operating mode of the port.
Current (mA)	This column shows the operating current of the port.
Voltage (V)	This column shows the operating voltage of the port.
Power (mW)	This column shows the power consumption of the port.
Determined Class	This column shows the PD's class.



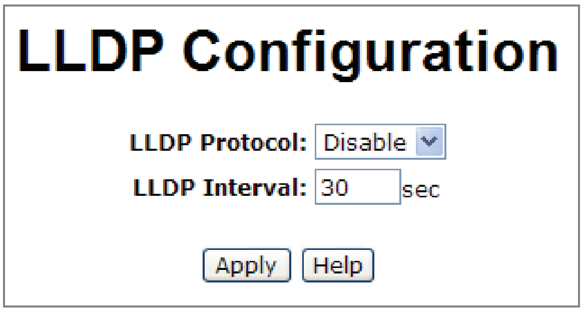
Port	Enable state	Power Limit From Classification	Legacy	Priority	Power Limit (<22600) (mW)	Mode	Current (mA)	Voltage (V)	Power (mW)	Determined Class
1	☑	□	□	Low	15400	Detecting	0	0.0	0	0:15.4W
2	☑	□	□	Low	15400	Detecting	0	0.0	0	0:15.4W
3	☑	□	□	Low	15400	Detecting	0	0.0	0	0:15.4W
4	☑	□	□	Low	15400	Detecting	0	0.0	0	0:15.4W
5	☑	□	□	Low	15400	Detecting	0	0.0	0	0:15.4W
6	☑	□	□	Low	15400	Detecting	0	0.0	0	0:15.4W
7	☑	□	□	Low	15400	Detecting	0	0.0	0	0:15.4W
8	☑	□	□	Low	15400	Detecting	0	0.0	0	0:15.4W

After finishing necessary configurations, click on **Apply** to save the settings.

4-6.20 LLDP

LLDP (Link Layer Discovery Protocol) function allows the switch to advertise its information to other nodes on the network and store the information it discovers.

LLDP Protocol	This column allows administrator to enable/disable the LLDP function
LLDP Interval	This column allows administrator to setup the interval of learning the information time in second.



LLDP Configuration

LLDP Protocol: Disable

LLDP Interval: 30 sec

After finishing necessary configurations, click on **Apply** to save the settings.

Chapter 5

Network Applications

This chapter contains information on advanced network applications. The topics include:

- X-Ring Application
- Couple Ring Application
- Dual Homing Application
- Dual Ring Application

5-1 X-Ring Application

X-Ring is an advanced industrial redundant technology introduced by Ethernet Direct. When compared with the commercial standard redundant technologies like STP or RSTP, the X-Ring can effectively reduce the recovery time to less than 300ms. The ring topology must be applied to all the connected switches. When all switches are connected in a ring topology with X-Ring function enabled, on of the switches will be appointed as Ring Master. The Ring Master will monitor the ring's health to make sure the ring is working properly. Once a failure is detected by the Ring Master, the Ring Master will activate the blocked backup path within milliseconds to replace the faulty primary transmission path to make sure the ring topology will continue to work. In addition, there are multiple Ring Masters allowed in the ring connections. Please see below figure 1 for the example of an X-Ring connection.

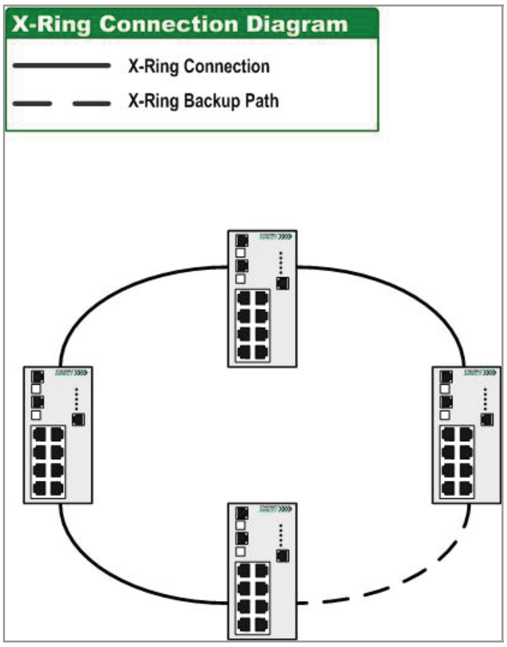


Figure 1 Example of X-Ring Connection Diagram

5-2 Couple Ring

In the real world implementation, there are cases that require two X-Ring groups to be connected together to ensure redundant protection. Couple Ring technology was introduced by Ethernet for this requirement. With Couple Ring function, each X-Ring group will need to assign two switches with 2 extra ports to achieve the structure. For this reason, the total switches needed for the Couple Ring to work will be four switches, and each switch is assigned with four ports for completing a Couple Ring (including the two X-Ring ports per switch). Please see below figure 2 for example of Couple Ring connection.

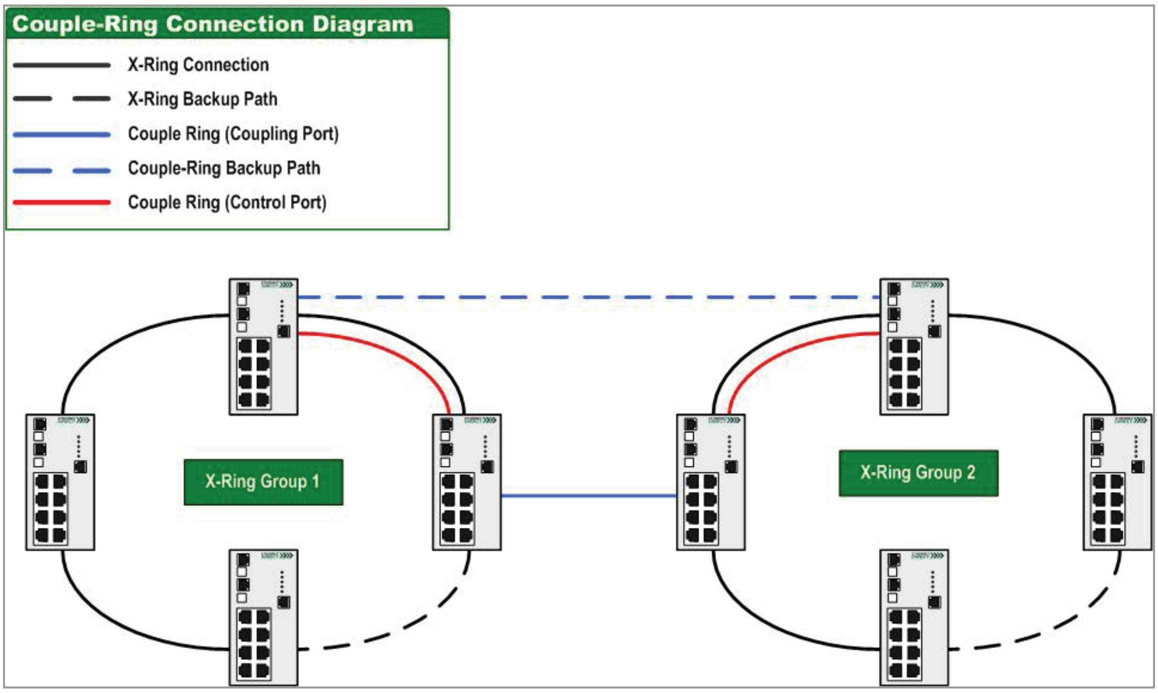


Figure 2 Example of Couple Ring Connection

5-3 Dual Homing

Dual Homing provides an advanced redundancy network solution by connecting switches running in different redundancy protocols such as IEEE 802.1w Rapid Spanning Tree Protocol and X-Ring to extend the network redundant coverage. Dual Homing feature can ensure a single or two X-Ring groups with redundant backup when connected to a backbone switch. Redundancy is achieved by connecting two ports from two separate switches using X-Ring ring protocol with two ports of managed switches using other redundancy protocol. An active link where data is transmitted is connected with on port in the switch. The other port connected with another switch is a hot standby link. The hot standby link is being constantly monitored and it will be switched over within seconds once the active link is disconnected or broken. This approach can open up LAN design options and expand device choices. For example, it can permit any industrial PLC devices with Ethernet interfaces to be part of a resilient network. With the implementation of Dual Homing feature, the X-Ring group will be allowed to connect to these backbone core switches and without sacrificing its redundant protections. Below, we show an example of connection diagram on how Dual Homing can be connected with 1 or 2 X-Ring groups.

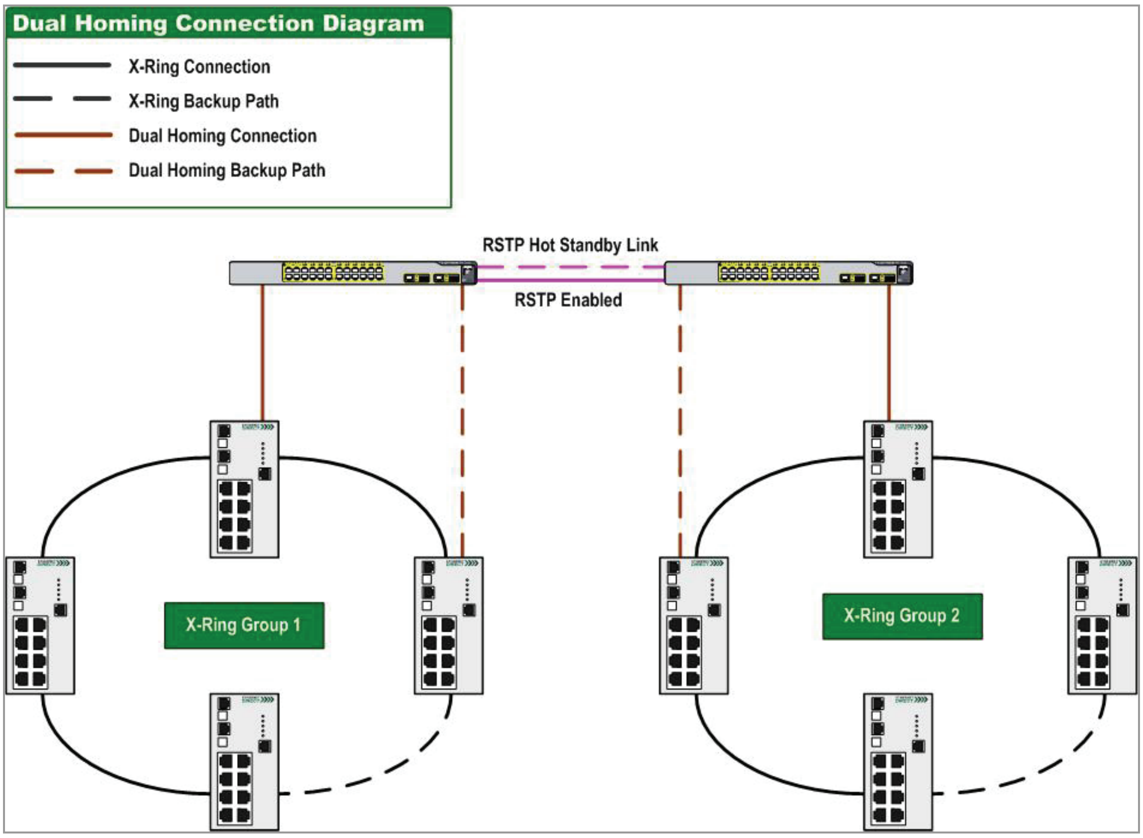


Figure 3 Example of Dual Homing with 2 X-Ring Groups Connection (Straight Through Connection)

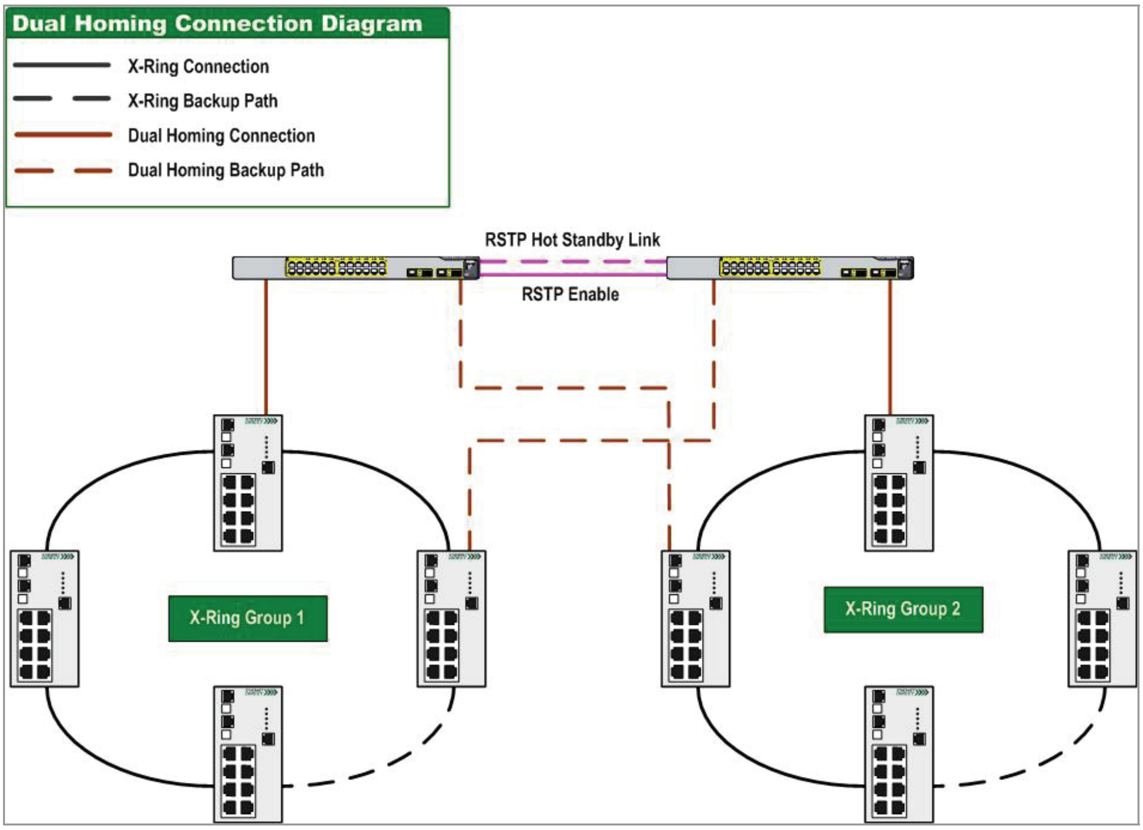


Figure 3 Example of Dual Homing with 2 X-Ring Groups Connection (Cross Through Connection)

⚠	In Dual Homing architecture, the RSTP protocol in the upper level switches needs to be enabled.

5-4 Dual Ring

Although Ethernet Direct provides the Dual Homing technology for the industrial customers who may need to connect their switches from field environment to the centralized backbone, some users may not deploy Cisco or HP switches. In some applications cases, customer would like their backbone switches to be the same as those switches in their field environment equipped with industrial-grade protection and yet serve as the backbone network. Considering the needs, Ethernet Direct released new redundant technologies called "Dual Ring". The Dual Ring is recommended when the concern is "cost" or small projects with lesser amount of switches. Dual Ring allows the connection up to two ring groups to the central backbone and the configuration will only exist in those switches with minimum 8 ports availability.

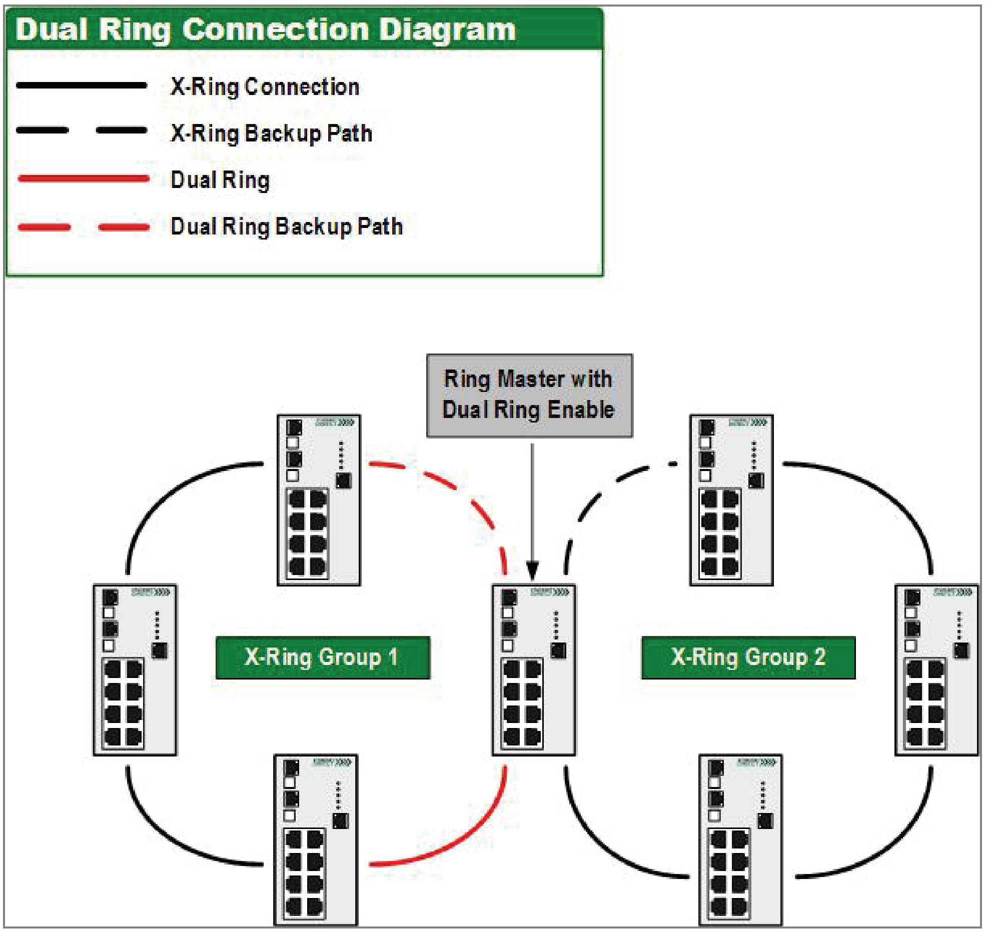


Figure 4 Example of Dual Ring Connection

Appendix A

Specifications

CME-822(E) Product Specifications are as follows:

Hardware		
Interface		
Total Ports	10 ports	
RJ-45 ports	8 10/100Base-T(X) auto-negotiation speed, Full/Half duplex, auto MDI/MDI-X	
Fiber ports	2 combo ports	
	Per Port	Link/Activity (Green)
LEDs	Per Unit	Power (Green), Power 1 (Green), Power 2 (Green), Fault (Orange), R.M.(Green)
	PoE	FWD 1-8 (Green)
Alarm Contact	1A@24VDC	
Power Requirements		
Power Input	48VDC redundant power with removable terminal block	
Power Consumption	9.7 watts max. (full load without PoE), 134 watts max. (full load with PoE)	
Power Protection	ESD (Ethernet) 6000VDC, Surge 3000VDC, Power Reverse Polarity	
Physical		
Dimensions	IP-30 standard, 72mm (W) x 105mm (D) x 152mm (H)	
Installation	DIN Rail mounting/Wall mounting	
Environmental		
Operating Temperature	Regular: -10 to 70℃ Extended: -40 to 80℃	
Storage Temperature	-40 to 85 ℃	
Operating Humidity	5% to 95% RH (Non-condensing)	
Technology		
Standard	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX/100Base-FX IEEE 802.3ab 1000Base-T IEEE 8023z Gigabit Fiber IEEE 802.3x Flow Control IEEE 802.3ad Port trunk with LACP IEEE 802.3af Power over Ethernet IEEE802.1D Spanning Tree Protocol IEEE802.1w Rapid STP IEEE802.1p Class of Service IEEE802.1Q VLAN Tagging IEEE 802.1X User Authentication (Radius)	

Protocol Technology	CSMA/CD
Switching Architecture	Store and Forward
Regulatory Approvals	
EMI	FCC Class A
EMS	EN 61000-4-2 EN 61000-4-3 EN 61000-4-4 EN 61000-4-5 EN 61000-4-6 EN 61000-4-8 EN 61000-4-11 EN 61000-4-12 EN 61000-6-2 EN 61000-6-4
Safety	UL, cUL, CE/EN 60950-1
Shock	IEC 60068-2-27
Vibration	IEC 60068-2-6
Free Fall	IEC 60068-2-32
Class 1 DIV 2	Pending
DNV	Pending
Environmental	WEEE, RoHS
MTBF	190,288 hrs based on Mil-Hdbk-217F, GB
Warranty	5 years
PoE Specifications	
PoE Compliance	100% IEEE 802.3af compliant
PoE Classification	Power Sourcing Equipment (PSE)
PoE Votage	48VDC
PoE Power	Up to 15.4 watts per port
PoE Protection	Over-temperature, over-current, over/under-voltage and transient
PoE Pin Assignment	RJ-45 port #1-8 supports IEEE 802.3af End-point, Alternative A mode. Postive (VCC+): RJ-45 pin 1, 2 Nagetive: (VCC-): RJ-45 pin 3, 6 Data: RJ-45 pin 1, 2, 3, 6
Management Specifications	
Redundancy	X-Ring with recovery time < 10 ms STP, RSTP, Dual Homing, Couple Ring, Dual Ring
Management	SNMP v1/v2c/v3/Web/Telnet/CLI management TFTP backup/restore configurations One default button for system default settings
SNMP Trap	Up to 3 Trap stations Cold start Port link up Port link down

	Authentication failure Private Trap for power status Port alarm configuration Fault alarm, X-Ring
RFC Standard	RFC 2030 SNTP RFC 2821 SMTP RFC 1215 Trap RFC 2233 MIBII RFC 1157 SNMP MIB RFC 1493 Bridge MIB RFC 2674 VLAN MIB RFC 2665 Ethernet like MIB RFC 2819 RMON MIB Private MIB
LLDP	Allows switch to advise its identification and capability on the LAN
Port Trunk	IEEE802.3ad with LACP function Max. 4 trunk groups Max. 4 ports per group (including 2 uplink ports)
VLAN	Port based VLAN and Tag VLAN (256 entries) VID: 1 to 4094 Static VLAN groups up to 256 GVRP groups up to 256
QoS	Port based and IEEE 802.1p QoS determined by port, per port 4 queues Tag and IPv4 ToS, IPv4/IPv6 DiffServ
IGMP	IGMP v1 and v2 snooping IGMP groups up to 256 Multicast filtering
Security	Port Security: MAC address entries/filter IP Security: IP address security to prevent unauthorized intruders Remote Access Security: IEEE802.1X/RADIUS
Port Mirror	RX, TX, and Both packet
Bandwidth Control	Network packet filtering options Ingress/Egress control per port
DHCP	DHCP Client/DHCP Server
SMTP	SMTP Client Up to 6 E-mail accounts with pre-defined warning events
SNTP	SNTP client to synchronize system clock from Internet
Firmware Upgrade	By TFTP

Appendix B

Troubleshooting

⚠	Make sure you are using the right power cord/adapter (DC 48V). Do not use power adapters with DC output higher than 48V. Or it will short circuit the switch.

⚠	Select the proper UTP cables to construct your network. Please check that you are using the right cables. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cables for RJ-45 connections: 100Ω Category 3, 4 or 5 cables for 10Mbps connections, and 100Ω Category 5 or above cables for 100Mbps. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

⚠	Diagnostic LED indicators located on the front panel of the switch can help users to easily monitor the switch.

⚠	IF the power indicator does not light on when the power cord is plugged in, you may have a problem with power cord. Then check for loose power connections, power losses or surges at power outlet. IF you still cannot resolve the problem, contact your local dealer for assistance.

⚠	If the switch LED indicators are normal, the cables are connected correctly, and the packets still cannot transmit, please check your system's Ethernet devices' configuration or status.

Appendix C

Command Set Lists

C-1 Commands Set List

User EXEC	**E**
Privileged EXEC	**P**
Global configuration	**G**
VLAN database	**V**
Interface configuration	**I**

C-2 System Commands Set

Commands	Level	Description	Example
show config	**E**	Show switch configuration	switch>**show config**
show terminal	**P**	Show console information	switch#**show terminal**
write memory	**P**	Save user configuration into permanent memory (flash rom)	switch#**write memory**
system name [System Name]	**G**	Configure system name	switch(config)#**system name xxx**
system location [System Location]	**G**	Set switch system location string	switch(config)#**system location xxx**
system description [System Description]	**G**	Set switch system description string	switch(config)#**system description xxx**
system contact [System Contact]	**G**	Set switch system contact window string	switch(config)#**system contact xxx**
show system-info	**E**	Show system information	switch>**show system-info**
ip address [Ip-address] [Subnet-mask] [Gateway]	**G**	Configure the IP address of switch	switch(config)#**ip address 192.168.16.1 255.255.255.0 192.168.16.254**
ip dhcp	**G**	Enable DHCP client function of switch	switch(config)#**ip dhcp**
show ip	**P**	Show IP information of switch	switch#**show ip**
no ip dhcp	**G**	Disable DHCP client function of switch	switch(config)#**no ip dhcp**
reload	**G**	Halt and perform a cold restart	switch(config)#**reload**
default	**G**	Restore to default	switch(config)#**default**
admin username [Username]	**G**	Changes a login username. (maximum 10 words)	switch(config)#**admin username xxxxxx**

admin password [Password]	**G**	Specifies a password (maximum 10 words)	switch(config)#**admin password xxxxxx**
show admin	**P**	Show administrator information	switch#**show admin**
dhcpserver enable	**G**	Enable DHCP Server	switch(config)#**dhcpserver enable**
Dhcpserver disable	**G**	Disable DHCP Server	switch(config)#**no dhcpserver**
dhcpserver lowip [Low IP]	**G**	Configure low IP address for IP pool	switch(config)#**dhcpserver lowip 192.168.16.100**
dhcpserver highip [High IP]	**G**	Configure high IP address for IP pool	switch(config)#**dhcpserver highip 192.168.16.200**
dhcpserver subnetmask [Subnet mask]	**G**	Configure subnet mask for DHCP clients	switch(config)#**dhcpserver subnetmask 255.255.255.0**
dhcpserver gateway [Gateway]	**G**	Configure gateway for DHCP clients	switch(config)#**dhcpserver gateway 192.168.16.254**
dhcpserver dnsip [DNS IP]	**G**	Configure DNS IP for DHCP clients	switch(config)#**dhcpserver dnsip 192.168.16.1**
dhcpserver leasetime [Hours]	**G**	Configure lease time (in hour)	switch(config)#**dhcpserver leasetime 1**
dhcpserver ipbinding [IP address]	**I**	Set static IP for DHCP clients by port	switch(config)#**interface fastEthernet 2** switch(config)#**dhcpserver ipbinding 192.168.16.1**
show dhcpserver configuration	**P**	Show configuration of DHCP server	switch#**show dhcpserver configuration**
show dhcpserver clients	**P**	Show client entries of DHCP server	switch#**show dhcpserver clients**
show dhcpserver ip-binding	**P**	Show IP-Binding information of DHCP server	switch#**show dhcpserver ip-binding**
no dhcpserver	**G**	Disable DHCP server function	switch(config)#**no dhcpserver**
security enable	**G**	Enable IP security function	switch(config)#**security enable**
security http	**G**	Enable IP security of HTTP server	switch(config)#**security http**
security telnet	**G**	Enable IP security of telnet server	switch(config)#**security telnet**
security ip [Index(1..10)] [IP Address]	**G**	Set the IP security list	switch(config)#**security ip 1 192.168.16.55**
show security	**P**	Show the information of IP security	switch#**show security**
no security	**G**	Disable IP security function	switch(config)#**no security**
no security http	**G**	Disable IP security of HTTP server	switch(config)#**no security http**
no security telnet	**G**	Disable IP security of telnet server	switch(config)#**no security telnet**

C-3 Port Commands Set

Commands	Level	Description	Example
interface fastEthernet [Portid]	G	Choose the port for modification.	switch(config)#**interface fastEthernet 2**
duplex [full | half]	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#**interface fastEthernet 2** switch(config-if)#**duplex full**
speed [10|100|1000|auto]	I	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet. The speed can't be set to 1000Mbps if the port isn't a giga port.	switch(config)#**interface fastEthernet 2** switch(config-if)#**speed 100**
no flowcontrol	I	Disable flow control of interface	switch(config-if)#**no flowcontrol**
security enable	I	Enable security of interface	switch(config)#**interface fastEthernet 2** switch(config-if)#**security enable**
no security	I	Disable security of interface	switch(config)#**interface fastEthernet 2** switch(config-if)#**no security**
bandwidth type all	I	Set interface ingress limit frame type to "accept all frame"	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type all**
bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to "accept broadcast, multicast, and flooded unicast frame"	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-multicast-flooded-unicast**
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to "accept broadcast and multicast frame"	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-multicast**
bandwidth type broadcast-only	I	Set interface ingress limit frame type to "only accept broadcast frame"	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-only**
bandwidth in [Value]	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth in 100**
bandwidth out [Value]		Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth out 100**
show bandwidth	I	Show interfaces bandwidth control	switch(config)#**interface fastEthernet 2** switch(config-if)#**show bandwidth**
state [Enable | Disable]	I	Use the state interface configuration command to specify the state mode of	switch(config)#**interface fastEthernet 2** switch(config-if)#**state Disable**

		operation for Ethernet ports. Use the disable form of this command to disable the port.	
show interface configuration	**I**	Show interface configuration status	switch(config)#**interface fastEthernet 2** switch(config-if)#**show interface configuration**
show interface status	**I**	Show interface actual status	switch(config)#**interface fastEthernet 2** switch(config-if)#**show interface status**
show interface accounting	**I**	Show interface statistic counter	switch(config)#**interface fastEthernet 2** switch(config-if)#**show interface accounting**
no accounting	**I**	Clear interface accounting information	switch(config)#**interface fastEthernet 2** switch(config-if)#**no accounting**

C-4 Trunk Commands Set

Commands	**Level**	**Description**	**Example**
aggregator priority [1~65535]	**G**	Set port group system priority	switch(config)#**aggregator priority 22**
aggregator activityport [Group ID] [Port Numbers]	**G**	Set activity port	switch(config)#**aggregator activityport 2**
aggregator group [GroupID] [Port-list] lacp workp [Workport]	**G**	Assign a trunk group with LACP active. [GroupID]: 1~3 [Port-list]: Member port list. This parameter could be a port range (ex.1-4) or a port list separate by a comma (ex.2, 3, 6) [Workport]: The amount of work ports. This value could not be less than zero or be large than the amount of member ports.	switch(config)#**aggregator group 1 1-4 lacp workp 2** or switch(config)#**aggregator group 2 1,4,3 lacp workp 3**
aggregator group [GroupID] [Port-list] nolacp	**G**	Assign a static trunk group. [GroupID]:1~3 [Port-list]: Member port list. This parameter could be a port range (ex.1-4) or a port list separate by a comma ex.2, 3, 6)	switch(config)#**aggregator group 1 2-4 nolacp** or switch(config)#**aggregator group 1 3,1,2 nolacp**
show aggregator	**P**	Show the information of trunk group	switch#**show aggregator 1** or switch#**show aggregator 2** or switch#**show aggregator 3**
no aggregator lacp [GroupID]	**G**	Disable the LACP function of trunk group	switch(config)#**no aggreator lacp 1**
no aggregator group [GroupID]	**G**	Remove a trunk group	switch(config)#**no aggreator group 2**

C-5 VLAN Commands Set

Commands	Level	Description	Example
vlan database	P	Enter VLAN configure mode	switch#**vlan database**
Vlanmode [portbase| 802.1q | gvrp]	V	To set switch VLAN mode.	switch(vlan)#**vlanmode portbase** or switch(vlan)#**vlanmode 802.1q** or switch(vlan)#**vlanmode gvrp**
no vlan	V	No VLAN	Switch(vlan)#**no vlan**
Ported based VLAN configuration			
vlan port-based grpname [Group Name] grpid [GroupID] port [PortNumbers]	V	Add new port based VALN	switch(vlan)#**vlan port-based grpname test grpid 2 port 2-4** or switch(vlan)#**vlan port-based grpname test grpid 2 port 2,3,4**
show vlan [GroupID] or show vlan	V	Show VLAN information	switch(vlan)#**show vlan 23**
no vlan group [GroupID]	V	Delete port base group ID	switch(vlan)#**no vlan group 2**
IEEE 802.1Q VLAN			
vlan 8021q name [GroupName] vid [VID]	V	Change the name of VLAN group, if the group didn't exist, this command can't be applied.	switch(vlan)#**vlan 8021q name test vid 22**
vlan 8021q port [PortNumber] access-link untag [UntaggedVID]	V	Assign a access link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 access-link untag 33**
vlan 8021q port [PortNumber] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 trunk-link tag 2,3,6,99** or switch(vlan)#**vlan 8021q port 3 trunk-link tag 3-20**
vlan 8021q port [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q port 3 hybrid-link untag 5 tag 6-8**
vlan 8021q trunk [PortNumber] access-link untag [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 access-link untag 33**
vlan 8021q trunk [PortNumber] trunk-link tag	V	Assign a trunk link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 trunk-link tag 2,3,6,99** or

[TaggedVID List]			switch(vlan)#**vlan 8021q trunk 3 trunk-link tag 3-20**
vlan 8021q trunk [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	**V**	Assign a hybrid link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q trunk 3 hybrid-link untag 5 tag 6-8**
show vlan [GroupID] or show vlan	**V**	Show VLAN information	switch(vlan)#**show vlan 23**
no vlan group [GroupID]	**V**	Delete port base group ID	switch(vlan)#**no vlan group 2**

C-6 Spanning Tree Commands Set

Commands	Level	Description	Example
spanning-tree enable	**G**	Enable spanning tree	switch(config)#**spanning-tree enable**
spanning-tree priority [0~61440]	**G**	Configure spanning tree priority parameter	switch(config)#**spanning-tree priority 32768**
spanning-tree max-age [seconds]	**G**	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputes the Spanning Tree Protocol (STP) topology.	switch(config)#**spanning-tree max-age 15**
spanning-tree hello-time [seconds]	**G**	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#**spanning-tree hello-time 3**
spanning-tree forward-time [seconds]	**G**	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins	switch(config)#**spanning-tree forward-time 20**

		forwarding.	
stp-path-cost [1~200000000]	I	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-cost 20**
stp-path-priority [Port Priority]	I	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-priority 128**
stp-admin-p2p [Auto|True|False]	I	Admin P2P of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-p2p Auto**
stp-admin-edge [True|False]	I	Admin Edge of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-edge True**
stp-admin-non-stp [True|False]	I	Admin NonSTP of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-non-stp False**
show spanning-tree	E	Displays a summary of the spanning-tree states.	switch>**show spanning-tree**
no spanning-tree	G	Disable spanning-tree.	switch(config)#**no spanning-tree**

C-7 QoS Commands Set

Commands	Level	Description	Example
qos policy [weighted-fair|strict]	G	Select QoS policy scheduling	switch(config)#**qos policy weighted-fair**
qos prioritytype [port-based|cos-only|tos-only|cos-first|tos-first]	G	Set up QoS priority type	switch(config)#**qos prioritytype**
qos priority portbased [Port] [lowest|low|middle|high]	G	Configure Port-based priority	switch(config)#**qos priority portbased 1 low**
qos priority cos [Priority][lowest|low|middle|high]	G	Configure COS Priority	switch(config)#**qos priority cos 0 middle**
qos priority tos [Priority][lowest|low|middle|high]	G	Configure TOS Priority	switch(config)#**qos priority tos 3 high**
show qos	P	Displays the information of QoS configuration	switch#**show qos**
no qos	G	Disable QoS function	switch(config)#**no qos**

C-8 IGMP Commands Set

Commands	Level	Description	Example
igmp enable	**G**	Enable IGMP snooping function	switch(config)#**igmp enable**
Igmp-query auto	**G**	Set IGMP query to auto mode	switch(config)#**Igmp-query auto**
Igmp-query force	**G**	Set IGMP query to force mode	switch(config)#**Igmp-query force**
show igmp configuration	**P**	Displays the details of an IGMP configuration.	switch#**show igmp configuration**
show igmp multi	**P**	Displays the details of an IGMP snooping entries.	switch#**show igmp multi**
no igmp	**G**	Disable IGMP snooping function	switch(config)#**no igmp**
no igmp-query	**G**	Disable IGMP query	switch#**no igmp-query**

C-9 MAC / Filter Table Commands Set

Commands	Level	Description	Example
mac-address-table static hwaddr [MAC]	**I**	Configure MAC address table of interface (static).	switch(config)#**interface fastEthernet 2** switch(config-if)#**mac-address-table static hwaddr 000012345678**
mac-address-table filter hwaddr [MAC]	**G**	Configure MAC address table(filter)	switch(config)#**mac-address-table filter hwaddr 000012348678**
show mac-address-table	**P**	Show all MAC address table	switch#**show mac-address-table**
show mac-address-table static	**P**	Show static MAC address table	switch#**show mac-address-table static**
show mac-address-table filter	**P**	Show filter MAC address table.	switch#**show mac-address-table filter**
no mac-address-table static hwaddr [MAC]	**I**	Remove an entry of MAC address table of interface (static)	switch(config)#**interface fastEthernet 2** switch(config-if)#**no mac-address-table static hwaddr 000012345678**
no mac-address-table filter hwaddr [MAC]	**G**	Remove an entry of MAC address table (filter)	switch(config)#**no mac-address-table filter hwaddr 000012348678**
no mac-address-table	**G**	Remove dynamic entry of MAC address table	switch(config)#**no mac-address-table**

C-10 SNMP Commands Set

Commands	Level	Description	Example
snmp system-name [System Name]	**G**	Set SNMP agent system name	switch(config)#**snmp system-name l2switch**
snmp system-location [System Location]	**G**	Set SNMP agent system location	switch(config)#**snmp system-location lab**
snmp system-contact [System Contact]	**G**	Set SNMP agent system contact	switch(config)#**snmp system-contact where**
snmp agent-mode [v1v2c|v3|v1v2cv3]	**G**	Select the agent mode of SNMP	switch(config)#**snmp agent-mode v1v2cv3**
snmp community-strings	**G**	Add SNMP community	switch(config)#**snmp**

[Community] right [RO/RW]		string.	**community-strings public right rw**
snmp-server host [IP address] community [Community-string] trap-version [v1|v2c]	**G**	Configure SNMP server host information and community string	switch(config)#**snmp-server host 192.168.1.50 community public trap-version v1** **(remove)** switch(config)# **no snmp-server host 192.168.1.50**
snmpv3 context-name [Context Name]	**G**	Configure the context name	switch(config)#**snmpv3 context-name Test**
snmpv3 user [User Name] group [Group Name] password [Authentication Password] [Privacy Password]	**G**	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#**snmpv3 user test01 group G1 password AuthPW PrivPW**
snmpv3 access context-name [Context Name] group [Group Name] security-level [NoAuthNoPriv|AuthNoPriv|AuthPriv] match-rule [Exact|Prifix] views [Read View Name] [Write View Name] [Notify View Name]	**G**	Configure the access table of SNMPV3 agent	switch(config)#**snmpv3 access context-name Test group G1 security-level AuthPriv** **match-rule Exact views V1 V1 V1**
snmpv3 mibview view [View Name] type [Excluded|Included] sub-oid [OID]	**G**	Configure the mibview table of SNMPV3 agent	switch(config)#**snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**
show snmp	**P**	Show SNMP configuration	switch#**show snmp**
no snmp community-strings [Community]	**G**	Remove the specified community.	switch(config)#**no snmp community-strings public**
no snmp-server host [Host-address]	**G**	Remove the SNMP server host.	switch(config)#**no snmp-server host 192.168.1.50**
no snmpv3 user [User Name]	**G**	Remove specified user of SNMPv3 agent.	switch(config)#**no snmpv3 user Test**
no snmpv3 access context-name [Context Name] group [Group Name]	**G**	Remove specified access table of SNMPv3 agent.	switch(config)#**no snmpv3 access context-name Test group G1 security-level AuthPr** **iv match-rule Exact views V1 V1 V1**

security-level [NoAuthNoPriv|AuthNoPriv|AuthPriv] match-rule [Exact|Prifix] views [Read View Name] [Write View Name] [Notify View Name]			
no snmpv3 mibview view [View Name] type [Excluded|Included] sub-oid [OID]	**G**	Remove specified mibview table of SNMPV3 agent.	switch(config)#**no snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**

C-11 Port Mirroring Commands Set

Commands	Level	Description	Example
monitor [RX|TX|Both]	**I**	Configure source port of monitor function	switch(config)#**interface fastEthernet 2** switch(config-if)#**monitor RX**
monitor rx [Port ID]	**G**	Set RX destination port of monitor function	switch(config)#**monitor rx 2**
monitor tx [Port ID]	**G**	Set TX destination port of monitor function	switch(config)#**monitor tx 3**
show monitor	**P**	Show port monitor information	switch#**show monitor**
show monitor	**I**	Show port monitor information	switch(config)#**interface fastEthernet 2** switch(config-if)#**show monitor**
no monitor	**I**	Disable source port of monitor function	switch(config)#**interface fastEthernet 2** switch(config-if)#**no monitor**

C-12 802.1x Commands Set

Commands	Level	Description	Example
8021x enable	**G**	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# **8021x enable**
8021x system radiusip [IP address]	**G**	Use the 802.1x system radius IP global configuration command to change the radius server IP.	switch(config)# **8021x system radiusip 192.168.1.1**
8021x system serverport [port ID]	**G**	Use the 802.1x system server port global configuration command to change the radius server port.	switch(config)# **8021x system serverport 1812**
8021x system accountport [port ID]	**G**	Use the 802.1x system account port global configuration command to change the accounting port.	switch(config)# **8021x system accountport 1813**

8021x system sharedkey [ID]	**G**	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# **8021x system sharedkey 123456**
8021x system nasid [words]	**G**	Use the 802.1x system nasid global configuration command to change the NAS ID.	switch(config)# **8021x system nasid test1**
8021x misc quietperiod [sec.]	**G**	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# **8021x misc quietperiod 10**
8021x misc txperiod [sec.]	**G**	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# **8021x misc txperiod 5**
8021x misc supptimeout [sec.]	**G**	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# **8021x misc supptimeout 20**
8021x misc servertimeout [sec.]	**G**	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#**8021x misc servertimeout 20**
8021x misc maxrequest [number]	**G**	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# **8021x misc maxrequest 3**
8021x misc reauthperiod [sec.]	**G**	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# **8021x misc reauthperiod 3000**
8021x portstate [disable | reject | accept | authorize]	**I**	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch(config)#**interface fastethernet 3** switch(config-if)#**8021x portstate accept**
show 8021x	**E**	Display a summary of the 802.1x properties and also the port sates.	switch>**show 8021x**
no 8021x	**G**	Disable 802.1x function.	switch(config)#**no 8021x**

C-13 TFTP Commands Set

Commands	Level	Description	Defaults Example
backup flash:backup_cfg	**G**	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#**backup flash:backup_cfg**
restore flash:restore_cfg	**G**	Get configuration from TFTP server, and specify the IP of	switch(config)#**restore flash:restore_cfg**

		TFTP server and the file name of image.	
upgrade flash:upgrade_fw	G	Upgrade firmware by TFTP, and specify the IP of TFTP server and the file name of image.	switch(config)#**upgrade flash:upgrade_fw**

C-14 SystemLog, SMTP and Event Commands Set

Commands	Level	Description	Example
systemlog ip [IP address]	G	Set System log server IP address.	switch(config)# **systemlog ip 192.168.16.100**
systemlog mode [client|server|both]	G	Specify the log mode.	switch(config)# **systemlog mode both**
show systemlog	E	Display system log.	Switch>**show systemlog**
show systemlog	P	Show system log client & server information.	switch#**show systemlog**
no systemlog	G	Disable systemlog function.	switch(config)#**no systemlog**
smtp enable	G	Enable SMTP function.	switch(config)#**smtp enable**
smtp serverip [IP address]	G	Configure SMTP server IP.	switch(config)#**smtp serverip 192.168.16.5**
smtp authentication	G	Enable SMTP authentication.	switch(config)#**smtp authentication**
smtp account [account]	G	Configure authentication account.	switch(config)#**smtp account John**
smtp password [password]	G	Configure authentication password.	switch(config)#**smtp password 1234**
smtp rcptemail [Index] [Email address]	G	Configure Rcpt e-mail Address.	switch(config)#**smtp rcptemail 1 Alert@test.com**
show smtp	P	Show the information of SMTP.	switch#**show smtp**
no smtp	G	Disable SMTP function.	switch(config)#**no smtp**
event device-cold-start [Systemlog|SMTP|Both]	G	Set cold start event type.	switch(config)#**event device-cold-start both**
event authentication-failure [Systemlog|SMTP|Both]	G	Set Authentication failure event type.	switch(config)#**event authentication-failure both**
event ring-topology-change [Systemlog|SMTP|Both]	G	Set X-ring topology changed event type.	switch(config)#**event ring-topology-change both**
event systemlog [Link-UP|Link-Down|Both]	I	Set port event for system log.	switch(config)#**interface fastethernet 3** switch(config-if)#**event systemlog both**
event smtp [Link-UP|Link-Down|Both]	I	Set port event for SMTP.	switch(config)#**interface fastethernet 3** switch(config-if)#**event smtp both**
show event	P	Show event selection.	switch#**show event**
no event device-cold-start	G	Disable cold start event type.	switch(config)#**no event device-cold-start**
no event authentication-failure	G	Disable Authentication failure event type.	Switch(config)#**no event authentication-failure**
no event	G	Disable X-ring topology	switch(config)#**no event**

ring-topology-change		changed event type.	**ring-topology-change**
no event systemlog	**I**	Disable port event for system log.	switch(config)#**interface fastethernet 3** switch(config-if)#**no event systemlog**
no event smpt	**I**	Disable port event for SMTP.	switch(config)#**interface fastethernet 3** switch(config-if)#**no event smtp**
show systemlog	**P**	Show system log client & server information.	switch#**show systemlog**

C-15 SNTP Commands Set

Commands	Level	Description	Example
sntp enable	**G**	Enable SNTP function.	switch(config)#**sntp enable**
sntp daylight	**G**	Enable daylight saving time. If SNTP function is inactive, this command can’t be applied.	switch(config)#**sntp daylight**
sntp daylight-period [Start time] [End time]	**G**	Set period of daylight saving time. If SNTP function is inactive, this command can’t be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# **sntp daylight-period 20060101-01:01 20060202-01:01**
sntp daylight-offset [Minute]	**G**	Set offset of daylight saving time. If SNTP function is inactive, this command can’t be applied.	switch(config)#**sntp daylight-offset 3**
sntp ip [IP]	**G**	Set SNTP server IP, if SNTP function is inactive, this command can’t be applied.	switch(config)#**sntp ip 192.169.1.1**
sntp timezone [Timezone]	**G**	Set timezone index, use “show sntp timzezone” command to get more information of index number.	switch(config)#**sntp timezone 22**
show sntp	**P**	Show SNTP information.	switch#**show sntp**
show sntp timezone	**P**	Show index number of time zone list.	switch#**show sntp timezone**
no sntp	**G**	Disable SNTP function.	switch(config)#**no sntp**
no sntp daylight	**G**	Disable daylight saving time.	switch(config)#**no sntp daylight**

C-16 X-Ring Commands Set

Commands	Level	Description	Example
ring enable	**G**	Enable X-Ring.	switch(config)#**ring enable**
ring master	**G**	Enable Ring Master.	switch(config)#**ring master**
ring couplering	**G**	Enable Couple Ring.	switch(config)#**ring couplering**
ring dualhoming	**G**	Enable Dual Homing	switch(config)#**ring dualhoming**

ring ringport [1st Ring Port] [2nd Ring Port]	**G**	Configure 1st/2nd Ring Port.	switch(config)#**ring ringport 7 8**
ring couplingport [Coupling Port]	**G**	Configure Coupling Port.	switch(config)#**ring couplingport 1**
ring controlport [Control Port]	**G**	Configure Control Port.	switch(config)#**ring controlport 2**
ring homingport [Dual Homing Port]	**G**	Configure Dual Homing Port.	switch(config)#**ring homingport 3**
ring dualring	**G**	Configure Dual Ring	switch(config)#**ring dualring**
ring dualport	**G**	Configure Dual Ring port	switch(config)#**ring dualport 3 4**
show ring	**P**	Show the information of X - Ring.	switch#**show ring**
no ring	**G**	Disable X-Ring.	switch(config)#**no ring**
no ring master	**G**	Disable Ring Master.	switch(config)# **no ring master**
no ring couplering	**G**	Disable Couple Ring.	switch(config)# **no ring couplering**
no ring dualhoming	**G**	Disable Dual Homing.	switch(config)# **no ring dualhoming**
no ring dualring	**G**	Disable Dual Ring	switch(config)# **no ring dualring**

C-17 LLDP Commands Set

Commands	Level	Description	Example
lldp enable	**G**	Enable LLDP function	switch(config)#lldp enable
lldp interval [TIME sec]	**G**	Configure LLDP interval	switch(config)#lldp interval 10
no lldp	**G**	Disable LLDP function	switch(config)#no lldp
show lldp	**G**	Show LLDP function	switch#show lldp

C-18 PoE Commands Set

Commands	Level	Description	Example
poe	**P**	Enter POE configure mode	switch#poe
system power-limit [Value] Parameter only [0~400]		Set PoE system System Power Limit	switch(poe)# system power-limit 350
system knockoff-disabled [Enable|Disable]		Set PoE system Port Knockoff Disabled	switch(poe)# system knockoff-disabled disable
system ac-dissconnect [Enable|Disable]		Set PoE system AC Dissconnect	switch(poe)# system ac-dissconnect disable
system capacitive-detect [Enable|Disable]		Set PoE system Capacitive Detection	switch(poe)# system capacitive-detect enable
port 1 state disable port [PortNumbers] stace [Enable|Disable]		Set PoE port State	switch(poe)# port 1 state disable
port 1 plfc enable port [PortNumbers] plfc [Enable|Disable]		Set PoE port Power Limit from Classification	switch(poe)# port 1 plfc enable

port 1 legacy enable port [PortNumbers] legacy [Enable|Disable]		Set PoE port Legacy	switch(poe)# port 1 legacy enable
port 1 priority high port [PortNumbers] priority [Low|High|Critical]		Set PoE port Priority	switch(poe)# port 1 priority high
port 1 powerlimit 15300 port [PortNumbers] powerlimit [Value] Parameter only [0~15400]		Set PoE port Power Limit Value	switch(poe)# port 1 powerlimit 15300
show poe	**P**	Show setting of PoE function	switch#show poe