Lantech

LPES-2208CA

User Manual

8 10/100TX + 2 100M/Giga SFP Combo w/ 8 PoE Injectors SNMP/Web Managed Switch w/X-Ring 10ms Self-Heal

Aug, 2009

Revision History

Document Release	Date	Revision	Initials
1.00	Aug 28, 2009	New Edit	Vincent

FCC Warning

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

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

CE Mark Warning

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

Content

Introduction

Power-over-Ethernet (PoE) eliminates the need to run VAC power to other devices on a wired LAN. Using Power-over-Ethernet system installers needs to run only a single Category 5 Ethernet cable that carries both power and data to each device. This allows greater flexibility in the locating of network devices and significantly decreasing installation costs in many cases.

There are two system components in PoE—the Power Sourcing Equipment (PSE) initiates the connection to the second component, and the Powered Device (PD). The current is transmitted over two of the four twisted pairs of wires in a Category-5 cable.

Power over Ethernet follows the IEEE 802.3af and is completely compatible with existing Ethernet switches and networked devices. Because the Power Sourcing Equipment (PSE) tests whether a networked device is PoE-capable, power is never transmitted unless a Powered Device is at other end of the cable. It also continues to monitor the channel. If the Powered Device does not draw a minimum current, because it has been unplugged or physically turned off, the PSE shuts down the power to that port. Optionally, the standard permits Powered Devices to signal to the PSEs exactly how much power they need.

The 8 10/100TX + 2 10/100/1000T / 100/1000Mini-GBIC Combo with 8 PoE Managed Switch is the multi-port switches that can be used to build high-performance switched workgroup networks. Any one of the switch is a store-and-forward device that offers low latency for high-speed networking. It also features a “store-and-forward “switching scheme. This allows the switch to auto-learn and store source address in an 8K-entry MAC address table. The switch is targeted at workgroup, department or backbone computing environment.

Features

- System Interface/Performance
  - RJ-45 ports support Auto MDI/MDI-X Function
  - Embedded 8-port PoE function
  - Store-and-Forward Switching Architecture
  - Back-plane (Switching Fabric): 5.6Gbps
  - 1Mbits Packet Buffer
  - 8K MAC Address Table
- VLAN
  - Port Based VLAN
  - Supports 802.1 Q Tag VLAN
  - GVRP
- Port Trunk with LACP
- QoS (Quality of Service)
  - Supports IEEE 802.1p Class of Service
  - Per port provides 4 priority queues
  - Port Base, Tag Base and Type of Service Priority
- Port Mirror: Monitor traffic in switched networks.
  - TX Packet only
  - RX Packet only
  - Both of TX and RX Packet
- Security
  - Port Security: MAC address entries/filter
  - IP Security: IP address security management to prevent unauthorized intruder.
  - Login Security: IEEE802.1X/RADIUS
- IGMP with Query mode for Multi Media Application
- Spanning Tree
  - Supports IEEE802.1d Spanning Tree
  - Supports IEEE802.1w Rapid Spanning Tree
- X-ring
  - X-ring, Dual Homing, and Couple Ring Topology

- Provides redundant backup feature and the recovery time below 300ms

- Bandwidth Control
  - Ingress Packet Filter and Egress Rate Limit
  - Broadcast / Multicast / Flooded Unicast Packet Filter Control
- System Event Log
  - System Log Server/Client
  - SMTP e-mail Alert
- SNMP Trap
  - Device cold start
  - Authentication failure
  - X-ring topology changed
  - Port Link up/Link down
- TFTP Firmware Update and System Configuration Restore and Backup

Hardware Feature

Standard	IEEE802.3 10Base-T IEEE 802.3u 100Base-TX IEEE 802.3z Gigabit fiber IEEE 802.3ab 1000Base-T IEEE 802.3x Flow control and Back pressure IEEE 802.3ad Port trunk with LACP IEEE 802.1d Spanning tree protocol IEEE 802.1w Rapid spanning tree IEEE 802.1p Class of service IEEE 802.1Q VLAN Tagging IEEE 802.1x user authentication IEEE 802.3af Power Over Ethernet
Switch architecture	Back-plane (Switching Fabric): 5.6Gbps Packet throughput ability (Full-Duplex): 8.3Mpps @64bytes
Transfer Rate	14,880pps for Ethernet port 148,800pps for Fast Ethernet port 1,488,000pps for Gigabit Ethernet port
Packet Buffer	1Mbits
MAC address	8K MAC address table
Flash ROM	4Mbytes
DRAM	32Mbytes

Connector	100Base-T: 8x RJ-45 with auto MDI/MDI-X and PoE inject function 10/100/1000T/ 100/1000Mini-GBIC Combo: 2 x RJ-45 + 2 x 100/1000 SFP sockets
PoE Pin Assignment	RJ-45 port # 1~# 8 support IEEE 802.3af End-point, Alternative A mode. Per port provides 15.4W ability Positive (VCC+): RJ-45 pin 1, 2 Negative (VCC-): RJ-45 pin 3, 6
LED	System Power (Green) 10/100TX Port: Link/Activity (Green), 100Mbps (Green), PoE (Green). Gigabit copper port: 1000/100Mbps (Green), Link/Activity (Green), 100/1000Mini-GBIC: Link/Activity (Green).
RS-232 Connector	One RS-232 DB-9 Female connector for switch management
Power	100 ~ 240V_{AC}, 50/60 Hz External Power
Power Consumption	81.3 Watts for the system (maximum)
Ventilation	Fanless
Operating Environment	0^{o}C ~ 40^{o}C, 5%~95%RH

Storage Environment	-40°C ~ 70°C, 5%~95%RH
Dimensions	217mm(W) x 43mm(H) x 140mm(D)
EMI	FCC Class A CE
Safety	LVD

Software Feature

Management	SNMP v1 SNMP v2c SNMP v3 Web/Telnet/Console (CLI)
VLAN	Port based VLAN IEEE802.1Q Tag VLAN(256 entries) / VLAN ID(Up to 4K, VLAN ID can be assigned from 1 to 4094) GVRP (256 Groups)
Port Trunk with LACP	LACP Port Trunk: 4 trunk groups of maximum 4 trunk members
Spanning Tree	IEEE802.1d Spanning tree IEEE802.1w Rapid spanning tree
X-ring	Supports X-ring, Dual Homing, and Couple Ring Provides redundant backup feature and recovery time below 300ms
Quality of service	The quality of service determined by port, Tag and IPv4 Type of service, IPv4 Different Service
Class of Service	Supports IEEE802.1p class of service, per port provides 4 priority queues
Port Security	Supports100 entries of MAC address for static MAC and another 100 for MAC filter

Port Mirror	Supports 3 mirroring types: “RX, TX and Both packet”
IGMP	Supports IGMP snooping v1 and v2 256 multicast groups IGMP query mode
IP Security	Supports 10 IP addresses that have permission to access the switch management to prevent unauthorized intruder
Bandwidth Control	Ingress rate limiting packet type: all of frames, broadcast, multicast, Flooded Unicast and broadcast packet. Egress rate shaping supports all of packet. Rate limiting levels: 100kbps to 102400kbps or up to 256Mbps for Gigabit port.
Login Security	Supports IEEE802.1x User Authentication and can report to RADIUS server
Flow Control	Supports Flow Control for Full-duplex and Back Pressure for Half-duplex
System log	Supports System log record and remote system log server
SMTP	Supports SMTP Server and 6 email accounts for receiving event alert
SNMP Trap	1. Device cold start 2. Authentication failure 3. X-ring topology changed 4. Port Link up/Link down

	Trap station up to 3
DHCP	Provide DHCP Client/DHCP Server/IP Binding functions
DNS	Provides DNS client feature and supports Primary and Secondary DNS server
SNTP	Supports Simple Network Time Protocol to synchronize system clock in Internet
Firmware Upgrade	Supports TFTP firmware upgrade
Configuration Upload and Download	Supports binary format configuration file for system quick installation (TFTP backup and restore)

Package Contents

Unpack the packing of the PoE Managed Switch then verify them against the checklist below.

- PoE Managed Switch x 1
- Rubber Pads x 4
- RS-232 cable x 1
- Power Adaptor x 1
- Power Cord x 1
- User Manual x 1

Compare the contents of the package with the standard checklist above. If any item is missing or damaged, please contact the local dealer for exchanging.

Hardware Description

This section mainly describes the hardware of the PoE Managed Switch and gives a physical and functional overview on the certain switch.

Physical Dimension

The physical dimensions of *8 10/100TX + 2 10/100/1000T / 100/1000Mini-GBIC Combo with 8 PoE Managed Switch* are **217mm(W) x 43mm(H) x 140mm(H)**.

Front Panel

The front panel of the 8 10/100TX + 2 10/100/1000T / 100/1000Mini-GBIC Combo with 8 PoE Managed Switch consists of 8 x 10/100Base-TX RJ-45 Ethernet ports (Auto MDI/MDIX), 2 Gigabit combo ports involve 2 10/100/1000Mbps Ethernet RJ-45 port (automatic MDI/MDIX) and 2 100/1000 Mini-GBIC ports. The LED Indicators are also located on the front panel of the switch.

The Front panel of the 8 10/100TX + 2 10/100/1000T / 100/1000Mini-GBIC Combo with 8 PoE Managed Switch

- **RJ-45 Ports:** There are 8 10/100 N-way auto-sensing for 10Base-T or 100Base-TX connections and 2 10/100/1000Mbps auto-sensing for 1000Base-T connection RJ-45 ports. The 8 10/100 ports also can supply power to PDs.

  In general, **MDI** means connecting to another Hub or Switch while **MDIX** means connecting to a workstation or PC. Therefore, **Auto MDI/MDIX** would allow connecting to another switch or workstation without changing non-crossover or

crossover cabling.

- **Mini-GBIC port:** The appropriate replaceable Mini-GBIC port is available with a variety of different transmitter and receiver types, allowing users to select the appropriate transceiver for each link to provide the required optical reach over the available optical fiber type.

LED indicators

LED	Status	Description
Power	Green	Power On
	OFF	No power inputs
PoE (port 1~8)	Green	The port is supplying power to the connected powered-device
	OFF	No powered device attached or power supplying failed
LNK/ACT (port 1~10) *(Port 9 lower LED, Port10 upper LED)*	Green	Connected to network
	Blinking	Networking is active
	OFF	Not connected to network
100M (port 1~8)	Green	The port is operating at speed of 100M
	OFF	The port is disconnected or not operating at speed of 100M

Rear Panel

The power plug is located on the rear panel of the 8 10/100TX + 2 10/100/1000T / 100/1000Mini-GBIC Combo with 8 PoE Managed Switch as shown below. The switch will work with AC in the voltage range of AC 100-240V with Frequency of 50-60Hz.

The Rear Panel of 8 10/100TX + 2 10/100/1000T / 100/1000Mini-GBIC Combo with 8 PoE Managed Switch

Desktop Installation

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

Attaching Rubber Pads

A. Make sure mounting surface on the bottom of the switch is grease and dust free.
B. Remove adhesive backing from your Rubber Pads.
C. Apply the Rubber Pads to each corner on the bottom of the switch. These footpads can prevent the switch from shock/vibration.

Power On

Connect the DC jack to the power socket on the rear panel of the switch. Connect the other side of power plug to the power outlet. The power adaptor works with voltage range of AC in the 100-240V_{AC}/Frequency of 50~60Hz for 8 10/100TX + 2 10/100/1000T / 100/1000Mini-GBIC Combo with 8 PoE Managed Switch. Check the power indicator on the front panel to see if power is properly supplied.

Network Application

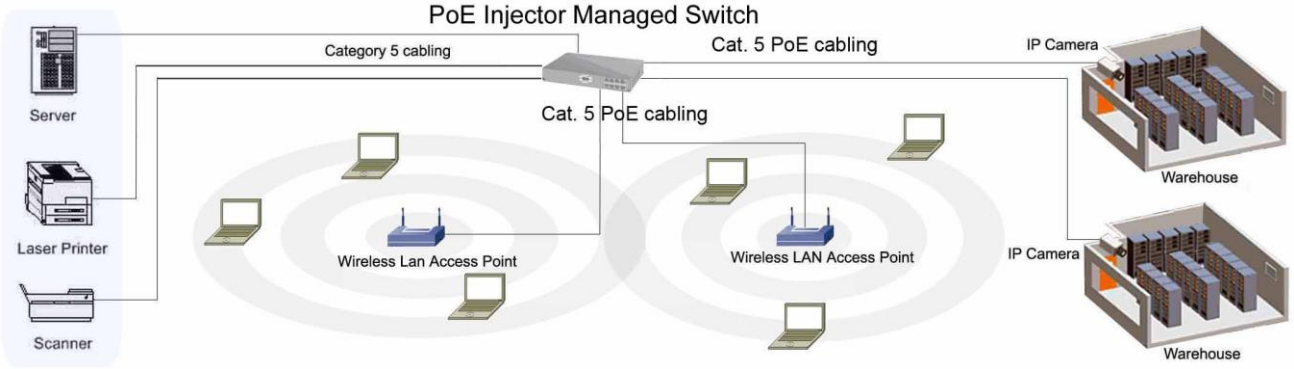
This section provides a few samples of network topology in which the switch is used. In general, the PoE Managed Switch is designed as a segment switch which has large address table (8k MAC addresses) and high performance to deal with interconnecting networking segments.

Using the uplink port (Giga Combo port), the switch can connect with another switch or hub to interconnect other small-switched workgroups to form a larger switched network. Besides, the PoE switch also injects power into the UTP cables for supplying the power that PDs (Power Devices) need.

The Power over Ethernet Switch can provide power to PDs that follow the IEEE 802.3af standard in the network. It can solve the problem of position limitation. The network devices can be installed in more appropriate position for better performance. The following figure is an example of network application for Power over Ethernet Switch.

Small Workgroup

The PoE managed switch can be used as a standalone switch to which personal computers, server, printer server, are directly connected to form a small workgroup.

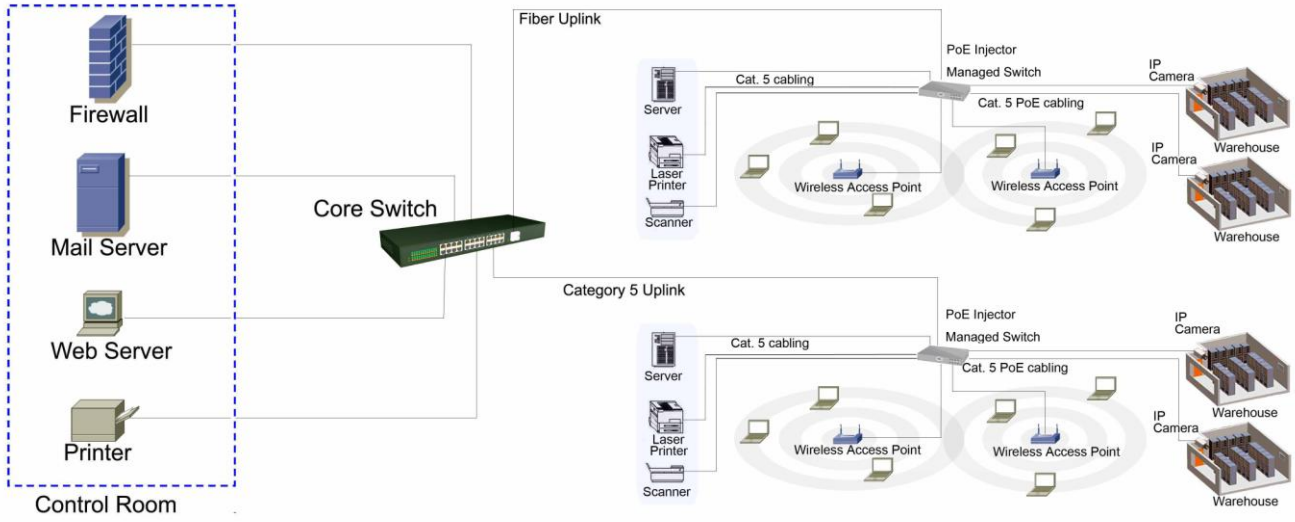


Small Workgroup application

Segment Bridge

For enterprise networks where large data broadcasts are constantly processed, this switch is an ideal solution for department users to connect to the corporate backbone.

In the illustration below, two managed PoE switches with PCs, print server, local server, wireless AP (IEEE 802.3af compliant), and IP camera (IEEE 802.3af compliant) attached are both connect to the core switch. All the devices in this network can communicate with each other through the core switch.



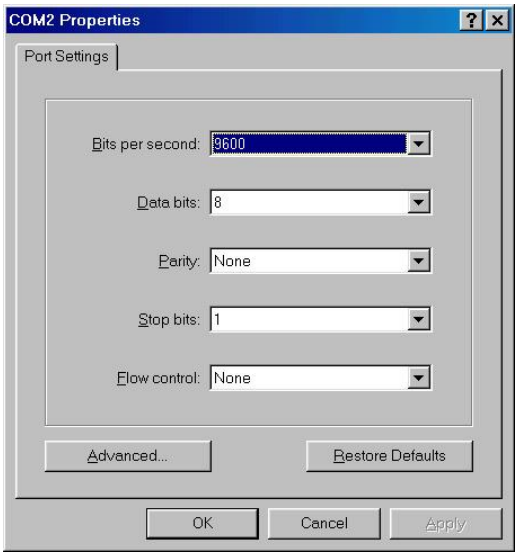
Segment Bridge application

Console Management

Login in the Console Interface

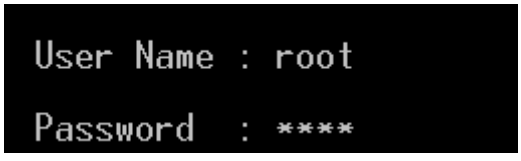
When the connection between switch and PC is ready, turn on the PC and run a terminal emulation program or **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

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



The settings of communication parameters

After having finished the parameter settings, click "**OK**". When the blank screen shows up, press Enter key to bring forth the login prompt. Key in the '**root**' (default value) for both User name and Password (use **Enter** key to toggle), then hit Enter key and the console management appears right after. Please see the figure below for login screen.



Console login screen

CLI Management

The system supports console management—CLI command. After you log in to the system, you will see a command prompt. To enter CLI management interface, enter "**enable**" command. The following table lists the CLI commands and description.

CLI command interface

Commands Level

Modes	Access Method	Prompt	Exit Method	About This Mode1
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 in advanced mode Privileged 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 parameters that apply to your switch as a whole.
VLAN database	Enter the vlan database command while in privileged EXEC mode.	switch (vlan)#	To exit to user EXEC mode, enter exit.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the interface command (with a specific interface) while in global configuration mode	switch (config-if) #	To exit to global configuration mode, enter exit. To exist to privileged EXEC mode, or end.	Use this mode to configure parameters for the switch and Ethernet ports.
PoE	Enter the PoE command while in privileged EXEC mode.	switch(PoE) #	To exit to privileged EXEC mode, enter exit	Use this mode to PoE parameters for the switch.

Commands Set List

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

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]**	**G**	Configure the IP address of switch	switch(config)#**ip address 192.168.16.1 255.255.255.0 192.168.16.254**

[Gateway]			
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 lowip [Low IP]	**G**	Configure low IP address for IP pool	switch(config)#**dhcpserver lowip 192.168.1.100**
dhcpserver highip [High IP]	**G**	Configure high IP address for IP pool	switch(config)#**dhcpserver highip 192.168.1.200**
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 192.168.1.254**
dhcpserver dnsip [DNS IP]	**G**	Configure DNS IP for DHCP clients	switch(config)#**dhcpserver dnsip 192.168.1.1**
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 192.168.1.1**
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 1 192.168.1.55**
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**

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 1000 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,	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type**

		multicast, and flooded unicast frame'	**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	switch(config)#**interface fastEthernet 2** switch(config-if)#**state Disable**

		the state mode of 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**

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**	**G**	Assign a trunk group with LACP active. [GroupID] :1~4	switch(config)#**aggregator group 1 1-4 lacp workp 2** or

workp **[Workport]**		[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 2 1,4,3 lacp workp 3**
aggregator group **[GroupID] [Port-list]** **nolacp**	**G**	Assign a static trunk group. [GroupID] :1~4 [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**

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	switch(vlan)#**vlan 8021q port 3 access-link untag 33**

		can't be applied.	
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** [TaggedVID List]	**V**	Assign a trunk link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 trunk-link tag 2,3,6,99** or 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**

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 recomputed 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	switch(config)#**spanning-tree forward-time 20**

		specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins 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(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-priority 128**

		switch.	
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**

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**	Setting of 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**

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 enable	**G**	Set IGMP query to enable mode	switch(config)#**Igmp query enable**
show igmp configuration	**P**	Displays the details of an IGMP configuration.	switch#**show igmp configuration**
igmp multi	**P**	Show IGMP multicast	switch#**show igmp multi**

		table	
no igmp	**G**	Disable IGMP snooping function	switch(config)#**no igmp**
no igmp query	**G**	Disable IGMP query	switch#**no igmp query**

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**

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 [Community] **right** [RO/RW]	G	Add SNMP community string.	switch(config)#**snmp 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]	**G**	Remove specified access table of SNMPv3 agent.	switch(config)#**no snmpv3 access context-name Test group G1 security-level AuthPr**

group [Group Name] **security-level** [NoAuthNoPriv|AuthNoPriv|AuthPriv] **match-rule** [Exact|Prifix] **views** [Read View Name] [Write View Name] [Notify View Name]			**iv match-rule Exact views V1 V1 V1**
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**

Port Mirroring Commands Set

Commands	Level	Description	Example
monitor rx	**G**	Set RX destination port of monitor function	switch(config)#**monitor rx**
monitor tx	**G**	Set TX destination port of monitor function	switch(config)#**monitor tx**
show monitor	**P**	Show port monitor information	switch#**show monitor**
monitor [RX|TX|Both]	**I**	Configure source port of monitor function	switch(config)#**interface fastEthernet 2** switch(config-if)#**monitor RX**
show monitor	**I**	Show port monitor	switch(config)#**interface**

		information	**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**

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	switch(config)# **8021x system sharedkey 123456**

		the shared key value.	
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**	Displays 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**

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

flash:upgrade_fw		TFTP and need to specify the IP of TFTP server and the file name of image.	**flash:upgrade_fw**

PoE Commands Set

Commands	Level	Description	Example
poe	**P**	Enter POE configure mode	switch#**poe**
system knockoff-disabled [Enable|Disable]	**P**	Set PoE system Port Knockoff Disabled	switch(poe)# **system knockoff-disabled disable**
system ac-disconnect [Enable|Disable]	**P**	Set PoE system AC Disconnect	switch(poe)# **system ac-disconnect disable**
system capacitive-detect [Enable|Disable]	**P**	Set PoE system Capacitive Detection	switch(poe)# **system capacitive-detect enable**
system power-limit [Value] Value[0~96]	**P**	Set Poe system Power Limit	switch(poe)# **system power-limit 90**
port 1 state disable port [PortNumbers] stace [Enable|Disable]	**P**	Set PoE port State	switch(poe)# **port 1 state disable**
port 1 plfc enable port [PortNumbers] plfc [Enable|Disable]	**P**	Set PoE port Power Limit from Classification	switch(poe)# **port 1 plfc enable**
port 1 legacy enable port [PortNumbers] legacy [Enable|Disable]	**P**	Set PoE port Legacy	switch(poe)# **port 1 legacy enable**
port 1 priority high port [PortNumbers]	**P**	Set PoE port Priority	switch(poe)# **port 1 priority high**

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

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 192.168.1.100**
systemlog mode [client|server|both]	**G**	Specified the log mode	switch(config)# **systemlog mode both**
show systemlog	**E**	Displays system log.	Switch>**show systemlog**
show systemlog	**P**	Show system log client & server information	switch#**show systemlog**
no systemlog	**G**	Disable systemlog functon	switch(config)#**no systemlog**
smtp enable	**G**	Enable SMTP function	switch(config)#**smtp enable**
smtp sender	**G**	Configuration SMTP server IP	switch(config)#smtp sender aaa@bbb.ccc
smtp serverip [IP address]	**G**	Configure SMTP server IP	switch(config)#**smtp serverip 192.168.1.5**
smtp authentication	**G**	Enable SMTP authentication	switch(config)#**smtp authentication**
smtp account [account]	**G**	Configure authentication account	switch(config)#**smtp account User**
smtp password [password]	**G**	Configure authentication	switch(config)#**smtp password**

		password	
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 typ	switch(config)#**no event authentication-failure**
no event ring-topology-change	**G**	Disable X-ring topology changed event type	switch(config)#**no event 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**

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	switch(config)#**sntp timezone 22**

		timzezone' command to get more information of index number	
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**

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**
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**

Web-Based Management

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

About Web-based Management

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

The Web-Based Management supports Internet Explorer 6.0 or later version. And, it is applied for Java Applets for reducing network bandwidth consumption, enhance access speed and present an easy viewing screen.

Preparing for Web Management

Before using web management, user can log in to the switch to check the default IP of the switch via the console. Please refer to **Console Management** Chapter for console login. If user needs to change IP address for the first time, user can use console mode to modify it. The default value is as below:

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

System Login

1. Launch the Internet Explorer on the PC
2. Key in “http:// “+” the IP address of the switch”, and then Press “**Enter**”.

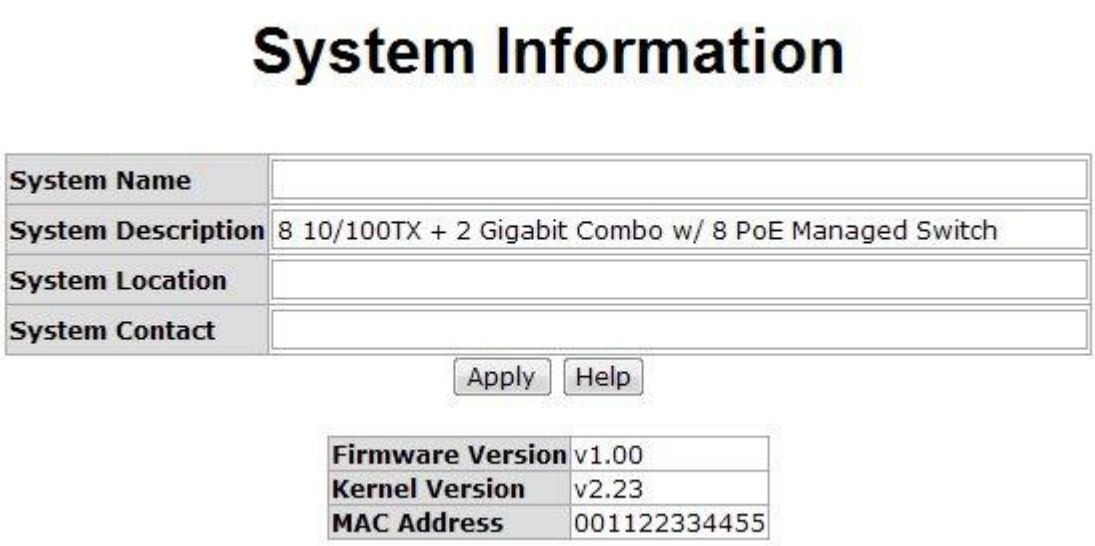
3. The login screen will appear right after
4. Key in the user name and password. The default user name and password are the same as ‘**root**’.
5. Press **Enter** or click the **OK** button, and then the home screen of the Web-based management appears.

Note: The web interface features shown below are introduced by the screen displays of 8 10/100TX + 2 10/100/1000T / 100/1000Mini-GBIC Combo model. Unless specifically identified, all of the screen displays are suitable for the switches involved in this manual.

System Information

User can assign the system name, description, location and contact personnel to identify the switch. The version table below is a read-only field to show the basic information of the switch.

- **System Name:** Assign the system name of the switch (The maximum length is 80 bytes)
- **System Description:** Describes the switch (The maximum length is 80 bytes).
- **System Location:** Assign the switch physical location (The maximum length is 80 bytes).
- **System Contact:** Enter the name of contact person or organization (The maximum length is 80 bytes).
- **Firmware Version:** Displays the switch's firmware version
- **Kernel Version:** Displays the kernel software version
- **MAC Address:** Displays the unique hardware address assigned by manufacturer (default)
- And then, click Apply.



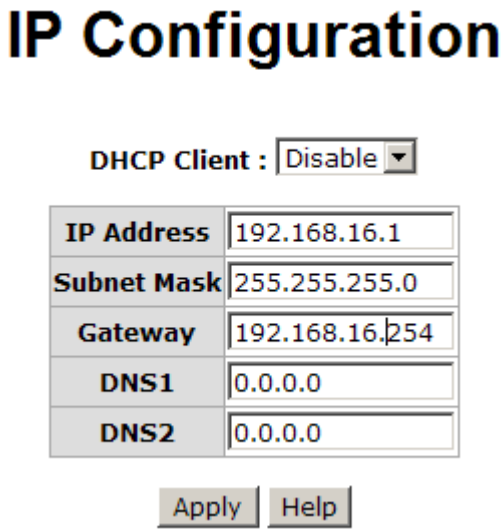
System Information interface

IP Configuration

The switch is a network device which needs to be assigned an IP address for being identified on the network. Users have to decide a means of assigning IP address to the switch.

- **DHCP Client:** Enable or disable the DHCP client function. When DHCP client function is enabled, the switch will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address on DHCP server. After the user clicks **Apply**, a popup dialog shows up to inform the user that when the DHCP client is enabled, the current IP will lose and user should find the new IP on the DHCP server.
- **IP Address:** Assign the IP address that the network is using. If DHCP client function is enabled, this switch is configured as a DHCP client. The network DHCP server will assign the IP address to the switch and display it in this column. The default IP is 192.168.16.1 or the user has to assign an IP address manually when DHCP Client is disabled.
- **Subnet Mask:** Assign the subnet mask to the IP address. If DHCP client function is disabled, the user has to assign the subnet mask in this column field.
- **Gateway:** Assign the network gateway for the switch. If DHCP client function is disabled, the user has to assign the gateway in this column field. The default gateway is 192.168.16.254.
- **DNS1:** Assign the primary DNS IP address.
- **DNS2:** Assign the secondary DNS IP address.
- And then, click 

.



IP Configuration interface

DHCP Configuration

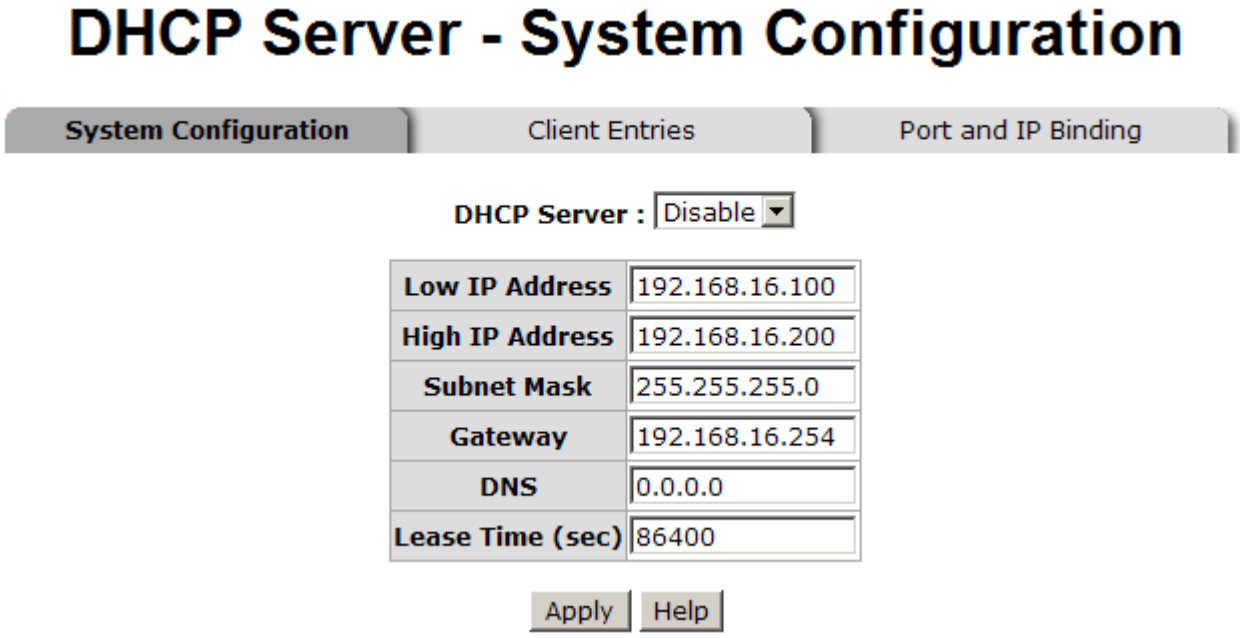
DHCP is the abbreviation of Dynamic Host Configuration Protocol that is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

The system provides the DHCP server function. Having enabled the DHCP server function, the switch system will be configured as a DHCP server.

DHCP Server Configuration

The system provides the DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.

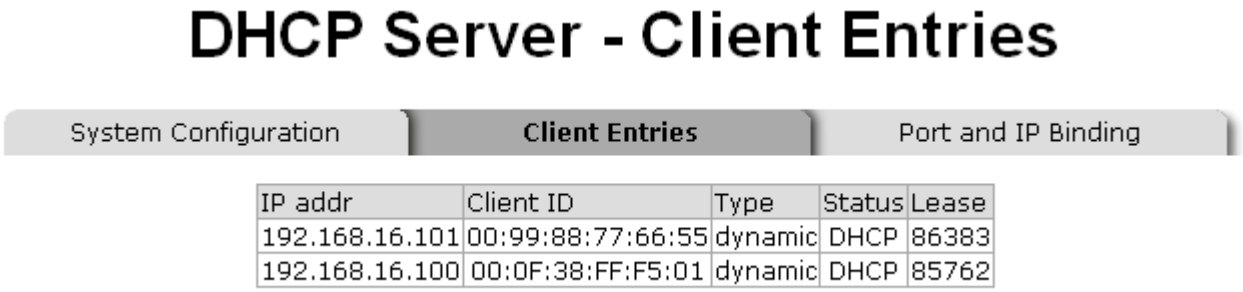
- **DHCP Server:** Enable or Disable the DHCP Server function. Enable—the switch will be the DHCP server on your local network
- **Low IP Address:** The dynamic IP range. Low IP address is the beginning of the dynamic IP range. For example: dynamic IP range is from 192.168.1.100 ~ 192.168.1.200. In contrast, 192.168.1.100 is the Low IP address
- **High IP Address:** The dynamic IP range. High IP address is the end of the dynamic IP range. For example: dynamic IP range is from 192.168.1.100 ~ 192.168.1.200. In comparison, 192.168.1.200 is the High IP address
- **Subnet Mask:** The dynamic IP assign range subnet mask
- **Gateway:** The gateway in your network
- **DNS:** The IP Address of the Domain Name Server 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 been occupied for a long time or the server doesn't know that the dynamic IP is idle



DHCP Server Configuration interface

DHCP Client Entries

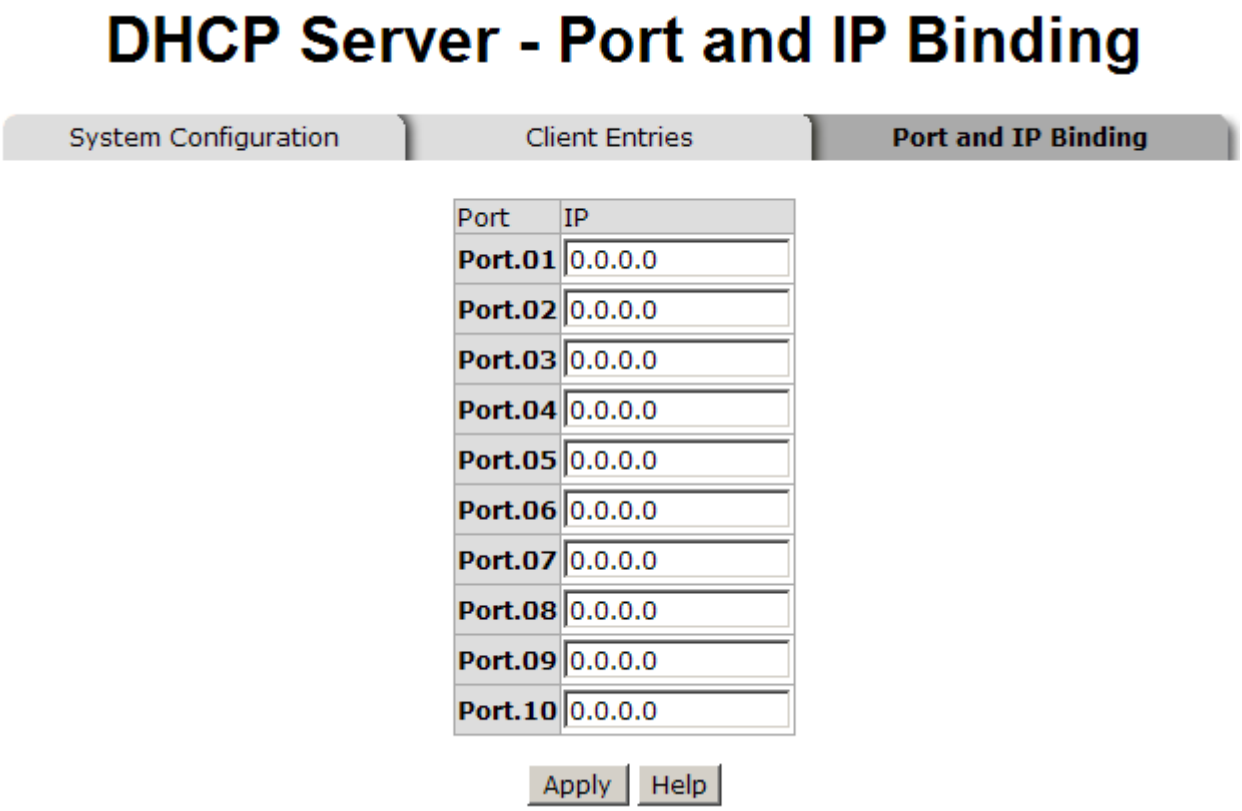
When the DHCP server function is enabled, the system will collect the DHCP client information including the assigned IP address, the MAC address of the client device, the IP assigning type, status and lease time.



DHCP Client Entries interface

Port and IP Binding

Assign the dynamic IP address bound with the port to the connected client. The user is allowed to fill each port column with one particular IP address. When the device is connecting to the port and asks for IP assigning, the system will assign the IP address bound with the port.

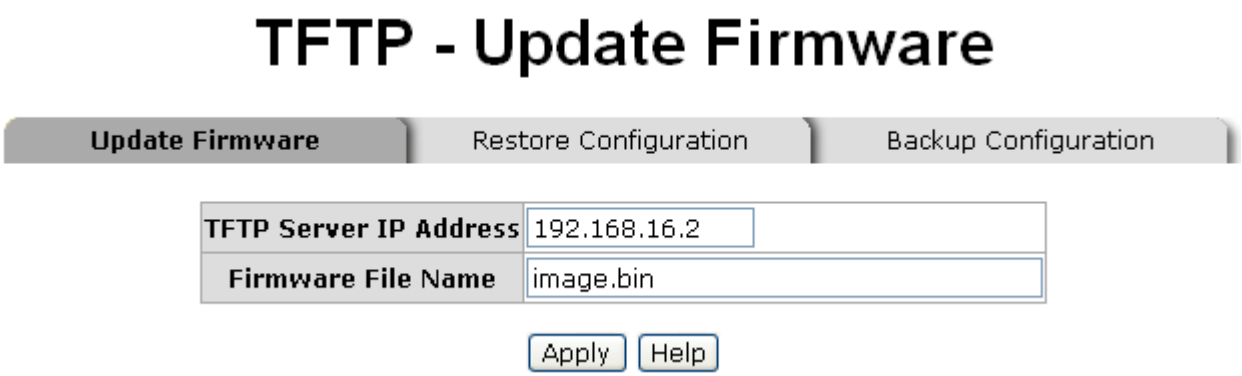


Port and IP Bindings interface

TFTP - Update Firmware

It provides the functions allowing the user to update the switch firmware via the Trivial File Transfer Protocol (TFTP) server. Before updating, make sure the TFTP server is ready and the firmware image is located on the TFTP server.

- **TFTP Server IP Address:** Key in the TFTP server IP
- **Firmware File Name:** The name of firmware image
- And then, click Apply.

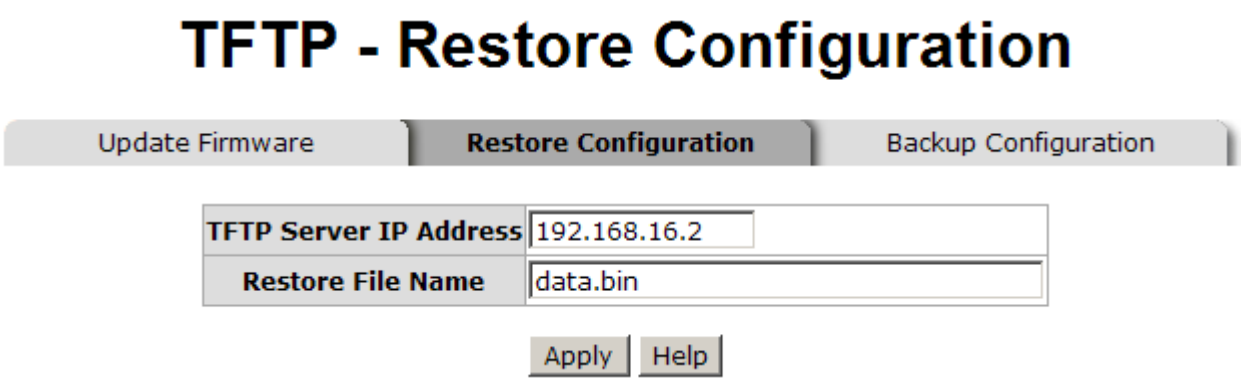


Update Firmware interface

TFTP - Restore Configuration

You can restore a previous backup configuration from the TFTP server to recover the settings. Before doing that, you must locate the image file on the TFTP server first and the switch will download back the flash image.

- **TFTP Server IP Address:** Type in the TFTP server IP.
- **Restore File Name:** Type in the correct file name for restoring.
- Click Apply.

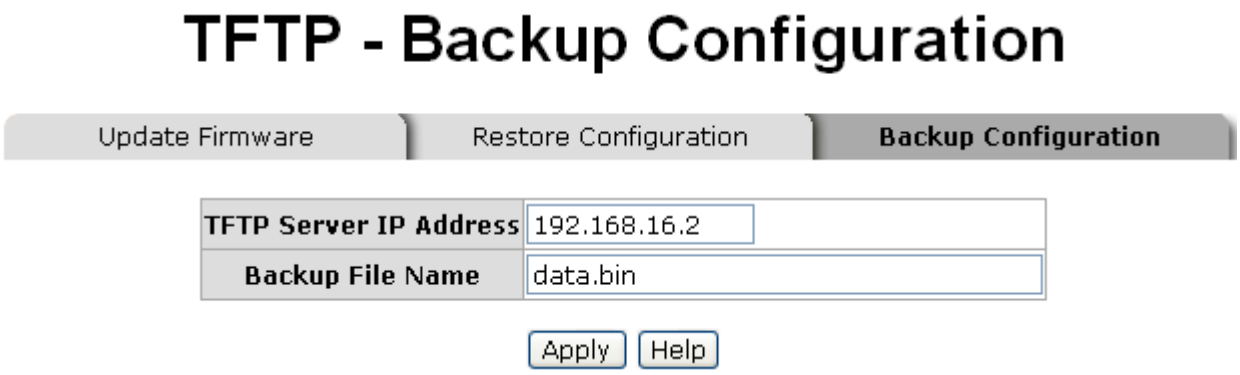


Restore Configuration interface

TFTP - Backup Configuration

You can back up the current configuration from flash ROM to the TFTP server for the purpose of recovering the configuration later. It helps you to avoid wasting time on configuring the settings by backing up the configuration.

- **TFTP Server IP Address:** Type in the TFTP server IP.
- **Backup File Name:** Type in the file name.
- Click Apply.



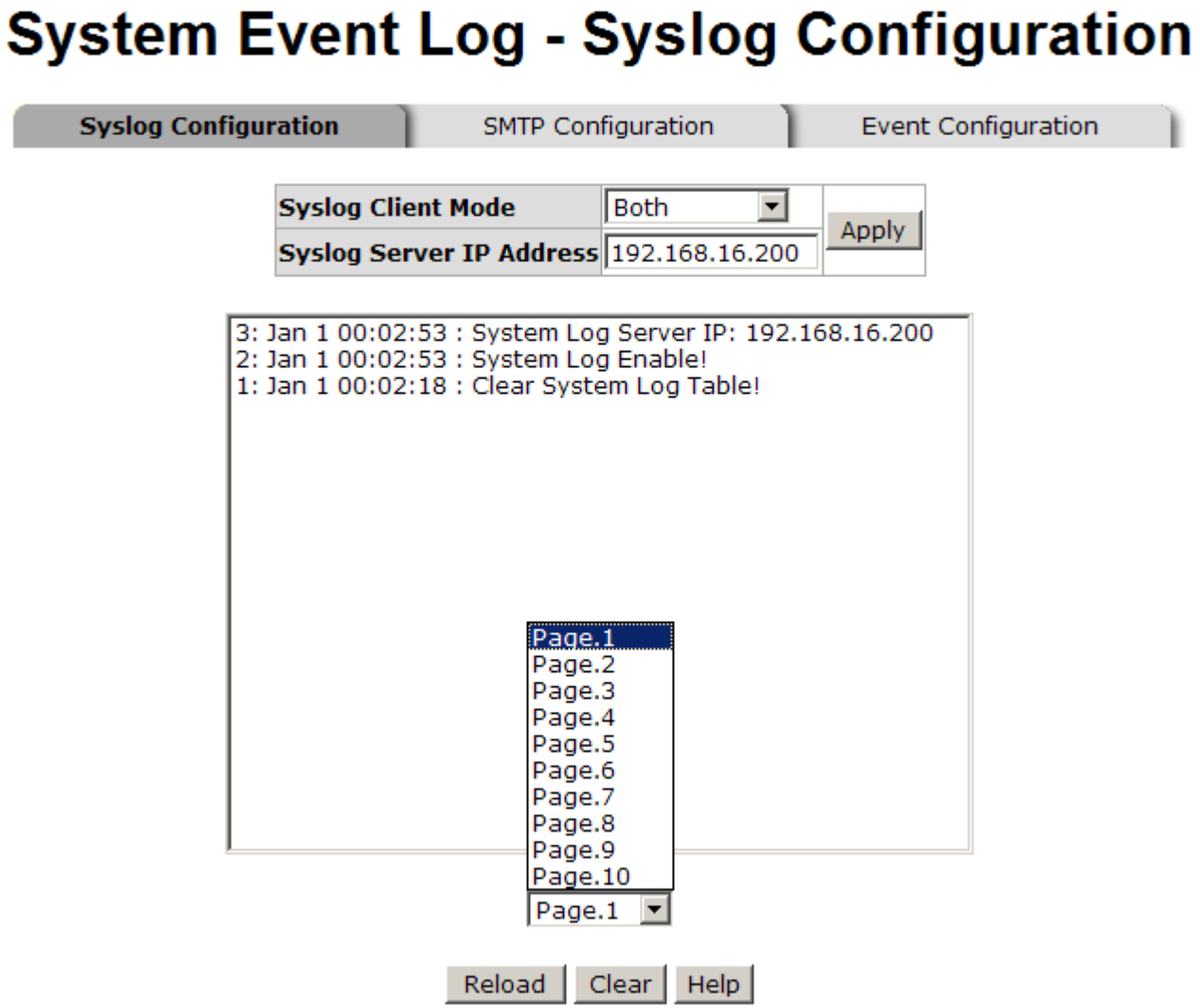
Backup Configuration interface

System Event Log Configuration

This page allows the user to decide whether to send the system event log, and select the mode which the system event log will be sent to client only, server only, or both client and server. What kind of event log will be issued to the client/server depends on the selection on the **Event Configuration** tab. There are four types of event—Device Cold Start, Authentication Failure, X-Ring Topology Change, and Port Event—available to be issued as the event log.

System Event Log—Syslog Configuration

- **Syslog Client Mode:** Select the system log mode—**Client Only**, **Server Only**, or **Both**. 'Client Only' means the system event log will only be sent to this interface of the switch, but on the other hand 'Server Only' means the system log will only be sent to the remote system log server with its IP assigned. If the mode is set in 'Both', the system event log will be sent to the remote server and this interface.
- **System Log Server IP Address:** When the 'Syslog Mode' item is set as Server Only/Both, the user has to assign the system log server IP address to which the log will be sent.
- Click Reload to refresh the event log displaying area.
- Click Clear to clear all the current event logs.
- Make sure the selected mode is correct, and click Apply to have the setting take effect.

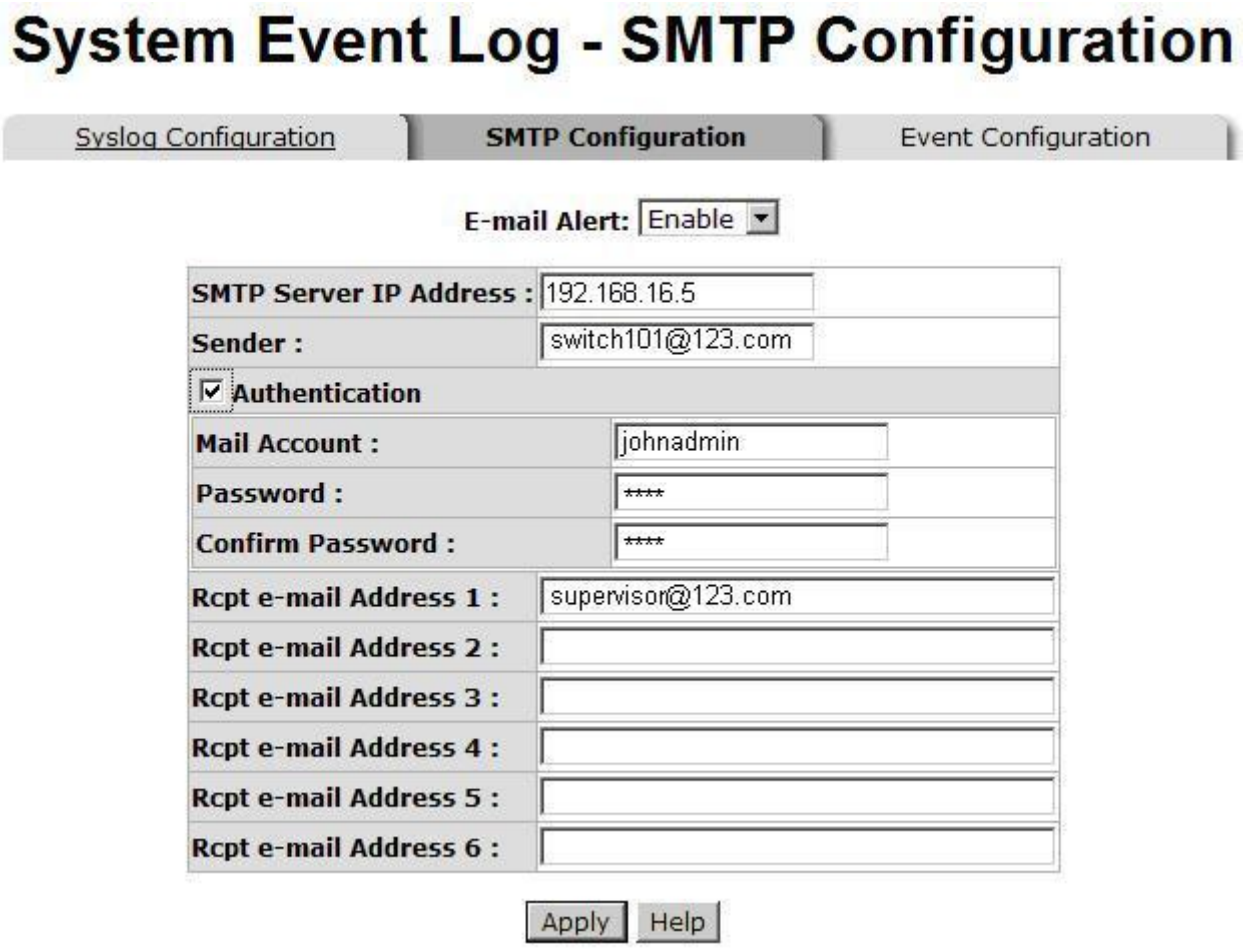


Syslog Configuration interface

System Event Log—SMTP Configuration

Simple Mail Transfer Protocol (SMTP) is the standard for email transmissions across the network. You can configure the SMTP server IP, sender, mail account, password, and the recipient email addresses which the e-mail alert will send to. There are also four types of event—Device Cold Start, Authentication Failure, X-Ring Topology Change, and Port Event—available to be issued as the e-mail alert. Besides, this function provides the authentication mechanism including an authentication step through which the client effectively logs in to the SMTP server during the process of sending e-mail alert.

- **Email Alert:** With this function being enabled, the user is allowed to configure the detail settings for sending the e-mail alert to the SMTP server when the events occur.
- **SMTP Server IP:** Assign the mail server IP address (when **Email Alert** is 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:** Having ticked this checkbox, the mail account, password and confirm password column fields will then show up. Configure the email account and password for authentication when this switch logs in to the SMTP server.
- **Mail Account:** Set up the email account, e.g. johnadmin, to receive the email alert. It must be an existing email account on the mail server.
- **Password:** Type in the password for the email account.
- **Confirm Password:** Reconfirm the password.
- **Rcpt e-mail Address 1 ~ 6:** You can also fill each of the column fields with up to 6 e-mail accounts to receive the email alert.
- Click Apply to have the configuration take effect.



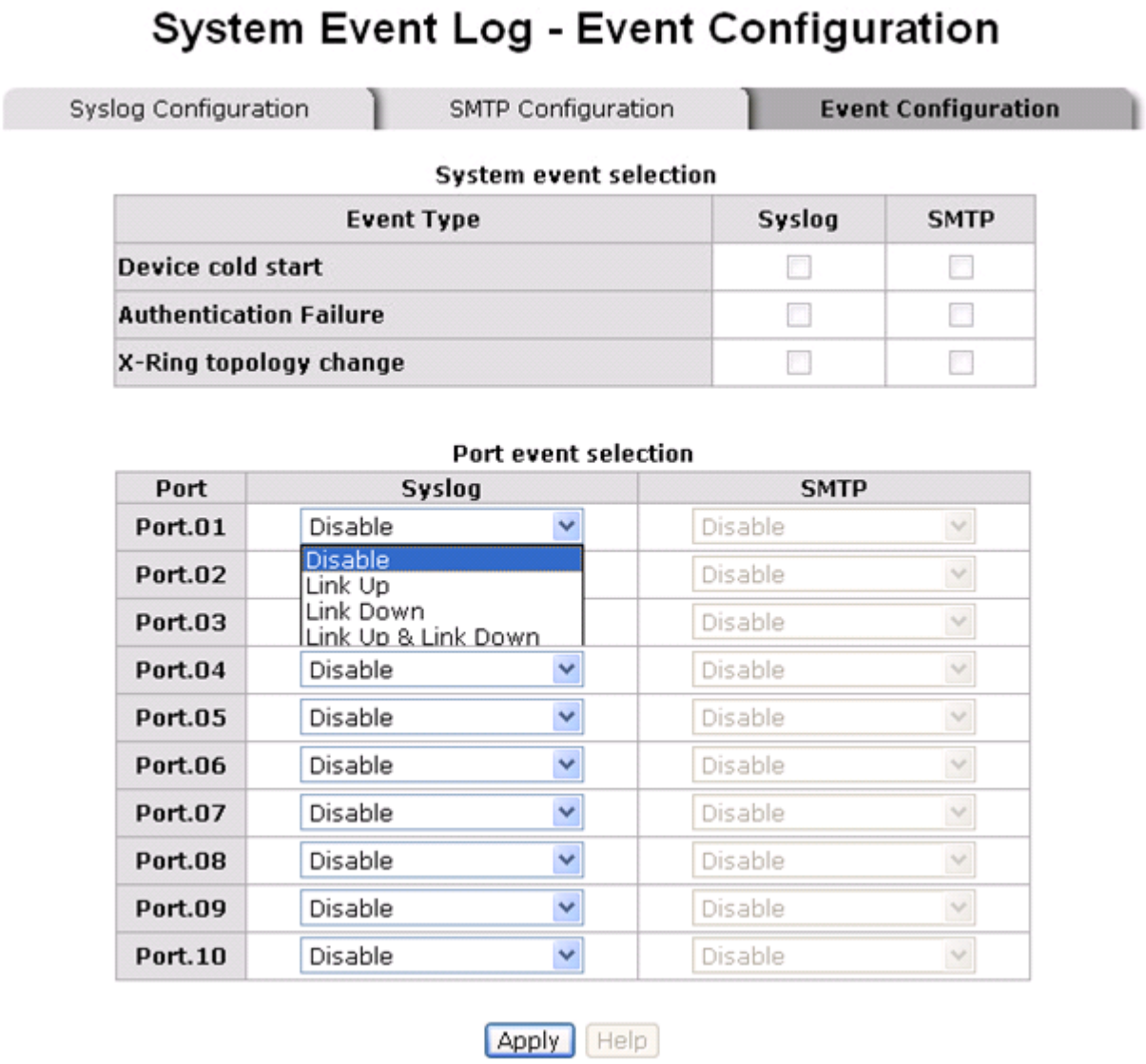
SMTP Configuration interface

System Event Log—Event Configuration

Having ticked the **Syslog**/**SMTP** checkboxes, the event log/email alert will be sent to the system log server and the SMTP server respectively. Also, Port event log/alert (link up, link down, and both) can be sent to the system log server/SMTP server respectively by setting the trigger condition.

- **System event selection:** There are 3 event types—Device Cold Start, Authentication Failure, and X-ring Topology Change. The checkboxes are not available for ticking unless the **Syslog Client Mode** on the Syslog Configuration tab and the **E-mail Alert** on the SMTP Configuration tab are enabled first.
  - **Device cold start:** When the device executes cold start action, the system will issue the event log/email alert to the system log/SMTP server respectively.
  - **Authentication Failure:** When the SNMP authentication fails, the system will issue the event log/email alert to the system log/SMTP server respectively.
  - **X-ring topology change:** When the X-ring topology has changed, the system will issue the event log/email alert to the system log/SMTP server respectively.

- **Port event selection:** Also, before the drop-down menu items are available, the **Syslog Client Mode** selection item on the Syslog Configuration tab and the **E-mail Alert** selection item on the SMTP Configuration tab must be enabled first. Those drop-down menu items have 3 selections—**Link UP**, **Link Down**, and **Link UP & Link Down**. Disable means no event will be sent to the system log/SMTP server.
  - **Link UP:** The system will only issue a log message when the link-up event of the port occurs.
  - **Link Down:** The system will only issue a log message when the link-down event of port occurs.
  - **Link UP & Link Down:** The system will issue a log message at the time when port connection is link-up and link-down.



Event Configuration interface

SNTP Configuration

SNTP (Simple Network Time Protocol) is a simplified version of NTP which is an Internet protocol used to synchronize the clocks of computers to some time reference. Because time usually just advances, the time on different node stations will be different. With the communicating programs running on those devices, it would cause time to jump forward and back, a non-desirable effect. Therefore, the switch provides comprehensive mechanisms to access national time and frequency dissemination services, organize the time-synchronization subnet and the local clock in each participating subnet peer.

Daylight saving time (DST) is the convention of advancing clocks so that afternoons have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

- **SNTP Client:** Enable/disable SNTP function to get the time from the SNTP server. *(SNTP Client default is "Disable".)*
- **Daylight Saving Time:** This is used as a control switch to enable/disable daylight saving period and daylight saving offset. Users can configure Daylight Saving Period and Daylight Saving Offset in a certain period time and offset time while there is no need to enable daylight saving function. Afterwards, users can just set this item as enable without assign Daylight Saving Period and Daylight Saving Offset again.
- **UTC Timezone:** Universal Time, Coordinated. Set the switch location time zone. The following table lists the different location time zone for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am

AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm

WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

- **SNTP Sever URL:** Set the SNTP server IP address. You can assign a local network time server IP address or an internet time server IP address.
- **Switch Timer:** When the switch has successfully connected to the SNTP server whose IP address was assigned in the column field of SNTP Server URL, the current coordinated time is displayed here.
- **Daylight Saving Period:** Set up the Daylight Saving beginning date/time and Daylight Saving ending date/time. Please key in the value in the format of 'YYYYMMDD' and 'HH:MM' (leave a space between 'YYYYMMDD' and 'HH:MM').
  - **YYYYMMDD:** an eight-digit year/month/day specification.
  - **HH:MM:** a five-digit (including a colon mark) hour/minute specification.

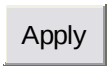
  For example, key in '20070701 02:00' and '20071104 02:04' in the two column fields respectively to represent that DST begins at 2:00 a.m. on March 11, 2007 and ends at 2:00 a.m. on November 4, 2007.
- **Daylight Saving Offset (mins):** For non-US and European countries, specify the amount of time for day light savings. Please key in the valid figure in the range of minute between 0 and 720, which means you can set the offset up to 12 hours.

- Click Apply to have the configuration take effect.

SNTP Configuration interface

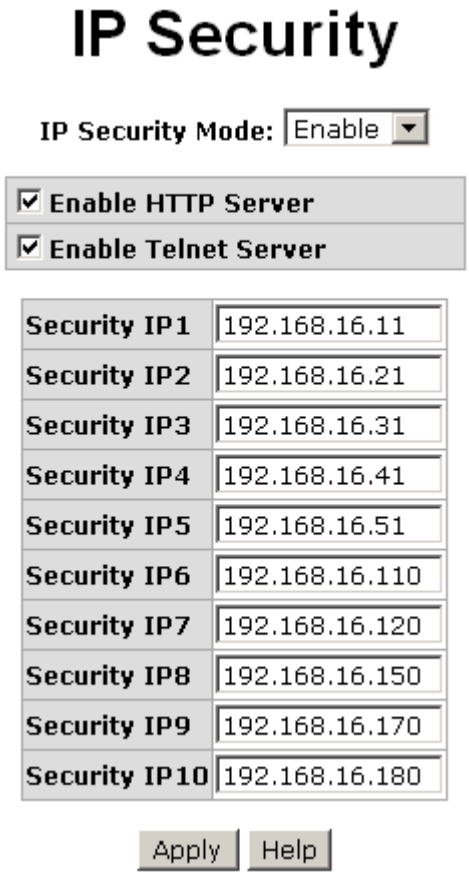
IP Security

IP security function allows the user to assign 10 specific IP addresses that have permission to manage the switch through the http and telnet services for the securing switch management. The purpose of giving the limited IP addresses permission is to allow only the authorized personnel/device can do the management task on the switch.

- **IP Security Mode:** Having set this selection item in the **Enable** mode, the **Enable HTTP Server**, **Enable Telnet Server** checkboxes and the ten security IP column fields will then be available. If not, those items will appear in grey.
- **Enable HTTP Server:** Having ticked this checkbox, the devices whose IP addresses match any one of the ten IP addresses in the Security IP1 ~ IP10 table will be given the permission to access this switch via HTTP service.
- **Enable Telnet Server:** Having ticked this checkbox, the devices whose IP addresses match any one of the ten IP addresses in the Security IP1 ~ IP10 table will be given the permission to access this switch via telnet service.
- **Security IP 1 ~ 10:** The system allows the user to assign up to 10 specific IP addresses for access security. Only these 10 IP addresses can access and manage the switch through the HTTP/Telnet service once **IP Security Mode** is enabled.
- And then, click 

to have the configuration take effect.

[NOTE] Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when the switch powers off.



IP Security interface

User Authentication

Change web management login user name and password for the management security issue.

- **User name:** Type in the new user name (The default is ‘root’)
- **Password:** Type in the new password (The default is ‘root’)
- **Confirm password:** Re-type the new password
- And then, click Apply

User Authentication interface

Port Statistics

The following chart provides the current statistic information which displays the real-time packet transfer status for each port. The user might use the information to plan and implement the network, or check and find the problem when the collision or heavy traffic occurs.

- **Port:** The index column of the ports.
- **Type:** Displays the connection media type of the port.
- **Link:** The status of linking—'**Up**' or '**Down**'.
- **State:** The user can set the state of the port as 'Enable' or 'Disable' via the **Port Control** interface the next function. When the state is disabled, the port will not transmit or receive any packet.
- **Tx Good Packet:** The counts of the transmitted good packets via this port.
- **Tx Bad Packet:** The counts of the transmitted bad packets (including undersize [less than 64 bytes], oversize, CRC Align errors, fragments and jabber packets) via this port.
- **Rx Good Packet:** The counts of the received good packets via this port.
- **Rx Bad Packet:** The counts of the received bad packets (including undersize [less than 64 bytes], oversize, CRC Align error, fragments and jabber packets) via this port.
- **Tx Abort Packet:** The aborted packet while transmitting.
- **Packet Collision:** The counts of collision packet.
- **Packet Dropped:** The counts of dropped packet.
- **Rx Bcast Packet:** The counts of broadcast packet.
- **Rx Mcast Packet:** The counts of multicast packet.
- Click  to clean all counts.

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	Up	Enable	7409	0	49631	0	0	0	0	32117	1023
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/mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.10	1GTX/mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0

Clear Help

Port Statistics interface

Port Control

In Port control you can configure the settings of each port to control the connection parameters, and the status of each port is listed beneath.

- **Port:** Use the scroll bar and click on the port number to choose the port to be configured.
- **State:** Current port state. The port can be set to disable or enable mode. If the port state is set as ‘Disable’, it will not receive or transmit any packet.
- **Negotiation:** Auto and Force. Being set as Auto, the speed and duplex mode are negotiated automatically. When you set it as Force, you have to set the speed and duplex mode manually.
- **Speed:** It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read-only.
- **Duplex:** It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read-only.
- **Flow Control:** Whether or not the receiving node sends feedback to the sending node is determined by this item. When enabled, 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. When disabled, the receiving device will drop the packet if too much to process.
- **Security:** When the Security selection is set as ‘**On**’, any access from the device which connects to this port will be blocked unless the MAC address of the device is included in the static MAC address table. See the segment of **MAC Address Table—Static MAC Addresses**.
- Click  to have the configuration take effect.

Port Control

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

Apply Help

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	Up	Enable	Auto	100 Full	100 Full	Enable	ON	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/mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.10	N/A	1GTX/mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF

Port Control interface

Port Trunk

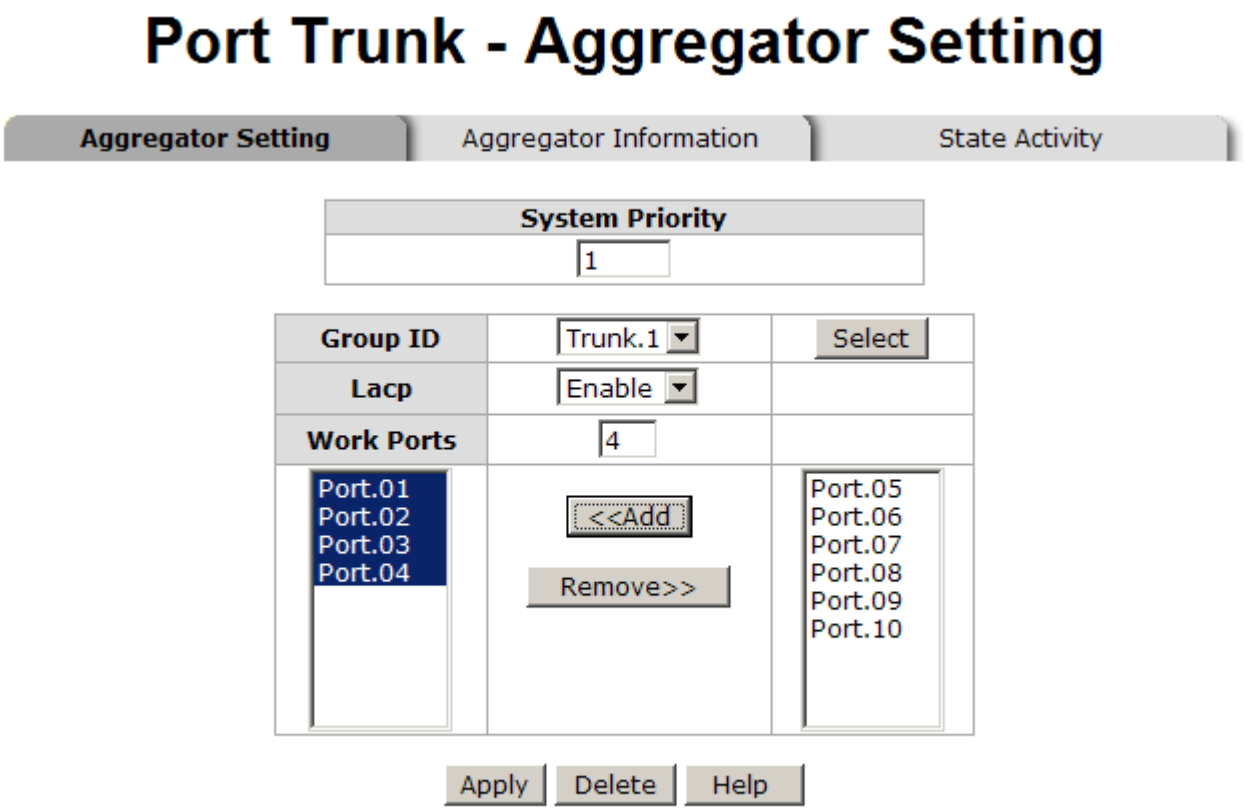
Port trunking is the combination of several ports or network cables to expand the connection speed beyond the limits of any one single port or network cable. Link Aggregation Control Protocol (LACP), which is a protocol running on layer 2, provides a standardized means in accordance with IEEE 802.3ad 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.

Port Trunk—Aggregator setting

- **System Priority:** A value which 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 to be selected. 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 split 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 user to type in the total number of active port up to four. With **LACP static 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.
- Select the ports to join the trunk group. The system allows a maximum of four ports to be aggregated in a trunk group. Click Add and the ports focused in the right side will be shifted to the left side. To remove unwanted ports, select the

ports and click Remove.

- When LACP enabled, you can configure LACP Active/Passive status for each port on the **State Activity** tab.
- Click Apply.
- Use Delete to delete Trunk Group. Select the Group ID and click Delete.

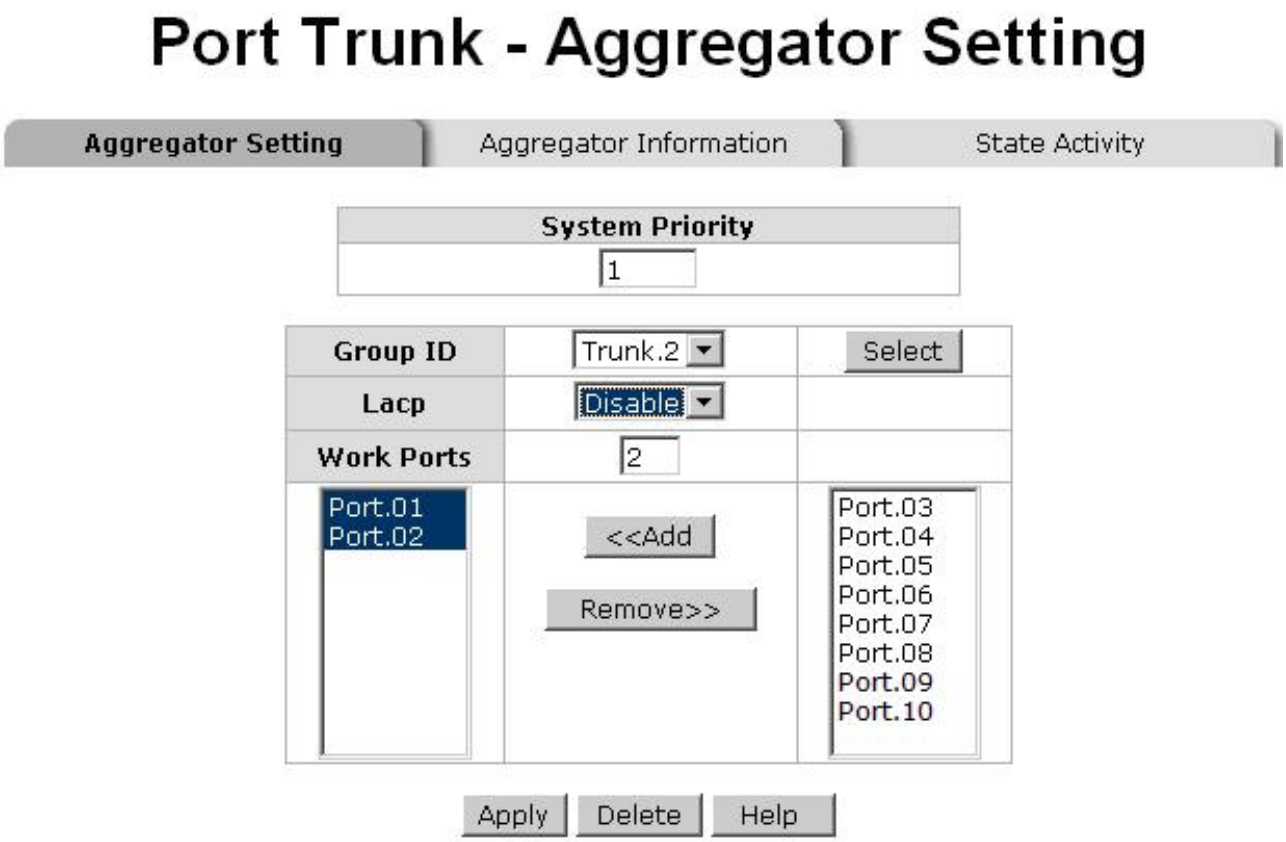


Port Trunk—Aggregator Setting interface (four ports are added to the left field with LACP enabled)

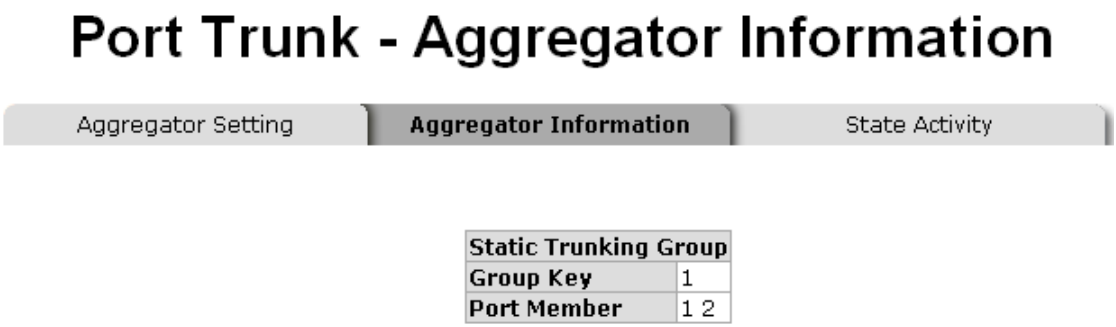
Port Trunk—Aggregator Information

- **LACP disabled**

Having set up the aggregator setting with LACP disabled, you will see the local static trunk group information on the tab of **Aggregator Information**.



Assigning 2 ports to a trunk group with LACP disabled



Static Trunking Group information

- **Group Key:** This is a read-only column field that displays the trunk group ID.

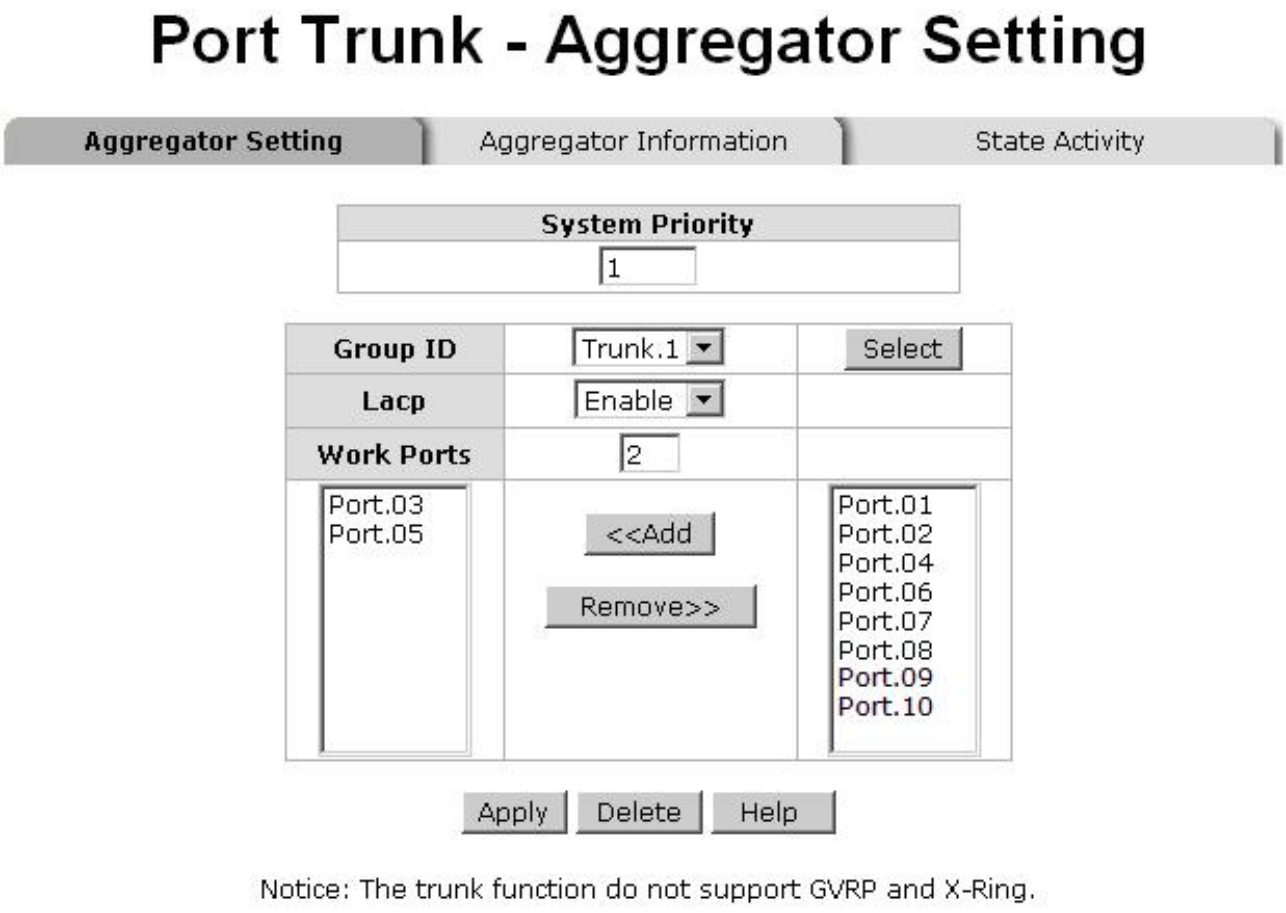
- **Port Member:** This is a read-only column field that displays the members of this static trunk group.

- **LACP enabled**

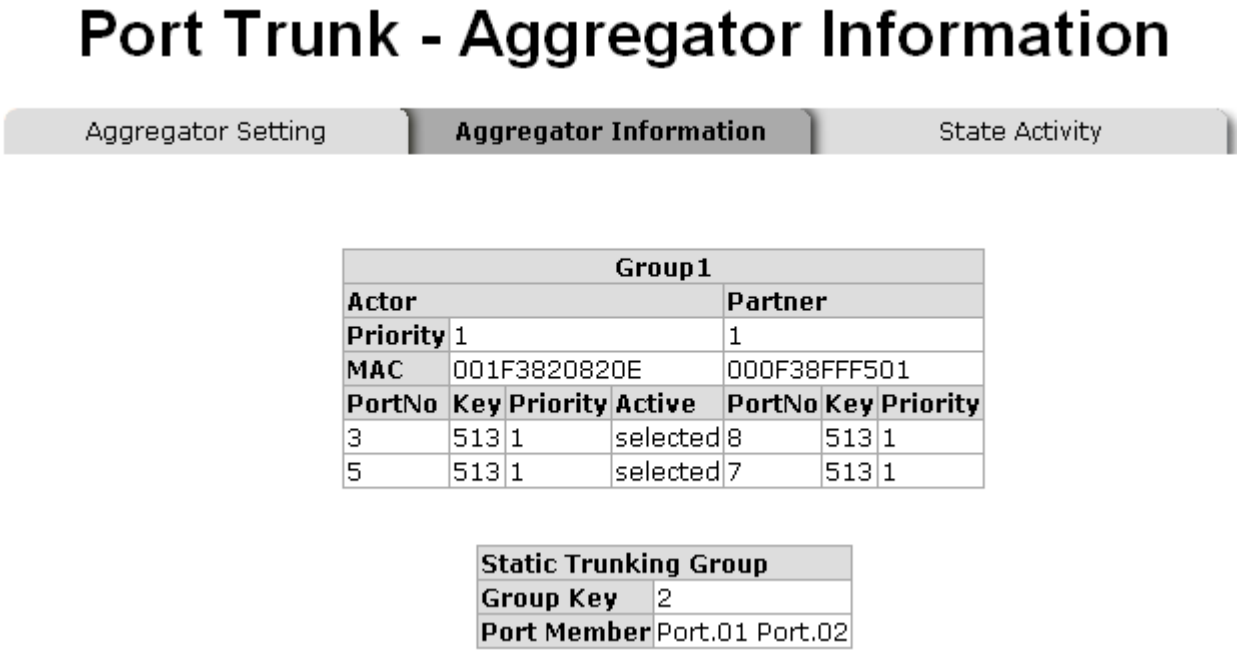
Having set up the aggregator setting with LACP enabled, you will see the trunking group information between two switches on the tab of **Aggregator Information**.

■ **Switch 1 configuration**

1. Set **System Priority** of the trunk group. The default is 1.
2. Select a **trunk group ID** by pull down the drop-down menu bar.
3. Enable LACP.
4. Include the member ports by clicking the **Add** button after selecting the port number and the column field of **Work Ports** changes automatically.



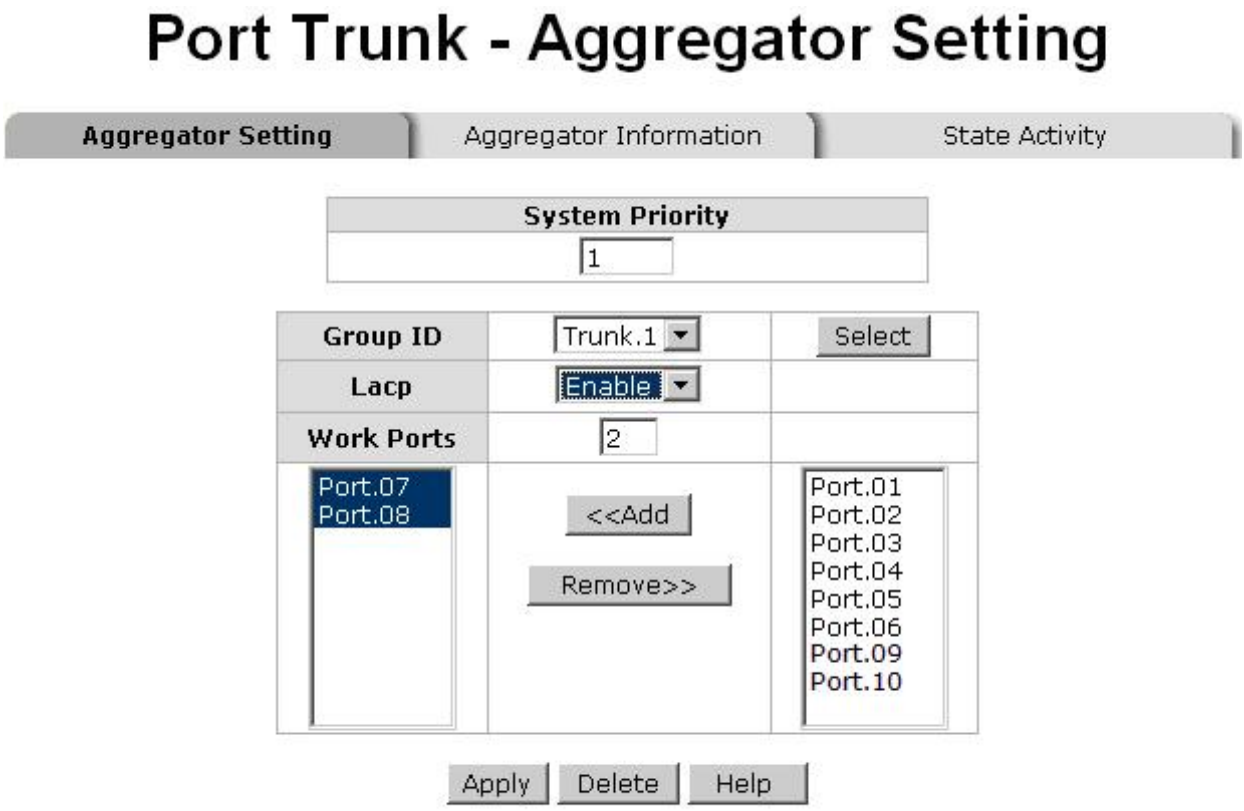
Switch 1 configuration interface



Aggregation Information of Switch 1

5. Click on the tab of **Aggregator Information** to check the trunked group information as the illustration shown above after the two switches configured.

- **Switch 2 configuration**



Switch 2 configuration interface

1. Set **System Priority** of the trunk group. The default is 1.
2. Select a **trunk group ID** by pull down the drop-down menu bar.
3. Enable LACP.
4. Include the member ports by clicking the **Add** button after selecting the port number and the column field of **Work Ports** changes automatically.

Group1						
Actor				**Partner**		
Priority	1			1		
MAC	000F38FFF501			001F3820820E		
PortNo	**Key**	**Priority**	**Active**	**PortNo**	**Key**	**Priority**
7	513	1	selected	5	513	1
8	513	1	selected	3	513	1

Aggregation Information of Switch 2

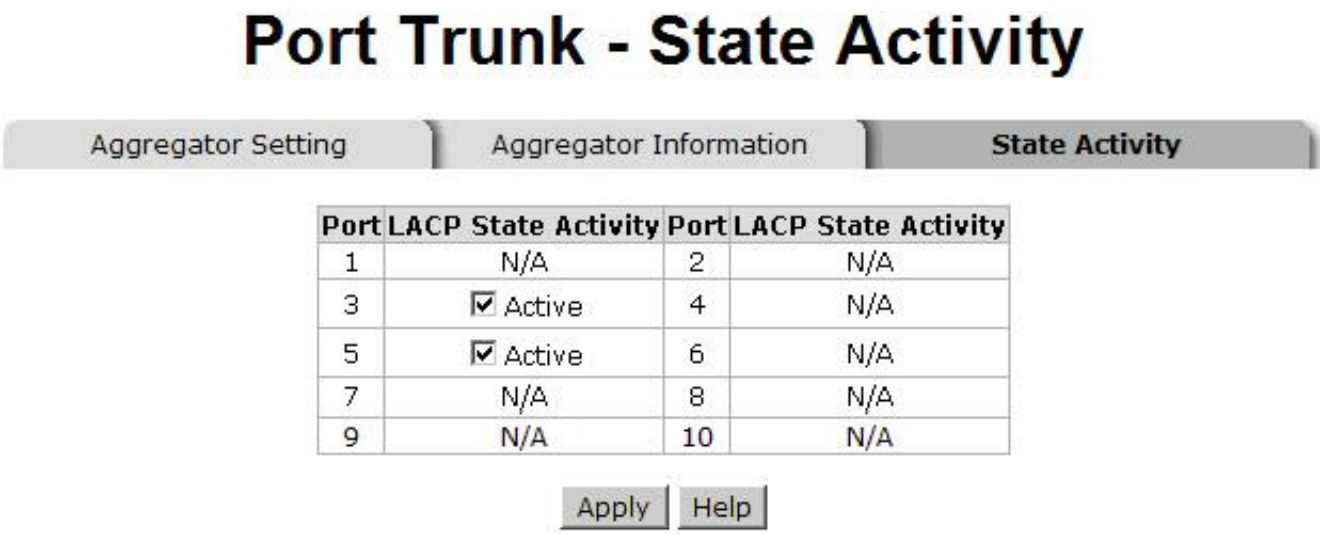
5. Click on the tab of **Aggregator Information** to check the trunked group information as the illustration shown above after the two switches configured.

Port Trunk—State Activity

Having set up the LACP aggregator on the tab of Aggregator Setting, you can configure the state activity for the members of the LACP trunk group. You can tick or cancel the checkbox beside the state label. When you remove the tick mark of the port and click Apply, the port state activity will change to **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.

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



State Activity of Switch 1

Port Trunk - State Activity

Aggregator Setting | Aggregator Information | **State Activity**

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

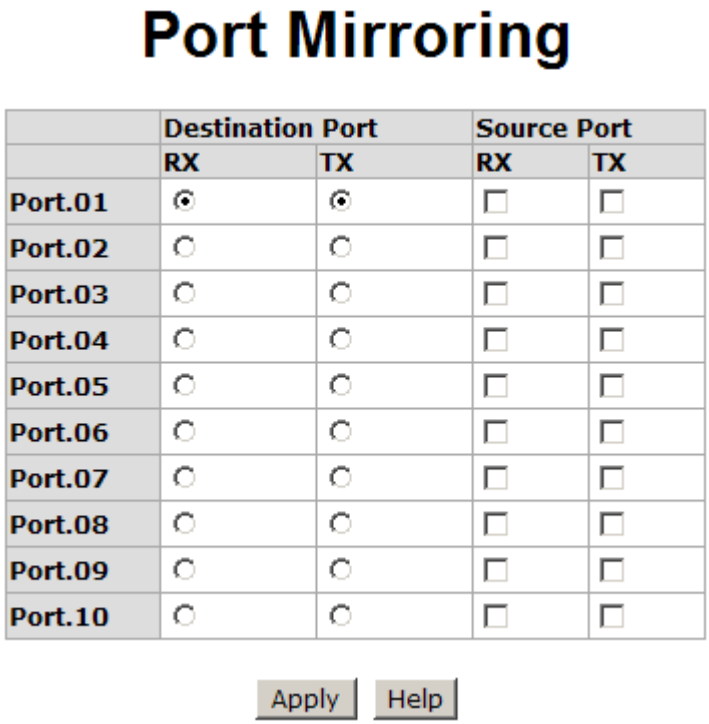
Apply Help

State Activity of Switch 2

Port Mirroring

The Port mirroring is a method for monitor traffic in switched networks. Traffic through ports can be monitored by one specific port, which means traffic goes in or out monitored (source) ports will be duplicated into mirror (destination) 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 port. Or, use one of two ports for monitoring RX traffic only and the other one for TX traffic only. User can connect mirror port to LAN analyzer or Netxray.
- **Source Port:** The ports that user wants to monitor. All monitored port traffic will be copied to mirror (destination) port. User can select multiple source ports by checking the **RX** or **TX** check boxes to be monitored.
- And then, click Apply button.



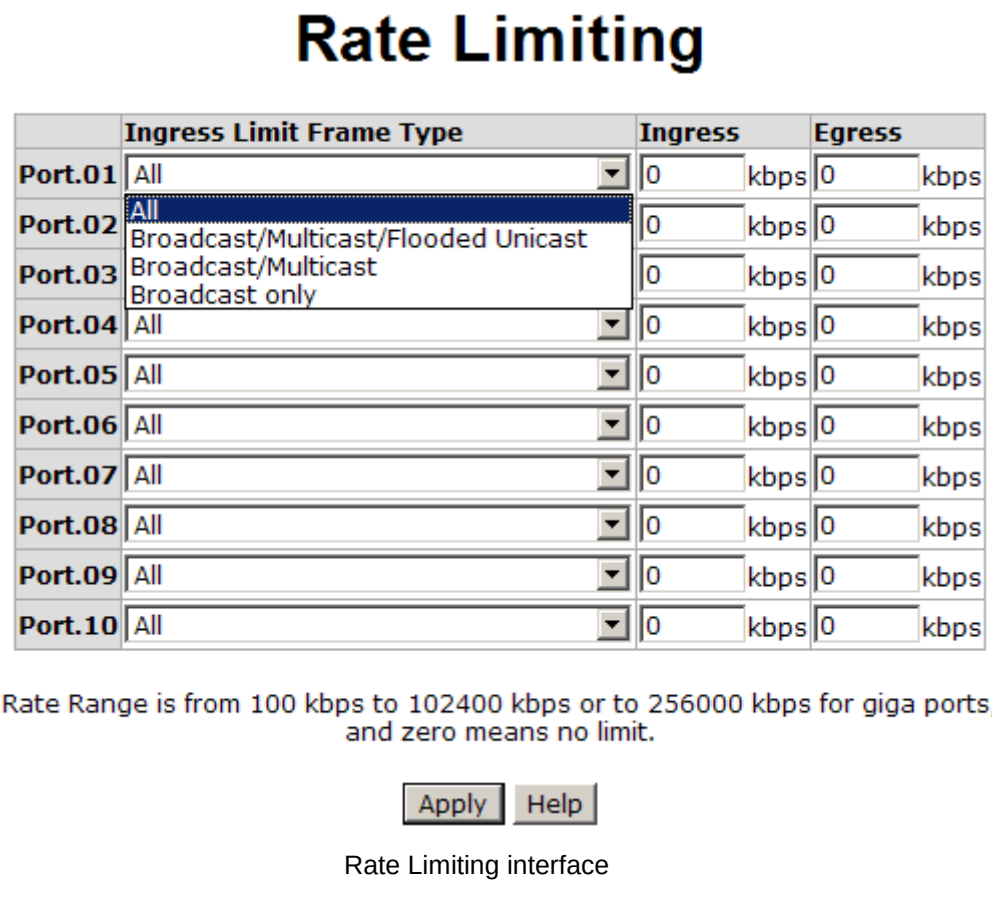
Port Trunk – Port Mirroring interface

Rate Limiting

You can set up every port's bandwidth rate and frame limitation type.

- **Ingress Limit Frame type:** select the frame type that wants to filter. There are four frame types for selecting:
  - **All**
  - **Broadcast/Multicast/Flooded Unicast**
  - **Broadcast/Multicast**
  - **Broadcast only**

  Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast and **Broadcast only** types are only for ingress frames. The egress rate only supports **All** type.



Rate Limiting interface

- All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set it's effective egress rate is 1Mbps, ingress rate is 500Kbps. The switch performs the ingress rate by packet counter to meet the

specified rate

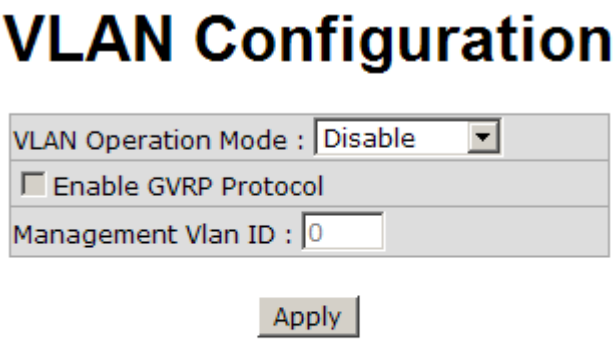
- **Ingress:** Enter the port effective ingress rate (The default value is “0”).
- **Egress:** Enter the port effective egress rate (The default value is “0”).

■ And then, click Apply to apply the settings

VLAN configuration

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

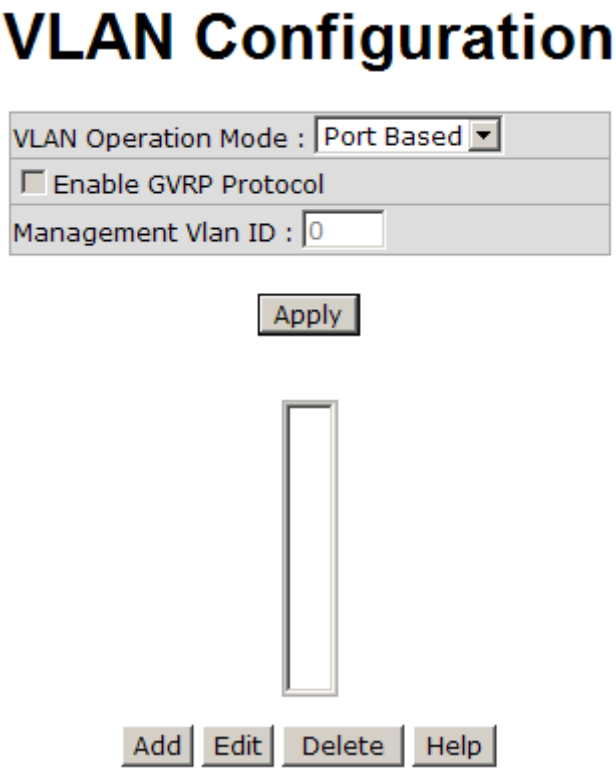
This switch supports **Port-based** and **802.1Q** (tagged-based) VLAN. The default configuration of VLAN operation mode is "**Disable**".



VLAN Configuration interface

VLAN configuration—Port-based VLAN

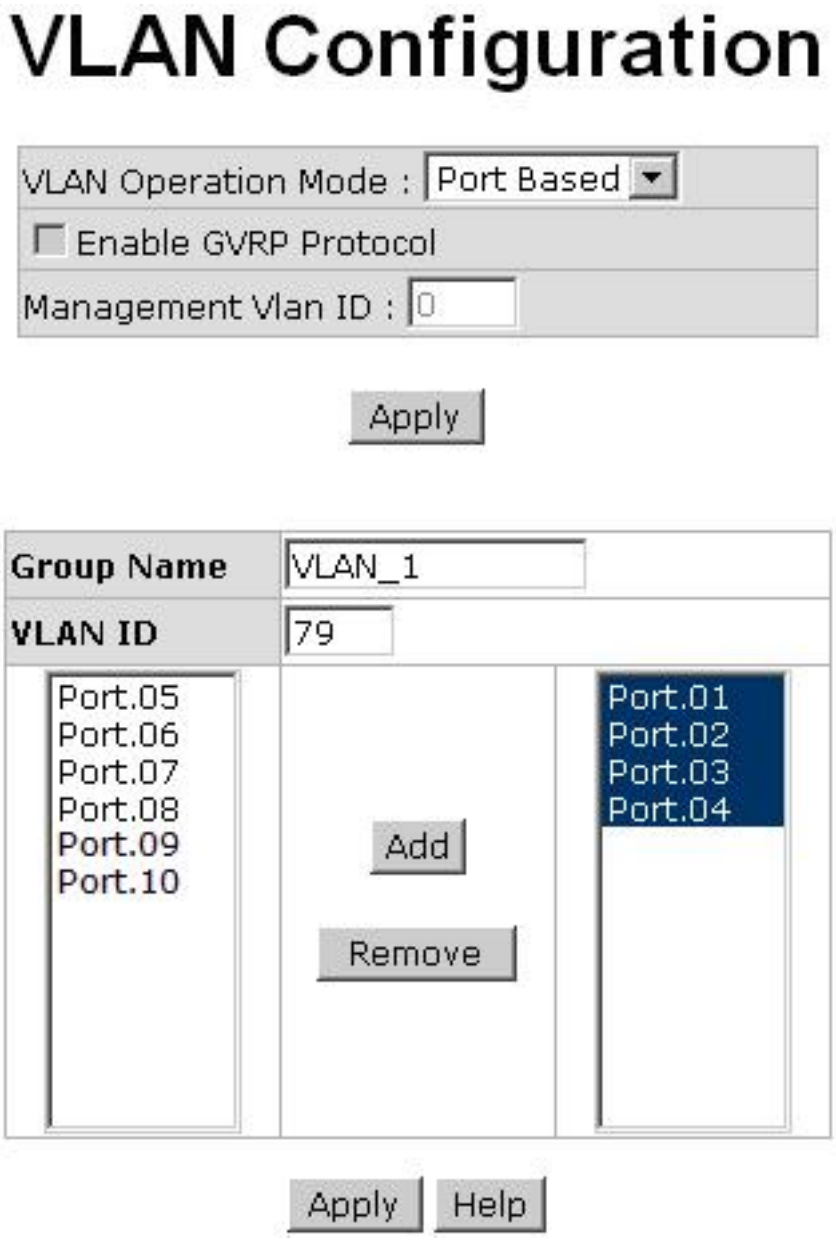
A port-based VLAN basically consists of its members—ports, which means the VLAN is created by grouping the selected ports. This method provides the convenience for users to configure a simple VLAN easily without complicated steps. Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored. The port-based VLAN function allows the user to create separate VLANs to limit the unnecessary packet flooding; however, for the purpose of sharing resource, a single port called a common port can belongs to different VLANs, which all the member devices (ports) in different VLANs have the permission to access the common port while they still cannot communicate with each other in different VLANs.



VLAN – Port Based interface

- Pull down the selection item and focus on **Port Based** then press Apply to set the VLAN Operation Mode in **Port Based** mode.

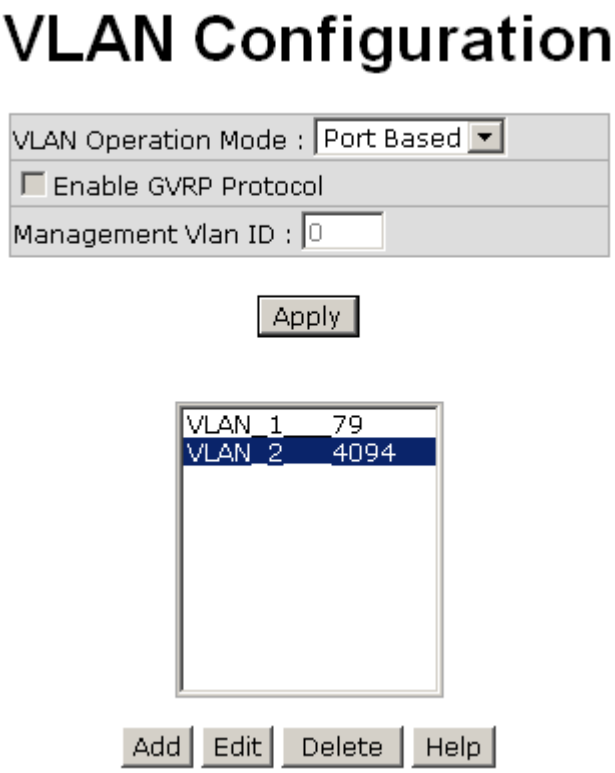
- Click Add to add a new VLAN group (The maximum VLAN groups are up to 64).



VLAN—Port Based Add interface

- Enter the group name and VLAN ID. Add the selected port number into the right field to group these members to be a VLAN group, or remove any of them listed in the right field from the VLAN.
- And then, click Apply to have the configuration take effect.

- You will see the VLAN list displays.



VLAN—Port Based Edit/Delete interface

- Use Delete to delete the VLAN.
- Use Edit to modify group name, VLAN ID, or add/remove the members of the existing VLAN group.

[NOTE] Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when switch power off.

802.1Q VLAN

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 regarded as members of the same broadcast domain. The valid VLAN ID is in the range of number between 1 and 4094. The amount of VLAN groups is up to 256 including default VLAN that cannot be deleted. Each member port of 802.1Q is on either an Access Link (VLAN-tagged) or a Trunk Link (no VLAN-tagged). All frames on an Access Link carry no VLAN identification. Conversely, all frames on a Trunk Link are VLAN-tagged. Besides, 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.

802.1Q Configuration

- Pull down the selection item and focus on **802.1Q** then press Apply to set the VLAN Operation Mode in **802.1Q** mode.
- **Enable GVRP Protocol:** 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, having enabled GVRP on two switches, they are able to automatically exchange the information of their VLAN database. Therefore, the user doesn't need to manually configure whether the link is trunk or hybrid, the packets belonging to the same VLAN can communicate across switches. Tick this checkbox to enable GVRP protocol. This checkbox is available while the VLAN Operation Mode is in **802.1Q** mode.
- **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' that means this limit is not enabled (all members in different VLANs can access this switch).
- Select the port you want to configure.
- **Link Type**: There are 3 types of link type.
  - **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 regarded as the same VLAN group members.

Note: Because the access port doesn't have an understanding of tagged frame, the column field of Tagged VID is not available.

- **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 depends on the values filled in the Tagged VID column field. Please insert a comma between two VIDs.

Note:

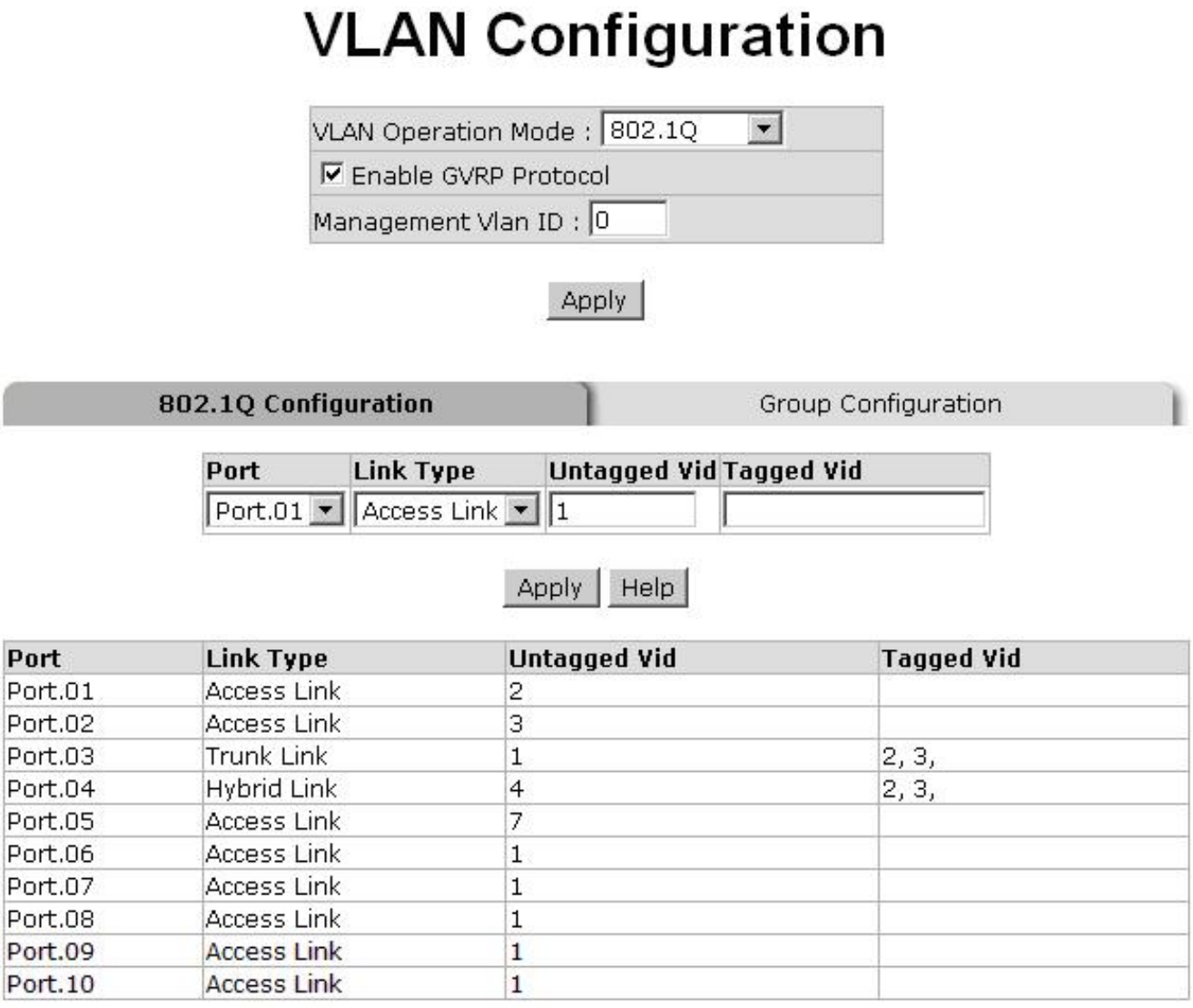
1. *A trunk port doesn't insert tag into an untagged frame, and therefore the untagged VID column field is not available.*
2. *It's not necessary to type '1' in the tagged VID. The trunk port will forward the frames of VLAN 1.*
3. *The trunk port has to be connected to a trunk/hybrid port of the other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

- **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.

Note:

1. *It's not necessary to type '1' in the tagged VID. The hybrid port will forward the frames of VLAN 1.*
2. *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.*

- **Untagged VID:** This column field is available when Link Type is set as Access Link and Hybrid Link. Assign a number in the range between 1 an 4094.
- **Tagged VID:** This column field is available when Link Type is set as Trunk Link and Hybrid Link. Assign a number in the range between 1 an 4094.
- Click Apply to have the configuration take effect.
- You can see the link type, untagged VID, and tagged VID information of each port in the table below on the screen.



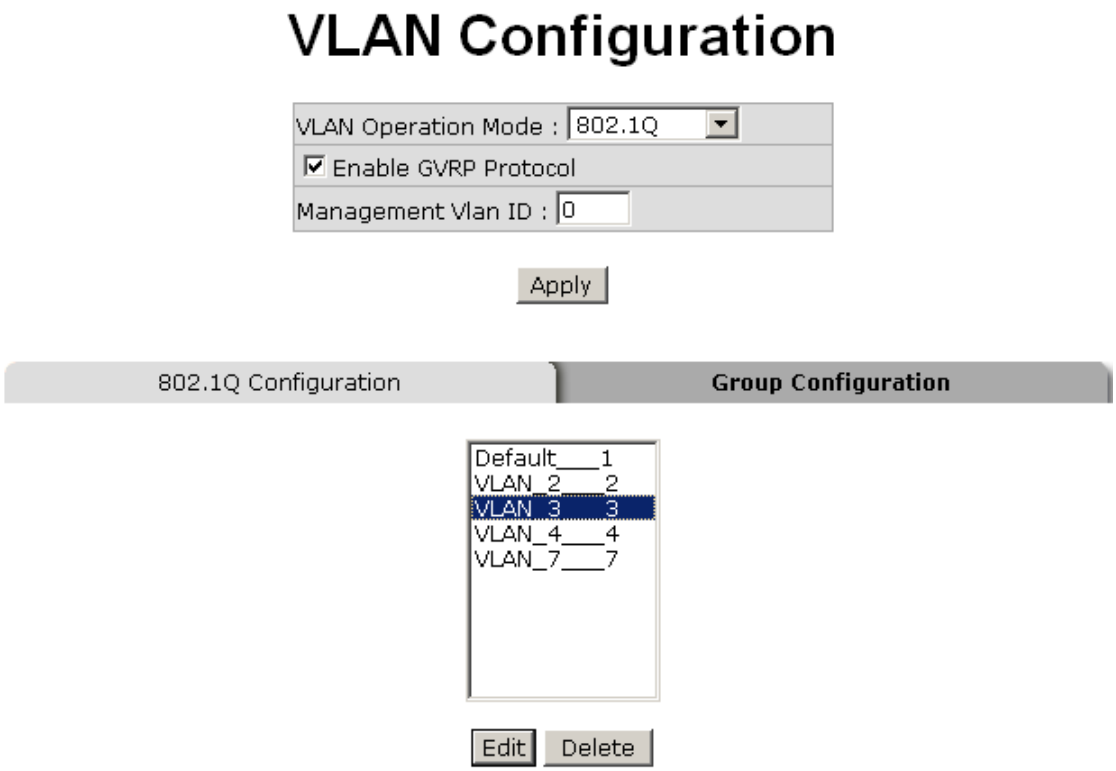
Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	2	
Port.02	Access Link	3	
Port.03	Trunk Link	1	2, 3,
Port.04	Hybrid Link	4	2, 3,
Port.05	Access Link	7	
Port.06	Access Link	1	
Port.07	Access Link	1	
Port.08	Access Link	1	
Port.09	Access Link	1	
Port.10	Access Link	1	

802.1Q VLAN interface

Group Configuration

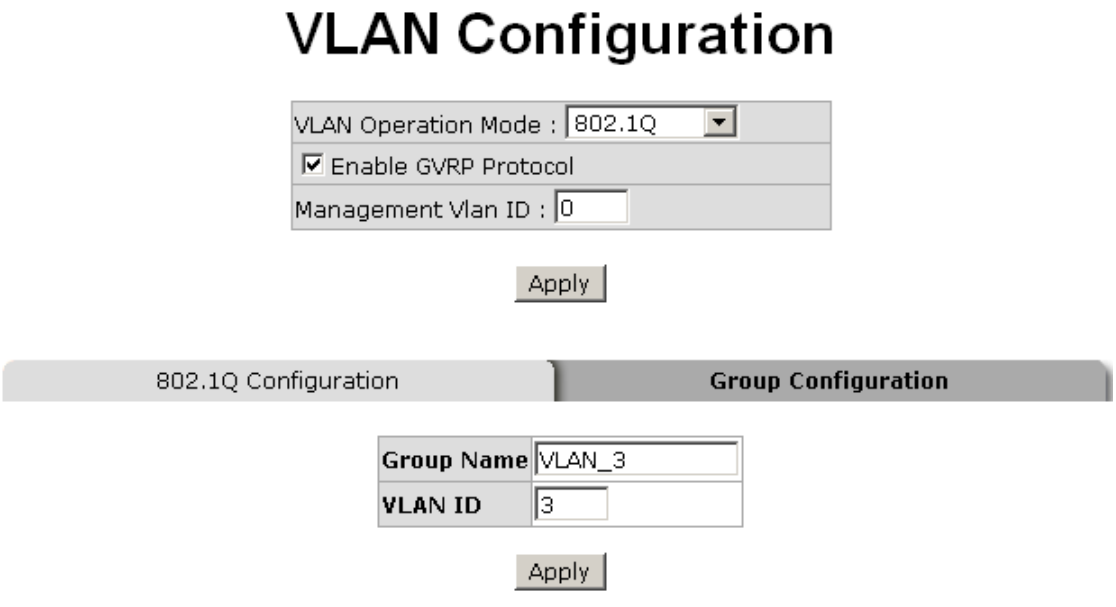
Edit the existing VLAN Group.

- Select the VLAN group in the table list.
- Click Edit.



Group Configuration interface

- You can modify the VLAN group name and VLAN ID.



Group Configuration interface

- Click Apply.

Rapid Spanning Tree

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

RSTP—System Configuration

- The user can view spanning tree information of Root Bridge.
- The user can modify RSTP state. After modification, click Apply.
  - **RSTP mode:** The user must enable the RSTP function first before configuring the related parameters.
  - **Priority (0-61440):** The switch with the lowest value has the highest priority and is selected as the root. If the value is changed, the user must reboot the switch. The value must be a multiple of 4094 according to the protocol standard rule.
  - **Max Age (6-40):** The number of seconds a switch waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
  - **Hello Time (1-10):** The time that controls the switch to send out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.
  - **Forward Delay Time (4-30):** The number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.

[NOTE]	Follow the rule as below to configure the MAX Age, Hello Time, and Forward Delay Time. **2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)**

RSTP - System Configuration

System Configuration | Port 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).

Apply | Help

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

RSTP System Configuration interface

RSTP—Port Configuration

This web page provides the port configuration interface for RSTP. You can assign higher or lower priority to each port. Rapid spanning tree will have the port with the higher priority in forwarding state and block other ports to make certain that there is no loop in the LAN.

- Select the port in the port column field.
- **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200,000,000.
- **Priority:** Decide which port should be blocked by setting its priority as the lowest. Enter a number between 0 and 240. The value of priority must be the multiple of 16.
- **Admin P2P:** The rapid state transitions possible within RSTP are dependent upon whether the port concerned can only be connected to exactly another 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 means the port is regarded as a point-to-point link. False means the port is regarded as a shared link. Auto means the link type is determined by the auto-negotiation between the two peers.
- **Admin Edge:** The port directly connected to end stations won't create bridging loop in the network. To configure the port as an edge port, set the port to "**True**" status.
- **Admin Non STP:** The port includes the STP mathematic calculation. **True** is not including STP mathematic calculation. **False** is including the STP mathematic calculation.
- Click Apply.

RSTP - Port Configuration

System Configuration | **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

Apply Help

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	Disabled	Disabled
Port.06	200000	128	True	True	False	Disabled	Disabled
Port.07	20000	128	False	True	False	Forwarding	Designated
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

RSTP Port Configuration interface

SNMP Configuration

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

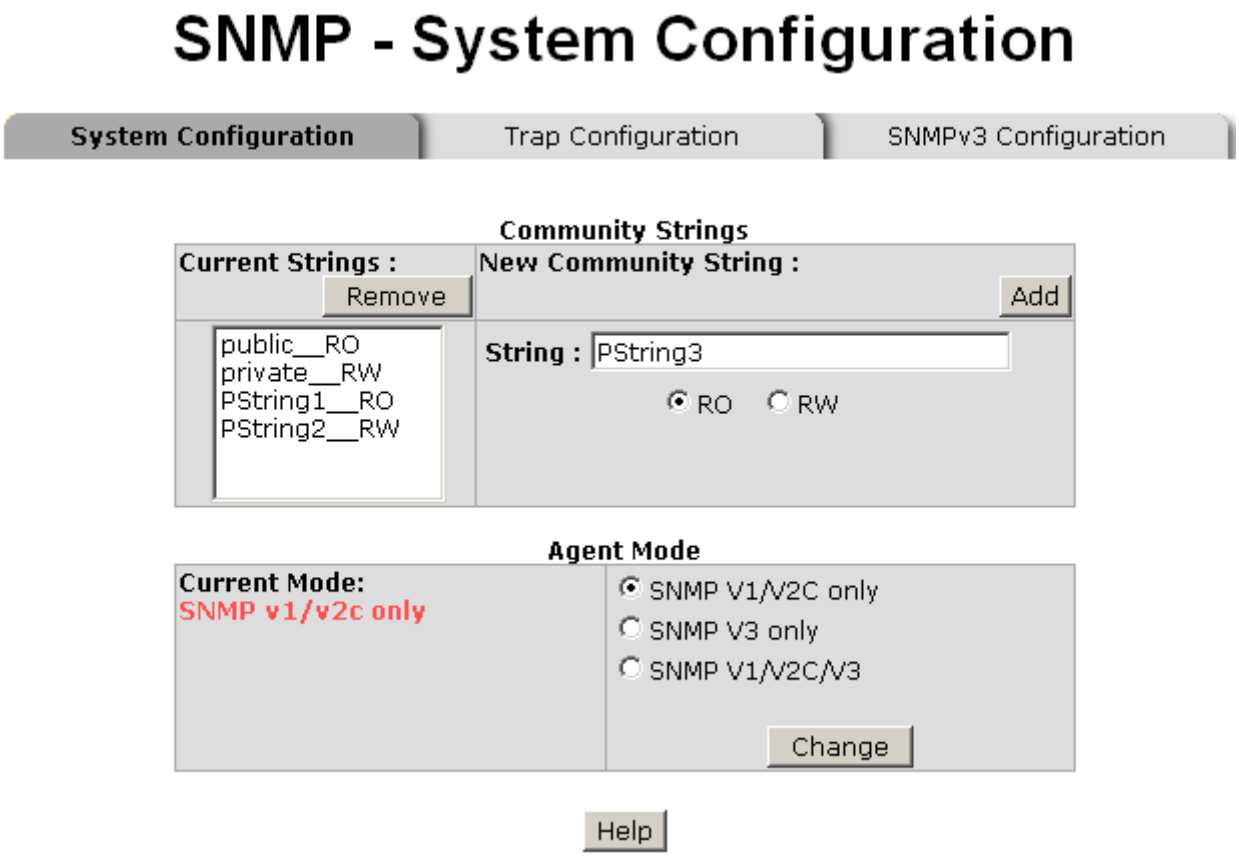
System Configuration

- **Community Strings**

Here you can define the new community string set and remove the unwanted community string.

- **String:** Fill the name string.
- **RO:** Read only. Enables requests accompanied by this community string to display MIB-object information.
- **RW:** Read/write. Enables requests accompanied by this community string to display MIB-object information and to set MIB objects.
- Click Add.
- To remove the community string, select the community string that you defined before and click Remove. The strings of Public_RO and Private_RW are default strings. You can remove them but after resetting the switch to default, the two strings show up again.

- **Agent Mode:** Select the SNMP version that you want to use it. And then click Change to switch to the selected SNMP version mode.

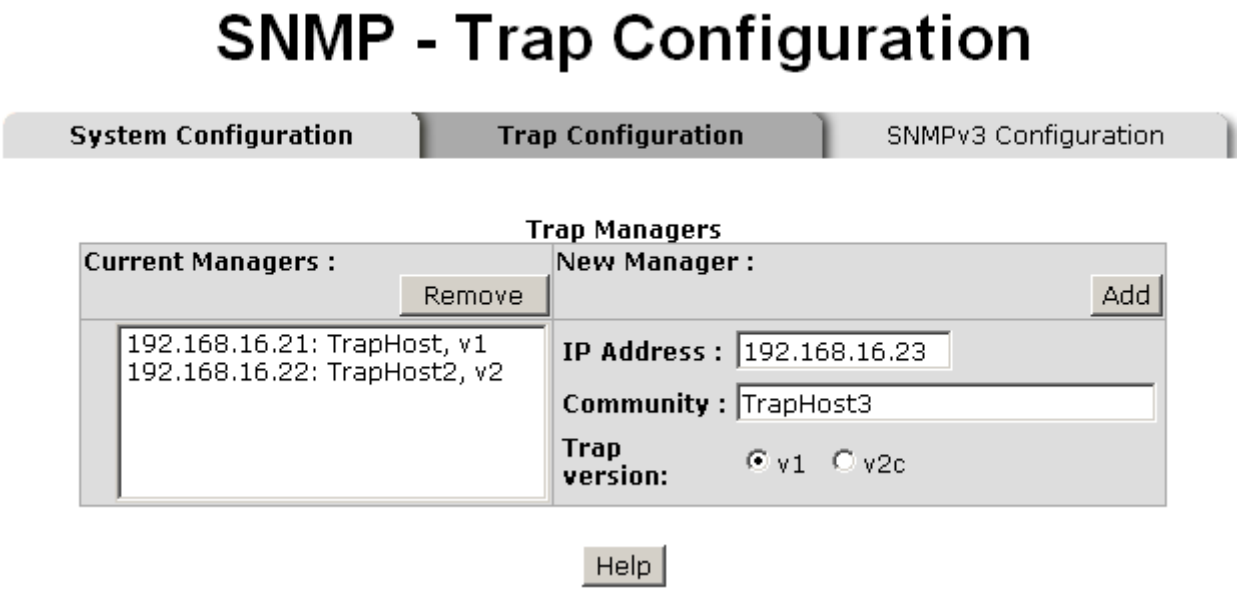


SNMP System Configuration interface

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:** Enter the IP address of the trap manager.
- **Community:** Enter the community string for the trap station.
- **Trap Version:** Select the SNMP trap version type—v1 or v2c.
- Click Add.
- To remove the community string, select the community string listed in the current managers field and click Remove.



Trap Managers interface

SNMPv3 Configuration

Configure the SNMP v3 function.

Context Table

Configure SNMP v3 context table. Assign the context name of context table. Click Apply to add context name.

User Profile

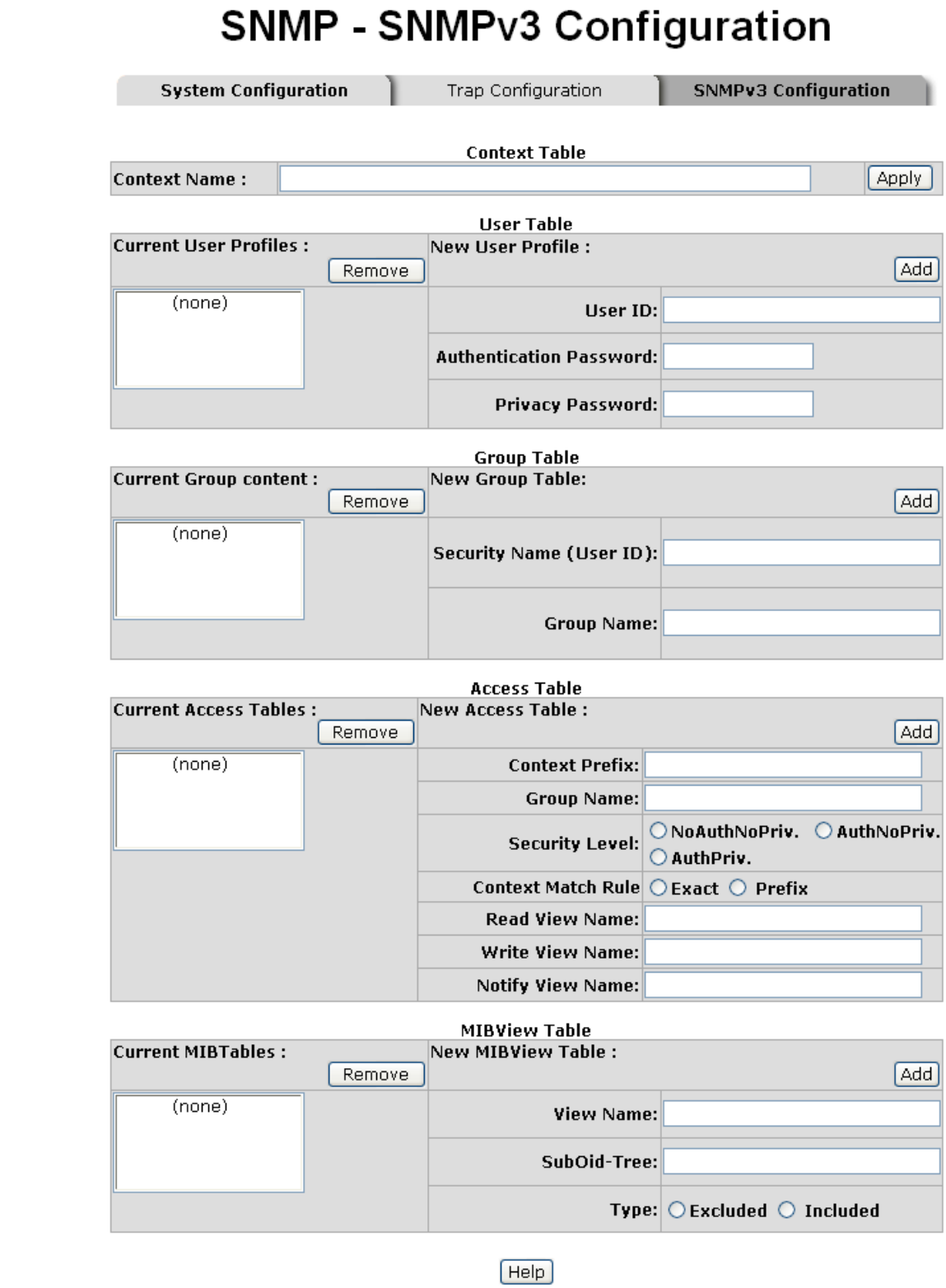
Configure SNMP v3 user table..

- **User ID:** Set up the user name.
- **Authentication Password:** Set up the authentication password.
- **Privacy Password:** Set up the private password.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

Group Table

Configure SNMP v3 group table.

- **Security Name (User ID):** Assign the user name that you have set up in user table.
- **Group Name:** Set up the group name.
- Click Add to add context name.
- Click Remove to remove unwanted context name.



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.

SNMP v3 configuration interface

Access Table

Configure SNMP v3 access table.

- **Context Prefix:** Set up the context name.
- **Group Name:** Set up the group.
- **Security Level:** Set up the access level.
- **Context Match Rule:** Select the context match rule.
- **Read View Name:** Set up the read view.
- **Write View Name:** Set up the write view.
- **Notify View Name:** Set up the notify view.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

MIBview Table

Configure MIB view table.

- **ViewName:** Set up the name.
- **Sub-Oid Tree:** Fill the Sub OID.
- **Type:** Select the type – exclude or included.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

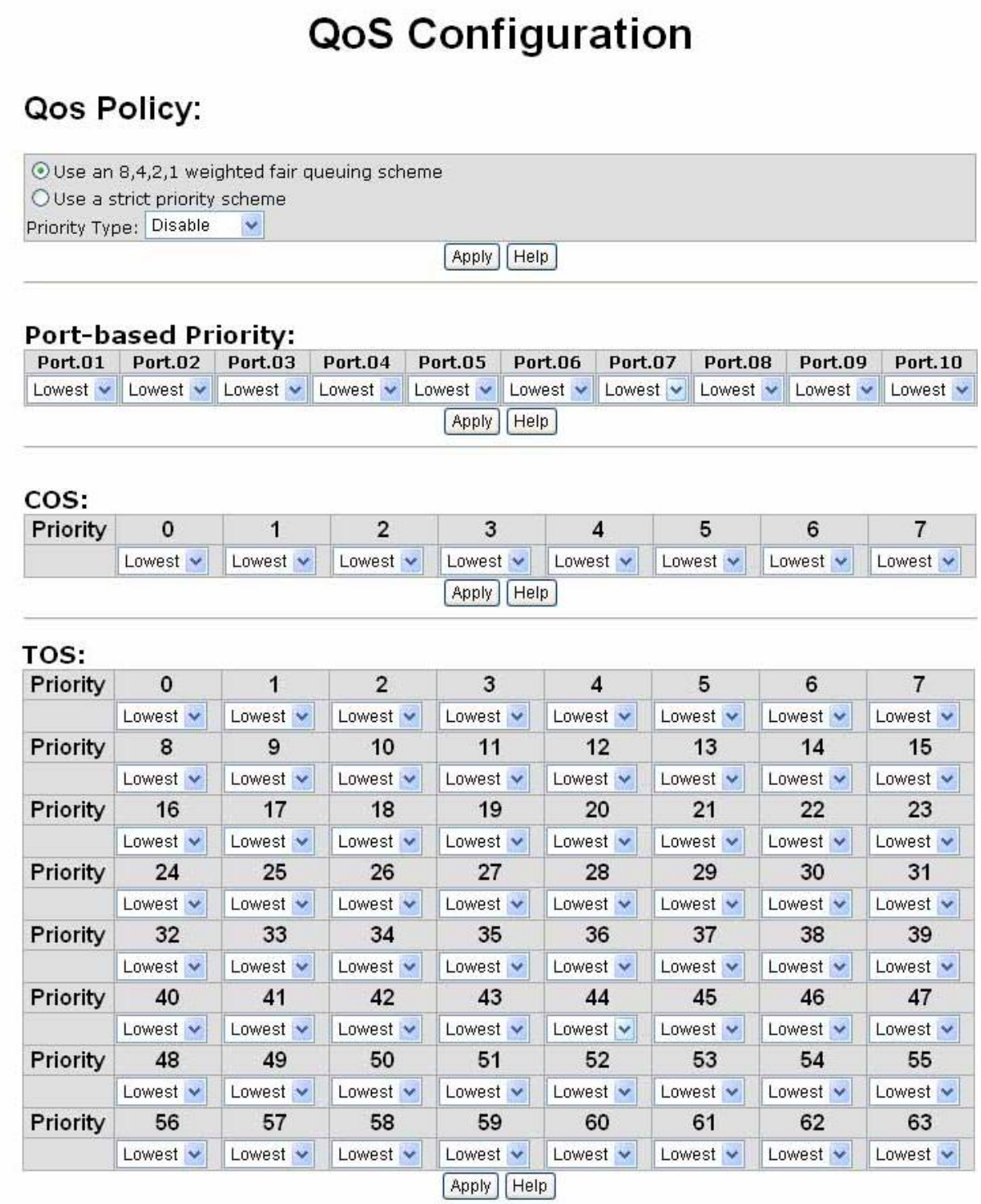
QoS Configuration

Quality of Service (QoS) is the ability to provide different priority to different applications, users or data flows, or to guarantee a certain level of performance to a data flow. QoS guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP or Video Teleconferencing, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication. In the absence of network congestion, QoS mechanisms are not required.

QoS Policy and Priority Type

Here you can choose to use an 8-4-2-1 queuing scheme or a strict priority scheme, or select the priority type to configure QoS policy.

- **QoS Policy:** Select the QoS policy rule.
  - **Using the 8,4,2,1 weight fair queue scheme:** The switch will follow 8:4:2:1 rate to process priority queue from High to lowest queue. For example, while the system processing, 1 frame of the lowest queue, 2 frames of the low queue, 4 frames of the middle queue, and 8 frames of the high queue will be processed at the same time in accordance with the 8,4,2,1 policy rule.
  - **Use a strict priority scheme:** Always the higher queue will be processed first, except the higher queue is empty.
  - **Priority Type:** There are 5 priority type selections available—**Port-based**, **TOS only**, **COS only**, **TOS first**, and **COS first**. Disable means no priority type is selected.
- Click Apply to have the configuration take effect.



QoS Configuration interface

Port-Based Priority

Configure per port priority level.

- **Port:** Each port has 4 priority levels – High, Middle, Low, and Lowest.
- Click Apply.

COS Configuration

Set up the COS priority level.

- **COS priority:** Set up the COS priority level 0~7 –High, Middle, Low, Lowest.
- Click Apply.

TOS Configuration

Set up the TOS priority.

- **TOS priority:** The system provides 0~63 TOS priority level. Each level has 4 types of priority – high, middle, low, and lowest. The default value is 'Lowest' priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that has received. For example, user set the TOS level 25 as high, the system 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 highest priority.
- Click Apply.

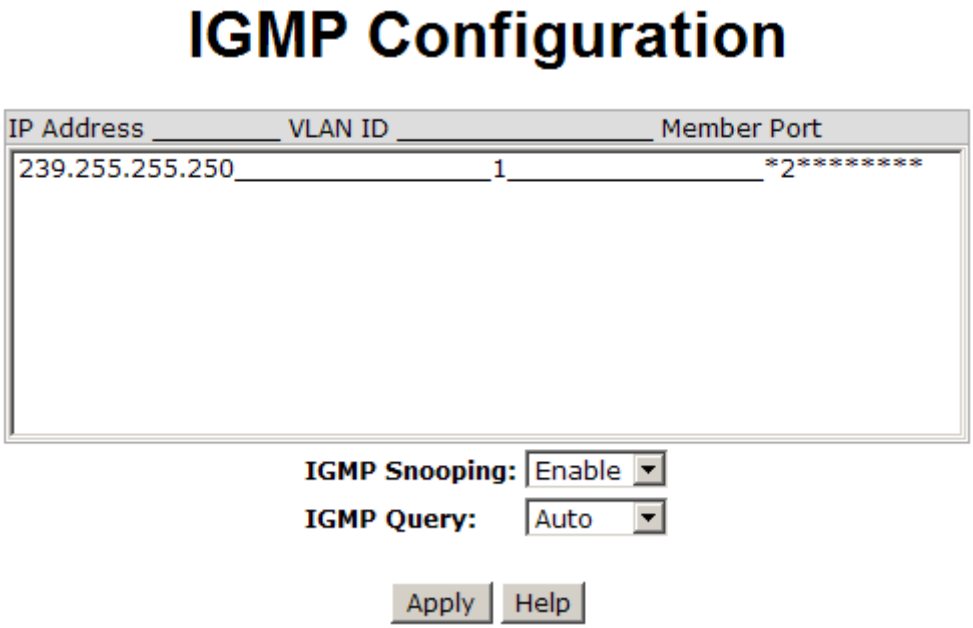
IGMP Configuration

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

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
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.

The switch supports IP multicast. You can enable IGMP protocol via setting IGMP configuration page to see the IGMP snooping information. IP multicast addresses are in the range of 224.0.0.0 through 239.255.255.255.

- **IGMP Protocol:** Enable or disable the IGMP protocol.
- **IGMP Query:** Select the IGMP query function as Enable or Auto to set the switch as a querier for IGMP version 2 multicast networks.
- Click Apply.



IGMP Configuration interface

X-Ring

X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms not the same.

In the X-Ring topology, every switch should enable X-Ring function and assign two member ports in the ring. Only one switch in the X-Ring group would be set as a master switch that would be blocked, called backup port, and another port is called working port. Other switches in the X-Ring group are called working switches and their two member ports are called working ports. When the failure of network connection occurs, the backup port will automatically become a working port to recovery the failure.

The switch supports the function and interface for setting the switch as the ring master or slave mode. The ring master can negotiate and place command to other switches in the X-Ring group. If there are 2 or more switches in master mode, then software will select the switch with lowest MAC address number as the ring master. The X-Ring master ring mode will be enabled by the X-Ring configuration interface.

The system also supports the coupling ring that can connect 2 or more X-Ring group for the redundant backup function and dual homing function that prevent connection lose between X-Ring group and upper level/core switch.

- **Enable X-Ring:** Enable the X-Ring function. Mark the check box to enable the X-Ring function.
- **Enable Ring Master:** Mark the check box to enable this machine to be the ring master.
- **1st & 2nd Ring Ports:** Pull down the selection menu to assign two ports as the member ports. The **1st Ring Port** and **2nd Ring Port** are basically assigned to be forwarding ports except for the Ring Master switch. With the Ring Master switch, one of its two Ring Ports is the blocking port and another one is the forwarding port. Once its forwarding port fails, the system will automatically upgrade its blocking port

to be the forwarding port of the Ring Master switch.

- **Enable Coupling Ring:** Enable the coupling ring function. Mark the check box to enable the coupling ring function.
- **Coupling port:** Assign the member port which is connected to the other ring group.
- **Control port:** When Couple Ring check box is marked, you have to assign the control port to form a couple-ring group between the two X-rings.
- **Enable Dual Homing:** Set up one of the ports on the switch to be the Dual Homing port. For a switch, there is only one Dual Homing port. Dual Homing function only works when the X-Ring function enabled.
- And then, click Apply to apply the configuration.

X-ring Interface

Note	When the X-Ring function enable, user must disable the RSTP. The X-Ring function and RSTP function cannot exist in a switch at the same time. Remember to execute the 'Save Configuration' action, otherwise the new configuration will lose when switch power off.

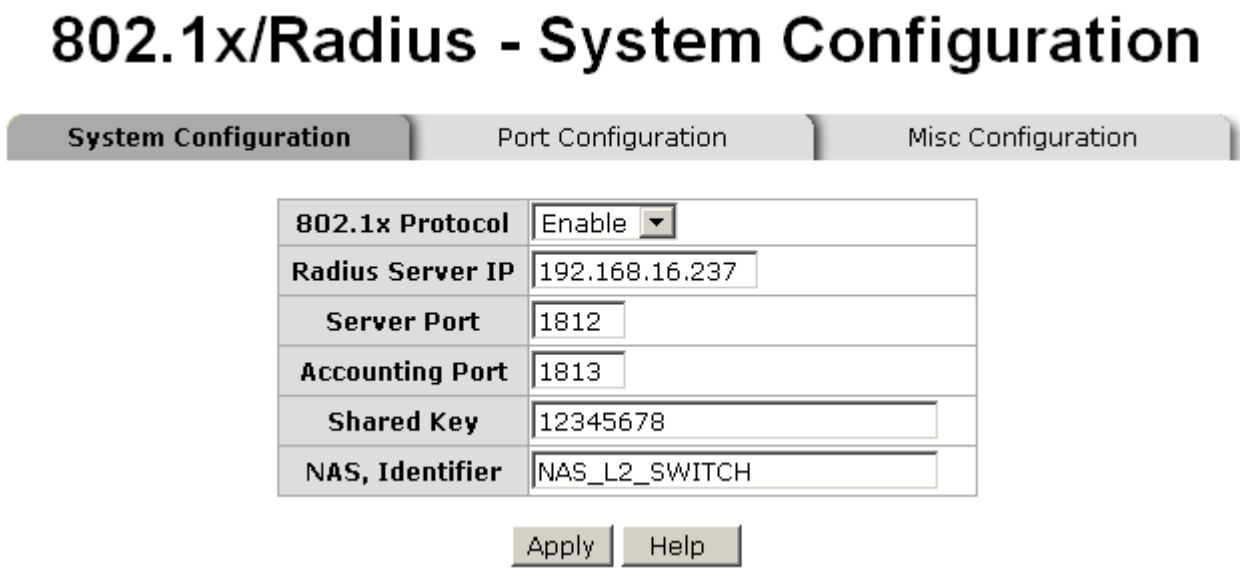
Security—802.1X/Radius Configuration

802.1x is an IEEE authentication specification which prevents the client from accessing a wireless access point or wired switch until it provides authority, like the user name and password that are verified by an authentication server (such as RADIUS server).

System Configuration

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

- **IEEE 802.1x Protocol:** Enable or disable 802.1x protocol.
- **Radius Server IP:** Assign the RADIUS Server IP address.
- **Server Port:** Set the UDP destination port for authentication requests to the specified RADIUS Server.
- **Accounting Port:** Set the UDP destination port for accounting requests to the specified RADIUS Server.
- **Shared Key:** Set an encryption key for using during authentication sessions with the specified RADIUS server. This key must match the encryption key used on the RADIUS Server.
- **NAS, Identifier:** Set the identifier for the RADIUS client.
- Click Apply.

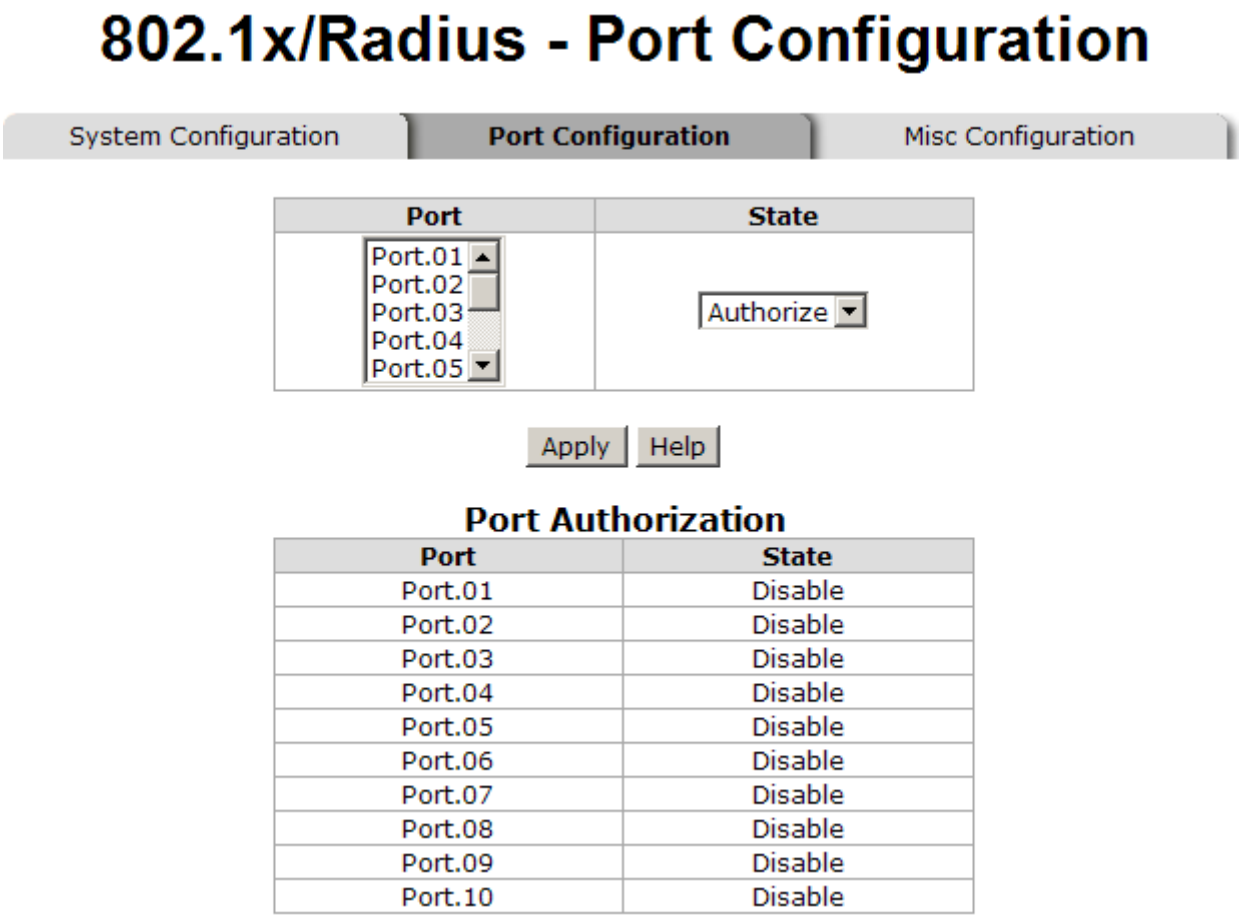


802.1x System Configuration interface

802.1x Port Configuration

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

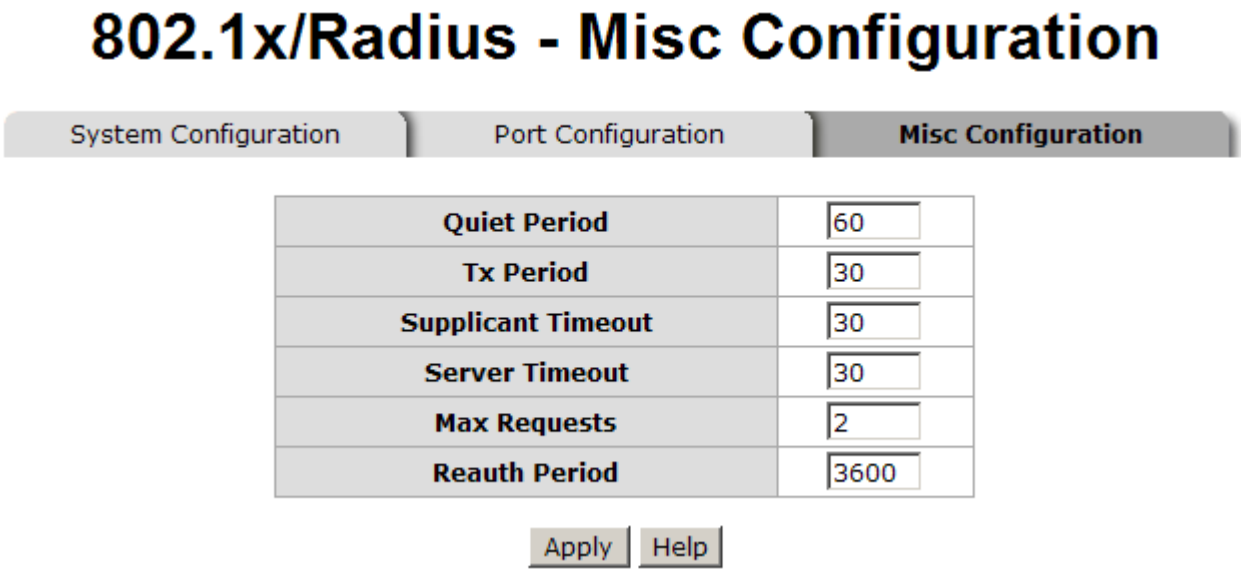
- **Reject:** The specified port is required to be held in the unauthorized state.
- **Accept:** The specified port is required to be held in the Authorized state.
- **Authorized:** The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange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



802.1x Per Port Setting interface

Misc Configuration

- **Quiet Period:** Set the period which the port doesn't try to acquire a supplicant.
- **TX Period:** Set the period the port waits for retransmit next EAPOL PDU during an authentication session.
- **Supplicant Timeout:** Set the period of time the switch waits for a supplicant response to an EAP request.
- **Server Timeout:** Set the period of time the switch waits for a server response to an authentication request.
- **Max Requests:** Set the number of authentication that must time-out before authentication fails and the authentication session ends.
- **Reauth period:** Set the period of time which clients connected must be re-authenticated.
- Click Apply.



802.1x Misc Configuration interface

MAC Address Table

Use the MAC address table to ensure the port security.

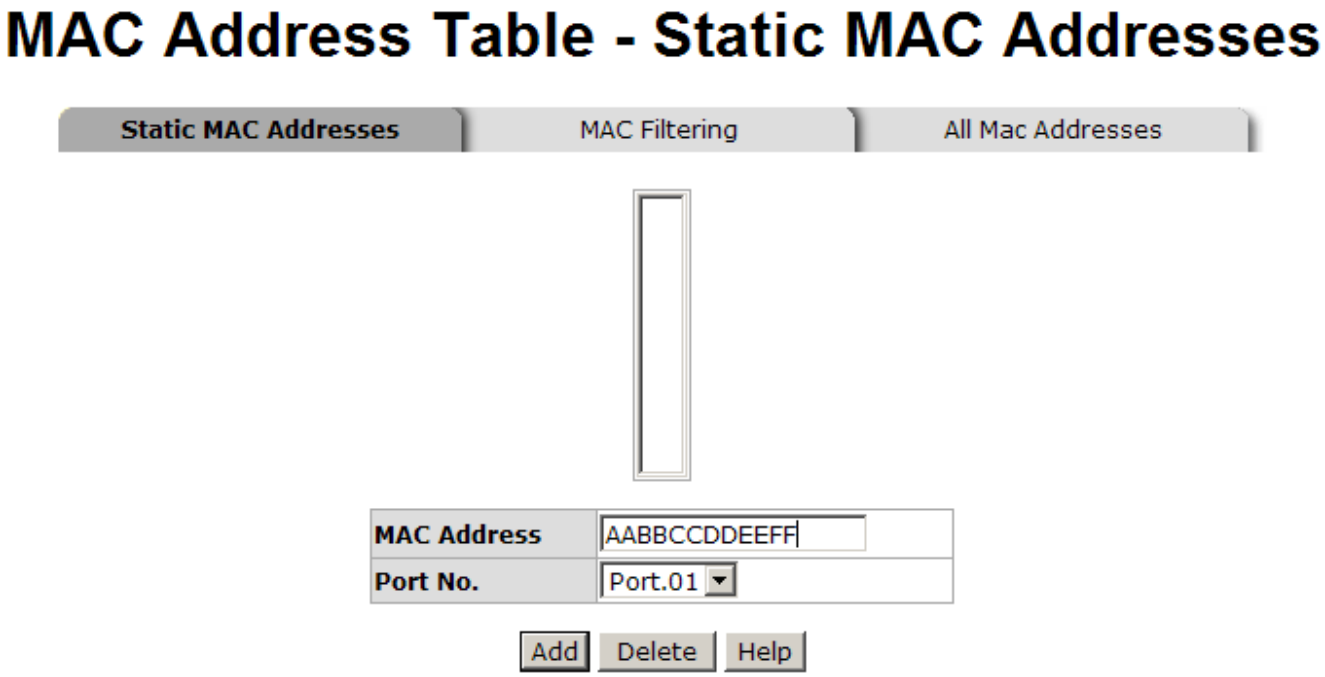
Static MAC Address

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

- **Add the Static MAC Address**

You can add static MAC address in the switch MAC table.

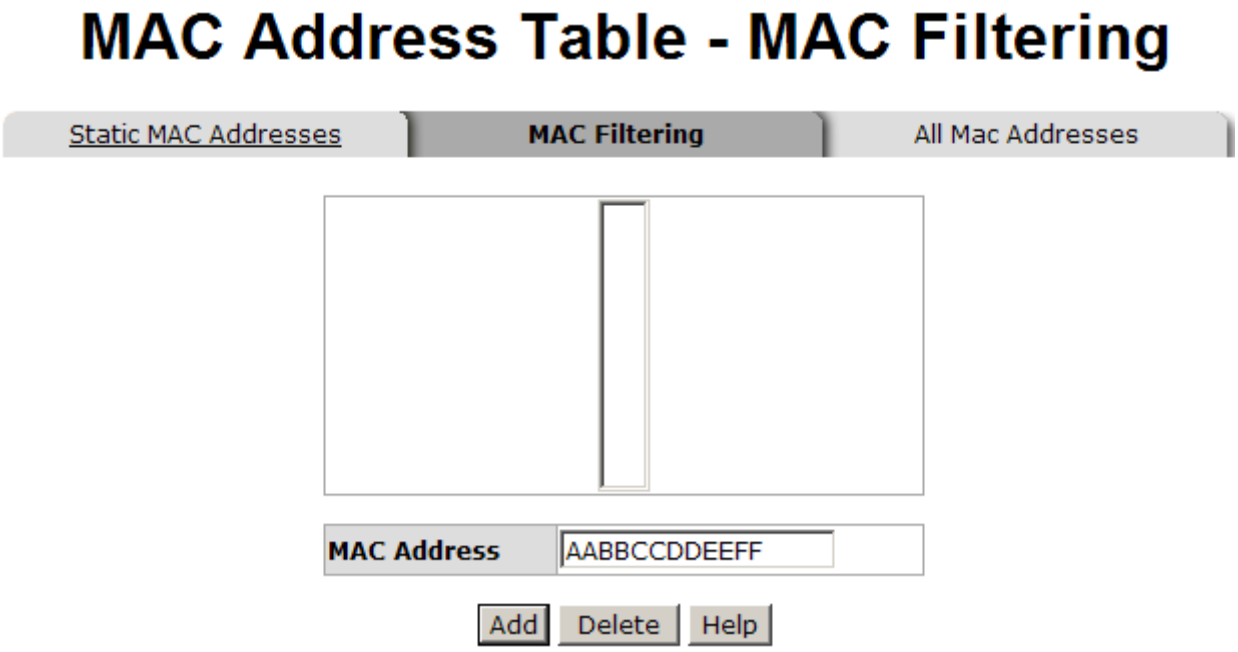
1. **MAC Address:** Enter the MAC address of the port that should permanently forward traffic regardless of the device network activity.
2. **Port No.:** Pull down the selection menu to select the port number.
3. Click Add .
4. If you want to delete the MAC address from filtering table, select the MAC address and click Delete .



Static MAC Addresses interface

MAC Filtering

By filtering MAC address, the switch can easily filter pre-configured MAC address and reduce the un-safety. You can add and delete filtering MAC address.



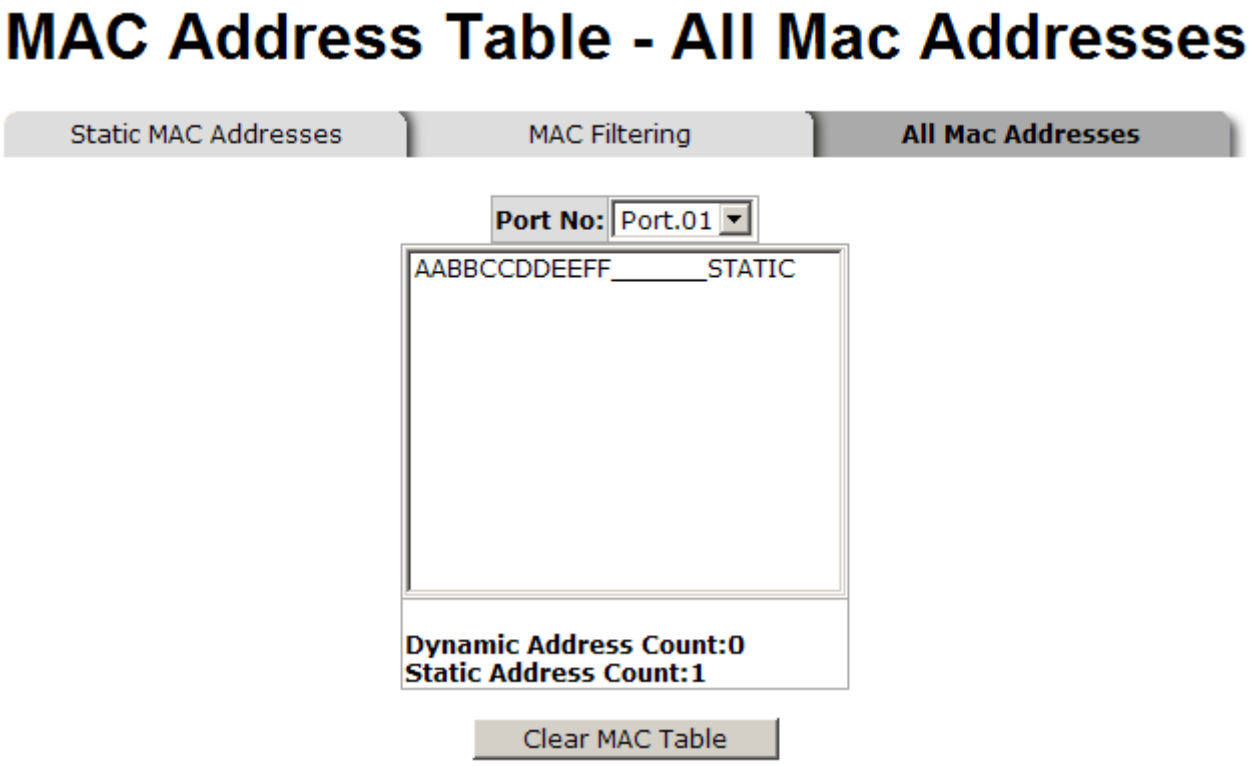
MAC Filtering interface

1. **MAC Address:** Enter the MAC address that you want to filter.
2. Click Add.
3. If you want to delete the MAC address from filtering table, select the MAC address and click Delete.

All MAC Addresses

You can view the port information of the connected device's MAC address and related devices' MAC address.

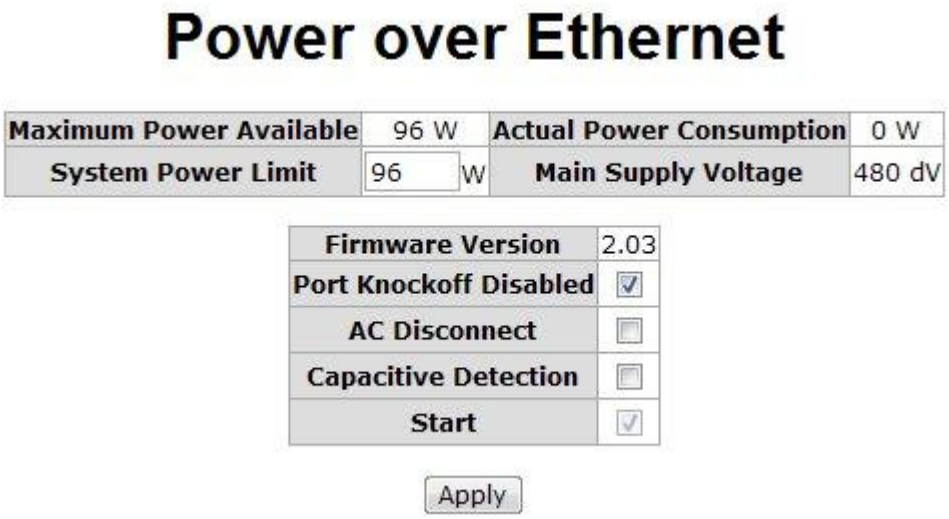
1. Select the port.
2. The selected port of dynamic & static MAC address information will be displayed here.
3. Click Clear MAC Table to clear the current port static MAC address information on screen.



All MAC Address interface

Power over Ethernet

This segment shows the Power over Ethernet function.



PoE Status

- **Maximum Power Available:** Displays the maximum power supply in Watt.
- **Actual Power Consumption:** This column shows the real-time total power consumption.
- **System Power Limit:** User can modify the value to this column field 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 chip's firmware version.
- **Port Knockoff Disabled:** 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:** Tick this checkbox 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:** Showing with a tick symbol, the system initializes and resets successfully.
- And then, click Apply to carry into effect.
- **Port:** The index of PoE ports.
- **Enable State:** Check it to enable the PoE function to the port.
- **Power Limit From:** Check it to decide the power limit method.
  - **Classification**: When this check box is ticked, the system will limit the power supply to the powered device in accordance with the related class.
- **Legacy:** Check it to support the legacy power devices.
- **Priority:** Pull down the selection menu item to choose the priority of power supplying.
- **Port Limit (<15400) mW:** User can key in the power limit value which is under 15.4 Watts.
- **Mode:** Displays the operating mode of the port.
- **Current (mA):** Displays the operating current of the port.
- **Voltage (V):** Displays the operating voltage of the port.
- **Power (mW):** Displays the power consumption of the port.
- **Determined Class:** Displays the PD's class.
- And then, click Apply to carry into effect.

Factory Default

Reset switch to default configuration. Click Reset to reset all configurations to the default value.

Factory Default interface

Save Configuration

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

Save Configuration interface

System Reboot

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

System Reboot interface

Troubleshooting

This section is intended to help solve the most common problems on the PoE Managed Switch.

Incorrect connections

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

■ Faulty or loose cables

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

■ Non-standard cables

Non-standard and miss-wired cables may cause numerous network collisions and other network problem, and can seriously impair network performance. A category 5e/6-cable tester is a recommended tool for network installation.

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

■ Improper Network Topologies

It is important to make sure that you have a valid network topology. Common topology

faults include excessive cable length and too many repeaters (hubs) between end nodes. In addition, you should make sure that your network topology contains no data path loops. Between any two end nodes, there should be only one active cabling path at any time. Data path loops will cause broadcast storms that will severely impact your network performance.

Diagnosing LED Indicators

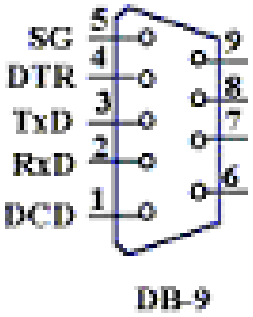
To assist in identifying problems, the Switch can be easily monitored through panel indicators, which describe common problems the user may encounter and where the user can find possible solutions.

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

Appendix

Console Port Pin Assignments

The DB-9 serial port on the switch is used to connect to the switch for out-of-band console configuration. The console—command line interface can be accessed from a terminal or a PC running a terminal emulation program. The pin assignments used to connect to the serial port are provided in the following tables.



DB-9 Console Port Pin Numbers

- **DB-9 Port Pin Assignments**

EIA Circuit	CCITT Signal	Description	Switch's DB9 DTE Pin #	PC DB9 DTE Pin #
BB	104	RxD (Received Data)	2	2
BA	103	TxD (Transmitted Data)	3	3
AB	102	SGND (Signal Ground)	5	5

- **Console Port to 9-Pin DTE Port on PC**

Switch's 9-Pin Serial Port	CCITT Signal PC's 9-Pin	DTE Port
2 RXD	<---------RXD ----------	3 TxD
3 TXD	----------TXD --------->	2 RxD
5 SGND	----------SGND ----------	5 SGND