Lantech

4 10/100/1000TX plus 4 Mini GBIC Managed Switch

MODEL: LGS-2404

User Manual

Notice

This manual contents are based on the below table listing software kernel version, hardware version, and firmware version. If the switch functions have any different from the manual contents description, please contact the local sale dealer for more information.

Firmware Version	V1.03
Kernel Version	V1.30
Hardware Version	----------

FCC Warning

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

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

CE Mark Warning

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

Content

Introduction

The 4 10/100/1000TX plus 4 Mini GBIC Managed Switch is a multi-port switch that can be used to build high-performance switched workgroup networks. It provides wire-speed, Gigabit Ethernet switching function that allows high-performance, low-cost connection. The Switches feature a store-and-forward switching and it can auto-learn and store source address on an 8K-entry MAC address table.

The 4 10/100/1000TX plus 4 Mini GBIC Managed Switch has 4 auto-sensing 10/100/1000Base-TX RJ-45 ports and 4 Mini GBIC port for higher connection speed.

Features

- 4-port 10/100/1000TX plus 4 Mini GBIC for SFP transceiver
- Confirms to IEEE802.3 10BASE-T, 802.3u 100BASE-TX, 802.3z Gigabit fiber and IEEE 802.3ab 1000Base-T
- IGMP snooping and Query mode support for Multi-Media application
- 16Gbps switch fabric
- 23.8Mpps throughput
- 802.1p CoS, per port 4 queues
- IEEE802.3x Flow control
  - Flow control for full duplex
  - Back pressure for half duplex
- Port Based VLAN /802 .1Q VLAN
- IEEE802.3ad Port trunk with LACP
- Spanning tree protocol
  - STP / Rapid STP
- QoS for below method:
  - Port based / Tag based
  - IPv4 ToS/ Ipv4, IPv6 DiffServe
- Port mirror and bandwidth control

- IEEE 802.1x user authentication
- Supports GVRP and MVR function
- Broadcast storm filter
- DHCP Client, Relay, Server
- Per port band width control
- SNTP and SMTP support
- Management IP address security
- MAC address security
- System log
- SNMP Trap support
- Configuration up-load and down-load
- TFTP firmware update
- SNMP/Web/ Telnet/CLI/Menu Driven management

Software Feature

Management	SNMP v1, SNMP v2c, SNMP v3, Telnet, Console (Command line interface), Web management
RFC standard	RFC2233 MIBII, RFC 1157 SNMP MIB, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC 2665 Ethernet like MIB, RFC1215 Trap MIB, RFC 2819 RMON MIB, Private MIB, RFC2030 SNTP, RFC 2821 SMTP, RFC 1757 RMON1 MIB
SNMP Trap	Up to 3 trap station Cold start, warm start, port link down, port link up, authentication failure, Private Trap for power status, X-ring topology change
Software Upgrade	TFTP firmware upgradeable. TFTP backup and restore.

Port Trunk with LACP	Support IEEE802.3ad with LACP function. Up to 4 trunk groups and maximum group member up to 4 ports.
Spanning Tree	IEEE802.1d Spanning tree IEEE802.1w Rapid spanning tree
VLAN	Port Based VLAN IEEE 802.1Q Tag VLAN (256 entries)/ VLAN ID (Up to 4K, VLAN ID can be assigned from 1 to 4096.) GVRP (256 Groups) Double Tag VLAN (Q in Q)* Private VLAN**
Class of Service	Support IEEE802.1p class of service, Per port supports 4 queues.
Quality of service	Port based, Tag based, IPv4 Type of service, IPv4/IPv6 Different service.
IGMP	Support IGMP snooping v1,v2 256 multicast groups and IGMP query
Port Security	Support 100 entries of MAC address for static MAC and another 100 for MAC filter
Port Mirror	Global system supports 3 mirroring types: "RX, TX and Both packet".
Bandwidth Control	Support ingress packet filter and egress packet limit The egress rate control supports all of packet type and the limit rates are 100K~256000Kbps Ingress filter packet type combination rules are Broadcast/Multicast/Unknown Unicast packet,

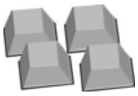
	Broadcast/Multicast packet, Broadcast packet only and all of packet. The packet filter rate can be set from 100k to 250Mbps
Login Security	Support IEEE802.1x User-Authentication and can report to RADIUS server. ■ Reject ■ Accept ■ Authorize ■ Disable
IP Security	Provide IP management security function with 10 IP addresses.
DHCP	DHCP Client, IP relay and DHCP Server. DHCP server provides port based and system based IP pool.
System log	Support System log record and remote system log server
DNS	Provide DNS client feature and support Primary and Secondary DNS server.
SNTP	Support SNTP to synchronize system clock in Internet
SMTP	Support SMTP Server and 6 e-mail accounts for receiving event alert
Configuration upload and download	Support text format configuration file for system quick configuration.

Package Contents

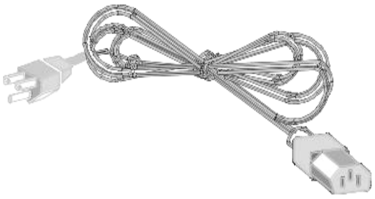
Unpack the contents of the 4 10/100/1000TX plus 4 Mini GBIC Managed Switch and verify them against the checklist below.

- 4 10/100/1000TX plus 4 Mini GBIC Managed Switch
- Power Cord
- Four Rubber Feet
- RS-232 cable
- User Manual

4 10/100/1000TX plus 4 MINI GBIC Managed Switch



Four Rubber Pads



Power Cord

RS-232 cable

User Manual

Compare the contents of the 4 10/100/1000TX plus 4 Mini GBIC Managed Switch package with the standard checklist above. If any item is missing or damaged, please contact your local dealer for service.

Hardware Description

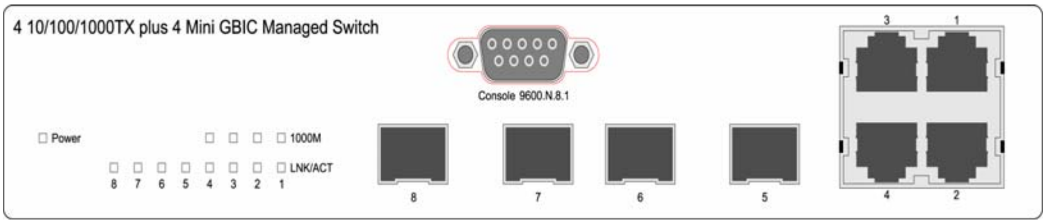
This section mainly describes the hardware of the 4 10/100/1000TX plus 4 Mini GBIC Managed Switch.

Physical Dimension

The physical dimensions of the 4 10/100/1000TX plus 4 Mini GBIC Managed Switch is **217mm(W) x 140mm(D) x 43mm(H)**

Front Panel

The Front Panel of the 4 10/100/1000TX plus 4 Mini GBIC Managed Switch consists of 4x auto-sensing 10/100/1000Mbps Ethernet RJ-45 ports (automatic MDI/MDIX), 4 Mini GBIC ports, and the LED indicators are also located on the frond panel of the switch.

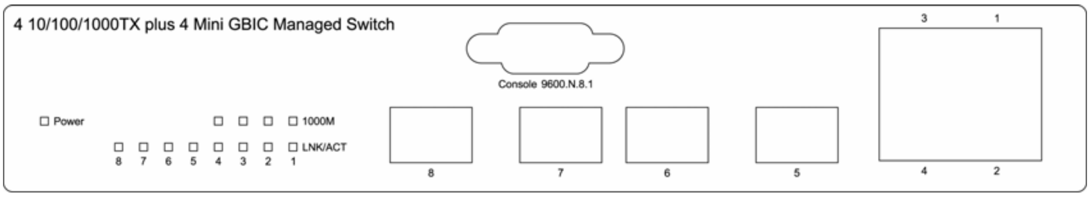


Front Panel of the 4 10/100/1000TX plus 4 Mini GBIC Managed Switch

- **RJ-45 Ports (Auto MDI/MDIX):** 4 10/100/1000 auto-sensing for 10Base-T or 100Base-TX or 1000Base-T connections.
  In general, MDI means connecting to another Hub or Switch while MDIX means connecting to a workstation or PC. Therefore, **Auto MDI/MDIX** means that user can connect to another Switch or workstation without changing non-crossover or crossover cabling.

- **4 Mini GBIC port:** 4 Mini GBIC ports for Gigabit fiber.

LED Indicators



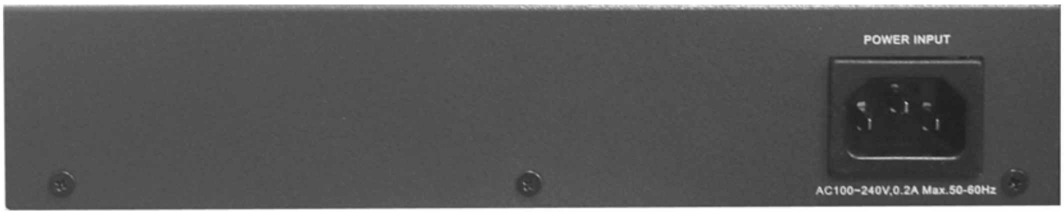
LED Indicators

The following table provides descriptions of the LED statuses and meaning. They provide a real-time indication of systematic operation status.

LED	Status	Description
Power	Green	Power On
1000M	Green	The port is operating at the speed of 1000Mbps.
	Off	The port is operating at the speed of 100/10Mbps or no device attached
LNK / ACT	Green	The port is successfully connecting with the device.
	Blinks	The port is receiving or transmitting data.
	Off	No device attached.

Rear Panel

The 3-pronged power plug are located at the Rear Panel of the 4 10/100/1000TX plus 4 Mini GBIC Managed Switch as shown in figure. The Switches will work with AC in the range 100-240V AC, 50-60Hz.



Rear Panel of the 4 10/100/1000TX plus 4 Mini GBIC Managed Switch

Desktop Installation

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

Attaching Rubber Feet

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

Power On

Connect the power cord to the power socket on the rear panel of the Switch. The other side of power cord connects to the power outlet. The internal power works with AC in the voltage range 100-240VAC, frequency 50~60Hz. Check the power indicator on the front panel to see if power is properly supplied.

Network Application

This section provides you a few samples of network topology in which the switch is used. In general, the 4 10/100/1000TX plus 4 Mini GBIC Managed Switch is designed to be used as a desktop or segment switch.

Desktop Application

The 4 10/100/1000TX plus 4 Mini GBIC Managed Switch is designed to be a desktop size switch that is an ideal solution for small workgroup. The Switch can be used as a standalone switch to which personal computers, server, printer server are directly connected to form small workgroup.

Segment Application

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

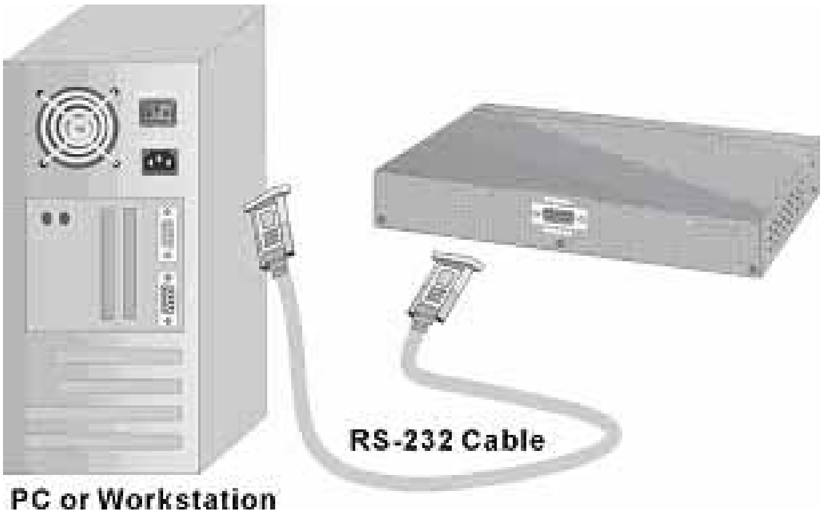
You can use the 4 10/100/1000TX plus 4 Mini GBIC Managed Switch to connect PCs, workstations, and servers to each other by connecting these devices directly to the Switch. All the devices in this network can communicate with each other. Connecting servers to the backbone switch allow other users to access the server's data.

The switch automatically learns node address, which are subsequently used to filter and forward all traffic based on the destination address. You can use any of the RJ-45 port of the 4 10/100/1000TX plus 4 Mini GBIC Managed Switch to connect with another Switch or Hub to interconnect each of your small-switched workgroups to form a larger switched network.

Console Management

Connecting to the Console Port

Use the supplied RS-232 cable to connect a terminal or PC to the console port. The terminal or PC to be connected must support the terminal emulation program.



Connecting the switch to a terminal via RS-232 cable

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:

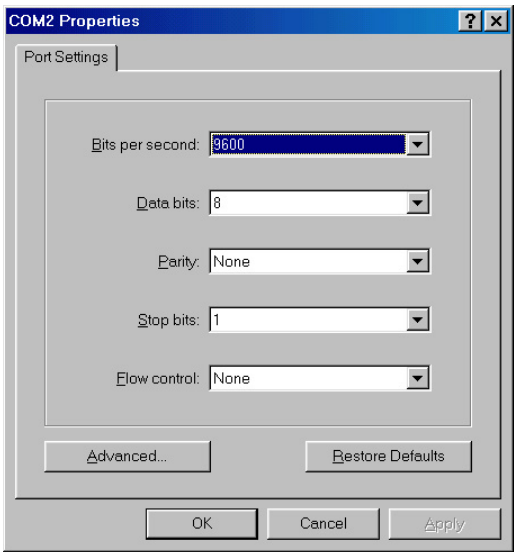
Baud Rate: 9600 bps

Data Bits: 8

Parity: none

Stop Bit: 1

Flow control: None



Bits per second: 9600

Data bits: 8

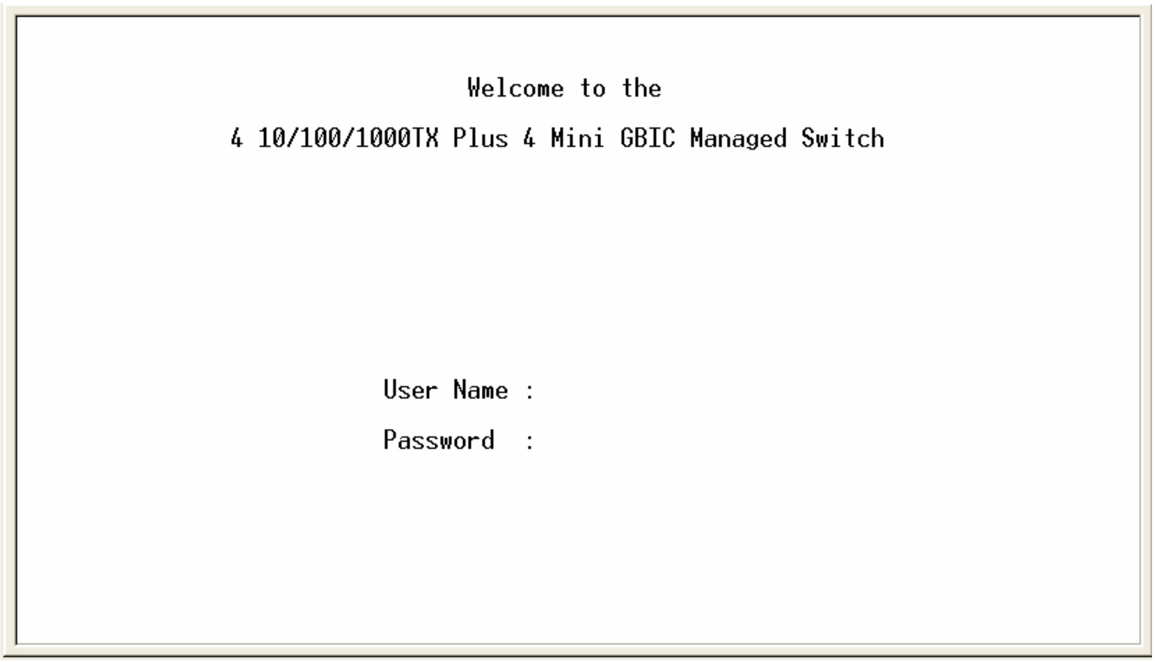
Parity: None

Stop bits: 1

Flow control: None

The settings of communication parameters

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

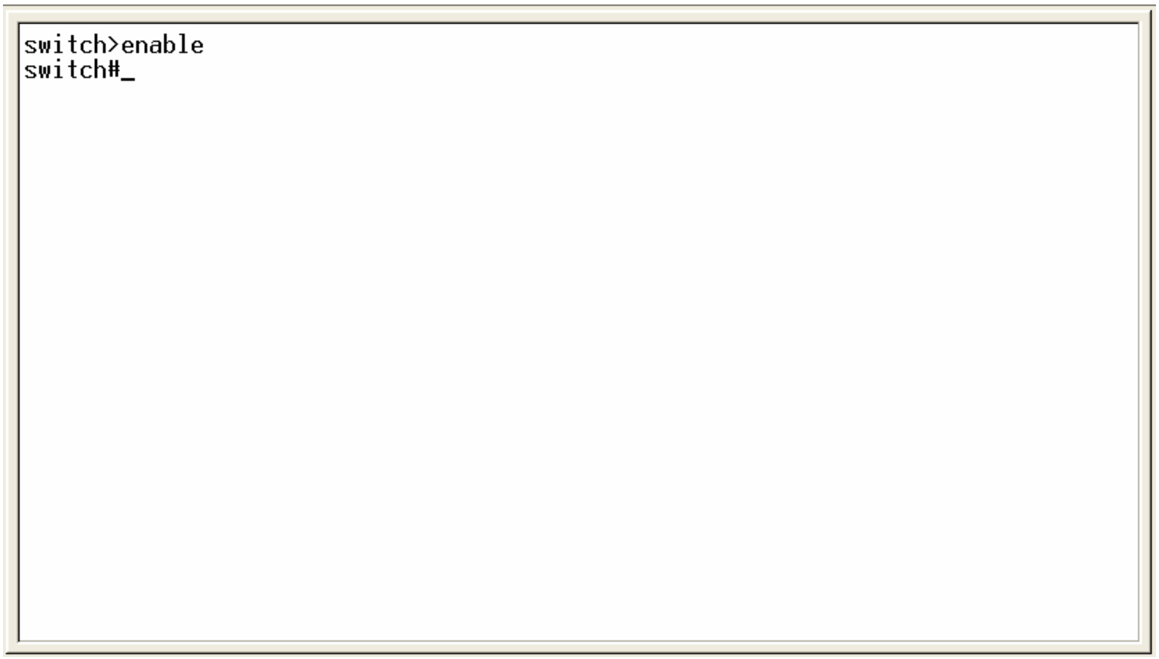


```
                 Welcome to the
   4 10/100/1000TX Plus 4 Mini GBIC Managed Switch




              User Name :
              Password  :
```

Console login interface

CLI Management

The system supports console management – CLI command. After you log in 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.



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

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 advance mode Privileged this mode to • Display advance function status • Save configures
Global Configuration	Enter the configure command while in privileged EXEC mode.	switch (config)#	To exit to privileged EXEC mode, enter exit or end	Use this mode to configure parameters that apply to your switch as a whole.
VLAN database	Enter the vlan database command while in privileged EXEC mode.	switch (vlan)#	To exit to user EXEC mode, enter exit.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the interface command (with a specific interface) while in global configuration mode	switch (config-if)#	To exit to global configuration mode, enter exit. To exist to privileged EXEC mode, or end.	Use this mode to configure parameters for the switch and Ethernet ports.

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

Commands Set List

System Commands Set

Netstar Commands	Level	Description	Example
show config	**E**	Show switch configuration	switch>**show config**
show terminal	**P**	Show console information	switch#**show terminal**
write memory	**P**	Save user configuration into permanent memory (flash rom)	switch#**write memory**
system name **[System Name]**	**G**	Configure system name	switch(config)#**system name xxx**
system location **[System Location]**	**G**	Set switch system location string	switch(config)#**system location xxx**
system description **[System Description]**	**G**	Set switch system description string	switch(config)#**system description xxx**
system contact **[System Contact]**	**G**	Set switch system contact window string	switch(config)#**system contact xxx**
show system-info	**E**	Show system information	switch>**show system-info**
ip address **[Ip-address]** **[Subnet-mask]** **[Gateway]**	**G**	Configure the IP address of switch	switch(config)#**ip address 192.168.1.1 255.255.255.0 192.168.1.254**
ip dhcp	**G**	Enable DHCP client function of switch	switch(config)#**ip dhcp**
show ip	**P**	Show IP information of	switch#**show ip**

		switch	
no ip dhcp	**G**	Disable DHCP client function of switch	switch(config)#**no ip dhcp**
reload	**G**	Halt and perform a cold restart	switch(config)#**reload**
default	**G**	Restore to default	switch(config)#**default**
admin username **[Username]**	**G**	Changes a login username. (maximum 10 words)	switch(config)#**admin username xxxxxx**
admin password **[Password]**	**G**	Specifies a password (maximum 10 words)	switch(config)#**admin password xxxxxx**
show admin	**P**	Show administrator information	switch#**show admin**
dhcpserver enable	**G**	Enable DHCP Server	switch(config)#**dhcpserver enable**
Dhcpserver disable	**G**	Disable DHCP Server	switch(config)#**no dhcpserver**
dhcpserver lowip **[Low IP]**	**G**	Configure low IP address for IP pool	switch(config)#**dhcpserver lowip 192.168.1.100**
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	switch#**show dhcpserver clients**

		DHCP server	
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

Netstar 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	switch(config)#**interface fastEthernet 2** switch(config-if)#**duplex full**

		Ethernet.	
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, multicast, and flooded unicast frame"	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-multicast-flooded-unicast**
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to "accept broadcast and multicast frame"	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-multicast**
bandwidth type	I	Set interface ingress	switch(config)#**interface**

broadcast-only		limit frame type to "only accept broadcast frame"	**fastEthernet 2** switch(config-if)#**bandwidth type broadcast-only**
bandwidth in **[Value]**	**I**	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth in 100**
bandwidth out **[Value]**		Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth out 100**
show bandwidth	**I**	Show interfaces bandwidth control	switch(config)#**interface fastEthernet 2** switch(config-if)#**show bandwidth**
state **[Enable | Disable]**	**I**	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#**interface fastEthernet 2** (config-if)#**state Disable**
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** (config-if)#**show interface status**
show interface accounting	**I**	show interface statistic counter	switch(config)#**interface fastEthernet 2** (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

Netstar Commands	Level	Description	Example
aggregator priority **[1~65535]**	**G**	Set port group system priority	switch(config)#**aggregator priority 22**
aggregator activityport **[Group ID]** **[Port Numbers]**	**G**	Set activity port	switch(config)#**aggregator activityport 2**
aggregator group **[GroupID] [Port-list]** **lacp** **workp** **[Workport]**	**G**	Assign a trunk group with LACP active. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount	switch(config)#**aggregator group 1 1-4 lacp workp 2** or switch(config)#**aggregator group 2 1,4,3 lacp workp 3**

		of member ports.	
aggregator group [GroupID] [Port-list] nolacp	G	Assign a static trunk group. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#**aggregator group 1 2-4 nolacp** or switch(config)#**aggregator group 1 3,1,2 nolacp**
show aggregator	P	Show the information of trunk group	switch#**show aggregator 1** or switch#**show aggregator 2** or switch#**show aggregator 3**
no aggregator lacp [GroupID]	G	Disable the LACP function of trunk group	switch(config)#**no aggreator lacp 1**
no aggregator group [GroupID]	G	Remove a trunk group	switch(config)#**no aggreator group 2**

VLAN Commands Set

Netstar 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	V	Add new port based VALN	switch(vlan)#**vlan port-based grpname test grpid 2 port 2-4**

[Group Name] **grpid** [GroupID] **port** [PortNumbers]			or switch(vlan)#**vlan port-based grpname test grpid 2 port 2,3,4**
show vlan [GroupID] or **show vlan**	V	Show VLAN information	switch(vlan)#**show vlan 23**
no vlan group [GroupID]	V	Delete port base group ID	switch(vlan)#**no vlan group 2**
IEEE 802.1Q VLAN			
vlan 8021q name [GroupName] **vid** [VID]	V	Change the name of VLAN group, if the group didn't exist, this command can't be applied.	switch(vlan)#**vlan 8021q name test vid 22**
vlan 8021q port [PortNumber] **access-link untag** [UntaggedVID]	V	Assign a access link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 access-link untag 33**
vlan 8021q port [PortNumber] **trunk-link tag** [TaggedVID List]	V	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 trunk-link tag 2,3,6,99** or switch(vlan)#**vlan 8021q port 3 trunk-link tag 3-20**
vlan 8021q port [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	V	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q port 3 hybrid-link untag 5 tag 6-8**
vlan 8021q trunk [PortNumber] **access-link untag** [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 access-link untag 33**

vlan 8021q trunk [PortNumber] trunk-link tag [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

Netstar 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 32767**
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	switch(config)#**spanning-tree max-age 15**

		the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	
spanning-tree hello-time [seconds]	**G**	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#**spanning-tree hello-time 3**
spanning-tree forward-time [seconds]	**G**	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)#**spanning-tree forward-time 20**
stp-path-cost [1~200000000]	**I**	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-cost 20**

		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.	
stp-path-priority **[Port Priority]**	**I**	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-priority 128**
stp-admin-p2p **[Auto|True|False]**	**I**	Admin P2P of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-p2p Auto**
stp-admin-edge **[True|False]**	**I**	Admin Edge of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-edge True**
stp-admin-non-stp **[True|False]**	**I**	Admin NonSTP of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-non-stp False**
show spanning-tree	**E**	Displays a summary of the spanning-tree states.	switch>**show spanning-tree**

no spanning-tree	**G**	Disable spanning-tree.	switch(config)#**no spanning-tree**

QOS Commands Set

Netstar 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

Netstar Commands	Level	Description	Example
igmp enable	**G**	Enable IGMP snooping function	switch(config)#**igmp enable**
Igmp-query auto	**G**	Set IGMP query to auto mode	switch(config)#**Igmp-query auto**
Igmp-query force	**G**	Set IGMP query to force mode	switch(config)#**Igmp-query force**
show igmp configuration	**P**	Displays the details of an IGMP configuration.	switch#**show igmp configuration**

show igmp multi	**P**	Displays the details of an IGMP snooping entries.	switch#**show igmp multi**
no igmp	**G**	Disable IGMP snooping function	switch(config)#**no igmp**
no igmp-query	**G**	Disable IGMP query	switch#**no igmp-query**

Mac / Filter Table Commands Set

Netstar 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

Netstar 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	**G**	Configure the access	switch(config)#**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]		table of SNMPV3 agent	**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 192.168.1.50**
no snmpv3 user [User Name]	**G**	Remove specified user of SNMPv3 agent.	switch(config)#**no snmpv3 user Test**
no snmpv3 access context-name [Context Name] group [Group Name]	**G**	Remove specified access table of SNMPv3 agent.	switch(config)#**no snmpv3 access context-name Test group G1 security-level AuthPr iv match-rule Exact views V1 V1 V1**

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

Port Mirroring Commands Set

Netstar 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 information	switch(config)#**interface fastEthernet 2** switch(config-if)#**show monitor**
no monitor	**I**	Disable source port of monitor function	switch(config)#**interface fastEthernet 2**

			switch(config-if)#**no monitor**

802.1x Commands Set

Netstar 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 1815**
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 1816**
8021x system sharekey [ID]	G	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# **8021x system sharekey 123456**
8021x system nasid [words]	G	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# **8021x system nasid test1**

8021x misc quietperiod [sec.]	**G**	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# **8021x misc quietperiod 10**
8021x misc txperiod [sec.]	**G**	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# **8021x misc txperiod 5**
8021x misc supportimeout [sec.]	**G**	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# **8021x misc supportimeout 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 |	**I**	Use the 802.1x port state interface	switch(config)#**interface fastethernet 3**

authorize]		configuration command to set the state of the selected port.	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

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

SystemLog, SMTP and Event Commands Set

Netstar 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 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 password	switch(config)#**smtp 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 X-ring-topology-change [Systemlog|SMTP|Both]	**G**	Set X-ring topology changed event type	switch(config)#**event X-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 X-ring-topology-change	**G**	Disable X-ring topology changed event type	switch(config)#**no event X-ring-topology-change**
no event systemlog	**I**	Disable port event for system log	switch(config)#**interface fastethernet 3** switch(config-if)#**no event systemlog**
no event smpt	**I**	Disable port event for SMTP	switch(config)#**interface fastethernet 3** switch(config-if)#**no event smtp**
show systemlog	**P**	Show system log client & server information	switch#**show systemlog**

SNTP Commands Set

Netstar 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,	switch(config)# **sntp daylight-period 20060101-01:01 20060202-01-01**

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

X-ring Commands Set

Netstar Commands	Level	Description	Example
Xring enable	G	Enable X-ring	switch(config)#**Xring enable**
Xring master	G	Enable ring master	switch(config)#**Xring master**
Xring couplering	G	Enable couple ring	switch(config)#**Xring couplering**

Xring dualhoming	**G**	Enable dual homing	switch(config)#**Xring dualhoming**
Xring ringport **[1st Ring Port] [2nd Ring Port]**	**G**	Configure 1st/2nd Ring Port	switch(config)#**Xring ringport 7 8**
Xring couplingport **[Coupling Port]**	**G**	Configure Coupling Port	switch(config)#**Xring couplingport 1**
Xring controlport **[Control Port]**	**G**	Configure Control Port	switch(config)#**Xring controlport 2**
Xring homingport **[Dual Homing Port]**	**G**	Configure Dual Homing Port	switch(config)#**Xring homingport 3**
show Xring	**P**	Show the information of X - Ring	switch#**show Xring**
no Xring	**G**	Disable X-ring	switch(config)#**no X ring**
no Xring master	**G**	Disable ring master	switch(config)# **no Xring master**
no Xring couplering	**G**	Disable couple ring	switch(config)# **no Xring couplering**
no Xring dualhoming	**G**	Disable dual homing	switch(config)# **no Xring dualhoming**

Web-Based Management

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

About Web-based Management

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

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

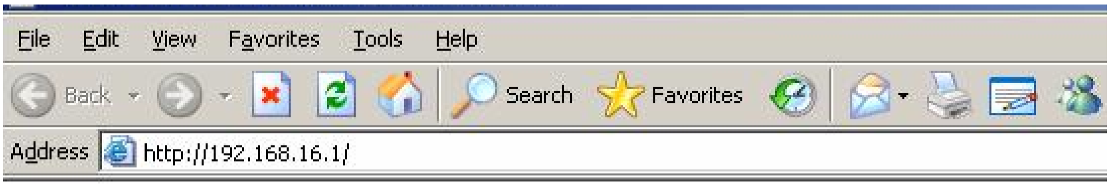
Preparing for Web Management

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

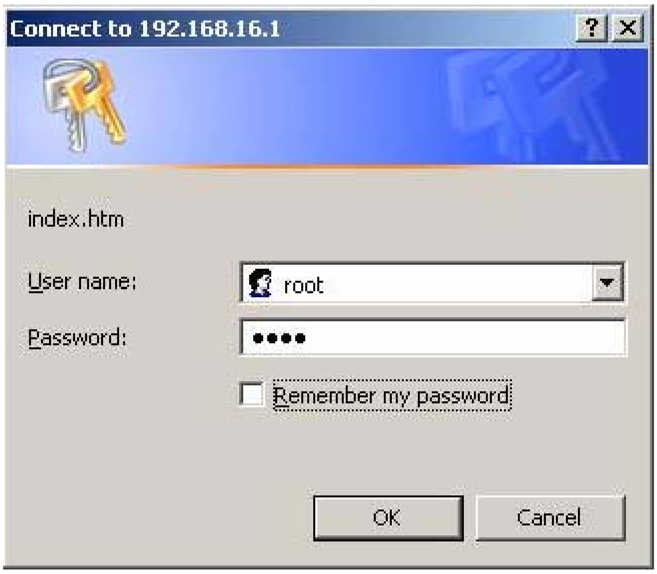
System Login

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



Address http://192.168.16.1/

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 "**OK**", and then the home screen of the Web-based management appears as below:



Connect to 192.168.16.1

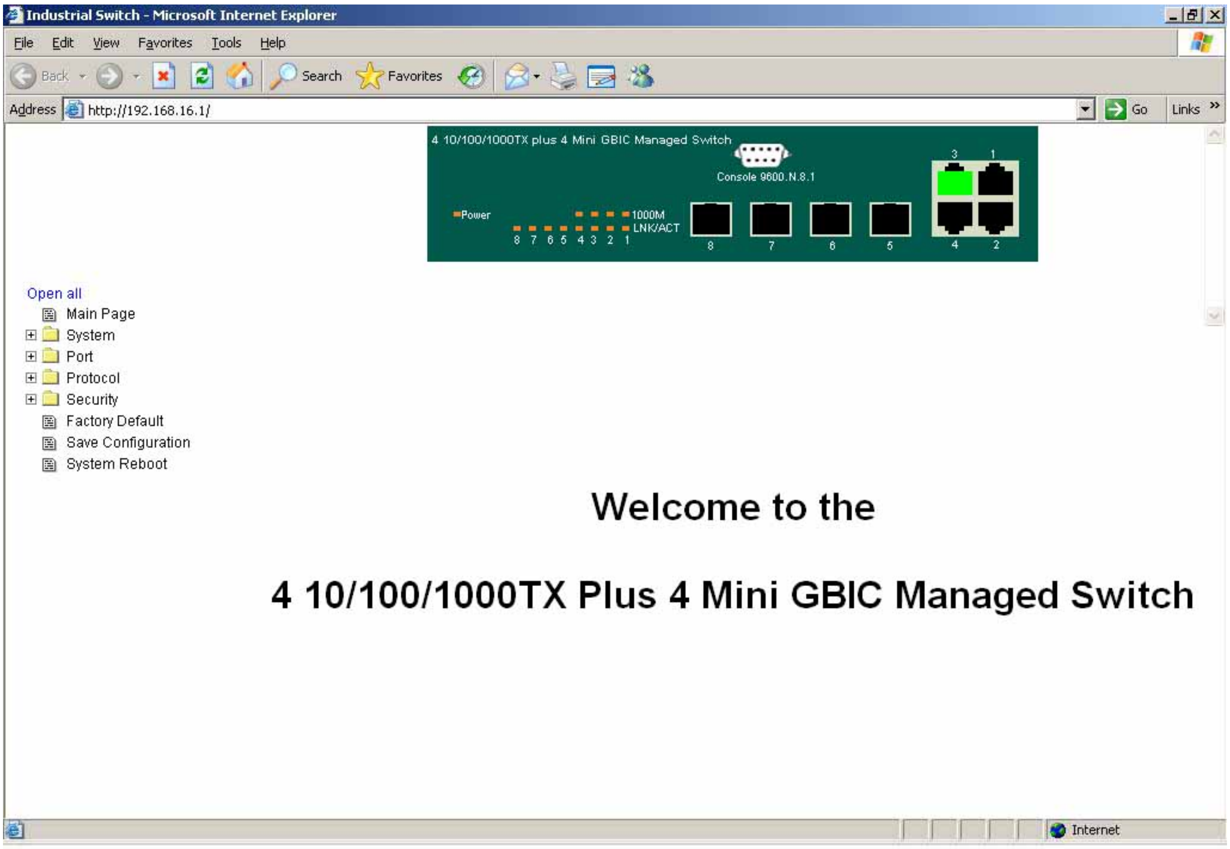
index.htm

User name: root

Password: ●●●●

□ Remember my password

Login screen



Welcome to the

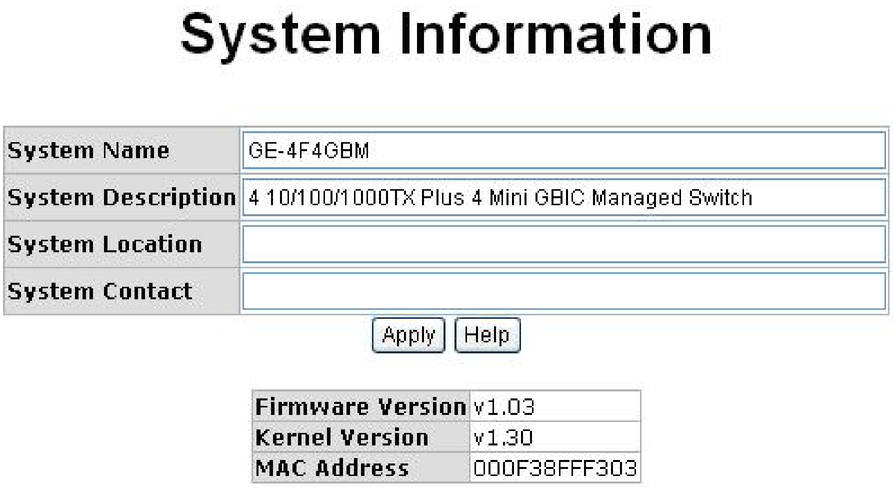
4 10/100/1000TX Plus 4 Mini GBIC Managed Switch

Main interface

System Information

Assigning the system name, location and view the system information

- **System Name:** Assign the name of switch. The maximum length is 64 bytes
- **System Description:** Displays the description of switch. Read only cannot be modified
- **System Location:** Assign the switch physical location. The maximum length is 64 bytes
- **System Contact:** Enter the name of contact person or organization
- **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)



System Information

System Name	GE-4F4GBM
System Description	4 10/100/1000TX Plus 4 Mini GBIC Managed Switch
System Location	
System Contact	

Firmware Version	v1.03
Kernel Version	v1.30
MAC Address	000F38FFF303

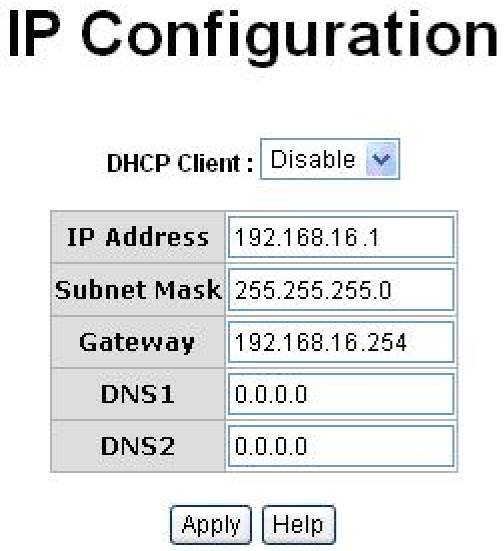
Switch settings interface

IP Configuration

User can configure the IP Settings and DHCP client function

- **DHCP Client:** To enable or disable the DHCP client function. When DHCP client function is enabling, the industrial switch will be assigned the IP address from the network DHCP server. The default IP address will be replace by the DHCP server assigned IP address. After user click “Apply” button, a popup dialog show up. It is to inform the user that when the DHCP client is enabling, the current IP will lose and user should find the new IP on the DHCP server. To cancel the enabling DHCP client function, click “cancel”
- **IP Address:** Assign the IP address that the network is using. If DHCP client function is enabling, and then user don’t need to assign the IP address. And, the network DHCP server will assign the IP address for the industrial switch and display in this column. The default IP is 192.168.16.1
- **Subnet Mask:** Assign the subnet mask of the IP address. If DHCP client function is enabling, and then user do not need to assign the subnet mask
- **Gateway:** Assign the network gateway for the industrial switch. 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 Apply button.



IP Configuration

DHCP Client : Disable

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

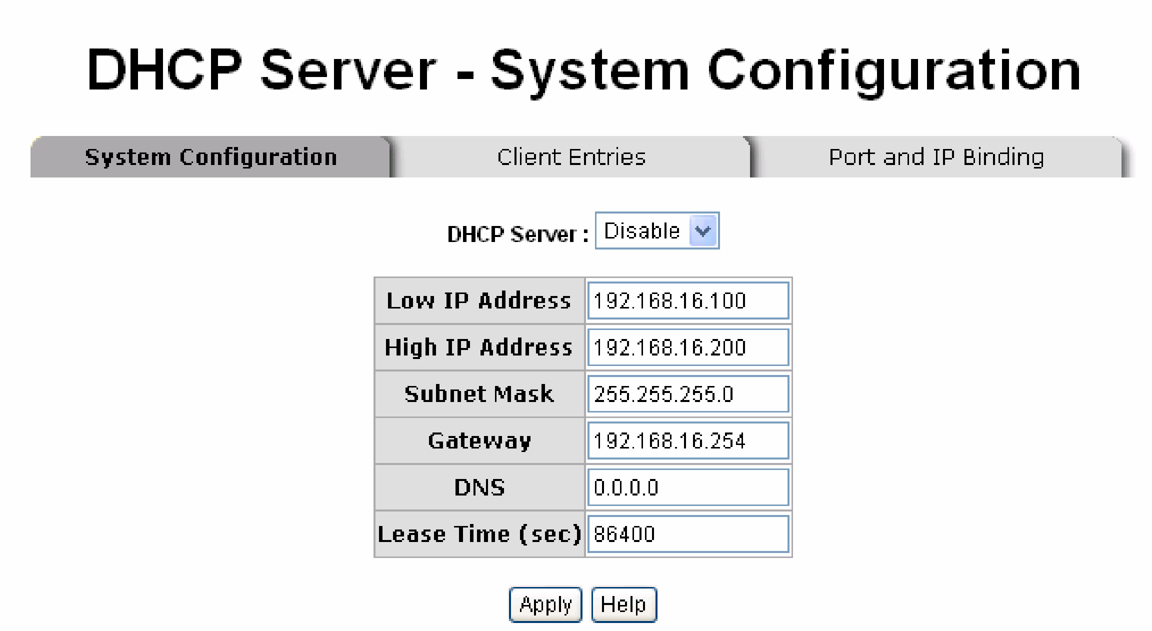
IP configuration interface

DHCP Server – System 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 assign range. Low IP address is the beginning of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 ~ 192.168.1.200. 192.168.1.100 will be the Low IP address.
- **High IP Address:** the dynamic IP assign range. High IP address is the end of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 ~ 192.168.1.200. 192.168.1.200 will be the High IP address.
- **Subnet Mask:** the dynamic IP assign range subnet mask.
- **Gateway:** the gateway in your network.
- **DNS:** Domain Name Server IP Address in your network.
- **Lease Time (sec):** It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server doesn’t know that the dynamic IP is idle.

- And then, click Apply



DHCP Server - System Configuration

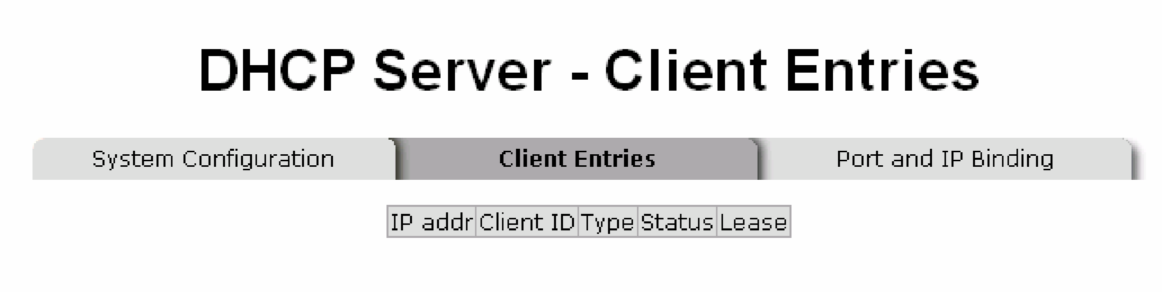
DHCP Server : Disable

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

DHCP Server Configuration interface

DHCP Client – System Configuration

When the DHCP server function is active, the system will collect the DHCP client information and display in here.



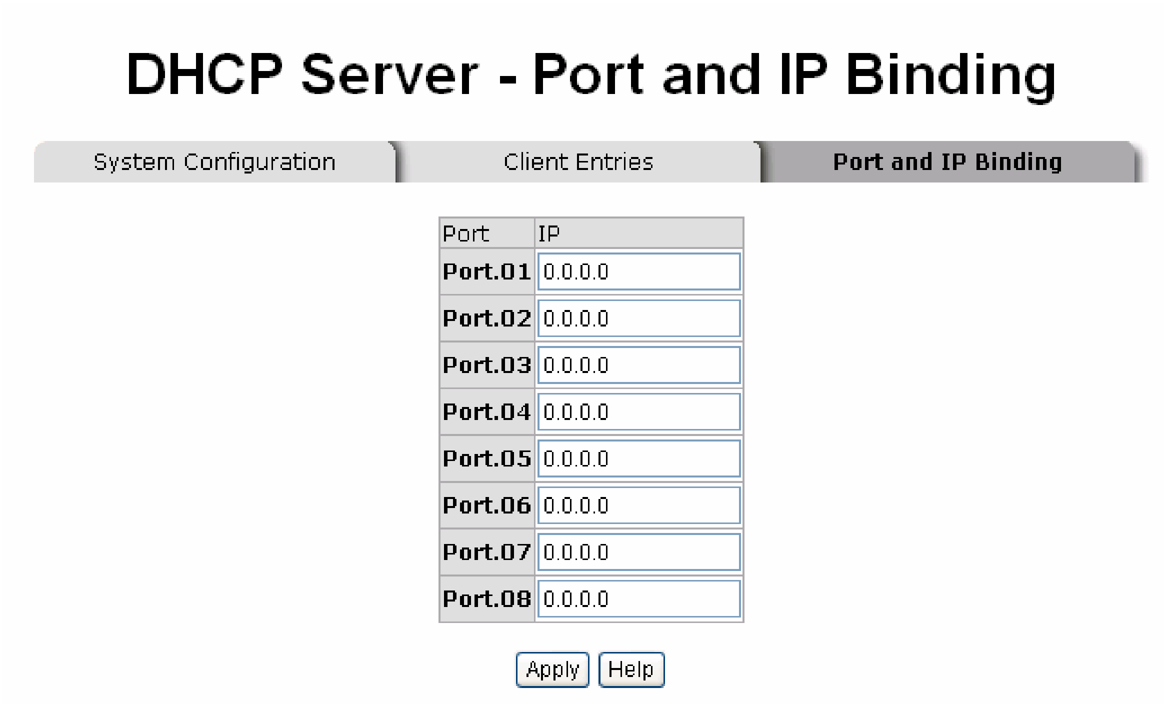
DHCP Server - Client Entries

IP addr	Client ID	Type	Status	Lease

DHCP Client Entries interface

DHCP Server - Port and IP Bindings

You can assign the specific IP address that is the IP in dynamic IP assign range to the specific port. When the device is connecting to the port and asks for dynamic IP assigning, the system will assign the IP address that has been assigned before to the connected device.



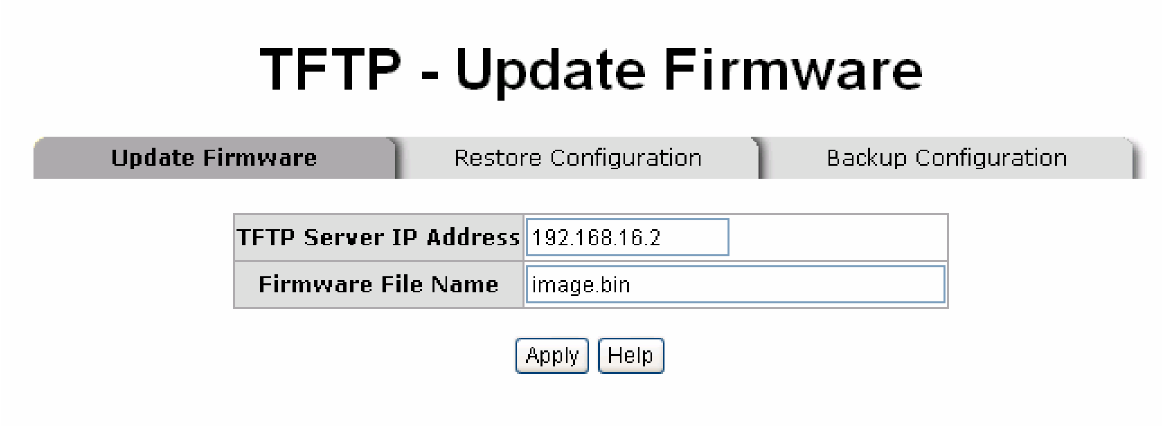
Port	IP
Port.01	0.0.0.0
Port.02	0.0.0.0
Port.03	0.0.0.0
Port.04	0.0.0.0
Port.05	0.0.0.0
Port.06	0.0.0.0
Port.07	0.0.0.0
Port.08	0.0.0.0

Port and IP Bindings interface

TFTP - Update Firmware

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

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



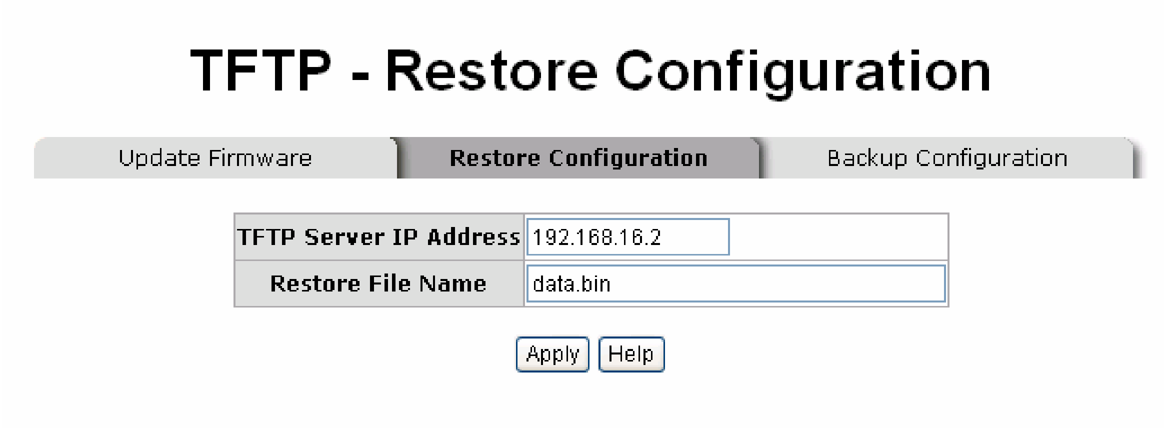
TFTP Server IP Address	192.168.16.2
Firmware File Name	image.bin

Update Firmware interface

TFTP – Restore Configuration

You can restore EEPROM value from TFTP server, but you must put back image in TFTP server, switch will download back flash image.

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



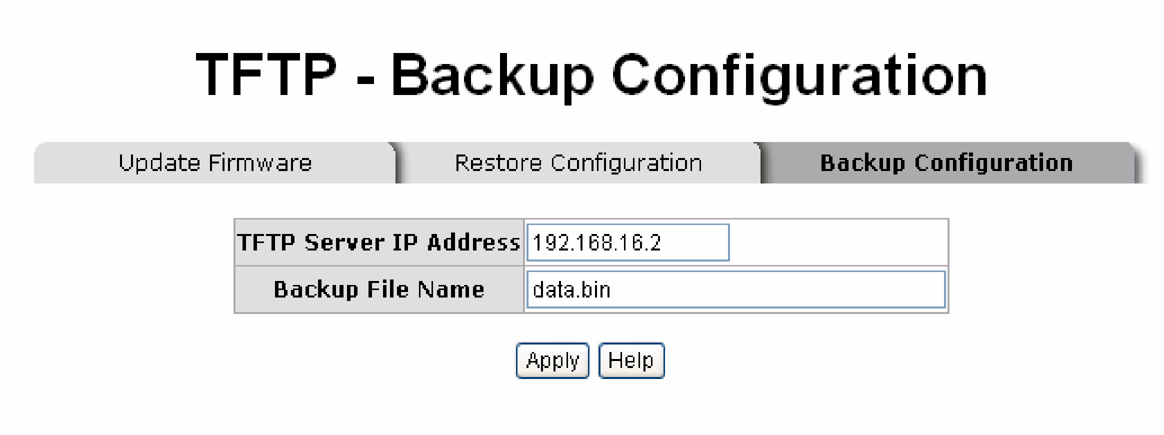
TFTP Server IP Address	192.168.16.2
Restore File Name	data.bin

Restore Configuration interface

TFTP - Backup Configuration

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

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



TFTP - Backup Configuration

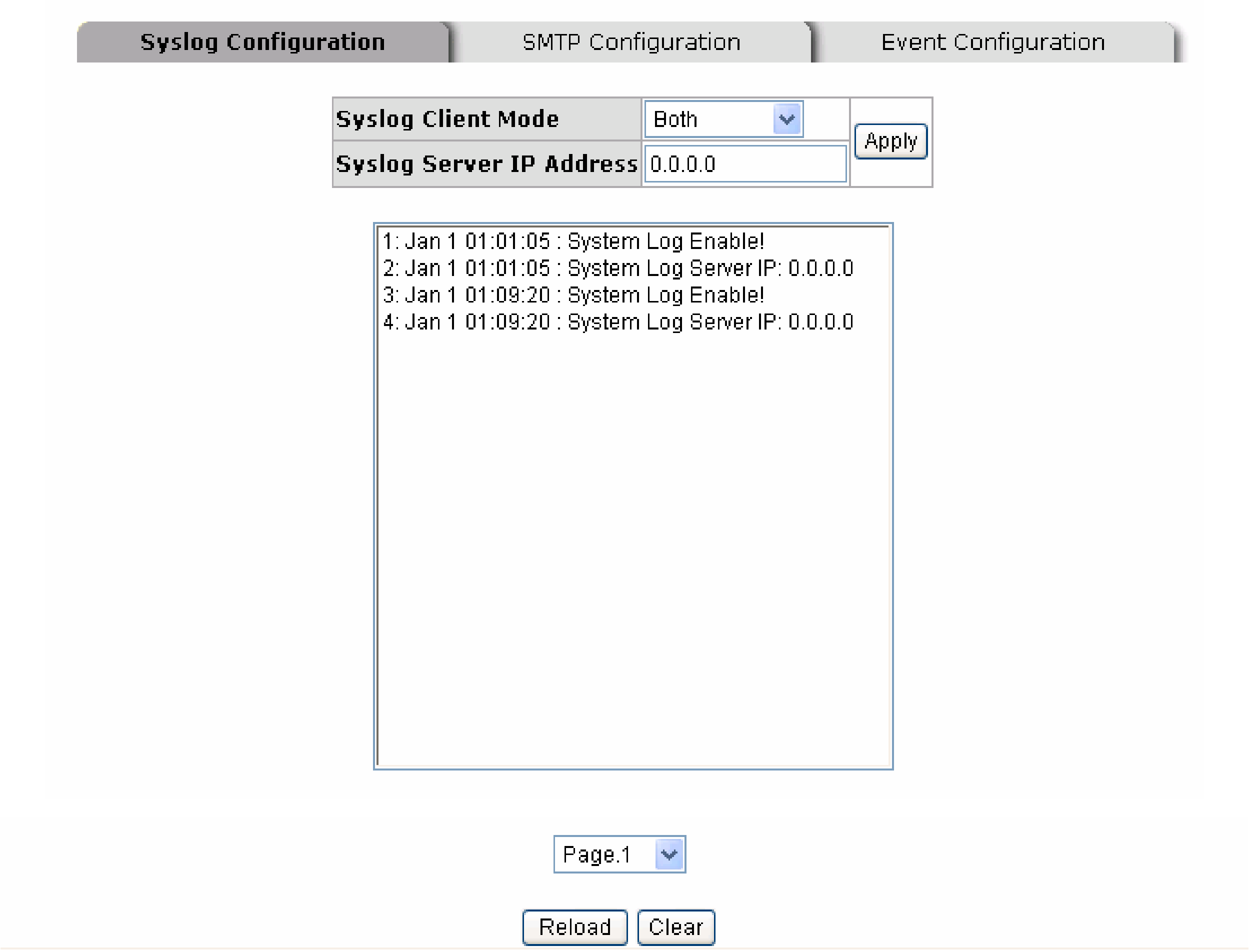
TFTP Server IP Address: 192.168.16.2
Backup File Name: data.bin

Backup Configuration interface

System Event Log – Syslog Configuration

Configuring the system event mode that want to be collected and system log server IP.

1. **Syslog Client Mode:** select the system log mode – client only, server only, or both S/C.
2. **System Log Server IP Address:** assigned the system log server IP.
3. Click Reload to refresh the events log.
4. Click Clear to clear all current events log.
5. After configuring, Click Apply.



Syslog Client Mode: Both

Syslog Server IP Address: 0.0.0.0

```
1: Jan 1 01:01:05 : System Log Enable!
2: Jan 1 01:01:05 : System Log Server IP: 0.0.0.0
3: Jan 1 01:09:20 : System Log Enable!
4: Jan 1 01:09:20 : System Log Server IP: 0.0.0.0
```

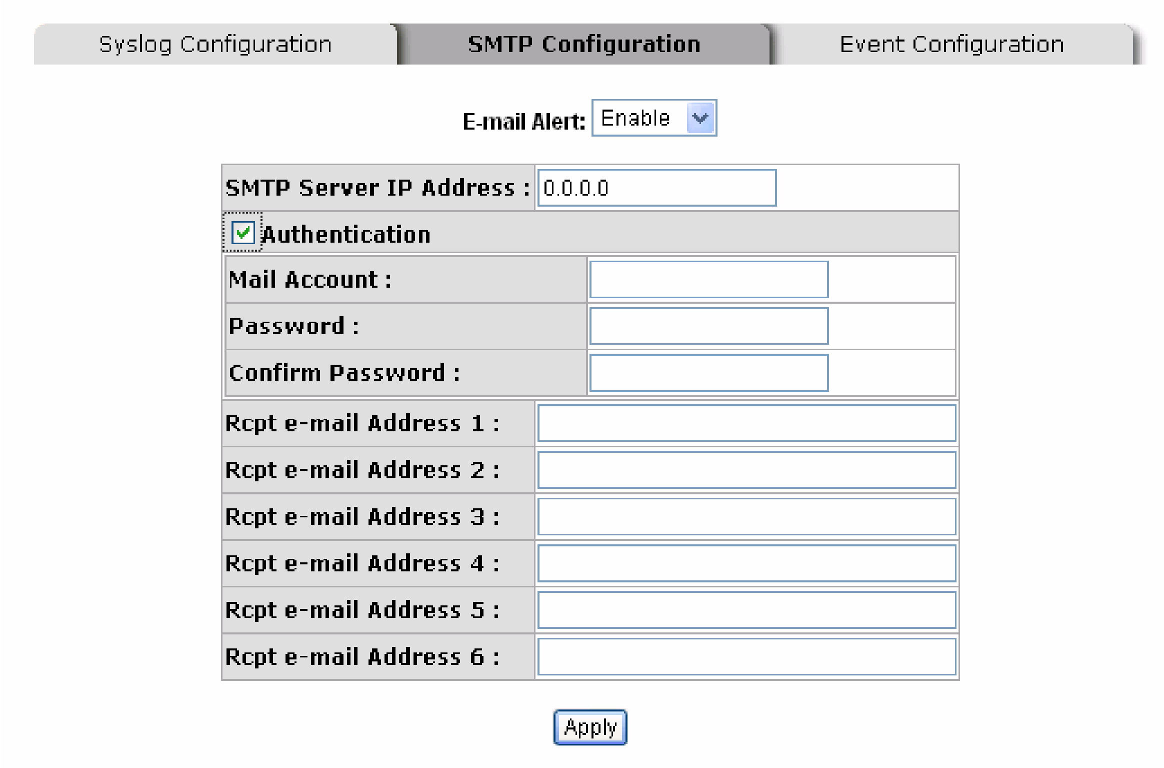
Syslog Configuration interface

System Event Log - SMTP Configuration

You can set up the mail server IP, mail account, account password, and forwarded email account for receiving the event alert.

1. **Email Alert:** enable or disable the email alert function.
2. **SMTP Server IP:** set up the mail server IP address (when **Email Alert** enabled, this function will then be available)..
3. **Authentication:** mark the check box to enable and configure the email account and password for authentication (when **Email Alert** enabled, this function will then be available)..
4. **Mail Account:** set up the email account, e.g. johnadmin@123.com, to receive the alert. It must be an existing email account on the mail server, which you had set up in **SMTP Server IP Address** column.

5. **Password:** The email account password.
6. **Confirm Password:** reconfirm the password.
7. **Rcpt e-mail Address 1 ~ 6:** you can assign up to 6 e-mail accounts also to receive the alert.
8. Click Apply.



Syslog Configuration | SMTP Configuration | Event Configuration

E-mail Alert: Enable

SMTP Server IP Address :	0.0.0.0
☑ Authentication	
Mail Account :	
Password :	
Confirm Password :	
Rcpt e-mail Address 1 :	
Rcpt e-mail Address 2 :	
Rcpt e-mail Address 3 :	
Rcpt e-mail Address 4 :	
Rcpt e-mail Address 5 :	
Rcpt e-mail Address 6 :	

Apply

SMTP Configuration interface

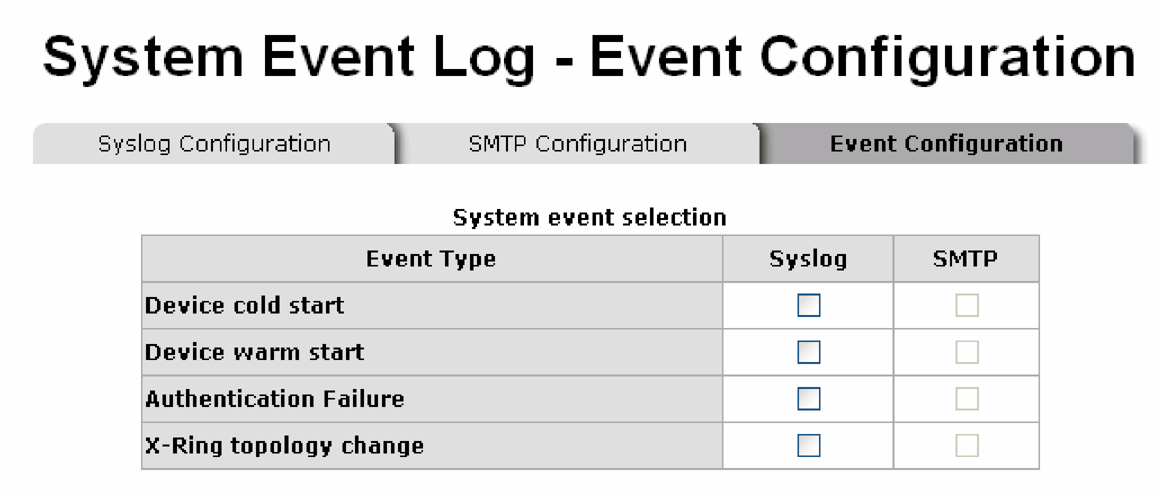
System Event Log - Event Configuration

You can select the system log events and SMTP events. When selected events occur, the system will send out the log information. Also, per port log and SMTP events can be selected. After configure, Click Apply.

- **System event selection:** 4 selections – Device cold start, Power status, SNMP Authentication Failure, and X-ring topology change. Mark the checkbox to select the event. When selected events occur, the system will issue the logs.
  - **Device cold start:** when the device executes cold start action, the system will

issue a log event.

- **Device warm start:** when the device executes warm start, the system will issue a log event.
- **Authentication Failure:** when the SNMP authentication fails, the system will issue a log event.
- **X-ring topology change:** when the X-ring topology has changed, the system will issue a log event.



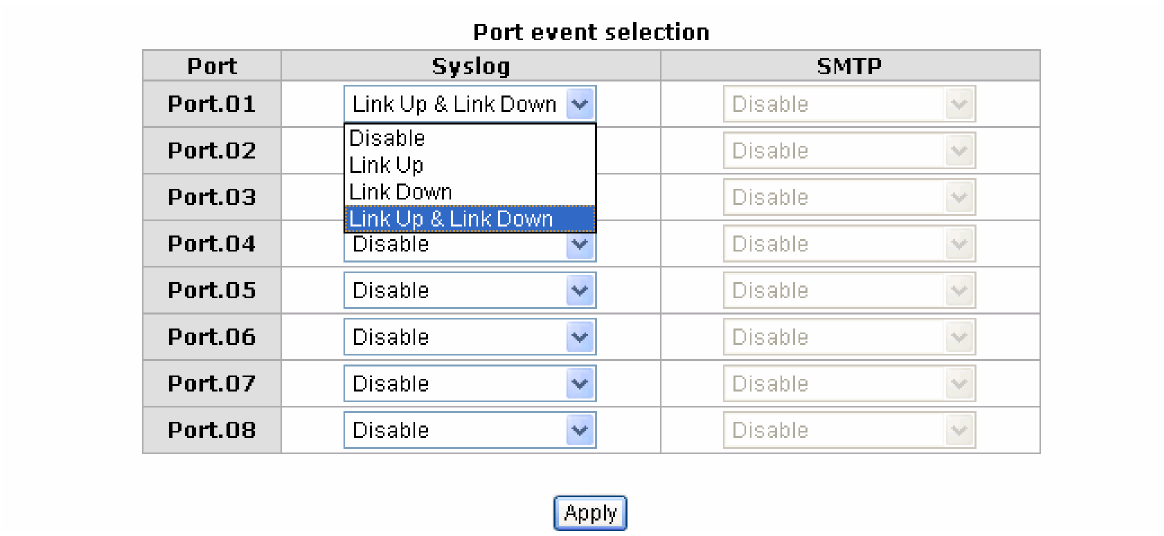
System Event Log - Event Configuration

System event selection

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

Event Configuration interface

- **Port event selection:** select the per port events and per port SMTP events. It has 3 selections – Link UP, Link Down, and Link UP & Link Down. Disable means no event is selected.
  - **Link UP:** the system will issue a log message when port connection is up only.
  - **Link Down:** the system will issue a log message when port connection is down only.
  - **Link UP & Link Down:** the system will issue a log message when port connection is up and down.



Port event selection

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

Event Configuration interface

SNTP Configuration

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

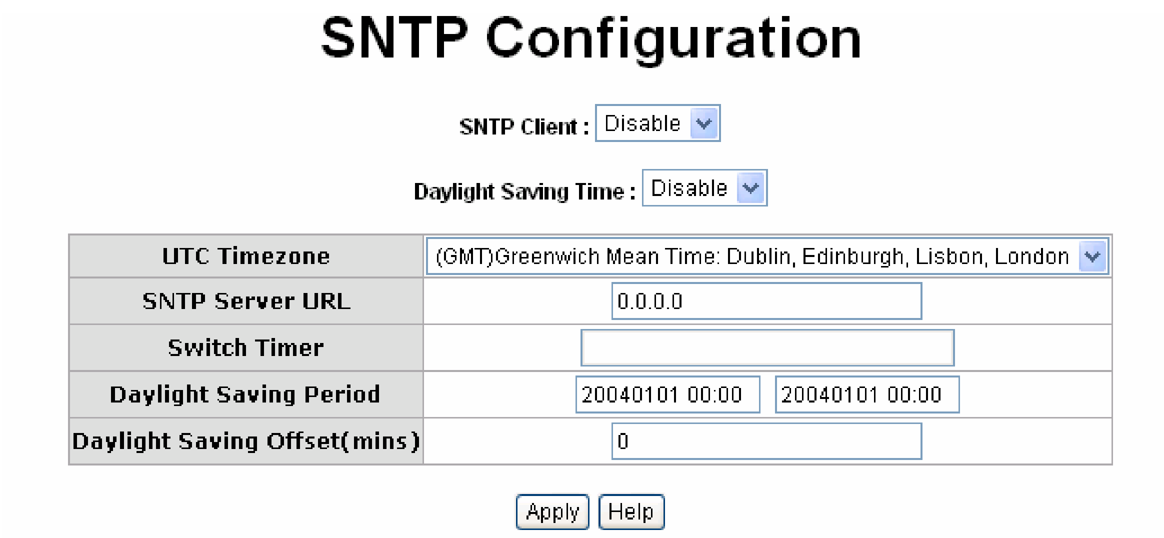
1. **SNTP Client:** enable or disable SNTP function to get the time from the SNTP server.
2. **Daylight Saving Time:** enable or disable daylight saving time function. When daylight saving time is enabling, user need to configure the daylight saving time period..
3. **UTC Timezone:** set the switch location time zone. The following table lists the different location time zone for 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	-4 hours	8 am

EDT - Eastern Daylight		
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

4. **SNTP Sever URL:** set the SNTP server IP address.
5. **Switch Timer:** display the switch current time.
6. **Daylight Saving Period:** set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different in every year.
7. **Daylight Saving Offset (mins):** set up the offset time.
8. Click Apply.



SNTP Configuration

SNTP Client : Disable

Daylight Saving Time : Disable

UTC Timezone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
SNTP Server URL	0.0.0.0
Switch Timer	
Daylight Saving Period	20040101 00:00 | 20040101 00:00
Daylight Saving Offset(mins)	0

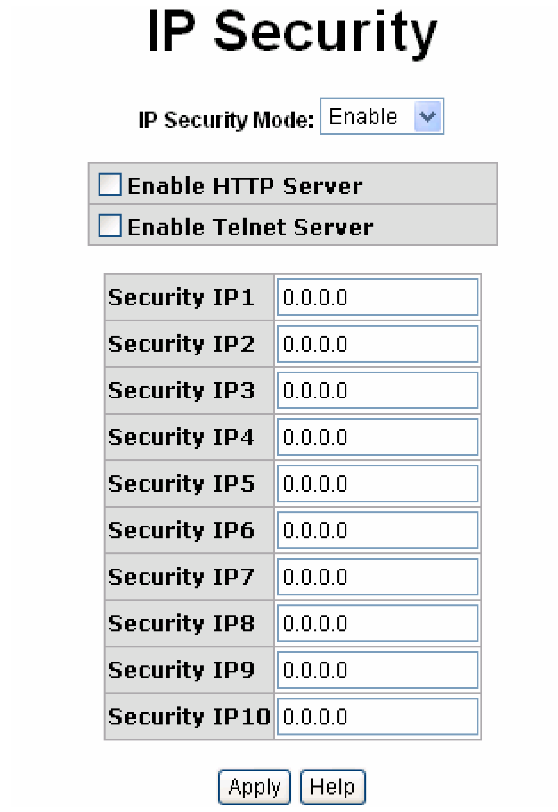
SNTP Configuration interface

IP Security

IP security function allows user to assign 10 specific IP addresses that have permission to access the switch through the web browser for the securing switch management.

- **Enable the IP Security:** Mark the check box to enable the IP security function
- **Security IP 1 ~ 10:** Assign up to 10 specific IP address. Only these 10 IP address can access and manage the switch through the Web browser
- And then, click Apply button to apply the configuration

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



IP Security

IP Security Mode: Enable

□ Enable HTTP Server

□ Enable Telnet Server

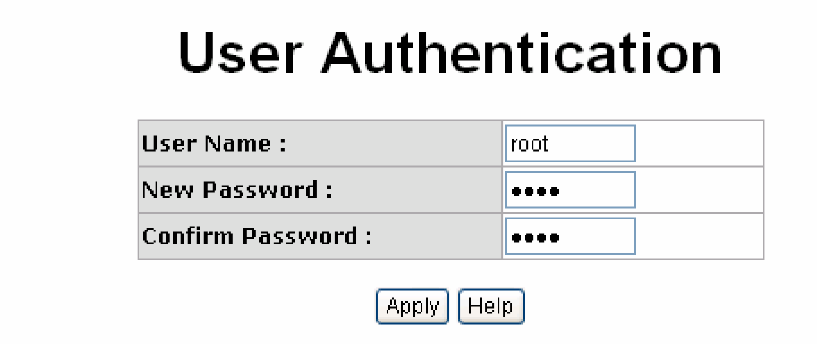
Security IP1	0.0.0.0
Security IP2	0.0.0.0
Security IP3	0.0.0.0
Security IP4	0.0.0.0
Security IP5	0.0.0.0
Security IP6	0.0.0.0
Security IP7	0.0.0.0
Security IP8	0.0.0.0
Security IP9	0.0.0.0
Security IP10	0.0.0.0

IP Security interface

User Authentication

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

1. **User name:** Key in the new user name(The default is "root")
2. **Password:** Key in the new password(The default is "root")
3. **Confirm password:** Re-type the new password
4. And then, click Apply



User Authentication

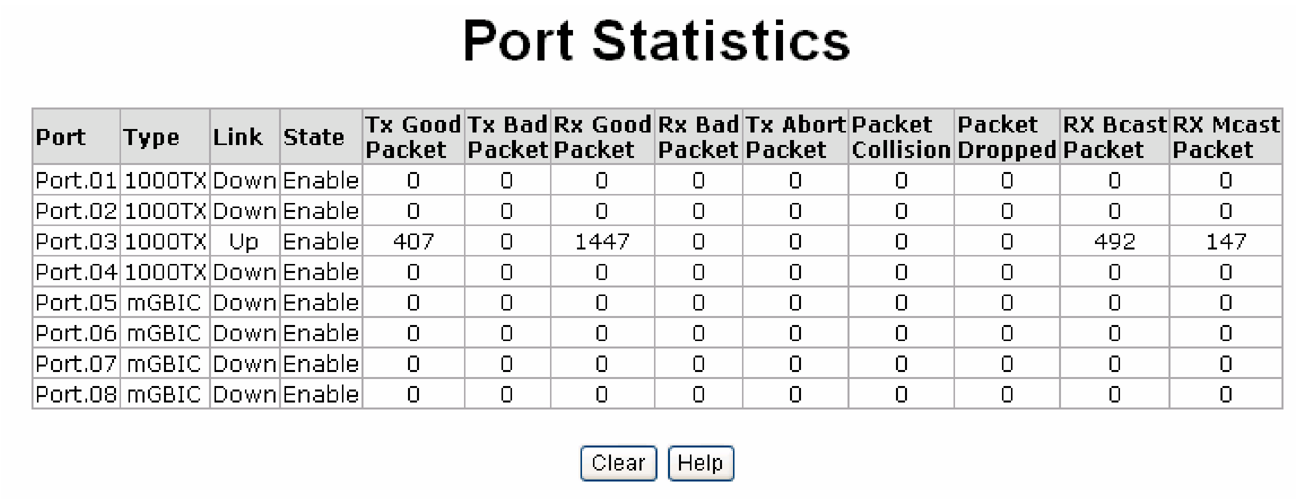
User Name :	root
New Password :	••••
Confirm Password :	••••

User Authentication interface

Port Statistics

The following information provides the current port statistic information

- Click Clear button to clean all counts



Port Statistics

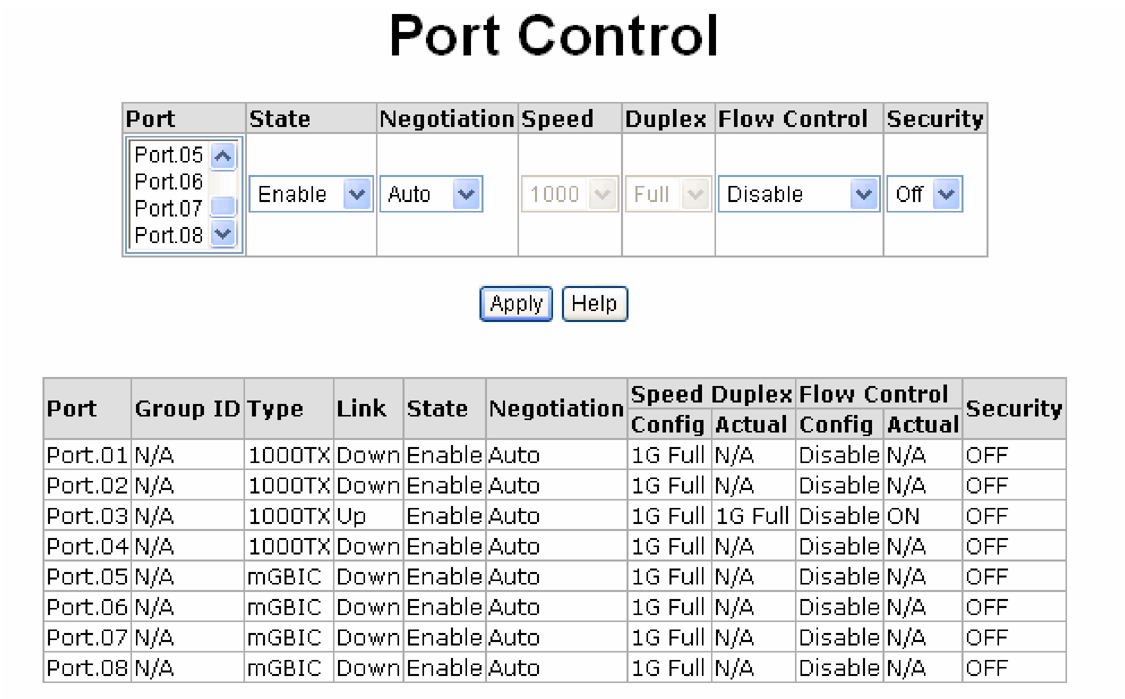
Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision	Packet Dropped	RX Bcast Packet	RX Mcast Packet
Port.01	1000TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.02	1000TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.03	1000TX	Up	Enable	407	0	1447	0	0	0	0	492	147
Port.04	1000TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.05	mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.06	mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.07	mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.08	mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0

Port Statistics interface

Port Control

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

1. **Port:** select the port that user wants to configure.
2. **State:** Current port status. The port can be set to disable or enable mode. If the port setting is disable then will not receive or transmit any packet.
3. **Negotiation:** set auto negotiation status of port.
4. **Speed:** set the port link speed.
5. **Duplex:** set full-duplex or half-duplex mode of the port.
6. **Flow Control:** set flow control function is **Symmetric** or **Asymmetric** in Full Duplex mode. The default value is **Disable**.
7. **Security:** When its state is “**On**”, means this port accepts only one MAC address.
8. Click Apply.



Port Control

Port	State	Negotiation	Speed	Duplex	Flow Control	Security
Port.05 Port.06 Port.07 Port.08	Enable	Auto	1000	Full	Disable	Off

Port	Group ID	Type	Link	State	Negotiation	Speed Duplex		Flow Control		Security
						Config	Actual	Config	Actual	
Port.01	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Disable	N/A	OFF
Port.02	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Disable	N/A	OFF
Port.03	N/A	1000TX	Up	Enable	Auto	1G Full	1G Full	Disable	ON	OFF
Port.04	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Disable	N/A	OFF
Port.05	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Disable	N/A	OFF
Port.06	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Disable	N/A	OFF
Port.07	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Disable	N/A	OFF
Port.08	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Disable	N/A	OFF

Port Control interface

Port Trunk

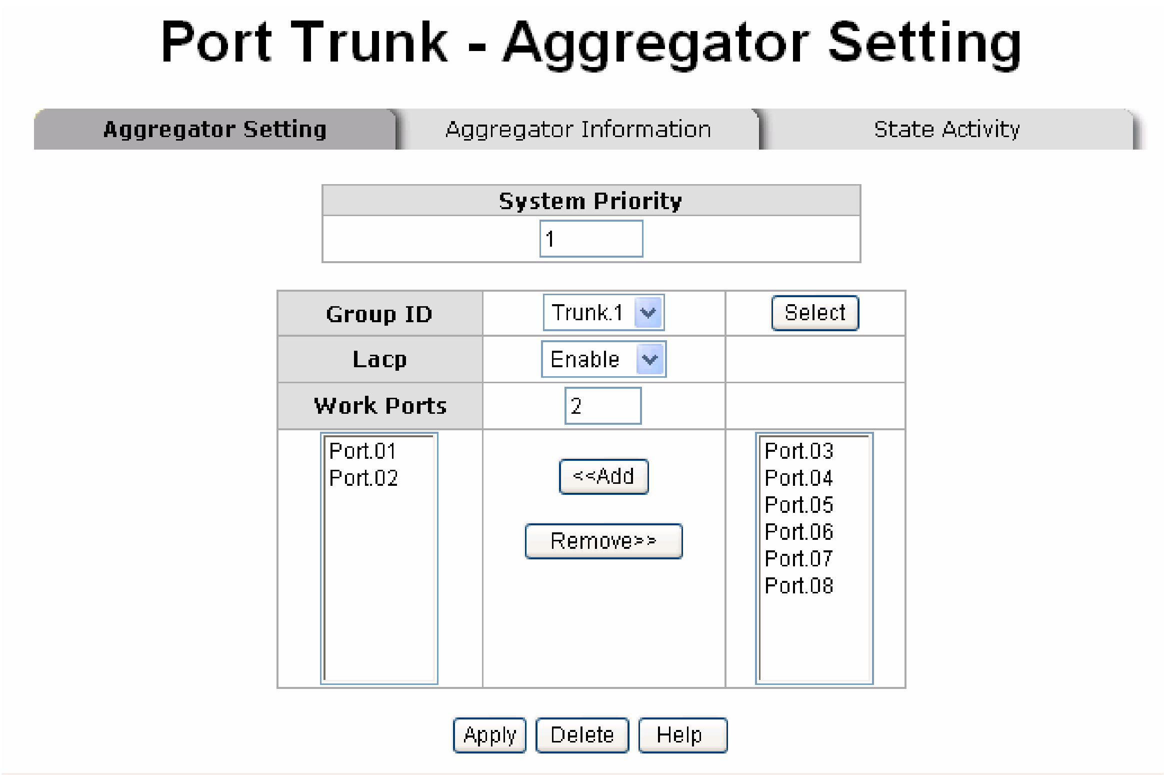
The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link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

Aggregator setting

1. **System Priority:** a value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
2. **Group ID:** There are three trunk groups to provide configure. Choose the "**Group ID**" and click Select .
3. **LACP:** If enable, the group is LACP static trunk group. If disable, the group is local static trunk group. All ports support LACP dynamic trunk group. If connecting to the device that also supports LACP, the LACP dynamic trunk group will be created automatically.
4. **Work ports:** allow max four ports can be aggregated at the same time. With LACP static trunk group, the exceed ports are standby and can be aggregated if work ports fail. If it is local static trunk group, the number of ports must be the same as the group member ports.
5. Select the ports to join the trunk group. Allow max four ports can be aggregated at the same time. Click Add button to add the port. To remove unwanted ports, select the port and click Remove button.
6. If LACP enable, user can configure LACP Active/Passive status in each ports on State Activity page.

7. Click Apply.

8. Use Delete button to delete Trunk Group. Select the Group ID and click Delete button.



Port Trunk - Aggregator Setting

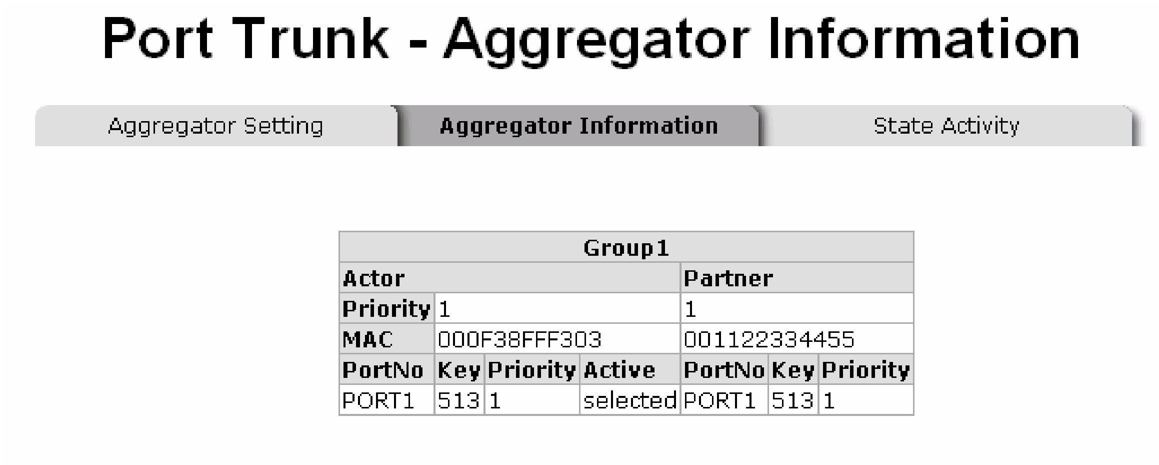
System Priority
1

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

Port Trunk—Aggregator Setting interface

Aggregator Information

When user has setup the LACP aggregator, user will see related information here.



Port Trunk - Aggregator Information

Group1						
Actor				Partner		
Priority	1			1		
MAC	000F38FFF303			001122334455		
PortNo	Key	Priority	Active	PortNo	Key	Priority
PORT1	513	1	selected	PORT1	513	1

Port Trunk – Aggregator Information interface

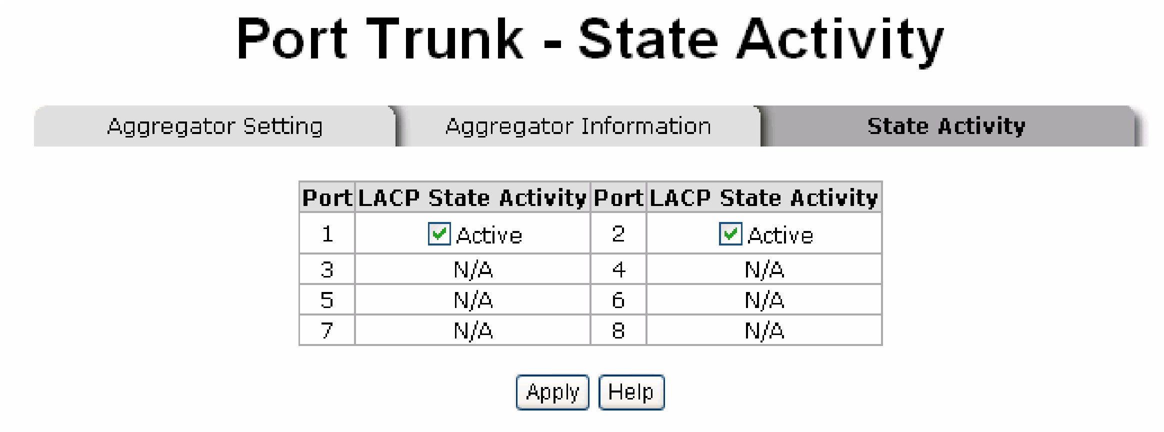
State Activity

When the LACP aggregator has been set up, user can configure port state activity. User can mark or un-mark the port. When user mark the port and click Apply button the port state activity will change to **Active**. Opposite is **Passive**.

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

[NOTE]

1. A link having either two active LACP ports or one active port can perform dynamic LACP trunk.
2. A link has two passive LACP ports will not perform dynamic LACP trunk because both ports are waiting for and LACP protocol packet from the opposite device.
3. If you are the actor of active LACP, after you have selected the trunk port, the active status will be created automatically.



Port Trunk - State Activity

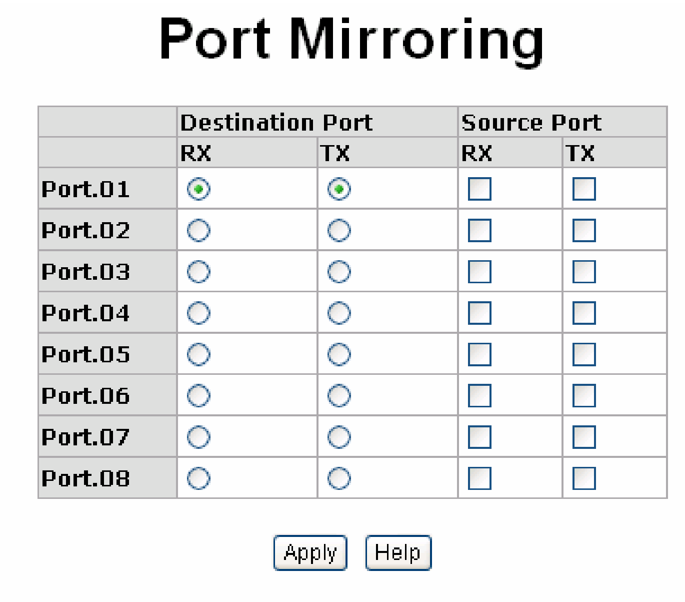
Port	LACP State Activity	Port	LACP State Activity
1	☑ Active	2	☑ Active
3	N/A	4	N/A
5	N/A	6	N/A
7	N/A	8	N/A

Port Trunk – State Activity interface

Port Mirroring

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

- **Port Mirroring Mode:** Set mirror mode -- Disable, TX, and Both. The default value is “Disable”
- **Analysis Port:** It means mirror port can be used to see all monitor port traffic. User can connect mirror port to LAN analyzer or Netxray
- **Monitor Port:** The ports user wants to monitor. All monitor port traffic will be copied to mirror port. User can select max 7 monitor ports in the switch. User can choose which port that wants to monitor in only one mirror mode. Mark the **State** check box to select the port
- And then, click Apply



Port Mirroring

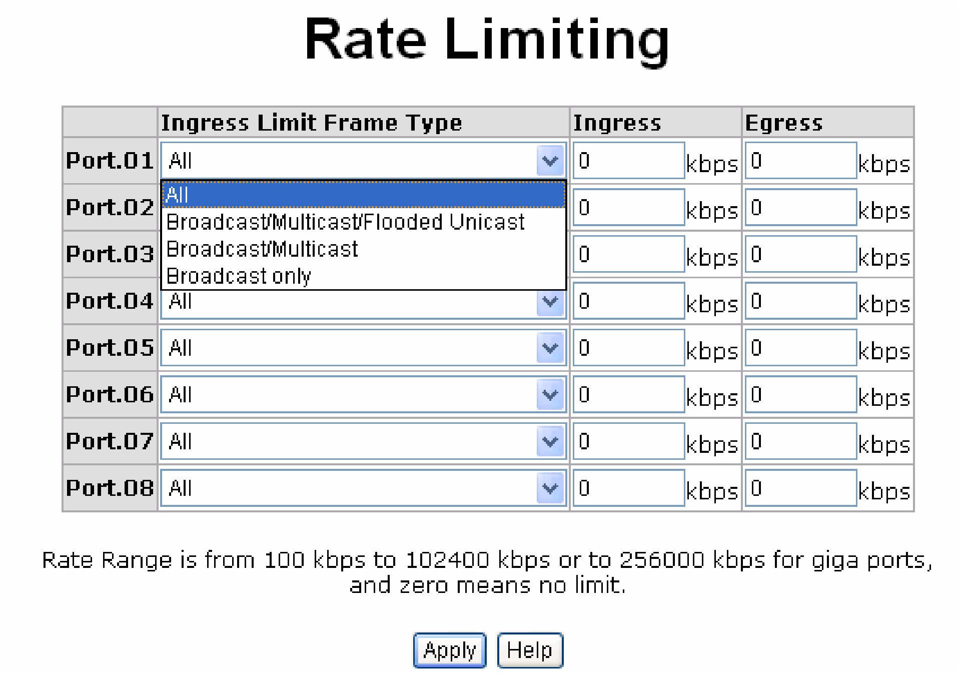
	Destination Port		Source Port	
	RX	TX	RX	TX
Port.01	●	●	□	□
Port.02	○	○	□	□
Port.03	○	○	□	□
Port.04	○	○	□	□
Port.05	○	○	□	□
Port.06	○	○	□	□
Port.07	○	○	□	□
Port.08	○	○	□	□

Port Trunk – Port Mirroring interface

Rate Limiting

User can set up every port's bandwidth rate and packet limitation type.

- **Ingress Limit Packet type:** select the packet type that wants to filter. The limit frame type selections have all type packet, broadcast/multicast/flooded unicast, broadcast/multicast, and broadcast only. The broadcast/multicast/flooded unicast packet, broadcast/multicast packet, and broadcast packet only are only for ingress packet. The egress rate supports all type packet.



Rate Limiting

	Ingress Limit Frame Type	Ingress	Egress
Port.01	All	0 kbps	0 kbps
Port.02		0 kbps	0 kbps
Port.03		0 kbps	0 kbps
Port.04	All	0 kbps	0 kbps
Port.05	All	0 kbps	0 kbps
Port.06	All	0 kbps	0 kbps
Port.07	All	0 kbps	0 kbps
Port.08	All	0 kbps	0 kbps

All
Broadcast/Multicast/Flooded Unicast
Broadcast/Multicast
Broadcast only

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

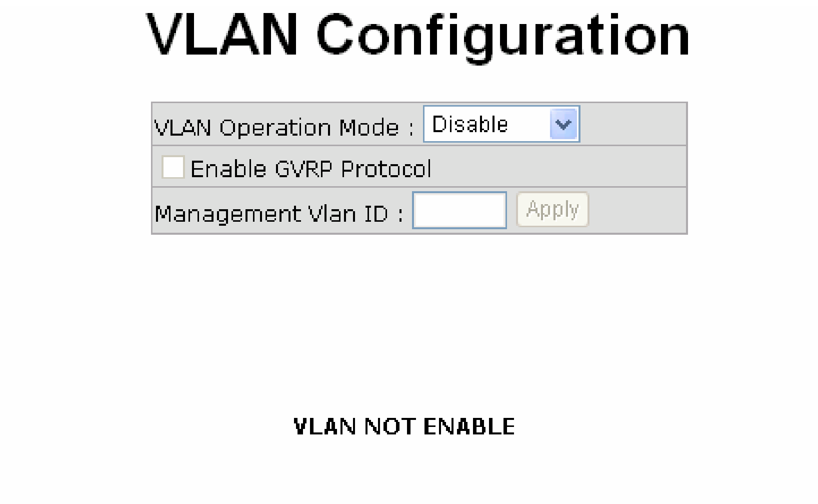
Rate Limiting interface

- 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 user to isolate network traffic so only the members of the VLAN will receive traffic from the same members of VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

The industrial switch supports port-based and 802.1Q (tagged-based) VLAN. In the default configuration, VLAN operation mode default is “**Disable**”.



VLAN Configuration

VLAN Operation Mode : Disable

□ Enable GVRP Protocol

Management Vlan ID :

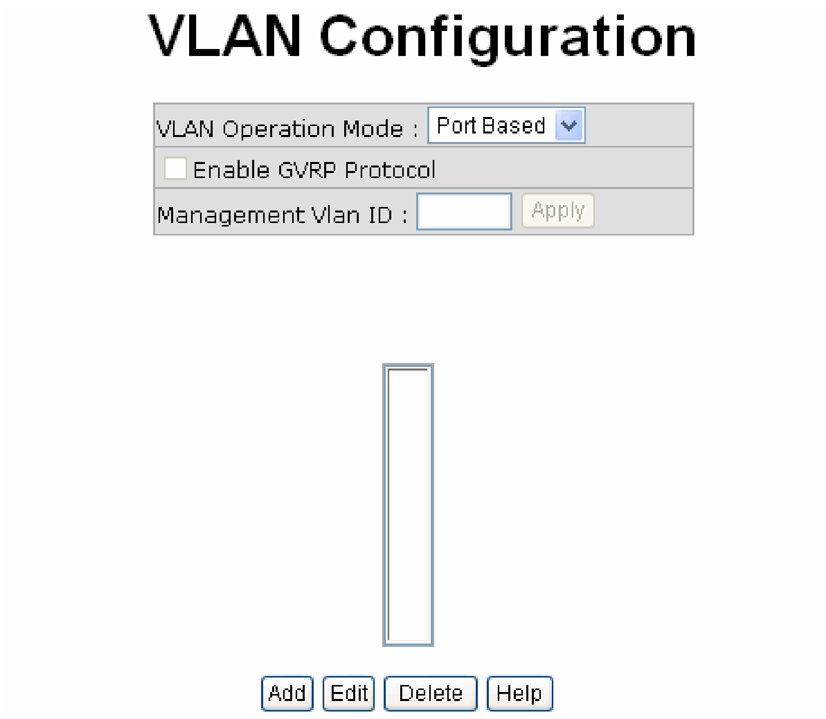
VLAN NOT ENABLE

VLAN Configuration interface

VLAN configuration - Port-based VLAN

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.

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



VLAN Configuration

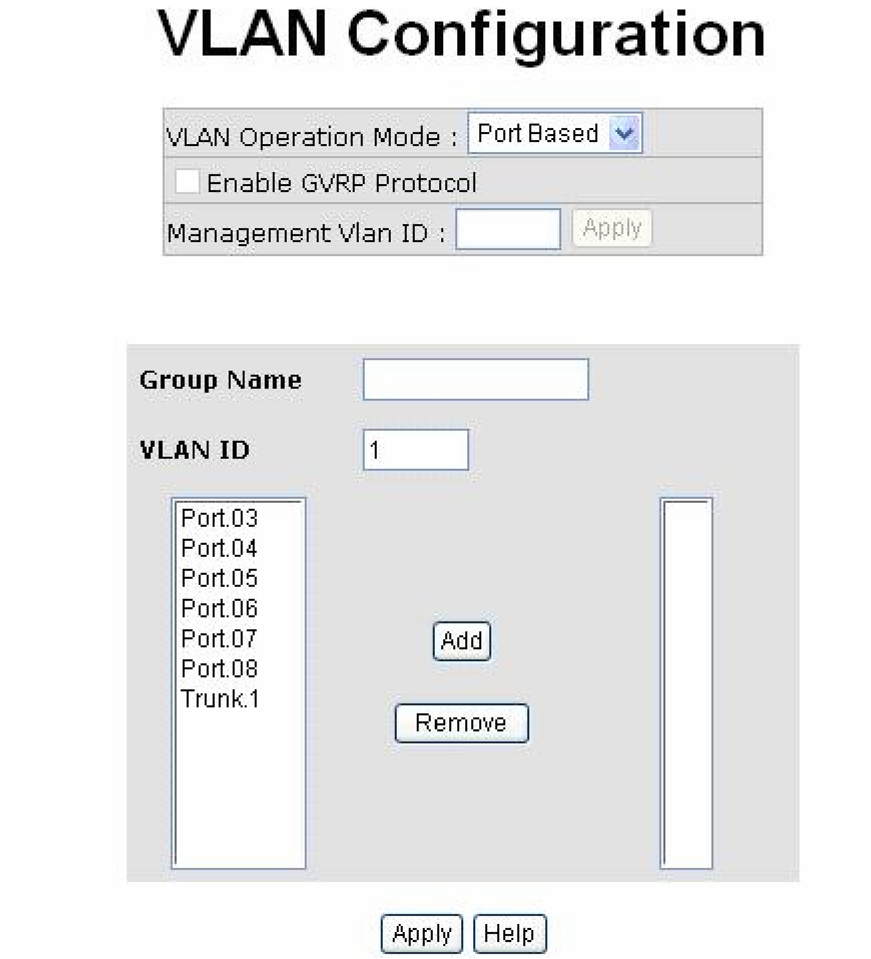
VLAN Operation Mode : Port Based

□ Enable GVRP Protocol

Management Vlan ID :

VLAN – Port Based interface

- Click Add to add a new VLAN group(The maximum VLAN group is up to 64 VLAN groups)
- Entering the VLAN name, group ID and grouping the members of VLAN group
- And then, click Apply



VLAN Configuration

VLAN Operation Mode : Port Based

□ Enable GVRP Protocol

Management Vlan ID :

Group Name

VLAN ID 1

Port.03
Port.04
Port.05
Port.06
Port.07
Port.08
Trunk.1

VLAN—Port Based Add interface

- User will see the VLAN displays.
- Use Delete button to delete unwanted VLAN.
- Use Edit button to modify existing VLAN group.

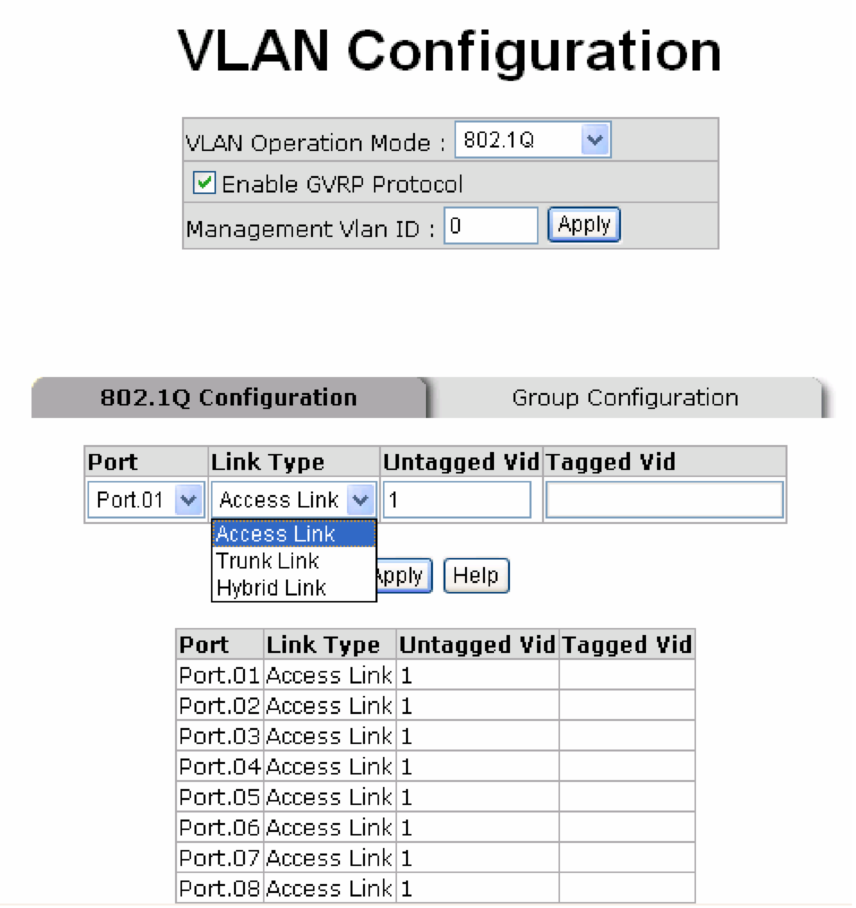
[NOTE] Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when switch power off.

802.1Q VLAN

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

User can create Tag-based VLAN, and enable or disable GVRP protocol. There are 256 VLAN groups to provide configure. Enable 802.1Q VLAN, the all ports on the switch belong to default VLAN, VID is 1. The default VLAN can’t be deleted.

GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, user can send a GVRP request using the VID of a VLAN defined on the switch; the switch will automatically add that device to the existing VLAN.



VLAN Configuration

VLAN Operation Mode : 802.1Q

☑ Enable GVRP Protocol

Management Vlan ID : 0

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

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	
Port.02	Access Link	1	
Port.03	Access Link	1	
Port.04	Access Link	1	
Port.05	Access Link	1	
Port.06	Access Link	1	
Port.07	Access Link	1	
Port.08	Access Link	1	

802.1q VLAN interface

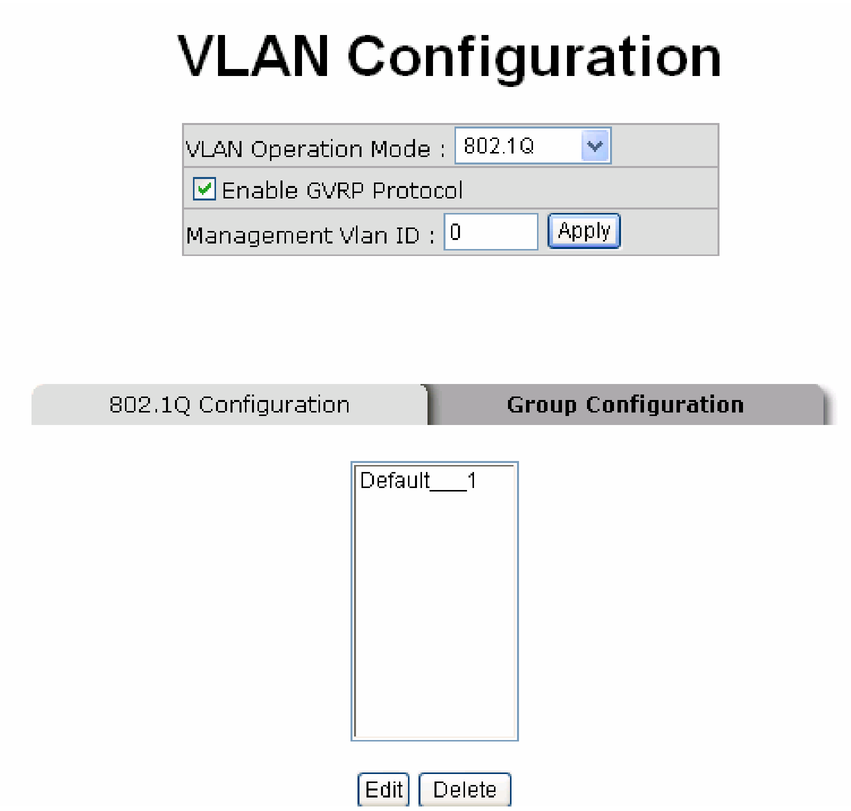
802.1Q Configuration

1. **Enable GVRP Protocol:** check the check box to enable GVRP protocol.
2. Select the port that wants to configure.
3. **Link Type**: there are 3 types of link type.
   - **Access Link:** single switch only, allow user to group ports by setting the same VID.
   - **Trunk Link:** extended application of **Access Link**, allow user to group ports by setting the same VID with 2 or more switch.
   - **Hybrid Link:** Both **Access Link** and **Trunk Link** are available.
4. **Untagged VID:** assign the untagged frame VID.
5. **Tagged VID:** assign the tagged frame VID.
6. Click Apply

Group Configuration

Edit the existing VLAN Group.

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



VLAN Configuration

VLAN Operation Mode : 802.1Q

☑ Enable GVRP Protocol

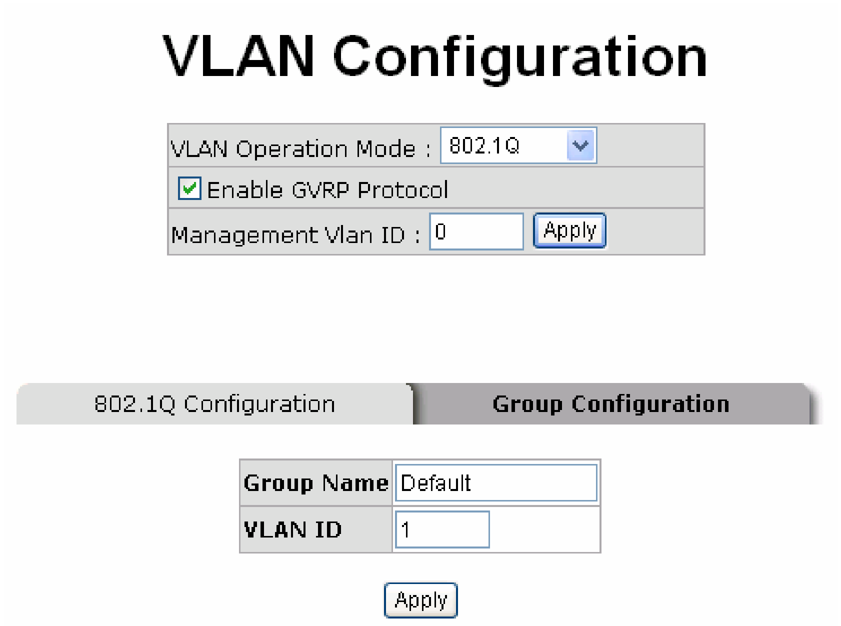
Management Vlan ID : 0

Default___1

Group Configuration interface

3. User can Change the VLAN group name and VLAN ID.

4. Click Apply.



VLAN Configuration

VLAN Operation Mode : 802.1Q

☑ Enable GVRP Protocol

Management Vlan ID : 0

Group Name	Default
VLAN ID	1

Group Configuration interface

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

1. User can view spanning tree information about the Root Bridge.

2. User can modify RSTP state. After modification, **save** the configuration.

1. **RSTP mode:** user must enable or disable RSTP function before configure the related parameters.

2. Priority (0-61440): a value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If user changes the value, user must reboot the switch assigned path priority number. The value must be a multiple of 4096 according to the protocol standard rule.

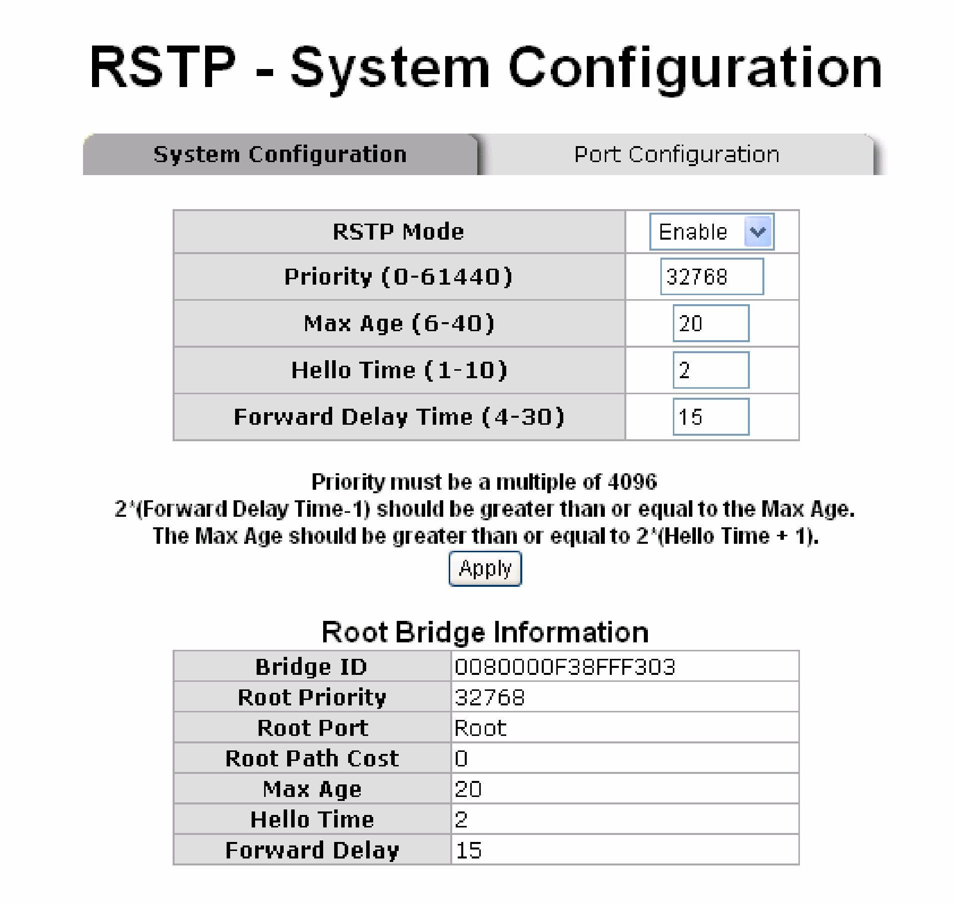
3. **Max Age (6-40):** the number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.

4. Hello Time (1-10): the time that controls switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.

5. Forward Delay Time (4-30): the number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.

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

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



RSTP - System Configuration

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

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

Root Bridge Information

Bridge ID	0080000F38FFF303
Root Priority	32768
Root Port	Root
Root Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15

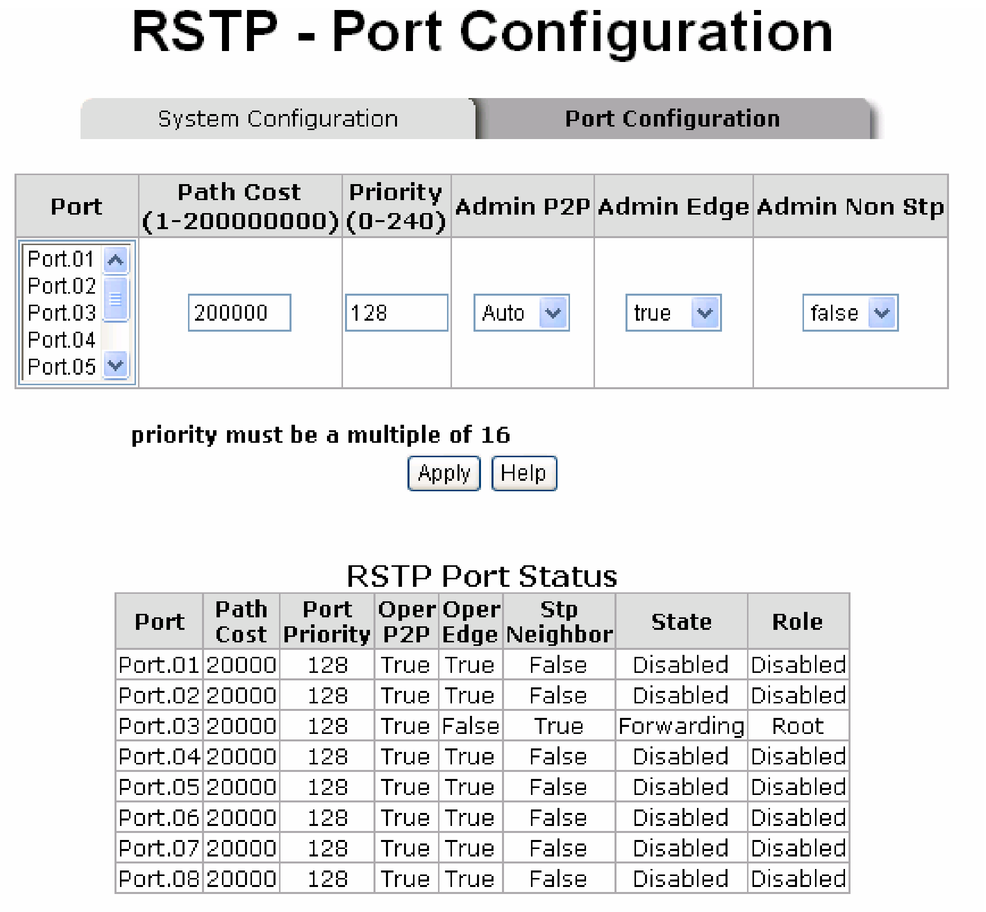
RSTP System Configuration interface

RSTP Per Port Configuration

User can configure path cost and priority of every port.

1. **Port:** Select the port in Port column.
2. **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000
3. **Priority:** Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16.
4. **Admin P2P:** Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True is P2P enabling. False is P2P disabling.

5. **Admin Edge:** The port directly connected to end stations cannot create a bridging loop in the network. To configure the port as an edge port, set the port to “**True**” status.
6. **Admin Non Stp:** The port includes the STP mathematic calculation. **True** is not including STP mathematic calculation. **False** is including the STP mathematic calculation.
7. Click Apply.



RSTP - Port Configuration

Port	Path Cost (1-200000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non Stp
Port.01 Port.02 Port.03 Port.04 Port.05	200000	128	Auto	true	false

priority must be a multiple of 16

RSTP Port Status

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

RSTP Per 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

■ System Option

Enter the system name, contact, and location information.

1. **Name:** assign a name for the switch.
2. **Contact:** Type the name of contact person or organization.
3. **Location:** Type the location of the switch.
4. Click Apply .

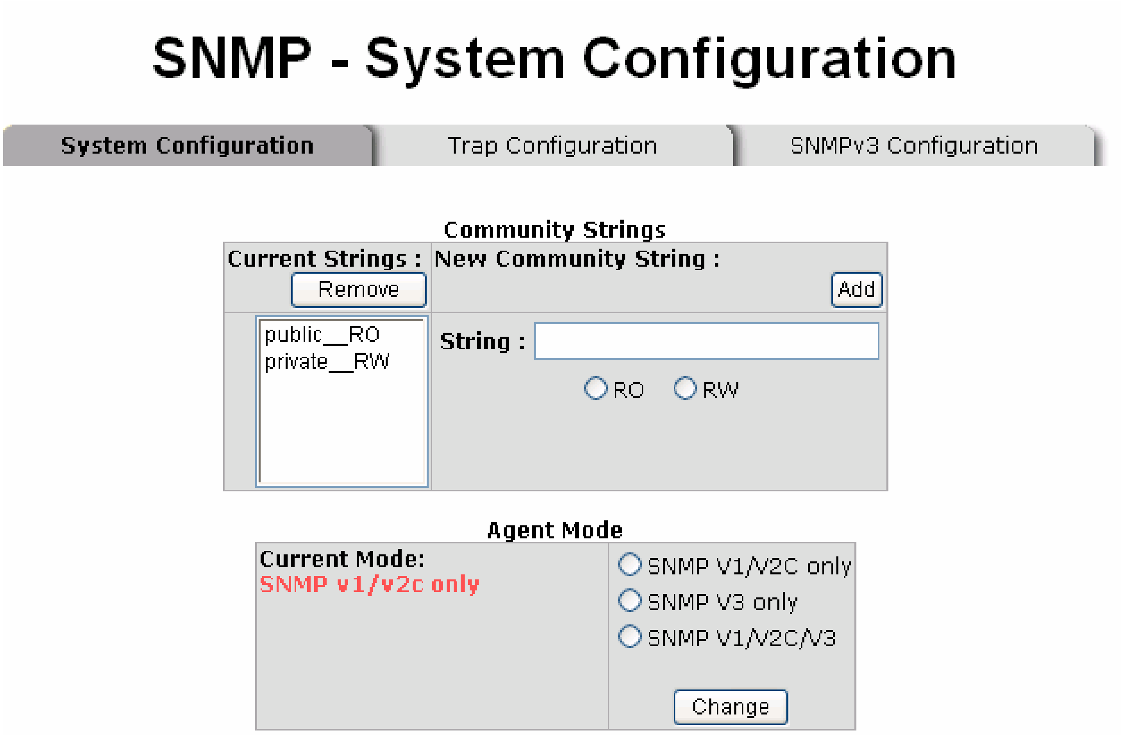
■ Community Strings

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

1. **String:** fill the name of string.
2. **RO:** Read only. Enables requests accompanied by this string to display MIB-object information.
3. **RW:** Read write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.

1. Click Add .
2. To remove the community string, select the community string that user has defined and click Remove . User cannot remove the default community string set.

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



SNMP - System Configuration

Community Strings

Current Strings :

public__RO
private__RW

New Community String :

String :

○ RO ○ RW

Agent Mode

Current Mode:
SNMP v1/v2c only

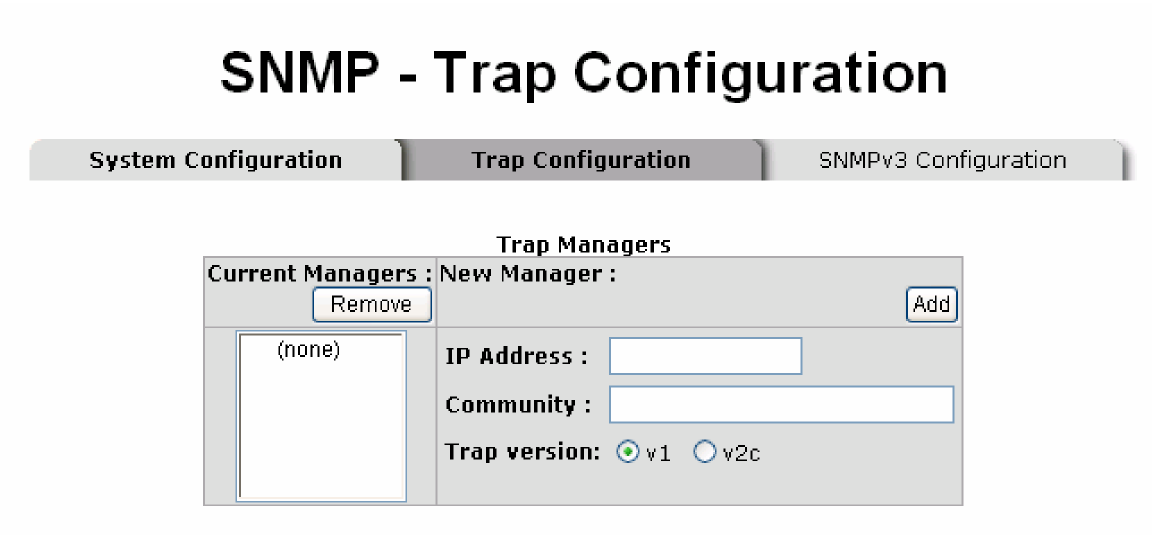
○ SNMP V1/V2C only
○ SNMP V3 only
○ SNMP V1/V2C/V3

SNMP System Configuration interface

Trap Configuration

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

1. **IP Address:** enter the IP address of trap manager.
2. **Community:** enter the community string.
3. **Trap Version:** select the SNMP trap version type – v1 or v2c.
4. Click Add.
5. To remove the community string, select the community string that user has defined and click Remove. User cannot remove the default community string set.



SNMP - Trap Configuration

Trap Managers

Current Managers : (none)

New Manager :

IP Address :

Community :

Trap version: ● v1 ○ v2c

Trap Managers interface

SNMPV3 Configuration

Configure the SNMP V3 function.

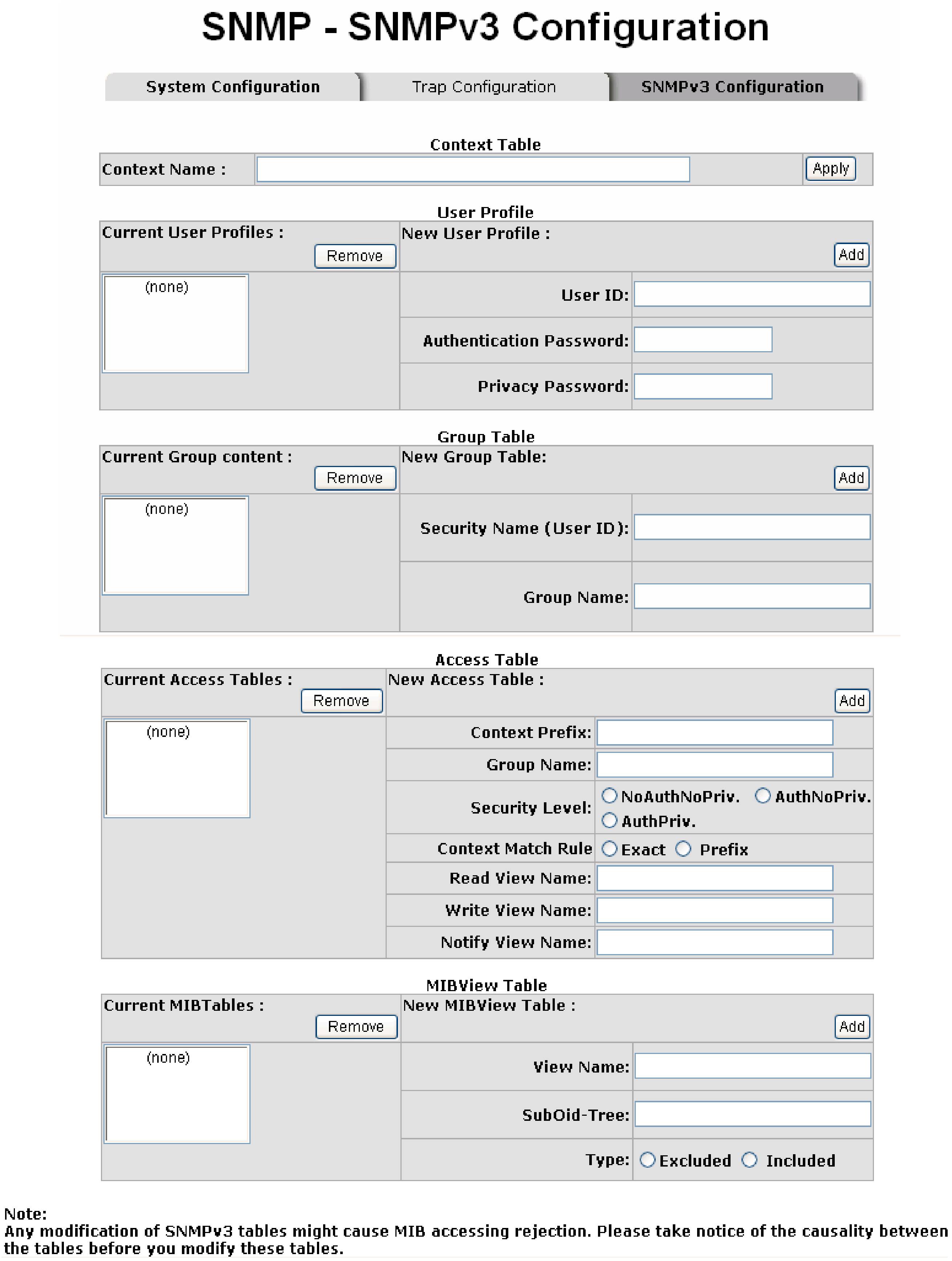
Context Table

Configure SNMP v3 context table. Assign the context name of context table. Click Add to add context name. Click Remove to remove unwanted 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.



SNMP - SNMPv3 Configuration

System Configuration | Trap Configuration | SNMPv3 Configuration

Context Table

Context Name :		Apply

User Profile

Current User Profiles : Remove	New User Profile : Add	
(none)	User ID:	
	Authentication Password:	
	Privacy Password:	

Group Table

Current Group content : Remove	New Group Table: Add	
(none)	Security Name (User ID):	
	Group Name:	

Access Table

Current Access Tables : Remove	New Access Table : Add	
(none)	Context Prefix:	
	Group Name:	
	Security Level:	○ NoAuthNoPriv. ○ AuthNoPriv. ○ AuthPriv.
	Context Match Rule	○ Exact ○ Prefix
	Read View Name:	
	Write View Name:	
	Notify View Name:	

MIBView Table

Current MIBTables : Remove	New MIBView Table : Add	
(none)	View Name:	
	SubOid-Tree:	
	Type:	○ Excluded ○ Included

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

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.

Access Table

Configure SNMP v3 access table.

- **Context Prefix:** set up the context name.
- **Group Name:** set up the group.
- **Security Level:** select the access level.
- **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.

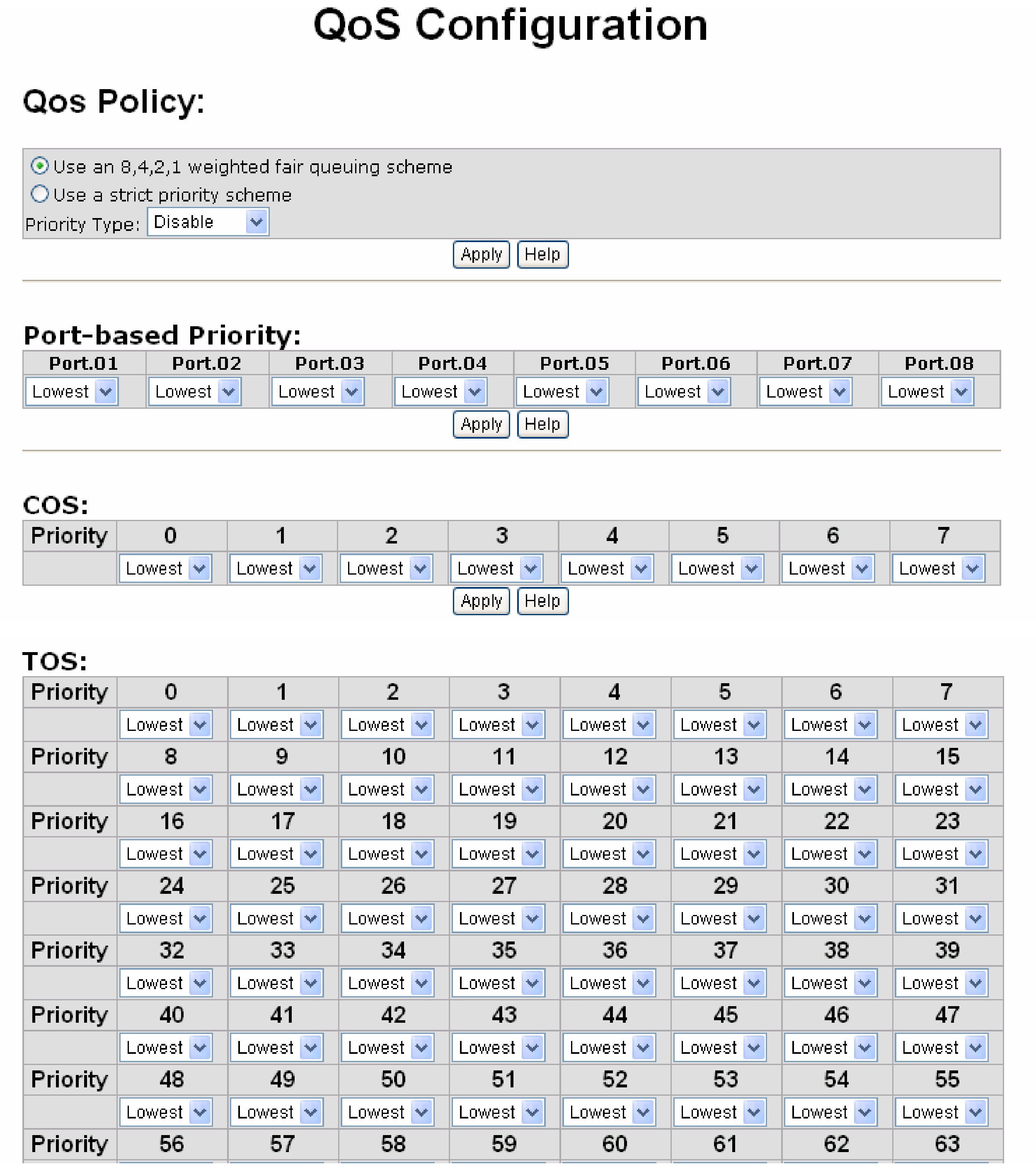
- **View Name:** set up the name.
- **Sub-Oid Tree:** fill the Sub OID.
- **Type:** select the type – exclude or included.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

QoS Configuration

User can configure Qos policy and priority setting, per port priority setting, COS and TOS setting.

QoS Policy and Priority Type

- **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 Hi to lowest queue. For example: the system will process 80 % high queue traffic, 40 % middle queue traffic, 20 % low queue traffic, and 10 % lowest queue traffic at the same time. And the traffic in the Low Priority queue are not transmitted until all High, Medium, and Normal traffic are serviced.
    - **Use the strict priority scheme:** Always higher queue will be process first, except higher queue is empty.
- **Priority Type:** every port has 5 priority type selections. Disable means no priority type is selected.
    - **Port-base:** the port priority will follow the **default port priority** that you have assigned – High, middle, low, or lowest.
    - **COS only:** the port priority will only follow the **COS priority** that you have assigned.
    - **TOS only:** the port priority will only follow the **TOS priority** that you have assigned.
    - **COS first:** the port priority will follow the COS priority first, and then other priority rule.
    - **TOS first:** the port priority will follow the TOS priority first, and the other priority rule.
- Click Apply.



QoS Configuration

Qos Policy:

● Use an 8,4,2,1 weighted fair queuing scheme

○ Use a strict priority scheme

Priority Type: Disable

Port-based Priority:

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

COS:

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

TOS:

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

QoS Configuration interface

Port Base Priority

Configure per port priority level.

- **Port 1 ~ Port 8:** 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 is high. The port 1 is following the TOS priority policy only. When the port 1 packet received, 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

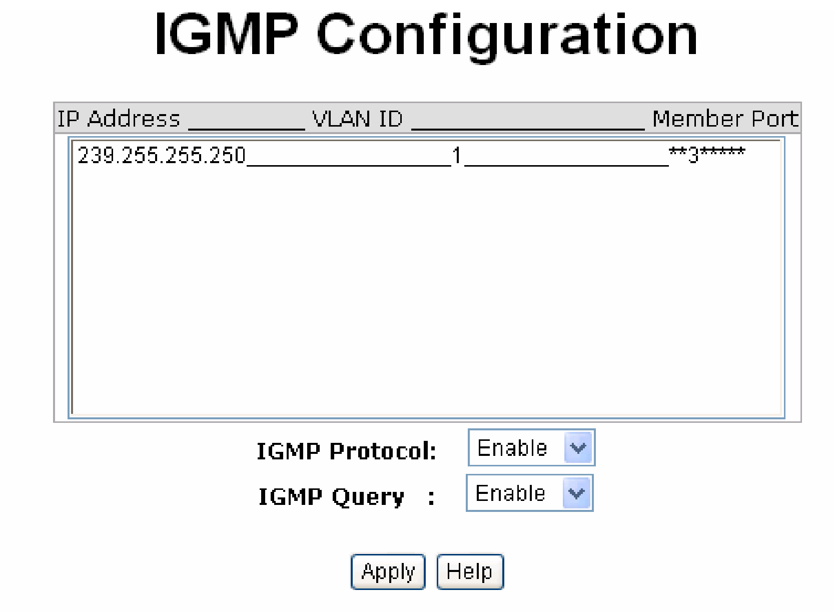
The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through 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 support IP multicast, user can enable IGMP protocol on web management's switch setting advanced page, the IGMP snooping information then is displayed. IP multicast addresses range from 224.0.0.0 through 239.255.255.255.

- **IGMP Protocol:** enable or disable the IGMP protocol.
- **IGMP Query:** enable or disable the IGMP query function. The IGMP query information will be display in IGMP status section.
- Click Apply.


IGMP Configuration

```
IP Address ________ VLAN ID ______________ Member Port
239.255.255.250______________1______________**3*****
```

IGMP Protocol: Enable

IGMP Query : Enable

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.

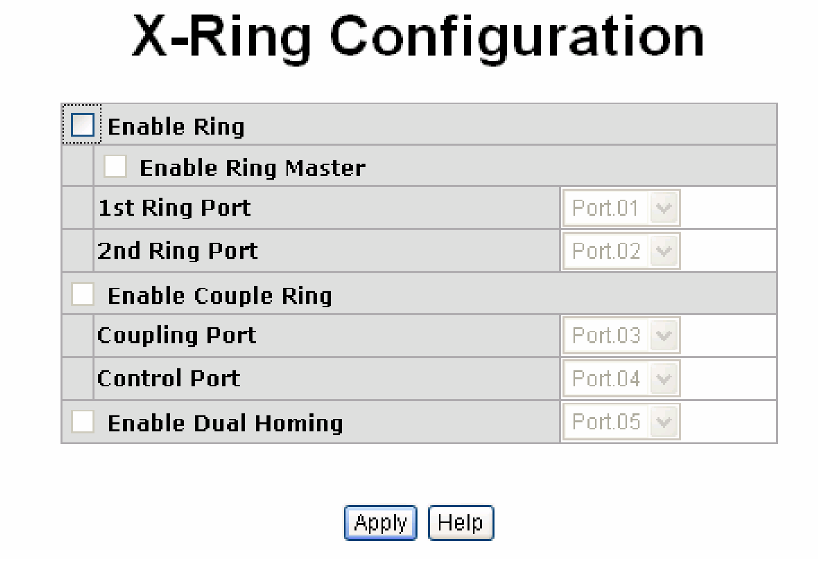
In the X-Ring topology, every switch should enable X-Ring function and assign two member ports in the ring. Only one switch in the X-Ring group would be set as a backup switch that would be blocked, called backup port, and another port is called working port. Other switches are called working switches 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 one Dipswitch 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 DIP Switch. When the switch is set to the master ring mode, the X-Ring configuration interface will display the switch as the master ring message. Also, user can identify the switch as the ring master from the R.M. LED panel of the LED panel on the switch.

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:** To enable the X-Ring function. Marking the check box to enable the X-Ring function.
- **1st & 2nd Ring Ports:** Assign two ports as the member ports. One port will be working port and the other one will be the backup port. The system will automatically decide which port is working port and which port is backup port.
- **Enable Coupling Ring:** To enable the coupling ring function. Marking the check box to enable the coupling ring function.
- **Coupling port:** Assign the member port.

- **Control port:** Set the switch as the master switch in the coupling ring.
- **Enable Dual Homing:** Set up one of port on the switch to be the Dual Homing port. In an X-Ring group, maximum Dual Homing port is one. Dual Homing only work when the X-Ring function enable.
- And then, click Apply to apply the configuration.



X-Ring Configuration

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

X ring Interface

[NOTE]

1. When the X-Ring function is enabled, user must disable the RSTP. The X-Ring function and RSTP function cannot exist at the same time.
2. Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when switch power off.

Security

In this section, user can configure 802.1x and MAC address table.

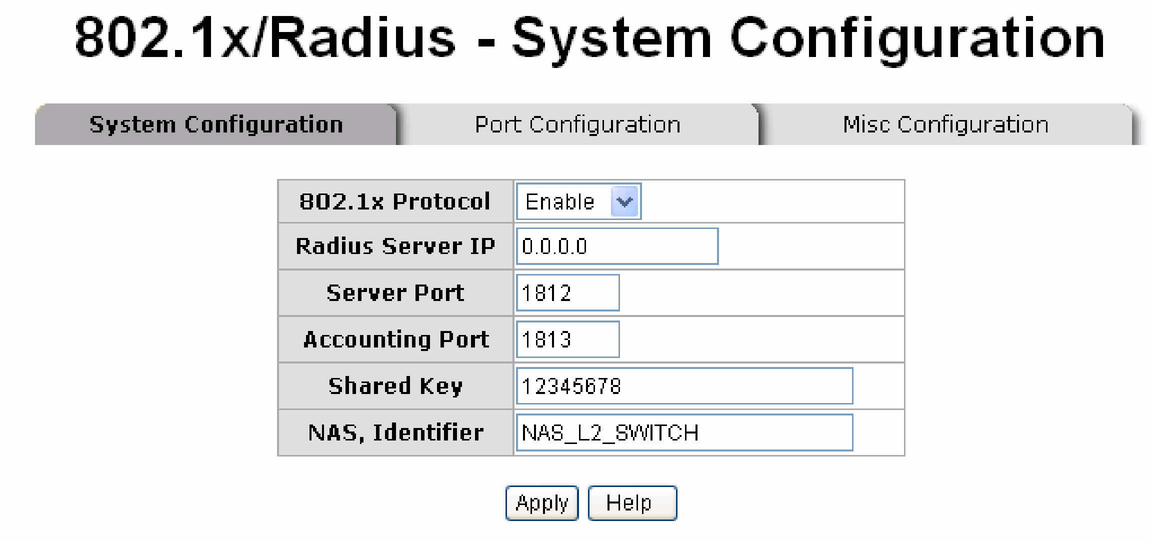
802.1X/Radius Configuration

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

System Configuration

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

1. **IEEE 802.1x Protocol:** .enable or disable 802.1x protocol.
2. **Radius Server IP:** set the Radius Server IP address.
3. **Server Port:** set the UDP destination port for authentication requests to the specified Radius Server.
4. **Accounting Port:** set the UDP destination port for accounting requests to the specified Radius Server.
5. **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.
6. **NAS, Identifier:** set the identifier for the radius client.
7. Click Apply .



802.1x/Radius - System Configuration

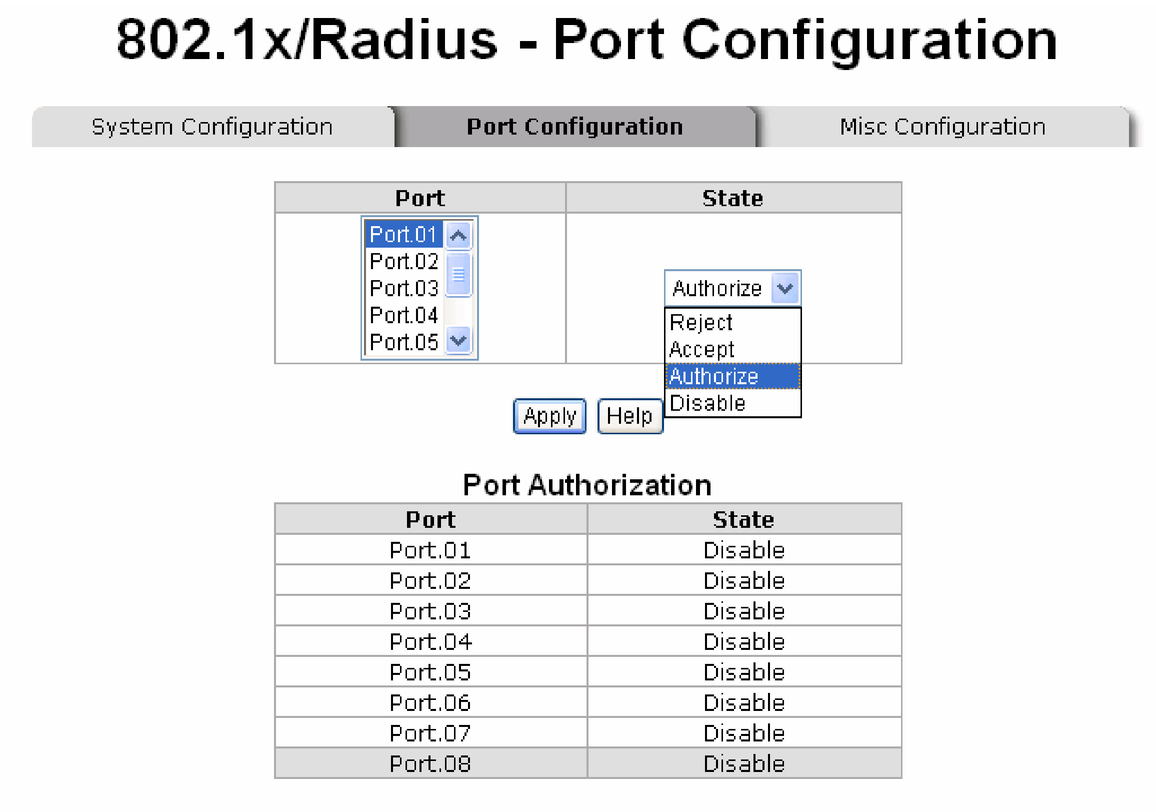
802.1x Protocol	Enable
Radius Server IP	0.0.0.0
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

802.1x System Configuration interface

802.1x Per Port Configuration

User can configure 802.1x authentication state for each port. The State provides Disable, Accept, Reject and Authorize. Use “**Space**” key change the state value.

- **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:** The specified port is required to be held in the Authorized state
- Click Apply.



802.1x/Radius - Port Configuration

Port	State
Port.01 Port.02 Port.03 Port.04 Port.05	Authorize

Port Authorization

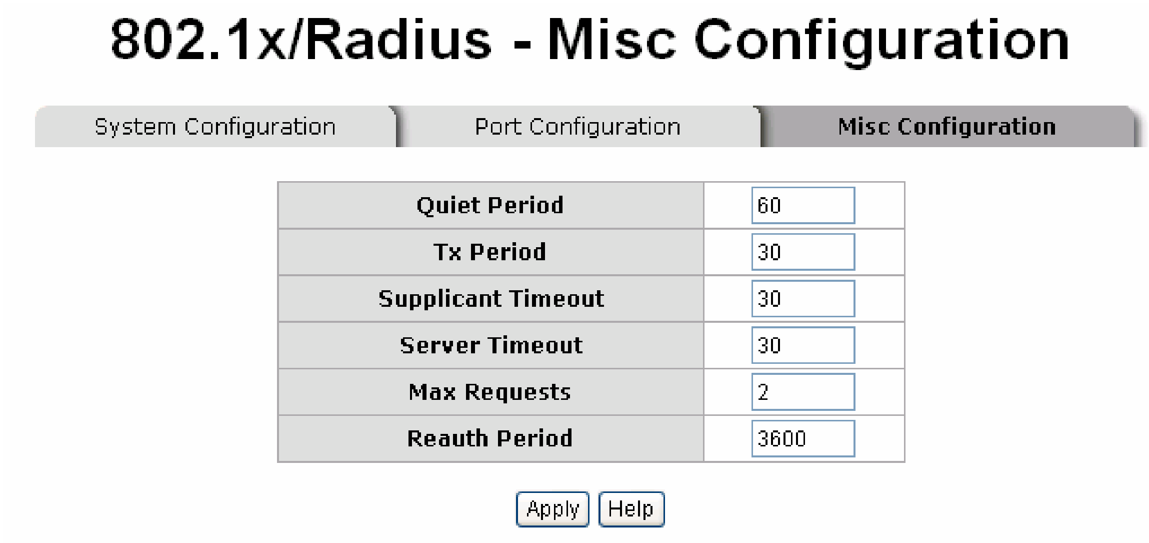
Port	State
Port.01	Disable
Port.02	Disable
Port.03	Disable
Port.04	Disable
Port.05	Disable
Port.06	Disable
Port.07	Disable
Port.08	Disable

802.1x Per Port Setting interface

Misc Configuration

1. **Quiet Period:** set the period during which the port doesn’t try to acquire a supplicant.

2. **TX Period:** set the period the port wait for retransmit next EAPOL PDU during an authentication session.
3. **Supplicant Timeout:** set the period of time the switch waits for a supplicant response to an EAP request.
4. **Server Timeout:** set the period of time the switch waits for a server response to an authentication request.
5. **Max Requests:** set the number of authentication that must time-out before authentication fails and the authentication session ends.
6. **Reauth period:** set the period of time after which clients connected must be re-authenticated.
7. Click Apply .



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

802.1x Misc Configuration interface

MAC Address Table

Use the MAC address table to ensure the port security.

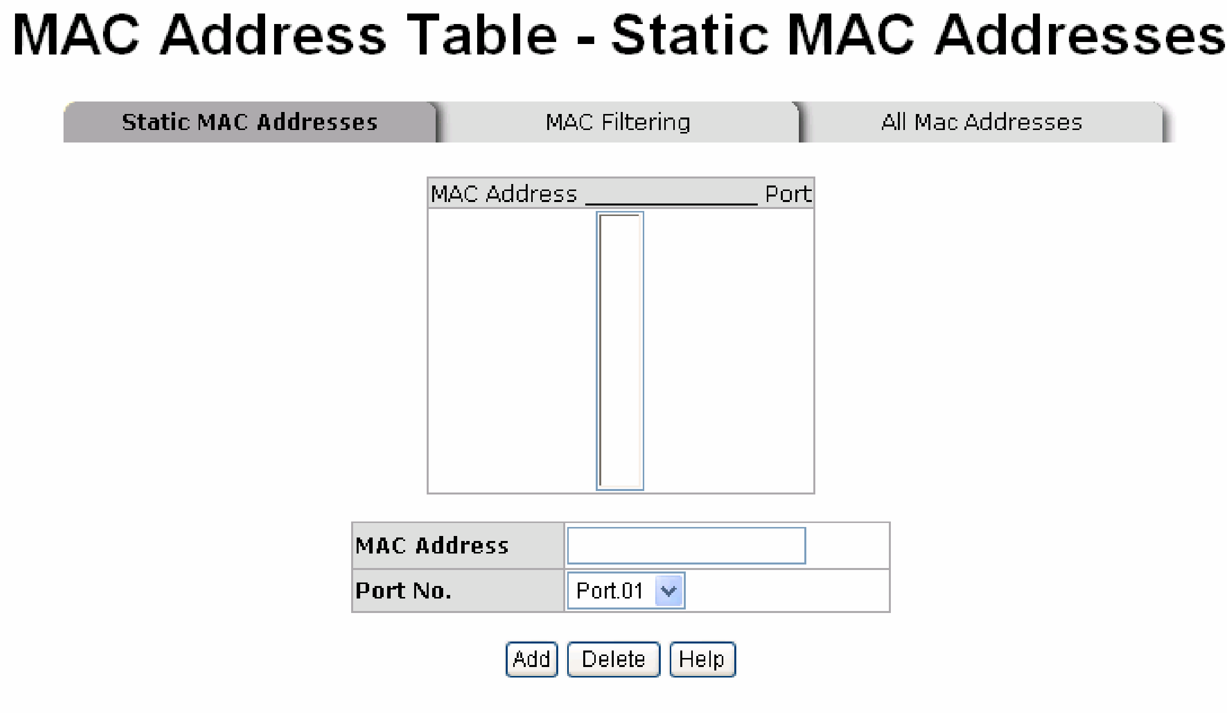
Static MAC Address

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

- **Add the Static MAC Address**

User can add static MAC address in 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. **VLAN ID:** enter the Mac address's VLAD ID, if the Mac address belongs to any VLAN group.
4. Click Add .
5. For deleting the MAC address from filtering table, select the MAC address and click Delete .

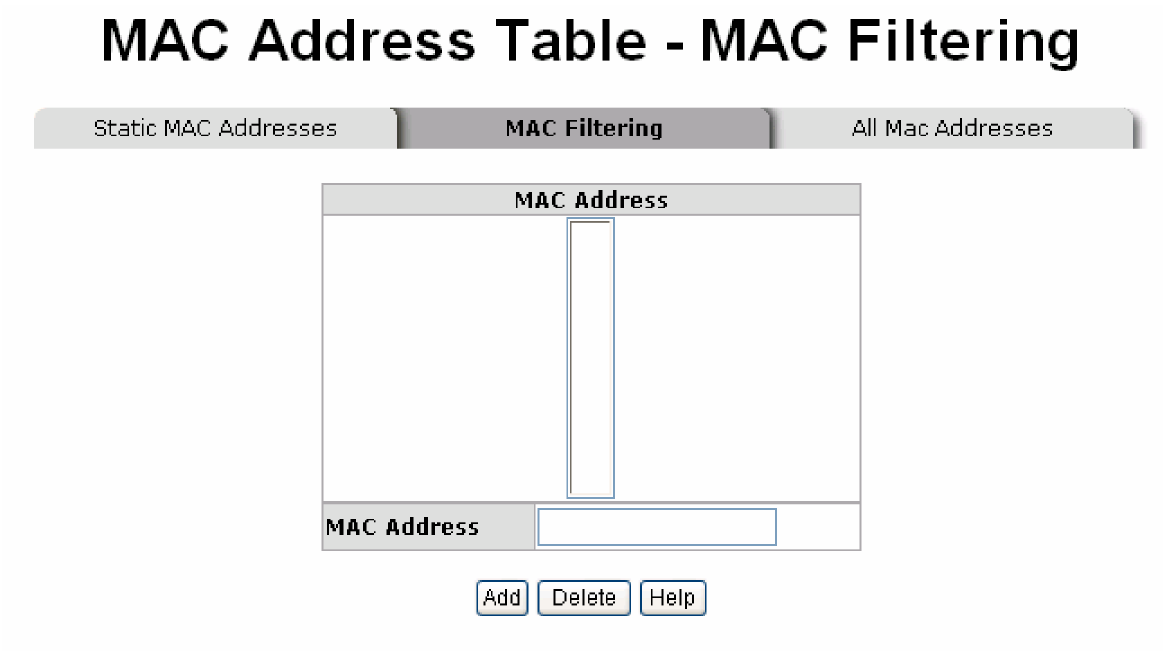

MAC Address Table - Static MAC Addresses

MAC Address	
Port No.	Port.01

Static MAC Addresses interface

MAC Filtering

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



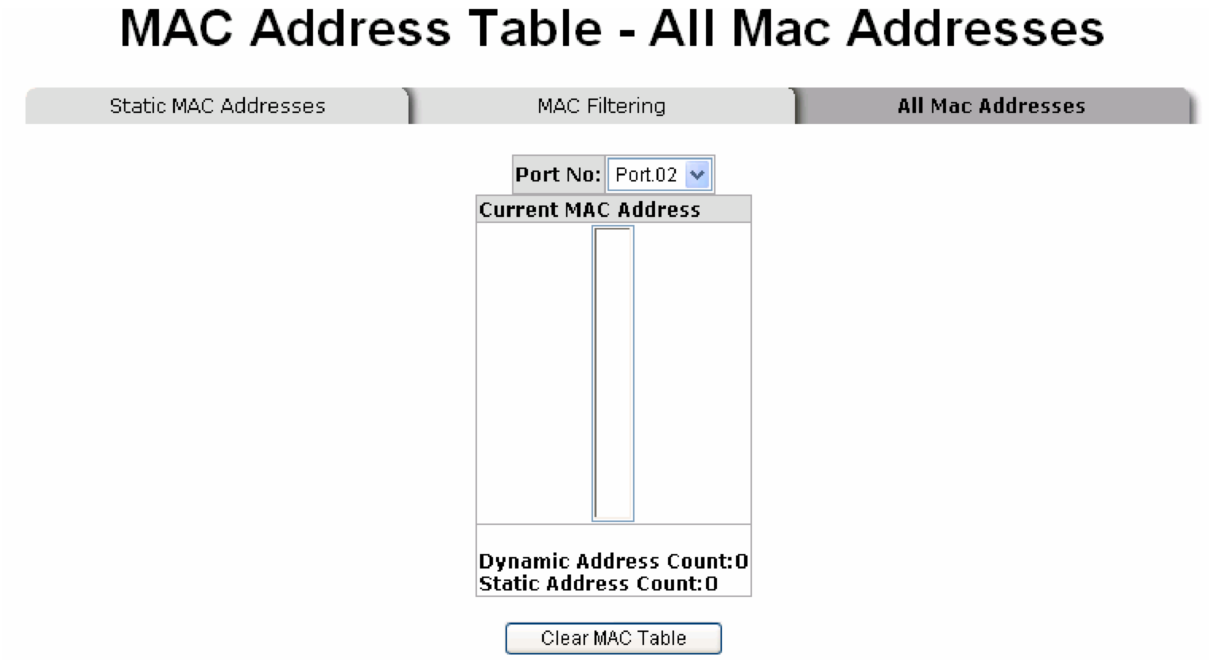
MAC Filtering interface

1. **MAC Address:** Enter the MAC address that user wants to filter.
2. **VLAN ID:** enter the Mac address's VLAD ID, if the Mac address belongs to any VLAN group.
3. Click Add.
4. For deleting the MAC address from filtering table, select the MAC address and click Delete.

All MAC Addresses

User can view the port that connected device's MAC address and related devices' MAC address.

1. Select the port.
2. The selected port of static MAC address information will display.
3. Click Clear MAC Table to clear the current port static MAC address information on screen.



MAC Address Table - All Mac Addresses

Static MAC Addresses | MAC Filtering | All Mac Addresses

Port No: Port.02

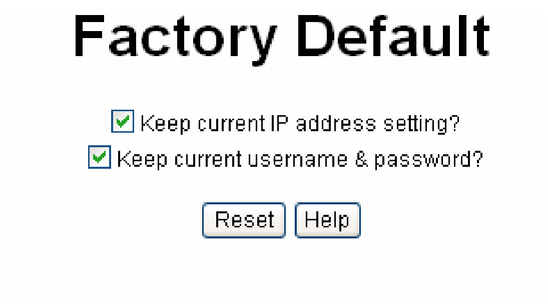
Current MAC Address

Dynamic Address Count:0
Static Address Count:0

All MAC Address interface

Factory Default

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



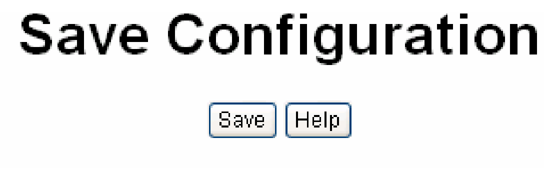
Factory Default

☑ Keep current IP address setting?
☑ Keep current username & password?

Factory Default interface

Save Configuration

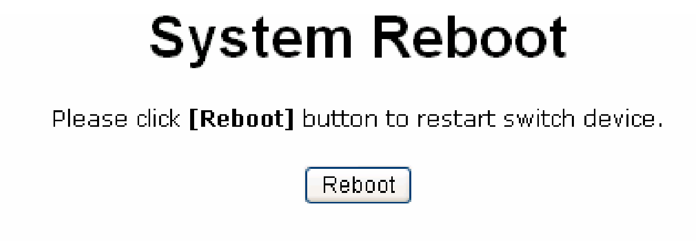
Save all configurations that user has made in the system. To ensure the all configuration will be saved. Click Save Flash to save the all configuration to the flash memory.



Save Configuration interface

System Reboot

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



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

System Reboot interface

Troubleshooting

This section is intended to help user solve the most common problems on the 4 10/100/1000TX plus 4 MINI GBIC Managed Switch.

Incorrect connections

The switch port can auto detect straight or crossover cable when user link switch with other Ethernet device. For the RJ-45 connector should use correct UTP or STP cable, 10/100/1000Mbps 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 matched.

■ Faulty or loose cables

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

■ Non-standard cables

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

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

■ Improper Network Topologies

It is important to make sure that user has a valid network topology. Common topology faults include excessive cable length and too many repeaters (hubs) between end nodes. In addition, user should make sure that the network topology contains no data path loops. Between any two ends nodes, there should be only one active cabling path at any time. Data path loops will cause broadcast storms that will severely impact the network performance.

Diagnosing LED Indicators

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

IF the power indicator does not light on when the power cord is plugged in, user 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.

Technical Specifications

This section provides the specifications of 4 10/100/1000TX plus 4 Mini GBIC Managed Switch and the following table lists these specifications.

Standards	IEEE802.3 10BASE-T IEEE802.3u 100BASE-TX IEEE802.3z Gigabit fiber IEEE802.3ab 1000Base-T IEEE802.3x Flow control and Back pressure IEEE802.3ad Port trunk with LACP IEEE802.1d Spanning tree protocol IEEE802.1w Rapid spanning tree IEEE802.1p Class of service IEEE802.1Q VLAN Tagging IEEE 802.1x user authentication
Protocol	CSMA/CD
LED Indicators	System Power (Green) 1000Base-T Port: Speed (1000Mbps Green), Link/Activity (Green), Mini GBIC: Link/Activity (Green)
Connector	1000Base-T: 4 x RJ-45 Gigabit fiber: 4 x MINI GBIC socket.
Switch architecture	Store and forward switch architecture. 16Gbps system backplane. System throughput up to 23.8Mpps.
Packet buffer	1Mbits for packet buffer
RS-232 connector	One RS-232 DB-9 Female connector for switch management

Dimensions	217mm(W) x 140mm(D) x 43mm(H)
MAC Address	8K MAC address table with Auto learning function
Storage Temp.	-40℃~70℃, 95% RH
Operational Temp.	0℃~45℃, 5%~95%RH
Operational Humidity	10% to 90% (Non-condensing)
Power Supply	AC 100~240V, 50/60Hz
Power Consumption	15 Watts (Maximum)
Ventilation	Fan-free design
EMI	Compliance with FCC Class A, CE
Safety	Compliance with UL, cUL, CE/EN60950-1