USER'S MANUAL

Management Ethernet Switch ESW-5242GP / ESW-5162GP

Ver. 1.0, Apr. 2007

Table of Content

1. Getting to Know Your Switch

1.1 About the ESW-5242GP / ESW-5162GP Switch

The ESW-5242GP / ESW-5162GP switches are powerful managed switches which have many features. These switches can be managed by WEB, TELNET, Consol or other third-party SNMP software as well. Besides, these switches can be managed by a useful utility that we called Super-VIEW.
Super-VIEW is a powerful network management software. With its friendly and powerful interface, you can easily configure multiple switches at the same time, and monitor switches' status.

1.2 Software Features

- World's fastest Redundant Ethernet Ring (Recovery time < 10ms for over 250 units connection)
- Supports Ring Coupling, Dual Homing, RSTP over The Ring
- Supports SNMPv1/v2/v3 & RMON & Port base/802.1Q VLAN Network Management
- Event notification by Email, SNMP trap and Relay Output
- Web-based ,Telnet, Console, CLI configuration
- Enable/disable ports, MAC based port security
- Port based network access control (802.1x)
- VLAN (802.1q) to segregate and secure network traffic
- Radius centralized password management
- SNMPv3 encrypted authentication and access security
- RSTP (802.1w)
- Quality of Service (802.1p) for real-time traffic
- VLAN (802.1q) with double tagging and GVRP supported
- IGMP Snooping for multicast filtering
- Port configuration, status, statistics, mirroring, security
- Remote Monitoring (RMON)

1.3 Hardware Features

- Wide Range AC power inputs (100VAC~240VAC, 50Hz~60Hz)
- Operating Temperature: -10 to 60°C
- Storage Temperature: -20 to 85 °C
- Operating Humidity: 5% to 95%, non-condensing
- 10/100/1000Base-T(X) Gigabit Ethernet port
- 10/100Base-T(X) Ethernet port
- 1000Base-X Fiber port on SFP
- Console Port
- Dimensions(W x D x H) : 440 mm(W)x 280 mm(D)x 44 mm(H)

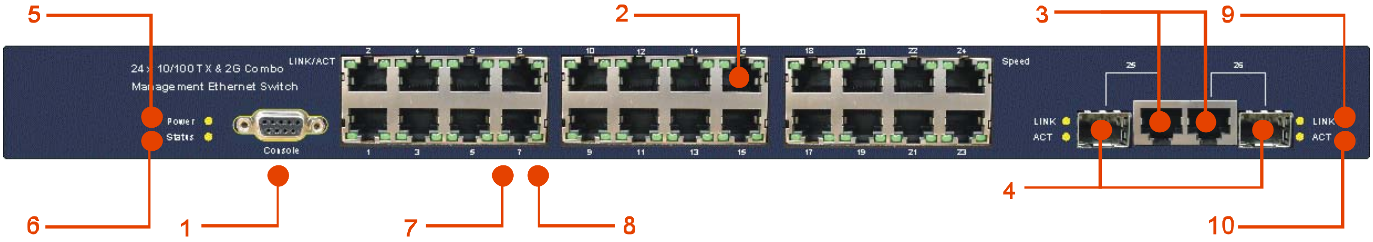
2. Hardware Overview

2.1 Front Panel

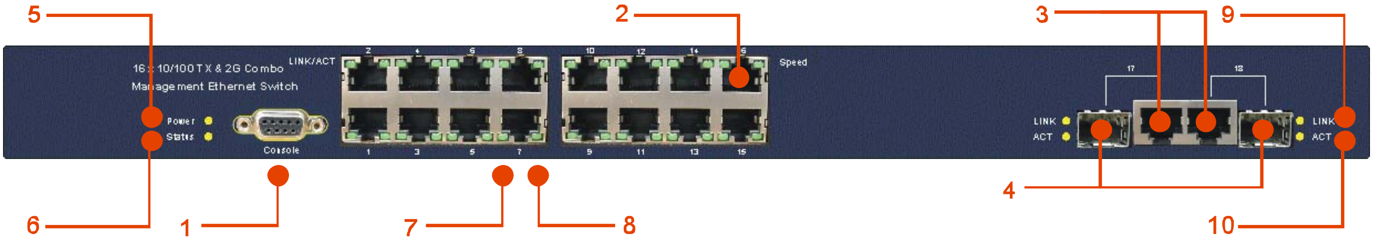
The following table describes the labels that stick on the ESW-5242GP / ESW-5162GP.

Port	Description
10/100 RJ-45 fast Ethernet ports	24/16 10/100Base-T(X) RJ-45 fast Ethernet ports support auto-negotiation. Default Setting : Speed: auto Duplex: auto Flow control : disable
Gigabit port	2 1000BaseT Giga ports (combo)
Fiber port	2 1000BaseX on SFP port (combo)
Console	Use RS-232 cable to manage switch.

ESW-5242GP



ESW-5162GP

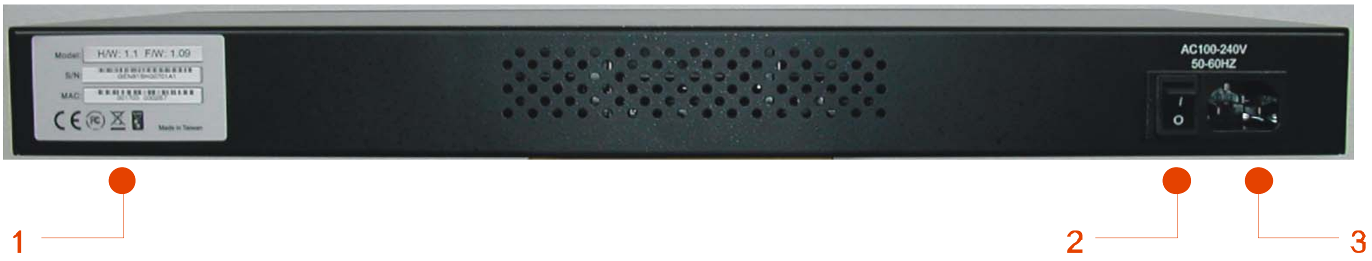


1. RS-232 Console Port. Set connection at 9600bps, 8N1.
2. 10/100Base-T(X) Ethernet ports.
3. 1000Base-T Ethernet port.
4. 1000BaseX fiber port in SFP socket.
5. LED for PWR. When the PWR links, the green led will be light on.
6. LED for Status. When the system is ready, the green led will be light on.
7. LED for Ethernet ports link status.
8. LED for Ethernet ports speed.
9. LED for gigabit combo Ethernet ports link status.
10. LED for gigabit combo Ethernet ports active.

2.2 Rare Panel

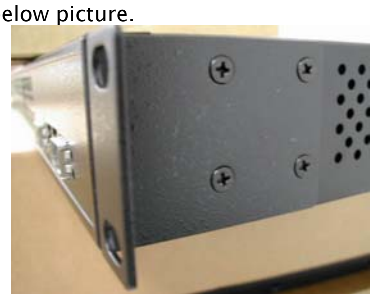
The rare panel of ESW-5242GP / ESW-5162GP is showed as below:

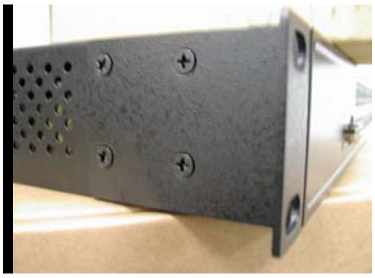
1. Label for MAC address and Serial Number.
2. Power Switch.
3. Power input for 100VAC~240VAC/50~60Hz.



2.3 Rack mount kit assembly

You can find the rack mount kit and the screws in the packing box. Please assembly the rack mount kit on the switch with screws as below picture.





3. Cables

3.1 Ethernet Cables

The ESW-5242GP / ESW-5162GP switches have standard Ethernet ports. According to the link type, the switches use CAT 3, 4, 5,5e UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45
1000BASE-TX	Cat. 5/Cat. 5e 100-ohm UTP	UTP 100 m (328ft)	RJ-45

3.1.1 100BASE-TX/10BASE-T Pin Assignments

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

RJ-45 Pin Assignments

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

The ESW-5242GP / ESW-5162GP switches support auto MDI/MDI-X operation. You can use a straight-through cable to make a connection between PC and switch. The following table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

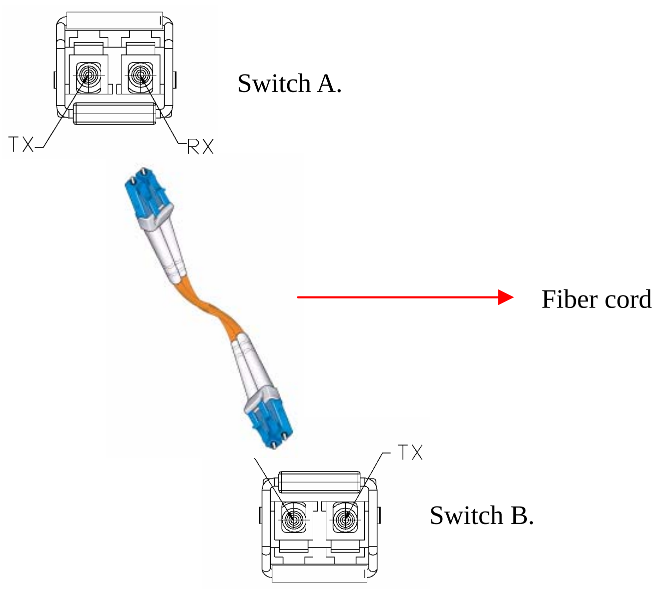
MDI/MDI-X pins assignment

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

Note: “+” and “-” signs represent the polarity of the wires that make up each wire pair.

3.2 Fibers

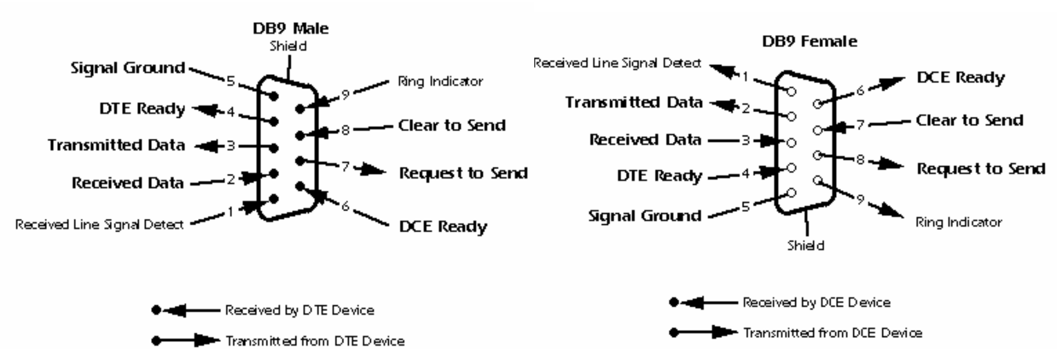
The ESW-5242GP / ESW-5162GP switches have fiber optical ports with SFP connectors. The fiber optical ports are in multi-mode (0 to 550M, 850 nm with 50/125 µm, 62.5/125 µm fiber) and single-mode with LC connector. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.



3.3 Console Cable

ESW-5242GP / ESW-5162GP switches can be management by console port. You can connect them to PC through a RS-232 cable

PC pin out (male) assignment	DB9 female connector on switch
Pin #2 RD	Pin #2 TD
Pin #3 TD	Pin #3 RD
Pin #5 GD	Pin #5 GD



4. WEB Management

4.1 Configuration by Web Browser

This section introduces the configuration by Web browser.

4.1.1 About Web-based Management

Inside the CPU board of the switch, an embedded HTML web site resides in flash memory. It contains advanced management features and allows you 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 5.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

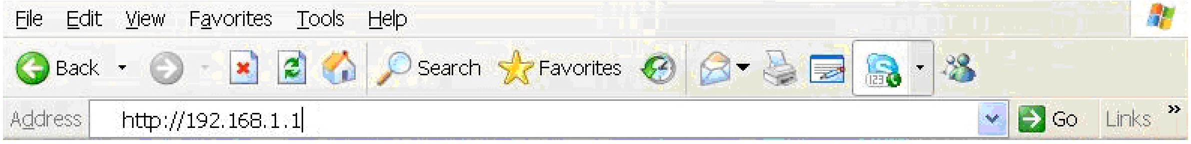
Note: By default, IE5.0 or later version does not allow Java Applets to open sockets. You need to explicitly modify the browser setting in order to enable Java Applets to use network ports.

4.1.2 Preparing for Web Management

The default value is as below:
IP Address: **192.168.1.1**
Subnet Mask: **255.255.255.0**
Default Gateway: **192.168.1.254**
User Name: **admin**
Password: **admin**

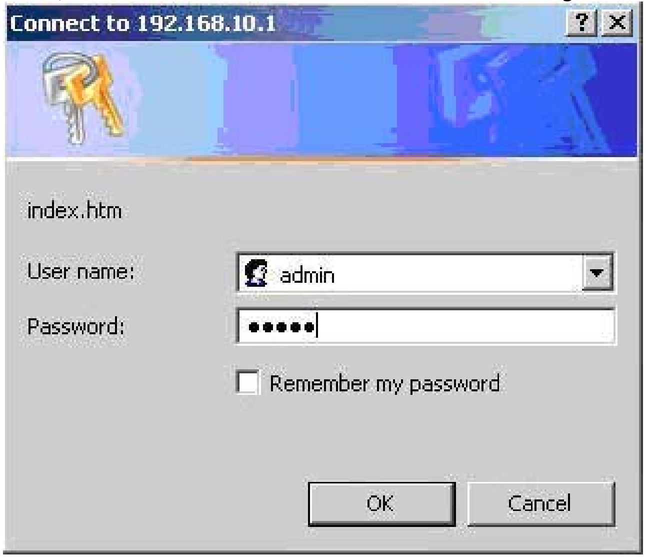
4.1.3 System Login

1. Launch the Internet Explorer.
2. Type http:// and the IP address of the switch. Press "**Enter**".



Address http://192.168.1.1

3. The login screen appears.
4. Key in the username and password. The default username and password is "**admin**".
5. Click "**Enter**" or "**OK**" button, then the main interface of the Web-based management appears.



Connect to 192.168.10.1

index.htm

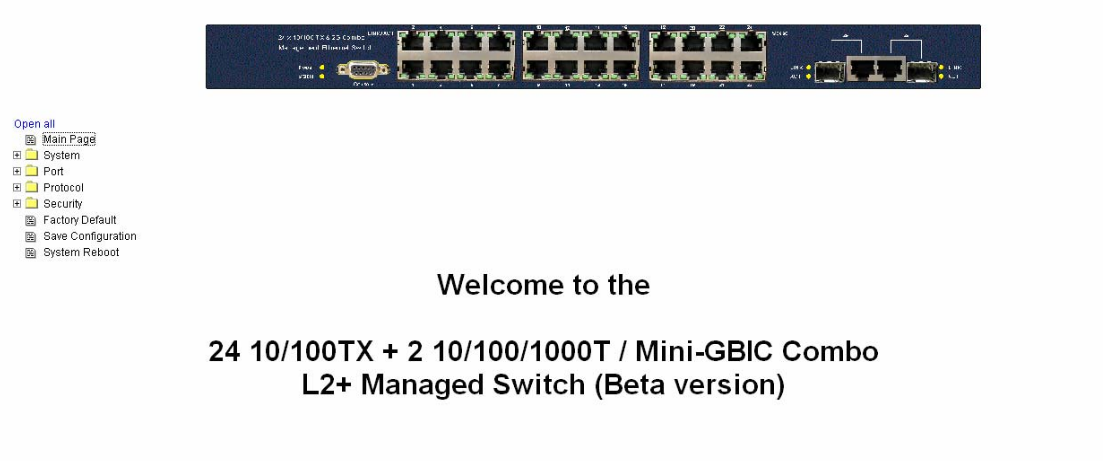
User name: admin

Password: •••••

□ Remember my password

Login screen

4.1.4 MAIN INTERFACE



Open all
- Main Page
- System
- Port
- Protocol
- Security
- Factory Default
- Save Configuration
- System Reboot

Welcome to the

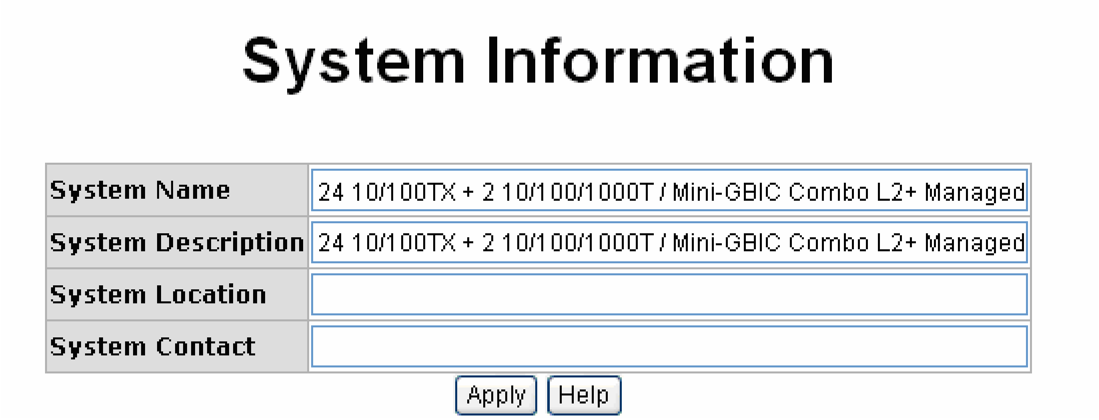
24 10/100TX + 2 10/100/1000T / Mini-GBIC Combo
L2+ Managed Switch (Beta version)

Main interface

4.1.5 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:** Display 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:** Display the switch's firmware version
- **Kernel Version:** Display the kernel software version
- **MAC Address:** Display the unique hardware address assigned by manufacturer (default)



System Information

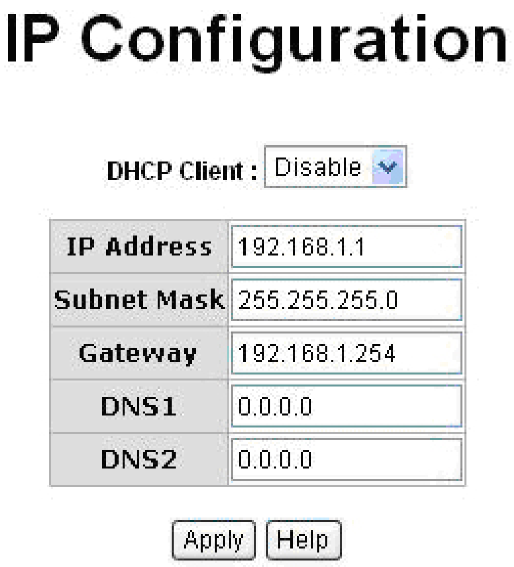
System Name	24 10/100TX + 2 10/100/1000T / Mini-GBIC Combo L2+ Managed
System Description	24 10/100TX + 2 10/100/1000T / Mini-GBIC Combo L2+ Managed
System Location	
System Contact	

System information interface

4.1.6 IP CONFIGURATION

To 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 assign the IP address from the network DHCP server. The default IP address will be replaced by the DHCP server assigned IP address. After user click "Apply" button, a popup dialog shows up. That is to inform users that when the DHCP client is enabling, the current IP will lose and users should find the new IP on the DHCP server.
- **IP Address:** Assign the IP address which the network is using. If DHCP client function is enabling, users do not need to assign the IP address. The network DHCP server will assign the IP address for the industrial switch and display in this column. The default IP is 192.168.1.1
- **Subnet Mask:** Assign the subnet mask of the IP address. If DHCP client function is enabling, users 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



IP Configuration

DHCP Client : Disable

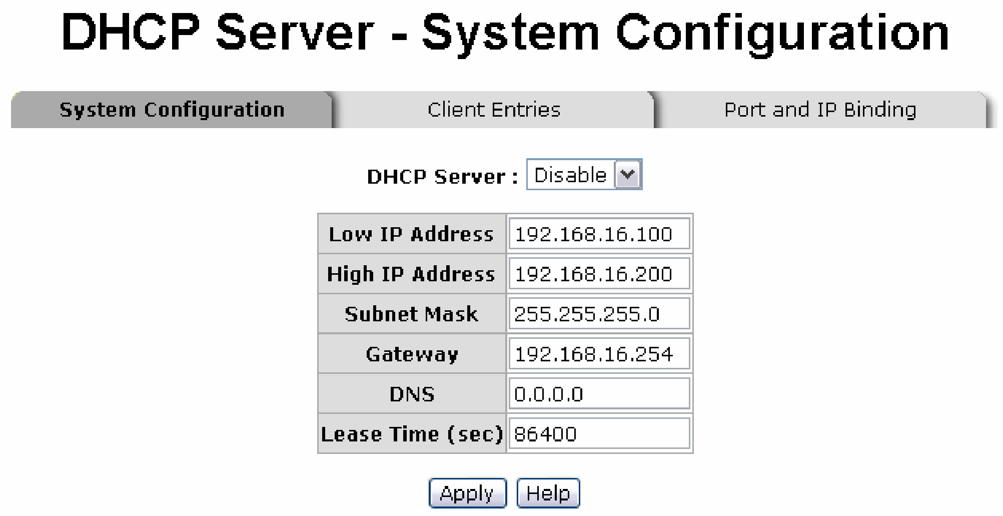
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
DNS1	0.0.0.0
DNS2	0.0.0.0

IP configuration interface

4.1.7 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 that the dynamic IP will not occupied for a long time or the server does not know that the dynamic IP is idle.
- And then, click Apply



DHCP Server - System Configuration

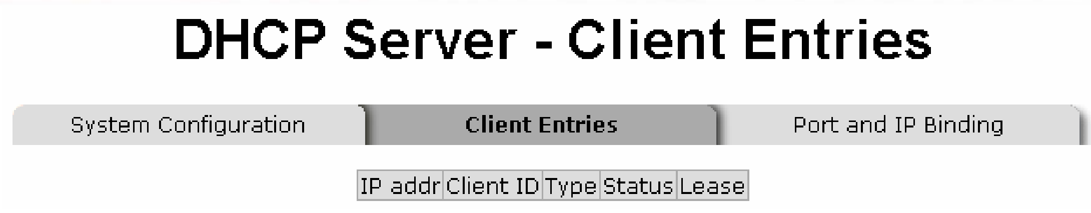
DHCP Server : Disable

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

4.1.8 DHCP CLIENT – SYSTEM CONFIGURATION

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



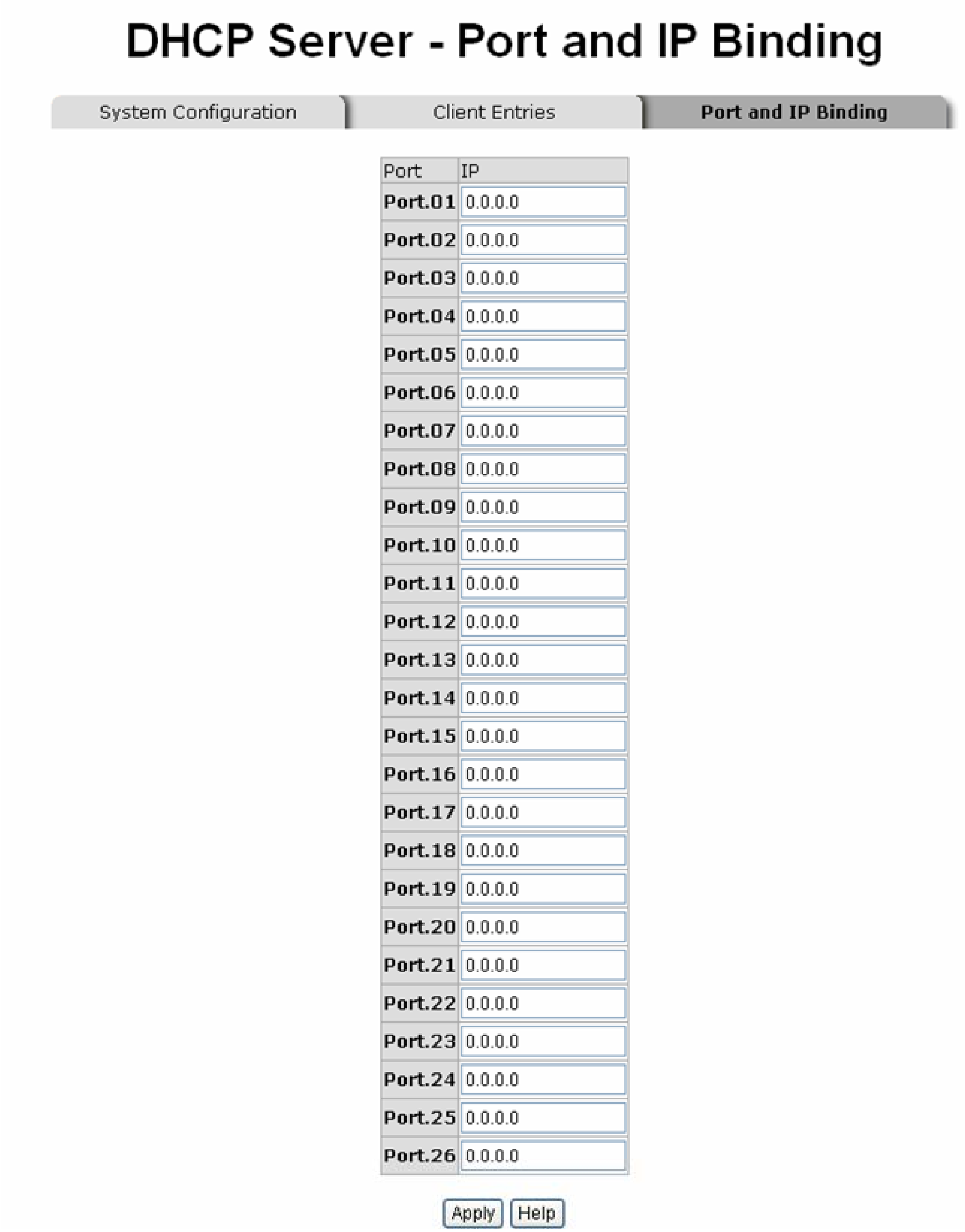
DHCP Server - Client Entries

IP addr	Client ID	Type	Status	Lease

DHCP Client Entries interface

4.1.9 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 asking for assigning dynamic IP, the system will assign the IP address which has been assigned before to the connected device.



DHCP Server - Port and IP Binding

Port	IP
Port.01	0.0.0.0
Port.02	0.0.0.0
Port.03	0.0.0.0
Port.04	0.0.0.0
Port.05	0.0.0.0
Port.06	0.0.0.0
Port.07	0.0.0.0
Port.08	0.0.0.0
Port.09	0.0.0.0
Port.10	0.0.0.0
Port.11	0.0.0.0
Port.12	0.0.0.0
Port.13	0.0.0.0
Port.14	0.0.0.0
Port.15	0.0.0.0
Port.16	0.0.0.0
Port.17	0.0.0.0
Port.18	0.0.0.0
Port.19	0.0.0.0
Port.20	0.0.0.0
Port.21	0.0.0.0
Port.22	0.0.0.0
Port.23	0.0.0.0
Port.24	0.0.0.0
Port.25	0.0.0.0
Port.26	0.0.0.0

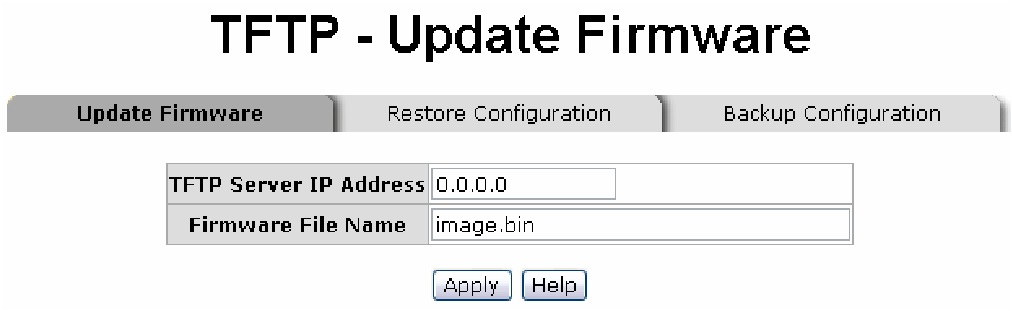
Port and IP Bindings interface

4.1.10 TFTP - Update Firmware

It provides the functions that allow users to update the switch firmware. Before update, 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 - Update Firmware

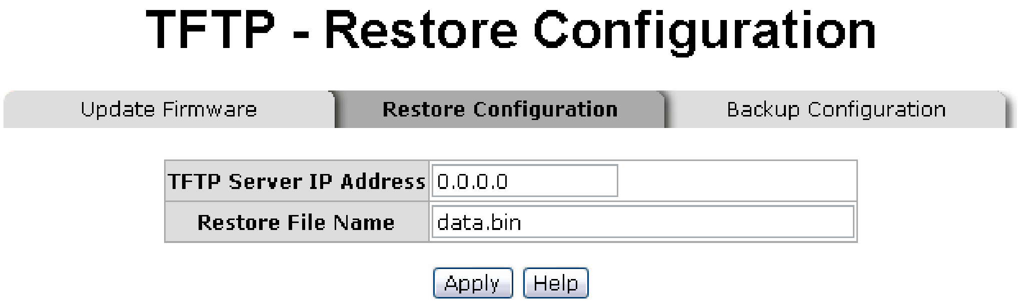
TFTP Server IP Address	0.0.0.0
Firmware File Name	image.bin

Update Firmware interface

4.1.11 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 - Restore Configuration

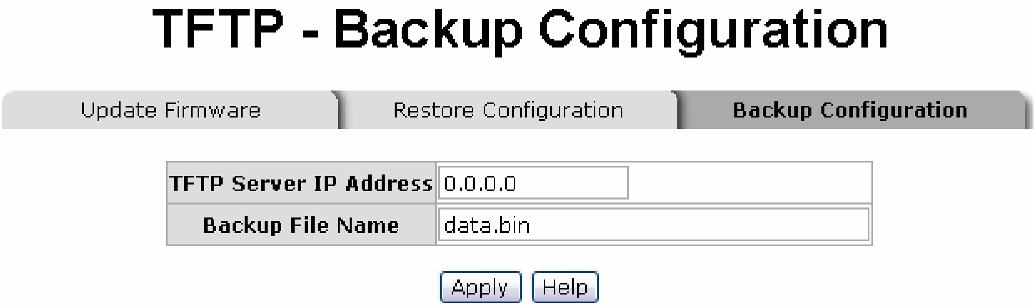
TFTP Server IP Address	0.0.0.0
Restore File Name	data.bin

Restore Configuration interface

4.1.12 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 in the file name
3. Click Apply.



TFTP - Backup Configuration

TFTP Server IP Address	0.0.0.0
Backup File Name	data.bin

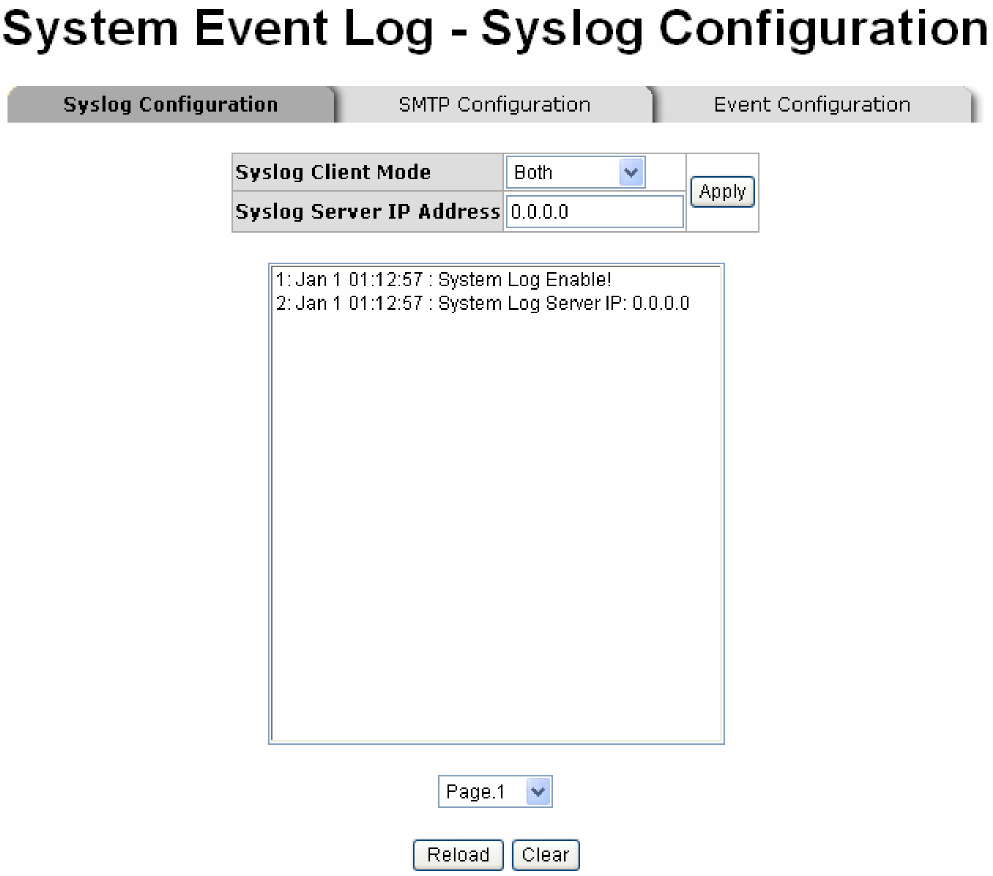
Backup Configuration interface

4.1.13 System Event Log – Syslog Configuration

To configure the system event mode that you wish 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.



System Event Log - Syslog Configuration

Syslog Client Mode	Both
Syslog Server IP Address	0.0.0.0

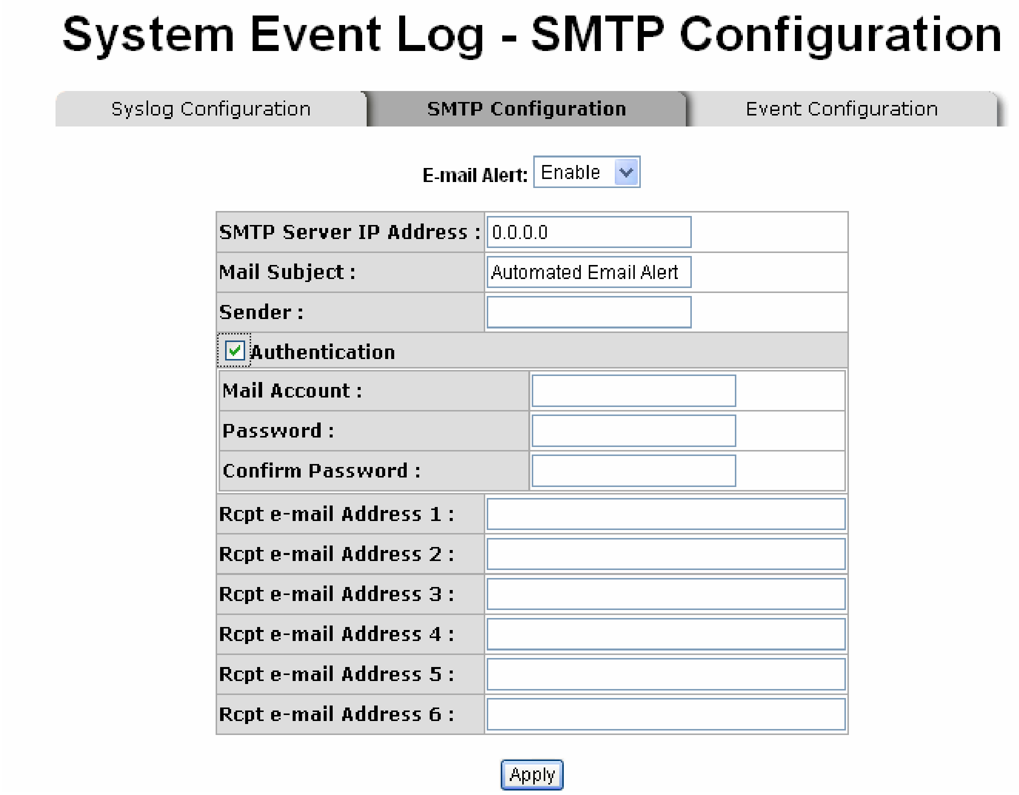
```
1: Jan 1 01:12:57 : System Log Enable!
2: Jan 1 01:12:57 : System Log Server IP: 0.0.0.0
```

Syslog Configuration interface

4.1.14 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 to receive the alert. Ex: admin@abc.com 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.



System Event Log - SMTP Configuration

E-mail Alert: Enable

SMTP Server IP Address :	0.0.0.0
Mail Subject :	Automated Email Alert
Sender :	
☑ 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 :	

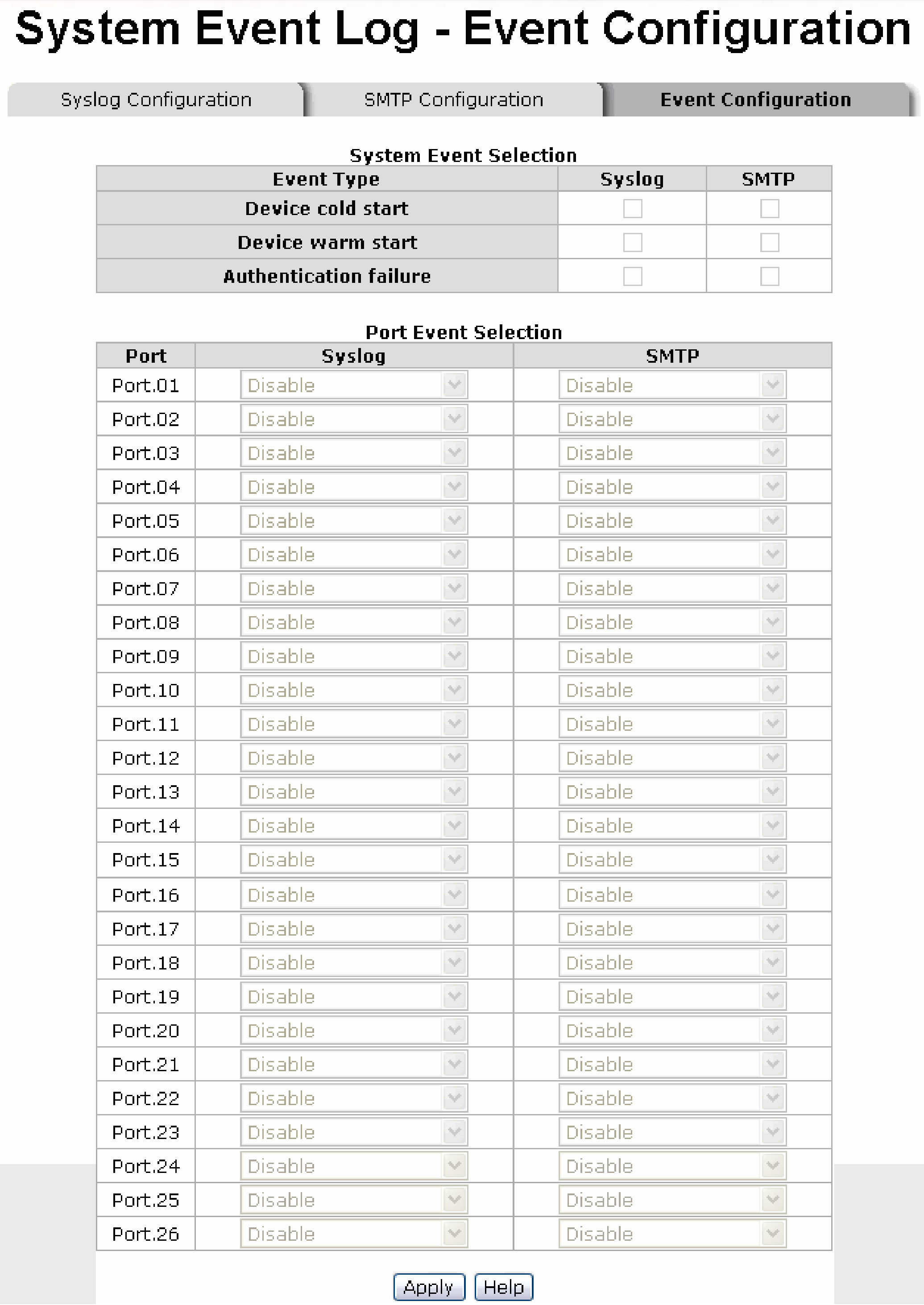
SMTP Configuration interface

4.1.15 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, each port log and SMTP events can be selected. After configure, Click Apply.

- **System event selection:** 4 selections – Device cold start, Device warm start, 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, 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.

- **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.



System Event Log - Event Configuration

System Event Selection

Event Type	Syslog	SMTP
Device cold start	□	□
Device warm start	□	□
Authentication failure	□	□

Port Event Selection

Port	Syslog	SMTP
Port.01	Disable	Disable
Port.02	Disable	Disable
Port.03	Disable	Disable
Port.04	Disable	Disable
Port.05	Disable	Disable
Port.06	Disable	Disable
Port.07	Disable	Disable
Port.08	Disable	Disable
Port.09	Disable	Disable
Port.10	Disable	Disable
Port.11	Disable	Disable
Port.12	Disable	Disable
Port.13	Disable	Disable
Port.14	Disable	Disable
Port.15	Disable	Disable
Port.16	Disable	Disable
Port.17	Disable	Disable
Port.18	Disable	Disable
Port.19	Disable	Disable
Port.20	Disable	Disable
Port.21	Disable	Disable
Port.22	Disable	Disable
Port.23	Disable	Disable
Port.24	Disable	Disable
Port.25	Disable	Disable
Port.26	Disable	Disable

Event Configuration interface

4.1.16 SNTP CONFIGURATION

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

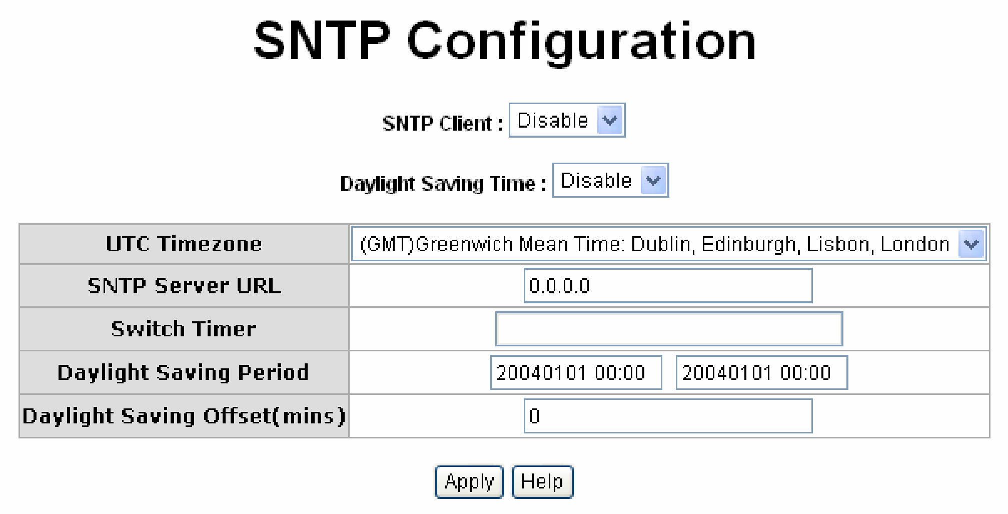
1. **SNTP Client:** enable or disable SNTP function to get the time from the SNTP server.
2. **Daylight Saving Time:** enable or disable daylight saving time function. When daylight saving time is enabling, you need to configure the daylight saving time period..
3. **UTC Timezone:** set the switch location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

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am

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

USSR Zone 9		
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. **Daylight Saving Period:** set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different in every year.
6. **Daylight Saving Offset (mins):** set up the offset time.
7. **Switch Timer:** display the switch current 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

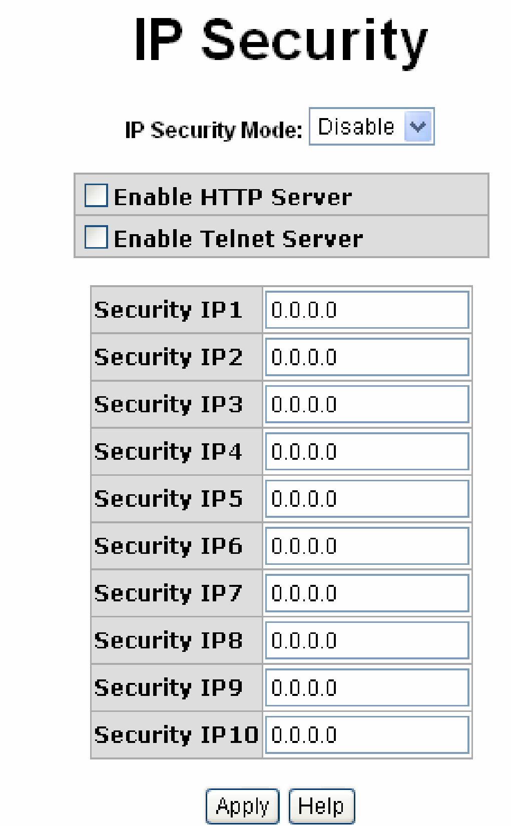
SNTP Configuration interface

4.1.17 IP Security

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

- **IP Security Mode:** when this option is in **Enable** mode, the **Enable HTTP Server** and **Enable Telnet Server** check boxes will then be available.
- **Enable HTTP Server:** when this check box is checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access via HTTP service.
- **Enable Telnet Server:** when checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access via telnet service.
- **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: Disable

□ Enable HTTP Server
□ Enable Telnet Server

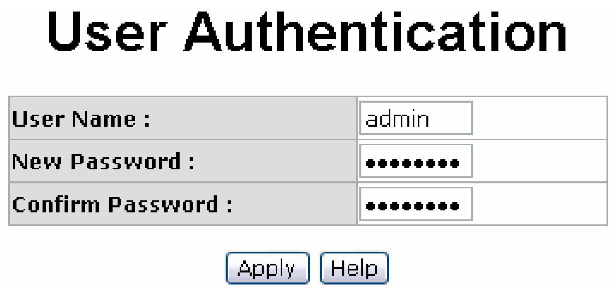
Security IP1	0.0.0.0
Security IP2	0.0.0.0
Security IP3	0.0.0.0
Security IP4	0.0.0.0
Security IP5	0.0.0.0
Security IP6	0.0.0.0
Security IP7	0.0.0.0
Security IP8	0.0.0.0
Security IP9	0.0.0.0
Security IP10	0.0.0.0

IP Security interface

4.1.18 User Authentication

Change login username and password for the web management security.

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



User Authentication

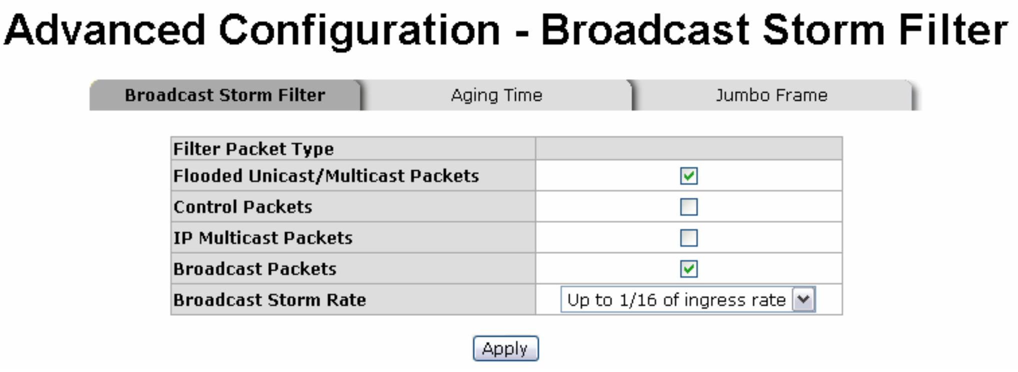
User Name :	admin
New Password :	●●●●●●●●
Confirm Password :	●●●●●●●●

User Authentication interface

4.1.19 Advanced Configuration– Broadcast Storm Filter

Set the broadcast storm rate to prevent network crash..

1. **Flooded Unicast / Multicast Packets:** Enable/disable to limit the frame type.
2. **Control Packets:** Enable/disable to limit the frame type.
3. **IP Multicast Packets:** Enable/disable to limit the frame type.
4. **Broadcast Packets:** Enable/disable to limit the frame type.

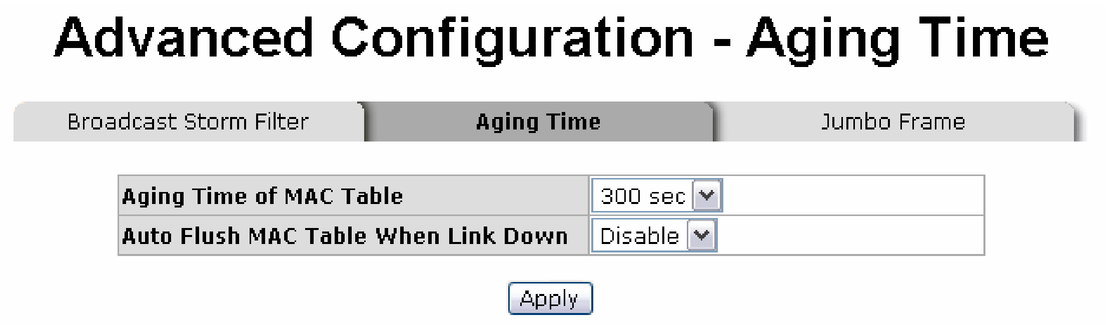


Advanced Configuration - Broadcast Storm Filter

Filter Packet Type	
Flooded Unicast/Multicast Packets	☑
Control Packets	□
IP Multicast Packets	□
Broadcast Packets	☑
Broadcast Storm Rate	Up to 1/16 of ingress rate

4.1.20 ADVANCED CONFIGURATION– AGING TIME

1. **Aging Time of MAC Table:** Default 300secs.
2. **Auto Flush MAC Table When Link Down:** enable/disable the function

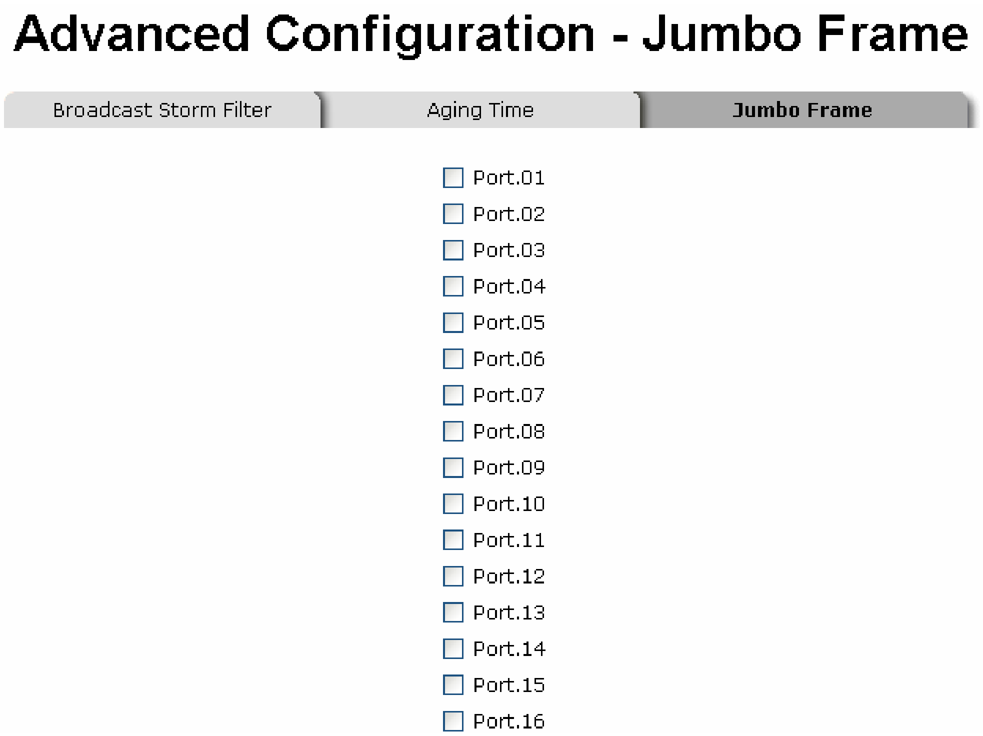


Advanced Configuration - Aging Time

Aging Time of MAC Table	300 sec
Auto Flush MAC Table When Link Down	Disable

4.1.21 ADVANCED CONFIGURATION– JUMBO FRAME

1. **Jumbo Frame:** Enable/disable per port Jumbo frame function.



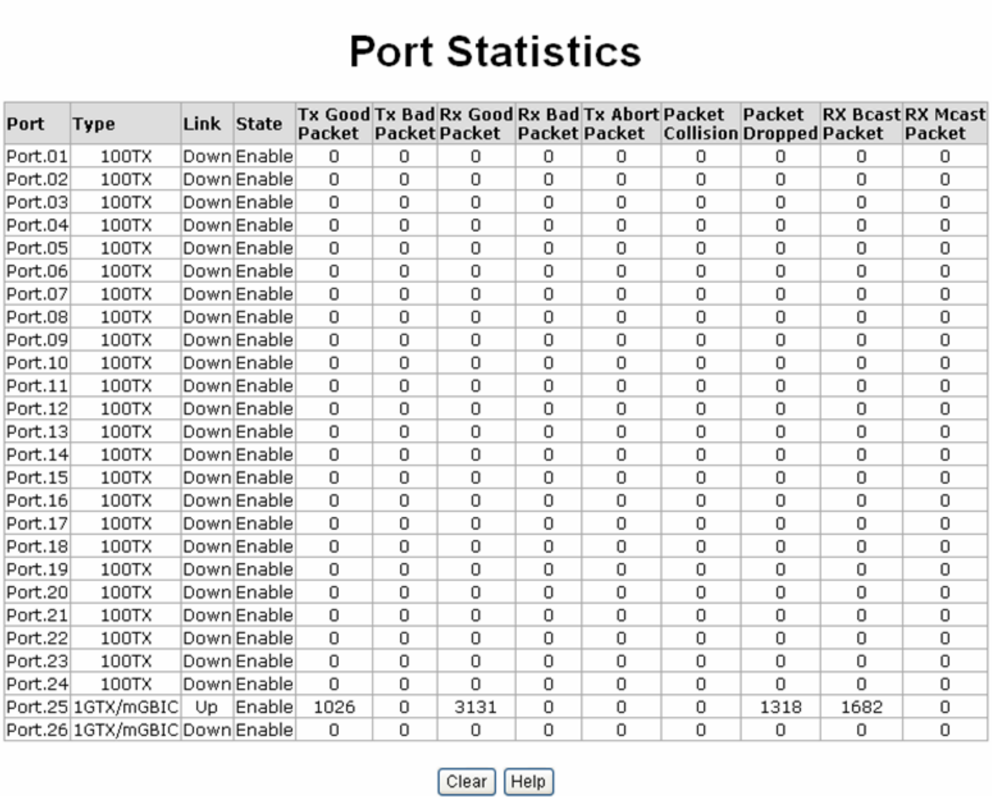
Advanced Configuration - Jumbo Frame

□ Port.01
□ Port.02
□ Port.03
□ Port.04
□ Port.05
□ Port.06
□ Port.07
□ Port.08
□ Port.09
□ Port.10
□ Port.11
□ Port.12
□ Port.13
□ Port.14
□ Port.15
□ Port.16

4.1.22 PORT STATISTICS

The following information provides the current port statistic information

- Click Clear button to clean all counts



Port Statistics

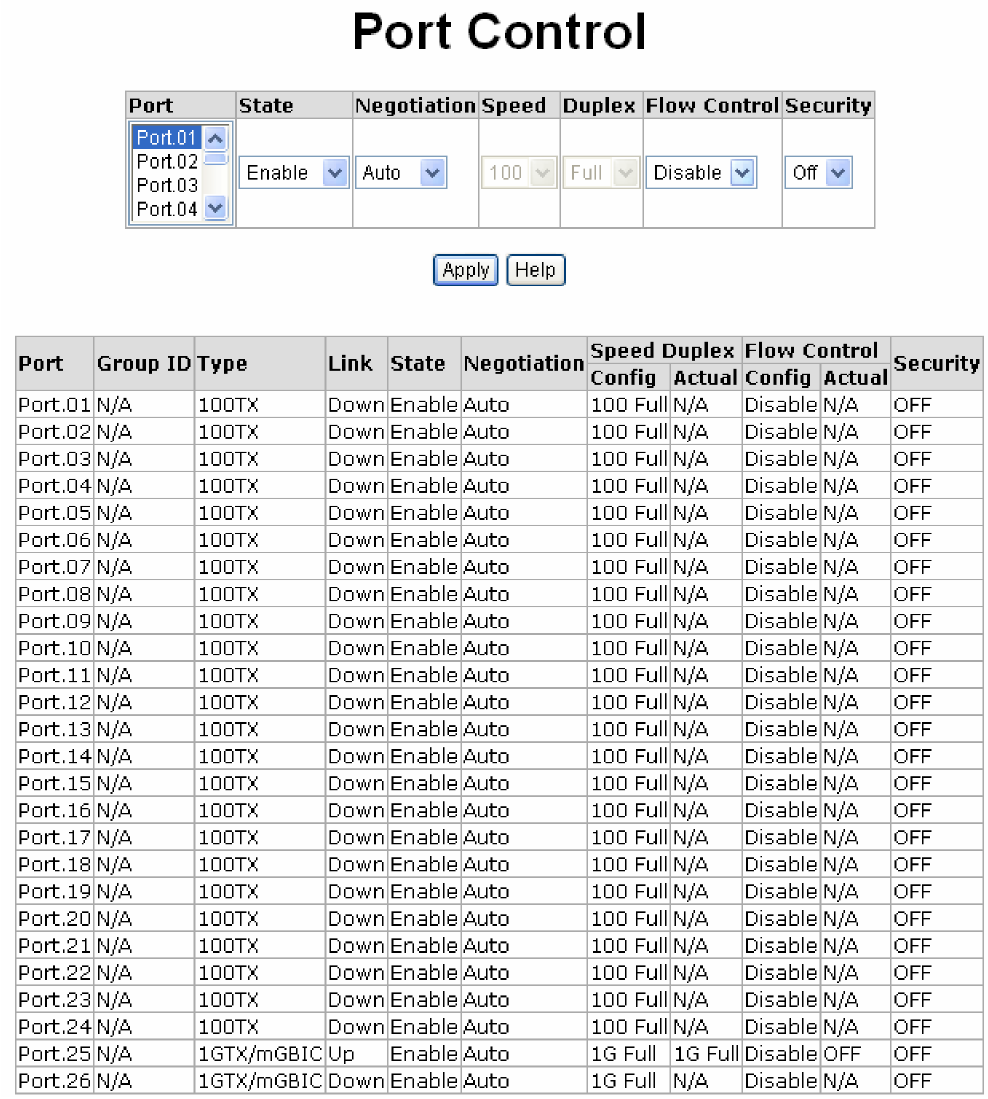
Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision	Packet Dropped	RX Bcast Packet	RX Mcast Packet
Port.01	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.07	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.08	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.09	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.10	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.11	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.12	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.13	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.14	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.15	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.16	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.17	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.18	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.19	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.20	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.21	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.22	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.23	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.24	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.25	1GTX/mGBIC	Up	Enable	1026	0	3131	0	0	0	1318	1682	0
Port.26	1GTX/mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0

Port Statistics interface

4.1.23 PORT CONTROL

In Port control, you can view every port status which depend on users' setting and the negotiation result.

1. **Port:** select the port that you want to configure.
2. **State:** Current port status. The port can be set to disable or enable mode. If the port setting is disabled then it 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
7. **Security:** When the state is "**On**", it means that this port accepts only one MAC address.
8. Click Apply .



Port Control

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

Port	Group ID	Type	Link	State	Negotiation	Speed Duplex		Flow Control		Security
						Config	Actual	Config	Actual	
Port.01	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.02	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.03	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.04	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.05	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.06	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.07	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.08	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.09	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.10	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.11	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.12	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.13	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.14	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.15	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.16	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.17	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.18	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.19	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.20	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.21	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.22	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.23	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.24	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.25	N/A	1GTX/mGBIC	Up	Enable	Auto	1G Full	1G Full	Disable	OFF	OFF
Port.26	N/A	1GTX/mGBIC	Down	Enable	Auto	1G Full	N/A	Disable	N/A	OFF

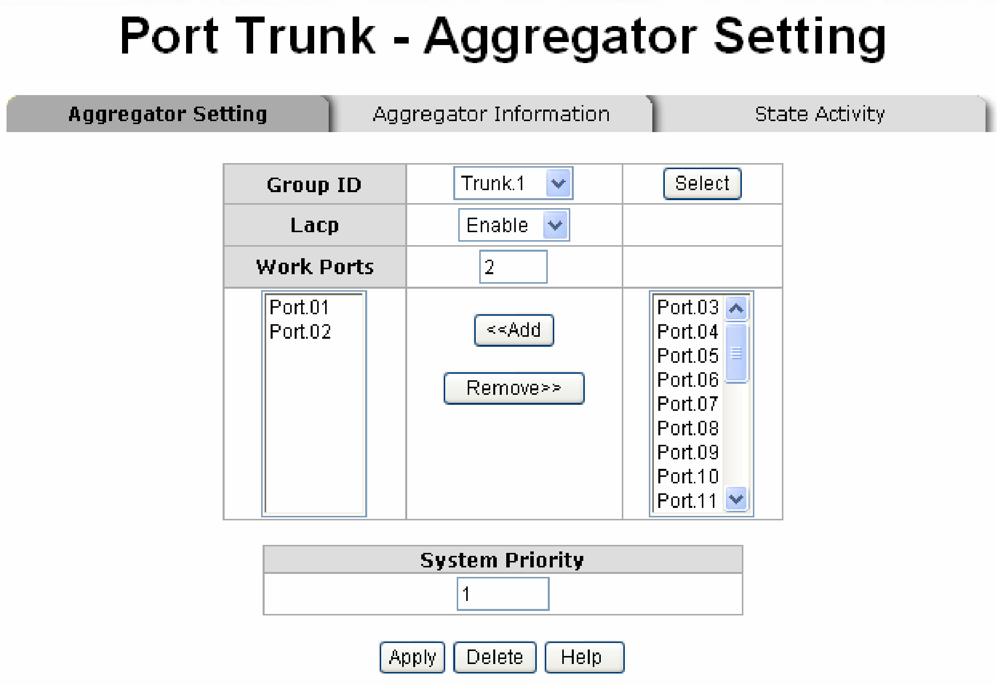
Port Control interface

4.1.24 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.

4.1.24.1 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 maximum four ports to 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 maximum four ports to 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, you 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

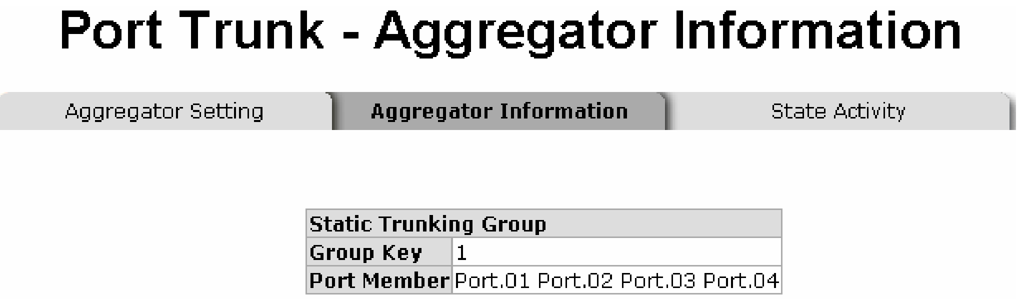
Group ID	Trunk.1	
Lacp	Enable	
Work Ports	2	
Port.01 Port.02		Port.03 Port.04 Port.05 Port.06 Port.07 Port.08 Port.09 Port.10 Port.11

System Priority
1

Port Trunk—Aggregator Setting interface

4.1.24.2 Aggregator Information

When you had setup the LACP aggregator, you will see relation information in here.



Port Trunk - Aggregator Information

Static Trunking Group	
Group Key	1
Port Member	Port.01 Port.02 Port.03 Port.04

Port Trunk – Aggregator Information interface

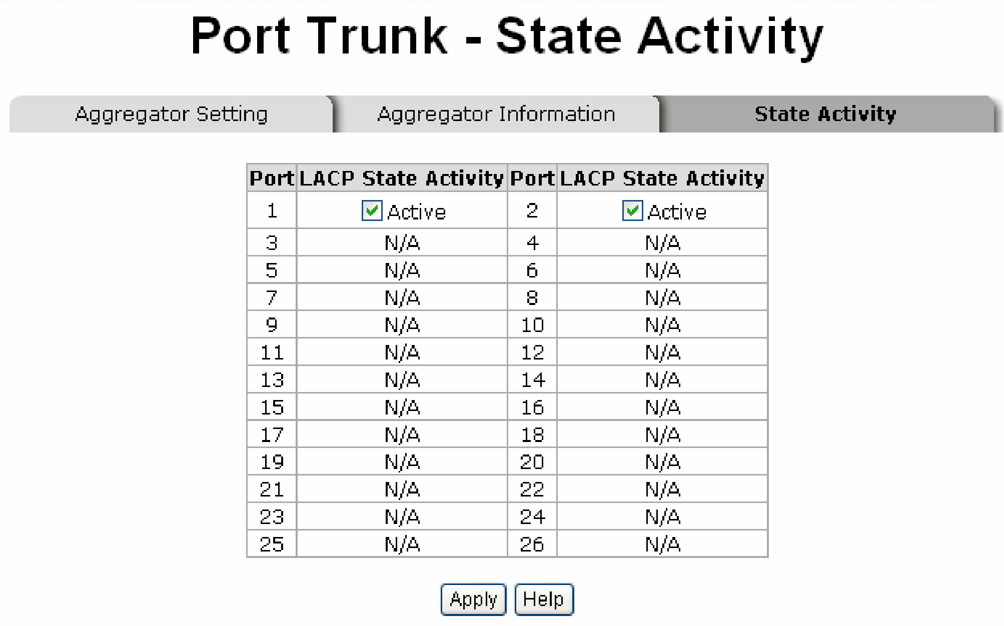
4.1.24.3 State Activity

After you setup the LACP aggregator, you can configure port state activity. You can mark or un-mark the port. When you mark the port and click Apply button the port state activity will change to **Active**. Opposite is **Passive**.

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

[NOTE]

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 active LACP's actor, after you have selected trunk port, the active status will be created automatically.



Port Trunk - State Activity

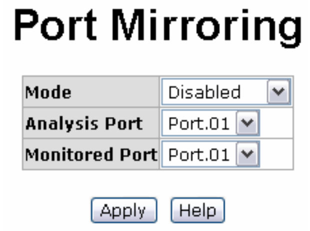
Port	LACP State Activity	Port	LACP State Activity
1	☑ Active	2	☑ Active
3	N/A	4	N/A
5	N/A	6	N/A
7	N/A	8	N/A
9	N/A	10	N/A
11	N/A	12	N/A
13	N/A	14	N/A
15	N/A	16	N/A
17	N/A	18	N/A
19	N/A	20	N/A
21	N/A	22	N/A
23	N/A	24	N/A
25	N/A	26	N/A

Port Trunk – State Activity interface

4.1.25 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 (source) ports will be duplicated into mirror (destination) port.

- **Analysis Port:** Only one port can be selected to be the destination (mirror) port for monitoring both RX and TX traffic which come from source port. Otherwise, use one of two ports for monitoring RX traffic only and the other one for TX traffic only. User can connect mirror port to LAN analyzer or Netxray
- **Monitored Port:** The ports that users want to monitor. All monitored port traffic will be copied to mirror (destination) port. Users can select one source port by checking the **RX** or **TX** radio group to be monitored.
- And then, click Apply button.



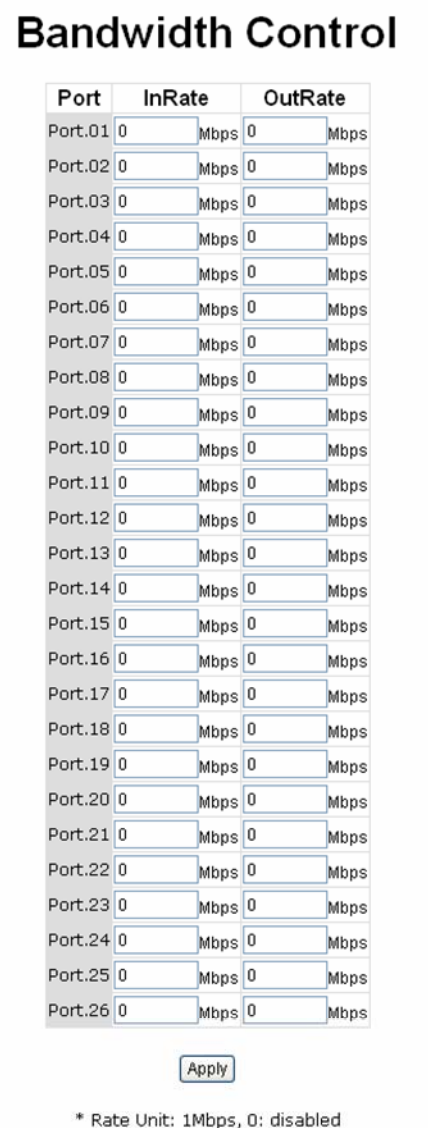
Port Mirroring

Mode	Disabled
Analysis Port	Port.01
Monitored Port	Port.01

Port Trunk – Port Mirroring interface

4.1.26 RATE LIMITING

You can set up the bandwidth rate for each port here.



Bandwidth Control

Port	InRate	OutRate
Port.01	0 Mbps	0 Mbps
Port.02	0 Mbps	0 Mbps
Port.03	0 Mbps	0 Mbps
Port.04	0 Mbps	0 Mbps
Port.05	0 Mbps	0 Mbps
Port.06	0 Mbps	0 Mbps
Port.07	0 Mbps	0 Mbps
Port.08	0 Mbps	0 Mbps
Port.09	0 Mbps	0 Mbps
Port.10	0 Mbps	0 Mbps
Port.11	0 Mbps	0 Mbps
Port.12	0 Mbps	0 Mbps
Port.13	0 Mbps	0 Mbps
Port.14	0 Mbps	0 Mbps
Port.15	0 Mbps	0 Mbps
Port.16	0 Mbps	0 Mbps
Port.17	0 Mbps	0 Mbps
Port.18	0 Mbps	0 Mbps
Port.19	0 Mbps	0 Mbps
Port.20	0 Mbps	0 Mbps
Port.21	0 Mbps	0 Mbps
Port.22	0 Mbps	0 Mbps
Port.23	0 Mbps	0 Mbps
Port.24	0 Mbps	0 Mbps
Port.25	0 Mbps	0 Mbps
Port.26	0 Mbps	0 Mbps

* Rate Unit: 1Mbps, 0: disabled

Rate Limiting interface

- All the ports support packet ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set the rate of effective egress to 2Mbps, and ingress rate to 1Mbps. The switch performs the ingress rate by packet counter to meet the specified rate

➢ **InRate:** Enter the port effective ingress rate(The default value is "0")

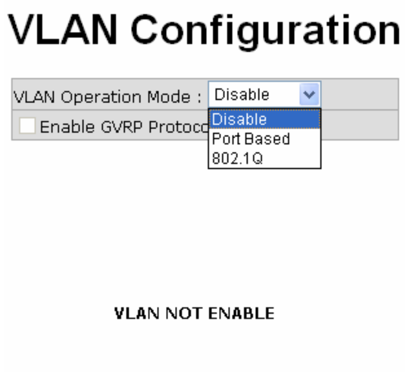
➢ **OutRate:** Enter the port effective egress rate(The default value is "0")

- And then, click Apply to apply the settings

4.1.27 VLAN CONFIGURATION

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which allows you 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. The default configuration of VLAN operation mode is at "**Disable**".



VLAN Configuration

VLAN Operation Mode : Disable

□ Enable GVRP Protoco

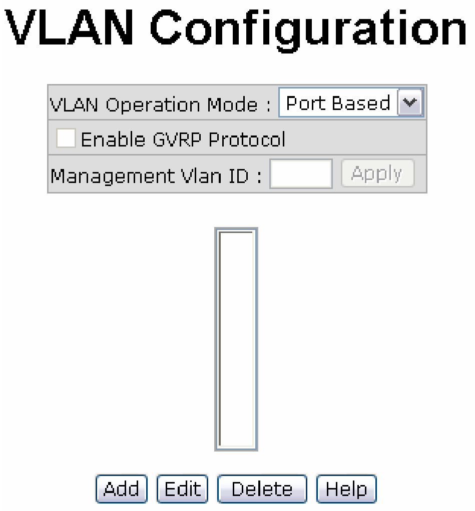
VLAN NOT ENABLE

VLAN Configuration interface

4.1.27.1 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 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

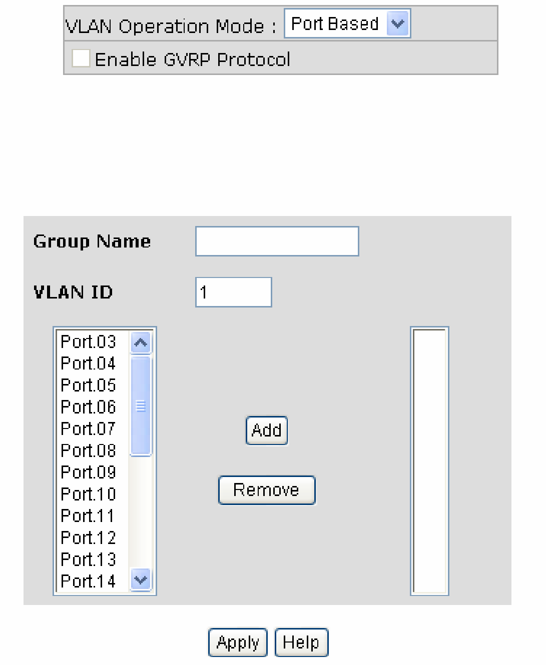
VLAN Operation Mode : Port Based

□ 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 Operation Mode : Port Based

□ Enable GVRP Protocol

Group Name

VLAN ID 1

Port.03 Port.04 Port.05 Port.06 Port.07 Port.08 Port.09 Port.10 Port.11 Port.12 Port.13 Port.14

VLAN—Port Based Add interface

- You 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.

4.1.27.2 802.1Q 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.
You 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 cannot be deleted.

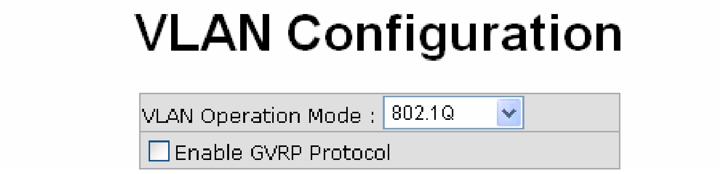
GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request using the VID of a VLAN defined on the switch; the switch will automatically add that device to the existing VLAN.

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 switches.
- **Hybrid Link:** Both **Access Link** and **Trunk Link** are available.

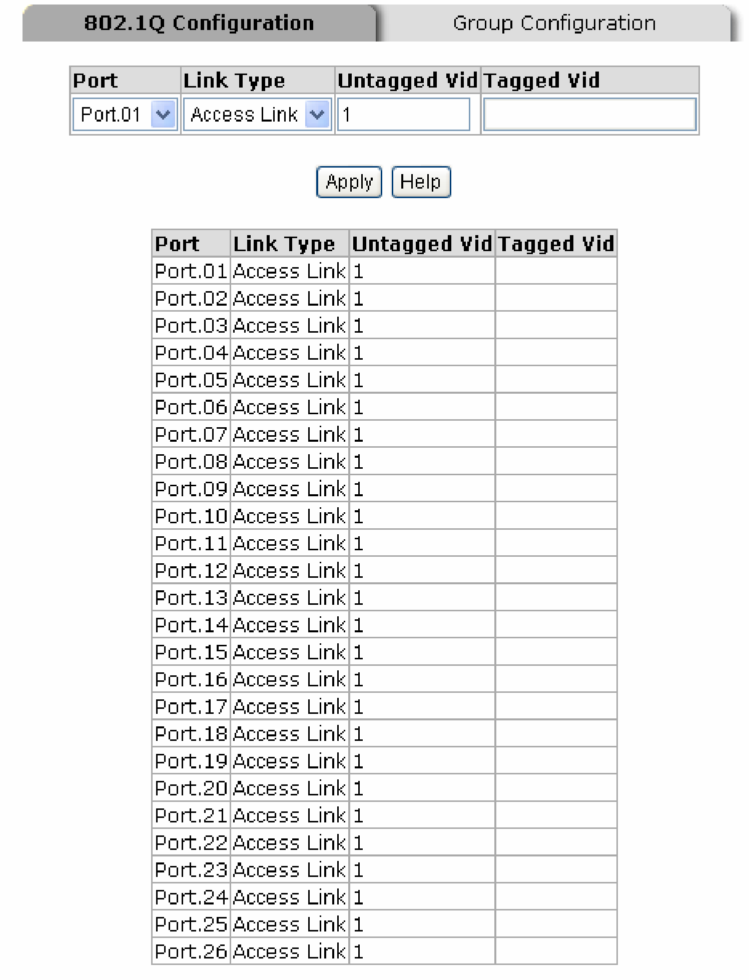
4. **Untagged VID:** assign the untagged frame VID.
5. **Tagged VID:** assign the tagged frame VID.
6. Click Apply



VLAN Configuration

VLAN Operation Mode : 802.1Q

□ Enable GVRP Protocol



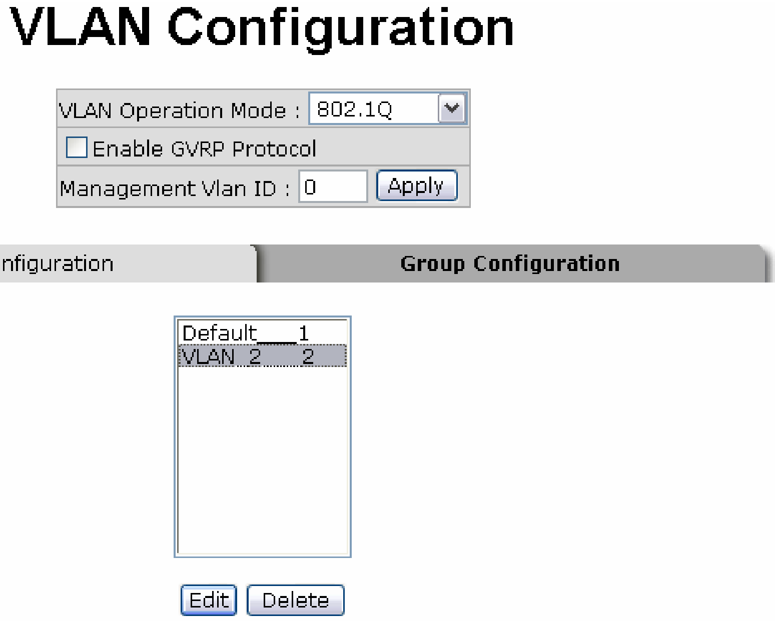
Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	

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	
Port.09	Access Link	1	
Port.10	Access Link	1	
Port.11	Access Link	1	
Port.12	Access Link	1	
Port.13	Access Link	1	
Port.14	Access Link	1	
Port.15	Access Link	1	
Port.16	Access Link	1	
Port.17	Access Link	1	
Port.18	Access Link	1	
Port.19	Access Link	1	
Port.20	Access Link	1	
Port.21	Access Link	1	
Port.22	Access Link	1	
Port.23	Access Link	1	
Port.24	Access Link	1	
Port.25	Access Link	1	
Port.26	Access Link	1	

802.1q VLAN interface

Group Configuration
Edit the existing VLAN Group.

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



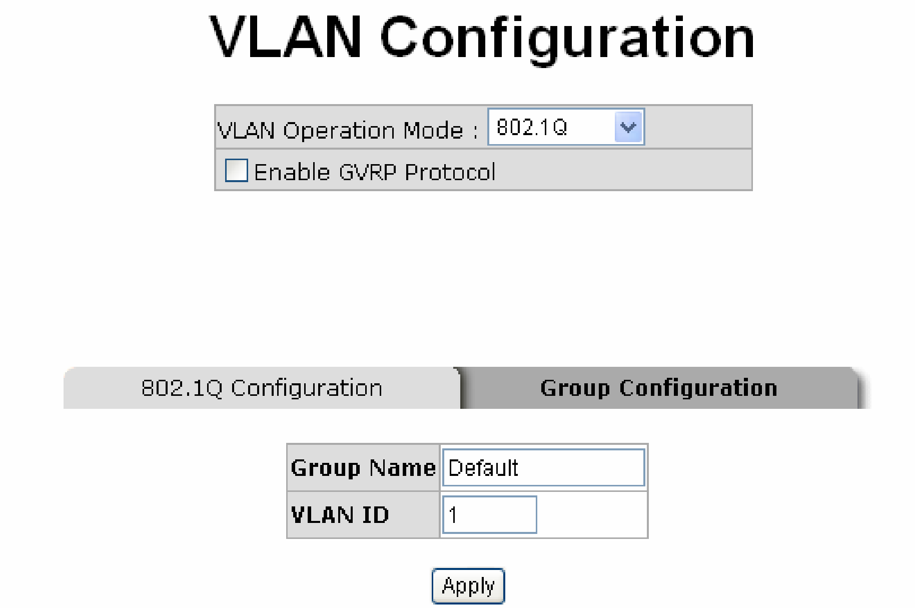
VLAN Configuration

VLAN Operation Mode : 802.1Q
□ Enable GVRP Protocol
Management Vlan ID : 0 Apply

Default 1
VLAN_2 2

Group Configuration interface

3. You can Change the VLAN group name and VLAN ID.
4. Click Apply.



VLAN Configuration

VLAN Operation Mode : 802.1Q

□ Enable GVRP Protocol

Group Name	Default
VLAN ID	1

Group Configuration interface

4.1.28 RAPID SPANNING TREE

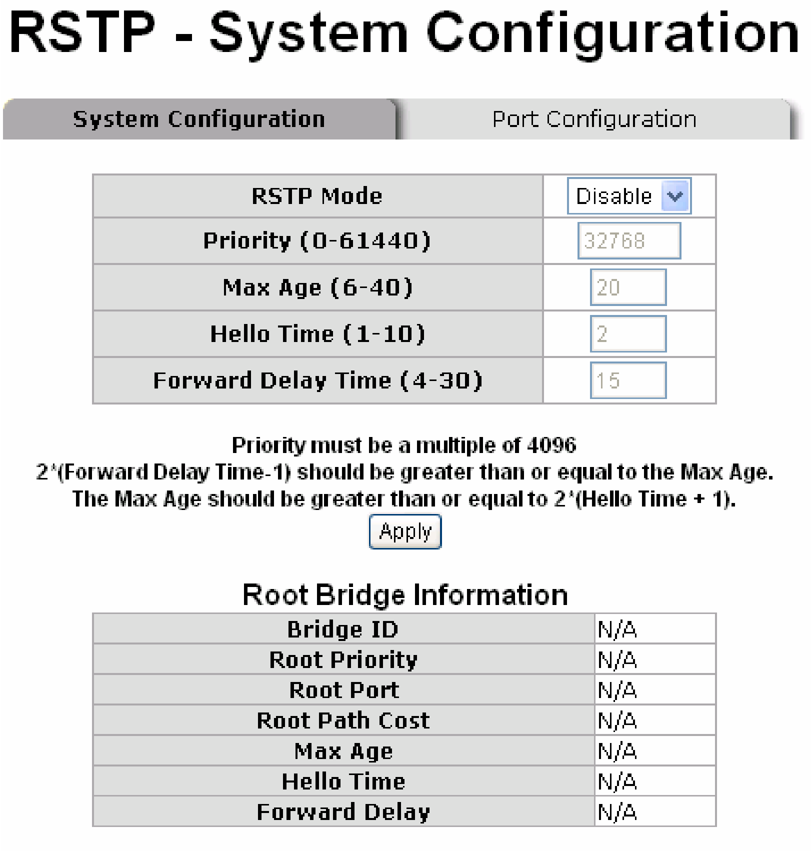
The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will auto detect the connected device that is running STP or RSTP protocol.

4.1.28.1 RSTP - System Configuration

- Users can view spanning tree information about the Root Bridge
- Users can modify RSTP state. After modification, click Apply button

- **RSTP mode:** users must enable or disable RSTP function before configure the related parameters
- **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 the value changes, user must reboot the switch. The value must be multiple of 4096 according to the protocol standard rule
- **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
- **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
- **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	Disable
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

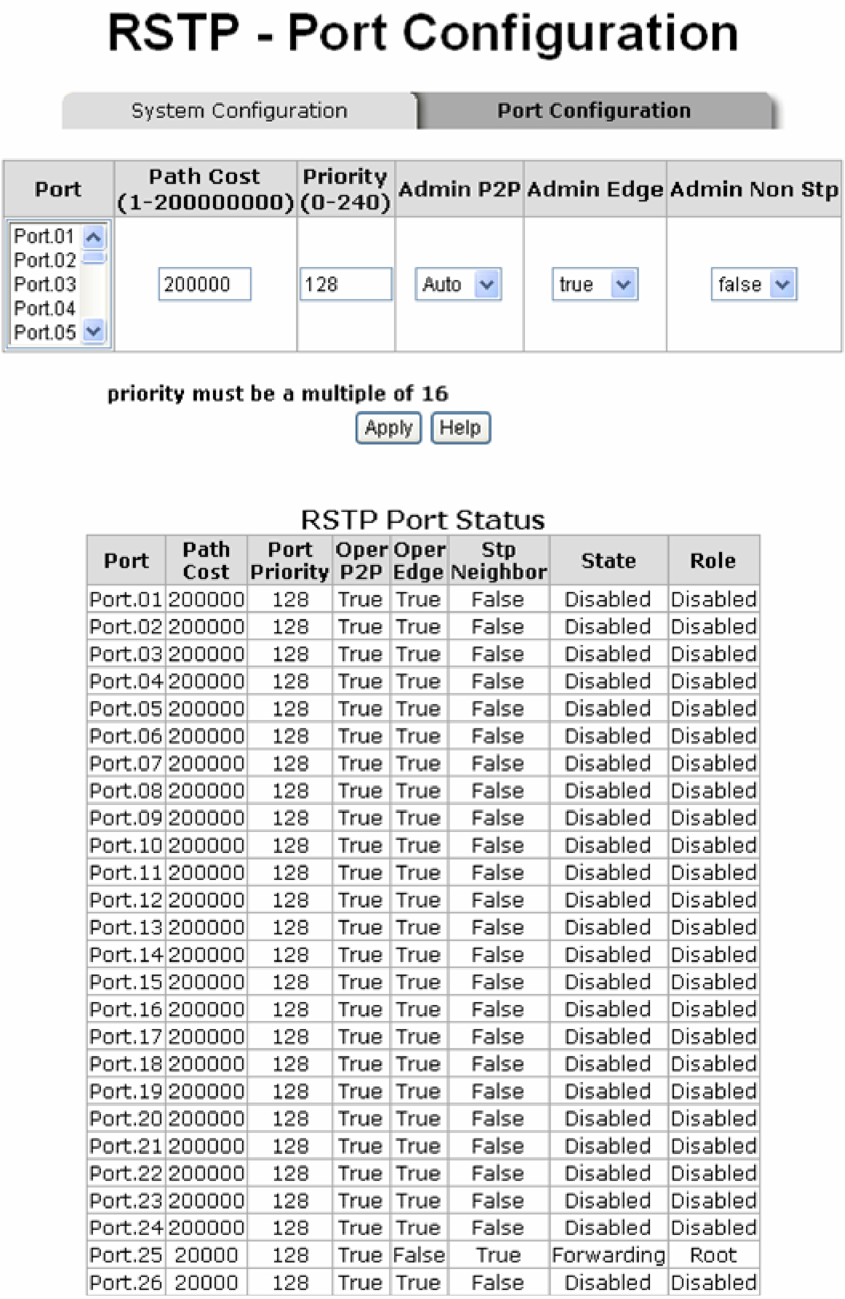
Bridge ID	N/A
Root Priority	N/A
Root Port	N/A
Root Path Cost	N/A
Max Age	N/A
Hello Time	N/A
Forward Delay	N/A

RSTP System Configuration interface

4.1.28.2 RSTP - Port Configuration

You can configure path cost and priority of every port.

1. Select the port in Port column.
1. **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.
2. **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.
3. **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.



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	200000	128	True	True	False	Disabled	Disabled
Port.02	200000	128	True	True	False	Disabled	Disabled
Port.03	200000	128	True	True	False	Disabled	Disabled
Port.04	200000	128	True	True	False	Disabled	Disabled
Port.05	200000	128	True	True	False	Disabled	Disabled
Port.06	200000	128	True	True	False	Disabled	Disabled
Port.07	200000	128	True	True	False	Disabled	Disabled
Port.08	200000	128	True	True	False	Disabled	Disabled
Port.09	200000	128	True	True	False	Disabled	Disabled
Port.10	200000	128	True	True	False	Disabled	Disabled
Port.11	200000	128	True	True	False	Disabled	Disabled
Port.12	200000	128	True	True	False	Disabled	Disabled
Port.13	200000	128	True	True	False	Disabled	Disabled
Port.14	200000	128	True	True	False	Disabled	Disabled
Port.15	200000	128	True	True	False	Disabled	Disabled
Port.16	200000	128	True	True	False	Disabled	Disabled
Port.17	200000	128	True	True	False	Disabled	Disabled
Port.18	200000	128	True	True	False	Disabled	Disabled
Port.19	200000	128	True	True	False	Disabled	Disabled
Port.20	200000	128	True	True	False	Disabled	Disabled
Port.21	200000	128	True	True	False	Disabled	Disabled
Port.22	200000	128	True	True	False	Disabled	Disabled
Port.23	200000	128	True	True	False	Disabled	Disabled
Port.24	200000	128	True	True	False	Disabled	Disabled
Port.25	20000	128	True	False	True	Forwarding	Root
Port.26	20000	128	True	True	False	Disabled	Disabled

RSTP Port Configuration interface

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

4.1.29 SNMP Configuration

Simple Network Management Protocol (SNMP) is the protocol which is 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 problems by receiving traps or change notices from network devices implementing SNMP.

4.1.29.1 System Configuration

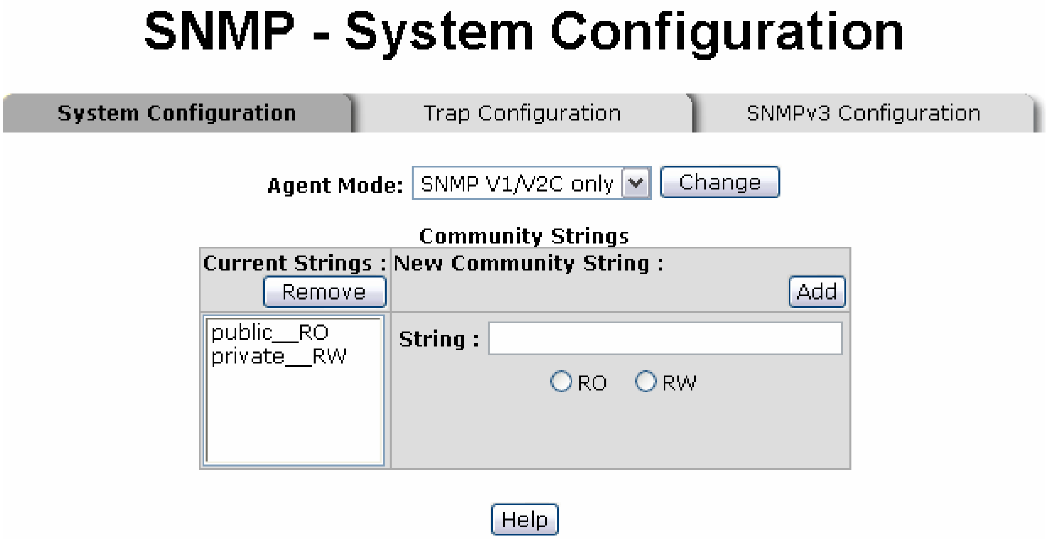
- **Community Strings**

You 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 you have defined and click Remove. You cannot remove the default community string set.

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



SNMP - System Configuration

System Configuration | Trap Configuration | SNMPv3 Configuration

Agent Mode: SNMP V1/V2C only Change

Community Strings

Current Strings : Remove
public__RO
private__RW

New Community String : Add
String :
○ RO ○ RW

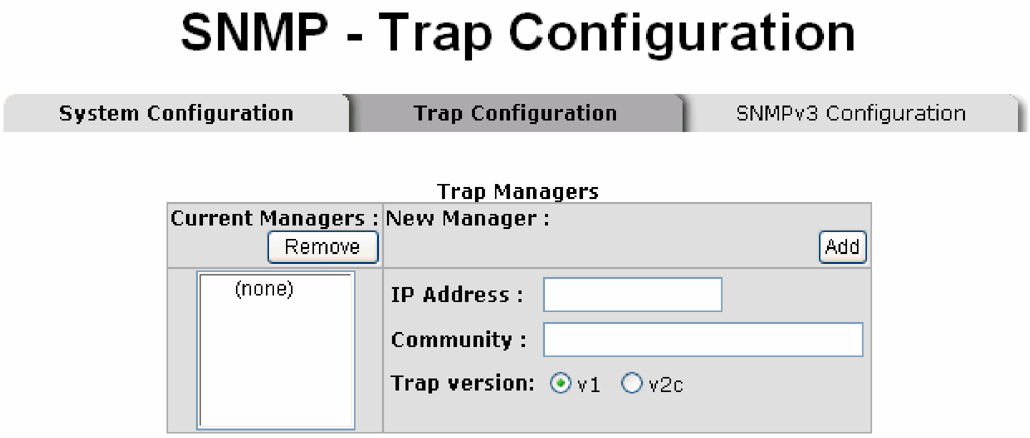
Help

SNMP System Configuration interface

4.1.29.2 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 issue. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager, users can 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 v2.
4. Click Add.
5. To remove the community string, select the community string that you have defined and click Remove. You cannot remove the default community string set.



SNMP - Trap Configuration

System Configuration | Trap Configuration | SNMPv3 Configuration

Trap Managers

Current Managers : Remove
(none)

New Manager : Add
IP Address :
Community :
Trap version: ● v1 ○ v2c

Trap Managers interface

4.1.29.3 SNMPV3 Configuration

Configure the SNMP V3 function including **Context Table**, **User Profile**, **Group Table**, **Access Table** and **MIBView Table**.

Context Table

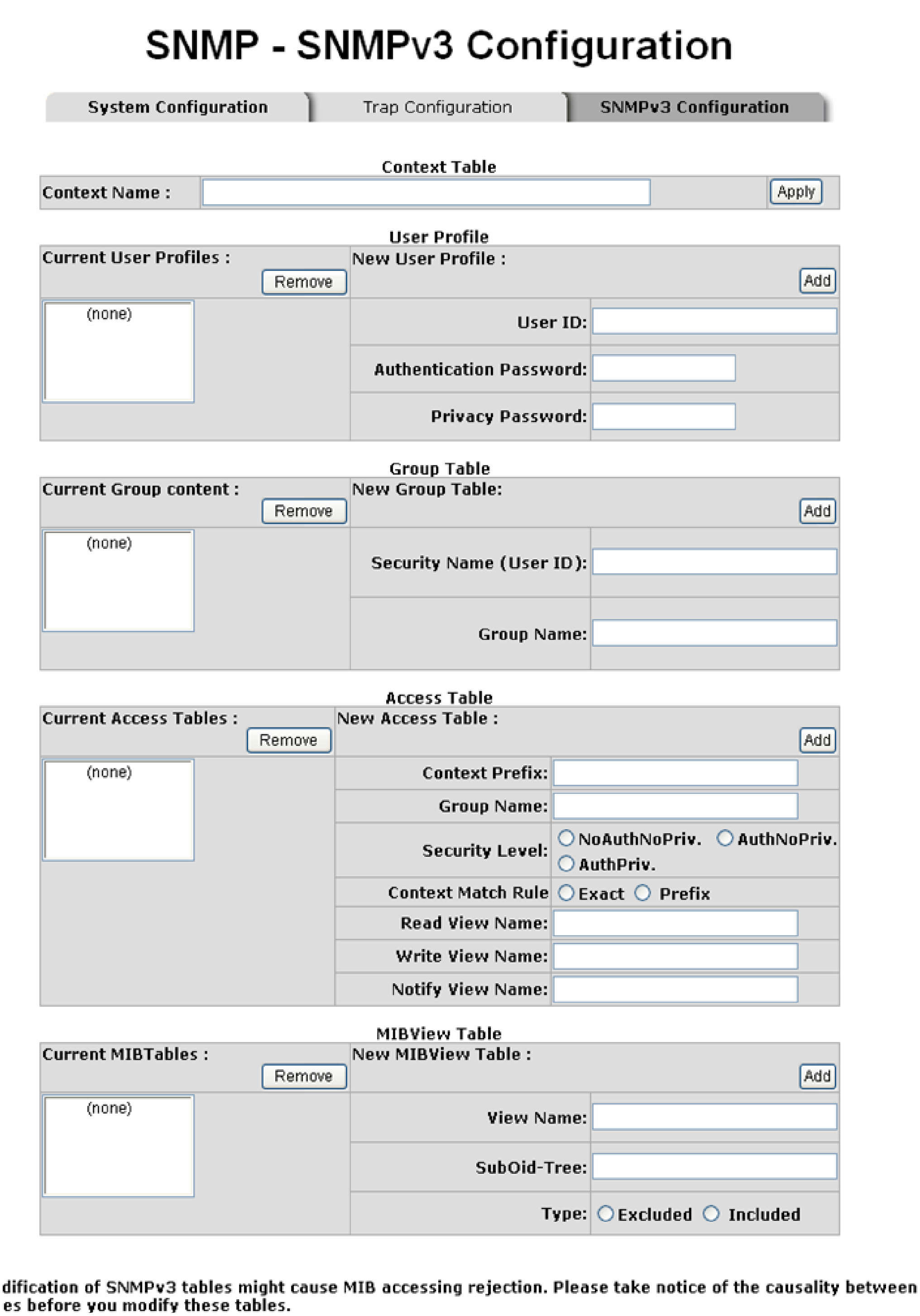
Configure SNMP v3 context table. Assign the context name of context table. Click Add to add context name.

Click Remove to remove unwanted context name.

User Profile

Configure SNMP v3 user table..

- **User ID:** set up the username.
- **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

Context Table

Context Name : Apply

User Profile

Current User Profiles : Remove
(none)

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

Group Table

Current Group content : Remove
(none)

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

Access Table

Current Access Tables : Remove
(none)

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

MIBView Table

Current MIBTables : Remove
(none)

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

dification of SNMPv3 tables might cause MIB accessing rejection. Please take notice of the causality between es before you modify these tables.

SNMP V3 configuration interface

Group Table

Configure SNMP v3 group table.

- **Security Name (User ID):** assign the username 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.
- **Context Match Rule:** select the context match rule.
- **Read View Name:** set up the read view.
- **Write View Name:** set up the write view.
- **Notify View Name:** set up the notify view.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

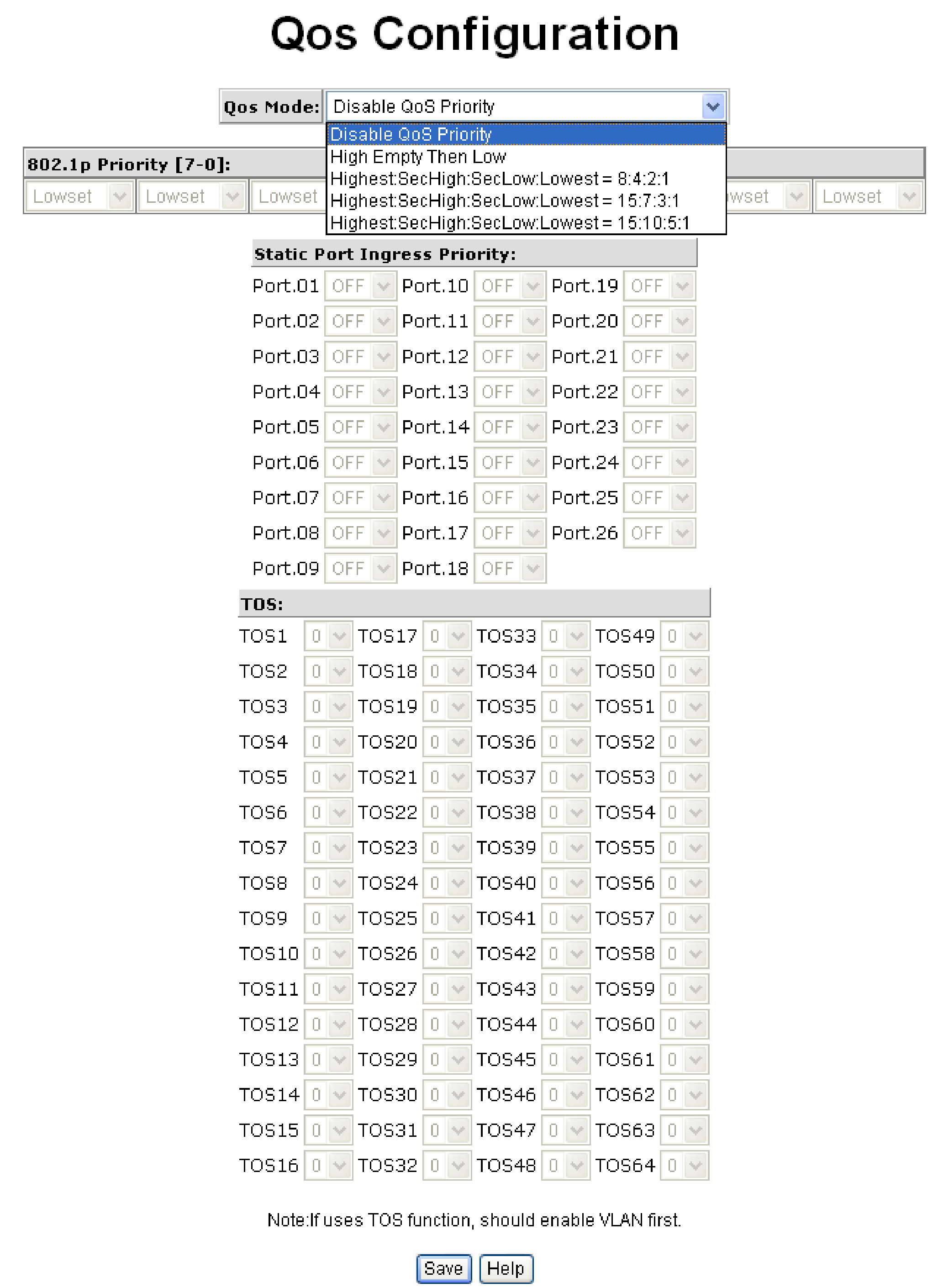
MIBview Table
Configure MIB view table.

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

4.1.30 QOS CONFIGURATION

You can configure **Qos mode**, **802.1p priority [7-0]** setting, **Static Port Ingress Priority** setting and **TOS** setting.

- **Select the Qos Mode:** Select the Qos policy rule
  - **Disable QoS Priority:** The default status of Qos Priority is disabled.
  - **High Empty Then Low:** When all the high priority packets are empty in queue, low priority packets will be processed then.
  - **Highest:SecHigh:SecLow:Lowest:8:4:2:1:** The switch will follow 8:4:2:1 rate to process priority queue from Highest to lowest queue. For example: the system will process 80% highest queue traffic, 40% SecHigh queue traffic, 20% SecLow queue traffic, and 10% Lowest queue traffic at the same time. Besides, the traffic in the Lowest Priority queue are not transmitted until all Highest, SecHigh, and SecLow traffic are serviced.
  - **Highest:SecHigh:SecLow:Lowest:15:7:3:1:** The process order is in compliance with the transfer rate of 15:7:3:1.
  - **Highest:SecHigh:SecLow:Lowest:15:10:5:1:** The process order is in compliance with the transfer rate of 15:10:5:1.
- **802.1p priority [7-0]:** Configure per priority level.
  - **Priority 0 ~ 7:** each priority has 4 priority levels – Highest, SecHigh, SecLow, and Lowest.
- **Static Port Ingress Priority:** The port ingress level is from 0 to 7.
- **TOS:** the system provides 1~64 TOS priority level. Each level has 8 priorities – 0~7.(Mapping to 802.1p configuration) The default value is "0" 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: when users set the TOS level 25 to 0, it will map to 802.1p configuration. If "0" is the highest priority, TOS level 25 will have the highest priority.
- Click Apply.



Qos Configuration

Qos Mode: Disable QoS Priority

Disable QoS Priority
High Empty Then Low
Highest:SecHigh:SecLow:Lowest = 8:4:2:1
Highest:SecHigh:SecLow:Lowest = 15:7:3:1
Highest:SecHigh:SecLow:Lowest = 15:10:5:1

802.1p Priority [7-0]: Lowset Lowset Lowset wset Lowset

Static Port Ingress Priority:

Port.01	OFF	Port.10	OFF	Port.19	OFF
Port.02	OFF	Port.11	OFF	Port.20	OFF
Port.03	OFF	Port.12	OFF	Port.21	OFF
Port.04	OFF	Port.13	OFF	Port.22	OFF
Port.05	OFF	Port.14	OFF	Port.23	OFF
Port.06	OFF	Port.15	OFF	Port.24	OFF
Port.07	OFF	Port.16	OFF	Port.25	OFF
Port.08	OFF	Port.17	OFF	Port.26	OFF
Port.09	OFF	Port.18	OFF		

TOS:

TOS1	0	TOS17	0	TOS33	0	TOS49	0
TOS2	0	TOS18	0	TOS34	0	TOS50	0
TOS3	0	TOS19	0	TOS35	0	TOS51	0
TOS4	0	TOS20	0	TOS36	0	TOS52	0
TOS5	0	TOS21	0	TOS37	0	TOS53	0
TOS6	0	TOS22	0	TOS38	0	TOS54	0
TOS7	0	TOS23	0	TOS39	0	TOS55	0
TOS8	0	TOS24	0	TOS40	0	TOS56	0
TOS9	0	TOS25	0	TOS41	0	TOS57	0
TOS10	0	TOS26	0	TOS42	0	TOS58	0
TOS11	0	TOS27	0	TOS43	0	TOS59	0
TOS12	0	TOS28	0	TOS44	0	TOS60	0
TOS13	0	TOS29	0	TOS45	0	TOS61	0
TOS14	0	TOS30	0	TOS46	0	TOS62	0
TOS15	0	TOS31	0	TOS47	0	TOS63	0
TOS16	0	TOS32	0	TOS48	0	TOS64	0

Note:If uses TOS function, should enable VLAN first.

QoS Configuration interface

4.1.31 IGMP Configuration

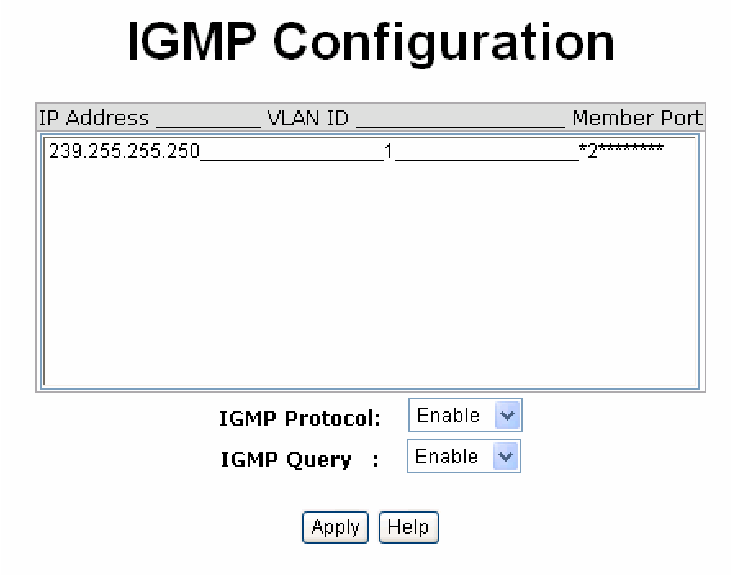
The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through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

Message	Description
Query	A message sent from the querist (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 querist 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 querist to indicate that the host has quit being a member of a specific multicast group.

The switch support IP multicast, you can enable IGMP protocol on web management's switch setting advanced page, then display the IGMP snooping information. 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	*2********

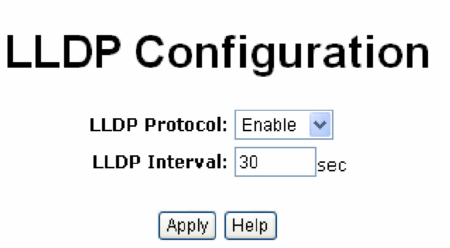
IGMP Protocol: Enable
IGMP Query : Enable

IGMP Configuration interface

- **LLDP**

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

- **LLDP Protocol:** Disable or enable LLDP function.
- **LLDP Interval:** Set the interval of learning the information time in second.
- Click Apply.


LLDP Configuration

LLDP Protocol: Enable
LLDP Interval: 30 sec

LLDP Configuration interface

4.1.32 SECURITY

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

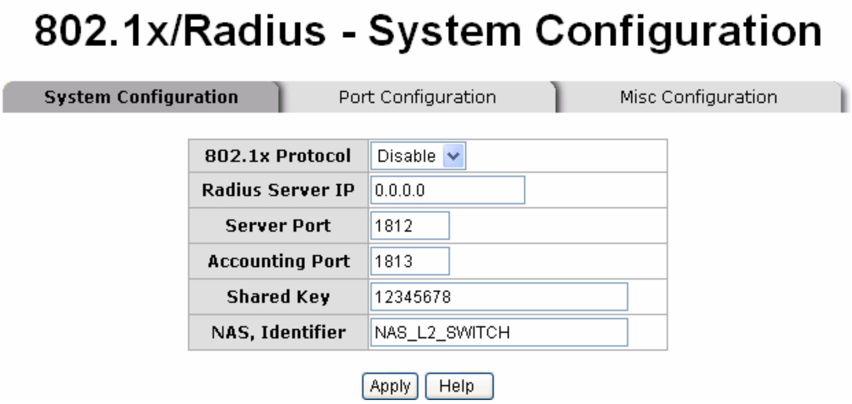
4.1.32.1 802.1X/Radius Configuration

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 username and password that are verified by a separate server.

System Configuration

After enabling the IEEE 802.1X function, you 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 which used on the Radius Server.
6. **NAS, Identifier:** set the identifier for the radius client.
7. Click Apply .



802.1x/Radius - System Configuration

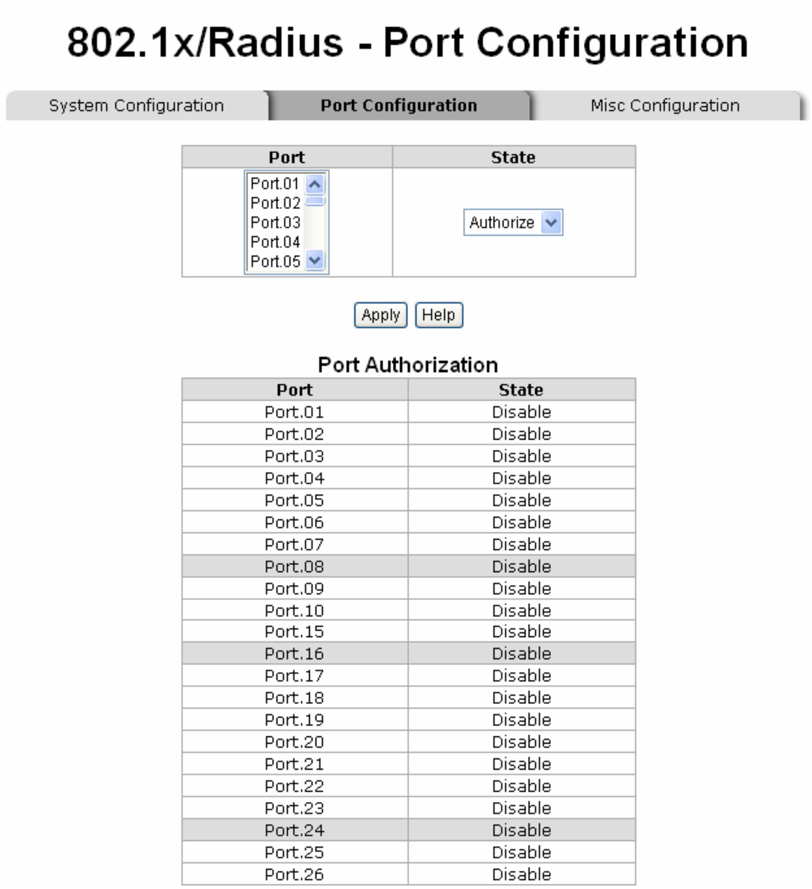
802.1x Protocol	Disable
Radius Server IP	0.0.0.0
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

802.1x System Configuration interface

802.1x Per Port Configuration

You 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

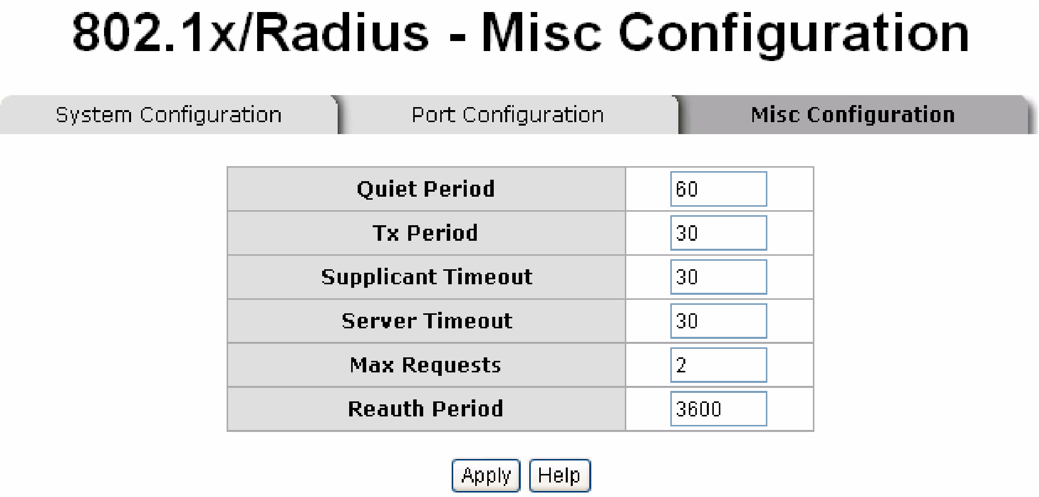
Port	State
Port.01	Disable
Port.02	Disable
Port.03	Disable
Port.04	Disable
Port.05	Disable
Port.06	Disable
Port.07	Disable
Port.08	Disable
Port.09	Disable
Port.10	Disable
Port.15	Disable
Port.16	Disable
Port.17	Disable
Port.18	Disable
Port.19	Disable
Port.20	Disable
Port.21	Disable
Port.22	Disable
Port.23	Disable
Port.24	Disable
Port.25	Disable
Port.26	Disable

802.1x Per Port Setting interface

Misc Configuration

1. **Quiet Period:** set the period of time which the port does not 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 times out before authentication fails and the authentication session ends.
6. **Reauth period:** set the period of time after the connection of clients be re-authenticated.
7. Click Apply.


802.1x/Radius - Misc Configuration

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

802.1x Misc Configuration interface

4.1.32.2 MAC Address Table

Use the MAC address table to ensure the port security.

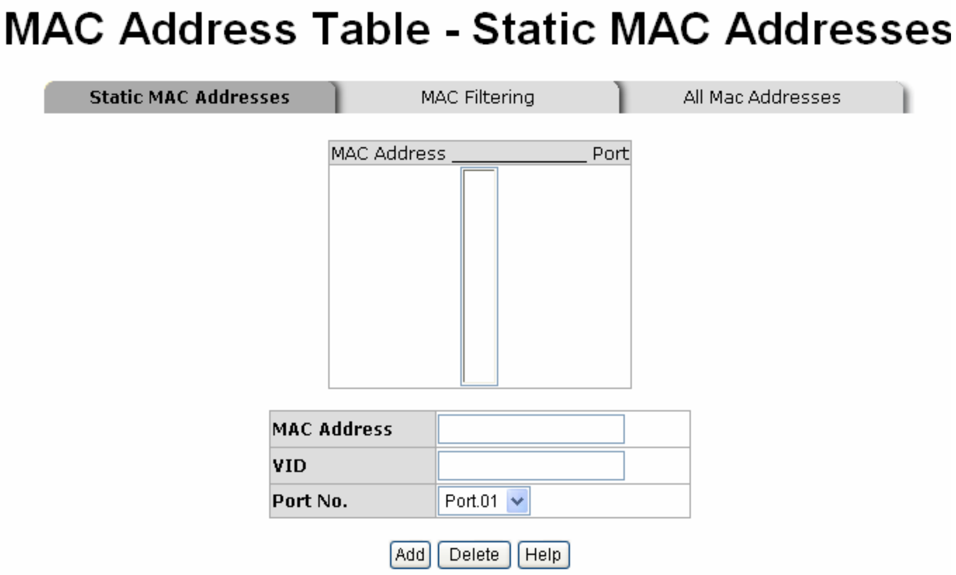
Static MAC Address

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

- **Add the Static MAC Address**

You can add static MAC address in 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. **VID:** Type in VID of the MAC address.
3. **Port No.:** pull down the selection menu to select the port number.
4. Click Add.
5. If you want to delete the MAC address from filtering table, select the MAC address and click Delete.

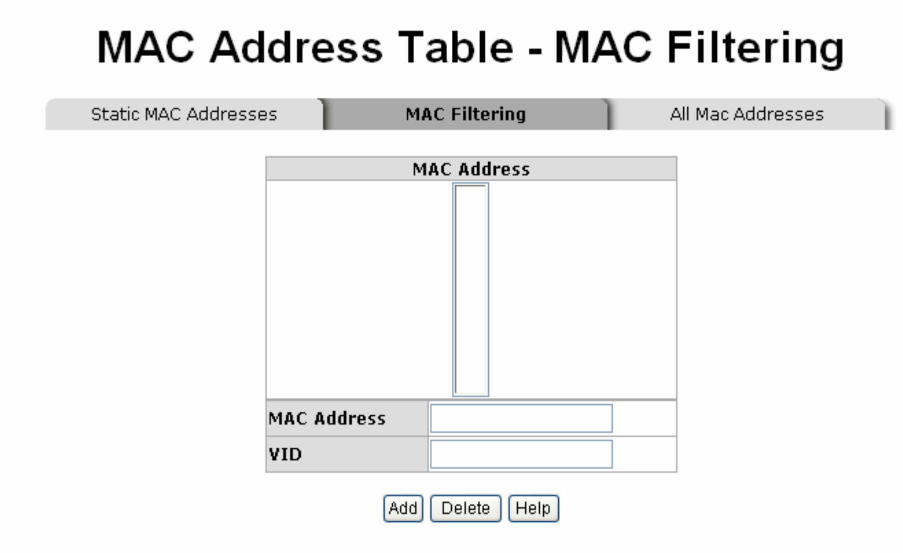

MAC Address Table - Static MAC Addresses

MAC Address	
VID	
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. You can add and delete filtering MAC address.



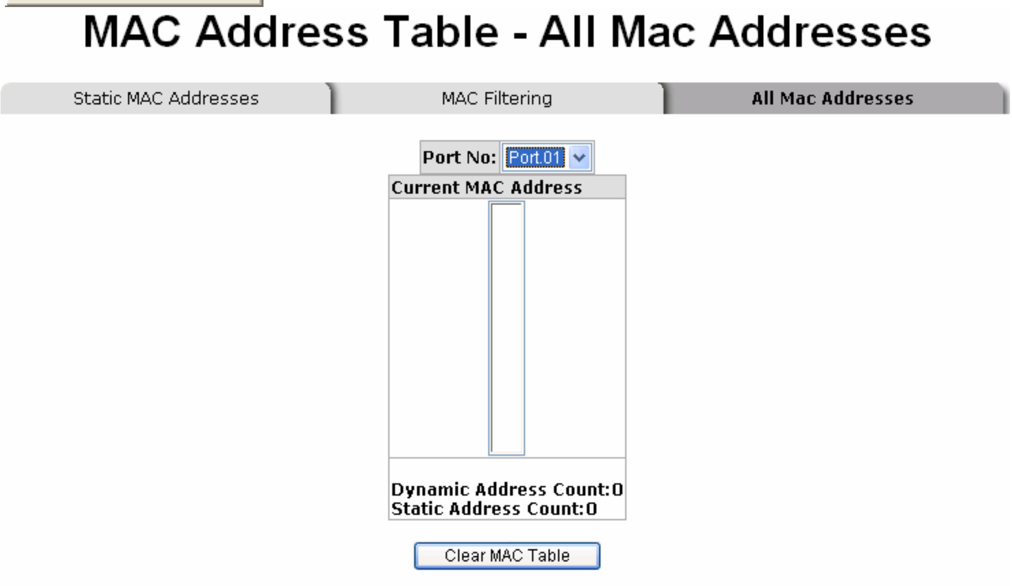
MAC Filtering interface

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

All MAC Addresses

You can view the port 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.

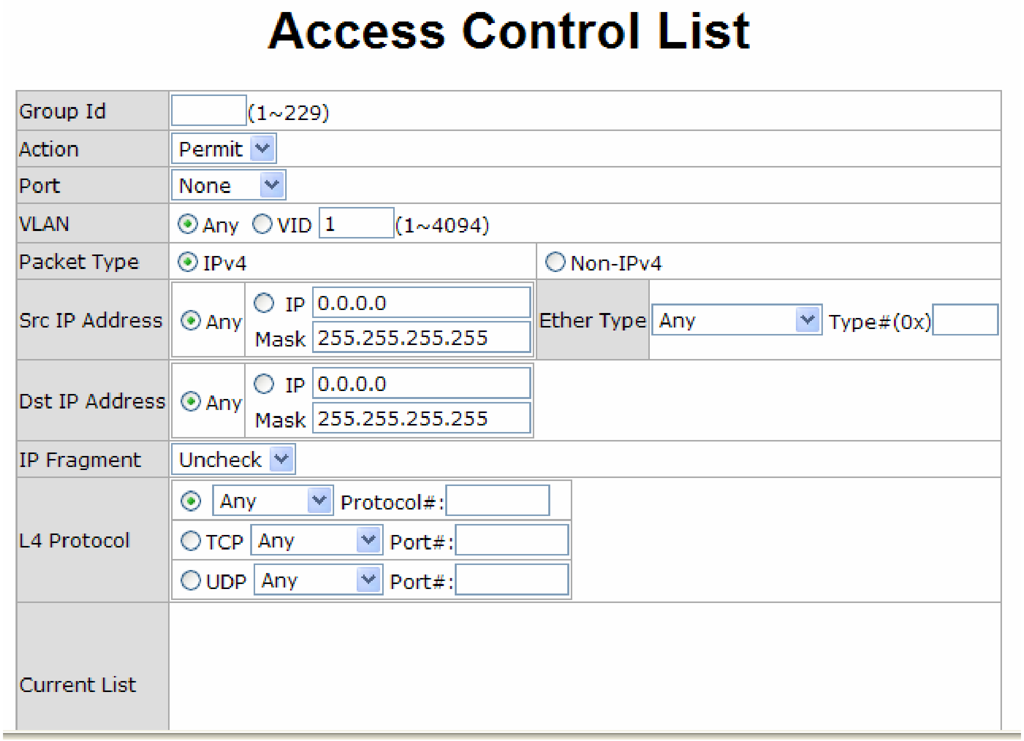


All MAC Address interface

4.1.32.3 Access Control List

- **Group Id:** Type in the Group ID from 1 to 229. (Maximum 255,26 rules for DHCP filter)
- **Action:** Permit and Deny.
- **Port:** Select specific port to apply the ACL,
- **VLAN:** Select any or a particular VID.
- **Packet type:** Select packet type – IPv4 or Non-IPv4
- **Src IP Address:** Select any or assign an IP address with Subnet Mask for source IP address.
- **Dst IP Address:** Select any or assign an IP address with Subnet Mask for destination IP address.
- **Ether Type:** Pull down the select menu for Any, ARP or IPX.
- **IP Fragment:** Set this item as to whether the fragment is checked or not.
- **L4 Protocol:** Assign the L4 protocol from among ICMP(1), IGMP(2), TCP or UDP.

- **Current List:** Display the current list information.



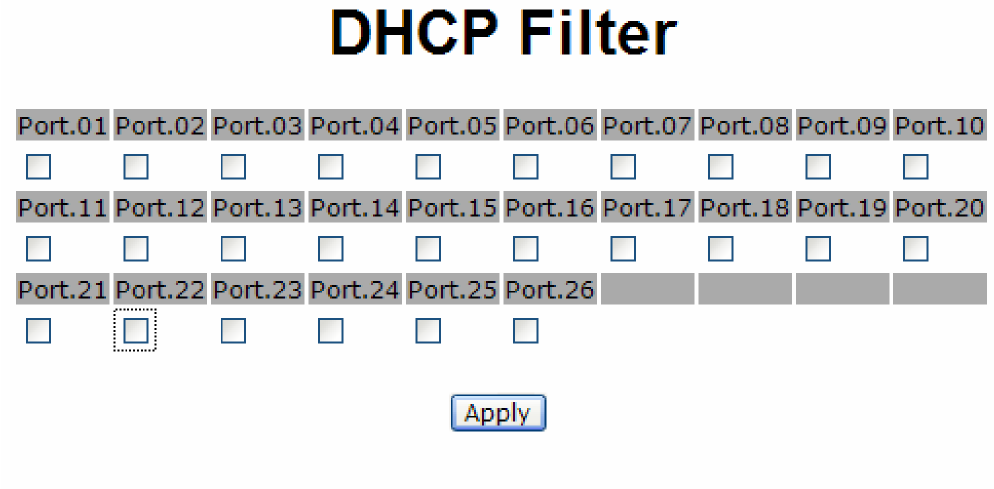
Access Control List

Group Id	(1~229)		
Action	Permit		
Port	None		
VLAN	● Any ○ VID 1 (1~4094)		
Packet Type	● IPv4	○ Non-IPv4	
Src IP Address	● Any ○ IP 0.0.0.0 Mask 255.255.255.255	Ether Type	Any Type#(0x)
Dst IP Address	● Any ○ IP 0.0.0.0 Mask 255.255.255.255		
IP Fragment	Uncheck		
L4 Protocol	● Any Protocol#: ○ TCP Any Port#: ○ UDP Any Port#:		
Current List			

Access Control List interface

4.1.32.4 DHCP Filter

By the function, DHCP discover and DHCP request packets will NOT be forwarded to the port that you selected.



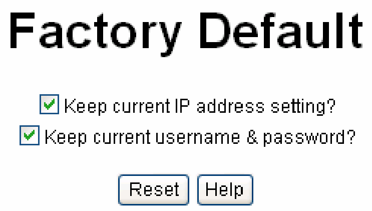
DHCP Filter

Port.01	Port.02	Port.03	Port.04	Port.05	Port.06	Port.07	Port.08	Port.09	Port.10
□	□	□	□	□	□	□	□	□	□
Port.11	Port.12	Port.13	Port.14	Port.15	Port.16	Port.17	Port.18	Port.19	Port.20
□	□	□	□	□	□	□	□	□	□
Port.21	Port.22	Port.23	Port.24	Port.25	Port.26				
□	□	□	□	□	□				

DHCP filter interface

4.1.33 FACTORY DEFAULT

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



Factory Default

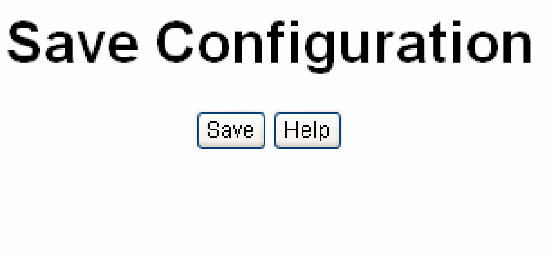
☑ Keep current IP address setting?

☑ Keep current username & password?

Factory Default interface

4.1.34 SAVE CONFIGURATION

Save all configurations that you have made in the system. Ensure all of the configuration is saved. Click Save to save the all configuration to the flash memory.

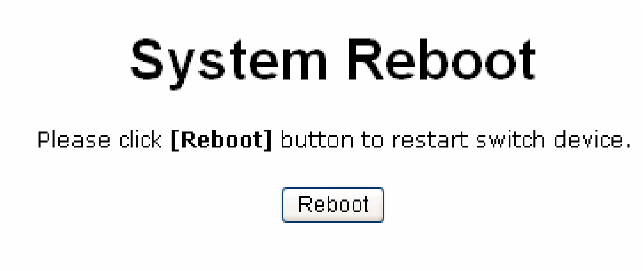


Save Configuration

Save Configuration interface

4.1.35 System Reboot

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



System Reboot

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

System Reboot interface

5. Command Line Interface Management

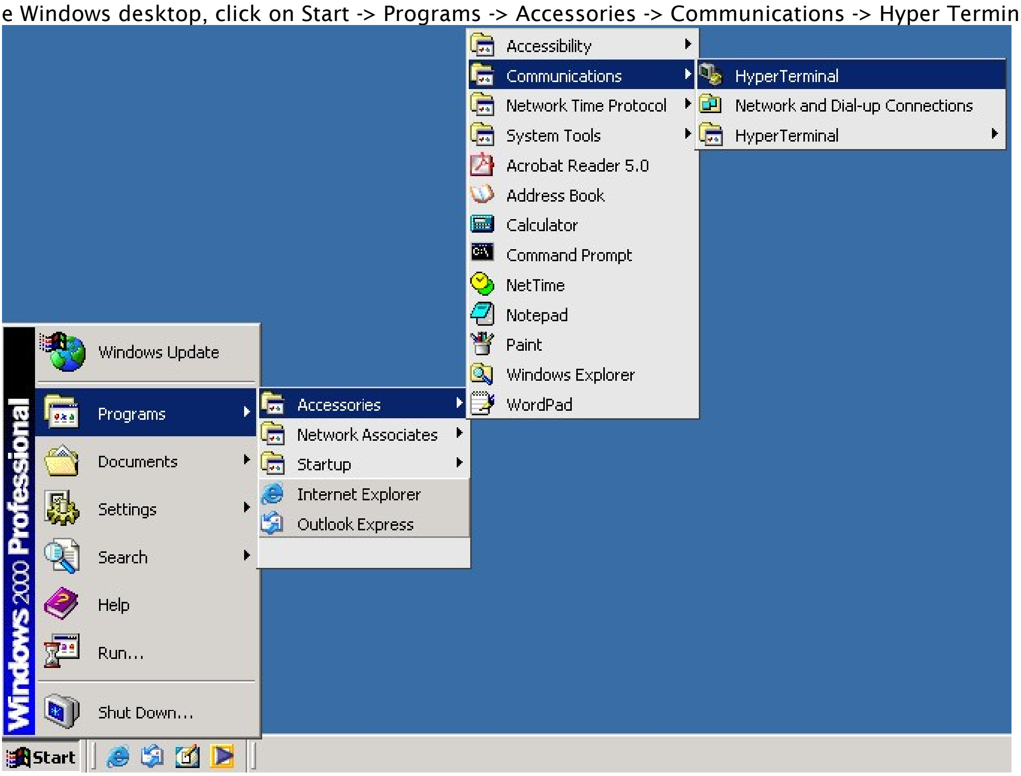
Configuration by Command Line Interface (CLI)

5.1 About CLI Management

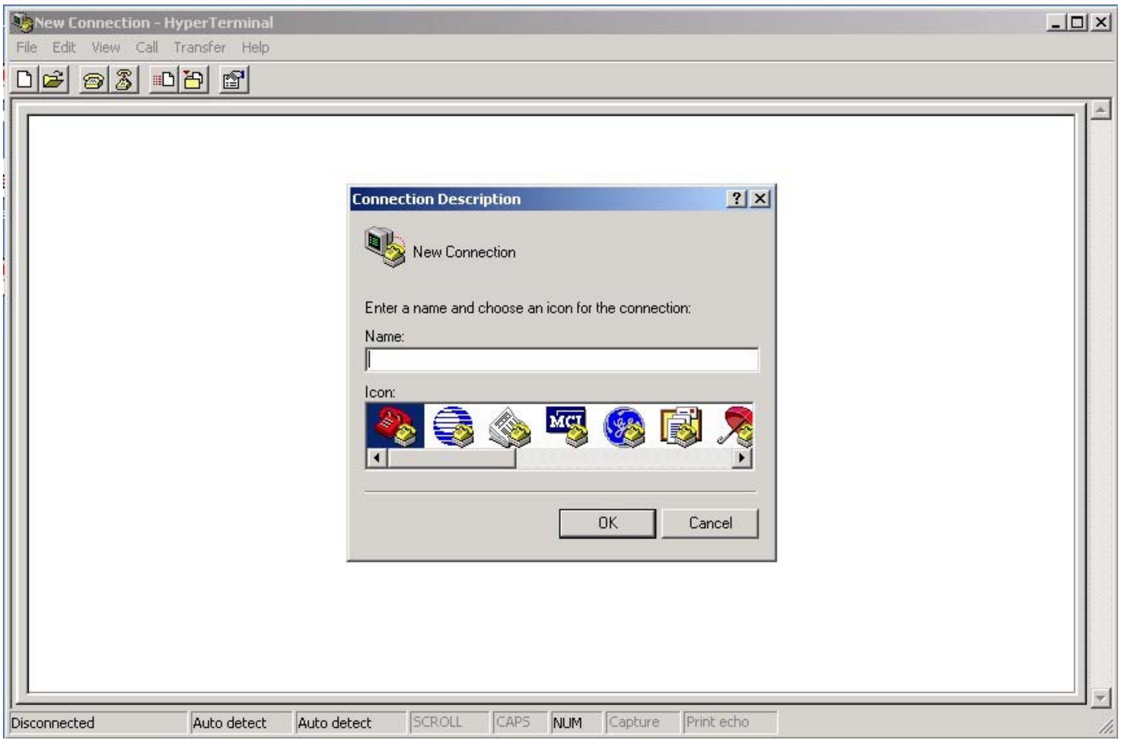
ESW-5242GP / ESW-5162GP also supports CLI management. You can use console or telnet to management switch by CLI.

CLI Management by RS-232 Serial Console (9600, 8, none, 1, none)
Before Configuring by RS-232 serial console, use an RJ45 to DB9-F cable to connect the Switches' RS-232 Console port to your PC's COM port.

Follow the steps below to access the console via RS-232 serial cable.
(1) From the Windows desktop, click on Start -> Programs -> Accessories -> Communications -> Hyper Terminal



(2)Input a name for new connection



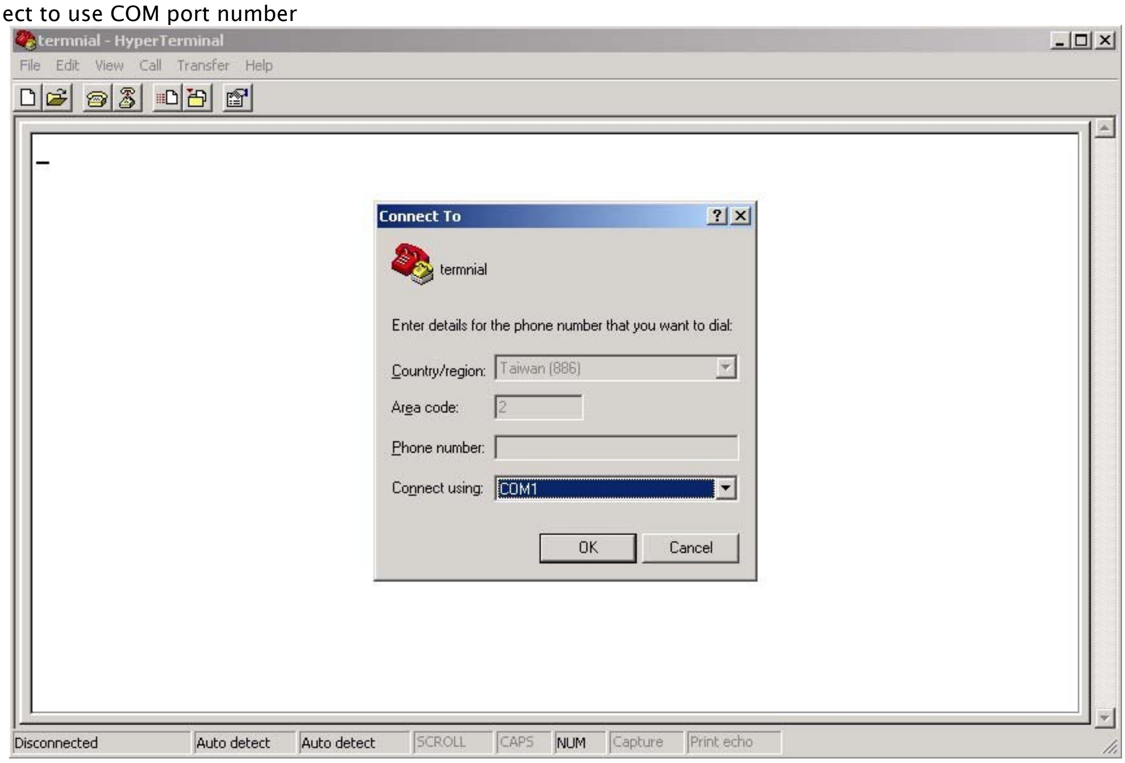
New Connection

Enter a name and choose an icon for the connection:

Name:

Icon:

(3)Select to use COM port number



termnial

Enter details for the phone number that you want to dial:

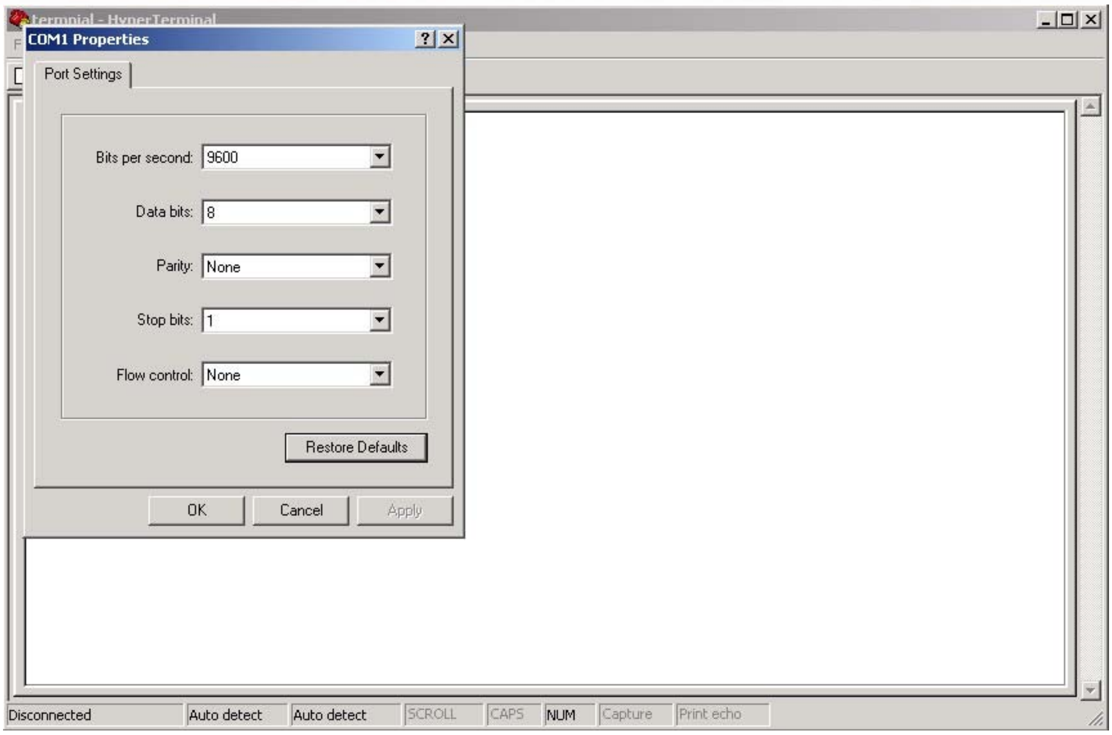
Country/region: Taiwan (886)

Area code: 2

Phone number:

Connect using: COM1

(4) The COM port properties setting, 9600 for Bits per second, 8 for Data bits, None for Parity, 1 for Stop bits and none for Flow control.



terminal - HyperTerminal

COM1 Properties

Port Settings

Bits per second: 9600

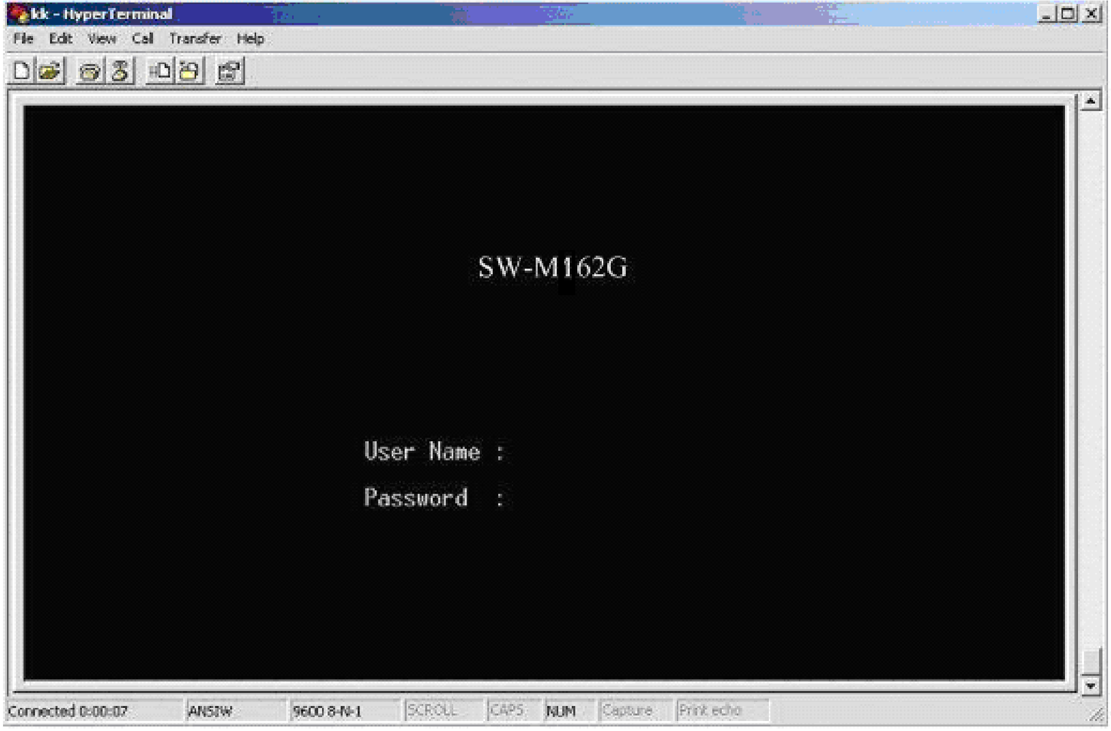
Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

(5) The Console login screen will appear. Use the keyboard enter the Console Username and Password that is same as the Web Browser password), and then press “**Enter**”.



kk - HyperTerminal

```
SW-M162G

User Name :
Password  :
```

5.2 Commands Level

Modes	Access Method	Prompt	Exit Method	About This Model
User EXEC	Begin a session with your switch.	switch>	Enter **logout** or **quit**.	The user’s commands available at the user’s level are a subset of those available of the privileged level. Use this mode to • Enter menu mode. • Display system information.
Privileged EXEC	Enter the **enable** command while in user EXEC mode.	switch#	Enter **diable** 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.

5.3 COMMANDS SET LIST

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

5.3.1 SYSTEM COMMANDS SET

Commands	Level	Description	Example
show config	**E**	Show switch configuration.	switch>show config
show terminal	**P**	Show console information.	switch#show terminal
menu	**E**	Enter MENU mode.	switch>menu
write memory	**G**	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.	switch#show ip
no ip dhcp	**G**	Disable DHCP client function of switch.	switch(config)#no ip dhcp
reload	**G**	Halt and perform a cold restart .	switch(config)#reload
Default	**G**	Restore to default.	Switch(config)#default
admin username [Username]	**G**	Changes a login username. (maximum 10 words).	switch(config)#admin username xxxxxx
admin password [Password]	**G**	Specifies a password (maximum 10 words).	switch(config)#admin password xxxxxx
show admin	**P**	Show administrator information.	switch#show admin
dhcpserver enable	**G**	Enable DHCP Server.	switch(config)#dhcpserver enable
dhcpserver lowip [Low IP]	**G**	Configure low IP address for IP pool.	switch(config)# dhcpserver lowip 192.168.1.1
dhcpserver highip [High IP]	**G**	Configure high IP address for IP pool.	switch(config)# dhcpserver highip 192.168.1.50
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-if)#dhcpserver ipbinding 192.168.1.1
Show dhcpserver configuration	P	Show configuration of DHCP server.	switch#show dhcpserver configuration
show dhcpserver clients	P	Show client entries of DHCP server.	switch#show dhcpserver clinets
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

5.3.2 PORT COMMANDS SET

Commands		Description	Example
interface fastEthernet [Portid]	G	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex [full | half]	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
speed [10|100|1000|auto]	I	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can’t be set to 1000 if the port isn’t a giga port.	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
flowcontrol mode [Symmetric|Asymmetric]	I	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion.	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol mode Asymmetric
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 in [Value]	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports,	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth in 100

		and zero means no limit.	
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 switch(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 switch(config-if)#show interface status
show interface accounting	I	show interface statistic counter.	switch(config)#interface fastEthernet 2 switch(config-if)#show interface accounting
no accounting	I	Clear interface accounting information.	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting

5.3.3 TRUNK COMMANDS SET

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

5.3.4 VLAN COMMANDS SET

Commands	Level	Description	Example
vlan database	P	Enter VLAN configure mode.	switch#vlan database

Vlanmode [portbase| 802.1q | gvrp]	V	To set switch VLAN mode.	switch(vlan)# vlanmode portbase or switch(vlan)# vlanmode 802.1q or switch(vlan)# vlanmode gvrp
no vlan	V	Disable VLAN.	
Ported based VLAN configuration			
vlan port-based grpname [Group Name] **grpid** [GroupID] **port** [PortNumbers]	V	Add new port based VALN.	switch(vlan)# vlan port-based grpname test grpid 2 port 2-4
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 test vid 22
vlan 8021q port [PortNumber] **access-link untag** [UntaggedVID]	V	Assign an 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 an 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

5.3.5 SPANNING TREE COMMANDS SET

Commands	Level	Description	Example
spanning-tree enable	G	Enable spanning tree.	switch(config)#spanning-tree enable
spanning-tree priority [0~61440]	G	Configure spanning tree priority parameter.	switch(config)#spanning-tree priority 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 the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)# spanning-tree max-age 15

spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
spanning-tree forward-time [seconds]	G	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the 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 Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20
stp-path-priority [Port Priority]	I	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-path-priority 127
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	Display a summary of the spanning-tree states.	switch>show spanning-tree
no spanning-tree	G	Disable spanning-tree.	switch(config)#no spanning-tree

5.3.6 QOS COMMANDS SET

Commands	Level	Description	Example
qos mode [SP|WRR|WRR1|WRR2] SP : High-Empty-Then-Low WRR : WRR_8_4_2_1 WRR1: WRR_15_7_3_1 WRR2: WRR_15_10_5_1	G	Set Qos mode.	switch(config)#qos mode sp switch(config)#qos mode wrr switch(config)#qos mode wrr1 switch(config)#qos mode wrr2
no qos	G	Disable QoS.	switch(config)#no qos
qos 8021p-priority [Index][LowSet|SecLow|SecHigh|Highest]	G	Configure 802.1p Priority.	switch(config)#qos 8021p-priority 1 LowSet
qos priority-static-port-ingress [Priority]	I	Configure Static Port Ingress Priority.	switch(config)#interface fastEthernet 2 switch(config-if)#qos priority-static-port-ingress 7
no qos	I	Disable Static Port Ingress Priority.	switch(config)#interface fastEthernet 3 switch(config-if)#no qos
qos priority tos [Index][Priority]	G	Configure TOS Priority.	switch(config)#qos priority tos 1 3
show qos	P	Display the information of QoS configuration.	switch#show qos

5.3.7 IGMP COMMANDS SET

Commands	Level	Description	Example
igmp enable	G	Enable IGMP snooping function.	switch(config)#igmp enable

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

5.3.8 MAC / Filter Table Commands Set

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

5.3.9 SNMP Commands Set

Commands	Level	Description	Example
snmp system-name [System Name]	G	Set SNMP agent system name.	switch(config)#snmp system-name l2switch
snmp system-location [System Location]	G	Set SNMP agent system location.	switch(config)#snmp system-location lab
snmp system-contact [System Contact]	G	Set SNMP agent system contact.	switch(config)#snmp system-contact where
snmp agent-mode [v1v2c|v3|v1v2cv3]	G	Select the agent mode of SNMP.	switch(config)#snmp agent-mode v1v2cv3
snmp community-strings [Community] **right** [RO/RW]	G	Add SNMP community string.	switch(config)#snmp community-strings public right rw
snmp-server host [IP address] **community** [Community-string] **trap-version** [v1|v2c]	G	Configure SNMP server host information and community string.	switch(config)#snmp-server host 192.168.1.50 community public trap-version v1 (remove) Switch(config)# no snmp-server host 192.168.1.50
snmpv3 context-name [Context Name]	G	Configure the context name.	switch(config)#snmpv3 context-name Test
snmpv3 user [User Name] **group** [Group Name] **password** [Authentication Password] [Privacy Password]	G	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#snmpv3 user test01 group G1 password AuthPW PrivPW
snmpv3 access context-name [Context Name]	G	Configure the access table of SNMPV3 agent.	switch(config)#snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1

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

5.3.10 Port Mirroring Commands Set

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

5.3.11 802.1x Commands Set

Commands	Level	Description	Example
8021x enable	G	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiousip [IP address]	G	Use the 802.1x system radious IP global configuration command to change the radious server IP.	switch(config)# 8021x system radiousip 192.168.1.1
8021x system	G	Use the 802.1x system server port	switch(config)# 8021x system serverport 1815

serverport [port ID]		global configuration command to change the radious server port.	
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 supptimeout [sec.]	G	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# 8021x misc supptimeout 20
8021x misc servertimeout [sec.]	G	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#8021x misc servertimeout 20
8021x misc maxrequest [number]	G	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# 8021x misc maxrequest 3
8021x misc reauthperiod [sec.]	G	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# 8021x misc reauthperiod 3000
8021x portstate [disable | reject | accept | authorize]	I	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch(config)#interface fastethernet 3 switch(config-if)#8021x portstate accept
show 8021x	E	Display a summary of the 802.1x properties and also the port sates.	switch>show 8021x
no 8021x	G	Disable 802.1x function.	switch(config)#no 8021x

5.3.12 TFTP Commands Set

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

5.3.13 SystemLog, SMTP and Event Commands Set

Commands	Level	Description	Example
systemlog ip [IP address]	G	Set System log server IP address.	switch(config)# systemlog ip 192.168.1.100
systemlog mode [client|server|both]	G	Specified the log mode.	switch(config)# systemlog mode both
show systemlog	E	Display system log.	Switch>show systemlog

show systemlog	P	Show system log client & server information.	switch#show systemlog
no systemlog	G	Disable systemlog function.	switch(config)#no systemlog
smtp enable	G	Enable SMTP function.	switch(config)#smtp enable
smtp serverip [IP address]	G	Configure SMTP server IP.	switch(config)#smtp serverip 192.168.1.5
smtp subject [subject]	G	Configure subject of mail.	switch(config)#smtp subject SMTPTest
smtp sender [sendername]	G	Configure sender of mail.	switch(config)#smtp sender SenderTest
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-warm-start [Systemlog|SMTP|Both]	G	Set cold start event type.	switch(config)#event device-warm-start both
event authentication-failure [Systemlog|SMTP|Both]	G	Set Authentication failure event type.	switch(config)#event authentication-failure 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-warm-start	G	Disable cold start event type.	switch(config)#no event device-warm-start
no event authentication-failure	G	Disable Authentication failure event type.	switch(config)#no event authentication-failure
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

5.3.14 SNTP Commands Set

Commands	Level	Description	Example
sntp enable	G	Enable SNTP function.	switch(config)#sntp enable
sntp daylight	G	Enable daylight saving time, if SNTP function is inactive, this command cannot be applied.	switch(config)#sntp daylight
sntp daylight-period [Start time] [End time]	G	Set period of daylight saving time, if SNTP function is inactive, this command cannot be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# sntp daylight-period 20060101-01:01 20060202-01-01
sntp daylight-offset [Minute]	G	Set offset of daylight saving time, if SNTP function is inactive, this command cannot be applied.	switch(config)#sntp daylight-offset 3
sntp ip [IP]	G	Set SNTP server IP, if SNTP function is inactive, this command cannot 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

5.3.15 Access Control List Commands Set

Commands	Level	Description	Example
show acl	P	Show the information of access control list table.	switch#show acl
acl gid [Group Id]	G	Configure access control list group id.	switch(config)# acl gid 1
acl action [Permit|Deny]	G	Set access control list action.	switch(config)#acl action Permit or switch(config)#acl action Deny
acl port [None|Port#]	G	Apply ACL on specific port	switch(config)#acl port 2
acl vid [Any|VLAN Id]	G	Set access control list Vlan-ID	switch(config)#acl vid 2 or switch(config)#acl vid any
acl pktype [IPv4|Non-IPv4]	G	Set access control list packet type	switch(config)#acl pktype IPv4
acl ethtype [Any|ARP|IPX|Type value]	G	Set access control list ether type	switch(config)#acl ethtype ARP
acl sip [Any|IP][Mask]	G	Set access control list source IP address. It is automatically fill value 255.255.255.255 to Smask.	switch(config)#acl sip 192.168.16.1 255.255.255.255 or switch(config)#acl sip 192.168.16.2
acl dip [Any|IP][Mask]	G	Set access control list distinct IP address. It is automatically fill value 255.255.255.255 to Dmask.	switch(config)#acl dip Any
acl frg [Check|Uncheck]	G	Set access control list IP fragment	switch(config)#acl frg Check
acl l4 other [Any|ICMP|IGMP|Protocol value]	G	Set access control list L4 protocol other type	switch(config)#acl l4 other ICMP
acl l4 TCP [Any|FTP|HTTP|Port number]	G	Set access control list L4 protocol TCP	switch(config)#acl l4 TCP FTP
acl l4 UDP [Any|TFTP|Port number]	G	Set access control list L4 protocol UDP	switch(config)#acl l4 UDP TFTP
acl add	G	Add current rule to access control list table.	switch(config)#acl add
no acl [GroupID]	G	Delete rule from access control list table.	switch(config)#no acl 1
acl show	G	Show current temp rule.	switch(config)#acl show

5.3.16 DHCP filter Commands Set

Commands	Level	Description	Example
dhcp-filter [port#][on|off]	G	Enable dhcp filter by port	switch(config)#dhcp-filter 2 on

6. Technical Specifications

Technology	
Ethernet Standards	IEEE802.3 10BASE-T IEEE802.3u 100BASE-TX IEEE802.3z Gigabit Fiber IEE802.3ab 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 protocol IEEE802.1p Class of service IEEE802.1Q VLAN Tag IEEE802.1x User Authentication (Radius)
MAC addresses	8192
Priority Queues	4
Flow Control	IEEE 802.3x Flow Control and Back-pressure
Processing	Store-and-Forward
Interface	
RJ45 Ports	24/16 x 10/100Base-T(X), Auto MDI/MDI-X
Giga Fiber Ports	2 x 1000 Base-X(LC Connector) Multi-Mode: 0 to 550m, 850 nm (50/125 μm to 62.5/125 μm) Single Mode: 0 to 10Km, 1310 nm (9/125μm)
Giga Ports	2 x 10/100/1000 Base-T(X), Auto MDI/MDIX
LED Indicators	System power (Green) Gigabit Fiber: Link/Activity (Green) Gigabit Copper: Link/Activity (Green), Full Duplex/Collision (Orange) MINI GBIC: Link/Activity (Green)
Power Requirements	
Power Input Voltage	100VAC~240VAC, 50Hz~60Hz
Power Consumption	18 Watts Max
Environmental	
Operating Temperature	-10 to 60℃ (Wide temperature model -40 to 75°C)
Storage Temperature	-20 to 85℃
Operating Humidity	5% to 95%, non-condensing
Mechanical	
Dimensions(W x D x H)	440 mm(W)x 280 mm(D)x 44 mm(H)
Casing	IP-30 protection
Regulatory Approvals	
Regulatory Approvals	CE class A RoHS
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), Level 3, EN61000-4-6 (CS), Level 3