User’s Manual

PoE Management Switch

Model No.: SP1659P

http://www.micronet.info

Table of Content

1. Introduction

Micronet SP1659P PoE Management Switch features Power over Ethernet function, which helps user to centralize power distribution and reduces the cost of power infrastructure and installation. It also supports rich layer 2 management functions, suitable for high performance workgroups and server applications. With 2 Gigabit ports for copper or fiber-optic extension, it provides a perfect solution for huge data transmission and preserves the great flexibility of network infrastructure.

1.1 Package Content

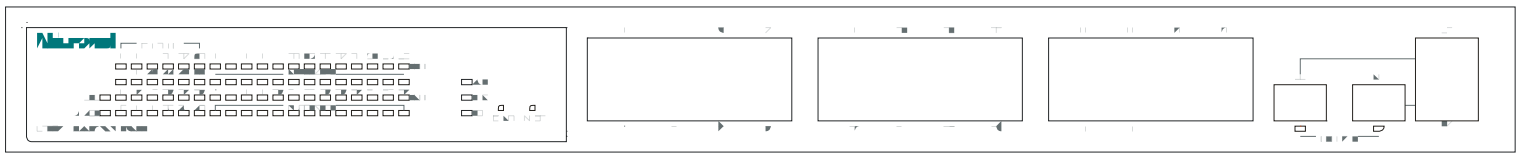
Before you start installing the device, verify the following items are in the package:

- SP1659P Management Switch
- Quick Installation Guide
- Manual CD
- RS-232 cable
- Mounting brackets
- Power cord

1.2 Key Features

- Compliant with IEEE802.3 10Base-T, IEEE802.3u 100Base-TX, IEEE802.3ab 1000Base-T, and IEEE802.3z 1000Base-LX/SX standards.
- Provide 24 RJ-45 ports of 10/100M, 2 RJ-45 ports of 10/100/1000M and 2 mini-GBIC slots for fiber extension
- Provide 24 IEEE802.3af PoE ports (Power Source)
- Power supplying up 185W totally
- Auto detect PD status, power consumption level, and power feeding priority
- Support IEEE 802.3ad Link Aggregation, up to 3 trunk groups
- Support IEEE802.1q tag-based VLAN, IEEE 802.1q-in-q nested VLAN, and IEEE802.1p traffic prioritization (CoS)
- Support traffic classification based on user-defined priority or information in MAC, and IP header
- Support 4 priority queues per port and Weighted Round-Robin (WRR) for packet transmission
- Support ingress and egress per port bandwidth control
- Support spanning tree protocols: 802.1d STP, 802.1w Rapid STP
- Support advanced standard 802.1w to make fast network convergence
- Support 802.1x and port security to control network access
- Support external RADIUS for authentication
- Support IGMPv2 (RFC 2236) snooping and filtering
- Support packet length up to 1536 bytes
- Support management security by IP filtering, controlling switch access mode for specified users
- Support virtual stack for centralized management
- Support MIBs: MIB II, RMON MIB (Group 1, 2, 3, 9), Bridge MIB, Ether-Like MIB, and private MIB
- Support SNMP trap, E-mail, and SMS alarm for any connectivity events

1.3 Physical Description



SP1659P front view

RESET Button

The button provides users to restart the switch.

LEDSET Button:

It is used to change LED display mode (ACT / FDX / SPD).

LED Status

Please refer to the following table for LED definition

LED	Status	Operation
POWER	On/Green	Power is on
CPU	Blink/Green	CPU is active
ACT	On/Green	LEDSET set to Active mode
FDX	On/Green	LEDSET set to FDX mode
SPD	On/Green	LEDSET set to Speed mode
10/100M Port (#1 - #24):		
LINK	On/Green	Link detected
ACT/FDX/SPD	On/Amber	Traffic detected (ACT mode)
		Full duplex (FDX mode)
		100M link (SPD mode)
PoE Status	On/Green	PoE is active
Gigabit Port (#25 - #26):		
LINK	On/Green	Link detected
mini-GBIC	On/Green	1000M fiber link detected
ACT/FDX/SPD	On/Green	Traffic detected (ACT mode)
		Full-duplex (FDX mode)
		1000M link (SPD mode)

2. Installation

This switch can be placed directly on your desktop, or mounted in a rack. If you install the device in a normal-standalone standard, the switch is an Intelligent Switch, and users can immediately use most of the features simply by attaching the cables and turning the power on.

Before installing the switch, we strongly recommend:

1. The switch is placed with appropriate ventilation environment. A minimum 25mm space around the unit is recommended.
2. The switch and the relevant components are away from sources of electrical noise such as radios, transmitters and broadband amplifiers
3. The switch is away from environment beyond recommend moisture

2.1 Installation without the Rack

Install the switch on a level surface that can support the weight of the unit and the relevant components. Plug the switch with the female end of the provided power cord and plug the male end to the power outlet. Attach the provided robber feet to the bottom of the switch to keep the switch from slipping. The recommend position has been square-marked.

2.2 Rack-mount Installation

The switch may standalone, or may be mounted in a standard 19-inch equipment rack. Rack mounting facilitate to an orderly installation when series of networking devices circumstance needed. The switch is supplied with rack mounting brackets and screws for rack mounting the unit.

Procedures to Rack-Mounting the Switch in the 19-inch rack:

1. Disconnect all cables from the switch before continuing.
2. Place the unit the right way up on a hard, flat surface with the front facing you.
3. Locate a mounting bracket over the mounting holes on one side of the unit.
4. Insert the screws and fully tighten with a suitable screwdriver.
5. Repeat the two previous steps for the other side of the unit.
6. Insert the unit into the 19" rack and secure with suitable screws.
7. Reconnect all cables.

2.3 Installing Network Cables

Station Connections

Connect each station with proper cables.

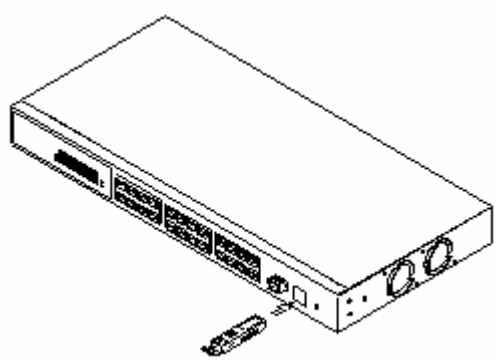
Switch-to-Switch Connections

The Gigabit ports provide the fat pipe to the server or backbone for boosting the total system performance.

Note: As the switch supports 802.3ad LACP (Link Aggregation Control Protocol) capability which up to 3 groups, to build up switch-to-switch connectivity with aggregation manner is provided.

2.4 Installation of mini-GBIC module

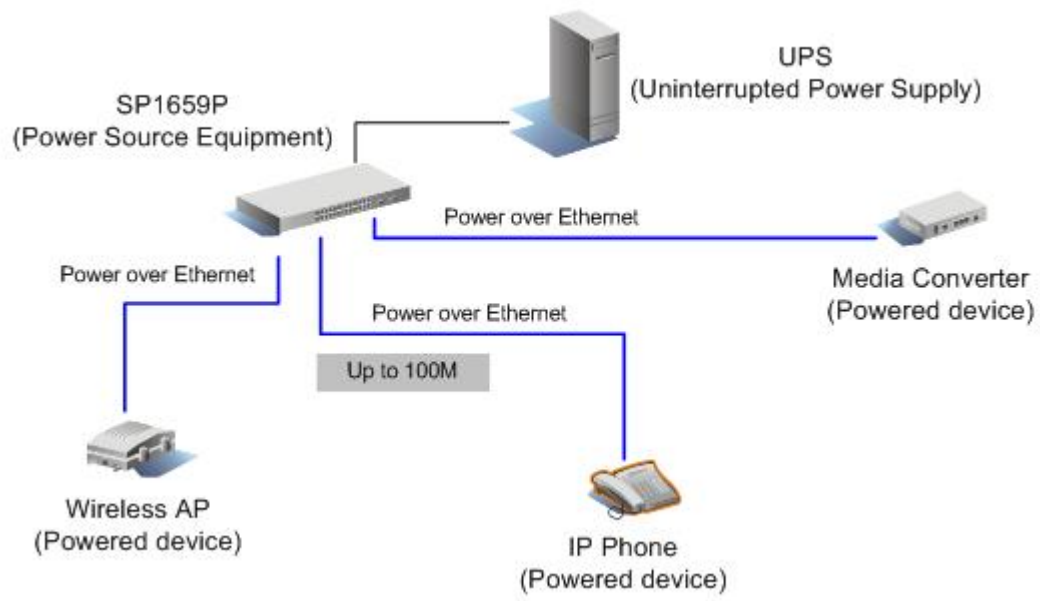
The switch provides 24 RJ-45 ports of 10/100/1000M and two mini-GBIC slots for fiber extension. Two mini-GBIC slots are respectively shared with RJ-45 port 23 & 24, but have higher priority than the two ports. If both RJ-45 port and mini-GBIC slot are in use, the mini-GBIC slot will be active and the RJ-45 port will be disabled and ignored.



The optional mini-GBIC modules are hot swappable, so you can plug or unplug it before or after powering on.

1. Verify that the mini-GBIC module is the right model and conforms to the chassis
2. Slide the module along the slot.
3. Be sure that the module is properly seated against the slot socket/connector
4. Install the media cable for network connection

2.5 Power Supply over Ethernet cable



3. Web-based User Interface

3.1 Setting up Connection

This switch can be managed using a standard Web Browser from any computer attached to the network. The SNMP management feature also permits the switch to be managed from any SNMP network management station running a network management program. Factory Default value of system is:

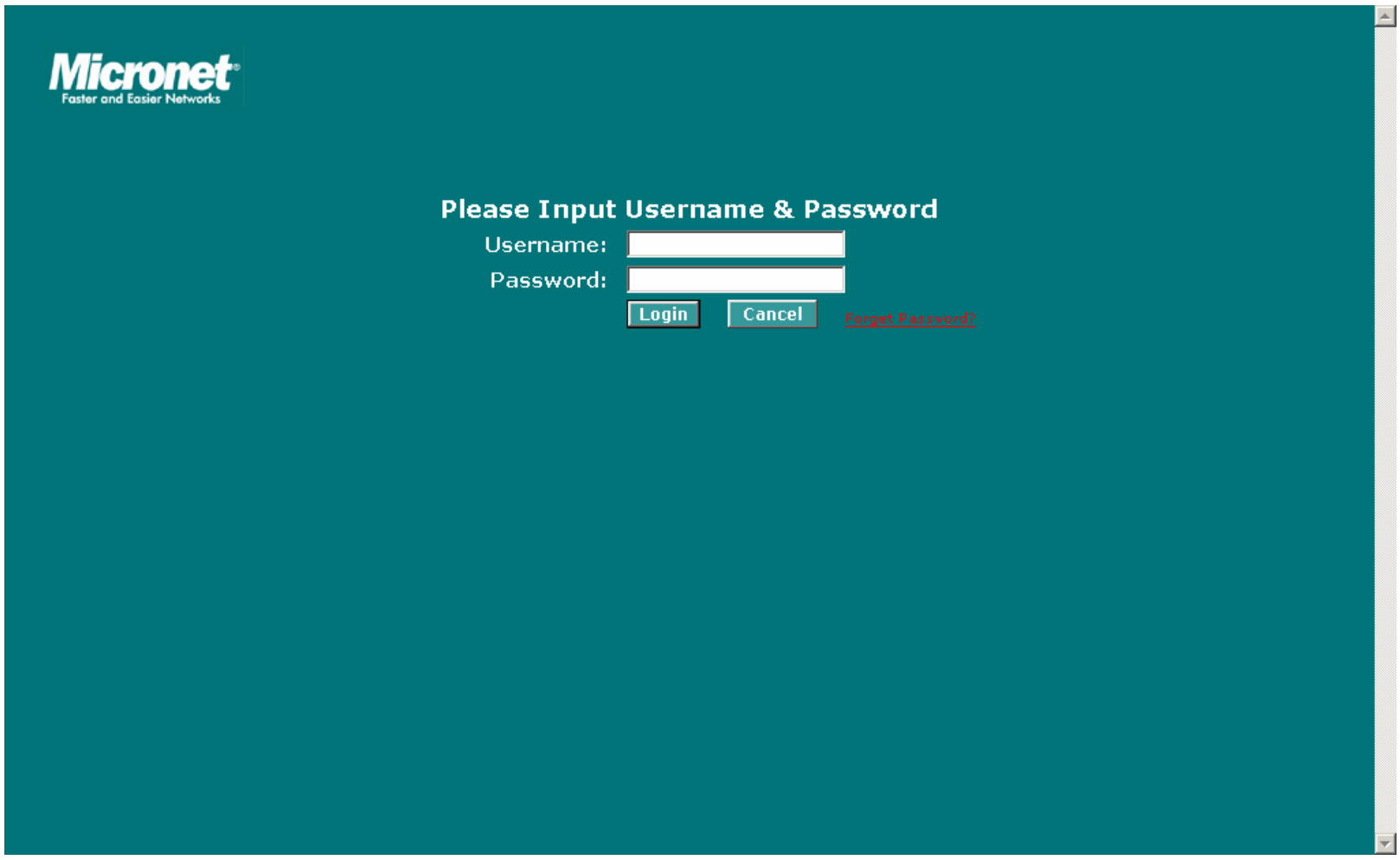
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.254

It supports a simple user management function allowing only one administrator to configure the system at the same time. If there are two or more users using administrator's identity, the switch will allow the only one who logins first to configure the system. The rest of users, even with administrator's identity, can only monitor the system. For those who have no administrator's identity, can only monitor the system. There are only a maximum of three users able to login simultaneously in the switch. To optimize the display effect, we recommend you use Microsoft IE and have the resolution 1024x768.

Login account by default is:

Username: ***admin*** Password: ***admin*** (read/write)

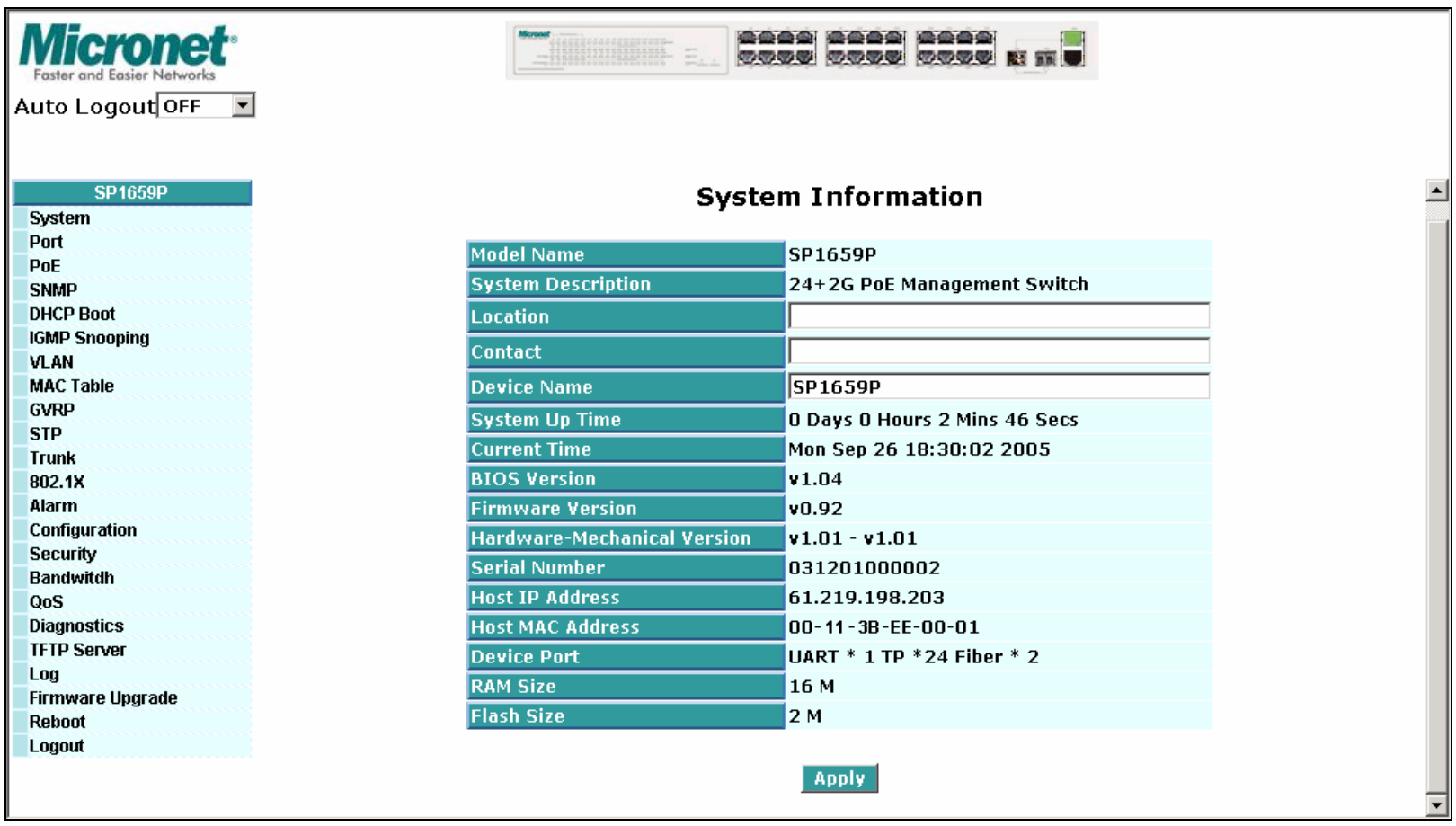
Username: ***guest*** Password: ***guest*** (read only)



Here is the whole function tree with web user interface and we will travel it through this chapter.

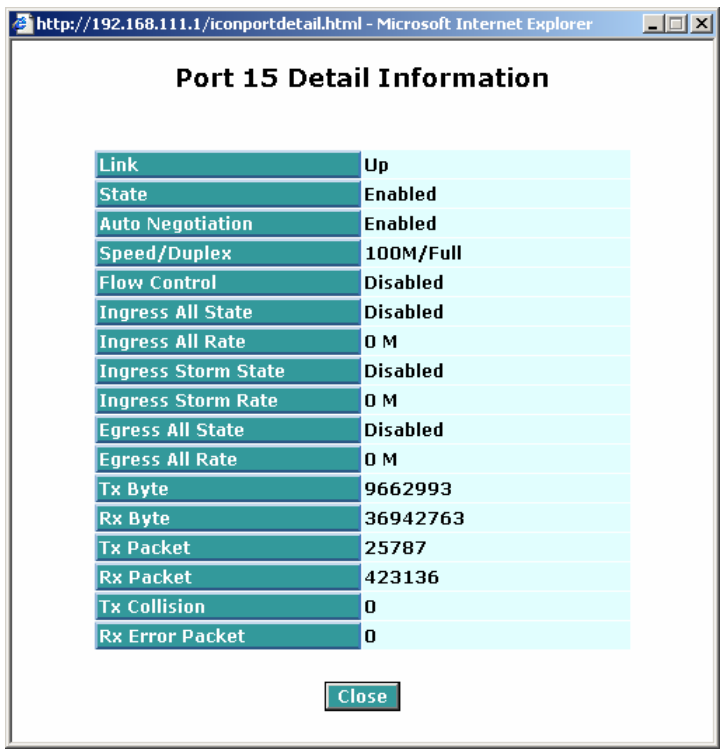
3.2 Web Management Overview

After you login, the switch shows you the system information as below. This page is default and tells you the basic information of the system, including “Model Name”, “System Description”, “Location”, “Contact”, “Device Name”, “System Up Time”, “Current Time”, “BIOS Version”, “Firmware Version”, “Hardware-Mechanical Version”, “Series Number”, “Host IP Address”, “Host Mac Address”, “Device Port”, “RAM Size” and “Flash Size”. With this information, you will know the software version used, MAC address, serial number, how many ports good and so on. This is helpful while malfunctioning.



On the top side, it shows the front panel of the switch. In the front panel, the linked ports will display green; as to the ports, which are link off, they will be dark. For the optional modules, the slot will show only a cover plate if no module exists and will show a module if a module is present. The image of module depends on the one you inserted. The same, if disconnected, the port will show just dark, if linked, green.

In this device, there are clicking functions on the panel provided for the information of the ports. These are very convenient functions for browsing the information of a single port. When clicking the port on the front panel, an information window for the port will be pop out as below. It shows the basic information of the clicked port. With this, you’ll see the information about the port status, traffic status and bandwidth rating for egress and ingress respectively.



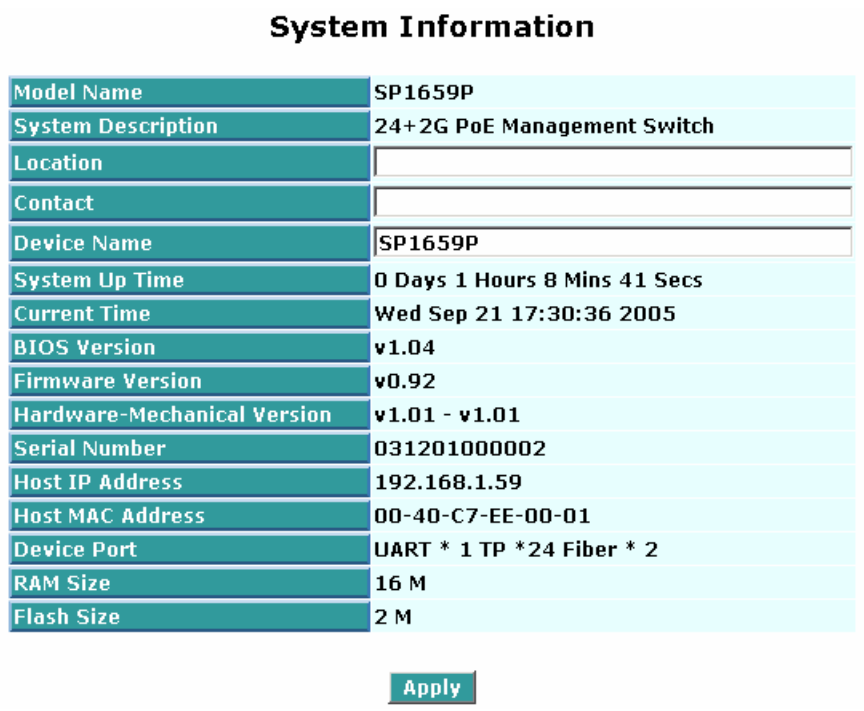
On the left-top corner, there is a pull-down list for Auto Logout. For the sake of security, we provide auto-logout function to protect you from illegal user as you are leaving. If you do not choose any selection in Auto Logout list, it means you turn on the Auto Logout function and the system will be logged out automatically when no action on the device 3 minutes later. If OFF is chosen, the screen will keep as it is. It is ON by default.

On the left side, the main menu tree for web is listed in the page. They are hierarchical menu. Open the function folder, a sub-menu will be shown. The functions of each folder are described in its corresponded section respectively. When clicking it, the function is performed.

3.3 System

3.3.1 System Information

Show the basic system information.

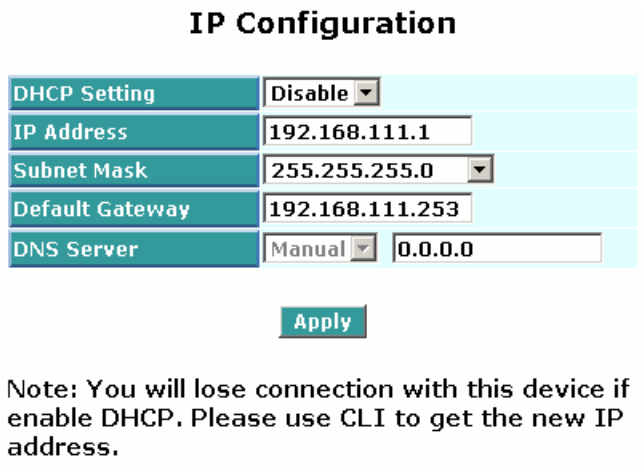


Parameter description:

- **Model name:** The model name of this device.
- **System description:** As it is, this tells what this device is.
- **Location:** The location where this switch is put. (User-defined).
- **Contact:** For easily managing and maintaining device, you may write down the contact person and phone here for getting help soon. You can configure this parameter through the device's user interface or SNMP.
- **Device name:** The name of the switch. (User-defined.)
- **System up time:** The time accumulated since this switch is powered up. Its format is day, hour, minute, second.
- **Current time:** Show the system time of the switch. Its format: day of week, month, day, hours : minutes : seconds, year. For instance, Wed, Apr. 23, 12:10:10, 2004.
- **BIOS version:** The version of the BIOS in this switch.
- **Firmware version:** The firmware version in this switch.
- **Hardware-Mechanical version:** The version of Hardware and Mechanical. The figure before the hyphen is the version of electronic hardware; the one after the hyphen is the version of mechanical.
- **Series number:** The serial number is assigned by the manufacturer.
- **Host IP address:** The IP address of the switch.
- **Host MAC address:** It is the Ethernet MAC address of the management agent in this switch.
- **Device Port:** Show all types and numbers of the port in the switch.
- **RAM size:** The size of the DRAM in this switch.
- **Flash size**: The size of the flash memory in this switch.

3.3.2 IP Configuration

IP configuration is one of the most important configurations in the switch. Without the proper setting, network manager will not be able to manage or view the device. The switch supports both manual IP address setting and automatic IP address setting via DHCP server. When IP address is changed, you must reboot the switch to have the setting taken effect and use the new IP to browse for web management and CLI management.



Parameter description:

- **DHCP Setting:**

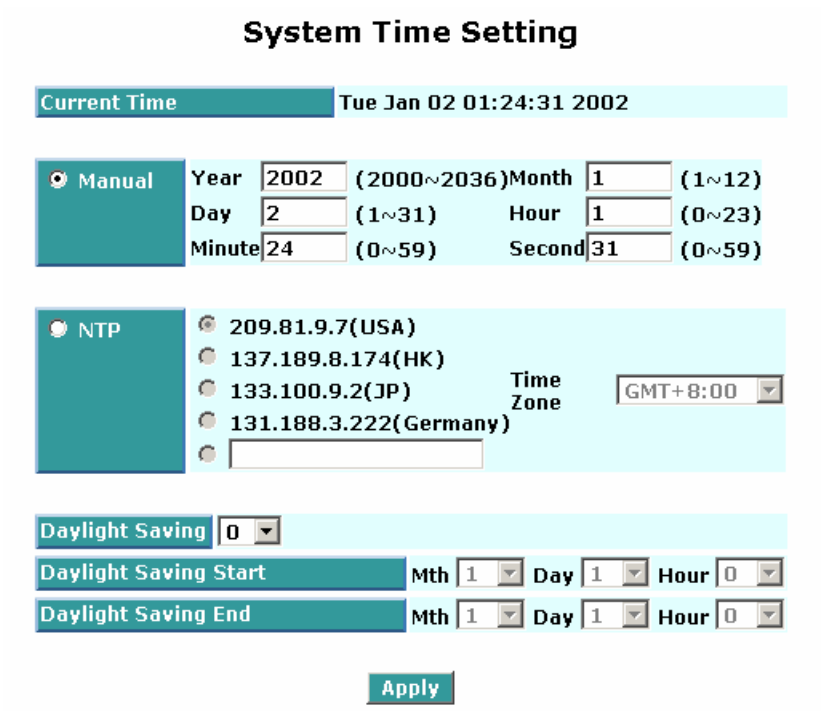
  DHCP is the abbreviation of Dynamic Host Configuration Protocol. Here DHCP means a switch to turn ON or OFF the function. The switch supports DHCP client used to get an IP address automatically if you set this function "Enable". When enabled, the switch will issue the request to the DHCP server resided in the network to get an IP address. If DHCP server is down or does not exist, the switch will issue the request and show IP address is under requesting, until the DHCP server is up. Before getting an IP address from DHCP server, the device will not continue booting procedures. If set this field "Disable", you'll have to input IP address manually.

- **IP address:**
  Users can configure the IP settings and fill in new values if users set the DHCP function “Disable”. Then, click <Apply> button to update. When DHCP is disabled, Default: 192.168.1.1. If DHCP is enabled, this field is filled by DHCP server and will not allow user manually set it any more.
- **Subnet mask:**
- **Default gateway:**
  Set an IP address for a gateway to handle those packets that do not meet the routing rules predefined in the device. If a packet does not meet the criteria for other pre-defined path, it must be forwarded to a default router on a default path. This means any packet with undefined IP address in the routing table will be sent to this device unconditionally. Default: 192.168.1.254.
- **DNS:**
  It is Domain Name Server used to serve the translation between IP address and name address. The switch supports DNS client function to re-route the mnemonic name address to DNS server to get its associated IP address for accessing Internet. User can specify a DNS IP address for the switch. With this, the switch can translate a mnemonic name address into an IP address. There are two ways to specify the IP address of DNS. One is fixed mode, which manually specifies its IP address, the other is dynamic mode, which is assigned by DHCP server while DHCP is enabled. DNS can help you easily remember the mnemonic address name with the meaningful words in it. Default is no assignment of DNS address. Default: 0.0.0.0

3.3.3 Time Configuration

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple and you just input “Year”, “Month”, “Day”, “Hour”, “Minute” and “Second” within the valid value range indicated in each item. If you input an invalid value, for example, 61 in minute, the switch will clamp the figure to 59.

NTP is a well-known protocol used to synchronize the clock of the switch system time over a network. NTP, an internet draft standard formalized in RFC 1305, has been adopted on the system is version 3 protocol. The switch provides four built-in NTP server IP addresses resided in the Internet and an user-defined NTP server IP address. The time zone is Greenwich-centered which uses the expression form of GMT+/- xx hours.



Parameter description:

- **Current Time**: Show the current time of the system.
- **Manual**:
  This is the function to adjust the time manually. Filling the valid figures in the fields of Year, Month, Day, Hour, Minute and Second respectively and press <Apply> button, time is adjusted. The valid figures for the parameter Year, Month, Day, Hour, Minute and Second are >=2000, 1-12, 1-31, 0-23, 0-59 and 0-59 respectively. Input the wrong figure and press <Apply> button, the device will reject the time adjustment request. There is no time zone setting in Manual mode.
- **NTP**:
  NTP is Network Time Protocol and is used to sync the network time based Greenwich Mean Time (GMT). If use the NTP mode and select a built-in NTP time server or manually specify an user-defined NTP server as well as Time Zone, the switch will sync the time in a short after pressing <Apply> button. Though it synchronizes the time automatically, NTP does not update the time periodically without user's processing.

  Time Zone is an offset time off GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and updated NTP time to come out the local time, otherwise, you will not able to get the correct time. The switch supports configurable time zone from –12 to +13 steps 1 hour.
  Default Time zone: +8 Hrs.
- **Daylight Saving**:
  Daylight saving is adopted in some countries. If set, it will adjust the time lag or in advance in unit of hours, according to the starting date and the ending date. For example, if you set the day light saving to be 1 hour. When the time passes over the starting time, the system time will be increased one hour after one minute at the time since it passed over. And when the time passes over the ending time, the system time will be decreased one hour after one minute at the time since it passed over.

The switch supports valid configurable day light saving time is –5 ~ +5 step one hour. The zero for this parameter means it need not have to adjust current time, equivalent to in-act daylight saving. You don't have to set the starting/ending date as well. If you set daylight saving to be non-zero, you have to set the starting/ending date as well; otherwise, the daylight saving function will not be activated.
Default for Daylight Saving: 0.

The following parameters are configurable for the function Daylight Saving and described in detail.

Day Light Saving Start:
This is used to set when to start performing the day light saving time.
Mth:
Range is 1 ~ 12.
Default: 1
Day:
Range is 1 ~ 31.
Default: 1
Hour:
Range is 0 ~ 23.
Default: 0

Day Light Saving End:
This is used to set when to stop performing the daylight saving time.
Mth:

Range is 1 ~ 12.
Default: 1

Day:

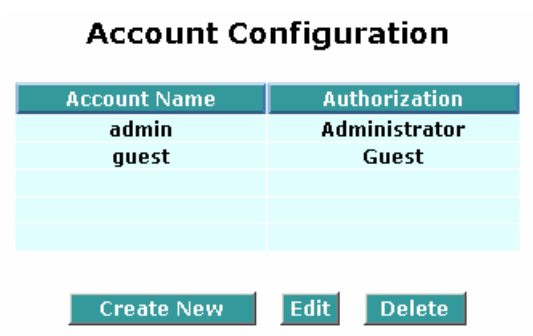
Range is 1 ~ 31.
Default: 1

Hour:

Range is 0 ~ 23.
Default: 0

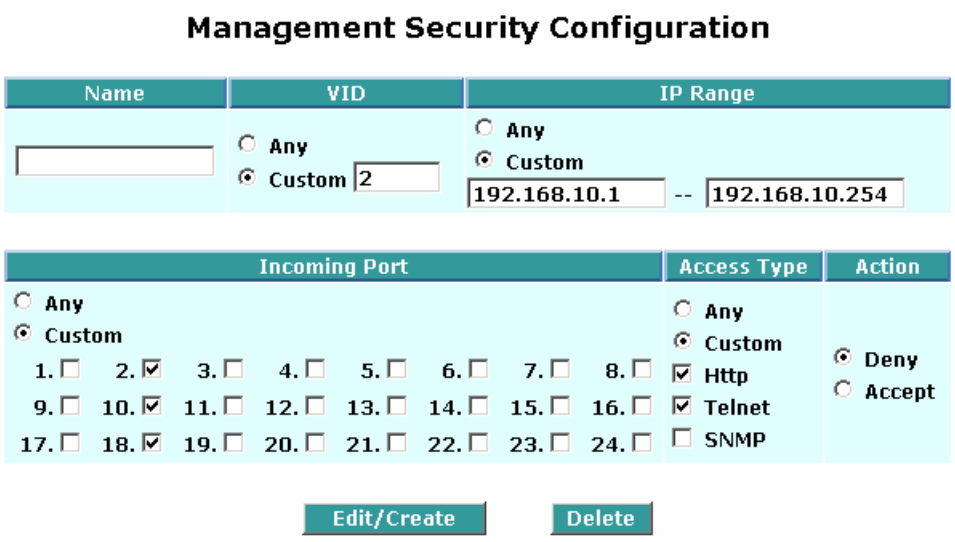
3.3.4 Account Configuration

In this function, only administrator can create, modify or delete the username and password. Administrator can modify other guest identities' password without confirming the password but it is necessary to modify the administrator-equivalent identity. Guest-equivalent identity can modify his password only. Please note that you must confirm administrator/guest identity in the field of Authorization in advance before configuring the username and password. Only one administrator is allowed to exist and unable to be deleted. In addition, up to 5 guest accounts can be created.



3.3.5 Management Policy

Through the management security configuration, the manager can control the mode via which user access this switch. According to the mode, users can be classified into two types: Those who are able to connect to the switch (Accept) and those who are unable to connect to the switch (Deny). Some restrictions also can be placed on the mode that the user connect to the switch, for example, we can decide that which VLAN VID is able to be accepted or denied by the switch, the IP range of the user could be accepted or denied by the switch, the port that the user is allowed or not allowed to connect with the switch, or the way of controlling and connecting to the switch via Http, Telnet or SNMP.



Name	VID	IP Range	Incoming Port	Access Type	Action
	Any	Any	2	Telnet,SNMP	Deny
	10	192.168.10.1-192.168.10.254	10	Http,Telnet,SNMP	Deny
	2	192.168.10.1-192.168.10.254	2,10,18	Http,Telnet	Deny

Parameter description:

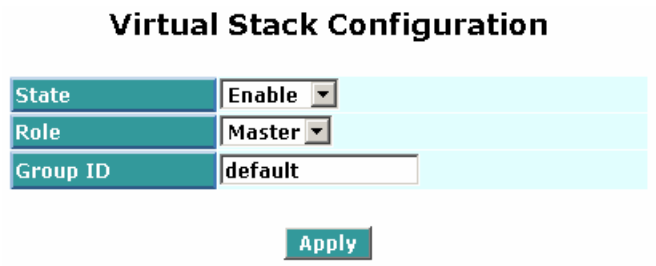
- **Name:** A name is composed of any letter (A-Z, a-z) and digit (0-9) with maximal 8 characters.
- **VID:**
  The switch supports two kinds of options for managed valid VLAN VID, including “Any” and “Custom”. Default is “Any”. When you choose “Custom”, you can fill in VID number. The valid VID range is 1~4094.
- **IP Range:**
  The switch supports two kinds of options for managed valid IP Range, including “Any” and “Custom”. Default is “Any”. In case that ”Custom” had been chosen, you can assign effective IP range. The valid range is 0.0.0.0~255.255.255.255.
- **Incoming Port:**
  The switch supports two kinds of options for managed valid Port Range, including “Any” and “Custom”. Default is “Any”. You can select the ports that you would like them to be worked and restricted in the management security configuration if ”Custom” had been chosen.
- **Access Type:**
  The switch supports two kinds of options for managed valid Access Type, including “Any” and “Custom”. Default is “Any”. “Http”, “Telnet” and “SNMP” are three ways for the access and managing the switch in case that” Custom” had been chosen.
- **Action:**
  The switch supports two kinds of options for managed valid Action Type, including “Deny” and “Accept”. Default is “Deny”. When you choose “Deny” action, you will be restricted and refused to manage the switch due to the “Access Type” you choose. However, while you select “Accept” action, you will have the authority to manage the switch.
- **Edit/Create:**
  A new entry of Management Security Configuration can be created after the parameters as mentioned above had been setup and then press <Edit/Create> button. Of course, the existed entry also can be modified by pressing this button.
- **Delete:** Remove the existed entry of Management Security Configuration from the management security table.

3.3.6 Virtual Stack

Virtual Stack Management (VSM) is the group management function. Through the proper configuration of this function, switches in the same LAN will be grouped automatically. And among these switch, one switch will be a master machine, and the others in this group will become the slave devices.

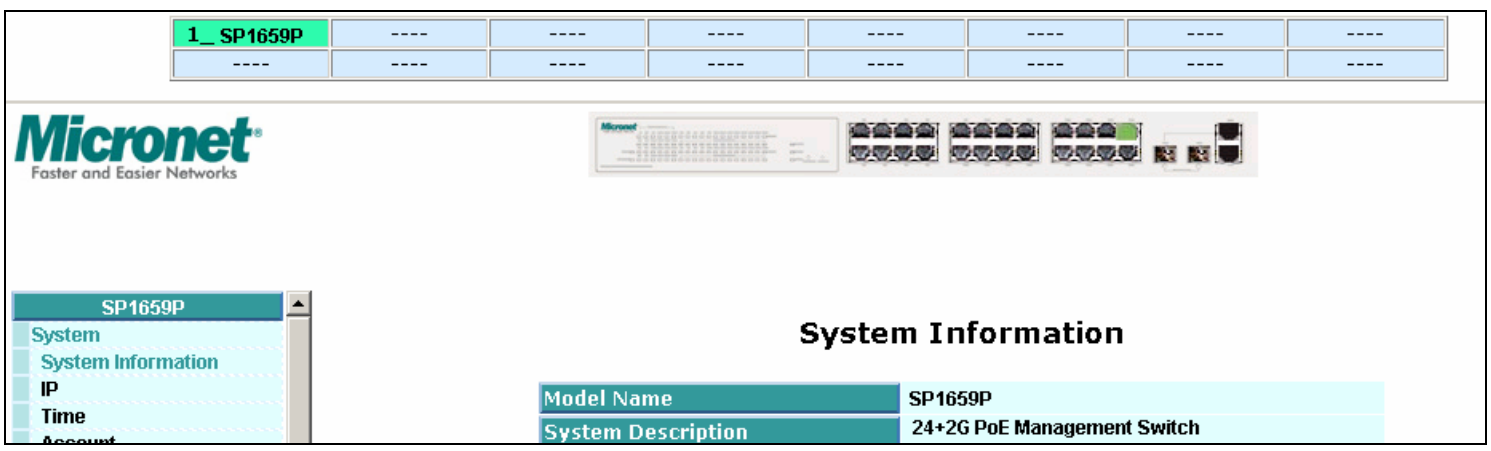
VSM offers a simple centralized management function. It is not necessary to remember the address of all devices; manager is capable of managing the network with knowing the address of the Master machine. Instead of SNMP or Telnet UI, VSM is only available in Web UI. While one switch becomes the Master, two rows of buttons for group device will appear on the top of its Web UI. By pressing these buttons, user will be allowed to connect the Web UI of the devices of the group in the same window without the login of these

devices.



Parameter description:

- **State:** It is used for the activation or de-activation of VSM. Default is Enable.
- **Role:** The role that the switch would like to play in virtual stack. Two types of roles, including master and slave are offered for option. Default is Master.
- **Group ID:** It is the group identifier (GID) which signs for VSM. Valid letters are A-Z, a-z, 0-9, " - " and "_" characters. The maximal length is 15 characters.



The most top-left button is only for Master device. The background color of the button you press will be changed to represent that the device is under your management.

Note: It will remove the grouping temporarily in case that you login the switch via the console.

The device of the group will be shown as station address (the last number of IP Address) + device name on the button (e.g. 1_SP1659P), otherwise it will show " ---- " if no corresponding device exists.

Once the devices join the group successfully, then they are merely able to be managed via Master device, and user will fail to manage them via telnet/console/web individually.

Up to 16 devices can be grouped for VSM, however, only one Master is allowed to exist in each group. For Master redundancy, user may configure more than two devices as Master device; however, the Master device with the smaller MAC value will be the Master one. All of these 16 devices can become Master device and back up with each other.

3.4 Port Configuration

3.4.1 Status

The function Port Status gathers the information of all ports' current status and reports it by the order of port number, media, link status, port state, Auto-Negotiation status, speed/duplex, Rx Pause and Tx Pause. Extra media type information for the module ports 25 and 26 is also offered. It reports the latest updated status of all

ports in this switch. When any one of the ports in the switch changes its parameter displayed in the page, it will be automatically refreshed the port current status about every 5 seconds.

Port Current Status

Port No	Media	Link	State	Auto Nego.	Speed/Duplex	Rx Pause	Tx Pause
1	TP	Down	Enabled	Enabled	---/----	------	------
2	TP	Down	Enabled	Enabled	---/----	------	------
3	TP	Up	Enabled	Enabled	100M/Full	On	On
4	TP	Down	Enabled	Enabled	---/----	------	------
5	TP	Down	Enabled	Enabled	---/----	------	------
6	TP	Down	Enabled	Enabled	---/----	------	------
7	TP	Down	Enabled	Enabled	---/----	------	------
8	TP	Down	Enabled	Enabled	---/----	------	------
9	TP	Down	Enabled	Enabled	---/----	------	------
10	TP	Down	Enabled	Enabled	---/----	------	------
11	TP	Down	Enabled	Enabled	---/----	------	------
12	TP	Down	Enabled	Enabled	---/----	------	------

Parameter description:

- **Port No**:
  Display the port number. The number is 1 – 26. Both port 25 and 26 are optional modules.

- **Media**:
  Show the media type adopted in all ports. The Port 25 and Port 26 are optional modules, which support either fiber or UTP media with either Gigabit Ethernet (1000Mbps) or 10/100Mbps Fast Ethernet port. They may have different media types and speed. Especially, fiber port has comprehensive types of connector, distance, fiber mode and so on. The switch describes the module ports with the following page.

- **Link**:
  Show that if the link on the port is active or not. If the link is connected to a working-well device, the Link will show the link “Up”; otherwise, it will show “Down”. This is determined by the hardware on both devices of the connection.
  No default value.

- **State**:
  Show that the communication function of the port is “Enabled” or “Disabled”. When it is enabled, traffic can be transmitted and received via this port. When it is disabled, no traffic can be transferred through this port. Port State is configured by user.
  Default: Enabled.

- **Auto Negotiation**:
  Show the exchange mode of Ethernet MAC. There are two modes supported in the switch. They are auto-negotiation mode “Enabled” and forced mode “Disabled”. When in “Enabled” mode, this function will automatically negotiate by hardware itself and exchange each other the capability of speed and duplex mode with other site which is linked, and comes out the best communication way. When in “Disabled” mode, both parties must have the same setting of speed and duplex, otherwise, both of them will not be linked. In this case, the link result is “Down”.
  Default: Enabled

- **Speed / Duplex**:
  Display the speed and duplex of all port. There are three speeds 10Mbps, 100Mbps and 1000Mbps supported for TP media, and the duplex supported is half duplex and full duplex. If the media is 1Gbps fiber, it is 1000Mbps supported only. The status of speed/duplex mode is determined by 1) the negotiation of both local port and link partner in “Auto Speed” mode or 2) user setting in “Force” mode.

The local port has to be preset its capability.

In port 1 – 24, they are supported Fast Ethernet with TP media only, so the result will show 100M/Full or 100M/Half, 10M/Full and 10M/Half duplex.

In port 25 and port 26, if the media is 1000Mbps with TP media, it will show the combinations of 10/100M and Full/Half duplex, 1000Mbps and Full duplex only. If the media is 1000Mbps with fiber media, it will show only 1000M/Full duplex.

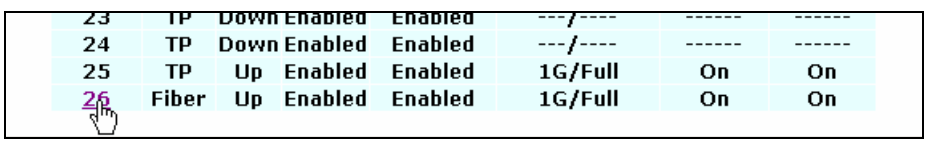
Default: None, it depends on the result of the negotiation.

Rx Pause:
The way that the port adopts to process the PAUSE frame. If it shows “on”, the port will care the PAUSE frame; otherwise, the port will ignore the PAUSE frame.

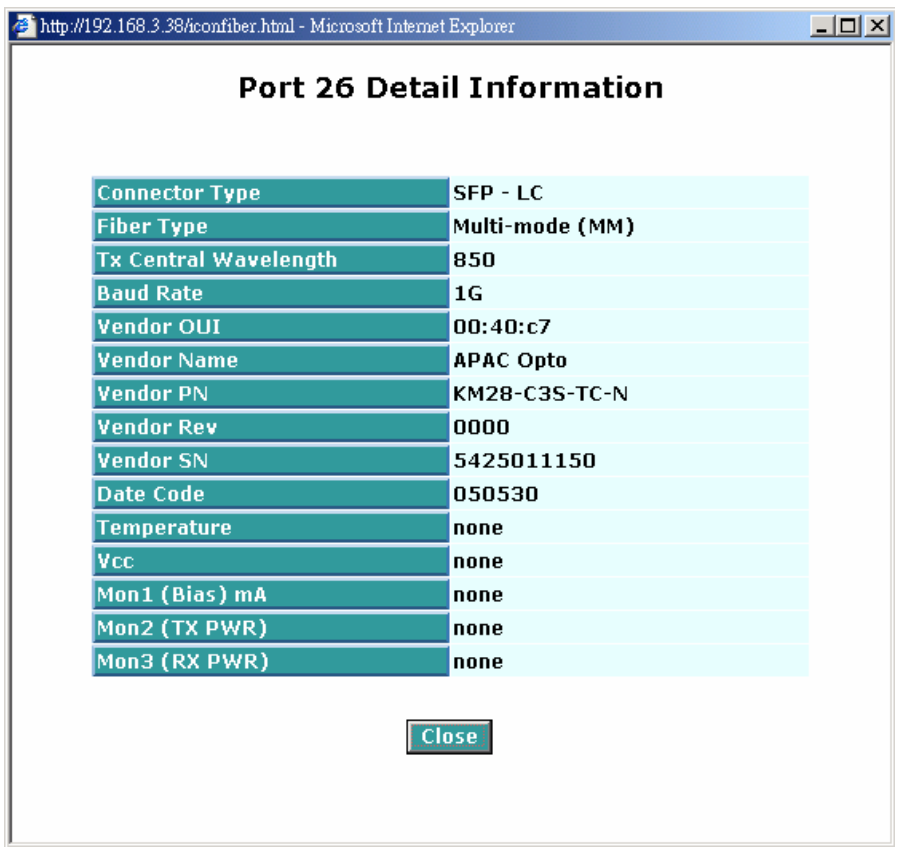
Default: None

Tx Pause:
It decides that whether the port transmits the PAUSE frame or not. If it shows “on”, the port will send PAUSE frame; otherwise, the port will not send the PAUSE frame.
Default: None

Parameter description of Port 25 and Port26:
(Click on the hyper-link, when fiber link is connected.)



23	TP	Down	Enabled	Enabled	---/----	------	------
24	TP	Down	Enabled	Enabled	---/----	------	------
25	TP	Up	Enabled	Enabled	1G/Full	On	On
26	Fiber	Up	Enabled	Enabled	1G/Full	On	On



Connector Type:
Display the connector type, for instance, UTP, SC, ST, LC and so on.

Fiber Type:
Display the fiber mode, for instance, Multi-Mode, Single-Mode.
Tx Central Wavelength:

Display the fiber optical transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm and so on.

Baud Rate:
Display the maximum baud rate of the fiber module supported, for instance, 10M, 100M, 1G, 10G and so on.

Vendor OUI:
Display the Manufacturer's OUI code which is assigned by IEEE.

Vendor Name:
Display the company name of the module manufacturer.

Vendor P/N:
Display the product name of the naming by module manufacturer.

Vendor Rev (Revision):
Display the module revision.

Vendor SN (Serial Number):
Show the serial number assigned by the manufacturer.

Date Code:
Show the date this module was made.

Temperature:
Show the current temperature of module.

Vcc:
Show the working DC voltage of module.

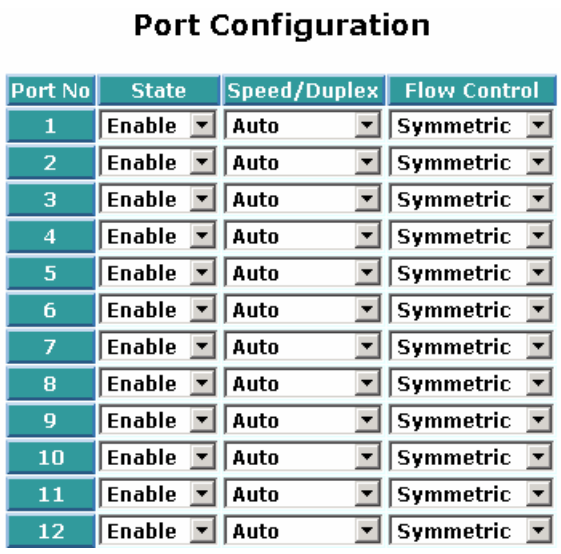
Mon1(Bias) mA:
Show the Bias current of module.

Mon2(TX PWR):
Show the transmit power of module.

Mon3(RX PWR):
Show the receiver power of module.

3.4.2 Configuration

Port Configuration is applied to change the setting of each port. In this configuration function, you can set/reset the following functions. All of them are described in detail below.



Parameter description:

- **State:**
  Set the communication capability of the port is enabled or disabled. When enabled, traffic can be transmitted and received via this port. When disabled, the port is blocked and no traffic can be transferred through this port. Port State is configurable by the user. There are only two states “Enable” and “Disable” able to choose. If you set a port’s state “Disable”, then that port is prohibited to pass any traffic, even it looks Link up.
  Default: Enable.

- **Speed / Duplex:**
  Set the speed and duplex of the port. In speed, 10/100Mbps baud rate is available for Fast Ethernet, Gigabit module in port 25, 26. If the media is 1Gbps fiber, it is always 1000Mbps and the duplex is full only. If the media is TP, the Speed/Duplex is comprised of the combination of speed mode, 10/100/1000Mbps, and duplex mode, full duplex and half duplex. The following table summarized the function the media supports.

Media type	NWay	Speed	Duplex
100M TP	ON/OFF	10/100M	Full/Half
1000M TP	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1000M Fiber	ON/OFF	1000M	Full

  In Auto-negotiation mode, no default value. In Forced mode, default value depends on your setting.

- **Flow Control:**
  There are two modes to choose in flow control, including Symmetric and Asymmetric. If flow control is set Symmetric, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. When it is set Asymmetric, this will let the receiving port care the PAUSE frame from transmitting device(s), but it doesn’t send PAUSE frame. This is one-way flow control.

  Default: Symmetric.

3.4.3 Simple Counter

The function of Simple Counter collects any information and provides the counting about the traffic of the port, no matter the packet is good or bad. As below, the window can show all ports’ counter information at the same time. Each data field has 12-digit long. If the counting is overflow, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The valid range is 3 to 10 seconds. The Refresh

Interval is used to set the update frequency. Default update time is 3 seconds.

Simple Counter

Refresh Interval 3 sec Reset

Time elapsed since last reset: 0 Days 1 Hours 38 Mins 15 Secs

Port No	Tx Byte	Rx Byte	Tx Packet	Rx Packet	Tx Collision	Rx Error Packet
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	4375178	3478408	8696	36633	0	0

Parameter description:

- **Tx Byte:** Total transmitted bytes.
- **Rx Byte:** Total received bytes.
- **Tx Packet:** The counting number of the packet transmitted.
- **Rx Packet:** The counting number of the packet received.
- **Tx Collision:** Number of collisions transmitting frames experienced.
- **Rx Error Packet:** Number of bad packets received.

3.4.4 Detailed Counter

The function of Detail Counter collects any information and provides the counting about the traffic of the port, no matter the packet is good or bad. As below, the window can show only one port counter information at the same time. To see another port's counter, you have to pull down the list of Select, then you will see the figures displayed about the port you had chosen. Each data field has 12-digit long. If the counting is overflow, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The valid range is 3 to 10 seconds. The Refresh Interval is used to set the update frequency. Default update time is 3 seconds.

Detail Counter

Select Port 25 Refresh Interval 3 sec Reset

Time elapsed since last reset: 0 Days 3 Hours 10 Mins 17 Secs

Receive Total		Transmit Error Counters	
Rx Packets	3528	Tx Collisions	0
Rx Octets	517521	Tx Single Collision	0
Rx Errors	0	Tx Multiple Collision	0
Rx Unicast Packets	3083	Tx Drop Packets	0
Rx Broadcast Packets	445	Tx Deferred Transmit	0
RX Multicast Packets	0	Tx Late Collision	0
Rx Pause Packets	0	Tx Excessive Collision	0
Receive Size Counters		**Transmit Total**	
Packets 64 Octects	2218	Tx Packets	3196
Packets 65 to 127 Octects	691	Tx Octets	1337304
Packets 128 to 255 Octects	23	Tx Unicast Packets	3196
Packets 256 to 511 Octects	76	Tx Broadcast Packets	0

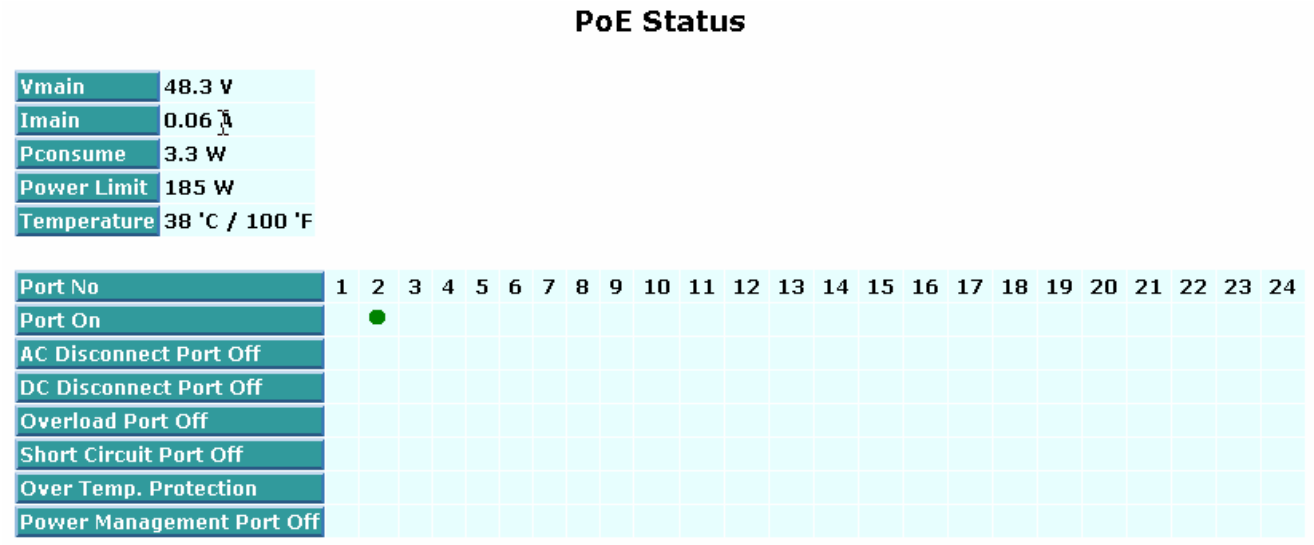
Parameter description:

- **Rx Packets:** The counting number of the packet received.
- **Rx Octets:** Total received bytes.
- **Rx Errors:** Number of bad packets received.
- **Rx Unicast Packets:** Show the counting number of the received unicast packet.
- **Rx Broadcast Packets:** Show the counting number of the received broadcast packet.
- **Rx Multicast Packets:** Show the counting number of the received multicast packet.
- **Rx Pause Packets:** Show the counting number of the received pause packet.
- **Tx Collisions:** Number of collisions transmitting frames experienced.
- **Tx Single Collision:** Number of frames transmitted that experienced exactly one collision.
- **Tx Multiple Collision:** Number of frames transmitted that experienced more than one collision.
- **Tx Drop Packets:** Number of frames dropped due to excessive collision, late collision, or frame aging.
- **Tx Deferred Transmit:** Number of frames delayed to transmission due to the medium is busy.
- **Tx Late Collision:** Number of times that a collision is detected later than 512 bit-times into the transmission of a frame.
- **Tx Excessive Collision:** Number of frames that are not transmitted because the frame experienced 16 transmission attempts**.**
- **Packets 64 Octets:** Number of 64-byte frames in good and bad packets received.
- **Packets 65-127 Octets:** Number of 65 ~ 127-byte frames in good and bad packets received.
- **Packets 128-255 Octets:** Number of 128 ~ 255-byte frames in good and bad packets received.
- **Packets 256-511 Octets:** Number of 256 ~ 511-byte frames in good and bad packets received.
- **Packets 512-1023 Octets:** Number of 512 ~ 1023-byte frames in good and bad packets received.
- **Packets 1024- 1522 Octets:** Number of 1024-1522-byte frames in good and bad packets received.
- **Tx Packets:** The counting number of the packet transmitted.
- **TX Octets:** Total transmitted bytes.
- **Tx Unicast Packets:** Show the counting number of the transmitted unicast packet.
- **Tx Broadcast Packets:**
- Show the counting number of the transmitted broadcast packet.
- **Tx Multicast Packets:** Show the counting number of the transmitted multicast packet.
- **Tx Pause Packets:** Show the counting number of the transmitted pause packet.
- **Rx FCS Errors:** Number of bad FSC packets received.
- **Rx Alignment Errors:** Number of Alignment errors packets received.
- **Rx Fragments:** Number of short frames (< 64 bytes) with invalid CRC.
- **Rx Jabbers:** Number of long frames(according tomax_length register) with invalid CRC.
- **Rx Drop Packets:** Frames dropped due to the lack of receiving buffer.
- **Rx Undersize Packets:** Number of short frames (<64 Bytes) with valid CRC.
- **Rx Oversize Packets:** Number of long frames(according to max_length register) with valid CRC.
-

3.5 PoE

3.5.1 PoE Status

Display the information about the PoE status.



Parameter description:

- **Vmain:** The volt is supplied by the PoE.
- **Imain:** The sum of the current that every port supplies.
- **Pconsume:** The sum of the power that every port supplies.
- **Power Limit:** The maximal power that the switch can supply (Read Only).
- **Temperature:** The temperature of the chip on PoE.
- **Port No:** Port number.
- **Port On:** Show whether the port is supplying the power to the PD or not.
- **AC Disconnect Port Off:** Port is turned off due to the AC Disconnect function.
- **DC Disconnect Port Off:** Port is turned off due to the DC Disconnect function.
- **Overload Port Off:** The switch will stop supplying the power to the port due to the power required by the PD that is linked to the port on the switch excesses the Class setting of the PD.
- **Short Circuit Port Off:** The switch will stop supplying the power to the port if it detects that the PD linked to the port is short circuit.
- **Over Temp. Protection:** The port of the switch will be disabled due to fast transient rise in temperature to 240oC or slow rise in temperature to 200oC.
- **Power Management Port Off:** Due to total power required by all PDs linked to the switch excesses the power limit, so the switch stops supplying the power to this port after referring to the information of the priority.

3.5.2 PoE Configuration

In PoE Port Management function, user can configure the settings about PoE. The switch complies with IEEE 802.3af protocol and be capable of detecting automatically that whether the device linked to the port on the switch is PD (Powered Device) or not. The switch also manage the power supplement based on the Class of the PD, and it will stop supplying the power once the power required by the PD excesses the Class, Short Circuit or over temperature occurs.

PoE Configuration

Port No	Status	State	Priority	Power(W)	Current(mA)	Class
1	Normal	Enable	Normal	0	0	0
2	Active	Enable	Normal	3.2	67	2
3	Normal	Enable	Normal	0	0	0
4	Normal	Enable	Normal	0	0	0
5	Normal	Enable	Normal	0	0	0
6	Normal	Enable	Normal	0	0	0
7	Normal	Enable	Normal	0	0	0
8	Normal	Enable	Normal	0	0	0
9	Normal	Enable	Normal	0	0	0
10	Normal	Enable	Normal	0	0	0
11	Normal	Enable	Normal	0	0	0
12	Normal	Enable	Normal	0	0	0

Parameter description:

- **Status:** Include “Normal” or “Active” two kinds of status. The former means the port is ready to link and supply the power to the PD at any time. The latter means the port is in the condition of supplying the power.
- **State:** ”Enable” means the manager allows the power supplied to the PD is legal while the port linked to the PD; “Disable” means the port does not own PoE function.
- **Priority:** Three options are offered for the user to choose, including Normal, Low and High. Default is Normal. The switch will stop supplying the power to the port based on the order of the priority Low → Normal → High in case total power required by all PDs linked to the switch excesses the power limit. As the ports have the same priority, then the switch will cease the power supplement from the port with the highest port id (12→1).
- **Power(W):** The power is consumed by the port.
- **Current(mA):** The current is supplied to the PD by the port.
- **Class:** The Class of the PD linked to the port of the switch.

3.6 SNMP

This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click <Apply> button, the setting takes effect.

SNMP Configuration

SNMP	◉ Enable ○ Disable			
Get Community	public			
Set Community	private	Enable		
Trap Host 1 IP Address	0.0.0.0	162	Community	public
Trap Host 2 IP Address	0.0.0.0	162	Community	public
Trap Host 3 IP Address	0.0.0.0	162	Community	public
Trap Host 4 IP Address	0.0.0.0	162	Community	public
Trap Host 5 IP Address	0.0.0.0	162	Community	public
Trap Host 6 IP Address	0.0.0.0	162	Community	public

Parameter description:

- **SNMP:**
  The term SNMP here is used for the activation or de-activation of SNMP. Default is Enable.

- **Get/Set/Trap Community:**
  Community name is used as password for authenticating if the requesting network management unit belongs to the same community group. If they both don't have the same community name, they don't belong to the same group. Hence, the requesting network management unit can not access the device with different community name via SNMP protocol; If they both have the same community name, they can talk each other.

  Community name is user-definable with a maximum length of 15 characters and is case sensitive. There is not allowed to put any blank in the community name string. Any printable character is allowable.

  The community name for each function works independently. Each function has its own community name. Say, the community name for GET only works for GET function and can't be applied to other function such as SET and Trap.

    - Default SNMP function : Enable
    - Default community name for GET: public
    - Default community name for SET: private
    - Default community name for Trap: public
    - Default Set function : Enable
    - Default trap host IP address: 0.0.0.0
    - Default port number :162

- **Trap:**
  In the switch, there are four trap hosts supported. Each of them has its own community name and IP address; is user-definable. To set up a trap host means to create a trap manager by assigning an IP address to host the trap message. In other words, the trap host is a network management unit with SNMP manager receiving the trap message from the managed switch with SNMP agent issuing the trap message. 6 trap hosts can prevent the important trap message from losing.

  For each public trap, the switch supports the trap event Cold Start, Warm Start, Link Down, Link Up and Authentication Failure Trap. They can be enabled or disabled individually. When enabled, the corresponded trap will actively send a trap message to the trap host when a trap happens. If all public traps are disabled, no public trap message will be sent. As to the Enterprise (no. 6) trap is classified as private trap, which are listed in the Trap Alarm Configuration function folder.

  Default for all public traps: Enable.

3.7 DHCP Boot

The DHCP Boot function is used to spread the request broadcast packet into a bigger time frame to prevent the traffic congestion due to broadcast packets from many network devices which may seek its NMS, boot server, DHCP server and many connections predefined when the whole building or block lose the power and then reboot and recover. At this moment, a bunch of switch or other network device on the LAN will try its best to find the server to get the services or try to set up the predefined links, they will issue many broadcast packets in the network.

The switch supports a random delay time for DHCP and boot delay for each device. This suppresses the broadcast storm while all devices are at booting stage in the same time. The maximum user-defined delay

time is 30 sec. If DHCP Broadcasting Suppression function is enabled, the delay time is set randomly, ranging from 0 to 30 seconds, because the exactly delay time is computed by the switch itself. The default is “Disable”.

3.8 IGMP Snooping

The function, IGMP Snooping, is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping can not tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch supported IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

Enabling IGMP with either passive or active mode, you can monitor the IGMP snooping information, which contains the multicast member list with the multicast groups, VID and member port.

Parameter description:

- **IGMP snooping mode selection:**
  The switch supports three kinds of IGMP Snooping status, including “Passive”, “Active” and “Disable”.

  Disable:
  Set “Disable” mode to disable IGMP Snooping function.
  Default: Disable

  Active:
  In Active mode, IGMP snooping switch will periodically issue the Membership Query message to all hosts attached to it and gather the Membership report message to update the database of the Multicast table. By the way, this also reduces the unnecessary multicast traffic.

  Passive:
  In Passive Snooping mode, the IGMP snooping will not periodically poll the hosts in the groups. The switch will send a Membership Query message to all hosts only when it has received a Membership

Query message from a router.

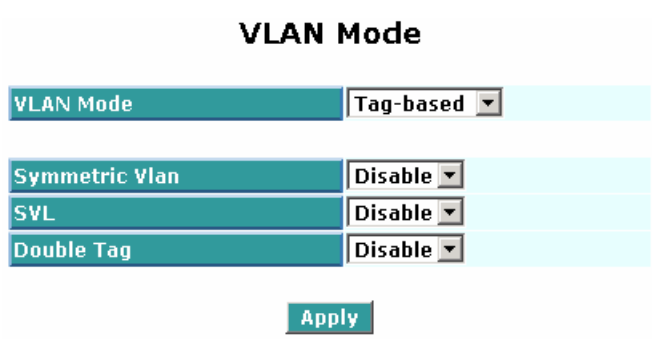
- **IP Address:**
  Show all multicast groups IP addresses that are registered on this device.
- **VLAN ID:**
  Show VLAN ID for each multicast group.
- **Member Port:**
  Show member ports that join each multicast group. Member port may be only or more than one.

3.9 VLAN

The switch supports Tag-based VLAN (802.1q) and Port-based VLAN. Support 256 active VLANs and VLAN ID 1~4094. VLAN configuration is used to partition your LAN into small ones as your demand. Properly configuring it, you can gain not only improving security and increasing performance but greatly reducing VLAN management.

3.9.1 VLAN Mode

The VLAN Mode Selection function includes two modes: Port-based and Tag- based, you can choose one of them by pulling down list and pressing the <Downward> arrow key. Then, click Apply button, the settings will take effect immediately.



Parameter description:

- **VLAN Mode:**

  Tag-based: (This is the default setting.)

  Tag-based VLAN identifies its member by VID. This is quite different from port-based VLAN. If there are any more rules in ingress filtering list or egress filtering list, the packet will be screened with more filtering criteria to determine if it can be forwarded. The switch supports supplement of 802.1q.

  Each tag-based VLAN you built up must be assigned VLAN name and VLAN ID. Valid VLAN ID is 1-4094. User can create total up to 256 Tag VLAN groups.

  Port-based:

  Port-based VLAN is defined by port. Any packet coming in or outgoing from any one port of a port-based VLAN will be accepted. No filtering criterion applies in port-based VLAN. The only criterion is the physical port you connect to. For example, for a port-based VLAN named PVLAN-1 contains port members Port 1&2&3&4. If you are on the port 1, you can communicate with port 2&3&4. If you are on the port 5, then you cannot talk to them. Each port-based VLAN you built up must be assigned a group name. This switch can support up to maximal 26 port-based VLAN groups.

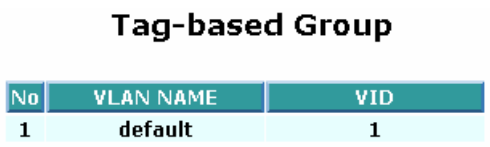
- **Symmetric Vlan:**
  This is called Ingress Rule (Rule 1, The Ingress Filtering Rule 1 is “forward only packets with VID matching this port’s configured VID”.). For example, if port 1 receives a tagged packet with VID=100 (VLAN name=VLAN100), and if Symmetric-Vlan function is enabled, the switch will check if port 1 is a member of VLAN100. If yes, the received packet is forwarded; otherwise, the received packet is dropped.
  Note: If Symmetric is enabled and port 1, for example, receives an untagged packet, the switch will apply the PVID of port 1 to tag this packet, the packet then will be forwarded. But if the PVID of port 1 is not 100, the packet will be dropped.

- **SVL:**
  While SVL is enable, all VLANs use the same filtering database storing the membership information of the VLAN to learn or look up the membership information of the VLAN. While SVL is disabled, it means learning mode is IVL. In this mode, different VLAN uses different filtering database storing the membership information of the VLAN to learn or look up the information of a VLAN member.

- **Double Tag:**
  Double-tag mode belongs to the tag-based mode, however, it would treat all frames as the untagged ones, which means that tag with PVID will be added into all packets. Then, these packets will be forwarded as Tag-based VLAN. So, the incoming packets with tag will become the double-tag ones.

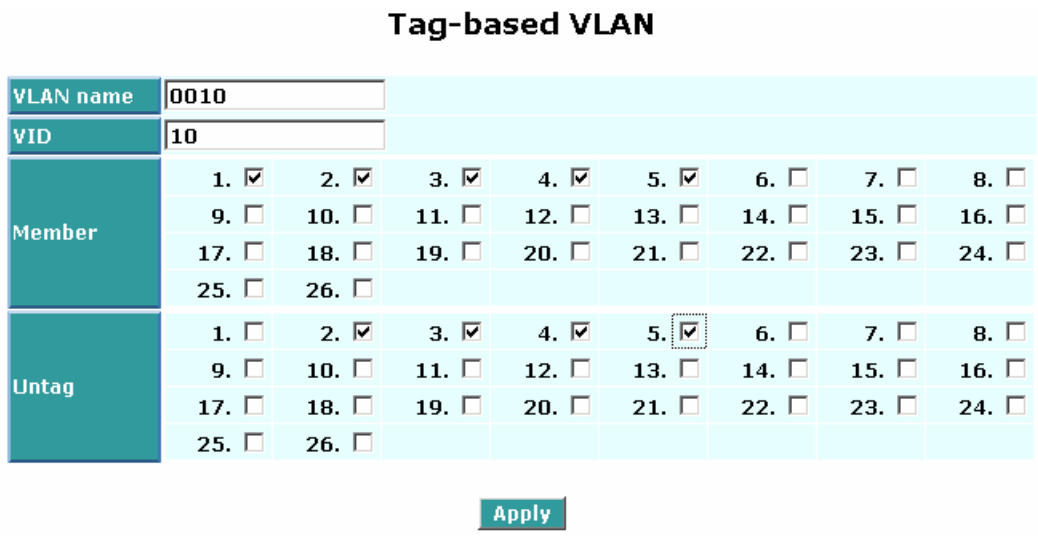
3.9.2 Tag-based Group

It shows the information of existed Tag-based VLAN Groups. You can also easily create, edit and delete a Tag-based VLAN group by pressing Add, Edit and Delete function buttons. User can add a new VLAN group by inputting a new VLAN name and VLAN ID after pressing <Add> button.



Parameter description:

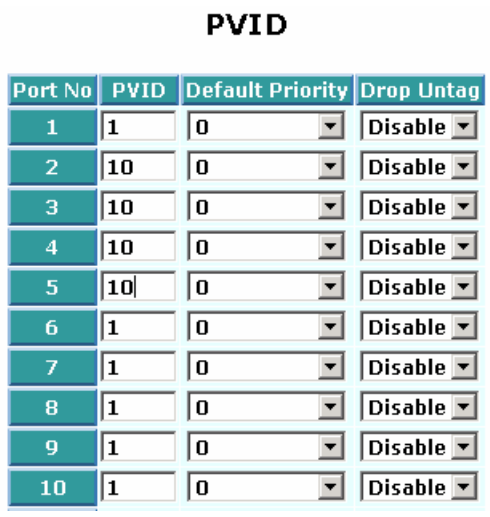
- **Add Group:**
  Input the VLAN name, VID and then choose the member by ticking the check box beside the port No. to create a new Tag-based VLAN. As to the parameter of Untag, it stands for an egress rule of the port. If you tick the check box beside the port No., packets with this VID outgoing from this port will be untagged. Finally, press the Apply button to have the setting taken effect.
- **Delete Group:**
  Just press the Delete button to remove the selected group entry from the Tag-based group table.
- **Edit a group:**
  Just select a group entry and press the Edit button, then you can modify a group’s description, member and untag settings.



- **VLAN Name:**
  The name defined by administrator is associated with a VLAN group. Valid letters are A-Z, a-z, 0-9, " - " and "_" characters. The maximal length is 15 characters.
- **VID:**
  VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based and Double-tag mode.
- **Member:**
  This is used to enable or disable if a port is a member of the new added VLAN, "Enable" means it is a member of the VLAN. Just tick the check box beside the port x to enable it.
- **Untag:**
  Select "untag" on the specified ports. Tag will be removed when packet is transmitted out of the ports.

3.9.3 PVID

In PVID Setting, user can input VID number to each port. The range of VID number is from 1 to 4094. User also can choose ingress filtering rule (Rule 2) to each port. The Ingress Filtering Rule 2 is "drop untagged frame". While Rule 2 is enabled, the port will discard all Untagged-frames.



Parameter description:

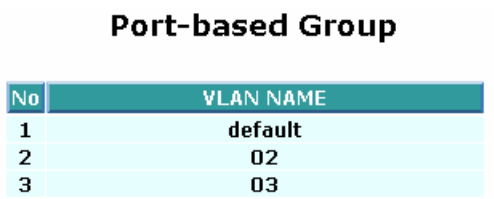
- **PVID:**
  This PVID range will be 1-4094. Before you set a number x as PVID, you have to create a Tag-based VLAN with VID x. For example, if port x receives an untagged packet, the switch will apply the PVID (assume as VID y) of port x to tag this packet, the packet then will be forwarded as the tagged packet with VID y.
- **Default Priority:**

It bases on 802.1p QoS and affects untagged packets. When the packets enter the switch, it would get the priority precedence according to your Default Priority setting and map to 802.1p priority setting in QoS function. For example, while you set Default Priority of port 2 with 2 and transmit untagged packets to port 2, these packets will own priority 2 precedence due to your default 802.1p Priority Mapping setting in QoS function and be put into Queue 1.

- **Drop Untag:**
  Drop untagged frame. You can configure a given port to accept all frames (Tagged and Untagged) or just receive tagged frame. If the former is the case, then the packets with tagged or untagged will be processed. If the later is the case, only the packets carrying VLAN tag will be processed, the rest packets will be discarded.

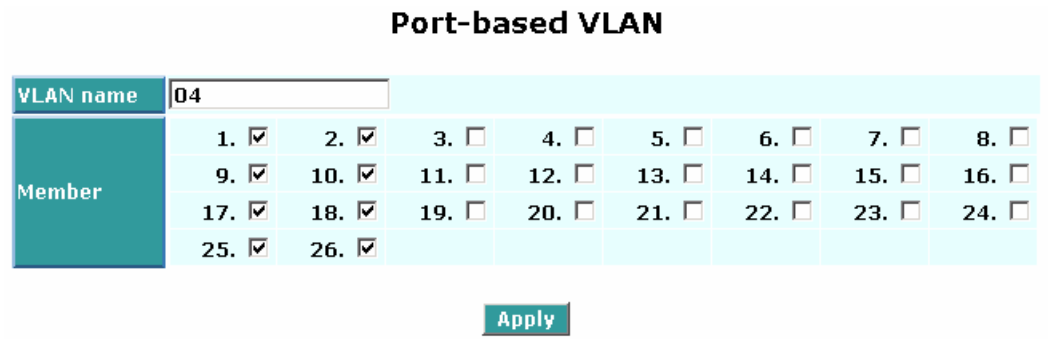
3.9.4 Port-based Group

It shows the information of the existed Port-based VLAN Groups. You can easily create, edit and delete a Port-based VLAN group by pressing Add, Edit and Delete function buttons. User can add a new VLAN group by inputting a new VLAN name.



Parameter description:

- **Add Group:**
  Create a new Port-based VLAN. Input the VLAN name and choose the member by ticking the check box beside the port No., then, press the <Apply> button to have the setting taken effect.
- **Delete Group:**
  Just press the <Delete> button to remove the selected group entry from the Port-based group table.
- **Edit a group:**
  Just select a group entry and press the <Edit> button, then you can modify a group‘s description and member set.



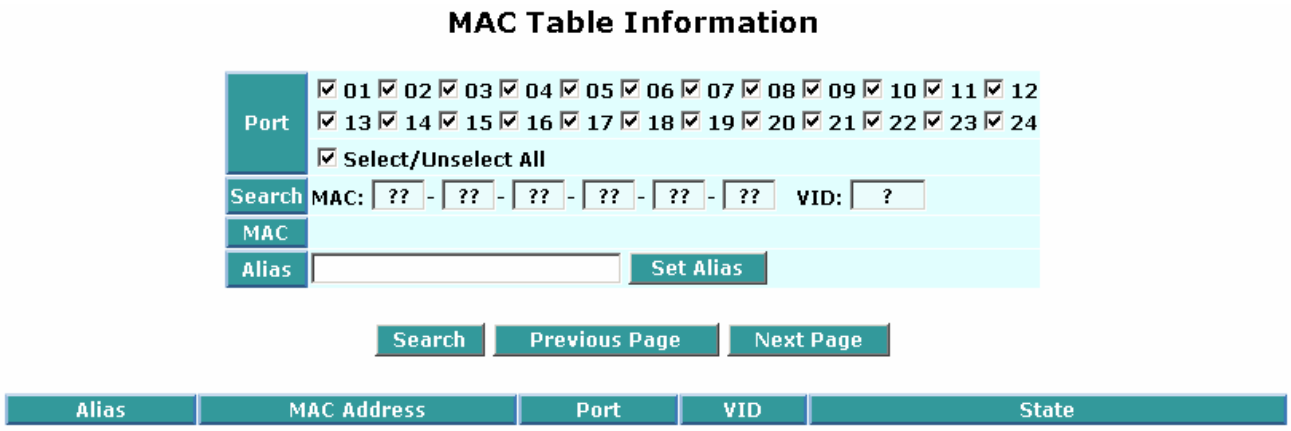
- **VLAN Name:**
  The name defined by administrator is associated with a VLAN group. Valid letters are A-Z, a-z, 0-9, “ - “ and “_” characters. The maximal length is 15 characters.
- **Member:**
  This is used to enable or disable if a port is a member of the new added VLAN, “Enable” means it is a member of the VLAN. Just tick the check box beside the port x to enable it.

3.10 MAC

MAC Table Configuration gathers many functions, including MAC Table Information, MAC Table Maintenance, Static Forward, Static Filter and MAC Alias, which cannot be categorized to some function type.

3.10.1 Information

The function displays the static or dynamic learning MAC entry and the state for the selected port.



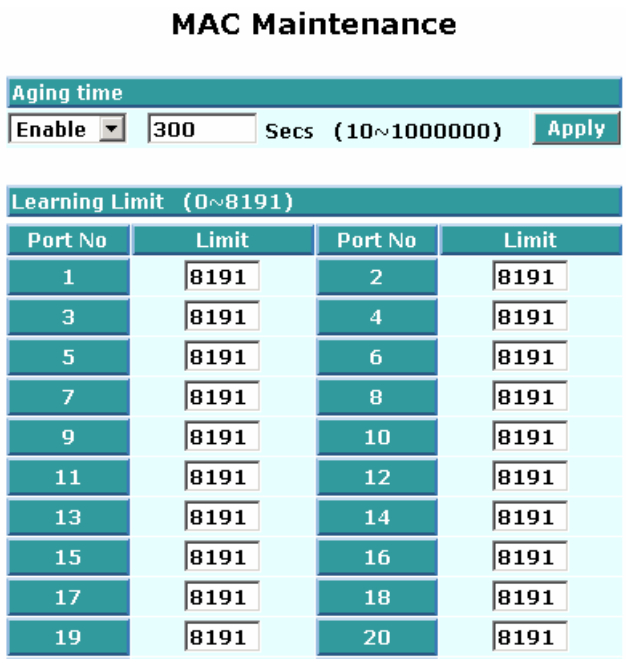
Parameter description:

- **Port:** Select the port you would like to inquire.
- **Search:** Set up the MAC entry you would like to inquire. The default is ??-??-??-??-??-??
- **MAC:** Display the MAC address of one entry you selected from the searched MAC entries table.
- **Alias:** Set up the Alias for the selected MAC entry.
- **Set Alias:** Save the Alias of MAC entry you set up.
- **Search:** Find the entry that meets your setup.
- **Previous Page:** Move to the previous page.
- **Next Page:** Move to the next page.
- **Alias:** The Alias of the searched entry.
- **MAC Address:** The MAC address of the searched entry.
- **Port:** The port that exists in the searched MAC Entry.
- **VID:** VLAN Group that MAC Entry exists.
- **State:** Display the method that this MAC Entry is built. It may show “Dynamic MAC” or “Static MAC”.

3.10.2 Maintenance

This function can allow the user to set up the processing mechanism of MAC Table. An idle MAC address exceeding MAC Address Age-out Time will be removed from the MAC Table. The range of Age-out Time is 10-1000000 seconds, and the setup of this time will have no effect on static MAC addresses.

In addition, the learning limit of MAC maintenance is able to limit the amount of MAC that each port can learn.



Parameter description:

- **Aging Time:**
  Delete a MAC address idling for a period of time from the MAC Table, which will not affect static MAC address. Range of MAC Address Aging Time is 10-1000000 seconds. The default Aging Time is 300 seconds.

- **Learning Limit:**
  This is to set up the maximum amount of MAC that each port can learn. Valid learning limit ranges from 0-8191. As to port 25~port 26, only the fixed value “8192” is assigned to these two ports and user cannot configure this value.

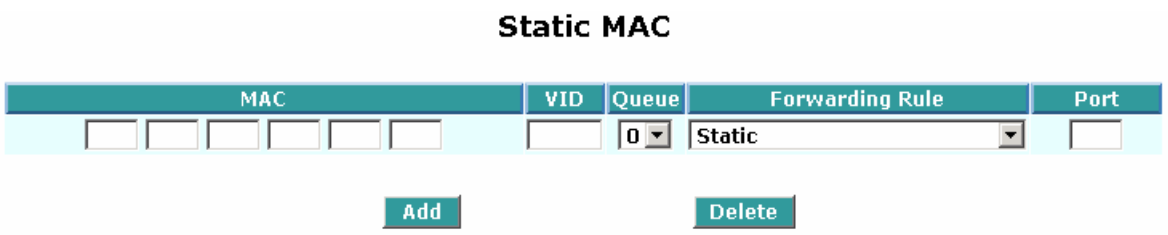
3.10.3 Static

The function of Static is used to configure MAC’s real manners inside of the switch. Three kinds of manners including static, static with destination drop and static with source drop are contained in this function.

As “static” is chosen, assign a MAC address to a specific port, all of the switch’s traffics sent to this MAC address will be forwarded to this port.

As “static with destination drop” is chosen, the packet will be dropped if its DA is equal to the value you set up. Due to this setting belongs to the global one, so, it may affect all ports’ transmission of the packets.

As “static with source drop” is chosen, the packet will be dropped if its SA is equal to the value you set up. Due to this setting belongs to the global one, so, it may affect all ports’ transmission of the packets.



Parameter description:

- **MAC:**
  It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example,

  00 - 40 - C7 - D6 - 00 - 01

- **VID:** VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.
- **Queue (Priority):**

  Set up the priority (0~3) for the MAC.
- **Forwarding Rule(Drop Policy):**

  Static:
  A MAC address is assigned to a specific port, all of the switch's traffics sent to this MAC address will be forwarded to this port.

  Static with Destination Drop:
  While the DA of the incoming packets meets the value you set up, these packets will be dropped.

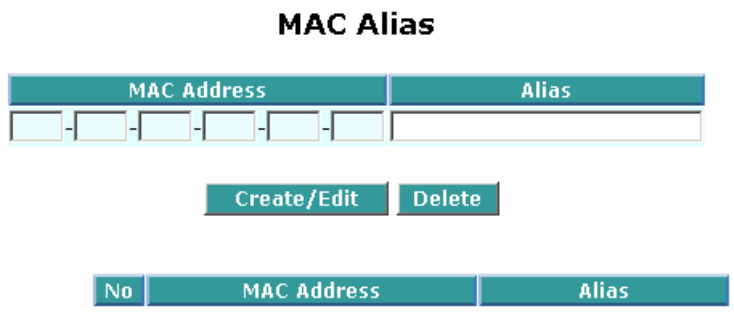
  Static with Source Drop:
  While the SA of the incoming packets meets the value you set up, these packets will be dropped.
- **Port :**

  Select the port No. you would like to do setup in the switch. It is 1 ~26.

3.10.4 MAC Alias

MAC Alias function is used to let you assign MAC address a plain English name. This will help you tell which MAC address belongs to which user in the illegal access report. At the initial time, it shows all pairs of the existed alias name and MAC address.

There are three MAC alias functions in this function folder, including MAC Alias Add, MAC Alias Edit and MAC Alias Delete. You can click <Create/Edit> button to add/modify a new or an existed alias name for a specified MAC address, or mark an existed entry to delete it. Alias name must be composed of A-Z, a-z and 0-9 only and has a maximal length of 15 characters.



In the MAC Alias function, MAC Alias Add/Edit function is used to let you add or modify an association between MAC address and a plain English name. User can click <Create/Edit> button to add a new record with name.

As to MAC Alias Delete function is used to let you remove an alias name to a MAC address. You can select an existed MAC address or alias name to remove.

Parameter description:

- **MAC:**
  It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example,

  00 - 40 - C7 - D6 - 00 - 01
- **Alias:** MAC alias name you assign.

Note: If there are too many MAC addresses learned in the table, we recommend you inputting the MAC

address and alias name directly.

3.11 GVRP

GVRP is an application based on Generic Attribute Registration Protocol (GARP), mainly used to automatically and dynamically maintain the group membership information of the VLANs. The GVRP offers the function providing the VLAN registration service through a GARP application. It makes use of GARP Information Declaration (GID) to maintain the ports associated with their attribute database and GARP Information Propagation (GIP) to communicate among switches and end stations. With GID information and GIP, GVRP state machine maintain the contents of Dynamic VLAN Registration Entries for each VLAN and propagate these information to other GVRP-aware devices to setup and update their knowledge database, the set of VLANs associated with currently active members, and through which ports these members can be reached.

3.11.1 Config

It is used to configure each port's GVRP operation mode, in which there are seven parameters needed to be configured described below.

GVRP Configuration

GVRP State: Enabled | Apply

Port	Join Time	Leave Time	LeaveAll Time	Default Applicant Mode	Default Registrar Mode	Restricted Mode
1	20	60	1000	Normal	Normal	Disabled
2	20	60	1000	Normal	Normal	Disabled
3	20	60	1000	Normal	Normal	Disabled
4	20	60	1000	Normal	Normal	Disabled
5	20	60	1000	Normal	Normal	Disabled
6	20	60	1000	Normal	Normal	Disabled
7	20	60	1000	Normal	Normal	Disabled
8	20	60	1000	Normal	Normal	Disabled
9	20	60	1000	Normal	Normal	Disabled
10	20	60	1000	Normal	Normal	Disabled
11	20	60	1000	Normal	Normal	Disabled
12	20	60	1000	Normal	Normal	Disabled

Parameter description:

- **GVRP State Setting:**
  This function is simply to let you enable or disable GVRP function. You can pull down the list and click the <Downward> arrow key to choose "Enable" or "Disable". Then, click the <Apply> button, the system will take effect immediately.
- **Join Time:**
  Used to declare the Join Time in unit of centi-second. Valid time range: 20 –100 centi-second, Default: 20 centi-second.
- **Leave Time:**
  Used to declare the Leave Time in unit of centi-second. Valid time range: 60 –300 centi-second, Default: 60 cent second.
- **Leave All Time:**
  A time period for announcement that all registered device is going to be de-registered. If someone still issues a new join, then a registration will be kept in the switch. Valid range: 1000-5000 unit time, Default: 1000 unit time.

- **Default Applicant Mode:**
  The mode here means the type of participant. There are two modes, normal participant and non-participant, provided for the user's choice.

- **Normal:**
  It is Normal Participant. In this mode, the switch participates normally in GARP protocol exchanges. The default setting is Normal.

- **Non-Participant:**
  It is Non-Participant. In this mode, the switch does not send or reply any GARP messages. It just listens messages and reacts for the received GVRP BPDU.

- **Default Registrar Mode:**
  The mode here means the type of Registrar. There are three types of parameters for registrar administrative control value, normal registrar, fixed registrar and forbidden registrar, provided for the user's choice.

  Normal:
  It is Normal Registration. The Registrar responds normally to incoming GARP messages. The default setting is Normal.

  Fixed:
  It is Registration Fixed. The Registrar ignores all GARP messages, and all members remain in the registered (IN) state.

  Forbidden:
  It is Registration Forbidden. The Registrar ignores all GARP messages, and all members remain in the unregistered (EMPTY) state.

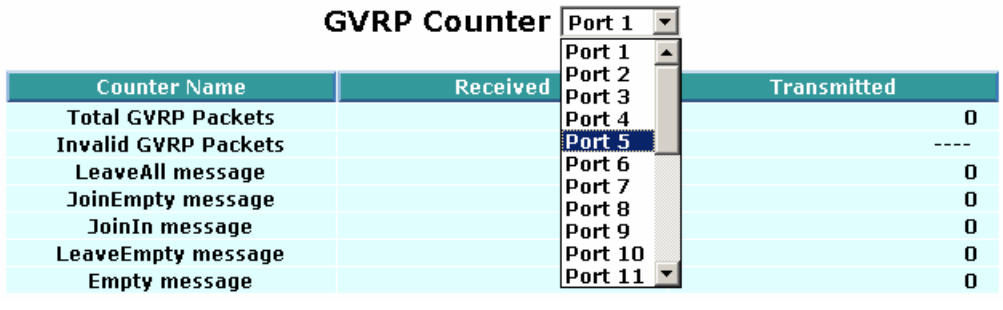
- **Restricted Mode:**
  This function is used to restrict dynamic VLAN be created when this port received GVRP PDU. There are two modes, disable and enable, provided for the user's choice.

  Disabled:
  In this mode, the switch dynamic VLAN will be created when this port received GVRP PDU. The default setting is Normal.

  Enabled:
  In this mode, the switch does not create dynamic VLAN when this port received GVRP PDU. Except received dynamic VLAN message of the GVRP PDU is an existed static VLAN in the switch, this port will be added into the static VLAN members dynamically.

3.11.2 GVRP Counter

All GVRP counters are mainly divided into Received and Transmitted two categories to let you monitor the GVRP actions. Actually, they are GARP packets.



Parameter description:

- **Received:**
  Total GVRP Packets:
  Total GVRP BPDU is received by the GVRP application.

  Invalid GVRP Packets:
  Number of invalid GARP BPDU is received by the GARP application.

  LeaveAll Message Packets:
  Number of GARP BPDU with Leave All message is received by the GARP application.

  JoinEmpty Message Packets:
  Number of GARP BPDU with Join Empty message is received by the GARP application.

  JoinIn Message Packets:
  Number of GARP BPDU with Join In message is received by the GARP application.

  LeaveEmpty Message Packets:
  Number of GARP BPDU with Leave Empty message is received by the GARP application.

  Empty Message Packets:
  Number of GARP BPDU with Empty message is received by the GARP application.

- **Transmitted:**
  Total GVRP Packets:
  Total GARP BPDU is transmitted by the GVRP application.

  Invalid GVRP Packets:
  Number of invalid GARP BPDU is transmitted by the GVRP application.

  LeaveAll Message Packets:
  Number of GARP BPDU with Leave All message is transmitted by the GARP application.

  JoinEmpty Message Packets:
  Number of GARP BPDU with Join Empty message is transmitted by the GARP application.

  JoinIn Message Packets:
  Number of GARP BPDU with Join In message is transmitted by the GARP application.

  LeaveEmpty Message Packets:
  Number of GARP BPDU with Leave Empty message is transmitted by the GARP application.

  Empty Message Packets:
  Number of GARP BPDU with Empty message is transmitted by the GARP application.

3.11.3 Group

It shows the dynamic group member and their information.

Parameter description:

- **VID:**

VLAN identifier. When GVRP group creates, each dynamic VLAN group owns its VID. Valid range is 1 ~ 4094.

- **Member Port:**
  Those are the members belonging to the same dynamic VLAN group.
- **Edit Administrative Control:**
  When you create GVRP group, you can use Administrative Control function to change Applicant Mode and Registrar Mode of GVRP group member.
- **Refresh:**
  Refresh function can help you to see current GVRP group status.

3.12 STP

The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in switched networks. When STP is enabled, ensure that only one path is active between any two nodes on the network at a time. User can enable Spanning Tree Protocol on switch's web management and then set up other advanced items. We recommend that you enable STP on all switches to ensure a single active path on the network.

3.12.1 Status

In the Spanning Tree Status, user can read 12 parameters to know STP current status. The 12 parameters' description is listed in the following table.

STP Status

STP State	Enabled
Bridge ID	00:40:C7:E7:00:07
Bridge Priority	32768
Designated Root	00:40:C7:E7:00:07
Designated Priority	32768
Root Port	0
Root Path Cost	0
Current Max. Age(sec)	20
Current Forward Delay(sec)	15
Hello Time(sec)	2
STP Topology Change Count	0
Time Since Last Topology Change(sec)	89

Parameter description:

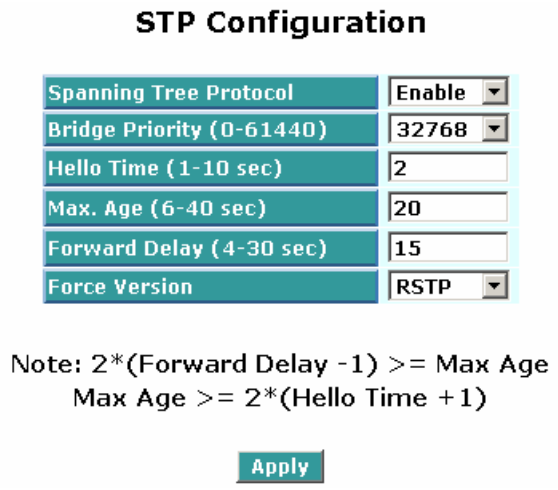
- **STP State:**
  Show the current STP Enabled / Disabled status. Default is "Disabled".
- **Bridge ID:**
  Show switch's bridge ID which stands for the MAC address of this switch.
- **Bridge Priority:**
  Show this switch's current bridge priority setting. Default is 32768.
- **Designated Root:**
  Show root bridge ID of this network segment. If this switch is a root bridge, the "Designated Root" will show this switch's bridge ID.
- **Designated Priority:**

Show the current root bridge priority.

- **Root Port:**
  Show port number connected to root bridge with the lowest path cost.
- **Root Path Cost:**
  Show the path cost between the root port and the designated port of the root bridge.
- **Current Max. Age:**
  Show the current root bridge maximum age time. Maximum age time is used to monitor if STP topology needs to change. When a bridge does not receive a hello message from root bridge until the maximum age time is counted down to 0, the bridge will treat the root bridge malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges. All bridges in the LAN will re-learn and determine which the root bridge is. Maximum Age time is assigned by Root Bridge in unit of seconds. Default is 20 seconds.
- **Current Forward Delay:**
  Show the current root bridge forward delay time. The value of Forward Delay time is set by root. The Forward Delay time is defined as the time spent from Listening state moved to Learning state or from Learning state moved to Forwarding state of a port in bridge.
- **Hello Time:**
  Show the current hello time of the root bridge. Hello time is a time interval specified by root bridge, used to request all other bridges periodically sending hello message every “hello time” seconds to the bridge attached to its designated port.
- **STP Topology Change Count:**
  STP Topology Change Count expresses the time spent in unit of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once the STP change is converged, the Topology Change count will be reset to 0. The figures showing in the screen may not be the exact time it spent but very close to, because the time is eclipsing.
- **Time Since Last Topology Change:**
  Time since Last Topology Change is the accumulated time in unit of seconds the STP has been since the last STP Topology Change was made. When Topology Change is initiated again, this counter will be reset to 0. And it will also count again once STP topology Change is completed.

3.12.2 STP Configuration

User can set the following Spanning Tree parameters to control STP function enable/disable, select mode RSTP/STP and affect STP state machine behavior to send BPDU in this switch. The default setting of Spanning Tree Protocol is “Disable”.



Parameter description:

- **Spanning Tree Protocol:**
  Set 802.1W Rapid STP function Enable / Disable. Default is “Disable”

- **Bridge Priority:**
  The lower the bridge priority is, the higher priority it has. Usually, the bridge with the highest bridge priority is the root. If you want to have the 24 Gigabit L2 managed switch as root bridge, you can set this value lower than that of bridge in the LAN. The valid value is 0 ~ 61440. The default is 32768.

- **Hello Time:**
  Hello Time is used to determine the periodic time to send normal BPDU from designated ports among bridges. It decides how long a bridge should send this message to other bridge to tell I am alive. When the 24 Gigabit L2 managed switch is the root bridge of the LAN, for example, all other bridges will use the hello time assigned by this switch to communicate with each other. The valid value is 1 ~ 10 in unit of second.
  Default is 2 seconds.

- **Max. Age:**
  When the 24 Gigabit L2 managed switch is the root bridge, the whole LAN will apply this figure set by this switch as their maximum age time. When a bridge received a BPDU originated from the root bridge and if the message age conveyed in the BPDU exceeds the Max. Age of the root bridge, the bridge will treat the root bridge malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges. All bridges in the LAN will re-calculate and determine who the root bridge is. The valid value of Max. Age is 6 ~ 40 seconds. Default is 20 seconds.

- **Forward Delay:**
  You can set the root bridge forward delay time. This figure is set by root bridge only. The forward delay time is defined as the time spent from Listening state moved to Learning state and also from Learning state moved to Forwarding state of a port in bridge. The forward delay time contains two states, Listening state to Learning state and Learning state to Forwarding state. It assumes that forward delay time is 15 seconds, then total forward delay time will be 30 seconds. This has much to do with the STP convergent time which will be more than 30 seconds because some other factors.
  The valid value is 4 ~ 30 seconds, default is 15 seconds.

- **Force Version:**
  Two options are offered for the user’s choosing STP algorithm. One is RSTP and the other is STP. If STP is chosen, RSTP will run as a legacy STP. The switch supports RSTP (802.1w) which is backward compatible with STP (802.1d).

3.12.3 STP Port Configuration

In the STP Port Setting, one item selection and five parameters settings are offered for user's setup. User can disable and enable each port by selecting each Port Status item. User also can set "Path Cost" and "Priority" of each port by filling in the desired value and set "Admin Edge Port" and "Admin Point To Point" by selecting the desired item.

STP Port Configuration

Port No	Port Status	Path Cost Status	Configured Path Cost	Priority	Admin Edge Port	Admin Point To Point
1	DISCARDING	2000000	0	128	No	Auto
2	DISCARDING	2000000	0	128	No	Auto
3	DISCARDING	2000000	0	128	No	Auto
4	DISCARDING	2000000	0	128	No	Auto
5	DISCARDING	2000000	0	128	No	Auto
6	DISCARDING	2000000	0	128	No	Auto
7	DISCARDING	2000000	0	128	No	Auto
8	DISCARDING	2000000	0	128	No	Auto
9	DISCARDING	2000000	0	128	No	Auto
10	DISCARDING	2000000	0	128	No	Auto
11	DISCARDING	2000000	0	128	No	Auto
12	DISCARDING	2000000	0	128	No	Auto
13	DISCARDING	2000000	0	128	No	Auto
14	DISCARDING	2000000	0	128	No	Auto
15	FORWARDING	200000	0	128	No	Auto
16	DISCARDING	2000000	0	128	No	Auto

Parameter description:

- **Port Status:**

  It displays the current state of a port. We cannot manually set it because it displays the status only. There are three possible states. (according to 802.1w specification)

  DISCARDING state:

  It indicates that this port can neither forward packets nor contribute learning knowledge.

  Notice: Three other states (Disable state, BLOCKING state and LISTENING state) defined in the 802.1d specification are now all represented as DISCARDING state.

  LEARNING state:

  It indicates this port can now contribute its learning knowledge but cannot forward packets still.

  FORWARDING state:

  It indicates this port can both contribute its learning knowledge and forward packets normally.

- **Path Cost Status:**

  It is the contribution value of the path through this port to Root Bridge. STP algorithm determines a best path to Root Bridge by calculating the sum of path cost contributed by all ports on this path. A port with a smaller path cost value would become the Root Port more possibly.

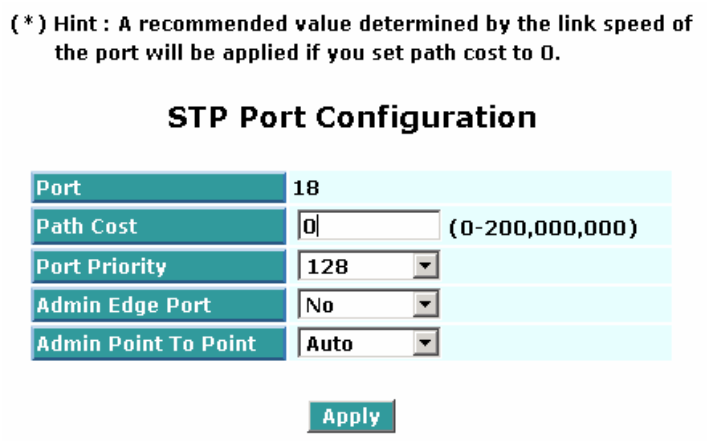
- **Configured Path Cost:**

  The range is 0 - 200,000,000. In the switch, if path cost is set to be zero, the STP will get the recommended value resulted from auto-negotiation of the link accordingly and display this value in the field of Path Cost Status. Otherwise, it may show the value that the administrator set up in Configured Path Cost and Path Cost Status.
  802.1w RSTP recommended value: (Valid range: 1 - 200,000,000)
  10 Mbps: 2,000,000
  100 Mbps: 200,000
  1000 Mbps: 20,000

- **Priority:**
  Priority here means Port Priority. Port Priority and Port Number are mixed to form the Port ID. Port IDs are often compared in order to determine which port of a bridge would become the Root Port. The range is 0 – 240.
  Default is 128.

- **Admin Edge Port:**
  If user selects “Yes”, this port will be an edge port. An Edge Port is a port connected to a device that knows nothing about STP or RSTP. Usually, the connected device is an end station. Edge Ports will immediately transit to forwarding state and skip the listening and learning state because the edge ports cannot create bridging loops in the network. This will expedite the convergence. When the link on the edge port toggles, the STP topology keeps unchanged. Unlike the designate port or root port though, an edge port will transit to a normal spanning-tree port immediately if it receives a BPDU.
  Default: No

- **Admin Point To Point:**
  We say a port is a point-to-point link, from RSTP’s view, if it is in full-duplex mode but is shared link if it is in half-duplex mode. RSTP fast convergence can only happen on point-to-point links and on edge ports. This can expedite the convergence because this will have the port fast transited to forwarding state.
  There are three parameters, Auto, True and False, used to configure the type of the point-to-point link. If configure this parameter to be Auto, it means RSTP will use the duplex mode resulted from the auto-negotiation. In today’s switched networks, most links are running in full-duplex mode. For sure, the result may be half-duplex, in this case, the port will not fast transit to Forwarding state. If it is set as True, the port is treated as point-to-point link by RSTP and unconditionally transited to Forwarding state. If it is set as False, fast transition to Forwarding state will not happen on this port.
  Default: Auto



- **M Check:**
  Migration Check. It forces the port sending out an RSTP BPDU instead of a legacy STP BPDU at the next transmission. The only benefit of this operation is to make the port quickly get back to act as an RSTP port. Click on M Check button to send a RSTP BPDU from the port you specified.

3.13 Trunk

The Port Trunk Configuration is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipments to build

the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port has.
The switch supports two kinds of port trunk methods:

LACP:

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunk method can choose their unique LACP GroupID (1~3) to form a logic “trunk port”. The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a “trunk group” (also called aggregator). LACP is safer than the other trunk method - static trunk.

The switch LACP does not support the followings:

- Link Aggregation across switches
- Aggregation with non-IEEE 802.3 MAC link
- Operating in half-duplex mode
- Aggregate the ports with different data rates

Static Trunk:

Ports using Static Trunk as their trunk method can choose their unique Static GroupID (also 1~3, this Static groupID can be the same with another LACP groupID) to form a logic “trunked port”. The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregate together to form a “logic trunkd port”. Using Static Trunk on both end of a link is strongly recommended. Please also note that low speed links will stay in “not ready” state when using static trunk to aggregate with high speed links.

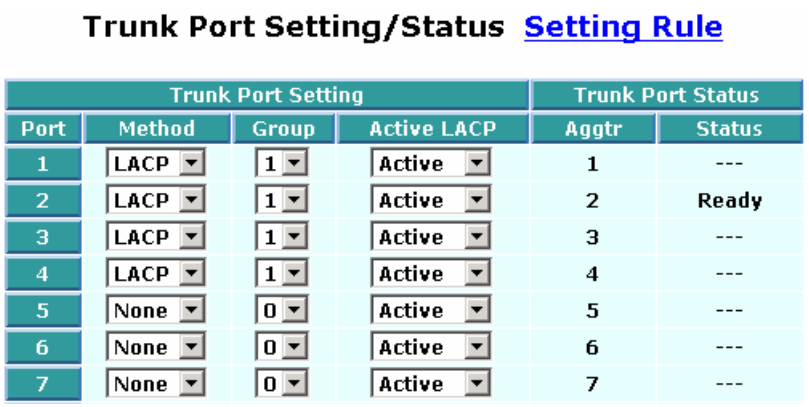
As to system restrictions, the switch supports maximum 3 trunk groups for LACP and additional 3 trunk groups for Static Trunk. But in the system capability view, only 3 “real trunked” groups are supported. An LACP trunk group with more than one ready member-ports is a “real trunked” group. An LACP trunk group with only one or less than one ready member-ports is not a “real trunked” group. Any Static trunk group is a “real trunked” group.

Per Trunk Group supports a maximum of 4 ready member-ports. Please note that some decisions will automatically be made by the system while you are configuring your trunk ports. Trunk Setting Rules are listed below:

1. Maximum 3 groups are allowed
2. The members of each group cannot exceed more than 4 ports
3. Group 1 and 2 cannot exist member 25 and 26 port
4. Group 3 cannot exist member from 1 to 24 ports

3.13.1 Trunk Port Setting / Status

Port setting/status is used to configure the trunk property of each and every port in the switch system.



Parameter description:

- **Method:**

  This determines the method a port uses to aggregate with other ports.

  None:

  A port does not want to aggregate with any other port should choose this default setting.

  LACP:

  A port use LACP as its trunk method to get aggregated with other ports also using LACP.

  Static:

  A port use Static Trunk as its trunk method to get aggregated with other ports also using Static Trunk.

- **Group:**

  Ports choosing the same trunk method other than “None” must be assigned a unique Group number (i.e. Group ID, valid value is from 1 to 8) in order to declare that they wish to aggregate with each other.

- **Active LACP:**

  This field is only referenced when a port’s trunk method is LACP.

  Active:

  An Active LACP port begins to send LACPDU to its link partner right after the LACP protocol entity started to take control of this port.

  Passive:

  A Passive LACP port will not actively send LACPDU out before it receives an LACPDU from its link partner.

- **Aggtr:**

  Aggtr is an abbreviation of “aggregator”. Every port is also an aggregator, and its own aggregator ID is the same as its own Port No. We can regard an aggregator as a representative of a trunk group. Ports with same Group ID and using same trunk method will have the opportunity to aggregate to a particular aggregator port. This aggregator port is usually the port with the smallest Port No. within the trunk group.

- **Status:**

  This field represents the trunk status of a port which uses a trunk method other than “None”. It also represents the management link status of a port which uses the “None” trunk method. “---“ means “not ready”

3.13.2 Aggregator View

To display the current port trunk information from the aggregator point of view.

Aggregator View

Aggregator	Method	Member Ports	Ready Ports
1	LACP	1	
2	LACP	2	
3	LACP	3	
4	LACP	4	
5	LACP	5	
6	LACP	6	
7	LACP	7	
8	LACP	8	
9	LACP	9	
10	LACP	10	
11	LACP	11	
12	LACP	12	
13	None	13	
14	LACP	14	
15	None	15	15
16	None	16	

Parameter description:

- **Aggregator:**
  It shows the aggregator ID (from 1 to 26) of every port. In fact, every port is also an aggregator, and its own aggregator ID is the same as its own Port No.
- **Method:**
  Show the method a port uses to aggregate with other ports.
- **Member Ports:**
  Show all member ports of an aggregator (port).
- **Ready Ports:**
  Show only the ready member ports within an aggregator (port).

Aggregator 10 Information

Actor			Partner	
System Priority	MAC Address		System Priority	MAC Address
32768	00-40-c7-e7-00-07		32768	00-00-00-00-00-00
Port	Key	Trunk Status	Port	Key
10	257	---	10	0

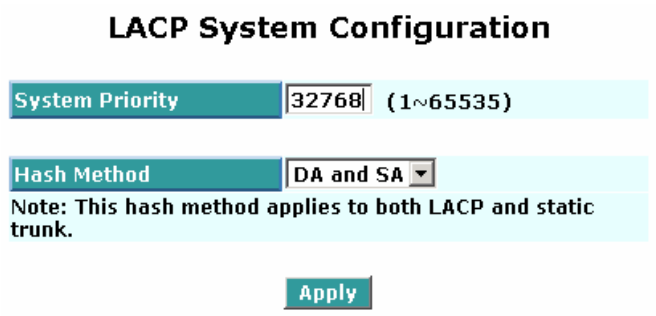
Parameter description:

- **Actor:**
  The switch you are watching on.
- **Partner:**
  The peer system from this aggregator’s view.
- **System Priority:**
  Show the System Priority part of a system ID.
- **MAC Address:**
  Show the MAC Address part of a system ID.
- **Port:**
  Show the port number part of an LACP port ID.

- **Key:**
  Show the key value of the aggregator. The key value is determined by the LACP protocol entity and can't be set through management.
- **Trunk Status:**
  Show the trunk status of a single member port."---" means "not ready"

3.13.3 LACP System Config

It is used to set the priority part of the LACP system ID. LACP will only aggregate together the ports whose peer link partners are all on a single system. Each system supports LACP will be assigned a globally unique System Identifier for this purpose. A system ID is a 64-bit field comprising a 48-bit MAC Address and 16-bit priority value.



Parameter description:

- **System Priority:**
  The System Priority can be set by the user. Its range is from 1 to 65535. Default: 32768.
- **Hash Method:**
  DA+SA, DA and SA are three Hash methods offered for the Link Aggregation of the switch. Packets will decide the path to transmit according to the mode of Hash you choose.

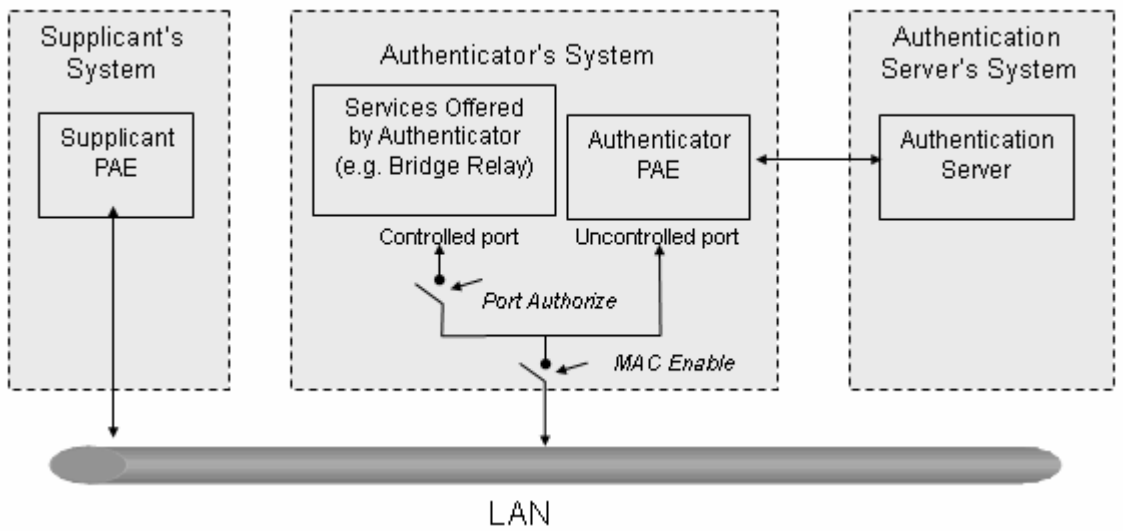
  Default: DA and SA

3.14 802.1x Configuration

802.1x port-based access control provides a method to restrict users to access network resources via authenticating user's information. This restricts users from gaining access to the network resources through a 802.1x-enabled port without authentication. If a user wishes to touch the network through a port under 802.1x control, he (she) must firstly input his (her) account name for authentication and waits for gaining authorization before sending or receiving any packets from a 802.1x-enabled port.

Before the devices or end stations can access the network resources through the ports under 802.1x control, the devices or end stations connected to a controlled port send the authentication request to the authenticator, the authenticator pass the request to the authentication server to authenticate and verify, and the server tell the authenticator if the request get the grant of authorization for the ports.

According to IEEE802.1x, there are three components implemented. They are Authenticator, Supplicant and Authentication server shown below.



Supplicant:

It is an entity being authenticated by an authenticator. It is used to communicate with the Authenticator PAE (Port Access Entity) by exchanging the authentication message when the Authenticator PAE request to it.

Authenticator:

An entity facilitates the authentication of the supplicant entity. It controls the state of the port, authorized or unauthorized, according to the result of authentication message exchanged between it and a supplicant PAE. The authenticator may request the supplicant to re-authenticate itself at a configured time period. Once start re-authenticating the supplicant, the controlled port keeps in the authorized state until re-authentication fails.

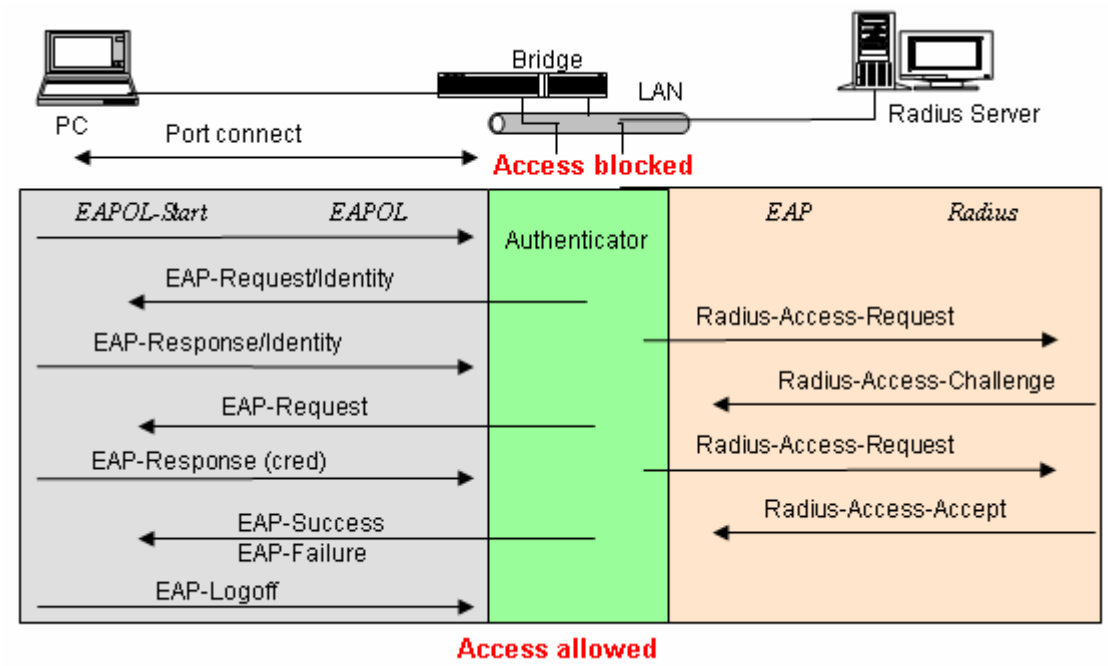
A port acting as an authenticator is thought to be two logical ports, a controlled port and an uncontrolled port. A controlled port can only pass the packets when the authenticator PAE is authorized, and otherwise, an uncontrolled port will unconditionally pass the packets with PAE group MAC address, which has the value of 01-80-c2-00-00-03 and will not be forwarded by MAC bridge, at any time.

Authentication server:

A device provides authentication service, through EAP, to an authenticator by using authentication credentials supplied by the supplicant to determine if the supplicant is authorized to access the network resource.

When Supplicant PAE issues a request to Authenticator PAE, Authenticator and Supplicant exchanges authentication message. Then, Authenticator passes the request to RADIUS server to verify. Finally, RADIUS server replies if the request is granted or denied.

While in the authentication process, the message packets, encapsulated by Extensible Authentication Protocol over LAN (EAPOL), are exchanged between an authenticator PAE and a supplicant PAE. The Authenticator exchanges the message to authentication server using EAP encapsulation. Before successfully authenticating, the supplicant can only touch the authenticator to perform authentication message exchange or access the network from the uncontrolled port.



The figure as above shows the procedure of 802.1x authentication. There are steps for the login based on 802.1x port access control management. The protocol used in the right side is EAPOL and the left side is EAP.

1. At the initial stage, the supplicant A is unauthenticated and a port on switch acting as an authenticator is in unauthorized state. So the access is blocked in this stage.

2. Initiating a session. Either authenticator or supplicant can initiate the message exchange. If supplicant initiates the process, it sends EAPOL-start packet to the authenticator PAE and authenticator will immediately respond EAP-Request/Identity packet.

3. The authenticator always periodically sends EAP-Request/Identity to the supplicant for requesting the identity it wants to be authenticated.

4. If the authenticator doesn’t send EAP-Request/Identity, the supplicant will initiate EAPOL-Start the process by sending to the authenticator.

5. And next, the Supplicant replies an EAP-Response/Identity to the authenticator. The authenticator will embed the user ID into Radius-Access-Request command and send it to the authentication server for confirming its identity.

6. After receiving the Radius-Access-Request, the authentication server sends Radius-Access-Challenge to the supplicant for asking for inputting user password via the authenticator PAE.

7. The supplicant will convert user password into the credential information, perhaps, in MD5 format and replies an EAP-Response with this credential information as well as the specified authentication algorithm (MD5 or OTP) to Authentication server via the authenticator PAE. As per the value of the type field in message PDU, the authentication server knows which algorithm should be applied to authenticate the credential information, EAP-MD5 (Message Digest 5) or EAP-OTP (One Time Password) or other else algorithm.

8. If user ID and password is correct, the authentication server will send a Radius-Access-Accept to the authenticator. If not correct, the authentication server will send a Radius-Access-Reject.

9. When the authenticator PAE receives a Radius-Access-Accept, it will send an EAP-Success to the supplicant. At this time, the supplicant is authorized and the port connected to the supplicant and under 802.1x control is in the authorized state. The supplicant and other devices connected to this port can access the network. If the authenticator receives a Radius-Access-Reject, it will send an EAP-Failure to the supplicant. This means the supplicant is failed to authenticate. The port it

connected is in the unauthorized state, the supplicant and the devices connected to this port won't be allowed to access the network.

10. When the supplicant issue an EAP-Logoff message to Authentication server, the port you are using is set to be unauthorized.

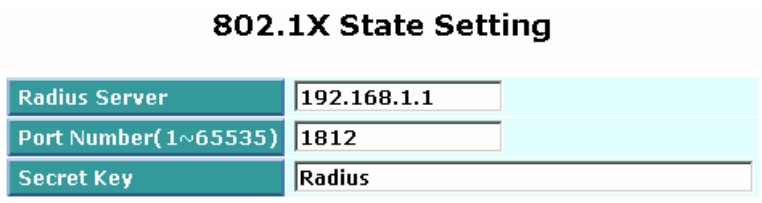
Only MultiHost 802.1X is the type of authentication supported in the switch. In this mode, for the devices connected to this port, once a supplicant is authorized, the devices connected to this port can access the network resource through this port.

802.1x Port-based Network Access Control function supported by the switch is little bit complex, for it just support basic Multihost mode, which can distinguish the device's MAC address and VID. The following table is the summary of the combination of the authentication status and the port status versus the status of port mode, set in 802.1x Port mode, port control state, set in 802.1x port setting. Here Entry Authorized means MAC entry is authorized.

Port Mode	Port Control	Authentication	Port Status
Disable	Don't Care	Don't Care	Port Uncontrolled
Multihost	Auto	Successful	Port Authorized
Multihost	Auto	Failure	Port Unauthorized
Multihost	Force Unauthorized	Don't Care	Port Unauthorized
Multihost	Force Authorized	Don't Care	Port Authorized

3.14.1 State

This function is used to configure the global parameters for RADIUS authentication in 802.1x port security application.



Parameter description:

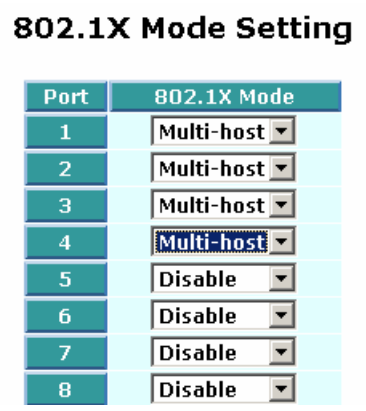
- **Radius Server:**
  RADIUS server IP address for authentication.
  Default: 192.168.1.1

- **Port Number:**
  The port number to communicate with RADIUS server for the authentication service. The valid value ranges 1-65535.
  Default port number is 1812.

- **Secret Key:**
  The secret key between authentication server and authenticator. It is a string with the length 1 – 31 characters. The character string may contain upper case, lower case and 0-9. It is character sense. It is not allowed for putting a blank between any two characters.
  Default: Radius

3.14.2 Mode

Set the operation mode of 802.1X for each port. In this device, it supports only Multi-host operation mode.



Parameter description:

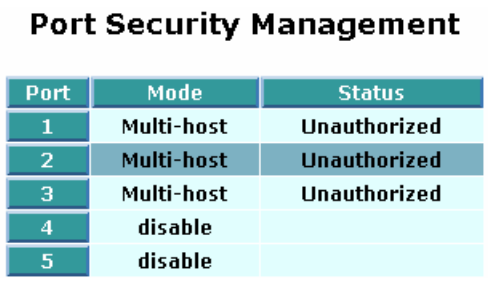
- **Port Number:**
  Indicate which port is selected to configure the 802.1x operation mode.
- **802.1x Mode:**
  802.1x operation mode. There are two options, including Disable and Multi-host mode. Default is Disable.

  Disable:
  It will have the chosen port acting as a plain port, that means no 802.1x port access control working on the port.

  802.1x with Multi-host:
  In Multi-host mode, for the devices connected to this port, once a supplicant is authorized, the devices connected to this port can access the network resource through this port.

3.14.3 Security

Shows each port status and configure the parameters for each port in 802.1x port security application. In Multihost mode, it shows the port number and its status, authorized or unauthorized.

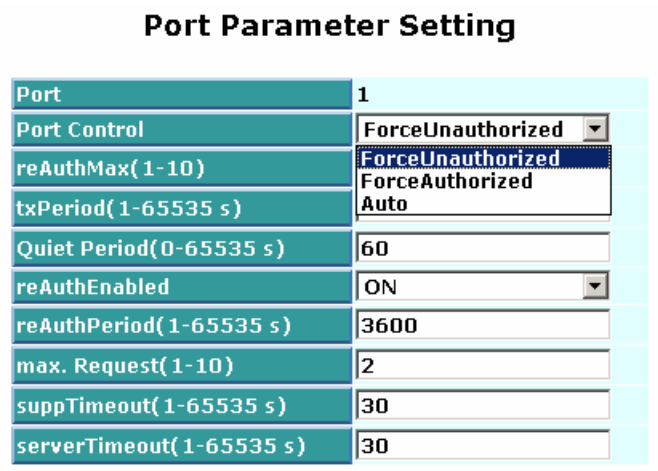


Parameter description:

- **Disable Mode:**
  When selecting Disable mode for a port in the function 802.1X Port Mode Configuration, the port is in the uncontrolled port state and does not apply 802.1X authenticator on it. Any node attached on this port can access the network without the admittance of 802.1X authenticator. The Port Status will show the following screen.
- **Port Number:**
  The port number to be chosen to show its 802.1X Port Status. The valid number is Port 1 – 24.
- **Port Status:**

The current 802.1X status of the port. In Disable mode, this field is Disabled.

- **802.1x with Multihost mode:**
  When selecting 802.1x with Multihost mode for a port in the function 802.1X Port Mode Configuration, Devices can access the network through this port once the authenticator is authorized. The Port Status will show the following screen. If the port is granted to access the network, the port status is authorized, otherwise, unauthorized.



Parameter description:

- **Port:**
  It is the port number to be selected for configuring its associated 802.1x parameters which are Port control, reAuthMax, txPeriod, Quiet Period, reAuthEnabled, reAuthPeriod, max. Request, suppTimeout, serverTimeout and Controlled direction.

- **Port Control:**
  This is used to set the operation mode of authorization. There are three type of operation mode supported, ForceUnauthorized, ForceAuthorized, Auto.

  ForceUnauthorized:
  The controlled port is forced to hold in the unauthorized state.

  ForceAuthorized:
  The controlled port is forced to hold in the authorized state.

  Auto:
  The controlled port is set to be in authorized state or unauthorized state depends on the result of the authentication exchange between the authentication server and the supplicant.

  Default: Auto

- **reAuthMax(1-10):**
  The number of authentication attempt that is permitted before the port becomes unauthorized.

  Default: 2

- **txPeriod(1-65535 s):**
  A time period to transmitted EAPOL PDU between the authenticator and the supplicant.

  Default: 30

- **Quiet Period(0-65535 s):**
  A period of time during which we will not attempt to access the supplicant.

  Deafult: 60 seconds

- **reAuthEnabled:**

Choose whether regular authentication will take place in this port.

Default: ON

- **reAuthPeriod(1-65535 s):**
  A non-zero number seconds between the periodic re-authentication of the supplicant.

  Default: 3600

- **max. Request(1-10):**
  The maximum of number times that the authenticator will retransmit an EAP Request to the supplicant before it times out the authentication session. The valid range: 1 – 10.

  Default: 2 times

- **suppTimeout(1-65535 s):**
  A timeout condition in the exchange between the authenticator and the supplicant. The valid range: 1 –65535.

  Default: 30 seconds.

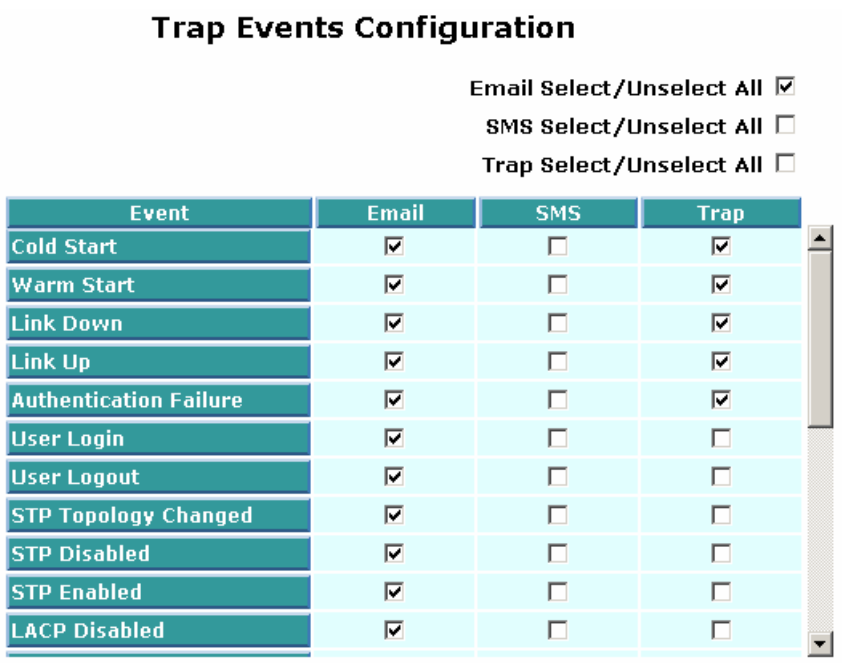
- **serverTimeout(1-65535 s):**
  A timeout condition in the exchange between the authenticator and the authentication server. The valid range: 1 –65535.

  Default: 30 seconds

3.15 Alarm

3.15.1 Event

The Trap Events Configuration function is used to enable the switch to send out the trap information while pre-defined trap events occurred. The switch offers 24 different trap events to users for switch management. The trap information can be sent out in three ways, including email, mobile phone SMS (short message system) and trap. The message will be sent while users tick (☑) the trap event individually on the web page shown as below.



Parameter description:

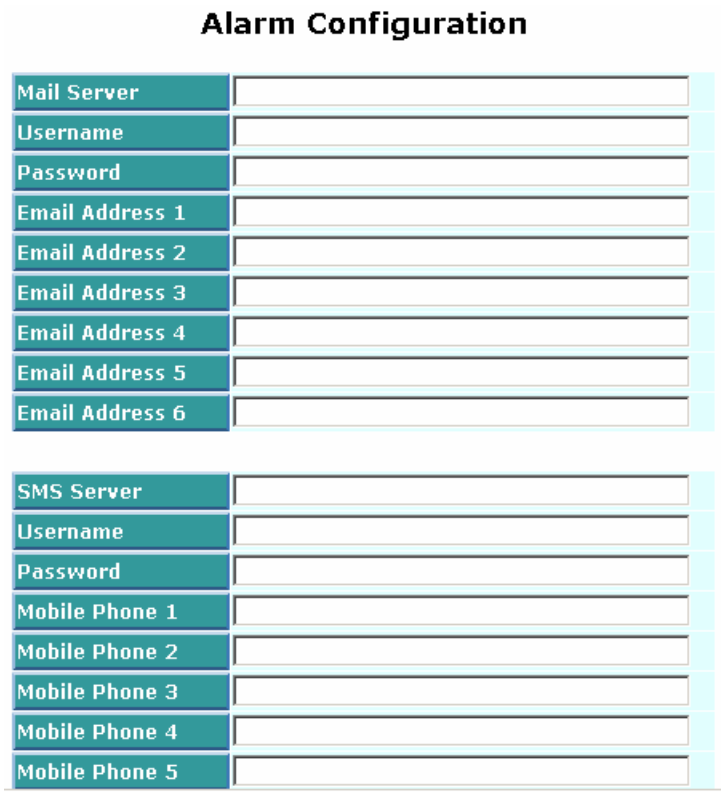
These trap functions are as they describe. The special one is Module Swap. It means that when the switch detects a module with the different module ID to be inserted, the switch treats it as Module swapped. The traps that the switch supports are listed below.

- **STP:** STP Topology Change, STP Disabled, STP Enabled
- **LACP:** LACP Disabled, LACP Enabled, LACP Member Added, LACP Port Failure
- **GVRP:** GVRP Disabled, GVRP Enabled
- **VLAN:** VLAN Disabled, Port-based VLAN Enable, Tag-based VLAN, Enable, Metro-mode VLAN Enabled, Double-tag VLAN Enabled
- **Module Swap:** SEP Inserted, SEP Removed, Dual-media Swapped
- **Trap:** Cold Start, Warm Start, Link Down, Link Up, Authentication Failure, User login, User logout

3.15.2 Email/SMS

Alarm configuration is used to configure the persons who should receive the alarm message via either email or SMS, or both. It depends on your settings. An email address or a mobile phone number has to be set in the web page of alarm configuration. Then, user can read the trap information from the email or the mobile phone. This function provides 6 email addresses and 6 mobile phone numbers at most. The 24 different trap events will be sent out to SNMP Manager when trap event occurs. After ticking trap events, you can fill in your desired email addresses and mobile phone numbers. Then, please click <Apply> button to complete the alarm configuration. It will take effect in a few seconds.

Note: SMS may not work in your mobile phone system. It is customized for different systems.



Parameter description:

- **Email:**
  - **Mail Server:** the IP address of the server transferring your email.

- **Username:** your username on the mail server.
- **Password:** your password on the mail server.
- **Email Address 1 – 6:** Email address that would like to receive the alarm message.

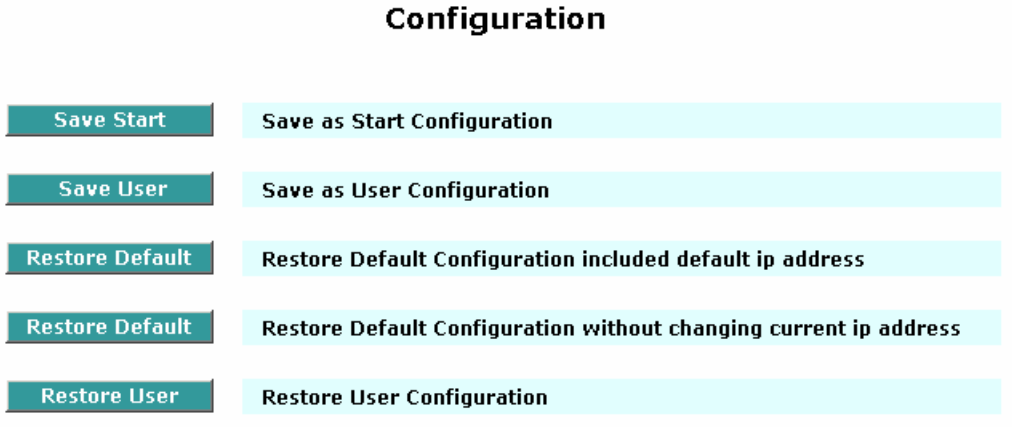
- **SMS:**
  - **SMS Server:** the IP address of the server transferring your SMS.
  - **Username:** your username in ISP.
  - **Password:** your username in ISP.
  - **Mobile Phone 1-6:** the mobile phone number that would like to receive the alarm message.

3.16 Configuration

The switch supports three copies of configuration, including the default configuration, working configuration and user configuration for your configuration management. All of them are listed and described below respectively.

- Default Configuration:
  This is the ex-factory setting and cannot be altered.
- Working Configuration:
  It is the configuration you are using currently and can be changed any time. The configurations you are using are saved into this configuration file. This is updated each time as you press <Apply> button.
- User Configuration:
  It is the configuration file for the specified or backup purposes and can be updated while having confirmed the configuration. You can retrieve it by performing Restore User Configuration.

3.16.1 Save/Restore



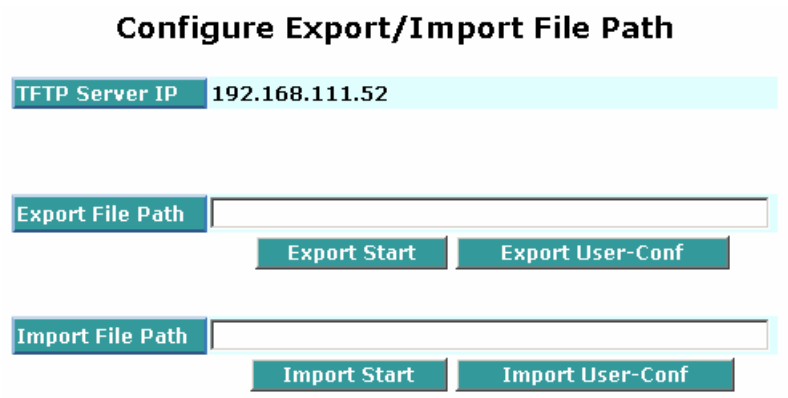
Parameter description:

- **Save Start:** Save the current configuration as a start configuration file in flash memory.
- **Save User:** Save the current configuration as a user configuration file in flash memory.
- **Restore Default/Default IP address:** Retrieve the ex-factory setting, including default IP address, to replace the start configuration.
- **Restore Default:** Retrieve the ex-factory setting, without changing current default IP address, to replace the start configuration.

- **Restore User:** Retrieve the previous confirmed working configuration stored in the flash memory to update start configuration. When completing to restore the configuration, the system's start configuration is updated and will be changed its system settings after rebooting the system.

3.16.2 Config File

User can back up or reload the config files of Save As Start or Save As User via TFTP.



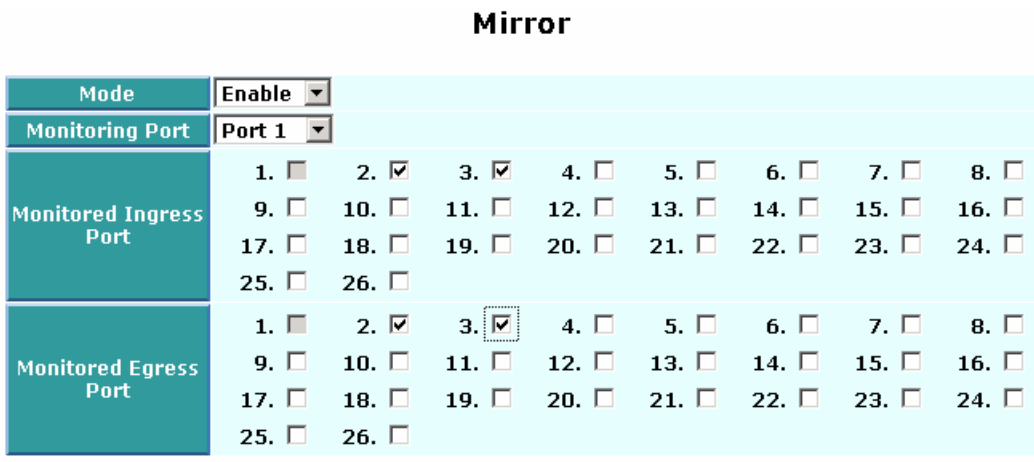
Parameter description:

- **Export File Path:**
  - **Export Start:** Export Save As Start's config file stored in the flash.
  - **Export User-Conf:** Export Save As User's config file stored in the flash.
- **Import File Path:**
  - **Import Start:** Import Save As Start's config file stored in the flash.
  - **Import User-Conf:** Import Save As User's config file stored in the flash.

3.17 Security

3.17.1 Mirror

Mirror Configuration is to monitor the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.

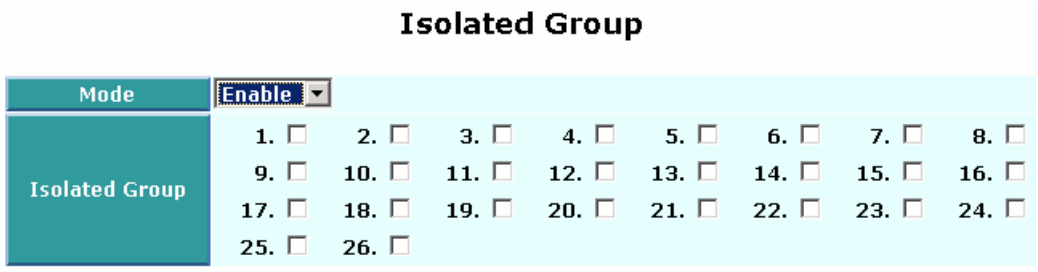


Parameter description:

- **Mode:** Used for the activation or de-activation of Port Mirror function. Default is disabled.
- **Monitoring Port:** Set up the port for monitoring. Valid port is Port 1~26 and default is Port 1.
- **Monitored Ingress Port:** Set up the port for being monitored. It only monitors the packets received by the port you set up. Just tick the check box (☑) beside the port x and valid port is Port 1~26.
- **Monitored Egress Port:** Set up the port for being monitored. It only monitors the packets transmitted by the port you set up. Just tick the check box (☑) beside the port x and valid port is Port 1~26.

3.17.2 Isolated Group

Isolated Group function can let the port be independent of other ports in the isolated group, and the communication is also forbidden between these ports. But, the ports of the isolated group are still able to communicate with the ports of the non-Isolated group. With this design, it will be helpful to the administrator to immediately find and solve the port that results in the occurrence of looping problems in the network.

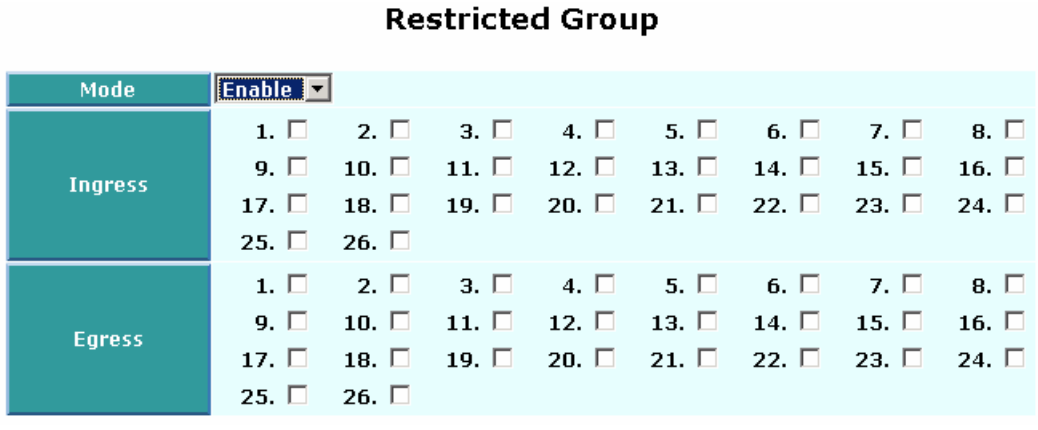


Parameter description:

- **Mode:** Used for the activation or de-activation of Isolated Group function. Default is disabled.
- **Isolated Group:** User can choose any port to be the member of this group. Just tick the check box ( ) beside the port x and valid port is Port 1~26. In this group, all of these member ports cannot forward packets with each other. Thus, the switch will not be capable of forwarding any packets in case its all ports become the members of the isolated group.

3.17.3 Restricted Group

The function of the Restricted Group can decide the direction of transmitting packets for the specific port. The packets received by the port with the “Ingress” mode of Restricted Group will be sent to the ports with the “Egress” mode of Restricted Group.



Parameter description:

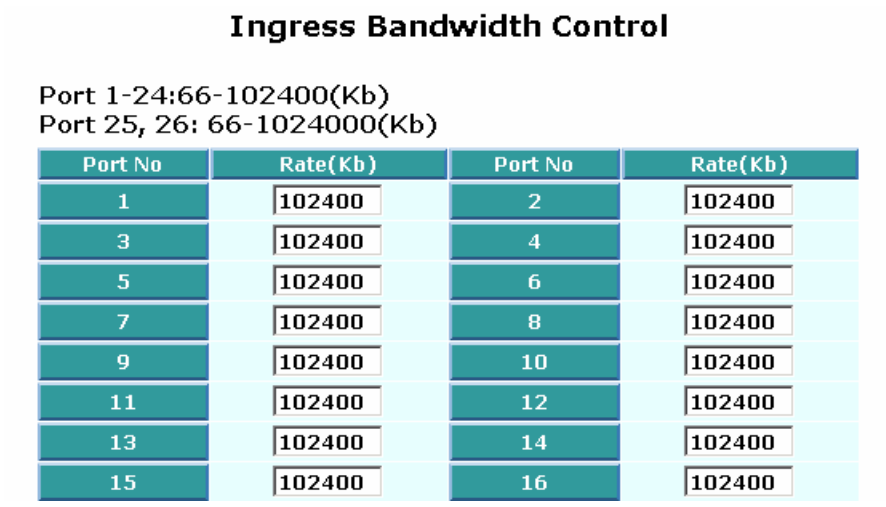
- **Mode:** Used for the activation or de-activation of Restricted Group function. Default is disabled.
- **Ingress:** Select the ports that you would like their Restricted Group to set into “Ingress” mode. Just tick the check box beside the port x and valid port is Port 1~26.

- **Egress:** Select the ports that you would like their Restricted Group to set into “Egress” mode. Just tick the check box beside the port x and valid port is Port 1~26.

3.18 Bandwidth

3.18.1 Ingress

Ingress Bandwidth setting function is used to set up the limit of Ingress bandwidth for each port.

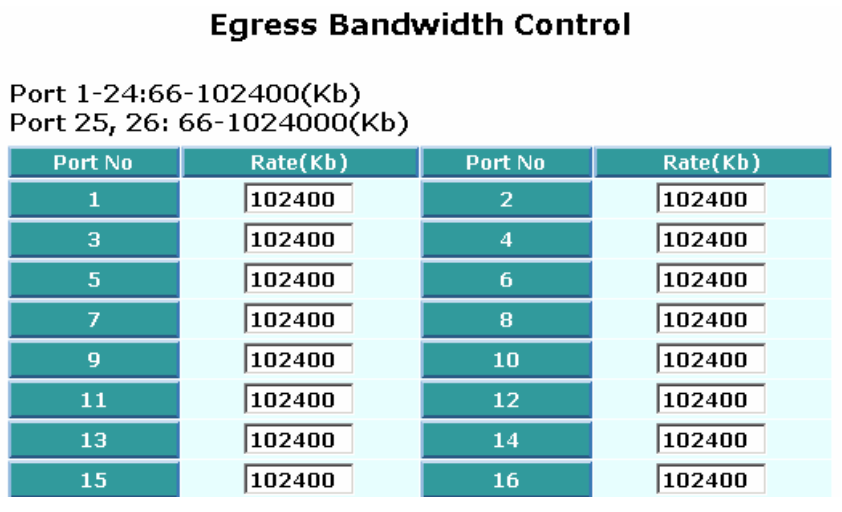


Parameter description:

- **Port No.:** Choose the port that you would like this function to work on it. Valid range of the port is 1~26.
- **Rate:** Set up the limit of Ingress bandwidth for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~24 ranges from 66~102400, and Port 25~26 ranges from 66~1024000 with the minimum unit of 1. Default value of Port 1~24 is 102400 and Port 25~26 is 1024000.

3.18.2 Egress

Egress Bandwidth Setting function is used to set up the limit of Egress bandwidth for each port.

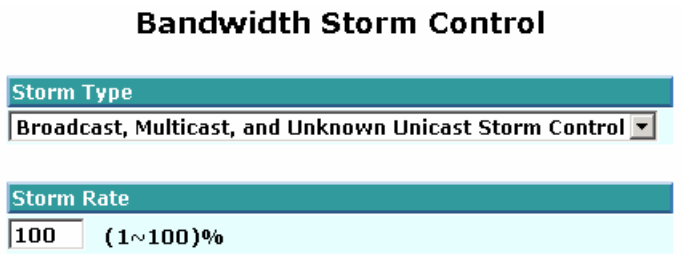


Parameter description:

- **Port No.:** Choose the port that you would like this function to work on it. Valid range of the port is 1~26.
- **Rate:** Set up the limit of Egress bandwidth for the port you choose. Packet transmission will be delayed if the rate exceeds the value you set up in Data Rate field. Traffic may be lost if egress buffers run full. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~24 ranges from 66~102400, and Port 25~26 ranges from 66~1024000 with the minimum unit of 1. Default value of Port 1~24 is 102400 and Port 25~26 is 1024000.

3.18.3 Storm

Bandwidth Management function is used to set up the limit of Ingress and Egress bandwidth for each port.



Parameter description:

- **Storm Type:**

  Disable:

  Disable the function of the bandwidth storm control.

  Broadcast Storm Control:

  Enable the function of bandwidth storm control for broadcast packets.

  Multicast Storm Control:

  Enable the function of bandwidth storm control for multicast packets.

  Unknown Unicast Storm Control:

  Enable the function of bandwidth storm control for unknown unicast packets. These packets are the MAC address that had not completed the learning process yet.

  Broadcast, Multicast, Unknown Unicast Storm Control:

  Enable the function of bandwidth storm control for all packets in transmission.

- **Storm Rate :**

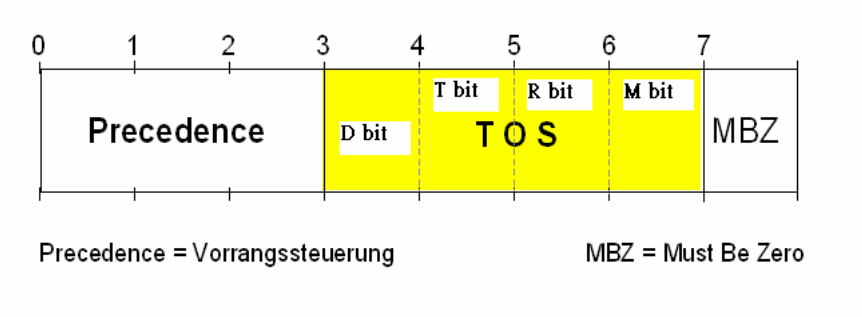
  Set up the limit of bandwidth for storm type you choose. Valid value of the storm rate ranges from 1-100 with the minimum unit of 1. And only integer is acceptable. Default is 100.

3.19 QoS

The switch supports 5 kinds of QoS, are as follows, MAC Priority, 802.1p Priority, IP TOS Priority, and DiffServ DSCP Priority. Port Based Priority has a special name called VIP Port in the switch. Any packets enter VIP Port will have highest transmitting priority. MAC Priority act on the destination address of MAC in packets. VLAN tagged Priority field is affected by 802.1p Priority setting. IP TOS Priority affects TOS fields of IP header, and you can find it has 8-bit SERVICE TYPE field that specifies how the datagram should be handled. The field could be divided into six subfields as follows, PRECEDENCE (3 bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1bit), R-Type (Reliability Priority, 1bit), M-Type (Monetary Cost Priority, 1bit), and

UNUSED (1bit).

User can randomly control these fields to achieve some special QoS goals. When bits D, T, R, or M set, the D bit requests low delay, the T bit requests high throughput, the R bit requests high reliability, and the M bit requests low cost.



DiffServ DSCP Priority act on DSCP field of IP Header. In the late 1990s, the IETF redefined the meaning of the 8-bit SERVICE TYPE field to accommodate a set of differentiated services (DS). Under the differentiated services interpretation, the first six bits comprise a codepoint, which is sometimes abbreviated DSCP, and the last two bits are left unused.

High Priority Packet streams will experience less delay into the switch. For handing different priority packets, each egress port has designed up to 4 queues. Each QoS is influenced by two scheduling, WRR (Weighted Round Robin) and Strict Priority as well. When you finish setting the priority mapping to the queue, WRR scheduling will distribute the bandwidth according to the weight you set for 4 queues (queue 0 to queue 3). Another scheduling is Strict Priority dedicated for the function named VIP Port of QoS. While we select some ports as the VIP Port, these ports will own the highest transmitting priority in egress queue of the switch.

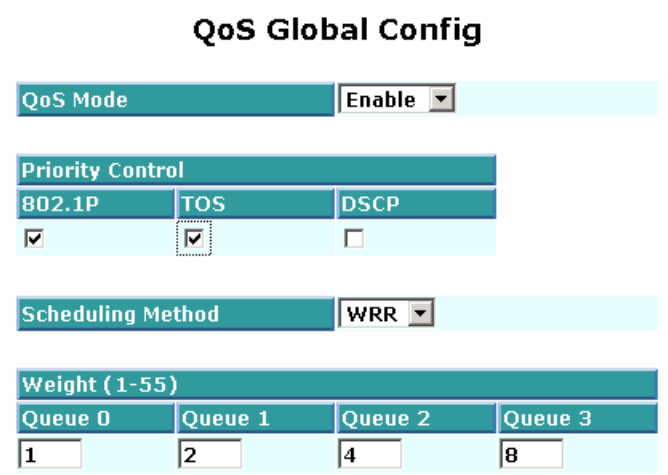
The QoS functions as we mentioned above are able to enable at the same time. But, the following precedence will decide whether these functions work or not.

- Enable both VIP and TOS --- Choose priorities of VIP and TOS.
- Enable both VIP and DSCP --- Choose priorities of VIP and DSCP.
- Enable both TOS and DSCP --- Choose "DSCP".
- Enable both VIP and DSCP --- Choose priorities of VIP and DSCP.
- Enable both 802.1p and TOS --- Choose "TOS".
- Enable both 802.1p and DSCP --- Choose "DSCP".
- Enable both 802.1p and DSCP and TOS --- Choose "DSCP".
- Enable both 802.1p and DSCP and TOS and VIP --- Choose priorities of VIP and DSCP.

** VIP/DSCP > TOS > 802.1p (Final result)

3.19.1 Global

When you want to use QoS function, please enable QoS Mode in advance. Then you can use MAC Priority, 802.1p Priority, IP TOS Priority, DiffServ DSCP Priority, or VIP Port functions and take effect. In this function, you can Enable QoS Mode. Choose any of Priority Control, such as 802.1p, TOS, DSCP. Moreover, you can select Scheduling Method of WRR (Weighted Round Robin) or Strict Priority. Next, you can arrange Weight values for queue 0 to queue 3.

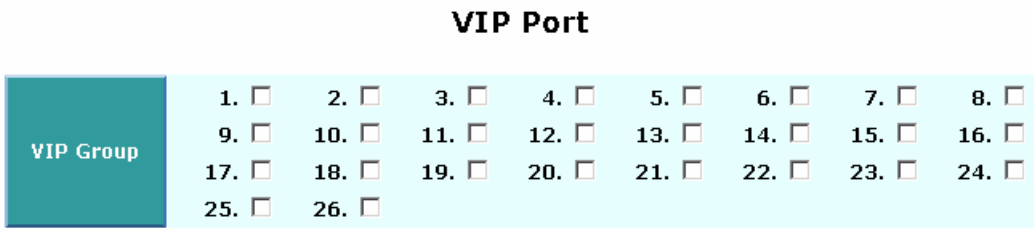


Parameter description:

- **QoS Mode:** You can Enable QoS Mode and let QoS function become effective. Default is disabled.
- **Priority Control:** Just tick the check box (☑) of 802.1P, TOS, or DSCP Qos and click Apply button to be in operation.
- **Scheduling Method:** There are two Scheduling Method, WRR and Strict Priority. Default is WRR. After you choose any of Scheduling Method, please click Apply button to be in operation.
- **Weight (1~55):** Over here, you can make an arrangement to Weight values of Queue 0 to Queue 3. The range of Weight you can set is 1~55. In default, the weight of Queue 0 is 1, the weight of Queue 1 is 2, the weight of Queue 2 is 4, and the weight of Queue 3 is 8.

3.19.2 VIP

When the port is set as VIP Port, the packets enter this port and will have highest transmitting priority. For example, as you choose port 2 is VIP Port, simultaneously transmit packets from port 2 and port 3 to port 1 at speed of 100MB and let congestion happen. The packets for port 3 will be dropped because the packets from port 2 own highest precedence. For the sake of this function taking effect, you must choose Scheduling Method of Strict Priority ahead.



Parameter description:

- **VIP Port:** Just tick the check box (☑) to select any port (port 1~26) as the VIP Port. Then, click the Apply button to have the setting taken effect.

3.19.3 802.1p

This function will affect the priority of VLAN tag. Based on priority of VLAN tag, it can arrange 0~8 priorities, priorities can map to 4 queues of the switch (queue 0~3) and possess different bandwidth distribution according to your weight setting.

Each Priority can select any of Queue 0 ~ Queue 3. In Default, Priority 0 is mapping to Queue 0, Priority 1 is mapping to Queue 0, Priority 2 is mapping to Queue 1, Priority 3 is mapping to Queue 1, Priority 4 is mapping to Queue 2, Priority 5 is mapping to Queue 2, Priority 6 is mapping to Queue 3, and Priority 0 is mapping to

Queue 3.

802.1p Priority Mapping

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

Apply

3.19.4 D/T/R/M - Type ToS

IP TOS Priority affect TOS fields of IP header, you can find it has 8-bit SERVICE TYPE field that specifies how the datagram should be handled. The field could be divided into six subfields as follows, PRECEDENCE (3 bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1bit), R-Type (Reliability Priority, 1bit), M-Type (Monetary Cost Priority, 1bit), and UNUSED. PRECEDENCE 3-bits can arrange 8 kinds of priorities corresponding to the 0~7 priority in the following priority diagram.

TOS Delay Priority Mapping works while D-TYPE in TOS field of IP header of the packets received by the switch is configured.

TOS Delay Priority Mapping

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

Apply

TOS Throughput Priority Mapping works while T-TYPE in TOS field of IP header of the packets received by the switch is configured.

TOS Throughput Priority Mapping

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

Apply

TOS Reliability Priority Mapping works while R-TYPE in TOS field of IP header of the packets received by the switch is configured.

TOS Reliability Priority Mapping

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

Apply

TOS Monetary Cost Priority Mapping works while M-TYPE in TOS field of IP header of the packets received by the switch is configured.

TOS Monetary Cost Priority Mapping

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

Apply

3.19.5 DSCP

In the late 1990s, the IETF redefined the meaning of the 8-bit SERVICE TYPE field to accommodate a set of differentiated services (DS). Under the differentiated services interpretation, the first six bits comprise a codepoint, which is sometimes abbreviated DSCP, and the last two bits are left unused.

DSCP can form total 64 (0~63) kinds of Traffic Class based on the arrangement of 6-bit field in DSCP of the IP packet. In the switch, user is allowed to set up these 64 kinds of Class that belong to any of queue 0~3.

DSCP Priority Mapping

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

64 kinds of priority traffic as mentioned above, user can set up any of Queue 0~3. In default, Priority 0~15 are

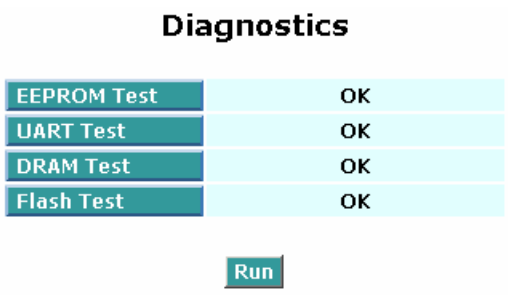
mapping to Queue 0, Priority 16~31 are mapping to Queue 1, Priority 32~47 are mapping to Queue 0, Priority 48~63 are mapping to Queue 0.

3.20 Diagnostics

Three functions, including Diagnostics, Loopback Test and Ping Test are contained in this function folder for device self-diagnostics. Each of them will be described in detail orderly in the following sections.

3.20.1 Diagnostics

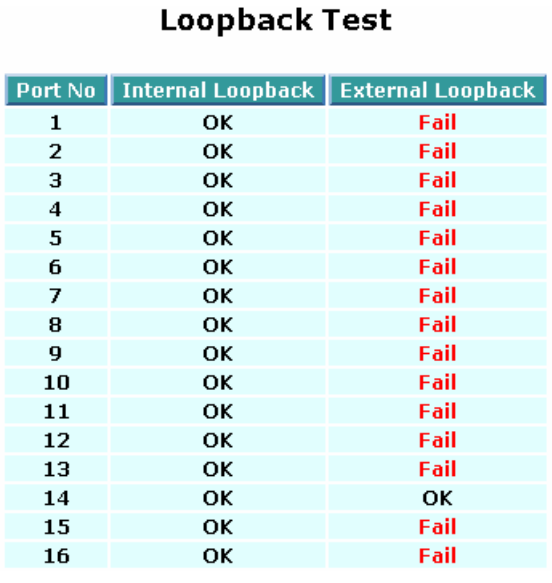
Diagnostics function provides a set of basic system diagnosis. It let users know that whether the system is health or needs to be fixed. The basic system check includes EEPROM test, UART test, DRAM test and Flash test.



3.20.2 Loopback Test

In the Loopback Test function, there are two different loopback tests. One is Internal Loopback Test and the other is External Loopback Test. The former test function will not send the test signal outside the switch box. The test signal only wraps around in the switch box. As to the latter test function, it will send the test signal to its link partner. If you do not have them connected to active network devices, i.e. the ports are link down, the switch will report the port numbers failed. If they all are ok, it just shows OK.

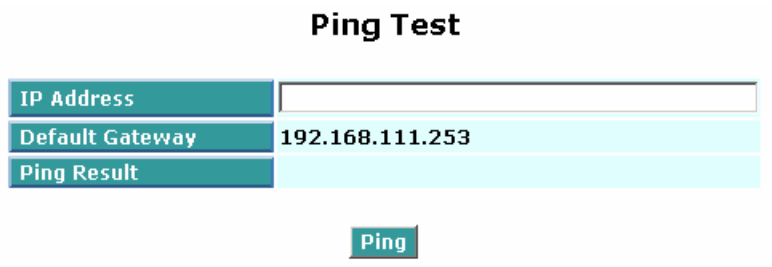
Note: Whatever you choose Internal Loopback Test or External Loopback Test, these two functions will interfere with the normal system working, and all packets in sending and receiving also will stop temporarily.



3.20.3 Ping

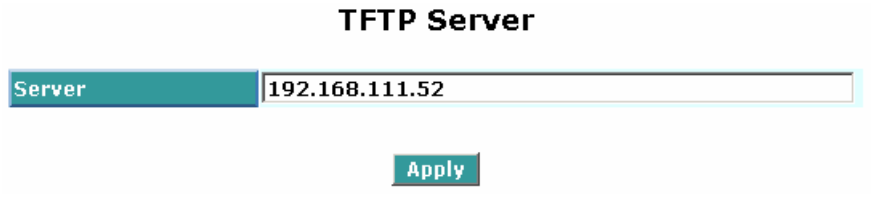
Ping Test function is a tool for detecting if the target device is alive or not through ICMP protocol which abounds with report messages. The switch provides Ping Test function to let you know that if the target device

is available or not. You can simply fill in a known IP address and then click <Ping> button. After a few seconds later, the switch will report you the pinged device is alive or dead in the field of Ping Result.



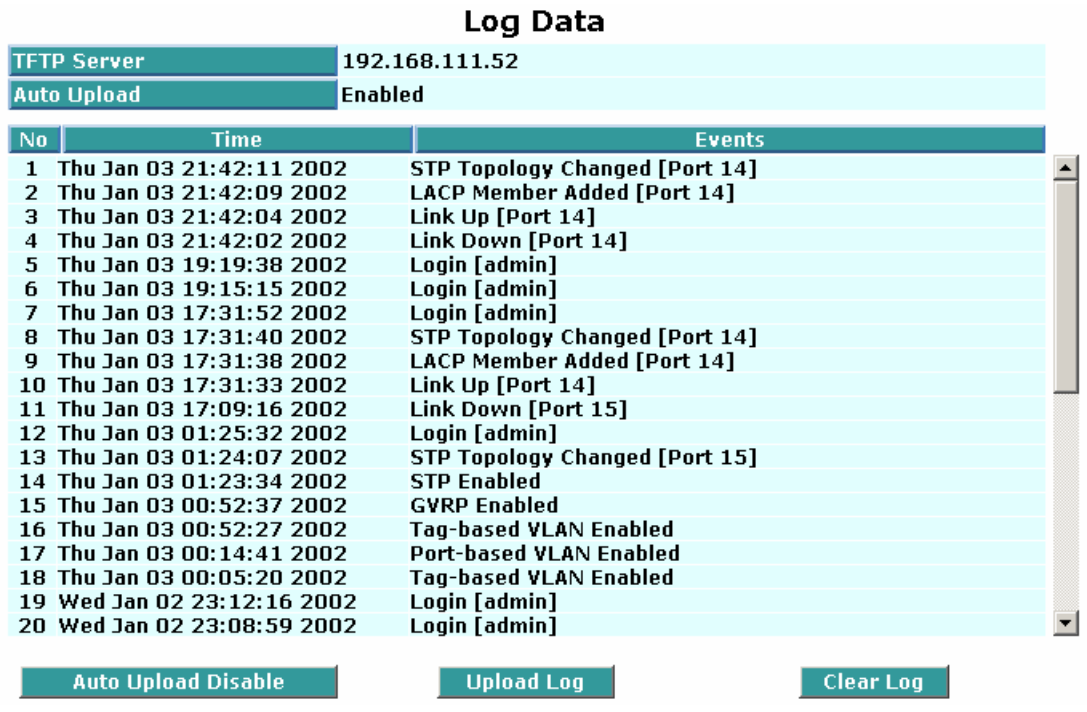
3.21 TFTP Server

Specify the IP address where the TFTP server locates. Fill in the IP address of your TFTP server, then press Apply button to have the setting taken effect.



3.22 Log

This function shows the log data. The switch provides system log data for users. There are 19 private trap logs, 5 public trap logs. It displays the log items including all SNMP Private Trap events, SNMP Public traps and user logs occurred in the system. In the report table, No., Time and Events are three fields contained in each trap record. The switch supports total 120 log entries. For more details on log items, please refer to the section of Trap/Alarm Configuration and SNMP Configuration.



Parameter description:

- **No.:** Display the order number that the trap happened.
- **Time:** Display the time that the trap happened.
- **Events:** Display the trap event name.

- **Auto Upload Enable:** Switch the enabled or disabled status of the auto upload function.
- **Upload Log:** Upload log data through tftp.
- **Clear Log:** Clear log data.

3.23 Firmware Upgrade

The switch supports TFTP upgrade tool for upgrading software. If you assure to upgrade software to a newer version one, you must follow two procedures:

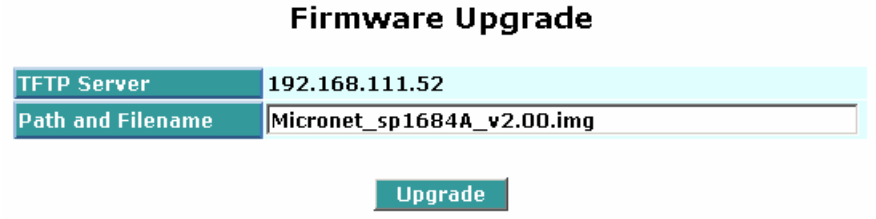
1. Specifying the IP address where TFTP server locates. In this field, the IP address of your TFTP server should be filled in.
2. Specifying what the filename and where the file is. You must specify full path and filename.

Once you press Upgrade button, the switch will prompt the screen for you to reconfirm. Then, the switch starts downloading software from TFTP server if you choose OK button. It will be just back to “Software Upgrade” if you choose Cancel button.

If your download is not successful, the switch will also be back to “Software Upgrade”, and it will not upgrade the software as well.

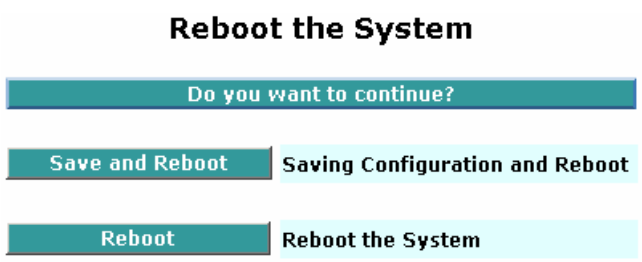
When download is completed, the switch starts upgrading software. A reboot message will be prompted after completing upgrading software. At this time, you must reboot the switch to have new software worked.

Note: Software upgrade is hazardous if power is off. You must do it carefully.



3.24 Reboot

We offer you many ways to reboot the switch, including power up, hardware reset and software reset. You can press the RESET button in the front panel to reset the switch. After upgrading software, changing IP configuration or changing VLAN mode configuration, then you must reboot to have the new configuration taken effect. Here, Reboot takes the same effect as the RESET button on the front panel of the switch. It will take around thirty (30) seconds to complete the system boot.



3.25 Logout

The switch allows you to logout the system to prevent other users from the system without the permission. If you do not logout and exit the browser, the switch will automatically have you logout. Besides this manually logout and implicit logout, you can pull down the **Auto Logout** list at the left-top corner to explicitly ON/OFF this logout function.

4. Text-based User Interface

4.1 Setup the Connection

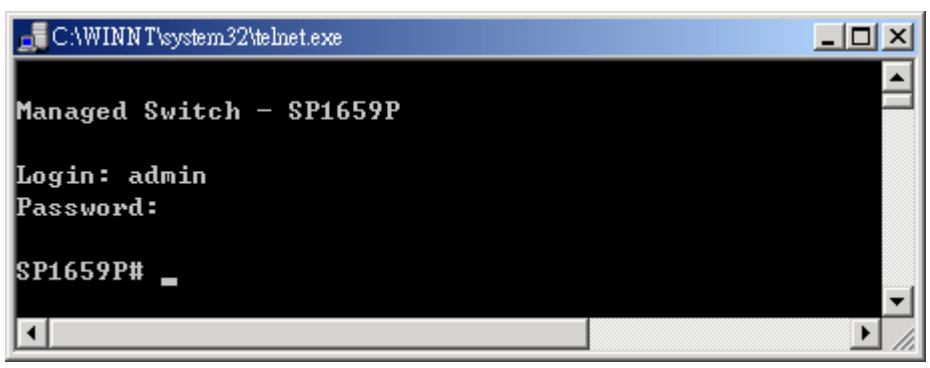
The switch provides other user interface to access by telnet and direct console. The management functions of Telnet program or console are exactly the same with web-based management interface but in text mode.

In-band Connection (Telnet)

To access the switch through a Telnet session, just start the Telnet program on a PC and connect to the switch. Factory Default value of system is:

IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.254

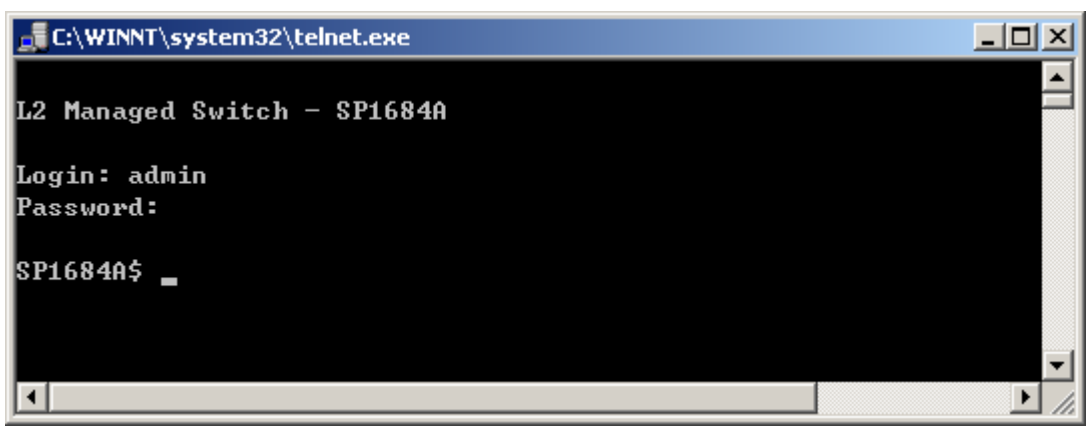
Press “Enter” key to begin login screen. Enter the username and password to login the system.



Login accounts:

- Username: ***admin*** Password: ***admin*** (read/write)
- Username: ***guest*** Password: ***guest***

After you login successfully, the prompt will be shown as “#“ if you are the first login person and your authorization is administrator; otherwise it may show “$“. See the following two figures. The former means you behave as an administrator and have the access right of the system. As to the latter, it means you behave as a guest and are only allowed to view the system without the permission to do any setting for this switch.



Out-of-band Connection (Console)

To activate console port connection, attach a RS-232 cable (Straight-through) to the serial port of a PC running a terminal emulation program and configure the program as follows:

Baud rate:	**57600**
Parity:	**None**

Data bit: **8**
Stop bit: **1**
Flow control: **None**

Press “Enter” key to begin login screen. Enter the username and password to login the management console.

To see the commands of the mode, please input “?” after the prompt, then all commands will be listed in the screen. All commands can be divided into two categories, including global commands and local commands. Global commands can be used wherever the mode you are. They are “exit”, “end”, “help”, “history”, “logout”, “save start”, “save user”, “restore default” and “restore user”.

Command instructions reside in the corresponding modes are local commands. The same command with the same command name may occur but perform totally different function in different modes. For example, “show” in IP mode performs displaying the IP information; however, it performs displaying the system information in system mode.

4.2 Global Command

4.2.1 end

Syntax: end
Description: Back to the top mode.
When you enter this command, your current position would move to the top mode. If you use this command in the top mode, you are still in the position of the top mode.
Argument: None.
Possible value: None.
Example:

```
SP1659P# alarm
SP1659P(alarm)# events
SP1659P(alarm-events)# end
SP1659P#
```

4.2.2 exit

Syntax: exit
Description: Back to the previous mode.
When you enter this command, your current position would move back to the previous mode. If you use this command in the top mode, you are still in the position of the top mode.
Argument: None.
Possible value: None.
Example:

```
SP1659P# trunk
SP1659P(trunk)# exit
SP1659P#
```

4.2.3 help

Syntax: help

Description: To show available commands.

Some commands are the combination of more than two words. When you enter this command, the CLI would show the complete commands. Besides, the command would help you classify the commands between the local commands and the global ones.

Argument: None.

Possible value: None.

Example:

```
SP1659P# ip
SP1659P(ip)# help
Commands available:
  ------------<< Local commands >>------------
  set ip                    Set ip,subnet mask and gateway
  set dns                   Set dns
  enable dhcp               Enable DHCP, and set dns auto or manual
  disable dhcp              Disable DHCP
  show                      Show IP Configuration
  ------------<< Global commands >>------------
  exit                      Back to the previous mode
  end                       Back to the top mode
  help                      Show available commands
  history                   Show a list of previously run commands
  logout                    Logout the system
  save start                Save as start config
  save user                 Save as user config
  restore default           Restore default config
  restore user              Restore user config
```

4.2.4 history

Syntax: history [#]

Description: To show a list of previous commands that you had ever run.

When you enter this command, the CLI would show a list of commands which you had typed before. The CLI supports up to 256 records. If no argument is typed, the CLI would list total records up to 256. If optional argument is given, the CLI would only show the last numbers of records, given by the argument.

Argument: [#]: show last number of history records (optional).

Possible value: [#]: 1, 2, 3, …., 256

Example:

```
SP1659P(ip)# history
 Command history:
  0. trunk
  1. exit
  2. SP1659P# trunk
  3. SP1659P(trunk)# exit
  4. SP1659P#
  5. ?
  6. trunk
  7. exit
  8. alarm
  9. events
 10. end
```

```
 11. ip
 12. help
 13. ip
 14. history
SP1659P(ip)# history 3
 Command history:
 13. ip
 14. history
 15. history 3
```

4.2.5 restore default

Syntax: restore default

Description:

To restore the startup configuration as factory default configuration. If restoring default successfully, the CLI would prompt if reboot immediately or not. If you press Y or y, the system would reboot immediately; others would be back to the CLI system. After restoring default configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would reset to factory default.

Argument: None

Possible value: None

Example:

```
SP1659P# restore default
Restoring ...
Restore Default Configuration Successfully
Press any key to reboot system.
```

4.2.6 restore user

Syntax: restore user

Description:

To restore the startup configuration as user defined configuration. If restoring default successfully, the CLI would prompt if reboot immediately or not. If you press Y or y, the system would reboot immediately; others would back to the CLI system. After restoring user-defined configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would replace as user defined one.

Argument: None

Possible value: None

Example:

```
SP1659P# restore user
Restoring ...
Restore User Configuration Successfully
Press any key to reboot system.
```

4.2.7 save start

Syntax: save start

Description:

Save the current configuration as the start one. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH. If you want the configuration still works after rebooting, save the configuration using the command ‘save stat’.

Argument: None.

Possible value: None.

Example:

```
SP1659P# save start
Saving start...
Save Successfully
```

4.2.8 save user

Syntax: save user

Description:

Save the current configuration as the user-defined configuration. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH as user-defined configuration.

Argument: None.

Possible value: None.

Example:

```
SP1659P# save user
Saving user...
Save Successfully
```

4.3 Local Command

4.3.1 802.1x

set max-request

Syntax: set max-request <port-range> <times>

Description:

That is the maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session.

Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<times>: max-times , range 1-10

Possible value:

<port range> : 1 to 24

<times>: 1-10, default is 2

Example:

```
SP1659P(802.1x)# set max-request 2 2
```

set mode

Syntax: set mode <port-range> <mode>

Description: To set up the 802.1X authentication mode of each port.

Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<mode>: set up 802.1x mode

0:disable the 802.1x function

1:set 802.1x to Multi-host mode

Possible value:

<port range> : 1 to 24

<mode>: 0 or 1

Example:

```
SP1659P(802.1x)# set mode 2 1
SP1659P(802.1x)#
```

set port-control

Syntax: set port-control <port-range> <authorized>

Description: To set up 802.1X status of each port.

Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<authorized> : Set up the status of each port

0:ForceUnauthorized

1:ForceAuthorized

2:Auto

Possible value:

<port range> : 1 to 24

<authorized> : 0, 1 or 2

Example:

```
SP1659P(802.1x)# set port-control 2 2
```

set quiet-period

Syntax:

set quiet-period <port-range> <sec>

Description:

A timer used by the Authenticator state machine to define periods of time during when it will not attempt to acquire a Supplicant.

Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<sec> : timer , range 0-65535

Possible value:

<port range> : 1 to 24

<sec> : 0-65535, default is 60

Example:

```
SP1659P(802.1x)# set quiet-period 2 30
```

set reAuthEnabled

Syntax: set reAuthEnabled <port-range> <ebl>

Description: A constant that define whether regular reauthentication will take place on this port.

Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<ebl> :

0:OFF Disable reauthentication

1:ON Enable reauthentication

Possible value:

<port range> : 1 to 24

<ebl> : 0 or 1, default is 1

Example:

```
SP1659P(802.1x)# set reAuthEnabled 2 1
```

set reAuthMax

Syntax: set reAuthMax <port-range> <max>

Description: The number of reauthentication attempts that are permitted before the port becomes Unauthorized.

Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<max> : max. value , range 1-10

Possible value:

<port range> : 1 to 24

<max> : 1-10, default is 2

Example:

```
SP1659P(802.1x)# set reAuthMax 2 2
```

set reAuthPeriod

Syntax: set reAuthPeriod <port-range> <sec>

Description: A constant that defines a nonzero number of seconds between periodic reauthentication of the supplicant.

Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<sec> : timer , range 1-65535

Possible value:

<port range> : 1 to 24

<sec> : 1-65535, default is 3600

Example:

```
SP1659P(802.1x)# set reAuthPeriod 2 3600
```

set serverTimeout

Syntax: set serverTimeout <port-range> <sec>

Description:

A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.

Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<sec> : timer , range 1-65535

Possible value:

<port range> : 1 to 24

<sec> : 1-65535, default is 30

Example:

```
SP1659P(802.1x)# set serverTimeout 2 30
```

set state

Syntax: set state <ip> <port-number> <secret-key>

Description: To configure the settings related with 802.1X Radius Server.

Argument:

<ip> : the IP address of Radius Server

<port-number> : the service port of Radius Server(Authorization port)

<secret-key>: set up the value of secret-key, and the length of secret-key is from 1 to 31

Possible value: <port-number> : 1~65535, default is 1812

Example:

```
SP1659P(802.1x)# set state 192.168.1.115 1812 WinRadius
```

set suppTimeout

Syntax: set suppTimeout <port-range> <sec>

Description:

A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.

Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<sec> : timer , range 1-65535

Possible value:

<port range> : 1 to 24

<sec> : 1-65535, default is 30

Example:

```
SP1659P(802.1x)# set suppTimeout 2 30
```

set txPeriod

Syntax: set txPeriod <port-range> <sec>

Description: A timer used by the Authenticator PAE state machine to determine when an EAPOL PDU is to be transmitted

Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<sec> : timer , range 1-65535

Possible value:

<port range> : 1 to 24

<sec> : 1-65535, default is 30

Example:

```
SP1659P(802.1x)# set txPeriod 2 30
```

show mode

Syntax: show mode

Description: To display the mode of each port.

Argument: None

Possible value: None

Example:

```
SP1659P(802.1x)# show mode
 Port        Mode
====== ============
   1        Disable
   2        Multi-host
   3        Disable
   4        Disable
   5        Disable
   6        Disable
                 :
                 :
                 :
```

show parameter

Syntax: show parameter

Description: To display the parameter settings of each port.

Argument: None

Possible value: None

Example:

```
SP1659P(802.1x)# show parameter
port   1) port control   : Auto
          reAuthMax       : 2
          txPeriod        : 30
          Quiet Period    : 60
          reAuthEnabled : ON
          reAuthPeriod    : 3600
          max. Request    : 2
          suppTimeout     : 30
          serverTimeout : 30
port   2) port control   : Auto
          reAuthMax       : 2
          txPeriod        : 30
          Quiet Period    : 60
          reAuthEnabled : ON
          reAuthPeriod    : 3600
          max. Request    : 2
          suppTimeout     : 30
          serverTimeout : 30
                                :
                                :
                                :
```

show security

Syntax: show security

Description: To display the authentication status of each port.

Argument: None

Possible value: None

Example:

```
SP1659P(802.1x)# show security
 Port       Mode            Status
====== ============ ==============
   1       Disable
   2       Multi-host     Unauthorized
   3       Disable
   4       Disable
   5       Disable
   6       Disable
                        :
                        :
```

show state

Syntax: show state

Description: Show the Radius server configuration

Argument: None

Possible value: None

Example:

```
SP1659P(802.1x)# show state
Radius Server: 192.168.1.115
Port Number    : 1812
Secret Key     : WinRadius
```

4.3.2 account

add

Syntax: add <name>

Description: To create a new guest user. When you create a new guest user, you must type in password and confirm password.

Argument: <name>: new account name

Possible value: A string must be at least 5 character.

Example:

```
SP1659P(account)# add aaaaa
Password:
Confirm Password:
Save Successfully
SP1659P(account)#
```

del

Syntax: del <name>

Description: To delete an existing account.

Argument: <name> : existing user account

Possible value: None.

Example:

```
SP1659P(account)# del aaaaa
Account aaaaa deleted
```

modify

Syntax: modify <name>

Description: To change the username and password of an existing account.

Argument: <name> : existing user account

Possible value: None.

Example:

```
SP1659P(account)# modify aaaaa
username/password: the length is from 5 to 15.
Current username (aaaaa):bbbbb
New password:
Confirm password:
Username changed successfully.
Password changed successfully.
```

show

Syntax: show

Description: To show system count, including account name and identity.

Argument: None.

Possible value: None.

Example:

```
SP1659P(account)# show
Account Name          Identity
---------------- ---------------
 admin                Administrator
 guest                    guest
```

4.3.3 alarm

<<email>>

del mail-address

Syntax: del mail-address <#>

Description: The Del here is used to remove the configuration of E-mail address.

Argument: <#>: email address number, range: 1 to 6

Possible value: <#>: 1 to 6

Example:

```
SP1659P(alarm-email)# del mail-address 2
```

del server-user

Syntax: del server-user <#>

Description: The Del here is used to remove the server, user account and password.

Argument: <#>: email address number, range: 1 to 6

Possible value: None

Example:

```
SP1659P(alarm-email)# del server-user
```

set

Syntax:

set server <ip>

set user <username>

set mail-address <#> <mail address>

Description: The Set here is used for the configuration of e-mail server, username, password and address.

Argument:

<ip>: E-mail server ip

<username>: email server account and password

<#>: email address number, range: 1 to 6

<mail address>: email address

Possible value: <#>: 1 to 6

Example:

```
SP1659P(alarm-email)# set server 192.168.1.6
SP1659P(alarm-email)# set user admin
Password:
Confirm Password:
SP1659P(alarm-email)# set mail-address 1 abc@mail.abc.com
```

show

Syntax: show

Description: The Show here is used to display the configuration of e-mail trap event.

Argument: None.

Possible value: None.

Example:

```
SP1659P(alarm-email)# show
Mail Server      : 192.168.1.6
Username         : admin
```

```
Password          : ****************
Email Address 1: abc@mail.abc.com
Email Address 2:
Email Address 3:
Email Address 4:
Email Address 5:
Email Address 6:
```

<<events>>

del

Syntax:

del sms <range>

del email <range>

del trap <range>

del all <range>

Description: The Del here is used for the de-activation of sms, email and trap event.

Argument: <range>:trap number.

Possible value: available from 1 to 24.

Example:

```
SP1659P(alarm-events)# del sms 1-3
SP1659P(alarm-events)# del email 1-3
SP1659P(alarm-events)# del trap 1-3
SP1659P(alarm-events)# del all 1-3
```

set

Syntax:

set sms <range>

set email <range>

set trap <range>

set all <range>

Description: The Set here is used for the activation of sms, email and trap event.

Argument: <range>: syntax 1,5-7, trap number.

Possible value: available from 1 to 24.

Example:

```
SP1659P(alarm-events)# set sms 1-3
SP1659P(alarm-events)# set email 1-3
SP1659P(alarm-events)# set trap 1-3
SP1659P(alarm-events)# set all 1-3
```

show

Syntax: show

Description: The Show here is used to display the configuration of alarm event.

Argument: None.

Possible value: None.

Example:

```
SP1659P(alarm-events)# show
    Events                          Email SMS Trap
-----------------------------------------
1   Cold Start                            v
2   Warm Start                              v
3   Link Down                               v
4   Link Up                                 v
```

5 Authentication Failure v
6 User Login
7 User Logout
8 STP Topology Changed
9 STP Disabled
10 STP Enabled
11 LACP Disabled
12 LACP Enabled
13 LACP Member Added
14 LACP Port Failure
15 GVRP Disabled
16 GVRP Enabled
17 Port-based Vlan Enabled
18 Tag-based Vlan Enabled
19 Module Inserted
20 Module Removed
21 Moudle Media Swapped
22 PoE Failure

show

Syntax: show

Description: The Show for alarm here is used to display the configuration of Trap, SMS or E-mail.

Argument: None.

Possible value: None.

Example:

```
SP1659P(alarm)# show events
SP1659P(alarm)# show email
SP1659P(alarm)# show sms
```

<<sms>>

del

Syntax:

del phone-number <#>

del server-user

Description: To delete sms phone number, sms server, user account and password.

Argument: <#>: mobile phone number, range: 1 to 6

Possible value: <#>: 1 to 6

Example:

```
SP1659P(alarm-sms)# del phone-number 3
SP1659P(alarm-sms)# del server-user
```

set

Syntax:

set server <ip>

set user <username>

set phone-number <#> <phone-number>

Description: The Set here is used for the configuration of SMS server, username, password and phone number.

Argument:

<ip>: SMS server ip

<username>: SMS server account and password

<#>: mobile phone number, range: 1 to 6

<phone-number>: phone number

Possible value: <#>: 1 to 6

Example:

```
SP1659P(alarm-sms)# set server 192.168.1.7
SP1659P(alarm-sms)# set user ruby
Password:
Confirm Password:
SP1659P(alarm-sms)# set phone-number 1 0968777777
```

show

Syntax: show

Description: The Show here is to display the configuration of SMS trap event.

Argument: None.

Possible value: None.

Example:

```
SP1659P(alarm-sms)# show
SMS Server       : 192.168.1.7
Username         :
Password         : ****************
Mobile Phone   1: 0968777777
Mobile Phone   2:
Mobile Phone   3:
Mobile Phone   4:
Mobile Phone   5:
Mobile Phone   6:
```

4.3.4 autologout

autologout

Syntax: autologout <time>

Description: To set up the timer of autologout.

Argument: <time>: range 1 to 3600 seconds, 0 for autologout off, current setting is 180 seconds.

Possible value: <time>: 0, 1-3600

Example:

```
SP1659P# autologout 3600
Set autologout time to 3600 seconds
```

4.3.5 bandwidth

set egress-rate

Syntax: set egress-rate <range> <data_rate>

Description: To setup the egress-rate of the port.

Argument:

<range>:syntax 1,5-7, available from 1 to 26

<data_rate>: 66-1024000(Kb). #1-24: 66-102400(Kb, # 25-26: 66-1024000(Kb)

Possible value:

<range>: 1 to 26

<data_rate>: #1-24: 66-102400(Kb), # 25-26: 66-1024000(Kb)

Example:

```
SP1659P(bandwidth)# set egress-rate 1-16 299
```

set ingress-rate

Syntax: set ingress-rate <range> <data_rate>

Description: To setup the Ingress-rate of the port.

Argument:

<range>:syntax 1,5-7, available from 1 to 26

<data_rate>: 66-1024000(Kb). #1-24: 66-102400(Kb, # 25-26: 66-1024000(Kb)

Possible value:

<range>: 1 to 26

<data_rate>: #1-24: 66-102400(Kb), # 25-26: 66-1024000(Kb)

Example:

```
SP1659P(bandwidth)# set ingress-rate 1-16 100
```

set storm-rate

Syntax: set storm-rate <range> <data_rate>

Description: To setup the storm-ate of the port.

Argument:

<range>:syntax: 1,3-5, available from 1 to 5

1: Disable 2: Broadcast Storm Control

3: Multicast Storm Control

4: Unknown Unicast Storm Control

5: Broadcast, Multicast, Unknown Unicast Storm Control

<data_rate>: 1-100. The value must be the integer. The value 100 disables broadcast storm control.

Possible value:

<range>: 1 to 5

<data_rate>: 1-100.

Example:

```
SP1659P(bandwidth)# set storm-rate 2 99
```

show

Syntax: show

Description: To display all current settings of the bandwidth.

Argument: None

Possible value: None

Example:

```
SP1659P(bandwidth)# show
Port    Ingress Rate(Kb)      Egress Rate(Kb)
====== ==================  =================
   1        102400                102400
   2        102400                102400
   3        102400                102400
   4        102400                102400
   5        102400                102400
   6        102400                102400
   7        102400                102400
   8        102400                102400
   9        102400                102400
  10        102400                102400
  11        102400                102400
  12        102400                102400
```

13	102400	102400
14	102400	102400
15	102400	102400
16	102400	102400
17	102400	102400
18	102400	102400
19	102400	102400
20	102400	102400
21	102400	102400
22	102400	102400
23	102400	102400
24	102400	102400
25	1024000	1024000
26	1024000	1024000

```
   Broadcast Storm Control
==========================================================
Type: Disable
Rate: 100 %
```

4.3.6 config-file

export start

Syntax: export start

Description: To run the export start function.

Argument: None

Possible value: None

Example:

```
SP1659P(config-file)# export start
Export successful.
```

export user-conf

Syntax: export user-conf

Descrption: To run the export user-conf function.

Argument: None

Possible value: None

Example:

```
SP1659P(config-file)# export user-conf
Export successful.
```

import start

Syntax: import start

Description: To run the import start function.

Argument: None

Possible value: None

Example:

```
SP1659P(config-file)# import start
Import successful.
```

import user-conf

Syntax: import user-conf

Description: To run the import user-conf function.

Argument: None

Possible value: None

Example:

```
SP1659P(config-file)# import user-conf
Import successful.
```

set export-path

Syntax: set export-path <filepath>

Description: To set up the filepath and filename that will be exported.

Argument: <filepath>:filepath and filename

Possible value: <filepath>:filepath and filename

Example:

```
SP1659P(config-file)# set export-path log/21511.txt
```

set import-path

Syntax: set import-path <filepath>

Description:

To set up the filepat and filename that will be imported.

Argument: <filepath>:filepath and filename

Possible value: <filepath>:filepath and filename

Example:

```
SP1659P(config-file)# set import-path log/21511.txt
```

show

Syntax: show

Description: To display the config-file information.

Argument: None

Possible value: None

Example:

```
SP1659P(config-file)# show
TFTP Server IP Address: 192.168.3.111
Export Path and Filename: nmap/123.ts
Import Path and Filename: user123.txt
```

4.3.7 dhcp-boot

set dhcp-boot

Syntax: set dhcp-boot <sec>

Description: To set up the delay time for DHCP Boot.

Argument: <sec>:range syntax: 0, 1-30. The value “0” is to disable dhcp-boot delay

Possible value: <sec>:0-30

Example:

```
SP1659P(dhcp-boot)# set dhcp-boot 30
```

show

Syntax: show

Description: To display the status of DHCP Boot.

Argument: None

Possible value: None

Example:

```
SP1659P(dhcp-boot)# show
Dhcp Boot : Enable
Second      : 10
```

4.3.8 diag

diag

Syntax: diag

Description: Diag is used to test whether UART, DRAM, Flash and EEPROM is normal or not.

Argument: None.

Possible value: None.

Example:

```
SP1659P(diag)# diag
EEPROM Test : OK
UART Test     : OK
DRAM Test     : OK
Flash Test    : OK
```

loopback

Syntax: Loopback

Description: For Internal/External Loopback Test.

Argument: None.

Possible value: None.

Example:

```
SP1659P(diag)# loopback
Internal Loopback Test : OK

External Loopback Test : Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 Fail
```

ping

Syntax: ping <ip>

Description: To confirm that whether the remote end-station or switch itself is alive or not.

Argument: [ip] : ip address or domain name

Possible value: IP address, e.g. 192.168.2.65 or domain name, e.g. tw.yahoo.com

Example:

```
SP1659P(diag)# ping 192.168.1.115
Gateway         : 192.168.1.253
192.168.1.115 is alive.
```

4.3.9 firmware

set upgrade-path

Syntax: set upgrade-path <filepath>

Description: To set up the image fie that will be upgraded.

Argument: <filepath>: upgrade file path

Possible value: <filepath>: upgrade file path

Example:

```
SP1659P(firmware)# set upgrade-path sp1659P_v0.92.bin.gz
```

show

Syntax: show

Description: To display the information of tftp server and upgrade-path.

Argument: None

Possible value: None

Example:

```
SP1659P(firmware)# show
TFTP Server IP Address: 192.168.3.111
Path and Filename       : sp1659P_v0.92.bin.gz
```

upgrade

Syntax: upgrade

Description: To run the upgrade function.

Argument: None

Possible value: None

Example:

```
SP1659P(firmware)# upgrade
Upgrading firmware ...
```

4.3.10 gvrp

disable

Syntax: disable

Description: To disable the gvrp function.

Argument: None

Possible value: None

Example:

```
SP1659P(gvrp)# disable
```

enable

Syntax: enable

Description: To enable the gvrp function.

Argument: None

Possible value: None

Example:

```
SP1659P(gvrp)# enable
```

group

Syntax: group <group number>

Description: To enter any of gvrp group for changing gvrp group setting. You can change the applicant or registrar mode of existing gvrp group per port.

Argument:

<group number>: enter which gvrp group you had created, using value is vid. Available range: 1 to 4094

Possible value: <group number>: 1~4094

Example:

```
SP1659P(gvrp)# show group
```

```
GVRP group information
Current Dynamic Group Number: 1
VID    Member Port
---- -------------------------------------------------
2      5

SP1659P(gvrp)# group 2
SP1659P(gvrp-group-2)# set applicant 1-6 non-participant

SP1659P(gvrp-group-2)# show
GVRP group VID: 2
Port Applicant          Registrar
---- -------------- ---------
1      Non-Participant Normal
2      Non-Participant Normal
3      Non-Participant Normal
4      Non-Participant Normal
5      Non-Participant Normal
6      Non-Participant Normal
7      Normal              Normal
8      Normal              Normal
12     Normal              Normal
13     Normal              Normal
                             :
                             :
23     Normal              Normal
24     Normal              Normal
25     Normal              Normal
26     Normal              Normal


SP1659P(gvrp-group-2)# set registrar 1-10 fixed

SP1659P(gvrp-group-2)# show
GVRP group VID: 2
Port Applicant          Registrar
---- -------------- ---------
1      Non-Participant Fixed
2      Non-Participant Fixed
3      Non-Participant Fixed
4      Non-Participant Fixed
5      Non-Participant Fixed
6      Non-Participant Fixed
7      Normal              Fixed
8      Normal              Fixed
9      Normal              Fixed
10     Normal              Fixed
17     Normal              Normal
                   :
                                 :
23     Normal              Normal
24     Normal              Normal
25     Normal              Normal
26     Normal              Normal
```

set applicant

Syntax: set applicant <range> <normal|non-participant>

Description: To set default applicant mode for each port.

Argument:

<range>: port range, syntax 1,5-7, available from 1 to 26

<normal>: set applicant as normal mode

<non-participant>: set applicant as non-participant mode

Possible value:

<range>: 1 to 24

<normal|non-participant>: normal or non-participant

Example:

```
SP1659P(gvrp)# set applicant 1-10 non-participant
```

set registrar

Syntax: set registrar <range> <normal|fixed|forbidden>

Description: To set default registrar mode for each port.

Argument:

<range>: port range, syntax 1,5-7, available from 1 to 26

<normal>: set registrar as normal mode

<fixed>: set registrar as fixed mode

<forbidden>: set registrar as forbidden mode

Possible value:

<range>: 1 to 24

<normal|fixed|forbidden>: normal or fixed or forbidden

Example:

```
SP1659P(gvrp)# set registrar 1-5 fixed
```

set restricted

Syntax: set restricted <range> <enable|disable>

Description: To set the restricted mode for each port.

Argument:

<range>: port range, syntax 1,5-7, available from 1 to 26

<enable>: set restricted enabled

<disable>: set restricted disabled

Possible value:

<range>: 1 to 24

<enable|disable>: enable or disable

Example:

```
SP1659P(gvrp)# set restricted 1-10 enable
SP1659P (gvrp)# show config
GVRP state: Enable
Port Join Time Leave Time LeaveAll Time      Applicant      Registrar Restricted
---- --------- ---------- ------------ --------------- --------- ----------
  1       20         60         1000          Normal     Normal     Enable
  2       20         60         1000          Normal     Normal     Enable
  3       20         60         1000          Normal     Normal     Enable
  4       20         60         1000          Normal     Normal     Enable
  5       20         60         1000          Normal     Normal     Enable
  6       20         60         1000          Normal     Normal     Enable
  7       20         60         1000          Normal     Normal     Enable
  8       20         60         1000          Normal     Normal     Enable
  9       20         60         1000          Normal     Normal     Enable
 10       20         60         1000          Normal     Normal     Enable
                                                :
                                                :
 22       20         60         1000          Normal     Normal     Disable
 23       20         60         1000          Normal     Normal     Disable
 24       20         60         1000          Normal     Normal     Disable
 25       20         60         1000          Normal     Normal     Disable
 26       20         60         1000          Normal     Normal     Disable
```

set timer

Syntax: set timer <range> <join> <leave> <leaveall>

Description: To set gvrp join time, leave time, and leaveall time for each port.

Argument:

<range> : port range, syntax 1,5-7, available from 1 to 26

<join>: join timer, available from 20 to 100

<leave>: leave timer, available from 60 to 300

<leaveall>: leaveall timer, available from 1000 to 5000

Leave Time must equal double Join Time at least.

Possible value:

<range> : 1 to 26

<join>: 20 to 100

<leave>: 60 to 300

<leaveall>: 1000 to 5000

Example:

```
SP1659P(gvrp)# set timer 2-8 25 80 2000
```

show config

Syntax: show config

Description: To display the gvrp configuration.

Argument: none

Possible value: none

Example:

```
SP1659P(gvrp)# show config
GVRP state: Enable
Port Join Time Leave Time LeaveAll Time      Applicant      Registrar Restricted
---- --------- ---------- ------------- --------------- --------- ----------
  1       20         60          1000         Normal        Normal    Disable
  2       25         80          2000         Normal        Normal    Disable
  3       25         80          2000         Normal        Normal    Disable
  4       25         80          2000         Normal        Normal    Disable
  5       25         80          2000         Normal        Normal    Disable
  6       25         80          2000         Normal        Normal    Disable
  7       25         80          2000         Normal        Normal    Disable
  8       25         80          2000         Normal        Normal    Disable
                                                :
                                                :
 23       20         60          1000         Normal        Normal    Disable
 24       20         60          1000         Normal        Normal    Disable
 25       20         60          1000         Normal        Normal    Disable
 26       20         60          1000         Normal        Normal    Disable
```

show counter

Syntax: show counter

Description: Usage: show counter <port>

Argument: <port>: port number

Possible value: <port>: available from 1 to 26

Example:

```
SP1659P(gvrp)# show counter 2
GVRP Counter port: 2
Counter Name                 Received Transmitted
--------------------     -------- -----------
```

```
Total GVRP Packets          0              0
Invalid GVRP Packets        0            ----
LeaveAll message            0              0
JoinEmpty message           0              0
JoinIn message              0              0
LeaveEmpty message          0              0
Empty message               0              0
```

show group

Syntax: show group

Description: To show the gvrp group.

Argument: none

Possible value: none

Example:

```
SP1659P(gvrp)# show group
GVRP group information
VID   Member Port
---- ---------------------------------------------
```

4.3.11 hostname

hostname

Syntax: hotsname <name>

Description: To set up the hostname of the switch.

Argument: <name>: hostname, max 128 characters.

Possible value: <name>: hostname, max 128 characters.

Example:

```
SP1659P# hostname Company

Company#
```

4.3.12 igmp-snooping

set mode

Syntax: set mode <status>

Description: To set up the mode of IGMP Snooping.

Argument: <status>: 0: disable, 1: active, 2: passive

Possible value: <status>: 0,1or 2

Example:

```
SP1659P(igmp-snooping)# set mode 1
```

show

Syntax:

show igmp-snooping

show multicast

Description: To display IGMP snooping mode and IP Multicast Table.

Argument: None

Possible value: None

Example:

```
SP1659P(igmp-snooping)# show igmp-snooping
Snoop Mode: Active

SP1659P(igmp-snooping)# show multicast
Snoop Mode: Active

IP Multicast:
 1)   IP Address      : 224.1.1.1
      VLAN ID         : 0
      Member Port: 22
```

4.3.13 ip

disable dhcp

Syntax: disable dhcp

Description: To disable the DHCP function of the system.

Argument: None

Possible value: None

Example:

```
SP1659P(ip)# disable dhcp
: Disabled system DHCP function.
```

enable dhcp

Syntax: enable dhcp <manual|auto>

Description: To enable the system DHCP function and set DNS server via manual or auto mode.

Argument: <manual|auto>: set dhcp by using manual or auto mode.

Possible value: <manual|auto>: manual or auto

Example:

```
SP1659P(ip)# enable dhcp manual
: Enabled system DHCP function and set DNS server via manual mode.
```

set dns

Syntax: set dns <ip>

Description: To set the IP address of DNS server.

Argument: <ip> : dns ip address

Possible value: 168.95.1.1

Example:

```
SP1659P (ip)# set dns 168.95.1.1
set DNS server IP address to 168.95.1.1
```

set ip

Syntax: set ip <ip> <mask> <gateway>

Description: To set the system IP address, subnet mask and gateway.

Argument:

<ip> : ip address

<mask> : Subnet Mask

<gateway> : Default Gateway

Possible value:

<ip> : 192.168.1.2 or others

<mask> : 255.255.255.0 or others

<gateway> : 192.168.1.253 or others

Example:

```
SP1659P(ip)# set ip 192.168.1.2 255.255.255.0 192.168.1.253
set system IP address : 192.168.1.2
              subnet mask        : 255.255.255.0
              default gateway : 192.168.1.253
```

show

Syntax: show

Description:

To display the system's DHCP function state, IP address, subnet mask, default gateway, DNS mode, DNS server IP address and current IP address.

Argument: None

Possible value: None

Example:

```
SP1659P(ip)# show

DHCP                : Disable
IP Address          : 192.168.2.65
Subnet mask         : 255.255.255.0
Gateway             : 192.168.2.252
DNS Setting         : Manual
DNS Server          : 168.95.1.1
Current IP          : 192.168.2.65
```

4.3.14 log

clear

Syntax: clear

Description: To clear the log data.

Argument: None.

Possible value: None.

Example:

```
SP1659P(log)# clear
```

disable auto-upload

Syntax: disable auto-upload

Description: To disable the auto-upload function.

Argument: None.

Possible value: None.

Example:

```
SP1659P(log)# disable auto-upload
```

enable auto-upload

Syntax: enable auto-upload

Description: To enable the auto-upload function.

Argument: None.

Possible value: None.

Example:

```
SP1659P(log)# enable auto-upload
```

show

Syntax: show

Description:

To show a list of trap log events. When any of log events happens, it will be recorded and using show command in log function to query. Up to 120 log records are supported.

Argument: None.

Possible value: None.

Example:

```
SP1659P(log)# show

Tftp Server : 0.0.0.0
Auto Upload : Disable

1)   Wed Apr 13 12:13:27 2005   Link Up [Port 1]
2)   Wed Apr 13 12:13:26 2005   Link Down [Port 1]
3)   Wed Apr 13 11:58:31 2005   Login [admin]
4)   Wed Apr 13 11:19:45 2005   Login [admin]
5)   Wed Apr 13 11:19:37 2005   Logout [admin]
```

upload

Syntax: Upload

Description: To upload log data through tftp.

Argument: None.

Possible value: None.

Example:

```
SP1659P(log)# upload
```

4.3.15 mac-table

<<alias>>

del

Syntax: del <mac>

Description: To delete the mac alias entry.

Argument: <mac> : mac address, format: 00-02-03-04-05-06

Possible value: <mac> : mac address

Example:

```
SP1659P(mac-table-alias)# del 00-44-33-44-55-44
```

set

Syntax: set <mac> <alias>

Description: To set up the mac alias entry.

Argument:

<mac> : mac address, format: 00-02-03-04-05-06

<alias> : mac alias name, max. 15 characters

Possible value: None

Example:

```
SP1659P(mac-table-alias)# set 00-44-33-44-55-44 www
```

show

Syntax: show

Description: To display the mac alias entry.

Argument: None

Possible value: None

Example:

```
SP1659P(mac-table-alias)# show
MAC Alias List
      MAC Address          Alias
----- ----------------- ----------------
1)    00-02-03-04-05-06 aaa
2)    00-33-03-04-05-06 ccc
3)    00-44-33-44-55-44 www
```

<<information>>

search

Syntax: search <port> <mac> <vid>

Description: To look for the relative mac information in mac table.

Argument:

<port> : set up the range of the ports to search for, syntax 1,5-7, available form 1 to 24

<mac> : mac address, format: 01-02-03-04-05-06, '?' can be used

<vid> : vlan id, from 1 to 4094; '?' as don't care, 0 as untagged

Possible value: None

Example:

```
SP1659P(mac-table-information)# search 1-24 ??-??-??-??-??-?? ?
MAC Table List
Alias              MAC Address        Port VID   State
---------------- ----------------- ---- ---- -----------------
                   00-11-3B-88-00-06     1    0   Dynamic
SP1659P(mac-table-information)#
```

show

Syntax: Show

Description: To display all mac table information.

Argument: None

Possible value: None

Example:

```
SP1659P(mac-table-information)# show
MAC Table List
Alias              MAC Address        Port VID   State
---------------- ----------------- ---- ---- -----------------

SP1659P(mac-table-information)#
```

<<maintain>>

set aging

Syntax: set aging <#>

Description: To set up the age out time of dynamic learning mac.

Argument: <#>: age-timer in seconds, 0, 10 to 65535. The value “0” means to disable aging

Possible value: <#>: 0, 10 to 65535.

Example:

```
SP1659P(mac-table-maintain)# set aging 300
SP1659P(mac-table-maintain)#
```

set learning

Syntax: set learning

Description: To set up the maximum amount of MAC that each port can learn.

Argument:

<port>: port range, syntax 1,5-7, available form 1 to 24

<num>: MAC address numbers which can be dynamically learned.

Num range: between 0 to 8191; 0 for learning disabled

Possible value:

<port>: 1 to 24

<num>: 0 to 8191

Example:

```
SP1659P(mac-table-maintain)# set learning 5 100
```

show

Syntax: show

Description: To display the settings of age-timer.

Argument: None

Possible value: None

Example:

```
SP1659P(mac-table-maintain)# show
Mac table ageout time: 300 seco
 Port    Dynamically learn limit
------ ----------------------
    1     8191
    2     8191
    3     8191
    4     8191
    5     8191
    6     8191
    7     8191
    8     8191
    9     8191
   10     8191
   11     8191
   12     8191
   13     8191
   14     8191
   15     8191
   16     8191
   17     8191
   18     8191
   19     8191
   20     8191
   21     8191
   22     8191
   23     8191
   24     8191
   25     8192
   26     8192

SP1659P(mac-table-maintain)#
```

<<static-mac>>

add

Syntax: add <mac> <vid> <queue> <rule> <port>

Description: To add the static mac entry.

Argument:

<mac>: mac address, format: 01-02-03-04-05-06

<vid>: vlan id, from 1 to 4094

<queue>: which queue you want to set, from 0 to 3

<rule>: forwarding rule, from 0 to 2

0: static

1: drop destination address matches

2: drop source address matches

<port>: forwarded destination port, form 1 to 26

Possible value:

<vid>: 1 to 4094

<queue>: 0 to 3

<rule>: 0 to 2

<port>: 1 to 26

Example:

```
SP1659P(mac-table-static-mac)# add 00-22-44-55-66-77 1 0 0 6
SP1659P(mac-table-static-mac)#
```

del

Syntax: del <mac>

Description: To remove the static MAC entry.

Argument:

<mac> : mac address, format: 00-02-03-04-05-06

Possible value:

<mac> : mac address

Example:

```
SP1659P(mac-table-static-mac)# del 00-02-03-04-05-06
SP1659P(mac-table-static-mac)#
```

show

Syntax: show

Description: To display the static MAC entry.

Argument: None

Possible value: None

Example:

```
SP1659P(mac-table-static-mac)# show filter
SP1659P(mac-table-static-mac)# show
          MAC                VID     Queue      Forwarding Rule                Port
------ ----------------- ------ -------- ------------------------------ ------
   1)  00-22-44-55-66-77      1         0    Static                           6

SP1659P(mac-table-static-mac)#
```

4.3.16 Management

add

Syntax:

Usage: set [<name> <value>] [<vid> <value>] [<ip> <value>] [<port> <value>] [<type> <value>] <action> <value>

Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90 port 2-5,8 type h,s action a

Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90

Description: To save the adding management policy records.

Argument:

[<name> <value>]	CL entry name.
[<vid> <value>]	VLAN ID.
[<ip> <value>]	IP range.
[<port> <value>]	Incoming port.
[<type> <value>]	Access type.
<action> <value>	a(ccept) or d(eny).

Possible value:

[<vid> <value>]	The range is 1-4095 and can be set to any.
[<ip> <value>]	For example, 192.168.1.90-192.168.1.90 or any.
[<port> <value>]	For example, 1 or 1-8 or 1,3-5 or any
[<type> <value>]	For example, h(ttp),s(nmp),t(elnet) or any.
<action> <value>	No default and it must be set.

Example:

```
SP1659P(management-add)# set name Mary vid 20 ip 192.168.1.1-192.168.1.90 port 2-5,8 type h,s action
a
SP1659P(management-add)# show

 #: 1
Name : Mary                VlanID : 20          IP : 192.168.1.1-192.168.1.90
Type : Http,SNMP           Action : Accept      Port : 2,3,4,5,8
```

delete

Syntax: delete #

Description: To delete a specific record or range.

Argument: <#>: a specific or range management security entry(s)

Possible value: none

Example:

```
SP1659P(management)# show

 #: 1
Name : Tom                 VlanID : 2           IP : 192.168.1.30-192.168.1.80
Type : SNMP                Action : Deny        Port : 1,2

SP1659P(management)# delete 1

SP1659P(management)# show

Security rule list is empty now
```

edit

Syntax:

Usage: edit [<name> <value>] [<vid> <value>] [<ip> <value>] [<port> <value>] [<type> <value>] <action> <value>

Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90 port 2-5,8
type h,s action a

Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90

Description: To edit management policy record.

Argument:

[<name> <value>]	ACL entry name.
[<vid> <value>]	VLAN ID.
[<ip> <value>]	IP Range.
[<port> <value>]	Incoming port.
[<type> <value>]	Access type.
<action> <value>	a(ccept) or d(eny).

Possible value:

[<name> <value>]	No default and it must be set.
[<vid> <value>]	The range is 1-4095 and can be set to any.
[<ip> <value>]	For example, 192.168.1.90-192.168.1.90 or any
[<port> <value>]	For example, 1 or 1-8 or 1,3-5 or any
[<type> <value>]	For example, h(ttp),s(nmp),t(elnet) or any
<action> <value>	No default and it must be set.

Example:

```
SP1659P(management)# edit 1

SP1659P(management-edit-1)# set name Tom vid 2 ip 192.168.1.30-192.168.1.80 port 1-2 type s action d
SP1659P(management-edit-1)# show

 #: 1
Name : Tom                VlanID : 2          IP : 192.168.1.30-192.168.1.80
Type : SNMP               Action : Deny       Port : 1,2
```

show

Syntax: show

Description: To show the specific management policy record.

Argument: none

Possible value: none

Example:

```
SP1659P(management)# show

#: 1
Name : Tom                VlanID : 2          IP : 192.168.1.30-192.168.1.80
Type : SNMP               Action : Deny       Port : 1,2
```

4.3.17 poe

set priority

Syntax: set priority <port-range> <priority>

Description: To set the PoE priority on ports.

Argument:

<port-range>：which port(s) you want to set, syntax 1,5-7, available from 1 to 24

<priority>: set priority as 0:Low, 1:Normal, 2:High

Possible value:

<port range>: 1 to 24

<priority>: 0, 1 or 2

Example:

```
SP1659P(poe)# set priority 1-12 2
```

set state

Syntax: set state <port-range> <state>

Description: To set the PoE state on ports.

Argument:

<port-range>：which port(s) you want to set, syntax 1,5-7, available from 1 to 24

<state>: enable or disable PoE function. 0: Disable, 1: Enable

Possible value:

<port-range>：1 to 24

<state>: 0 or 1

Example:

```
SP1659P(poe)# set state 11 0
SP1659P(poe)#
```

show

Syntax: Show

Description: To display the PoE status.

Argument: None

Possible value: None

Example:

```
SP1659P(poe)# show
Vmain              : 48.1 V
Imain              : 0.06 A
Pconsume           : 3.1 W
Power Limit        : 185 W
Temperature        : 40 'C / 104 'F

Port No                      | 1  2  3  4  5  6  7  8  9  10  11  12
-----------------------------| -  -  -  -  -  -  -  -  -  --  --  --
Port On                      | X  V  X  X  X  X  X  X  X  X   X   X
AC Disconnect Port Off       | X  X  X  X  X  X  X  X  X  X   X   X
DC Disconnect Port Off       | X  X  X  X  X  X  X  X  X  X   X   X
Overload Port Off            | X  X  X  X  X  X  X  X  X  X   X   X
Short Circuit Port Off       | X  X  X  X  X  X  X  X  X  X   X   X
Over Temp. Protection        | X  X  X  X  X  X  X  X  X  X   X   X
Power Management Port Off    | X  X  X  X  X  X  X  X  X  X   X   X

Port No                      | 13 14 15 16 17 18 19 20 21 22  23  24
-------------------------    | -- -- -- -- -- -- -- -- -- --  --  --
Port On                      | X  X  X  X  X  X  X  X  X  X   X   X
AC Disconnect Port Off       | X  X  X  X  X  X  X  X  X  X   X   X
DC Disconnect Port Off       | X  X  X  X  X  X  X  X  X  X   X   X
Overload Port Off            | X  X  X  X  X  X  X  X  X  X   X   X
Short Circuit Port Off       | X  X  X  X  X  X  X  X  X  X   X   X
Over Temp. Protection        | X  X  X  X  X  X  X  X  X  X   X   X
Power Management Port Off    | X  X  X  X  X  X  X  X  X  X   X   X

Port Status   State      Priority  Power(W) Current(mA) Class
-------------------------------------------------------------------
   1  Normal Enable     Normal      0.0        0          0
   2  Active Enable     Normal      3.0        66         2
   3  Normal Enable     Normal      0.0        0          0
   4  Normal Enable     Normal      0.0        0          0
   5  Normal Enable     Normal      0.0        0          0
   6  Normal Enable     Normal      0.0        0          0
   7  Normal Enable     Normal      0.0        0          0
   8  Normal Enable     Normal      0.0        0          0
   9  Normal Enable     Normal      0.0        0          0
```

10	Normal Enable	Normal	0.0	0	0
11	Normal Enable	Normal	0.0	0	0
12	Normal Enable	Normal	0.0	0	0
13	Normal Enable	Normal	0.0	0	0
14	Normal Enable	Normal	0.0	0	0
15	Normal Enable	Normal	0.0	0	0
16	Normal Enable	Normal	0.0	0	0
17	Normal Enable	Normal	0.0	0	0
18	Normal Enable	Normal	0.0	0	0
19	Normal Enable	Normal	0.0	0	0
20	Normal Enable	Normal	0.0	0	0
21	Normal Enable	Normal	0.0	0	0
22	Normal Enable	Normal	0.0	0	0
23	Normal Enable	Normal	0.0	0	0
24	Normal Enable	Normal	0.0	0	0

```
SP1659P(poe)#
```

4.3.18 port

clear counter

Syntax: clear counter

Description: To clear all ports' counter (include simple and detail port counter) information.

Argument: None

Possible value: None

Example:

```
SP1659P (port)# clear counter
```

disable state

Syntax: disable state <range>

Description: To disable the communication capability of the port.

Argument: <range>: syntax 1, 5-7, available from 1 to 26

Possible value: <range>: 1 ~ 26

Example:

```
SP1659P (port)# disable state 12
```

enable state

Syntax: enable state <range>

Description: To enable the communication capability of the port.

Argument: <range>: syntax 1, 5-7, available from 1 to 26

Possible value: <range>: 1 ~ 24

Example:

```
SP1659P (port)# enable state 3-12
```

set flow-control

Syntax: set flow-control <range> <symmetric | asymmetric>

Description: To set the flow control function of all ports.

Argument:

<range>:port range, syntax 1,5-7, available from 1 to 26

<symmetric>: set its flow control as symmetric

<asymmetric>: set its flow control as asymmetric

Possible value:

<range>: 1 to 26

<symmetric | asymmetric>:symmetric or asymmetric

Example:

```
SP1659P(port)# set flow-control 3-6 symmetric
```

set speed-duplex

Syntax: set speed-duplex <range> <auto>|[<10 | 100 | 1000> <half | full>]

Description: To set up the speed and duplex of all ports.

Argument:

<range>:syntax 1,5-7, available from 1 to 26

auto: set auto-negotiation mode

10: set speed to 10M

100: set speed to 100M

1000: set speed to 1000M

half: set to half duplex

full: set to full duplex

Possible value:

<range>: 1 to 26

<port-speed> : auto, 10, 100, 1000

<port-duplex> : full, half

Example:

```
SP1659P(port)# set speed-duplex 8 100 full
```

show conf

Syntax: show conf

Description: To display the each port's configuration about state, speed-duplex and flow control.

Argument: None

Possible value: None

Example:

```
SP1659P (port)# show conf
```

show detail-counter

Syntax: show detail-counter <range>

Description: To display the detailed counting number of each port's traffic.

Argument: <range>: port, syntax 1,5-7, available from 1 to 24

Possible value: <range>:1 ~ 24

Example:

```
SP1659P (port)# show detail-counter 5
```

show media

Syntax: show sfp <port>

Description: To display the module 25 or 26 information.

Argument: <port>: available 25, 26

Possible value: <port>: 25, 26

Example:

```
SP1659P (port)# show media 26
Port 26 Fiber Media Information
-----------------------------------------------
Connector Type          : SFP - LC
Fiber Type              : Single Mode (SM)
```

```
Tx Central Wavelength  : 0
Baud Rate              : 1G
Vendor OUI             : 00:00:00
Vendor Name            : TechCOM
Vendor PN              : PT4-S1-4103C
Vendor Rev             :
Vendor SN              : 5061852001
Date Code              : 050601
Temperature            : none
Vcc                    : none
Mon1 (Bias) mA         : none
Mon2 (TX PWR)          : none
Mon3 (RX PWR)          : none
```

show simple-counter

Syntax: show simple-counter

Description: To display the summary counting of each port's traffic.

Argument: None

Possible value: None

Example:

```
SP1659P (port)# show simple-counter
```

show status

Syntax: show status

Description: To display the port's current status.

Argument: None

Possible value: None

Example:

```
SP1659P (port)# show status
```

4.3.19 qos

disable 1q

Syntax: disable 1q

Description: To disable 802.1q QoS.

Argument:

None

Possible value:

None

Example:

```
SP1659P(qos)# disable 1q
```

disable dscp

Syntax: disable dscp

Description: To disable dscp QoS.

Argument:

None

Possible value:

None

Example:

```
SP1659P(qos)# disable dscp
```

disable qos

Syntax: disable qos

Description: To disable QoS.

Argument:

None

Possible value:

None

Example:

```
SP1659P(qos)# disable qos
```

disable tos

Syntax: disable tos

Description: To disable ToS.

Argument:

None

Possible value:

None

Example:

```
SP1659P(qos)# disable tos
```

enable 1q

Syntax: enable 1q

Description: To enable 802.1q QoS.

Argument:

None

Possible value:

None

Example:

```
SP1659P(qos)# enable 1q
```

enable dscp

Syntax: enable dscp

Description: To enable dscp QoS.

Argument:

None

Possible value:

None

Example:

```
SP1659P(qos)# enable dscp
```

enable qos

Syntax: enable qos

Description: To enable QoS.

Argument:

None

Possible value:

None

Example:

```
SP1659P(qos)# enable qos
```

enable tos

Syntax: enable tos

Description: To enable ToS.

Argument:

None

Possible value:

None

Example:

```
SP1659P(qos)# enable tos
```

set dscp

Syntax: set dscp [<q0><priority>] [<q1><priority>] [<q2><priority>] [<q3><priority>]

Description: To set IP DSCP qos weighting for 4 queues.

Argument:

<q>: queue level, q0: queue 0; q1: queue 1; q2: queue 2; q3: queue 3.

<priority>: priority level. One queue has been assigned 2 different priorities. You don't need to use all of queue, but must assign queue in order. Syntax: 1, 2 or 2, 5-7, available from 0 to 63.

Possible value: <priority>: 0 to 63

Example:

```
SP1659P(qos)# set dscp q0 2 q1 2 q2 2 q3 3
```

set pri-tag

Syntax: set pri-tag [<q0><priority>] [<q1><priority>] [<q2><priority>] [<q3><priority>]

Description: To set 802.1p qos weighting for 4 queues.

Argument:

<q>: queue level, q0: queue 0, q1: queue 1, q2: queue 2, q3: queue 3.

<priority>: priority level. One queue has been assigned 2 different priorities. You don't need to use all of queues, but must assign queues in order. Syntax: 1, 2 or 2, 5-7, available from 0 to 7.

Possible value:

<priority>: 0 to 7.

Example:

```
SP1659P(qos)# set pri-tag q0 0 q1 2 q3 4
```

set sche

Syntax: set sche <wrr|strict> <wrr_0> <wrr_1> <wrr_2> <wrr_3>

Description: To qos schedule and weight for 4 queues.

Argument:

<wrr>: scheduling weighted round robin method

<strict>: scheduling strict method.

<wrr_0 to 3>: weighted for every queue. Weighted range: 1-55.

Possible value:

<wrr|strict>: wrr or strict

<wrr_0 to 3>: 1-55.

Example:

```
SP1659P(qos)# set sche wrr 1 2 8 16
```

set tos

Syntax: set tos <type_value> [<q0><priority>] [<q1><priority>] [<q2><priority>] [<q3><priority>]

Description: To set IP tos qos weighting for 4 queues.

Argument:
<type_value>: Delay Priority: 0;
Throughput Priority: 1;
Reliability Priority: 2;
Monetary Cost Priority: 3.
<q>: queue level, q0: queue 0, q1: queue 1, q2: queue 2, q3: queue 3.
<priority>: priority level. One queue has been assigned 2 different priorities. You don't need to use all of queues, but must assign queues in order (from low queue to high queue).
Syntax: 1, 2 or 2, 5-7, available from 0 to 7.
Possible value:
<type_value>: 0 to 3.
<priority>: 0 to 7.
Example:

```
SP1659P(qos)# set tos 0 q0 1 q1 2 q2 4 q3 6
```

set vip

Syntax: set vip <port_range> <mode>
Description: To set vip port for strict priority.
Argument:
<port_range>: syntax 1, 5-7, available from 1 to 26
<mode>: enable/disable vip port for each port. 1: enable. 0: disable.
Possible value:
<port_range>: 1 to 26
<mode>: 1 or 0
Example:

```
SP1659P(qos)# set vip 1-6 1
```

show

Syntax:
show dscp
show port
show priority-tag
show tos
Description: To display Qos configuration.
Argument: None
Possible value: None
Example:

```
SP1659P (qos)# show dscp
ip diffserv classification
====================
Global QoS mode:  Disable QoS
                  Disable 802.1p Priority
                  Disable ip tos classification
                  Disable ip diffserv classification
Scheduling:       weighted round robin method.
Weight:           wrr 0 = 1; wrr 1 = 2; wrr 2 = 4; wrr 3 = 8.
                  Weighted range: 1~55.
P0~63:            Priority 0~63.
Default mode:     Queue0: P0~15; Queue1: P16~31; Queue2: P32~47; Queue3: P48~63.
```

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

```
SP1659P(qos)# show port
Port Based Priority
====================
Global QoS mode:  Disable QoS
                  Disable 802.1p Priority
                  Disable ip tos classification
                  Disable ip diffserv classification
```

Port No	Mode	Port No	Mode
1	Disable	2	Disable
3	Disable	4	Disable
5	Disable	6	Disable
7	Disable	8	Disable
9	Disable	10	Disable
11	Disable	12	Disable
13	Disable	14	Disable
15	Disable	16	Disable
17	Disable	18	Disable
19	Disable	20	Disable
21	Disable	22	Disable
23	Disable	24	Disable
25	Disable	26	Disable

```
SP1659P(qos)# show priority-tag
802.1p priority
====================
Global QoS mode:  Disable QoS
                  Disable 802.1p Priority
                  Disable ip tos classification
                  Disable ip diffserv classification
Scheduling:       weighted round robin method.
weight:           wrr 0 = 1; wrr 1 = 2; wrr 2 = 4; wrr 3 = 8.
                  weighted range: 1~55.
P0~7:             Priority 0~7.
Default mode:     Queue0: P0,P1; Queue1: P2,P3; Queue2: P4,P5; Queue3: P6,P7.
```

	P0	P1	P2	P3	P4	P5	P6	P7
Queue	0	0	1	1	2	2	3	3

```
SP1659P(qos)# show tos
ip tos classification
====================
Global QoS mode:  Disable QoS
```

```
                    Disable 802.1p Priority
                    Disable ip tos classification
                    Disable ip diffserv classification
Scheduling:         weighted round robin method.
weight:             wrr 0 = 1; wrr 1 = 2; wrr 2 = 4; wrr 3 = 8.
                    weighted range: 1~55.
P0~7:               Priority 0~7.
Default mode:       Queue0: P0,P1; Queue1: P2,P3; Queue2: P4,P5; Queue3: P6,P7.

        P0   P1   P2   P3   P4   P5   P6   P7
       ---- ---- ---- ---- ---- ---- ---- ----
Queue   0    0    1    1    2    2    3    3
TOS type: Delay Priority

        P0   P1   P2   P3   P4   P5   P6   P7
       ---- ---- ---- ---- ---- ---- ---- ----
Queue   0    0    1    1    2    2    3    3
TOS type: Throughput Priority

        P0   P1   P2   P3   P4   P5   P6   P7
       ---- ---- ---- ---- ---- ---- ---- ----
Queue   0    0    1    1    2    2    3    3
TOS type: Reliability Priority

        P0   P1   P2   P3   P4   P5   P6   P7
       ---- ---- ---- ---- ---- ---- ---- ----
Queue   0    0    1    1    2    2    3    3
TOS type: Monetary Cost Priority
```

4.3.20 reboot

reboot

Syntax: reboot

Description: To reboot the system.

Argument: None

Possible value: None

Example:

```
SP1659P# reboot
```

4.3.21 security

<<Isolated Group>>

set

Syntax: set <port>

Description: To set up the function of the isolated group.

Argument: <port>: isolated port; range syntax: 1, 5-7, available from 0 to 26. Set 0 as disabled

Possible value: <port>:0 to 26

Example:

```
SP1659P(security)# isolated-group
SP1659P(security-isolated-group)# set 2,3,4
```

show

Syntax: show

Description: To display the current setting status of isolated group.

Argument: None

Possible value: None

Example:

```
SP1659P(security-isolated-group)# show
Isolated group:
2 3 4
```

<<Mirror>>

enable

Syntax: enable mirror

Description: To enable the function of mirror.

Argument: None

Possible value: None

Example:

```
SP1659P(security-mirror)# enable mirror
```

disable

Syntax: disable mirror

Description: To disable the function of mirror.

Argument: None

Possible value: None

Example:

```
SP1659P(security-mirror)# disable mirror
```

set

Syntax: set <spy> <ingress> <egress>

Description:

To set up the monitoring port and monitored ports of the mirror function. User can monitor the ports that receive or transmit the packets.

Argument:

<spy>: monitoring port

<ingress>: monitored ingress port; range syntax: 1,5-7, available from 0 to 26

<egress>: monitored egress port; range syntax: 1,5-7, available from 0 to 26

Set ingress/egress to 0 as ingress/egress disabled

Possible value:

<ingress>: 0 to 26

<egress>: 0 to 26

Example:

```
SP1659P(security-mirror)# set 1 4 2-3
```

show

Syntax: show

Description: To display the current setting status of isolated group.

Argument: None

Possible value: None

Example:

```
SP1659P(security-isolated-group)# show
Isolated group:
2 3 4
```

<<Restricted Group>>

set

Syntax: set <ingress> <egress>

Description: To set up the function of the restricted group.

Argument:

<ingress>: ingress group port; range syntax: 1,5-7, available from 0 to 26

<egress>: egress group port; range syntax: 1,5-7, available from 0 to 26

Set ingress or egress to 0 as disabled

Possible value: <port>:0 to 26

<ingress>: 0 to 26

<egress>: 0 to 26

Example:

```
SP1659P(security-restricted-group)# set 5 8-10
```

show

Syntax: show

Description: To display the current setting status of restricted group.

Argument: None

Possible value: None

Example:

```
SP1659P(security-restricted-group)# show
Restricted group:
Ingress:5
Egress :8 9 10
```

4.3.22 snmp

disable

Syntax:

disable set-community

disable snmp

Description: The Disable here is used for the de-activation of snmp or set-community.

Argument: None

Possible value: None

Example:

```
SP1659P(snmp)# disable snmp
SP1659P(snmp)# disable set-community
```

enable

Syntax:

enable set-community

enable snmp

Description: The Enable here is used for the activation snmp or set-community.

Argument: None

Possible value: None

Example:

```
SP1659P(snmp)# enable snmp
SP1659P(snmp)# enable set-community
```

set

Syntax:

set get-community <community>

set set-community <community>

set trap <#> <ip> [port] [community]

Description:

The Set here is used for the setup of get-community, set-community, trap host ip, host port and trap-community.

Argument:

<#>: trap number

<ip>: ip address or domain name

<port>: trap port

<community>: trap community name

Possible value:

<#>: 1 to 6

<port>:1~65535

Example:

```
SP1659P(snmp)# set get-community public
SP1659P(snmp)# set set-community private
SP1659P(snmp)# set trap 1 192.168.1.1 162 public
```

show

Syntax: show

Description: The Show here is to display the configuration of SNMP.

Argument: None.

Possible value: None.

Example:

```
SP1659P(snmp)# show
SNMP                : Enable
Get Community   : public
Set Community   : private [Enable]
Trap Host 1 IP Address: 192.168.1.1   Port: 162  Community: public
Trap Host 2 IP Address: 0.0.0.0       Port: 162  Community: public
Trap Host 3 IP Address: 0.0.0.0       Port: 162  Community: public
Trap Host 4 IP Address: 0.0.0.0       Port: 162  Community: public
Trap Host 5 IP Address: 0.0.0.0       Port: 162  Community: public
Trap Host 6 IP Address: 0.0.0.0       Port: 162  Community: public
```

4.3.23 stp

MCheck

Syntax: MCheck <range>

Description: To force the port to transmit RST BPDUs.

Argument: <range>: syntax 1, 5-7, available from 1 to 26

Possible value: <range>: 1 to 26

Example:

```
SP1659P(stp)# Mcheck 1-8
```

disable

Syntax: disable

Description: To disable the STP function.

Argument: None

Possible value: None

Example:

```
SP1659P(stp)# disable
```

enable

Syntax: enable

Description: To enable the STP function.

Argument: None

Possible value: None

Example:

```
SP1659P(stp)# enable
```

set config

Syntax: set config <Bridge Priority> <Hello Time> <Max. Age> <Forward Delay>

Description: To set up the parameters of STP.

Argument:

<Bridge Priority>: priority must be a multiple of 4096, available from 0 to 61440.

<Hello Time>: available from 1 to 10.

<Max. Age>: available from 6 to 40.

<Forward Delay>: available from 4 to 30.

Note: 2*(Forward Delay -1) >= Max Age, Max Age >= 2*(Hello Time +1)

Possible value:

<Bridge Priority>: 0 to 61440

<Hello Time>: 1 to 10

<Max. Age>: 6 to 40

<Forward Delay>: 4 to 30

Example:

```
SP1659P(stp)# set config 61440 2 20 15
```

set port

Syntax: set port <range> <path cost> <priority> <edge_port> <admin p2p>

Description: To set up the port information of STP.

Argument:

<range>: syntax 1,5-7, available from 1 to 26

<path cost>: 0, 1-200000000. The value zero means auto status

<priority>: priority must be a multiple of 16, available from 0 to 240

<edge_port>: Admin Edge Port, <yes|no>

<admin p2p>: Admin point to point, <auto|true|false>

Possible value:

<range>:1 to 26

<path cost>: 0, 1-200000000

<priority>: 0 to 240

<edge_port>: yes / no

<admin p2p>: auto / true / false

Example:

```
SP1659P(stp)# set port 1-16 0 128 yes auto
```

set version

Syntax: set version <stp|rstp>

Description: To set up the version of STP.

Argument: <stp|rstp>:stp / rstp

Possible value: <stp|rstp>:stp / rstp

Example:

```
SP1659P(stp)# set version rstp
```

show config

Syntax: show config

Description: To display the configuration of STP.

Argument: None

Possible value: None

Example:

```
SP1659P(stp)# show config
STP State Configuration      :
Spanning Tree Protocol       : Enabled
Bridge Priority (0-61440)    : 61440
Hello Time (1-10 sec)        : 2
Max. Age (6-40 sec)          : 20
Forward Delay (4-30 sec)     : 15
Force Version                : RSTP
```

show port

Syntax: show port

Description: To display the port information of STP.

Argument: None

Possible value: None

Example:

```
SP1659P# stp
SP1659P(stp)# show port
```

Port	Port Status	Path Cost	Priority	Admin Edge Port	Admin Point To Point
1	DISCARDING	2000000	128	No	Auto
2	DISCARDING	2000000	128	No	Auto
3	DISCARDING	2000000	128	No	Auto
4	DISCARDING	2000000	128	No	Auto
5	DISCARDING	2000000	128	No	Auto
6	DISCARDING	2000000	128	No	Auto
7	DISCARDING	2000000	128	No	Auto
8	DISCARDING	2000000	128	No	Auto
9	DISCARDING	2000000	128	No	Auto
10	DISCARDING	2000000	128	No	Auto
11	DISCARDING	2000000	128	No	Auto
12	DISCARDING	2000000	128	No	Auto
13	DISCARDING	2000000	128	No	Auto
14	DISCARDING	2000000	128	No	Auto
15	DISCARDING	2000000	128	No	Auto
16	DISCARDING	2000000	128	No	Auto
17	DISCARDING	2000000	128	No	Auto
18	DISCARDING	2000000	128	No	Auto
19	DISCARDING	2000000	128	No	Auto
20	DISCARDING	2000000	128	No	Auto
21	DISCARDING	2000000	128	No	Auto

22	DISCARDING	2000000	128	No	Auto
23	DISCARDING	2000000	128	No	Auto
24	DISCARDING	2000000	128	No	Auto

show status

Syntax: show status

Description: To display the status of STP.

Argument: None

Possible value: None

Example:

```
SP1659P(stp)# show status
STP Status :
STP State                          : Enabled
Bridge ID                          : 00:11:3B:D8:09:1D
Bridge Priority                    : 61440
Designated Root                    : 00:11:3B:D8:09:1D
Designated Priority                : 61440
Root Port                          : 0
Root Path Cost                     : 0
Current Max. Age(sec)              : 20
Current Forward Delay(sec)         : 15
Hello Time(sec)                    : 2
STP Topology Change Count          : 0
Time Since Last Topology Change(sec)  : 848
```

4.3.24 system

set contact

Syntax: set contact <contact string>

Description: To set the contact description of the switch.

Argument: <contact>:string length up to 40 characters.

Possible value: <contact>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.

Example:

```
SP1659P(system)# set contact Taipei
```

set device-name

Syntax: set device-name <device-name string>

Description: To set the device name description of the switch.

Argument: <device-name>: string length up to 40 characters.

Possible value: <device-name>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.

Example:

```
SP1659P(system)# set device-name CR-2600
```

set location

Syntax: set location <location string>

Description: To set the location description of the switch.

Argument: <location>: string length up to 40 characters.

Possible value: <location>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.

Example:

```
SP1659P(system)# set location Taipei
```

show

Syntax: show

Description: To display the basic information of the switch.

Argument: None

Possible value: None

Example:

```
SP1659P(system)# show
Model Name                      : SP1659P
System Description              : 24+2G PoE Management Switch
Location                        :
Contact                         :
Device Name                     : SP1659P
System Up Time                  : 0 Days 18 Hours 50 Mins 57 Secs
Current Time                    : Fri Sep 23 14:04:07 2005
BIOS Version                    : v1.04
Firmware Version                : v0.92
Hardware-Mechanical Version     : v1.01-v1.01
Serial Number                   : 031201000002
Host IP Address                 : 61.219.198.203
Host MAC Address                : 00-11-3b-ee-00-01
Device Port                     : UART * 1   TP *24   Fiber * 2
RAM Size                        : 16 M
Flash Size                      : 2 M

SP1659P(system)#
```

4.3.25 tftp

set server

Syntax: set server <ip>

Description: To set up the IP address of tftp server.

Argument: <ip>: the IP address of tftp server

Possible value: <ip>: tftp server ip

Example:

```
SP1659P(tftp)# set server 192.168.3.111
```

show

Syntax: show

Description: To display the information of tftp server.

Argument: None

Possible value: None

Example:

```
SP1659P(tftp)# show
Tftp Server : 192.168.3.111
```

4.3.26 time

set daylightsaving

Syntax: set daylightsaving <hr> <MM/DD/HH> <mm/dd/hh>

Description: To set up the daylight saving.

Argument:

hr: daylight saving hour, range: -5 to +5

MM: daylight saving start Month (01-12)
DD: daylight saving start Day (01-31)
HH: daylight saving start Hour (00-23)
mm: daylight saving end Month (01-12)
dd: daylight saving end Day (01-31)
hh: daylight saving end Hour (00-23)

Possible value:

hr: -5 to +5
MM: (01-12)
DD: (01-31)
HH: (00-23)
mm: (01-12)
dd: (01-31)
hh: (00-23)

Example:

```
SP1659P(time)# set daylightsaving 3 10/12/01 11/12/01
Save Successfully

SP1659P(time)#
```

set manual

Syntax: set manual <YYYY/MM/DD> <hh:mm:ss>

Description: To set up the current time manually.

Argument:

YYYY: Year (2000-2036)
MM: Month (01-12)
DD: Day (01-31)
hh: Hour (00-23)
mm: Minute (00-59)
ss: Second (00-59)

Possible value:

YYYY: (2000-2036)
MM: (01-12)
DD: (01-31)
hh: (00-23)
mm: (00-59)
ss: (00-59)

Example:

```
SP1659P(time)# set manual 2004/12/23 16:18:00
SP1659P(time)#
```

set ntp

Syntax: set ntp <ip> <timezone>

Description: To set up the current time via NTP server.

Argument:

<ip>: ntp server ip address or domain name
<timezone>: time zone (GMT), range: -12 to +13

Possible value:

<timezone>: -12,-11…,0,1…,13

Example:

```
SP1659P(time)# set ntp 210.59.157.10 8
SP1659P(time)#
```

show

Syntax: show

Description:

To show the time configuration, including “Current Time”, “NTP Server”,” Timezone”, ” Daylight Saving”,” Daylight Saving Start” and “Daylight Saving End”

Argument: None

Possible value: None

Example:

```
SP1659P(time)# show
Current Time              : Thu Thu 14 15:04:03 2005
NTP Server                : 209.81.9.7
Timezone                  : GMT+8:00
Day light Saving          : 0 Hours
Day light Saving Start    : Mth: 1 Day: 1 Hour: 0
Day light Saving End      : Mth: 1 Day: 1 Hour: 0
SP1659P(time)#
```

4.3.27 trunk

del trunk

Syntax: del trunk <port-range>

Description: To delete the trunk port.

Argument: <port-range>: port range, syntax 1,5-7, available from 1 to 24

Possible value: <port-range>: 1 to 24

Example:

```
SP1659P(trunk)# del trunk 1
SP1659P(trunk)#
```

set priority

Syntax: set priority <range>

Description: To set up the LACP system priority.

Argument: <range>: available from 1 to 65535.

Possible value: <range>: 1 to 65535, default: 32768

Example:

```
SP1659P(trunk)# set priority 33333
SP1659P(trunk)#
```

set hash

Syntax: set hash <method>

Description: To set up trunk hash method.

Argument:

<method>: lacp hash method

0: DA and SA

1: SA

2: DA

Possible value: <method>: 0~2

Example:

```
SP1659P(trunk)# set hash 2
SP1659P(trunk)#
```

set trunk

Syntax: set trunk <port-range> <method> <group> <active LACP>

Description: To set up the status of trunk, including the group number and mode of the trunk as well as LACP mode.

Argument:

<port-range> : port range, syntax 1,5-7, available from 1 to 24

<method>:

static : adopt the static link aggregation

lacp : adopt the dynamic link aggregation- link aggregation control protocol

<group>: 1-8.

<active LACP>:

active : set the LACP to active mode

passive : set the LACP to passive mode

Possible value: None

Example:

```
SP1659P(trunk)# set trunk 1-4 lacp 1 active
```

show aggtr-view

Syntax: show aggtr-view

Description: To display the aggregator list.

Argument: None

Possible value: None

Example:

```
SP1659P(trunk)# show aggtr-view
Aggregator  1)     Method: None
                   Member Ports: 1
                   Ready Ports:1

Aggregator  2)     Method: LACP
                   Member Ports: 2
                   Ready Ports:
                                :
                                :
                                :
```

show lacp-config

Syntax: show lacp-config

Description: To display the value of LACP Priority.

Argument: None

Possible value: None

Example:

```
SP1659P(trunk)# show lacp-config
LACP System Priority  : 32768
Hash Method           : DA and SA
```

show lacp-detail

Syntax: show lacp-detail <aggtr>

Description: To display the detailed information of the LACP trunk group.

Argument: <aggtr>: aggregator, available from 1 to 24

Possible value: <aggtr>: 1 to 24

Example:

```
SP1659P(trunk)# show lacp-detail 2
Aggregator 2 Information:
                    Actor                                  Partner
---------------------------------------- ----------------------------------------
System Priority      MAC Address          System Priority      MAC Address
---------------      -------------------- -----------------    ----------------------
     32768           00-11-3B-e8-00-02        32768            00-00-00-00-00-00

 Port      Key       Trunk Status           Port                 Key
------ --------      ----------------    -------------- -----------------
   2       257             ---              2                    0
```

show status

Syntax: show status

Description: To display the aggregator status and the settings of each port.

Argument: None

Possible value: None

Example:

```
SP1659P(trunk)# show status
            Trunk Port Setting                Trunk Port Status
------------------------------------ ----------------------
 port     Method     Group     Active LACP     Aggregator     Status
=== ======== ======= ============= =========
   1        None        0          Active           1          Ready
   2        LACP        1          Active           2           ---
   3        LACP        1          Active           3           ---
   4        LACP        1          Active           4           ---
   5        LACP        1          Active           5           ---
   6        LACP        1          Active           6           ---
   7        LACP        1          Active           7           ---
                                          :
                                          :
  19        None        0          Active          19           ---
  20        None        0          Active          20           ---
  21        None        0          Active          21           ---
  22        None        0          Active          22           ---
  23        None        0          Active          23           ---
  24        None        0          Active          24           ---
  25        None        0          Active          25          Ready
  26        None        0          Active          26          Ready
```

4.3.28 vlan

del port-group <name>

Syntax: del port-group <name>

Description: To delete the port-based vlan group.

Argument: <name>: which vlan group you want to delete.

Possible value: <name>: port-vlan name

Example:

```
SP1659P(vlan)# del port-group VLAN-2
```

del tag-group <vid>

Syntax: del tag-group <vid>

Description: To delete the tag-based vlan group.

Argument: <vid>: which vlan group you want to delete, available from 1 to 4094

Possible value: <vid>: 1 to 4094

Example:

```
SP1659P(vlan)# del tag-group 2
```

disable double-tag

Syntax: disable double-tag

Description: To disable double-tag

Argument: None

Possible value: None

Example:

```
SP1659P(vlan)# disable double-tag
```

disable drop-untag

Syntax: disable drop-untag <range>

Description: Don’t drop the untagged frames.

Argument: <range> : which port(s) you want to set, syntax 1,5-7, available from 1 to 26

Possible value: <range>: 1 to 26

Example:

```
SP1659P(vlan)# disable drop-untag 5-10
```

disable svl

Syntax: disable svl

Description: To enable Independent VLAN Learning.

Argument: None

Possible value: None

Example:

```
SP1659P(vlan)# disable svl
```

disable symmetric

Syntax: disable symmetric

Description: Don’t drop frames from the non-member port.

Argument: None

Possible value: None

Example:

```
SP1659P(vlan)# disable symmetric
```

enable double-tag

Syntax: enable double-tag

Description: To enable double-tag

Argument: None

Possible value: None

Example:

```
SP1659P(vlan)# enable double-tag
```

enable drop-untag

Syntax: enable drop-untag <range>

Description: Drop the untagged frames.

Argument: <range> : which port(s) you want to set, syntax 1,5-7, available from 1 to 26

Possible value: <range>: 1 to 26

Example:

```
SP1659P(vlan)# enable drop-untag 5-10
```

enable svl

Syntax: enable svl

Description: To enable Shared VLAN Learning.

Argument: None

Possible value: None

Example:

```
SP1659P(vlan)# enable svl
```

enable symmetric

Syntax: enable symmetric

Description: Drop frames from the non-member port.

Argument: None

Possible value: None

Example:

```
SP1659P(vlan)# enable symmetric
```

set mode

Syntax: set mode <port|tag>

Description: To switch vlan mode between port-based and tag-based modes.

Argument:

<port|tag>: port or tag

tag: set tag-based vlan

port: set port-based vlan

Possible value:

<port|tag>: port or tag

Example:

```
SP1659P(vlan)# set mode tag
```

set port-group

Syntax: set port-group <name> <range>

Description: To add or edit a port-based VLAN group.

Argument:

<name>: port-vlan name

<range>: syntax 1,5-7, available from 1 to 26

Possible value: <range>: 1 to 26

Example:

```
SP1659P(vlan)# set port-group VLAN-1 2-5,6,15-13
```

set pvid

Syntax: set pvid <port_range> <pvid> <default_priority>

Description: To set vlan PVID and port pripority.

Argument:

<port_range>: which port(s) you want to set PVID(s). Syntax 1, 5-7, available from 1 to 26

<pvid>: which PVID you want to set, available from 1 to 4094

<default_priority>: which priority you want to set, available from 0 to 7

Possible value:

<range>: 1 to 26

<pvid>: 1 to 4094

<default_priority>: 0 to 7

Example:

```
SP1659P(vlan)# set pvid 3,5,6-8 5 6
```

set tag-group

Syntax: set tag-group <vid> <name> <member_range> <untag_range>

Description: To add or edit the tag-based vlan group.

Argument:

<vid>: vlan id, from 1 to 4094

<name>: tag-vlan group name

<member_range>: member port; syntax: 1,5-7, available from 1 to 26

<untag_range>: untagged out port; syntax: 1,5-7, available from 0 to 26

Set untag_range to 0, as none of the ports are force untagged.

Possible value:

<vid>: 1 to 4094

<name>: tag-vlan group name

<member_range>: 1 to 26

<untag_range>: 0 to 26

Example:

```
SP1659P(vlan)# set tag-group 2 vlan-2 2-5,6,15-13 0
```

show config

Syntax: show config

Description: To display the current vlan mode, Symmetric vlan, SVL and Double tag states.

Argument: None

Possible value: None

Example:

```
SP1659P(vlan)# show config
Current vlan mode    :Tag-based vlan
Global setting:
Symmetric vlan       : Disable (Asymmetric)
SVL                  : Disable (IVL)
Double tag           : Disable

SP1659P(vlan)#
```

show group

Syntax: show group

Description: To display the vlan mode and vlan group.

Argument: None

Possible value: None

Example:

```
SP1659P(vlan)# show group
Vlan mode is tag-based.

1)  Name       :default
    VID        :1
    Member     :1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
    Untag      :1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

2)  Name       :VLAN-2
    VID        :2
```

```
    Member    :2 3 4 5 6 13 14 15
    Untag     :

SP1659P(vlan)#
```

show pvid

Syntax: show pvid

Description: To display pvid, priority and drop untag result.

Argument: None

Possible value: None

Example:

```
SP1659P(vlan)# show pvid
```

Port	PVID	Priority	Drop Untag
1	1	0	Disable
2	1	0	Disable
3	5	6	Disable
4	1	0	Disable
5	5	6	Disable
6	5	6	Disable
7	5	6	Disable
8	5	6	Disable
9	1	0	Disable
10	1	0	Disable
11	1	0	Disable
12	1	0	Disable
13	1	0	Disable
14	1	0	Disable
15	1	0	Disable
16	1	0	Disable
17	1	0	Disable
18	1	0	Disable
19	1	0	Disable
20	1	0	Disable
21	1	0	Disable
22	1	0	Disable
23	1	0	Disable
24	1	0	Disable
25	1	0	Disable
26	1	0	Disable

4.3.29 vs

disable

Syntax: disable

Description: To disable the virtual stack.

Argument: None

Possible value: None

Example:

```
SP1659P(vs)# disable
```

enable

Syntax: enable

Description: To enable the virtual stack.

Argument: None

Possible value: None

Example:

```
SP1659P(vs)# enable
```

set gid

Syntax: set gid <gid>

Description: To set the group id.

Argument: <gid>:Group ID

Possible value: <gid>:a-z,A-Z,0-9

Example:

```
SP1659P(vs)# set gid group1
```

set role

Syntax: set role <master|slave>

Description: To set role.

Argument: <master|slave>: master: act as master, slave: act as slave

Possible value: <master|slave>: master or slave

Example:

```
SP1659P(vs)# set role master
```

show

Syntax: show

Description: To display the configuration of the virtual stack.

Argument: None

Possible value: None

Example:

```
SP1659P(vs)# show
Virtual Stack Config:
State       : Enable
Role        : Master
Group ID    : group1
```

5. Specification

IEEE Standards		IEEE802.3, 10BASE-T IEEE802.3u, 100BASE-TX IEEE802.3ab, 1000BASE-T IEEE802.3z, 1000BASE-SX/LX IEEE802.3x, Flow Control IEEE802.3af, Power over Ethernet IEEE802.1q, Tag-based VLAN IEEE802.1q-in-q, Nested VLAN IEEE802.1p, Traffic Prioritization IEEE802.3ad, Link Aggregation Control Protocol IEEE802.1d, Spanning Tree Protocol IEEE802.1w, Rapid Spanning Tree Protocol IEEE802.1x, Port-based Authentication
Hardware & Performance	Processor SDRAM	16MB
	Processor Flash	2MB
	Packet Buffer	256KBytes
	MAC address table	8K entries
	10/100M, RJ-45	24
	10/100/1000M, RJ-45	2
	mini-GBIC slots	2 (share with Gigabit RJ-45 ports)
	Switching Fabric	8.8 Gbps
	Filtering/Forwarding Rate	10Mbps: 14,880pps/14,880pps 100Mbps: 148,800pps/148,800pps 1000Mbps: 1,488,000pps/1,488,000pps
	Switching Mechanism	Store and Forward
PoE		24 PoE ports of IEEE802.3af Power supplying up 185W totally (15.4 per port for 12 ports, 7.7W per port for 24 ports) Auto detect PD status, power consumption level, and power feeding priority

Key Features	Auto Negotiation Auto Uplink Flow Control for full duplex (IEEE802.3x) Link Aggregation Control Protocol (IEEE802.3ad) * Up to 3 groups of port trunk Port-based VLAN Tag-based VLAN (IEEE802.1q) * Max. 256 VLANs Nested (double tag) VLAN (IEEE802.q-in-q) GAVP VLAN Registration Protocol IGMPv1/2 Snooping and Filtering Spanning Tree Protocol (IEEE802.1d) Rapid Spanning Tree Protocol (IEEE802.1w) Port Mirror Broadcast Storm Control
Quality of Service	Traffic Classification (by CoS, ToS/IP Precedence, ToS/DSCP) Queuing (4 priority queuing per port) Scheduling (WRR, Strict) Bandwidth Control (Policing & Shaping)
Security	Port-based Authentication (IEEE802.1x) Built-in RADIUS proxy client Port Security with MAC address User Account Management Switch Access Mode Control (by IP filtering)
Management	Http, Telnet/Console (CLI), SNMP Virtual Stack (Single IP Management) E-mail / SMS alarm
SNMP & MIBs	SNMP v1/2c MIB II (RFC1213) Bridge MIB (RFC1493) RMON group 1,2,3,9 (RFC2819) Ether-like MIB (RFC1643) Private enterprise MIB
Emission	FCC Class A, CE
Environment	Temperature: 0 to 50˚C (operating) Humidity: 5% - 95%, non-condensing (operating)
Dimension & Weight	442 × 209 × 44 mm, 3.3 kg
Power Supply	100-240V AC, 50-60Hz