Gigabit Management Switch

SWG0802-SFP
SWG1604-SFP
SWG2404-SFP
SWG0816-SFP

User's Manual

Rev. 1.12c

About this manual

This manual is a general manual for different models of our Gigabit Management Switch. They are similar in operation but have different hardware configurations.

1. 8 * 10/100/1000TX + 2 * SFP Giga ports model (SWG0802-SFP)

This model supports 8 TX ports and two extra SFP ports for Giagbit Ethernet connections.

2. 16 * 10/100/1000TX + 4 * SFP Giga ports model (SWG1604-SFP)

This model supports 16 1000TX ports and four share SFP ports. Port 13~16 are 1000TX RJ45 port / SFP port optional for Gigabit connection.

3. 24 * 10/100/1000TX + 4 * SFP Giga ports model (SWG2404-SFP)

This model supports 24 TX ports and four share SFP ports. Port 21~24 are 1000TX RJ45 port / SFP port optional for Gigabit connection. And they can auto-detect the connection from 1000TX RJ45 port or SFP port.

4. 8* 10/100/1000TX + 16 * SFP (24G) ports model (SWG0816-SFP)

This model supports 8 TX ports and 16 SFP ports. Port 9~16 are TX ports. Other ports are SFP ports.

Contents

1. Introduction

There are four models for the Gigabit Management Switch Series –

SWG0802-SFP
SWG1604-SFP
SWG2404-SFP
SWG0816-SFP

This Gigabit Management Switch is a Layer2 management switch with lots of advanced network functions including VLAN, trunking, spanning tree, mirror port, rate limit, IGMP and port configuration. Console is supported for command-line settings. Web, Telnet, and SNMP interfaces are for remote switch management through network. IEEE 802.1x is supported for port security application. These functions can meet most of the management request for current network.

1.1 Package Contents

- One Gigabit Management Switch
- One AC power cord (*for AC power model only)
- One console cable
- Two rack-mount kits and screws (only SWG1604-SFP/SWG2404-SFP/SWG0816-SFP)
- user's manual

2. Where To Place the Switch

This Switch can be placed on a flat surface (your desk, shelf or table).
Place the Switch at a location with these connection considerations in mind:

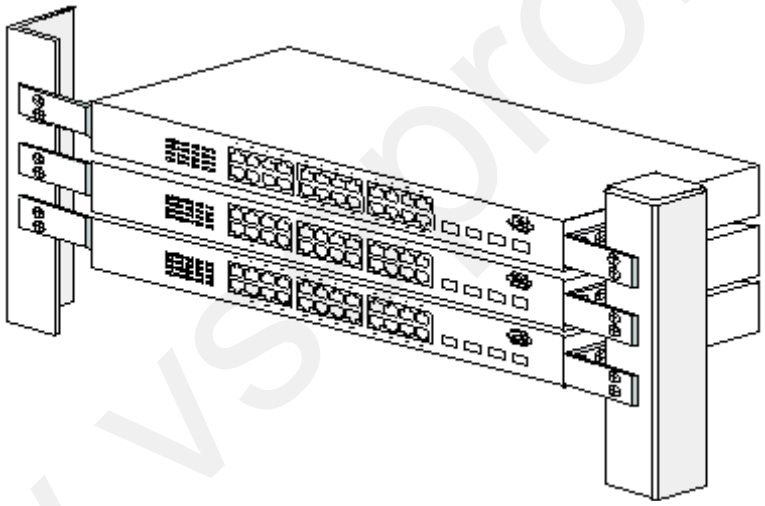
The switch configuration does not break the rules as specified in Section 3.

The switch is accessible and cables can be connected easily to it.

The cables connected to the switch are away from sources of electrical interference such as radio, computer monitor, and light fixtures.

There is sufficient space surrounding the switch to allow for proper ventilation (the switch may not function according to specifications beyond the temperature range of 0 to 50 degrees C).

For SWG1604-SFP/SWG2404-SFP/SWG0816-SFP model, you can also install the switch on a 19" rack with the rack-mount kits as the picture.



[Rack-Mount Installation]

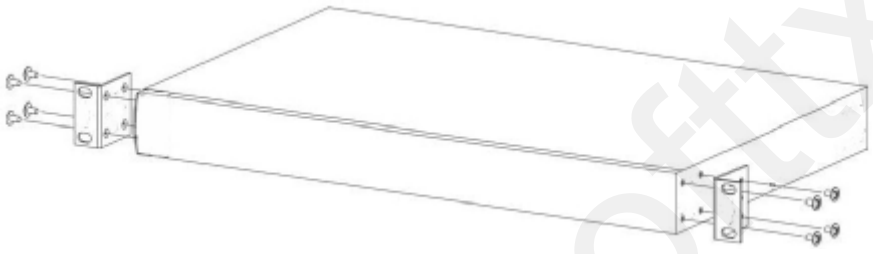
Before rack mounting the switch, please pay attention to the following factors :

1. **Temperature** - Because the temperature in a rack assembly could be higher than the ambient room temperature, check that the rack-environment temperature is within the specified operating temperature range. (Please refer to Product Specifications in the manual.) Air flow is necessary in a rack for temperature stable.
2. **Mechanical Loading** - Do not place any equipment on top of this rack-mounted switch.

3. Circuit Overloading - Be sure that the supply circuit to the rack assembly is not overload after installing this switch.

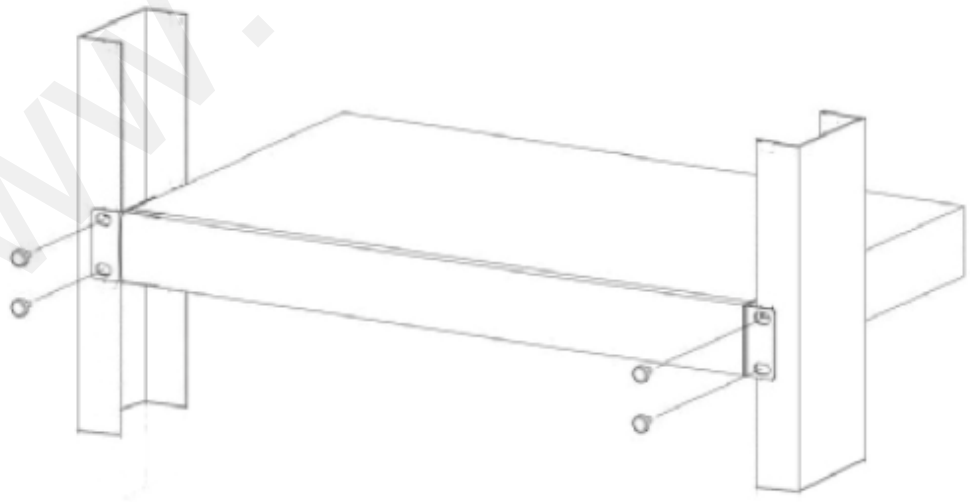
4. Grounding - Rack-mounted equipment should be properly and well grounded.

Particular attention should be given to supply connections other than direct connections to the mains.



[Rack-Mount Brackets to the Switch]

1. Position a Rack-Mount Bracket on one side of the Switch.
2. Line up the screw holes on the bracket with the screw holes on the side of the switch.
3. Use a screwdriver to install the M3 flat head screws through the mounting bracket holes into the switch. (There could have two or four screws for one bracket. That depends on the model that installed.)
4. Repeat Step 1~3 to install another bracket to the switch.
5. Now it is ready to mount to a rack.



[Mount the Switch on a Rack]

- Position a bracket that is already attached to the switch on one side of the rack.
- Line up the screw holes on the bracket with the screw holes on the side of the rack.
- Use a screwdriver to install the rack screws through the mounting bracket holes into the rack.
- Repeat Step 1~3 to attach another bracket that is already attached to the switch on another side of the rack.

3. Configure Network Connection

3.1 Connecting Devices to the Switch

[Connection Guidelines:]

For 10BaseT connection : Category 3 or 5 twisted-pair Ethernet cable

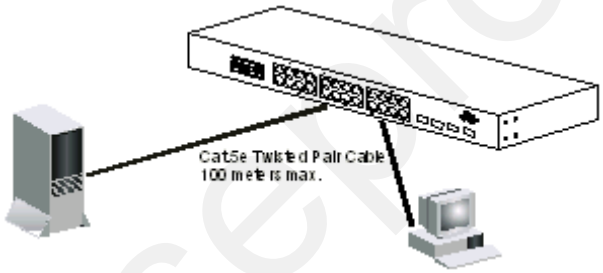
For 100BaseTX connection : Category 5 twisted-pair Ethernet cable

For 1000BaseTX connection: Category 5e or 6 twisted-pair Ethernet cable

For TX cable connection, always limit the cable distance to 100 meters (328 ft) as defined by IEEE specification

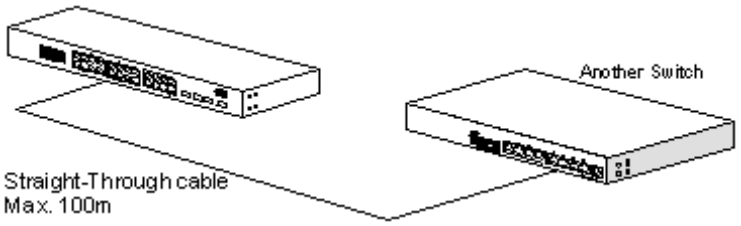
If your switch has 1000BaseSX/1000BaseLX connections, you can connect long distance fiber optic cable to the switch.

Because this switch supports Auto MDI/MDI-X detection on each TX port, you can use normal straight through cable for both workstation connection and hub/switch cascading.



3.2 Connecting to Another Ethernet Switch/Hub

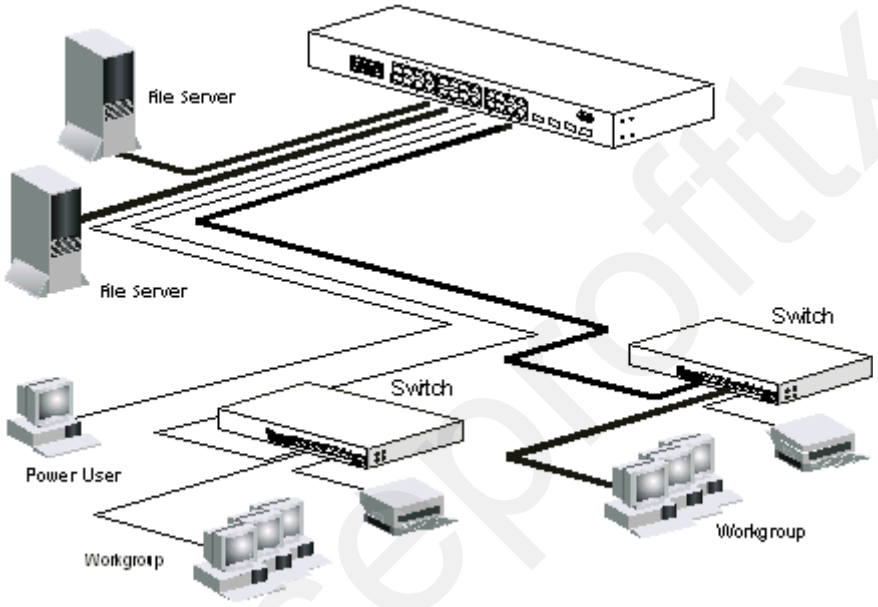
This Switch can be connected to existing 10Mbps / 100Mbps / 1000Mbps hubs/switches. Because all TX ports on the Switch support Auto MDI/MDI-X function, you can connect from any TX port of the Switch to the MDI or MDI-X port of another hub/switch with Straight Through or Crossover cables. If the switches have fiber-optic ports, you can cascade them with fiber optic cable.



3.3 Application

A switch can be used to overcome the hub-to-hub connectivity limitations as well as improve overall network performance. Switches make intelligent

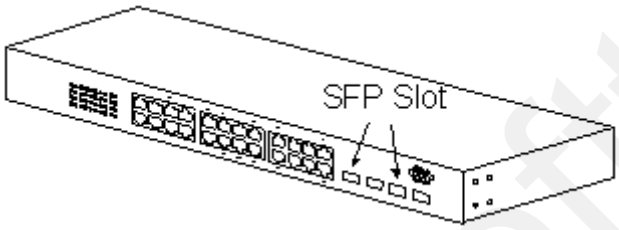
decisions about where to send network traffic based on the destination address of the packet. As a result, the switch can significantly reduce unnecessary traffic. The example below demonstrates the switch ability to segment the network. The number of nodes on each segment is reduced thereby minimizing network contention (collisions) and boosting the available bandwidth per port. With Management function of the switch, network administrator is easy to monitor network status and configure for different applications.



4. Adding Module

This switch supports have cisco compatible connectors for gigabit ports. SFP slots support hot-swap function, you can plug/unplug the SFP transceiver to/from the SFP slot directly. The switch can auto-detect the gigabit connection from SFP slot.

Follow the steps for module adding and removing.



[Add SFP Transceiver]

1. Plug in the SFP Transceiver to SFP slot directly.
2. Connect network cable to the SFP Transceiver. If the connected devices are working, the Link/Act LED will be ON.

[Remove SFP Transceiver]

Unplug the SFP Transceiver from SFP slot directly.

5. LEDs Conditions Definition

The LEDs provide useful information about the switch and the status of all individual ports.

[For SWG0802-SFP/SWG1604-SFP/SWG2404-SFP/SWG0816-SFP]

LED	STATUS	CONDITION
Power	ON	Switch is receiving power.
System	OFF	System is booting.
	Yellow	System is initializing.
	Green	System is running.
Link / Act	ON	Port has established a valid link.
	Flashing	Data packets being received or sent.
	Green	The connection speed is 1000Mbps.
	Yellow	The connection speed is 10/100Mbps.
FDX/Col.	ON	The connection is Full Duplex.
	Flashing	Collisions happen for Half Duplex.

Note: For CL-SWG0802-SFP Model, only Link/Act LED for each SFP port. Its SFP
ports are always link as 1000/Full. And the LED status of its SFP ports is different from TX ports when system initialization.

6. Manage / Configure the Switch

6.1 Introduction of the management functions

This switch is a L2 Management switch. It supports in-band management function from Http/Telnet/SNMP interfaces. Console is supported for local command-line settings. It supports network configuration functions, like VLAN, Trunking, Port Mirror, QoS, spanning tree and software backup/update. Users can configure these functions for different network applications. The following is a brief introduction about these functions before the detail operation sections.

1.VLAN (Virtual LAN)

VLAN can divide the switch to several broadcast domains to prevent network traffic between different user groups. This switch supports 802.1Q tag-based VLAN and Port-based VLAN. Users with the same VLAN ID can transfer data to each other. The network traffic will be blocked if they have different VLAN ID. VLAN Stacking function for 802.1Q tag-based VLAN is supported. It allows two VLAN tags in a packet for 802.1Q VLAN tunnelling application through a central network.

2. Trunk

If two switches are cascaded together, the bottleneck will happen at the cascading connection. If more cables could be used for the cascading connection, it will reduce the bottleneck problem. In normal case, switches will become unstable because of traffic looping when more than one cable is connected between them. If the switches support trunk function, they can treat these cables as one connection between them. The traffic looping will not happen between these cables and the switches will work stable with bigger bandwidth between them.

Notes: About redundant application

The trunk connection supports redundant function. If any trunk cable is broken, the traffic going through that cable will be transferred to another trunk cable automatically. For example, if traffic of user port Port 6 is assigned to Port 1 in a Trunk and Port 1 connection breaks, Port 2 will take over the traffic for Port 6 automatically. (It could be used for redundant application.)

3. Spanning Tree Protocol / Rapid Spanning Tree Protocol Spanning tree is a protocol to prevent network loop in network topology. If network loop happens, it will cause switches in the network unstable because more and more traffic will loop in the network. If network loop happens, spanning tree protocol will block one connection in the loop automatically. But it will also cause a period of delay (30 seconds for STP and shorter time for RSTP) if any network connection is changed because of the network topology detection operation of the protocol. Because there could be more than one switch in the network, users can configure this function for their network spanning tree application.

4.Port Mirror

This switch operates in store-and-forward algorithm so it is not possible to monitor network traffic from another connection port. But the port mirror function can copy packets from some monitored port to another port for network monitor.

5.QoS

For Quality of Service request in a network, packets could be classified to different forwarding priorities. For real-time network traffic (like video, audio), it needs higher priority than normal network traffic. With the definition of packet priority, it could have 8 priority levels (from 0 to 7). This switch supports four priority level queues on each port. It could be configured for port-based, 802.1P tagged based, or DiffServ of IP packets priority. User can define the mapping of priority values to the priority queues.

6.Static Mac ID in ARL table The switch can learn the Mac address from user's packets and keep these Mac address in the ARL table for store-and-forward table lookup operation. But these Mac addresses will be deleted from ARL table after some time when users do not send any packets to the switch. This operation is called aging and the time is called aging time. It is about 5 minutes normally (it could be changed by users.) If users want to keep a Mac address always in ARL table on some port, they can assign the Mac address to ARL table. These Mac ID are called Static Mac address. This switch supports static Mac address assignment. The static Mac address assignment will also limit the Mac address could be used on the assigned port only with the port security configuration function. For example, assigning "00-00-e2-11-22-33" to Port 5 will always keep this Mac ID alive on Port 5 but also limit this Mac address could work on Port 5 only.

Note**:** About Static Mac Address Filter-in (port binding) function
There is a "Mac Security Configuration" function for port security. If it is set to "Accept function", only these static Mac addresses can access network through the assigned port. The other Mac addresses will be forbidden for network access through that port. This function can be used for port binding security application. Please refer to Section 6.3 for the details of the Mac address filter-in operation of the switch.

7.Dynamic Mac ID Number Limit
Beside Static Mac ID Limit, there is another Dynamic Mac ID Number Limit function for Mac address security on port. This function can limit the Mac ID number to access network through a port. For example, five Mac ID are allowed for Port 2. That means up to five users are allowed, but don't care who the users are. It is done by "Limit by Mac no." option in "Mac Security Configuration" function.

8. IEEE 802.1x Port Security Function
If the 802.1x function is enabled, the switch will act as an authenticator for users accessing network through the switch. It will need a RADIUS server for the authentication function. Users will be asked for username and password before network access. If the RADIUS server authenticates it, the switch will enable the port for network access. This function is very useful for network security application to prevent illegal users access network through the switch.

9.Rate Control This function can limit the traffic rate for physical ports. The traffic could be ingress traffic or egress traffic. This function can limit the network bandwidth utilization of users.

10. Private VLAN
Three kinds of VLAN are defined for this application – Primary VLAN, Community VLAN, and Isolated VLAN. Community VLAN and Isolated VLAN can communicate with Primary VLAN, but they cannot communicate with each other. And users in Isolated VLAN cannot communicate with each other. This is a special VLAN configuration. This switch supports a dedicated configure interface for such application.

11. IP Multicast with IGMP Snooping

IP multicast function can forward packets to a group of users connected on different ports. The user group is learned by the switch from packets of IGMP active router with IGMP snooping function. It is often used for video applications

12. MVR (Multicast VLAN Registration)

VLAN function will isolate traffic between VLAN groups. But it will also isolate IP multicast traffic for subscribers in different VLANs. The MVR function allows one multicast VLAN to be shared by subscribers in different VLANs. That can reduce the multicast traffic for VLANs.

13. DHCP Relay & DHCP Option 82

DHCP Relay function will control DHCP requests and forward DHCP requests to the assigned DHCP server. DHCP Option 82 function will add port and switch information to DHCP requests and then send to the assigned DHCP server. Based on those information, DHCP server will assign an IP configuration in the DHCP reply. This is a security function.

14. IP Filtering

This function can limit the IP address and the subnet for accessing network from switch port. That can prevent illegal IP problem in network.

15. Software Backup/Update

This switch supports backup and update functions for its internal software and its network configuration. It could be done in two ways.

a. From console when booting : doing by Xmodem protocol and by terminal pr ogram for boot code and run-time code updating.
b. From web browser : doing byhttp protocol and by web browser for run-time code and configuration backup/update.
c. From telnet or console command : doing by tftp protocol for run-time code and configuration backup/update.

6.2 Settings with Console Connection

6.2.1 Basic of the Console Interface

<< Enter Console Interface >>

Please follow the steps to complete the console hardware connection first.
1. Connect from console port of the switch to COM port of PC with the console cable.
2. Start the terminal program of Windows. Create a new connection and select COM port of PC used for the console. Set the configuration of the terminal as **[9600,8,N,1]**. (You can find the terminal program in [Start] -> [Programs] -> [Accessory Programs] -> [Communication] -> [Terminal]. If you cannot find it, please install it from your Windows Installation Disk. Please refer to your Windows user manual for the installation.)
3. Power on the switch.

If everything is correct, the booting screen will appear in the terminal program when the switch is powered on. It will stop at the following screen after some initializing messages.

Booting Program Version 1.04.04-SI/PI, built at 12:04:53, Sep 17 2008
RAM: 0x00000000-0x00800000, 0x0000cc78-0x007f3000 available
FLASH: 0x05800000 - 0x05a00000, 32 blocks of 0x00010000 bytes each.
==> enter ^C to abort booting within 3 seconds .....
Start to run system initialization task...
[System Configuration]
Company Name :
Model Name : Switch
MAC Address : 00:12:34:64:99:6F
Firmware version : 1.06.01
Username:

<< User Modes >>

There are two user modes for the switch - one is administrator mode (privileged mode), another is guest mode (normal mode).

[administrator mode]

The default user name and password is "super / oem_super.

After login the switch, a prompt will be shown. Because this switch supports command-line for console interface, you can press "?" to check the command list first. With "?" command, you can find the command list as follow.

```
# ?
Exit                Exit from current mode
Help                Show available commands
History             Show a list of previously run commands
Logout              Disconnect
Ping                Sends ICMP echo packets to other network nodes
Quit                Quit commands
Reload              Halts and performs a warm restart
Show                Shows information
calendar            Data and time information
Configure           Enter configuration mode
copy                Copies from one file to another

#
```

These are the basic system commands for the switch.

For system configuring, "**configure**" command can enter the configure mode. And the prompt will become ...

```
# configure
xxxx(config)#
```

In the configure mode, the general configuration of switch can be done. And "exit" command can leave this mode.

If settings for port, "**interface**" command is used. And the prompt will become ...

---
xxxx(config)# interface ethernet 1/5
xxxx(config-if)#

"ethernet 1/5" means Ethernet interface 1, port 5. And "exit" command can leave this mode.
"interface" command has another sub-command "**vlan**". IP address of the switch can be configured in this mode.
---
xxxx(config)# interface vlan 10
xxxx(config-if)#

[guest mode]
If "guest" / "guest" is used for username / password, the console inerface will enter guest mode. Its prompt is ended with ">". With "?" command, you can find the command list as follow.

> ?

exit	Exit from current mode
help	Show available commands
history	Show a list of previously run commands
logout	Disconnect
ping	Sends ICMP echo packets to other network nodes
quit	Quit commands
show	Show the counters that the system uses

>

In guest mode, it is allowed to view the switch configuration only. No setup/ configure commands are supported.

<< Function Keys >>
Here is the function keys for console interface.
[Tab] key: this key can help to get the full command keyword with just several beginning letters. For example, "cal-Tab" will get the full "calendar" command word.

[Esc] key: this key can use to break message display and go back to command prompt.
[Up-Arrow] key: this key can get last input command.
[Down-Arrow] key: this key can get next input command.
[Left-Arrow]/[Right-Arrow] key: the key can move the cursor.
[Backspace] key: this key can delete the letter in front of cursor
[?] key: this key can get the command list.

<< Command Mode >>

There are four command modes for console interface.

1. General Basic Commands

These are basic commands after login. Users can show switch configueartion/status, ping network device, reboot switch, ... The prompt is "xxx#" for admin user, and "xxx>" for guest user.

2. Configure Mode Commands

With "configure" command, user can enter Configure Mode. Commands in Configuring Mode are for general switch settings. And its prompt is "(config)#".

3. Interface Configuring Commands for Port / VLAN Group

If the settings are for ports, it is done with "interface ethernet 1/x" command in configure mode. And the prompt will become "(config-if)#". For example, "interface ethernet 1/5" is for settings on Port 5.

If the settings are for VLAN group, it is done with "interface vlan x" command in configure mode. And the prompt will become "(config-if)#". For example, "interface vlan 100" is for settings on VLAN 100.

4. VLAN Configuring Commands

If the settings are general VLAN settings, it is done with "vlan database" command in configure mode. And its prompt will become "(config-vlan)#".

6.2.2 General Basic Commands

When "admin" / "admin" is used for username/password, the console will enter administrator mode. Enter "?", command list will be shown.

```
-----------------------------------------------------------------------------------------
# ?

exit            Exit from current mode
help            Show available commands
history         Show a list of previously run commands
logout          Disconnect
ping            Sends ICMP echo packets to other network nodes
quit            Quit commands
reload          Halts and performs a warm restart
show            Show the counters that the system uses
calendar        Data and time information
configure       Enter configuration mode
copy            Copies from one file to anothe

#
-----------------------------------------------------------------------------------------
```

1. exit command

This command is used to leave current operation mode. It will do logout at this basic command interface.

2. help command

This is a help command and the console will prompt with all available commands.

3. history command

This command will show the history of entering commands.

4. logout command

This is a logout command.

5. ping command

User can use this command to ping another network device to verify the network connection and activity. (It is similar to the ping command in MS-DOS.) Enter "ping ?" at the prompt, the command syntax will be shown.

```
# ping ?
Syntax: ping [-n count] [-l length] [-t] [-w timeout] ip
```

-n count : Number of echo requests to send.
-l length : Send buffer size, and length is between 64~8148
-t : Ping the specified host until stopped by <ESC> key.
-w : Timeout in milliseconds to wait for each reply.
ip : IP address (xxx.xxx.xxx.xxx)

For example, "ping 192.168.1.80". "Esc" can be used to break continuous ping operation.

6. quit command

This command is used to quit the console interface.

7. reload command

This command is used to reset switch. It will halt and perform a warm restart.
Enter "reload" at the prompt, you will be asked to confirm the action.
reload
Are you sure to reset switch now?(Y/N)
If "y" is entered, the switch will reboot. If "n" is entered, just leave and no any action will go.

8. show command

This command is used to show current system information and system configuration.
Enter "show ?" at the prompt, the sub-command list will be shown.
show ?

aaa	Show AAA service configuration
calendar	Date and time information
dhcp-relay	DHCP Relay Configuration
dot1x	802.1x content
gvrp	GVRP configuration
history	History information
interface	Interface information
ip	IP information
ip-filter	IP Filter Configuration
lacp	LACP statistics
line	TTY line information
log	Log records
mac-address-table	Configuration of the address table

mac-security	MAC Security Configuration
management	Management IP filter
map	Maps priority
mvr	Show MVR Status
port	Port characteristics
queue	Priority queue information
radius-server	RADIUS server information
running-config	Information on the running configuration
rate-limit	Configures rate-limits
snmp	Simple Network Management Protocol statistis
sntp	Simple Network Time Protocol configuration
spanning-tree	Spanning-tree configuration
system	System information
trunk	Trunk information
version	System hardware and software versions
vlan	Virtual LAN settings

With sub-commands, different configuration settings will be displayed. More help information for them will be prompted with "show xxxx ?" (xxxx is the sub-command). For example, entering "show ip ?" will get the prompt message...
show ip ?

igmp	IGMP snooping
interface	Interface information
redirects	Default gateway configured for this device

And entering "show ip igmp ?" will get next help message...
show ip igmp ?
snooping IGMP snooping configuration

And entering "show ip igmp snooping" will get the IGMP settings...
show ip igmp snooping
IGMP Status: Disable
IGMP Querying: Disable
IGMP Querying: Disable

IGMP Query Interval: 125 seconds
IGMP Report Delay: 15 seconds
IGMP Query Timeout: 255 seconds
If the display is more than one console page, "Esc" can be used to break the display.

For the details, please refer to section **6.2.6 Show commands**.

9. calendar command

This command is used to set the system time. It is entered in <hour minute second month day year> order.
For example,
calendar set 10 30 0 october 15 2008
show calendar
Current Time : 2008/10/15-10:30:18
It is 18 seconds passby after the setting command.

10. configure command

This command will change the console interface to configure mode. And the prompt will become "(config)#". In this mode, administrator can do system configuration of the switch.
The operation of configure mode will be described in next section.
"exit" command can be used to quit this operation mode.

11. copy command

This command is used to backup system configuration/firmware to TFTP server,
restore system configuration from TFTP server, and update firmware from TFTP server.
copy ?

binary-config	Copies binary configuration file
config	Copies configuration file
firmware	Copies run-time firmware

copy binary-config running-config tftp xxx.xxx.xxx.xxx yyy command is

used to backup current switch running configuration to TFTP Server at IP "xxx.xxx.xxx.xxx" as file name "yyy" in binary format.
copy binary-config tftp running-config xxx.xxx.xxx.xxx yyy command is used to restore binary configuration file "yyy" from TFTP Server at IP "xxx.xxx.xxx.xxx".
copy config running-config tftp xxx.xxx.xxx.xxx yyy command is used to backup current switch running configuration to TFTP Server at IP "xxx.xxx.xxx.xxx" as file name "yyy" in text format.
copy config tftp running-config xxx.xxx.xxx.xxx yyy command is used to restore text configuration file "yyy" from TFTP Server at IP "xxx.xxx.xxx.xxx".
copy firmware running-firmware tftp xxx.xxx.xxx.xxx yyy command is used to backup current running firmware to TFTP Server at IP "xxx.xxx.xxx.xxx" as file
name "yyy" in binary format
copy firmware tftp running-firmware xxx.xxx.xxx.xxx yyy command is used to update the running firmware file "yyy" from TFTP Server at IP "xxx.xxx.xxx.xxx".

6.2.3 Configure Mode Commands

Entering "configure" command at console interface, the prompt will become ... "(configure)#".
All the general settings for the switch can be done in this mode.
If the settings are for ports, it is done with "interface" command in configure mode.
For example, "interface ethernet 1/5" is for settings on Port 5 and "interface ethernet 1/5,6,10-15" is for settings on Port 5, 6, 10, 11, 12, 13, 14, 15. Please refer to next section for the details of this command.
Enter "?" at the prompt, the sub-command list will be shown.

(config)# ?

exit	Exit from current mode
help	Show available commands
history	Show a list of previously run commands
logout	Disconnect

quit	Quit commands
aaa	AAA Service
automode	Set Auto Negotiation or Auto Detect mode
default	Restore to factory default setting
dhcp-relay	DHCP relay setting
dot1x	Configures 802.1x port-based access control
end	Exit from configure mode
hostname	Sets system's network name
interface	Enters privileged interface configuration
ip	Global IP configuration sub commands
ip-filter	Enable IP address filtering function
lacp	Configures LACP status
logging	Modifies message logging facilities
mac-address-table	Configuration of the address table
management	Specifies management IP filter
mirror	Configuration of mirror
mvr	Multicast VLAN Registration
no	Negates a command or sets its defaults
prompt	Sets system's prompt
qos	Configuration of QoS
queue	Assigns priority queues
radius-server	Configures login to RADIUS server
rate-limit	Configures rate-limits
snmp-server	Modifies SNMP server parameters
sntp	Simple Network Time Protocol configuration
spanning-tree	Configures spanning tree parameters
storm-control	Configures storm control
trunk	Configures trunk function
username	Establishes user name authentication
vlan	Switch Virtual LAN interface

---

1. exit command

This command is used to leave current operation mode. Go back to last mode.

2. help command

This command is used to show all the available commands in this mode.

3. history command

This command is used to show the history of entering commands.

4. logout command

This command is used to logout from console interface.

5. quit command

This command is used to quit from console interface. It has the same function as logout.

6. aaa command

This command is used to set the authentication manner for administrator of the switch when login by http(s)/telnet for management. It could be authenticated by local switch or by RADIUS Server.

Here is the command for the setting.

aaa authentication login local command will set the authentication manner for administrator by local switch when login by http(s)/telnet for management.

aaa authentication login radius command will set the authentication manner for administrator by RADIUS Server when login by http(s)/telnet for management.

aaa authentication login local radius command will set the authentication manner for administrator by local switch first when login by http(s)/telnet for management. If authentication fail, try by RADIUS Server next.

RADIUS Server is set by radius-server command for command line interface or set in 802.1x function for web interface.

7. automode command

With the command, user can select the operation mode of port when "auto" is set to disabled.

For "Auto Negotiation" mode, the switch will disable port auto-negotiation function when the auto function of port (in Port Configuration setting) is disabled.

For "Auto Detect" mode, the switch will always keep port auto-negotiation function ON but just modify its attribution if auto function of port (in Port Configuration setting) is disabled.

For applications, you should select "Auto Detect"mode if the connected device is auto-negotiation enabled. (For example, customer's PC is auto-negotiation enable and you want to set his network connection to work at 10Mbps.)

And you can select "Auto Negotiation"mode if the connected device is

auto-negotiation disabled (it is called forced mode, sometimes). Some old TX-FX Converters needs to work in this mode because FX supports 100/Full forced mode only. For most applications, "Auto Detect" mode is OK.
With "automode ?", the sub-commands will be shown.
(config)# automode ?
detect Auto Detect mode
negotiation Auto Negotiation mode
automode detect command will set it to auto-detect mode.
automode negotiation command will set it to auto-negotiation mode.

8. default command

This command is used to restore factory default settings. Before start it, a confirm message wil be prompted.

9. dhcp-relay command

This command is used to configure DHCP Relay Option 82 function.
Note: The DHCP-Relay function here does not support relay between different IP subnets. But it supports relay cross VLANs.
DHCP Relay function can relay DHCP requests to a specified DHCP server.
And Option 82 function will add the following information to DHCP request packet.
1. Port number that DHCP request packet comes from
2. VLAN ID for this DHCP request
3. Mac address of the switch
4. A additional string as information. (*Adding the information string must be enabled first.)
And DHCP server will assign IP configuration according to the information in Option 82.
Note: Not every DHCP server supports Option 82 function. **If DHCP server does not support it, please disable this DHCP Relay Option 82 function.**
Here is the Option 82 definition of the switch.
1. Circuit ID sub-option setup information for DHCP server :
<Format>
[Slot ID/1-Byte] [Port ID/1-Byte] [VLAN ID/2-Bytes] [Information/XBytes]
Slot ID - please set to "0".
Port ID - please set according to the port number of the switch.

VLAN ID - please set according to its VLAN ID.
Information - this is a string with variable length
For example, "000500c8" means Slot ID 0, Port 5, VLAN ID 200, no information. All of the numbers are hexadecimal numbers.
2. Remote ID sub-option setup information for DHCP server :
<Format>
[Mac Address/6-Bytes]
Mac Address - this is the Mac Address of the switch. For example, "000000828ce6" in hexadecimal numbers.
If the Option 82 of DHCP request meets these settings, DHCP server will assign the IP configuration according to this Option 82 content.

Entering "dhcp-relay ?", the sub-commands will be shown.
(config)# dhcp-relay ?

helper-address	Specif y DHCP servers' IP addresses
information	Specify a additional information for DHCP Option 82
option	Enable to add the additional information to Option 82
<cr>	Enable DHCP relay

dhcp-relay command is used to enable DHCP Relay function. "no dhcp-relay" command is used to disable it.
dhcp-relay helper-address xxx.xxx.xxx.xxx command is used to assign the DHCP server for DHCP Relay operation. "xxx.xxx.xxx.xxx" is the IP address of DHCP server.
dhcp-relay information xxx command is used to specify the additional information string for DHCP Option 82 operation. "xxx" is the string.
dhcp-relay option command is used to enable adding the additional string to Option 82. "no dhcp-relay option" command is used to disable it.

10. dot1x command

This command is used configure the general settings of 802.1x function of the switch. Entering "dot1x ?", the sub-commands will be shown.

(config)# dot1x ?

authcount	Set 802.1x Re-authentication Max Count
dynamic-vlan	VLANs are assigned based on a MAC address
guest-vlan	Migrating end users to an 802.1X environment and for delivering
limited	services to unauthorized users
max-req	Max EAP request/identity packet retransmissions
re-authentication	Forces re-authentication on all ports/interfaces
system-auth-control	Enables/disables 802.1x to change port modes
timeout	Timeout value
transparent	Transparent 802.1x packets

dot1x authcount x command is used to set max count for re-authentication request in the re-authentication process. If the max count is met, it will become un-authentication state. The valid value of "x" is 1~10.

dot1x dynamic-vlan command is used to enable Dynamic VLAN function for 802.1x operation. If it is enabled, the switch will assign the user to the VLAN assigned from RADIUS server. And no dot1x dynamic-vlan command can be used to disable it.

dot1x guest-vlan x command is used to enable and select the VLAN for users fail to authenticated by RADIUS server. "x" is the VLAN ID. And no dot1x **guest-vlan** command can be used to disable it.

dot1x max-req x command is used to set max request timeout count between the switch and RADIUS server before authentication fail. The valid value of "x" is 1~10.

dot1x re-authentication command is used to force re-authentication on all ports.

dot1x system-auth-control command is used to enable 802.1x function on the switch. And no dot1x system-auth-control command can be used to disable it.

dot1x timeout command is used to setup timeout values in 802.1x operation. Entering "dot1x timeout ?", the sub-command will be shown.

(config)# dot1x timeout ?

quiet-period	Time after Max Request Count before gets new client
re-authperiod	Time after connected client must be re-authenticated
server-period	Time after an authenticator sends a RADIUS Access-Request packet to the authentication server
supplicant-period	Time after an authenticator sends an EAP-Request/ MD5 Challenge frame to a supplicant
tx-period	Time switch waits before re-transmitting EAP packet

dot1x timeout quiet-period x command is used to set the quiet time value between the switch and the user before next authentication process when authentication fail. The valid value of "x" is 0~65535.
dot1x timeout re-authperiod x command is used to set the timeout period for doing re-authentication process. The valid value of "x" is 0~65535.
dot1x timeout server-period x command is used to set the request timeout value between the switch and RADIUS server. The valid value of "x" is 0~65535.
dot1x timeout supplicant-period x command is used to set the timeout value between the switch and users (called "supplicant" in 802.1x) after first identification. The valid value of "x" is 0~65535.
dot1x timeout tx-period x command is used to set the timeout value for the identification request from the switch to users. The request will be re-tried until the authcount is met. After that, authentication fail message will be sent. The valid value of "x" is 0~65535.

Note:
1. Setting 802.1x function on ports, use "dot1x" command in interface
28
configuring mode.
2. Setting for RADIUS server, use "radius-server" command.
Please refer to sections for the commands.

11. end command

This command is used to exit from configure mode.

12. hostname command

This command is used to set the name of the switch in network. This name is also used as the hostname for SNMP agent function of the switch.

13 interface command

This command is used to entering interface configuring mode. There are two sub-commands for it - one is "ethernet", it is for port setting, another is "vlan", it is for VLAN groups characteristics setting.

(config)# interface ?

ethernet Ethernet port

vlan Switch Virtual LAN interface

All the port setting commands are put in interface configuring mode - like rate-limit setting, speed-duplex setting, ... And characteristics settings for VLAN groups are also done in interface configuring mode - like IP address assignment.

For example, the console will enter interface configuring mode for Port 5 with "interface ethernet 1/5" command. And the prompt will become ...

(config)# interface ethernet 1/5

(config-if)#

With "interface ethernet 1/5,6,10-13", the console will enter interface configuring

mode for Port 5, 6, 10, 11, 12, 13. And all the settings will be applied to those ports at the same time.

The description of commands in interface configuring mode is put in Section

6.2.4 Interface Configuring Commands. Please refer to the section for the details.

14 ip command

This command is used to configure some IP-depending functions. Entering "ip ?", the sub-commands will be shown.

(config)# ip ?

default-gateway Specif ies the default gateway

http HTTP server configuration

igmp IGMP protocol

ip default-gateway x.x.x.x command is used to specify the default gateway for IP configuration of the switch. x.x.x.x is the IP address of the gateway

device.
ip http command is used to configure http service of the switch.
Entering "ip http ?", the sub-command will be shown.
(config)# ip http ?
secure-server Enable secure HTTP server
server Enable HTTP server

ip http secure-server command is used to enable the SSL function of http service (https) of the switch. And no ip http secure-server command can be used to disable it.
ip http server command is used to enable http service of the switch. And no ip http server command can be used to disable it.
Because hacker or worm/virus (like ColdRed) often attacks http server, this command is provided to enable/disable http service to prevent it. (If this switch is installed in public Internet without any firewall protection, we suggest users to disable the http interface and use Telnet or SNMP instead.)

ip igmp ... command is used to configure IGMP operation of the switch.
Entering "ip igmp snooping ?", the sub-command will be shown.
(config)# ip igmp snooping ?
mrouter Multicast router
query Enable IGMP query function
query-interval Configures query interval
query-max-response-time Configures the report delay
router-port-expire-time Configures router port expire time
unregflood Enable IGMP unregister flood function
<cr>

ip igmp command is used to enable IGMP function of the switch. And no ip **igmp** command can be used to disable it.
ip igmp snooping mrouter ethernet 1/x command is used to set the port that connecting to the IP Multicast router (the IGMP active device). "x" is the port number.
ip igmp snooping query command is used to enable the IGMP query function. And no ip igmp snooping query command can be used to disable it.

ip igmp snooping query-interval x command is used to set the IGMP query time interval if query function is enabled. "x" is the time interval, and its valid value is 60-125.
ip igmp snooping query-max-response-time x command is used to set the maximum response time for query operation. "x" is the time interval, and its valid value is 5-25.
ip igmp snooping router-port-expire-time x command is used to set the time interval of router port expire time. "x" is the time interval, and its valid value is 255-500.
ip igmp snooping unregflood command is used to enable IGMP unregister traffic flooding function. And no ip igmp snooping unregflood can be used to disable it. If it is enable, the unregistered (not joined) IP multicast traffic will be flooded to every port. If it is disable, the unregistered (not joined) IP multicast traffic will be flood to IGMP member ports only.

15. ip-filter command

This command is used to enable IP Filtering function on port. Only the allowed IP addresses can access network through the switch ports.
ip-filter command is used to enable this function. "no ip-filter" command is used to disable this function.
And assigning the filtering IP/Subnet to ports is done by "ip-filter" command in "(config-if)#" mode (go with "interface ethernet 1/x" command. "x" is the port number.) Please refer to "ip-filter" command in Section 6.2.4.1 for the details.

16. lacp command

This command is used to configure LACP function of the switch. Entering "lacp ?", the sub-commands will be shown.

```
(config)# lacp ?
system-priority          Combined with MAC address to form LAG identifier
```

lacp system-priority x command is used to configure the system priority for LACP operation of the switch. Its value is 1~65535 and higher numbers have lower priority. Combining with the Mac address of the switch, it is used to identify this switch in LACP protocol operation.
Adding ports to LACP trunk group is by "lacp" command in "Interface Configuring Commands for Port". Please refer to Section 6.2.4.1 for the

details.

17. logging command

This command is used to configure logging function of the switch. The logging function can record events at local flash or remote log server. Entering "logging ?", the sub-commands will be shown.

```
(config)# logging ?
log-level       Log     level
on Enable       logging    to all supported destination
remote-log      Enable logging to remote host
```

logging log-level x command is used define the log level of events. The valid value of "x" is 0~7.

logging on command is used to enable the logging function. And no logging on command is used to disable the logging function.

logging remote-log command is used to configure remote logging function. Entering "logging remote-log ?", the sub-commands will be shown.

```
(config)# logging remote-log ?
<1-5> Index
<cr>
```

logging remote-log command is used to enable the remote logging function. Events will also be sent to syslog servers. no logging remote-log command is used to disable it.

logging remote-log x host y.y.y.y command is used to set IP address (y.y.y.y) to syslog server with index x. Up to five (x=1~5) syslog servers are supported.

18. mac-address-table command

This command is used to configure functions for Mac address table of the switch. Entering "mac-address-table ?", the sub-commands will be shown.

```
(config)# mac-address-table ?
aging-time      Aging     time for entries in the address table
static                Sets MAC address table static information
```

mac-address-table aging-time x command is used to set to aging time of the switch. The valid value of "x"(aging time in seconds) is 10-1000000 and 0. If

x=0, the aging operation will be disable.
mac-address-table static x-x-x-x-x-x interface ethernet 1/y command is used to assign a static Mac address x-x-x-x-x-x to Port y of the switch. The static mac address will not be aging out by the switch.

19. management command

This command is used to setup the management interface security function. The management interface security function can limit the IP / subnet / remote interfaces(http,telnet,snmp) / access right(view,modify) for management from network. Different administrators could have different rights to manage this switch. This is for security of this management switch. (Four user groups are supported for this function.)
Entering "management ?", the sub-commands will be shown.

```
(config)# management ?
<1-4> Index
(config)# management 2 ?
enable      Set    enable for a specified set
ipaddr          Set IP and net mask for a specified set
mode            Set mode for a specified set
protocol        Set protocol for a specified set
```

management x enable command is used to enable the security settings for some user groups ("x" is the index of the user group). And no management x enable command can be used to disable it. And users for this setting are allowed to manage this switch remotely.
management x ipaddr y.y.y.y z.z.z.z command is used to set the IP/subnet for some user groups ("x" is the index of the user group, y.y.y.y is the IP address, z.z.z.z is the IP subnet mask). Users in this IP subnet will belong to this users groups.
management x mode modify/view command is used to set the access right for some user groups ("x" is the index of the user group). If "management x
mode modify" command, users in this groups have "modify" right for management. If "management x mode view" command, users in this groups have "view" right only.
management x protocol http|snmp|telnet command is used to enable

the remote management protocol for some user groups ("x" is the index of the user group). More than one protocols can be enabled at the same time - e.g. "management 2 protocol http snmp telnet". And no management x protocol command is used to disable all remote management protocols for the user group.

20. mirror command

This command is used to enable mirror function of the switch. And no mirror command can be used to disable mirror function of the switch.

21 mvr command

This command is used to configure MVR (Multicast VLAN Registration) function. VLAN function will isolate traffic between VLAN groups. But it will also isolate IP multicast traffic for subscribers in different VLANs. The MVR function allows one multicast VLAN to be shared by subscribers in different VLANs. That can reduce the multicast traffic for VLANs.

** Before configuring MVR function, complete the VLAN setting first

** Using MVR function, you have to enable IGMP snooping function first.

This switch supports three MVR VLANs. They are referred with their VLAN ID. For any MVR setting, you have to assign the VLAN ID in the command. Entering "mvr x ?", the sub-commands will be shown. "x" is a VLAN ID with number in 2~4094. For example, "mvr 10".

```
(config)# mvr 10 ?
8021p-priority      Conf   igure 802.1p priority tagging
active                 Active a MVR VLAN
group                  Create a multicast group for MVR VLAN
mode                   Set MVR VLAN operation mode
name                   Set MVR VLAN name
<cr>                   Create a MVR VLAN
```

mvr x command is used to create a MVR VLAN with VLAN ID "x". "no mvr x" command is used to delete a MVR VLAN.

mvr x 8021p-priority y command is used to set the 802.1P priority (0~7) for MVR operation. The IGMP control packets for this VLAN will be assigned this priority when tag is added. "x" is the MVR VLAN ID. "y" is the 802.1P priority value.

mvr x active command is used to set the MVR VLAN to "active" state. "x" is the MVR VLAN ID. "no mvr x active" command is used to set the MVR VLAN

to "inactive" state.

mvr x group yyy start-address m.m.m.m end-address n.n.n.n command is used to create a IP multicast group for the MVR VLAN. After MVR VLAN is created, you can assign IP multicast groups (video channels) to the MVR VLAN.

And you can assign more than one IP multicast groups (video channels) to one MVR VLAN. "x" is the MVR VLAN ID. "yyy" is the name of the IP multicast group. "m.m.m.m" is the start IP multicast address. "n.n.n.n" is the end IP multicast address. For example, "mvr 10 group abc start-address 224.0.0.1 end-address 224.0.0.2". "no mvr x group yyy" command is used to delete the IP multicast group named "yyy" from MVR VLAN "x".

mvr x mode compatible / mvr x mode dynamic command is used to set the operation mode of the MVR VLAN. There are two operation modes for this MVR function. One is Dynamic mode. Another is Compatible mode. In Dynamic mode, the switch will send IGMP reports to every MVR source port in the MVR VLAN. In Compatible mode, the switch will not send IGMP reports. "x" is the MVR VLAN ID.

mvr x name yyy command is used to assign a name to the MVR VLAN. "x" is the MVR VLAN ID. "yyy" is the name string.

After MVR VLAN is created, source port of IP multicast traffic and receiver ports of subscribers will be assigned next. Assigning source port and receiver port to MVR VLAN is done in "(config-if)#" mode (go with "interface ethernet 1/x" command. "x" is the port number.) Please refer to "mvr" command in Section 6.2.4.1 for the details.

22. no command

This command is used to disable a function or restore a setting to factory default of the switch.

```
(config)# no ?
aaa                  AAA          Service
automode                    Set Auto Negotiation or Auto Detect mode
dhcp-relay                  Set Auto Negotiation or Auto Detect mode
dot1x                Conf          igures 802.1x port-based access control
hostname                    Sets system's network name
ip                          Global IP configuration sub commands
ip-filter                        Enable IP address filtering function
```

lacp		Configures LACP status
logging	Modif	ies message logging facilities
mac-address-table		Configuration of the address table
management		Specifies management IP filter
mirror		Configuration of mirror
mvr		Multicast VLAN Registration
qos		Configuration of QoS
queue		Assigns priority queues
radius-server		Configures login to RADIUS server
rate-limit		Configures rate-limits
snmp-server		Modifies SNMP server parameters
sntp		Simple Network Time Protocol configuration
spanning-tree		Configures spanning tree parameters
storm-control		Configures storm control
trunk		Configures trunk function

For example,

"mirror" command can enable the mirror function and "no mirror" command can disable it.

"ip default-gateway 192.168.1.100" will set the IP gateway of the switch to 192.168.1.100, and "no ip default-gateway" will put it to factory default setting 192.168.1.254.

23. prompt command

This command is used to set the prompt word for console.

For example,

(config)# prompt AAA

AAA(config)#

24. qos command

This command is used to enable QoS function of the switch. And "no qos" can be used to disable it.

The traffic scheduling mode (strict priority - ST or weight round robin - WRR) is selected in "queue" command. And the weighting of each queue is also set in "queue" command if WRR is selected.

The other QoS settings on ports are configured in "(config-if)#" mode (go with "interface ethernet 1/x" command. "x" is the port number.) Please refer to

"qos" command in Section 6.2.4.1 for the details.

25. queue command

This command is used to select traffic scheduling mode (strict priority or weight round robin). If WRR is selected, weighting of each queue is also set with this command.

Entering "queue ?", the sub-commands will be shown.

```
(config)# queue ?
bandwidth          Assigns WRR weights to QoS priority queues
mode               Assigns priority queues
```

queue bandwidth x y z command is used to set the weighting of Normal, Medium, and High priority queues for WRR operation. (Low priority queue is always weight1). "x" is the weighting of Normal priority queue. "y" is the weighting of Medium priority queue. "z" is the weighting of High priority queue. And their valid number is 0~3. (0:weight1 / 1:weight2 / 2:weight4 / 3:weight8).

queue mode strict / wrr command is used to select the traffic scheduling mode.

If "strict" is selected, the higher priority queue always get bandwidth service first. If "wrr" is selected, bandwidth is shared between queues with their weighting.

26. radius-server command

This command is used to configure the settings for RADIUS Server. The settings will be used in 802.1x operation.

Entering "radius-server ?", the sub-commands will be shown.

```
(config)# radius-server ?
host               Sets the port as a host port
key                Sets the RADIUS encryption key
port               Sets the RADIUS server network port
```

radius-server host x.x.x.x command is used to setthe IP address of RADIUS Server for 802.1x operation. "x.x.x.x" is the IP address.

radius-server key xxx command is used to set the security key to handshake with RADIUS Server. "xxx" is the key string.

radius-server port x command is used to set the communication port of RADIUS Server. "x" is the port number and its valid value is 1~65535.

27. rate-limit command

This command is used to define the unit and operation mode of rate limit operation. The unit could be 128Kbps to 30Mbps. And the rate limit on each port is done with the level number of each port multiplied with this unit.
rate-limit unit x command is used to set the unit for rate limit operation. "x" is the unit number and its valid value is 128-30000. (Kbps)
rate-limit mode command is used to disable "Packet Drop of Ingress Limit" function. When Ingress traffic rate exceeds Ingress Rate Limit, the switch can drop packets or pause the traffic. If packet drop is enabled, flow control of ports will be disabled and packets could be dropped. If packet drop is disabled, flow control of ports will be enabled and pause frame will be sent when ingress traffic rate exceeds the limit. "no rate-limit mode" command can be used to enable it.

28. snmp-server command

This command is used to configure SNMP operation of the switch.
Entering "snmp-server ?", the sub-commands will be shown.
(config)# snmp-server ?
<1-5> Index of Trap
community Defines SNMP community access string
contact Sets the system contact string
location Sets the system location string
username Sets the snmpv3 user informations
version Sets the snmp version
snmp-server community get xxx command is used to set the community string of get command for SNMP operation. "xxx" is the community string.
snmp-server community set xxx command is used to set the community string of set command for SNMP operation. "xxx" is the community string.
snmp-server contact xxx command is used to set the contact information forthis switch. "xxx" is the contact information string.
snmp-server location xxx command is used to set the location information for this switch. "xxx" is the location information string.
snmp-server version x command is used to select the SNMP operation

version. "x" could be v1, v2c, v3, v3v2c, v3v2cv1.
The following commands are for SNMPv3 function.
snmp-server username xxx securitylevel y command is used set security level of user xxx. "xxx" is the user name. "y" could be noauth, auth, or priv.
- "noauth" : no authentication, no encryption
- "auth" : do authentication, no encryption
- "priv" : do authentication and encryption(by DES)

snmp-server username xxx authentication y command is used to set the authentication manner. "xxx" is the user name. "y" could be md5 or sha.

29. sntp command

This command is used to configure SNTP protocol of the switch.
Entering "sntp ?", the sub-commands will be shown.

```
(config)# sntp ?
client                Accepts time from specified time server
server                Specified one time server
zone                  Set time zone
dst                   Config daylight saving time function.
start-time            Set start time of daylight saving time
end-time              Set end time of daylight saving time
```

sntp client command is used to enable SNTP protocol. And no sntp client command can be used to disable it. If it is disabled, the system time will be got from manual setting.
sntp server x.x.x.x command is used to set the IP address of network time server for SNTP protocol operation. "x.x.x.x" is the IP address.
sntp zone xxx command is used to set the time zone. "xxx" is the location of the time zone. With "sntp zone ?", the locations will be shown.
sntp dst command is used enabled Daylight Saving Time function. And no sntp dst command can be used to disabled it. Daylight Saving Time function will set the system time one-hour early than normal time in a period of time. "start-time" and "end-time" sub-commands can be used to set the time period.
sntp start-time w/x/y/z command is used to set the start time of Daylight Saving Time.
- "w" is the week number in the month. Its value is 1~5.
- "x" is the day number in the week. Its value is 0~6.

- "y" is the month number. Its value is 1~12.
- "z" is the hour number in the day. Its value is 0~23.

sntp end-time w/x/y/z command is used to set the end time of Daylight Saving Time.

- "w" is the week number in the month. Its value is 1~5.
- "x" is the day number in the week. Its value is 0~6.
- "y" is the month number. Its value is 1~12.
- "z" is the hour number in the day. Its value is 0~23.

30. spanning-tree command

This command is used to configure spanning tree protocol of the switch. Entering "spanning-tree", the sub-commands will be shown.

(config)# spanning-tree ?

compatible	Compatible with old STP
forward-time	Global STA forward time configuration. Range: <4-30 seconds>
hello-time	Global STA hello time configuration. Range: <1-10 seconds>
max-age	Global STA maximum age configuration. Range <6-40 seconds>
priority	Specifies spanning tree priority
<cr>	

spanning-tree command is used to enable spanning tree protocol function. And no spanning-tree command is used to disable it.

spanning-tree compatible command is used to change its operation to 802.1D STP instead of 802.1w RSTP. And no spanning-tree complatible command is used to set it back.

spanning-tree forward-time x command is used to set the forwarding delay of spanning tree operation. It is the maximum waiting time before changing states. This delay is required because every device must receive information about topology changes before it starts to forward frames. "x" is the delay time, and its valid value is 4-30 in seconds

spanning-tree hello-time x command is used to set the period to send spanning tree maintenance packet if the switch is the root of spanning tree. "x" is the period time, and its valid value is 1-10 in seconds.

spanning-tree max-age x command is used to set the spanning tree aging time if no spanning tree maintenance packet is received. "x" is the time, and its valid value is 6-40 in seconds.
spanning-tree priority x command is used to set the bridge priority of the switch. Bridge priority is for selecting the root device, root port, and designated port. The device with the highest priority (lowest value) becomes the STA root device. If all devices have the same priority, the device with the lowest MAC address will then become the root device. "x" is the priority, and its valid value is 0-61440.
The settings of spanning tree on port are done in "interface" command. The settings here are for bridge only.

31. storm-control command

This command is used to set the storm control rate. The packet storms that could be controlled are broadcast, multicast, and unicast flooding traffic. And the rate is counted with packet per second(pps), not bit per second(bps).
storm-control bc-rate x command is used to set rate limit for broadcast traffic. "x" is the limit rate number, and its valid value is 0-7. (0:disable, 1:1Kpps,2:2Kpps, 3:4Kpps, 4:8Kpps, 5:16Kpps, 6:32Kpps, 7:64Kpps)
storm-control mc-rate x command is used to set rate limit for multicast traffic."x" is the limit rate number, and its valid value is 0-7. (0:disable, 1:1Kpps, 2:2Kpps, 3:4Kpps, 4:8Kpps, 5:16Kpps, 6:32Kpps, 7:64Kpps)
storm-control fc-rate x command is used to set rate limit for unicast flooding traffic. "x" is the limit rate number, and its valid value is 0-7. (0:disable, 1:1Kpps,2:2Kpps, 3:4Kpps, 4:8Kpps, 5:16Kpps, 6:32Kpps, 7:64Kpps)

32. trunk command

This command is used to enable trunk function of the switch. And no trunk comand can be used to disable it.

The trunk function for the switch works with LACP protocol. The system priority of LACP is set by "lacp" command. And the settings on ports is done in "interface" command.

33. username command

This command is used to set the username and password for administrator and guest.

username admin www xxx yyy zzz command is used to set the username and password for administrator. "www" is the old username. "xxx" is the old password. "yyy" is the new username. "zzz" is the new password.

username guest yyy zzz command is used to set the username and password for guest. "yyy" is the new username. "zzz" is the new password.

Administrator is the user who has the right to do configuration modification. Guest is the user who has the right to view configuration only.

34. vlan command

This command is used to enter VLAN configuring mode. And the prompt will become ...

(config)# vlan database

(config-vlan)#

The operations for VLAN are configured in VLAN configuring mode. Please refer to **6.2.5 VLAN Configuring Commands** section for the details.

6.2.4 Interface Configuring Commands

Commands in Configuring Mode are for general switch settings. And its prompt is "(config)#".

The port interface function and VLAN group interface function are set with "interface" command.

(config)# interface ?

ethernet	Ethernet port
vlan	Switch Virtual LAN interface

interface ethernet 1/x command is used to configure settings for Port x. Please refer to section 6.2.4.1 Interface Configuring Commands for Port for the details.

interface vlan x command is used to configure VLAN Group x interface ("x" is the VLAN ID). Please refer to section 6.2.4.2 Interface Configuring Commands for VLAN for the details.

Both commands will change the prompt from "(config)#" to "(config-if)#".

Note: The general VLAN settings are done with "vlan database" command. Please refer to section 6.2.5 VLAN Configuring Commands for the details. And interface vlan x command is used to assign characteristics to a VLAN interface. For example, assigning IP address to a VLAN interface is done with this command.

6.2.4.1 Interface Configuring Commands for Port

Commands in Configuring Mode are for general switch settings. And its prompt is "(config)#".

If the settings are for ports, it is done with "interface ethernet 1/x" command in configure mode. For example, "interface ethernet 1/5" is for settings on Port 5. Some syntax are supported for port selection.

1. interface ethernet 1/x and "x" is port number. All the settings after this command will be applied to this port. For example, "interface ethernet 1/5" and all the settings after this command will be applied to Port 5.
2. interface ethernet 1/x,y,z,... and "x", "y", "z",.. are port number. All the settings after this command will be applied to these ports. For example, "interface ethernet 1/2,4,7" and the settings after this command will be applied

to Port 2, Port 4, and Port 7.
3. interface ethernet 1/x-y and "x","y" are port number. All the settings after this command will be applied to ports in this range. For example, "interface ethernet 1/4-7" and the settings after this command will be applied to Port 4, Port 5, Port 6, and Port 7. (Port 4~7)
4. interface ethernet 1/w,x,..,y-z and "w","x","y","z" are port number. All the settings after this command will be applied to those ports. For example, "interface ethernet 1/1,2,4-7" and the settings after this command will be applied to Port 1, Port 2, Port 4, Port 5, Port 6, and Port 7. (Port 4~7)
Entering "interface ethernet 1/5", and its prompt will become ...

```
(config)# interface ethernet 1/5
(config-if)#
```

Enter "?" at the prompt, the sub-command list will be shown.

```
(config-if)# ?

exit                    Exit from current mode
help                    Show available commands
history                 Show a list of previously run commands
logout                  Disconnect
quit                    Quit commands
channel-group           Adds a port to a trunk
description             Interface specific description
dot1x                   Configures 802.1x port-based access control
duplex                  Configures duplex operation
end                     Exit from interface mode
flowcontrol             Enables flow control during autoneg
interface               Enters privileged interface configuration
ip-filter               Set ipaddress filter
lacp                    Configures LACP status
map                     Maps priority
maximum-packet-length   Configures the maximum packet length of the port
mdi-mdix                Configures the MDI or MDIX of the port
mvr                     Multicast VLAN Registration
no                      Negates a command or sets its defaults
port                    Configures the characteristics of the port
```

port-vlan	Configures Port-Based VLAN
power-saving	Decrease energy consumption
qos	Configuration of QoS
rate-limit	Configures rate-limits
shutdown	Shuts down the selected interface
spanning-tree	Specifies spanning tree configuration
speed	Configures speed operation
switchport	Configures switching mode characteristics

---

1. exit command

This command is used to leave current operation mode. Go back to last mode.

2. help command

This command is used to show all the available commands in this mode.

3. history command

This command is used to show the history of entering commands.

4. logout command

This command is used to logout from console interface.

5. quit command

This command is used to quit from console interface. It has the same function as logout.

6. channel-group command

This command is used to add the interface port(s) to a trunk group. This is a static port-trunk assignment. And the static assigned port(s) will be ignored by LACP protocol.

channel-group x will add the interface port(s) to the trunk group "x". "x" is the trunk group number, and its valid value is 1-8.

no channel-group will remove the interface port(s) from any trunk group.

7. description command

This command is used to assign a description string for the port(s). description xxx command will assign a description string for the port(s). "xxx" is the string. no description command will clear the description string.

8. dot1x command

This command is used to configure 802.1x function for the interface port(s).

dot1x port-control auto command is used to set the interface port(s) to need dot1x-aware client RADIUS server authorization.
dot1x port-control force-authorized command is used to set the interface port(s) to grant access to all clients.
dot1x port-control force-unauthorized command is used to set the interface port(s) to deny access to all clients.
dot1x port-control none command is used to set the interface port(s) not to need dot1x operation.

9. duplex command

This command is used to set the duplex mode of the interface port(s). It could be full duplex or half duplex.
Note: Half duplex is for 10M and 100M speed mode only. 1000M speed mode don't support half duplex.
duplex full command will set the interface port(s) to full duplex.
duplex half command will set the interface port(s) to half duplex.

10. end command

This command is used to exit from interface mode.
(config-if)# end
(config)#

11. flowcontrol command

This command is used to enable flow control function of the interface port(s).
flowcontrol command is used to enable flow control function of the interface port(s).
no flowcontrol command is used to disable flow control function of the interface port(s).

12. interface command

This command is used to change the interface port(s) or interface VLAN groups for next setup commands.
(config-if)# interface ?
ethernet Ethernet port
vlan Switch Virtual LAN interface
For example,

"(config)# interface ethernet 1/5" will set current setup interface to Port 5 and all the commands will be applied to Port 5.
"(config-if)# interface ethernet 1/6-7" will change current setup interface to Port 6-7 and all the commands will be applied to Port 6-7.
If "vlan" sub-command is used, current setup interface will be changed to some VLAN groups. For example,
"(config-if)# interface vlan 100" will change current setup interface to VLAN 100
and all next commands will be applied to VLAN 100.
The description of commands in interface configuring mode is put in Section **6.2.4 Interface Configuring Commands**. Please refer to the section for the details.

13. ip-filter command

This command is used to set the IP address and subnet for IP-Filtering operation on the port(s). If the IP address is set and IP-Filtering function is 43
enabled, only network devices in this IP subnet can access network through the port(s).
ip-filter xxx.xxx.xxx.xxx y command is used to set the IP address and subnet
for IP-Filtering operation on the port(s). "xxx.xxx.xxx.xxx" is the IP address. y (0~32) is the network ID bit number, or called subnet mask. For example, "ip-filter 192.168.1.10 32" will allow 192.168.1.10 for network access only.
no ip-filter command is used to clear the setting on the port(s).

14. lacp command

This command is used to enable LACP protocol working on the interface port(s).
lacp command will enable LACP protocol working on the interface port(s).
no lacp command will disable LACP protocol working on the interface port(s).
If the interface port(s) are already assigned to trunk by "channel-group" command, its LACP function will be ignored.

15. map command

For a IP packet, there is priority information in ToS field of IP header. The

priority could be 3-bit precedence (0~7) or 6-bit DSCP (0~63).
For DSCP, this switch supports seven DSCP values for QoS operation and other values will be assigned to one priority.
This command is used to map 802.1P priority values and DSCP priority values to priority queues on the interface port(s). There are four priority queues for each port. They are Low, Normal, Medium, and High priority queues. This command can map the priority values to the four priority queues.
map dscp x y z command is used to map IP DSCP values to priority queues. "x" is the index of DSCP values and it could be 0-6 and "other". "y" is the DSCP value, and its valid value is 0-63. "z" is the prirority queue, and its value is 0-3 (0:Low,1:Normal,2:Medium,3:High).
map priority x y command is used to map 802.1P priority values to priority queues. "x" is the value of 802.1P priority, and its valid value is 0-7. "y" is the prirority queue and its value is 0-3 (0:Low, 1:Normal, 2:Medium, 3:High).

16. maximum-packet-length command

This command is used to set the maximum packet size allowed on the interface port(s). For normal Etherent packets, the packet size is 64~1514 bytes. For some gigabit connections, "jumbo frame" is allowed for higher data transfering efficiency. This switch supports up to 9600 bytes packet size.

```
(config-if)# maximum-packet-length ?
1518        max.    packet length=1518
1532        max.    packet length=1532
9216        max.    packet length=9216
9600        max.    packet length=9600
```

17. mdi-mdix command

This command is used to set the MDI/MDI-X mode of port(s). This switch supports Auto-MDi/MDIX function. And this command can force it MDI or MDI-X mode. (MDI is for hub/switch cascading. MDI-X is for PC/device connecting.)
mdi-mdix mdi command is used to set the port(s) to MDI mode.
mdi-mdix mdix command is used to set the port(s) to MDI-X mode.
no mdi-mdix command is used to set the port(s) to Auto-MDI/MDI-X mode.

18. mvr command

This command is used to assign the port(s) as source port of IP multicast traffic or as receiver port of subscribers for some MVR VLAN.

mvr x receiver-port command is used to set the port(s) as the IP multicast traffic receiver port of MVR VLAN. "x" is the MVR VLAN ID.

mvr x source-port command is used to set the port as the IP multicast traffic source port of MVR VLAN. "x" is the MVR VLAN ID.

19. no command

This command is used to disable a function or restore a setting to factory default of the switch.

(config-if)# no ?

channel-group	Adds a port to a trunk
description	Interface specific description
dot1x	Configures 802.1x port-based access control
duplex	Configures duplex operation
flowcontrol	Enables flow control during autoneg
ip-filte	Set ipaddress filter
lacp	Configures LACP status
map	Maps priority
maximum-packet-length	Configures the maximum packet length of the port
mdi-mdix	Configures the MDI or MDIX of the port
mvr	Multicast VLAN Registration
port	Configures the characteristics of the port
port-vlan	Configures Port-Based VLAN
power-saving	Decrease energy consumption
qos	Configuration of QoS
rate-limit	Configures rate-limits
shutdown	Shuts down the selected interface
spanning-tree	Specifies spanning tree configuration
speed	Configures speed operation
switchport	Configures switching mode characteristics

For example,

"lacp" command can enable the LACP function on the interface port(s) and "no

lacp" command can disable it.
"maximum-packet-length 9600" will set the maximum packet size to 9600, and "no maximum-packet-length" will put it to factory default setting 1518.

20. port command

This command can be used to setup monitor function and security function on the interface port(s).
(config-if)# port ?
monitor Monitors another interface
security Specif ies port security

port monitor ethernet 1/x rx command is used to add Port x to the monitored port list. All the receive traffic from monited ports will be copied to the interface port(s). "x" is the monitored port number. And no port monitor ethernet 1/x rx command will remove Port x from monitored port list.
For example, "port monitor ethernet 1/2 rx" command will add Port 2 to the monitored port list, and receive traffic to Port 2 will be copied to the interface port(s). If current setup interface port is Port 5, Port 5 will be the monitoring port.
port security action command will set the interface port(s) to "accept" mode. In "accept" mode, only devices/PC with static Mac addresses assigned on the interface port(s) can access network through the interface port(s). Other devices/PC will be rejected.
port security max-mac-count x command is used to set the maximum Mac address number allowed on the interface port(s). "x" is the maximum number and its valid value is 0-8192. For example, x=5 will allow up to five network devices / PC access network through the interface port(s). And the port security will be set to this operation mode with this command.
no port security command can be used to disablethe security function on the interface port(s).

21. port-vlan command

This command is used to assign the interface port(s) to a Port-based VLAN, and set the name(description) for the Port-based VLAN.
port-vlan x yyy command will assign the interface port(s) to a Port-based VLAN, and set the name(description) to the Port-based VLAN. "x" is the index

of the Port-based VLAN. "yyy" is the name(description) for it.

22. power-saving command

This command is used to enable the power-saving function for the interface port(s). If it is enabled and auto-negotiation is also enabled, the interface port(s) will go to low-power mode when link down. That can reduce power consumption of the switch. When link is detected, ports will come back to normal working state automatically.

power-saving command is used to enable the power-saving function for the interface port(s).

no power-saving command is used to disable this function on the interface port(s).

23. qos command

This command is used to set port-based priority on the interface port(s). And enable 802.1P priority, DSCP priority on the interface port(s).

(config-if)# qos ?

dscp		enable IP DSCP priority
port		Port priority map
precedence	enable	IP precedence priority

qos dscp command is used to enable DSCP priority operation on the interface port(s). And no qos dscp command is used to disable it.

qos precedence command is used to enable 802.1P priority operation on the interface port(s). And no qos precedence command is used to disable it.

qos port x command is used to set port-based priority on the interface port(s). "x" is the priority queue, and its value is 0-3 (0:Low, 1:Normal, 2:Medium, 3:High).

Note: If DSCP priority, 802.1P priority and Port-based priority are enabled on the interface port(s) at the same time, its decision flow is DSCP -> 802.1P -> Port-base.

24. rate-limit command

This command is used to set the ingress and egress rate limit level of the interface port(s). The working rate limit number is counted with (rate limit level)x(rate limit unit). The rate limit unit is set by "rate-limit unit x"

command in general configuring mode (under "(config)#" prompt). And the rate-limit level is set by this command.

rate-limit input level x command is used to specify the ingress rate-limit level of the interface port(s). "x" is the level number and its valid value is 0~31. If "x"=0, it means "no limit".

rate-limit output level x command is used to specify the egress rate-limit level of the interface port(s). "x" is the level number and its valid value is 0~31. If "x"=0, it means "no limit".

25. shutdown command

This command is used to disable the interface port(s).

shutdown command is used to disable the interface port(s).

no shutdown command is used to enable it.

26 spanning-tree command

This command is used to configure spanning tree function on interface port(s).

(config-if)# spanning-tree ?

cost	Specifies spanning tree cost
edge-port	Specifies spanning tree edge port
port-priority	Specifies spanning tree port priority
spanning-disabled	Disables the spanning tree

spanning-tree cost x command is used to set spanning tree port path cost value on the interface port(s). It is used to determine the best path between devices if looping happens. Lower values will be forwarded and should be assigned to ports with fast connections. Higher values will be blocked and should be assigned to ports with slow connections. "x" is the cost value and its valid value is 1~65535. The suggestion values are 100(50~600) for 10M, 19(10~60) for 100M and 4(3~10) for 1000M connections.

spanning-tree edge-port command is used to set the interface port(s) as edge port. And no spanning-tree edge-port command is used to set it as non-edge port. "Edge port" means the interface port(s) are connected to end device(s) but not switch-to-switch connection.

spanning-tree port-priority x command is used to set the spanning tree port priority value on the interface port(s). "x" is the port-priority value and its valid value is 0~240. If the path cost for all ports on a switch are the same, the

port with the highest priority (lowest value) will be forwarded when looping happens. If more than one port have the same highest priority, the port with lowest port number will be forwarded.

spanning-tree spanning-disabled command is used to disable spanning tree function on the interface port(s). And no spanning-tree spanning-disabled command will enable it.

27. speed command

This command is used to set the operation speed of the interface port(s).

(config-if)# speed ?

auto	Set port speed to be auto
10	Set port speed to be 10M
100	Set port speed to be 100M
1000	Set port speed to be 1G

speed auto command will set the interface port(s) to auto-negotiation mode.

speed 10 command will set the interface port(s) to 10M speed.

speed 100 command will set the interface port(s) to 100M speed.

speed 1000 command will set the interface port(s) to 1000M(gigabit) speed.

28. switchport command

This command is used to configure some switch function characteristics for the interface port(s).

(config-if)# switchport ?

acceptable-frame-types	Specifies frame type
allowed	Configures the VLAN port list
mode	Configures the port mode
native	Configures the PVID of the port
private-vlan	Private VLAN
untag-vid	Configures the port untag vid
vlan-stacking	VLAN Stacking port mode

[Accept Frame Type]

switchport acceptable-frame-types all command is used to allow the interface port(s) to accept all types of frame.

switchport acceptable-frame-types tagged command is used to allow the interface port(s) to accept tagged frame only. Other frame type will be

rejected.
[VLAN Port Assignment]
switchport allowed vlan add x command will add the interface port(s) to VLAN x. "x" is the VLAN ID and its valid value is 2~-4094.
switchport allowed vlan remove x command will remove the interface port(s) from VLAN x. "x" is the VLAN ID and its valid value is 2~-4094.

[VLAN Port Mode Setting for Private VLAN]
switchport mode private-vlan host command will set the port type of the interface port(s) in Private VLAN as "host". "host" port(s) could be for Community VLAN or Isolated VLAN.
switchport mode private-vlan promiscuous command will set the port type of the interface port(s) in Private VLAN as "promiscuous". "promiscuous" port(s) could be for Primary VLAN or Isolated VLAN.
no switchport mode private-vlan command will set the port type of the interface port(s) in Private VLAN as "normal". "normal" port(s) is for normal 802.1Q VLAN operation.

[VLAN Port Tag/Untag Setting for 802.1Q VLAN]
switchport mode hybrid command will set the interface port(s) as hybrid port(s) for 802.1Q VLAN operation. If a port is defined as "hybrid", it is a tag port basically. But it will act as an untag port for packets working in VLAN defined in "Untag VID". So, it is called a hybrid port.
For example, set Port 5 as "hybrid" and its Untag VID as 10. Port 5 will act as a tag port for all packets except packets for VLAN 10. Port 5 will act as an untag port for packets working for VLAN 10.
switchport mode trunk command will set the interface port(s) as tag port(s) for 802.1Q VLAN operation. Tag port will always send tagged packets and is used for switch-to-switch cascading. It is a VLAN trunk connection because there could be more than one VLAN working through it.
switchport mode access command will set the interface port(s) as untag port(s) for 802.1Q VLAN operation. Untag port will always send untagged packets and is used for switch to users connection. And its role is a "access" connection for users.

[Port VLAN ID Setting]

switchport native vlan x command is used to assign VLAN ID of the native VLAN for classifying untagged frames on ingress port. "x" is the port VLAN ID (PVID) and its valid value is 1~4094.

When untagged packet is received, PVID of the ingress port will be used as its working VLAN ID. PVID is also used as the VLAN ID for tag adding when untagged packet is translated to tagged packet.

[Untag VLAN ID Setting for Hybrid Ports]

switchport untag-vid x command is used to set untag-VID of the port. It is used when this port is set to "hybrid" role for 802.1Q function. And packets for this untag-VLAN will be forwarded with untagged. Other packets will be forwarded with tagged. "x" is the VLAN ID and its valid value is 1~4094.

[Private VLAN Port Assignment]

switchport private-vlan host-association x command is used to assign this interface port(s) to a Community VLAN. And the port type of the interface port(s) must be "host" first. "x" is the VLAN ID of the Community VLAN and its valid value is 2~4094.

switchport private-vlan isolated x command is used to assign this interface port(s) to a Isolated VLAN. And the port type of the interface port(s) must be "host" or "promiscuous" first. "x" is the VLAN ID of the Isolated VLAN and its valid value is 2~4094.

switchport private-vlan mapping x command is used to assign this interface port(s) to a Primary VLAN. And the port type of the interface port(s) must be "promiscuous" first. "x" is the VLAN ID of the Primary VLAN and its valid value is 2~4094.

[VLAN Stacking (Q-in-Q) Setting]

switchport vlan-stacking normal command is used to set the port(s) as normal 802.1Q VLAN port(s). And the tagged/untagged setting will follow the settings in 802.1Q VLAN.

switchport vlan-stacking access command is used to set the port(s) as access port(s) for VLAN stacking operation. It will strip a tag from tagged or double-tagged packets before forwarding. It is for downward connection of VLAN stacking operation.

switchport vlan-stacking tunnel command is used to set the port as tunnel

port for VLAN stacking operation. It will add a tag and allow two 802.1Q VLAN tags in a packet. It is for tunnel and upward connection of VLAN stacking operation.

6.2.4.2 Interface Configuring Commands for VLAN

Commands in Configuring Mode are for general switch settings. And its prompt is "(config)#".

If the characteristics are for VLAN group, it is done with "interface vlan x" command in configure mode. For example, "interface vlan 100" is for characteristics settings on VLAN 100.

Note: The general VLAN settings are done with "vlan database" command. Please refer to section 6.2.5 VLAN Configuring Commands for the details. And interface vlan x command is used to assign characteristics to a VLAN group interface. For example, assigning IP address to a VLAN interface is done with this command.

Entering "interface vlan 100", and its prompt will become ...

```
(config)# interface vlan 100
(config-if)#
```

Enter "?" at the prompt, the sub-command list will be shown.

```
-------------------------------------------------------------------------------
(config-if)# ?
exit                Exit from current mode
help                Show available commands
history             Show a list of previously run commands
logout              Disconnect
quit                Quit commands
interface           Enters privileged interface configuration
ip                  Internet protocol
no                  Negates a command or sets its defaults
-------------------------------------------------------------------------------
```

1. exit command

This command is used to leave current operation mode. Go back to last mode.

2. help command

This command is used to show all the available commands in this mode.

3. history command

This command is used to show the history of entering commands.

4. logout command

This command is used to logout from console interface.

5. quit command

This command is used to quit from console interface. It has the same function as logout.

6. interface command

This command is used to change to interface port(s) or another interface VLAN groups for next setup commands.

(config-if)# interface ?

ethernet Ethernet port

vlan Switch Virtual LAN interface

For example,

"(config)# interface ethernet 1/5" will change the setup interface to Port 5 and all the following commands will be applied to Port 5.

"(config-if)# interface ethernet 1/6-7" will change the setup interface to Port 6-7 and all the following commands will be applied to Port 6-7.

If "vlan" sub-command is used, the setup interface will be changed to some VLAN groups. For example,

"(config-if)# interface vlan 100" will change the setup interface to VLAN 100 and all following commands will be applied to VLAN 100.

The description of commands in interface configuring mode is put in Section 6.2.4 Interface Configuring Commands. Please refer to the section for the details.

7. ip command

This command is used to set IP address of the switch on this VLAN interface. And only users in this VLAN can access this switch with the IP address remotely.

(config-if)# ip address ?

dhcp	Dynamic host configuration protocol
A.B.C.D	IP address
renew	Renew IP
release	Release IP

ip address dhcp command is used to enable DHCP client function. DHCP client function will try to get IP configuration from DHCP server in network. And no ip address dhcp command can be used to disable it.
ip address x.x.x.x y.y.y.y command is used to set IP address of the switch on this VLAN. "x.x.x.x" is the IP address. "y.y.y.y" is the subnet mask.
For example, "ip address 192.168.1.12 255.255.255.0" will set the IP address of the switch on this VLAN group for remote management.
ip address renew command is used to refresh the lease time of the IP address got by DHCP. If IP configuration is not got when boot-up, this command will try to get IP configuration again.
ip address release command is used to release current IP address got by DHCP. Then, you can try to get the IP configuration again by "ip address renew" command.

8. no command

This command is used to disable a function or restore a setting to factory default of the switch.

```
(config-if)# no ?
ip                  Internet protocol
```

For example,
"ip address dhcp" command can enable DHCP client function on the VLAN group interface and "no ip address dhcp" command can disable it.

6.2.5 VLAN Configuring Commands

Commands in Configuring Mode are for general switch settings. And its prompt is "(config)#".

If the settings are for VLANs, it should enter VLAN configuring mode first by "vlan database" command in configure mode. And its prompt will become "(config-vlan)#".

Note: If the settings are for some VLAN group (VLAN ID is known), it should enter

interface configuring mode for VLAN first by "interface vlan x" command. ("x" is the VLAN ID.) And its prompt is "(config-if)#". It is described in Section 6.2.4.2.

Entering "vlan database", and the prompt will become ...

```
(config)# vlan database
(config-vlan)#
```

Enter "?" at the prompt, the sub-command list will be shown.

```
-------------------------------------------------------------------------------
(config-vlan)# ?
exit                Exit from current mode
help                Show available commands
history             Show a list of previously run commands
logout              Disconnect
quit                Quit commands
end                 Exit from vlan mode
1q-vlan             Configures 802.1Q VLAN
no                  Negates a command or sets its defaults
port-vlan           Configures Port-Based VLAN
private-vlan        Private VLAN
vlan                Switch Virtual LAN interface
-------------------------------------------------------------------------------
```

1. exit command

This command is used to leave current operation mode. Go back to last mode.

2. help command

This command is used to show all the available commands in this mode.

3. history command

This command is used to show the history of entering commands.

4. logout command

This command is used to logout from console interface.

5. quit command

This command is used to quit from console interface. It has the same function as logout.

6. end command

This command is used to exit from VLAN Configuring mode.

(config-vlan)# end

(config)#

7. 1q-vlan command

This command is used to configure 802.1Q VLAN characteristics.

(config-vlan)# 1q-vlan ?

gvrp Enables GVRP globally for the switch

ingress-filtering Conf igures frame filtering base on VLAN membership

<cr>

1q-vlan command can enable 802.1Q VLAN function. And no 1q-vlan command can disable it.

1q-vlan gvrp command is used to enable GVRP function of 802.1Q VLAN. This command works only if 802.1Q VLAN is enabled. And GVRP will be disable automatically when 802.1Q VLAN is set to disable. no 1q-vlan gvrp command can disable it.

1q-vlan ingress-filtering command is used to enable doing VLAN membership filtering at ingress port instead of egress port. no 1q-vlan **ingress-filtering** command can disable it.

8. no command

This command is used to disable a function or restore a setting to factory default of the switch.

(config-vlan)# no ?

1q-vlan	Conf igures 802.1Q VLAN
port-vlan	Configures Port-Based VLAN
private-vlan	Private VLAN
vlan	Switch Virtual LAN interface

For example,

"1q-vlan" command can enable 802.1Q VLAN function and "no 1q-vlan"

command can disable it. “no vlan 100” command will remove VLAN 100.

9. port-vlan command

This command is used to enable Port-base VLAN. And 802.1Q VLAN function will be disable at the same time.
port-vlan command is used to enable Port-base VLAN.
no port-vlan command is used to disable it.

10. private-vlan command

This command is used to create VLAN groups for Private VLAN and create the associations between Primary VLAN and Community VLAN.
(config-vlan)# private-vlan 100 ?

association	Association
name	VLAN interface name

private-vlan x association y command is used to create the association between Primary VLAN “x” and Community VLAN “y”
private-vlan x association add y command is used to add the association between Primary VLAN “x” and Community VLAN “y”.
private-vlan x association remove y command is used to remove the association between Primary VLAN “x” and Community VLAN “y”.
no private-vlan x association command is used to reomove all the association for Primary VLAN “x”.
(config-vlan)# private-vlan 100 name sales ?

community	Community
isolated	Isolated
primary	Primary

private-vlan x name yyy community command is used to create a Community VLAN with VLAN ID “x”, VLAN name “yyy” for Private VLAN application.
private-vlan x name yyy isolated command is used to create a Isolated VLAN with VLAN ID “x”, VLAN name “yyy” for Private VLAN application.
private-vlan x name yyy primary command is used to create a Primary VLAN with VLAN ID “x”, VLAN name “yyy” for Private VLAN application.
no private-vlan x command can be used delete a Private VLAN “x”. (“x” is the

VLAN ID).

11. vlan command

This command is used to create a 802.1Q VLAN. In this command, you have to assign the VLAN ID and VLAN name for VLAN creation.

vlan x name yyy media ethernet command is used to create a 802.1Q VLAN with VLAN ID "x" and VLAN name "yyy". For example, "vlan 500 name sales media ethernet" will create a VLAN with VLAN ID 500 and VLAN name "sales".

no vlan x command can be used to remove the VLAN with VLAN ID "x". (Note: If VLAN "x" already exists but name "yyy" is different, this command will rename the VLAN.)

6.2.6 Show Commands

Show command is put in General Basic Commands for viewing system configuration and information.

Enter "show ?" at the prompt, the sub-command list will be shown.

```
# show ?

aaa                 Show AAA service configuration
calendar            Date and time information
dhcp-relay          DHCP Relay Configuration
dot1x               802.1x content
gvrp                GVRP configuration
history             History information
interface           Interface information
ip                  IP information
ip-filter           IP Filter Configuration
lacp                LACP statistics
line                TTY line information
log                 Log records
mac-address-table   Configuration of the address table
mac-security        MAC Security Configuration
management          Management IP filter
map                 Maps priority
```

mvr	Show MVR Status
port	Port characteristics
queue	Priority queue information
radius-server	RADIUS server information
running-config	Information on the running configuration
rate-limit	Configures rate-limits
snmp	Simple Network Management Protocol statistis
sntp	Simple Network Time Protocol configuration
spanning-tree	Spanning-tree configuration
system	System information
trunk	Trunk information
version	System hardware and software versions
vlan	Virtual LAN settings

---

1. show aaa authentication login command

This command will show the authentication settings for admin of the switch when login for management. It could be authenticated by local switch or RADIUS Server, or local switch first RADIUS Server next.

For example,

show aaa authentication login

Authentication:

local

2. show calendar command

This command will show current system time.

For example,

show calendar

Current Time : 2010/05/29-11:20:12

3. show dhcp-relay command

This command will show current DHCP Relay/Option 82 settings.

For example,

show dhcp-relay

DHCP Relay Configuration

DHCP Relay Status: Disable

Add additional option82 information: Disable

Relay Agent information:

DHCP Server IP Address:

4. show dot1x command

This command is used to show 802.1x configuration and status.

show dot1x command is used to show current 802.1x configuration and status of each port. For example,

show dot1x

[Port Authentication Configuration]

Port	Status	Authentication Mode
1/1		Force-Authorized
1/2		Force-Authorized
1/3	Yes	Force-Authorized
1/4		Force-Authorized
1/5		Force-Authorized
1/6		Force-Authorized
1/7		Force-Authorized
1/8		Force-Authorized
1/9		Force-Authorized
1/10		Force-Authorized

show dot1x configuration command is used to show 802.1x configuration and status of the switch. For example,

show dot1x configuration

[802.1x Configuration]

802.1x System Authentication Status: Disable

Re-authentication: Disable

Re-authentication Timeout Period : 3600 seconds

Re-authentication Max Count: 2

Max Request Count: 2

Server Timeout Period: 30 seconds

Supplicant Timeout Period: 30 seconds

Quiet Timeout Period: 60 seconds

Tx Timeout Period: 30 seconds

Supplicant Allowed In Guest Vlan: Disable

Dynamic vlan: Disable

5. show gvrp command

This command is used to show current GVRP configuration.

show gvrp configuration command will show current GVRP configuration.

```
# show gvrp configuration
GVRP configuration: Disable
```

6. show history command

This command is used to show the history of input commands.

```
# show history
0. show
1. show gvrp configuration
2. show history
```

7. show interface command

This command is used to show port information and status.

```
# show interface ?
counters                Interface counters information
status                  Interface status information
switchport              Interface switchport information
```

show interface counters command will show total statistics counters for all ports.

show interface counters ethernet 1/x command will show statistics counters for Port x. ("x" is the port number).

For example,

```
# show interface counters ethernet 1/3
Port: 1/3
=========================================
Rx Counter                          Statistics
Good Unicast Frame                    4109
Good Broadcast Frame          9946
Good Multicast Frame          158
Discarded Frame                         0
Errors                                  0
Total Receive Byte Count      15498     16
```

==========

Tx Counter	Statistics
Good Unicast Frame	2001
Good Broadcast Frame	18
Good Multicast Frame	0
Discarded Frame	0
Errors	0
Total Transmit Byte Count	873047

show interface status command will show port status of all ports (one after another).

show interface status ethernet 1/x command will show port status of Port x.("x" is the port number).

For example,

show interface status ethernet 1/5

Basic information:

Port type: 1000TX

Mac address: 00:11:22:64:99:6F

Configuration:

Name: Port 5

Port admin: Enable

Speed-duplex: Auto_on

Capabilities: 10half,10full,100half,100full,1000full

Broadcast storm: Disable

Flooded unicast storm: Disable

Multicast storm: Disable

Flow control: Disable

Power saving: Disable

LACP: Disable

Max MAC count: 0

Maximum Packet Length: 9600

IPaddress Filter: 1

Current status:

Link status: Up

Operation speed-duplex: 100Half

MDI/MDI-X: Auto

show interface switchport command will show function configuration of all ports (one after another).
show interface switchport ethernet 1/x command will show function configuration of Port x. ("x" is the port number).
For example,
show interface switchport ethernet 1/5
Information of Eth 1/5
Rate-limit level of input: 0
Ingress rate limit: Disable
Rate-limit level of output: 0
Egress rate limit: Disable
VLAN membership mode: access
VLAN stacking role: normal
Ingress rule: Disable
Acceptable frame type: All frames
Native VLAN: 1
Untag vid: 1
Priority for untagged traffic:Low
Private-VLAN mode: Normal
IP Address of IP Filter:
Netmask of IP Filter:

8. show ip command

This command is used to show current IGMP configuration and switch IP configuration.
60
show ip ?

igmp	IGMP snooping
interface	Interface information
redirects	Default gateway configured for this device

show ip igmp snooping command will show current switch IGMP configuration.
show ip igmp snooping mrouter command will show current IGMP multicast router setting.

For example,
show ip igmp snooping
IGMP Status: Disable
IGMP Querying: Disable
IGMP Querying: Disable
IGMP Query Interval: 125 seconds
IGMP Report Delay: 15 seconds
IGMP Query Timeout: 255 seconds
show ip igmp snooping mrouter
Type M'cast Router Ports
---
static Eth 1/
show ip interface command will show current switch IP configuration.
For example,
show ip interface
IP address and netmask: 192.168.1.12 255.255.255.0 on VLAN 1
show ip redirects command will show current IP gateway setting of the switch.
For example,
show ip redirects
gateway: 192.168.1.254

9. show ip-filter command

This command is used to show current IP-Filter function status of the switch.
show ip-filter
IP Filter Configuration
IP Address Filter: Disable

For showing filter IP address, "show interface switchport" command will show port settings one after another. And "show interface switchport ethernet 1/x" command will show Port x settings.

10.show lacp command

This command is used to show current LACP configuration of the switch.
show lacp ?
internal Shows config settings/operational state for local side

portstatus Shows LACP Port Status
sysid Shows channel groups system priority/MAC address

show lacp internal command is used to show system priority and protocol enable/disable status of ports.

```
# show lacp internal
[Lacp Port Configuration]
System Priority: 65535
Port Protocol Enabled
-------------------------
Eth 1/1 Disable
Eth 1/2 Disable
Eth 1/3 Disable
Eth 1/4 Disable
Eth 1/5 Disable
Eth 1/6 Disable
Eth 1/7 Disable
Eth 1/8 Disable
Eth 1/9 Disable
Eth 1/10 Disable
```

show lacp portstatus command is used to show LACP working status of ports.

```
# show lacp portstatus
[ LACP Port Status ]
Port      Protocol Active      Partner Port Number      Operational Port Key
1              no
2              no
3              no
4              no
5              no
6              no
7              no
8              no
9              no
10             no
```

show lacp sysid command is used to show system ID of the switch for LACP protocol.

```
# show lacp sysid
65535
```

11. show line command

This command is used to show current console line configuration.

show line console command is used to show current console line configuration.

```
# show line console
Password threshold: open-end time
Baudrate: 9600
Databits: 8
Parity : 0 [0|1|2|3][NONE|EVEN|ODD|MARK|SPACE]
Stopbits: 1
```

12. show log command

This command is used to show current system log and system log configuration.

```
# show log ?
configuration          log     ging configuration
<cr>
```

show log command is used to show current system log content.

For example,

```
# show log
[5] Thu Jan 01 09:00:02 1970
Level: 4 System Started [port 0]
[4] Thu Jan 01 09:08:20 1970
Level: 4 Link down [port 8]
[3] Thu Jan 01 09:07:50 1970
Level: 4 Link up [port 8]
[2] Thu Jan 01 09:07:45 1970
Level: 4 Link down [port 8]
[1] Thu Jan 01 09:00:06 1970
Level: 4 System Started
```

show log configuration command is used to show current system log configuration.

For example,

```
# show log configuration
[System Log]
System Log Status : Enable
Log Level(0-7): 7
Remote Log              : Disable
Remote Log Server IP : Empty
Remote Log Server IP : Empty
Remote Log Server IP : Empty
Remote Log Server IP : Empty
Remote Log Server IP : Empty
```

13. show mac-address-table command

This command is used to set Mac address table and configuration about it.

```
# show mac-address-table ?
aging-time          Aging time for entries in the address table
address             Address information
interface           Ethernet or port channel-interface
multicast           Knowns multicast addresses
<cr>
```

show mac-address-table command will show mac address table content.

For example,

```
# show mac-address-table
Interface MAC Address VLAN Type
============================================
Eth 1/3 00-00-01-00-00-20 Learned
Eth 1/3 00-0E-A0-00-03-28 Learned
Eth 1/3 00-90-08-A7-76-C6 Learned
Eth 1/3 00-C0-F6-01-11-40 Learned
Eth 1/3 00-80-C8-BF-10-D2 Learned
Eth 1/3 00-C0-F6-01-15-87 Learned
Eth 1/3 00-90-CC-82-A5-D6 Learned
Eth 1/3 00-00-E2-82-8C-E6 Learned
```

show mac-address-table aging-time command will show aging time of mac
address table.
For example,
show mac-address-table aging-time
Status: Enable
Aging time: 300 sec

show mac-address-table address x-x-x-x-x-x command will show the mac address table for mac address "x-x-x-x-x-x".
For example,
show mac-address-table address 00-00-e2-82-8c-e6
Interface MAC Address VLAN Type
==========
Eth 1/3 00-00-E2-82-8C-E6 Learned

show mac-address-table interface ethernet 1/x command will show the mac address table for Port x. ("x" is the port number).
For example,
show mac-address-table interface ethernet 1/3
Interface MAC Address VLAN Type
==========
Eth 1/3 00-00-01-00-00-20 Learned
Eth 1/3 00-90-CC-82-A5-D6 Learned
Eth 1/3 00-00-E2-82-8C-E6 Learned
Eth 1/3 00-C0-F6-01-04-28 Learned
show mac-address-table multicast command will show multicast address table for IGMP function.
For example,
show mac-address-table multicast
Group VID Group Address Members Port
---

14. show mac-security command

This command is used to show mac address security settings on port. There are two mac address security functions for ports. One is "accept" function that

allows static mac addresses on ports to access network only. Another is "limit by mac no." function and up to a limit number of mac addresses are allowed to access network from the port.

For example,

show mac-security

[MAC Security Configuration]

==========

Port#	Max.	MAC no.	Learned no	Security Control
Eth 1/ 1	0		N/A	No Security
Eth 1/ 2	0		N/A	No Security
Eth 1/ 3	0		N/A	No Security
Eth 1/ 4	0		N/A	No Security
Eth 1/ 5	0		N/A	No Security
Eth 1/ 6	10		0	Limited by MAC no
Eth 1/ 7	0		N/A	No Security
Eth 1/ 8	0		N/A	Accept function
Eth 1/ 9	0		N/A	No Security
Eth 1/ 10	0		N/A	No Security

15. show management command

This command is used to show switch management security settings. The IP/subnet, access mode, and protocol functions security settings will be shown.

For example,

show management

[Management IP configuration]

Index Enabled Address / Net Mask Mode Http Telnet SNMP

==========

1 Yes 0.0.0.0/0.0.0.0 Modify Yes Yes Yes

2 No 0.0.0.0/255.255.255.255 View No No No

3 No 0.0.0.0/255.255.255.255 View No No No

4 No 0.0.0.0/255.255.255.255 View No No No

==========

16. show map command

This command is used to show 802.1P priority, DSCP priority, and port-based priority to priority queues mapping. There are four priority queues on each port

of the switch.

```
# show map ?
dscp                IP DSCP priority map
port                IP port priority
priority        802.1p      priorities map
```

show map dscp command is used to show IP DSCP QoS function enable/disable status, and DSCP values(0~63) to priority queue mapping on each port.

show map dscp ethernet 1/x command is used to show DSCP values(0~63) to priority queues mapping on Port x. ("x" is the port number.)

show map port command is used to show connection port to priority queues mapping. This is called port-based priority.

show map priority command is used to show 802.1P priority values(0~7) to priority queues mapping on each port.

show map priority ethernet 1/x command is used to show 802.1P priority values(0~7) to priority queues mapping on Port x. ("x" is the port number.)

17. show mvr command

This command is used to show MVR configuration.

show mvr command is used to show MVR VLAN setting one after another.

show mvr x command is used to show a MVR VLAN setting. "x" is the VLAN ID.

For example,

```
# show mvr 11
Active: Yes
Name:
MVLAN: 11
802.1p Priority: 0
Mode: Dynamic
Source Port: Eth1/ 10
Receiver Port: Eth1/ 5 Eth1/ 6 Eth1/ 7
MVR Group Configuration:
Name          Start Address       End Address
---------------   ---------------       ---------------
```

abc 224.0.0.1 224.0.0.2
abcd 224.0.0.3 224.0.0.4

18. show port command

This command is used to show port mirror function setting.
show port monitor command is used to show port mirror function setting.
For example,
show port monitor
Mode: Disable
Destination port: 1
Source port:

19. show queue command

This command is used to show traffic scheduling settings for priority queues on ports.
show queue ?
bandwidth Shows weighted round-robin (WRR) bandwidth
mode Priority queue information

show queue bandwidth command is used to show weighting of priority queues for bandwitdh sharing of WRR operation.
show queue mode command is used to show traffic scheduling mode for priority queues. One is Strict Priority (higher priority always get bandwidth service first), another is WRR (Weight Round Robin, bandwidth is shared between priority queues with weighting).
For example,
show queue bandwidth
Queue Scheduling
WRR Setting Table

Priority	Weight
Traffic Class 0	1
Traffic Class 1	2
Traffic Class 2	4
Traffic Class 3	8

show queue mode
Queue mode: Strict

20. show radius-server command

This command is used to show settings for RADIUS Server of 802.1x function.
For example,
show radius-server
[Redius Server Configuration Menu]
Redius Server IP Address : 192.168.1.222
Redius Server Port Number : 1812
Security Key : 87922019

21. show running-config command

This command is used to show current running configuration of the switch.
For example,
show running-config
!building running-config, please wait.....
!
calendar set 9 30 14 january 1 1970
! interface VLAN 1
IP address 192.168.1.1 255.255.255.0
!
SNTP server 220.130.158.54
!
……
……
! interface ethernet 1/10
port-vlan 1 Default_VLAN
!! !
End

22. show rate-limit command

This command is used to show rate limit settings.
For example,
#show rate-limit
Ingress Drop Mode: Enable
Rate Control Unit(Kbps): 128
[Rate Control Configuration]

Port	Ingress	Egress
1/1	No Limit	No Limit
1/2	No Limit	No Limit
1/3	No Limit	No Limit
1/4	No Limit	No Limit
1/5	No Limit	No Limit
1/6	No Limit	No Limit
1/7	No Limit	No Limit
1/8	No Limit	No Limit
1/9	No Limit	No Limit
1/10	No Limit	No Limit

23. show snmp command

This command is used to show SNMP configuration of the switch.

For example,

```
# show snmp
[SNMP Configuration]
Object ID : 1.3.6.1.4.1.x.60.10
System up Time: 597 (seconds)
System Name :
Location :
Contact name :
Get Community : public
Set Community : private
[Trap Community]
ID Status Community IP Address
1 Disabled public 0.0.0.0
2 Disabled public 0.0.0.0
3 Disabled public 0.0.0.0
4 Disabled public 0.0.0.0
5 Disabled public 0.0.0.0
Version: V3V2cV1
Username: admin
SnmpSecurityLevel: noauth
Authentication: MD5
```

Privacy: Des
24. show sntp command
This command is used to show system time settings of the switch.
For example,
show sntp
==========
[Time Configuration]
==========
Get Time By : Manually
Time Server : 220.130.158.54
Time Zone : Japan(+9)(37)
Current Time : 1970/01/01-09:29:45
D.S.T. status: Disable
D.S.T. start : 1st/SUN/JAN/0:00
D.S.T. end : 1st/SUN/JAN/0:00
==========
* D.S.T. Is Daylight Saving Time.

25. show spanning-tree command
This command is used to show spanning tree configuration of the switch.
show spanning-tree command is used to show all spanning tree configuration(for bridge and ports).
show spanning-tree ethernet 1/x command is used show spanning tree configuration of Port x. ("x" is the port number.)
For example,
show spanning-tree ethernet 1/5
Bridge Port Number: 5
Port Priority (0..255): 128
Port State: Linked Down
Port Enable : Enabled
Is edge : No
Port Path Cost(1..65535): 19
Port Designated Root: 00:00:00:00:00:00 [0]
Port Designated Cost: 0
Port Designated Bridge: 00:00:00:00:00:00 [0]
Designated Port: 5: [128]

Port Forward Transitions: 0
Port Role: Nonstp
Point To Point: Yes

26. show system command

This command is used to show general system information/configuration of the switch.
For example,
show system
System Configuration
Main Board Information:
Firmware Version: 1.12.14
Mac Address: 00:11:29:33:44:45
Number of Ports: 10
1Q VLAN Max. Group: 1024
DHCP Client: Disable
Time Server: Disable
System Log Status: Enable
Remote Log: Disable
Web server: Enable
Web server port: 80
Web secure server: Disable
Web secure server port: 443

27. show trunk command

This command is used to show trunk configuration of the switch.
show trunk ?
configuration Show Trunk Configuration
all Shows all Trunking Group Configuration
group Shows Each Trunking Group Configuration

show trunk configuration command is used to show trunk function enable/disable setting.
show trunk all command is used to show port member settings of all trunk groups.
show trunk group x command is used to show port member settings of

Trunk
Group x. (“x” is the trunk group index.)

28. show version command

This command is used to show system version information and model information.
For example,
show version
Firmware Version: 1.05.00
Number of Ports: 24
Model Name: CL-SWG-XXXX-SFP SNMP Management

29. show vlan command

This command is used to show VLAN configuration of the switch.
show vlan ?

private-vlan	Private VLAN
id	VLAN interface
name	VLAN interface name
port-based	Port-Based Virtual LAN Configuration
<cr>	

show vlan command is used to show all 802.1Q VLAN settings (enable/disable, VLAN ID, VLAN Name, VLAN Type, and Assigned ports).
show vlan id x command is used to show VLAN setting of VLAN x. (“x” is the VLAN ID).
show vlan name yyy command is used to show VLAN setting of VLAN yyy. (“yyy” is the VLAN name).
For example,
70
show vlan id 100
Vlan ID: 100
VLAN Type: Static
Name: P100
Ports/Port channel: Eth1/ 1(s) Eth1/ 2(s) Eth1/ 3(s) Eth1/ 4(s)
show vlan name P100
Vlan ID: 100

VLAN Type: Static
Name: P100
Ports/Port channel: Eth1/ 1(s) Eth1/ 2(s) Eth1/ 3(s) Eth1/ 4(s)
show vlan private-vlan command is used to show Private VLAN settings.
For example,
show vlan private-vlan
[Private VLAN Port Configuration]

Port#	PortType	Primary VLAN	Community VLAN	Isolated VLAN
Eth 1/ 1	Normal	none	none	none
Eth 1/ 2	Normal	none	none	none
Eth 1/ 3	Normal	none	none	none
Eth 1/ 4	Normal	none	none	none
Eth 1/ 4	Normal	none	none	none
Eth 1/ 6	Normal	none	none	none
Eth 1/ 7	Normal	none	none	none
Eth 1/ 8	Normal	none	none	none
Eth 1/ 9	Normal	none	none	none
Eth 1/10	Normal	none	none	none

show vlan port-based command is used to show Port-based VLAN configuration.
For example,
show vlan port-based
[Port-based VLAN Configuration]
Port-based VLAN : Disabled

[VLAN]	[Port List]
[1]	1 2 3 4 5 6 7 8 9 10

6.3 About Telnet and SNMP Management Interfaces

6.3.1 About Telnet Management Interface

If you want to use Telnet to manage the switch from remote site, you have to set the IP/NetMask/Gateway address to the switch first from console. Then use "telnet <IP>" command to connect to the switch. Its operation interface is the same as console interface.

6.3.2 About SNMP Management Interface

If you want to use NMS to management the switch from remote site, you have to set the IP/NetMask/Gateway address to the switch and configure the SNMP setting of the switch from console first. Then you can use SNMP management program to manage this switch.

This switch supports SNMP v1, v2c, v3 agent function and MIB II(Interface), Bridge MIB, 802.1Q MIB and Private MIB. The default GET community name is “public” and SET community name is “private”.

This switch supports up to five trap receivers with different trap community names.

6.4 Management with Http Connection

Users can manage the switch with Http Web Browser connection. The default IP setting is **192.168.1.1** and NetMask 255.255.255.0. The default IP Gateway is **192.168.1.254**. Before http connection, IP address configuration of the switch could be changed first.

1 Please follow the instruction in Section 6.2 to complete the console connection.
2 Login in with "super" (password is also "oem_super" by default.)
3 Use "show ip interface" command to check IP address of the switch first.
4 If IP address needs to be changed, follow the steps ...
4.1 Enter "config" command, and the prompt will become "(config)#".
4.2 Enter "interface vlan 1" command, and the prompt will become "(config-if)#".
4.3 Enter "ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy" command (xxx.xxx.xxx.xxx is the IP address and yyy.yyy.yyy.yyy is the netmask) to modify IP address of the switch.
4.4 Enter "exit" command to go back to "(config)#" prompt.
4.5 If IP Gateway will be set, enter "ip default-gateway xxx.xxx.xxx.xxx" command to set the IP gateway of the switch. (xxx.xxx.xxx.xxx is the IP address.)
4.6 Enter "exit" command to go back to "#" prompt.
4.7 Enter "show ip interface" to check the IP settings.
4.8 Enter "show ip redirects" to check IP gateway setting.

After IP address configuration done and the switch is connected to network, users can start Http connection by entering IP address of the switch to the web address line in Web Browser. A login screen will be prompted for user name and password. The default user name and password is "super" / "oem_super". Then the management homepage will appear.

Left part of the homepage is a function list. Users can select one of them for status monitoring or switch configuration.

Upper part of the homepage is the link status of the switch. Three different colors are used to show different status of ports – Link Up, Link Down and Port Disable.

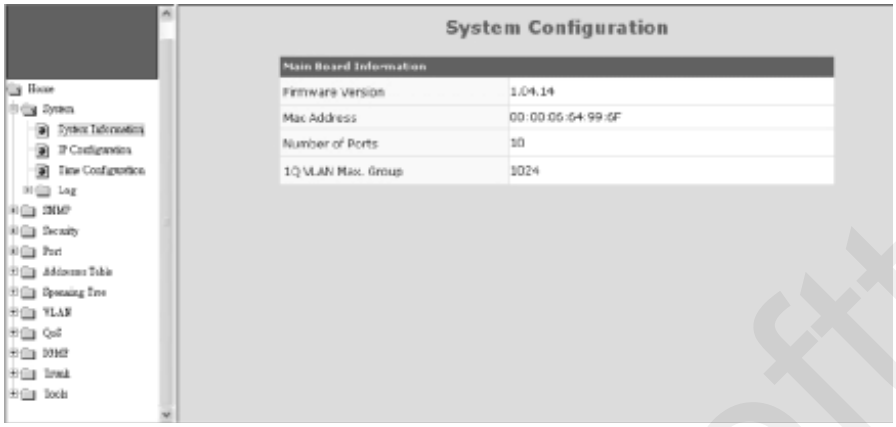
Middle part of homepage is the main operation area for each function.

The details about management with http connection will be shown in the following sub-sections.

6.4.1 System

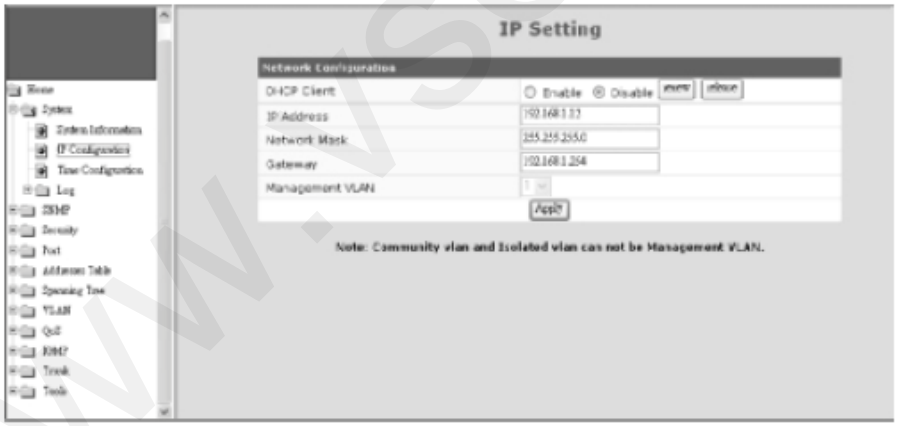
"System Information" is the homepage of the switch. And there are four sub-functions for it.

1). System Information



This function lists the system information about the switch. You can find the firmware version, Mac address, connection port number, and maximum VLAN group number here.

2). IP Configuration



This function is used to setup IP configuration of the switch.
You can enable DHCP client function to get IP configuration from DHCP server automatically. Or, disable DHCP client function and set IP configuration

manually.

Management VLAN : This is used to setup the VLAN ID for remote

management interface of the switch. Only users in the same VLAN can manage the switch remotely. For example, setting it to "5" will allow users in the VLAN with VLAN ID 5 to manage the switch remotely. It works only 802.1Q VLAN function is enable.

About DHCP Client [renew] and [release] button ...
[renew] button: If DHCP client function is enabled, you can click [renew] button to refresh the lease time of the IP address. If IP configuration is not got when boot-up, clicking [renew] button will try to get IP configuration again.
[release] button: If DHCP client function is enabled and IP configuration is got, clicking [release] button will release current IP configuration. After that, you can click [renew] button to get the IP configuration again.

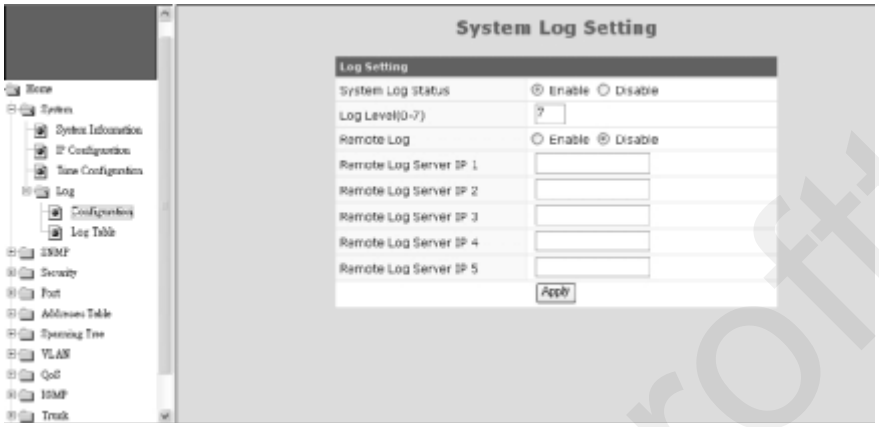
3). Time Configuration

There are two ways to get the system time.
a). Get time from Time Server
This switch support NTP protocol to get time from Internet time server. For such application, you have to select Get Time by "Time Server", input the IP of Time Server, and select the Time Zone of your location. Then click [Apply]
If time is got from Time Server, it will be shown at "Current Time".
For such application, you have to get the IP of Time Server from your network administrator first.
b). Set time manually
This switch can count time internal. You can select Get Time by "Manually", and input current time manually. Then click [Apply].
About [Daylight Saving Time] ...

Daylight Saving Time function will set the system time one-hour early than normal time in a period oftime. [Start Time] and [EndTime] can be used to set the time period.

4). Log

[Configuration]



Users can configure System Log function and view log records here. If this function is enabled, the switch will record events to a log file and put the log file to flash.

Up to 512 records are allowed for local logging. If more than 512 events happen, the records will be overwritten from beginning. And if remote syslog server is applied, the switch will also send event record to the syslog server.

About log function configuration ...

System Log Status : This can enable/disable system logging function.

Log Level (0~7) : Log levels 0~7 are defined as below. And events with lower log level than this number will be recorded.

Level	Name	Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant condition
6	Informational	Informational messages

7	Debug	Debug-level messages

Remote Log : This can enable/disable remote syslog function.
Remote Log Server IP : This is the syslog server IP for remote logging. Up to five syslog servers is supported. Event logs will be sent to those syslog servers at the same time.
[Log Table]

You can view log content here.
There could be more than one page. You may change the page or go to a page by its operation icons.
Clicking [clear log] button will clear the local log table.

6.4.2 SNMP

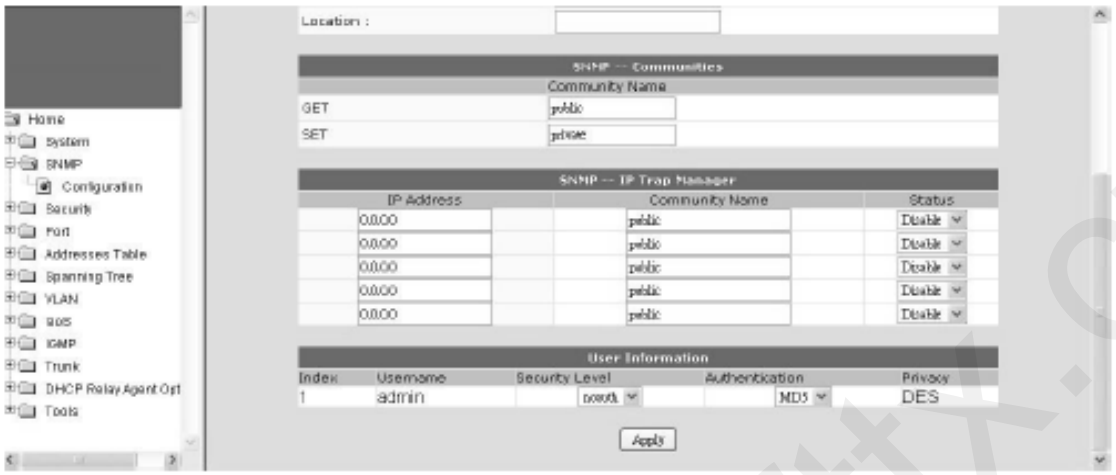
This function is used to configure SNMP function of the switch. This switch supports SNMP v1, v2c, and v3 agent function and MIB II(Interface), Bridge MIB, 802.1Q MIB and Private MIB.

[System Information]

Object ID: this is the SNMP Object ID of the switch for SNMP management.
Up Time: this is the power-up running time of the switch.
Version: this is used to select SNMP agent operation version.
Name: this the host name of the switch.
Contact: this is the contact information for the switch.
Location: this is the location information of the switch.

[SNMP -- Communities]

Get: this is the community string of GET command for SNMP operation. GET command is used to read switch configuration/information.
Set: this is the community string of SET command for SNMP operation. SET command is used to set switch configuration.



[SNMP — IP Trap Manager]

Trap function will send notice message to SNMP management station when some events happen. Up to five SNMP management stations are supported for Trap function.

The community string and enable/disable setting for each trap are set here.

[User Information]

This is used to configure SNMPv3 administrator settings. The default user name is “admin”. The security level and authentication manner could be configured here. The default encryption for privacy is by DES.

The security level could be ...

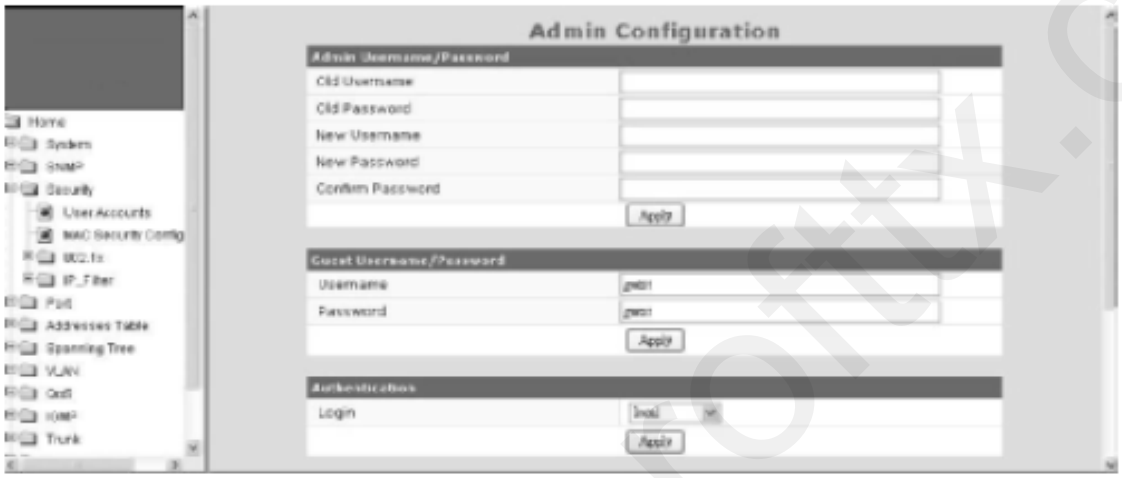
- noauth : no authentication, no encryption
- auth : do authentication, no encryption
- priv : do authentication and encryption(by DES)

The authentication manner could be MD5 or SHA.

6.4.3 Security

This function is used to configure security functions of the switch. Those security functions are Administrator Management Security, Mac ID Access Security, and 802.1x Authentication Security.

1). User Accounts (Administrator Management Security)



Administrator Username/Password : This is for network administrator to change his/her username and password. (Default is super/oem_super.)

Guest Username/Password : This is used to setup the username/password of guest-right user who just can view the setting of the switch.

Authentication : This is used to setup the authentication manner for administrator of the switch when login by http(s)/telnet for management. It could be authenticated by local switch or by RADIUS Server.

- local: authenticated by local switch
- radius: authenticated by RADIUS Server
- local, radius: authenticated by local switch first. If authentication fail, try by RADIUS Server next

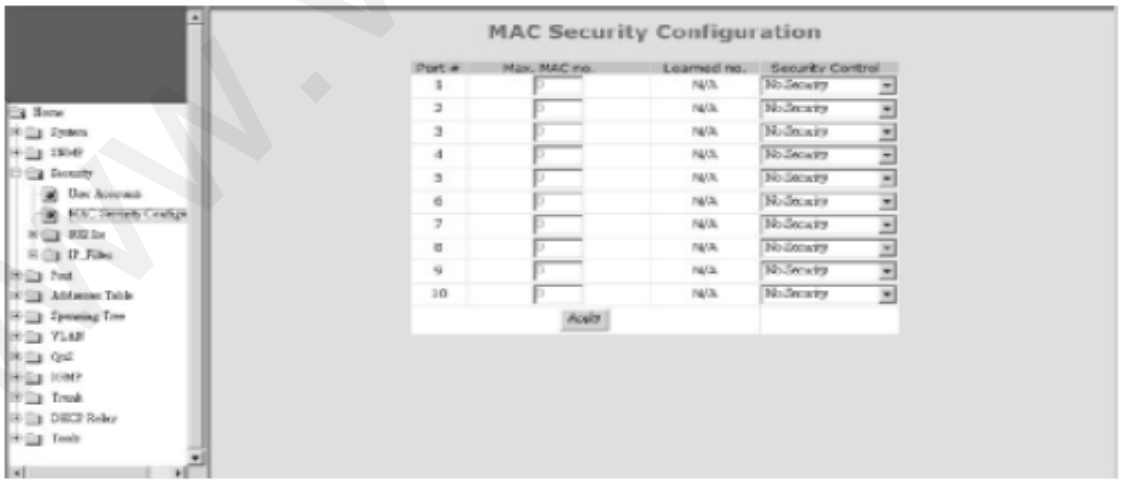
RADIUS Server is set in 802.1x function.

[Security Policy]

This is used to setup the IP addresses that can manage this switch. They have different access rights set in "Mode". And the remote management interfaces (Http/Telnet/SNMP) could be enable/disable for different administrators. This function is for security policy of switch management.

Note: Remember to enable at least one IP/Subnet with Modify right for Http/ Telnet/SNMP interface. Otherwise, configuring switch from remote will become impossible. In that case, you can manage the switch from console only.

2). Mac Security Configuration



There are two Mac ID security modes for the switch. One is Static Mac ID Filter on Port, another is Dynamic Mac ID Number Limit on Port.

[Static Mac ID Filter on Port]

This function can limit only those static Mac addresses on the port can access network. Other Mac addresses will be rejected by the port. Sometimes it is called "Mac-Port Binding".

Follow the steps to configure it.

a. Set the "Security Control" to "Accept" on those ports that will apply static Mac ID security. Then click [Apply].

b. Set Static Mac Addresses that are allowed for network access at [Static Address] of [Address Table] function. Please refer to that section for the details.

[Dynamic Mac ID Number Limit on Port]

This function can limit the Mac ID number to access network through a port. For example, five Mac ID are allowed for Port 2. That means up to five users are allowed, but don't care who the users are.

Follow the steps to configure it.

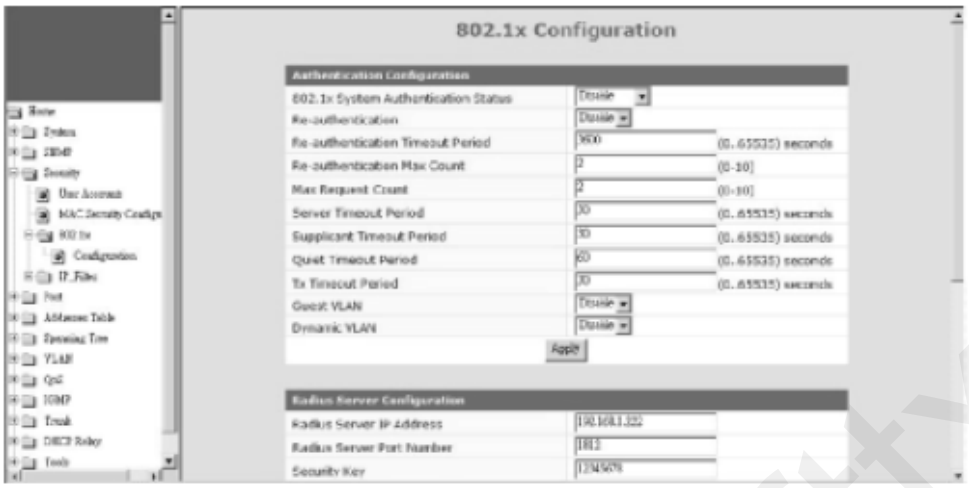
a. Set the "Security Control" to "Limited by MAC no." on those ports that will apply dynamic Mac ID number security. And set the "Max. MAC no." to the users number allowed on the ports.

b. Then click [Apply].

The switch will learn users automatically and show current user number at "Learned no.".

3). 802.1x Configuration

If 802.1x function is enabled, the switch will act as an authenticator for users accessing network through the switch. It needs a RADIUS server for the authentication function. Users will be asked for username and password before network access. If the RADIUS server authenticates it, the switch will enable the port for network access. This function is very useful for network security application to prevent illegal users access network through the switch.



The function here is for 802.1x function configuration.

1. 802.1x Authentication Status: [Enable/Disable/Transparent]

Enable: enable 802.1x function in authentication mode

Disable: disable 802.1x function

Transparent: only forwarding 802.1x packets

2. Re-authentication (enable/disable), Timeout Period and Max Count:

The re-authentication function will re-authenticate users after the timeout period. The Max Count is the maximum re-try count between the switch and users before authentication fail.

3. Max Request Count and Server Timeout Period:

The Server Timeout Period is the timeout period for the request between the switch and RADIUS server.

The Max Request Count is the maximum re-try count between the switch and RADIUS server before authentication fail.

4. Supplicant Timeout Period:

This is the timeout value between the switch and users (called "supplicant" in 802.1x) after first identification. The valid value is 0~65535.

5. Quiet Timeout Period:

This is the quiet timeout value between the switch and user before next authentication process when authentication fails.

6. Tx Timeout Period:

This is the timeout value for the identification request from the switch to users. The request will be re-tried until the Re-authentication Max Count is met. After that, authentication fail message will be sent. The valid value

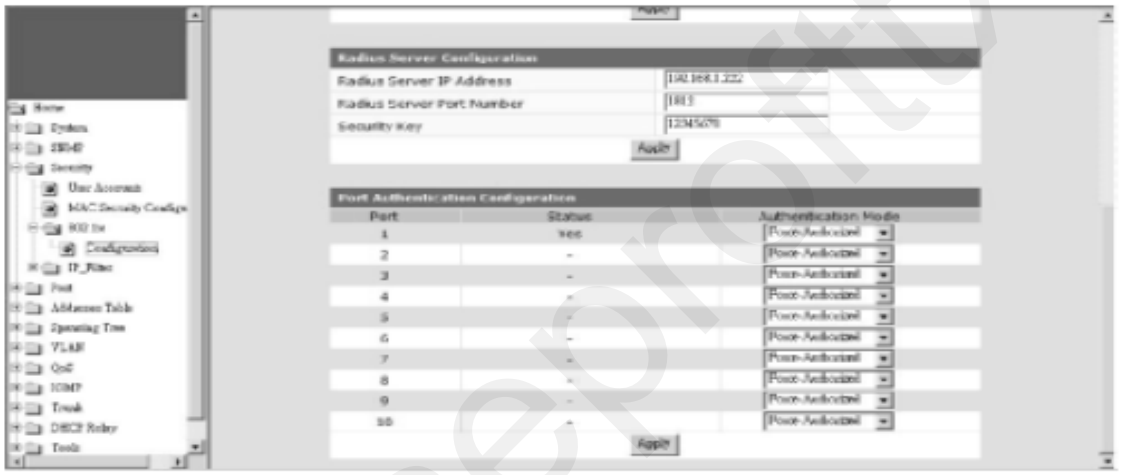
is 0~65535.

7. Guest VLAN:

This function will put those users who are authenticated fail in 802.1x operation to a "Guest VLAN". The Guest VLAN could be selected here.

8. Dynamic VLAN:

This function will assign user to a VLAN that are indicated by RADIUS Server when 802.1x authentication is pass. That is, VLAN for users are assigned from RADIUS Server.



[Radius Server Configuration]

This function is for the configuration between switch and RADIUS server. You can assign the IP address of Radius Server, the protocol port number, and the security key.

[Port Authentication Configuration]

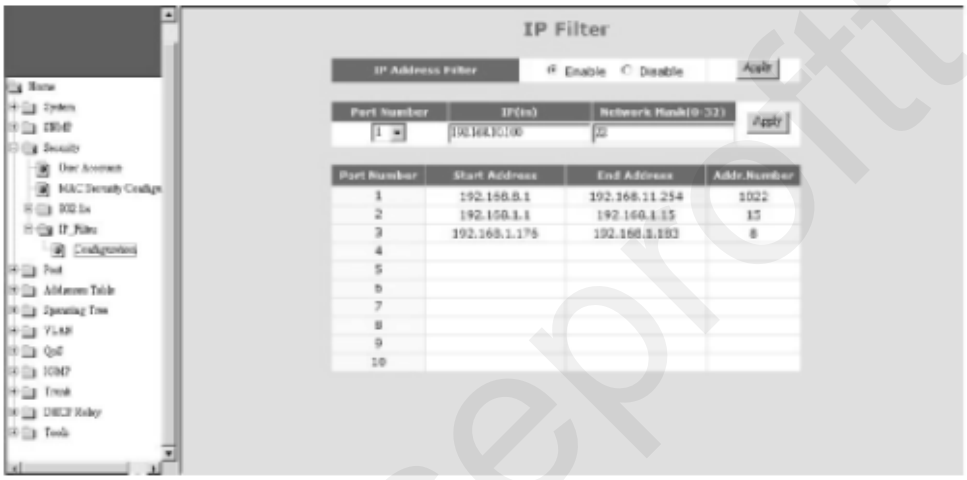
The Port Authentication Configuration is used to select the authentication mode for each port of the switch.

1. Auto: This is the normal 802.1x operation mode. The authentication status (authenticated or unauthenticated) depends on the authentication result of port.
2. Force-Authorized: This mode will force the port always being authentication successful in 802.1x process and the real authentication result will be ignored.
3. Force-Unauthorized: This mode will force the port always being authentication fail in 802.1x process and the real authentication result will be

ignored.
4. None: This mode will disable 802.1x operation on this port.
And you can see current 802.1x status on each port.

4). IP Filter Configuration

This function is used to configure IP Filtering function of port. An IP address with a subnet mask can be defined for each port. If this function is enabled, only devices with IP address in the subnet can access network through the port.

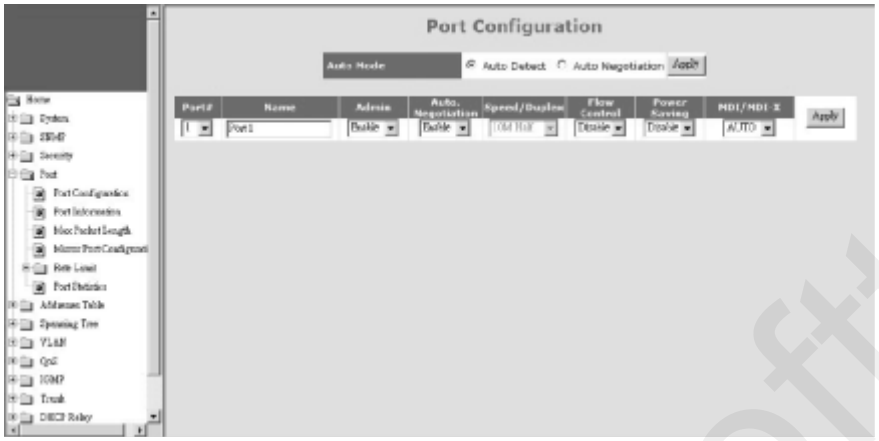


Because it is a subnet specified by IP address/Network ID Number(0~32, or called Subnet Mask), the start IP address, end IP address and allowed IP address number are shown in the table.
If some specified IP address will be assigned, set the Subnet Mask as 32. For example, 192.168.1.82/32.

6.4.4 Port

This section is about configurations for ports. For port speed setting, maximum packet size setting, mirror port setting, port bandwidth limit, and port statistics.

1). Port Configuration



This function is used to configure port settings of the switch. You can enable /disable a port, set it to fixed 10M or 100M or 1000M ... and so on.

Auto Mode : User can select the operation mode of port when "auto" is set to disabled.

For "Auto Negotiation" mode, the switch will do port auto-negotiation function ON/OFF when the auto function of port (in Port Configuration setting) is enabled/disabled.

For "Auto Detect" mode, the switch will always keep port auto-negotiation function

ON but just modify its attribution if auto function of port (in Port Configuration setting) is disabled.

For applications, you should select "Auto Detect"mode if the connected device is auto-negotiation enabled. (For example, customer's PC is auto-negotiation enable and you want to set his network connection to work at 10Mbps.)

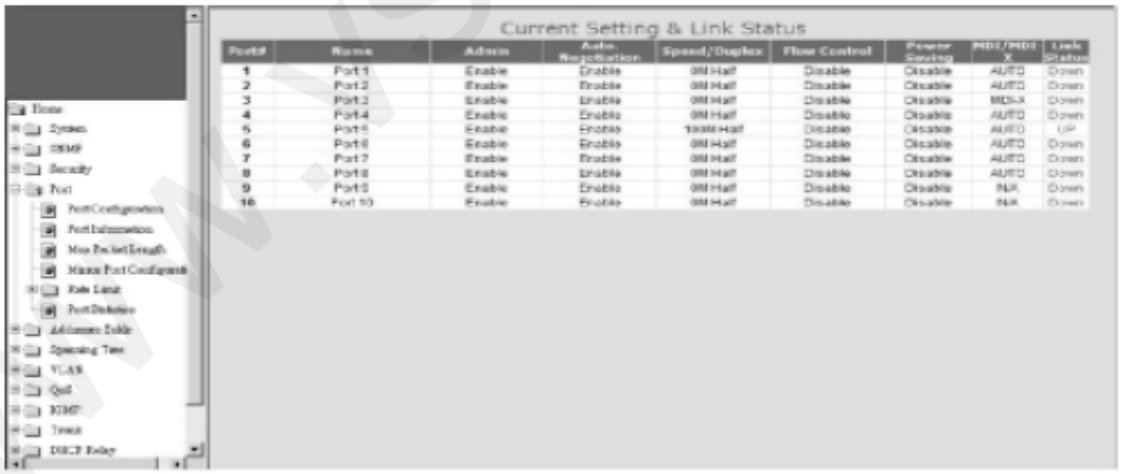
And you can select "Auto Negotiation"mode if the connected device is auto-negotiation disabled (it is called forced mode, sometimes). Some of old TX-FX Converters needs to work in this mode because FX supports 100/Full forced mode only.

For most applications, "Auto Detect" mode is OK.

Port Setting : It is for modifying the setting of port. Follow the steps to do it.

1. Select the port that you want to modify in "Port#" first.
2. Fill the name of the port.
3. Select Enable/Disable state in "Admin". If Disable is selected, this port will be disabled for any network access.
4. Select the Enable/Disable state of Auto function of port. The auto mode could be auto-negotiation or auto-detect operation when auto is set to disable.
5. If Auto is disabled, select the operation speed and duplex mode of the port in "Speed/Duplex" .
6. Select the Enable/Disable state of Flow Control function of port.
7. Select the Enable/Disable state of Power Saving function of port. If it is enabled, port will go to low power state when link down.
8. Select MDI/MDI-X operation mode. It could be "Auto", "MDI", or "MDI-X". "Auto" can auto-detect and get the correct connection mode. "MDI" will set the port to MDI mode for switch-to-switch connection. "MDI-X" will set the port to MDI-X mode for user PC connection.
9. Click [Apply] after any modification.

2). Port Information



Current Setting & Link Status : It is current status of ports.

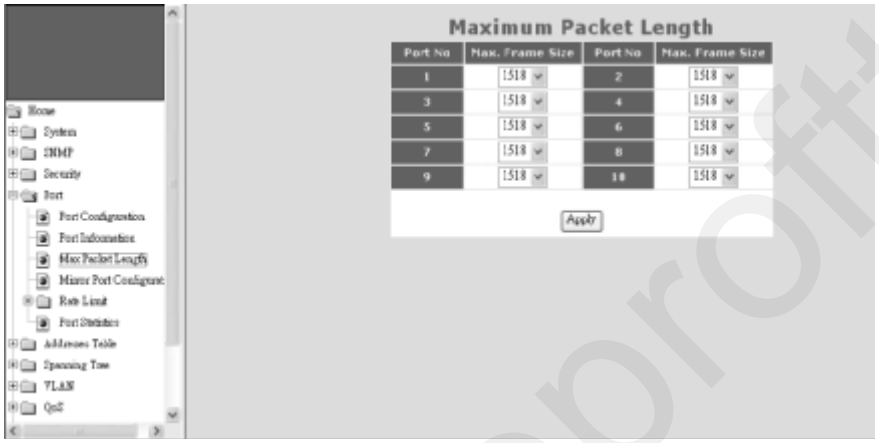
Name: The name of the port.

Admin: It shows current port enable/disable status.

Auto: It shows current Auto enable/disable status of ports.

Speed/Duplex: It shows current working speed and duplex mode if ports are link up. Or the setting of speed/duplex when auto is disable.
Flow Control: It shows current Flow Control function status of ports.
Power Saving: It shows current Power Saving enable/disable status of ports.
MDI/MDI-X: It shows current MDI/MDI-X setting of ports.
Link: It shows the link status of each port.

3). Max Packet Length



This switch supports Jumbo Frame function. And the maximum packet size could be up to 9600 byte/packet. You can select the maximum packet size for each port here.

4). Mirror Port Configuration

This switch operates in store-and-forward algorithm so it is not possible to monitor network traffic from another connection port. But the port mirror function can copy packets from some monitored port to another port for network monitor.

Mode: This is used to enable/disable Mirror function.
Monitering Port: This is used to set the capture port. The switch will copy the traffic from Monitored Port to this port if Mirror function is enabled.
Monitored Port: This is the monitored port. The switch will copy the traffic from this port to Monitoring Port.

5). Rate Control

Two traffic rates could be controlled by the switch. One is the ingress/egress traffic of each port. Another is Broadcast/Multicast/Unicast Storm Control.

5-1) Rate Control Configuration
This function can setup the ingress and egress rate limit of ports.

Follow the steps to configure ...

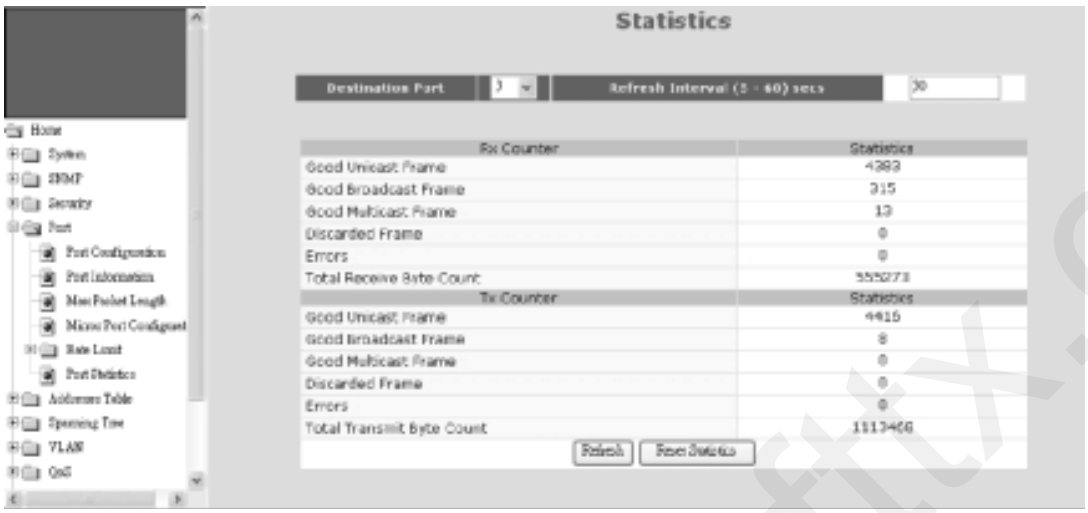
a. Set “Unit” first. It could be selected from pre-defined units, or define by user. Click [Apply] after the setting.
b. Select the Port Number.
c. Enter the rate limit level for Ingress and Egress traffics. “0” means NO LIMIT. Click [Apply] after the setting.
About “Packet Drop for Ingress Limit” function ...
When Ingress traffic rate exceeds Ingress Rate Limit, the switch can drop packets
or pause the traffic. If packet drop is enabled, flow control of ports will be disabled and packets could be dropped. If packet drop is disabled, flow control of ports will be enabled and pause frame will be sent when ingress traffic rate exceeds the limit.

5-2) Storm Control Configuration

This function can setup the broadcast, multicast, and unicast storm rate of the switch.

Please follow the rules in table to setup the maximum storm rates.
Note: The storm rate is counted by pps (packet per second).

6). Port Statistics



Port statistics counters could be read here.

Select a port to get its counters.

[Refresh]

The counters will be refreshed automatically. You can modify the refresh interval.

And you can click [Refresh] to refresh the counters immediatelly.

[Reset Counters]

Click [Reset Statistics] can reset the counters to "0".

6.4.5 Address Table

These are functions about Mac address table. They are "Static Address Assign", "Dynamic Address Table", and "Aging Time Setup".

1). Static Addresses

This switch supports static Mac address assignment. You can assign static Mac addresses by the following steps ...

a. Give an Entry ID. This ID is used as the index of the entry in Static Addr ess Table.
b. Give the VLAN ID. If 802.1Q is disable, the VID will always be 1. This VID will put the static Mac address in some VLAN for 802.1Q VLAN operation.
c. Fill the Mac address. This is the Static Mac Address for this entry.
d. Select the port for this Static Address.
e. Click [Confirm Add/Change] button.
Then this entry will be added to the table.
In "Current Static Address Setting" table, you can edit and delete an entry. (Different Mac Address will be another entry. Mac Address is not allowed to edit for an entry.)

The switch will not age out these static Mac addresses. But there is a limitation for these static Mac addresses - they are allowed to work on the assigned port only because they are static fixed on the assigned port.
If you want to delete an entry in the static Mac address table, click [Delete] button of the entry and the static Mac address will be removed from the table.
If you want to modify an entry, click [Edit] button of the entry. Do the modification and click [Confirm Add/Change] button. (Different Mac Address will be another entry. Mac Address is not allowed to edit for an entry.)
About Port Security function . . .

You can configure "Mac Security Configuration" function (in "Security" page) for port access security with Mac address. Select "Accept" for such security application..

2). Dynamic Addresses

This function can show the dynamic Mac addresses learned by the switch. This table will refresh every 30 seconds.
The address table could be more than one page. You can click [Previous Page], [Next Page] to change page. Or, give the page number directly.
Query function is supported by the switch. It could be queried by Port or queried
by Mac Address. Select the query function and input the query target. Then click [Query]. The result will be shown.
For example,

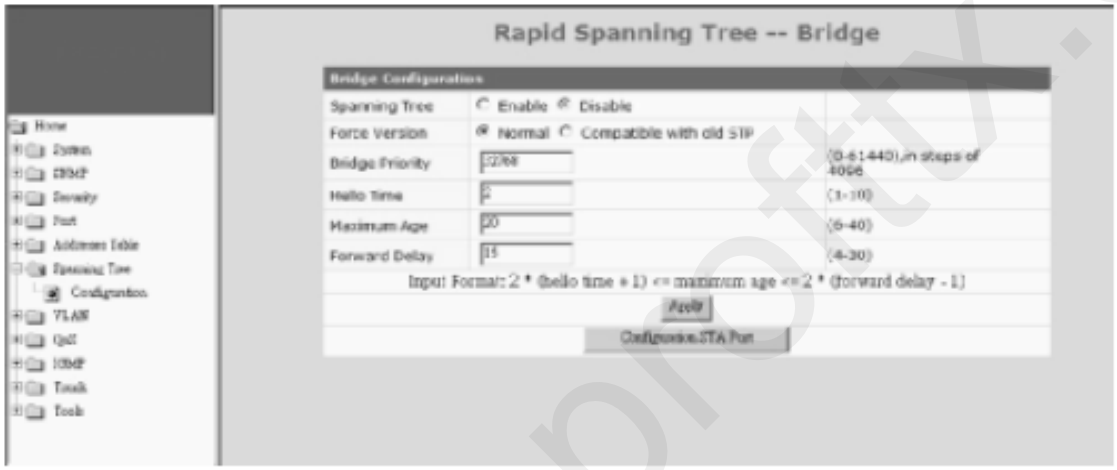
3). Address Aging

The switch will learn Mac addresses to an ARL table automatically. And follow the table to do packet forwarding operation. If Mac addresses are not received for some time, the Mac addresses will be removed from the table. This operation is called aging.
The aging operation could be disable here. And all the learned Mac addresses will not be removed from the ARL table.
The time interval for aging operation could be modified here. It is 300 seconds by default.

6.4.6 Spanning Tree

Spanning Tree Protocol can prevent traffic looping in network. It can be configured for switch unit (bridge) and port unit. If spanning tree function is enabled, any link down to link up will have several seconds delay for the port going to forwarding state.

[Setting of Bridge]



Here are the parameters for Spanning Tree operation on the switch.

Enable / Disable : enable/disable spanning tree operation

Force Version : It will operate as Rapid Spanning Tree in "Normal" state. And it can be forced to operate at old Spanning Tree mode if "Compatible with old STP"is selected.

Bridge Priority (0~61440) : Bridge priority is for selecting the root device, root port, and designated port. The device with the highest priority (lowest value) becomes the STA root device. If all devices have the same priority, the device with the lowest MAC address will then become the root device.

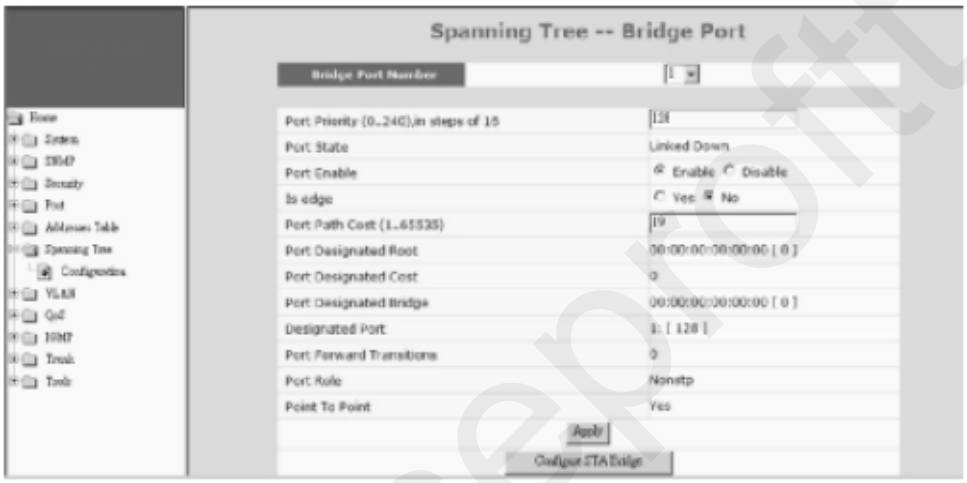
Hello Time (1~10) : the period to send the spanning tree maintenance packet if the switch is the root of the spanning tree. Default is 2 seconds.

Maximum Age (6~40) : the spanning tree aging time if no spanning tree maintenance packet is received. It will cause the spanning tree to re-create. Default is 20 seconds.

Forward Delay (4~30): the maximum waiting time before changing states (i.e., learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames.

In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.
The parameters have relation with each other. And here is the rule for it.
2*(Hello Time +1) is less or equal to Maximum Age, and Maximum Age is less or equal to 2*(Forward Delay -1).

[Setting of Port]
Click [Configuration STA Port]. You can configure RSTP/STP on ports.

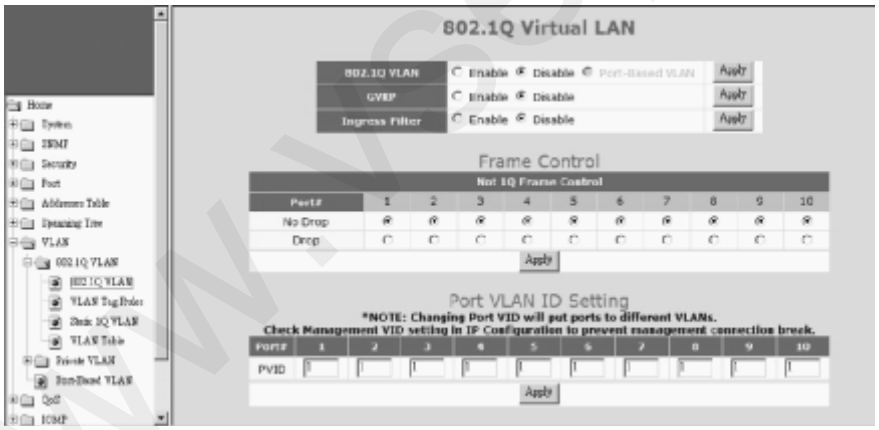


Bridge Port Number is the Ethernet port that will be configured.
Port Priority (0~240) : If the path cost for all ports on a switch are the same, the port with the highest priority (lowest value) will be forwarded when looping happens. If more than one port have the same highest priority, the port with lowest port number will be forwarded.
Port State : It is current spanning tree operation state of the port.
Port Enable : enable/disable spanning tree function on the port.
Is edge : If this switch is at "edge" of the network tree, please select "Yes". If there are another switches connected, please select "No". This parameter is used by RSTP to increase its operation speed.
Port Path Cost (1~65535) : It is used to determine the best path between devices if looping happens. Lower values will be forwarded and should be assigned to ports with high speed connections. Higher values will be blocked and should be assigned to ports with low speed connections. The suggestion values are 100(50~600) for 10M, 19(10~60) for 100M and 4(3~10) for 1000M connections.

Port Designated Root : This shows the root bridge ID of this segment and its bridge priority.
Port Designated Cost : This shows the path cost between the root port and the designated port of the root bridge.
Port Designated Bridge : This shows the switch's bridge ID and its bridge priority setting.
Designated Port : This shows the port number and its port priority..
Port Forward Transitions : This is the forwarding transition counter on the port.
Port Role : It is the role of the port for the STP operation. It could be Root, Designated, Backup, or Alternated. If the port is link down, the port role will be Nonstp.
Point To Point : This is a Point-to-Point link on the port.

6.4.7 VLAN

This switch supports 802.1Q VLAN, Port-based VLAN, and Private VLAN.
1). 802.1Q VLAN
1-1). 802.1Q VLAN

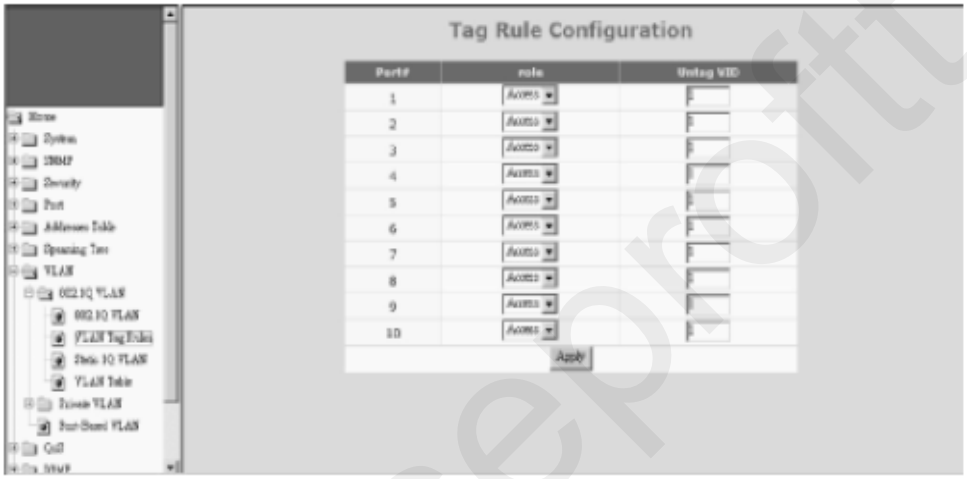


802.1Q VLAN : This is used to enable/disable 802.1Q VLAN function.
GVRP : The GVRP protocol can learn remote 802.1Q VLAN on other switches and add to dynamic 802.1Q VLAN table. You can enable/disable the operation of this protocol.
Ingress Filter : This is used to enable/disable doing VLAN filtering function at ingress port. If it is enable, the ingress port must be in the same VLAN for packet forwarding. If it is disable, VLAN filtering function will be done at egress port.

[Frame Control]
This function could be used to drop non-802.1Q frames (untagged packets).

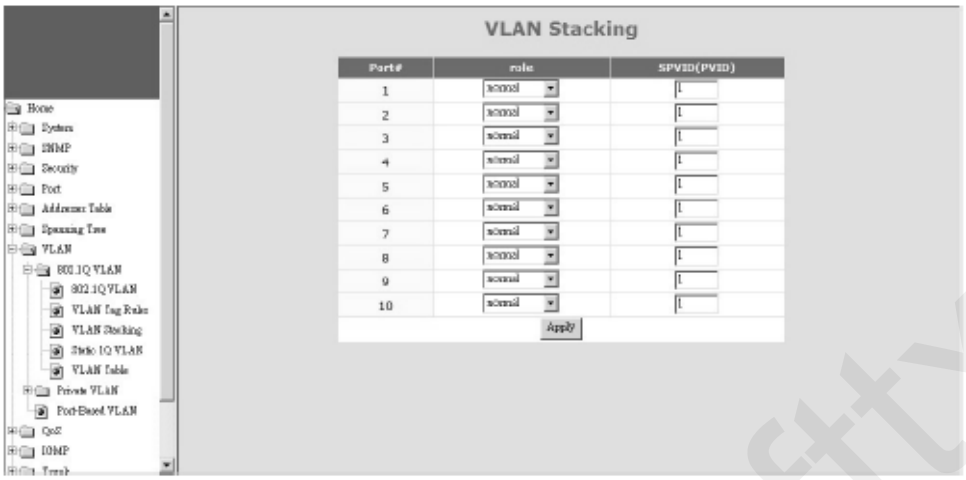
[Port VLAN ID Setting]
PVID is used to set Port VLAN ID. When untagged packet is received, PVID of the ingress port will be used as the its VLAN ID. PVID is also used as the VLAN ID for tag adding when untagged packet is translated to tagged packet.

1-2).VLAN Tag Rules



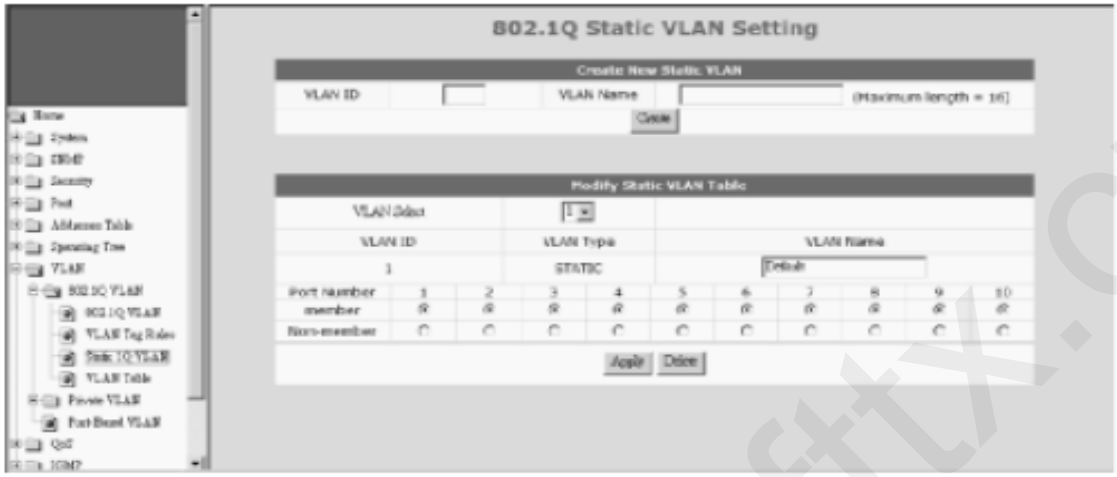
For 802.1Q VLAN, every port could be tag port or untag port.
Tag port will always send tagged packets and is used for switch-to-switch cascading. It is a VLAN trunk connection because there could be more than one VLAN working through it. And its role is a "Trunk" for 802.1Q VLAN groups operation between switches.
Untag port will always send untagged packets and is used for switch to users connection. And its role is a "Access" connection for users.
You can define ports as "Trunk" or "Access" according to their connection devices and your applications.
If a port is defined as "Hybrid", it is a tag port basically. But it will act as an untag port for packets working in VLAN defined in "Untag VID". So, it is called a hybrid port.
For example, set Port 5 as "Hybrid" and its Untag VID as 10. Port 5 will act as a tag port for all packets except packets for VLAN 10. Port 5 will act as an untag port for packets working for VLAN 10.

1-3). VLAN Stacking



VLAN Stacking function allows two VLAN tags in a packet for 802.1Q VLAN tunnelling application through a central network.
For VLAN Stacking operation, port role definition is needed for each port. There are three roles for a port - Normal, Tunnel, and Access.
Normal - It will set the port(s) as normal 802.1Q VLAN port(s). And the tagged/untagged setting will follow the settings in 802.1Q VLAN.
Access - It will set the port(s) as access port(s) for VLAN stacking operation. It will strip a tag from tagged or double-tagged packets before forwarding. It is for downward connection of VLAN stacking operation.
Tunnel - It will set the port as tunnel port for VLAN stacking operation. It will add a tag and allow two 802.1Q VLAN tags in a packet. It is for tunnel and upward connection of VLAN stacking operation.
SPVID is used as the Port VLAN ID of VLAN Stacking (L2 Tunnel) operation if the port role is "access".

1-4). Static 1Q VLAN



This function is used to maintain 802.1Q static VLAN.

Create an 802.1Q VLAN:

1. Input the VLAN ID and VLAN Name in "Create New Static VLAN". Click [Create] to create the VLAN. The valid VLAN ID is 1 ~ 4094.
2. Select the VLAN in "Modify Static VLAN Table". The new VLAN is empty by default. You can select ports for the VLAN. After that, click [Apply] to complete the VLAN configuration.

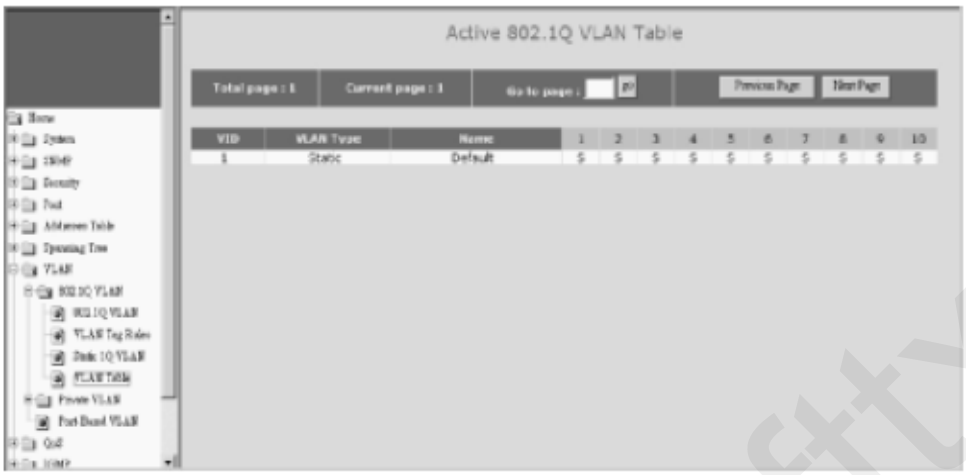
Modify an 802.1Q VLAN:

1. Select the VLAN in "Modify Static VLAN Table".
2. Modify its setting and click [Apply] to activate the new setting.

Delete an 802.1Q VLAN:

1. Select the VLAN in "Modify Static VLAN Table".
2. Click [Delete] to delete the 802.1Q VLAN.

1-5). VLAN Table

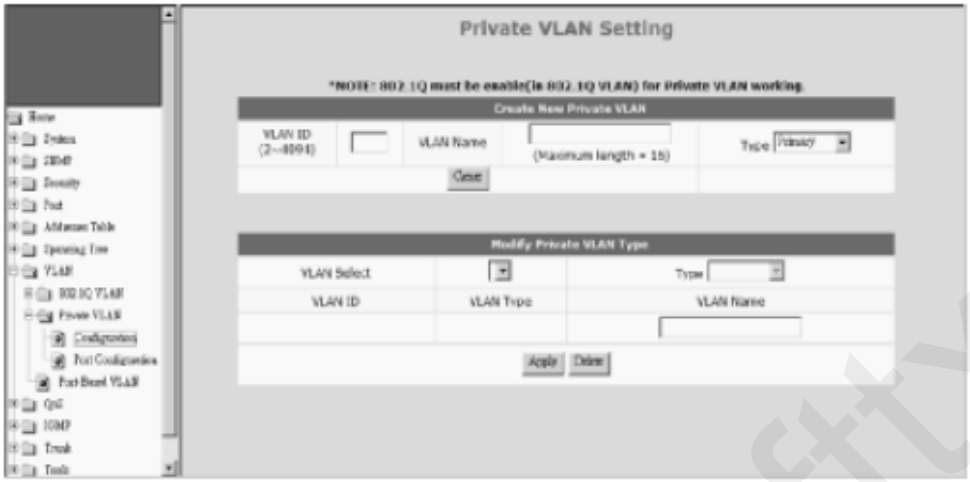


This table will show the activity of 802.1Q VLAN. Both static and dynamic 802.1Q VLAN will be shown in the table.
For ports, "S" means static member and "D" means dynamic member.
If GVRP protocol is enabled, this table will also show the learned remote 802.1Q VLAN.

2). Private VLAN

Three kinds of VLAN are defined for this application – Primary VLAN, Community
VLAN, and Isolated VLAN. Community VLAN and Isolated VLAN can communicate with Primary VLAN, but they cannot communicate with each other.
And users in Isolated VLAN cannot communicate with each other. This is a special 802.1Q VLAN configuration.

2-1). Configuration

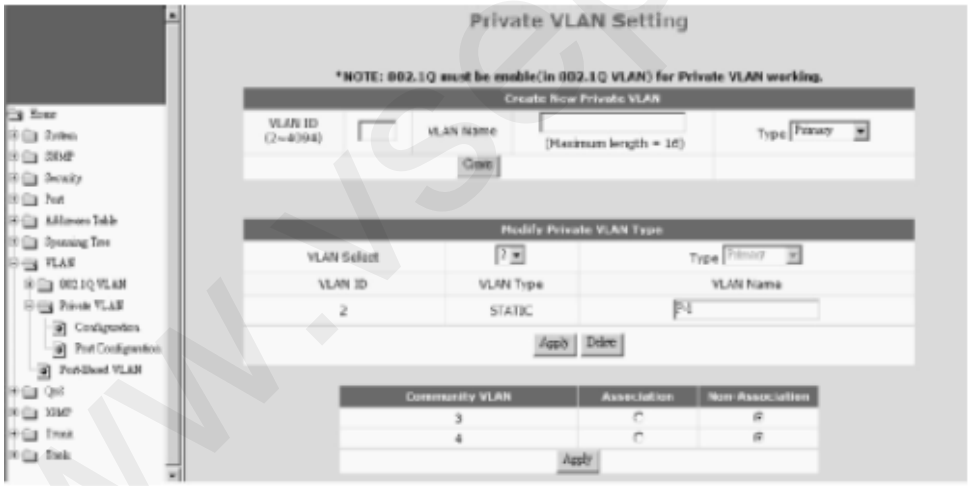


Creating Private VLAN, do the steps first.

a. Create VLAN groups, and define as "Primary", "Community", or "Isolated".

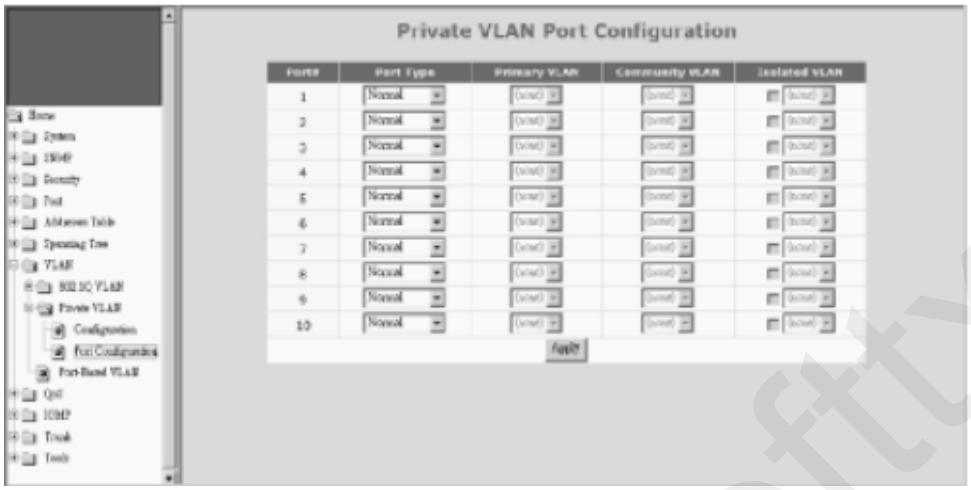
b. Associate Community VLAN with Primary VLAN. If more than one Primary VLAN, select Primary VLAN first and then do the association.

See the following picture.

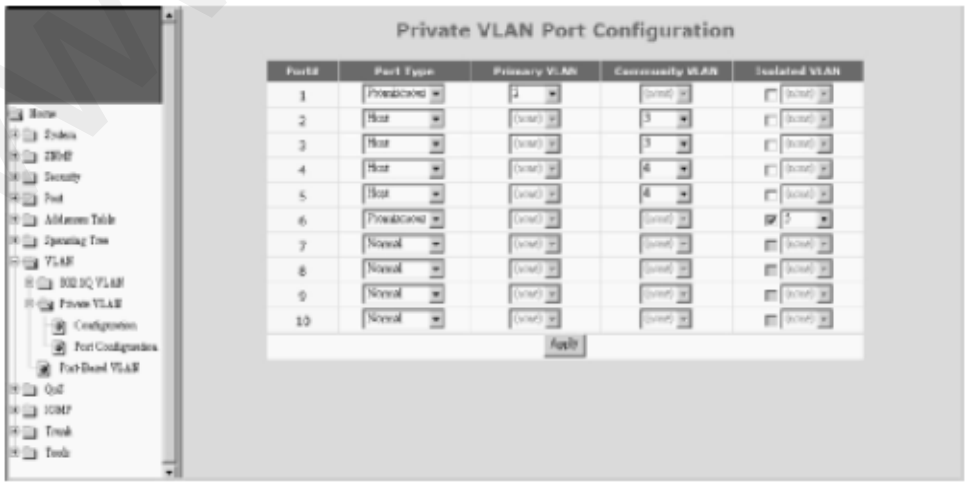


2-2). Port Configuration

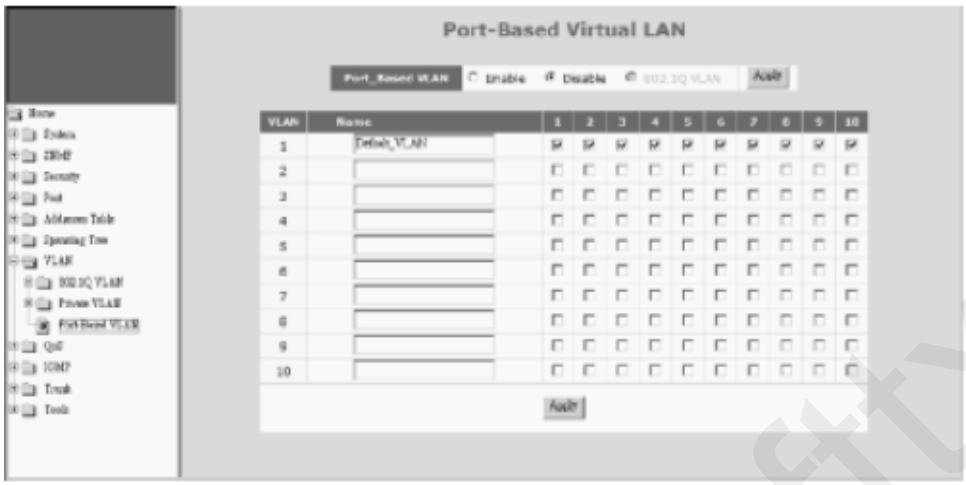
After VLANs are created, assign ports to VLANs.



There are three types for a port - Normal, Host, and Promiscuous.
"Normal" is for ports doing normal 802.1Q operation instead of Private VLAN.
"Host" is for ports that could be in Community VLAN or Isolated VLAN.
"Promiscuous" is for ports that could be in Primary VLAN or Isolated VLAN.
Follow the steps to do the port assignment.
a. Select the type for a port.
b. If it is "Host", you can select a VLAN from Community VLAN or mark Isolated VLAN and select from it. (Community VLAN must be associated first.)
c. If it is "Promiscuous", you can select a VLAN from Primary VLAN or mark Isolated VLAN and select from it.
d. Repeat a.~c. to complete the port assigment.
e. Click [Apply].
Please see the following picture.



3). Port-based VLAN



Follow the steps to configure Port-based VLAN.

a. Enable Port-based VLAN. And click [Apply] button.

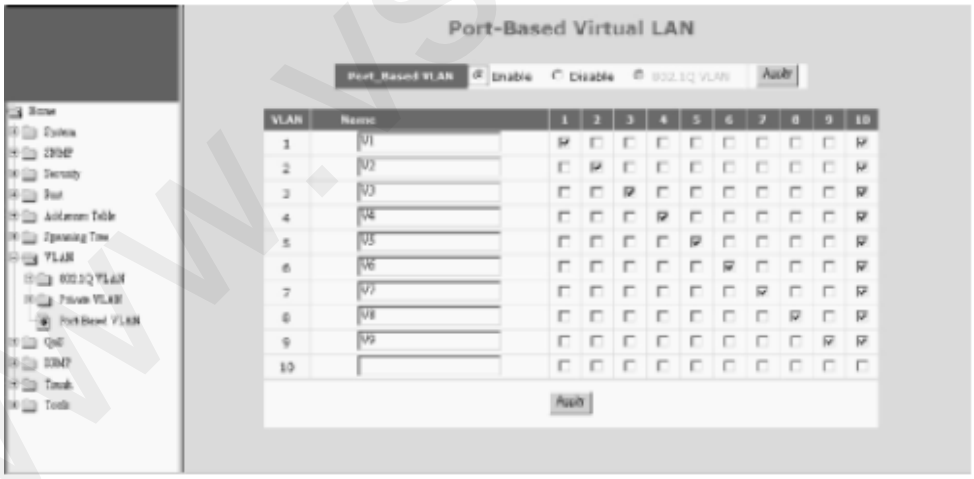
b. Give VLAN name.

c. Select ports for each VLAN.

d. Click [Apply] button.

Note: About Concentration VLAN

This is a very popular application for VLAN setting.

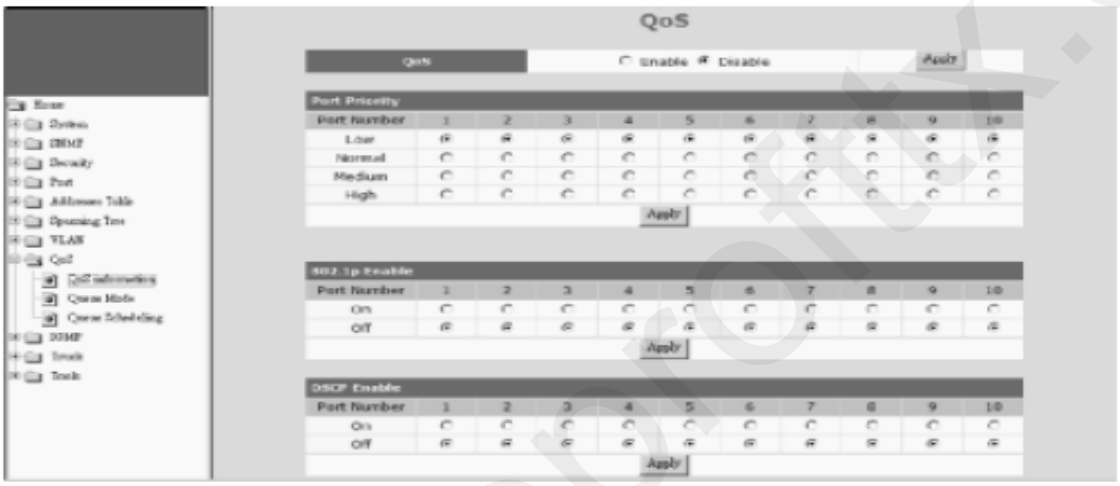


Port 10 is the uplink port. Port 1~9 are isolated to each other but communicate with Port 10 (uplink port).

6.4.8 QoS

This switch supports Port-based priority, 802.1P priority, and DSCP priority. These priority operations could be enable/disable on each port.
For 802.1P and DSCP priority operations, their priority values can be mapped to four priority queues on each port of the switch for QoS operation.

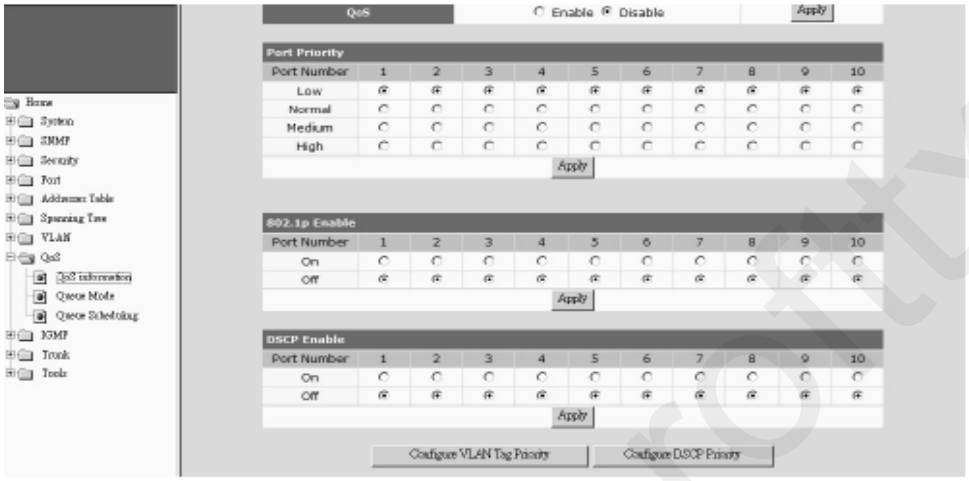
1). QoS Information



QoS : this is for QoS function enable/disable.
Port Priority : this is used to define the priority setting of each port. It will map to the four priority queues of the switch.
802.1P Enable : this is for 802.1P priority operation enable/diable on each port.
802.1P priority operation will use the priority setting in tag of packets for QoS operation.
The mapping of 802.1P priority values (0~7) to priority queue could be defined at "VLAN Tag Priority" page by clicking [Configure VLAN Tag Priority] button.
DSCP Enable : this is for DSCP(Differential Service Code Point) priority operation enable/disable on each port. DSCP priority operation will use the priority setting in ToS field of IP packets for QoS operation.
Seven DSCP values (0~63) could be defined and map to priority queue at "IP Differential Service (DiffServ) Configuration" page by clicking [Configure DSCP Priority] button.
[Configure VLAN Tag Priority] button : Click this button can go to the "VLAN Tag Priority" page for 802.1P priority values (0~7) to priority queue

mapping setting.

[Configure DSCP Priority] button : Click this button can go to the "IP Differential Service (DiffServ) Configuration" page for DSCP priority values (0~63) to priority queue mapping setting.



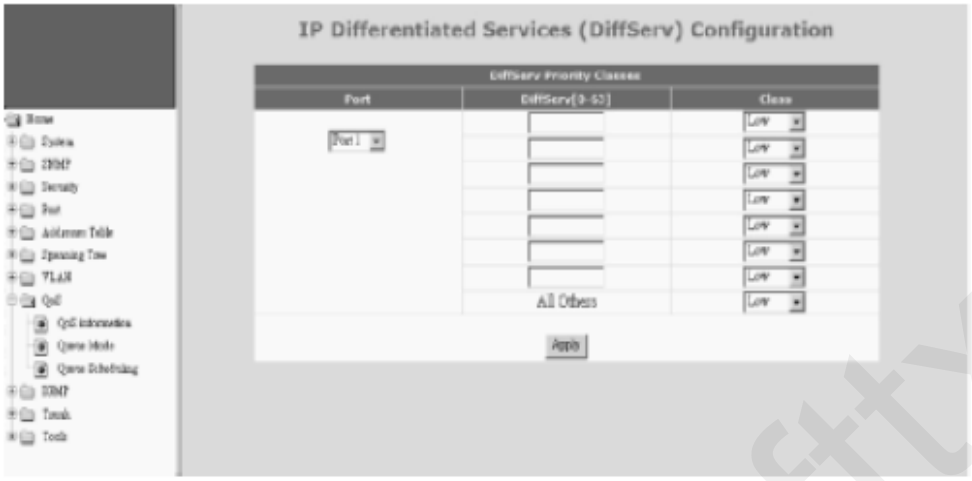
[802.1P Priority Mapping]

For 802.1P priority, priority value (0~7) in VLAN tag will be used for QoS operation. And the mapping of priority values to priority queues (High/Middle /Normal/Low) could be defined here.

This mapping is done by port. And "All" could be selected for every port.

If 802.1P priority function is enabled, these settings will be followed for QoS operation.

[DiffServ Priority Mapping]



DSCP priority operation will use the priority setting in ToS field of IP packets for QoS operation.
Seven DSCP values (0~63) could be defined and map to priority queues (High /Middle/Normal/Low).
This mapping is done by port. And "All" could be selected for every port.

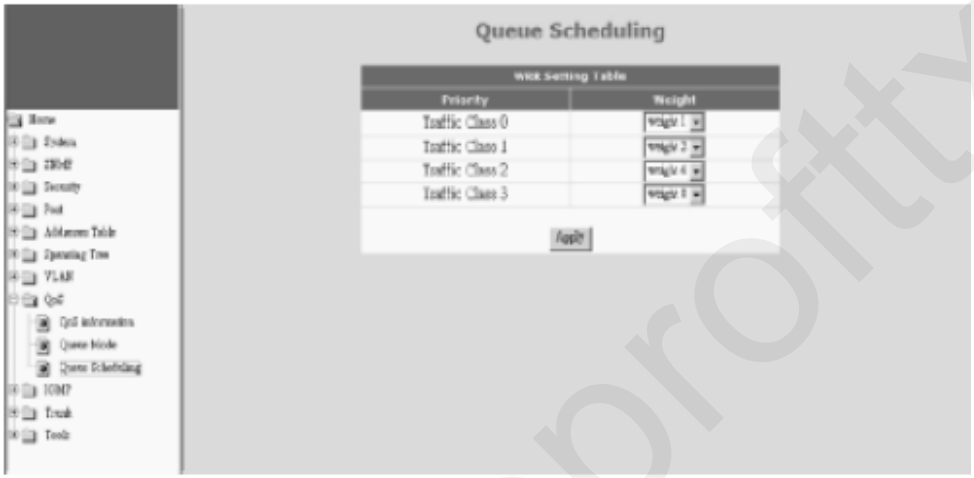
If DSCP priority function is enabled, these settings will be followed for QoS operation.

2). Queue Mode

This switch supports Strict Priority and WRR (Weight Round Robin) operation for sending out packets from piority queues.
If Strict Priority is selected, packets in higher priority queues will always get

bandwidth service first. Lower priority queues will get service when higher priority queues are empty.
If WRR is selected, priority queues will be served with the weighting of priorities.
And the setting of weight could be configured at "Queue Scheduling".

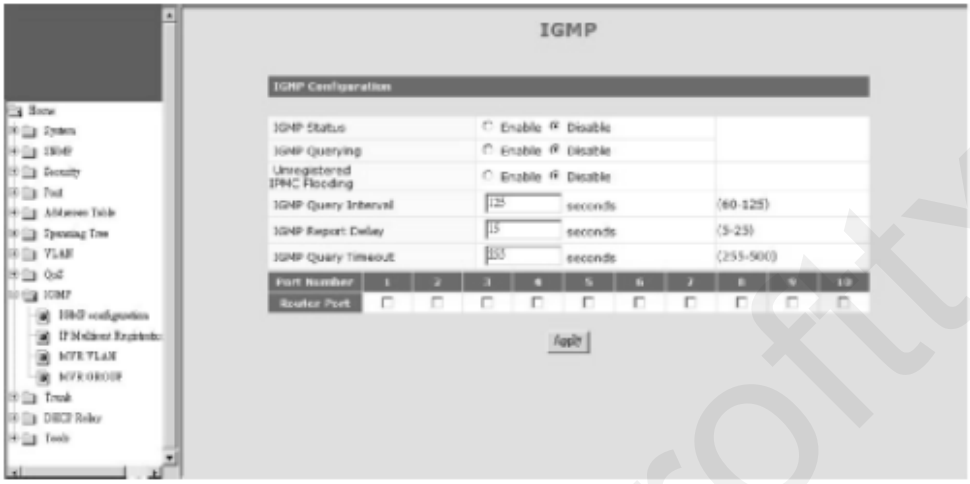
3). Queue Scheduling



This function is used to configured the weighting of priority queues for WRR operation. And the output bandwidth will be shared with the ratio of weighting between priority queues.

6.4.9 IGMP

This switch supports IGMP Snooping function for IP Multicast traffic. Switch will learn IP Multicast Groups from IGMP protocol packets. Here is for IGMP function configuration settings.



1). IGMP Configuration

IGMP Status: this is used to enable/disable IGMP function.

IGMP Querying: this is used to enable/disable IGMP Query function. This switch

will send IGMP Query at a fixed interval if it is enable. The IGMP query responses, known as IGMP reports (which look very much like an IGMP join) keep the switch updated with the current multicast group membership on a port-by-port basis.

Unregistered IPMC Flooding: unregistered (un-joined) IP multicast traffic will be flooded to every port if this setting is enable. If it is disable, the unregistered IP multicast traffic will be flooded to IP multicast members only

IGMP Query Interval: this is used to set the IGMP query packet sending interval if IGMP Query function is enable.

IGMP Report Delay: this is used to set the delay time to send report after receiving a query. When a host receives a Query, it doesn't send a report immediately but it starts a report delay timer for each group membership on the network interface of the incoming Query. When the timer expires, a report is generated for the corresponding host group.

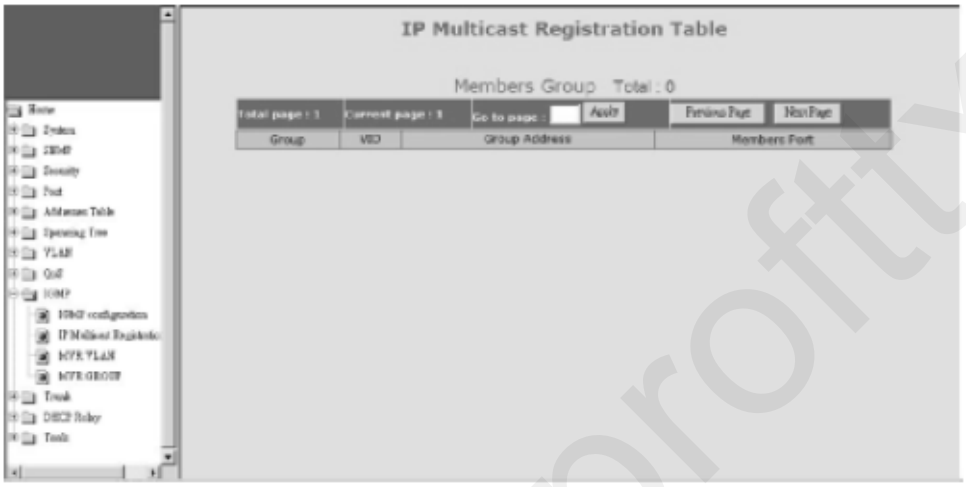
IGMP Query Timeout: this is used to set the timeout interval for IGMP Query operation. If the switch does not receive updated membership information in a

timely fashion, it will stop forwarding multicasts to the delinquent port where the end-device is located.

[Router Port]

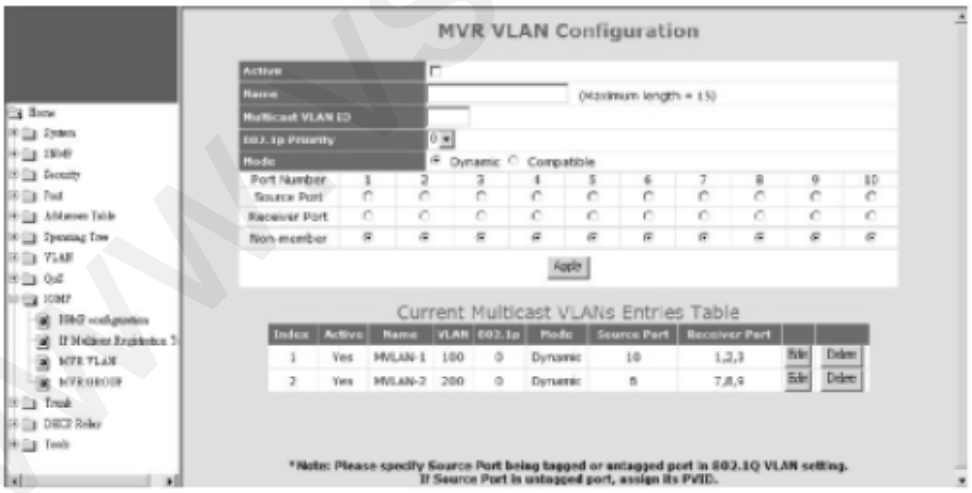
This is used to select the port that connected to IGMP active router.

2). IP Multicast Registration Table



This table will show the learned IP multicast groups.

3).MVR VLAN



This page is used to configure MVR (Multicast VLAN Registration) function. VLAN function will isolate traffic between VLAN groups. But it will also isolate IP multicast traffic for subscribers in different VLANs. The MVR function allows one multicast VLAN to be shared by subscribers in different VLANs. That can reduce the multicast traffic for VLANs.

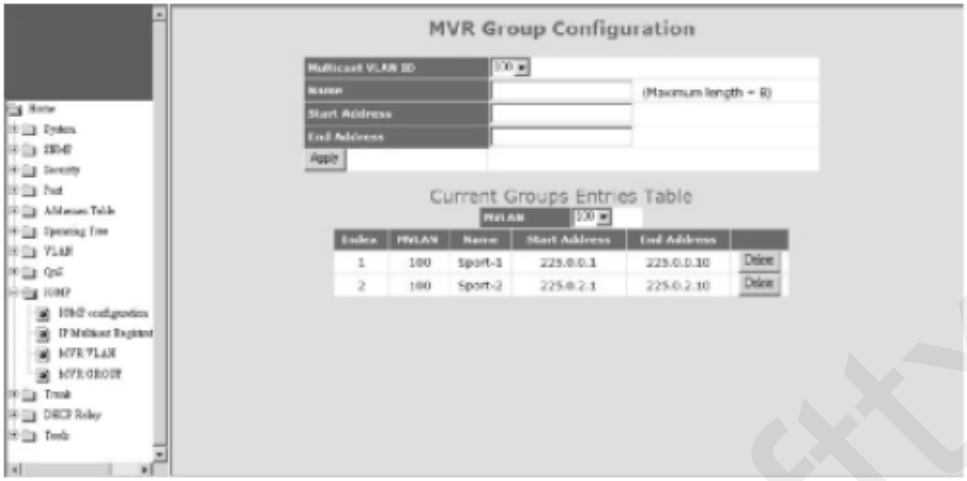
Before configure MVR, complete the following two functions configuration first.
1. Complete 802.1Q VLAN setting first.
2. Enable IGMP snooping function first.
This switch supports three MVR VLANs and MVR VLAN can be created in this page.

Here is the description about those settings.
Active – this MVR VLAN is enabled/disabled.
Name – you can assign a name for the MVR VLAN for identification.
Multicast VLAN ID – this is the VLAN ID for this MVR VLAN. It is 1 ~ 4094.
802.1P Priority – this is an 802.1P priority (0~7). The IGMP control packets for this VLAN will be assigned this priority when tag is added.
Mode – there are two operation modes for MVR function. One is Dynamic mode. Another is Compatible mode. In Dynamic mode, the switch will send IGMP reports to every MVR source port in the MVR VLAN. In Compatible mode, the switch will not send IGMP reports.
Source Port – this is the uplink port of this MVR VLAN to the IGMP traffic source.
It could be tagged port or untagged port.
Receiver Port – this is the ports connecting to subscribers receiving IP multicast traffic in the MVR VLAN.

After the MVR VLAN is configured, you can assign IP multicast groups (video channels) to the MVR VLAN in "MVR Group" page. You can assign more than one IP multicast groups (video channels) to one MVR VLAN.

Note:
1. After MVR VLAN are created, those VLAN will be added to 802.1Q VLAN. Checking "VLAN Table" of 802.1Q VLAN, those VLAN will be seen.
2. Source Port of MVR VLAN could be tagged or untagged port. Please set it at "VLAN Tag Rules" of 802.1Q VLAN. It should be tagged port in most cases. If it is an untagged port, remember to set its Port VLAN ID according to your application.

4). MVR Group



After the MVR VLAN is configured, you can assign IP multicast groups (video channels) to the MVR VLAN in "MVR Group" page. You can assign more than one IP multicast groups (video channels) to one MVR VLAN.
Assigning IP multicast groups to MVR VLAN, you have to select one MVR VLAN first.
For an IP multicast group for MVR VLAN, you have to assign the following settings.
Name – this is the name for this IP multicast group for identification.
Start Address – this is the start IP multicast address for the IP multicast group.
End Address – this is the end IP multicast address for the IP multicast group.
Then click [Apply].

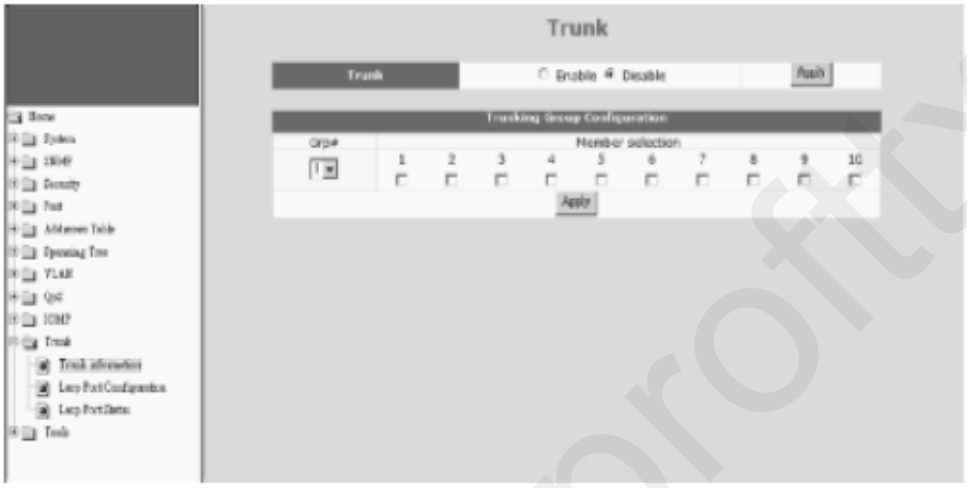
After both MVR VLAN and IP multicast groups are configured, subscribers at the receive ports can receive IP multicast traffic in the IP multicast groups from source port even they are in difference VLANs.
If you want to remove an IP multicast group, click [Delete]. The IP multicast group will be removed from the list.

Note: The list does not support edit function. If you want to make any modification, you have to remove it first. Then create the new one.

6.4.10 Trunk

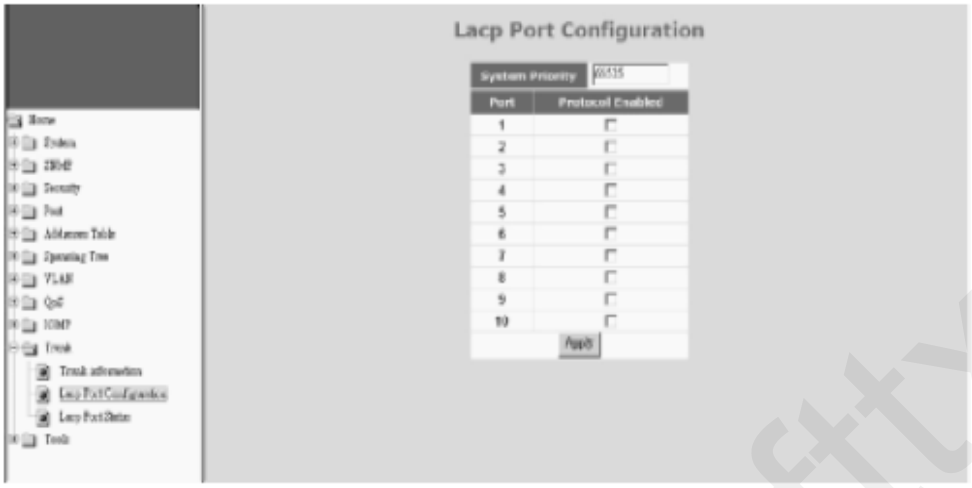
This switch supports up to eight trunk groups. And the trunk could be configured with static assigned or by LACP (Link Aggregation Control Protocol) protocol.

1). Trunk Information



This table is used to assign ports to Trunk groups statically.
Follow the steps to do it. (*Don't connect trunk cables until this function is set.)
a. Enable Trunk function first. Then click [Apply].
b. Select a Trunk Group at "Grp#".
c. Select the member ports.
d. Click [Apply].
e. Repeat b.~d. for another Trunk group setting.
Note: If a port are used as static port for any Trunk group, its LACP function will be disable.

2). Lacp Port Configuration



This page is used to configure LACP function. With LACP protocol, switches can learn trunk connections automatically.

Follow the steps to do it. (*Don't connect trunk cables until this function is set.)

a. Enable Trunk function at "Trunk Information" page first. Then click [Apply].
b. Assign System Priority. (Its value is 1~65535 and higher number has lower priority. Combining with the Mac address of the switch, it is used to identify this switch in LACP protocol operation.)
c. Select ports that will run LACP protocol.
d. Click [Apply].

Note: If ports are already in static trunk group, they are not allowed to apply as LACP ports. If static ports are selected as LACP ports, warning message will be prompted when [Apply] is clicked.

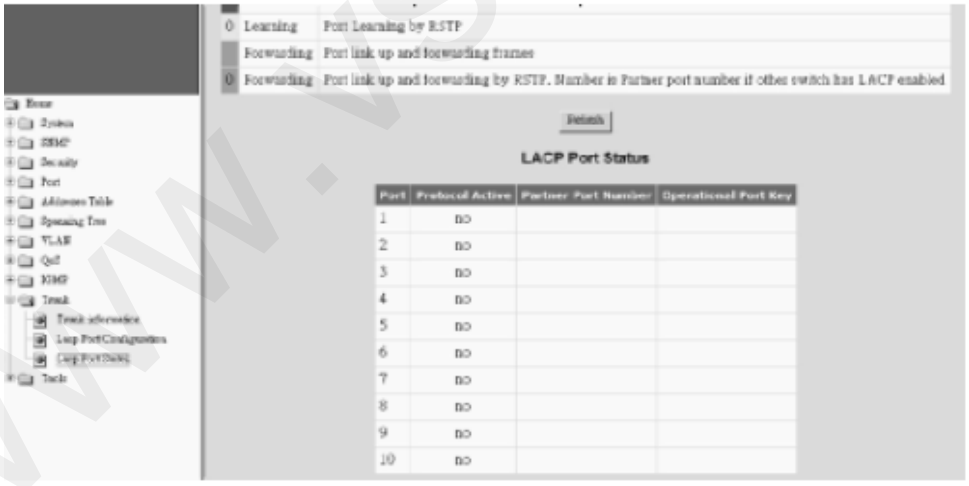
3). Lacp Port Status

This is for LACP protocol running status.

You can see current port status with colors. If LACP trunk is created, another port groups message will be shown.

Click [Refresh] can update the status information.

The following table will show the LACP enable/disable status of each port. Port number and port key of the partner switch will also be shown in the table when LACP Trunk is running.



6.4.11 DHCP Relay Agent Option 82

DHCP Relay function will control DHCP requests and forward DHCP requests to the assigned DHCP server. DHCP Relay Agent Option 82 function will add connection port, VLAN ID and switch information to DHCP requests and then send to the specified DHCP server. Based on those information, DHCP server will assign an IP configuration in the DHCP reply. This is a security function. This page is used to configure DHCP Relay Option 82 function. DHCP Relay Option 82 function will add the following information to DHCP request packet ...

1. Port number that DHCP request packet comes from
2. VLAN ID for this DHCP request
3.Mac address of the switch
4. A additional string as information. (*Adding the information string must be enabled first.)

And DHCP server will assign IP configuration according to the information in Option 82.

Note: Not every DHCP server supports Option 82 function. If DHCP server does not support it, please disable this DHCP-Relay Agent Option 82 function.

Here is the Option 82 definition of the switch.

1. Circuit ID sub-option setup information for DHCP server :
<Format>
[Slot ID/1-Byte] [Port ID/1-Byte] [VLAN ID/2-Bytes] [Information/XBytes]
Slot ID - plase set to "0".

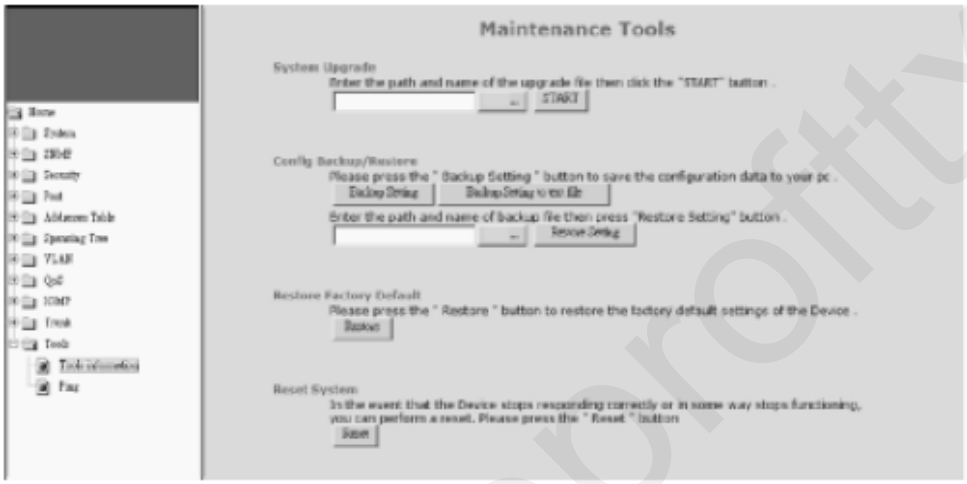
Port ID - please set according to the port number of the switch.
VLAN ID - please set according to its VLAN ID.
Information - this is a string with variable length
For example, "000500c8" means Slot ID 0, Port 5, VLAN ID 200, no information. All of the numbers are hexadecimal numbers.
.
2. Remote ID sub-option setup information for DHCP server :
<Format>
[Mac Address/6-Bytes]
Mac Address - this is the Mac Address of the switch. For example, "000000828ce6" in hexadecimal numbers.
If the Option 82 of DHCP request meets these settings, DHCP server will assign the IP configuration according to this Option 82 content.
Here are the setup item in this web page.
DHCP Relay Agent Option 82 Status is used to enable/disable DHCP Relay function.
Relay Agent Information is the information (a string) about this agent. Check "Add information" and then input the agent information.
DHCP Server IP Address is used to specify the DHCP server for DHCP Relay operation.

6.4.12 Tools

The follow functions are used for system maintenance. They are Software Upgrade, Configuration Backup/Restore, Restore Factory Default, Reset System,and Ping functions.

1). Tools Information

Four functions are supported as the system maintenance tools.



System Upgrade : This function will upgrade the system operation software from the web management PC.

Config Backup/Restore :

[Backup Setting]: Clicking this button, the switch will backup the configuration of the switch to the web management PC.

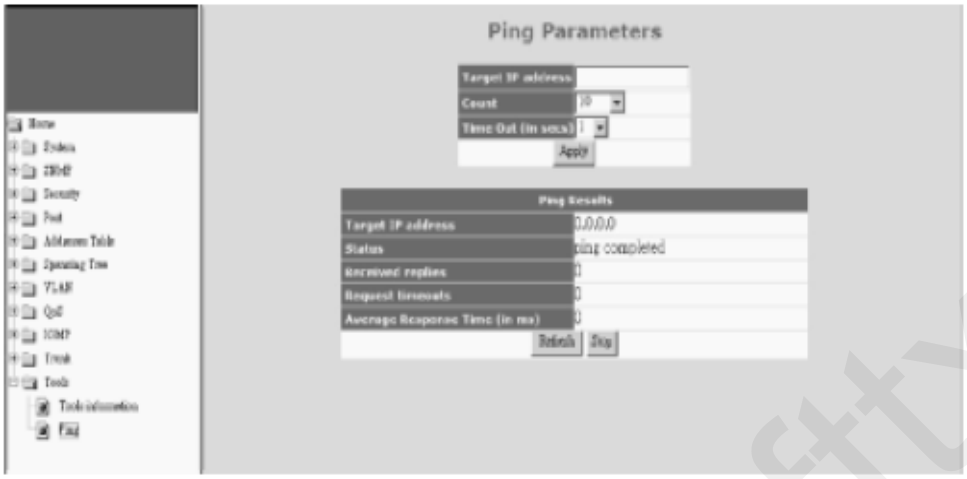
[Backup Setting to text file]: Clicking this button, the switch will backup the configuration of the switch to the web management PC in text format.

[Restore Setting]: The configuration of the switch can be restored to switch by clicking this button after the configuration file is selected.

Restore Factory Default : This function will restore the switch configuration to factory default setting.

Reset System : This function will cause the switch to reboot itself.

2). Ping



This function is used to ping network devices from the switch. It can be used to verify network connection.

Target IP address : This is the target IP address for the ping operation.
Count : This is the repeat count for the ping operation.
Time Out : This is the timeout value for the ping operation.
After the above items are set, click [Apply] to start the ping operation.

Then the result of ping operation will be shown.

7. Software Update and Backup

This switch supports software update and configuration backup/update/restore functions. It could be done in two ways.

1. From console when booting: by Xmodem protocol and doing by terminal program. This function can be used for run-time code and boot code updating. (Boot code works only at boot time - before the main program starts.)

Press Ctrl-C when the switch is booting, the following message will be shown.

```
            Boot Menu
============================
0: Start the Run-time code
1: Upgrade Run-time code
2: Upgrade Boot Code
=> Select:
```

a. Start Run-time code : This option will continue the booting process.

b. Upgrade Run-time code : This option will try to update run-time code (main code) from terminal program with Xmodem protocol. If this option is selected, the following message will be shown.
"Waiting to receive file by Xmodem ...."
Then user can select "Send File" function of terminal program and select Xmodem protocol and the update file, then start the file upgrade.

c. Upgrade Boot Code : This option will try to update boot code from terminal program with Xmodem protocol. User can select "Send File" function of terminal program and select Xmodem protocol and the update file, then start the file upgrade.

2. From web browser: Doing by http protocol and by web browser. Please refer to the description of "Tools" function in Section 6.4.12.

3. From console/telnet command: Doing by tftp protocol and done by "copy" command. Please refer to the description of "copy" command in Section 6.2.2.

A. Product Specifications

See details on datasheet

SWG0802-SFP
SWG1604-SFP
SWG2404-SFP
SWG0816-SFP

B. Compliances

EMI Certification FCC Class A Certification (USA)

Warning: This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A digital device pursuant to Subpart B of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are required to correct the interference.

CE Mark Declaration of Conformance for EMI and Safety (EEC)

This is to certify that this product complies with ISO/IEC Guide 22 and EN45014.
It conforms to the following specifications:
EMC: EN55022(1988)/CISPR-22(1985) class A
EN60555-2(1995) class A
EN60555-3
IEC1000-4-2(1995) 4kV CD, 8kV AD
IEC1000-4-3(1995) 3V/m
IEC1000-4-4(1995) 1kV - (power line), 0.5kV - (signal line)
This product complies with the requirements of the Low Voltage Directive 2006/95/EC and the EMC Directive 2004/108/EC.

Warning! Do not plug a phone jack connector into the RJ-45 port. This may damage this device.

C. Warranty

We warrant to the original owner that the product delivered in this package will be free from defects in material and workmanship for a period of warranty time from the date of purchase from us or the authorized reseller. The warranty does not cover the product if it is damaged in the process of being installed. We recommend that you have the company from whom you purchased this product install it.