Gigabit Management Switch
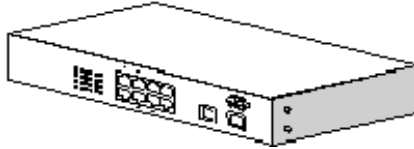# User's Manual

Rev. 0.10-EV

About this manual …

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

These models are

1. **8 * TX + 2 * SFP (10G) ports model**
   This model supports eight TX ports and two extra SFP ports for Giagbit Ethernet connections.

2. **16 * TX + 4 * SFP (16G) ports model**
   This model supports sixteen TX ports and four share SFP ports.   Port 13~16 are 1000TX RJ45 port / SFP port optional for Gigabit connection. And they can auto-detect the connection from 1000TX RJ45 port or SFP port.
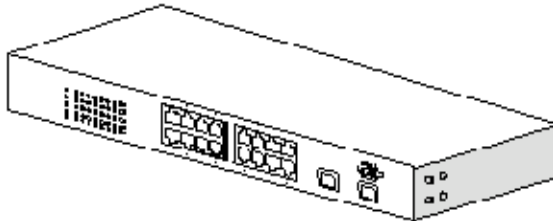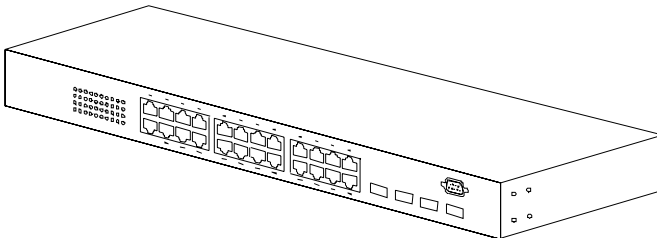

3. **24 * TX + 4 * SFP (24G) ports model**
   This model supports twenty-four TX ports and four share SFP ports.   Port 21~24 are 1000TX RJ45 port / SFP port optional for Gigabit connection. And they can auto-detect the connection from 1000TX RJ45 port or SFP port.

Contents

1.   Introduction

There are three models for the Gigabit Web Smart Switch Series – 8TX+2SFP(10G) model, 16TX+2SFP(18G) model and 24TX+4SFP(24G) model. This Gigabit Web Smart Switch is a Layer2 Web Smart switch with lots of advanced network functions including VLAN, trunking, spanning tree, mirror port, rate limit and port configuration.   Console is supported for some basic settings. Web interface is for switch management.   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 Web Smart Switch
- One AC power cord
- One console cable
- Two rack-mount kits and screws   (*for 16TX+2SFP/24TX+4SFP models only)
- This 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 16TX+2SFP/24TX+4SFP model, you can also install the switch on a 19" rack with the rack-mount kits as the picture.
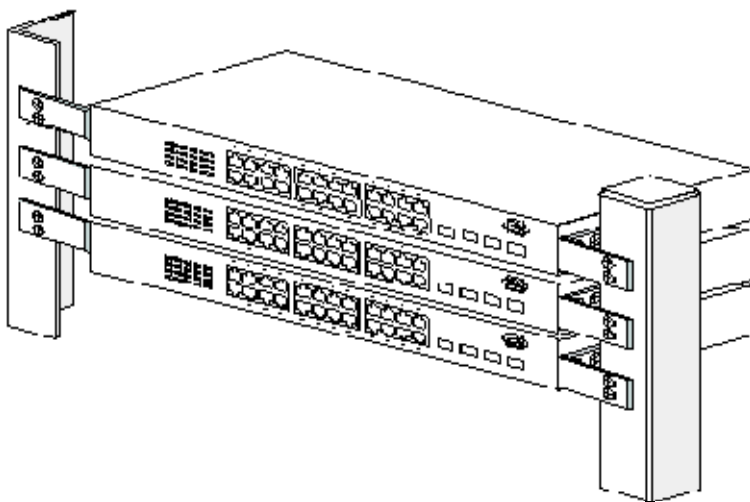
3. Configure Network Connection

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.

Cat5e Twisted Pair Cable
100 meters max.
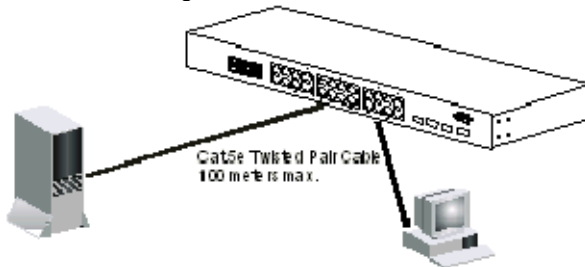
3.2 Connecting to Another Ethernet Switch/Hub

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.

Another Switch

Straight-Through cable
Max. 100m
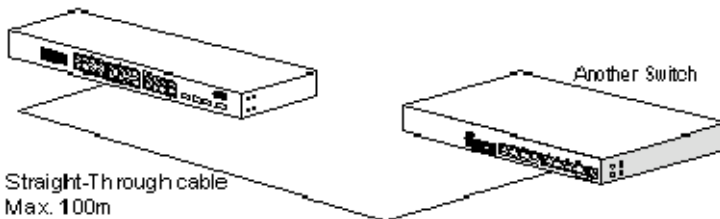
3.3 Application

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 Web Smart function of the switch, network administrator is easy to monitor network status and configure for different applications.
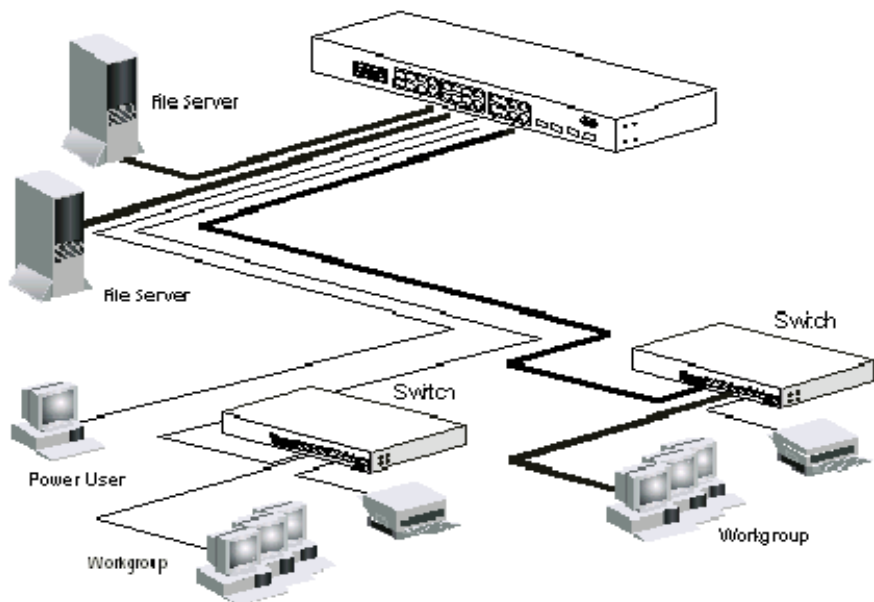
4. Adding Module

This switch supports SFP (for 1000SX/LX/…) connectors for gigabit ports. Because the 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.
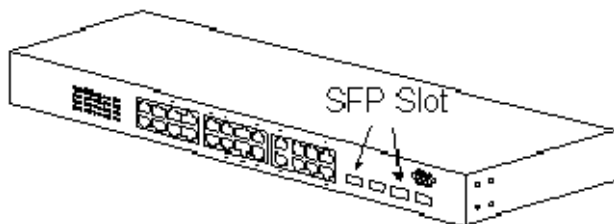
Follow the steps for module adding and removing.
[Add SFP Transceiver]
1.   Plug in the SFP Transceiver to SFP slot directly.
2.   Connect network cable to the SFP Transceiver.   If the connected devices are working, the Link/Act LED will be ON.

[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 8TX+2SFP / 16TX+2SFP / 24TX+4SFP Models]

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.

6. Manage / Configure the Switch

6.1 Introduction of the management functions

This switch is a L2 Web Smart switch.   It supports in-band management function from Http interface.   Console is supported for some basic settings.   It supports network configuration functions, like VLAN, Trunking, Port Mirror, QoS, spanning tree and software backup/update.   Users can configuration 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.

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

10

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. 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 program for boot code and run-time code updating..

b. From web browser : doing by http 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

Please follow the steps to complete the console hardware connection first.
1.   Connect from the 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, built at 15:25:28, Jul 21 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:C0:F6:64:99:6F

Firmware version : 1.01.09 (built at Aug   6 2008 14:38:24)
Username:
--------------------------------------------------------------------------------------------------
```

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 "**admin**" / "**admin**".
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
   disable              Turn off privileged commands
   enable                Turn on privileged 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 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.

13

```
-------------------------------------------------------------------------------------
> ?
   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 of 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.

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
   disable                   Turn off privileged commands
   enable                    Turn on privileged 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 another
#
-----------------------------------------------------------------------------------------
```

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.)

15

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. **disable** command
   This command is used to leave privileged mode, and the prompt will become ">".   Only the guest access right is available.

8. **enable** command
   This command is used to enter privileged mode, and the prompt will become "#".   And the administrator access right is available.

9. **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.

10.   **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 ?
   calendar   Date and time information
   dot1x   802.1x content
   gvrp   GVRP configuration
   history   History information
   interface   Interface information
   ip   IP information
   lacp   LACP statistics
   line   TTY line information

16

logging	Login setting
mac-address-table	Configuration of the address table
mac-security	MAC Security Configuration
management	Management IP filter
map	Maps priority
port	Port characteristics
queue	Priority queue information
radius-server	RADIUS server information
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**.

11.   **calendar** command
This command is used to set the system time.   It is entered in the <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

17

It is 18 seconds passby after the setting command.

12.　　**configure** command
This command will change the console interface to configure mode.　And the prompt will become "(configure)#".　In this mode, administrator can do system configuration of the switch.

The operation of configure mode will be describe in next section.

"exit" command can be used to quit this operation mode.

13.　　**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.

Here are the examples.
Backup configuration to TFTP server at 192.168.1.10 ...
copy config running-config tftp 192.168.1.10

Backup firmware to TFTP server at 192.168.1.10 ...
copy firmware running-firmware tftp 192.168.1.10

Restore configuration from TFTP server at 192.168.1.10 ...
copy config tftp running-config 192.168.1.10

Update firmware from TFTP server at 192.168.1.10 ...
copy firmware tftp running-firmware 192.168.1.10

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
  automode                      Set Auto Negotiation or Auto Detect mode
  default                    Restore to factory default 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
  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
  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 entering command history.

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. **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.

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

8. **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
    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

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 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:
Setting 802.1x function on ports, "dot1x" command in interface configuring mode is used.   Setting for RADIUS server, "radius-server" command is used. Please refer to sections for the commands.

9. **end** command
   This command is used to exit from configure mode.

10.   **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.

11.   **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.

12.   **ip** command
   This command is used to configure some IP-depending functions.   Entering "ip ?", the sub-commands will be shown.
   (config)# ip ?
     default-gateway   Specifies 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 ... comand 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 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.

13.   **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 identifie

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.

14.   **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.

15.   **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

24

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.

16.   **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.

17.   **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.

18.   **no** command
This command is used to disable a function or restore a setting to factory default   of the switch.

```
(config)# no ?
  automode              Set Auto Negotiation or Auto Detect mode
  dot1x                 Configures 802.1x port-based access control
  hostname              Sets system's network name
  ip                    Global IP configuration sub commands
  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
  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.

19.   **prompt** command
This command is used to set the prompt word for console.
For example,
(config)# prompt AAA
AAA(config)#

20.   **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 "interface" command.

21.   **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.

22.   **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 set the 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.

23.   **rate-limit** command

This command is used to define the unit for rate limit operation.   The unit could be from 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)

24.   **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

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 for this 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.

25.   **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

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.

26.   **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.

27.   **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 set rate limit for broadcast traffic. "**x**" is the limit rate number, and its valid value is 0-11. (0:disable, 1:1Kpps, 2:2Kpps, 3:4Kpps, 4:8Kpps, 5:16Kpps, 6:32Kpps, 7:64Kpps, 8:128Kpps, 9:256Kpps, 10:512Kpps, 11:1024Kpps)

storm-control mc-rate x command is used set rate limit for multicast traffic. "**x**" is the limit rate number, and its valid value is 0-11. (0:disable, 1:1Kpps, 2:2Kpps, 3:4Kpps, 4:8Kpps, 5:16Kpps, 6:32Kpps, 7:64Kpps, 8:128Kpps, 9:256Kpps, 10:512Kpps, 11:1024Kpps)

storm-control fc-rate x command is used set rate limit for unicast flooding traffic. "**x**" is the limit rate number, and its valid value is 0-11. (0:disable, 1:1Kpps, 2:2Kpps, 3:4Kpps, 4:8Kpps, 5:16Kpps, 6:32Kpps, 7:64Kpps, 8:128Kpps, 9:256Kpps, 10:512Kpps, 11:1024Kpps)

28.   **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.

29.   **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.

30.   **vlan** command
This command is used to enter VLAN configuring mode.   And the prompt will become ...
vlan database
(config-vlan)#

The operations for VLAN are done 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 "(configure)#".

The port interface and VLAN interface 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 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 "(configure)#".
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,

31

"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
  lacp                     Configures LACP status
  map                      Maps priority
  maximum-packet-length   Configures the maximum packet length of the port
  no                       Negates a command or sets its defaults
  port                     Configures the characteristics of the port
  port-vlan               Configures Port-Based VLAN
  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 entering command history.

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.   **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.

14.   **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 ip dscp x y z command is used to map DSCP values to priority queues. "**x**" is the index of the 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 ip precedence x y command is used to map 802.1P priority values to priority queues.   "**x**" is the value of IP Precedence in ToS, 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).

15.   **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

16.   **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
    lacp   Configures LACP status
    map   Maps priority
    maximum-packet-length   Configures the maximum packet length of the port
    port   Configures the characteristics of the port
    port-valn   Configures Port-Based VLAN
    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.

17.   **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 | Specifies 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).

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 disable the security function on the interface port(s).

18.   **port-vlan** command

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

19.   **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.

20.   **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".

21.   **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.

22.   **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.

23.   **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.

24.   **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

[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 1~-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 1~-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 the its VLAN ID.   PVID is also used as the VLAN ID for tag adding when untagged packet is translated to tagged packet.

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 xxx]
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.

6.2.4.2 Interface Configuring Commands for VLAN

Commands in Configuring Mode are for general switch settings.   And its prompt is "(configure)#".
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 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 entering command history.

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 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

41

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.

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

   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.

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 "(configure)#".

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

Entering "vlan database", and its 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 entering command history.

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 interface mode.
   (config-if)# 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   Configures 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 filtering based on VLAN membership 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   Configures 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.

   port-vlan command is used to enable Port-base VLAN.
   no port-vlan command can be 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 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". And **no vlan x** command can remove the VLAN with VLAN ID "**x**".

If VLAN "x" exists already but name "yyy" is different, the 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 ?
    calendar              Date and time information
    dot1x                 802.1x content
    gvrp                  GVRP configuration
    history               History information
    interface             Interface information
    ip                    IP information
    lacp                  LACP statistics
    line                  TTY line information
    logging               Login setting
    mac-address-table     Configuration of the address table
    mac-security          MAC Security Configuration
    management            Management IP filter
    map                   Maps priority
    port                  Port characteristics
    queue                 Priority queue information
    radius-server         RADIUS server information
    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 calendar** command
   This command will show current system time.
   For example,
   ```
   # show calendar
   Current Time : 2008/08/29-11:27:12
   ```

2. **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
   ```

46

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
```

3.   **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
```

4.   **show history** command
   This command is used to show the input commands history.
```
# show history
  0. show
  1. show gvrp configuration
  2. show history
```

5.   **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 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         1549816
=======================================
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:C0:F6:64:99:6F
Configuration:
 Name:
 Port admin:             Enable
 Speed-duplex:           Auto_off
 Capabilities:           10half,10full,100half,100full,1000full
 Broadcast storm:        Disable
 Flooded unicast storm:  Disable
 Multicast storm:        Disable
 Flow control:           Disable
 LACP:                   Disable
 Max MAC count:          10
 Maximum Packet Length:  1518
Current status:
 Link status:            Down
 Operation speed-duplex: 1000Half
```

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
 LACP:                   Disable
 Ingress rate limit:     Disable
 Egress rate limit:      Disable
 VLAN membership mode:   access
```

```
    Ingress rule:                  Disable
    Acceptable frame type:         All frames
    Native VLAN:                   100
    Priority for untagged traffic:Low
    GVRP status:                   Disable
    Private-VLAN mode:             Normal
```

6. **show ip** command

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

    ```
    # 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:       192.168.1.11
    netmask: 255.255.255.0
    ```

    show ip redirects command will show current gateway setting of the switch IP configuration.

    For example,
    ```
    # show ip redirects
    gateway: 192.168.1.254
    ```

7. **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
32768,00C0.F664.996F
```

8. **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   : NONE
Stopbits: 1
```

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

```
# show logging ?
  configuration          logging configuration
  <cr>
```

show logging command is used to show current system log content.
For example,
```
# show logging
[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 logging configuration command is used to show current system log configuration.
For example,
```
# show logging configuration
 [System Log]
System Log Status     : Disable
Log Level(0-7): 4
Remote Log            : Enable
Remote Log Server IP : Empty
```

10. **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 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
```
51

```
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
-----    ---    --------------    ------------
```

11. **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" mode that allows static mac addresses on ports to access network only. Another is "limit by mac no." mode 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
```

52

Eth 1/ 3	0	N/A	No Security
Eth 1/ 4	0	N/A	No Security
Eth 1/ 5	10	0	Limited by MAC no
Eth 1/ 6	0	N/A	No Security
Eth 1/ 7	0	N/A	Accept function
Eth 1/ 8	0	N/A	No Security
Eth 1/ 9	0	N/A	No Security
Eth 1/10	0	N/A	No Security

12. **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

13. **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 ip ?
  dscp                IP DSCP priority map
  port                IP port priority
  precedence          IP precedence priority map
```

show map ip 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 ip port command is used to show port to priority queues mapping. This is called port-based priority.
show map ip precedence command is used to show 802.1P priority values(0~7) to priority queues mapping on all ports.
show map ip precedence 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.)

14. **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
Destination port: 6
Source port: Eth1/2 Eth1/7
Mode   : Disable

15. **show queue** command
This command is used to show traffic scheduling settings for 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 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

16. **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   : 12345678

17. **show rate-limit** command
This command is used to show rate limit settings on ports.

For example,
show rate-limit
[Rate Control Configuration]
    Port   Ingress   Egress

54

```
=============================================
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
```

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

   For example,
   ```
   # show snmp
   [SNMP Configuration]
   Object ID      : 1.3.6.1.4.1.655.100.2.1
   System up Time: 4015 (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
   ```

19. **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 : 1970/01/01-10:08:38
   ===================================
   ```

20. **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
```

21. **show system** command
   This command is used to show general system configuration of the switch.

   For example,
```
# show system
System Configuration
Main Board Information:
Firmware Version:   1.01.09 (built at Aug   6 2008 14:38:24)
Mac Address:        00:C0:F6:64:99:6F
Number of Ports:    10
1Q VLAN Max. Group: 256
DHCP Client:        Disable
Time Server:        Disable
System Log Status:  Disable
Remote Log:         Enable
```

22. **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.

56

show trunk group x command is used to show port member settings of Trunk Group x.   ("**x**" is the trunk group index.)

23. **show version** command
This command is used to show system version information and model information.

For example,
```
# show version
Serial number::        0000000001
Firmware Version:      1.01.09 (built at Aug   6 2008 14:38:24)
Number of Ports:       10
Model Name:            Gigabit L2 Management Switch
```


24. **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
   <cr>
```

show vlan command is used to show all VLAN settings (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,
```
# show vlan id 100
Vlan ID:    100
VLAN Type:   Static
Name:           P100
Ports/Port channel:
```
```
# show vlan name P100
Vlan ID:    100
VLAN Type:   Static
Name:           P100
Ports/Port channel:
```

show vlan private-vlan command is used to show Private VLAN setting.
For example,
```
# show vlan private-vlan
[Private VLAN Port Configuration]
 Port#     Port Type    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	100	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

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/Mask/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/Mask/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 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.   Before http connection, IP address configuration of the switch should be done first.

Please follow the instruction in Section 6.2 to complete the console connection and use "**show ip interface**" command to check IP address of the switch first. If users want to change the IP address of the switch, use "**ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy**" (**xxx.xxx.xxx.xxx** is the IP address and **yyy.yyy.yyy.yyy** is the netmask) command in interface-vlan configuring mode (under "(config-if)#" prompt) to modify the IP address of the switch.   The default IP configuration is **192.168.1.1** and mask **255.255.255.0**.

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 "**admin**" / "**admin**".   Then the management homepage will appear.
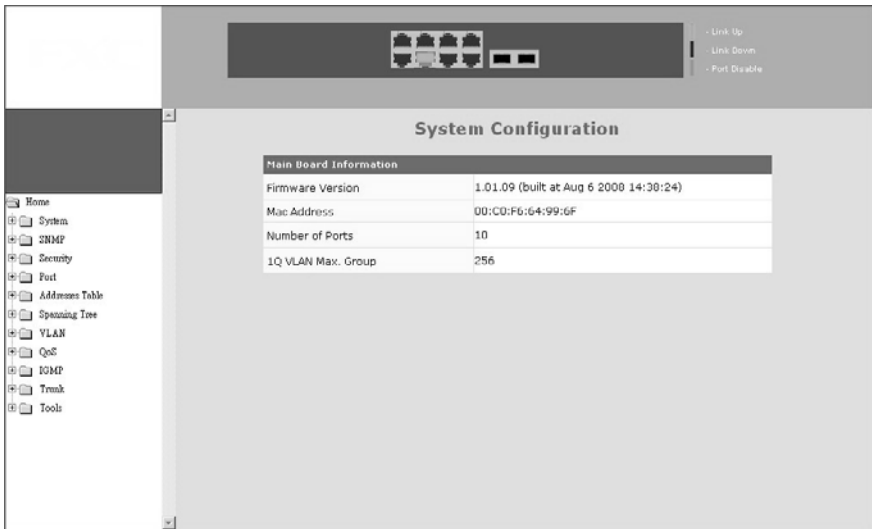
Left part of the homepage is a function list.   Users can select one of them for status monitoring or switch configuration.
Upper part of the homepage is the link status of the switch.   Three different colors are used to show different status of ports – Link Up, Link Down and Port Disable.
Middle part 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
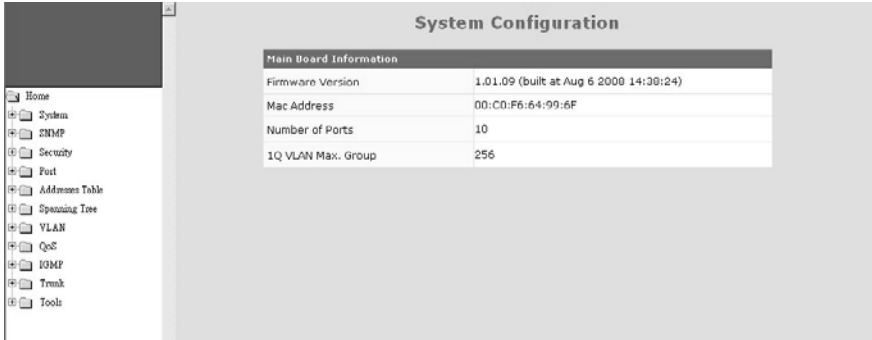
This function lists the system information about the switch.   You can find the firmware version, Mac address, connection port number, and maximum VLAN group number here.

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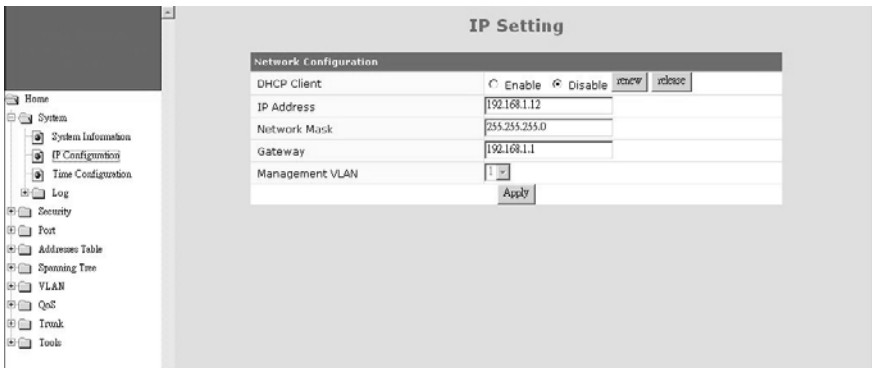
This function is used to setup the IP configuration of the switch.
You can enable DHCP client function to get IP configuration from DHCP server automatically.   Or, disable DHCP client function and set IP configuration manually.

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 the 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
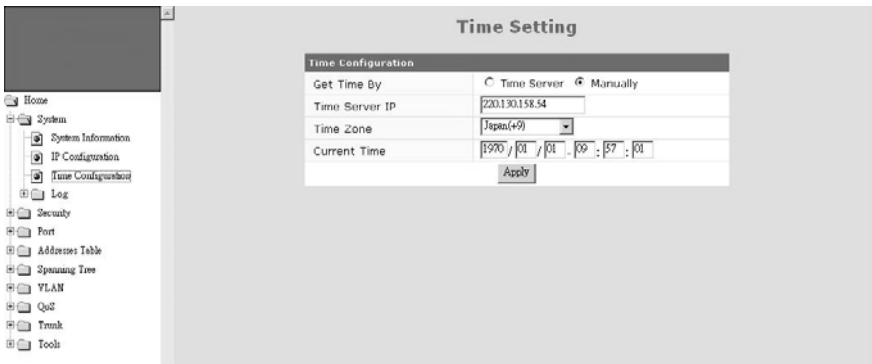
There are two ways to get the system time.

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].

4). Log

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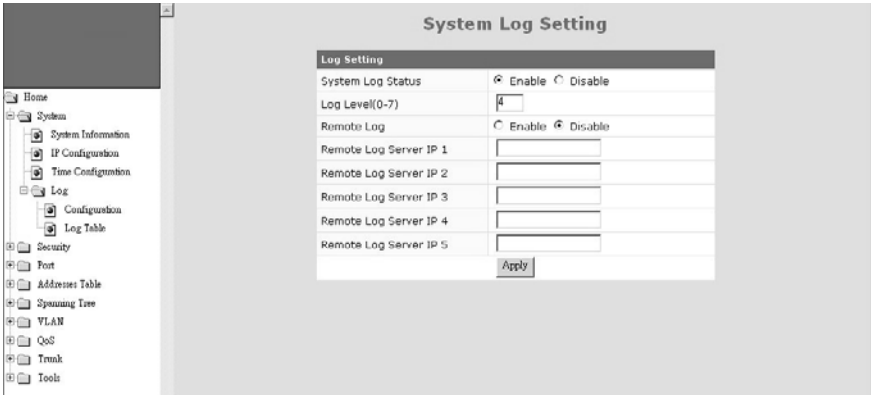
Users can configure System Log function and view log records here. If this function is enabled, the switch will record events to a log file and put the log file to flash.

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 ad below.

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 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.
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.

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 admin/admin.)

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

[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) could be enable/disable for different administrators.   This is for security
policy for switch management.

Note: Remember to enable at least one IP/Subnet with Modify right for Http
interface.   Otherwise, configuring switch from remote will become impossible.
In that case, you have to use the "default" command from console to restore
settings to factory default for switch management.

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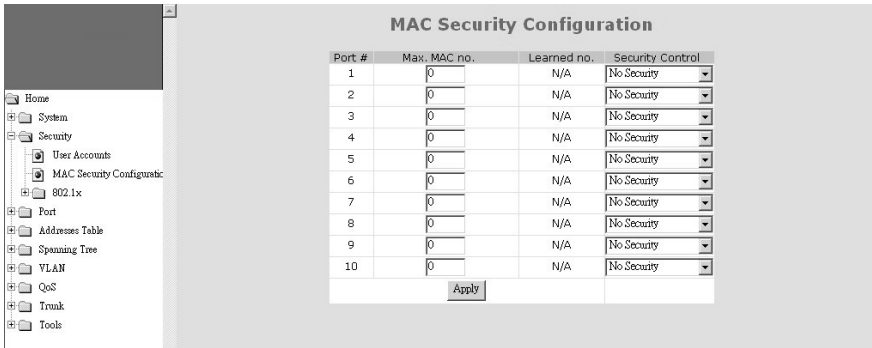
There two Mac ID security modes for the switch.   One is Static Mac ID Filter on
Port, another is Dynamic Mac ID Number Limit on Port.

[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 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.
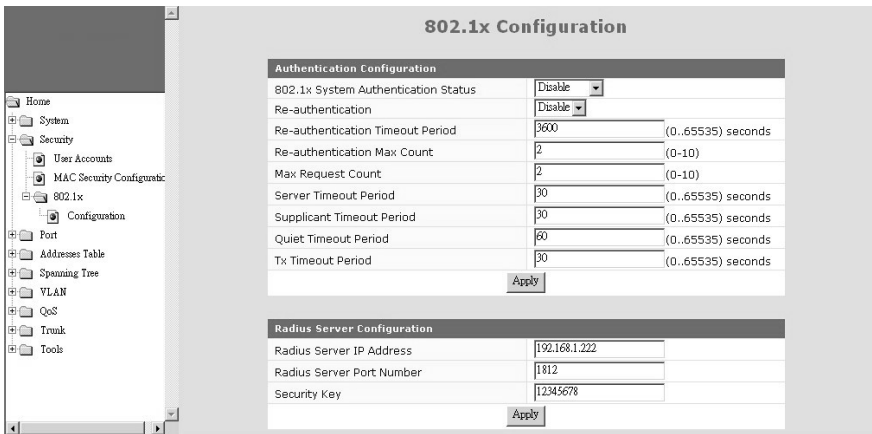
The function here is for 802.1x function configuration.
1. **802.1x Authentication Status**: [Enable/Disable/Transparent]
   Enable: enable 802.1x function in authentication mode
   Disable: disable 802.1x function
   Transparent: only forwarding 802.1x packets
2. **Re-authentication (enable/disable)**, **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 time value between the switch and the 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.

[Radius Server Configuration]
This function is for 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]
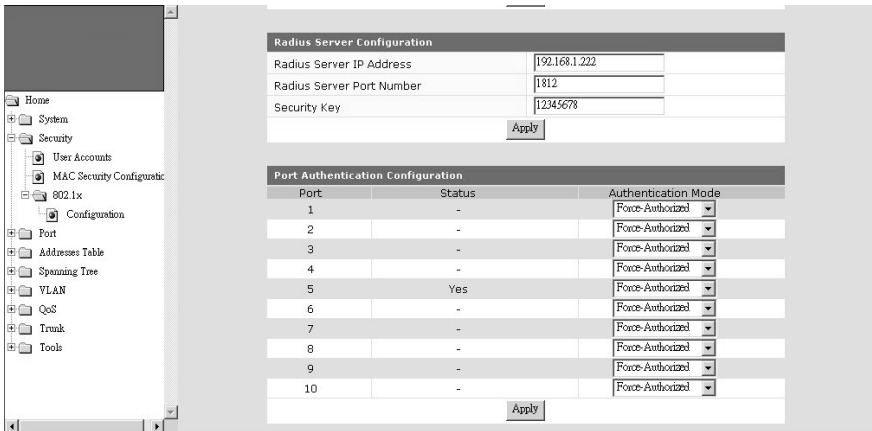
The Port Authentication Configuration is used to select the authentication mode for each port of the switch.

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.

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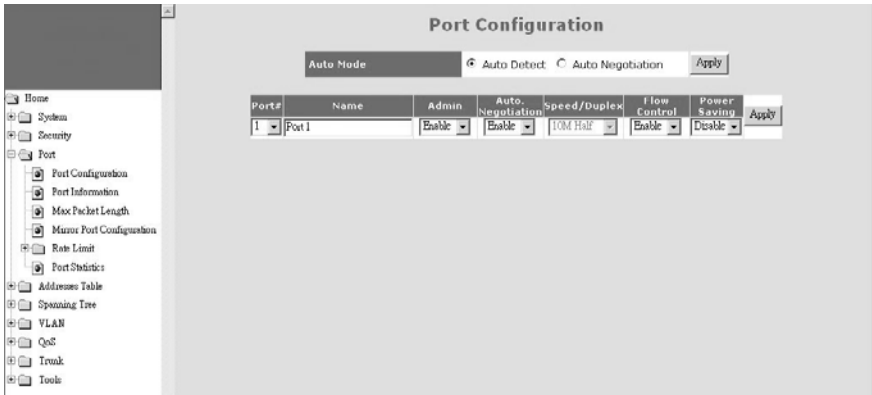
This function is used to configure port settings of the switch.   You can enable /disable a port, set it to fixed 10M or 100M or 1000M ... and so on.

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.

71

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. Click [Apply] after any modification.

2). Port Information

Current Setting & Link Status

Port#	Name	Admin	Auto. Negotiation	Speed/Duplex	Flow Control	Power Saving	Link Status
1	Port 1	Enable	Enable	0M Half	Enable	Disable	Down
2	Port 2	Enable	Enable	0M Half	Enable	Disable	Down
3	Port 3	Enable	Enable	0M Half	Enable	Disable	Down
4	Port 4	Enable	Enable	0M Half	Enable	Disable	Down
5	Port 5	Enable	Enable	100M Half	Enable	Disable	UP
6	Port 6	Enable	Enable	0M Half	Enable	Disable	Down
7	Port 7	Enable	Enable	0M Half	Enable	Disable	Down
8	Port 0	Enable	Enable	0M Half	Enable	Disable	Down
9	Port 9	Enable	Enable	0M Half	Enable	Disable	Down
10	Port 10	Enable	Enable	0M Half	Enable	Disable	Down

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 will show 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.
 Link: It shows the link status of each port.

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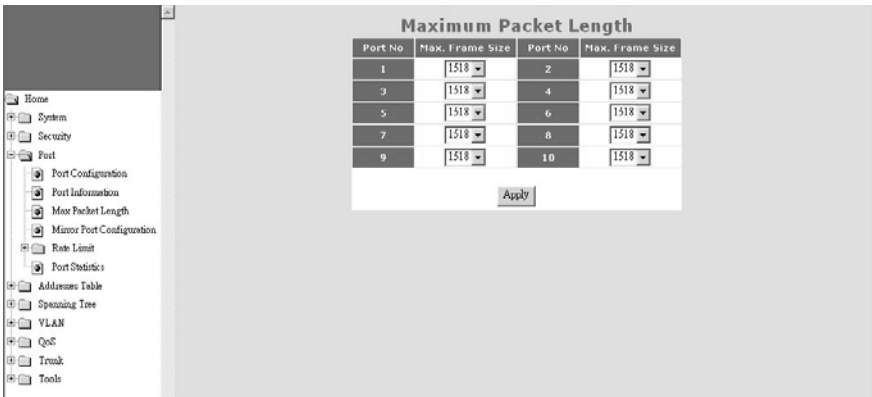
This switch supports Jumbo Frame function. And the maximum packet size could be up to 9600 byte/packet. You can select the maximum packet size for each port here.

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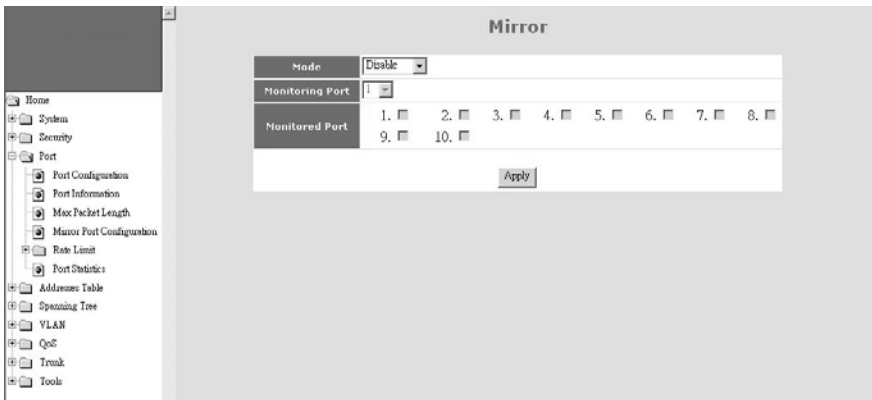
Mode: This is used to enable/disable Mirror function.
Monitering Port: This is used to set the capture port. The switch will copy the traffic from Monitored Port to this port if Mirror function is enabled.
Monitored Port: This is the monitored port. The switch will copy the traffic from this port to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

73

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 number for Ingress and Egress traffics. "0" means NO LIMIT. Click [Apply] after the setting.

5-2) Storm Control Configuration
This function can setup the broadcast, multicast, and unicast storm rate of the switch.
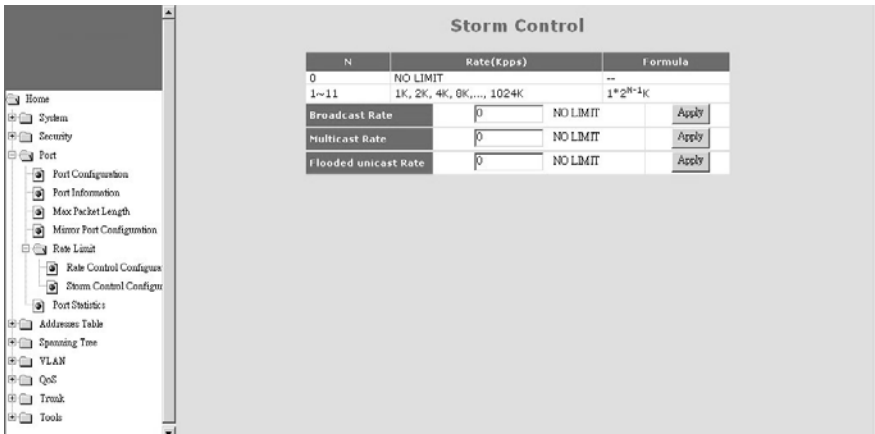
Please follow the rules in table to setup the maximum storm rates.

Note: The storm rate is counted by pps (packet per second).

6). Port Statistics
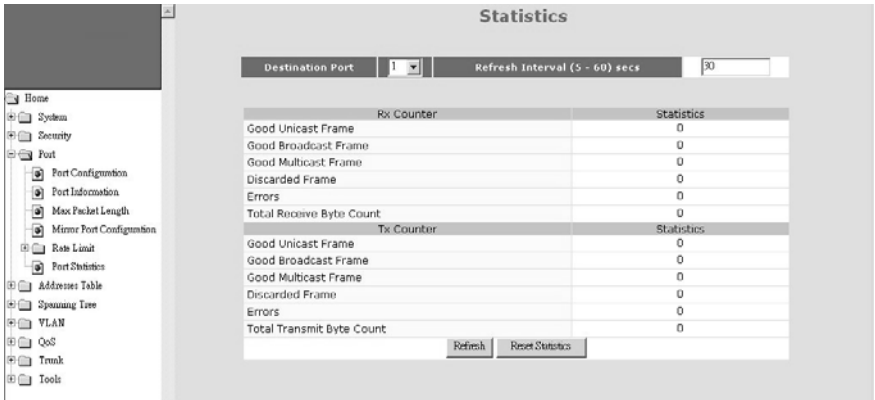
Port statistics counters could be read here.
Select a port to get its counters.

[Refresh]
The counters will be refreshed automatically.   You can modify the refresh interval.
And you can click [Refresh] to refresh the counters immediatelly.
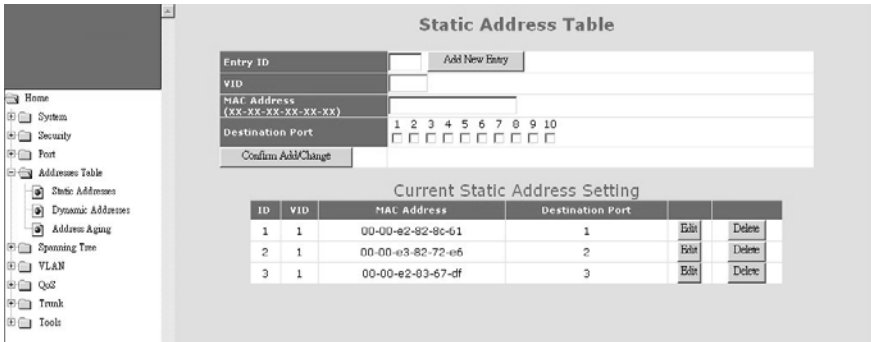
[Reset Counters]
Click [Reset Statistics] can reset the counters to "0".

6.4.5 Address Table

These are functions about Mac address table. One is "Static Address Assign" and another is "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 Address 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

Port Aging Time Setting

Port Aging Time Setting	
ARL Aging	⊙ Enable ○ Disable
ARL Aging Time (seconds)	300
	Apply

The switch will learn Mac addresses to an ARL table automatically.   And follow the table to do packet store-and-forward operation.   If Mac addresses are not received for some time, those 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.

And the time for aging operation could be modified here.   It is 300 seconds by default.

6.4.6 Spanning Tree

Spanning 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]
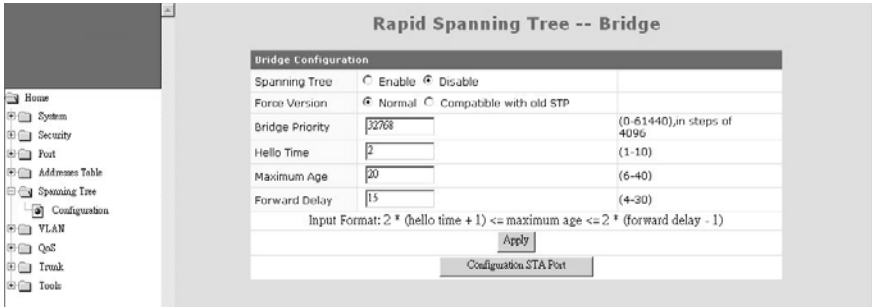
Here are the parameters for Spanning Tree operation on the switch.
Enable/Disable : enable/disable spanning tree operation
Force Version : It will operate as Rapid Spanning Tree in "Normal" state.   And it can be forced to operate at old Spanning Tree mode if "Compatible with old STP" is selected.
Bridge 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 <u>less or equal to</u> Maximum Age, and Maximum Age is <u>less or equal to</u> 2*(Forward Delay -1).

[Setting of Port]
Click [Configuration STA Port].   You can configure RSTP/STP on ports.
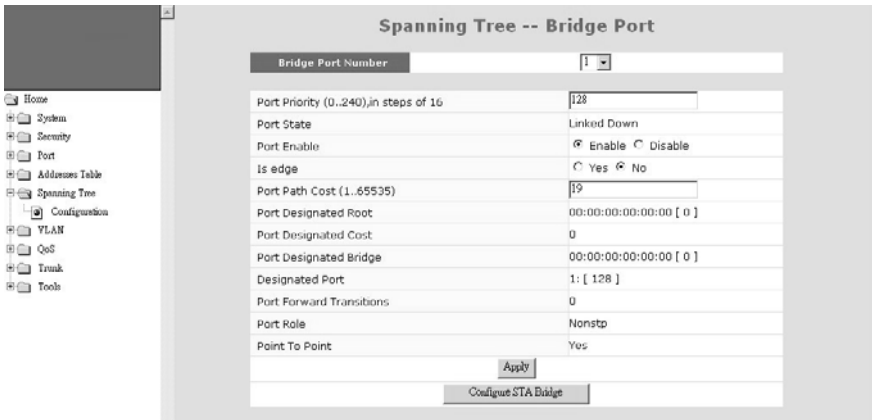
Bridge Port Number is the Ethernet port that will be configured.

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 fast connections. Higher values will be blocked and should be assigned to ports with slow 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 will show the root bridge ID of this segment and its bridge priority.

Port Designated Cost : This will show the path cost between the root port and the designated port of the root bridge.

Port Designated Bridge : This will show the switch's bridge ID and its bridge priority setting.

Designated Port : This will show 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.
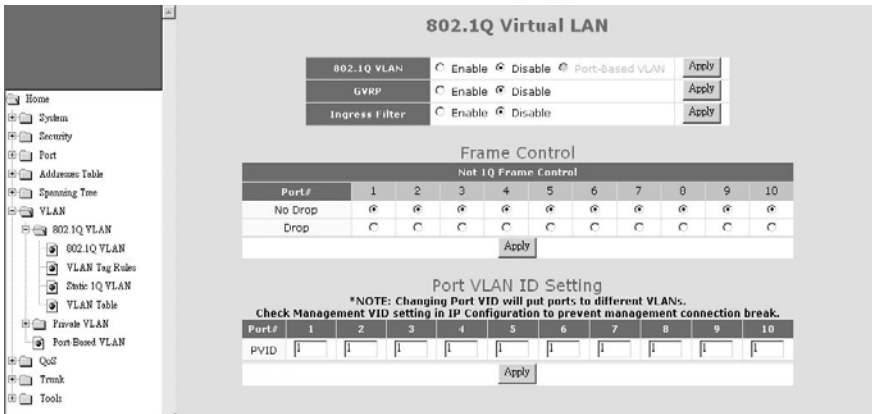
Point To Point : This is a Point-to-Point link on the port.

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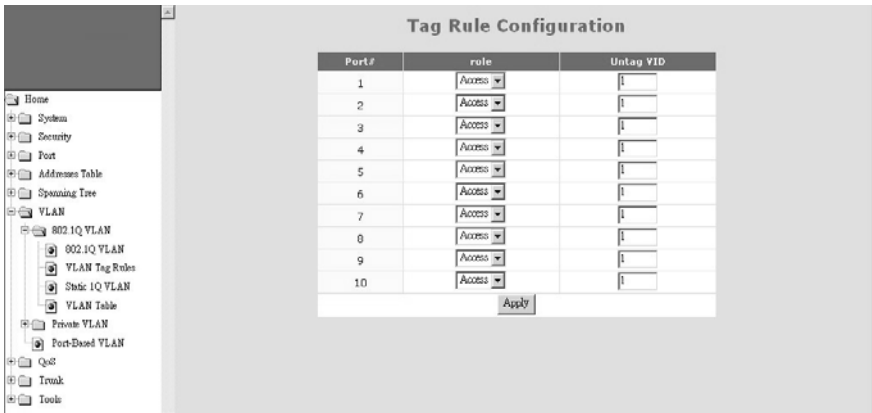
[Frame Control]
This function could be used to drop non-802.1Q frames (untagged packets).

[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

Tag Rule Configuration

Port#	role	Untag VID
1	Access ▾	1
2	Access ▾	1
3	Access ▾	1
4	Access ▾	1
5	Access ▾	1
6	Access ▾	1
7	Access ▾	1
8	Access ▾	1
9	Access ▾	1
10	Access ▾	1

Apply

Navigation menu:
- Home
- System
- Security
- Port
- Addresses Table
- Spanning Tree
- VLAN
  - 802.1Q VLAN
    - 802.1Q VLAN
    - VLAN Tag Rules
    - Static 1Q VLAN
    - VLAN Table
  - Private VLAN
  - Port-Based VLAN
- QoS
- Trunk
- Tools

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.

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). Static 1Q VLAN
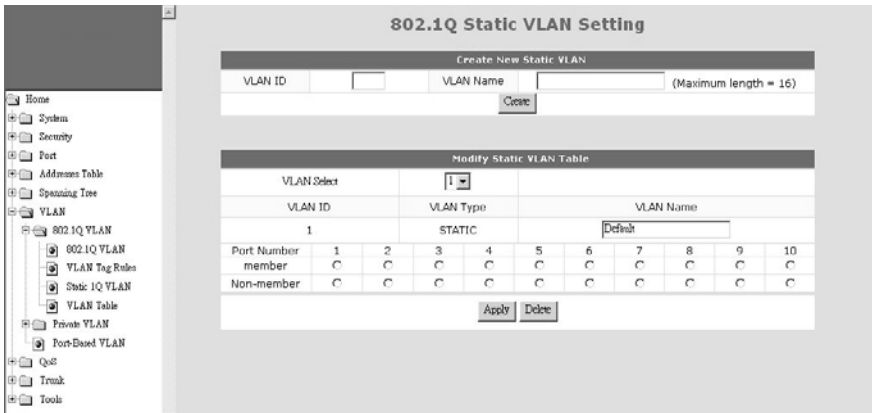
This function is used to maintain 802.1Q static VLAN.

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.

1-4). VLAN Table

Active 802.1Q VLAN Table

| Total page : 1 | Current page : 1 | Go to page : [ ] Apply | Previous Page | Next Page |

VID	VLAN Type	Name	1	2	3	4	5	6	7	8	9	10
1	Static	Default	S	S	S	S	S	S	S	S	S	S

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 VLAN configuration.
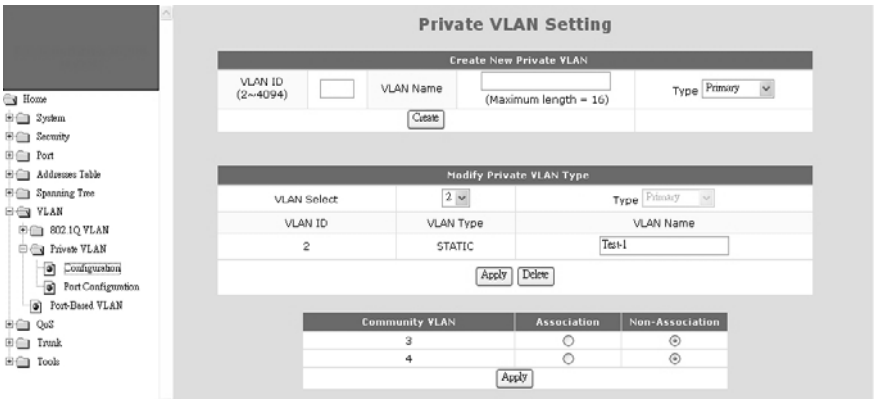
2-1). Configuration
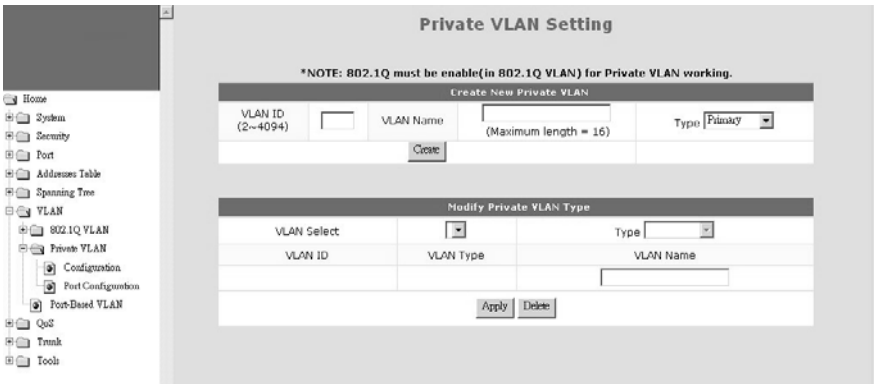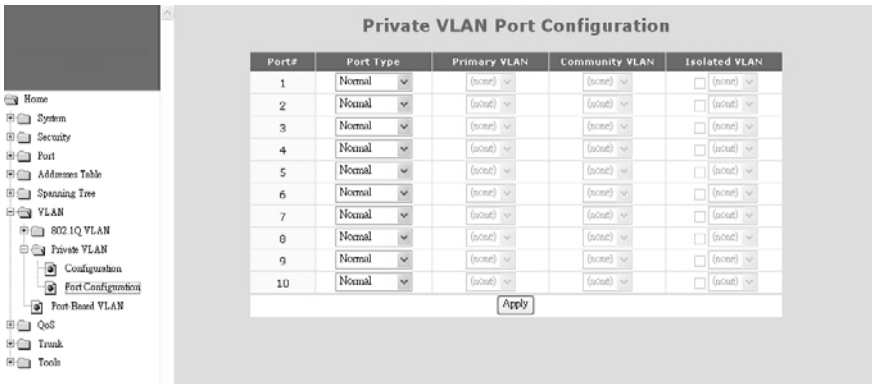
Creating Private VLAN, do the steps first.
a. Create VLAN groups, and define as "Primary", "Community", or "Isolated".
b. Associate Community VLAN with Primary VLAN.   If more than one Primary
    VLAN, select Primary VLAN first and then do the association.

See the following picture.

2-2). Port Configuration
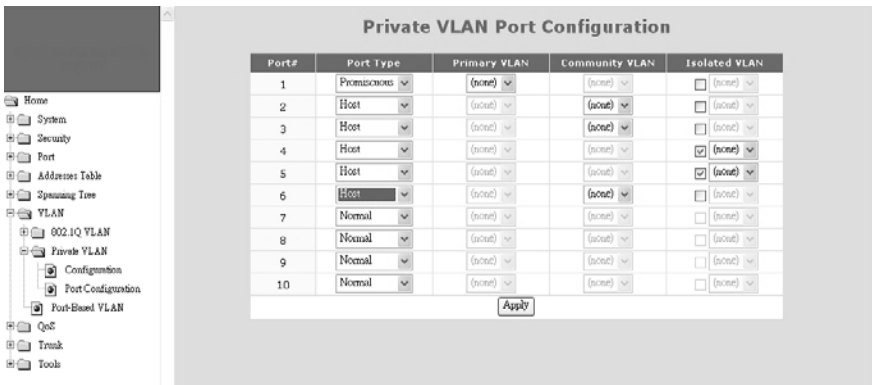
After VLANs are created, assign ports to VLANs.

Private VLAN Port Configuration

Port#	Port Type	Primary VLAN	Community VLAN	Isolated VLAN
1	Normal	(none)	(none)	☐ (none)
2	Normal	(none)	(none)	☐ (none)
3	Normal	(none)	(none)	☐ (none)
4	Normal	(none)	(none)	☐ (none)
5	Normal	(none)	(none)	☐ (none)
6	Normal	(none)	(none)	☐ (none)
7	Normal	(none)	(none)	☐ (none)
8	Normal	(none)	(none)	☐ (none)
9	Normal	(none)	(none)	☐ (none)
10	Normal	(none)	(none)	☐ (none)

[Apply]

There are three types for a port - Normal, Host, and Promiscuous.
"Normal" is for ports doing normal operation instead of Private VLAN.
"Host" is for ports that could be in Community VLAN or Isolated VLAN.
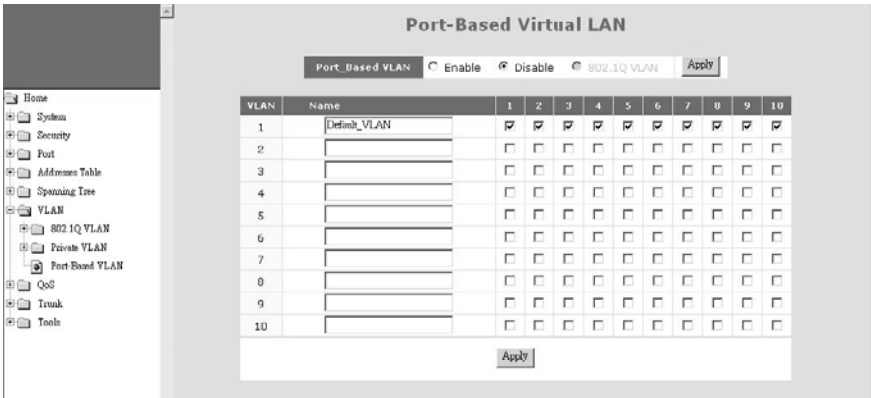"Promiscuous" is for ports that could be in Primary VLAN or Isolated VLAN.

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.
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.

Private VLAN Port Configuration

Port#	Port Type	Primary VLAN	Community VLAN	Isolated VLAN
1	Promiscuous	(none)	(none)	☐ (none)
2	Host	(none)	(none)	☐ (none)
3	Host	(none)	(none)	☐ (none)
4	Host	(none)	(none)	☑ (none)
5	Host	(none)	(none)	☑ (none)
6	Host	(none)	(none)	☐ (none)
7	Normal	(none)	(none)	☐ (none)
8	Normal	(none)	(none)	☐ (none)
9	Normal	(none)	(none)	☐ (none)
10	Normal	(none)	(none)	☐ (none)

[Apply]

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.

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 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.
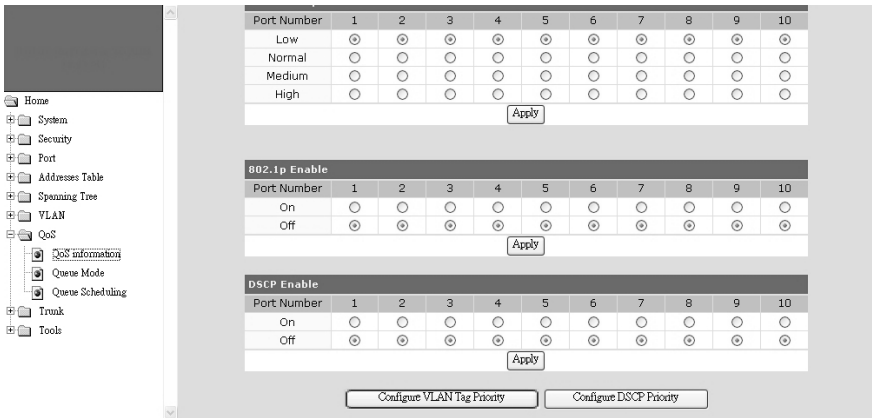**802.1P Enable** : this is for 802.1P priority operation enable/diable on each port. 802.1P priority operation will use the priority setting in tag of packets for QoS operation.
The mapping of 802.1P priority values (0~7) to priority queue could be defined at "VLAN Tag Priority" page by clicking [Configure VLAN Tag Priority] button.
**DSCP Enable** : (see the following picture) 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.
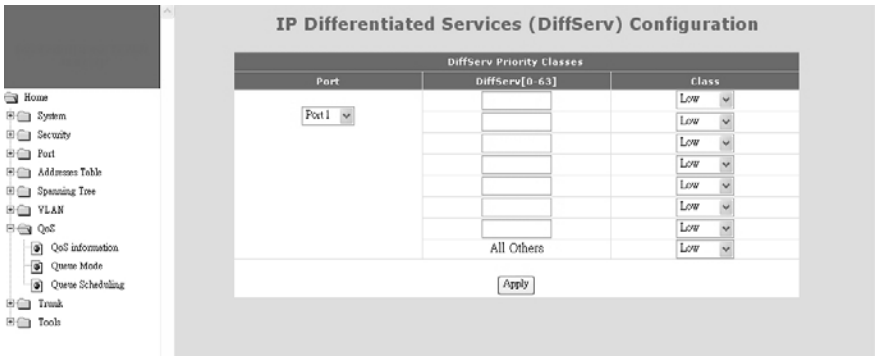
[802.1P Priority Mapping]
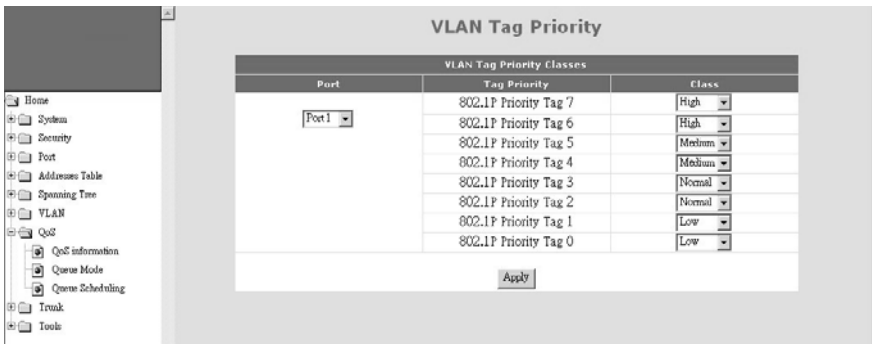
For 802.1P priority, priority value (0~7) in VLAN tag will be used for QoS operation. And the mapping of priority values to priority queues (High/Middle /Normal/Low) could be defined here.

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

[DiffServ Priority Mapping]

IP Differentiated Services (DiffServ) Configuration

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).

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".

90

3). Queue Scheduling
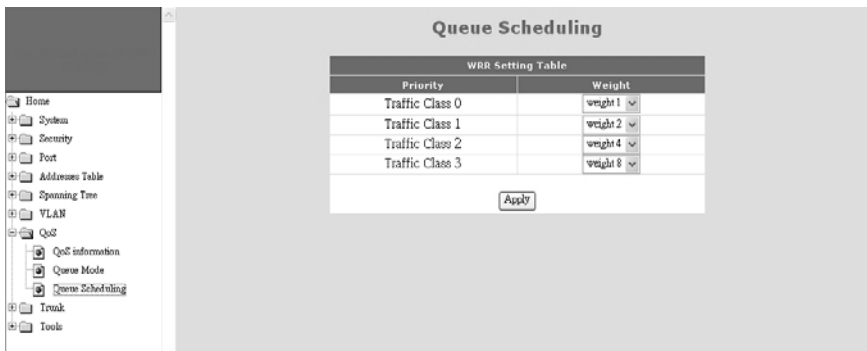
This function is used to configured the weight of priority queues for WRR operation. And the output bandwidth will be shared with the ratio of weight between priority queues.

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.

[IGMP Configuration]
IGMP Status: this is used to enable/disable IGMP function.
IGMP Querying: this is used to enable/disable IGMP Query function. The 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 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 a 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.

[IP Multicast Registration Table]
This table will show the learned IP multicast groups.

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
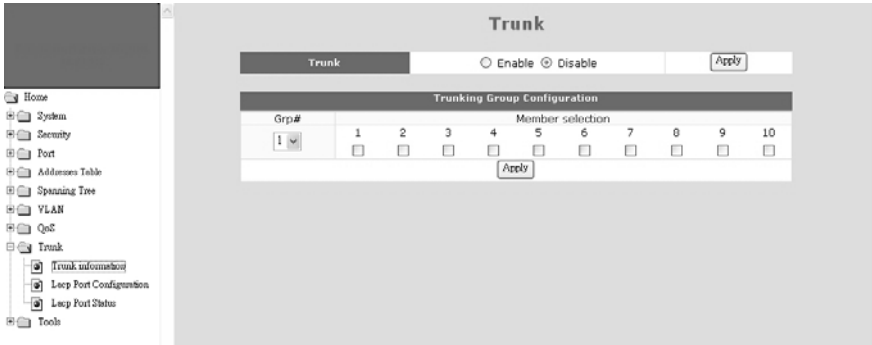
This table is used to assign ports to Trunk groups statically.

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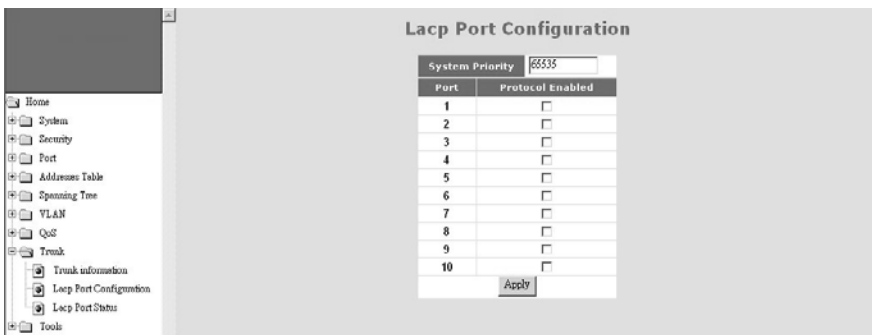
This page is used to configure LACP function.   With LACP protocol, switches can learn trunk connections automatically.

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 numbers have 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.   And the port number and port key of the partner switch will also be shown in the table when LACP Trunk is running.

0	Forwarding	Port link up and forwarding by RSTP. Number is Partner port number if other switch has LACP enabled	

Home
System
Security
Port
Addresses Table
Spanning Tree
VLAN
QoS
Trunk
   Trunk information
   Lacp Port Configuration
   Lacp Port Status
Tools

Refresh

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		

96

6.4.11 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.
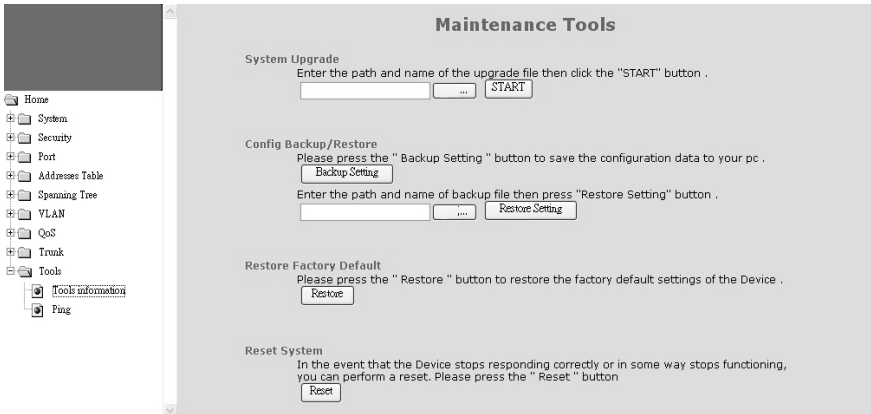
System Upgrade : This function will upgrade the system operation software from the web management PC.
Config Backup/Restore : Clicking [Backup Setting] button, the switch can backup the configuration of the switch to the web management PC.
And the configuration of the switch can be restored to switch by [Restore Setting] 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

Ping Parameters

Target IP address	
Count	1 ⌄
Time Out (in secs)	1 ⌄
	Apply

Ping Results	
Target IP address	0.0.0.0
Status	ping completed
Received replies	0
Request timeouts	0
Average Response Time (in ms)	0
	Refresh Stop

Home
System
Security
Port
Addresses Table
Spanning Tree
VLAN
QoS
Trunk
Tools
    Tools information
    Ping
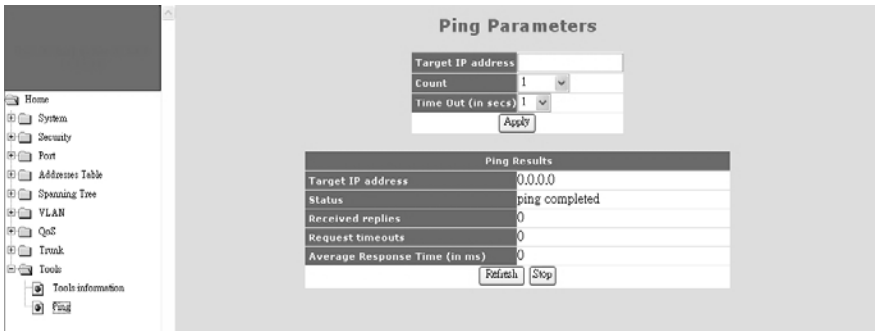
This function is used to ping network devices from the switch.   It can be used to verify network connection.

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 6.4.11.

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

A. Product Specifications

[8TX+2SFP Model]

Access Method   Ethernet, CSMA/CD
Standards Conformance   IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE
                             IEEE 802.3z, IEEE 802.3ab (1000Base)
Communication Rate   10/100/1000Mbps,
                             Full / Half duplex (auto-negotiation)
MDI/MDIX   Auto-detect for each TX port
Indicator Panel   LEDs for each unit : Power, System
                                         each port : Link/Act(Green:1000M,
                                             Yellow:10/100M), FDX/Col.
Number of Ports   8* RJ45 TX, 2* SFP ports (10 GE Ports totally)
Dimensions   250 x 117 x 37 mm
Certification   CE Mark, FCC Class A
Temperature   Standard Operating: 0 to 50℃
Humidity   10% to 90% (Non-condensing)

Bridging Function   Filtering, forwarding and learning
Switching Method   Store-and-forward
Address Table   8K entries
Filtering/Forwarding Rate Line speed
Maximum Packet Size   9600 Bytes
Flow Control   802.3x for full duplex, backpressure for half duplex

VLAN   802.1Q VLAN, Port-based VLAN, Private VLAN
QoS   4 transmit priorities per ports, for port-based/802.1P
                             tagged-based/DSCP priority operation
Spanning Tree   Support RSTP/STP protocol
Trunking   8 groups max., Static and LACP are supported
Mirror Port   Yes
IGMP Snooping   Yes, for IP multicast traffic
Mac ID Security on Port Static Mac address access limit on port,
                             and Dynamic Mac address number limit on port
802.1x   Yes, support Authentication and Transparent modes
Rate Control   Yes, 128Kbps~1000Mbps, for ingress/egress traffic
Storm Control   Broadcast, Multicast, and Unicast Storm Control
Admin Manage Security   Yes, by IP/Subnet/Interface limit
System Time   Yes, by NTP protocol
System Log   Yes, Local and Remote (by syslog) logging
Out-band Management   Console
In-band Management   http, telnet, and SNMP
SNMP   v1 and v2c agent, support MIB-II,Bridge MIB,802.1Q
                             MIB and Private MIB
Software Update/Backup by http,TFTP protocols, Xmodem, for firmware/
                             configuration

[16TX+4SFP Model]

Access Method	Ethernet, CSMA/CD
Standards Conformance	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE
	IEEE 802.3z, IEEE 802.3ab (1000Base)
Communication Rate	10/100/1000Mbps,
	Full / Half duplex (auto-negotiation)
MDI/MDIX	Auto-detect for each TX port
Indicator Panel	LEDs for each unit : Power, System
	each port : Link/Act(Green:1000M,
	Yellow:10/100M), FDX/Col.
Number of Ports	16* RJ45 TX, 4* SFP(shared)　ports (16 GE Ports
	totally)
Dimensions	330 x 204 x 43 mm
Certification	CE Mark, FCC Class A
Temperature	Standard Operating: 0 to 50℃
Humidity	10% to 90% (Non-condensing)
Bridging Function	Filtering, forwarding and learning
Switching Method	Store-and-forward
Address Table	8K entries
Filtering/Forwarding Rate	Line speed
Maximum Packet Size	9600 Bytes
Flow Control	802.3x for full duplex, backpressure for half duplex
VLAN	802.1Q VLAN, Port-based VLAN, Private VLAN
QoS	4 transmit priorities per ports, for port-based/802.1P
	tagged-based/DSCP priority operation
Spanning Tree	Support RSTP/STP protocol
Trunking	8 groups max., Static and LACP are supported
Mirror Port	Yes
IGMP Snooping	Yes, for IP multicast traffic
Mac ID Security on Port	Static Mac address access limit on port,
	and Dynamic Mac address number limit on port
802.1x	Yes, support Authentication and Transparent modes
Rate Control	Yes, 128Kbps~1000Mbps, for ingress/egress traffic
Storm Control	Broadcast, Multicast, and Unicast Storm Control
Admin Manage Security	Yes, by IP/Subnet/Interface limit
System Time	Yes, by NTP protocol
System Log	Yes, Local and Remote (by syslog) logging
Out-band Management	Console
In-band Management	http, telnet, and SNMP
SNMP	v1 and v2c agent, support MIB-II,Bridge MIB,802.1Q
	MIB and Private MIB
Software Update/Backup	by http,TFTP protocols, Xmodem, for firmware/
	configuration

[24TX+4SFP Model]

Access Method	Ethernet, CSMA/CD
Standards Conformance	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE IEEE 802.3z, IEEE 802.3ab (1000Base)
Communication Rate	10/100/1000Mbps, Full / Half duplex (auto-negotiation)
MDI/MDIX	Auto-detect for each TX port
Indicator Panel	LEDs for each unit : Power, System each port : Link/Act(Green:1000M, Yellow:10/100M), FDX/Col.
Number of Ports	24* RJ45 TX, 4* SFP(shared) ports (24 GE Ports totally)
Dimensions	440 x 172 x 43 mm
Certification	CE Mark, FCC Class A
Temperature	Standard Operating: 0 to 50℃
Humidity	10% to 90% (Non-condensing)
Bridging Function	Filtering, forwarding and learning
Switching Method	Store-and-forward
Address Table	8K entries
Filtering/Forwarding Rate	Line speed
Maximum Packet Size	9600 Bytes
Flow Control	802.3x for full duplex, backpressure for half duplex
VLAN	802.1Q VLAN, Port-based VLAN, Private VLAN
QoS	4 transmit priorities per ports, for port-based/802.1P tagged-based/DSCP priority operation
Spanning Tree	Support RSTP/STP protocol
Trunking	8 groups max., Static and LACP are supported
Mirror Port	Yes
IGMP Snooping	Yes, for IP multicast traffic
Mac ID Security on Port	Static Mac address access limit on port, and Dynamic Mac address number limit on port
802.1x	Yes, support Authentication and Transparent modes
Rate Control	Yes, 128Kbps~1000Mbps, for ingress/egress traffic
Storm Control	Broadcast, Multicast, and Unicast Storm Control
Admin Manage Security	Yes, by IP/Subnet/Interface limit
System Time	Yes, by NTP protocol
System Log	Yes, Local and Remote (by syslog) logging
Out-band Management	Console
In-band Management	http, telnet, and SNMP
SNMP	v1 and v2c agent, support MIB-II,Bridge MIB,802.1Q MIB and Private MIB
Software Update/Backup	by http,TFTP protocols, Xmodem, for firmware/ configuration

103

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 73/23/EEC and the EMC Directive 89/336/EEC.

Warning! Do not plug a phone jack connector in 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.