Intelligent Switch
User's Manual

Rev.06

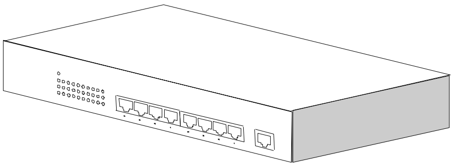
We make no warranties with respect to this documentation and disclaim any implied warranties of merchantability, quality, or fitness for any particular purpose. The information in this document is subject to change without notice. We reserve the right to make revisions to this publication without obligation to notify any person or entity of any such changes.

About this manual …

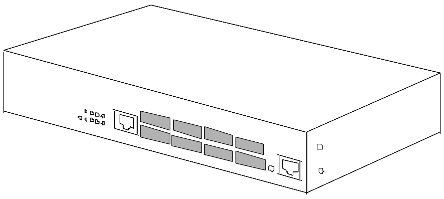
This manual is a general manual for different models of our Intelligent Switch. They are similar in operation but have different hardware configurations.

These models are

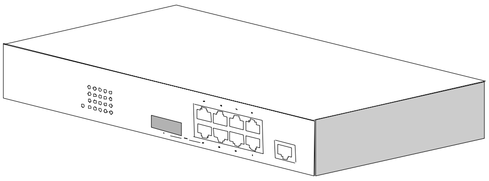
1. **8 * UTP ports model**
   This model supports eight UTP ports for Ethernet connections.



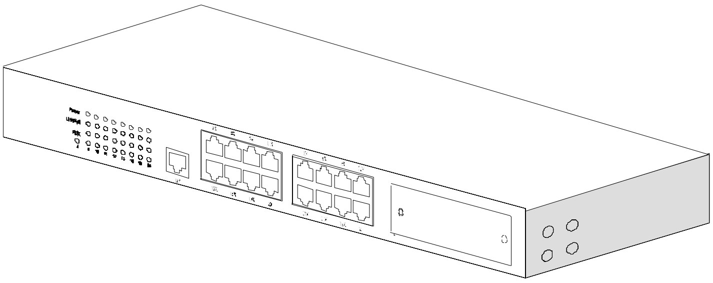
2. **8 * 100FX ports model**
   This model supports eight 100FX ports for Ethernet fiber-optic connections. Port 8 of 100FX ports could be switched to a UTP port by a push-button.



3. **7 * UTP + 1 * 100FX ports model**
   This model supports seven UTP ports and one 100FX port. Port 1 is the 100FX port, but it could be a UTP port depending on which connector (100FX or UTP) is selected.

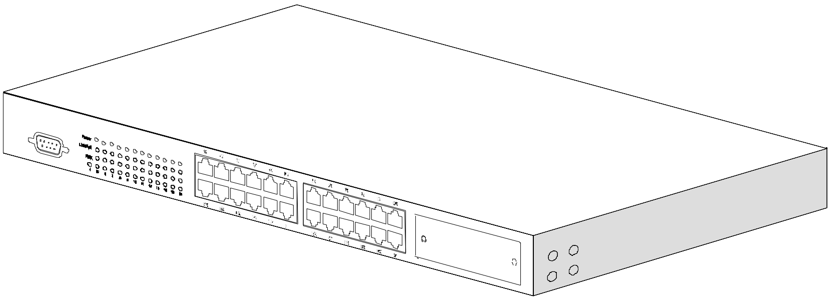


4. **16 * UTP + 1 * module ports model**
   This model supports sixteen UTP ports and one module slot. If a 100FX module is inserted to the slot, which is Port 17 for 100FX connection.



5. **24 * UTP + 1 * module ports model**

   This model supports twenty-four UTP ports and one module slot. If a 100FX module is inserted to the slot, which is Port 25(, 26 if two-100FX module) for 100FX connection.



Contents

1. INTRODUCTION 1

1.1 PACKAGE CONTENTS..1

2. WHERE TO PLACE THE INTELLIGENT SWITCH..2

3. CONFIGURE NETWORK CONNECTION..3

3.1 CONNECTING DEVICES TO THE INTELLIGENT SWITCH 3
3.2 CONNECTING TO ANOTHER ETHERNET SWITCH/HUB 3
3.3 APPLICATION 4

4. ADDING MODULE 5

4.1 ADDING 100BASEFX MODULE FOR 16+1FX/24+2FX MODEL............................5

5. LEDS CONDITIONS DEFINITION 6

5.1 LEDS DEFINED...6

6. MANAGE / CONFIGURE THE SWITCH 7

6.1 INTRODUCTION OF THE MANAGEMENT FUNCTIONS...7
6.2 MANAGEMENT WITH CONSOLE CONNECTION 10
6.3 MANAGEMENT WITH HTTP CONNECTION...43
6.4 ABOUT TELNET INTERFACE 73
6.5 ABOUT SNMP INTERFACE 73

7. SOFTWARE UPDATE AND BACKUP..74

A. PRODUCT SPECIFICATIONS..75

B. COMPLIANCES..80

C. WARRANTY 81

1. Introduction

There are five models for the Intelligent Switch Series – 8 UTP ports model, 8 100FX ports model, 7 UTP + 1 100FX ports model, 16 UTP + 1 100BaseFX (module) ports model and 24 UTP + 2 100BaseFX (module) ports model. This Intelligent switch is a Layer2 management switch with lots of advanced network functions including VLAN, trunking, spanning tree, mirror port, IP multicast, rate limit and port configuration. It supports console, telnet, http and SNMP interface 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

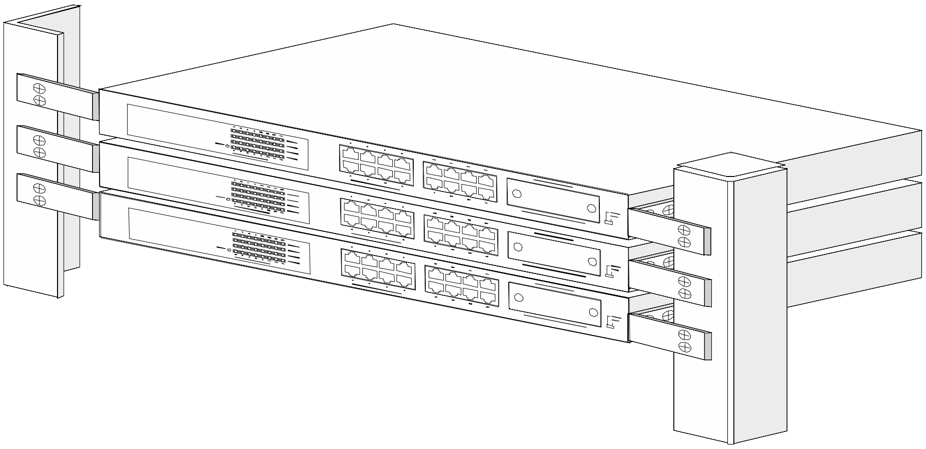
- One Intelligent Switch
- One AC power cord (* for AC power model)
- One console cable
- Two rack-mount kits and screws (*for 16+1FX/24+2FX model only)
- This user's manual

2. Where To Place the Intelligent Switch

This Intelligent Switch can be placed on a flat surface (your desk, shelf or table). Place the Intelligent 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 16+1FX/24+2FX model, you can also install this Intelligent switch on a 19" rack with the rack-mount kits as the picture.

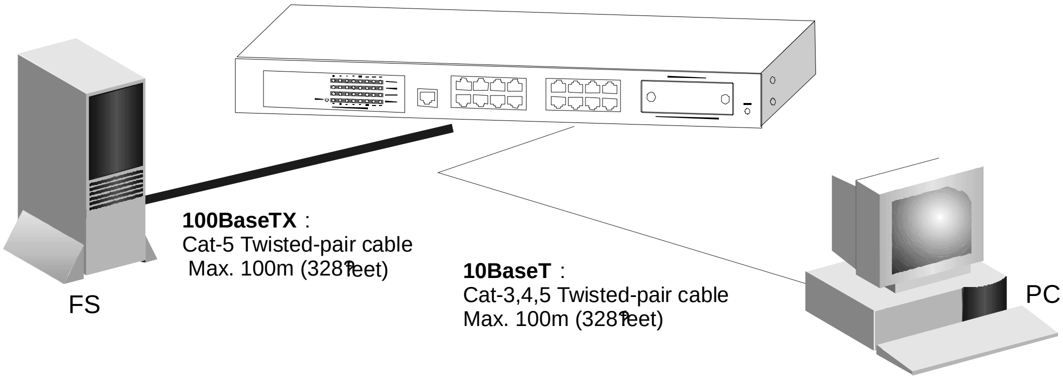


3. Configure Network Connection

3.1 Connecting Devices to the Intelligent Switch

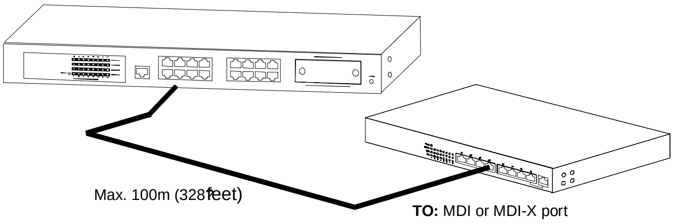
[Connection Guidelines:]

- For 10BaseT connection : Category 3 or 5 twisted-pair Ethernet cable
- For 100BaseTX connection : Category 5 twisted-pair Ethernet cable
- For UTP cable connection, always limit the cable distance to 100 meters (328 ft) as defined by IEEE specification
- For 100BaseFX port, you can connect long distance fiber optic cable to the switch (depending on the 100FX connector type).
- Because this switch supports **Auto MDI/MDI-X** detection on each UTP port, you can use normal straight through cable for both workstation connection and hub/switch cascading.



3.2 Connecting to Another Ethernet Switch/Hub

This Intelligent Switch can be connected to existing 10 Mbps or 100 Mbps hubs/switches. Because all UTP ports on the Intelligent Switch support Auto MDI/MDI-X function, you can connect from any UTP port of the Intelligent Switch to the MDI or MDI-X port of another hub/switch with Straight Through or Crossover cables.

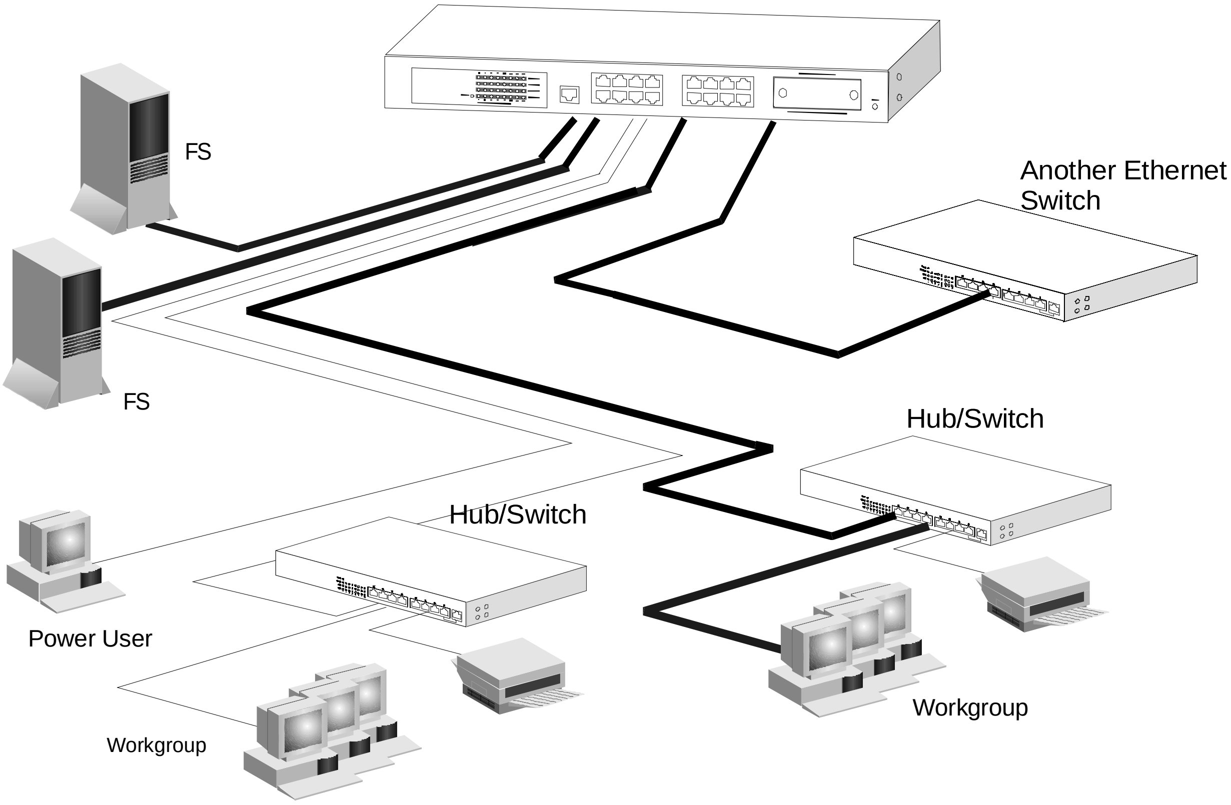


3.3 Application

A switch can be used to overcome the hub-to-hub connectivity limitations as well as improve overall network performance. Switches make intelligent decisions about where to send network traffic based on the destination address of the packet. As a result, the switch can significantly reduce unnecessary traffic.

The example below demonstrates the switch ability to segment the network. The number of nodes on each segment is reduced thereby minimizing network contention (collisions) and boosting the available bandwidth per port.

With management function of the switch, network administrator is easy to monitor network status and configure for different applications.

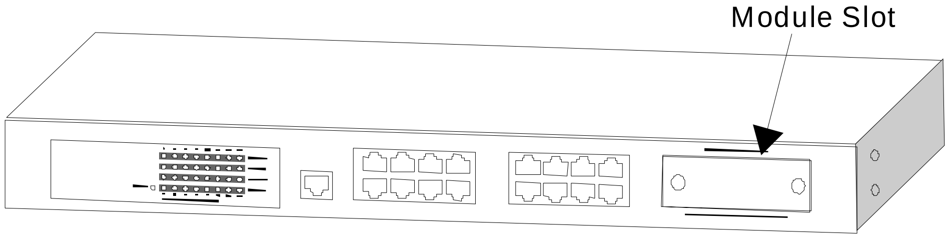


4. Adding Module

4.1 Adding 100BaseFX Module for 16+1FX/24+2FX model

The 16+1FX/24+2FX model has a module slot for 100BaseFX-connection extension at front panel. You can add a 100BaseFX module to the switch and this switch gets one 100BaseFX port (Port 17/25) for long distance fiber optic cable connection. (For 24+2FX model, the module could have one or two 100FX ports with different modules and the FX port will be Port 25/26.)

Note: This switch does not support hot-swap function. Turn off the power first before adding or removing module. Otherwise, the switch and module could be damaged.



Please follow the steps to add the module to the switch.

1. Turn off the switch first.
2. Loosen the screws of slot cover and remove the cover from the module slot.
3. Slide in the module into the module slot.
4. Tighten the screws of the module to the switch.
5. Connect the fiber optic cable to the FX port of the module.
6. Power on the switch.
7. Check Port 17/25(,26) configuration from Console, Telnet or Web interface. It should be 100Mbps, full duplex.

5. LEDs Conditions Definition

5.1 LEDs Defined

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

[For 8*UTP ports model]

LED	STATUS	CONDITION
Power	ON	Switch is receiving power.
Link / Act	ON	Port has established a valid link.
	Flashing	Data packets being received or sent.
100M	ON	The connection is 100Mbps.
	OFF	The connection is 10Mbps.
	ON	The connection is Full Duplex.
		The connection is Half Duplex.

[For 8*100FX ports model]

LED	STATUS	CONDITION
Power	ON	Switch is receiving power.
Link / Act	ON	Port has established a valid link.
	Flashing	Data packets being received or sent.

[For 7+1FX / 16+1FX / 24+2FX ports model]

LED	STATUS	CONDITION
Power	ON	Switch is receiving power.
Link / Act	ON	Port has established a valid link.
	Flashing	Data packets being received or sent.
	Green	The connection speed is 100Mbps.
	Yellow	The connection speed is 10Mbps.
	ON	The connection is Full Duplex.
		The connection is Half Duplex.

6. Manage / Configure the switch

6.1 Introduction of the management functions

This switch is a L2 management switch. It supports in-band management function from SNMP, Http and Telnet interface. It also supports out-band management function from RS232 console interface. Besides, 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. 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.
   This switch supports trunk function and users can configure it with the following steps.
   a. Enable trunk function.
   b. Select the port partition for trunk.
   c. Assign ports to a trunk. For example, assign Port 1,2,3 for Trunk 1.

   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 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 could copy packets from some monitored port to another port for network monitor. This switch also provides Ethernet ID (Mac address) filtering function for monitoring the traffic to/from some user.

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 ToS/DiffServ for IP packets. User can define the mapping (0 – 7) to the four 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 for 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 or rejected 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 or rejected from Port 5 - depending on the setting of its port security mode.

<u>Note</u>: About Static Mac Address Filter-in (port binding) function
There is a "Mac Security Configuration" function for port security mode. If it is set to Accept mode, 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 6.2 / 6.3 for the details of the Mac address filter-in operation of the switch.

7. IEEE 802.1x Port Security Function
If the 802.1x function is enabled, the switch will act as an authenticator for users accessing network through the switch. It will need a RADIUS server for the authentication function. Users will be asked for username and password

before network access. If the RADIUS server authenticates it, the switch will enable the port for network access. This function is very useful for network security application to prevent illegal users access network through the switch. This switch supports MD5, TLS and PEAP authentication types.

8. Rate Control
   This function can limit the burst traffic rate for physical ports. The traffic could be ingress traffic or egress traffic. This function can limit the network bandwidth usage by different users.

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

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

11. Software Backup/Update
    This switch supports backup and update functions for its internal software and its network configuration. It could be done in three ways.

    a. From console when booting : doing by Xmodem protocol and by terminal program for boot code and run-time code updating.

    b. From console/Telnet when running : doing by TFTP protocol and it will need a TFTP server in network for run-time code and configuration backup/update.

    c. From web browser : doing by http protocol and by web browser for run-time code and configuration backup/update.

6.2 Management with Console Connection

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 **[38400,8,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 1.04.02, built at 10:57:19, Dec 30 2005

RAM: 0x00000000-0x00800000, 0x0000cc78-0x007f3000 available
FLASH: 0x05800000 - 0x05900000, 16 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       : Intelligent Switch
MAC Address      : 00:11:22:64:80:5A
Firmware Version : 2.11.14

Press <ENTER> key to start.
UCD-SNMP version 4.1.2
----------------------------------------------------------------------------------------------------
```

Press Enter key, user name and password will be requested. The default user name and password is "**admin**" / ”**123456**”.

After login the switch, a prompt will be shown. Because this switch supports command-line for console interface, you can press “**?**” or “**help**” to check the command list first.

Note: Management with **Telnet** connection has the same interface as console connection.

With **help** command, you can find the command list as follow.

```
----------------------------------------------------------------------------------------------------
>help
[Command List]
?............. Help commands
backup......... backup run-time firmware or configuration file
del........... Del commands
find.......... Find commands
exit.......... Logout
help.......... Help commands
logout......... Logout
ping.......... Ping a specified host with IP address
reset.......... Reset system or reset factory default setting
set........... Set commands
show.......... Show commands
upgrade........ Upgrade run-time firmware or configuration file
>
----------------------------------------------------------------------------------------------------
```

Here is the detail about these commands.

1. **Backup** command

   This switch supports TFTP protocol for firmware and configuration update and backup. You should select backup *firmware* or *configuration* first. And provide the IP address of the TFTP server and the backup file name for the backup operation.

   Enter "backup" at the prompt, the command syntax will be shown.

   ```
   >backup
   Syntax: backup [firmware | config] ip filename
   ```

   For example, "back config 192.168.1.80 abcd" will backup the configuration to TFTP server 192.168.1.80 and its file name is "abcd".

2. **Del** command

   The "del" command can delete static entries in ARL table, disable Mirror function, remove ports in a trunk group, and remove forwarding ports for trunk port.

   Enter "del" at the prompt, the command syntax will be shown.

   ```
   >del
   [Command List]
   ?............. Help commands
   help.......... Help commands
   arl........... Delete a specified MAC address from ARL table
   mirror......... Disable mirror and delete mirror capture port
   trunk.......... Destroy a specified trunk group
   1qvlan......... Destroy a specified VLAN
   ```

- *Delete static entries in ARL table . . .*

```
>del arl
Del ARL [xx-xx-xx-xx-xx-xx] [port#]
```

xx-xx-xx-xx-xx-xx is an assigned static Mac ID in ARL table of the switch. You can remove it from the table with the command. For example, “del arl 00-11-22-33-44-55 3” will delete the Port 3 static Mac ID “00-11-22-33-44-55” from ARL table.

- *Disable Mirror function . . .*

```
>del mirror
Disable mirror function
```

- *Remove All Ports in a Trunk Group . . .*

```
>del trunk
Syntax: Del TRUNK [trunk#]
```

[trunk#] is the trunk group number and all the trunk ports in this trunk will be removed by this command. For example,”del trunk 3” will remove all trunk ports from Trunk 3 and Trunk 3 becomes a null trunk.

- *Delete a 802.1Q VLAN . . .*

```
>del 1qvlan
Syntax: del 1qvlan Vid
```

This command will delete the 802.1Q VLAN with the VLAN ID. For example, “del 1qvlan 5” will delete the 802.1Q VLAN with VLAN ID 5.

3. **Find** command

The “find” command can find a Mac address in the ARL table.

Enter “find” at the prompt, the command syntax will be shown.

```
>find
[Command List]
?.............. Help commands
help........... Help commands
arl............ Search a specified MAC address in ARL table
```

The syntax is as follow.

```
>find arl
Find ARL [xx-xx-xx-xx-xx-xx]
```

If the Mac address is in ARL table, it will be shown as follow.

```
>find arl 00-00-e2-11-22-33
```

```
This MAC [00-00-e2-11-22-33] is DYNAMIC in port [2]!
```

If the Mac address is not in ARL table, it will be shown as follow.

```
>find arl 00-00-e2-77-88-99
Failed!
```

Note: "Dynamic" means the Mac address could be dynamic learning and aging by the switch. "Static" means the Mac address is fixed in ARL table.

4. **Exit** command

   This is a logout command – the same as Logout command.

5. **Help** command

   This is a help command (the same as "?" command) and the switch will prompt command list for this command.

6. **Logout** command

   This is a logout command – the same as Exit command.

7. **Ping** command

   User can use this command to ping another network device to verify the network connection and activity. (It is similar to the ping command in MS-DOS.)

   Enter "ping" at the prompt, the command syntax will be shown.

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

   For example, "ping 192.168.1.80". "Ctrl-C" can be used to break continuous ping operation.

8. **Reset** command

   This command can be used to reset switch or restore factory default setting.

   Enter "reset" at the prompt, the command syntax will be shown.

   ```
   >reset
   Syntax: reset [configuration | system]
   ```

   "reset configuration" will restore the configuration to the factory default setting.
   "reset system" will reset the switch and the switch will reboot.

9. **Set** command

   This command can be used to configure most functions of the switch. Lots of sub-commands are needed for this command.

Enter “set” at the prompt, the sub-command list will be shown.

```
>set
[Command List]
?.............. Help commands
help........... Help commands
admin.......... Set administrator name and password
arl............ Add a static MAC address in ARL table
eth0........... Set network eth0 configuration
idle........... Set idle time for CLI session.
igmp........... Set IGMP configuration
mirror......... Set mirror configuration
mvr............ Set MVR function
age............ Set switch age
automode....... Set Auto Negotiation or Auto Detect mode
loopback....... Set Loopback Detection
mgr............ Set management IP configuration
port........... Set switch port configuration
qos............ Set QoS configuration
snmp........... Set snmp configuration
trunk.......... Set a port to join/leave a specified Trunk Group
sta............ Set Spanning Tree setting
http........... Set HTTP Protocol setting
gvrp........... Set GVRP Protocol setting
1qvlan......... Set 802.1q VLAN Configuration
dot1x.......... Set 802.1x Configuration
security....... Set MAC Security Configuration
ratecontrol.... Set Rate Control Configuration
stormcontrol... Set Storm Control Configuration
telnet......... Set TELNET Protocol setting
```

9.1 **set ?** and **set help** command

These two commands will show the sub-command list for set command.

9.2 **set admin** command

This command can be used to modify the user name and password for administrator.

9.3 **set arl** command

This command is for adding static Mac ID to ARL table of the switch.

Its syntax is . . .

```
>set arl
Set ARL [xx-xx-xx-xx-xx-xx] [port#]
```

For example, “set ARL 00-00-01-11-22-33 5” will add a static Mac ID “00-00-01-11-22-33” to ARL table for Port 5 and this Mac ID will never be aged out from Port 5.

Note: Because the static Mac address is fixed on the assigned port by the switch, the static Mac address can access network through the assigned port only. It will fail to access network through other ports of the switch.

9.4 **set eth0** command

This command is used to configure IP address of the switch.

Its syntax is . . .

```
>set eth0
[Syntax]set eth0 [arg_1 data_1] [arg_1 data_1] ... [arg_n data_n]
[Argument List]
dhcp........... Set DHCP client
ip............. Set IP Address
netmask........ Set netmask
gateway........ Set gateway IP address
```

This switch supports DHCP client function. If you set DHCP enable, it will try to get IP configuration from DHCP server when it boots up. You can use "show net" command to check the DHCP setting and current IP configuration of the switch. If DHCP is enable and the switch cannot find a DHCP server in the network, a message "*BOOTP/DHCP failed on eth0*" will be shown and it will use "192.168.1.5 / 255.255.255.0" as its IP configuration.

If you set DHCP disable, you can set the IP configuration with *ip*, *netmask* and *gateway* commands. For example, "set eth0 ip 192.168.1.250 netmask 255.255.255.0 gateway 192.168.1.154" will set these parameters as the IP address configuration of the switch. After the command, you can use "show net" to verify the setting.

9.5 **set idle** command

This command is used to set idle time for console connection. If no any key operation in this idle time, the switch logout automatically for security.

Its syntax is . . .

```
>set idle
Syntax: Set idle [timeout value]
```

For example, "set idle 300" will change the idle time to 300 seconds. It is 10 minutes default. Its valid range is 30 ~ 3600 seconds.

9.6 **set igmp** command

This command is used to enable/disable IGMP snooping function for IP multicast operation.

Its syntax is . . .

```
>set igmp
[Command List]
enable......... Enable IGMP function
disable........ Disable IGMP function
```

9.7 **set mirror** command

This command is used to configure mirror port function. The following is the sub-command for it.

```
>set mirror
[Command List]
?............. Help commands
help........... Help commands
ingress........ Set mirror ingress setting
egress......... Set mirror egress setting
port........... Set mirror capture port setting
enable......... Enable mirror function
disable........ Disable mirror function
```

9.7.1 **set mirror ?** and **set mirror help** command

This command can show the sub-command list for “set mirror” command.

9.7.2 **set mirror ingress** command

This command is used to configure the mirror operation for ingress traffic. Its syntax is . . .

```
>set mirror ingress
[Syntax]set mirror ingress [arg_1 data_1] [arg_1 data_1] ... [arg_n data_n]
[Argument List]
div............ Set mirror ingress/egress [div=%d]
mode........... Set mirror ingress/egress [mode=ALL/SA/DA]
mac............ Set mirror ingress/egress [mac=xx-xx-xx-xx-xx-xx]
monitor........ Set mirror ingress/egress [monitor=xx,xx,xx]
```

set mirror ingress div x : every x packets, capture one for mirror. For example, “set mirror ingress div 10” will capture one packet from every ten packets from ingress traffic.

set mirror ingress mode xx : mirror all packets or mirror packets with some DA or SA only. For example, “set mirror ingress mode all” will mirror all packets.

set mirror ingress mac xx-xx-xx-xx-xx-xx : if the mirror mode is for the packets with some DA/SA, users can assign the DA/SA here.

set mirror ingress monitor xx,xx,xx : set the monitored ports here. For example, “set mirror ingress monitor 1,2,5” will mirror the ingress traffic from Port 1,2,5. (Notes: If the monitored traffic exceeds the maximum bandwidth of capture port, flow control function will work on these monitored ports.)

9.7.3 **set mirror egress** command

This command is used to configure the mirror operation for egress traffic. Its syntax is similar to the mirror operation for ingress traffic. Please refer to “**set mirror ingress** command” section.

9.7.4 **set mirror port** command

This command is used to set the capture port for mirror operation. For example, “set mirror port 3” will capture the mirror traffic to Port 3.

9.7.5 **set mirror enable** command

This command is used to enable the mirror operation.

9.7.6 **set mirror disable** command

This command is used to disable the mirror operation.

Note: For 24+2FX model, the capture port and the monitored port are suggested in the same port group (Port 1~8, 9~16, 17~24 are three port groups).

9.8 **set mvr** command

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

* Before configuring MVR function, complete the VLAN setting first
* Using MVR function, you have to enable IGMP snooping function first.

This switch supports four MVR VLANs. They are referred as Index 1,2,3,4. For any MVR setting, you have to assign an index in the command. And all the settings will be assigned to the indexed MVR VLAN.

```
>set mvr
Syntax: set mvr [vlan|group] [index#] ....
```

For a MVR VLAN, you have to assign the following settings. (“1” is the index of the MVR VLAN. It could be 1,2,3,4.)

```
>set mvr vlan 1
[Syntax]set mvr vlan [vlan index] [arg_1 data_1] [arg_1 data_1] ... [arg_n data_
n]
[Argument List]
active......... Set mvr vlan # active [1:enable|0:disable]
name........... Set mvr vlan # name [name string]
vid............ Set mvr vlan # vid [vid#]
priority....... Set mvr vlan # priority [priority#]
mode........... Set mvr vlan # mode [1:dynamic|2:compatible]
source......... Set mvr vlan # source [port#] [0:untagged|1:tagged]
receiver....... Set mvr vlan # receiver [+|-] [port#] [0:untagged|1:tagged]
```

active – this MVR VLAN is enabled/disabled.
name – you can assign a name for the MVR VLAN for identification.
vid – this is the VLAN ID for this MVR VLAN. It is 1 ~ 4094.
priority – this is a 802.1P priority (0~7). The IGMP control packets for this VLAN will be assigned this priority when tag is added.

mode – there are two operation modes for this MVR function. One is Dynamic mode. Another is Compatible mode. In Dynamic mode, the switch will send IGMP reports to every MVR source port in the MVR VLAN. In Compatible mode, the switch will not send IGMP reports.
source – this is the uplink port of this MVR VLAN to the IGMP traffic source. It could be tagged port or untagged port.
receiver – this is the ports connecting to subscribers receiving IP multicast traffic in the MVR VLAN.

After the MVR VLAN is configured, you can assign IP multicast groups (video channels) to the MVR VLAN. You can assign more than one IP multicast groups (video channels) to one MVR VLAN. These IP multicast groups (video channels) are referred with an index.

For an IP multicast group for MVR VLAN, you have to assign the following settings. ("1" is the index of the IP multicast group. It could be 1,2,3,4, …)

```
>set mvr group 1
[Syntax]set mvr group [group index] [arg_1 data_1] [arg_1 data_1] ... [arg_n dat
a_n]
[Argument List]
active......... Set mvr group # active [1:enable|0:disable]
index.......... Set mvr group # index [Multicast VLAN index#]
name........... Set mvr group # name [name string]
start.......... Set mvr group # start [xxx.xxx.xxx.xxx]
end............ Set mvr group # end [xxx.xxx.xxx.xxx]
```

active – this IP multicast group is enabled/disabled.
index – this is the MVR VLAN index for this IP multicast group.
name – this is the name for this IP multicast group for identification.
start – this is the start IP multicast address for the IP multicast group.
end – the is the end IP multicast address for the IP multicast group.

After both MVR VLAN and the IP multicast groups are configured, subscribers at the receive ports can receive IP multicast traffic in the IP multicast groups from source port even they are in difference VLANs.

9.9 **set age** command

This command is used to change the aging time of the switch.
Its syntax is . . .

```
>set age
Syntax: set age [time]
```

The aging time is 300 seconds default and its valid range is 0 ~ 65535. If [time] is set to 0, the aging function will be disabled. (Notes: It is different from static Mac ID in ARL table. The connection port is fix for a static Mac ID, but the connection port could be changed for a Mac ID with no aging.)

9.10 **set automode** command

This command is used to set the auto mode function of connection ports. There are two modes for it – an(auto negotiation) and ad(auto detection).

an mode – if the *auto* function of a port is disabled in port configuration, the switch will disable its auto-negotiation function and the Auto-MDIX function of the port is also disabled. That is the real force-mode setting of the port.

ad mode – if the *auto* function of a port is disabled in port configuration, the switch will not disable its auto-negotiation function but just modify its auto-negotiation attribute for the speed/duplex mode setting. And the Auto-MDIX function of the port is still enabled.

If the connected device is *auto-negotiation enabled* and you want to set the speed of the connection (for example, 10M/Half), you can select ad mode. If the connected device is in forced mode (for example, 10M/Half) and it is *auto-negotiation disabled*, you can use an mode and set the port to the same configuration as the device in port configuration function.

You can select **an** mode or **ad** mode depending on your applications. In most of the connection cases, **ad** mode is suggested.

9.11 **set loopback** command

This command is used to set the loopback detection function of the switch. If loopback condition happens at some connection port, all the transmitted packets will come back to the switch and cause packet storm in the switch. That may cause the switch unstable. If this function is enabled and loopback condition is found at some port, that port will be disabled by the switch. You can use “release” sub-command to enable the port after its loopback condition is removed.

Its syntax is …

Syntax: set loopback [enable|disable|release].
[enable] : enable loopback detection on port
[disable]: disable loopback detection on port
[release]: release the ports that loopback are detected

Note: This function is useful for UTP ports to prevent loopback happening because of Transmit-Receive circuit short together.

9.12 **set mgr** command

This command is used to configure the administrator groups and their access rights for managing this switch. The administrators could be specific IP addresses or in a specific IP subnet. 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.)

Its syntax is …

```
>set mgr
[Syntax]set mgr [arg_1 data_1] [arg_1 data_1] ... [arg_n data_n]
```

```
[Argument List]
enable......... Set enabled for a specified set.
disable........ Set disabled 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.
```

enable sub-command is used to enable this function.
disable sub-command is used to disable this function.
ipaddr sub-command is used to set the specified IP addresses or subnet.
Its syntax is …

```
>set mgr ipaddr
Index should be < 1-4 >.
syntax: set mgr ipaddr [index#] [IP Addr] [Net Mask]
```

The "index#" is the entry of the setup item. Then are the IP address and net mask. The net mask should be 255.255.255.255 if it is for some specified IP address (administrator). If the net mask is not 255.255.255.255, it will be for some subnet user group.

mode sub-command is used to set the access mode for the specified administrator(s).
Its syntax is …

```
>set mgr mode
Index should be < 1-4 >.
syntax: set mgr mode [index#] [Mode type]
```

The "index#" is the entry of the setup item. The "Mode type" could be "1" for View Only and "2" for View and Modify rights.

protocol sub-command is used to enable/disable the remote management protocols for the specified administrator(s).
Its syntax is …

```
>set mgr protocol
Index should be < 1-4 >.
syntax: set mgr protocol [index#] [1|0:http] [1|0:telnet] [1|0:snmp]
```

The "index#" is the entry of the setup item. And then are the enable/disable of Http, Telnet, and SNMP protocols one after another.

9.13 **set port** command

This command is used to change the connection configuration of ports.
Its syntax is . . .

```
>set port 2
[Syntax]set port [port#] [arg_1 data_1] [arg_1 data_1] ... [arg_n data_n]
[Argument List]
name........... Set port # name [string]
admin.......... Set port # admin [enable|disable]
speed.......... Set port # speed [auto|10|100]
duplex......... Set port # duplex [full|half]
flowctrl....... Set port # flowctrl [ON|OFF]
```

User can configure the following items for each port.

a. *Name of a port* with “**name**” sub-command.

b. *Enable/Disable a port* with “**admin**” sub-command.

c. *Operation speed of a port* with “**speed**” sub-command.

d. *Duplex mode of a port* with “**duplex**” sub-command.

e. *Flow Control function of a port* with “**flowctrl**” sub-command. (There is also a flow control setting command in QoS function. Please refer to the description for “set qos flowctrl” command for the details.)

For example, “set port 1 name YYY admin enable speed 10 duplex half” command will enable Port 1 and set it to 10Mbps/Half Duplex and name it as “YYY”.

Note: For 100FX ports, only 100Mbps, full duplex setting is allowed.

9.14 **set qos** command

This switch support port-based priority, 802.1P priority, and ToS/DiffServ priority operation. And there are four priorities(P0~P3) for each port. The traffic scheduling for each port could be SP(Strict Priority) for high priority or WRR (Weighted Round Robin with 8:4:2:1) for the four priority queues.

This command is used to configure QoS function of the switch.
Its syntax is . . .

```
>set qos
[Syntax]set QoS [arg_1 data_1] [arg_1 data_1] ... [arg_n data_n]
[Argument List]
enable......... Set QoS enabled.
disable........ Set QoS disabled.
priority....... Set QoS priority for specified port.
flowctrl....... Set QoS flow ccontrol for specified port.
1p............. Set 802.1p for specified port.
mapping........ Set 802.1p priority to priority queue mapping.
pm............. Set Priority Mechanism of Priority Queue.
tdsel.......... Set selection of TOS or Differentiated Service.
dsport......... Set Differentiated Service for specified port.
dscp........... Set QoS priority for specified DSCP.
tos............ Set TOS priority for specified type and precedence.
```

enable - this command is used to enable QoS function.

disable - this command is used to disable QoS function.

priority - this command is used to configure port-based priority. All packets coming from high priority port will always be forwarded to highest priority queue P3. All packets coming from low priority port will always be forwarded to lowest priority queue P0. For example, “set qos priority 3 high” command will set Port 3 as a high priority port.

flowctrl - this command is used to configure flow control function of port when QoS is enabled. There is also a flow control enable/disable function in port configuration. Here is the table about the flow control settings.

Flow control setting in QoS *when QoS Enable*	Flow control setting in port configuration	Flow control operation
Enable	**Enable**	**Enable**
Enable	Disable	Disable
Disable	Enable	Disable
Disable	Disable	Disable

When flow control function is ON, the switch will send pause frame to prevent packet lost when traffic congestion happens. If flow-control function is OFF, the switch will drops packets when traffic congestion happens.

Note: QoS and flow control functions are two conflict operations for a switch. For real QoS request, flow control function should be OFF to allow packets to come in switch and being forwarded by priority when congestion happens. But it depends on user's application.

For example, "set qos flowctrl 5 off" command will disable flow control operation of Port 5 when QoS is enabled.

1p – this command is used to enabled/disable 802.1P priority function on ports. Its syntax is . . .

```
>set qos 1p
Syntax: Set QoS 1p [port#] [on/off]
```

For example, "set qos 1p 2 off" will disable 802.1P priority function on Port 2.

mapping - this command is used to map the 802.1P priority 0~7 to the four priority queues. For example, "set qos mapping 3 1" command will map the 802.1P tag priority 3 to priority queue P1 and packets with tag priority 3 will be forwarded to priority queue P1 of egress port.

pm – this command is used to set priority mechanism (scheduling) for the four priority queues. It could be SP(Strict Priority – high priority will be serviced first), or WRR(Weighted Round Robin with 8:4:2:1). Its syntax is …

```
>set qos pm
Syntax:  set qos pm [1:wrr|2:sp].
Example: set qos pm 1
         set qos pm sp
```

tdsel – this command is used to select ToS priority function or DiffServ priority function for IP packets. (They use the same byte in IP header.) Its syntax is …

```
>set qos tdsel
Syntax:  set qos tdsel [1:tos|2:diffserv].
Example: set qos tdsel 1
         set qos tdsel diffserv
```

dsport – this command is used to enable/disable ToS/DiffServ priority function on each port. Its syntax is …

```
>set qos dsport
Incorrect port number!
Syntax: Set QoS dsport [port#] [on/off]
```

For example, “set qos dsport 2 off” will disable ToS/DiffServ priority function on Port 2.

dscp – this command is used to configure DSCP(DiffServ Code Point, 0~63) to 802.1P(0~7) mapping. Every DSCP value can be mapped to an 802.1P value (0~7). And then map to the priority through the 802.1P to priority mapping. Its syntax is …

```
>set qos dscp
Incorrect index number for DSCP! Valid index number: 0-63.
Syntax: Set QoS dscp [index#] [value]
```

For example, “set qos dscp 10 5” will map the DSCP value 10 to 802.1P priority 5. If 802.1P priority 5 is mapped to priority queue P2, the DSCP value 10 will also map to P2.

tos – this command is used to configure ToS priority to priority queue (P0~P3) mapping. There is priority 0~7 in Precedence of ToS. There is also a Delay, Throughput, Reliability, and Cost bit in ToS. Those bits with 0~7 Precedence create the priority property of ToS. You can define the 0~7 Precedence to priority queues (P0~P3) mapping. Its syntax is …

```
>set qos tos
set qos tos 0~7(ToS Precedence) 0~3(Priority Queue)
```

For example, “set qos tos 0 0” will map ToS Precedence “0” to priority queue P0.

9.15 **set snmp** command

This command is used to configure SNMP function of the switch.

Its syntax is . . .

```
>set snmp
[Syntax]set snmp [arg_1 data_1] [arg_1 data_1] ... [arg_n data_n]
[Argument List]
name........... Set system name
location....... Set system location
contact........ Set system contact name
getcommunity... Set GET community
setcommunity... Set SET community
trapcommunity.. Set TRAP community
trapip......... Set TRAP IP address
txtrap......... Send Trap for test
```

User can use the command to configure the following items for SNMP operation.

a. *Name of the switch* with “**name**” sub-command.
b. *Location of the switch* with “**location**” sub-command.
c. *Contact for the switch* with “**contact**” sub-command.
d. *GET Community string* with “**getcommunity**” sub-command
e. *SET Community string* with “**setcommunity**” sub-command.
f. *TRAP Community string* with “**trapcommunity**” sub-command.
g. *TRAP IP Address* with “**tapip**” sub-command.
h. *Test TRAP Operation* with “**txtrp**” sub-command

For example, “set snmp name ABC location AAA-1F contact Jack” command will set these SNMP information to switch.

9.16 **set trunk** command

This switch supports four trunk groups (Trunk 1 ~ 4) maximum. They are disabled and null trunk groups default. Users can use this command to configure trunk function of the switch.

Its syntax is . . .

```
>set trunk
Syntax     : Set trunk enable
Description: Enable trunk function.

Syntax     : Set trunk disable
Description: Disable trunk function.

Syntax     : Set trunk [+/-] [port#] [trunk#]
Examples   : Set trunk +1+5-7 1
Description: Add port 1,5 to trunk group 1 and
             remove port 7 from trunk group 1
```

a. **enable** and **disable** sub-commands are used to enable/disable trunk function of the switch.
b. **set trunk [+/-] [port#] [trunk#]** is sub-command to add/remove ports to/ from trunk groups. Only Port 1~8 is available for trunk operation.

9.17 **set sta** command

This command is used to configure spanning tree protocol of the switch. (This switch runs 802.1w RSTP protocol with compatible with 802.1D STP function.)

Its syntax is . . .

```
>set sta
[Command List]
?............. Help commands
help........... Help commands
enable......... Enable Spanning Tree function
disable........ Disable Spanning Tree function
bridge......... Set Spanning Tree bridge configuration
port........... Set Spanning Tree port configuration
```

a. **set sta ?** and **set sta help** commands will show the sub-command list
b. **set sta enable** and **set sta disable** commands will enable/disable spanning tree function of the switch.
c. **set sta bridge** command is used to configure spanning tree function for the switch.

Its syntax is . . .

```
>set sta bridge
[Syntax]set sta bridge [arg_1 data_1] [arg_1 data_1] ... [arg_n data_n]
[Argument List]
priority....... Set bridge priority.
hello.......... Set bridge hello time
```

```
age............ Set bridge maximum age
delay.......... Set bridge forward delay time
```

priority (0~65535) : 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 (0~65535) : the period to send the spanning tree maintenance packet if the switch is the root of the spanning tree. Default is 2 seconds.
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.
delay (4~30): the maximum waiting time before changing states (i.e., listening to 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.

d. **set sta port** command is used to configure for ports of the switch.
Its syntax is . . .

```
>set sta port
Syntax: set sta port [port#] [enable] [disable] [cost=xxxx] [priority=xxxx]
```

enable : enable spanning tree function on the port.
disable : disable spanning tree function on the port.
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.
priority (0~255) : 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.

9.18 **set http** command

This command is used to enable/disable the http function of the switch. Because hacker or worm/virus (like ColdRed) often attacks http server, this command is provided to 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.)

Its syntax is . . .

```
>set http
Syntax     : Set http enable
```

Description: Enable http protocol function.
Syntax : Set http disable
Description: Disable http protocol function.

9.19 **set gvrp** command

This command is used to enable/disable the GVRP function for 802.1Q VLAN. If this function is enabled, this switch will learn the 802.1Q VLAN from another 802.1Q network devices if it receives their packets. The learned remote 802.1Q VLAN will be shown in the dynamic 802.1Q VLAN table.

Its syntax is . . .

```
>set gvrp
Syntax: set gvrp [1|0]  <1:enable,0:disable>
```

9.20 **set 1qvlan** command

This command is used to configure 802.1Q VLAN of the switch.
Its syntax is . . .

```
>set 1qvlan
[Syntax]set 1qvlan [arg_1 data_1] [arg_1 data_1] ... [arg_n data_n]
[Argument List]
enable......... Set 802.1Q VLAN enabled.
disable........ Set 802.1Q VLAN disabled.
ingressfilter.. Set ingress filter Enable or Disable.
create......... Create new 802.1Q vlan with specified VLAN ID and VLAN Name.
modify......... Modify forward and untagged memeber.
pvid........... Set the Port VLANID of specified port.
mgrpvid........ Set the Port VLANID of management port.
priority....... Set the priority of specified port.
block.......... Set the Block of VID.
mode........... Set the VLAN Mode.
```

enable and **disable** sub-commands are used to enable/disable 802.1Q VLAN function of the switch.
ingressfilter sub-command is used to enable/disable VLAN filtering executed at ingress port.
Enable: the VLAN filtering function will be executed when packet is received at ingress port. If the ingress port is in the same VLAN of the received packet, this packet will go to forwarding stage. Otherwise, the packet will be discarded by VLAN filtering at ingress port.
Disable: the VLAN filtering function will be executed when packet is forwarded to egress port.
create sub-command is used to create a static 802.1Q VLAN. For example, “set 1qvlan create ABC 20” will create a static 802.1Q VLAN with name “ABC” and ID 20.
modify sub-command is used to modify a static 802.1Q VLAN setting.
Its syntax is . . .

```
>set 1qvlan modify
Syntax    : set 1qvlan modify [+|-] [port#] VLANID [1:<tagged>|0:<untagged>]
```

Examples : Set 1qvlan +1+5-7 2 1
Description: Add port 1,5 to VLAN 2 as tagged port and remove port 7 from VLAN 2

pvid sub-command is used to set Port VLAN ID. The Port VLAN ID is used as the VLAN ID for tag adding when untagged packet is translated to tagged packet. For example, "set 1qvlan pvid 3 10" will set the PVID of Port 3 as 10.

mgrpvid sub-command is used to select the VLAN group that is allowed to management the switch. Only the users in the selected VLAN can manage the switch by Http, Telnet and SNMP. For example, "set 1qvlan mgrpvid 5" will allow the users in the VLAN with VLAN ID 5 to manage the switch remotely.

priority sub-command is used to set port priority for tag adding when untagged packet is translated to tagged packet. For example, "set 1qvlan priority 3 2" will set the port priority of Port 3 as 2. The priority information in tag will be filled with 2 when the untagged packet coming to Port 3 is translated to tagged packet.

block sub-command is used to set active VLAN ID block range for 802.1Q VLAN operation. The valid VLAN ID number is 1 ~ 4094. Because this switch can support up to 512 active VLAN ID number, the valid VLAN ID number is divided into eight blocks as below.

Syntax : set 1qvlan block [Block#]
Examples : Set 1qvlan block 0
Description: Set current block as 0 and active VID: 1~511

Block	Active VID	Block	Active VID
0	1~ 511	4	2048~2559
1	512~1023	5	2560~3071
2	1024~1535	6	3072~3583
3	1536~2047	7	3584~4094

Select one of the blocks and only the selected VLAN ID range is active for 802.1Q VLAN operation of the switch.

mode sub-command is used to select the VLAN mode for 802.1Q VLAN operation. There are three modes for VLAN function –SVL (Shared VLAN), IVL (Individual VLAN) and SVL/IVL.

Syntax : set 1qvlan mode [0:SVL|1:IVL]
Examples : Set 1qvlan mode 0
Description: Set current vlan mode as SVL
0: SVL mode
1: IVL mode
2: SVL/IVL mode

SVL mode – the switch will do packet forwarding according to its Mac address only.

IVL mode – the switch will do packet forwarding according to its Mac address and its VLAN ID.

SVL/IVL mode – its operation is the same as IVL mode but for untagged port is used as the uplink port in MDU/MTU application.

For most VLAN applications, SVL mode is suggested.

9.21 **set dot1x** command

This command is used to configure the 802.1x function of the switch.
Its syntax is . . .

```
>set dot1x
[Syntax]set dot1x [arg_1 data_1] [arg_1 data_1] ... [arg_n data_n]
[Argument List]
enable......... Set 802.1x enable
disable........ Set 802.1x disable
transparent.... Set 802.1x transparent
re_au.......... Set 802.1x Re-authentication
reauthtime..... Set 802.1x Re-authentication Timeout Period
reauthcnt...... Set 802.1x Re-authentication Max Count
reqcnt......... Set 802.1x Max Request Count
sertime........ Set 802.1x Server Timeout Period
supptime....... Set 802.1x Supplicant Timeout Period
quiettime...... Set 802.1x Quiet Timeout Period
txtime......... Set 802.1x Tx Timeout Period
rsip........... Set Radius Server Address
authport....... Set Authenticate Port of Radius Server
shkey.......... Set 802.1x Security Key
portauth....... Set 802.1x port auth mode
```

enable sub-commands is used to enable 802.1x authentication function.
disable sub-command is used to disable 802.1x function. 802.1x protocol packets will also not be forwarded.
transparent sub-command is used to set the operation of 802.1x function to transparent mode. In this mode, the switch will forward 802.1x protocol packets but no authentication function.
re_au sub-command is used to enable the re-authentication function of the switch. When the re-authentication time is up, the switch will start the re-authentication process.
reauthtime sub-command is used to set the timeout period of the re-authentication process.
reauthcnt sub-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 is 1~10.
reqcnt sub-command is used to set max request timeout count between the switch and RADIUS server before authentication fail. The valid value is 1~10.
sertime sub-command is used to set the request timeout value between the switch and RADIUS server. The valid value is 0~65535.
supptime sub-command is used to set the timeout value between the switch and users (called “supplicant” in 802.1x) after first identification. The valid value is 0~65535.
quiettime sub-command is used to set the quiet time value between the switch and the user before next authentication process when authentication fail.
txtime sub-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

reauthcnt is met. After that, authentication fail message will be sent. The valid value is 0~65535.

rsip sub-command is used to set the IP address of RADIUS server.

authport sub-command is used to set the handshaking port number between the switch and RADIUS server. It could be different for different RADIUS servers.

shkey sub-command is used to set the security key between the switch and RADIUS server.

portauth sub-command is used to set the authentication mode for a physical port. Its syntax is . . .

set dot1x portauth [port#] [auto|fa|fu|no]

- auto: the authentication mode of the port depending on the authentication result of the port
- fa (force-authenticated): will force the port always being authentication successful in 802.1x process and the real authentication result will be ignored.
- fu (force-unauthenticated): will force the port always being authentication unsuccessful in 802.1x process and the real authentication result will be ignored.
- none: 802.1x function will not be executed on the port, i.e. disabled on the port.

Note: This switch supports MD5, TLS and PEAP authentication types.

9.22 **set security** command

This command is used to set the Mac address security mode of physical port. Its syntax is . . .

```
>set security
Syntax     : Set security [port#] [mode]
Examples   : Set security 1 1
Description: Set the MAC Security of port 1 to Static mode with Accept function.
        mode 0 = No Security
        mode 1 = Accept function
        mode 2 = Reject function
```

For examples, “set security 1 1” will set Port 1 to accept the users with the static Mac addresses configured on Port 1. Please refer to “set arl” command for static address setting. Or, you can set static address from the “Dynamic Mac Address Table” in web interface. The table will show the learned Mac addresses and you just need to select from the learned address list.

Note: Here is an *Application Note* for Mac address filter-in function.
It needs two conditions for Mac address filter-in function working.
1. The port security mode is set to “Accept”.
2. Static Mac address is assigned on Port (for example, Mac 1 on Port 1).
In this case, only Mac 1 can access network through Port 1. But there is also a limitation for Mac 1 - it can access network through Port 1 only because it is a static fixed address on Port 1.

9.23 **set ratecontrol** command

This command is used to set the maximum traffic rate to/from physical ports of the switch.

Its syntax is . . .

```
>set ratecontrol
Syntax 1   : Set ratecontrol drop [0|1]
Examples   : Set ratecontrol drop 1
Description: Set Packet Drop for Ingress Limit.

Syntax 2   : Set ratecontrol [ingress|egress] [port#] [0-127]
Examples   : Set ratecontrol ingress 1 10
Description: Set port 1 ingress rate control with 10*64K=640K
             No Limit of rate control, with N=0.
             Rate = N*64 Kb,    with N=1~28.
             Rate = (N-27)*1Mb, with N=29~127.
```

set ratecontrol drop [0|1] : this subcommand is used to enable/disable the packet dropping operation when ingress traffic exceeds the maximum ingress rate. If it is set to "disable", flow control operation will be used instead of packet dropping.

set ratecontrol [ingress|egress] [port#] [0-127] : this subcommand is used to set the maximum traffic rate for ingress/egress traffic through physical ports of the switch. The rate control could be from 64Kbps to 100Mbps.

N=0 : rate control is disable, rate = No Limit.

N=1~28 : rate = Nx64Kbps, for rate 64K, 128K, …, 1792Kbps control

N=29~127 : rate = (N-27)x1Mbps, for rate 2M, 3M, …, 100Mbps control

9.24 **set stormcontrol** command

This switch supports broadcast storm, multicast storm and flooding storm control functions. With this command, you can configure the storm control function of the switch.

```
>set stormcontrol
[Syntax]set StormControl [arg_1 data_1] [arg_1 data_1] ... [arg_n data_n]
[Argument List]
rate........... Set Control Rate for Storm Control.
bc............. Set Broadcast Control for each Port.
mc............. Set Multicast Control for each Port.
fd............. Set Flooding Control for each Port.
```

set stormcontrol rate : this subcommand is used to set the maximum storm rate that is allowed for the control.

```
Syntax     : set stormcontrol rate [rate#]
Examples   : Set stormcontrol rate 0
Description: Set storm control rate as 3.3%
    Rate#      Control Rate
      0            3.3%
      1             5%
      2            10%
```

3	20%

set stormcontrol bc : this subcommand is for broadcast storm control.
set stormcontrol mc : this subcommand is for multicast storm control.
set stormcontrol fd : this subcommand is for flooding storm control.

Syntax : set stormcontrol [bc|mc|fd] [all|none|byport|port#] [1|0]
Examples 1 : Set stormcontrol bc all
Description: Set storm control to suppression broadcast packet for all port.
Examples 2 : Set stormcontrol mc none
Description: Set storm control not to suppression multicastcast packet for all port.
Examples 3 : Set stormcontrol fd byport
Description: Set storm control to suppression flooding packet according to each port setting.
Examples 4 : Set stormcontrol fd 1 1
Description: Set storm control to suppression flooding packet for port 1 enabled.

9.25 **set telnet** command

This command can be used to enable, disable, and setting service port number for Telnet interface of the switch.

Its syntax is …

```
>set telnet
Syntax     : Set telnet enable
Description: Enable telnet protocol function.
Syntax     : Set telnet disable
Description: Disable telnet protocol function.
Syntax     : Set telnet port xx
Description: Set telnet port_no function.
```

10. **Show** command

This command is used to show configurations of the switch. Here is the sub-command for showing different configuration.

```
>show
[Command List]
?.............. Help commands
help........... Help commands
arl............ Show ARL table
dynamic........ Show dynamic learning table
cfg............ Show system configuration
net............ Show network configuration
igmp........... Show IGMP configuration
mirror......... Show mirror configuration
mvr............ Show MVR function
automode....... Show Auto mode setting
loopback....... Show the setting of Loopback Detection
mgr............ Show management IP configuration
port........... Show switch port configuration
```

```
qos............ Show QoS configuration
snmp........... Show snmp configuration
trunk.......... Show all TRUNK groups with their members
sta............ Show Spanning Tree setting
http........... Show HTTP Protocol setting
gvrp........... Show GVRP Protocol Status
1qvlan......... Show 802.1q VLAN Configuratuin
dot1x.......... Show 802.1x Protocol Status
security....... Show MAC Security Configuration
ratecontrol.... Show Rate Control Configuration
stormcontrol... Show Storm Control Configuration
statistics..... Show the port's statistics
telnet......... Show TELNET Protocol setting
```

10.1 **show ?** and **show help** commands will show the sub-command list.

10.2 **show arl** command will show static Mac ID setting in ARL table. For example,

```
>show arl
Item  Port  Mac Address
  1      5    00-00-E2-11-22-33
```

10.3 **show dynamic** command will show current Mac address table content of the switch. For example,

```
>show dynamic
[Dynamic Adress Learning Table]
 Item Port       Mac Address           VID
================================================
   1)    9      00-00-e2-64-64-64      1(0x001)
================================================
```

The extra port is the interface to internal CPU.

10.4 **show cfg** command will show Model Name, Mac ID of the switch and Firmware version. For example,

```
>show cfg
[System Configuration]
Company Name     :
Model Name       : Intellignet Switch
MAC Address      : 00:00:00:FF:0D:01
Firmware Version : 2.11.14 < Aug 24 2007 11:16:49 >
```

10.5 **show net** command will show current IP address configuration of the switch. For example,

```
>show net
[eth0] Network Configuration:
DHCP       : ENABLE
IP Address: 192.168.1.5
Netmask   : 255.255.255.0
```

```
Gateway   : 192.168.1.120
```

10.6 **show igmp** command will show current IGMP snooping function enable/disable status and the IP multicast groups that learned by the switch. For example,

```
>show igmp
[IGMP Configuration]
IGMP Switch     : Enabled
Total Groups    : 3
=====================================================
[Group 1]  IP Address    :  224.0.0.9
           Member Port :  1
[Group 2]  IP Address    :  224.0.0.2
           Member Port :  1
[Group 3]  IP Address    :  224.2.188.136
           Member Port :  4,5
=====================================================
```

10.7 **show mirror** command will show mirror function configuration of the switch. For example,

```
>show mirror
[Mirror Configuration]
Mirror Switch:Disabled
Capture port :1
Ingress DIV=3     Mode=SA  MAC=00-00-00-11-22-33
       Port List: 2
Egress  DIV=1     Mode=ALL MAC=00-00-00-00-00-00
       Port List:
```

This setting will mirror those packets that with source Mac address 000000112233 ingress to Port 2 to Port 1 for every three matched packets.

10.8 **show mvr** command will show current MVR settings. There are two sub-commands – vlan and group.

“show mvr vlan” command will show the four MVR VLAN settings one after another. For example,

```
>show mvr vlan
[MVR : VLAN Configuration]
=====================================================
Name              :
Active            : No
Multicast VLAN ID: 1
802.1p Priority  : 0
Mode              : Dynamic
Source Port       : 1 (T)
Receiver Port (T):
Receiver Port (U):
=====================================================
Press any key to continue ...
```

"show mvr group" command will show current IP multicast groups for MVR VLANs. For example,

```
>show mvr group
[MVR : Group Configuration]
==========================================================
Index VLANID          Name              Start Addr.      End Addr.
==========================================================
  1      1            News                224.0.0.9         224.0.0.12
  2      1            Movie            224.2.188.136   224.2.188.140
==========================================================
```

Please refer to the description of "set mvr" command for the details for MVR function.

10.9 **show automode** command will show current auto mode setting for port configuration. It could be **Auto Negotiation** and **Auto Detect**.
For *Auto Negotiation* mode, the switch will do auto-negotiation ON/OFF when the auto function of port is enabled/disabled. But the Auto-MDIX function will also be disabled when the auto-negotiation function of port is OFF.
For *Auto Detect* mode, the switch will always keep auto-negotiation function ON but just modify its attribution if the auto function of port is disabled. The Auto-MDIX function will be always enabled in this mode.
For applications, you should select *Auto Detect* mode if the connected device is auto-negotiation enabled. And you can select *Auto Negotiation* mode if the connected device is auto-negotiation disabled.
For most applications, *Auto Detect* mode is OK.

10.10 **show loopback** command will show current setting of loopback detection function. For example,

```
>show loopback
[Loopback Detection]: Disable
```

If the loopback detection function is enabled, the switch will send detecting packet periodically. If loopback is found, the port will be disabled to prevent packet storm happening. Then you have to use "*set loopback release*" command to release the port if the loopback condition is removed.

Loopback may happen on UTP port if its Transmit-Receive circuit is short together.

10.11 **show mgr** command will show the specified IP setup and their access rights for managing the switch. If this function is enabled, only these IP addresses can manage the switch with the assigned access rights.

```
>show mgr
[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
=====================================================
```

"Mode" is the access right assigned to the administrator.
"Http", "Telnet", and "SNMP" are the management interface enable/disable status for the administrator.

10.12 **show port** command will show status and configuration of each switch port. For example,

```
>show port
[Port Configuration]
Port Name            Status    Disable   Auto.  Speed   Duplex   Flow
Control
  1   10/100M base-T   DOWN      NO       ON     10      Half      OFF
  2   10/100M base-T   DOWN      NO       ON     10      Half      OFF
  3   10/100M base-T   DOWN      NO       ON     10      Half      OFF
  4   10/100M base-T   DOWN      NO       ON     10      Half      OFF
  5   10/100M base-T   DOWN      NO       ON     10      Half      OFF
  6   10/100M base-T   DOWN      NO       ON     10      Half      OFF
  7   10/100M base-T   DOWN      NO       ON     10      Half      OFF
  8   10/100M base-T   DOWN      NO       ON     10      Half      OFF
```

10.13 **show qos** command will show QoS configuration of the switch. This switch support port-based priority, 802.1P priority, and ToS/DiffServ priority operation. And there are four priorities(P0~P3) for each port. The traffic scheduling for each port could be SP(Strict Priority) for high priority or WRR (Weighted Round Robin with 1:2:4:8) for the four priority queues. You can use this command to check current QoS setting of the switch.

For example,

```
>show qos
[QoS Configuration]
Qos setting      :  Enabled
Priority Mechanism:  WRR (1:2:4:8)
TOS/DiffServ     :  TOS
=====================================
802.1p Priority Tag 7 ==> P0
802.1p Priority Tag 6 ==> P0
802.1p Priority Tag 5 ==> P1
802.1p Priority Tag 4 ==> P1
802.1p Priority Tag 3 ==> P2
802.1p Priority Tag 2 ==> P2
802.1p Priority Tag 1 ==> P3
802.1p Priority Tag 0 ==> P3
Press any key to continue ...
```

```
=========================================================
Port  Priority  Port  Priority  Port  Priority  Port  Priority
=========================================================
[ 1]   Low     [ 2]   Low     [ 3]   Low     [ 4]   Low
[ 5]   Low     [ 6]   Low     [ 7]   Low     [ 8]   Low
=========================================================
Port  FlowCtrl  Port  FlowCtrl  Port  FlowCtrl  Port  FlowCtrl
=========================================================
[ 1]    OFF     [ 2]    OFF     [ 3]    OFF     [ 4]    OFF
[ 5]    OFF     [ 6]    OFF     [ 7]    OFF     [ 8]    OFF
=========================================================
Press any key to continue ...
=========================================================
Port   802.1p   Port   802.1p   Port   802.1p   Port   802.1p
=========================================================
[ 1]    ON      [ 2]    ON      [ 3]    ON      [ 4]    ON
[ 5]    ON      [ 6]    ON      [ 7]    ON      [ 8]    ON
=========================================================
Port  TOS/Diff  Port  TOS/Diff  Port  TOS/Diff  Port  TOS/Diff
=========================================================
[ 1]    ON      [ 2]    ON       [ 3]    ON       [ 4]    ON
[ 5]    ON      [ 6]    ON       [ 7]    ON       [ 8]    ON
=========================================================
Press any key to continue ...
=========================================================
 # value  # value  # value  # value  # value  # value  # value  # value
=========================================================
 0)  0    1)  0    2)  0    3)  0    4)  0    5)  0    6)  0    7)  0
 8)  1    9)  1   10)  1   11)  1   12)  1   13)  1   14)  1   15)  1
16)  2   17)  2   18)  2   19)  2   20)  2   21)  2   22)  2   23)  2
24)  3   25)  3   26)  3   27)  3   28)  3   29)  3   30)  3   31)  3
32)  4   33)  4   34)  4   35)  4   36)  4   37)  4   38)  4   39)  4
40)  5   41)  5   42)  5   43)  5   44)  5   45)  5   46)  5   47)  5
48)  6   49)  6   50)  6   51)  6   52)  6   53)  6   54)  6   55)  6
56)  7   57)  7   58)  7   59)  7   60)  7   61)  7   62)  7   63)  7
=========================================================
Press any key to continue ...
===================================
 TOS Precedence   Priority Queue
===================================
     111             P0
     110             P0
     101             P1
     100             P1
     011             P2
     010             P2
     001             P3
     000             P0
===================================
```

The first part is the QoS enable/disable status, Priority queue scheduling SP/WRR setting, and ToS/DiffServ selection.
The second part is the mapping of 802.1P priority values 0~7 to the four priority queues of the switch.
The third part is the port-based priority setting.
The fourth part is the flow control setting for each port. (Please refer to the description of “set qos flowctrl” command for the details of its operation.)
The fifth part is the 802.1P priority function status for each port.
The sixth part is the ToS/DiffServ priority function status for each port.
The seventh part is the DSCP values to 802.1P priority mapping.
The eighth part is the ToS precedence values to priority queue mapping.

10.14 **show snmp** command will show SNMP configuration of the switch. For example,

```
>show snmp
[SNMP Configuration]
System Name   : Switch
Location       : 3F
Contact name   : Jack
Get Community : public
Set Community : private
Trap Community 1: public
Trap IP 1      : 0.0.0.0
Trap Community 2: public
Trap IP 2      : 0.0.0.0
Trap Community 3: public
Trap IP 3      : 0.0.0.0
Trap Community 4: public
Trap IP 4      : 0.0.0.0
Trap Community 5: public
Trap IP 5      : 0.0.0.0
```

10.15 **show trunk** command will show trunk configuration of the switch. For example,

```
>show trunk
[Trunk Group Setting]
Trunk Setting       :  Enabled
[TRUNK]   [Port List]
=======  ========================================
 [ 1]       1  2  3
=======  ========================================
```

10.16 **show sta** command will show spanning tree configuration of the switch. For example,

```
>show sta
[Spanning Tree Configuration]
Spanning Tree Function: Disabled
Bridge Priority       : 32768
Bridge Hello Time     : 2
Bridge Max Age        : 20
Bridge Forward Delay  : 15
==========================================================
Port  Priority  Path Cost    Status      State        Designated Root
==========================================================
  1      128         19          Enabled      None      00:00:00:00:00:00 [0]
  2      128         19          Enabled      None      00:00:00:00:00:00 [0]
  3      128         19          Enabled      None      00:00:00:00:00:00 [0]
  4      128         19          Enabled      None      00:00:00:00:00:00 [0]
  5      128         19          Enabled      None      00:00:00:00:00:00 [0]
  6      128         19          Enabled      None      00:00:00:00:00:00 [0]
  7      128         19          Enabled      None      00:00:00:00:00:00 [0]
  8      128         19          Enabled      None      00:00:00:00:00:00 [0]
==========================================================
```

It shows the Bridge and Port spanning tree configuration.

10.17 **show http** command will show http enable/disable state. For example,

```
>show http
[HTTP Protocol Setting]
HTTP Setting: Enabled
```

10.18 **show gvrp** command will show the GVRP function status for 802.1Q VLAN operation.

For example,

```
>show gvrp
GVRP Protocol : Disable
```

10.19 **show 1qvlan** command will show current 802.1Q VLAN status and settings.

Its syntax is . . .

```
>show 1qvlan
Syntax: show 1qvlan [status|static|table|pvid]
   status : show 802.1q, Ingress Filter and GVRP protocol status
   static : show STATIC VLAN table content
   table  : show ALL VLAN table content
   pvid   : show the PVID of ports
```

For example,

```
>show 1qvlan status
802.1Q VLAN     : Enable
Ingress Filter  : Disable
Curent Block    : 0, Active VID: < 0 ~ 511 >
Curent VLAN Mode: SVL

>show 1qvlan static
---------------- Static 802.1Q VLAN Table ----------------
VLAN ID  :    1(0x001) , VLAN Name: Default VLAN
Tagged Member Port   :
```

```
Untagged Member Port :  1  2  3  4  5  6  7  8

VLAN ID  :    2(0x002) , VLAN Name:
Tagged Member Port   :
Untagged Member Port :
-----------------------  Finish ------------------------

>show 1qvlan table
----------------- All 802.1Q VLAN Table -----------------
VLAN Type:   STATIC
VLAN ID  :    1(0x001) , VLAN Name: Default VLAN
Tagged Member Port   :
Untagged Member Port :  1  2  3  4  5  6  7  8

VLAN Type:   STATIC
VLAN ID  :    2(0x002) , VLAN Name:
Tagged Member Port   :
Untagged Member Port :
-----------------------  Finish -----------------------

>show 1qvlan pvid
 PORT       PVID
======================
  1         1(0x001)
  2         1(0x001)
  3         1(0x001)
  4         1(0x001)
  5         1(0x001)
  6         1(0x001)
  7         1(0x001)
  8         1(0x001)
======================
Management Port :    1
======================
```

The PVID of Management Port is for the management interface of the switch. Only the users in the VLAN with VLAN ID equal to the PVID of Management Port can manage the switch from network because they are in the same VLAN.

10.20 **show dot1x** command will show current 802.1x status and settings.

Its syntax is . . .

```
>show dot1x
Syntax: show dot1x [config|radius|port]
               config : show 802.1x protocol status
               radius : show radius server status
                port  : show ALL ports status
```

For example,

```
>show dot1x config
```

```
[802.1x Configuration]
802.1x Protocol                  : Disabled
Re-authentication                : Disabled
Re-authentication Timeout Period : 3600
Re-authentication Max Count      : 2
Max Request Count                : 2
Server Timeout Period            : 30
Supplicant Timeout Period        : 30
Quiet Timeout Period             : 60
Tx Timeout Period                : 30

>show dot1x radius
[Redius Server Configuration Menu]
Redius Server IP Address  : 192.168.1.222
Redius Server Port Number : 1812
Security Key              : 12345678

>show dot1x port
802.1X Port Authentication Configuration Menu
PORT     Status     Auth.Mode
==================================
  1           -           FA
  2           -           FA
  3           -           FA
  4           -           FA
  5           -           FA
  6           -           FA
  7           -           FA
  8           -           FA
```

The Auth. Mode could be Auto, FA(Forced Authenticated), FU(Forced Unauthenticated) and No(No 802.1x function).

10.21 **show security** command will show current Mac address security mode for port.

Its syntax is . . .

```
>show security
[MAC Security Configuration]
===========================================================
  Port    Static MAC Number          Security Control
===========================================================
    1          0                        No Security
    2          0                        No Security
    3          0                        No Security
    4          0                        No Security
    5          0                        No Security
    6          0                        No Security
    7          0                        No Security
    8          0                        No Security
```

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

The “Security Control” could be *No*, *Accept*, *Reject* modes. “No” is for no Mac address security. “Accept” is for only the static Mac address can access. “Reject” is for only the static Mac address cannot access.

10.22 **show ratecontrol** command will show current rate control setting for each port. For example,

```
>show ratecontrol
[Rate Control Configuration]
Packet Drop for Ingress Limit: Disable
==========================================
 Port     Ingress      Egress
==========================================
   1      Disable      Disable
   2      Disable      Disable
   3      Disable      Disable
   4      Disable      Disable
   5      Disable      Disable
   6      Disable      Disable
   7      Disable      Disable
   8      Disable      Disable
==========================================
```

10.23 **show stormcontrol** command will show current packet storm control settings. This switch supports broadcast storm, multicast storm and flooding storm control functions. With this command, you can find the maximum storm rate setting and the port list doing the storm control.

For example,

```
>show stormcontrol
[Storm Control Configuration]
=============================
Control Rate    :   3.3%
Broadcast Control: By Port
Multicast Control: By Port
Flooding Control : By Port
============================================
 Port  Broadcast  Multicast  Flooding
============================================
  1        -          -         -
  2        -          -         -
  3        -          -         -
  4        -          -         -
  5        -          -         -
  6        -          -         -
  7        -          -         -
  8        -          -         -
============================================
```

10.24 **show statistics** command will show statistics counters content for each port. For example, “show statistics 2” will show statistics counters of Port 2.

```
>show statistics 2

Rx Counter Statistics
Good Unicast Frame      =1017
Good Broadcast Frame     =3
Good Multicast Frame     =18673
802.3X MAC Control      =0
Total Receive Byte Count =2394260
CRC Error               =151
Fragment                =0
Jabbers                =0

Tx Counter Statistics
Good Unicast Frame      =1041
Good Broadcast Frame     =514
Good Multicast Frame     =2
802.3X MAC Control      =0
Total Transmit Byte Count=193498

Press <ENTER> key to continue.
```

You can press Enter key to refresh the counters, and press any key to leave.

10.25 **show telnet** command will show current configuration of telnet interface of the switch.
For example,

```
>show telnet
[Telnet Protocol Setting]
Telnet Status: Enabled
Port Number  : 23
```

11. **Upgrade** command

This switch supports firmware or configuration upgrade with TFTP protocol. This command is used to upgrade firmware or configuration to the switch.
Its syntax is . . .

```
>upgrade
Syntax: upgrade [firmware | config] ip filename
```

ip is the IP address of TFTP server.
filename is the upgrade file name in the TFTP server.

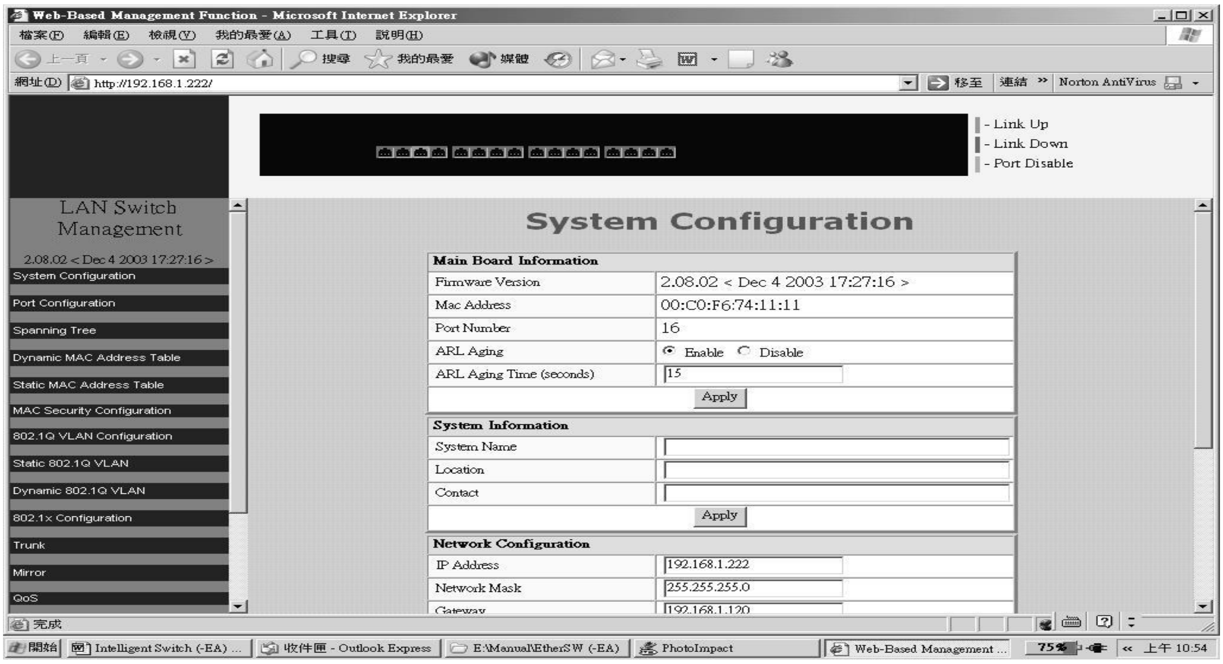
For example, “upgrade config 192.168.1.80 abcd” command will load file “abcd” from TFTP server 192.168.1.80 as its configuration setting.

6.3 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 net**” command to check IP address of the switch first. If users want to change the IP address of the switch, use “**set eth0 ip xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx gateway xxx.xxx.xxx.xxx**” command to modify the IP address of the switch. The default IP configuration is **192.168.1.5** 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**" / ”**123456**”. Then the management homepage will appear.


Web-Based Management Function - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛 媒體
網址(D) http://192.168.1.222/
移至 連結 Norton AntiVirus
- Link Up
- Link Down
- Port Disable
LAN Switch Management
2.08.02 < Dec 4 2003 17:27:16 >
System Configuration
Port Configuration
Spanning Tree
Dynamic MAC Address Table
Static MAC Address Table
MAC Security Configuration
802.1Q VLAN Configuration
Static 802.1Q VLAN
Dynamic 802.1Q VLAN
802.1x Configuration
Trunk
Mirror
QoS
完成
開始
Intelligent Switch (-EA) ...
收件匣 - Outlook Express
E:\Manual\EtherSW (-EA)
PhotoImpact
Web-Based Management ...
75%
上午 10:54

System Configuration

Main Board Information	
Firmware Version	2.08.02 < Dec 4 2003 17:27:16 >
Mac Address	00:C0:F6:74:11:11
Port Number	16
ARL Aging	● Enable ○ Disable
ARL Aging Time (seconds)	15
Apply	
System Information	
System Name	
Location	
Contact	
Apply	
Network Configuration	
IP Address	192.168.1.222
Network Mask	255.255.255.0
Gateway	192.168.1.120

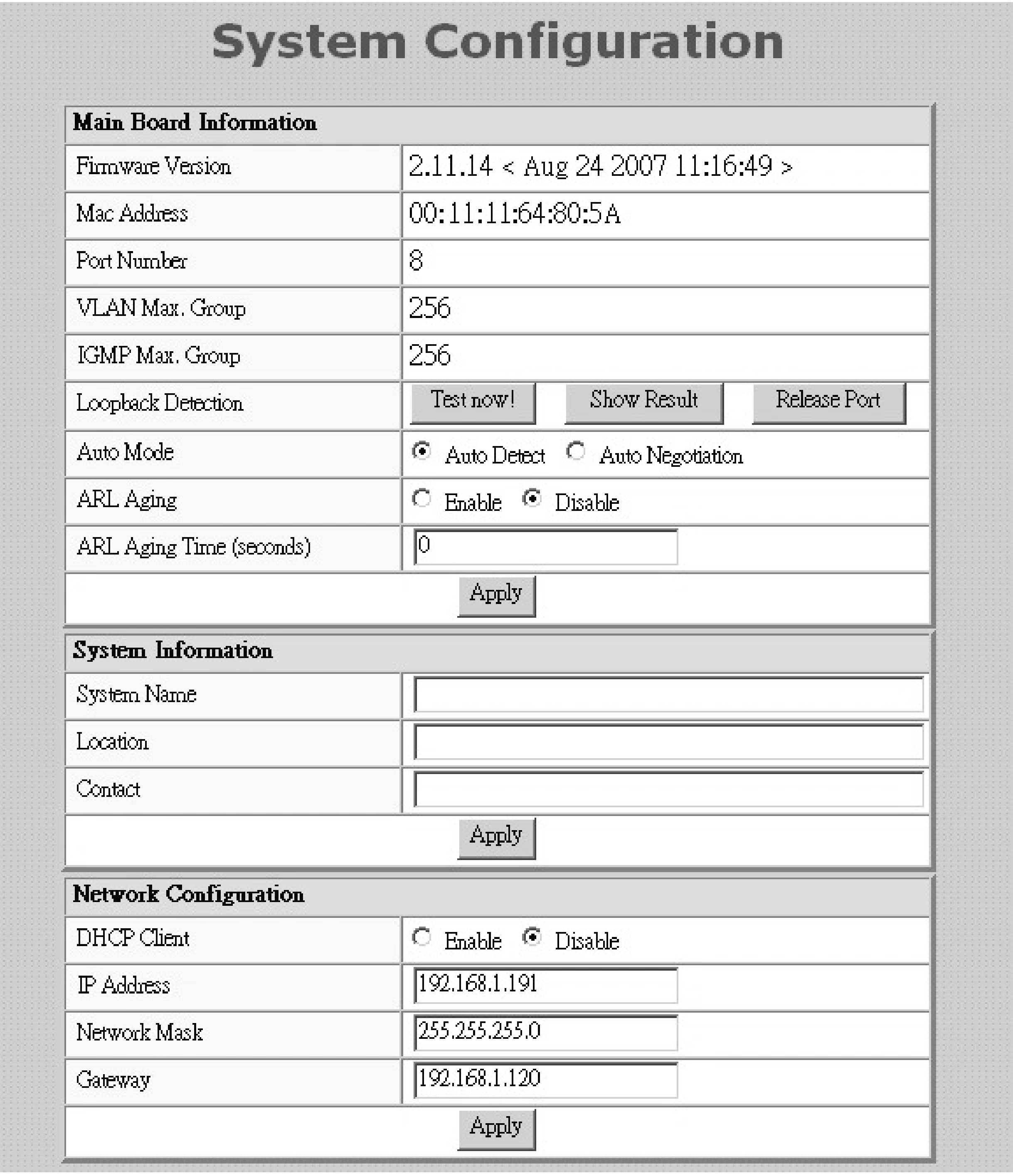
Left part of the homepage is a function list. Users can select one of them for status monitoring or switch configuration.

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.

1. System Configuration



System Configuration

Main Board Information	
Firmware Version	2.11.14 < Aug 24 2007 11:16:49 >
Mac Address	00:11:11:64:80:5A
Port Number	8
VLAN Max. Group	256
IGMP Max. Group	256
Loopback Detection	Test now! Show Result Release Port
Auto Mode	● Auto Detect ○ Auto Negotiation
ARL Aging	○ Enable ● Disable
ARL Aging Time (seconds)	0
Apply	

System Information	
System Name	
Location	
Contact	
Apply	

Network Configuration	
DHCP Client	○ Enable ● Disable
IP Address	192.168.1.191
Network Mask	255.255.255.0
Gateway	192.168.1.120
Apply	

“System Configuration” is the homepage of the switch.

Users can find firmware version and Mac address of the switch in this page. And users can configure the following items in this page.

a. **Loopback Detection** : Users can do loopback detection by click [Test now!]. And check the test result by click [Show Result]. If any port is blocked because of loopback is found, you can click [Release Port] to release it after the loopback condition is removed. This function can be used to prevent the possible packet storm caused by Transmit-Receive circuit short together (Loopback) on UTP port connections.

b. **Auto Mode** : User can select the auto function of connection port here.

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

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

   For applications, you should select *Auto Detect* mode if the connected device is auto-negotiation enabled. And you can select *Auto Negotiation* mode if the connected device is auto-negotiation disabled.

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

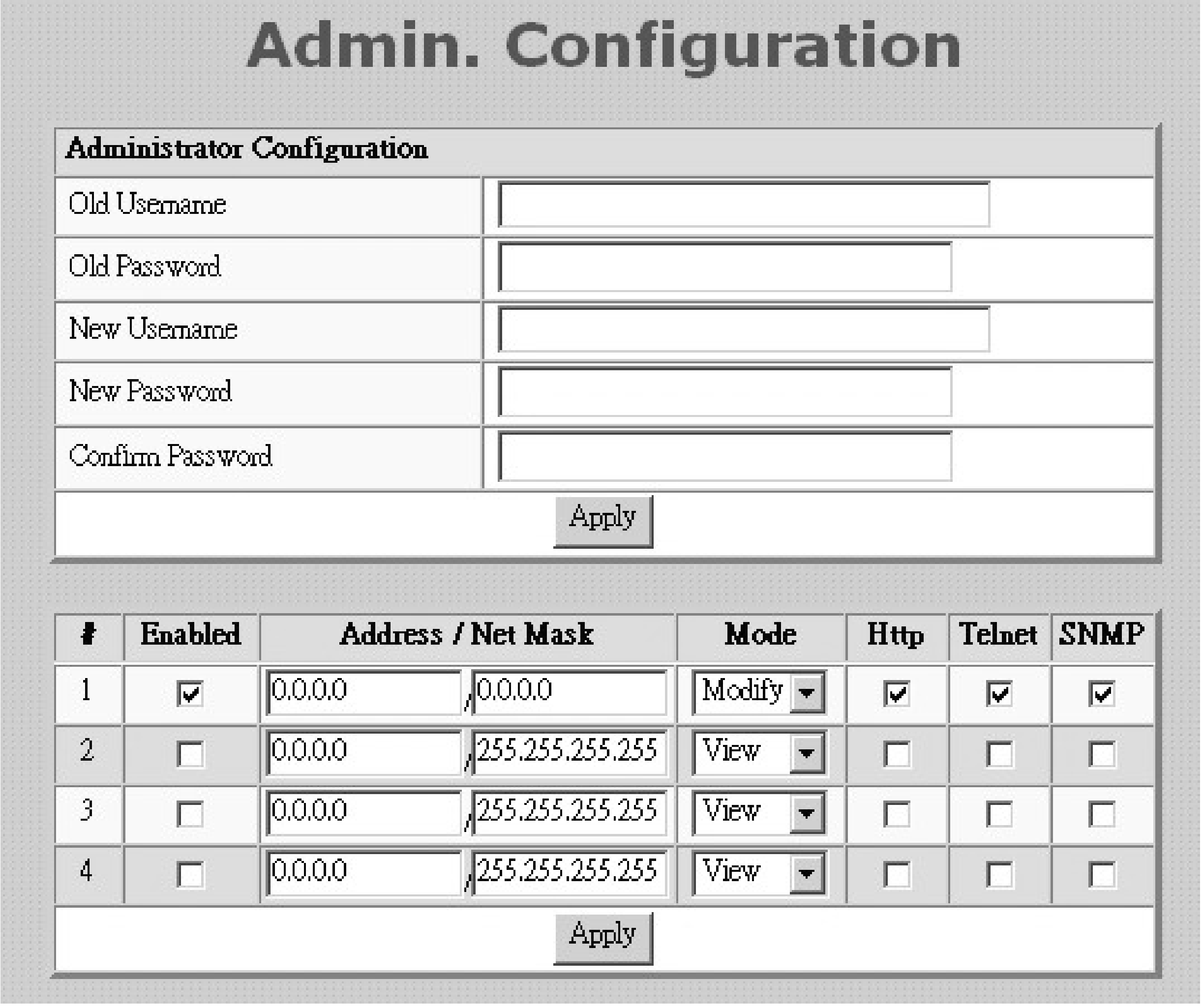
c. **ARL Aging** : You can enable/disable the aging operation of the switch and modify the aging time here. (Default is 300 seconds.)

d. **System Name / Location / Contact** : These information is useful for switch management in a network system. It is the system information used in SNMP protocol.

e. **DHCP / IP Address / Network Mask / Gateway** : This switch supports DHCP client function. If DHCP Client is enabled, this switch will try to get the IP configuration from DHCP server. If DHCP server is not found, it will use the default IP 192.168.1.5 instead. If DHCP Client is disabled, you can set IP address configuration of the switch here.

If any modification, click [Apply] to activate the new setting.

2. Admin. Configuration



Admin. Configuration

Administrator Configuration	
Old Username	
Old Password	
New Username	
New Password	
Confirm Password	
Apply	

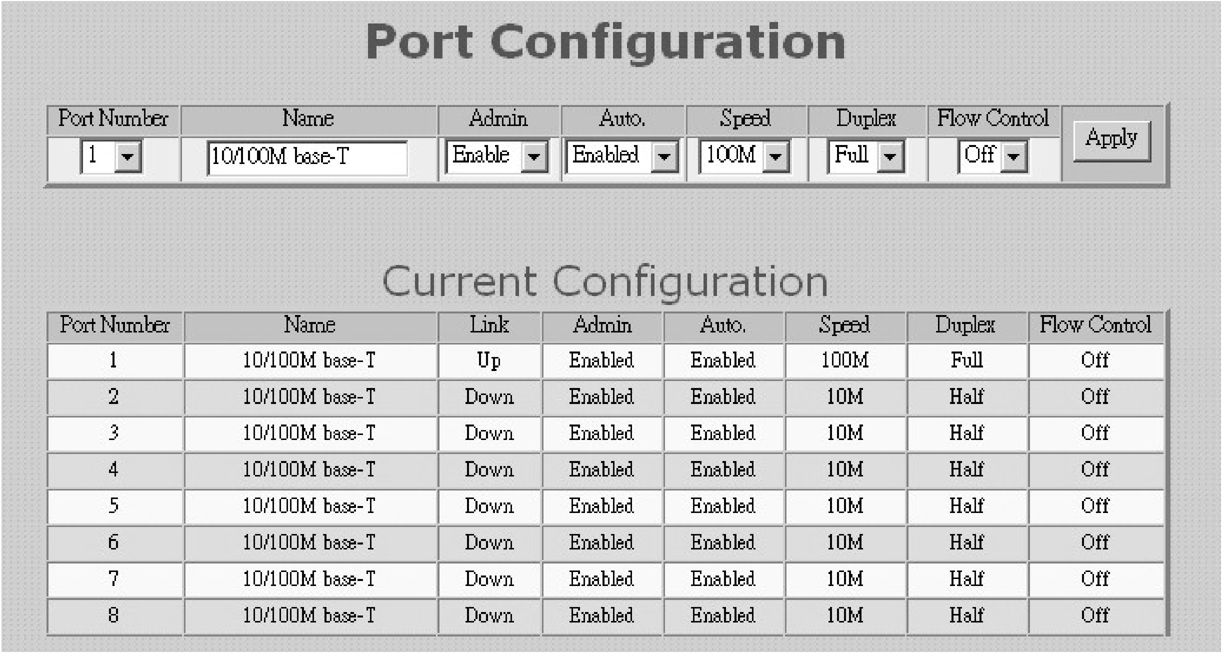
#	Enabled	Address / Net Mask		Mode	Http	Telnet	SNMP
1	☑	0.0.0.0	0.0.0.0	Modify	☑	☑	☑
2	□	0.0.0.0	255.255.255.255	View	□	□	□
3	□	0.0.0.0	255.255.255.255	View	□	□	□
4	□	0.0.0.0	255.255.255.255	View	□	□	□
Apply							

You can use this page to manage the administrator setting of the switch.

Administrator Configuration : This is for network administrator to change his/her username and password. (Default is admin/123456.)

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

3. Port Configuration



Port Configuration

Port Number	Name	Admin	Auto.	Speed	Duplex	Flow Control	
1	10/100M base-T	Enable	Enabled	100M	Full	Off	Apply

Current Configuration

Port Number	Name	Link	Admin	Auto.	Speed	Duplex	Flow Control
1	10/100M base-T	Up	Enabled	Enabled	100M	Full	Off
2	10/100M base-T	Down	Enabled	Enabled	10M	Half	Off
3	10/100M base-T	Down	Enabled	Enabled	10M	Half	Off
4	10/100M base-T	Down	Enabled	Enabled	10M	Half	Off
5	10/100M base-T	Down	Enabled	Enabled	10M	Half	Off
6	10/100M base-T	Down	Enabled	Enabled	10M	Half	Off
7	10/100M base-T	Down	Enabled	Enabled	10M	Half	Off
8	10/100M base-T	Down	Enabled	Enabled	10M	Half	Off

There are two parts in the setting page.

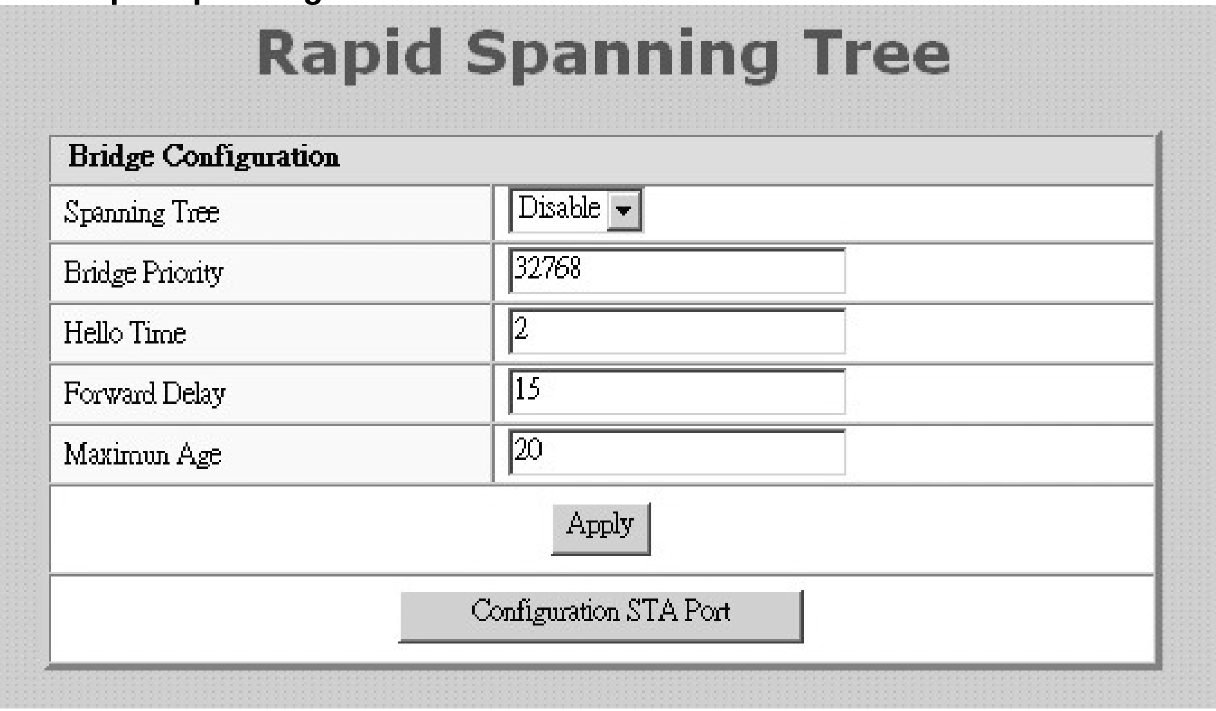
The *upper part* is for modifying the setting of port. Follow the steps to do it.

1. Select the port that you want to modify in “Port Number” 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. You can select the auto mode in *System Configuration* page.
5. Select the operation speed and duplex mode of the port if Auto is disabled in “Speed” and “Duplex”.
6. Select the Enable/Disable state of Flow Control function of port. (Note: Flow Control function will work if both Flow Control setting in Port Configuration and QoS is ON.)
7. Click [Apply] after any modification.

The *lower part* is current status of ports.
Name: The name of the port.
Link: It shows the link status of each port.
Admin: It shows current port enable/disable status.
Auto: It shows current Auto status of ports.
Speed: It shows the operation speed here when auto is disabled.
Duplex: It shows the operation duplex mode when auto is disabled.
Flow Control: It shows current Flow Control function status of ports.

Note: If 100FX port, only 100Mbps/Full Duplex setting is allowed (Auto disable).

4. Rapid Spanning Tree

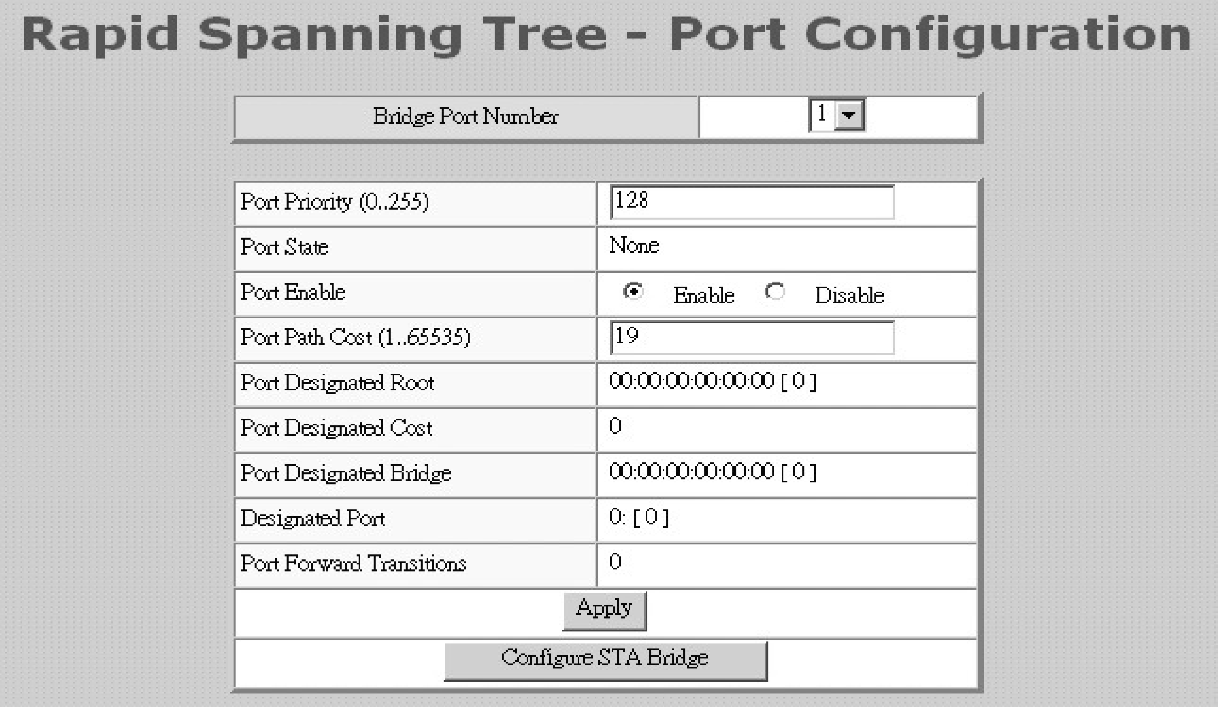


Rapid Spanning Tree

Bridge Configuration	
Spanning Tree	Disable
Bridge Priority	32768
Hello Time	2
Forward Delay	15
Maximun Age	20

In the page, users can enable/disable spanning tree function and configure the bridge parameters. Please refer to **9.17 of Section 6.2** for the details of these parameters. Press [Apply] after any modification.

Configuring port parameters for spanning tree, click [Configuration STA Port] and the configuration page will appear.



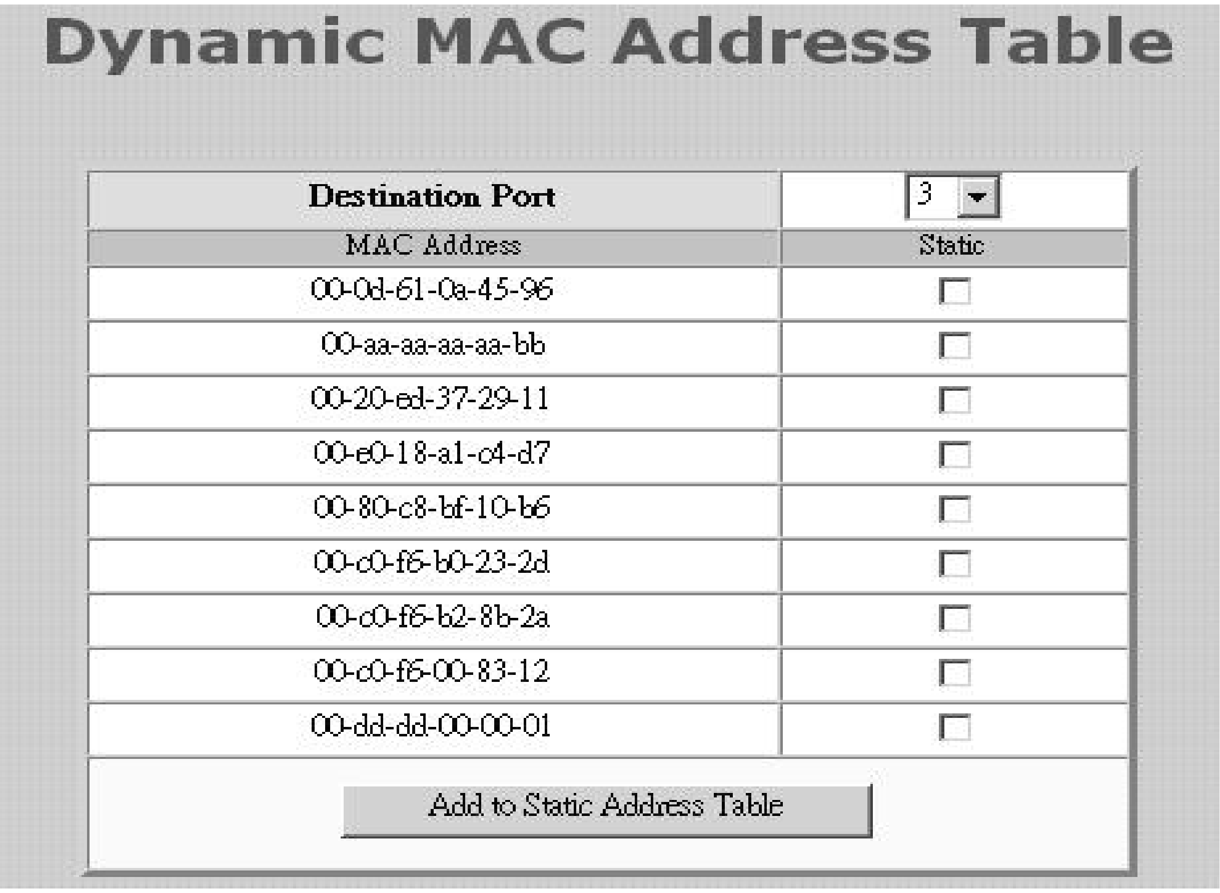
Rapid Spanning Tree - Port Configuration

Bridge Port Number	1

Port Priority (0..255)	128
Port State	None
Port Enable	● Enable ○ Disable
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	0: [0]
Port Forward Transitions	0

Users can select a port number and check its spanning tree status. Users can also modify these parameters. Please refer to **9.17 of Section 6.2** for the details of these parameters. Press [Apply] after any modification.

5. Dynamic Mac Address Table



Dynamic MAC Address Table

Destination Port	3 ▾
MAC Address	Static
00-0d-61-0a-45-96	□
00-aa-aa-aa-aa-bb	□
00-20-ed-37-29-11	□
00-e0-18-a1-c4-d7	□
00-80-c8-bf-10-b6	□
00-c0-f6-b0-23-2d	□
00-c0-f6-b2-8b-2a	□
00-c0-f6-00-83-12	□
00-dd-dd-00-00-01	□

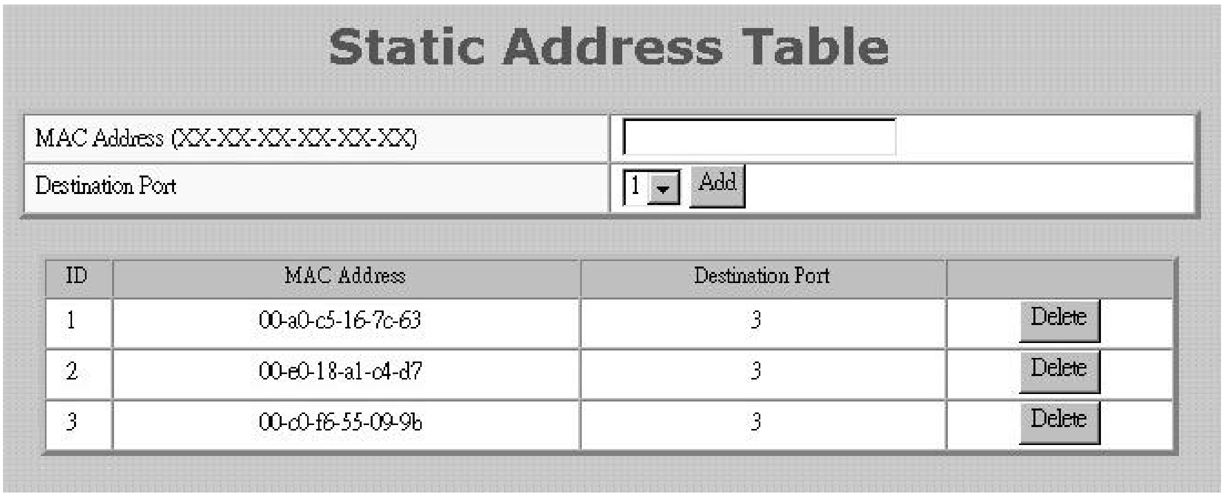
This web page will show the Mac address table content of the switch for connection ports. Select the port first and the Mac address learned by the switch on the port will be shown. Up to 128 Mac addresses will be shown.

Users can select the Mac addresses that will be assigned as the static Mac addresses for the port here. Click [Add to Static Address Table] after the selection. Then, the selected Mac addresses will be moved to Static Mac Address table and will not be shown in this table any more. Users can click "Static Address Table" at the left side of the web page to check the static address assignment.

For the details about Static Address, please refer to Section for "Static Address Table".

Note: Because of *aging time operation* of switch, wrong Mac addresses could be found in the Mac Address Table sometimes. These wrong Mac addresses are the machines that had ever accessed to the port and the switch learns them into the learning table. The switch will clear them when the aging time is up. Users can shorten the aging time and refresh the web page when they want to get the correct Mac address table content. Then, recover the aging time when the correct Mac address table content is got.

6. Static Address Table



Static Address Table

MAC Address (XX-XX-XX-XX-XX-XX)	
Destination Port	1 ▾ Add

ID	MAC Address	Destination Port	
1	00-a0-c5-16-7c-63	3	Delete
2	00-e0-18-a1-c4-d7	3	Delete
3	00-c0-f6-55-09-9b	3	Delete

This switch supports static Mac address assignment. Users can assign static Mac addresses by the two methods.

a. Select from the Mac address list in “Dynamic Mac Address Table” page.

b. Assign manual. Enter a Mac address and select the port, then add this entry to the static Mac address table.

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 assignment port*.

If users 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.

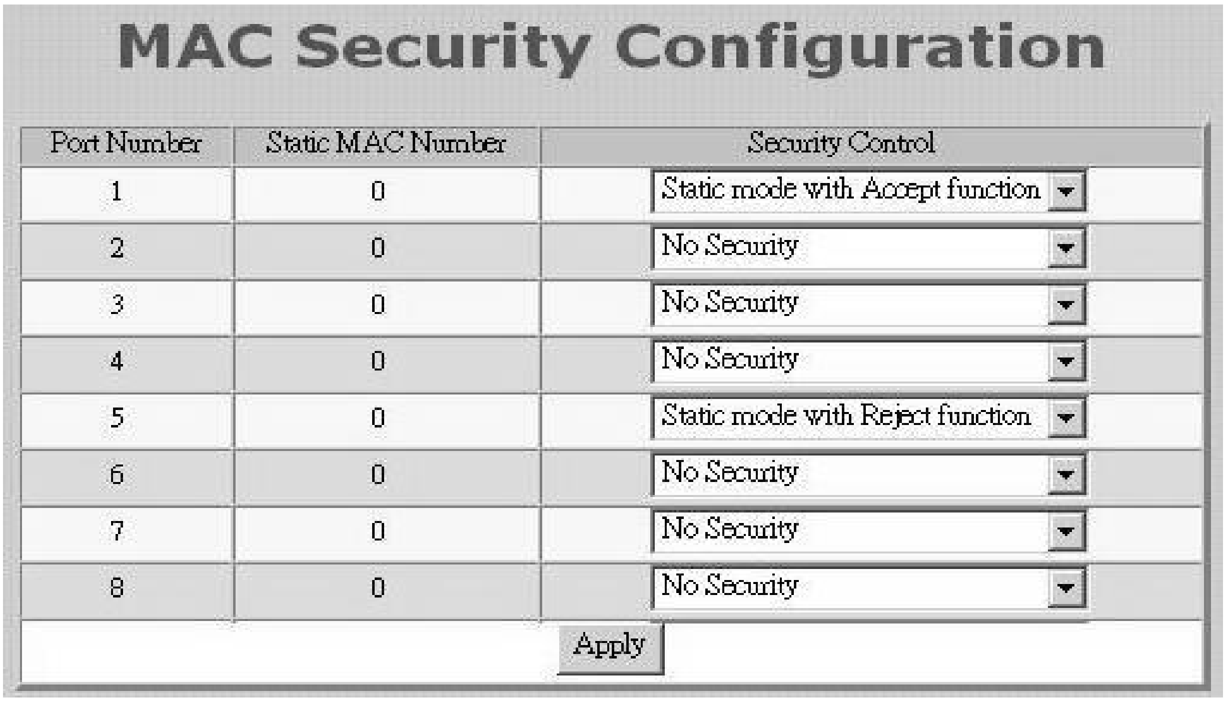
About Port Security function . . .

You can configure “Mac Security Configuration” function for port access security with Mac address. There are “Accept” and “Reject” modes for it.

“Accept” mode: Only the static address can access network via the port.

“Reject” mode: Only the static address cannot access network via the port.

7. Mac Security Configuration



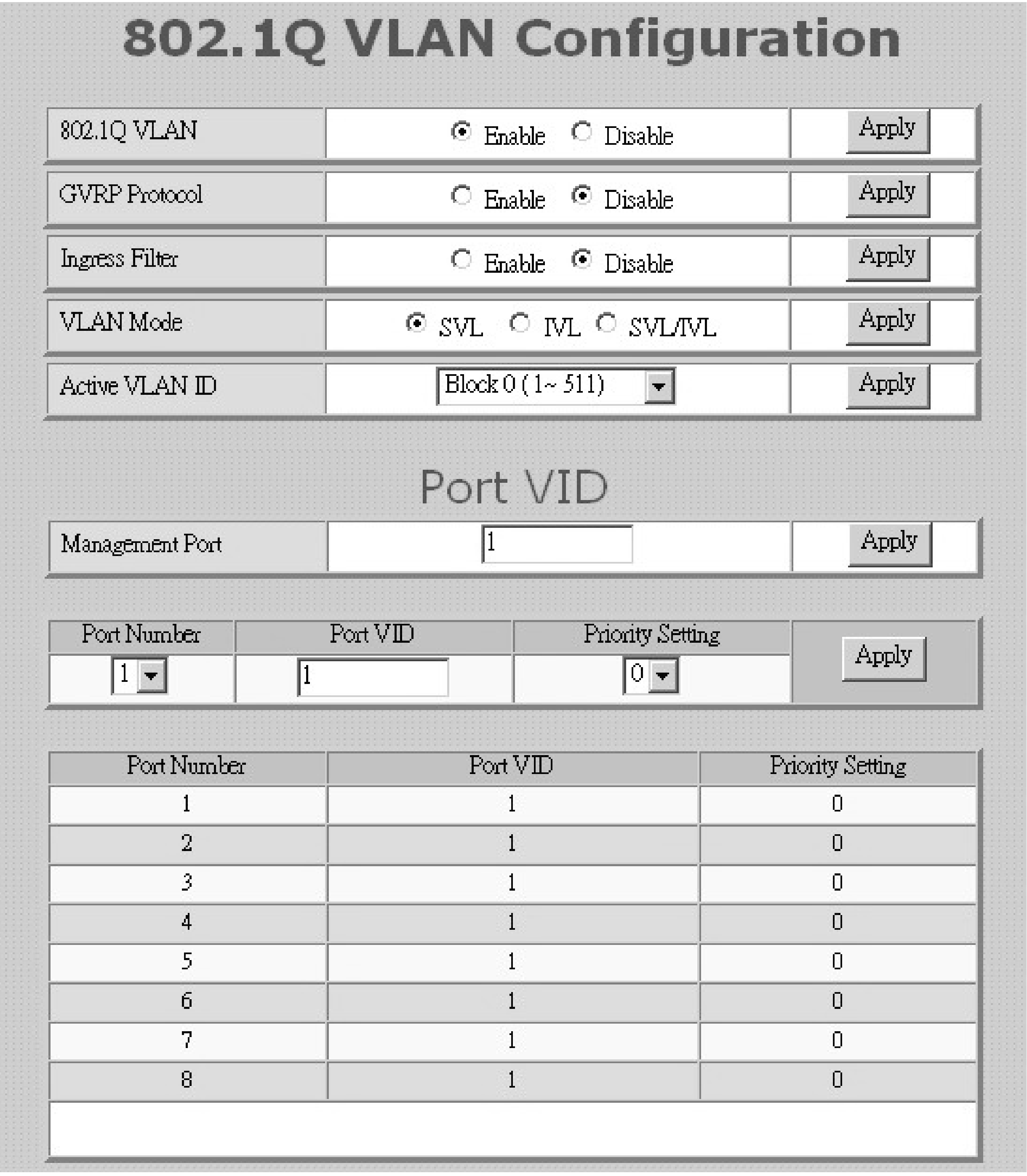
MAC Security Configuration

Port Number	Static MAC Number	Security Control
1	0	Static mode with Accept function
2	0	No Security
3	0	No Security
4	0	No Security
5	0	Static mode with Reject function
6	0	No Security
7	0	No Security
8	0	No Security

This function is used to set the security modes for static Mac address on the port. There could be three options for this function.

1. **No Security**: No any Mac address access limitation for the port, i.e. every Mac address could access network via the port.
2. **Static mode with Accept function**: Only the static Mac addresses can be accepted by the port, i.e. only the user with the static Mac address can access network via the port.
3. **Static mode with Reject function**: Only the static address will be rejected by the port, i.e. other Mac address except the static Mac address can access network via the port.

8. 802.1Q VLAN Configuration



802.1Q VLAN Configuration

802.1Q VLAN	● Enable ○ Disable	Apply
GVRP Protocol	○ Enable ● Disable	Apply
Ingress Filter	○ Enable ● Disable	Apply
VLAN Mode	● SVL ○ IVL ○ SVL/IVL	Apply
Active VLAN ID	Block 0 (1~ 511)	Apply

Port VID

Management Port	1	Apply

Port Number	Port VID	Priority Setting	
1	1	0	Apply

Port Number	Port VID	Priority Setting
1	1	0
2	1	0
3	1	0
4	1	0
5	1	0
6	1	0
7	1	0
8	1	0

This function is used to configure 802.1Q VLAN function.

802.1Q VLAN: This function can enable/disable 802.1Q VLAN operation.

GVRP Protocol: The GVRP protocol can learn remote 802.1Q VLAN on other devices and add to dynamic 802.1Q VLAN table. You can enable/disable the operation of this protocol.

Ingress Filter: The ingress-filter function is for doing VLAN filtering at ingress port. If the VLAN of the packet is in the same VLAN of the ingress port, it will be forwarded to egress port. Otherwise, it will be discarded.

VLAN Mode: This function can select different VLAN modes of 802.1Q VLAN operation. There are three modes for VLAN function – SVL (Shared VLAN), IVL (Individual VLAN) and SVL/IVL.
SVL mode – the switch will do packet forwarding according to its Mac address only.
IVL mode – the switch will do packet forwarding according to its Mac address and its VLAN ID.
SVL/IVL mode – its operation is the same as IVL mode but for untagged port is used as the uplink port in MDU/MTU application.
For most VLAN applications, SVL mode is OK.

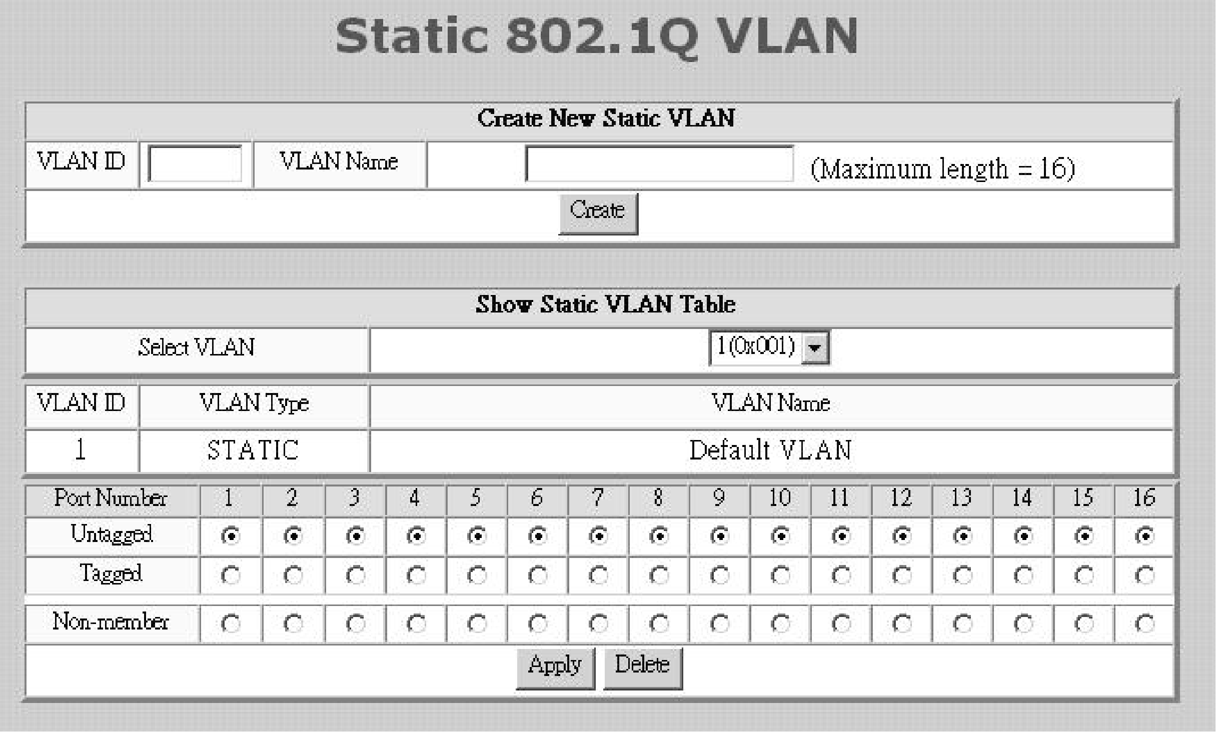
Active VLAN ID: This function is used to set active VLAN ID block range for 802.1Q VLAN operation. The valid VLAN ID number is 1 ~ 4094. Because this switch can support up to 512 active VLAN ID number, the valid VLAN ID number is divided into eight blocks as below.

Block	Active VID	Block	Active VID
0	1 ~ 511	4	2048 ~ 2559
1	512 ~ 1023	5	2560 ~ 3071
2	1024 ~ 1535	6	3072 ~ 3583
3	1536 ~ 2047	7	3584 ~ 4094

Select one of the blocks and only the selected VLAN ID range is active for 802.1Q VLAN operation of the switch.

Port VID: This setting is for untagged packet translated to tagged packet. The Port VID and Priority Setting will be used for tag adding in the translation. The ***Management Port*** is the management interface of the switch. You can configure its PVID here. It will limit *only the users in the VLAN with VLAN ID equal to Management Port PVID can manage the switch from network by Http, Telnet and SNMP*.
You can select the port in Port Number first. Then assign the Port VID and priority for it. Click [Apply] to complete the setting.

9. Static 802.1Q VLAN



Static 802.1Q VLAN

Create New Static VLAN			
VLAN ID		VLAN Name	(Maximum length = 16)
Create			

Show Static VLAN Table	
Select VLAN	1(0x001)

VLAN ID	VLAN Type	VLAN Name
1	STATIC	Default VLAN

Port Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Untagged	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Tagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Non-member	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

You can create static 802.1Q VLAN group here. You need to input the VLAN ID and VLAN Name to create a VLAN. The valid VLAN ID is 1 ~ 4094. The VLAN ID should be in the active VLAN ID block set in “802.1Q VLAN Configuration” page.

After a VLAN is created, you can select the VLAN in “**Show Static VLAN Table**” to get the configuration of the VLAN. The new VLAN is empty by default. You can select the port for the VLAN and tagged/untagged for it. After that, click [Apply] to complete the VLAN configuration. (It is also for VLAN modification.)

About Tagged/Untagged

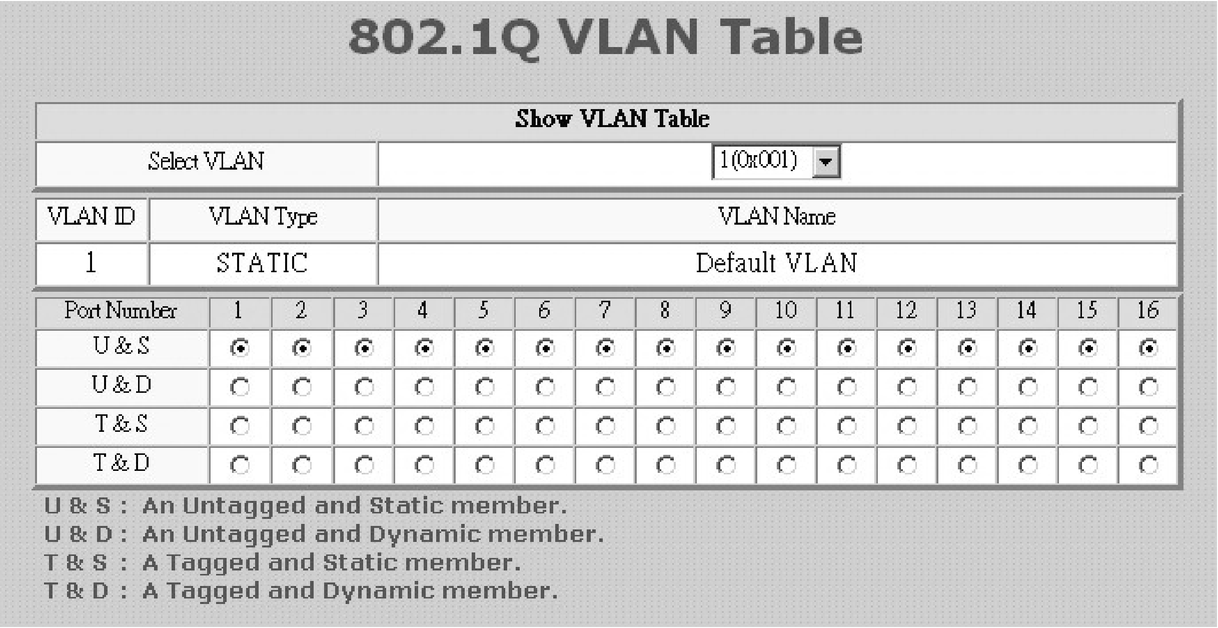
The tagged port will always send out packets with tag. If untagged packet is received from ingress port, tag will be added with the PVID setting of ingress port before forwarded to tagged port. The 802.1Q VLAN information will be carried in the tag.

The untagged port will always send out packets without tag. If tagged packet is received from ingress port, tag will be removed from the packet before forwarded to untagged port. Most the network adapters or devices are untagged devices. If they are connected to tagged port, they will fail to access network because of the tag in packet.

About Switch Management from Users

Only the users in the same VLAN as Management Port PVID (set in “802.1Q VLAN Configuration” page) can manage the switch via Web/Telnet/SNMP. The users in other VLAN cannot manage the switch from network.

10. 802.1Q VLAN Table



802.1Q VLAN Table

Show VLAN Table	
Select VLAN	1(0x001)

VLAN ID	VLAN Type	VLAN Name
1	STATIC	Default VLAN

Port Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
U & S	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
U & D	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
T & S	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
T & D	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

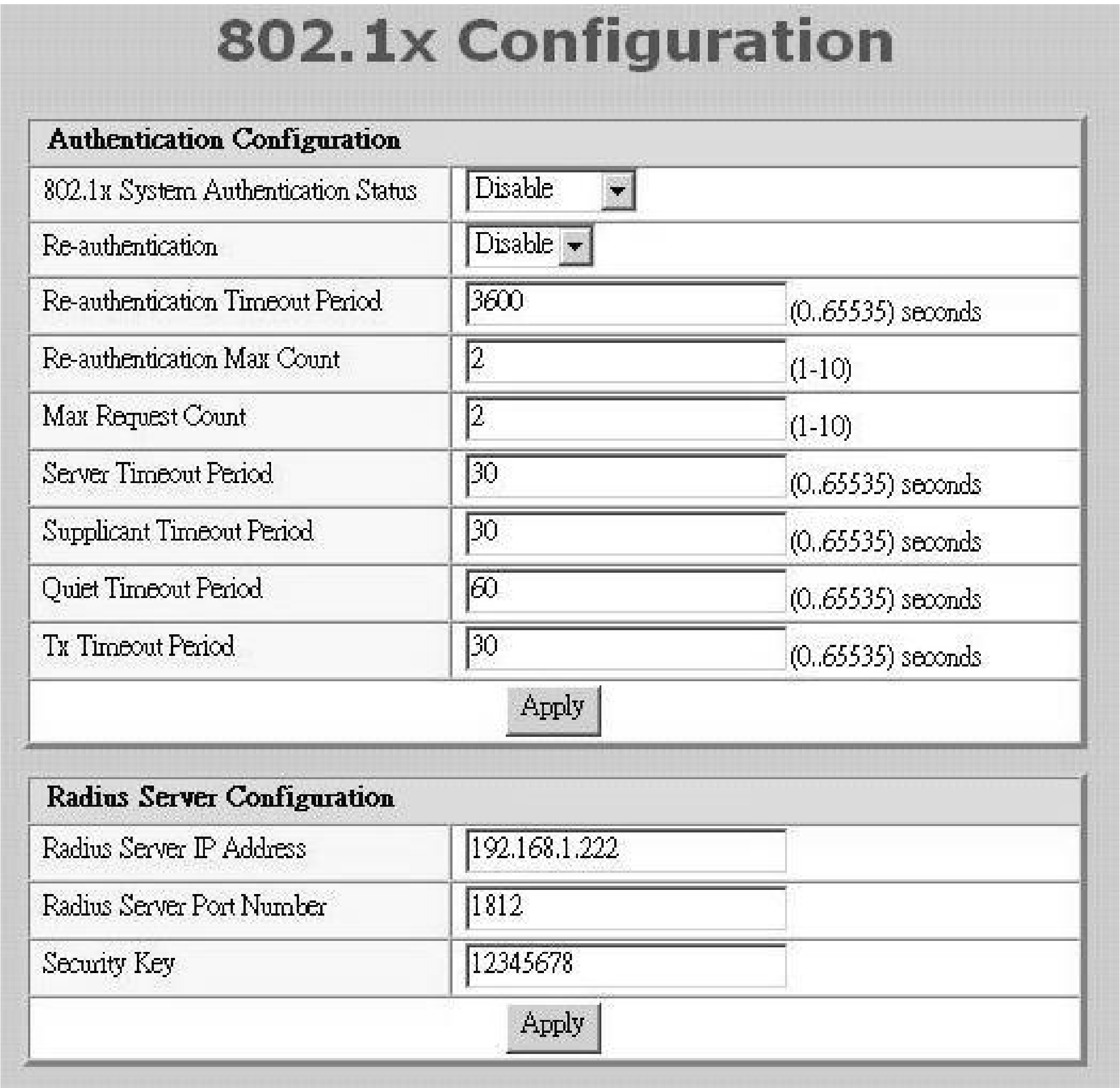
U & S : An Untagged and Static member.
U & D : An Untagged and Dynamic member.
T & S : A Tagged and Static member.
T & D : A Tagged and Dynamic member.

This table will show the activity of 802.1Q VLAN.

Select a VLAN in “**Show VLAN Table**”. The 802.1Q VLAN activity status will be shown for the selected VLAN.

If GVRP protocol is enabled, this table will also show the learned remote 802.1Q VLAN.

11. 802.1x Configuration



802.1x Configuration

Authentication Configuration		
802.1x System Authentication Status	Disable	
Re-authentication	Disable	
Re-authentication Timeout Period	3600	(0..65535) seconds
Re-authentication Max Count	2	(1-10)
Max Request Count	2	(1-10)
Server Timeout Period	30	(0..65535) seconds
Supplicant Timeout Period	30	(0..65535) seconds
Quiet Timeout Period	60	(0..65535) seconds
Tx Timeout Period	30	(0..65535) seconds

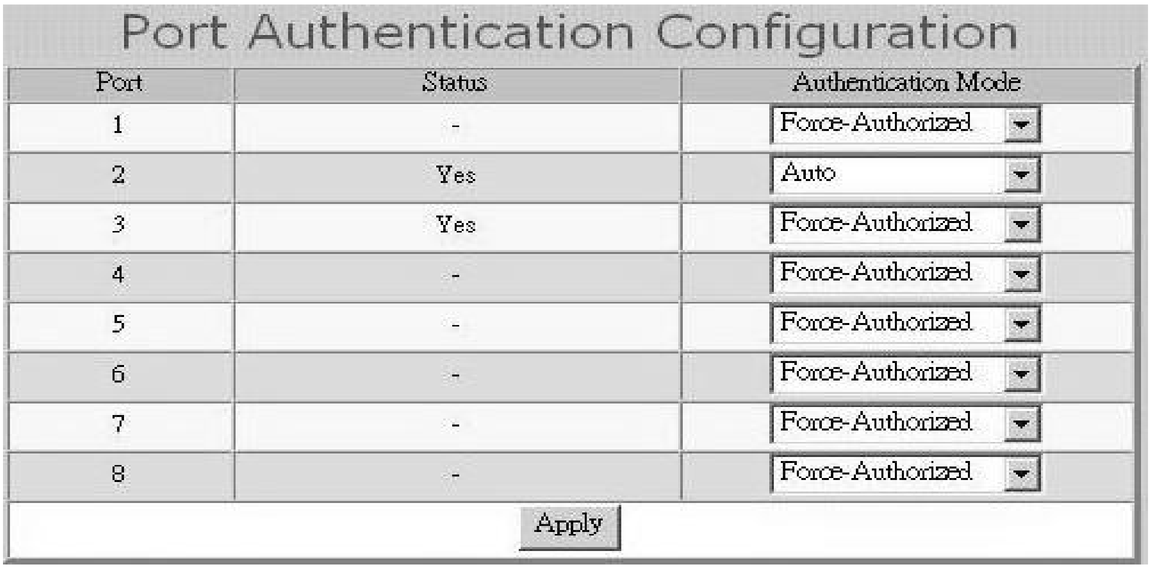
Radius Server Configuration	
Radius Server IP Address	192.168.1.222
Radius Server Port Number	1812
Security Key	12345678

The 802.1x function can limit the port access for authentication users only. It needs a RADIUS server for the authentication process and the switch acts as an authenticator.

The function here is for 802.1x function configuration.

1. 802.1x System Authentication Status: [Enable/Disable/Transparent]
   Enable: enable 802.1x function in authentication mode
   Disable: disable 802.1x function, 802.1x protocol packets will be dropped.
   Transparent: 802.1x protocol packets will be forwarded but no authentication function working.
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.
7. Radius Server Configuration:
   This is for configuration between switch and RADIUS server.



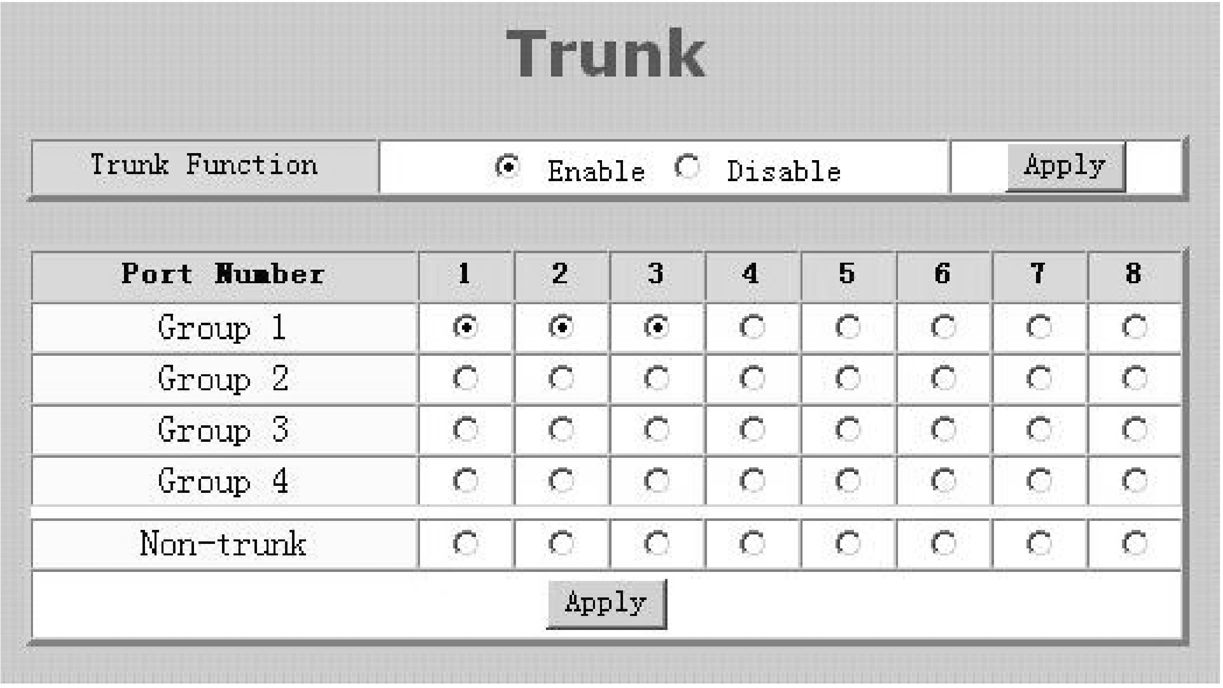
Port Authentication Configuration

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

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.

12. Trunk



Trunk

Trunk Function	● Enable ○ Disable	Apply

Port Number	1	2	3	4	5	6	7	8
Group 1	●	●	●	○	○	○	○	○
Group 2	○	○	○	○	○	○	○	○
Group 3	○	○	○	○	○	○	○	○
Group 4	○	○	○	○	○	○	○	○
Non-trunk	○	○	○	○	○	○	○	○

Apply

This switch supports 4 trunk groups and they are null by default. If users want to use trunk function, follow the steps to configure it.

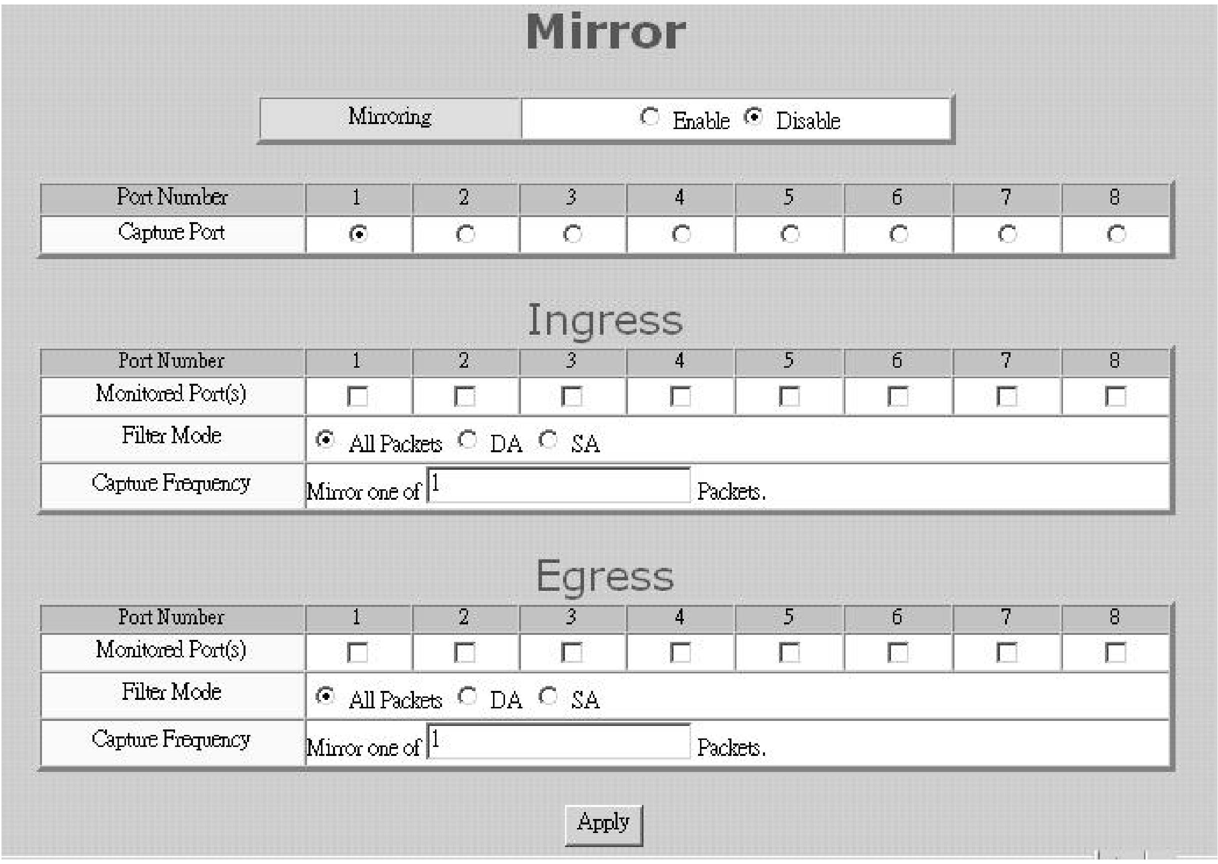
a. Enable Trunk function first.
b. Assign ports to the trunk. Then click [Apply].
c. If you want to remove ports from trunk, put them to Non-trunk and click [Apply]. The selected ports will be removed from trunk groups.

If users want to disable trunk function, select "Disable" and click [Apply] button. The switch will clear the Trunk configuration.

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 in the trunk connection automatically.

13. Mirror



Mirror

Mirroring	○ Enable ● Disable

Port Number	1	2	3	4	5	6	7	8
Capture Port	●	○	○	○	○	○	○	○

Ingress

Port Number	1	2	3	4	5	6	7	8
Monitored Port(s)	□	□	□	□	□	□	□	□
Filter Mode	● All Packets ○ DA ○ SA							
Capture Frequency	Mirror one of 1 Packets.							

Egress

Port Number	1	2	3	4	5	6	7	8
Monitored Port(s)	□	□	□	□	□	□	□	□
Filter Mode	● All Packets ○ DA ○ SA							
Capture Frequency	Mirror one of 1 Packets.							

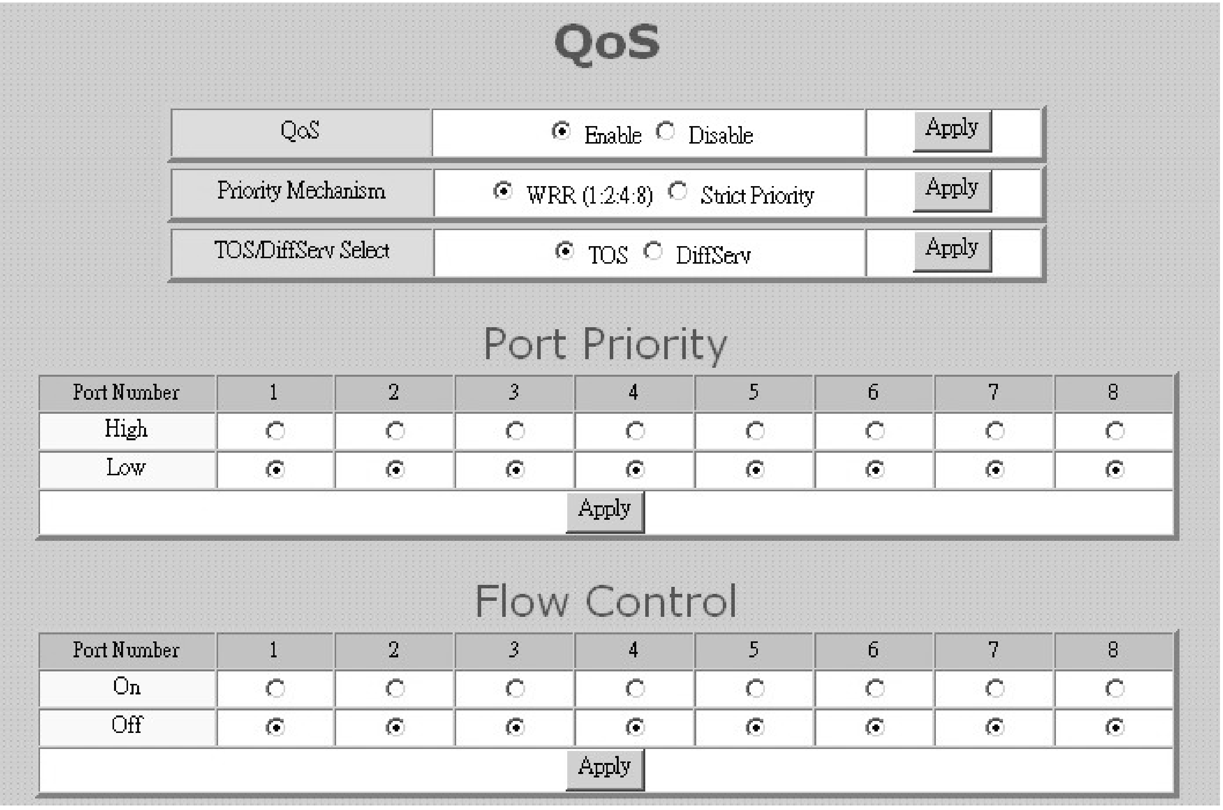
Follow the steps to configure Mirror function.

a. Enable Mirroring first.
b. Select the capture port.
c. Select the monitored port from Ingress or Egress table – depending on the traffic direction.
d. Select the capture mode – All packets or for some special DA/SA address. If DA/SA is selected, enter the special Mac address in "xx-xx-xx-xx-xx-xx" format.
e. Select the capture frequency.
f. Press [Apply] button.

If users want to disable Mirror function, select Disable and click [Apply].

Note: For 24+2FX model, the capture port and monitored port is suggested at the same port groups (Port 1~8, 9~16, 17~24 are three port groups).

14. QoS



QoS

QoS	● Enable ○ Disable	Apply
Priority Mechanism	● WRR (1:2:4:8) ○ Strict Priority	Apply
TOS/DiffServ Select	● TOS ○ DiffServ	Apply

Port Priority

Port Number	1	2	3	4	5	6	7	8
High	○	○	○	○	○	○	○	○
Low	●	●	●	●	●	●	●	●

Flow Control

Port Number	1	2	3	4	5	6	7	8
On	○	○	○	○	○	○	○	○
Off	●	●	●	●	●	●	●	●

This switch support port-based priority, 802.1P priority, and ToS/DiffServ priority operation. And there are four priorities (P0~P3) for each port. The traffic scheduling for each port could be SP(Strict Priority) for highest priority or WRR (Weighted Round Robin with 1:2:4:8) for the four priority queues.

Follow the steps to configure QoS function.

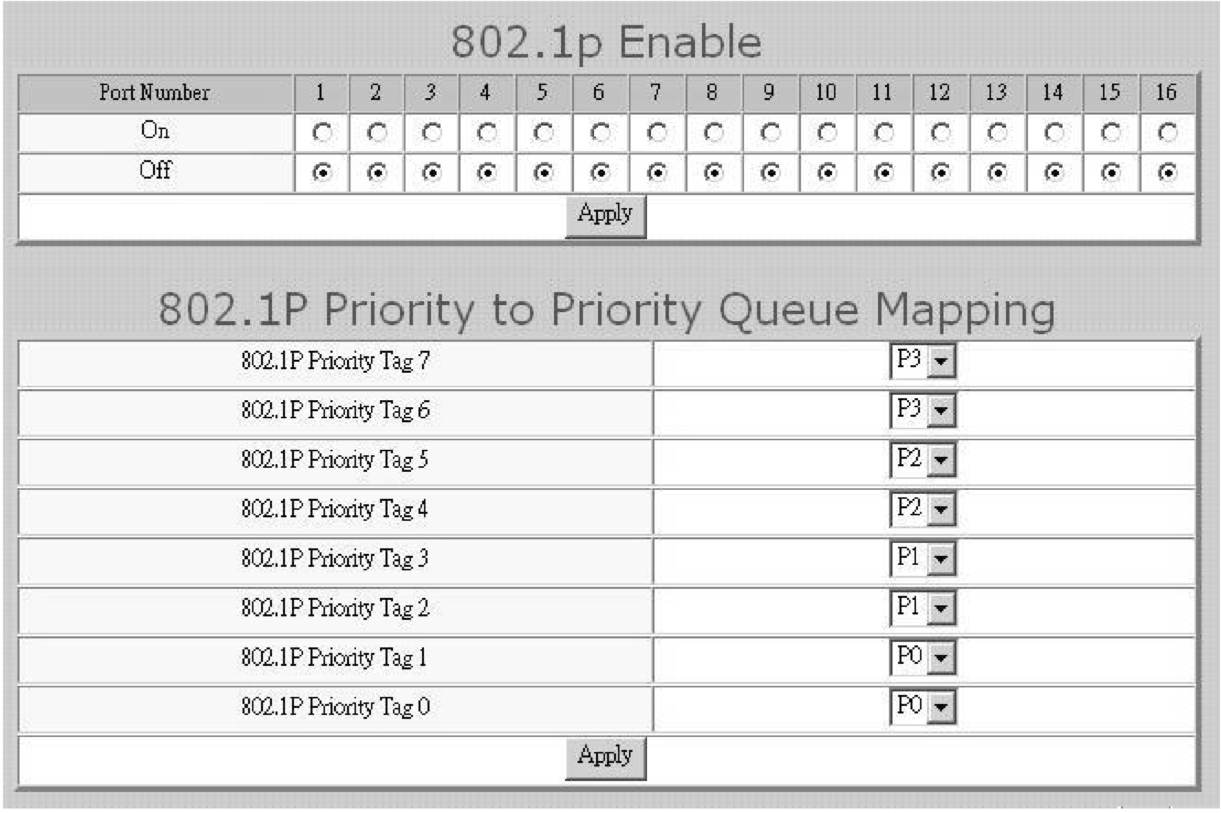
a. Enable QoS first.

b. Select the traffic scheduling method in Priority Mechanism.

c. Setting the Flow Control. There is also a Flow Control option in “Port Configuration” page. If Flow Control is ON at both “Port Configuration” page and “QoS” page, the Flow Control function of a port is ON. Otherwise, it is OFF. If you don’t expect any packet lost, set the Flow Control function ON. But it will conflict with the real QoS request because packets will be paused by the switch when congestion happens. And the switch cannot do the QoS request for the packets.

d. If port-based priority is used, select ports for High and Low priorities. The packets from High priority port will be forwarded to highest priority queue on egress port. And the packets from Low priority port will be forwarded to lowest priority queue on egress port.

e. If 802.1P priority is used, select the ports that enable the 802.1P priority function, i.e. it will forward packets with the priority information in tag. Then you can configure the 802.1P priority (0~7) mapping to priority queue of port.



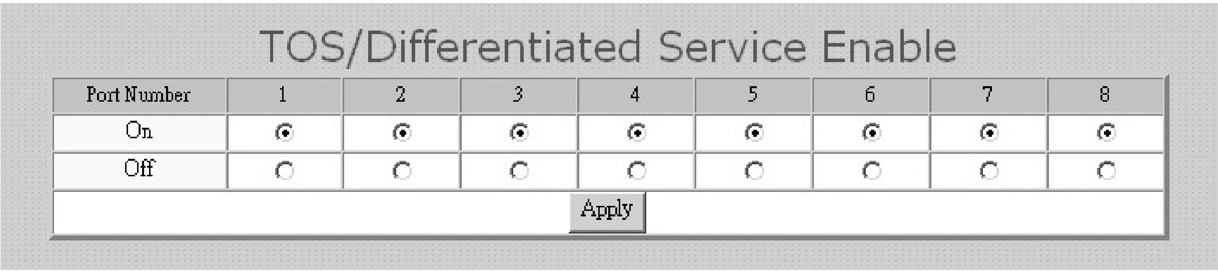
802.1p Enable

Port Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
On	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Off	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

802.1P Priority to Priority Queue Mapping

802.1P Priority Tag 7	P3
802.1P Priority Tag 6	P3
802.1P Priority Tag 5	P2
802.1P Priority Tag 4	P2
802.1P Priority Tag 3	P1
802.1P Priority Tag 2	P1
802.1P Priority Tag 1	P0
802.1P Priority Tag 0	P0

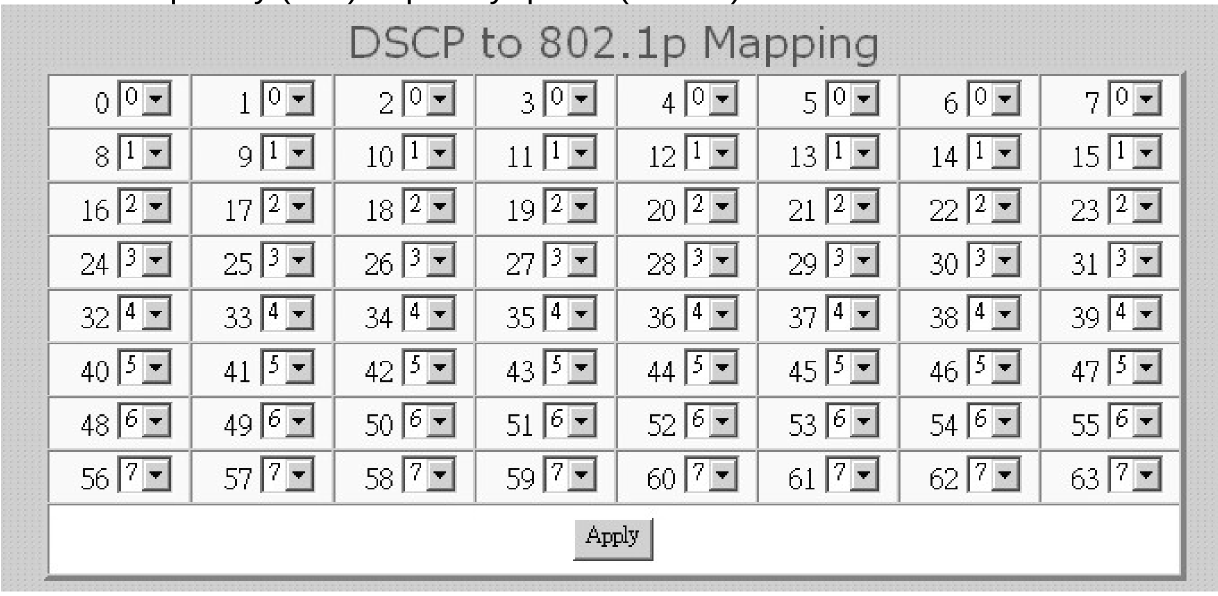
f. If ToS/DiffServ priority is used, select the ports that enable the TOS/Differentiated Service priority function, i.e. it will forward packets with the priority information in IP Header. Then select TOS or DiffServ in [TOS/DiffServ Select].



TOS/Differentiated Service Enable

Port Number	1	2	3	4	5	6	7	8
On	●	●	●	●	●	●	●	●
Off	○	○	○	○	○	○	○	○

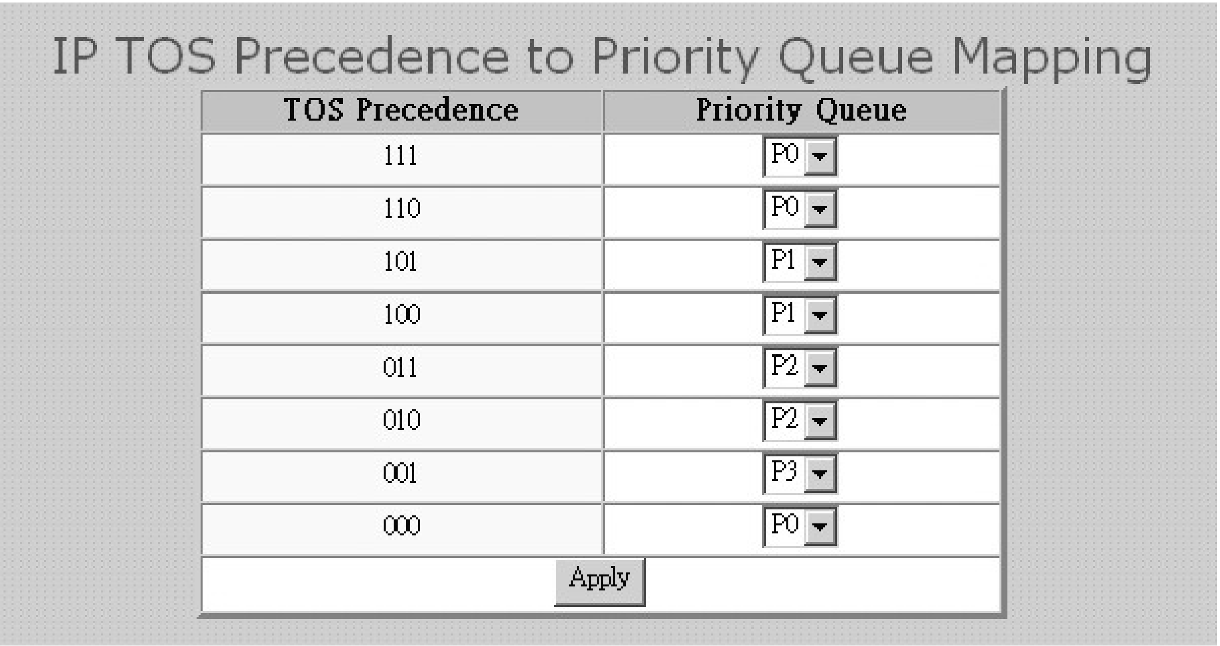
g. If DiffServ priority will be applied, assign 802.1P priority (0~7) to each DSCP value (0~63). Then it will map to priority queue through the mapping of 802.1P priority (0~7) to priority queue (P0~P3).



DSCP to 802.1p Mapping

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

h. If TOS priority will be applied, assign the TOS Precedence (0~7) to priority queue (P0~P3) mapping.



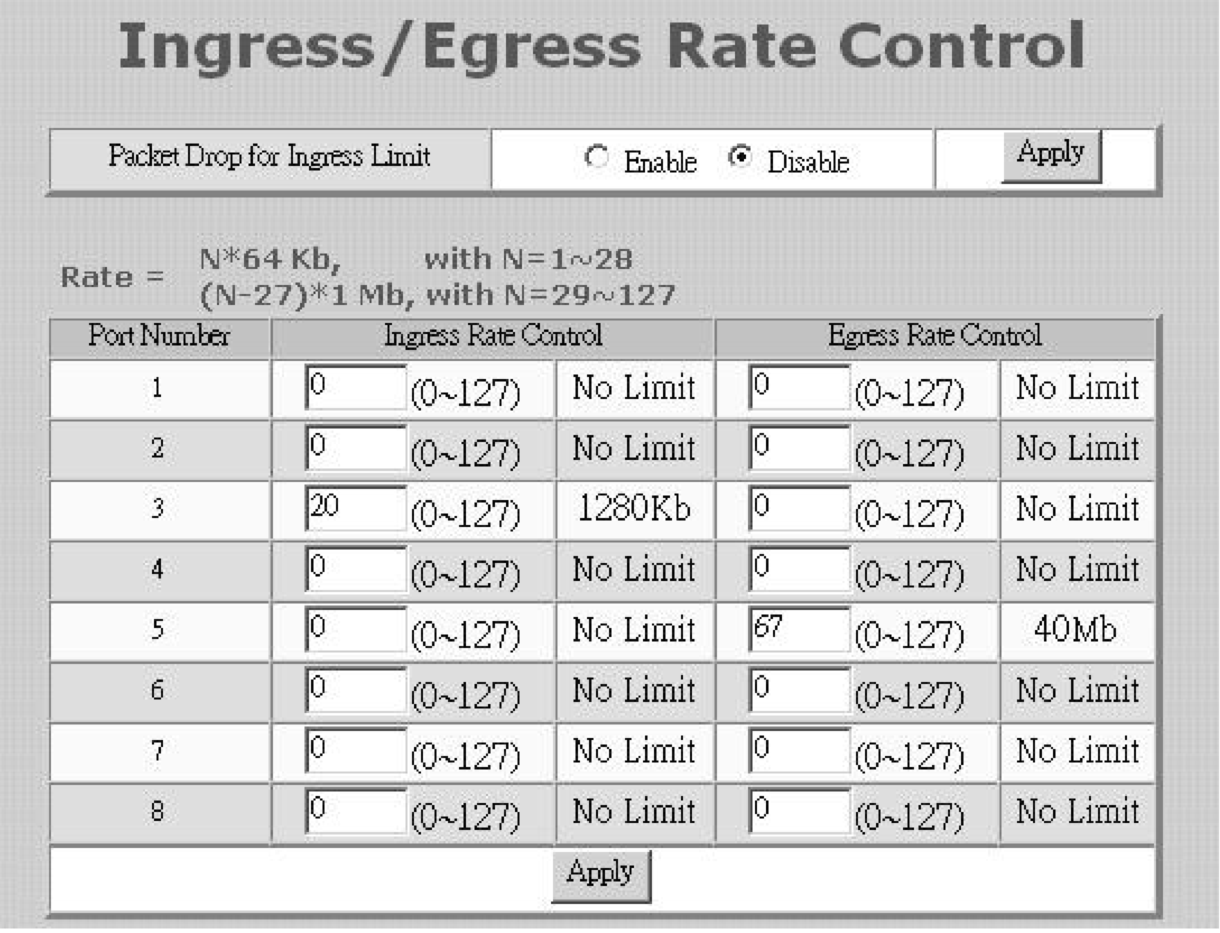
IP TOS Precedence to Priority Queue Mapping

TOS Precedence	Priority Queue
111	P0
110	P0
101	P1
100	P1
011	P2
010	P2
001	P3
000	P0

Click [Apply] to activate the setting after configuration.

If you want to disable QoS operation, select Disable and click [Apply] button.

15. Rate Control



Ingress/Egress Rate Control

Packet Drop for Ingress Limit	○ Enable ● Disable	Apply

Rate = N*64 Kb, with N=1~28
(N-27)*1 Mb, with N=29~127

Port Number	Ingress Rate Control		Egress Rate Control	
1	0 (0~127)	No Limit	0 (0~127)	No Limit
2	0 (0~127)	No Limit	0 (0~127)	No Limit
3	20 (0~127)	1280Kb	0 (0~127)	No Limit
4	0 (0~127)	No Limit	0 (0~127)	No Limit
5	0 (0~127)	No Limit	67 (0~127)	40Mb
6	0 (0~127)	No Limit	0 (0~127)	No Limit
7	0 (0~127)	No Limit	0 (0~127)	No Limit
8	0 (0~127)	No Limit	0 (0~127)	No Limit

The rate control function can limit the maximum traffic rate for each physical port. The traffic could be ingress traffic or egress traffic.

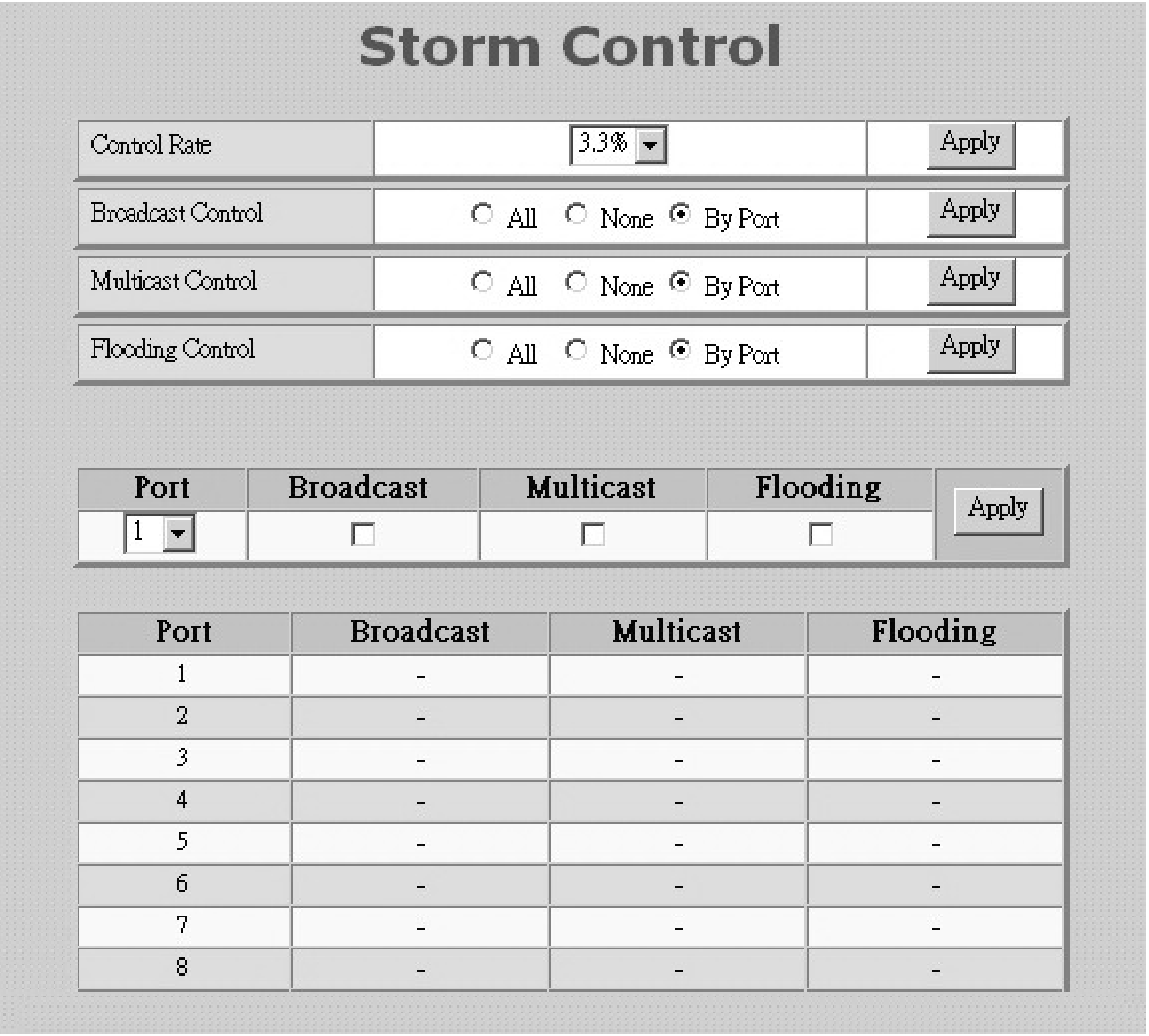
The rate control range is 64Kbps ~ 100Mbps. Here is the rule for the setting.

Maximum Rate	Rate Control Number (N)	Rule
No Limit	0	0 means no limit.
64K,128K,192K,…,1792Kbps	1 ~ 28	Rate = N x 64Kbps
2M,3M,4M, …,100Mbps	29 ~ 127	Rate = (N-27) x 1Mbps

For example, if you want to limit the download traffic rate of Port 2 to 512Kbps, you should set the Egress Rate Control of Port 2 to 8 (8=512/64 and egress is for download operation and ingress is for upload operation).

The **Packet Drop for Ingress Limit** is for packet dropping operation when ingress traffic rate exceeds the Ingress Rate Control. If it is enabled, the extra packets will be dropped to limit the ingress traffic rate. If it is disabled, flow control function will be used to pause the ingress traffic.

16. Storm Control



Storm Control

Control Rate	3.3% ▾	Apply
Broadcast Control	○ All ○ None ● By Port	Apply
Multicast Control	○ All ○ None ● By Port	Apply
Flooding Control	○ All ○ None ● By Port	Apply

Port	Broadcast	Multicast	Flooding	
1 ▾	□	□	□	Apply

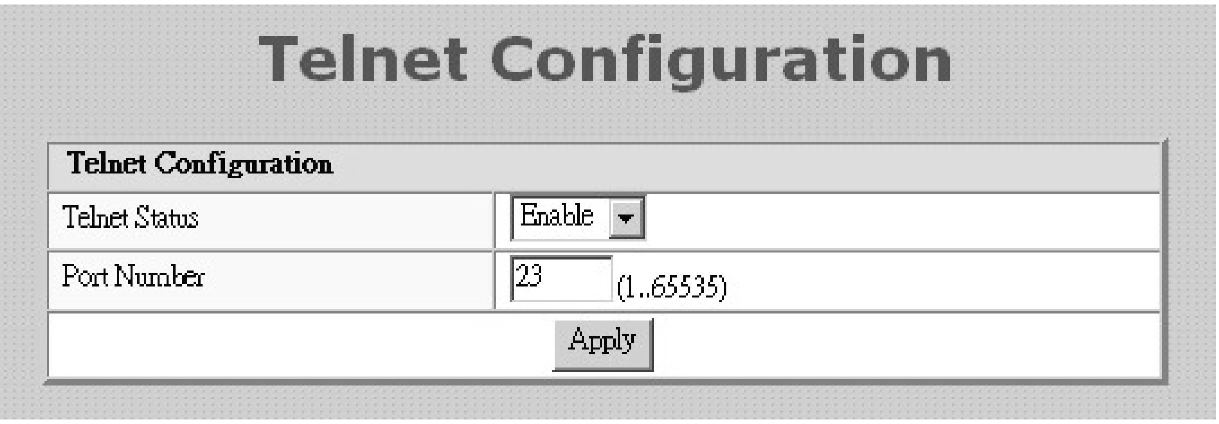
Port	Broadcast	Multicast	Flooding
1	-	-	-
2	-	-	-
3	-	-	-
4	-	-	-
5	-	-	-
6	-	-	-
7	-	-	-
8	-	-	-

The storm control function can limit the maximum traffic rate for packet storm. There are three traffic storms could be limited – broadcast storm, multicast storm and flooding packet storm. You can enable the storm control by port. Follow the steps to do the storm control settings.

1. Select the control rate.
2. Select which storm will be controlled and which ports will be applied – all of the ports, none of the ports or selected by port in the table.
3. If “By Port” is selected, select the port and select the storm control. Then click [Apply].

<u>Note</u>:
Broadcast – it is ”one to all” traffic. Every port will receive the packets.
Multicast – it is ”one to many” traffic. A group of ports will receive the packets.
Flooding - it is “one to all” traffic caused by Mac address not found in the switch. Every port will receive the packets.

17. Telnet



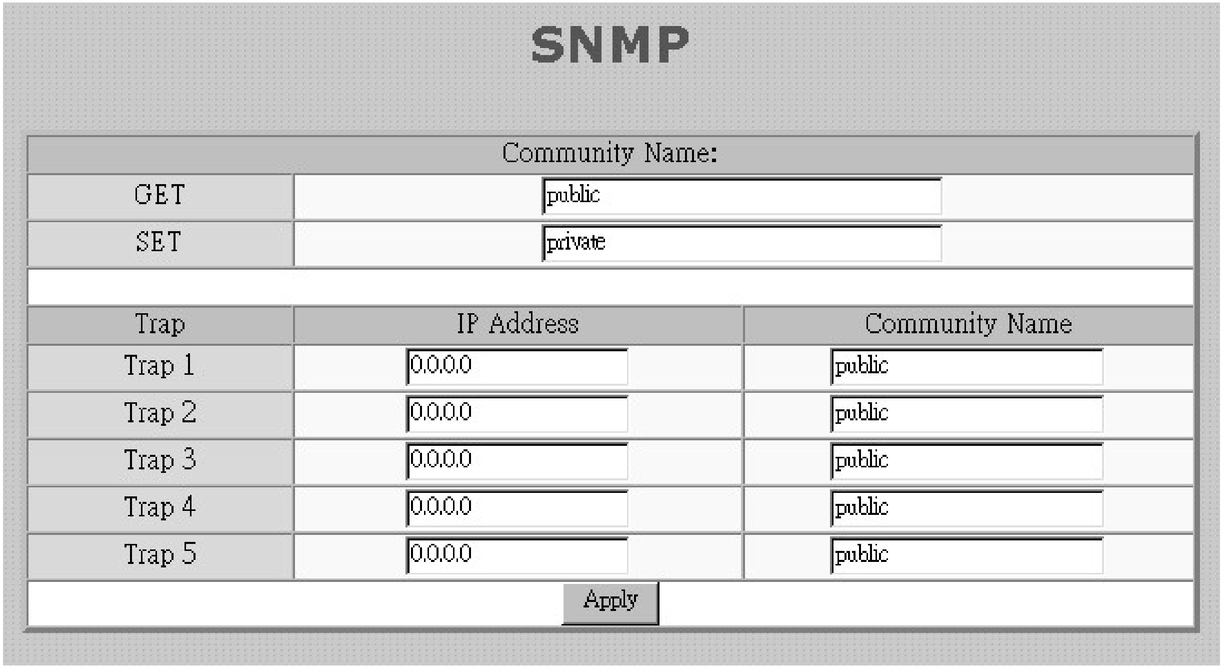
Telnet Configuration

Telnet Configuration	
Telnet Status	Enable
Port Number	23 (1..65535)

In this page, user can enable/disable Telnet function of the switch in [Telnet Status].

And user can change the service port number for Telnet service of the switch.

18. SNMP

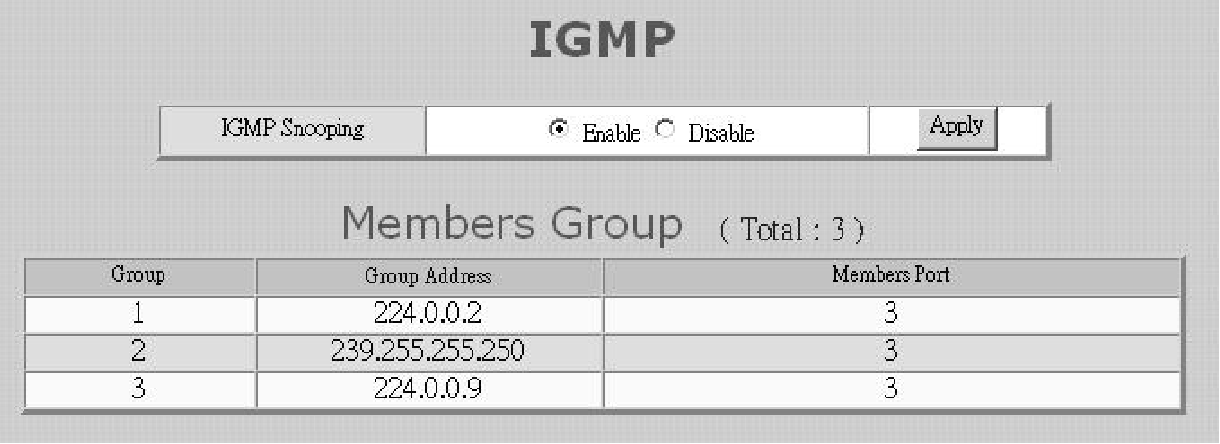


SNMP

Community Name:		
GET	public	
SET	private	
Trap	IP Address	Community Name
Trap 1	0.0.0.0	public
Trap 2	0.0.0.0	public
Trap 3	0.0.0.0	public
Trap 4	0.0.0.0	public
Trap 5	0.0.0.0	public

In this page, users can configure GET/SET/Trap Community Name and the IP address for trap operation. Then users can manage this switch with these settings from SNMP management program.

19. IGMP



IGMP

IGMP Snooping	● Enable ○ Disable	Apply

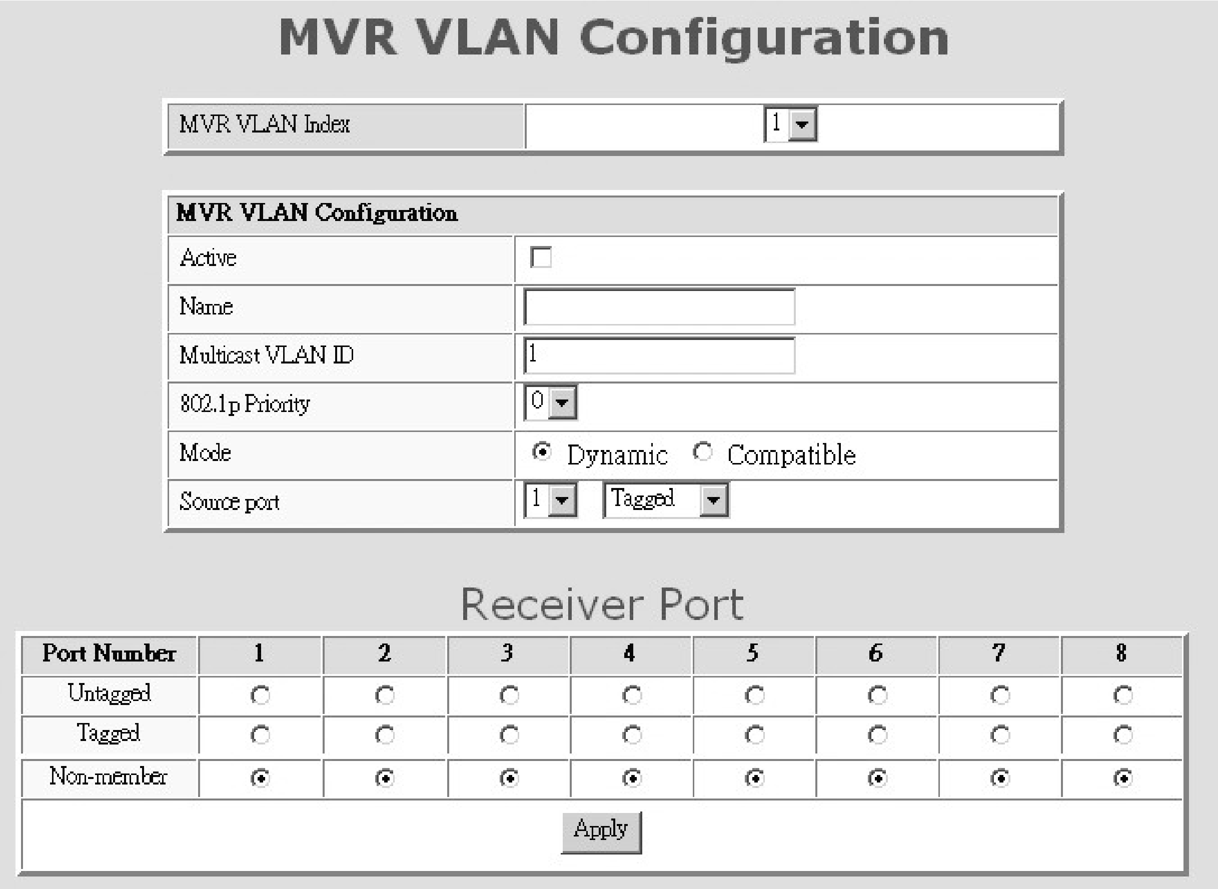
Members Group (Total : 3)

Group	Group Address	Members Port
1	224.0.0.2	3
2	239.255.255.250	3
3	224.0.0.9	3

The IGMP function is for IP multicast operation in network. This switch can do IGMP Snooping function to get the IP multicast group information from IGMP active device. The learned IP multicast member group will be shown in the IGMP web page. This switch will forward IP multicast traffic to these member ports that it learned in the group information.

The IGMP snooping function can be enabled/disabled in this page.

20. MVR VLAN



MVR VLAN Configuration

MVR VLAN Index	1 ▾

MVR VLAN Configuration	
Active	□
Name	
Multicast VLAN ID	1
802.1p Priority	0 ▾
Mode	● Dynamic ○ Compatible
Source port	1 ▾ Tagged ▾

Receiver Port

Port Number	1	2	3	4	5	6	7	8
Untagged	○	○	○	○	○	○	○	○
Tagged	○	○	○	○	○	○	○	○
Non-member	●	●	●	●	●	●	●	●

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

* Before configuring MVR function, complete the VLAN setting first
* Using MVR function, you have to enable IGMP snooping function first.

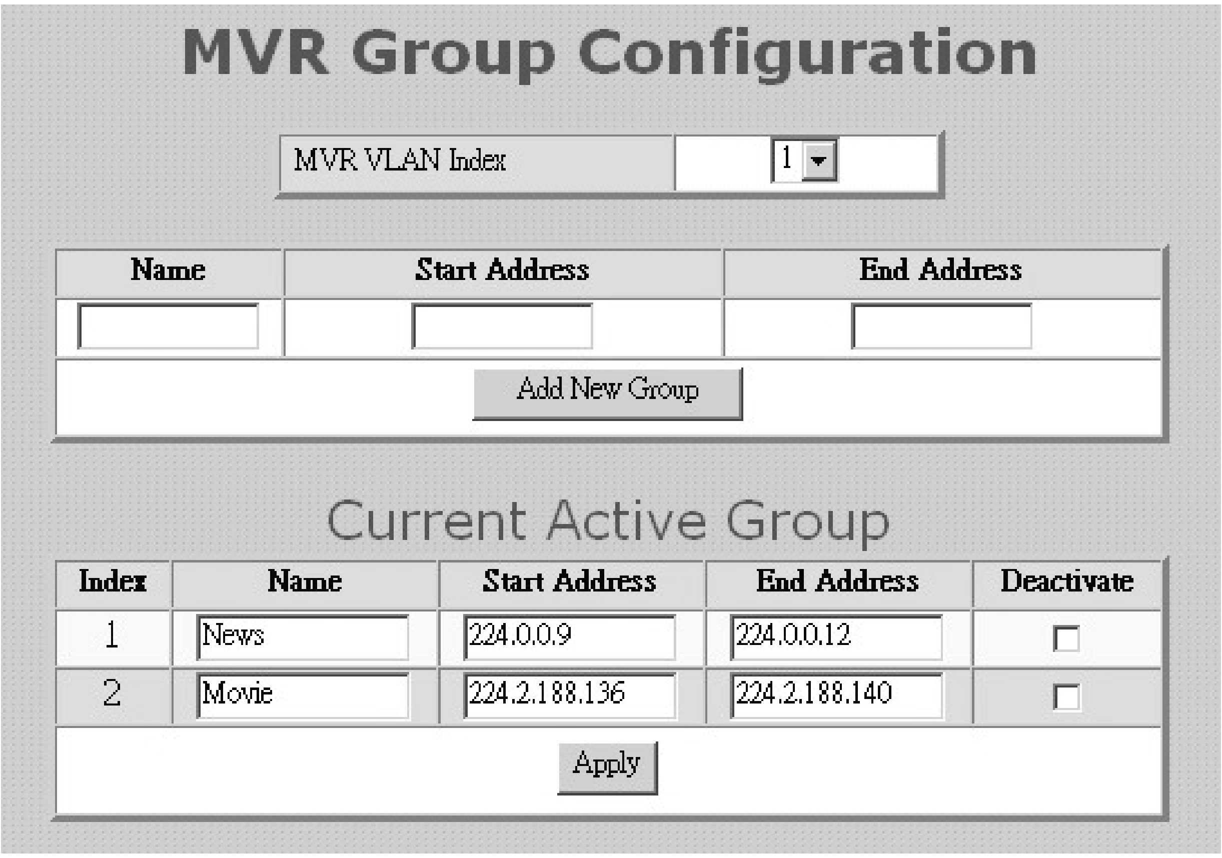
This switch supports four MVR VLANs. They are referred as Index 1,2,3,4. For the MVR VLAN setting, you have to select the index first. And all the settings will be assigned to the indexed MVR VLAN.

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

Source Port – this is the uplink port of this MVR VLAN to the IGMP traffic source. It could be tagged port or untagged port.
Receiver Port – this is the ports connecting to subscribers receiving IP multicast traffic in the MVR VLAN.

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

21. MVR Group



MVR Group Configuration

MVR VLAN Index	1

Name	Start Address	End Address

Current Active Group

Index	Name	Start Address	End Address	Deactivate
1	News	224.0.0.9	224.0.0.12	□
2	Movie	224.2.188.136	224.2.188.140	□

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

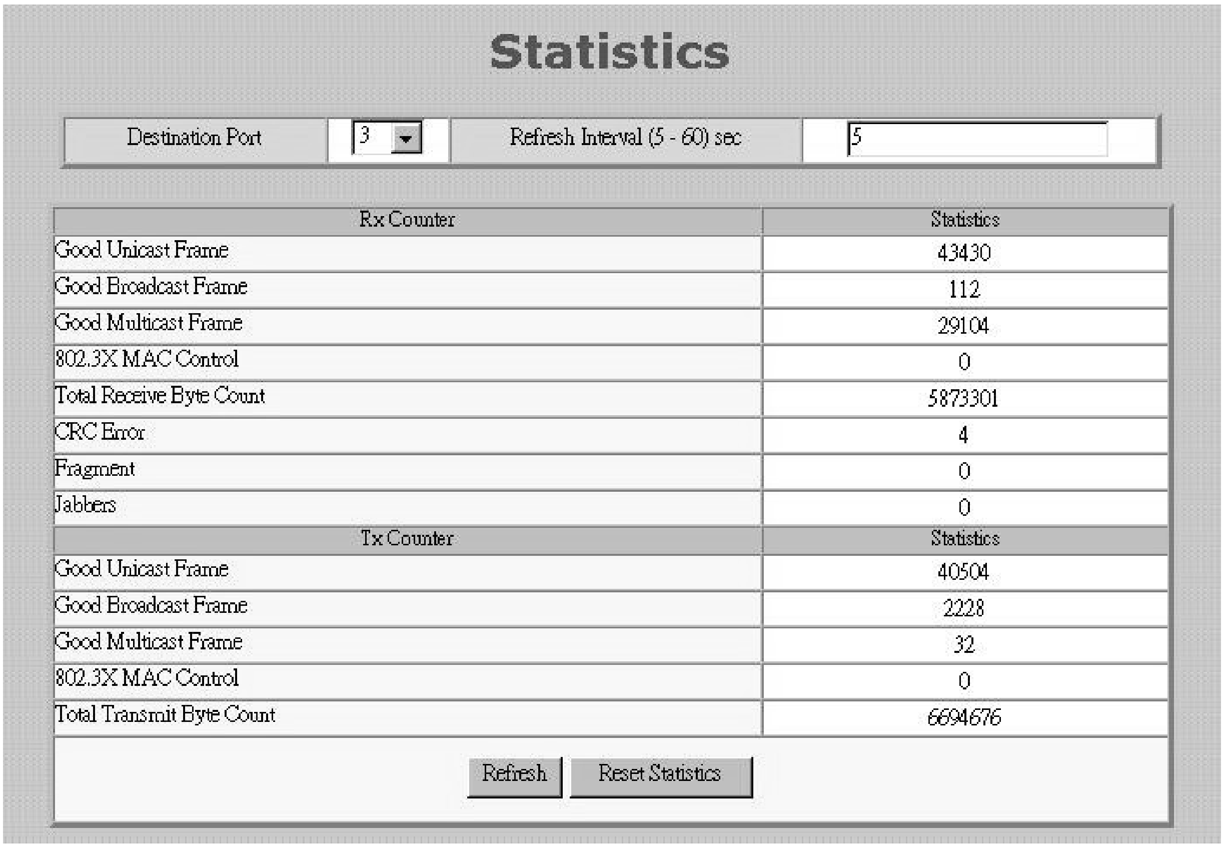
Assigning IP multicast groups to MVR VLAN, you have to select one MVR VLAN first with index 1~4.

For an IP multicast group for MVR VLAN, you have to assign the following settings.
Name – this is the name for this IP multicast group for identification.
Start Address – this is the start IP multicast address for the IP multicast group.
End Address – this is the end IP multicast address for the IP multicast group.
Then click [Add New Group].

After both MVR VLAN and the IP multicast groups are configured, subscribers at the receive ports can receive IP multicast traffic in the IP multicast groups from source port even they are in difference VLANs.

If you want to remove an IP multicast group, mark the Deactivate and click [Apply]. The IP multicast group will be removed from the list.
Note: The list does not support edit function. If you want to make any modification, you have to remove it first. Then create the new one.

22. Statistics



Statistics

Destination Port	3	Refresh Interval (5 - 60) sec	5

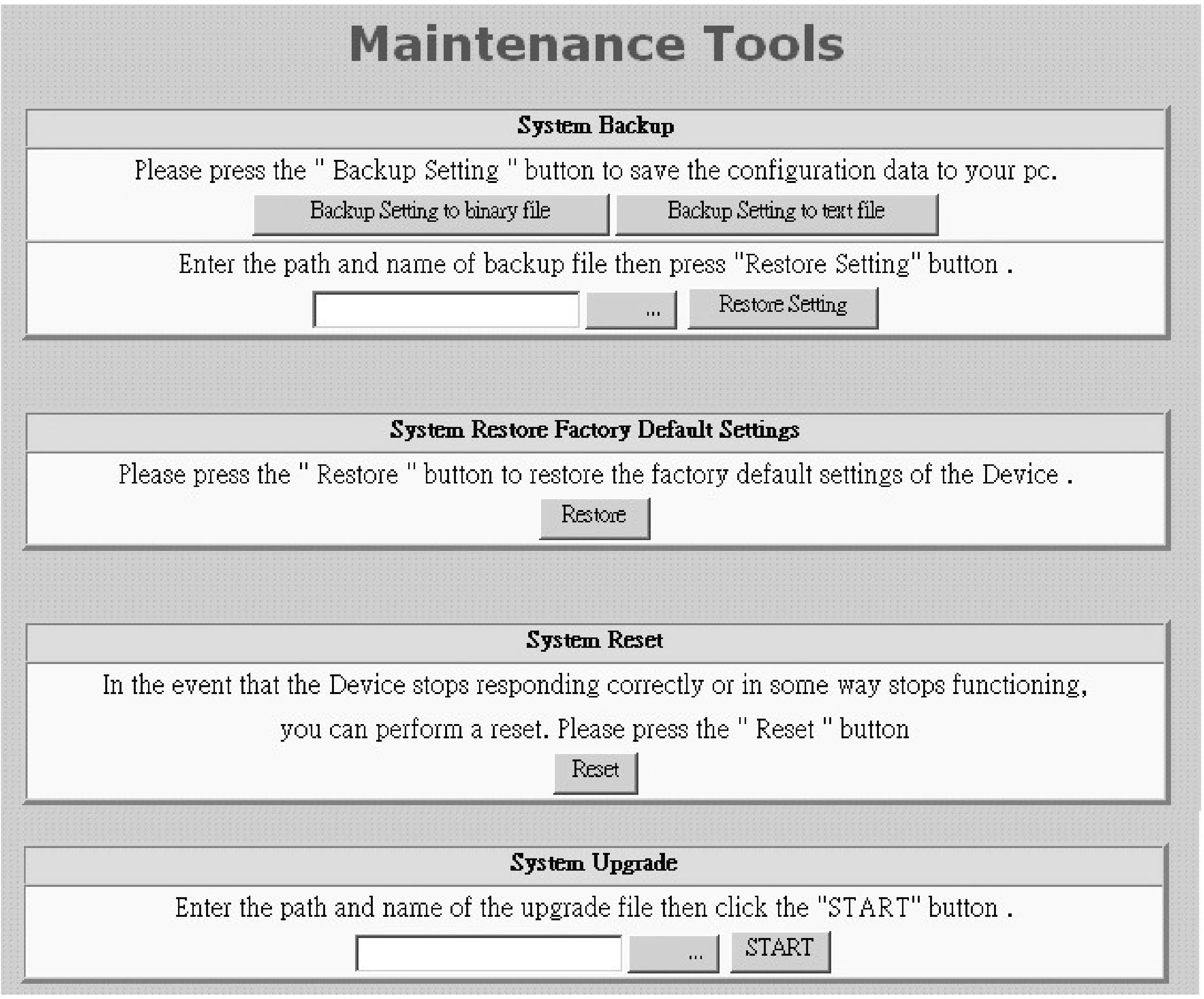
Rx Counter	Statistics
Good Unicast Frame	43430
Good Broadcast Frame	112
Good Multicast Frame	29104
802.3X MAC Control	0
Total Receive Byte Count	5873301
CRC Error	4
Fragment	0
Jabbers	0
Tx Counter	**Statistics**
Good Unicast Frame	40504
Good Broadcast Frame	2228
Good Multicast Frame	32
802.3X MAC Control	0
Total Transmit Byte Count	6694676

Users can find the traffic statistics here. Select port number to get the counters for different port.

Users can modify the refresh interval to get different counter updating period. Click “Refresh” button can update the counter immediately.

Users can reset counters to zero with the “Reset Statistics” button.

23. Tools



Maintenance Tools

System Backup

Please press the " Backup Setting " button to save the configuration data to your pc.

Enter the path and name of backup file then press "Restore Setting" button .

System Restore Factory Default Settings

Please press the " Restore " button to restore the factory default settings of the Device .

System Reset

In the event that the Device stops responding correctly or in some way stops functioning, you can perform a reset. Please press the " Reset " button

System Upgrade

Enter the path and name of the upgrade file then click the "START" button .

Four functions are supported as the system maintenance tools.

a. System Backup
[Backup Setting to binary file] will backup the configuration of the switch to the web management PC in binary format.
[Backup Setting to text file] will backup the configuration of the switch to the web management PC in text format for offline editing.
[Restore Setting] will get the configuration backup file from the web management PC and restore it to the switch.

b. System Restore Factory Default Setting
This function will restore the switch configuration to factory default setting.

c. System Reset
This function will cause the switch reset.

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

6.4 About Telnet 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 in DOS. Its operation interface is the same as console interface.

6.5 About SNMP 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 Version 1 agent function and MIB II(Interface), Bridge MIB, Etherlike 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.

7. Software Update and Backup

This switch supports software/configuration backup and update/restore functions. It could be done in three 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 console/Telnet when running**: Doing by TFTP protocol and it will need a TFTP server in network. Please refer to the description of "*Upgrade*" function in console operation in Section 6.2.

3. **From web browser**: Doing by http protocol and by web browser. Please refer to the description of "*Tools*" function in Section 6.3.

A. Product Specifications

[8*UTP Ports Model]

Access Method	Ethernet , CSMA/CD
Standards Conformance	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX
Communication Rate	10/100Mbps, Full / Half duplex (auto-negotiation)
MDI/MDIX	Auto-detect for each port
Media Supported	*10BASE-T* - 100 Ohm Category 3,4,5 twisted-pair *100BASE-TX* - 100 Ohm Category 5 twisted-pair
Indicator Panel	LEDs for each unit : Power, each port : Link/Act, 100M, FDX
Number of Ports	8* RJ45 TX ports
Dimensions	250 x 117 x 37 mm
Certification	CE Mark, FCC Class A
Power Consumption	8 Watts max.
Temperature	Standard Operating: 0 to 50℃
Humidity	5% to 95% (Non-condensing)

Bridging Function	Filtering, forwarding and learning
Switching Method	Store-and-forward
Address Table	4K entries
Filtering/Forwarding Rate	Line speed
Maximum Packet Size	1536 Bytes
Flow Control	802.3x for full duplex, backpressure for half duplex

VLAN	802.1Q VLAN
QoS	4 transmit priorities per ports, for port-based/802.1P tagged-based/ToS/DiffServ priority operation
Spanning Tree	Support IEEE 802.1w RSTP protocol
Trunking	4 groups max.
Mirror Port	1 capture port for Ingress/Egress traffic, DA/SA filtering function is supported
SNMP	Ver. 1, Supports MIB II(Interface), Bridge MIB, Etherlike MIB, Private MIB
Static Mac ID Access Limit	Static Mac address access limit on port
802.1x	Yes, support Authentication and Transparent modes
Rate Control	Yes, 64Kbps~100Mbps, for ingress/egress traffic
IGMP	Yes, IGMP snooping function and MVR function
Out-band Management	Console
In-band Management	Telnet, http, SNMP
Software Update/Backup	by TFTP protocol, Xmodem, for firmware/ configuration

[8*100FX Ports Model]

Access Method	Ethernet, CSMA/CD
Standards Conformance	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX/FX
Communication Rate	10/100Mbps, Full / Half duplex (auto-negotiation) for TX port, 100Mbps / Full duplex for 100FX ports
MDI/MDIX	Auto-detect for the 10/100TX port
Indicator Panel	LEDs for each unit : Power(PWR), each port : Link/Act
Number of Ports	8* FX ports, 1*TX port(option for Port 8)
Dimensions	250 x 117 x 37 mm
Certification	CE Mark, FCC Class A
Power Consumption	10 Watts max.
Temperature	Standard Operating: 0 to 40℃
Humidity	15% to 95% (Non-condensing)

Bridging Function	Filtering, forwarding and learning
Switching Method	Store-and-forward
Address Table	4K entries
Filtering/Forwarding Rate	Line speed
Maximum Packet Size	1536 Bytes
Flow Control	802.3x for full duplex, backpressure for half duplex

VLAN	802.1Q VLAN
QoS	4 transmit queues per ports, for port-based/802.1P tagged-based/ToS/DiffServ priority operation
Spanning Tree	Support IEEE 802.1w RSTP protocol
Trunking	4 groups max.
Mirror Port	1 capture port for Ingress/Egress traffic, DA/SA filtering function is supported
SNMP	Ver. 1, Supports MIB II(Interface), Bridge MIB, Etherlike MIB, Private MIB
Static Mac ID Access Limit	Static Mac address access limit on port
802.1x	Yes, support Authentication and Transparent modes
Rate Control	Yes, 64Kbps~100Mbps, for ingress/egress traffic
IGMP	Yes, IGMP snooping function and MVR function
Out-band Management	Console
In-band Management	Telnet, http, SNMP
Software Update/Backup	by TFTP protocol, Xmodem, for firmware/ configuration

[7*UTP + 1*100FX Ports Model]

Access Method	Ethernet, CSMA/CD
Standards Conformance	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX/FX
Communication Rate	10/100Mbps, Full / Half duplex (auto-negotiation) for TX ports, 100Mbps/Full duplex for 100FX port
MDI/MDIX	Auto-detect for TX port
Media Supported	*10BASE-T* - 100 Ohm Category 3,4,5 twisted-pair *100BASE-TX* - 100 Ohm Category 5 twisted-pair *100BASE-FX* fiber cable
Indicator Panel	LEDs for each unit : Power, each port : Link/Act(/Speed), FDX
Number of Ports	8* RJ45 TX ports, 1* 100FX port (Port 1)
Dimensions	250 x 117 x 37 mm
Certification	CE Mark, FCC Class A
Power Consumption	8 Watts max.
Temperature	Standard Operating: 0 to 50℃
Humidity	5% to 95% (Non-condensing)

Bridging Function	Filtering, forwarding and learning
Switching Method	Store-and-forward
Address Table	4K entries
Filtering/Forwarding Rate	Line speed
Maximum Packet Size	1536 Bytes
Flow Control	802.3x for full duplex, backpressure for half duplex

VLAN	802.1Q VLAN
QoS	4 transmit priorities per ports, for port-based/802.1P tagged-based/ToS/DiffServ priority operation
Spanning Tree	Support IEEE 802.1w RSTP protocol
Trunking	4 groups max.
Mirror Port	1 capture port for Ingress/Egress traffic, DA/SA filtering function is supported
SNMP	Ver. 1, Supports MIB II(Interface), Bridge MIB, Etherlike MIB, Private MIB
Static Mac ID Access Limit	Static Mac address access limit on port
802.1x	Yes, support Authentication and Transparent modes
Rate Control	Yes, 64Kbps~100Mbps, for ingress/egress traffic
IGMP	Yes, IGMP snooping function and MVR function
Out-band Management	Console
In-band Management	Telnet, http, SNMP
Software Update/Backup	by TFTP protocol, Xmodem, for firmware/ configuration

[16+1FX Ports Model]

Access Method	Ethernet , CSMA/CD
Standards Conformance	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE
Communication Rate	10/100Mbps, Full / Half duplex (auto-negotiation)
MDI/MDIX	Auto-detect for each port
Media Supported	*10BASE-T* - 100 Ohm Category 3,4,5 twisted-pair *100BASE-TX* - 100 Ohm Category 5 twisted-pair
Indicator Panel	LEDs for each unit : Power, each port : Link/Act(/Speed), FDX
Number of Ports	16* RJ45 TX ports, 1* 100FX module slot (Port 17)
Dimensions	430W x 105D x 44H mm
Certification	CE Mark, FCC Class A
Power Consumption	12 Watts max.
Temperature	Standard Operating: 0 to 50℃
Humidity	5% to 95% (Non-condensing)
Bridging Function	Filtering, forwarding and learning
Switching Method	Store-and-forward
Address Table	4K entries
Filtering/Forwarding Rate	Line speed
Maximum Packet Size	1536 Bytes
Flow Control	802.3x for full duplex, backpressure for half duplex
VLAN	802.1Q VLAN
QoS	4 transmit priorities per ports, for port-based/802.1P tagged-based/ToS/DiffServ priority operation
Spanning Tree	Support IEEE 802.1w RSTP protocol
Trunking	4 groups max.
Mirror Port	1 capture port for Ingress/Egress traffic, DA/SA filtering function is supported
SNMP	Ver. 1, Supports MIB II(Interface), Bridge MIB, Etherlike MIB, Private MIB
Static Mac ID Access Limit	Static Mac address access limit on port
802.1x	Yes, support Authentication and Transparent modes
Rate Control	Yes, from 64Kbps to 100Mbps for both ingress and egress traffic
IGMP	Yes, IGMP snooping function and MVR function
Out-band Management	Console
In-band Management	Telnet, http, SNMP
Software Update/Backup	by TFTP protocol, Xmodem, for firmware / configuration

[24+2FX Ports Model]

Access Method	Ethernet, CSMA/CD
Standards Conformance	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE
Communication Rate	10/100Mbps, Full / Half duplex (auto-negotiation)
MDI/MDIX	Auto-detect for each port
Media Supported	*10BASE-T* - 100 Ohm Category 3,4,5 twisted-pair *100BASE-TX* - 100 Ohm Category 5 twisted-pair
Indicator Panel	LEDs for each unit : Power, each port : Link/Act, FDX
Number of Ports	24* RJ45 TX ports, 1* 100FX module slot for one or two 100FX port (Port 25/26)
Dimensions	440W x 172D x 43H mm
Certification	CE Mark, FCC Class A
Power Consumption	13 Watts max.
Input Power	Full range: 100 to 240V, 50 to 60 Hz
Temperature	Standard Operating: 0 to 50℃
Humidity	5% to 95% (Non-condensing)

Bridging Function	Filtering, forwarding and learning
Switching Method	Store-and-forward
Address Table	4K entries
Filtering/Forwarding Rate	Line speed
Maximum Packet Size	1536 Bytes
Flow Control	802.3x for full duplex, backpressure for half duplex

VLAN	802.1Q VLAN
QoS	4 transmit queues per ports, for port-based/802.1P tagged-based/ToS/DiffServ priority operation
Spanning Tree	Support IEEE 802.1w RSTP protocol
Trunking	4 groups max.
Mirror Port	1 capture port for Ingress/Egress traffic, DA/SA filtering function is supported
SNMP	Ver. 1, Supports MIB II(Interface), Bridge MIB, Etherlike MIB, Private MIB
Static Mac ID Access Limit	Static Mac address access limit on port
802.1x	Yes, support Authentication and Transparent modes
Rate Control	Yes, from 64Kbps to 100Mbps for both ingress and egress traffic
IGMP	Yes, IGMP snooping function and MVR function
Out-band Management	Console
In-band Management	Telnet, http, SNMP
Software Update/Backup	by TFTP protocol, Xmodem, for firmware / configuration

B. Compliances

EMI Certification

FCC Class A Certification (USA)

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

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

This is to certify that this product complies with ISO/IEC Guide 22 and EN45014.
It conforms to the following specifications:

EMC:	EN55022(1988)/CISPR-22(1985)	class A
	EN60555-2(1995)	class A
	EN60555-3	
	IEC1000-4-2(1995)	4kV CD, 8kV AD
	IEC1000-4-3(1995)	3V/m
	IEC1000-4-4(1995)	1kV - (power line), 0.5kV - (signal line)

This product complies with the requirements of the Low Voltage Directive 2006/95/EC and the EMC Directive 2004/108/EC.

Warning! Do not plug a phone jack connector 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.