

**ALLOY**

**8-Port Gigabit Web Smart Switch  
(GSS-8T2SFP)**

**User's Manual**

**Version: 1.0.6**

**Oct 12, 2004**

# TABLE OF CONTENT

<b>1.</b>	<b>Introduction.....</b>	<b>4</b>
1.1	Main Features.....	5
1.2	Initial Setup .....	6
1.3	Main Configuration Functions .....	7
<b>2</b>	<b>Configuration .....</b>	<b>8</b>
2.1	Port Status .....	8
2.2	Port Configuration.....	10
2.3	About the Copper/Fibre Media Auto-Detection.....	11
2.4	Port-Based VLAN .....	12
2.4.1	Add Port-Based VLAN Groups .....	13
2.4.2	Delete Port-Based VLAN Groups .....	14
2.4.3	Edit Port-Based VLAN Groups .....	15
2.5	802.1Q VLAN .....	16
2.5.1	Enable/Disable VLAN.....	17
2.5.2	Frames for which VID is not in VLAN Table .....	17
2.5.3	802.1Q Control Per Port Config .....	18
2.5.4	802.1Q VLAN Table Config .....	19
2.6	Trunk .....	22
2.6.1	Trunking Rules.....	23
2.6.2	Get/Refresh the Latest Trunk Settings .....	24
2.6.3	Enable Trunk .....	25
2.6.4	Modify Trunk Settings .....	26
2.6.5	Disable Trunk .....	27
2.7	Port Mirroring .....	28
2.7.1	Get/Refresh the Latest Mirror Settings .....	29
2.7.2	Enable Mirror .....	30
2.7.3	Modify Mirror Settings.....	31
2.7.4	Disable Mirror.....	32
2.7.5	Get/Refresh the Latest Mirror Filter Settings .....	33
2.7.6	Configure Mirror Filter.....	34
2.7.7	Disable Mirror Filter .....	35
2.8	QOS (Quality of Service).....	36
2.8.1	Get/Refresh the Latest QOS Settings .....	37
2.8.2	Enable QOS .....	38
2.8.3	Modify QOS Settings .....	39
2.8.4	Disable QOS .....	40
2.8.5	Get/Refresh the Latest QOS Detailed Settings .....	41
2.8.6	Configure Detailed QOS Settings .....	42
2.9	Rate Control .....	43
2.9.1	Enable/Disable Rate Control.....	44

2.9.2	<b>Ingress Rate Control Common Config</b> .....	45
2.9.3	<b>Ingress Rate Limit Config for Buckets</b> .....	46
2.10	<b>Address Management</b> .....	<b>48</b>
2.10.1	<b>Get/Refresh the Latest Address Management Settings</b> .....	49
2.10.2	<b>Add a New Entry</b> .....	50
2.10.3	<b>Modify an Existing Entry</b> .....	51
2.10.4	<b>Delete an Existing Entry</b> .....	52
2.11	<b>System Configuration</b> .....	<b>53</b>
2.12	<b>Account Settings</b> .....	<b>54</b>
2.13	<b>Reset System</b> .....	<b>55</b>
2.14	<b>Firmware Update</b> .....	<b>56</b>
<b>3</b>	<b>Application Notes</b> .....	<b>57</b>
3.1	<b>In-Band/Out-of-Band Switch Management</b> .....	<b>57</b>

# 1. Introduction

The GSS-8T2SFP is a high performance web-smart switch that provides up to 8 10/100/1000Mbps copper Ethernet ports and 2 mini-GBIC ports. The versatility of this switch allows users to migrate easily from existing Ethernet or Fast Ethernet networks while providing an easy upgrade path to a Gigabit Ethernet network. It also provides users with a simple management interface via an out-of-band Ethernet port rather than a sophisticated SNMP management structure.

User-friendly web management is supported through any web browser. This gives you total control of the switch much the same as you would have with an SNMP switch but at a smart switch cost. An out-of-band Ethernet port (Cfg Port) is supported for initial setup. The out-of-band Ethernet port provides an independent control channel which is secure from the main network. It can optionally be connected back to your main network, or left as a secure separated network.

Non-blocking, maximum wire speed performance is implemented on all switched ports. The switch supports auto-negotiation and AUTO-MDIX functions on all switched 10/100/1000M RJ-45 Gigabit copper ports. These functions make it easy to use and eliminate the need for both straight through and cross-over cables when up-linking.

The GSS-8T2SFP supports both port-based and 802.1Q (tag-based) VLAN's. To increase bandwidth for back bone applications, it supports a single trunk group with a total of 4 ports. These trunk ports are supported with a fail-over function to provide redundant back-up when one or more ports loose connection.

# 1.1 Main Features

This switch provides the following main features:

- Non-blocking, full-line speed, store-and-forward
- Jumbo frame support, Max. packet length 9728 bytes
- Auto-Negotiation and Auto-MDIX on all 10/100/1000M copper ports
- Up to 8x 10/100/1000 RJ-45 copper ports and 2 mini-GBIC ports with optional fibre transceivers.
- Automatic media detection is provided for the last two shared ports for copper/fibre connection.
- 1.5M-bit packet buffer
- 4K MAC entries
- Support for port-based VLAN and tag-based (802.1Q) VLAN
- MAC-based trunk with fail-over capability
- Port, weighted priority, and 802.1Q-based QOS with four queues
- Support flow control for both full and half duplex operations
- Support broadcast storm prevention and rate control
- Support port mirroring
- Address management for static MAC entries
- LED display for each port to show link and activity status
- Wall mount, Rack mount or desktop

## 1.2 Initial Setup

Plug-in the power source to power-up the switch. After the switch is powered-on and in a ready state (both the LED indicators POWER and DIAG are lit), you can use the **configuration port** (a standalone, out-of-band Ethernet port on the left side of the front panel) to connect to the switch. The **default IP and related settings** for this interface are shown below:

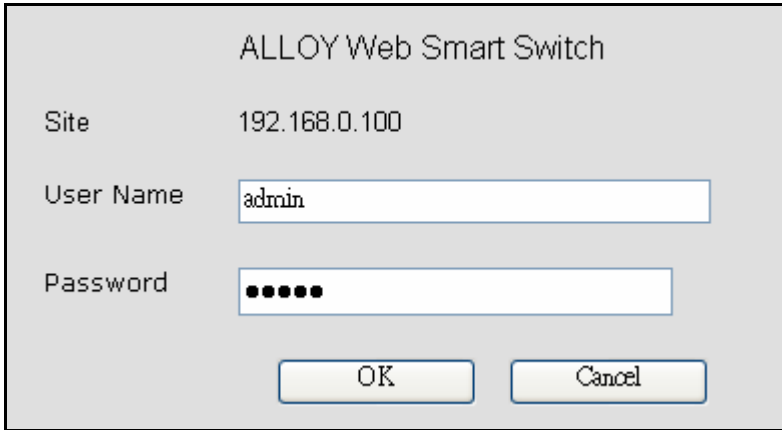
- IP address: **192.168.0.100**
- Network mask: **255.255.255.0**
- Default gateway: **192.168.0.1**

**NOTE:** Connecting to the **configuration port** is the **ONLY** way to control the switch. All Gigabit (in-band) ports can't be used to control the switch unless one gigabit port is linked to the configuration port.

Try to PING the switch from your PC to make sure the network connection is successful. The IP address on this switch can be modified later for your needs.

Now you can use a web browser to launch the user-friendly web management interface for this switch. Currently (October 2004) the switch only supports **Microsoft Internet Explorer** for web interface configuration. Please check with Alloy to determine support for other Web Browser systems.

The login dialog box (shown below) is the first screen you will see when the switch's IP address is entered into your browser.



ALLOY Web Smart Switch	
Site	192.168.0.100
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="••••••"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

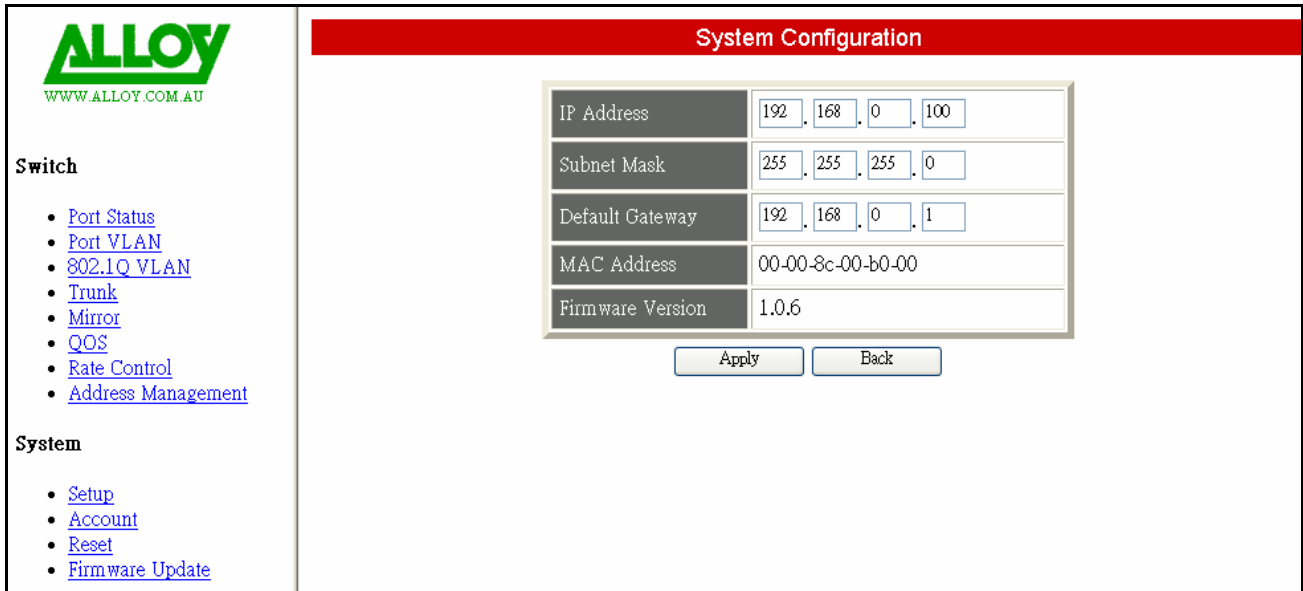
Use the **default username and password** shown as below to complete the login procedure:

- Username: **admin**
- Password: **admin**

This username/password can be modified if required.

# 1.3 Main Configuration Functions

After the login is successfully validated, the switch's home page – **System Configuration** will be displayed. The left section of the page provides various function menus to activate the individual configuration pages. The home page is shown below:



The function menu contains two parts:

**Switch** for setting up the switch functions and **System** for maintaining the system parameters.

Switch functions :

- **Port Status** – Indicates port status and enables port configuration parameters
- **Port VLAN** – Configures port-based VLAN's
- **802.1Q VLAN** – Configures tag-based VLAN's
- **Trunk** –Enable and configure Trunking
- **Mirror** – Setup port mirroring functions
- **QOS** – Configure Quality of Service functions
- **Rate Control** –Limit traffic rate and broadcast storm suppression on a per-port-basis
- **Address Management** – Manage static MAC entries in the address table

System functions:

- **Setup** – Configure system information (such as IP address, etc.)
- **Account** – Maintain login information for access to the switch
- **Reset** – Reboot the switch with or without writing default configurations
- **Firmware Update** – Update the firmware through TFTP

The following sections will describe how to configure these functions in detail.

# 2 Configuration

## 2.1 Port Status

This page provides the current link status for all 8 ports.

Port Status									
Select	Port No	Link Status	Port Status	Auto-Nego.	Speed	Duplex	Flow Control	Protected	Jumbo Frame
<input type="radio"/>	1	Down	Enable	--	--	--	Disable	Disable	Disable
<input checked="" type="radio"/>	2	Up	Enable	Enable	100M	Full	Disable	Disable	Disable
<input type="radio"/>	3	Down	Enable	--	--	--	Disable	Disable	Disable
<input type="radio"/>	4	Down	Enable	--	--	--	Disable	Disable	Disable
<input type="radio"/>	5	Disable	Disable	Enable	100M	Full	Disable	Disable	Disable
<input type="radio"/>	6	Down	Enable	--	--	--	Disable	Disable	Disable
<input type="radio"/>	7	Up	Enable	Enable	100M	Full	Disable	Disable	Disable
<input type="radio"/>	8	Down	Enable	--	--	--	Disable	Disable	Disable

This page provides the following information:

- **Port No.** – The specific port on the switch
- **Link Status** – Show the port link status: **Up / Down / Disable**
  - **Up** – port link is up.
  - **Down** – port link is down.
  - **Disable** – Traffic will be blocked while the link status is up and the port’s **Status** option is “Disable” in **Port Configuration** page.
- **Port Status** – Show the port’s Enabled option: **Enable / Tx / Rx / Disable**
  - **Enable** – Enables both packet forwarding (Tx) and receiving (Rx) through the port
  - **Tx** – Only enable packet forwarding from this port. Packet receiving is not allowed.
  - **Rx** – Only enable packet reception on this port. Packet forwarding is not allowed.
  - **Disable** – Block all traffic through this port even when the link status is up.
- **Auto-Nego.** – Auto negotiation. This will display the negotiation status when the port has link.
  - **Enable** – Indicates the port link is up by auto negotiation mode
  - **Disable** – Indicates the port link is up by forced mode

**NOTE:** The switch automatically uses Auto-Negotiation for all 8 COPPER Interfaces. Only port 7 and 8 can be configured to either Enable or Disable Auto-Negotiation while using FIBRE media.

- **Speed** – to show the current link speed (**1G / 100M / 10M bps**) while the port link is up.



- **Duplex** – Indicates the port as **Full or Half** duplex mode while the link is up.
- **Flow Control** –Shows the flow control capability as **Enabled / Disabled** for this port.
- **Protected** – Shows the protected capability as **Enabled / Disabled** for this port.

Defining a port as Protected, is like defining a simple port based VLAN. A port selected as Protected, cannot communicate with other ports that have been selected as protected, but can communicate with non protected ports. For example.

You have a School class room that is used by students. You need to ensure that all students can access the file server, but cannot communicate directly with each other. You could connect Port 1 of the switch to the File Server. Ports 2 to 8 would then be connected to the student workstations. Defining ports 2 to 8 as Protected and leaving port 1 un-protected, will achieve the desired result. ie. Port 3 cannot communicate with port 4, but Port 3 can communicate with port 1

- **Jumbo Frame** – Shows the current settings for Jumbo Frame capability as **Enabled / Disabled** for this port. Jumbo frames (packets that are longer than 1518 byte but shorter than 9728 bytes) are only supported **while the port is in 1000Base-T mode, link is active and Jumbo Frames is Enabled.**

**NOTE:** To ensure system performance, it is recommended that only **TWO** ports be enabled for this function.

Note: **Auto-Nego, Speed** and **Duplex** will not appear while the port link is down.

(The ‘-’ character indicates that the status is unavailable.)

If a *trunk* ports have been enabled, then the port numbers for all member trunk ports will be marked with a ‘\*’ symbol. The following example shows the port status with trunk ports configured. Only the leading port (e.g. port 3) (the trunk member with the lowest port number) can be configured, configurations for the other member ports (e.g. port 4 & port 5) will be synchronized with the leading port (port 3). Section 2.6 (Trunk) describes port trunking in detail.

Port Status									
Select	Port No	Link Status	Port Status	Auto-Nego.	Speed	Duplex	Flow Control	Protected	Jumbo Frame
<input type="radio"/>	1	Down	Enable	--	--	--	Disable	Disable	Disable
<input type="radio"/>	2	Down	Enable	--	--	--	Disable	Disable	Disable
<input checked="" type="radio"/>	*3	Down	Enable	--	--	--	Disable	Disable	Disable
<input type="radio"/>	*4	Down	Enable	--	--	--	Disable	Disable	Disable
<input type="radio"/>	*5	Down	Enable	--	--	--	Disable	Disable	Disable
<input type="radio"/>	6	Down	Enable	--	--	--	Disable	Disable	Disable
<input type="radio"/>	7	Down	Enable	--	--	--	Disable	Disable	Disable
<input type="radio"/>	8	Down	Enable	--	--	--	Disable	Disable	Disable
<input type="button" value="Configure"/>									

# Port Configuration

If you need to edit the port configuration, select one of the desired ports by clicking its radio button in the **Select** column of the **Port Status** page. The **Configure** button will be enabled when any port is selected. Click the **Configure** button to enter the **Port Configuration** page (shown below) for the selected port (e.g. port3):

### Port Configuration

Port	3
Enable Option	<input checked="" type="radio"/> Tx/Rx <input type="radio"/> Tx <input type="radio"/> Rx <input type="radio"/> Disable
Auto-Negotiation	Fiber: <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Flow Control	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Protected Port	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Jumbo Frame Support	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

The following parameters will be provided and configured in the **Port Configuration** page :

- **Port** – the selected port number to be configured (read only)
- **Enable Option**
  - **Tx/Rx** – Enable bi-directional traffic for the port
  - **Tx** – Enable one way only (forwarding) traffic for the port
  - **Rx** – Enable one way only (receiving) traffic for the port
  - **Disable** – Block all traffic for the port
- **Auto-Nego.** – Auto negotiation option **for fibre media only**. This option can be changed only for port 7 and port 8. (Port 7 and port 8 are capable of using either copper or fibre media.)
  - **Enable** – Use auto negotiation mode to setup the link with the connecting device
  - **Disable** – Force the mode (**1000Base-X, full duplex**) used in establishing link with the connecting device.

**NOTE:** The switch uses auto negotiation mode for all ports using copper media.

- **Flow Control**
  - **Enable** – Enable flow control for this port
  - **Disable** -- Disable flow control for this port
- **Protected Port**
  - **Enable** – to enable this function for the port (to be a protected port)
  - **Disable** -- to disable this function for the port (to be an unprotected port)
- **Jumbo Frame Support**
  - **Enable** – Enable Jumbo frames
  - **Disable** – Disable Jumbo frames

After the desired options have been selected for the above functions, click the **Submit** button to save the current settings to the switch and revert back to the **Port Status** Page. Click the **Back** button to abort the modifications.

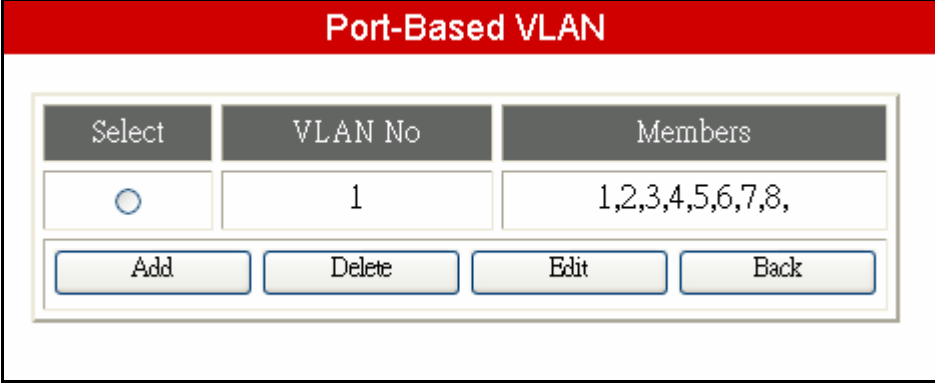
## 2.2 About the Copper/Fibre Media Auto-Detection

The switch provides 2 optional mini-GBIC (SFP) ports for use with either copper or fibre modules. These ports are paired with copper ports **7 and 8**. These paired ports enable Fibre uplinks to other Gigabit Fibre switches for backbone or cascading applications. This switch will automatically detect which media is plugged in to the port. If both copper and fibre media are plugged in, **the fibre media has higher priority, and will become the default port for the pair**. The link for the copper media is disabled while the fibre port is enabled. Copper link will re-established once the fibre media has been un-plugged.

## 2.3 Port-Based VLAN

Port-based VLAN segregates ports into various groups. Once you define Port Based VLAN groups only ports that are members of the same VLAN group can communicate with each other. Broadcast, Multicast and Unicast packets are limited to within their respective ports VLAN group.

The initial VLAN setting page is shown below:



Select	VLAN No	Members
<input type="radio"/>	1	1,2,3,4,5,6,7,8,

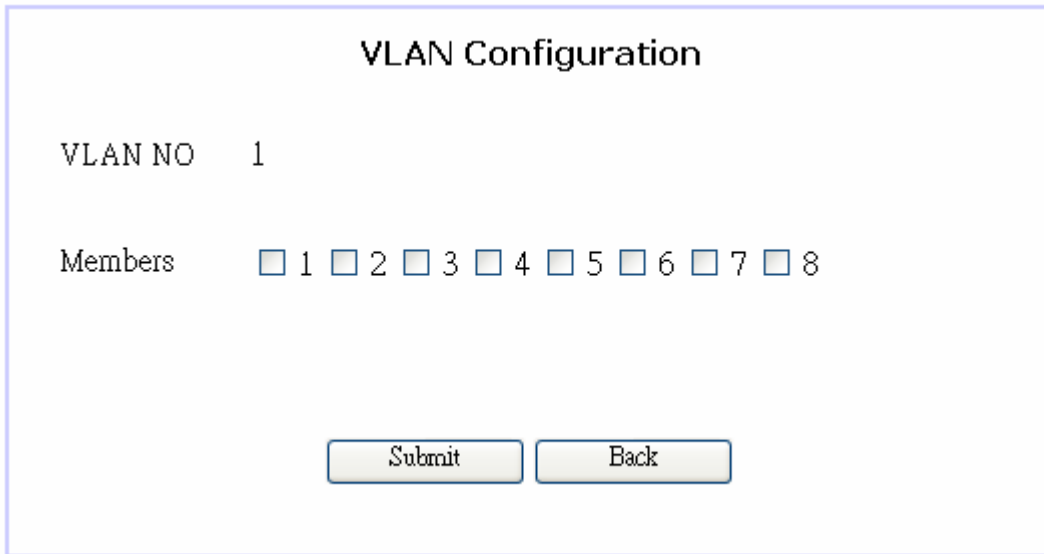
You can add, delete, and modify the port-based VLAN's based on your particular requirements. The switch supports **up to 8** port-based VLAN groups for manual entry.

The following pages will describe in detail how to configure port-based VLAN's.

**NOTE:** A **default port-based VLAN entry (No=1)** is initially created by the system. This VLAN entry contains all ports as members. With all ports as members of VLAN 1, the system will operate as a normal switch and not block traffic between any ports (VLAN can be regarded as **“disabled”**). If additional port-based VLANs are enabled then you should remove the required ports from the default VLAN 1. Conversely, if you want to **“disable”** the port-based VLAN function, re-add all ports to VLAN 1.

### 2.3.1 Add Port-Based VLAN Groups

To add a port-based VLAN group, click the **Add** button in **Port-Based VLAN** page, the following web page will be shown: (if the default entry had previously been removed):



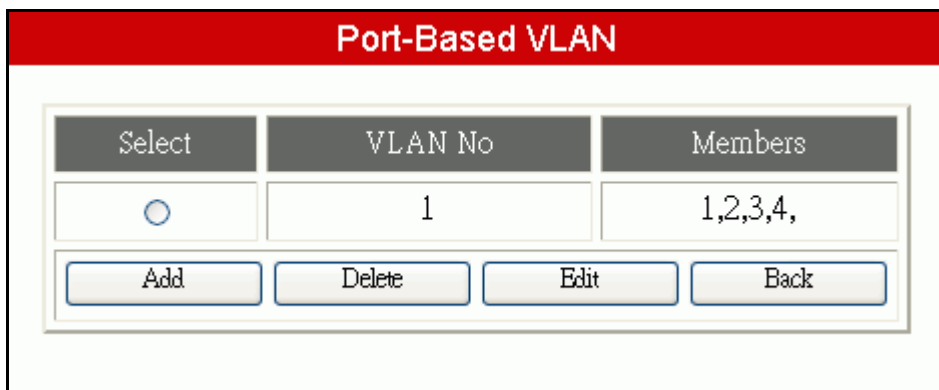
**VLAN Configuration**

VLAN NO    1

Members     1  2  3  4  5  6  7  8

The VLAN NO is automatically configured to the next available. The switch administrator needs to add the VLAN Port Members. After you have completed your configuration, press the **Submit** button you will then be redirected back to the VLAN initial set up page. The **Back** button allows the user to disregard all changes and revert back to the VLAN initial set up page. Below is an example page where Ports 1, 2, 3 and 4 have been added to VLAN Group1.



**Port-Based VLAN**

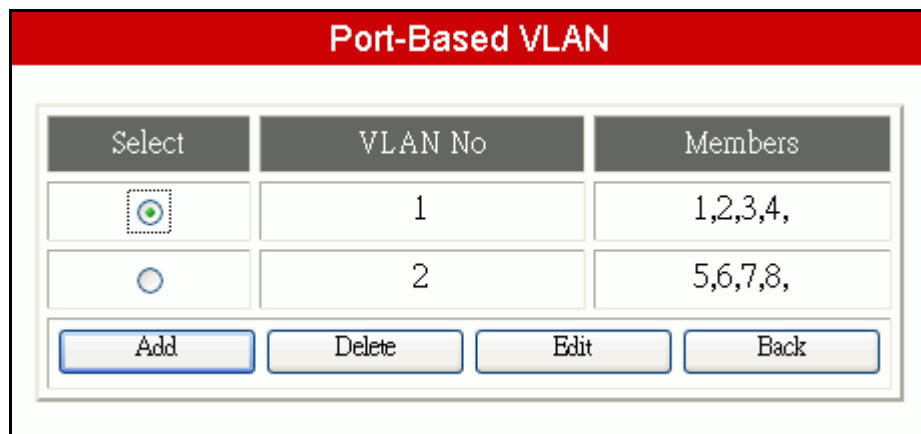
Select	VLAN No	Members
<input type="radio"/>	1	1,2,3,4,

VLAN group 1 contains member Ports 1, 2, 3 and 4.

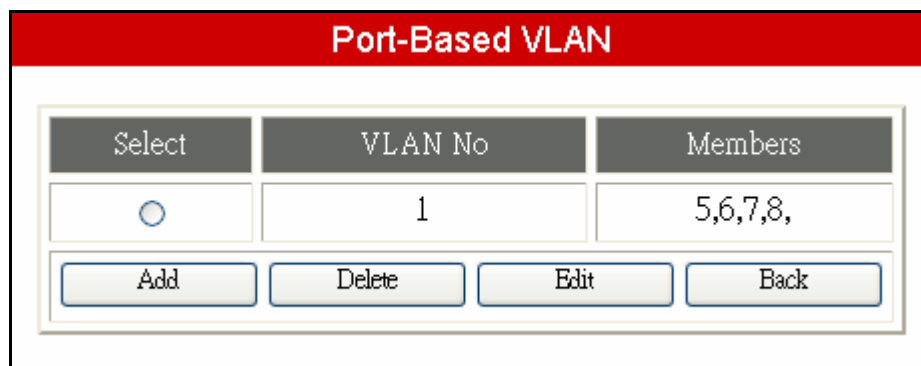
## 2.3.2 Delete Port-Based VLAN Groups

To delete a port-based VLAN group, just select the desired group to be removed and click the **Delete** button.



Select	VLAN No	Members
<input checked="" type="radio"/>	1	1,2,3,4,
<input type="radio"/>	2	5,6,7,8,

As shown in the figure above, there are 2 port-based VLAN groups 1 and 2. Check the radio button at the head of each row and press the **Delete** Button. The result is shown in the following figure.

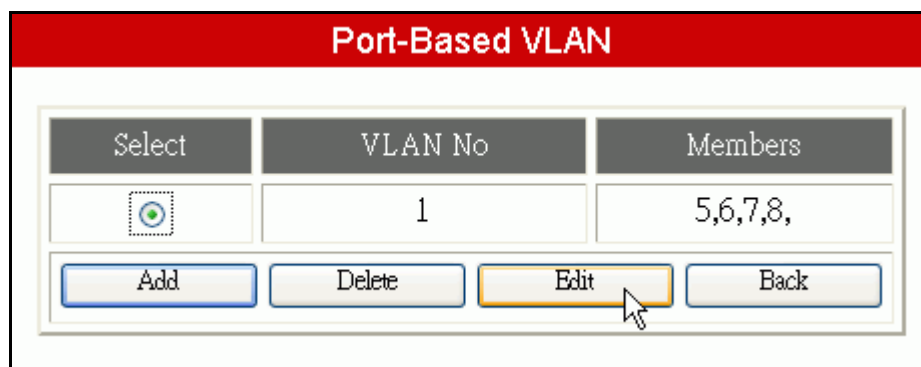


Select	VLAN No	Members
<input type="radio"/>	1	5,6,7,8,

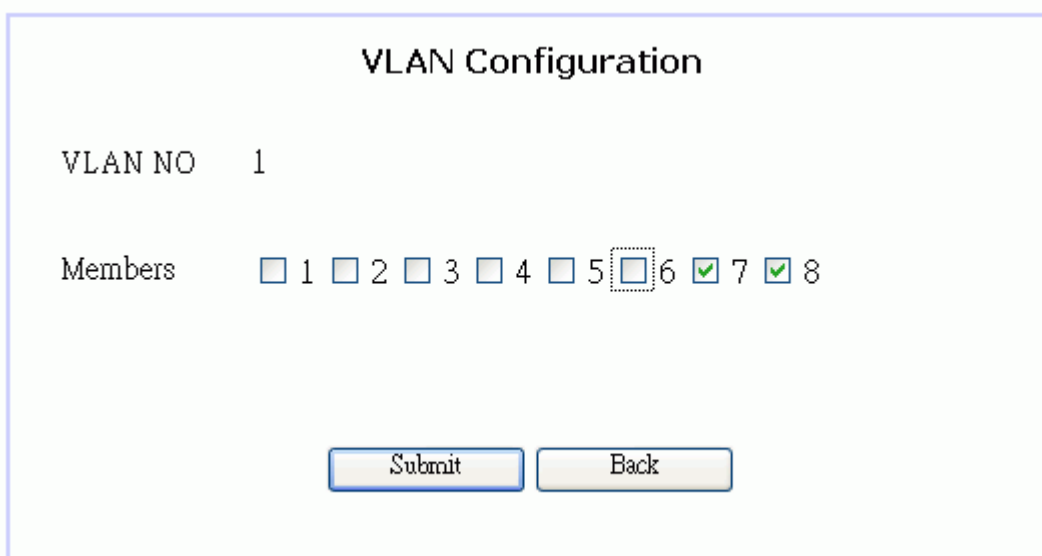
The port-based VLAN Group 1 and its members P1, P2, P3, P4 have now been deleted. The port-based VLAN Group2 now becomes VLAN Group1.

### 2.3.3 Edit Port-Based VLAN Groups

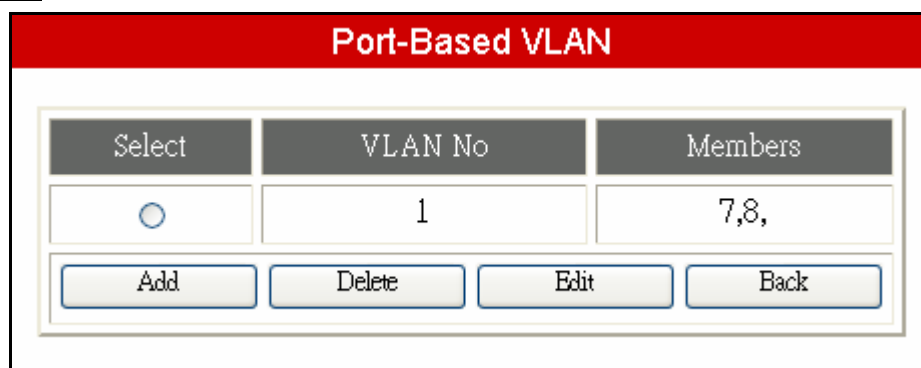
To edit the current port-based VLAN group, first check the radio button of the group you want to edit and click the **Edit** button.



Then set the member Ports 7 and 8



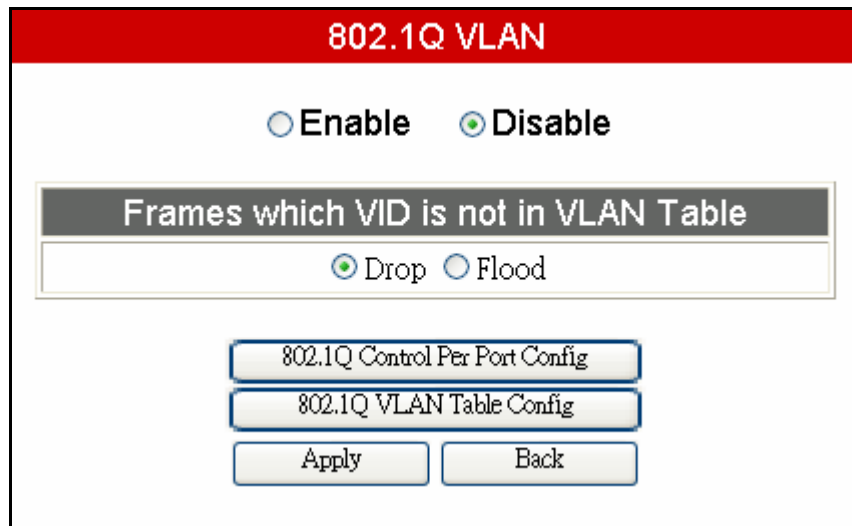
Press the **Submit** button to complete the Edit function.



The port-based VLAN Group Member changes to Port 7 and 8 from Port 5, 6, 7 and 8.

## 2.4 802.1Q VLAN

IEEE 802.1Q (tag-based) VLAN operates by reading/writing 802.1Q tags depending on the requirements of the individual transmitting port. To configure this type of VLAN, Click on the [802.1Q VLAN](#) menu.



The screenshot shows a web-based configuration interface for 802.1Q VLAN. At the top, there is a red header bar with the text "802.1Q VLAN". Below the header, there are two radio buttons: "Enable" (unselected) and "Disable" (selected). Underneath, there is a section titled "Frames which VID is not in VLAN Table" with a dark grey background. Below this title, there are two radio buttons: "Drop" (selected) and "Flood" (unselected). At the bottom of the interface, there are four buttons: "802.1Q Control Per Port Config", "802.1Q VLAN Table Config", "Apply", and "Back".

This page provides the following functions to configure the 802.1Q VLAN:

- Enable / Disable VLAN
- Frames which VID's are not in the VLAN table
- 802.1Q control per port configuration
- 802.1Q VLAN table configuration

Currently this system supports **up to 16** tag-based VLAN groups for manual entry. The following pages will describe in detail how to configure 802.1Q VLAN's.



## 2.4.1 Enable/Disable VLAN

In the **802.1Q VLAN** page, there are two options provided to enable/disable tag-based VLAN functions:

- **Enable** – Activate tag-based VLAN functions. If any tag-based VLAN entry is created.
- **Disable** – De-activate tag-based VLAN functions, even if there are some VLAN entries created. (i.e. Tag-based VLAN entries are retained even though the tag-based VLAN function is disabled.)

Remember to click the **Apply** button to activate and save the settings to the switch.

## 2.4.2 Frames for which VID is not in VLAN Table

There are two options provided to make the system manipulate the frames for which VIDs are not found in the tag-based VLAN table:

- **Drop** – Drop packets without a Valid VID entry. This is the default setting.
- **Flood** – Accept packets without a Valid VID entry. These frames will be broadcast to all ports.

Click the **Apply** button to activate and save the settings to the switch.

**Note:** It is recommended that you use the **Drop** option to prevent the broadcasting unwanted traffic.

## 2.4.3 802.1Q Control Per Port Config

Port NO.	Tag Config	Non 1Q Frame
1	Priority 0 VID 1 (1-4094)	<input type="radio"/> Drop <input checked="" type="radio"/> Not Drop

The above screen allows you to control individual port 802.1Q settings:

- **Port No** – Select the port to be configured. Only the **red-colored** leading port will be shown in the dropdown if a trunk group has been created.
- **Tag Config** – There are two parameters in this field: **Priority** (0-7) and **VID** (1-4094). Set the 2 parameters to determine the 802.1Q tag contents.
- **Non 1Q Frame** – This determines what will occur to packets that do not match the 802.1Q VID assigned to this port. Options are: **Drop** :- to drop the non matching packet, and **Not Drop** :- to forward the packet.

Below the configuration screen, there are three buttons to select from:

**View Settings**: Select the **Port No** from the above table and click this button to see the specified port tag settings.

**Apply**: To submit the port configuration settings to the switch.

**Back**: To go back to the 802.1Q main settings page.

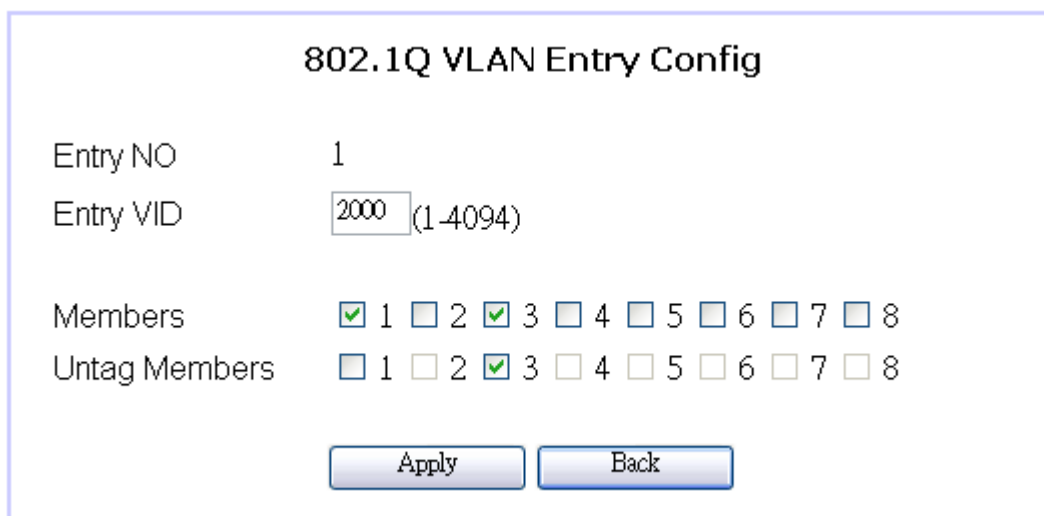
## 2.4.4 802.1Q VLAN Table Config

The following screen capture shows the page used to add/delete/edit the 802.1Q VLAN entry. Each VLAN entry has 3 parameters, **VID**, **Members** and **UnTag Members**.



After clicking the **Add** button, the figure shown below will be displayed:

- **VID** – a unique VLAN ID, range is from 1 to 4094
- **Members** – the port members in an 802.1Q VLAN group.
- **UnTag Members** – When you specified the 802.1Q VLAN group, you can decide whether the egress frames (packets leaving the specified port) from this port are **Tagged** or **Untagged**. If you want a port untagged, select the checkbox beside the port number in the Untagged Members row. Checkboxes in the Untagged Members row can only be configured when the corresponding checkboxes in the **Members** row are selected. In the example below, port1 and port3 are members of the VLAN entry1 with a VID = 2000. Only checkboxes on port1 and port3 are available to be set in as Untagged Members.



Entry NO	1
Entry VID	<input type="text" value="2000"/> (1-4094)
Members	<input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8
Untag Members	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8

Enter the **VID** (1-4094) and select the checkboxes in the **Members** row to select the ports which belong to this VLAN group. Also select the checkboxes in the **Untag Members** row for this group's member ports which egress frames will be untagged. After these settings are completed, click the **Apply** button to submit the changes to the switch. Click the **Back** button to abort the actions and revert back to the **VLAN Table Config** page.

Here is an example showing how to configure the 802.1Q VLAN Table Config parameters. There are four existing 802.1Q VLAN entries as shown below.

**802.1Q VLAN Table Config**

Select	Entry	VID	Members	UnTag Members
<input type="radio"/>	1	526	1,2,3,	3,
<input type="radio"/>	2	285	4,5,6,	4,5,
<input type="radio"/>	3	3	6,7,8,	6,
<input type="radio"/>	4	4	1,3,5,6,7,	

To delete the 802.1Q VLAN entry, click a radio button on the **Select** column (e.g. Entry No.2, VID = 285), then click the **Delete** button to do perform the deletion.

**802.1Q VLAN Table Config**

Select	Entry	VID	Members	UnTag Members
<input type="radio"/>	1	526	1,2,3,	3,
<input checked="" type="radio"/>	2	285	4,5,6,	4,5,
<input type="radio"/>	3	3	6,7,8,	6,
<input type="radio"/>	4	4	1,3,5,6,7,	

Once the above has been completed, the 802.1Q VLAN table will be changed accordingly:

**802.1Q VLAN Table Config**

Select	Entry	VID	Members	UnTag Members
<input type="radio"/>	1	526	1,2,3,	3,
<input type="radio"/>	2	3	6,7,8,	6,
<input type="radio"/>	3	4	1,3,5,6,7,	

The VID entry (No.2, VID=285) has been successfully deleted.

If you would like to edit the parameters of an 802.1Q VLAN entry, select the entry that you require changed (e.g. entry No.2, VID = 3) then click the **Edit** button to perform the modifications: VID is changed to 333 and port 1 and port 8 are selected to be members of this group. Then select the port 1 as a Untagged Member for the 802.1Q VLAN entry.

### 802.1Q VLAN Entry Config

Entry NO            2

Entry VID             (1-4094)

Members              1  2  3  4  5  6  7  8

Untag Members      1  2  3  4  5  6  7  8

Finally, click the **Apply** button to apply the changes.

The 802.1Q VLAN table will be updated accordingly:

### 802.1Q VLAN Table Config

Select	Entry	VID	Members	UnTag Members
<input type="radio"/>	1	526	1,2,3,	3,
<input type="radio"/>	2	333	1,8,	1,
<input type="radio"/>	3	4	1,3,5,6,7,	

The parameters for 802.1Q VLAN entry 2 have been changed and saved to the switch.

## 2.5 Trunk

The GSS-8T2SFP supports MAC-based trunking. This allows more than one port to be grouped together as a single link connection between two switch devices. The GSS-8T2SFP allows one trunk group that can accommodate up to 4 trunk members. This feature provides redundancy and increases the effective bandwidth through the link. Trunking operates via a dynamic MAC-based algorithm. It provides dynamic failover when a port within the group fails or is disconnected. If a port within the trunk group fails, the other ports of the trunk group assume the traffic load automatically.

The following parameters are required to be set:

- **Enable/Disable** – click the **Enable** button to enable the trunk function or the **Disable** button to disable it
- **Member** – the member port(s) of the trunk group

Select the **Trunk** menu on the web page to activate the page shown below.

**Port Trunking**

Enable  Disable

Port No	Member
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

This function will be limited by some configuration rules. Please read the User's Manual in detail.

Because a trunk port is aggregated with the other member ports within the group, **there are some rules to limit the configuration of ports within the trunking group**. The following section will list the related rules for this function.

## 2.5.1 Trunking Rules

The following rules are applied to ports defined within a Trunk Group:

- The attributes of all trunk member ports in Port Status, Mirror, QOS and Rate Control functions must be the same.
- All trunk member ports can not be a capture port within the Mirror function.
- If port 7 or port 8 are in use as fibre media and you want to truncate them with ports using copper (port1—port6) as a trunk group, then the auto-negotiation option should always be Enabled; If both port 7 and port 8 are the only trunk member ports within a Trunk group and they are using fibre media, then auto-negotiation option can be Enabled or Disabled.
- All trunk member ports must be in the same group in Port VLAN and 802.1Q VLAN functions.
- After enabling a trunk group, a ‘\*’ symbol will be marked before the port numbers which belong to the trunk group in most function pages shown as below (e.g. Trunk member ports 3, 4 and 5 in Port Mirroring function).
- The leading port is the master port of all trunk member ports.
- After enabling a trunk group, users can only change the leading port settings in each function page. All settings for the other trunk member ports will be synchronized to the leading port.
- When a trunk group is set to disabled, all trunk member ports will be released to ordinary port status and their functions can be configured individually. At that moment, their configuration attributes will be retained to the last settings used while they were member ports of a trunk.

Port Mirroring

Enable    Disable

Port No	Status
1	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
2	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
*3	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
*4	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
*5	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
6	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
7	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
8	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF

## 2.5.2 Get/Refresh the Latest Trunk Settings

Click the **Trunk** menu on the web page to review the current trunk settings on the switch.

### Port Trunking

Enable  Disable

Port No	Member
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>



### 2.5.3 Enable Trunk

- **Step 1:** Choose the member port(s) up to 4 within a trunk group.
- **Step 2:** Check the corresponding checkbox for these member ports (ex: port1, port2, port4, port5).
- **Step 3:** Click the **Enable** radio button.
- **Step 4:** Click the **Apply** button to enable trunk settings.

Port No	Member
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

Apply Cancel

## 2.5.4 Modify Trunk Settings

- **Step 1:** Choose the member port(s) up to 4 within the trunk group.
- **Step 2:** Check the corresponding checkbox for these member ports (ex: port3, port4, port6).
- **Step 3:** Click the **Apply** button to modify the trunk settings.

### Port Trunking

Enable  Disable

Port No	Member
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>
5	<input type="checkbox"/>
6	<input checked="" type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

## 2.5.5 Disable Trunk

- **Step 1:** Uncheck the checkboxes.
- **Step 2:** Click the **Disable** radio button.
- **Step 3:** Click the **Apply** button to disable the trunk.

### Port Trunking

Enable  **Disable**

Port No	Member
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

## 2.6 Port Mirroring

Port mirroring allows ingress and/or egress (Received and/or Transmitted) traffic to be monitored by a single port. The single port is a “mirror capture port”. The GSS-8T2SFP can be configured to mirror the ingress and/or egress traffic of any other port(s). Several filter rules are used to avoid congestion when multiple ports are mirrored at the same time.

Port Mirroring can be configured to capture ingress and/or egress traffic of a port with the defined source/destination MAC address. A divider value can also be defined to on both ingress and/or egress types to adjust the sampling frequency by the divider value.

Select the **Mirror** menu on the web page to activate the configuration page.

## 2.6.1 Get/Refresh the Latest Mirror Settings

Click the **Mirror** menu on the web page, the latest mirror settings on the switch will be displayed.

Port Mirroring

Enable  Disable

Port No	Status
1	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
2	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
3	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
4	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
5	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
6	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
7	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
8	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF

This page provides the following parameters

- **Enable/Disable** – Click the **Enable** option to enable mirroring function or the **Disable** option to disable it.
- **Mirroring Options** – There are five options for each port:
  - **Capture** – to set the corresponding port to be a capture (monitoring) port.
  - **Ingress&Egress** – to set the corresponding port to be a monitored port to investigate bi-directional traffic.
  - **Ingress Only** – to set the corresponding port to be a monitored port to investigate only ingress (receiving, Rx) traffic.
  - **Egress Only** – to set the corresponding port to be a monitored port to investigate only egress (forwarding, Tx) traffic.
  - **OFF** – no mirroring function for the corresponding port. This is the default option.

## 2.6.2 Enable Mirror

- **Step 1:** Choose the **Capture** port (ex: port2).
- **Step 2:** Check the corresponding checkbox for monitored ports (ex: port4 **Ingress&Egress**, port6 **Ingress Only**, port8 **Egress Only**, and other ports **OFF**).
- **Step 3:** Click the **Enable** radio button.
- **Step 4:** Click the **Apply** button to enable mirroring settings.

Port Mirroring

**Enable**    **Disable**

Port No	Status
1	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
2	<input checked="" type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input type="radio"/> OFF
3	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
4	<input type="radio"/> Capture <input checked="" type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input type="radio"/> OFF
5	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
6	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input checked="" type="radio"/> Ingress Only <input type="radio"/> Egress Only <input type="radio"/> OFF
7	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
8	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input checked="" type="radio"/> Egress Only <input type="radio"/> OFF

### 2.6.3 Modify Mirror Settings

- **Step 1:** Change the capture or monitored ports (ex: port3 **Capture**, port5 **Ingress/Egress**, port7 **Ingress Only**, port8 **Egress Only**, and other ports **OFF**).
- **Step 2:** Click the **Apply** button to modify the mirroring settings.

**Port Mirroring**

**Enable**    **Disable**

Port No	Status
1	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
2	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
3	<input checked="" type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input type="radio"/> OFF
4	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
5	<input type="radio"/> Capture <input checked="" type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input type="radio"/> OFF
6	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
7	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input checked="" type="radio"/> Ingress Only <input type="radio"/> Egress Only <input type="radio"/> OFF
8	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF

## 2.6.4 Disable Mirror

- **Step 1:** Click the **Disable** button.
- **Step 2:** Click **OFF** for all ports.
- **Step 3:** Click the **Apply** button to disable mirroring.

**Port Mirroring**

Enable  **Disable**

Port No	Status
1	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
2	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
3	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
4	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
5	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
6	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
7	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF
8	<input type="radio"/> Capture <input type="radio"/> Ingress&Egress <input type="radio"/> Ingress Only <input type="radio"/> Egress Only <input checked="" type="radio"/> OFF



## 2.6.5 Get/Refresh the Latest Mirror Filter Settings

Click the **Mirror** menu and click the **Filter** button. The latest mirror filter settings on the switch will be displayed.

### Mirror Filter Configuration

Ingress Filter       All Frames    Source Address    Destination Address

Ingress MAC Address  -  -  -  -  -

Ingress Divider       (0 ~ 1023)

Egress Filter         All Frames    Source Address    Destination Address

Egress MAC Address  -  -  -  -  -

Egress Divider         (0 ~ 1023)

This page provides the following parameters:

- **Ingress/Egress Filter**
  - **All Frames** – to mirror all frames of monitored port(s) for ingress/egress direction.
  - **Source Address** – to mirror frames with a source address matching the Ingress/Egress MAC Address.
  - **Destination Address** – to mirror frames with a destination address matching the Ingress/Egress MAC Address.
- **Ingress/Egress MAC Address** – Enter the specific MAC address that you want to monitor.
- **Ingress/Egress Divider** – Enter the specific divider number (0 ~ 1023). Divider is used to decrease congestion when multiple ports are monitored. The divider value determine the number of frames between each sample frame. ie each nth frame matching the **Ingress/Egress Filter** settings will be mirrored. If the divider value is equal to 0 (default value), each frame matching the **Ingress/Egress Filter** settings will be mirrored. If the divider value is equal to 5, then each 5<sup>th</sup> frame is mirrored.

## 2.6.6 Configure Mirror Filter

- **Step 1:** Choose Ingress Filter to be a **Source Address**, and choose Egress Filter to be a **Destination Address**.
- **Step 2:** Enter Ingress MAC Address (00-01-02-03-04-05), and Egress MAC Address (0A-0B-0C-0D-0E-0F).
- **Step 3:** Enter Ingress Divider as 5, and enter Egress Divider as 8.
- **Step 4:** Click the **Apply** button to activate the mirroring filter settings.

### Mirror Filter Configuration

Ingress Filter       All Frames    Source Address    Destination Address

Ingress MAC Address    -  -  -  -  -

Ingress Divider       (0 ~ 1023)

Egress Filter       All Frames    Source Address    Destination Address

Egress MAC Address    -  -  -  -  -

Egress Divider       (0 ~ 1023)

**Result:** Every fifth frame with source address (00-01-02-03-04-05) in ingress direction on monitored port(s) and every eight frame with destination address (0A-0B-0C-0D-0E-0F) in egress direction on monitored port(s) will be mirrored.

## 2.6.7 Disable Mirror Filter

- **Step 1:** Change Ingress/Egress Filter to **All Frames**.
- **Step 2:** Set Ingress/Egress Divider equal to 0.
- **Step 2:** Click the **Apply** button to modify mirroring filter settings.

### Mirror Filter Configuration

Ingress Filter       All Frames    Source Address    Destination Address

Ingress MAC Address    -  -  -  -  -

Ingress Divider       (0 ~ 1023)

Egress Filter         All Frames    Source Address    Destination Address

Egress MAC Address    -  -  -  -  -

Egress Divider         (0 ~ 1023)

## 2.7 QOS (Quality of Service)

The GSS-8T2SFP provides up to four internal transmit queues per port to support four different traffic priorities. The high-priority traffic experiences less delay in the switch than that of lower priority traffic under congested conditions. For sensitive traffic, minimizing the delay time can be very important. The GSS-8T2SFP provides three types of QOS. It can assign packets to one of four transmit queues according to Port-Based QOS, 802.1P QOS or MAC-Based QOS. Port-Based QOS arranges packets into one of four transmit queues by priority id of 802.1Q VLAN tag set in 802.1Q VLAN page (802.1Q Control Per Port Config). 802.1P QOS arranges packet in to one of four transmit queues by priority of ingress packet with 802.1Q VLAN tag. MAC-Based QOS arranges packets in to one of four transmit queues by priority of ingress packet with the priority being set in the Address Management page.

The GSS-8T2SFP also provides a remap function. The GSS-8T2SFP always inserts the packets into the Tx Queue by it's priority ID when the QOS function is enabled. Switch administrators can modify the Priority ID to Tx Queue ID Map. Switch administrators can also remap 802.1Q priority levels to priority ID's. The GSS-8T2SFP handles the packets transmitted by the Tx Queue Weight Setting when Weighted Round-Robin algorithm is selected and QOS functions are enabled.

Select the **QOS** menu on the web page to activate the QOS configuration.

## 2.7.1 Get/Refresh the Latest QOS Settings

Click the **QOS** menu on the web page, the latest QOS settings on the switch will be displayed.

The screenshot shows a web interface for configuring Quality of Service (QOS). At the top, a red banner reads "Quality Of Service". Below this, there are two radio buttons: "Enable" (unselected) and "Disable" (selected). The interface is divided into two main sections. The first section, "Transmit Queue Algorithm", contains two radio buttons: "Highest Queue Preempt" (unselected) and "Weighted Round-Robin" (selected). The second section, "QOS Type", contains two checkboxes: "Port-Based QOS" (unchecked) and "802.1P QOS" (unchecked). At the bottom of the configuration area, there are three buttons: "Apply", "Configure", and "Back".

The following parameters are provided:

### ■ Enable/Disable

- **Enable** – Enable the QOS functions
- **Disable** – Disable the QOS functions. When QOS is disabled, GSS-8T2SFP will transmit all packets in FIFO (First in First Served) mode.

### ■ Transmit Queue Algorithm

- **Highest Queue Preempt** – Transmit all packets in highest queue first, and transmit other lower queues in weighted-round robin mode.
- **Weighted-Round Robin** – Transmit all packets in weighted-round robin mode.

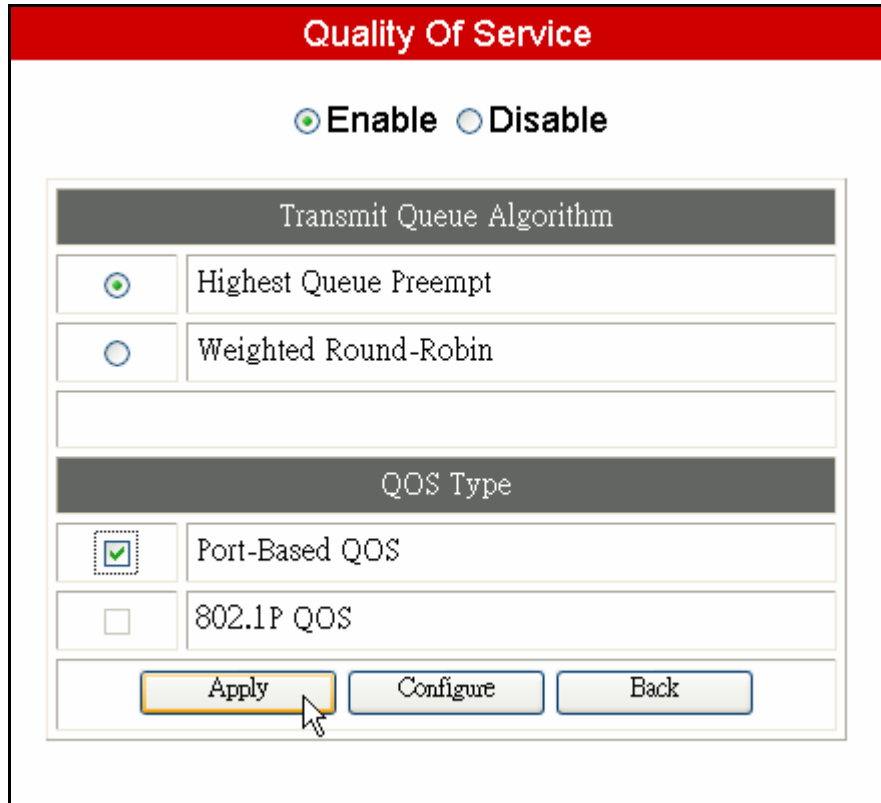
### ■ QOS Type

- **Port-Based QOS** – Enable port-based QOS type.
- **802.1P QOS** – Enable 802.1P QOS type.

**Note:** If the administrator selects Port-Based QOS and enables the QOS function, the GSS-8T2SFP will handle all packets as Port-Based QOS types. If the administrator selects 802.1P QOS and enables the QOS function, then the GSS-8T2SFP will handle packets with an 802.1Q tags as a 802.1P QOS type, and handle packets without 802.1Q tags as a MAC-Based QOS type. If user select no QOS type and enables the QOS function, the GSS-8T2SFP will handle all packets as MAC-Based QOS type.

## 2.7.2 Enable QOS

- **Step 1:** Choose the **Transmit Queue Algorithm** (ex: Highest Queue Preempt).
- **Step 2:** Choose the **QOS Type** (ex: Port-Based QOS).
- **Step 3:** Click the **Enable** radio button.
- **Step 4:** Click the **Apply** button to enable the QOS settings.



The image shows a web-based configuration interface for Quality of Service (QoS). The interface has a red header bar with the text "Quality Of Service". Below the header, there are two radio buttons: "Enable" (which is selected) and "Disable". Underneath, there are two sections. The first section is titled "Transmit Queue Algorithm" and contains two radio button options: "Highest Queue Preempt" (selected) and "Weighted Round-Robin". The second section is titled "QOS Type" and contains two checkbox options: "Port-Based QOS" (checked) and "802.1P QOS" (unchecked). At the bottom of the interface, there are three buttons: "Apply" (highlighted with a yellow border and a mouse cursor), "Configure", and "Back".

## 2.7.3 Modify QOS Settings

- **Step 1:** Choose the **Transmit Queue Algorithm** (ex: Weight-Round Robin).
- **Step 2:** Choose the **QOS Type** (ex: 802.1P QOS).
- **Step 3:** Click the **Apply** button to modify QOS settings.

**Quality Of Service**

**Enable**  **Disable**

**Transmit Queue Algorithm**

Highest Queue Preempt

Weighted Round-Robin

**QOS Type**

Port-Based QOS

802.1P QOS

**Apply** **Configure** **Back**

## 2.7.4 Disable QOS

- **Step 1:** Click the **Disable** button.
- **Step 2:** Click the **Apply** button to disable QOS.

The image shows a web-based configuration interface for Quality of Service (QoS). The title bar is red and contains the text "Quality Of Service". Below the title bar, there are two radio buttons: "Enable" (unselected) and "Disable" (selected). The "Disable" button is highlighted with a dashed border. Below this, there are two sections: "Transmit Queue Algorithm" and "QOS Type". The "Transmit Queue Algorithm" section has two radio buttons: "Highest Queue Preempt" (unselected) and "Weighted Round-Robin" (selected). The "QOS Type" section has two checkboxes: "Port-Based QOS" (unselected) and "802.1P QOS" (checked). At the bottom of the interface, there are three buttons: "Apply" (highlighted with a yellow border and a mouse cursor), "Configure", and "Back".



## 2.7.5 Get/Refresh the Latest QOS Detailed Settings

Select the **QOS** menu and click the **Configure** button, the latest detailed QOS settings on the switch will be displayed.

QOS Configuration								
Priority ID to Tx Queue ID Map								
Priority ID	0	1	2	3	4	5	6	7
Tx Queue ID (0 ~ 3)	0	0	1	1	2	2	3	3
Tx Queue ID : 3 = Highest, 2 = High, 1 = Low, 0 = Lowest								
802.1p Priority Level to Priority ID Map								
802.1p Priority Level	0	1	2	3	4	5	6	7
Priority ID (0 ~ 7)	0	1	2	3	4	5	6	7
Tx Queue Weight Setting								
Tx Queue	Highest	High	Low	Lowest				
Weight (1 ~ 255)	008	004	002	001				
<input type="button" value="Apply"/> <input type="button" value="Back"/>								

The parameters provided are:

- **Priority ID to Tx Queue ID Map** – Enter the corresponding Tx Queue ID (0 ~ 3) for each Priority ID.
- **802.1p Priority Level to Priority ID Map** – Enter the corresponding Priority ID (0 ~ 7) for each 802.1p Priority Level.
- **Tx Queue Weight Setting** – Enter the corresponding Weight (1 ~ 255) for each Tx Queue.

## 2.7.6 Configure Detailed QOS Settings

- **Step 1:** Enter Tx Queue ID by the following order (e.g. 0, 0, 0, 1, 2, 2, 2, 3)
- **Step 2:** Enter Priority ID by the following order (e.g. 0, 1, 2, 3, 4, 5, 6, 7)
- **Step 3:** Enter Tx Queue Weight by the following order (e.g. 100, 20, 10, 5)
- **Step 4:** Click the **Apply** button to activate the QOS settings

QOS Configuration								
Priority ID to Tx Queue ID Map								
Priority ID	0	1	2	3	4	5	6	7
Tx Queue ID (0 ~ 3)	0	0	0	1	2	2	2	3
Tx Queue ID : 3 = Highest, 2 = High, 1 = Low, 0 = Lowest								
802.1p Priority Level to Priority ID Map								
802.1p Priority Level	0	1	2	3	4	5	6	7
Priority ID (0 ~ 7)	0	1	2	3	4	5	6	7
Tx Queue Weight Setting								
Tx Queue	Highest	High	Low	Lowest				
Weight (1 ~ 255)	100	20	10	5				
<input type="button" value="Apply"/> <input type="button" value="Back"/>								

### Results of the Configuration Example:

- (1) All packets with priority id equal to 0, 1 and 2 will be stored in transmit queue id equal to 0 (the transmit queue with lowest priority).
- (2) All packets with priority id equal to 3 will be stored in transmit queue id equal to 1 (the transmit queue with low priority).
- (3) All packets with priority id equal to 4, 5 and 6 will be stored in transmit queue id equal to 2 (the transmit queue with high priority).
- (4) All packets with priority id equal to 7 will be stored in transmit queue id equal to 3 (the transmit queue with highest priority).
- (5) This system will map the priority id of all packets with 802.1Q VLAN tags to their equivalent 802.1Q VLAN tag.
- (6) If QOS type is Weighted-Round Robin, this system will transmit 100 packets from the highest priority queue, then 50 packets from the high priority queue, then 10 packets from the low priority queue and lastly 5 packets in lowest priority queue, before repeat the procedure again from the highest priority queue.

## 2.8 Rate Control

The GSS-8T2SFP's rate control works on a credit-based rate system that figuratively uses buckets to track the bandwidth of each port. You can set a **bucket bit rate** to control the bandwidth of each port, and set which packet type you want to monitor with this bucket.

The rate control function in this switch employs two buckets to track the rate of ingress (received) packets. Each of the two buckets, Bucket 0 and Bucket 1, can be set to monitor a specified packet type. For example, Bucket 0 could monitor broadcast packets, while Bucket 1 could monitor unicast packets. Multiple packet types can be monitored by each bucket, and a packet type can be monitored by both buckets.

The **Bucket bit rate** can be set by the **rate count** which ranges from 1 to 125. The rate count value must be set on a per port basis and bucket number. Whenever you set the rate count value, the switch will auto-negotiate the current link speed (10/100/1000 Mbps) to calculate the resultant rate limit. For example, if you set Bucket 0 on port 1's rate count to a value of 20, the actual rate percentage will be 16%. If the current link speed is 10Mbps, the rate limit will be 1.6Mbps. If the current link speed is 100Mbps, the rate limit will be 16Mbps. If the current link speed is 1000Mbps, the rate limit will be 160Mbps.

## 2.8.1 Enable/Disable Rate Control

In the following page, you can enable/disable the rate control function on a per port basis. Use the Enable option to define the port(s) speed limit for forwarding traffic based on the rate value of the ingress port. For example, traffic flows from port1 to port2 (ordinary link speed 1000Mbps for both ports) and the rate control is enabled on port1 with rate value 50%, the actual outgoing traffic speed on port2 will be 500Mbps (50% of 1000Mbps).

**Rate Control**

Port 1	Enable <input type="button" value="v"/>
Port 2	Enable <input type="button" value="v"/>
Port 3	Disable <input type="button" value="v"/>
Port 4	Disable <input type="button" value="v"/>
Port 5	Disable <input type="button" value="v"/>
Port 6	Enable Disable <input type="button" value="v"/>
Port 7	Disable <input type="button" value="v"/>
Port 8	Disable <input type="button" value="v"/>

After you have selected the Enable/Disable field values, you must click the Apply button to activate the settings.

## 2.8.2 Ingress Rate Control Common Config

To configure this function, click the **Ingress Rate Control Common Config** button. The following page is presented.

Packets To Be Monitored	Bucket 0	Bucket 1
Unicast Frame	Enable	Enable
Broadcast with Packet Length >= 1536 Bytes	Disable	Disable
Broadcast with Packet Length < 1536 Bytes	Disable	Disable
Destination Lookup Fail	Disable	Disable

Apply Back

You can monitor four types of packets and choose which bucket to monitor the specified packets from

- **Unicast Frame** : Unicast are directed point-to-point packets, choose Bucket 0 and/or Bucket 1.
- **Broadcast with Packet Length >= 1536 Bytes**: This option enables Rate control of Jumbo Frame size broadcast packets. This can be used to limit problems associated with system performance caused excessive broadcast packets.
- **Broadcast with Packet Length <1536 Bytes**: This option enables Rate control of ordinary frame size broadcast packets. This can be used to limit problems associated with system performance caused excessive broadcast packets.
- **Destination Lookup Fail**: Used to apply Rate control to packets whose destination addresses (DA) don't exist in the switches address table for lookup. These packets are normally broadcast on all ports of the switch, and excessive amounts of this type of traffic can cause congestion problems. Select this to limit the max rate of Destination Lookup Fail packets.

As mentioned before, you can select the same packet type in both buckets. For example, select unicast frames for monitoring on both buckets. You can also select multiple packet types in the same bucket. For example, select all packet types in Bucket 0, or Bucket 1.

### Note: Why 2 bucket system?

A one bucket system does not allow for heavy traffic conditions. Excessive traffic of one particular type can cause bucket overflow, so that the switch as a whole is affected. Using 2 buckets and distributing the packet types to different buckets minimizes the likelihood of a bucket overflow affecting the switch.

### 2.8.3 Ingress Rate Limit Config for Buckets

To limit the traffic rate for specified port(s), click the **Ingress Rate Limit Config for Bucket0** or **Ingress Rate Limit Config for Bucket1** button in the **Rate Control** page to open the page for configuring the ingress rate limit for Bucket0 or Bucket1 respectively.

The Ingress Rate Limit Config for Bucket 0 page is shown below:

**Ingress Rate Limit Config for Bucket 0**

Rate Limit depends on Link speed 10/100/1000Mb

Port	Ingress Rate(1-125)	Rate(%)
1	<input type="text" value="125"/>	100%
2	<input type="text" value="100"/>	80%
3	<input type="text" value="80"/>	64%
4	<input type="text" value="70"/>	56%
5	<input type="text" value="60"/>	48%
6	<input type="text" value="50"/>	40%
7	<input type="text" value="40"/>	32%
8	<input type="text" value="30"/>	24%

The field **Ingress Rate(1-125)** is an integer that increments/decrements the ingress rate at a given port and must be specified on a per port basis. After you enter the **Ingress Rate(1-125)** value, the rate percent field will automatically update to the rate value as a percentage. The page shown above displays this feature. Ingress rate value and its calculated percentage of rate for each port.

(e. g. ingress rate value 125 = 100%, 50 = 40%)

Remember to click the **Apply** button to activate the settings.

The maximum forwarding traffic rate will be limited by the percentage of rate for the current link speed on the specified ingress port. The following table shows the limited traffic speeds based on the different rates in different link speeds (10/100/1000Mbps).

Rate	Link Speed		
	10Mbps	100Mbps	1000Mbps
100%	10Mbps	100Mbps	1000Mbps
80%	8Mbps	80Mbps	800Mbps
64%	6.4Mbps	64Mbps	640Mbps
56%	5.6Mbps	56Mbps	560Mbps
48%	4.8Mbps	48Mbps	480Mbps
47%	4.7Mbps	47Mbps	470Mbps
32%	3.2Mbps	32Mbps	320Mbps
24%	2.4Mbps	24Mbps	240Mbps

The Identical interface to configure the ingress rate limit for Bucket 1.

**Ingress Rate Limit Config for Bucket 1**

Rate Limit depends on Link speed 10/100/1000Mb

Port	Ingress Rate(1-125)	Rate(%)
1	<input type="text" value="50"/>	40%
2	<input type="text" value="95"/>	76%
3	<input type="text" value="85"/>	68%
4	<input type="text" value="75"/>	60%
5	<input type="text" value="65"/>	52%
6	<input type="text" value="55"/>	44%
7	<input type="text" value="45"/>	36%
8	<input type="text" value="35"/>	28%

## 2.9 Address Management

The GSS-8T2SFP provides **up to 10** static MAC address entries. These entries always exist in the switch's address table and will never be dropped through normal switch MAC aging out. (All dynamic MAC entries from the address learning mechanism will be retained in the address table for up to 300 seconds.)

If the switch administrator adds a static MAC address entry in to the switch and a 802.1Q VLAN is not enabled, the GSS-8T2SFP will search for the MAC address in the address table according to the MAC address.

If a 802.1Q VLAN is enabled, the GSS-8T2SFP will search this MAC address in the address table according to both the MAC address and the VLAN id. The priority of the static entry is inserted for MAC-Based QOS services. If the switch administrator enables QOS and does not select Port-Based or 802.1P based QOS types, then the priority ID of the ingress packets is equal to the priority of the matched MAC address that is inserted in the static MAC address table.



## Get/Refresh the Latest Address Management Settings

Click the **Address Management** menu on the web page, the latest Address Management settings on the switch will be displayed.

Static MAC Entry Table					
Select	Entry	Port	MAC Address	VID	Priority
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Back"/>					

The following options are provided:

- **Add**: Add a new entry into the static MAC entry table.
- **Delete**: Remove an existing entry from the static MAC entry table.
- **Edit**: Modify an existing entry in static MAC entry table.

## 2.9.1 Add a New Entry

- **Step 1:** Click the **Add** button.
- **Step 2:** Choose the **Port No.** (e.g.: Port 3)
- **Step 3:** Enter the **MAC Address.** (e.g.: 31-32-33-34-35-36)
- **Step 4:** Enter the **VLAN ID.** (e.g.: 3333) (Range: 1 ~ 4094)
- **Step 5:** Choose the **Priority.** (e.g.: Priority = 3)

### Static MAC Entry Configuration

Entry No

Port No

MAC Address  -  -  -  -  -

VLAN ID  (1 - 4094)

Priority

After clicking the **Apply** button, the result will be shown on the page as below.

Static MAC Entry Table					
Select	Entry	Port	MAC Address	VID	Priority
<input type="radio"/>	1	3	31-32-33-34-35-36	3333	3
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Back"/>					

## 2.9.2 Modify an Existing Entry

- **Step 1:** Choose Entry No 1 and click the **Edit** button in the **Static MAC Entry Table** page.
- **Step 2:** Modify Port No to be Port 6.
- **Step 3:** Modify MAC Address to be 61-62-63-64-65-66.
- **Step 4:** Modify VLAN ID to be 666.
- **Step 5:** Modify Priority to be 6.
- **Step 6:** Click the **Apply** button.

### Static MAC Entry Configuration

Entry No                    1

Port No                   

MAC Address               -  -  -  -  -

VLAN ID                     (1 - 4094)

Priority

After clicking the **Apply** button, the result will be shown as below.

Static MAC Entry Table					
Select	Entry	Port	MAC Address	VID	Priority
<input type="radio"/>	1	6	61-62-63-64-65-66	666	6
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Back"/>					

### 2.9.3 Delete an Existing Entry

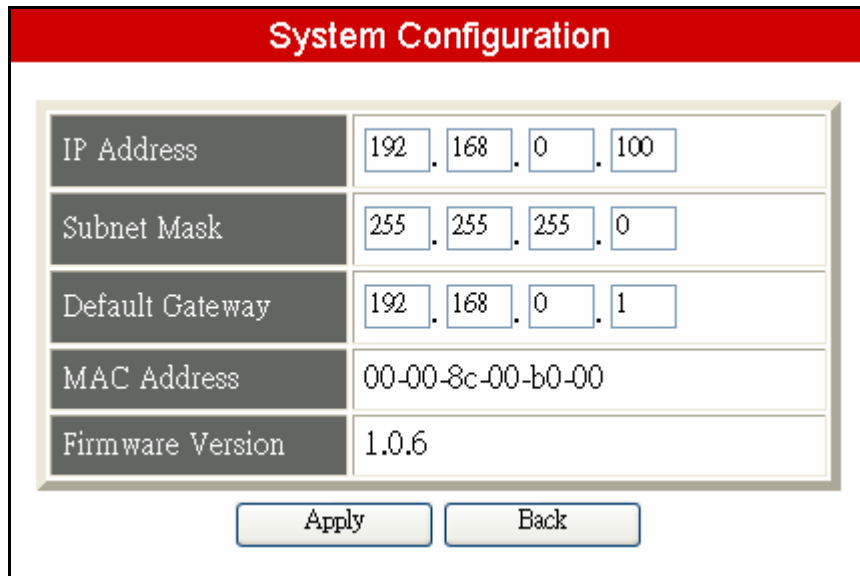
Choose a desired entry to be removed (e.g. entry1) and click the **Delete** button to complete the deletion.

After deletion, the content in the Static MAC Entry Table will be refreshed.

Static MAC Entry Table					
Select	Entry	Port	MAC Address	VID	Priority
<input checked="" type="checkbox"/>	1	6	61-62-63-64-65-66	666	6
<div style="display: flex; justify-content: space-around;"><span>Add</span><span>Delete</span><span>Edit</span><span>Back</span></div>					

## 2.10 System Configuration

The **System Configuration** page provides the management information for the switch. The page shown below can be activated by clicking the **Setup** menu under the System section.



The screenshot displays the 'System Configuration' interface. It features a red header with the title 'System Configuration'. Below the header is a table with five rows, each representing a configuration parameter. The first three rows (IP Address, Subnet Mask, and Default Gateway) have input fields for each octet of the address. The last two rows (MAC Address and Firmware Version) are read-only. At the bottom of the table are two buttons: 'Apply' and 'Back'.

System Configuration	
IP Address	192 . 168 . 0 . 100
Subnet Mask	255 . 255 . 255 . 0
Default Gateway	192 . 168 . 0 . 1
MAC Address	00-00-8c-00-b0-00
Firmware Version	1.0.6

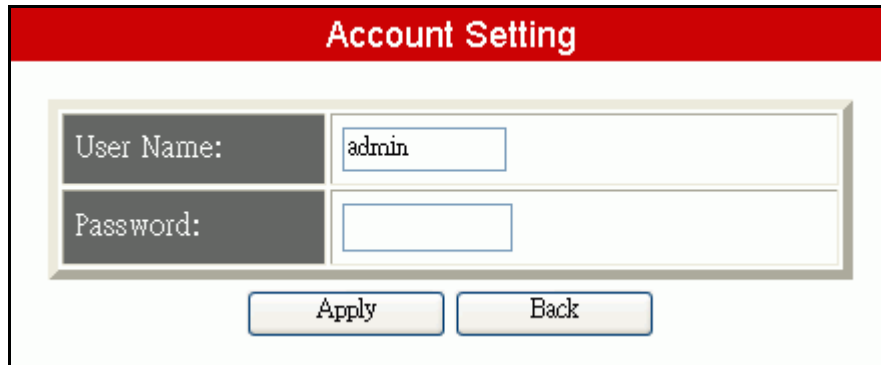
Apply      Back

The following parameters can be configured / displayed:

- **IP Address** – the IP address used to manage this switch through the configuration port.
- **Subnet Mask** – the network mask to identify the sub-network address
- **Default Gateway** – the IP address of the default gateway to reach to the outside network
- **MAC Address** – the MAC address for the configuration port interface (read-only)
- **Firmware Version** – the current version of firmware running in the switch (read-only)

## 2.11 Account Settings

Account setting is used to maintain the username and password for login validation. The switch provides only one login account for configuration management. Click the **Account** menu to activate the **Account Setting** page shown below:



Account Setting	
User Name:	<input type="text" value="admin"/>
Password:	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Back"/>	

- **User Name** – Set the username string (max. 6 characters)
- **Password** – Set the password string (max. 8 characters)

## 2.12 Reset System

This switch can be rebooted or reset to default configuration.

To reset the system, go to the **Reset** menu and open the following configuration page:



This page provides two options :

- **Reboot Only** – Reboot the system. All configuration settings will be retained to the latest changes before the reboot procedure. If you want to keep your configuration, select this option.
- **Reboot after Write Default** – Reset all configurations (including the username, password and IP address; only the MAC address will not be changed) to default settings before rebooting the system. All customized settings will be lost and unless manually reentered, will not be recoverable.

The GSS-8T2SFP also provides two alternatives to perform a **Reboot after Write Default** option by using the **Reset button** on the front panel of the switch:

- While the system is running (the DIAG LED indicator is ON), *pressing and holding the Reset button (for greater than 2 seconds) until the DIAG LED indicator begins to flash* will activate the **Write Default** procedure.
- If the system will not boot up (the DIAG LED indicator is still OFF after 7 seconds from power on), *pressing and holding the Reset button while turning the power on to the system until the DIAG LED indicator starts to flash* will activate the **Write Default** procedure.

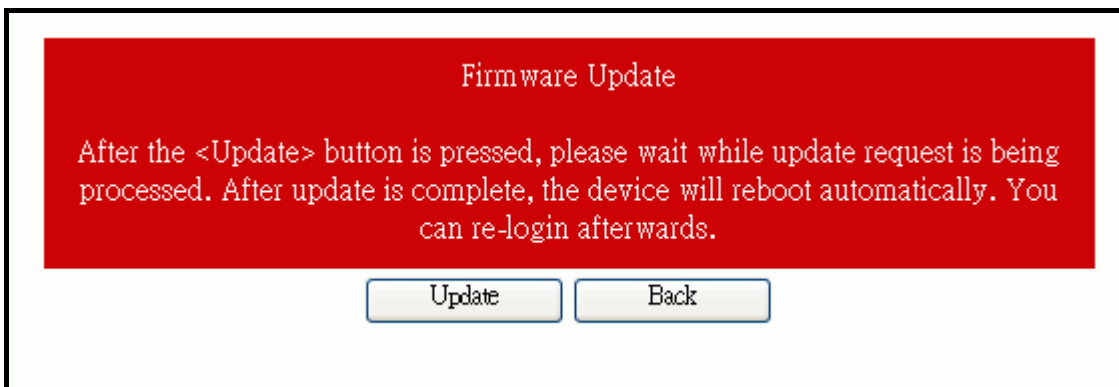
After the procedure mentioned above is done, the switch will reboot and initialize using the default settings.

Note: system rebooting time is approximately 5 seconds.

You will need to log back in to the system to continue configuring the switch.

## 2.13 Firmware Update

This switch provides the capability to update the firmware for new features, customized requests and system fault recovery. Click the **Firmware Update** menu to activate this page shown as below:



Before you update the firmware, it is required to correctly prepare the **BOOTP server** (e.g. haneWIN DHCP server) and have the **firmware file** which will be uploaded to the switch by the BOOTP server available. (Please refer to the instruction guide for setting up the BOOTP server. The **firmware filename**, **file location**, and the **IP address** to assign to the switch are three important parameters to setup the BOOTP server.)

When the BOOTP server and the firmware file is ready, click on the **Update** button to start the firmware update through the configuration port. Click the **Back** button to cancel this action.

To process the firmware update file will take approximately 40 seconds, assuming no communication problems between the switch and the BOOTP server, and assuming the firmware file can be located by BOOTP server.

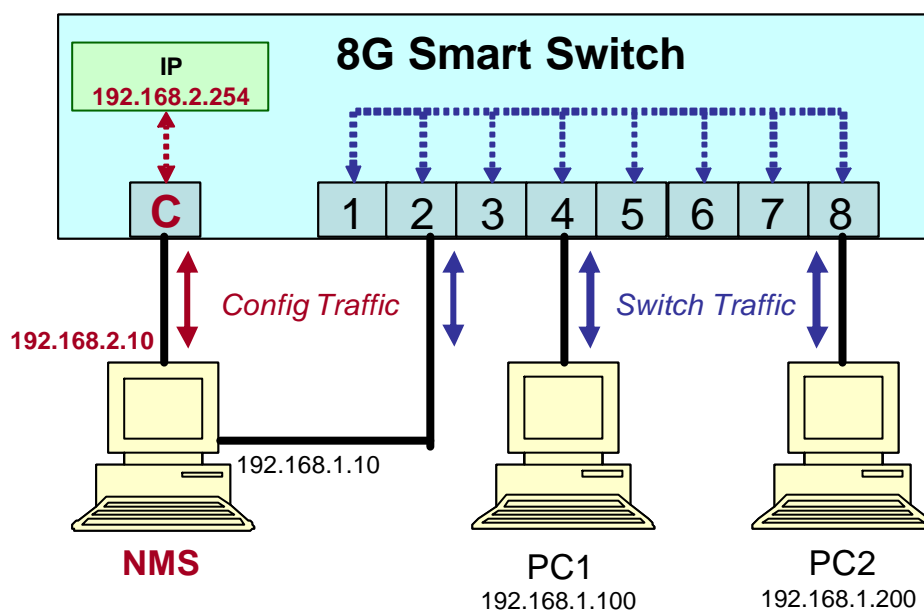


# 3 Application Notes

## 3.1 In-Band/Out-of-Band Switch Management

### ■ Out-of-Band Management

To configure the switch, a network management station (NMS) normally can connect directly via the the *Cfg Port*. This kind of connection can be regarded as an **out-of-band** switch management as the configuration traffic is totally separate from the normal (in-band) traffic through the switch ports. An example figure for out-of-band management is shown as below. The NMS needs two network interfaces to have both the in-band access and out-of-band control for switch configuration in different IP domains.

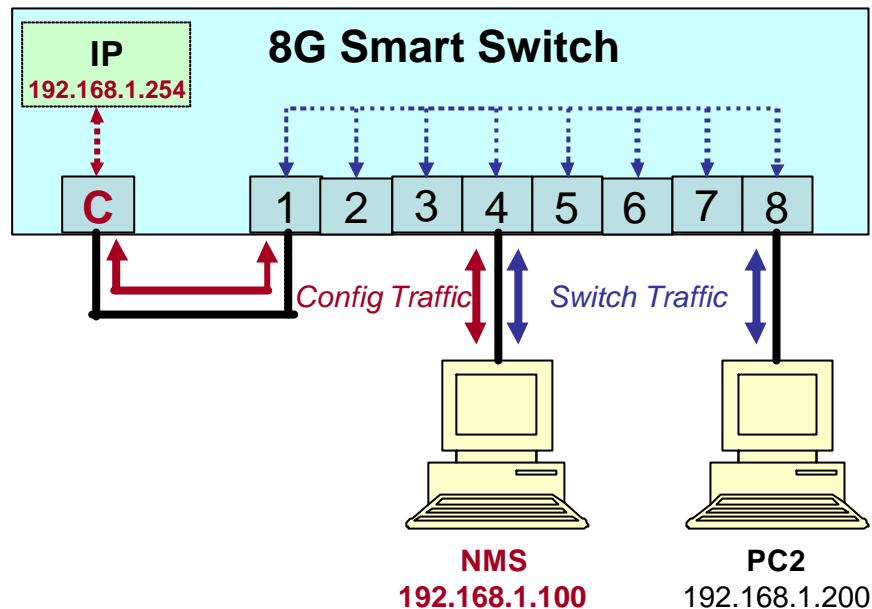


The advantages of out-of-band management, is that the configuration traffic won't be affected by switch configuration, even if all ports are disabled. The configuration traffic will be secured because of the "out-of-band" traffic isolation. In many cases switches are located in secure server rooms, so having the management port isolated from the working network is a definite security advantage.

The disadvantage is that the switch can only be configured by the PCs (e.g. PC1 or PC2) through an in-band connection when one of the 8 ports is used to link the configuration port to the in-band ports. See next heading.

## ■ In-Band Management

It is possible to achieve in-band management for the switch if necessary. The switch administrator needs to connect the *Cfg Port* to any of the normal switch ports (e.g. Port 1), then the NMS can be located anywhere within the network. The following figure shows a connection example for in-band switch management.



The advantage of in-band management is that any PC within the network can be a NMS to configure the switch.

The main disadvantage is that the switch configuration is more accessible to network users and you are relying on username/password security over physical security. By using in-band management you also lose one of the 8 Gigabit ports.