

# GV-PoE Switch

---

## *GV-POE0801 User's Manual*





© 2013 GeoVision, Inc. All rights reserved.

Under the copyright laws, this manual may not be copied, in whole or in part, without the written consent of GeoVision.

Every effort has been made to ensure that the information in this manual is accurate. GeoVision, Inc. makes no expressed or implied warranty of any kind and assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages arising from the use of the information or products contained herein. Features and specifications are subject to change without notice.

GeoVision, Inc.  
9F, No. 246, Sec. 1, Neihu Rd.,  
Neihu District, Taipei, Taiwan  
Tel: +886-2-8797-8377  
Fax: +886-2-8797-8335  
<http://www.geovision.com.tw>

Trademarks used in this manual: *GeoVision*, the *GeoVision* logo and GV series products are trademarks of GeoVision, Inc. *Windows* and *Windows XP* are registered trademarks of Microsoft Corporation.

July 2013

# Contents

1.	Safety Precautions .....	1
2.	Introduction.....	2
3.	Hardware Description .....	5
4.	Preparation for Web Configuration .....	8
5.	Login.....	10
6.	Administrator .....	11
7.	Port Management .....	17
8.	VLAN Setting.....	22
9.	Per Port Counter .....	27
10.	QoS Setting .....	28
11.	Security .....	31
12.	Spanning Tree .....	33
13.	Trunking .....	36
14.	Backup / Recovery .....	38
15.	Miscellaneous .....	39
16.	Logout .....	42
17.	Restoring Default Settings.....	43
18.	Specifications .....	44

# 1. Safety Precautions

## **FCC Warning**

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the users are encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

## **CE Mark Warning**

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the users may be required to take adequate measures.

## 2. Introduction

### Product Overview

The switch is a 8-port 10/100BaseTX, PSE plus 2-port Gigabit uplink (1xTP+1xSFP) Desktop Web Smart PoE Switch. The switch supports IEEE 802.3at Power over Ethernet standard, maximum 130 W power consumption per system and no special network cable required for connecting your powered devices (PD), such as IP cameras. The switch also provides exceptionally smart Web management features, such as VLAN, QoS, RSTP, IGMP Snooping, LACP, Port Security, etc. The switch is designed for small or medium network environment to strengthen its network connection and efficiency. It also gives you the option of installing it in a 19" cabinet with a rack-mount kit or underneath a desk.

### Key Features

#### Interface

- Number of Ports: 10

Fast Ethernet: 8-port 10/100BaseTX with IEEE 802.3at PSE

Gigabit Ethernet: 1-port 10/100/1000 Base-T, 1-port Gigabit SFP

#### Performance

- MAC Address: Up to 4K
- Buffer Memory: 2.75 Mb
- Transmission Method: Store and Forward Mechanism

### Software Feature Description

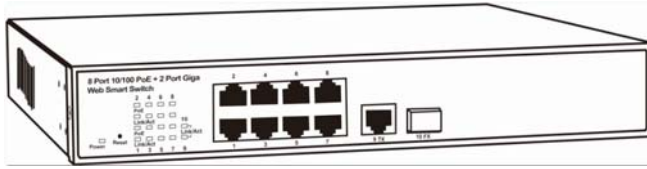
- Port Management
  - Port Configuration: Enable / Disable such as Link State, Speed / Duplex, Flow Control, Address Learning; Monitor Link Status
  - Port Mirroring: One to one, one to many, many to one mirroring
  - Bandwidth Control: Up to 256 levels Bandwidth Control for TX and RX Rate
  - Broadcast Storm Control: Broadcast Storm Control and Threshold Setting
  - PoE Control: PoE Enable / Disable, PoE Status
  - Port Counter (Statistic): Monitor the port statistic

- VLAN Setting
  - VLAN Mode: Port-based and Tag-based VLAN
  - Port Based VLAN: Up to 10 ports Port-Based VLAN
  - Tag Based VLAN: Up to 32 VLANs, Available VID from 1~4094
- QoS Setting
  - Support High & Low Priority Queue
  - Priority Mode: First-In-First-Out, Strict and Weight-Round-Robin (WRR) Priority Mode
  - Class of Service schemes: 802.1p, IP TOS / DS or Port Base
  - TCP / UDP Port & Priority queue mapping
- Security Setting
  - Port Security - Port & MAC Address Binding, up to 3 MAC Address per port
  - TCP / UDP Filtering: Protocol Port Filter for secure WAN Port
- Spanning Tree Protocol
  - Version: Support Legacy Spanning Tree Protocol & Rapid Spanning Tree Protocol
  - Loopback Detection: Loopback detection to avoid loopback on the same port.
- Trunking
  - Trunking Type: Static Trunk or LACP
  - Trunk Group: 1, Gigabit Port 9 and Port 10 can be aggregated
  - LACP Long / Short Timeout time
- IGMP Snooping V1&V2
- Basic Features
  - Embedded HTTP web Management
  - User name / Password Authentication Configuration
  - Configuration Backup / Recovery
  - Secure Management

## Package Contents

Before you start to install this switch, verify your package that contains the following items:

1. GV-POE0801 x 1



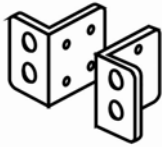
2. AC Power Cord x 1



3. Screw x 8



4. Rack Mount Kit x 1



5. User's Manual CD x 1



6. GV-POE0801 Quick Start Guide x 1

## 3. Hardware Description

This section mainly describes the hardware of the 8 PoE port Ethernet Combo Web-Smart Switch and gives a physical and functional overview on the certain switch.

### Product Overview

#### Front Ethernet Ports

The front panel of the web smart switch consists of 8 10/100Base-TX RJ-45 ports, 1 10/100/1000 M RJ-45 and 1 Gigabit SFP uplink ports.

---

**Important:** For combo uplink ports, both RJ-45 Gigabit Ethernet port and Gigabit SFP port can be used at the same time. The maximum cable length for RJ-45 Gigabit Ethernet is 100 meters. For connection that exceeds 100 meters, you can use the Gigabit SFP port.

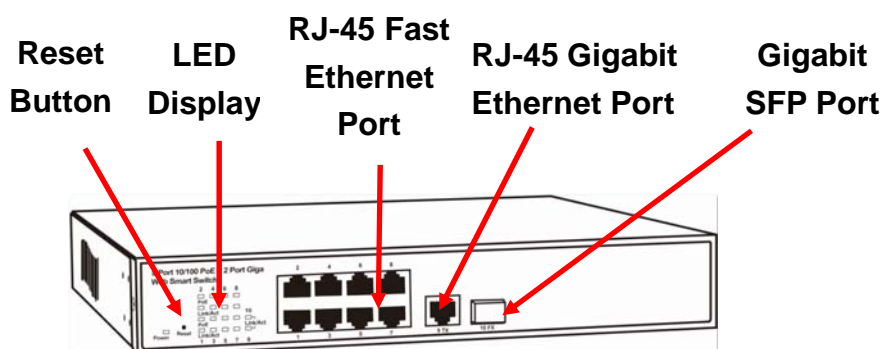
---

#### LED

The LED Indicators are also located on the front panel. They indicate the System and Port Status.

#### Reset Button

The button allows you to restore the configuration to default. For details see *17. Restoring Default Settings*.





## Rear Panel

The 3-pronged power plug is placed at the rear panel of the switch right side shown as below.



## LED Indicators

The LED Indicators present real-time information of systematic operation status. The following table provides description of LED status and their meaning.

No.	Color/Status	Description	No. of LED
Power	Amber On	Power on	Power
	Off	Power off	
Link/ ACT	Green On	Link Up	10/100 M (1~8) 1000 M (9~10)
	Green Blinking	Data is transmitting or receiving	
	Off	No connection	
PoE	Amber On	Port is linked to Power Device	10/100 M (1~8)
	Off	No Power Device is connected	

## Hardware Installation

Set the switch on a large flat space with a power socket close by. The flat space should be clean, smooth, level and sturdy. Make sure there is enough clearance around the switch to allow attachment of cables, power cord and allow air circulation. The last, use twisted pair cable to connect this switch to your PC and then users could start to operate the switch.

## AC Power Input

Connect the attached power cord to the AC power input connector; the available AC power input is range from 100-240 VAC.

## Ethernet cable Request

The wiring cable types are as below.

**10BaseT:** 2-pair UTP/STP Cat. 3, 4, 5 cable, EIA / TIA-568 100-ohm (Max. 100 m)

**100BaseTX:** 2-pair UTP/STP Cat. 5 cable, EIA / TIA-568 100-ohm (Max. 100 m)

**1000BaseT:** 4-pair UTP/STP Cat. 6 cable, EIA / TIA-568 100-ohm (Max. 100 m)

**PoE:** To delivery power without problem, the Cat 5 / 5e and Cat 6 cable is suggested. The high quality Ethernet cable reduces the lost while power transmission.

### SFP Installation

While install the SFP transceiver, make sure the SFP type of the 2 ends is the same and the transmission distance, wavelength, fiber cable can meet your request. The way to connect the SFP transceiver is to Plug in SFP fiber transceiver fist. The SFP transceiver has 2 plug for fiber cable, one is TX (transmit), the other is RX (receive). Cross-connect the transmit channel at each end to the receive channel at the opposite end.

## 4. Preparation for Web Configuration

The web management page allows you to use a standard web-browser such as Microsoft Internet Explorer, Google Chrome or Mozilla Firefox, to configure and interrogate the switch from anywhere on the network.

Before you attempt to use the web user interface to manage switch operation, verify that your switch is properly installed on your network and that every PC on this network can access the switch via the web browser.

Verify that your network interface card (NIC) is operational, and that your operating system supports TCP/IP protocol.

Wire the switch power and connect your computer to the switch. The switch default IP address is **192.168.0.250**. The switch and the connected PC should locate within the same IP Subnet.

Change your computer's IP address to 192.168.0.xxx or other IP address which is located in the 192.168.0.xxx (For example: IP Address: 192.168.0.2; Subnet Mask: 255.255.255.0) subnet.

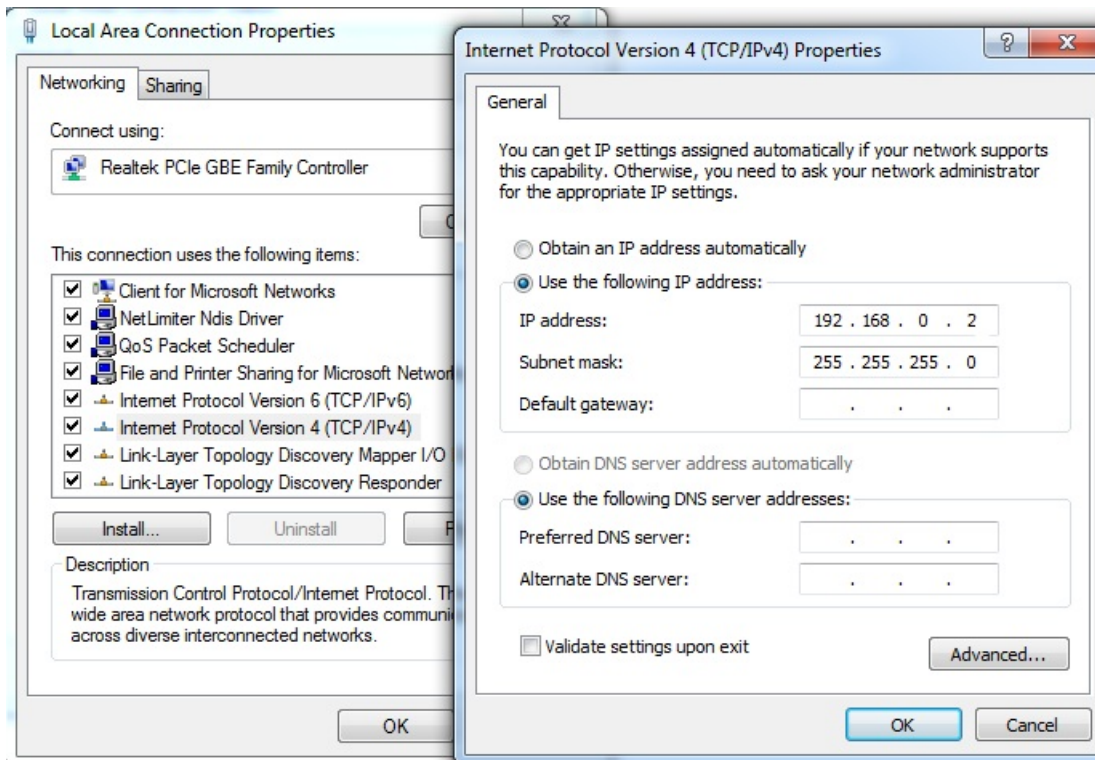


Figure 4-1

Launch the web browser and Login.

1. Launch the web browser (Internet Explorer or Mozilla Firefox) on the PC.
2. Type **http://192.168.0.250** (or the IP address of the switch). And then press **Enter**.
3. The login screen will appear next.
4. Type the default user name and password: **admin**.

If you can't login the switch, the following steps can help you to identify the problem.

1. Switch to DOS command mode and type the "**ipconfig**" to check the NIC's setting. Type the "**ping 192.168.0.250**" to verify a normal response time.
2. Check the security or Firewall settings, high security level may limit the web access.
3. Try a different web browser, like the Mozilla or Google Chrome.

## 5. Login

This part instructs users how to set up and manage the switch through the web user interface. Follow the description to understand the procedure.

At first, open the web browser, type **http://192.168.0.250** and then the users will see the login page. Type the default ID and password **admin** and click **OK** to pass the authentication. Once you are logged in, the main page will appear.

### Login Page



Figure 5-1

### Main Page

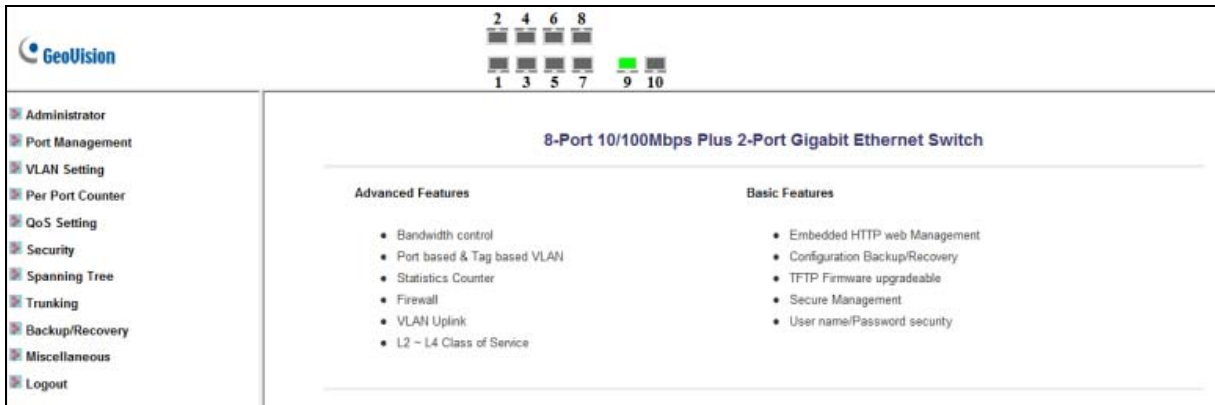


Figure 5-2

## 6. Administrator

### Authentication Configuration

This page shows authentication configuration information. Users can set new Username and Password in this page.

Authentication Configuration	
Setting	Value
Username	<input type="text" value="admin"/> max:15
Password Confirm	<input type="password" value="••••"/> max:15 <input type="password" value="••••"/>
<input type="button" value="Update"/>	

**Note:**  
Username & Password can only use "a-z","A-Z","0-9","\_","+","-","=".

Figure 6-1

### System IP Configuration

This page shows system configuration including the current IP address and sub-net mask and gateway.

Setting	Value
IP Address	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="0"/> . <input type="text" value="250"/>
Subnet Mask	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
Gateway	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="2"/> . <input type="text" value="254"/>
IP Configure	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
<input type="button" value="Update"/>	

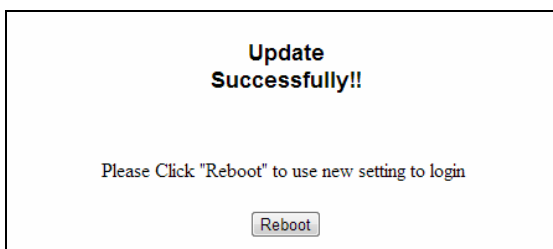
Figure 6-2

Users can configure the IP settings, Subnet Mask, Gateway as below:

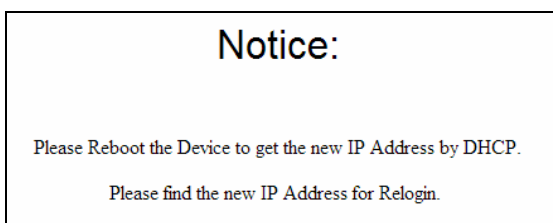
- **IP address:** Manually assign the IP address that the network is using. The default IP is 192.168.0.250.
- **Subnet Mask:** Assign the subnet mask to the IP address. The default Subnet Mask is 255.255.255.0.
- **Gateway:** Assign the network gateway for industrial switch. The default Gateway is 192.168.2.254.
- **IP Configure:** Select the **Static** or **DHCP**.

The default setting is **Static**. You can manually configure the IP Address settings. Select **DHCP** mode means the switch acts as the **DHCP** client and the switch will try getting the IP Address from the DHCP server.

Click **Update** to update the new settings.



It will show **update successfully** and then press **Reboot** button. It will enter user login screen automatically.



---

**Note:** After changed to DHCP mode, the switch must be restarted to get new IP address. However, since the switch only provide web management, it is hard for users to find its new IP. Don't try this mode without pre-configured DHCP setting in DHCP Server.

---

## System Status

This page displays the information about the switch of MAC address, how many ports it has, system version and. Besides, users can also fill in up to 15 characters in the Comment, Contact and Location field for note.

System Status	
MAC Address	10:f0:13:f0:18:26
Number of Ports	8+2
Comment	<input type="text" value="switch"/> MAX:15
System Version	V110613
<input type="checkbox"/> Idle Time Security	Idle Time: <input type="text" value="0"/> (1~30 Minutes) <input type="radio"/> Auto Logout(Default). <input type="radio"/> Back to the last display.
<input type="button" value="Update"/>	
<small>Note:            Comment name only can use "a-z","A-Z","_"," ","+","-","0-9"</small>	

Figure 6-3

- **MAC Address:** Displays the unique hardware address assigned by manufacturer (default).
- **Number of Ports:** Displays number of ports in the switch.
- **System Version:** Displays the switch's firmware version.
- **Idle Time Security:** User can set the time security. When user leave the computer for a moment, the software will auto logout or back to the last display.

And then click **Update** button. The system may request you to restart the switch, follow the instruction.

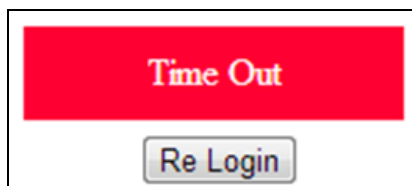


Figure 6-4



## Load Default Setting

Clicking the **Load** button will make the switch being set to the original configuration.



*Figure 6-5*

---

**Note:** Loading default from the web interface does not include user name, password and IP configuration. If you want to restore default settings including IP, user name and password, you can press the **Reset** button on the front panel of the switch. For details, see *17 Loading Default Settings..*

---

### Firmware Update

Before the firmware update procedure is executed, you should enter the password twice and then press **Update** button.

Notice:  
After clicking the "UPDATE" button, IF the firmware update webpage is not redirected correctly or is shown as "Webpage not found". Please connect to <http://192.168.0.250>

Figure 6-6

The popup warning window appears for making sure you want to proceed the firmware upgrading process. The flash memory will be erased, and all functions will be disabled temporarily except the firmware update itself. Click **Yes** to continue. If not, click **Cancel**.

Figure 6-7

The smart switch will erase the flash memory. There is a self-protection mechanism in the Boot Loader, so the Boot Loader will keep intact. Even though the power is turned off or the cable link fails during the firmware update procedure, the Boot loader will restore the code to firmware update page.

After pressing **Update** button, the old web code will be erased. Then you can click **Browse** to select the image file (.bin), and click **Update** to continue the firmware upgrading process.

Figure 6-8

The below screen shows the Uploading process is starting.

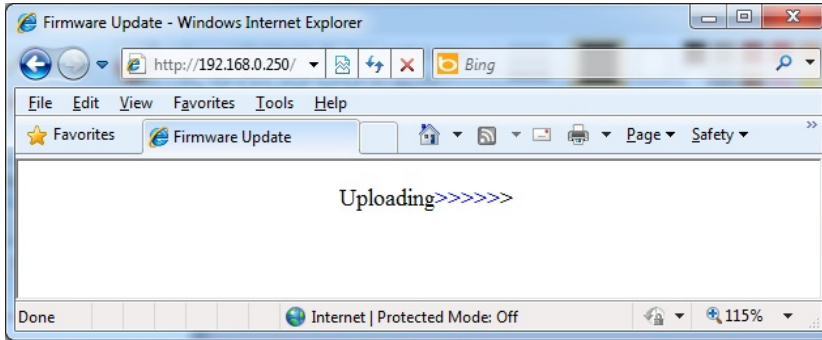


Figure 6-9

After firmware is correctly uploaded, the web page shows OK. Click **Continue** to re-login the switch.

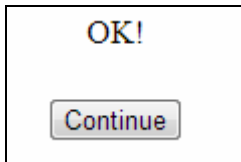


Figure 6-10

### Reboot Device

Click **Confirm** button to restart the switch.



Figure 6-11

## 7. Port Management

Port Management includes Port Configuration, Port Mirroring, Bandwidth Control, Broadcast Storm Control and PoE.

### Port Configuration

In Port Configuration, you can set and view the operation mode for each port.

Port Configuration													
Function	Tx/Rx Ability		Auto-Negotiation		Speed		Duplex		Pause		Backpressure		Addr. Learning
Select Port No.	1 2 3 4 5 6 7 8 9 10												
Update													
Port	Current Status					Setting Status							
	Link	Speed	Duplex	FlowCtrl	Tx/Rx Ability	Auto-Nego	Speed	Duplex	Pause	Backpressure	Addr. Learning		
1	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	ON		
2	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	ON		
3	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	ON		
4	●	100M	FULL	ON	ON	AUTO	100M	FULL	ON	ON	ON		
5	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	ON		
6	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	ON		
7	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	ON		

Figure 7-1

#### ● Function:

- **TX / RX-Ability: Enable or Disable.** The default value is **Enable**. Being set as **Enable**, the port can Transmit and Receive packet without any problem. After changed to **Disable**, the selected ports cannot access the network any more.
- **Auto-Negotiation: Enable and Disable.** Being set as **Enable**, the Speed, Duplex mode, Pause, Backpressure and Address Learning are negotiated automatically. When you set it as **Disable**, you have to assign those items manually.
- **Speed:** When the Auto-Negotiation column is set as **Disable**, users have to set the connection speed to the ports ticked.
- **Duplex:** When the Auto-Negotiation column is set as **Disable**, users have to set the connection mode in Half/Full to the ports ticked.
- **Pause:** Flow Control for connection at speed of 10/100Mbps in Full-duplex mode.
- **Backpressure:** Flow Control for connection at speed of 10/100Mbps in Half-duplex mode.
- **Addr. Learning:** When the Auto-Negotiation column is set as **Disable**, users have to set this column as **Enable** or **Disable**.

- **Select Port No.:** Select the port/ports you want to apply to. You can select one or multiple ports here.

Click **Update** to have the configuration take effect.

### Port Mirroring

The Port mirroring is a method for monitoring traffic in switched networks. That Traffic through ports can be monitored by any of the ports means traffic goes in or out monitored (source) ports will be duplicated into mirroring (destination) port.

Dest Port	1	2	3	4	5	6	7	8	9	10
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Monitored Packets	<div style="border: 1px solid #ccc; padding: 2px;"> <span style="background-color: #e0e0e0; padding: 2px;">Disable</span> </div>									
Source Port		2	3	4	5	6	7	8	9	10
		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Update"/>										
Multi to Multi Sniffer function										

*Figure 7-2*

- **Destination (mirroring) port** for monitoring RX only, TX only or both RX and TX traffic which come from the source port. Users can connect the mirroring port to LAN analyzer or NetXRay.
- **Monitored Packets:** Pull down the selection menu to choose what kind of packet is to be monitored. RX indicates the Received Packets; TX indicates the Transmitted Packets. TX & RX indicates Both Transmitted and Received.
- **Source Port:** The ports that the users want to monitor. All monitored port traffic will be copied to mirroring (destination) port. Users can select multiple source ports by ticking the check boxes beneath the port number label to be monitored.

And then, click **Update** to have the configuration take effect.

**Bandwidth Control**

This page allows the setting of the bandwidth for each port. The TX rate and RX rate can be filled with the number ranging from 1 to 255. This number should be multiplied by the selected bandwidth resolution to get the actual bandwidth.

Bandwidth Control		
Port No	Tx Rate	Rx Rate
01	(0-255) <input type="text"/> (0:Full Speed)	(0-255) <input type="text"/> (0:Full Speed)
Speed Base	High <input type="text"/> Low: (1)32Kbps Tx/Rx bandwidth resolution for port 1~ port 10. Actual Tx/Rx bandwidth =Rate value x 32 kbps. The rate value is 1-255. High: (1)256Kbps Tx/Rx bandwidth resolution for port 1~ port 8. Actual Tx/Rx bandwidth=Rate value x 256Kbps. The rate value is 1-255. When link speed is 10MB. The rate value is 1-39. (2)the bandwidth resolution is 2048Kbps for port 9, port 10. Actual Tx/Rx bandwidth=Rate value x 2048Kbps. The rate value is 1-255. When link speed is 10MB. The rate value is 1-4. When link speed is 100MB. The rate value is 1-48.	
<input type="button" value="Update"/> <input type="button" value="LoadDefault"/>		
If the link speed of selected port is lower than the rate that you setting, this system will use the value of link speed as your setting rate.		

Figure 7-3

- **Port No.:** Select the port number you want to configure.
- **TX Rate:** Type the TX Rate value. The value is range from 0-255.
- **RX Rate:** Type the RX Rate value. The value is range from 0-255.
- **Speed Base:** Low: step by 32 Kbps. High: step by 256Kbps for Fast Ethernet Ports. 2048 Kbps for Gigabit Ports.

Click **Update** to have the configuration take effect.

Example: Type 5 for both TX and RX Rate and select the High as speed base for port 1 and port 10. The actual rate for port 1 (Fast Ethernet) is "1280", for port 9 (Gigabit Port) is 10240. You could see the table is updated as below.

Port No.	Tx Rate	Rx Rate	Link Speed	Port No.	Tx Rate	Rx Rate	Link Speed
1	1280	1280	---	6	Full Speed	Full Speed	100M
2	Full Speed	Full Speed	---	7	Full Speed	Full Speed	---
3	Full Speed	Full Speed	---	8	Full Speed	Full Speed	---
4	Full Speed	Full Speed	---	9	10240	10240	---
5	Full Speed	Full Speed	---	10	Full Speed	Full Speed	---

Figure 7-4

### Broadcast Storm Control

The switch implements a broadcast storm control mechanism. Tick the check boxes to have them beginning to drop incoming broadcast packets if the received broadcast packet counts reach the threshold defined. Each port's broadcast storm protection function can be enabled individually by ticking the check boxes.

Broadcast Storm Control										
Threshold	<input type="text" value="63"/> 1~63									
Enable Port	<input type="checkbox"/> 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"/> 9	<input type="checkbox"/> 10
<input type="button" value="Update"/>										
<small>This value indicates the number of broadcast packet which is allowed to enter each port in one time unit. One time unit is 50us for Gigabit speed, 500 us for 100Mbps speed and 5000us for 10Mbps speed</small>										
<small><b>Note:</b> This effect may be not significant for long broadcast packet, since the broadcast packet count passing through the switch in a time unit is probably less than the specified number.</small>										

Figure 7-5

The broadcast packet is only checked at the selected port and the number of broadcast packets is counted in every time unit. The one time unit indicates the number of broadcast packet which is allowed to enter each port in one time unit. The one time unit is 50us for Gigabit speed, 500 us for 100Mbps speed and 5000us for 10Mbps speed. The excessive broadcast packet will be discarded. For those broadcast packets incoming from the un-selected port, the switch treats it as the normal traffic.

- **Threshold:** Type in the threshold in the range between 1 and 63 to limit the maximum byte counts, which a port can send or receive in a period of time.
- **Enable Port:** Having ticked the boxes, the port will stop transmitting or receiving data when their sending byte counts or receiving byte counts reach the defined threshold.

#### Example to change one time unit to pps:

The port 1 is 100M port. The one time of it is 500us, it indicates there are 2,000packets can be sent within one second. While type 10 to port 1, that means 10x2000 packets can be sent in one second.

Click **Update** to have the configuration take effect.

## PoE

Users could know per PoE port out power status in this page and also enable or disable per port.

POE Configuration								
Port	1	2	3	4	5	6	7	8
Enable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Output Power	---	---	---	---	---	---	---	---
PoE Class	---	---	---	---	---	---	---	---
<input type="button" value="Update"/>								
<p><b>Update:</b> Update the power control funtion.</p> <p><b>Enable</b><input checked="" type="checkbox"/>:Power On</p> <p><b>Enable</b><input type="checkbox"/>:Power Off</p>								

Figure 7-6

- **Port:** The port number.
- **Enable:** Enable PoE feature of the specific ports.
- **Output Power:** The output power of the port.
- **PoE Class:** The PoE class of the connected port.



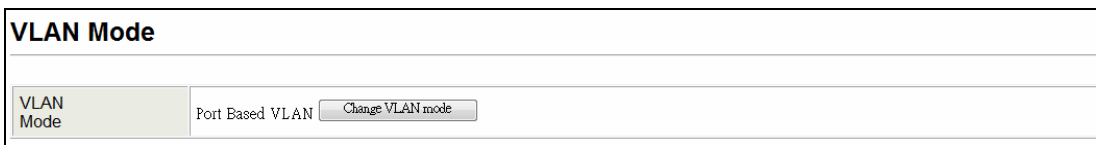
## 8. VLAN Setting

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allow you to isolate network traffic, so only the members of the same VLAN will receive traffic from the ones of the same VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

### VLAN Mode

You may select the VLAN Mode of the switch.

**Port-based VLAN** is for separating traffic only on this single switch. There is no handover of network traffic within VLAN groups to other switches. For the handover to other switches use **Tag Based VLAN**. In VLAN Mode you can switch from Tag to Port Based VLAN. Port Based VLAN is the default mode.

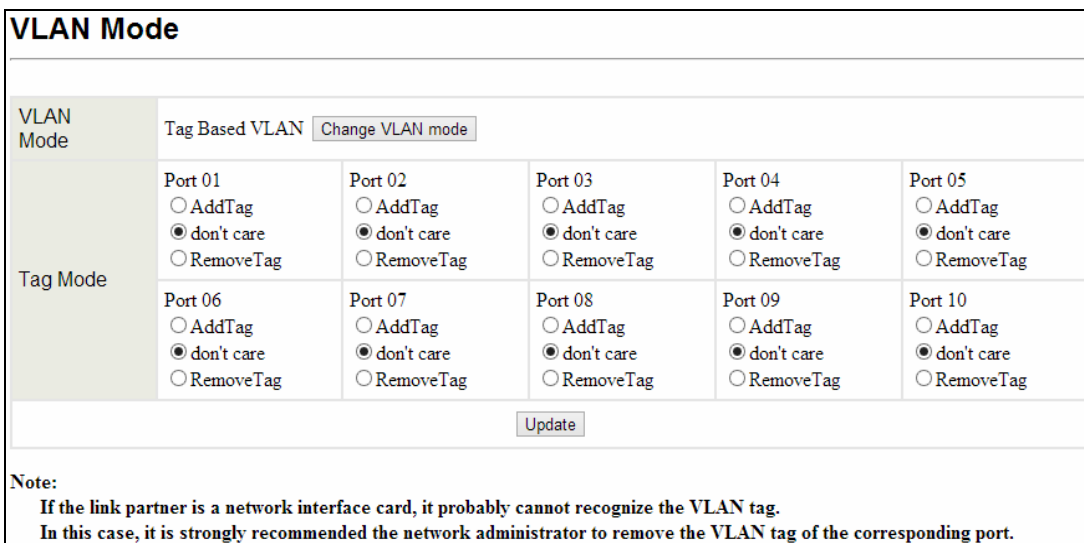


The screenshot shows a web interface titled "VLAN Mode". On the left, there is a vertical menu with "VLAN Mode" selected. The main content area shows "Port Based VLAN" selected, with a "Change VLAN mode" button next to it.

Figure 8-1

After having switched to Tag Based VLAN Mode, the screen changes. On this screen you can now define and configure your Up- and Downlink ports. These are important since here the handover between the switches of your network takes place.

### Tag Based VLAN Mode



The screenshot shows a web interface titled "VLAN Mode". On the left, there is a vertical menu with "Tag Mode" selected. The main content area shows "Tag Based VLAN" selected, with a "Change VLAN mode" button next to it. Below this, there is a table of 10 ports (Port 01 to Port 10). Each port has three radio button options: "AddTag", "don't care" (which is selected for all ports), and "RemoveTag". At the bottom of the table is an "Update" button.

VLAN Mode	Tag Based VLAN				
Tag Mode	Port 01	Port 02	Port 03	Port 04	Port 05
	<input type="radio"/> AddTag <input checked="" type="radio"/> don't care <input type="radio"/> RemoveTag	<input type="radio"/> AddTag <input checked="" type="radio"/> don't care <input type="radio"/> RemoveTag	<input type="radio"/> AddTag <input checked="" type="radio"/> don't care <input type="radio"/> RemoveTag	<input type="radio"/> AddTag <input checked="" type="radio"/> don't care <input type="radio"/> RemoveTag	<input type="radio"/> AddTag <input checked="" type="radio"/> don't care <input type="radio"/> RemoveTag
	Port 06	Port 07	Port 08	Port 09	Port 10
	<input type="radio"/> AddTag <input checked="" type="radio"/> don't care <input type="radio"/> RemoveTag	<input type="radio"/> AddTag <input checked="" type="radio"/> don't care <input type="radio"/> RemoveTag	<input type="radio"/> AddTag <input checked="" type="radio"/> don't care <input type="radio"/> RemoveTag	<input type="radio"/> AddTag <input checked="" type="radio"/> don't care <input type="radio"/> RemoveTag	<input type="radio"/> AddTag <input checked="" type="radio"/> don't care <input type="radio"/> RemoveTag

Note:  
 If the link partner is a network interface card, it probably cannot recognize the VLAN tag.  
 In this case, it is strongly recommended the network administrator to remove the VLAN tag of the corresponding port.

Figure 8-2

- **VLAN Mode:** Displays VLAN mode: port based / Tag based VLAN. Here you can also switch back to Port Based VLAN Mode.
- **Tag Mode:**
  - **Add tag** means the outgoing packet of the selected port will be inserted a 802.1Q tag. Use this setting for your Up- and Downlink Ports in your VLAN Tagged Network.
  - **Don't care** means the outgoing packet of the selected port keep the original packet received at the source port. This is the default setting when starting VLAN configuration. You should change to either Add or Remove Tag.
  - **Remove tag** means the 802.1Q tag of the outgoing packet of the selected port will be removed. Use this setting for your Network Connections to PCs. Only packets of the VLAN Group will be sent.

### VLAN Member

The ports need to be made member of your VLAN groups. This is for Tag Based and Port Based VLAN Mode. The screen here looks different whether you run Tag Based or Port Based Mode.

### VLAN Member in Port Based Mode

**VLAN Member Setting (Port Based)**

Port	02 <input type="button" value="Read"/>									
Dest PORT	01	02	03	04	05	06	07	08	09	10
select	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

VLAN MEMBER										
Port	1	2	3	4	5	6	7	8	9	10
1	v	v	v	v	-	-	-	-	-	-
2	v	v	v	v	-	-	-	-	-	-
3	v	v	v	-	-	-	-	-	-	-
4	v	v	v	v	v	v	v	v	v	v
5	v	v	v	v	v	v	v	v	v	v
6	v	v	v	v	v	v	v	v	v	v
7	v	v	v	v	v	v	v	v	v	v
8	v	v	v	v	v	v	v	v	v	v
9	v	v	v	v	v	v	v	v	v	v
10	v	v	v	v	v	v	v	v	v	v
Port	1	2	3	4	5	6	7	8	9	10

VLAN MEMBER

Figure 8-3

In Port Based Mode you see a matrix of your 8 Ports. Simply select the port on top screen you want to configure, click on **Read**, and then select or deselect the ports that are on the same VLAN group. In this configuration mode you do not need to worry about defining VLAN groups and VLAN IDs.

### VLAN Member in Tag Based Mode

In Tag Based Mode you need to define and configure your VLAN groups. Assign the VLAN ID, select the VLAN member ports, assign the PVID and check the configuration result.

**VLAN Member Setting (Tag Based)**

VID:  (1~4094)

Add: Enter a VID, select the VLAN member for this entry and then press this button to add a VLAN entry to the table.  
 Del: Select a VID in the table and then press this button to remove a VID entry from the table.  
 Update: Modify the existing VID entry, select VID and then press the button.

VLAN Member Port	01	02	03	04	05	06	07	08	09	10
select	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Note: If you do not select any port, this VID will be treated as a VID embedded in a 802.1Q tag.

VID Source port	01	02	03	04	05	06	07	08	09	10
select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Port VID Map.										
Port	01	02	03	04	05	06	07	08	09	10
VID	---	---	---	---	---	---	---	---	---	---

VLAN MEMBER										
VID \ Port	1	2	3	4	5	6	7	8	9	10

Figure 8-4

- **VLAN ID (VID):**

Since you want the handover to other switches take place smoothly, the VLAN IDs (Numbers) need to be like on the rest of your network. (On other switches you may have the chance to configure names. These are just for your reference. Only the numbers are important!)

VID:  (1~4094)

100

Add: Enter a VID, select the VLAN member for this entry and then press this button to add a VLAN entry to the table.  
 Del: Select a VID in the table and then press this button to remove a VID entry from the table.  
 Update: Modify the existing VID entry, select VID and then press the button.

Figure 8-5

- **Add:** Enter a VID, select the VLAN member for this entry and then press the **ADD** button to add a VLAN entry to the table. The available range of VID is from 1-4094.
- **Delete:** Select a VID in the table and then press the **Delete** button to remove a VID entry from the table. After deleted, the VLAN and its member port setting is gone.
- **Update:** Modify the existing VLAN setting. Select the VID, the below settings will be displayed, you can change the settings and then press the **Update** button to update the settings.

● **VLAN Member Port Select:**

Select the VLAN Member here.

VLAN Member Port	01	02	03	04	05	06	07	08	09	10
select	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Note: If you do not select any port, this VID will be treated as a VID embedded in a 802.1Q tag.

Figure 8-6

● **VID Source Port:**

This table allows you to configure PVID of the port. Select the port number while you add VLAN and select VLAN member ports, the selected ports' PVID will be the VID you typed.

---

**Note:** One port only can have one PVID. While one port joins multiple VLAN groups, the PVID is important to identify where the incoming traffic will be forwarded to.

---

**For example:** Port 3 is the member of VLAN 100 and 200, PVID of it is 100. The traffic received from the connected PC is usually untagged, the incoming packets will then be tagged with PVID within the switch and then follow the VID table to forward traffic.

VID Source port	01	02	03	04	05	06	07	08	09	10
select	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 8-7

● **Port VID Map:**

This table shows the PVID of the ports.

Port VID Map.										
Port	01	02	03	04	05	06	07	08	09	10
VID	200	200	100	100	---	---	---	---	---	---

Figure 8-8

● **VLAN Member Table:**

This table shows the VID and its member ports.

VLAN MEMBER										
VID \ Port	1	2	3	4	5	6	7	8	9	10
2	v	v	v	v	v	v	v	v	v	v
3	v	v	v	v	-	-	-	-	-	-
100	v	v	v	v	v	v	v	v	v	v
200	v	v	-	-	-	-	-	-	-	-

Figure 8-9

### Configuration Steps:

First, add your VLAN Groups (identified throughout your network by unique and constant numbers). Start with IDs from 100 and up is often. Starting with 100 gives you enough free room and less compatibility issues.

Second, enter “100” in the field right of VID Setting, and select or deselect which ports are member of that group. Your up- and downlink ports need to be the member of every existing group. If the port joins different VLAN groups, the VID Source Port allows you to define the PVID.

After configured and selected, clicking on **Add** to create the table and related port mapping. The new group with its setting will be displayed at the bottom of the screen.

### Multi to 1 Setting

Multi to 1 VLAN is used in CPE side of Ethernet-to-the-Home and is exclusive to VLAN setting on **VLAN Member Setting**. When VLAN Member Setting is updated, multi to 1 setting will be void and vice versa. The disable port means the port which will be excluded in this setting. All ports excluded in this setting are treated as the same VLAN group. In a normal Tag Based VLAN network you will not need this configuration option.

#### Multi to 1 Setting

Destination PortNo.	01 ▾																				
Current Setting	Port:-																				
Disable Port	<table style="margin: 0 auto; border-collapse: collapse;"> <tr> <td style="padding: 2px 10px;">01</td><td style="padding: 2px 10px;">02</td><td style="padding: 2px 10px;">03</td><td style="padding: 2px 10px;">04</td><td style="padding: 2px 10px;">05</td><td style="padding: 2px 10px;">06</td><td style="padding: 2px 10px;">07</td><td style="padding: 2px 10px;">08</td><td style="padding: 2px 10px;">09</td><td style="padding: 2px 10px;">10</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td><td style="text-align: center;"><input type="checkbox"/></td><td style="text-align: center;"><input type="checkbox"/></td><td style="text-align: center;"><input type="checkbox"/></td><td style="text-align: center;"><input type="checkbox"/></td><td style="text-align: center;"><input type="checkbox"/></td><td style="text-align: center;"><input type="checkbox"/></td><td style="text-align: center;"><input type="checkbox"/></td><td style="text-align: center;"><input type="checkbox"/></td><td style="text-align: center;"><input type="checkbox"/></td> </tr> </table>	01	02	03	04	05	06	07	08	09	10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
01	02	03	04	05	06	07	08	09	10												
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												

Note: "Disabled port" defines the switch physical port which is disabled.

1. A example for Multi-to-1 structure

**Destination Port/  
Current Setting**

06

→

→

⋮

→

**Ports**

01

02

⋮

08

**VLAN Groups**

1

2

⋮

2. The original setting of the VLAN Group will be cleared and replaced by this special structure if you enable this function. On the other hand, If you set the VLAN Group again, this special structure will be cleared and replaced by your newest setting.

Figure 8-10

## 9. Per Port Counter

### Port Counter

This page provides port counter of each port. There are 4 categories: Receive Packet & Transmit Packet / Transmit & Collision / Receive Packet & Drop / Receive & CRC error. Once you change the counter category, the counter will be cleared automatically.

Counter Category			
Counter Mode Selection: <span>Transmit Packet &amp; Receive Packet</span> <input type="button" value="Update"/>			
Port	Transmit Packet		Receive Packet
01	0		0
02	0		0
03	0		0
04	0		0
05	0		0
06	17687		58577
07	0		0
08	0		0
09	0		0
10	0		0

Figure 9-1

- **Transmit packet & Receive packet:** This category shows both the received packet count (excluding the incorrect packet) and the transmitted packet count.
- **Collision Count & Transmit packet:** This category shows the packets outgoing from the switch and the count of collision.
- **Drop packet & Receive packet:** This category shows the number of received valid packet and the number of dropped packet.
- **CRC packet & Receive packet:** This category shows the received correct packet and received CRC error. Once you see CRC error increasing here, notice that there may be hardware issues. The possible reasons could be port failure, cable lose/broken, cable/fiber connector failure, etc.
- **Clear:** Press **clear** will clear all counters.
- **Refresh:** Press **Refresh** button will aggregate the number of the counter for all ports.

## 10. QoS Setting

Here you can configure QoS policy priority mode and CoS (Class of Service) configuration. QoS (Quality of Service) refers to mechanisms in the network software that make the actual determination of which packets have priority. CoS refers to feature sets, or groups of services, that are assigned to users based on company policy. If a feature set includes priority transmission, and then CoS winds up being implemented in QoS functions within the routers and switches in the network. In an enterprise network, class of service (CoS) differentiates high-priority traffic from lower-priority traffic. Tags may be added to the packets to identify such classes, but they do not guarantee delivery as do quality of service (QoS) functions, which are implemented in the network devices.

### Priority Mode

There are three priority modes available to specify the priority of packets being serviced. Those include First-In-First-Out, All-High-Before-Low, and Weight-Round-Robin.

Priority Mode	
Priority Mode	
Mode	<input checked="" type="radio"/> First-In-First-Out <input type="radio"/> All-High-before-Low <input type="radio"/> Weight-Round-Robin.
	Low weight: <input type="text" value="0"/> High weight: <input type="text" value="0"/>
<input type="button" value="Update"/>	
<small>Note: When the queue weight is set to "0", it will be treated as "8".            The "low weight" and "high weight" means the ratio of the packet in the transmit queue. For example,            if "low weight" and "high weight" are set to "3" and "5", the ratio of the trasmit packet for the low priority to high priority is 3/5.</small>	

Figure 10-1

- **First-In-First-Out:** Packets are placed into the queue and serviced in the order they were received.
- **All-high-before-low (Strict priority) :** All packets will be assigned to either high priority queue (Queue 2) or low priority queue (Queue 1). The packet on the low priority queue will not be forwarded until the high priority queue is empty.
- **WRR mode:** There are 4 priority queues for Weighted-and-round-robin (WRR) mode. When this mode is selected, the traffic will be forwarded according to the number set in each queue.

### Port, 802.1p, IP / DS based

The page allows you to enable Port Based, VLAN Tag or IP/DS mode of COS.

Class of Service Configuration							
<input checked="" type="checkbox"/> =Enable High Priority							
Port No./Mode	Port Base	VLAN Tag	IP / DS	Port No./Mode	Port Base	VLAN Tag	IP / DS
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

As long as any of three COS schemes(802.1p,IP TOS/DS or Port Base) is mapped to "high", the data packet will be treated as the high priority.  
 VLAN Tag priority: high priority -> 4~7 ; low priority -> 0~3  
 IPv4 DS and IPv6 TC: high priority -> 10,18,26,34,46,48,56 ; low priority -> others

Figure 10-2

#### ● Class of Service Configuration

- **Enable High Priority:** After Enabled High Priority, the following enabled Port Based parameter will become High Priority.
- **Port Base:** The selected port equipped with High Priority. The non-selected port is Low priority. A packet received by a high priority port is handled as a high priority packet.
- **VLAN Tag:** The switch follows the VLAN tag of the incoming packets to forward traffic. VLAN Tag priority: high priority -> 4~7 ; low priority -> 0~3
- **IP/DS:** The switch follows the IP TOS / Diff Serve of the incoming packets to forward traffic. IPv4 DS and IPv6 TC: high priority -> 10,18,26,34,46,48,56 ; low priority -> others



### TCP / UDP Port Based

This page allows users to define the Option type of the pre-defined protocols or user-defined protocols. Select the Option of the Protocol as below figure shown.

Class of Service Configuration				
Protocol	Option			
FTP(20,21)	F-I-F-O ▾			
SSH(22)	F-I-F-O ▾			
TELNET(23)	F-I-F-O ▾			
SMTP(25)	F-I-F-O ▾			
DNS(53)	F-I-F-O ▾			
TFTP(69)	F-I-F-O ▾			
HTTP(80,8080)	F-I-F-O ▾			
POP3(110)	F-I-F-O ▾			
NEWS(119)	F-I-F-O ▾			
SNTP(123)	F-I-F-O ▾			
FTP(20,21)	F-I-F-O ▾			
SSH(22)	F-I-F-O ▾			
TELNET(23)	F-I-F-O ▾			
SMTP(25)	F-I-F-O ▾			
DNS(53)	F-I-F-O ▾			
TFTP(69)	F-I-F-O ▾			
HTTP(80,8080)	F-I-F-O ▾			
POP3(110)	F-I-F-O ▾			
NEWS(119)	F-I-F-O ▾			
SNTP(123)	F-I-F-O ▾			
User_Define_d	F-I-F-O ▾			
User_Define Port number (1~65535) Mask(0~255)	User_Define_a Port: <input type="text"/> Mask: 0 <input type="text"/>	User_Define_b Port: <input type="text"/> Mask: 0 <input type="text"/>	User_Define_c Port: <input type="text"/> Mask: 0 <input type="text"/>	User_Define_d Port: <input type="text"/> Mask: 0 <input type="text"/>
<p><b>Note:</b> The mask defines which bit is ignored within the IP address bit 0 ~ bit 7. For example, UDP/TCP port = 65535 and mask = 5, this means 65530, 65531, 65534 and 65535 are all taken into account. UDP/TCP port = 65535 and mask = 0, this means only 65535 is taken into account.</p> <p><b>TCP/UDP port QoS function</b> Not Override ▾</p> <p><b>Note:</b> When the "override" item is selected, the Port_based, Tag_based, IP TOS_based, CoS listed above will be ignored.</p>				
<input type="button" value="Update"/>				
<p>The Class of Service for TCP/UDP port number allows the network administrator to assign the specific application to a priority queue.</p> <p><b>F-I-F-O:</b> The incoming packet will be forwarded in first-in-first-out scheme.</p> <p><b>Discard:</b> The incoming packet will be discarded at the source port.</p> <p><b>High:</b> The incoming packet will be forwarded with the high priority.</p> <p><b>Low:</b> The incoming packet will be forwarded with the Low priority.</p>				

Figure 10-3

The Class of Service for TCP/UDP port number allows the network administrator to assign the specific application to a priority queue.

- **F-I-F-O:** The incoming packet will be forwarded in first-in-first-out scheme.
- **Discard:** The incoming packet will be discarded at the source port.
- **High:** The incoming packet will be forwarded with the high priority.
- **Low:** The incoming packet will be forwarded with the Low priority.

## 11. Security

The Security feature allows you to enable Port Security (MAC Address Binding) and TCP\_UDP Filter feature.

### MAC Address Binding

This is also known as Port Security function of some other switch. The feature allows you to bind 1-3 MAC address to one physical port. After the port and MAC address is bound, only the allowed MAC Address can access the switch.

The upper table allows you to bind the MAC address to one specific port.

**MAC Address Binding**

Port No.	MAC Address
1	<div style="display: flex; justify-content: space-between;"> <div style="width: 15%;">00</div> <div style="width: 15%;">: 11</div> <div style="width: 15%;">: 22</div> <div style="width: 15%;">: 11</div> <div style="width: 15%;">: 22</div> <div style="width: 15%;">: 33</div> </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="width: 15%; border: 1px solid #ccc; height: 15px;"></div> <div style="width: 15%;">: </div> <div style="width: 15%; border: 1px solid #ccc; height: 15px;"></div> <div style="width: 15%;">: </div> <div style="width: 15%; border: 1px solid #ccc; height: 15px;"></div> <div style="width: 15%;">: </div> <div style="width: 15%; border: 1px solid #ccc; height: 15px;"></div> </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="width: 15%; border: 1px solid #ccc; height: 15px;"></div> <div style="width: 15%;">: </div> <div style="width: 15%; border: 1px solid #ccc; height: 15px;"></div> <div style="width: 15%;">: </div> <div style="width: 15%; border: 1px solid #ccc; height: 15px;"></div> <div style="width: 15%;">: </div> <div style="width: 15%; border: 1px solid #ccc; height: 15px;"></div> </div> <div style="text-align: center; margin-top: 5px;"> <input type="button" value="Read"/> </div>
Select Port <span style="border: 1px solid #ccc; padding: 2px;">01</span> Binding <span style="border: 1px solid #ccc; padding: 2px;">Enable</span> <input type="button" value="Update"/>	

Note: If you enable the MAC address binding function, the address learning function will be disabled automatically.

Port No.	Binding Status	Port No.	Binding Status
1	Enable	6	Disable
2	Disable	7	Disable
3	Disable	8	Disable
4	Disable	9	Disable
5	Disable	10	Disable

Note: The MAC address of current management connection is 04:7d:7b:bf:af:0d at port 6.

Figure 11-1

- **Port No:** Displays the port number being assigned the MAC addresses.
- **MAC Address:** Type the target MAC address you want to bind for the specific port. User can assign up to 3 MAC addresses to the port.
- **Select Port:** Select the port number and click the **Read** button. If you have not entered any MAC Address before, the address is blank. If you have entered any MAC address, the field will display the MAC addresses you previously entered.
- **Binding:** Enable or Disable. Select **Enable** to enable the MAC Address Binding feature.

Click **Update** to have the configuration take effect.

## TCP / UDP Filter

TCP_UDP Filter Configuration							
Function Enable	Disable ▾						
Port Filtering Rule	negative ▾ Note: (1)The outgoing packet with selected protocol will be either forwarded or dropped at secure WAN port as the figure shown below. (2)"negative" means the selected protocol will be dropped and other protocols will be forwarded. "positive" means the selected protocol will be forwarded and other protocol will be dropped.						
Protocol	<input type="checkbox"/> FTP(20,21)	<input type="checkbox"/> SSH(22)	<input type="checkbox"/> TELNET(23)	<input type="checkbox"/> SMTP(25)	<input type="checkbox"/> DNS (53)	<input type="checkbox"/> TFTP(69)	<input type="checkbox"/> HTTP(80)
	<input type="checkbox"/> SNTIP(123)	<input type="checkbox"/> NetBIOS (137~139)	<input type="checkbox"/> IMAP (143,220)	<input type="checkbox"/> SNMP (161,162)	<input type="checkbox"/> HTTPS (443)	<input type="checkbox"/> XRD_RDP (3389)	<input type="checkbox"/> BOOTP (67,68)
	<input type="checkbox"/> User_Define_a	<input type="checkbox"/> User_Define_b	<input type="checkbox"/> User_Define_c	<input type="checkbox"/> User_Define_d			
Secure WAN port	<input type="checkbox"/> Port01	<input type="checkbox"/> Port02	<input type="checkbox"/> Port03	<input type="checkbox"/> Port04	<input type="checkbox"/> Port05	<input type="checkbox"/> Port06	<input type="checkbox"/> Port07
	<input type="checkbox"/> Port10						

Figure 11-2

- **Function Enable:** To Enable or Disable the function.
- **Port Filtering Rule:** The outgoing packet with selected protocol will be either forwarded or dropped at secure WAN port as the figure shown below.
  - **"negative"** means the selected protocol will be dropped and other protocols will be forwarded.
  - **"positive"** means the selected protocol will be forwarded and other protocol will be dropped.
- **Protocol:** Select the pre-defined known protocol or User\_Define Protocol number.
- **Secure WAN Port:** The port number of the Secured WAN Port. The secured WAN port is the Egress Port. The configured limit packet will be dropped.

## 12. Spanning Tree

The switch supports IEEE 802.1D-2004 STP protocol, the RSTP protocol can backward compatible to legacy Spanning Tree Protocol (STP) and 802.1w Rapid Spanning Tree Protocol (RSTP).

### STP Bridge Settings

#### STP Bridge Settings

Spanning Tree Settings				
STP Mode	Bridge Priority	Hello Time	Max Age	Forward Delay
	(0-61440)	(1-10 Sec)	(6-40 Sec)	(4-30 Sec)
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Submit"/>				
Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$ $\text{Max Age} \geq 2 * (\text{Hello Time} + 1)$ Bridge Priority must be multiples of 4096				

Note: If you enable the MAC address binding function, the address learning function will be disabled automatically. Then both RSTP/STP and address learning will be affected.

Bridge Status				
STP Mode	Bridge ID	Hello Time	Max Age	Forward Delay
RSTP	32768:00 0F C9 05 BB 57	2	20	15

Root Status			
Root ID	Hello Time	Max Age	Forward Delay
I'm the root bridge!	2	20	15

Figure 12-1

- **STP Mode:** Disable, STP and RSTP. Select the STP version you want to enable.
- **Bridge Priority:** This parameter configures the spanning tree priority globally for this switch. The device with the highest priority becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Number between 0 - 61440 in increments of 4096. Therefore, there are 8 distinct values.
- **Hello Time:** Interval (in seconds) at which the root device transmits a configuration message (BPDU frame). Number between 1-10 (default is 2).
- **Max Age:** The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. That also means the maximum life time for a BPDU frame. Number between 6-40 (default is 20).
- **Forward Delay:** The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). Number between 4 – 30 (default is 15)

## STP Port Settings

The STP Port Setting page allows you to change the port priority and its path cost. After STP/RSTP is enabled, the system automatically assigns the port priority and path cost to the port. Normally, it is necessary to change the parameters, however, you may need to control the root switch or block port in some condition.

This page allows you to change the STP port setting. Select the port number, type the value of the Priority and Root Path Cost. Click "**Submit**" to apply the settings.

### STP Port Settings

STP Port Settings						
Port No.	Priority (0~240)	RPC (1~200000000) 0=AUTO				
<input type="text"/>	<input type="text"/>	<input type="text"/>				
<input type="button" value="Submit"/>						
Priority should be a multiple of 16						

STP Port Status						
Port No.	RPC	Priority	State	Status	Designated Bridge	Designated Port
1	0	0x80	--	Disable	--	--
2	0	0x80	--	Disable	--	--
3	Auto:0	0x80	--	Disable	--	--
4	Auto:0	0x80	--	Disable	--	--
5	Auto:0	0x80	--	Disable	--	--
6	Auto:200000	0x80	Designated Port	Forwarding	--	--
7	Auto:0	0x80	--	Disable	--	--
8	Auto:0	0x80	--	Disable	--	--
9	Auto:0	0x80	--	Disable	--	--
10	Auto:0	0x80	--	Disable	--	--

Figure 12-2

- **Port No:** The port ID. It cannot be changed. Aggregations mean any configured trunk group.
- **Root Path Cost:** This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Set the RSTP path cost on the port. Number between 0 - 200000000. 0 means auto generated path cost.
- **State:** Show the current port state includes designated port, root port or blocked port.
- **Status:** Show the current port status includes forwarding, disable etc...

### Loopback Detection Settings

In some condition, the users may incorrectly connect the wrong cable and lead the port loop. The Loopback Detection feature can help you leave the risk.

#### Loopback Detection Settings

<b>Loopback Detect Function</b>	Disable ▾
<b>Auto Wake Up</b>	Disable ▾
<b>Wake-Up Time Interval</b>	10 sec ▾
<input type="button" value="Submit"/>	

Port No.	Status
1	--
2	--
3	--
4	--
5	--
6	--
7	--
8	--
G1	--
G2	--

Figure 12-3

- **Loopback Detection Function:** This column allows you to enable or disable Loopback Detection function.
- **Auto Wake Up:** Once the Loopback Detection function is running, the ports maybe be disabled to avoid the loop. The **Auto Wake Up** allows you to activate the port after Time Interval passed.
- **Wake-Up Time Interval:** Select the time interval here.

Click **Submit** to apply the settings.

## 13. Trunking

Port trunk allows multiple links to be bundled together and act as a single physical link for increased throughput. It provides load balancing, and redundancy of links in a switched inter-network. Actually, the link does not have an inherent total bandwidth equal to the sum of its component physical links.

Traffic in a trunk is distributed across an individual link within the trunk in a deterministic method that called a hash algorithm. The hash algorithm automatically applies load balancing to the ports in the trunk. A port failure within the trunk group causes the network traffic to be directed to the remaining ports. Load balancing is maintained whenever a link in a trunk is lost or returned to service. This switch may use Port ID, Source MAC Address, Destination MAC Address, or a combination of Source MAC Address and Destination MAC Address to be the selection for Trunk Hash Algorithm.

Traffic pattern on the network should be considered carefully before applying it. When a proper hash algorithm is used, traffic is kind of randomly decided to be transmitted across either link within the trunk and load balancing will be seen.

This switch supports one trunk group, port 9 and Port 10. Trunk hash algorithm support Source MAC, Source & Destination MAC Address.

### Trunking

<b>System Priority</b>	1	(1~65535)
<b>Link Aggregation Algorithm</b>	MAC Src&Dst ▼	
<input type="button" value="Submit"/>		

	Link Group	
<b>Member</b>	p9	P10
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	--	--
<b>State</b>	Enable ▼	
<b>Type</b>	Static ▼	
<b>Operation Key</b>	Static LACP (65535)	
<b>Time Out</b>	Long Time Out ▼	
<b>Activity</b>	Passive ▼	
<input type="button" value="Submit"/>		

Note: If you enable LACP on some specified ports and their link partners are normal port without LACP, these specified ports cannot transmit packet to receive packet from the link partner.

Figure 13-1

- **System Priority:** This column allows you to configure the system priority for LACP. Set a value between 1 and 65535. The default value is 1. The higher the number, the lower the priority. The system priority controls which links between LACP partner switches are active and determines the standby status of the links for each LACP port channel.
- **Link Aggregation Algorithm:**
  - **MAC Src:** Hash Algorithm based on Source MAC Address.
  - **MAC Src&Dst:** Hash Algorithm based on Source & Destination MAC Address XOR result.
- **Member:** This column allows you to select the member Ports.
- **Status:** This column allows you to Enable/Disable the Trunk Group.
- **Type:** This column allows you to choose **Static** Trunking or Dynamic **LACP** Trunking. After selecting the **LACP** Trunk type, the following parameters can be configured. Note that the parameters of the both ends of the LACP should be the same.
- **Operation Key:** This column allows you to type operation key. The selected ports in a manual / static aggregation group and the member ports in a dynamic aggregation group have the same operation key.
- **Time Out:** This column allows you to select **Long Time Out** Time or **Short Time Out** Time. The Long Time Out is around 30 seconds. The Short Time Out is around 3 seconds. However, the link partner of other supplier may not use the same value. The longer time then will be used.
- **Activity:** This column allows you to select **Passive** or **Active** mode.

---

**Note:** If you enable LACP on some specified ports and their link partners are normal port without LACP, these specified ports cannot transmit packet to/receive packet from the link partner.

---



## 14. Backup / Recovery

This function provides the users with a method to backup / recovery the switch configuration. The users can save configuration file to a specified file. If the users want to recover the original configuration, which is saved at the specified path, just enter the password and then press the **upload** button. Finally the original configuration of the switch will be recovered.

### Configuration Backup/Recovery

#### Backup(Switch→PC)

Please check "Download" to download EEPROM contents.

#### Recovery(PC→Switch)

Select the image file :

Password:

Figure 14-1

## 15. Miscellaneous

Miscellaneous setting is used to configure output queue aging time, VLAN stride and IGMP snooping.

Miscellaneous Setting				
<b>Output Queue Aging Time</b>				
Aging time <input type="button" value="Disable"/> ms	The output queue aging function allows the administrator to select the aging time of a packet stored in the output queue. A packet stored in the output queue for a long time will lower the free packet buffer, resulting in the poor utilization of the buffer and the poor switch performance.			
<b>VLAN Striding</b>				
VLAN Striding <input type="button" value="Disable"/>	When this function is enabled, the switch will forward a uni-cast packet to the destination port. No matter whether the destination port is in the same VLAN group.			
<b>IGMP Snooping V1 &amp; V2</b>				
IGMP Snooping <input type="button" value="Disable"/>	IGMP Snooping V1 & V2 function enable			
IGMP Leave Packet <input type="button" value="Disable"/>	Leave packet will be forwarded to IGMP router ports.			
<b>VLAN Uplink Setting</b>				
Port 01 <input type="radio"/> Uplink1 <input type="radio"/> Uplink2	Port 02 <input type="radio"/> Uplink1 <input type="radio"/> Uplink2	Port 03 <input type="radio"/> Uplink1 <input type="radio"/> Uplink2	Port 04 <input type="radio"/> Uplink1 <input type="radio"/> Uplink2	Port 05 <input type="radio"/> Uplink1 <input type="radio"/> Uplink2
Port 06 <input type="radio"/> Uplink1 <input type="radio"/> Uplink2	Port 07 <input type="radio"/> Uplink1 <input type="radio"/> Uplink2	Port 08 <input type="radio"/> Uplink1 <input type="radio"/> Uplink2	Port 09 <input type="radio"/> Uplink1 <input type="radio"/> Uplink2	Port 10 <input type="radio"/> Uplink1 <input type="radio"/> Uplink2
<input type="radio"/> Clear Uplink1 <input type="radio"/> Clear Uplink2				
<input type="button" value="Update"/>				

Figure 15-1

- **Output Queue Aging Time:**
  - **Purpose:** This function is used to avoid the traffic jam on one port will not cause the congestion of other ports. In some application, for example the IPTV Multicast communication, the multicast stream is continuously generating from the source port, the client port may be congested because of the limited bandwidth or slow network processing ability. Then, the Pause frame of Flow Control will be generated once the packet buffer is full. With the Output Queue Aging Time feature, when a packet is stored at output queue in a switch for a long time will be aged out and become a useless packet.
  - **Aging Time:** This command allows users to disable the feature or configure the aging timeout time to 200ms, 400ms, 600ms or 800ms.

- **VLAN Striding:**
  - **Purpose:** For some network environment, the network administrator probably wants to filter undesired broadcast or multicast packet to enhance the network bandwidth utilization and forward meaningful unicast to a specific destination. VLAN is a good mechanism to block broadcast packet, but it can also block the unicast packet communication between VLANs. To solve this issue, a special function called “VLAN striding” is designed to achieve this purpose. If VLAN striding is enabled, the packet will be forwarded to the destination port directly. The unicast packet can stride across VLAN.
  - **VLAN Striding:** By selecting this function, the switch will forward unicast packets to the destination port, no matter whether destination port is in the same VLAN.
  
- **IGMP Snooping V1 & V2:**
  - **Purpose:** A switch will, by default, flood multicast traffic to all ports in a broadcast domain. Multicast can cause unnecessary load on host devices by requiring them to process packets they have not solicited. The IGMP snooping is a feature that allows the switch to listen in on the IGMP conversation between hosts and routers. By listening (also known as snooping) to these conversations, the switch maintains a map of which ports (clients) need which multicast stream (source). Multicast may be filtered which do not need them, Multicast may be forwarded only to the IGMP group it joined.
  - **IGMP Snooping:** When this function is enabled, the switch will execute IGMP snooping version 1 and version 2 without the intervention of CPU. The IGMP report and leave packets are automatically handled by the switch. The next setting, IGMP Leave Packet can be enabled or disabled. After enabled, the Leave packet will be forwarded to IGMP router ports.
  
- **VLAN Uplink:**
  - **Purpose:** This switch does not implement Independent VLAN (IVL) MAC address table. It utilizes VLAN uplink to emulate the function of IVL. An independent VLAN MAC address table is based on both the source MAC address and the VLAN. In some application, if the Ethernet switch cannot build the separate MAC address table for different VLANs, there will be a conflict of MAC address table. To solve this problem, the switch controller utilizes the VLAN Uplink port to emulate the usage of Independent VLAN MAC Address Table.

- **VLAN Uplink Setting:** If VLAN uplink function is enabled and the destination port of an unicast packet is located at the next VLAN, this packet will be forwarded to the uplink port. Choose the Uplink Port X for the port ID. The Uplink X will be the uplink port of its VLAN.

---

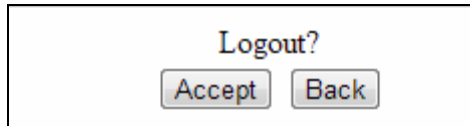
**Note:** There is a functional conflict between VLAN striding and VLAN uplink. When both functions are enabled simultaneously, the switch will select VLAN striding and ignore the VLAN uplink setting.

---

## 16. Logout

The administrator has write access for all parameters governing the onboard agent. Users should therefore assign a new administrator password as soon as possible, and store it in a safe place.

After finished configuring the switch, you can click **Logout** to leave the configuration page.



*Figure 16-1*

## 17. Restoring Default Settings

Follow the steps below to restore the switch to its default settings using the **Reset** button on the front panel of the switch.

---

**Note:** After restoring default settings, you will need to configure IP address, ID and Password again. To remain the set IP address, ID and Password, you can restore default settings using the web interface.

---

1. Turn on the switch.
2. Press and hold the **Reset** button for 5 seconds until all the LED start blinking.
3. Release the button. The switch is restored to its default settings.

## 18. Specifications

Ports		
Number of Ports	10 ports 8-port Fast Ethernet 10/100BaseTX, IEEE 802.3at PSE 2-port Gigabit Uplink (1*TP, 1*SFP)	
Performance		
MAC Address	4 K	
Buffer Memory	2.75 M bits	
Transmission Method	Store and Forward	
Transmission Media	10BaseT Cat. 3, 4, 5 UTP/STP 100BaseTX Cat. 5 UTP/STP 1000BaseT Cat. 5/5E, 6 UTP/STP	
Filtering/Forwarding Rates	10 Mbps port - 14,880 pps 100 Mbps port - 148,800 pps 1000 Mbps port - 1,488,000 pps	
Smart Features		
Port Based VLAN	10	
Tagged Based VLAN	32, VID = 1~4094	
IGMP Snooping	V1 & V2	
Link Aggregation	1, Gigabit ports	
Quality of Service (QoS)	High & Low priority queues, 802.1p	
Security	Port & MAC binding, 3 MAC per port	
Port Management	Port State, Speed/Duplex, Flow Control Configuration, Port Mirroring, Bandwidth Control, Broadcast Storm Control, PoE	
Administrator Management	Web Management, Password Protection, Configuration Backup/Restore, Firmware Upgrade	
Mechanical Characteristics		
LED Indicators	Per Port: Link/Act PoE Act/Status Power	
Electrical Characteristics		
PoE Power	Input	100 ~ 240 V/AC, 50 ~ 60 Hz
	Output	IEEE 802.3at Compliant Voltage, Per Port Max. 30 watts (8 Ports at Full 15.4 W / 4 Ports at Full 30 W)
Max. Power Consumption	130 W	
General		
Dimensions (H x W x D)	44 x 266 x 160 mm (1.73" x 10.47" x 6.3")	
Weight	1.8 kg (3.97 lb)	
Operating Temperature	0°C ~ 45°C (32°F ~ 113°F)	
Storage Temperature	-20°C ~ 90°C (-4°F ~ 194°F)	
Humidity	10 to 90% RH (non-condensing)	
Standards and Regulatory		
Standards	IEEE 802.3 10BaseT IEEE 802.3u 100BaseTX IEEE 802.ab 1000BaseT IEEE 802.3z 1000BaseSX/LX IEEE 802.3x Flow Control IEEE 802.3ad Link Aggregation Control Protocol IEEE 802.1Q VLAN IEEE 802.1p Class of Service IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.3at Power Over Ethernet (PoE+)	
Regulatory	CE, FCC Class A	

**Note:** Specifications are subject to change without prior notice.