cortex

User's Manual

SW-10200

PoE+ Switch 802.3at

8 x 10/100 PoE +802.3at plus 2 Gigabit Combo Ports RJ45/SFP

Rev. 141022

Trademarks

Disclaimer

i3 International does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. i3 International has made every effort to ensure that this User's Manual is accurate; i3 International disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of i3 International. i3 International assumes no responsibility for any inaccuracies that may be contained in this User's Manual. i3 International makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

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 when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the Instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at whose own expense.

CE Mark Warning

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

Energy Saving Note of the Device

This power required device does not support Standby mode operation.
For energy saving, remove the power cable to disconnect the device from the power circuit.
Without removing power cable, the device will still consume power from the power source. In the view of Saving the Energy and reduce the unnecessary power consuming, it is strongly suggested to remove the power connection for the device if this device is not intended to be active.

WEEE Warning

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

i3 International 8 x 10/100 PoE+ 802.3at plus 2 Gigabit Combo Ports RJ45/SFP Switch
Web Smart Switch User’s Manual
FOR MODELS: SW-10200
REVISION: 1.4.2

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Product Overview

This switch provides 8 10/100 Mbps PoE ports, 8 10/100BASE-TX ports that support the IEEE 802.3at PoE protocol, and includes auto MDI/MDIX crossover detection function providing an excellent choice in network flexibility. Each port transmits up to 30 watts, fully configurable from a convenient web UI. With this added PoE feature, this switch is an ideal solution for building wireless, IP surveillance, and VoIP networks.

It also provides a port-based and 802.1Q tag VLAN function to provide better traffic management, reduce latency, improve security and save bandwidth without the need to add additional hardware to the network.

1.1.1. Product Features

Web Management

- **Port Management**
  - Port Configuration Port Mirroring Bandwidth Control
  - Broadcast Storm Control
  - PoE On/Off Setting

- **VLAN Setting**
  - Port-based/ Tag-based
  - VLAN ID: 1~4094

- **Trunking**
  - 2 groups (1~4 port for each group)

- **QoS Setting**
  - Priority Mode
  - Class of Service Configuration
  - TCP/UDP Port-based

- **Trunking**
  - Link Aggregation Setting

- **Security Setting**
  - MAC address filtering
  - TCP/UDP Port filtering

- **STP/RSTP**

- **Spanning Tree Protocol**

- **Backup Recovery Configuration**

Specifications

- **Standard**
  - IEEE 802.3 10BaseT IEEE 802.3u 100BaseTX IEEE 802.ab 1000BaseT
  - IEEE 802.3z 1000BaseSX/LX
  - IEEE 802.3x Full-duplex and Flow Control
  - IEEE 802.at PoE+
  - IEEE 802.3ad Link Aggregation
  - IEEE 802.1d Spanning tree protocol
  - IEEE 802.1w Rapid Spanning tree protocol
  - IEEE 802.1Q VLAN
  - IEEE 802.1p Class of Service

- **Number of Ports**
  - 8-port 10/100BaseTX with PoE+ (Full power)
  - +2 Combo Gigabit RJ45/SFP Open Slots (SFP Slots can not be equipped with 100Mbps SFP Modules)

Mechanical

- **LED Indicator**
  - Per Port: Link/ Act PoE
  - Port: Act/Status Per Unit: Power

- **Power Consumption**
  - 260 Watts (Max)

- **Power Input**
  - 100~240V/AC, 50~60Hz

- **Power Output**
  - 48V/DC per Port Output – 30W Max per Port

- **Product Dimensions/ Weight**
  - 266 × 260 × 44 mm (L × W ×H) / 2.5kg

Performance

- **MAC Address**
  - 4K
- **Buffer Memory**
  - 2.75Mb
- **Transmission Method**
  - Store and Forward

2. INSTALLATION

2.1. Hardware Installation

2.1.1. Package Contents

Prior to installing this switch, verify that your package that contains the following items:

- One PoE Switch
- One Power Cord
- One User Manual CD
- One Rack-mount kit + 8 Screws

If any of these are missing or damaged, please contact your dealer immediately, if possible, retain the carton including the original packing material, and use them again to repack the product in case there is a need to return it for repair.

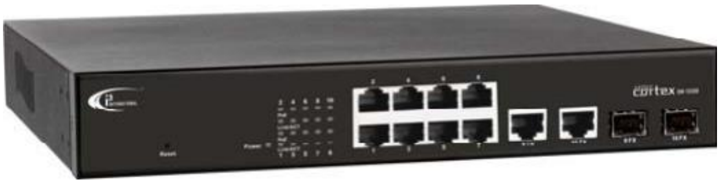


Figure 1 - SW-10200 switch

2.2. Hardware Description

This section describes the hardware features and installation of the 8 PoE port + 2-port Gigabit Ethernet Combo Web Managed Switch. For easier management and control, familiarize yourself with its display indicators and ports. Read this chapter completely before connecting any network device to it.

Physical Dimensions/ Weight

266 × 260 × 44 mm (L × W ×H) / 2.5kg

Front Panel

The front Panel of the Web Managed Switch consists of 8 10/100Base-TX RJ-45 ports (Auto MDI/MDIX) ＋ 2 gigabit RJ45/SFP open slot. The LED indicators are also located on the front panel.

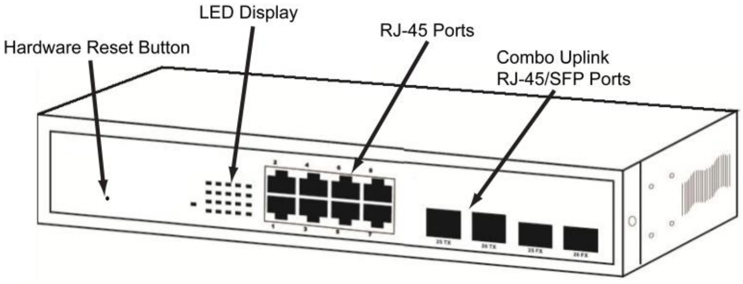


Figure 2 - Front panel overview

LED Indicators

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

LED	Status	Description
Power	On	Power switch is on
	Off	Power is off
Port	On	Link transmission at 10/100 Mbps
	Blinking	Networking is active
	Off	No device attached
PoE	On	Port is linked to powered device
	Off	No Powered device connected

Table 1 - LED status descriptions

Rear Panel

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

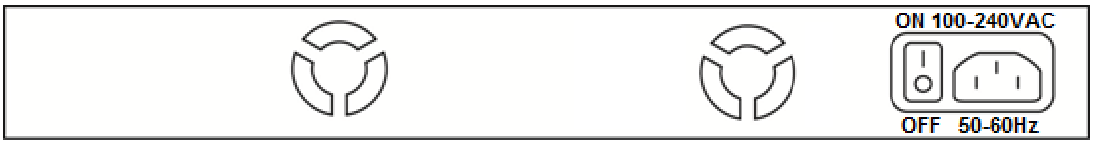


Figure 3 - Rear panel overview

Hardware Installation

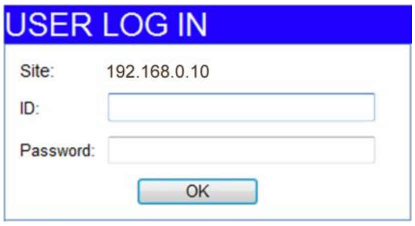
Set the switch on a large flat space with a power socket close by. The flat space should be clean, smooth, level and sturdy. Make sure there is enough clearance around the switch to allow attachment of cables, power cord and allow air circulation. Use twisted pair cable to connect this switch to your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

3. SOFTWARE CONFIGURATION

This section describes the software configuration of the SW-10200 switch using the Web Interface.

3.1. Logging In

Open a web browser, and enter the address ***192.168.0.10*** *(for switches with the F/W version V141015 or newer) or* ***192.0.0.20*** *(for switches with the F/W version V110613 or older).* A login screen will appear.



USER LOG IN

Site: 192.168.0.10

ID:

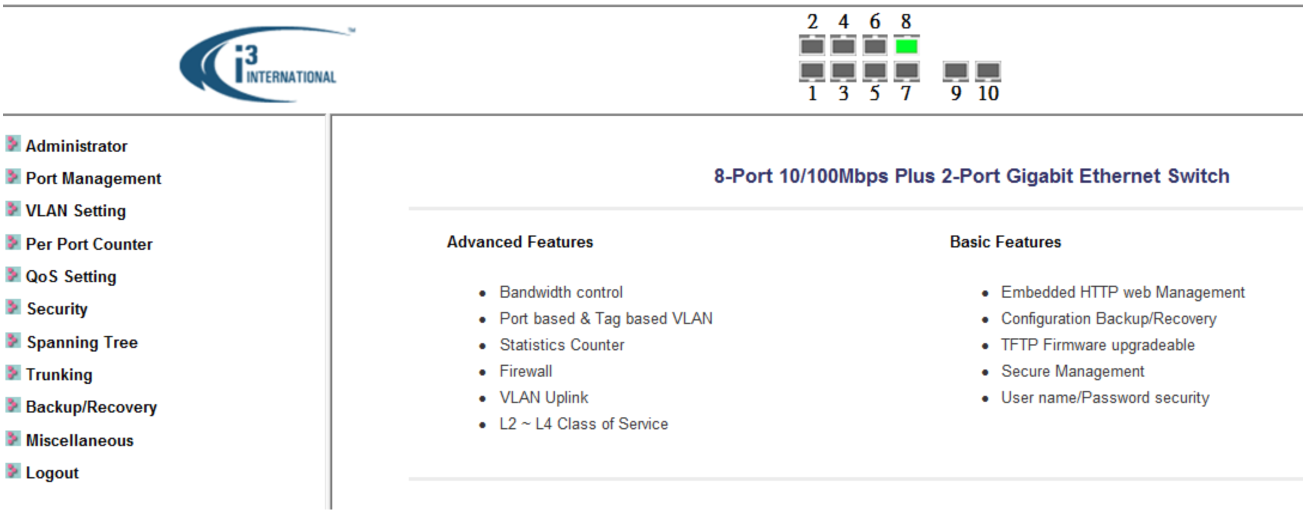
Password:

Figure 4 - Login screen

The factory default password and login for switches with the F/W version v141015 or newer: Username: **i3admin**; Password: **i3admin**

The factory default password and login for switches with the F/W version V110613 or older: Username: **admin**; Password: **admin**

On authentication, *“Password successfully entered”* will appear and you will be taken to the main page, as shown below.



8-Port 10/100Mbps Plus 2-Port Gigabit Ethernet Switch

Advanced Features

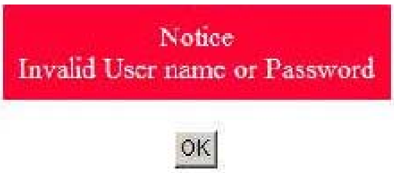
- Bandwidth control
- Port based & Tag based VLAN
- Statistics Counter
- Firewall
- VLAN Uplink
- L2 ~ L4 Class of Service

Basic Features

- Embedded HTTP web Management
- Configuration Backup/Recovery
- TFTP Firmware upgradeable
- Secure Management
- User name/Password security

Figure 5 – Web interface main page

If not, this message will appear.



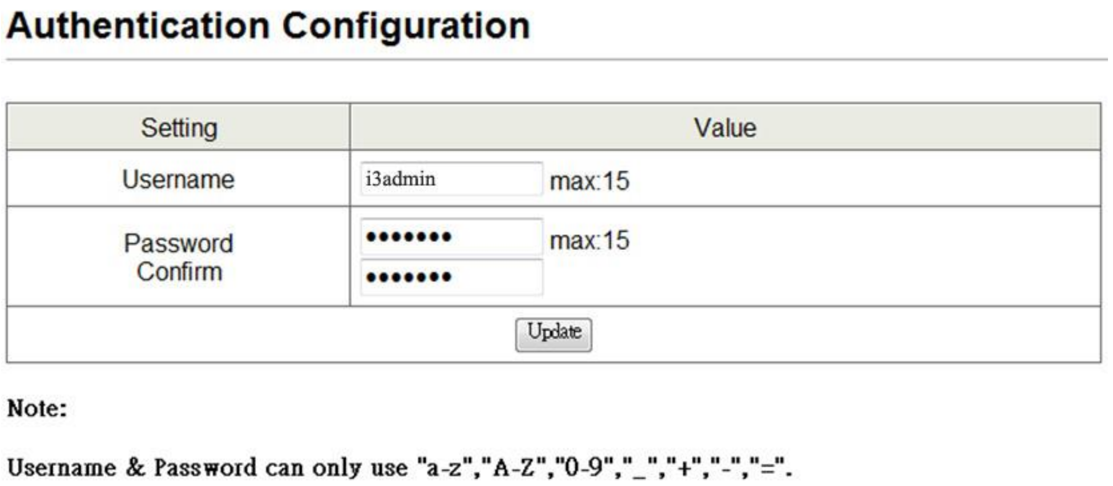
Notice
Invalid User name or Password

Figure 6 - Login error

3.2. Administration

3.2.1. Authentication Configuration

Clicking on **Administrator** in the navigation pane will bring up administrative options on the main pane. If this is your first login, change the username and password in the Authentication Configuration section.



Authentication Configuration

Setting	Value
Username	i3admin max:15
Password Confirm	••••••• max:15 •••••••
	Update

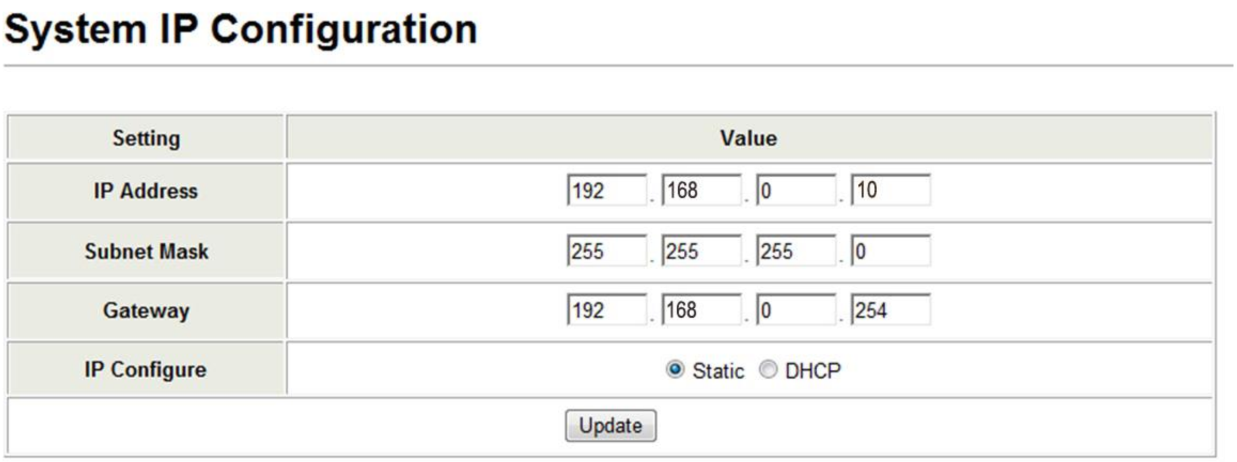
Note:

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

Figure 7 - Set the username and password

3.2.2. System IP Configuration

This page sets information on the system configuration including the current IP address, subnet mask and gateway.



System IP Configuration

Setting	Value
IP Address	192 . 168 . 0 . 10
Subnet Mask	255 . 255 . 255 . 0
Gateway	192 . 168 . 0 . 254
IP Configure	● Static ○ DHCP
	Update

Figure 8 - Configure the switch IP

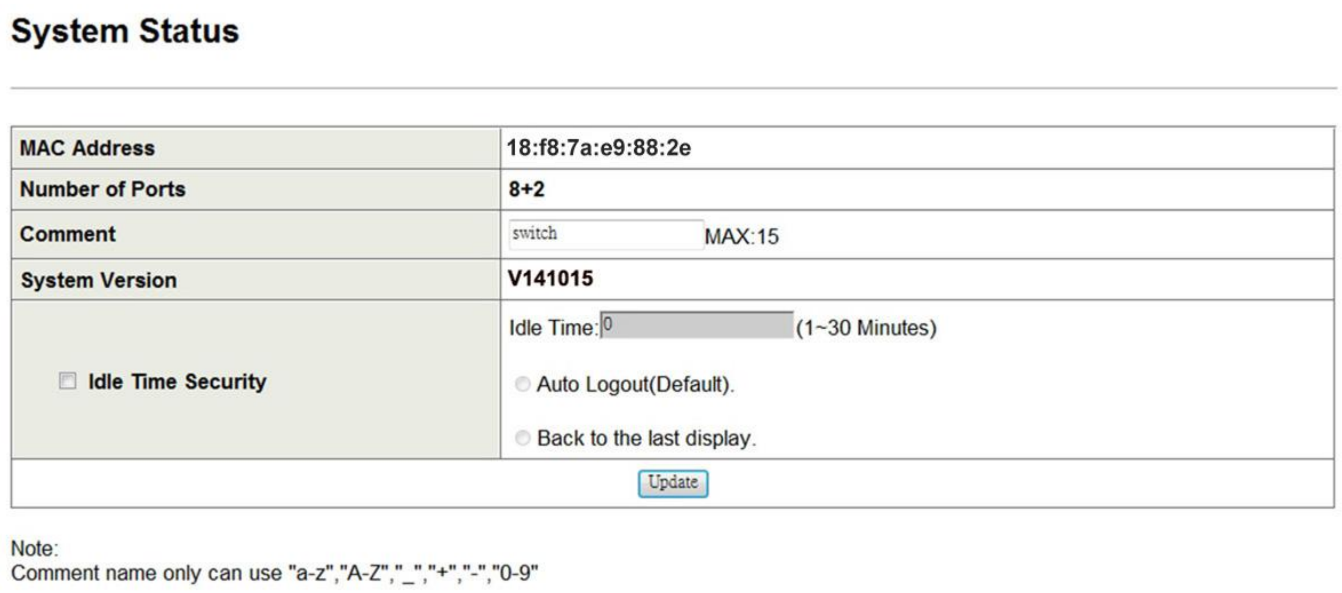
Parameters are as follows:

- IP address: Manually assign the IP address of the switch. The default IP Address is: ***192.168.0.10*** *(for switches with the F/W version V141015 or newer) or* ***192.0.0.20*** *(for switches with the F/W version V110613 or older).*
- Subnet Mask: Assign the subnet mask to the IP address.
- Gateway: Assign the network gateway. Default gateway is: ***192.168.0.254*** *(for switches with the F/W version V141015 or newer) or* ***192.0.0.254*** *(for switches with the F/W version V110613 or older).*
- IP Configure: Choose between Static or DHCP network IP assignment.

Click **Update** to save your changes. Note: Changing the IP address will require a reboot.

3.2.3. System Status

This page displays basic information about the switch.



System Status

MAC Address	18:f8:7a:e9:88:2e
Number of Ports	8+2
Comment	switch MAX:15
System Version	V141015
□ Idle Time Security	Idle Time: 0 (1~30 Minutes) ○ Auto Logout(Default). ○ Back to the last display.
Update	

Note:
Comment name only can use "a-z","A-Z","_","+","-","0-9"

Figure 9 - An overview of the switch

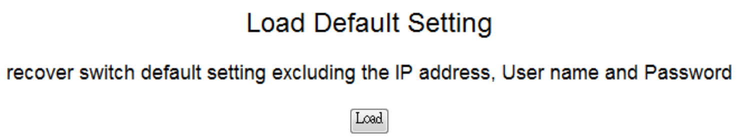
- MAC Address: Displays the unique hardware address assigned by manufacturer (default).
- Number of Ports: Displays number of ports in the switch.
- Comment: This field may be used for notes. A maximum of fifteen characters is allowed.
- System Version: Displays the switch’s firmware version.
- Idle Time Security: When the web interface has been idle for an amount of time, the software will auto logout or back to the last display. Set an **Idle Time** in the corresponding field. Click **Auto Logout (Default)** to shut down the switch when the interface has been idle for the duration specified. Click **Back to the last display** to revert the web interface back to the last screen when the interface has been idle for the duration specified.

Click **Update** to save your changes

3.3. Factory Settings

3.3.1. Software Reset

Clicking the **Load** button will revert the switch to its original factory configurations with the exception of the user name, password and IP configuration.



Load Default Setting

recover switch default setting excluding the IP address, User name and Password

Load

Figure 10 - Click to reset factory defaults

If a factory reset of the user name, password and IP configuration settings is desired, press the hard (physical) reset button on the switch.

3.3.2. Hardware Reset

Press the physical reset button on the switch to revert to its original factory configurations including settings which are not covered by the software reset.

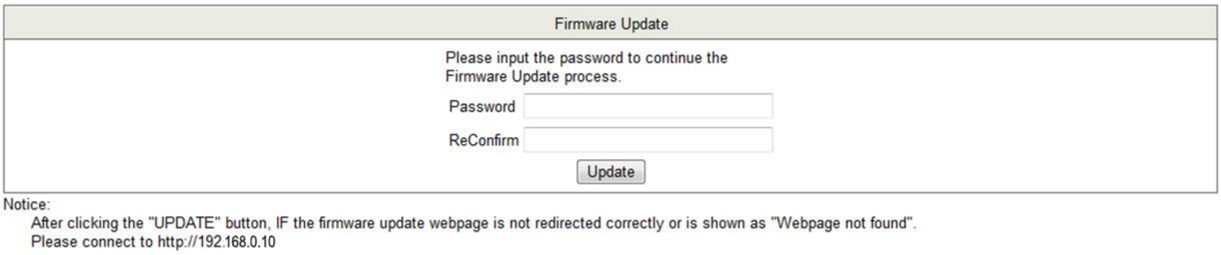
(1) To activate, press the factory reset button for 5 seconds until the LED begins to blink.

(2) The blinking LED signals that the CPU is executing the reset procedure. Release the button.

After completing this procedure, all the factory settings will be restored including the IP address, the user name, the password as well as all other switch configurations.

3.4. Firmware Update

Before updating the switch firmware, it is recommended that flash memory on the switch be erased. The Boot Loader will be kept intact by a self-protection mechanism which ensures correct functioning even in the event of power loss or network failure during the update.



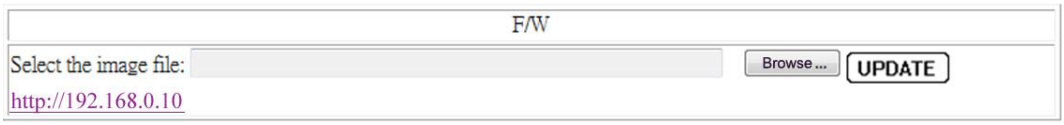
Firmware Update

Please input the password to continue the Firmware Update process.

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://192.168.0.10

Figure 11 - Confirm the firmware update

Enter your password and confirm it in the appropriate fields. Click **Update**. This screen will appear.



F/W

Figure 12 - Select an update file

Click **Browse...** to select the new firmware image and Click **Update** to save your changes.

3.5. Logging out

At any time, click the **Logout** link on the navigation pane to log out of the web interface.

4. PORT MANAGEMENT

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

4.1. Port Configuration

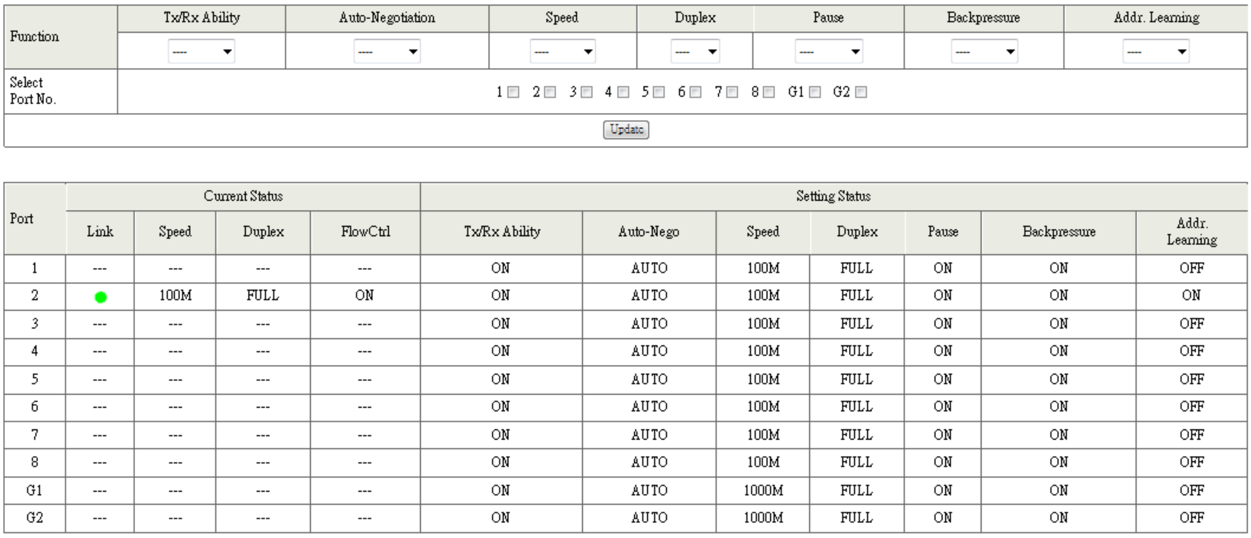
To access port configuration options, click on the link ***Port Configuration*** in the navigation pane of the web interface.

4.1.1 Auto-negotiation

Auto-negotiation automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detecting the modes and speeds both connected devices are capable of. Both 10Base-T and 100Base-TX devices can connect with the port in either Half- or Full-Duplex mode.

If attached device is:	**100Base-TX port will set to:**
10Mbps, no auto-negotiation	10Mbps.
10Mbps, with auto-negotiation	10/20Mbps (10Base-T/Full-Duplex)
100Mbps, no auto-negotiation	100Mbps
100Mbps, with auto-negotiation	100/200Mbps (100Base-TX/Full-Duplex)

Table 2 - Auto-negotiation summary



Function	Tx/Rx Ability	Auto-Negotiation	Speed	Duplex	Pause	Backpressure	Addr. Learning
	----	----	----	----	----	----	----

Select Port No. 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ G1 □ G2 □

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	OFF
2	●	100M	FULL	ON	ON	AUTO	100M	FULL	ON	ON	ON
3	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
4	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
5	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
6	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
7	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
8	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
G1	---	---	---	---	ON	AUTO	1000M	FULL	ON	ON	OFF
G2	---	---	---	---	ON	AUTO	1000M	FULL	ON	ON	OFF

Figure 13 - Configure auto-negotiation settings

In Port Configuration, you can set and view the operation mode for each port. Check the checkbox next to the port number to view or change its current configuration.

- Select Port No.: Check the check boxes beside the port numbers being set.

Configure the ports using the drop-down lists at the top. The parameters are:

- TX/RX Capability: When Auto-Negotiation is disabled, users must manually ***Enable*** or ***Disable*** TX/RX.
- Auto-Negotiation: Select ***Enable*** or ***Disable***. If enabled the Speed, Duplex mode, Pause, Backpressure, TX Capability and Address Learning are negotiated automatically. If disabled, these parameters must be assigned manually.
- Speed: When Auto-Negotiation is disabled, the speed must be manually specified.
- Duplex: When Auto-Negotiation is disabled, the connection mode, either Half or Full must be specified.
- Pause: Flow Control for the connection at a speed of 10/100Mbps in Full-duplex mode.
- Backpressure: Flow Control for the connection at a speed of 10/100Mbps in Half-duplex mode.
- Addr. Learning: When Auto-Negotiation is disabled, users must manually ***Enable*** or ***Disable*** Address

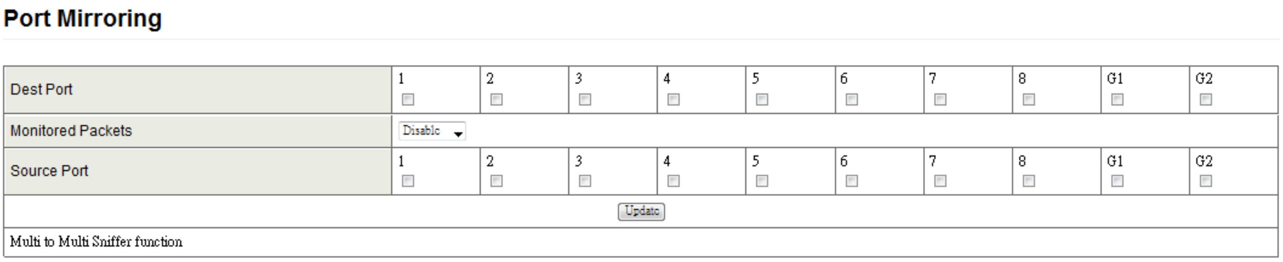
Learning.

Click **Update** to save your changes. A table at the bottom of the main pane displays a summary of each port’s configuration. The display shows the following information:

- Current Status: Displays current port status.
- Setting Status: Displays current status.

4.2. Port Mirroring

Configure port Mirroring on this page. This function monitors network traffic that forwards a copy of each incoming or outgoing packet from one port of a network switch to another port where the packet can be studied. It enables the manager to keep close track of switch performance and alter it if necessary.



Port Mirroring

Dest Port	1 □	2 □	3 □	4 □	5 □	6 □	7 □	8 □	G1 □	G2 □
Monitored Packets	Disable ▾									
Source Port	1 □	2 □	3 □	4 □	5 □	6 □	7 □	8 □	G1 □	G2 □
Update										
Multi to Multi Sniffer function										

Figure 14 - Configure port mirroring

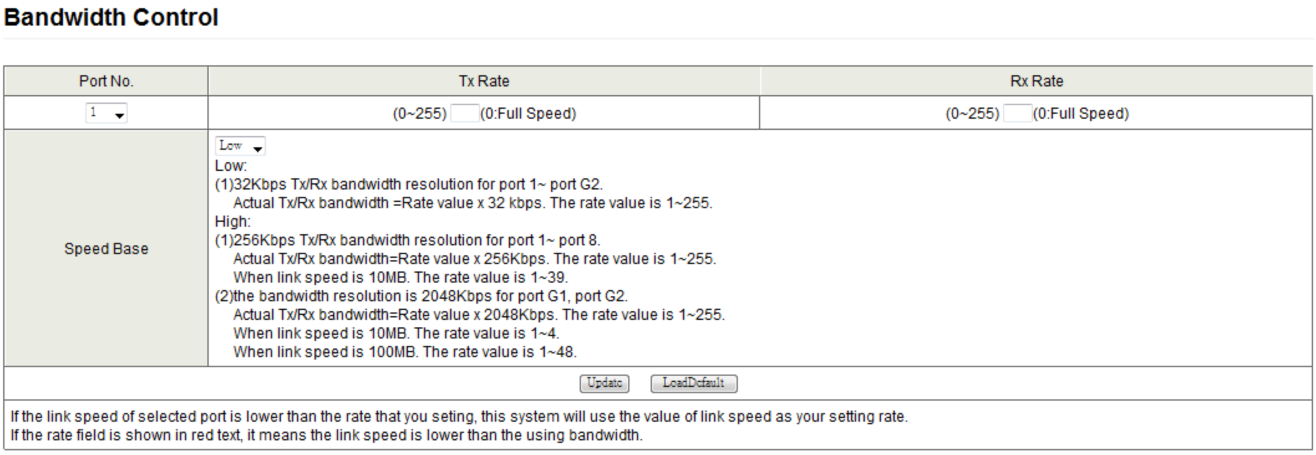
The parameters for this setting are:

- Destination (mirroring) port: For monitoring RX only, TX only or both RX and TX traffic from the source port. Mirroring ports can be connected to LAN analyzer or Netxray.
- Monitored Packets: Expand the drop-down menu to select between RX, TX or both RX and TX.
- Source Port: Select ports to monitor. All monitored port traffic will be copied to the mirroring (destination) port. Select multiple source ports by ticking the check boxes beneath the port number label to be monitored.

Click **Update** to save your changes

4.3. Bandwidth Control

Configure the allowed bandwidth on this page. The TX rate and Rx rate is given in a number ranging from ***1*** to ***255***. This number should be multiplied by the selected bandwidth resolution to get the actual bandwidth.

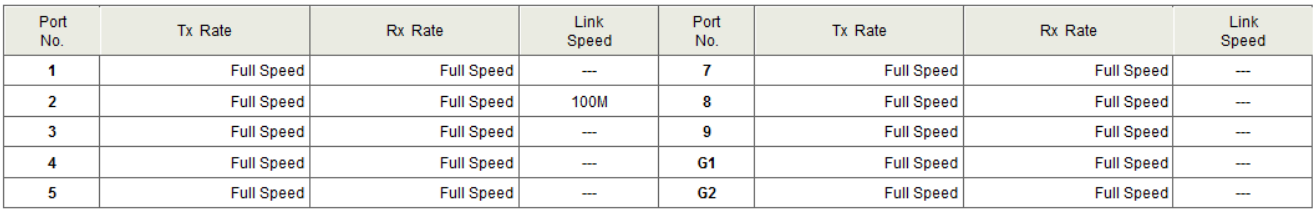


Bandwidth Control

Port No.	Tx Rate	Rx Rate
1 ▾	(0~255) ☐ (0:Full Speed)	(0~255) ☐ (0:Full Speed)
Speed Base	Low ▾ Low: (1)32Kbps Tx/Rx bandwidth resolution for port 1~ port G2. 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 G1, port G2. 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.	
Update LoadDefault		
If the link speed of selected port is lower than the rate that you seting, this system will use the value of link speed as your setting rate. If the rate field is shown in red text, it means the link speed is lower than the using bandwidth.		

Figure 15 - Set allowed bandwidth

A bandwidth usage summary is seen below.

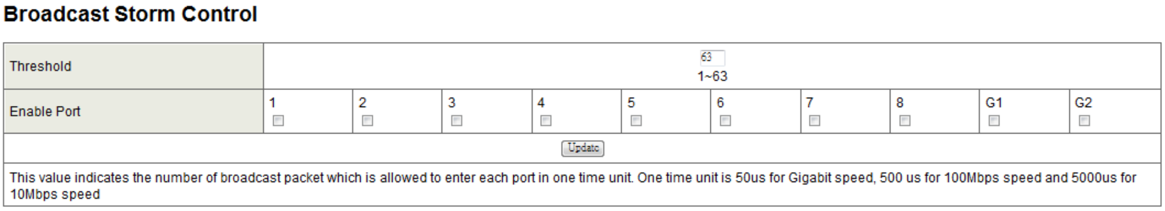


Port No.	Tx Rate	Rx Rate	Link Speed	Port No.	Tx Rate	Rx Rate	Link Speed
1	Full Speed	Full Speed	---	7	Full Speed	Full Speed	---
2	Full Speed	Full Speed	100M	8	Full Speed	Full Speed	---
3	Full Speed	Full Speed	---	9	Full Speed	Full Speed	---
4	Full Speed	Full Speed	---	G1	Full Speed	Full Speed	---
5	Full Speed	Full Speed	---	G2	Full Speed	Full Speed	---

Figure 16 - Bandwidth summary

4.3.1. Broadcast Storm Control

The switch implements a broadcast storm control mechanism. Check the ports next to **Enable Port** to select ports that will drop incoming broadcast packets if the number of received broadcast packets reaches the threshold defined. Each port's broadcast storm protection function can be enabled individually.



Broadcast Storm Control

Threshold	63 1~63									
Enable Port	1 □	2 □	3 □	4 □	5 □	6 □	7 □	8 □	G1 □	G2 □

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

Figure 17 - Configure broadcast storm control

Broadcast packets are only checked at selected ports. Timing is set to 500 us for 10Mbps speed and 5ms for 100Mbps. Excess broadcast packets will be discarded. Packets for un-selected ports are treated as normal traffic.

- Threshold: Type in a threshold between ***1*** and ***63*** to limit the maximum byte counts which a port can send or receive during a period of time.
- Enable Port: Checked ports will stop transmitting or receiving data when their thresholds given in Threshold are reached. Unchecked ports will function normally.

Click **Update** to save your changes.

4.4. PoE Settings

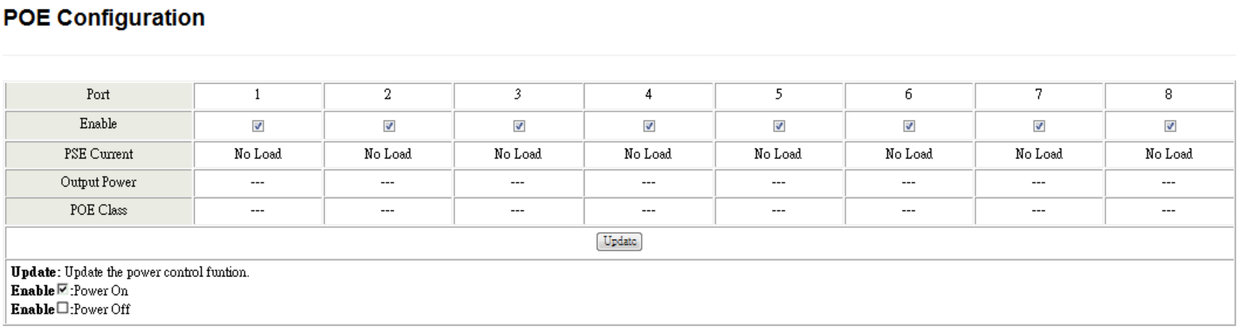
Various PoE settings can be set here. For more information about PoE, read the Appendix section "*PoE Provisioning Process*."

4.4.1. PoE Introduction

Based on the global standard IEEE 802.3af, PoE is a technology for wired Ethernet. PoE allows the electrical power necessary for the operation of each end-device (IP Cameras, VoIP phones, etc) to be carried by data cables rather than by separate power cords. Such a network configuration helps enterprises improve productivity by minimizing the number of wires that must be used to install the network, thus incurring lower cost, and less power failures. In the case of surveillance technology, IP cameras and access systems may be installed throughout a facility without incurring costs associated with hiring an electrician.

Providing up to 24 PoE, in-line power interface, the switch can easily build a power central-controlled IP phone system, IP Camera system or AP group for the enterprise. For instance, 24 camera / AP can be easily installed around the corner in the company for surveillance demands or build a wireless roaming environment in the office. Without the power-socket limitation, the PoE Switch makes the installation of cameras or WLAN AP easy and efficient.

This page displays PoE information about a port's PSE, Minimum Output and PoE Class. Check **Enable** to use the port for PoE.



POE Configuration

Port	1	2	3	4	5	6	7	8
Enable	☑	☑	☑	☑	☑	☑	☑	☑
PSE Current	No Load	No Load	No Load	No Load	No Load	No Load	No Load	No Load
Output Power	---	---	---	---	---	---	---	---
POE Class	---	---	---	---	---	---	---	---

Update: Update the power control funtion.
Enable☑ :Power On
Enable□ :Power Off

Figure 18 - Configure PoE

5. VLAN SETTING

5.1. Introduction to VLAN

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical location. VLAN can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLAN also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

Note

No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.

5.1.1. IEEE 802.1Q Standard

IEEE 802.1Q (tagged) VLAN is implemented on the Switch. 802.1Q VLAN require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLANs allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to IEEE 802.1Q enabled switches that are members of that VLAN, including broadcast, multicast and unicast packets from unknown sources.

VLAN can also provide a level of security to your network. IEEE 802.1Q VLAN will only deliver packets between stations that are members of the VLAN. Any port can be configured as either tagging or untagging.

- The untagging feature of IEEE 802.1Q VLAN allows a VLAN to work with legacy switches not recognizing VLAN tags in packet headers.
- The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled and working normally on all ports.

Some relevant terms:

- Tagging: The act of putting 802.1Q VLAN information into the packet header.
- Untagging: The act of stripping 802.1Q VLAN information out of the packet header.

802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the Ether Type field. When a packet's Ether Type field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLAN can be identified.

The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

The Ether Type and VLAN ID are inserted after the MAC source address, but before the original Ether Type/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

Port VLAN ID

Tagged packets (carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with VLAN information intact. This allows 802.1Q VLANs to span network devices or even the entire network provided that all network devices are 802.1Q compliant.

All physical ports on a switch have a PVID. 802.1Q ports are also assigned a PVID for use within the switch. If no VLANs are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Any untagged packet is assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID in so far as VLAN are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the VID is used to make packet forwarding decisions, rather than the PVID.

Tag-aware switches must keep a table to relate PVID within the switch to a network VID. The switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VIDs are different the switch, the packet is dropped. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices are allowed to coexist on the same network.

A switch port can have only one PVID, but can have as many VIDs as the switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted. If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Untagged VLANs

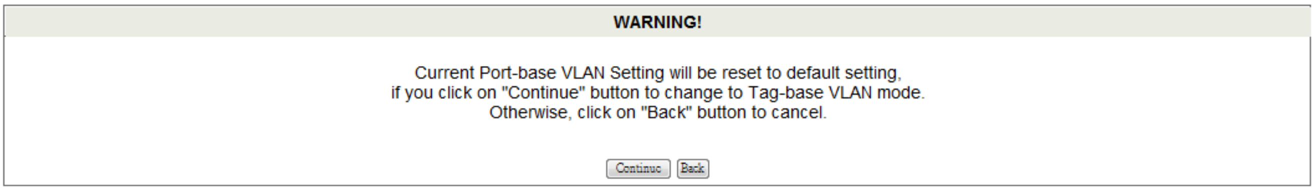
Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets.

5.2. VLAN Configuration

To access VLAN options, click on the link ***VLAN Configuration*** in the navigation pane of the web interface.

5.2.1. VLAN Mode

You may select the VLAN Mode of the switch. Port-based VLAN groups traffic onto a 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. Click **Change VLAN mode** to change the VLAN mode to Tag Based VLAN. This message may appear.

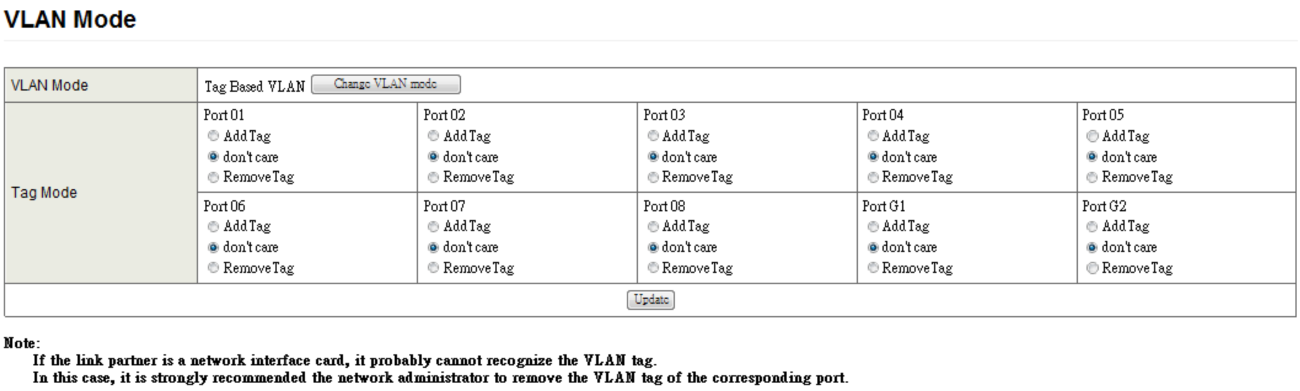


WARNING!

Current Port-base VLAN Setting will be reset to default setting,
if you click on "Continue" button to change to Tag-base VLAN mode.
Otherwise, click on "Back" button to cancel.

Figure 19 - Changing VLAN modes causes default VLAN settings to be loaded

Click **Continue** to confirm and to edit settings. The next screen will appear.



VLAN Mode

VLAN Mode	Tag Based VLAN [Change VLAN mode]				
Tag Mode	Port 01 ○ Add Tag ● don't care ○ Remove Tag	Port 02 ○ Add Tag ● don't care ○ Remove Tag	Port 03 ○ Add Tag ● don't care ○ Remove Tag	Port 04 ○ Add Tag ● don't care ○ Remove Tag	Port 05 ○ Add Tag ● don't care ○ Remove Tag
	Port 06 ○ Add Tag ● don't care ○ Remove Tag	Port 07 ○ Add Tag ● don't care ○ Remove Tag	Port 08 ○ Add Tag ● don't care ○ Remove Tag	Port G1 ○ Add Tag ● don't care ○ Remove Tag	Port G2 ○ Add Tag ● don't care ○ Remove Tag

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 20 - Select options for VLAN

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.

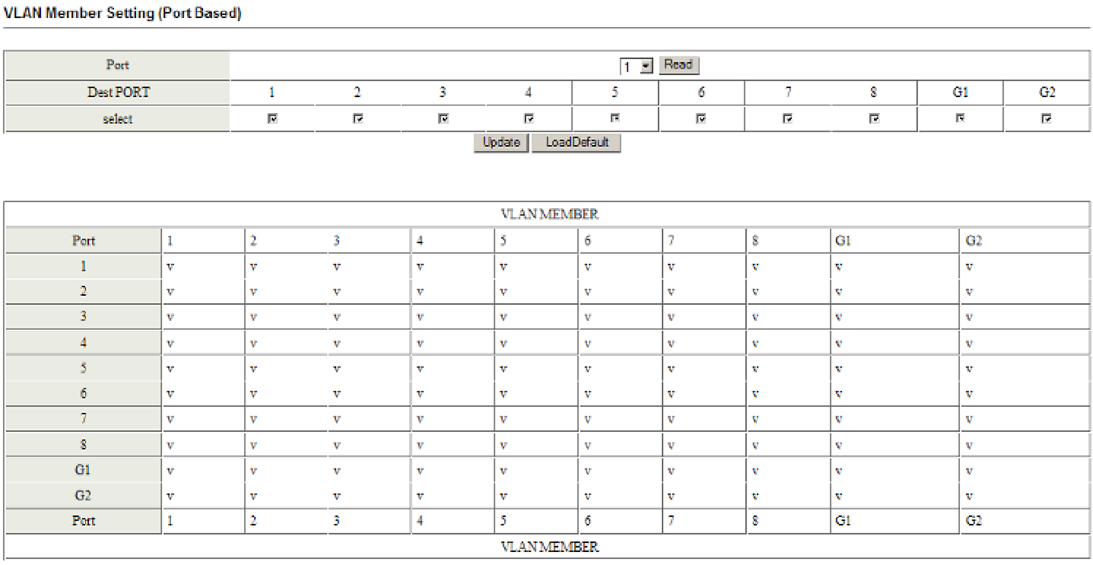
- VLAN Mode: Displays VLAN mode: port based/Tag based VLAN. Here you can also switch back to Port Based VLAN Mode
  - **Add tag** means the outgoing packet of the selected port will be inserted a 802.1Q tag. Use this setting for your Up- and Downlink Ports in your VLAN Tagged Network.
  - **Don’t care** 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. It is recommended that the option be changed to **Add** or **Remove Tag**.
  - **Remove tag** means the 802.1Q tag of the outgoing packet of the selected port will not be sent. Use this setting for your Network Connections to PCs. Only packets of the VLAN Group the Port is member of will be sent.

5.2.2. VLAN Member

The ports need to be made member of your VLAN groups. This is for Tag Based and Port Based VLAN Mode. The options available on this screen will depend on whether VLAN is running in Tag Based or Port Based Mode.

VLAN Member in Port Based Mode

In Port Based Mode you see a matrix of your 8+2 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 Setting (Port Based)

Port	1 [Read]									
Dest PORT	1	2	3	4	5	6	7	8	G1	G2
select	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

VLAN MEMBER

Port	1	2	3	4	5	6	7	8	G1	G2
1	v	v	v	v	v	v	v	v	v	v
2	v	v	v	v	v	v	v	v	v	v
3	v	v	v	v	v	v	v	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
G1	v	v	v	v	v	v	v	v	v	v
G2	v	v	v	v	v	v	v	v	v	v
Port	1	2	3	4	5	6	7	8	G1	G2

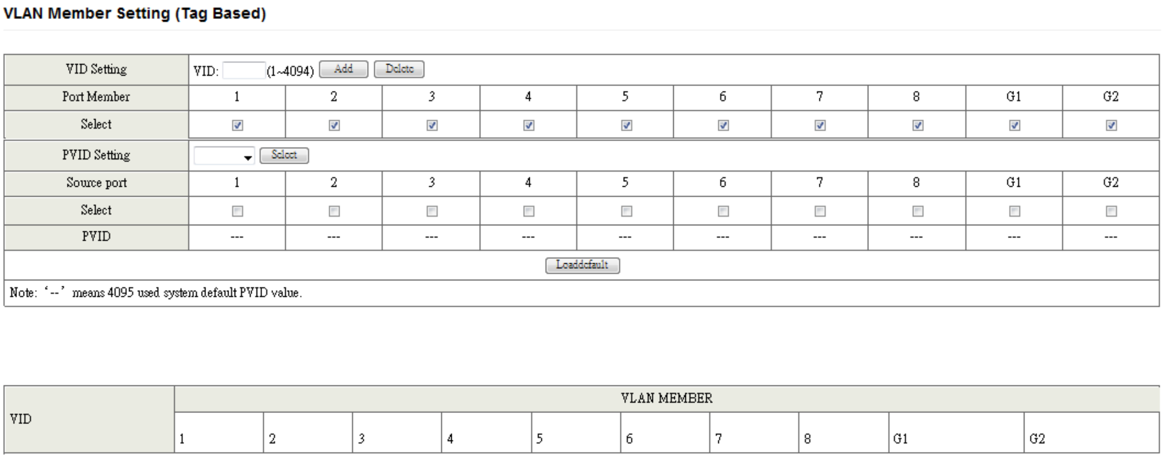
VLAN MEMBER

Figure 21 –Group ports for port-based VLAN mode

VLAN Member in Tag Based Mode

In Tag Based Mode you need to define and configure your VLAN groups. To ensure smooth handover, the VLAN IDs (Numbers) need to be like on the rest of your network.

Add VLAN Groups (identified throughout your network by unique and constant numbers). Start with IDs from 100 and up. Keep in mind that some switches use “*1*” as the default, while others use “*4095*” or “*4096*” as default. Starting with 100 gives you enough free room and less compatibility issues.



VLAN Member Setting (Tag Based)

VID Setting	VID: (1~4094) Add Delete									
Port Member	1	2	3	4	5	6	7	8	G1	G2
Select	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
PVID Setting	Select									
Source port	1	2	3	4	5	6	7	8	G1	G2
Select	□	□	□	□	□	□	□	□	□	□
PVID	---	---	---	---	---	---	---	---	---	---

Loaddefault

Note: ‘--’ means 4095 used system default PVID value.

VID	VLAN MEMBER									
	1	2	3	4	5	6	7	8	G1	G2

Figure 22 – Group ports for Tag Based VLAN mode

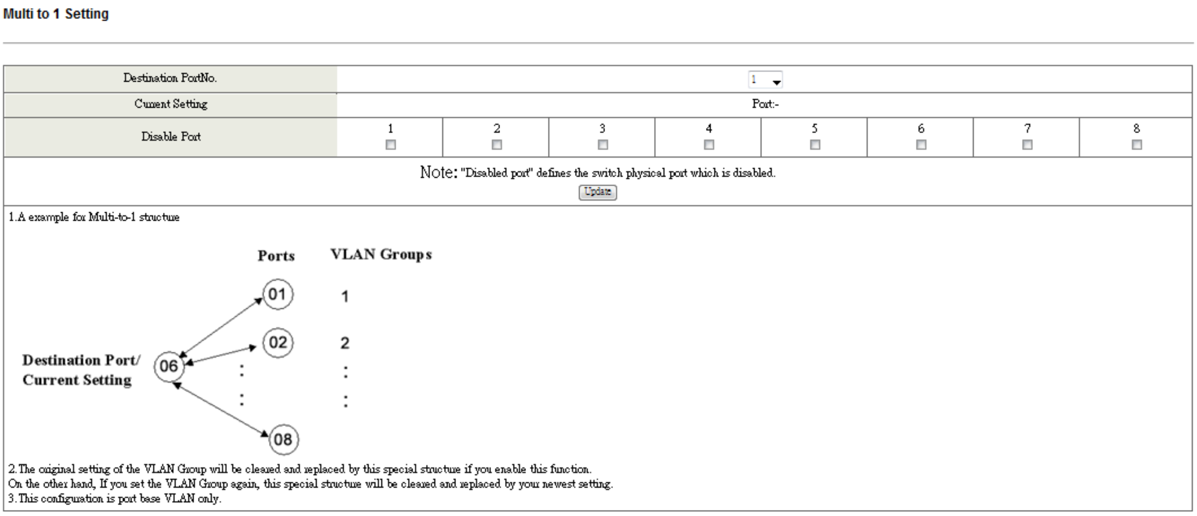
Enter ***100*** in the field right of VID Setting, then select or deselect which ports are member of that group. Bear in mind that the up- and downlink ports need to contain members of every existing group. When the ports are assigned, click **Add**. The new group with its setting will be displayed at the bottom of the screen.

With the PVID Setting, define to which VLAN group incoming traffic belongs. For example, port 1 is a member of group 100 and 101. A simple PC is connected to Port 1. If that PC is now sending out data, with PVID you define if that data is for group 100 or 101.

A summary of VLANs and their members is given in the VLAN Member table.

5.3. Multi to 1 Setting

Multi to 1 VLAN is used in the CPE side of Ethernet-to-the-Home. When VLAN member Settings is updated, multi to 1 setting will be negated. Disabling the port excludes it from this action. All ports excluded in this setting are treated as the same VLAN group. In a normal Tag Based VLAN network this configuration option is not necessary.



Multi to 1 Setting

Destination PortNo.	1							
Cuurent Setting	Port:-							
Disable Port	1 □	2 □	3 □	4 □	5 □	6 □	7 □	8 □

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

Update

1.A example for Multi-to-1 structure

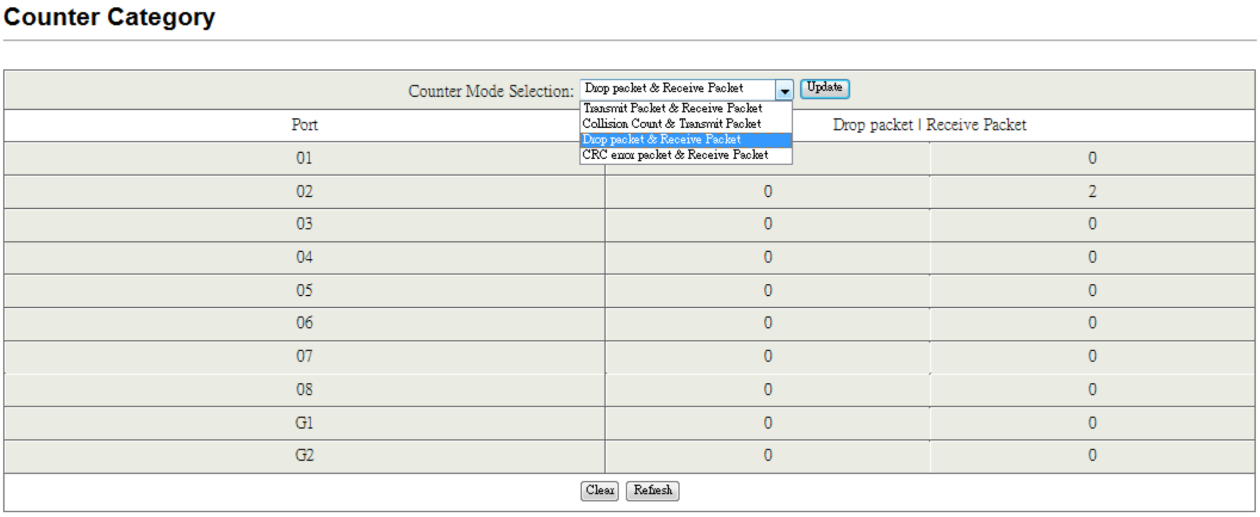
2.The original setting of the VLAN Group will be cleared and replaced by this special structure if you enable this function.
On the other hand, If you set the VLAN Group again, this special structure will be cleared and replaced by your newest setting.
3.This configuration is port base VLAN only.

Figure 23 - Set multi-to-1 in Port-Based VLAN to forward traffic to a port

6. PER PORT COUNTER

6.1. Port Counter

To access port statistics, click on the link ***Port Counter*** in the navigation pane of the web interface. This page provides statistics on each port. Figures are grouped into four categories: ***Receive Packet & Transmit Packet***/ ***Transmit & Collision*** / ***Receive Packet & Drop*** /***Receive & CRC error***. Select the category in the **Counter Mode Selection** drop-down list. Once you change the counter category, the counter will be cleared automatically.


Transmit Packet & Receive Packet
Collision Count & Transmit Packet
Drop packet & Receive Packet
CRC error packet & Receive Packet
Update
Clear
Refresh

Counter Category

Counter Mode Selection: Drop packet & Receive Packet

Port	Drop packet | Receive Packet	
01		0
02	0	2
03	0	0
04	0	0
05	0	0
06	0	0
07	0	0
08	0	0
G1	0	0
G2	0	0

Figure 24 - View statistics for each switch port on this screen

- Transmit packet & Receive packet: Both the received packet count (excluding incorrect packets) and the transmitted packet count.
- Collision Count & Transmit packet: The packets outgoing from the switch and collisions.
- Drop packet & Receive packet: The number of received valid packet and the number of dropped packets.
- CRC packet & Receive packet: Received correct packets and Received CRC errors.

Clicking **Clear** will clear all counters. Clicking **Refresh** will update counters for all ports.

7. QoS SETTING

7.1. About QoS

Here you can configure QoS policy priority mode and CoS (Class of Service) configuration. Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic. 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, 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.

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want the switch to treat selected applications and types of traffic.

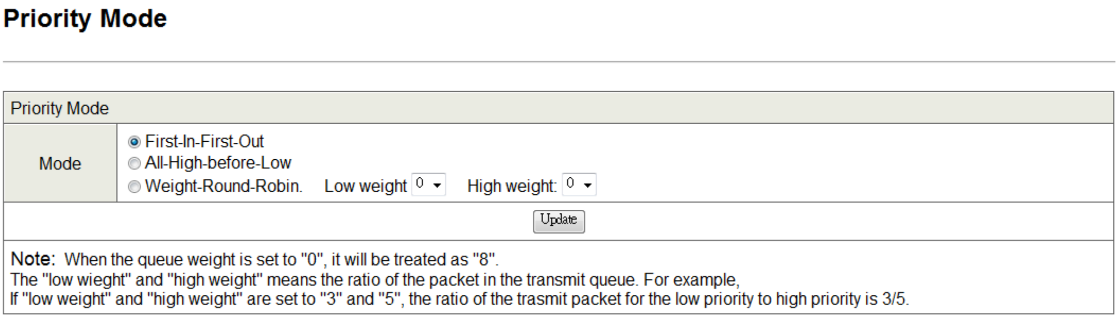
You can use QoS on your system to control a wide variety of network traffic by:

- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Provide predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage network congestion.

7.2. Configuring QoS

To access QoS configuration options, click on the link ***QoS Settings*** in the navigation pane of the web interface.

7.2.1. Priority Mode



Priority Mode

Priority Mode	
Mode	● First-In-First-Out ○ All-High-before-Low ○ Weight-Round-Robin. Low weight 0 ▾ High weight: 0 ▾

Update

Note: When the queue weight is set to "0", it will be treated as "8".
The "low wieght" 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.

Figure 25 - Specify packet priority

There are three priority modes available to specify the priority of packets being serviced:

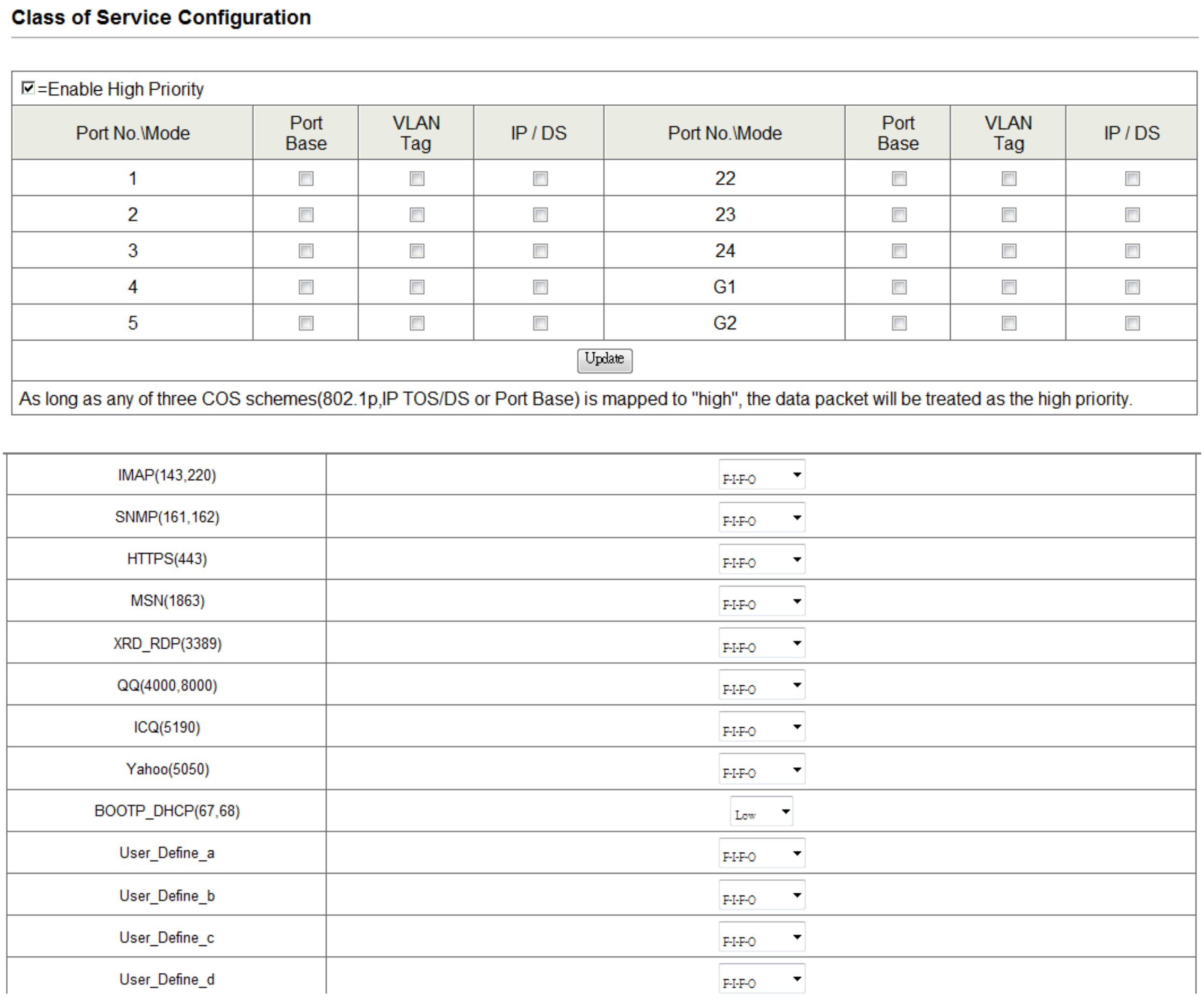
- First-In-First-Out: Packets are placed into the queue and serviced in the order they were received.
- All-high-before-low (Strict priority): All packets will be assigned to either a high priority queue (Queue 2) or a low priority queue (Queue 1). The packet on the low priority queue will not be forwarded 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.

Click **Update** to save your changes.

71B7.2.2. Port, 802.1p, IP/DS based

Note that checking **Port Base**, **VLAN Tag** or **IP/DS** will cause the port checked to be treated as high priority. Click **Update** to save your changes.



Class of Service Configuration

☑=Enable High Priority

Port No.\Mode	Port Base	VLAN Tag	IP / DS	Port No.\Mode	Port Base	VLAN Tag	IP / DS
1	☐	☐	☐	22	☐	☐	☐
2	☐	☐	☐	23	☐	☐	☐
3	☐	☐	☐	24	☐	☐	☐
4	☐	☐	☐	G1	☐	☐	☐
5	☐	☐	☐	G2	☐	☐	☐

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.

IMAP(143,220)	F-I-F-O
SNMP(161,162)	F-I-F-O
HTTPS(443)	F-I-F-O
MSN(1863)	F-I-F-O
XRD_RDP(3389)	F-I-F-O
QQ(4000,8000)	F-I-F-O
ICQ(5190)	F-I-F-O
Yahoo(5050)	F-I-F-O
BOOTP_DHCP(67,68)	Low
User_Define_a	F-I-F-O
User_Define_b	F-I-F-O
User_Define_c	F-I-F-O
User_Define_d	F-I-F-O

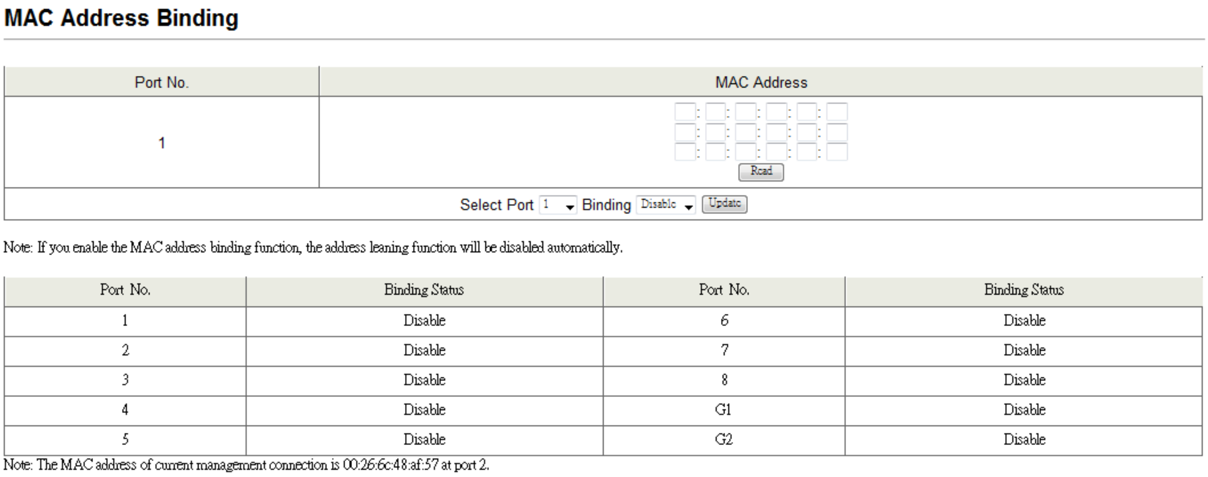
Figure 26 - Check any of the three options to enable high priority

8. SECURITY

To access security options, click on the link ***Security*** in the navigation pane of the web interface.

8.1. MAC Address Binding

Setting a MAC address allows interfaces to be uniquely identified on your network.



MAC Address Binding

Port No.	MAC Address
1	□:□:□:□:□:□ □:□:□:□:□:□ □:□:□:□:□:□ Read
Select Port 1 Binding Disable Update	

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

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

Note: The MAC address of current management connection is 00:26:6c:48:af:57 at port 2.

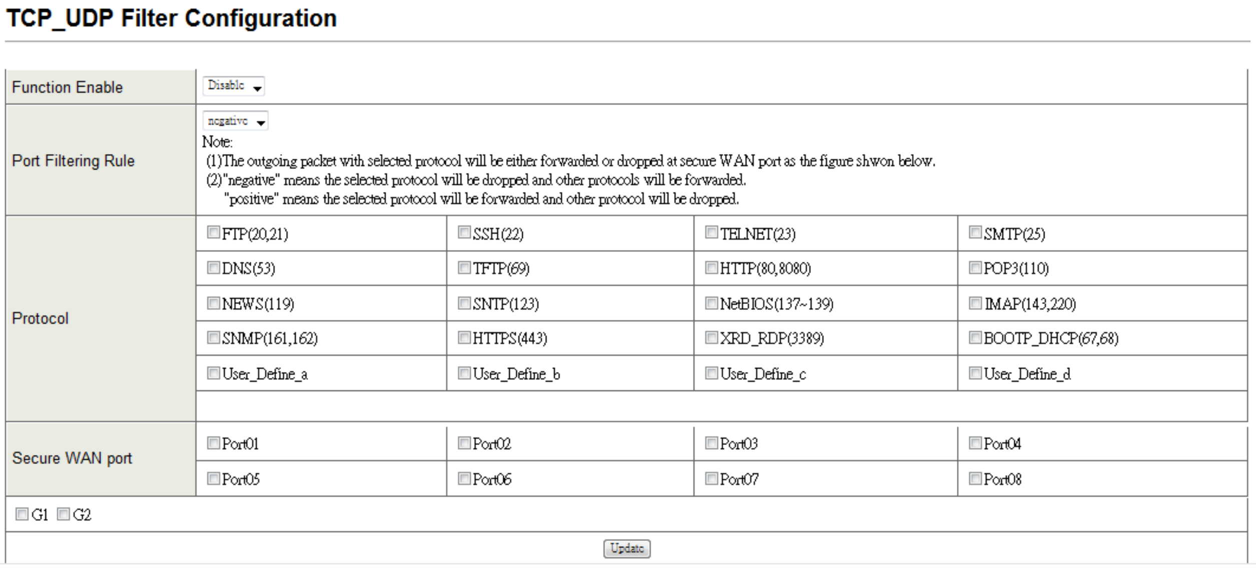
Figure 27 - Bind MAC addresses to ports

- Port No: Displays the port number being assigned the MAC addresses.
- MAC Address: Assign up to 3 MAC addresses to the port.
- Read: Click the read button to show the MAC addresses bound with a specified port or modify the MAC addresses.
- Select Port: Use the drop-down menu to choose a port number to be set.
- Binding: Select to ***Enable*** or ***Disable*** for the binding function.

Click **Update** to save your changes.

8.2. TCP/UDP Filter

Filter different types of connections to the network on this page.



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 shwon 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	□FTP(20,21)	□SSH(22)	□TELNET(23)	□SMTP(25)
	□DNS(53)	□TFTP(69)	□HTTP(80,8080)	□POP3(110)
	□NEWS(119)	□SNTP(123)	□NetBIOS(137~139)	□IMAP(143,220)
	□SNMP(161,162)	□HTTPS(443)	□XRD_RDP(3389)	□BOOTP_DHCP(67,68)
	□User_Define_a	□User_Define_b	□User_Define_c	□User_Define_d
Secure WAN port	□Port01	□Port02	□Port03	□Port04
	□Port05	□Port06	□Port07	□Port08
□G1 □G2				
Update				

Figure 28 - Check connections to filter

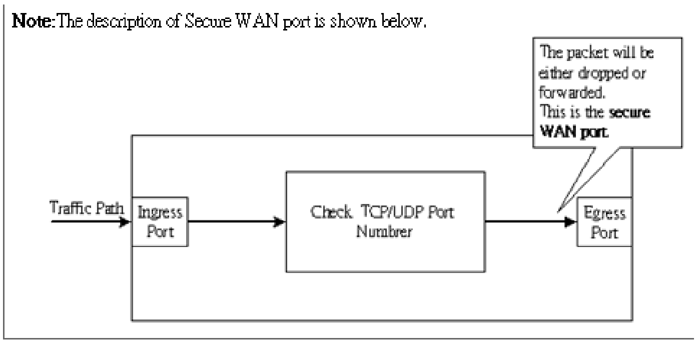

Note: The description of Secure WAN port is shown below.
The packet will be either dropped or forwarded. This is the secure WAN port.
Traffic Path
Ingress Port
Check TCP/UDP Port Numbrer
Egress Port

Figure 29 - Packet filtering overview

- Function Enable: ***Enable*** or ***Disable*** filtering.
- Port Filtering Rule: To allow forwarding (do not filter) select ***negative*** in the drop-down menu and in the Protocol section, select ports to forward. To disallow forwarding (filter) select ***positive*** in the drop-down menu and in the Protocol section, select ports to filter.
- Protocol: Check the protocols to filter/forward.
- Secure WAN port: Select the port on which WAN traffic is to be sent through.

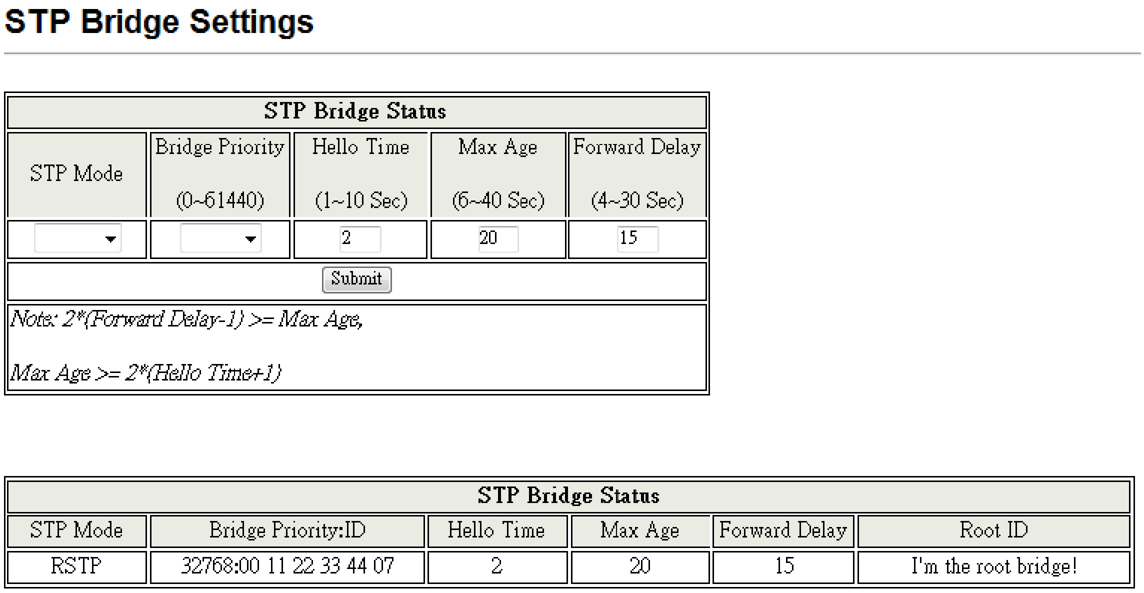
Click **Update** to save your changes.

9. SPANNING TREE PROTOCOL

The Spanning Tree protocol can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

The Protocol allows for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

To access Spanning Tree options, click on the link ***Spanning Tree*** in the navigation pane of the web interface.



STP Bridge Settings

STP Bridge Status

STP Mode	Bridge Priority (0~61440)	Hello Time (1~10 Sec)	Max Age (6~40 Sec)	Forward Delay (4~30 Sec)
		2	20	15

Note: 2(Forward Delay-1) >= Max Age,*

Max Age >= 2(Hello Time+1)*

STP Bridge Status

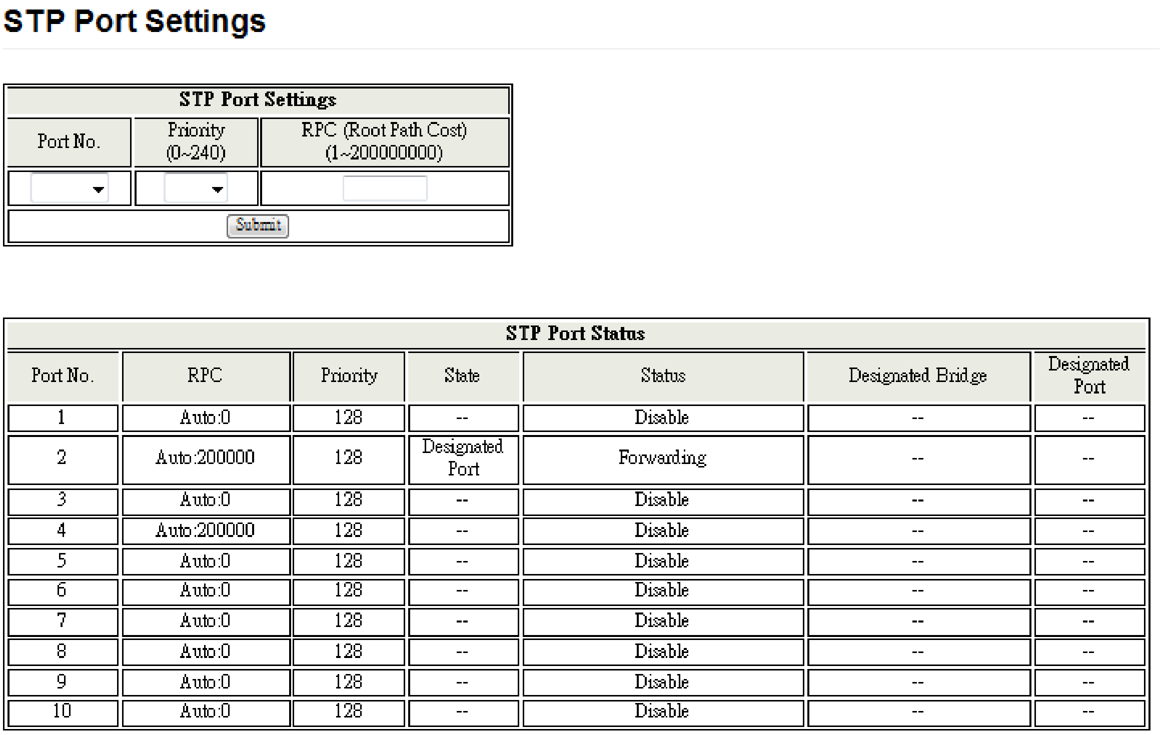
STP Mode	Bridge Priority:ID	Hello Time	Max Age	Forward Delay	Root ID
RSTP	32768:00 11 22 33 44 07	2	20	15	I'm the root bridge!

Figure 30 - Set options for the bridge in STP

- Bridge Priority: This parameter configures the spanning tree priority globally for this switch. The device with the highest priority becomes the STP root device. If all devices have the same priority, the device with the lowest MAC address will then become the root device. A number selected should be between ***0*** and ***61440*** in increments of 4096.
- Hello Time: Interval (in seconds) at which the root device transmits a configuration message (BPDU frame). Select a number between ***1*** and ***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. Select a number between ***6*** and ***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). Choose a number from ***4*** to ***30*** (default is ***15***).

Click **Submit** to save your changes. STP status is summarized in the table at the bottom of the screen.

9.2. STP Port Settings



STP Port Settings

STP Port Settings		
Port No.	Priority (0~240)	RPC (Root Path Cost) (1~200000000)

STP Port Status						
Port No.	RPC	Priority	State	Status	Designated Bridge	Designated Port
1	Auto:0	128	--	Disable	--	--
2	Auto:200000	128	Designated Port	Forwarding	--	--
3	Auto:0	128	--	Disable	--	--
4	Auto:200000	128	--	Disable	--	--
5	Auto:0	128	--	Disable	--	--
6	Auto:0	128	--	Disable	--	--
7	Auto:0	128	--	Disable	--	--
8	Auto:0	128	--	Disable	--	--
9	Auto:0	128	--	Disable	--	--
10	Auto:0	128	--	Disable	--	--

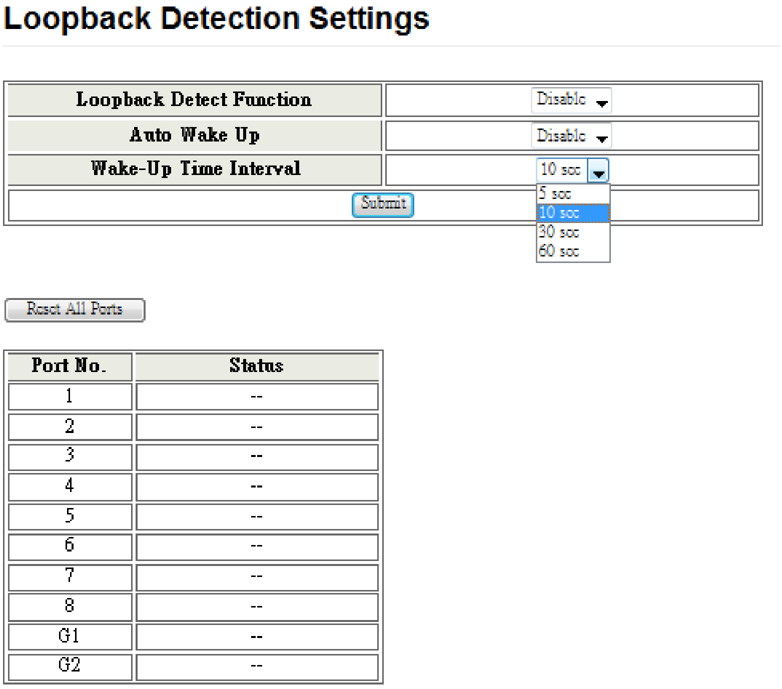
Figure 31 - Set options for the port in STP

- Port No: The port ID. It cannot be changed. Aggregations refer to 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 between ***0*** and ***200000000***. ***0*** indicates an automatically calculated path cost.
- State: Displays whether a port is a designated, root or blocked port.

Click **Update** to save your changes. A summary of port statuses can be viewed in the table at the bottom of the screen.

9.3. Loopback Detection Settings

This function detects the presence of network traffic routed back to its source. The status for all ports is given.



Loopback Detection Settings

Loopback Detect Function	Disable
Auto Wake Up	Disable
Wake-Up Time Interval	10 sec

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

Figure 32 - Prevent traffic collision by configuring Loopback Detection

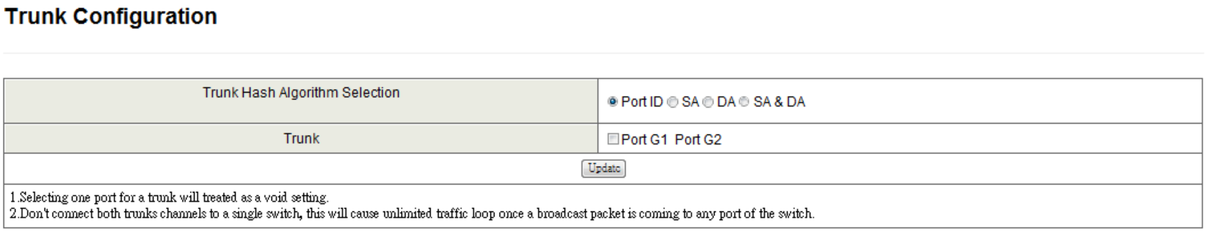
- Loopback Detect Function: Choose whether to ***Enable*** or ***Disable*** this function.
- Auto Wake Up: Determine whether or not the controller is set to wake up or not.
- Wake-Up Time Interval: Specify duration in the drop-down menu.

Click **Update** to save your changes. A summary of the configuration can be seen in the table at the bottom of the screen.

10. 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 network. As such, 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 as determined by 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 as the selecting factor for this algorithm. The Traffic pattern on the network should be considered carefully before applying it. When a proper hash algorithm is used network traffic will be load-balanced and transmitted across any link within the trunk.

To access Trunking options, click on the link ***Trunk Configuration*** in the navigation pane of the web interface.



Trunk Configuration

Trunk Hash Algorithm Selection	● Port ID ○ SA ○ DA ○ SA & DA
Trunk	□Port G1 Port G2
Update	

1.Selecting one port for a trunk will treated as a void setting.
2.Don't connect both trunks channels to a single switch, this will cause unlimited traffic loop once a broadcast packet is coming to any port of the switch.

Figure 33 - Set trunking options

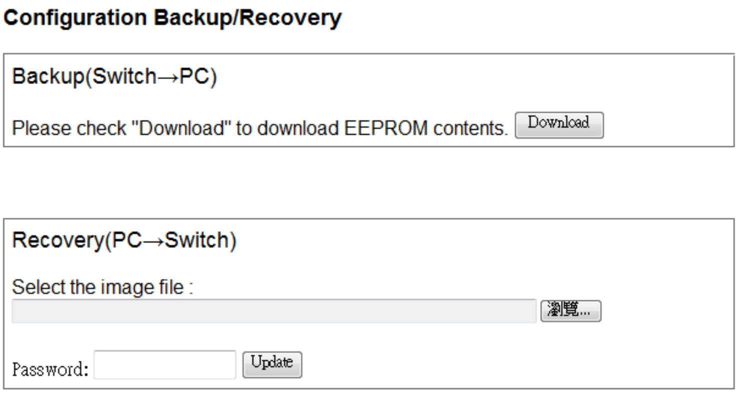
This managed switch supports two trunk groups, each trunk consists of 2~4 ports.

- Trunk Hash Algorithm Selection: Use either ***Port ID***, ***SA*** (Source MAC Address), ***DA*** (Destination MAC Address) or ***SA & DA*** (Source and Destination).
- Trunk: For each port, select either Port G1 or Port G2 to add them to the group.

Click **Update** to save your changes.

11. BACKUP/RECOVERY

To access backup and recovery options, click on the link ***Backup/Recovery*** in the navigation pane of the web interface.



Configuration Backup/Recovery

Backup(Switch→PC)

Please check "Download" to download EEPROM contents.

Recovery(PC→Switch)

Select the image file :

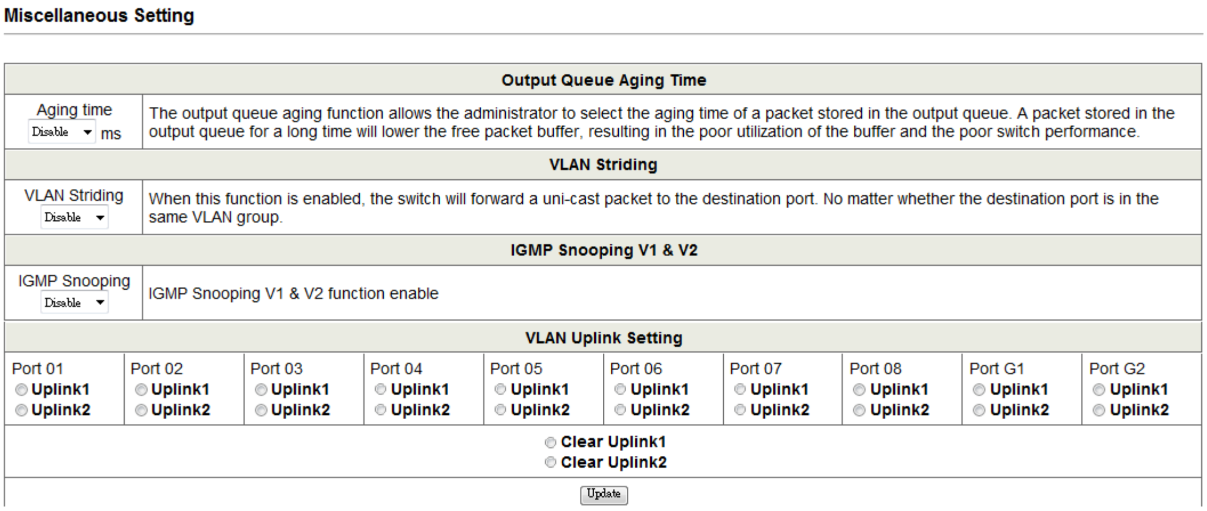
Password:

Figure 34 - Manage backup and recovery of switch settings

This function provides the user with a method to backup/recover switch configuration. Save a configuration file by clicking **Download**. This will save a file of current settings. To recover a configuration, type its path into the field and enter the administrator password. Click **Update** to save your changes.

12. MISCELLANEOUS SETTINGS

Miscellaneous settings can be used to configure output queue aging time, VLAN stride and IGMP snooping.



Miscellaneous Setting

Output Queue Aging Time	
Aging time 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.
VLAN Striding	
VLAN Striding 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.
IGMP Snooping V1 & V2	
IGMP Snooping Disable ▾	IGMP Snooping V1 & V2 function enable

VLAN Uplink Setting

Port 01	Port 02	Port 03	Port 04	Port 05	Port 06	Port 07	Port 08	Port G1	Port G2
○ **Uplink1**	○ **Uplink1**	○ **Uplink1**	○ **Uplink1**	○ **Uplink1**	○ **Uplink1**	○ **Uplink1**	○ **Uplink1**	○ **Uplink1**	○ **Uplink1**
○ **Uplink2**	○ **Uplink2**	○ **Uplink2**	○ **Uplink2**	○ **Uplink2**	○ **Uplink2**	○ **Uplink2**	○ **Uplink2**	○ **Uplink2**	○ **Uplink2**

○ **Clear Uplink1**
○ **Clear Uplink2**

Figure 35 - Configure Aging time, VLAN striding and IGMP snooping

- Output queue aging: When a packet is stored in a switch for a long time, it will expire from the allowable time defined by the protocol and become a useless packet. To prevent these packets from wasting the bandwidth, this option will remove them.
- VLAN Striding: By selecting this function, uni-cast packets are forwarded to the destination port, even if the destination port is in the same VLAN.
- IGMP Snooping: The switch will execute IGMP snooping version 1 and version 2 without CPU intervention. The IGMP report and leave packets are automatically handled by the switch.

Click **Update** to save your changes.

13. TROUBLESHOOTING

This chapter contains information to help you solve issues that might come up while using the switch.

The Link LED is not lit

- ➢ Solution: Check the cable connection and remove duplex mode of the Ethernet Switch

Some stations cannot talk to other stations located on the other port

- ➢ Solution: Please check the VLAN settings, trunk settings, or port enabled / disabled status.

Performance is bad

- ➢ Solution: Check the full duplex status of the Ethernet Switch. If the Ethernet Switch is set to full duplex and the partner is set to half duplex, then the performance will be poor. Please also check the in/out rate of the port.

The switch will not connect to a network

- ➢ Solution: Check the LNK/ACT LED on the switch

Try another port on the Switch

- ➢ Solution:
  - Make sure the cable is installed properly
  - Make sure the cable is the right type
  - Turn off the power. After a while, turn on power again

100Base-TX port link LED is lit, but the traffic is irregular

- ➢ Solution: Check that the attached device is not set to dedicate full duplex. Some devices use a physical or software switch to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.

Switch does not power up

- ➢ Solution: The AC power cord is either not inserted or faulty; check that the AC power cord is inserted correctly and replace it if necessary. Check that the AC power source is working by connecting a different device in place of the switch.

Lost admin password

- ➢ Solution: See the *Administration* section for information on how to reset the switch to factory settings.

APPENDIX A: NETWORKING HARDWARE

A.1. RJ-45 Pin Assignments

1000Mbps, 1000Base T pin assignment.

Contact	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

Table 3 - Pin assignment for 1000 Mbps, 1000 BaseT

Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

A.2. 10/100Mbps, 10/100Base-TX

When connecting your 10/100Mbps Ethernet Switch to another switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ-45 receptacle/ connector and their pin assignments:

Contact	MDI Media Dependant Interface	MDI-X Media Dependant Interface-Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

Table 4 - Pin assignment for 10/100 Mbps, 10/100 BaseTX

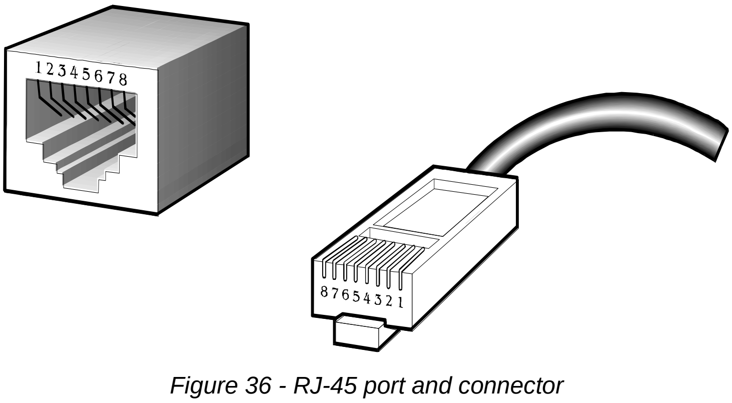


Figure 36 - RJ-45 port and connector

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:

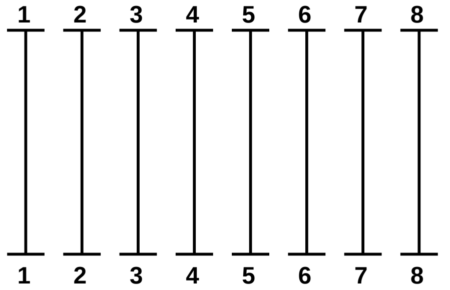
Straight Cable		SIDE 1	SIDE2
	SIDE 1 SIDE 2	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown

Table 5 - Straight through cable pins

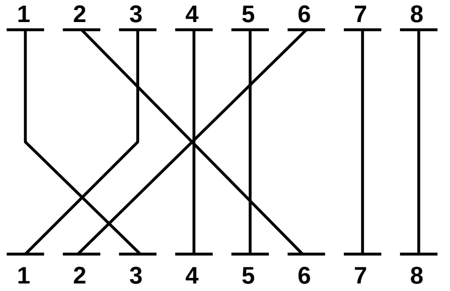
Crossover Cable		SIDE 1	SIDE2
	SIDE 1 SIDE 2	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown	1 = White / Green 2 = Green 3 = White / Orange 4 = Blue 5 = White / Blue 6 = Orange 7 = White / Brown 8 = Brown

Table 6 - Crossover cable pins

Please make sure your connected cables are with same pin assignment and color as above picture before deploying the cables into your network.

APPENDIX B: Store-and-Forward

Store-and-Forward is one type of packet-forwarding technique. A Store-and-Forward Ethernet switch stores the incoming frame in an internal buffer; complete error checking is done before transmission to eliminate the occurrence of error packets. This is the best choice when a network efficiency and stability are a priority.

The switch scans the destination address from the packet-header, searches the routing table provided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch ideal for connecting servers directly to the network, thereby increasing throughput and availability. However, the switch is most commonly used to segment existing hubs, which nearly always improves overall performance. An Ethernet switch can be easily configured in any network environment to significantly boost bandwidth using conventional cabling and adapters.

Due to the learning function of the switch, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain and reduce the overall load on the network.

The Switch performs "Store and forward" therefore, no error packets occur. More reliably, it reduces the rate of re-transmissions. No packet loss will occur.

APPENDIX C: PoE OVERVIEW

IEEE802.3af, also called Data Terminal equipment (DTE) power via Media dependent interface (MDI), is an international standard which defines the transmission for power over Ethernet. 802.3af delivers 48V power over RJ-45 wiring. Besides 802.3af, two types of source equipment are defined: Mid-Span and End-Span.

- Mid-Span: A Mid-Span device is placed between a legacy switch and the powered device. Mid-Span taps unused wire pairs 4/5 and 7/8 to carry power. The other four are reserved for data transmission.
- End-Span: An End-Span device connects directly with a power device. End-Span devices can also tap the 1/2 and 3/6 wire pairs.

C.1. PoE System Architecture

The specification of PoE typically requires two devices: the **Powered Source Equipment (PSE)** and the **Powered Device (PD)**. The PSE is either an End-Span or a Mid-Span, while the PD is a PoE-enabled terminal, such as IP Phones, Wireless LAN, etc. Power can be delivered over data pairs or spare pairs of standard CAT-5 cabling.

C.1.1. Power Transference through a CAT5 Ethernet cable

A standard CAT5 Ethernet cable has four twisted pairs, but only two of these are used for 10BASE-T and 100BASE-T specifications. The specification allows two options for using these cables for power, shown in Figure 8-1 and Figure 8-2:

The spare pairs are being used in these diagrams; Figure 8-1 shows the pair on pins 4 and 5 connected together, forming a positive supply and the pair on pins 7 and 8 connected, forming a negative supply. In actual use, either polarity may be used for power transference.

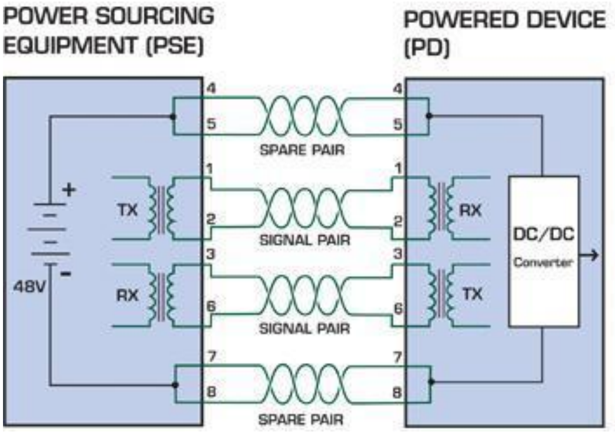


Figure 37 – Power supplied over spare pins

The data pairs are used in this next figure. Since Ethernet pairs are transformer coupled at each end, DC power may be applied to the center tap of the isolation transformer without upsetting the data transfer. In this mode of operation the pair on pins 3 and 6 and the pair on pins 1 and 2 can be of either polarity.

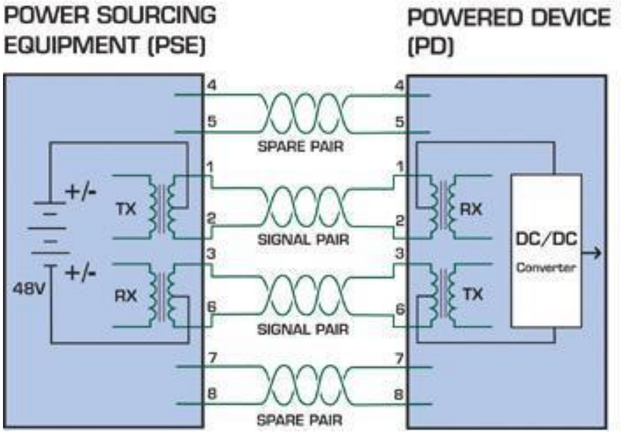


Table 7 - Power supplied over data pins

References:

- **IEEE Std 802.3af-2003**
  - (Amendment to IEEE Std 802.3-2002, including IEEE Std 802.3ae-2002), 2003 Page(s):0_1-121
- **White Paper on Power over Ethernet (IEEE802.3af)**
  - http://www.poweroverethernet.com/articles.php?article_id=52
- **Microsemi /PowerDsine**
  - http://www.microsemi.com/PowerDsine/
- **Linear Tech**
  - http://www.linear.com/

C.2. PoE Provisioning Process

It should be noted that proper preparation is needed prior to initializing a PoE network in order to minimize the risk of damage to hardware not designed for network-based power provisioning. Despite the fact that adding PoE support to network devices is a relatively simple operation, read this section carefully and understand this process before attempting to transfer power through CAT-5 to these devices.

The PSE is a device that manages the power flow over an Ethernet cable. During the detection period, a small voltage level is induced on the port's output until a PD is detected. The PSE may choose to perform classification; to estimate the amount of power to be consumed by this PD. After a time-controlled start-up, the PSE begins supplying the 48 VDC level to the PD, till it is physically or electrically disconnected, during which voltage and power will shut down.

Since the PSE is responsible for the PoE process timing, it is the one generating the probing signals prior to operating the PD and monitoring the various scenarios that may occur during operation.

All probing is done using voltage induction and current measurement in return.

Stage	Action	Volts specified per 802.3af	Volts managed by chipset
Detection	Measure whether powered device has the correct signature resistance of 15–33 kΩ	2.7-10.0	1.8–10.0
Classification	Measure which power level class the resistor indicates	14.5-20.5	12.5–25.0
Startup	Where the powered device will startup	>42	>38
Normal operation	Supply power to device	36-57	25.0–60.0

Table 8 - Stages of PoE

C.2.1. Line Detection

Before power is applied, for safety reasons a valid PD is connected to the PSE's output first. This process is referred to as "line detection", and involves the PSE seeking a specific 25 KΩ signature resistor. Detection of this signature indicates that a valid PD is connected, and that provision of power to the device may commence.

The signature resistor is isolated in the PD's PoE front-end, away from the rest of the PD's circuitries till detection is certified.

C.2.2. Classification

Once a PD is detected, the PSE may optionally perform classification to determine the maximal power a PD is to consume. The PSE induces 15.5-20.5 VDC, limited to 100 mA, for a period of 10 to 75 ms responded by a certain current consumption by the PD, indicating its power class.

The PD is assigned to one of 5 classes: 0 (default class) indicates that full 15.4 watts should be provided, 1-3 indicate various required power levels and 4 is reserved for future use. PDs that do not support classification are assigned class 0. Special care must be employed in the definition of class thresholds, as classification may be affected by cable losses.

Classifying a PD according to its power consumption ideally helps a PoE system in optimizing its power distribution, so that efficient power management based on classification results may reduce total system costs.

C.2.3. Start-up

Once line detection and optional classification stages are completed, the PSE must switch from low voltage to its full voltage capacity (44-57 Volts) over a minimal amount of time (above 15 microseconds). A gradual startup is required to avoid a sudden rise in voltage (reaching high frequencies) would introduce noise on the data lines. Once provision of power is initiated, it is common for an inrush current to be experienced at the PSE port, due to the PD's input capacitance. A PD must be designed to cease inrush current consumption (of over 350 mA) within 50 ms of power provision startup.

C.2.4. Operation

During normal operation, the PSE provides 44-57 VDC, able to support a minimum of 15.4 watts power.

C.2.5. Power Overloads

The IEEE 802.3af standard defines the handling of overload conditions. In the event of an overload (a PD drawing a higher power level than the allowed 12.95 Watts), or an outright short circuit caused by a failure in cabling or in the PD, the PSE must shut down power within 50 to 75 milliseconds, while limiting current drain during this period to protect the cabling infrastructure. Immediate voltage drop is avoided to prevent shutdown due to random fluctuations.

C.3. Power Disconnection Scenarios

The IEEE 802.3af standard requires that devices powered over Ethernet be disconnected safely (i.e. power needs be shut down within a short period of time following disconnection of a PD from an active port). When a PD is disconnected, there is a danger that it will be replaced by a non-PoE-ready device while power is still on to avoid damaging the device and risking injury.

The standard defines two means of disconnection, DC Disconnect and AC Disconnect, both of which provide the same functionality - the PSE shutdowns power to a disconnected port within 300 to 400ms. The upper boundary is a physical human limit for disconnecting one PD and reconnecting another.

DC Disconnect

DC Disconnect detection involves measurement of current. A disconnected PD stops consuming current, which can be inspected by the PSE. The PSE must therefore disconnect power within 300 to 400 ms from the current flow stop. The lower time boundary is important to prevent shutdown due to random fluctuations.

AC Disconnect

This method is based on the fact that when a valid PD is connected to a port, the AC impedance measured on its terminals is significantly lower than in the case of an open port (disconnected PD).

AC Disconnect detection involves the induction of low AC signal in addition to the 48 VDC operating voltage. The returned AC signal amplitude is monitored by the PSE at the port terminals. During normal operation, the PD's relatively low impedance lowers the returned AC signal while a sudden disconnection of this PD will cause a surge to the full AC signal level and will indicate PD disconnection.

APPENDEX D: GLOSSARY

A

Aggregation

Aggregation is a method wherein multiple ports are used in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

D

DEI

DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

DHCP

DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.
The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.10.

I

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IP

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over it is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

P

PD

PD is an acronym for Powered Device. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PING

ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

PoE

PoE is an acronym for Power Over Ethernet.

Power Over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

Private VLAN

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

Q

QCE

QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QoS

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

R

Router Port

A router port is a port on the Ethernet switch that leads a switch towards a multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SHA

SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

STP

Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

T

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

ToS

ToS is an acronym for Type of Service. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

U

UDP

UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame.

V

VLAN

Virtual LAN is a method restricting communication between switch ports. VLANs can be used for the following applications:

- **VLAN unaware switching:** This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.
- **VLAN aware switching:** This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.
- **Provider switching:** This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.