



# **GEP-2450**

**24 GE PoE with 4 Dual Speed Combo SFP  
Web Smart Switch**

## **User Manual**



# **GEP-2450**

## **User's Manual**

---

The information in this document is subject to change without notice. Unless the explicit written permission of DDC Corporation, this document in whole or in part shall not be replicated or modified or amended or transmitted, in any form, or by any means manual, electric, electronic, electromagnetic, mechanical, optical or otherwise for any purpose.

### **DURATION OF HARDWARE WARRANTY**

**HARDWARE:** In accordance with the provisions described under, DDC Corporation (hereinafter called "DDC") warrants its hardware products (hereinafter referred to as "Product") specified herein to be for a period of twelve (12) months from the date of shipment.

Should a Product fail to perform during the effective warranty period as described above, DDC shall replace the defective Product or part, or delivering a functionally equivalent Product or part in receipt of customer's request, provided that the customer complies with the return material authorization (RMA) procedures and returns all defective Product prior to installation of the replacements to DDC.

All defective Products must be returned to DDC with issuance of a Return Material Authorization number (RMA number) assigned to the reseller from whom the end customer originally purchased the Product. The reseller is responsible for ensuring the shipments are insured, with the transportation charges prepaid and the RMA number clearly marked on the outside of the package. DDC will not accept collect shipments or those returned without an RMA number.

DDC shall not be responsible for any software, firmware, information or memory data contained in, stored on or integrated with any Product returned to DDC pursuant to any warranty.

**EXCLUSIONS.** The warranty as mentioned above does not apply to the following conditions, in DDC's judgment, it contains (1) customer does not comply with the manual instructions offered by DDC in installation, operation, repair or maintenance, (2) Product fails due to damage from unusual external or electrical stress, shipment, storage, accident, abuse or misuse, (3) Product is used in an extra hazardous environment or activities, (4) any serial number on the Product has been removed or defaced, (5) this warranty will be of no effect if the repair is via anyone other than DDC or the approved agents, or (6) In the event of any failures or delays by either party hereto in the performance of all or any part of this agreement due to acts of God, war, riot, insurrection, national emergency, strike, embargo, storm, earthquake, or other natural forces, or by the acts of anyone not a party to this agreement, or by the inability to secure materials or transportation, then the party so affected shall be executed from any further performance for a period of time after the occurrence as may reasonably be necessary to remedy the effects of that occurrence, but in no event more than sixty (60) days. If any of the stated events should occur, Party A shall promptly notify Party B in writing as soon as commercially practicable, but in no event more than twenty (20) business days and provide documentation evidencing such occurrence. In no event shall the maximum liability of DDC under this warranty exceed the purchase price of the Product covered by this warranty.

**DISCLAIMER.** EXCEPT AS SPECIFICALLY PROVIDED ABOVE AS REQUIRED "AS IS" AND THE WARRANTIES AND REMEDIES STATED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHERS, ORAL OR WRITTEN, EXPRESS OR IMPLIED. ANY AND ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR THIRD PARTY RIGHTS ARE EXPRESSLY EXCLUDED.

### **DDC SOFTWARE LICENSE AGREEMENT**

**NOTICE:** Please carefully read this Software License Agreement (hereinafter referred to as this "Agreement") before copying or using the accompanying software or installing the hardware unit with pre-enabled software or firmware (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE PROVISIONS AND CONDITIONS OF THIS AGREEMENT. THE PROVISIONS EXPRESSED IN THIS AGREEMENT ARE THE ONLY PROVISION UNDER WHICH DDC WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these provisions and conditions, please immediately return the unused software, manual and the related product. Written approval is **NOT** a prerequisite to the validity or enforceability of this Agreement and no solicitation of any such written approval by or on behalf of DDC shall be deemed as an inference to the contrary.

**LICENSE GRANT.** The end user (hereinafter referred to as "Licensee") of the Software is granted a personal, non-sublicensable, nonexclusive, nontransferable license by DDC Corporation ("DDC"): (1) To use the DDC's software ("Software") in object code form solely on a single central processing unit owned or leased by Licensee or otherwise embedded in the equipment offered by DDC. (2) To copy the Software only for backup purposes in support of authorized use of the Software. (3) To use and copy the documentation related to the Software solely in support of authorized use of the Software by Licensee. The License applies to the Software only except other DDC's software or hardware products. Without the prior written consent of DDC, Licensee has no right to receive any source code or design documentation with respect to the Software.

**RESTRICTIONS ON USE; RESERVATION OF RIGHTS.** The Software and related documentation are protected under copyright laws. DDC and/or its licensors retain all title and ownership in both the Software and its related documentation, including any revisions made by DDC. The copyright notice must be reproduced and included with any copy of any portion of the Software or related documentation. Except as expressly authorized above, Licensee shall not copy or transfer the Software or related documentation, in whole or in part. Licensee also shall not modify, translate, decompile, disassemble, use for any competitive analysis, reverse compile or reverse assemble all or any portion of the Software, related documentation or any copy. The Software and related documentation embody DDC's confidential and proprietary intellectual property. Licensee is not allowed to disclose the Software, or any information about the operation, design, performance or implementation of the Software and related documentation that is confidential to DDC to any third party. Software and related documentation may be delivered to you subject to export authorization required by governments of Taiwan and other countries. You agree that you will not export or re-export any Software or related documentation without the proper export licenses required by the governments of affected countries.

**LIMITED SOFTWARE WARRANTY.** DDC warrants that any media on which the Software is recorded will be free from defects in materials under normal use for a period of twelve (12) months from date of shipment. If a defect in any such media should occur during the effective warranty period, the media may be returned to DDC, then DDC will replace the media. DDC shall not be responsible for the replacement of media if the failure of the media results from accident, abuse or misapplication of the media.

**EXCLUSIONS.** The warranty as mentioned above does not apply to the Software, which (1) customer does not comply with the manual instructions offered by DDC in installation, operation, or maintenance, (2) Product fails due to damage from unusual external or electrical stress, shipment, storage, accident, abuse or misuse, (3) Product is used in an extra hazardous environment or activities, (4) any serial number on the Product has been removed or defaced, or (5) this warranty will be of no effect if the repair is via anyone other than DDC or the authorized agents. The maximum liability of DDC under this warranty is confined to the purchase price of the Product covered by this warranty.

**DISCLAIMER.** EXCEPT AS PROVIDED ABOVE, THE SOFTWARE IS PROVIDED "AS IS " AND DDC AND ITS LICENSORS MAKE NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION. DDC AND ITS LICENSORS DISCLAIM ALL OTHER WARRANTIES, INCLUSIVE OF WITHOUT LIMITATION, IMPLIED WARRANTIES OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. FURTHER, DDC DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR THE RESULTS OF THE USE, OF THE SOFTWARE OR RELATED WRITTEN DOCUMENTATION IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE.

**CONSEQUENTIAL DAMAGES.** IN NO EVENT SHALL DDC OR ITS AUTHORIZED RESELLER BE LIABLE TO LICENSEE OR ANY THIRD PARTY FOR (A) ANY MATTER BEYOND ITS REASONABLE CONTROL OR (B) ANY CONSEQUENTIAL, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES ARISING OUT OF THIS LICENSE OR USE OF THE SOFTWARE PROVIDED BY DDC, EVEN IF DDC HAS BEEN NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE. IN NO EVENT SHALL THE LIABILITY OF DDC IN CONNECTION WITH THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO DDC FOR THE LICENSE.

**TERM AND TERMINATION.** The License is effective until terminated; however, all of the restrictions in regard to DDC's copyright in the Software and related documentation will cease being effective at the date of expiration; Notwithstanding the termination or expiration of the term of this agreement, it is acknowledged and agreed that those obligations relating to use and disclosure of DDC's confidential information shall survive. Licensee may terminate this License at any time by destroying the software together with all copies thereof. This License will be immediately terminated if Licensee fails to comply with any term and condition of the Agreement. Upon any termination of this License for any reason, Licensee shall discontinue to use the Software and shall destroy or return all copies of the Software and the related documentation.

**GENERAL.** This License shall be governed by and construed pursuant to the laws of Taiwan. If any portion hereof is held to be invalid or unenforceable, the remaining provisions of this License shall remain in full force and effect. Neither the License nor this Agreement is assignable or transferable by Licensee without DDC's prior written consent; any attempt to do so shall be void. This License constitutes the entire License between the parties with respect to the use of the Software.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN DDC AND LICENSEE.

# Table of Contents

CAUTION .....	VI
ELECTRONIC EMISSION NOTICES .....	VII
<b>1. INTRODUCTION.....</b>	<b>10</b>
1-1. OVERVIEW OF 24-PORT GBE WEB SMART POE SWITCH .....	10
1-2. CHECKLIST .....	12
1-3. FEATURES .....	12
1-4. VIEW OF 24-PORT GBE WEB SMART POE SWITCH .....	14
1-4-1. User Interfaces on the Front Panel (Button, LEDs and Plugs).....	14
1-4-2. User Interfaces on the Rear Panel.....	15
1-5. VIEW OF THE OPTIONAL MODULES.....	16
<b>2. INSTALLATION.....</b>	<b>17</b>
2-1. STARTING 24-PORT GBE WEB SMART POE SWITCH UP .....	17
2-1-1. Hardware and Cable Installation .....	17
2-1-2. Cabling Requirements .....	18
2-1-3. Configuring the Management Agent of 24-Port GbE Web Smart PoE Switch ..	23
2-1-4. IP Address Assignment .....	24
2-2. TYPICAL APPLICATIONS .....	28
<b>3. BASIC CONCEPT AND MANAGEMENT.....</b>	<b>30</b>
3-1. WHAT'S THE ETHERNET.....	30
3-2. MEDIA ACCESS CONTROL (MAC) .....	33
3-3. FLOW CONTROL .....	38
3-4. HOW DOES A SWITCH WORK? .....	41
3-5. VIRTUAL LAN .....	45
3-6. LINK AGGREGATION .....	51
<b>4. OPERATION OF WEB-BASED MANAGEMENT .....</b>	<b>53</b>
4-1. WEB MANAGEMENT HOME OVERVIEW .....	54
4-2. CONFIGURATION .....	56
4-2-1. System Information.....	57
4-2-2. System Time .....	60
4-2-3. Ports .....	61
4-2-4. VLAN Mode Configuration.....	63
4-2-5. VLAN Group Configuration .....	67
4-2-6. PoE.....	69
4-2-8. LACP .....	78
4-2-9. RSTP.....	80
4-2-10. 802.1X.....	84
4-2-11 IGMP Snooping .....	92
4-2-12. Mirror Configuration.....	93
4-2-13. QoS(Quality of Service) Configuration .....	94
4-2-14. Filter.....	97
4-2-15. Rate Limit .....	99
4-2-16. Storm Control .....	101
4-2-17. SNMP.....	102
4-3. MONITORING .....	104
4-3-1. Detailed Statistics.....	105
4-3-2. LACP Status.....	108

4-3-3. RSTP Status .....	109
4-3-4. IGMP Status .....	110
4-3-5. Ping Status.....	112
4-4. MAINTENANCE .....	114
4-4-1. Warm Restart .....	115
4-4-2. Factory Default .....	116
4-4-3. Software Upgrade.....	117
4-4-4. Configuration File Transfer.....	118
4-4-5. Logout.....	119
<b>5. MAINTENACE .....</b>	<b>120</b>
5-1. RESOLVING NO LINK CONDITION .....	120
5-2. Q&A .....	120
<b>APPENDIX A TECHNICAL SPECIFICATIONS.....</b>	<b>121</b>

## Caution

Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.
- If you need using outdoor device connect to this device with cable then you need to addition an arrester on the cable between outdoor device and this device.

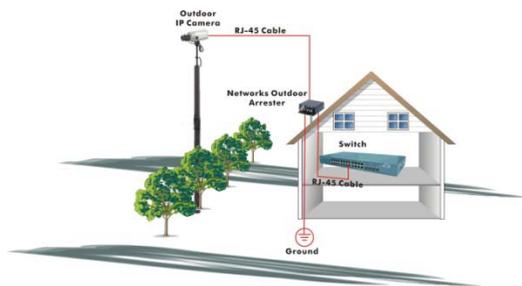


Fig. Addition an arrester between outdoor device and this switch

- The switch supports the SFP Vendor includes: LevelOne, Agilent, Avago and Finisa.
- The Web UI's Main Menu links are used to navigate to other menus, and display Configuration parameters and statistics with suggestive value 1024x 768.

## ***Electronic Emission Notices***

### **Federal Communications Commission (FCC) Statement**

This equipment has been tested and found to comply with the limits for a class A computing device pursuant to Subpart J of part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

### **European Community (CE) Electromagnetic Compatibility Directive**

This equipment has been tested and found to comply with the protection requirements of European Emission Standard **EN55022/EN61000-3** and the Generic European Immunity Standard EN55024.

EMC:

EN55022(2006)+A1:2007/CISPR 22:2006+A1:2006	class A
IEC61000-4-2 (2001)	4K V CD, 8KV, AD
IEC61000-4-3( 2006)	3V/m
IEC61000-4-4(2004)	1KV – (power line), 0.5KV – (signal line)
IEC61000-4-5 (2006)	Line to Line: 1KV, Line to Earth: 2KV
IEC61000-4-6 (2007)	130dBuV(3V) Level 2
IEC61000-4-8 (2001)	1A/m
	Voltage dips:
IEC61000-4-11(2004)	>95%, 0.5period, 30%, 25periods
	Voltage interruptions:
	>95%, 250periods

**Warning:**

- Self-demolition on Product is strictly prohibited. Damage caused by self-demolition will be charged for repairing fees.
- Do not place product at outdoor or sandstorm.
- Before installation, please make sure input power supply and product specifications are compatible to each other.
- Before importing / exporting configuration please make sure the firmware version is always the same.
- After firmware upgrade, the switch will remove the configuration automatically to latest firmware version.

# About this user's manual

This user's manual provides instructions on how to install your Web Smart Switch.

This guide also covers management options and detailed explanation about hardware and software functions.

## Overview of this user's manual

---

- Chapter 1 "Introduction" describes the features of 24 Gigabit Web Smart Switch
- Chapter 2 "Installation"
- Chapter 3 "Operating Concept and Management"
- Chapter 4 "Operation of Web-based Management"
- Chapter 5 "Maintenance"

# 1. Introduction

## 1-1. Overview of 24-Port GbE Web Smart PoE Switch

The 24-port Gigabit Web Smart PoE Switch is a standard switch that meets all IEEE 802.3/u/x/z Gigabit and Fast Ethernet specifications. The switch has 20 10/100/1000Mbps TP ports and 4 Gigabit TP/ (100/1000M) SFP transceiver slots, It supports http and SNMP interface for switch management. The network administrator can logon the switch to monitor, configure and control each port's activity. In addition, the switch implements the QoS (Quality of Service), VLAN, and Trunking. It is suitable for office application.

Others the switch increase support the Power saving for reduce the power consumption with "ActiPHY Power Management" and "PerfectReach Power Management" two technique.It could efficient saving the switch power with auto detect the client idle and cable length to provide different power.

This PSE switch also complies with IEEE 802.3af, its advanced auto-sensing algorithm enables providing powered devices (PD) discovery, classification, current limit, and other necessary functions. It also supports high safety with short circuit protection and power-out auto-detection to PD.

In this switch, Port 21, 22, 23, 24 includes two types of media --- TP and (100/1000M) SFP Fiber (LC, BiDi-SC...); this port supports 10/100/1000Mbps TP or (100/1000M) SFP Fiber with auto-detected function. (100/1000M) SFP Fiber transceiver is used for high-speed connection expansion.

10/100/1000Mbps TP is a standard Ethernet port that meets all IEEE 802.3/u/x/z Gigabit and Fast Ethernet specifications. (100/1000M) SFP Fiber transceiver is a Gigabit Ethernet port that fully complies with all IEEE 802.3z and 1000Base-SX/LX standards and 100Base-FX standards.

1000Mbps Single Fiber WDM (BiDi) transceiver is designed with an optic Wavelength Division Multiplexing (WDM) technology that transports bi-directional full duplex signal over a single fiber simultaneously.

## • Key Features in the Device

### QoS:

The switch offers powerful QoS function. This function supports 802.1p VLAN tag priority and DSCP on Layer 3 of network framework.

### VLAN:

Supports Port-based VLAN, IEEE802.1Q Tag VLAN. And supports 24 active VLANs and VLAN ID 1~4094.

### Port Trunking:

Allows one or more links to be aggregated together to form a Link Aggregation Group by the static setting.

### IGMP Snooping:

Support IGMP version 2 (RFC 2236): The function IGMP snooping is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoid wasting the bandwidth while IP multicast packets are running over the network.

### Q-in-Q VLAN for performance & security:

Limiting the broadcast traffic to within the same VLAN broadcast domain also enhances performance. Q-in-Q, the use of double VLAN tags is an efficient method for enabling Subscriber Aggregation. This is very useful in the MAN.

### SNMP:

SNMP agent In the device, SNMP agent is a client software which is operating over SNMP protocol used to receive the command from SNMP manager (server site) and echo the corresponded data, i.e. MIB object. Besides, SNMP agent will actively issue TRAP information when happened.

### Power Saving:

The Power saving using the "ActiPHY Power Management" and "PerfectReach Power Management" two techniques to detect the client idle and cable length automatically and provides the different power. It could efficient to save the switch power and reduce the power consumption.

### PoE/PoE Management:

24-PoE ports allow power to be supplied to end devices, such as Wireless Access Points or VoIP Phones, directly through the existing LAN cables, eliminating costs for additional AC wiring and reducing Installation Cost. It was compliant with IEEE802.3af standard. It provides the endpoint with 48VDC power through RJ-45 pin 1, 2, 3, 6. Also this device offers several PoE management functions like PoE Power Delay and PoE Scheduling.

## 1-2. Checklist

Before you start installing the switch, verify that the package contains the following:

- 24-Port GbE Web Smart PoE Switch
- Mounting Accessory (for 19" Rack Shelf)
- This User's Manual in CD-ROM
- AC Power Cord

Please notify your sales representative immediately if any of the aforementioned items is missing or damaged.

## 1-3. Features

The 24-Port GbE Web Smart PoE Switch, a standalone off-the-shelf switch, provides the comprehensive features listed below for users to perform system network administration and efficiently and securely serve your network.

### • Hardware

- 20 10/100/1000Mbps Auto-negotiation Gigabit Ethernet TP ports
- 4 10/100/1000Mbps TP or 100/1000Mbps SFP Fiber dual media auto sense
- 500KB on-chip frame buffer
- It supports 185 watts for PoE Power and up to 7.7 watts for 24 ports.
- Jumbo frame support 12.2KB
- Programmable classifier for QoS (Layer 2/Layer 3)
- 8K MAC address and support VLAN ID (1~4094)
- Per-port shaping, policing, and Broadcast Storm Control
- IEEE802.1Q-in-Q nested VLAN support
- Power Saving with "ActiPHY Power Management" and "PerfectReach Power Management" techniques.
- Full-duplex flow control (IEEE802.3x) and half-duplex backpressure
- Extensive front-panel diagnostic LEDs; System: Power, TP Port1-24: LINK/ACT/SPD , PoE, SFP Port 21, 22, 23,24: SFP(LINK/ACT)  
24 port IEEE802.3af PoE PSE.  
Endpoint with 48VDC power through RJ-45 pin 1, 2, 3, 6.  
Powered Device(PD) auto detection and classification.  
PoE-PSE status and activity LED indicator.

- **Management**

- Supports concisely the status of port and easily port configuration
- Supports per port traffic monitoring counters
- Supports a snapshot of the system Information when you login
- Supports port mirror function
- Supports the static trunk function
- Supports 802.1Q VLAN
- Supports user management and limits one user to login
- Maximal packet length can be up to 12.2KB for jumbo frame application
- Supports Broadcasting Suppression to avoid network suspended or crashed
- Supports to send the trap event while monitored events happened
- Supports default configuration which can be restored to overwrite the current configuration which is working on via Web UI and Reset button of the switch
- Supports on-line plug/unplug SFP modules
- Supports Quality of Service (QoS) for real time applications based on the information taken from Layer 2 to Layer 3.
- Built-in web-based management instead of using CLI interface, providing a more convenient GUI for the user

## 1-4. View of 24-Port GbE Web Smart PoE Switch



Fig. 1-1 Full View of 24-PORT GBE WEB SMART PoE SWITCH

### 1-4-1. User Interfaces on the Front Panel (Button, LEDs and Plugs)

There are 24 TP Gigabit Ethernet PoE ports and 4 (100/1000M) SFP fiber ports for optional removable modules on the front panel of the switch. LED display area, locating on the left side of the panel, contains a Power LED, which indicates the power status and 24 ports working status of the switch.

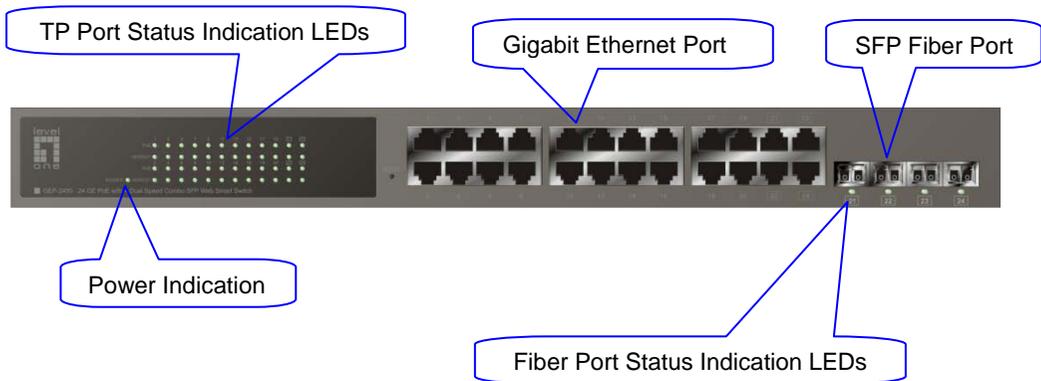


Fig. 1-2 Front View of 24-PORT GBE WEB SMART PoE Switch

- LED Indicators Description

LED	Color	Function
<b>System LED</b>		
POWER	Green	Lit when +5V power is coming up
<b>10/100/1000Ethernet TP Port 1 to 24 LED</b>		
LINK/ACT/SPD	Green/ Amber	Lit Green when 1000Mbps speed is active Lit Amber when 100/10Mbps speed is active Blinks when any traffic is present
PoE	Green	Lit when PoE Power is active
<b>Fiber Port 21, 22, 23, 24 LED</b>		
SFP(LINK/ACT)	Green/ Amber	Lit Green when 1000Mbps SFP connection with remote device is good Lit Amber when 100Mbps SFP connection with remote device is good Blinks when any traffic is present

Table1-1

#### 1-4-2. User Interfaces on the Rear Panel



Fig. 1-3 Rear View of 24-PORT GBE WEB SMART PoE SWITCH

## 1-5. View of the Optional Modules

In the switch, Port 21~24 include two types of media --- TP and (100/1000M) SFP Fiber (LC, BiDi-SC...); they support 10/100/1000Mbps TP or (100/1000M) SFP Fiber with auto-detected function. (100/1000M) SFP Fiber transceiver is used for high-speed connection expansion; nine optional (100/1000M)SFP types provided for the switch are listed below:

- 1000Mbps LC, MM, SFP Fiber transceiver
- 1000Mbps LC, SM 10km, SFP Fiber transceiver
- 1000Mbps LC, SM 30km, SFP Fiber transceiver
- 1000Mbps LC, SM 50km, SFP Fiber transceiver
- 1000Mbps BiDi LC, type 1, SM 20km, SFP Fiber WDM transceiver , 1310nm
- 1000Mbps BiDi LC, type 2, SM 20km, SFP Fiber WDM transceiver 1550nm
- 100Base-FX FE SFP Fiber Module, LC Multi-Mode
- 100Base-FX FE SFP Fiber Module, LC Single-Mode 20km



Fig. 1-4 Front View of 1000Base-SX/LX LC, SFP Fiber Transceiver



Fig. 1-5 Front View of 1000Base-LX BiDi SC SFP Fiber Transceiver

# 2. Installation

## 2-1. Starting 24-Port GbE Web Smart PoE Switch Up

This section will give users a quick start for:

- Hardware and Cable Installation
- Management Station Installation
- Software booting and configuration

### 2-1-1. Hardware and Cable Installation

First of all:

- ⇒ Wear a grounding device to avoid the damage from electrostatic discharge
- ⇒ Be sure that power switch is OFF before you insert the power cord to power source

- **Installing Optional SFP Fiber Transceivers to the 24-Port GbE Web Smart PoE Switch**

Note: If you have no modules, please skip this section.

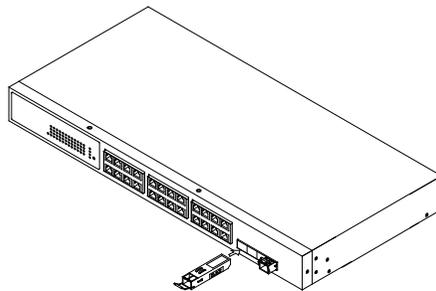


Fig. 2-1 Installation of Optional SFP Fiber Transceiver

- **Connecting the SFP Module to the Chassis:**

The optional SFP modules are hot swappable, so you can plug or unplug it before or after powering on.

1. Verify that the SFP module is the right model and conforms to the chassis
2. Slide the module along the slot. Also be sure that the module is properly seated against the slot socket/connector
3. Install the media cable for network connection
4. Repeat the above steps, as needed, for each module to be installed into slot(s)
5. Have the power ON after the above procedures are done

- **TP Port and Cable Installation**

- ⇒ In the switch, TP port supports MDI/MDI-X auto-crossover, so both types of cable, straight-through (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 1, 2, 3, 6 in 10/100M TP; 1, 2, 3, 4, 5, 6, 7, 8 to 1, 2, 3, 4, 5, 6, 7, 8 in Gigabit TP) and crossed-over (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 3, 6, 1, 2) can be used. It means you do not have to tell from them, just plug it.
- ⇒ Use Cat. 5 grade RJ-45 TP cable to connect to a TP port of the switch and the other end is connected to a network-aware device such as a workstation or a server.
- ⇒ Repeat the above steps, as needed, for each RJ-45 port to be connected to a Gigabit 10/100/1000 TP device.

Now, you can start having the switch in operation.

- **Power On**

The switch supports 100-240 VAC, 50-60 Hz power supply. The power supply will automatically convert the local AC power source to DC power. It does not matter whether any connection plugged into the switch or not when power on, even modules as well. After the power is on, all LED indicators will light up and then all off except the power LED still keeps on. This represents a reset of the system.

- **Firmware Loading**

After resetting, the bootloader will load the firmware into the memory. It will take about 30 seconds, after that, the switch will flash all the LED once and automatically performs self-test and is in ready state.

## **2-1-2. Cabling Requirements**

To help ensure a successful installation and keep the network performance good, please take a care on the cabling requirement. Cables with worse specification will render the LAN to work poorly.

### 2-1-2-1. Cabling Requirements for TP Ports

- ⇒ For Fast Ethernet TP network connection
  - The grade of the cable must be Cat. 5 or Cat. 5e with a maximum length of 100 meters.
- ⇒ Gigabit Ethernet TP network connection
  - The grade of the cable must be Cat. 5 or Cat. 5e with a maximum length of 100 meters. Cat. 5e is recommended.

### 2-1-2-2. Cabling Requirements for 1000SX/LX, 100Base-FX SFP Module

It is more complex and comprehensive contrast to TP cabling in the fiber media. Basically, there are two categories of fiber, multi mode (MM) and single mode (SM). The later is categorized into several classes by the distance it supports. They are SX, LX, LHX, XD, and ZX. From the viewpoint of connector type, there mainly are LC and BIDI SC.

- Gigabit Fiber with multi-mode LC SFP module
- Gigabit Fiber with single-mode LC SFP module
- 100Base-FX FE SFP Fiber Module, LC Multi-Mode
- 100Base-FX FE SFP Fiber Module, LC Single-Mode
- Gigabit Fiber with BiDi LC 1310nm SFP module
- Gigabit Fiber with BiDi LC 1550nm SFP module

The following table lists the types of fiber that we support and those else not listed here are available upon request.

	Multi-mode Fiber Cable and Modal Bandwidth				
	Multi-mode 62.5/125μm		Multi-mode 50/125μm		
IEEE 802.3z Gigabit Ethernet 1000SX 850nm	Modal Bandwidth	Distance	Modal Bandwidth	Distance	
		160MHz-Km	220m	400MHz-Km	500m
		200MHz-Km	275m	500MHz-Km	550m
1000Base-LX/LHX/XD/ZX	Single-mode Fiber 9/125μm				
	Single-mode transceiver 1310nm		10, 30Km		
	Single-mode transceiver 1550nm		50Km		
IEEE 802.3u 100Base-FX	Multi-mode 50/125, 62.5/125μm				
	Multi-mode transceiver 1310nm 2Km				
	Single-mode 9/125, 10/125μm				
	Single-mode transceiver 1310nm 20Km				
1000Base-LX Single Fiber (BIDI SC)	Single-Mode *20Km		TX(Transmit)	1310nm	
			RX(Receive)	1550nm	
	Single-Mode *20Km		TX(Transmit)	1550nm	
			RX(Receive)	1310nm	

Table2-1

### 2-1-2-3. Switch Cascading in Topology

- **Takes the Delay Time into Account**

Theoretically, the switch partitions the collision domain for each port in switch cascading that you may up-link the switches unlimitedly. In practice, the network extension (cascading levels & overall diameter) must follow the constraint of the IEEE 802.3/802.3u/802.3z and other 802.1 series protocol specifications, in which the limitations are the timing requirement from physical signals defined by 802.3 series specification of Media Access Control (MAC) and PHY, and timer from some OSI layer 2 protocols such as 802.1d, 802.1q, LACP and so on.

The fiber, TP cables and devices' bit-time delay (round trip) are as follows:

1000Base-X TP, Fiber		100Base-TX TP		100Base-FX Fiber	
Round trip Delay: 4096		Round trip Delay: 512			
Cat. 5 TP Wire:	11.12/m	Cat. 5 TP Wire:	1.12/m	Fiber Cable:	1.0/m
Fiber Cable :	10.10/m	TP to fiber Converter: 56			
Bit Time unit : 1ns (1sec./1000 Mega bit)		Bit Time unit: 0.01 $\mu$ s (1sec./100 Mega bit)			

Table 2-2

Sum up all elements' bit-time delay and the overall bit-time delay of wires/devices must be within Round Trip Delay (bit times) in a half-duplex network segment (collision domain). For full-duplex operation, this will not be applied. You may use the TP-Fiber module to extend the TP node distance over fiber optic and provide the long haul connection.

- **Typical Network Topology in Deployment**

A hierarchical network with minimum levels of switch may reduce the timing delay between server and client station. Basically, with this approach, it will minimize the number of switches in any one path; will lower the possibility of network loop and will improve network efficiency. If more than two switches are connected in the same network, select one switch as Level 1 switch and connect all other switches to it at Level 2. Server/Host is recommended to connect to the Level 1 switch. This is general if no VLAN or other special requirements are applied.

Case1: All switch ports are in the same local area network. Every port can access each other (See Fig. 2-2).

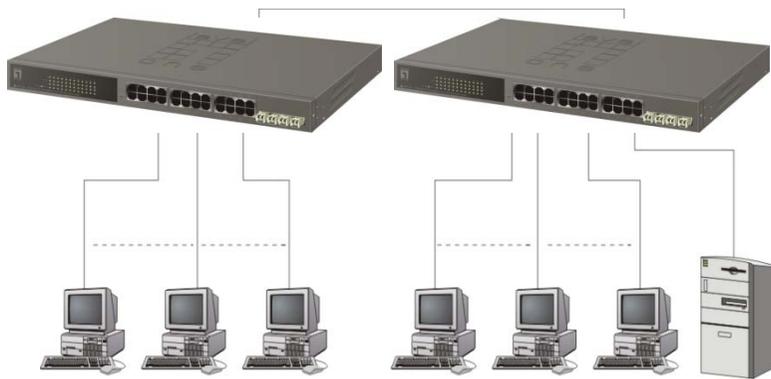


Fig. 2-2 No VLAN Configuration Diagram

If VLAN is enabled and configured, each node in the network that can communicate each other directly is bounded in the same VLAN area.

Here VLAN area is defined by what VLAN you are using. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical location. The following diagram shows how it works and what the difference they are.

Case2a: Port-based VLAN (See Fig.2-3).

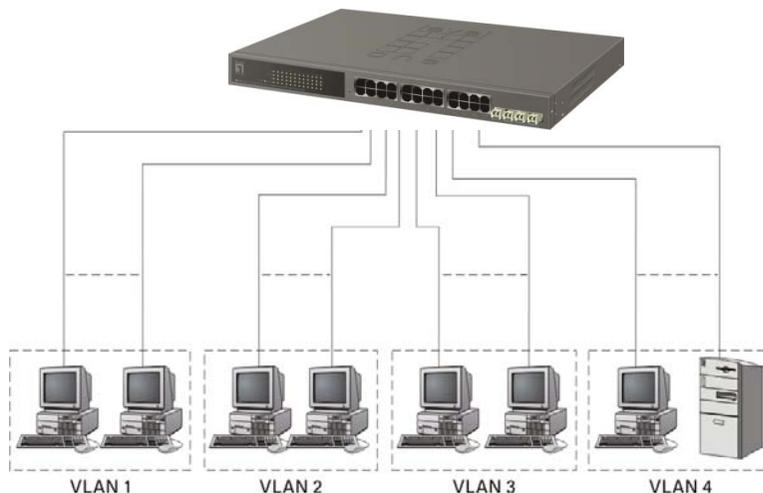


Fig. 2-3 Port-based VLAN Diagram

1. The same VLAN members could not be in different switches.
2. Every VLAN members could not access VLAN members each other.
3. The switch manager has to assign different names for each VLAN groups at one switch.

Case 2b: Port-based VLAN (See Fig.2-4).

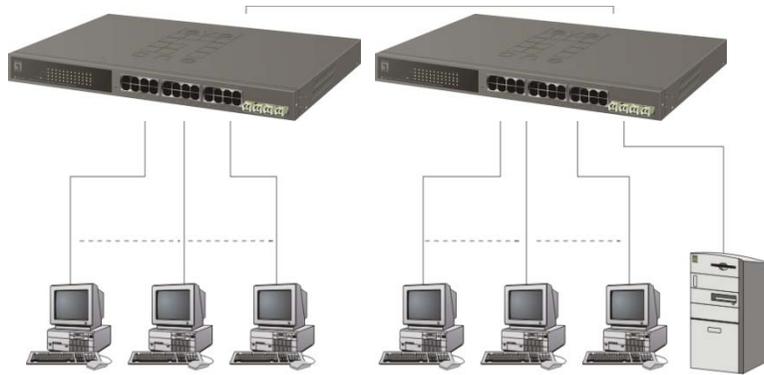


Fig. 2-4 Port-based VLAN Diagram

1. VLAN1 members could not access VLAN2, VLAN3 and VLAN4 members.
2. VLAN2 members could not access VLAN1 and VLAN3 members, but they could access VLAN4 members.
3. VLAN3 members could not access VLAN1, VLAN2 and VLAN4.
4. VLAN4 members could not access VLAN1 and VLAN3 members, but they could access VLAN2 members.

Case3a: The same VLAN members can be at different switches with the same VID (See Fig. 2-5).

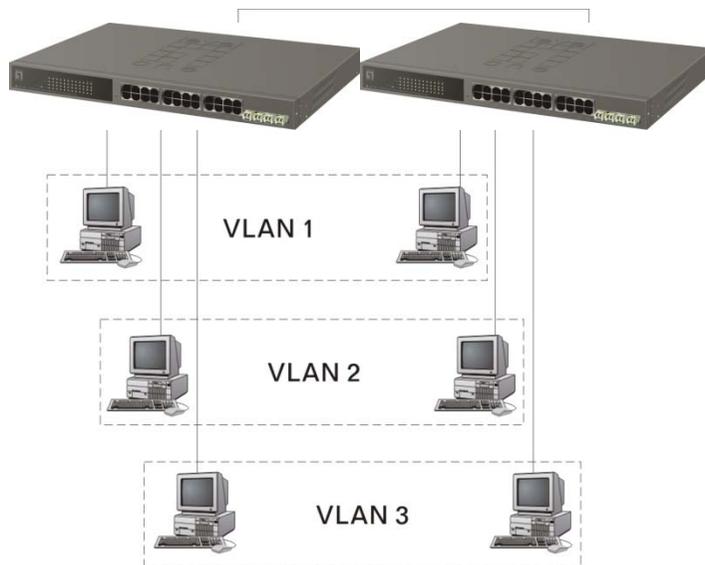


Fig. 2-5 Attribute-based VLAN Diagram

### 2-1-3. Configuring the Management Agent of **24-Port GbE Web Smart PoE Switch**

In the way of web, user is allowed to startup the switch management function. Users can use any one of them to monitor and configure the switch. You can touch them through the following procedures.

#### Section 2-1-3-1: Configuring Management Agent of 24-Port GbE Web Smart PoE Switch through Ethernet Port

##### 2-1-3-1. Configuring Management Agent of **24-Port GbE Web Smart PoE Switch** through Ethernet Port

There are two ways to configure and monitor the switch through the switch's Ethernet port. They are Web browser and SNMP manager. Web-based UI for the switch is an interface in a highly friendly way.

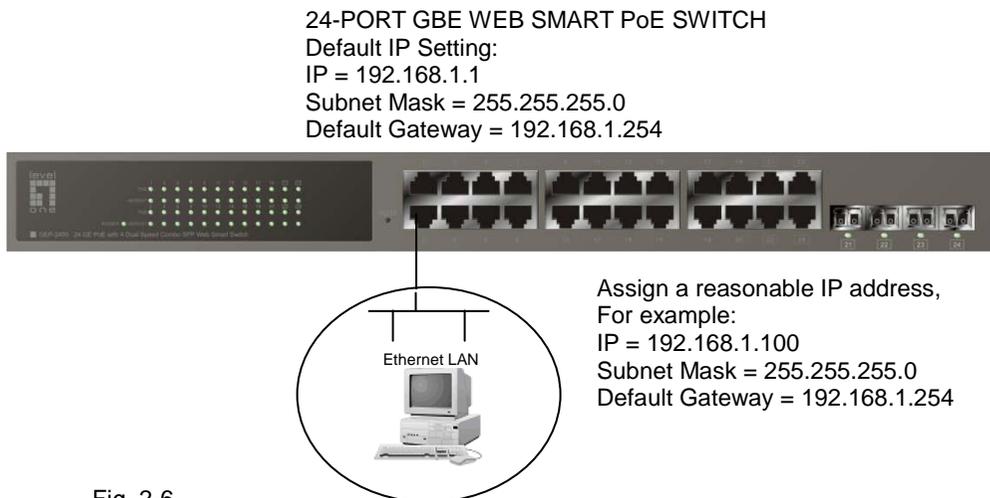


Fig. 2-6

#### • **Managing 24-Port GbE Web Smart PoE Switch through Ethernet Port**

Before you communicate with the switch, you have to finish first the configuration of the IP address or to know the IP address of the switch. Then, follow the procedures listed below.

1. Set up a physical path between the configured the switch and a PC by a qualified UTP Cat. 5 cable with RJ-45 connector.

Note: If PC directly connects to the switch, you have to setup the same subnet mask between them. But, subnet mask may be different for the PC in the remote site. Please refer to Fig. 2-6 about the 24-Port GbE Web Smart Switch default IP address information.

2. Run web browser and follow the menu. Please refer to Chapter 4.

## GEP-2450

Please enter password to login



The image shows a web login interface. At the top, it says "GEP-2450". Below that, it says "Please enter password to login". There is a text input field with the label "Password:" to its left. Below the input field is a blue button with the text "Apply".

Fig. 2-7 the Login Screen for Web

### 2-1-4. IP Address Assignment

For IP address configuration, there are three parameters needed to be filled in. They are IP address, Subnet Mask, Default Gateway and DNS.

IP address:

The address of the network device in the network is used for internetworking communication. Its address structure looks is shown in the Fig. 2-8. It is “classful” because it is split into predefined address classes or categories.

Each class has its own network range between the network identifier and host identifier in the 32 bits address. Each IP address comprises two parts: network identifier (address) and host identifier (address). The former indicates the network where the addressed host resides, and the latter indicates the individual host in the network which the address of host refers to. And the host identifier must be unique in the same LAN. Here the term of IP address we used is version 4, known as IPv4.

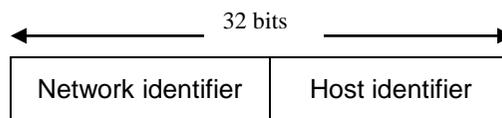
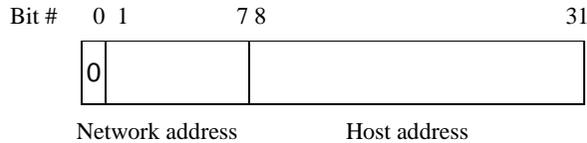


Fig. 2-8 IP address structure

With the classful addressing, it divides IP address into three classes, class A, class B and class C. The rest of IP addresses are for multicast and broadcast. The bit length of the network prefix is the same as that of the subnet mask and is denoted as IP address/X, for example, 192.168.1.0/24. Each class has its address range described below.

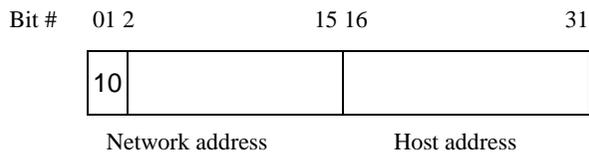
Class A:

Address is less than 126.255.255.255. There are a total of 126 networks can be defined because the address 0.0.0.0 is reserved for default route and 127.0.0.0/8 is reserved for loopback function.



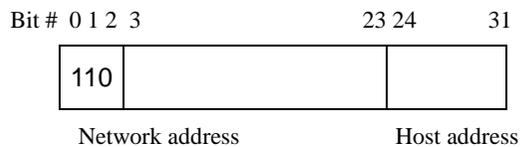
**Class B:**

IP address range between 128.0.0.0 and 191.255.255.255. Each class B network has a 16-bit network prefix followed 16-bit host address. There are 16,384 ( $2^{14}$ )/16 networks able to be defined with a maximum of 65534 ( $2^{16} - 2$ ) hosts per network.



**Class C:**

IP address range between 192.0.0.0 and 223.255.255.255. Each class C network has a 24-bit network prefix followed 8-bit host address. There are 2,097,152 ( $2^{21}$ )/24 networks able to be defined with a maximum of 254 ( $2^8 - 2$ ) hosts per network.



**Class D and E:**

Class D is a class with first 4 MSB (Most significance bit) set to 1-1-1-0 and is used for IP Multicast. See also RFC 1112. Class E is a class with first 4 MSB set to 1-1-1-1 and is used for IP broadcast.

According to IANA (Internet Assigned Numbers Authority), there are three specific IP address blocks reserved and able to be used for extending internal network. We call it Private IP address and list below:

Class A	10.0.0.0 --- 10.255.255.255
Class B	172.16.0.0 --- 172.31.255.255
Class C	192.168.0.0 --- 192.168.255.255

Please refer to RFC 1597 and RFC 1466 for more information.

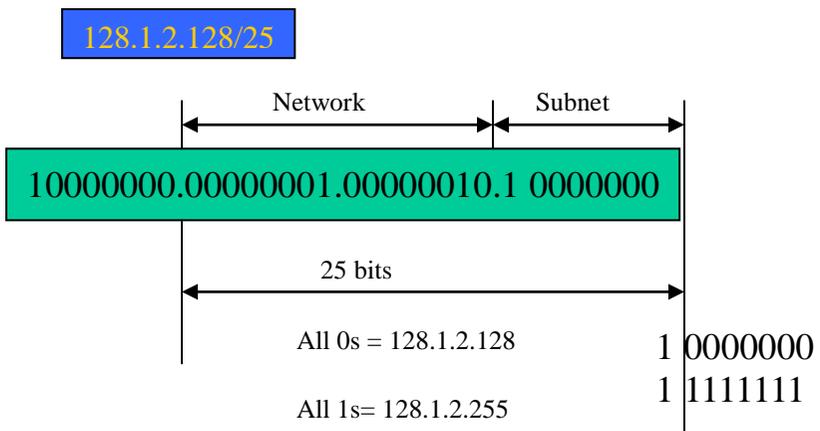
**Subnet mask:**

It means the sub-division of a class-based network or a CIDR block. The subnet is used to determine how to split an IP address to the network prefix and the host address in bitwise basis. It is designed to utilize IP address more efficiently and

ease to manage IP network.

For a class B network, 128.1.2.3, it may have a subnet mask 255.255.0.0 in default, in which the first two bytes is with all 1s. This means more than 60 thousands of nodes in flat IP address will be at the same network. It's too large to manage practically. Now if we divide it into smaller network by extending network prefix from 16 bits to, say 24 bits, that's using its third byte to subnet this class B network. Now it has a subnet mask 255.255.255.0, in which each bit of the first three bytes is 1. It's now clear that the first two bytes is used to identify the class B network, the third byte is used to identify the subnet within this class B network and, of course, the last byte is the host number.

Not all IP address is available in the sub-netted network. Two special addresses are reserved. They are the addresses with all zero's and all one's host number. For example, an IP address 128.1.2.128, what IP address reserved will be looked like? All 0s mean the network itself, and all 1s mean IP broadcast.



In this diagram, you can see the subnet mask with 25-bit long, 255.255.255.128, contains 126 members in the sub-netted network. Another is that the length of network prefix equals the number of the bit with 1s in that subnet mask. With this, you can easily count the number of IP addresses matched. The following table shows the result.

Prefix Length	No. of IP matched	No. of Addressable IP
/32	1	-
/31	2	-
/30	4	2
/29	8	6
/28	16	14
/27	32	30
/26	64	62
/25	128	126
/24	256	254
/23	512	510

/22	1024	1022
/21	2048	2046
/20	4096	4094
/19	8192	8190
/18	16384	16382
/17	32768	32766
/16	65536	65534

Table 2-3

According to the scheme above, a subnet mask 255.255.255.0 will partition a network with the class C. It means there will have a maximum of 254 effective nodes existed in this sub-netted network and is considered a physical network in an autonomous network. So it owns a network IP address which may looks like 168.1.2.0.

With the subnet mask, a bigger network can be cut into small pieces of network. If we want to have more than two independent networks in a worknet, a partition to the network must be performed. In this case, subnet mask must be applied.

For different network applications, the subnet mask may look like 255.255.255.240. This means it is a small network accommodating a maximum of 15 nodes in the network.

Default gateway:

For the routed packet, if the destination is not in the routing table, all the traffic is put into the device with the designated IP address, known as default router. Basically, it is a routing policy.

For assigning an IP address to the switch, you just have to check what the IP address of the network will be connected with the switch. Use the same network address and append your host address to it.

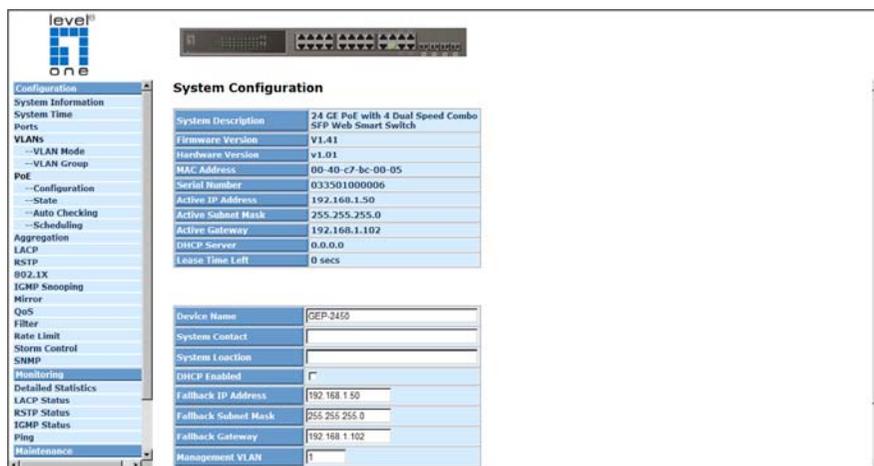


Fig. 2-9

First, IP Address: as shown in the Fig. 2-9, enter "192.168.1.1", for instance. For sure, an IP address such as 192.168.1.x must be set on your PC.

Second, Subnet Mask: as shown in the Fig. 2-9, enter "255.255.255.0". Any subnet mask such as 255.255.255.x is allowable in this case.

## 2-2. Typical Applications

The 24-Port GbE Web Smart Switch implements 24 Gigabit Ethernet TP ports with auto MDIX and four slots for the removable module supporting comprehensive fiber types of connection, including LC and BiDi-LC SFP modules. For more details on the specification of the switch, please refer to Appendix A.

The switch is suitable for the following applications.

- Central Site/Remote site application is used in carrier or ISP (See Fig. 2-10)
- Peer-to-peer application is used in two remote offices (See Fig. 2-11)
- Office network(See Fig. 2-12)

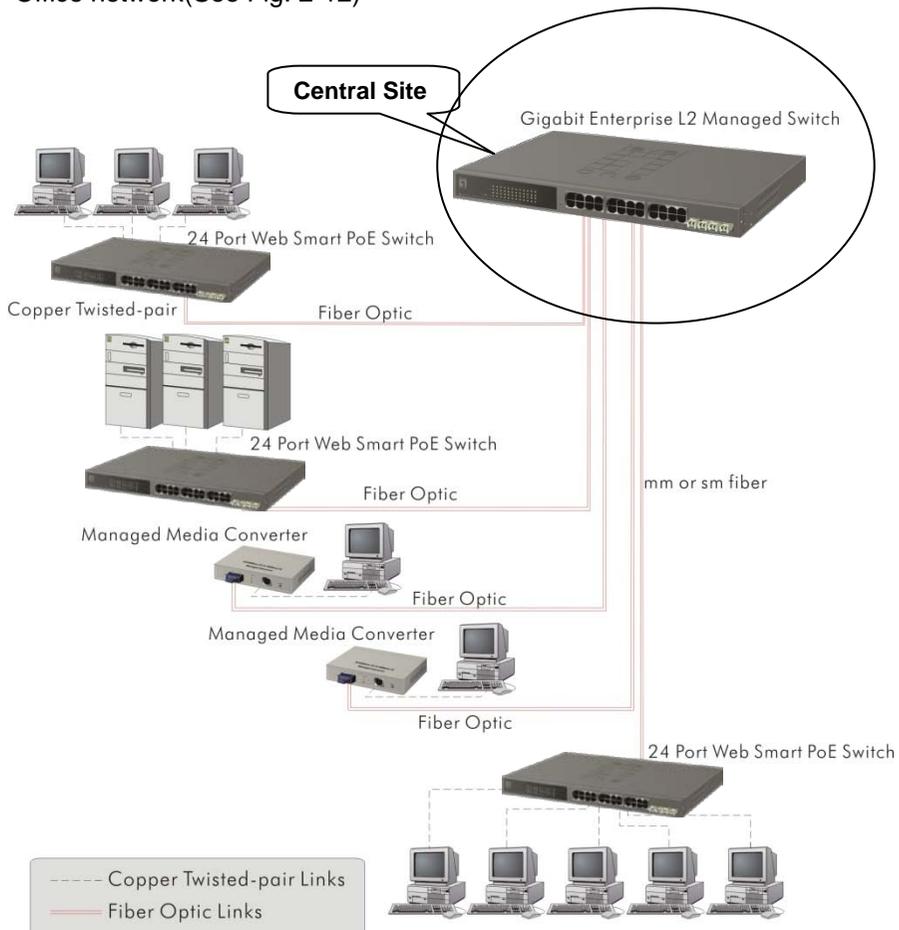


Fig. 2-10 Network Connection between Remote Site and Central Site

Fig. 2-10 is a system wide basic reference connection diagram. This diagram demonstrates how the switch connects with other network devices and hosts.

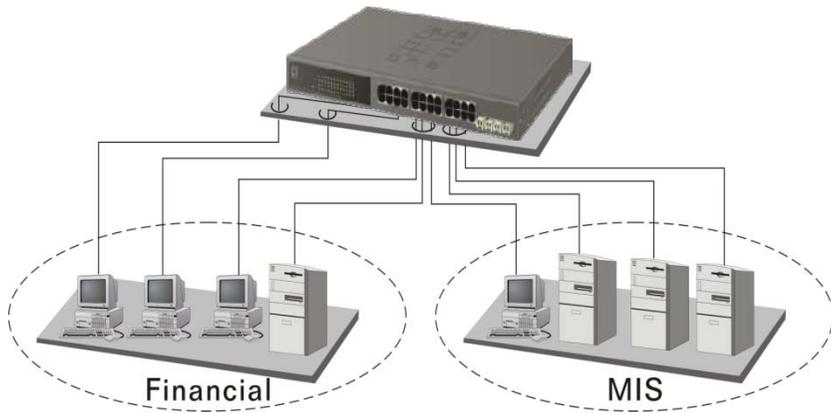


Fig. 2-11 Peer-to-peer Network Connection

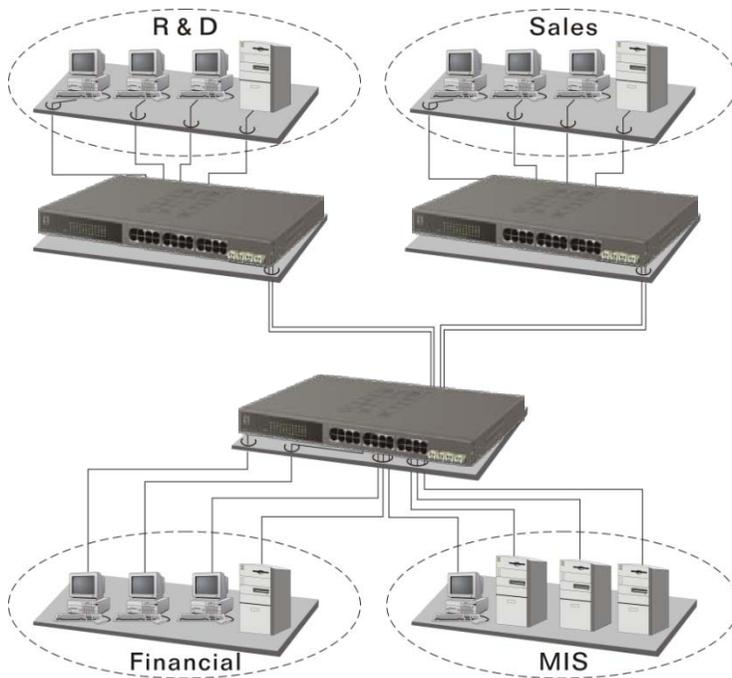


Fig. 2-12 Office Network Connection

# 3. Basic Concept and Management

This chapter will tell you the basic concept of features to manage this switch and how they work.

## 3-1. What's the Ethernet

Ethernet originated and was implemented at Xerox in Palo Alto, CA in 1973 and was successfully commercialized by Digital Equipment Corporation (DEC), Intel and Xerox (DIX) in 1980. In 1992, Grand Junction Networks unveiled a new high speed Ethernet with the same characteristic of the original Ethernet but operated at 100Mbps, called Fast Ethernet now. This means Fast Ethernet inherits the same frame format, CSMA/CD, software interface. In 1998, Gigabit Ethernet was rolled out and provided 1000Mbps. Now 10G/s Ethernet is under approving. Although these Ethernet have different speed, they still use the same basic functions. So they are compatible in software and can connect each other almost without limitation. The transmission media may be the only problem.

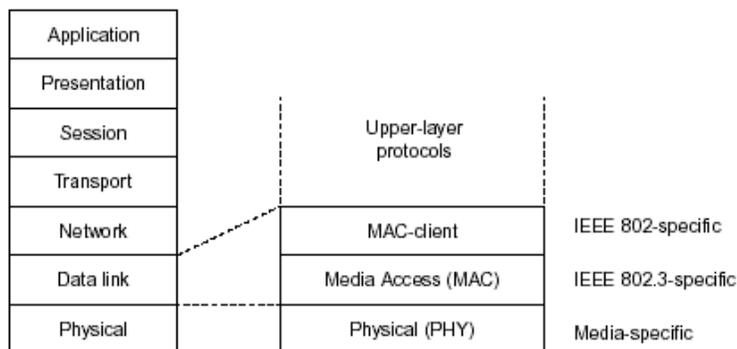
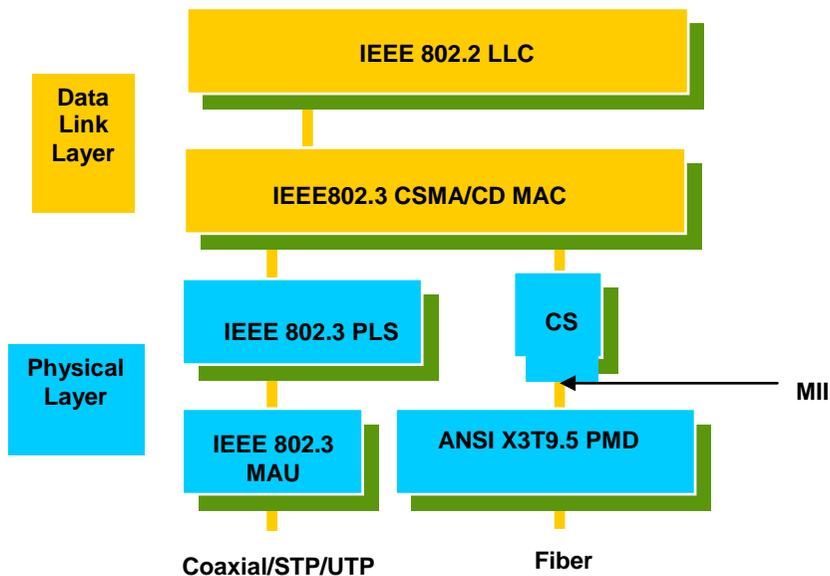


Fig. 3-1 IEEE 802.3 reference model vs. OSI reference mode

In Fig. 3-1, we can see that Ethernet locates at the Data Link layer and Physical layer and comprises three portions, including logical link control (LLC), media access control (MAC), and physical layer. The first two comprises Data link layer, which performs splitting data into frame for transmitting, receiving acknowledge frame, error checking and re-transmitting when not received correctly as well as provides an error-free channel upward to network layer.



This above diagram shows the Ethernet architecture, LLC sub-layer and MAC sub-layer, which are responded to the Data Link layer, and transceivers, which are responded to the Physical layer in OSI model. In this section, we are mainly describing the MAC sub-layer.

#### Logical Link Control (LLC)

Data link layer is composed of both the sub-layers of MAC and MAC-client. Here MAC client may be logical link control or bridge relay entity.

Logical link control supports the interface between the Ethernet MAC and upper layers in the protocol stack, usually Network layer, which is nothing to do with the nature of the LAN. So it can operate over other different LAN technology such as Token Ring, FDDI and so on. Likewise, for the interface to the MAC layer, LLC defines the services with the interface independent of the medium access technology and with some of the nature of the medium itself.

DSAP address	SSAP address	Control	Information
8 bits	8 bits	8 or 16 bits	M*8 bits

- DSAP address = Destination service access point address field
- SSAP address = Source service access point address field
- Control = Control field [16 bits for formats that include sequence numbering, and 8 bits for formats that do not (see 5.2)]
- Information = Information field
- \* = Multiplication
- M = An integer value equal to or greater than 0. (Upper bound of M is a function of the medium access control methodology used.)

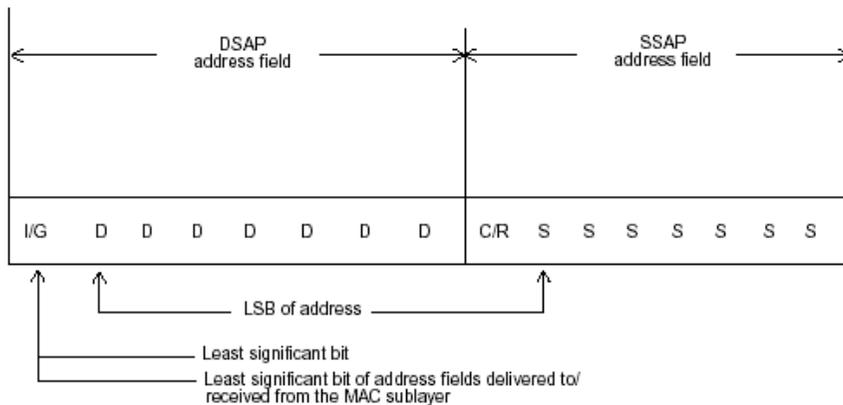
Table 3-1 LLC Format

The table 3-1 is the format of LLC PDU. It comprises four fields, DSAP, SSAP, Control and Information. The DSAP address field identifies the one or more service access points, in which the I/G bit indicates it is individual or group address. If all bit of DSAP is 1s, it's a global address. The SSAP address field identifies the specific services indicated by C/R bit (command or response). The DSAP and SSAP pair with some reserved values indicates some well-known services listed in the table below.

0xAAAA	SNAP
0xE0E0	Novell IPX
0xF0F0	NetBios
0xFEFE	IOS network layer PDU
0xFFFF	Novell IPX 802.3 RAW packet
0x4242	STP BPDU
0x0606	IP
0x9898	ARP

Table 3-2

LLC type 1 connectionless service, LLC type 2 connection-oriented service and LLC type 3 acknowledge connectionless service are three types of LLC frame for all classes of service. In Fig 3-2, it shows the format of Service Access Point (SAP). Please refer to IEEE802.2 for more details.



I/G = 0 Individual DSAP  
 I/G = 1 Group DSAP  
 C/R = 0 Command  
 C/R = 1 Response

XODDDDD DSAP address  
 XOSSSSS SSAP address

X1DDDDDD Reserved for ISO definition  
 X1SSSSSS Reserved for ISO definition

Fig. 3-2 SAP Format

## 3-2. Media Access Control (MAC)

### MAC Addressing

Because LAN is composed of many nodes, for the data exchanged among these nodes, each node must have its own unique address to identify who should send the data or should receive the data. In OSI model, each layer provides its own mean to identify the unique address in some form, for example, IP address in network layer.

The MAC is belonged to Data Link Layer (Layer 2), the address is defined to be a 48-bit long and locally unique address. Since this type of address is applied only to the Ethernet LAN media access control (MAC), they are referred to as MAC addresses.

The first three bytes are Organizational Unique Identifier (OUI) code assigned by IEEE. The last three bytes are the serial number assigned by the vendor of the network device. All these six bytes are stored in a non-volatile memory in the device. Their format is as the following table and normally written in the form as aa-bb-cc-dd-ee-ff, a 12 hexadecimal digits separated by hyphens, in which the aa-bb-cc is the OUI code and the dd-ee-ff is the serial number assigned by manufacturer.

Bit 47			bit 0		
1st byte	2nd byte	3rd byte	4th byte	5th byte	6th byte
OUI code			Serial number		

Table 3-3 Ethernet MAC address

The first bit of the first byte in the Destination address (DA) determines the address to be a Unicast (0) or Multicast frame (1), known as I/G bit indicating individual (0) or group (1). So the 48-bit address space is divided into two portions, Unicast and Multicast. The second bit is for global-unique (0) or locally-unique address. The former is assigned by the device manufacturer, and the later is usually assigned by the administrator. In practice, global-unique addresses are always applied.

A unicast address is identified with a single network interface. With this nature of MAC address, a frame transmitted can exactly be received by the target an interface the destination MAC points to.

A multicast address is identified with a group of network devices or network interfaces. In Ethernet, a many-to-many connectivity in the LANs is provided. It provides a mean to send a frame to many network devices at a time. When all bit of DA is 1s, it is a broadcast, which means all network device except the sender itself can receive the frame and response.

### Ethernet Frame Format

There are two major forms of Ethernet frame, type encapsulation and length encapsulation, both of which are categorized as four frame formats 802.3/802.2 SNAP, 802.3/802.2, Ethernet II and Netware 802.3 RAW. We will introduce the basic Ethernet frame format defined by the IEEE 802.3 standard required for all MAC implementations. It contains seven fields explained below.

PRE	SFD	DA	SA	Type/Length	Data	Pad bit if any	FCS
7	7	6	6	2		46-1500	4

Fig. 3-3 Ethernet frame structure

- **Preamble (PRE)** —The PRE is 7-byte long with alternating pattern of ones and zeros used to tell the receiving node that a frame is coming, and to synchronize the physical receiver with the incoming bit stream. The preamble pattern is:

10101010 10101010 10101010 10101010 10101010 10101010 10101010

- **Start-of-frame delimiter (SFD)** — The SFD is one-byte long with alternating pattern of ones and zeros, ending with two consecutive 1-bits. It immediately follows the preamble and uses the last two consecutive 1s bit to indicate that the next bit is the start of the data packet and the left-most bit in the left-most byte of the destination address. The SFD pattern is 10101011.
- **Destination address (DA)** — The DA field is used to identify which network device(s) should receive the packet. It is a unique address. Please see the section of MAC addressing.
- **Source addresses (SA)** — The SA field indicates the source node. The SA is always an individual address and the left-most bit in the SA field is always 0.
- **Length/Type** — This field indicates either the number of the data bytes contained in the data field of the frame, or the Ethernet type of data. If the value of first two bytes is less than or equal to 1500 in decimal, the number of bytes in the data field is equal to the Length/Type value, i.e. this field acts as Length indicator at this moment. When this field acts as Length, the frame has optional fields for 802.3/802.2 SNAP encapsulation, 802.3/802.2 encapsulation and Netware 802.3 RAW encapsulation. Each of them has different fields following the Length field.
- If the Length/Type value is greater than 1500, it means the Length/Type acts as Type. Different type value means the frames with different protocols running over Ethernet being sent or received.

For example,

0x0800	IP datagram
0x0806	ARP
0x0835	RARP
0x8137	IPX datagram
0x86DD	IPv6

- **Data** — Less than or equal to 1500 bytes and greater or equal to 46 bytes. If data is less than 46 bytes, the MAC will automatically extend the padding bits and have the payload be equal to 46 bytes. The length of data field must equal the value of the Length field when the Length/Type acts as Length.

- **Frame check sequence (FCS)** — This field contains a 32-bit cyclic redundancy check (CRC) value, and is a check sum computed with DA, SA, through the end of the data field with the following polynomial.

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

- It is created by the sending MAC and recalculated by the receiving MAC to check if the packet is damaged or not.

How does a MAC work?

The MAC sub-layer has two primary jobs to do:

1. *Receiving and transmitting data.* When receiving data, it parses frame to detect error; when transmitting data, it performs frame assembly.
2. *Performing Media access control.* It prepares the initiation jobs for a frame transmission and makes recovery from transmission failure.

### Frame transmission

As Ethernet adopted Carrier Sense Multiple Access with Collision Detect (CSMA/CD), it detects if there is any carrier signal from another network device running over the physical medium when a frame is ready for transmission. This is referred to as sensing carrier, also “Listen”. If there is signal on the medium, the MAC defers the traffic to avoid a transmission collision and waits for a random period of time, called backoff time, then sends the traffic again.

After the frame is assembled, when transmitting the frame, the preamble (PRE) bytes are inserted and sent first, then the next, Start of frame Delimiter (SFD), DA, SA and through the data field and FCS field in turn. The followings summarize what a MAC does before transmitting a frame.

1. MAC will assemble the frame. First, the preamble and Start-of-Frame delimiter will be put in the fields of PRE and SFD, followed DA, SA, tag ID if tagged VLAN is applied, Ethertype or the value of the data length, and payload data field, and finally put the FCS data in order into the responded fields.
2. Listen if there is any traffic running over the medium. If yes, wait.
3. If the medium is quiet, and no longer senses any carrier, the MAC waits for a period of time, i.e. inter-frame gap time to have the MAC ready with enough time and then start transmitting the frame.
4. During the transmission, MAC keeps monitoring the status of the medium. If no collision happens until the end of the frame, it transmits successfully. If there is a collision happened, the MAC will send the patterned jamming bit to guarantee the collision event propagated to all involved network devices, then wait for a random period of time, i.e. backoff time. When backoff time expires, the MAC goes back to the beginning state and attempts to transmit again. After a collision happens, MAC increases the transmission attempts. If the count of the transmission attempt reaches 16 times, the frame in MAC's queue will be discarded.

Ethernet MAC transmits frames in half-duplex and full-duplex ways. In half-duplex operation mode, the MAC can either transmit or receive frame at a moment, but cannot do both jobs at the same time.

As the transmission of a MAC frame with the half-duplex operation exists only in the same collision domain, the carrier signal needs to spend time to travel to reach the targeted device. For two most-distant devices in the same collision domain, when one sends the frame first, and the second sends the frame, in worst-case, just before the frame from the first device arrives. The collision happens and will be detected by the second device immediately. Because of the medium delay, this corrupted signal needs to spend some time to propagate back to the first device. The maximum time to detect a collision is approximately twice the signal propagation time between the two most-distant devices. This maximum time is traded-off by the collision recovery time and the diameter of the LAN.

In the original 802.3 specification, Ethernet operates in half duplex only. Under this condition, when in 10Mbps LAN, it's 2500 meters, in 100Mbps LAN, it's approximately 200 meters and in 1000Mbps, 200 meters. According to the theory, it should be 20 meters. But it's not practical, so the LAN diameter is kept by using to increase the minimum frame size with a variable-length non-data extension bit field which is removed at the receiving MAC. The following tables are the frame format suitable for 10M, 100M and 1000M Ethernet, and some parameter values that shall be applied to all of these three types of Ethernet.

Actually, the practice Gigabit Ethernet chips do not feature this so far. They all have their chips supported full-duplex mode only, as well as all network vendors' devices. So this criterion should not exist at the present time and in the future. The switch's Gigabit module supports only full-duplex mode.

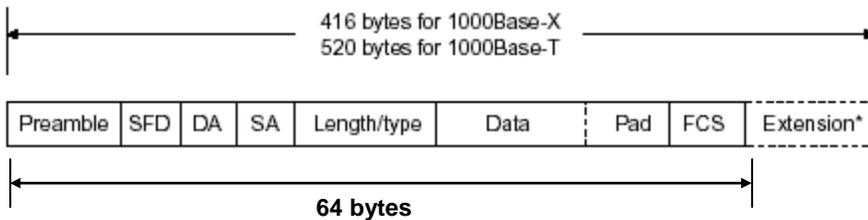
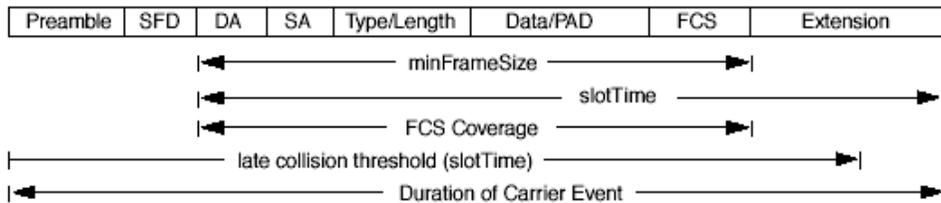


Fig. 3-4 Gigabit Ethernet Frame

Parameter value/LAN	10Base	100Base	1000Base
Max. collision domain DTE to DTE	100 meters	100 meters for UTP 412 meters for fiber	100 meters for UTP 316 meters for fiber
Max. collision domain with repeater	2500 meters	205 meters	200 meters
Slot time	512 bit times	512 bit times	512 bit times
Interframe Gap	9.6us	0.96us	0.096us
AttemptLimit	16	16	16
BackoffLimit	10	10	10
JamSize	32 bits	32 bits	32 bits
MaxFrameSize	1518	1518	1518
MinFrameSize	64	64	64
BurstLimit	Not applicable	Not applicable	65536 bits

Table 3-4 Ethernet parameters for half duplex mode



In full-duplex operation mode, both transmitting and receiving frames are processed simultaneously. This doubles the total bandwidth. Full duplex is much easier than half duplex because it does not involve media contention, collision, retransmission schedule, padding bits for short frame. The rest functions follow the specification of IEEE802.3. For example, it must meet the requirement of minimum inter-frame gap between successive frames and frame format the same as that in the half-duplex operation.

Because no collision will happen in full-duplex operation, for sure, there is no mechanism to tell all the involved devices. What will it be if receiving device is busy and a frame is coming at the same time? Can it use “backpressure” to tell the source device? A function flow control is introduced in the full-duplex operation.

### 3-3. Flow Control

Flow control is a mechanism to tell the source device stopping sending frame for a specified period of time designated by target device until the PAUSE time expires. This is accomplished by sending a PAUSE frame from target device to source device. When the target is not busy and the PAUSE time is expired, it will send another PAUSE frame with zero time-to-wait to source device. After the source device receives the PAUSE frame, it will again transmit frames immediately. PAUSE frame is identical in the form of the MAC frame with a pause-time value and with a special destination MAC address 01-80-C2-00-00-01. As per the specification, PAUSE operation can not be used to inhibit the transmission of MAC control frame.

Normally, in 10Mbps and 100Mbps Ethernet, only symmetric flow control is supported. However, some switches (e.g. 24-Port GbE Web Smart PoE Switch) support not only symmetric but asymmetric flow controls for the special application. In Gigabit Ethernet, both symmetric flow control and asymmetric flow control are supported. Asymmetric flow control only allows transmitting PAUSE frame in one way from one side, the other side is not but receipt-and-discard the flow control information. Symmetric flow control allows both two ports to transmit PASUE frames each other simultaneously.

#### Inter-frame Gap time

After the end of a transmission, if a network node is ready to transmit data out and if there is no carrier signal on the medium at that time, the device will wait for a period of time known as an inter-frame gap time to have the medium clear and stabilized as well as to have the jobs ready, such as adjusting buffer counter, updating counter and so on, in the receiver site. Once the inter-frame gap time expires after the de-assertion of carrier sense, the MAC transmits data. In IEEE802.3 specification, this is 96-bit time or more.

#### Collision

Collision happens only in half-duplex operation. When two or more network nodes transmit frames at approximately the same time, a collision always occurs and interferes with each other. This results the carrier signal distorted and un-discriminated. MAC can afford detecting, through the physical layer, the distortion of the carrier signal. When a collision is detected during a frame transmission, the transmission will not stop immediately but, instead, continues transmitting until the rest bits specified by jamSize are completely transmitted. This guarantees the duration of collision is enough to have all involved devices able to detect the collision. This is referred to as Jamming. After jamming pattern is sent, MAC stops transmitting the rest data queued in the buffer and waits for a random period of time, known as backoff time with the following formula. When backoff time expires, the device goes back to the state of attempting to transmit frame. The backoff time is determined by the formula below. When the times of collision is increased, the backoff time is getting long until the collision times excess 16. If this happens, the frame will be discarded and backoff time will also be reset.

$$0 \leq r < 2^k$$

where

$$k = \min(n, 10)$$

## Frame Reception

In essence, the frame reception is the same in both operations of half duplex and full duplex, except that full-duplex operation uses two buffers to transmit and receive the frame independently. The receiving node always “listens” if there is traffic running over the medium when it is not receiving a frame. When a frame destined for the target device comes, the receiver of the target device begins receiving the bit stream, and looks for the PRE (Preamble) pattern and Start-of-Frame Delimiter (SFD) that indicates the next bit is the starting point of the MAC frame until all bit of the frame is received.

For a received frame, the MAC will check:

1. If it is less than one slotTime in length, i.e. short packet, and if yes, it will be discarded by MAC because, by definition, the valid frame must be longer than the slotTime. If the length of the frame is less than one slotTime, it means there may be a collision happened somewhere or an interface malfunctioned in the LAN. When detecting the case, the MAC drops the packet and goes back to the ready state.
2. If the DA of the received frame exactly matches the physical address that the receiving MAC owns or the multicast address designated to recognize. If not, discards it and the MAC passes the frame to its client and goes back to the ready state.
3. If the frame is too long. If yes, throws it away and reports frame Too Long.
4. If the FCS of the received frame is valid. If not, for 10M and 100M Ethernet, discards the frame. For Gigabit Ethernet or higher speed Ethernet, MAC has to check one more field, i.e. extra bit field, if FCS is invalid. If there is any extra bits existed, which must meet the specification of IEEE802.3. When both FCS and extra bits are valid, the received frame will be accepted, otherwise discards the received frame and reports frameCheckError if no extra bits appended or alignmentError if extra bits appended.
5. If the length/type is valid. If not, discards the packet and reports lengthError.
6. If all five procedures above are ok, then the MAC treats the frame as good and de-assembles the frame.

What if a VLAN tagging is applied?

VLAN tagging is a 4-byte long data immediately following the MAC source address. When tagged VLAN is applied, the Ethernet frame structure will have a little change shown as follows.

Pre	SFD	DA	SA	VLAN type ID	Tag control information	Length/ type	Data	Pad	FCS	Ext
-----	-----	----	----	--------------	-------------------------	--------------	------	-----	-----	-----

Only two fields, VLAN ID and Tag control information are different in comparison with the basic Ethernet frame. The rest fields are the same.

The first two bytes is VLAN type ID with the value of 0x8100 indicating the received frame is tagged VLAN and the next two bytes are Tag Control Information

(TCI) used to provide user priority and VLAN ID, which are explained respectively in the following table.

<b>Bits 15-13</b>	User Priority 7-0, 0 is lowest priority
<b>Bit 12</b>	CFI (Canonical Format Indicator) 1: RIF field is present in the tag header 0: No RIF field is present
<b>Bits 11-0</b>	VID (VLAN Identifier) 0x000: Null VID. No VID is present and only user priority is present. 0x001: Default VID 0xFFFF: Reserved

Table 3-5

Note: RIF is used in Token Ring network to provide source routing and comprises two fields, Routing Control and Route Descriptor.

When MAC parses the received frame and finds a reserved special value 0x8100 at the location of the Length/Type field of the normal non-VLAN frame, it will interpret the received frame as a tagged VLAN frame. If this happens in a switch, the MAC will forward it, according to its priority and egress rule, to all the ports that is associated with that VID. If it happens in a network interface card, MAC will deprive of the tag header and process it in the same way as a basic normal frame. For a VLAN-enabled LAN, all involved devices must be equipped with VLAN optional function.

At operating speeds above 100 Mbps, the slotTime employed at slower speeds is inadequate to accommodate network topologies of the desired physical extent. Carrier Extension provides a means by which the slotTime can be increased to a sufficient value for the desired topologies, without increasing the minFrameSize parameter, as this would have deleterious effects. Nondata bits, referred to as extension bits, are appended to frames that are less than slotTime bits in length so that the resulting transmission is at least one slotTime in duration. Carrier Extension can be performed only if the underlying physical layer is capable of sending and receiving symbols that are readily distinguished from data symbols, as is the case in most physical layers that use a block encoding/decoding scheme.

The maximum length of the extension is equal to the quantity (slotTime - minFrameSize). The MAC continues to monitor the medium for collisions while it is transmitting extension bits, and it will treat any collision that occurs after the threshold (slotTime) as a late collision.

### 3-4. How does a switch work?

The switch is a layer 2 Ethernet Switch equipped with 24 Fast Ethernet ports and 2 optional modules which support Gigabit Ethernet or 100M Ethernet. Each port on it is an independent LAN segment and thus has 26 LAN segments and 26 collision domains, contrast to the traditional shared Ethernet HUB in which all ports share the same media and use the same collision domain and thus limit the bandwidth utilization. With switch's separated collision domain, it can extend the LAN diameter farther than the shared HUB does and highly improve the efficiency of the traffic transmission.

Due to the architecture, the switch can provide full-duplex operation to double the bandwidth per port and many other features, such as VLAN, bandwidth aggregation and so on, not able to be supported in a shared hub.

#### Terminology

##### Separate Access Domains:

As per the description in the section of "What's the Ethernet", Ethernet utilizes CSMA/CD to arbitrate who can transmit data to the station(s) attached in the LAN. When more than one station transmits data within the same slot time, the signals will collide, referred to as collision. The arbitrator will arbitrate who should gain the media. The arbitrator is a distributed mechanism in which all stations contend to gain the media. Please refer to "What's the Ethernet" for more details.

In Fig.3-5, assumed in half duplex, you will see some ports of the switch are linked to a shared HUB, which connects many hosts, and some ports just are individually linked to a single host. The hosts attached to a shared hub will be in the same collision domain, separated by the switch, and use CSMA/CD rule. For the host directly attached to the switch, because no other host(s) joins the traffic contention, hence it will not be affected by CSMA/CD. These LAN segments are separated in different access domains by the switch.

##### Micro-segmentation:

To have a port of the switch connected to a single host is referred to as micro-segmentation. It has the following interesting characteristics.

- There is no need the access contention (e.g.Collision). They have their own access domain. But, collision still could happen between the host and the switch port.
- When performing the full duplex, the collision vanishes.
- The host owns a dedicated bandwidth of the port.

The switch port can run at different speed, such as 10Mbps, 100Mbps or 1000Mbps. A shared hub cannot afford this.

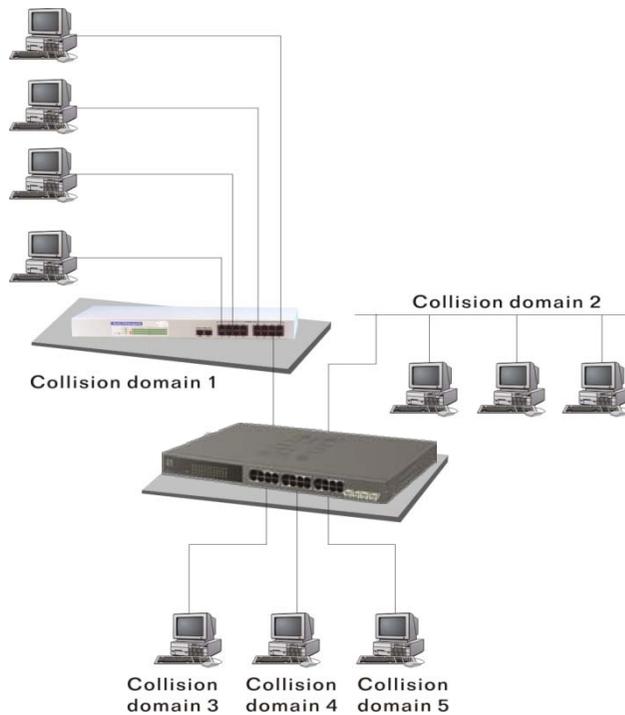


Fig.3-5 Collision Domain

#### Extended Distance Limitations:

The diameter of a half-duplex LAN segment is determined by its maximum propagation delay time. For example, in 10M LAN, the most distance of a LAN segment using yellow cable is 2500 meters and 185 meters when using coaxial cable. The switch with its per port per collision domain can extend the distance like a bridge does. And what's more, when operating in full-duplex mode, the distance can reach farther than half duplex because it is not limited by the maximum propagation delay time (512 bits time). If fiber media is applied, the distance can be up to tens of kilometers.

#### Traffic Aggregation:

Traffic aggregation is to aggregate the bandwidth of more than one port and treat it as a single port in the LAN. This single port possesses the features of a normal port but loading balance. This is a great feature for the port needing more bandwidth but cannot afford paying much cost for high bandwidth port.

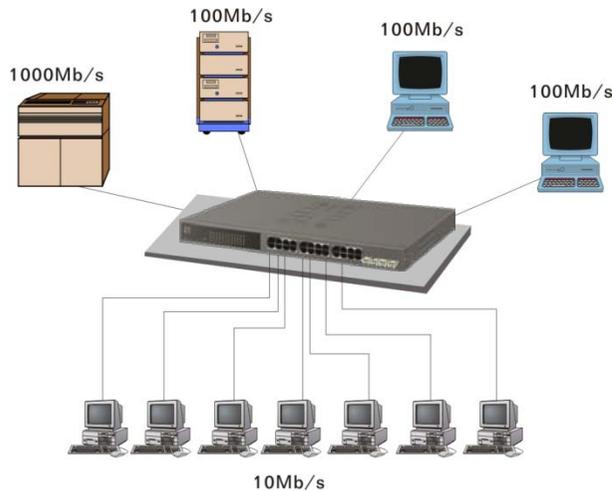


Fig. 3-6

How does a switch operate?

A Layer 2 switch uses some features of the Data Link layer in OSI model to forward the packet to the destination port(s). Here we introduce some important features of a switch and how they work.

#### MAC address table

When a packet is received on a port of switch, the switch first checks if the packet good or bad and extracts the source MAC address (SA) and destination MAC address (DA) to find 1) if SA is existed in the MAC address table, if no, puts it in the MAC address table, if yes, 2) looks up DA and its associated port to which the traffic is forwarded. If DA does not exist, have the packet broadcasted.

Due to the size of the MAC address limited, MAC address aging function is applied. When the MAC address has resided and keeps no update in the table for a long time, this means the traffic using that entry has yet come for a while. If this time period is more than the aging time, the entry will be marked invalid. The vacancy is now available for other new MAC.

Both learning and forwarding are the most important functions in a switch. Besides that, VLAN can be one of the rules to forward the packet. There are ingress rule and egress rule applied. The ingress rule is used to filter the incoming packet by VLAN ID and so on and to decide whether the packet is allowed to enter the switch or not. The egress rule is used to forward the packet to the proper port.

#### Mac address aging

There is a field in MAC address table used to put the entry's Age time which determines how long a MAC entry can reside in a switch. The age time is refreshed when a packet with that SA. Usually, the age time is programmable.

#### Transmission schedule

In most layer 2 switches, the QoS is supported. QoS in a switch must associate a transmission schedule to transmit the packet. This function is much to do with the priority level a packet has. With the given priority, the scheduler will do the proper action on it. The scheduler has many ways to implement, and different chips may support different schedule algorithms. Most common schedulers are:

FCFS: First Come First Service.

Strictly Priority: All High before Low.

Weighted Round Robin:

Set a weight figure to the packet with a priority level, say 5-7, and next, set another weight to the packet with a priority level, say 2-4 and so on. The WRR will transmit the packet with the weight. So the packet of each priority level can be allocated a fixed bandwidth.

#### Bandwidth rating

Bandwidth rating is the limitation set by administrator, and it can be applied to those with SLA. Bandwidth rating can be total bandwidth, types of service of a port with many steps. The switch supports by-port Ingress and Egress total bandwidth rate control capacity. The bandwidth rate resolution is 0.1 Mbps (100Kbps) and ranges from 0 to 100Mbps.

### 3-5. Virtual LAN

What is a VLAN?

It is a subset of a LAN. Before we discuss VLAN, we must understand what LAN is. In general, a LAN is composed of different physical network segments bridged by switches or bridges which attach to end stations in the same broadcast domain. The traffic can reach any station on the same LAN. Beyond this domain, the traffic cannot go without router's help. This also implies that a LAN is limited. If you need to communicate with the station outside the LAN, a router is needed which always lies on the edge of the LAN.

For a layer 2 VLAN, it assumes it is a logical subset of a physical LAN separated by specific rules such as tag, port, MAC address and so on. In other words, they can communicate with each other between separated small physical LANs within a LAN but can not be between any two separated logical LANs.

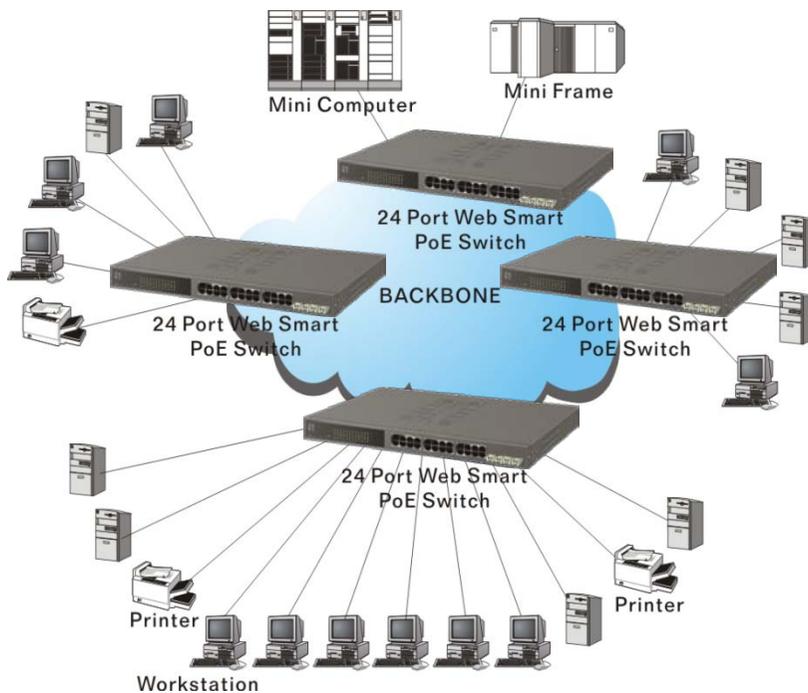


Fig. 3-7

In the figure above, all stations are within the same broadcast domain. For these stations, it is obviously that the traffic is getting congested while adding more stations on it. With the more and more users joining the LAN, broadcast traffic will rapidly decrease the performance of the network. Finally, the network may get down.

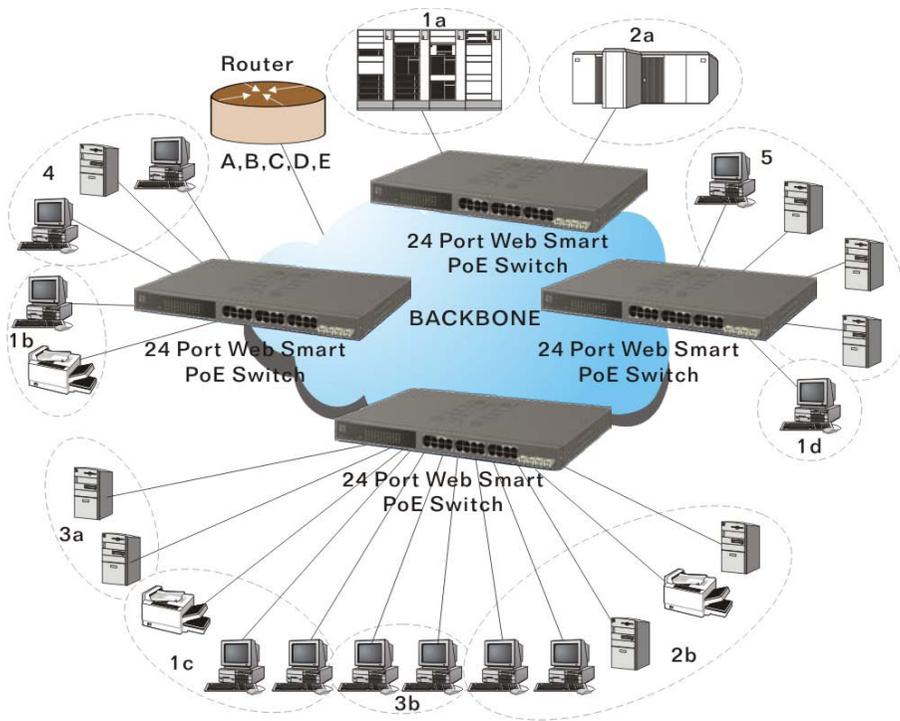


Fig. 3-8

Now we apply VLAN technology to configure the system shown as the figure above. We can partition the users into the different logical networks which have their own broadcast domain. The traffic will not disturb among these logical networks. The users 1x (x denotes a ~ d) are members of VLAN 1. Any traffic within VLAN 1 does not flow to VLAN 2 and others. This helps us configure the network easily according to the criteria needed, for example, financial, accounting, R&D and whatever you think it necessary. You can also easily move a user to a different location or join a new user somewhere in the building to VLAN. Without VLAN, it is very hard to do. Basically, VLAN can afford offering at least 3 benefits: move and change users, reduce broadcast traffic and increase performance, Security.

Besides, VLAN can highly reduce the traffic congestion and increase total performance because there are no more too many users in the same broadcast domain.

There are two types of VLAN applied. Most popular is port-based VLAN, tag-based VLAN

- Port-based VLAN

Some physical ports are configured as members of a VLAN. All stations attached on these ports can communicate with each other.

- Tag-based VLAN

It identifies the membership by VLAN ID, no matter where the packet comes from. It is also referred to as 802.1Q VLAN.

### Tagged Frame:

A frame, carrying a tag field following the source MAC address, is four bytes long and contains VLAN protocol ID and tag control information composed of user priority, Canonical Format Indicator (CFI) and optional VLAN identifier (VID). Normally, the maximal length of a tagged frame is 1522 bytes.

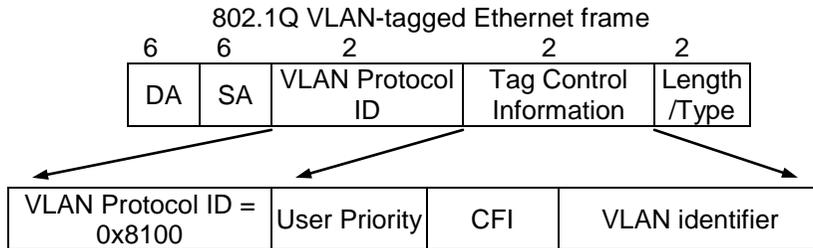


Fig.3-9 Tag Format

VLAN Protocol ID: 8100 is reserved for VLAN-tagged frame.

User Priority: 3 bits long. User priority is defined to 7 – 0. 0 is the lowest priority.

CFI: Canonical Format Indicator. 1 bit long. It is used to encapsulate a token ring packet to let it travel across the Ethernet. Usually, it is set to 0.

VLAN ID: 12 bits long. 0 means no VLAN ID is present. 1 means default VLAN, 4095 reserved.

### VLAN-tagged frame:

An Ethernet frame, carrying VLAN tag field, contains VLAN identification without the value of 0 and 4095, and priority information.

### Priority-tagged frame:

An Ethernet frame, carrying VLAN tag field, contains VLAN identification with the value of 0 and priority information.

### Untagged frame:

An Ethernet frame carries no VLAN tag information.

### VLAN Identifier:

Also referred to as VID. It is used to identify a member whether it belongs to the VLAN group with the VID. The assignable number is 1- 4094. If VID=0, the tagged frame is a priority packet. Both the value of 0 and 4095 also cannot be assigned in VLAN management.

### Port VLAN Identifier:

VLAN identifier of a port. It also can be referred to as PVID. When an untagged frame or a priority-tagged frame is received, the frame will be inserted the PVID of that port in the VLAN tag field. The frame with VID assigned by a port is called PVID. Each port can only be assigned a PVID. The default value for PVID is 1, the same as VID.

#### Ingress filtering:

The process to check a received packet and compare its VID to the VLAN membership of the ingress port. The ingress filtering can be set by per port. When receiving a packet, VLAN bridge examines if the VID in the frame's header presents.

If the VID of the received packet presents, the VID of the packet is used. And VLAN bridge will check its MAC address table to see if the destination ports are members of the same VLAN. If both are members of the tagged VLAN, then the packet will be forwarded.

If the packet is an untagged or a null tag packet, the ingress port's PVID is applied to the packet. VLAN bridge will then look up the MAC address table and determine to which ports the packet should be forwarded. Next, it will check to see if the destination ports belong to the same VLAN with that PVID. If the destination ports are members of the VLAN used by ingress port, the packet will be forwarded.

Note: VID can not be 0 or 4095.

#### Ingress Rule:

Each packet received by a VLAN-aware bridge will be classified to a VLAN. The classification rule is described as follows.

1. If the VID of the packet is null VID (VID=0) or this packet is an untagged packet:
  - a. If there are still some other ways (e.g. protocol, MAC address, application, IP-subnet, etc.) to classify the incoming packets beside port-based classification in implement and these approaches can offer non-zero VID, then, use the value of VID offered by other classifications for VLAN's classification.
  - b. If there is only port-based classification in implement or other classification approaches cannot offer non-zero VID for the incoming packets, then assign the PVID to the incoming packets as VID for the classification of the VLAN group.
2. If the VID is not a null VID (VID≠0), then use the value to classify the VLAN group.

#### Egress Rule:

An egress list is used to make the tagging and forwarding decision on an outgoing port. It specifies the VLANs whose packets can be transmitted out and specifies if the packet should be tagged or not. It can be configured for port's VLAN membership, and tagged or untagged for a transmitted packet. When a packet is transmitted out, the VLAN bridge checks the port's egress list. If the VLAN of the packet is on the egress list of the port on which the packet transmits out, the packet will be transmitted with the priority accordingly. If enabled, an egress port will transmit out a tagged packet if the port is connected to a 802.1Q-compliant device. If an egress port is connected to a non-802.1Q device or an end station, VLAN bridge must transmit out an untagged packet, i.e. the tag has been stripped off in an egress port. Egress rule can be set by per port.

#### Independent VLAN Learning (IVL):

It specifies the mode how to learn MAC address. For a specified VLAN, it will use an independent filtering database (FID) to learn or look up the membership information of the VLAN and decide where to go.

#### Shared VLAN Learning (SVL):

It specifies the mode how to learn MAC address. In this mode, some VLAN or all VLANs use the same filtering database storing the membership information of the VLAN to learn or look up the membership information of the VLAN. In 24-Port GbE Web Smart Switch, you can choose a VID for sharing filtering database in Shared VID field if you wish to use the existed filtering database. For a specified VLAN, when a MAC address is learned by a switch, VLAN will use this formation to make forwarding decision.

#### Filtering Database:

Referred to as FID. It can provide the information where the packet will be sent to. Filtering database will supply the outgoing port according to the request from forwarding process with VID and DA. When a packet is received, if it has a non-zero VID, then FID will offer the associated outgoing ports information to the packet.

In SVL, VLANs use the same Filtering Database. In IVL, VLANs use different FIDs. Any VID can be assigned to the same FID by administrator.

#### How does a Tagged VLAN work?

If the ingress filtering is enabled and when a packet is received, VLAN bridge will first check if the VID of the packet presents.

- 1). If the packet has a non-zero VID, VLAN bridge will apply this VID as the VLAN ID of the packet in the network.
- 2). For a packet with null tag or no VLAN tag, if VLAN bridge provides rules to decide its VID, then apply this VID to the packet.

If VLAN bridge does not support any rule for VID, then apply the PVID of the port to the packet which came from that port. VLAN bridge checks to see if the ingress port and the received packet are on the same VLAN. If not, drops it. If yes, forwards it to the associated ports. Meanwhile, this VLAN must be applied to the egress port, or the packet will be dropped.

If ingress filtering is disabled, VLAN bridge will only check the MAC address table to see if the destination VLAN exists. If VLAN does not exist, then drop the packet, and if both DA and VLAN do not exist, forwards the packet. If just knows VLAN existed, then floods the packet to all the ports the VLAN covers.

If we plan to deploy four VLANs in an office and use a switch to partition them, we should check which ports belong to which VLAN first. Assuming a 24-port switch is applied.

<b>Name</b>	<b>VID</b>	<b>Port Members</b>
Marketing	2	1,2,3,4,5
Service	3	6,7,20,21,22
Sales	4	8,9,10,11,12,13,14,15,16
Administration	1	17,18,19,23,24

Table 3-6

Next, assigns IP address to each VLAN. Usually, we use 10.x.x.x as internal IP block. Because there are total four VLANs in the network, we must assign 4 IP blocks to each of them.

<b>Name</b>	<b>VID</b>	<b>Network Address</b>
Marketing	2	10.1.2.0/24
Service	3	10.1.3.0/24
Sales	4	10.1.4.0/24
Administration	1	10.1.1.0/24

Table 3-7

Here we apply the subnet mask 255.255.255, and each VLAN is capable of supporting 254 nodes.

### 3-6. Link Aggregation

Basically, Link Aggregation is to aggregate the bandwidth of more than one port to an assigned logical link. This highly increases total bandwidth to the targeted device. There is more than one Link Aggregation technology in many vendors' switch products already, which may cause the problem of interoperability. This is the reason why now we have 802.3ad Link Aggregation Control Protocol (LACP).

Why 802.3ad (LACP)?

Network is varying. For example, if a port malfunctioned or unplugged accidentally in a static trunk port, administrator has to reconfigure it, or the network will get trouble. Therefore, offering a tool with automatic recovery capability is necessary for an administrator. LACP is a protocol that allows a switch able to know whether its partner has the capability to co-setup a trunk between them.

Usually, if administrator wishes to increase the bandwidth of a specific link, he may:

1. Buy new network equipments with higher throughput, or
2. Aggregate the bandwidth of more than one port to a logical link.

If the item 1 is the case, you will pay much more cost beyond your budget, and the solution caused by the limitation of hardware performance may not be scalable.

If the item 2 is the case, now you do not have to pay much more extra cost and can keep flexible according to the demand of bandwidth because all equipments are there already. And what's more, you can avoid worrying about the interoperability issue. Applying LACP in your network, you will not only gain benefits below to improve the performance of your network but also have these investments usable to future new products.

1. Public standardized specification
2. No interoperability issue
3. No change to IEEE 802.3 frame format, no change in software and management.
4. Increased bandwidth and availability
5. Load sharing and redundancy
6. Automatic configuration
7. Rapid configuration and reconfiguration
8. Deterministic behavior
9. Low risk of duplication or mis-ordering
10. Support existing IEEE 802.3 MAC Clients
11. Backwards compatibility with aggregation-unaware devices

There are also some constraints when applying LACP.

1. LACP does not support inter-switch bandwidth aggregation.
2. The ports aggregated must operate in full-duplex mode.
3. The ports in the same Link Aggregation Group must have the same speed, for example, all with 100Mbps or all 1000Mbps. You cannot aggregate a 1000Mbps and two 100Mbps for a 1.2Gbps trunk port.

## Terminology

### Link Aggregation:

It is a method to have multiple physical links with the same media and speed bundled to be a logical link forming a Link Aggregation Group with a group ID. With the viewpoint of MAC client, each Link Aggregation Group is an independent link.

There are three cases of link used in the network, which are switch to switch, switch to station and station to station. Here station may be a host or a router.

Link Aggregation, called port trunking sometimes, has two types of link configuration, including static port trunk and dynamic port trunk.

- **Static Port Trunk:**

When physical links are changed, administrator needs to manually configure the switches one by one.

- **Dynamic Port Trunk:**

When physical links are changed, LACP takes over and automatically reconfigure. Administrator does not have to do anything and may see the trap message of LACP changed in NMS.

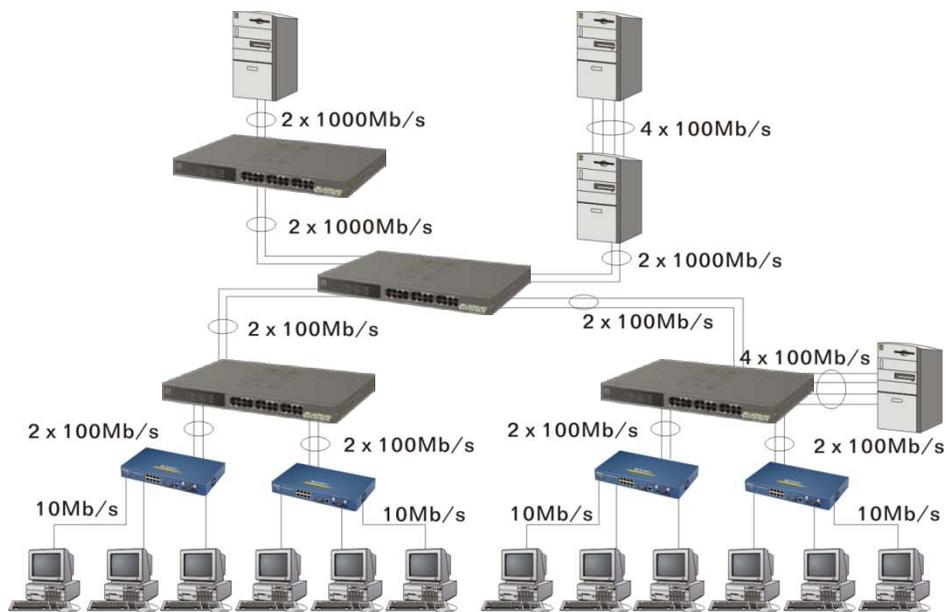


Fig. 3-10 Example of Link Aggregation Application

# 4. Operation of Web-based Management

This chapter would introduce how to manage your Web Smart Switch and how to configure the 10/100/1000Mbps TP Ports and Gigabit TP/(100/1000M) SFP Fiber dual media ports on the switch via web user interfaces. Web Smart Switch provides 20 fixed Gigabit Ethernet TP ports and 4 optional Gigabit dual media ports. With this facility, you can easily access and monitor the status like MIBs, port activity, and multicast traffic through any ports on the switch.

The default values of 24-Port GbE Web Smart PoE Switch are listed in the table below:

<b>IP Address</b>	192.168.1.1
<b>Subnet Mask</b>	255.255.255.0
<b>Default Gateway</b>	192.168.1.254
<b>Password</b>	admin

Table 4-1

When the configuration of your Web Smart PoE Switch is finished, you can browse it by the IP address you set up. For instance, type <http://192.168.1.1> in the address row in a browser, then the following screen (see Fig.4-1) would show up and ask for your password input for login and access authentication. The default password is “admin”. For the first time access, please enter the default password, and click **<Apply>** button. The login process now would be completed.

Web Smart PoE Switch supports a simplified user management function which allows only one administrator to configure the switch at one time.

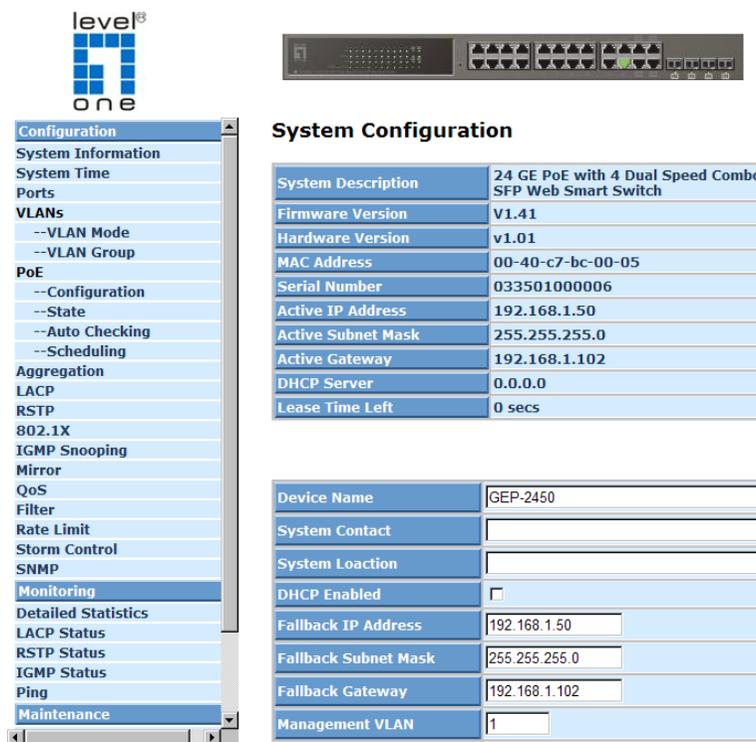
To optimize the display effect, we recommend Microsoft IE and 1024x768 display resolution.



Fig. 4-1

## 4-1. Web Management Home Overview

After login, System Information would be displayed as Fig. 4-2 illustrated. This page lists default values and shows you the basic information of the switch, including “System Information”, “Ports”, “VLANs”, “PoE”, “Aggregation”, “LACP”, “RSTP”, “802.1X”, “IGMP Snooping”, “Mirror”, “QoS”, “Filter”, “Rate Limit”, “Storm Control”, “SNMP”, “Monitoring” and “Maintenance”. With this information, you will know the software version, MAC address, ports available and so on. It would be helpful while malfunction occurred. For more details, please refer to Section 4-4-1.



The screenshot displays the Level One web management interface. At the top left is the Level One logo. Below it is a navigation menu with categories: Configuration, System Information, System Time, Ports, VLANs, PoE, Aggregation, LACP, RSTP, 802.1X, IGMP Snooping, Mirror, QoS, Filter, Rate Limit, Storm Control, SNMP, Monitoring, Detailed Statistics, and Maintenance. The 'System Configuration' page is active, showing a table of system details and a form for configuration.

**System Configuration**

System Description	24 GE PoE with 4 Dual Speed Combo SFP Web Smart Switch
Firmware Version	V1.41
Hardware Version	v1.01
MAC Address	00-40-c7-bc-00-05
Serial Number	033501000006
Active IP Address	192.168.1.50
Active Subnet Mask	255.255.255.0
Active Gateway	192.168.1.102
DHCP Server	0.0.0.0
Lease Time Left	0 secs

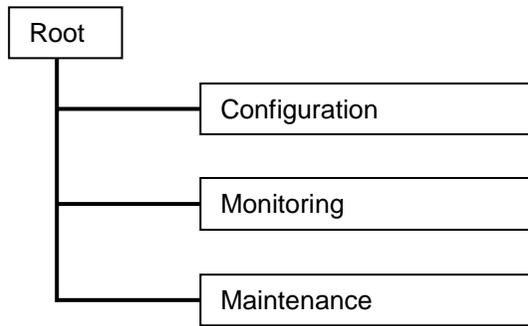
  

Device Name	GEP-2450
System Contact	
System Location	
DHCP Enabled	<input type="checkbox"/>
Fallback IP Address	192.168.1.50
Fallback Subnet Mask	255.255.255.0
Fallback Gateway	192.168.1.102
Management VLAN	1

Fig. 4-2

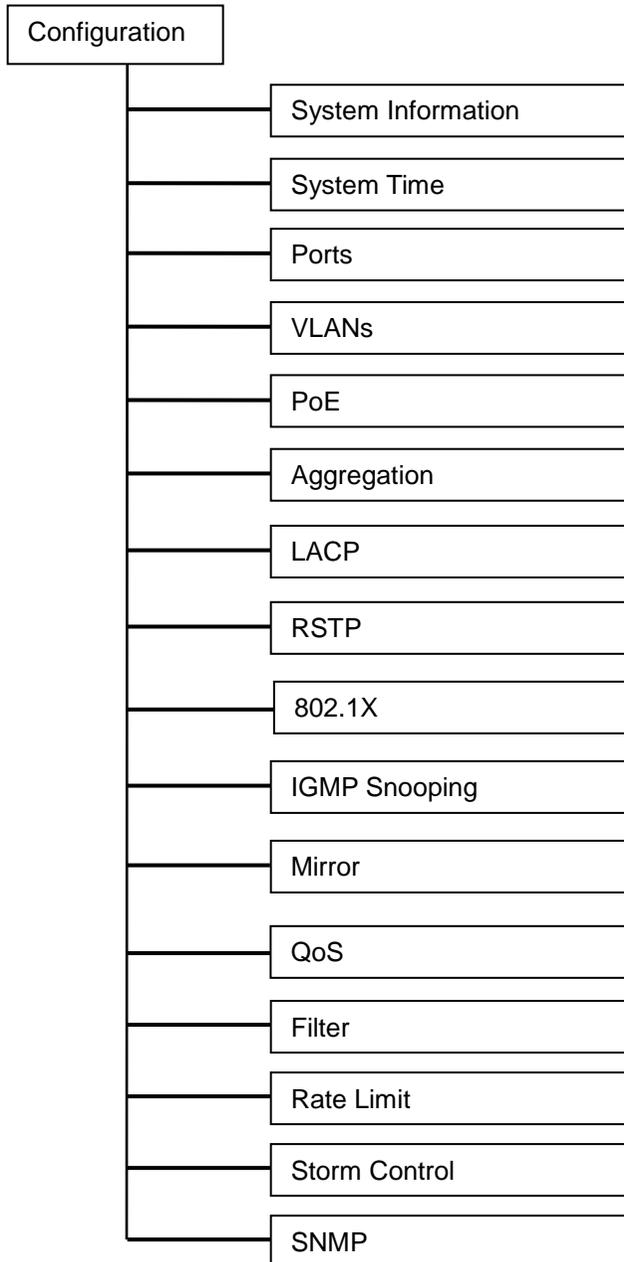
### • The Information of Page Layout

- On the top part of the information page, it shows the front panel of the switch. Linked ports will be displayed in green color, and linked-off ones will be in black. For the optional modules, the slots with no module will only show covered plates, the other slots with installed modules would present modules. The images of modules would depend on the ones you insert. Vice versa, if ports are disconnected, they will show just in black.
- On the left side, the main menu tree for web is listed in the page. According to the function name in boldface, all functions can be divided into three parts, including “Configuration”, “Monitoring” and “Maintenance”. The functions of each folder are described in its corresponded section respectively. As to the function names in normal type are the sub-functions. When clicking it, the function is performed. The following list is the main function tree for web user interface.



## 4-2. Configuration

Configuration includes the following functions: System Configuration, Ports Configuration, VLANs Configuration, PoE Configuration, Aggregation, LACP, RSTP, 802.1X, IGMP Snooping, Mirror, QoS, Filter, Rate Limit, Storm Control and SNMP.



## 4-2-1. System Information

System Information is one of the most important functions. Without a proper setting, network administrator would not be able to manage the device. The switch supports manual IP address setting.

### System Configuration

System Description	24 GE PoE with 4 Dual Speed Combo SFP Web Smart Switch
Firmware Version	V1.41
Hardware Version	v1.01
MAC Address	00-40-c7-bc-00-05
Serial Number	033501000006
Active IP Address	192.168.1.50
Active Subnet Mask	255.255.255.0
Active Gateway	192.168.1.102
DHCP Server	0.0.0.0
Lease Time Left	0 secs

Device Name	GEP-2450
System Contact	
System Location	
DHCP Enabled	<input type="checkbox"/>
Fallback IP Address	192.168.1.50
Fallback Subnet Mask	255.255.255.0
Fallback Gateway	192.168.1.102
Management VLAN	1
Password	•••••
Inactivity Timeout (0, 60-10000 Secs)	0

Fig. 4-3

#### **Function name:**

System Configuration

#### **Function description:**

Show system description, firmware version, hardware version, MAC address, serial number, active IP address, active subnet mask, active gateway, DHCP server and Lease time left.

Set device name, DHCP enable, fallback IP address, fallback subnet mask, fallback gateway, management VLAN, password and inactivity timeout.

#### **Parameter description:**

System Description:

The simple description of this switch.

Firmware Version:

The firmware version of this switch.

Hardware Version:

The hardware version of this switch.

MAC Address:

It is the Ethernet MAC address of the management agent in this switch.

Serial Number:

The serial number is assigned by the manufacturer.

Active IP Address:

Show the active IP address of this switch.

Active Subnet Mask:

Show the active subnet mask of this switch.

Active Gateway:

Show the active gateway of this switch.

DHCP Server:

Show the IP address of the DHCP server.

Default: 0.0.0.0

Lease Time Left:

Show the lease time left of DHCP client.

Device Name:

Set a special name for this switch. Up to 16 characters are allowed in this parameter. Any alphanumeric character and null are acceptable.

Default: Giga Switch

DHCP Enabled:

Enable DHCP snooping, Just tick the check box () to enable it.

Default: disable

Fallback IP Address:

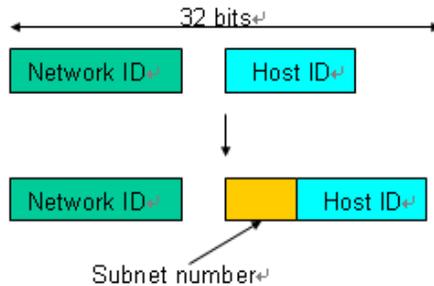
Users can configure the IP settings and fill in new values. Then, click **<Apply>** button to update.

Default: 192.168.1.1

Fallback Subnet Mask:

Subnet mask is made for the purpose to get more network address because any IP device in a network must own its IP address, composed of Network address and Host address, otherwise can't communicate with other devices each other. But unfortunately, the network classes A, B, and C are all too large to fit for almost all networks, hence, subnet mask is introduced to solve this problem. Subnet mask uses some bits from host address and makes an IP address looked Network address, Subnet mask number and host address. It is shown in the following figure. This reduces the total IP number of a network able to support, by the amount

of 2 power of the bit number of subnet number ( $2^{\text{(bit number of subnet number)}}$ ).



Subnet mask is used to set the subnet mask value, which should be the same value as that of the other devices resided in the same network it attaches.

For more information, please also see the Section 2-1-4 "IP Address Assignment" in this manual.

Default: 255.255.255.0

Fallback Gateway:

Set an IP address for a gateway to handle those packets that do not meet the routing rules predefined in the device. If a packet does not meet the criteria for other pre-defined path, it must be forwarded to a default router on a default path. This means any packet with undefined IP address in the routing table will be sent to this device unconditionally.

Default: 192.168.1.254

Management VLAN:

Show the management VLAN number.

Password:

Set a password for this switch. Up to 16 characters are allowed in this parameter. Any alphanumeric character is acceptable.

Default: admin

Inactivity Timeout(secs):

Set the auto-logout timer. The valid value is 0 ~ 60 in the unit of minute and a decimal point is not allowed. The value 0 means auto-logout timer is disabled.

Default: 0

## 4-2-2. System Time

### **Function name:**

Enable/Disable NTP function

### **System Time**

State	Disable ▾
NTP Server	0.0.0.0
Time Zone	GMT+8:00 ▾
Current Time	

Apply

Refresh

## 4-2-3. Ports

### Function name:

Port Configuration

### Function description:

Port Configuration is applied for the settings of the ports on the switch. By this function, you can set or reset the values for Mode and Flow Control. Others you could set the power saving mode for switch power consumption.

### Port Configuration

Enable Jumbo Frames   
 (Jumbo Frame support up to 9600 bytes.)  
 Power Saving

### TP Ports

Port	Link	Mode	Flow Control	Flow Control Status	Port Description
1	1000FDX	Auto Speed	<input type="checkbox"/>	disabled	
2	Down	Auto Speed	<input type="checkbox"/>	disabled	
3	Down	Auto Speed	<input type="checkbox"/>	disabled	
4	Down	Auto Speed	<input type="checkbox"/>	disabled	
5	Down	Auto Speed	<input type="checkbox"/>	disabled	
6	Down	Auto Speed	<input type="checkbox"/>	disabled	
7	Down	Auto Speed	<input type="checkbox"/>	disabled	
8	Down	Auto Speed	<input type="checkbox"/>	disabled	
9	Down	Auto Speed	<input type="checkbox"/>	disabled	
10	Down	Auto Speed	<input type="checkbox"/>	disabled	
11	Down	Auto Speed	<input type="checkbox"/>	disabled	
12	Down	Auto Speed	<input type="checkbox"/>	disabled	
13	Down	Auto Speed	<input type="checkbox"/>	disabled	
14	Down	Auto Speed	<input type="checkbox"/>	disabled	
15	Down	Auto Speed	<input type="checkbox"/>	disabled	
16	Down	Auto Speed	<input type="checkbox"/>	disabled	
17	Down	Auto Speed	<input type="checkbox"/>	disabled	
18	Down	Auto Speed	<input type="checkbox"/>	disabled	
19	Down	Auto Speed	<input type="checkbox"/>	disabled	
20	Down	Auto Speed	<input type="checkbox"/>	disabled	
21	Down	Auto Speed	<input type="checkbox"/>	disabled	
22	Down	Auto Speed	<input type="checkbox"/>	disabled	
23	Down	Auto Speed	<input type="checkbox"/>	disabled	
24	Down	Auto Speed	<input type="checkbox"/>	disabled	

### Fiber Ports

Port	Link	Mode	Flow Control	Flow Control Status
21	Down	Auto Speed	<input type="checkbox"/>	disabled
22	Down	Auto Speed	<input type="checkbox"/>	disabled
23	Down	Auto Speed	<input type="checkbox"/>	disabled
24	Down	Auto Speed	<input type="checkbox"/>	disabled

Drop frames after excessive collisions   
 (Use in Half Duplex flow control environment.)

Fig. 4-4 Port Configuration

**Parameter description:**

Enable Jumbo Frames:

This function support jumbo frames of up to 12.2KB, Just tick the check box () to enable it.

Default: disable

Perfect Reach/Power Saving Mode:

This function supports Power Saving and perfect Reach, Just select with the Full/ Link-up/ Link-down/ Disable

Default: disable

Power Saving:

The parameter will enable or disable to verify switches have the ability to consider the length of any Ethernet cable connected for adjustment of power usage accordingly. Shorter lengths require less power. link-down mode removes power for each port that does not have a device attached.

**Default: Disable.**

Link:

Show link status of this port.

Mode:

Set the speed and duplex of the port. If the media is 1Gbps fiber, there are three modes to choose: Auto Speed, 1000 Full and Disable. If the media is TP, the Speed/Duplex is comprised of the combination of speed mode, 10/100/1000Mbps, and duplex mode, full duplex and half duplex. The following table summarized the function the media supports.

Media type	NWay	Speed	Duplex
1000M TP	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1000M Fiber	ON/OFF	1000M	Full

In Auto Speed mode, no default value. In Forced mode, default value depends on your setting.

Flow Control:

You can Just tick the check box () to enable flow control. If flow control is set Enable, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. When it is set Disable, there will be no flow control in the port. It drops the packet if too much to handle.

Default: Disable

Flow Control status:

To display the Flow control status.

Port Description:

To type the port description for port identity and purpose

## 4-2-4. VLAN Mode Configuration

Web Smart Switch supports Port-based VLAN and Tag-based VLAN (802.1q). Its VLAN mode supports 24 active VLANs and the available VLAN ID range is from 1~4094. VLAN configuration is used to divide a LAN into smaller ones. With proper configuration, you can gain not only improved security and increased performance, but also save a lot of VLAN management effort.

### **Function name:**

VLAN Mode Setting

### **Function description:**

The VLAN Mode Selection function includes four modes: Port-based, Tag-based, Metro mode or Disable, you can choose one of them by pulling down list and pressing the **<Downward>** arrow key. Then, click **<Apply>** button, the settings will take affect immediately.

## VLAN Mode

VLAN Mode	Tag-based ▾
Double Tag	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>Apply</b>	

Fig. 4-5 Select VLAN Mode

## VLAN Mode

VLAN Mode	Metro mode ▾
Up-link Port	21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24 <input type="checkbox"/>
<b>Apply</b>	

Fig. 4-6 Metro mode

## VLAN Mode

VLAN Mode	Tag-based ▾
Double Tag	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Up-link Port	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="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/>
	17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24 <input type="checkbox"/>
<b>Apply</b>	

Fig. 4-6-1 Double Tag mode

**Parameter description:**

VLAN Mode:

Port-based:

Port-based VLAN is defined by port. Any packet coming in or outgoing from any one port of a port-based VLAN will be accepted. No filtering criterion applies in port-based VLAN. The only criterion is the physical port you connect to. For example, for a port-based VLAN named PVLAN-1 contains port members Port 1&2&3&4. If you are on the port 1, you can communicate with port 2&3&4. If you are on the port 5, then you cannot talk to them. Each port-based VLAN you built up must be assigned a group name. This switch can support up to maximal 24 port-based VLAN groups.

Tag-based:

Tag-based VLAN identifies its member by VID. This is quite different from port-based VLAN. If there are any more rules in ingress filtering list or egress filtering list, the packet will be screened with more filtering criteria to determine if it can be forwarded. The switch supports supplement of 802.1q. For more details, please see the section VLAN in Chapter 3.

Each tag-based VLAN you built up must be assigned VLAN name and VLAN ID. Valid VLAN ID is 1-4094. User can create total up to 24 Tag VLAN groups.

Double-tag:

Double-tag mode belongs to the tag-based mode, however, it would treat all frames as the untagged ones, which means that tag with PVID will be added into all packets. Then, these packets will be forwarded as Tag-based VLAN. So, the incoming packets with tag will become the double-tag ones

Metro Mode:

The Metro Mode is a quick configuration VLAN environment method on Port-based VLAN. It will create 21, 22, 23 or 24 Port-based VLAN groups.

**Function name:**

VLAN Port Configuration (Tag based VLAN mode)

**Function description:**

In VLAN Tag Rule Setting, user can input VID number to each port. The range of VID number is from 1 to 4094. User also can choose ingress filtering rules to each port. There are two ingress filtering rules which can be applied to the switch. The Ingress Filtering Rule 1 is “forward only packets with VID matching this port’s configured VID”. The Ingress Filtering Rule 2 is “drop untagged frame”. You can also select the Role of each port as Access, Trunk, or Hybrid.

**Tag-Based VLAN Configuration**

Add a VLAN

VLAN ID

Add

VLAN Configuration List

Port Config

	VID	Description	Member
<input checked="" type="radio"/>	1	Default	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

NOTE:

Before deleting a VLAN, please make sure the PVID of all ports is different from the VID being deleted.

Modify Delete Refresh

Fig. 4-5-1 tag- VLAN Mode

**VLAN Per Port Configuration**

Port	Ingress Filtering Enabled	Packet Type	Role	Untagged VID	Pvid
Port 1	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access	4094	1
Port 2	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access	4094	1
Port 3	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access	4094	1
Port 4	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access	4094	1
Port 5	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access	4094	1
Port 6	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access	4094	1
Port 7	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access	4094	1
Port 8	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access	4094	1
Port 9	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access	4094	1
Port 10	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access	4094	1
Port 11	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access	4094	1
Port 12	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access	4094	1

Fig. 4-5-2 Per port configuration

**Parameter description:**

Port 1-24:

Port number.

Ingress Filtering Enabled:

Discard other VLAN group packets, only forward this port joined VLAN group packets.

Packet Type:

All:

Forward all tagged and untagged packets.

Tagged Only:

Forward tagged packets only and discard untagged packets.

Tag Out Enabled:

It means the outgoing packets in this port must carry VLAN tag header.

Role:

This is an egress rule of the port. Here you can choose Access, Trunk or Hybrid. Trunk means the outgoing packets must carry VLAN tag header. Access means the outgoing packets carry no VLAN tag header. If packets have double VLAN tags, one will be dropped and the other will still be left. As to Hybrid, it is similar to Trunk, and both of them will tag-out. When the port is set to Hybrid, its packets will be untagged out if the VID of the outgoing packets with tag is the same as the one in the field of Untag VID of this port.

Untag VID:

Valid range is 1~4094. It works only when Role is set to Hybrid.

Pvid:

This PVID range will be 1-4094. Before you set a number x as PVID, you have to create a Tag-based VLAN with VID x. For example, if port x receives an untagged packet, the switch will apply the PVID (assume as VID y) of port x to tag this packet, the packet then will be forwarded as the tagged packet with VID

## 4-2-5. VLAN Group Configuration

### **Function name:**

VLAN Group Configuration

### **Function description:**

It shows the information of VLAN Groups, and allows administrators to maintain them by modifying and deleting each VLAN group. User also can add a new VLAN group by inputting a new VLAN name and VLAN ID.

If you are in port-based VLAN, it will just show the ID - Member of the existed port-based VLAN group. If you are in tag-based VLAN, it will show the ID - VID - Member of the existed tag-based VLAN group. The switch can store the configuration of port-based VLAN and tag-based VLAN separately. When you choose one of VLAN mode, the switch will bring you the responded VLAN configuration which keeps the default data. You can easily create and delete a VLAN group by pressing **<Add>** and **<Delete>** function buttons, or click the Group ID directly to edit it.

### **Port-Based VLAN Configuration**

#### Add a VLAN

ID	<input type="text" value="2"/>
----	--------------------------------

**Add**

#### VLAN Configuration List

	ID	Description	Member
	1	Default	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

**Modify** **Delete** **Refresh**

Fig. 4-7 Port-Based VLAN Configuration

### **Parameter description:**

ID (Group ID):

When you want to edit a VLAN group, you must select the Group ID field. Then, you will enter Tag Base VLAN Group Setting or Port Base VLAN Group Setting page, which depends on your VLAN mode selection.

VID:

VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based mode.

Member:

In modify function this is used to enable or disable if a port is a member of the new added VLAN, "Enable" means it is a member of the VLAN.

Just tick the check box (☑) beside the port x to enable it.

Add Group:

Create a new port-based VLAN or tag-based VLAN, which depends on the VLAN mode you choose in VLAN mode function.

### VLAN Setup

Description

ID: 2

Port	Member	Port	Member
Port 1	<input type="checkbox"/>	Port 13	<input type="checkbox"/>
Port 2	<input type="checkbox"/>	Port 14	<input type="checkbox"/>
Port 3	<input type="checkbox"/>	Port 15	<input type="checkbox"/>
Port 4	<input type="checkbox"/>	Port 16	<input type="checkbox"/>
Port 5	<input type="checkbox"/>	Port 17	<input type="checkbox"/>
Port 6	<input type="checkbox"/>	Port 18	<input type="checkbox"/>
Port 7	<input type="checkbox"/>	Port 19	<input type="checkbox"/>
Port 8	<input type="checkbox"/>	Port 20	<input type="checkbox"/>
Port 9	<input type="checkbox"/>	Port 21	<input type="checkbox"/>
Port 10	<input type="checkbox"/>	Port 22	<input type="checkbox"/>
Port 11	<input type="checkbox"/>	Port 23	<input type="checkbox"/>
Port 12	<input type="checkbox"/>	Port 24	<input type="checkbox"/>

Select All Apply Refresh

Fig. 4-8 Add or Remove VLAN Member

Delete Group:

Just tick the check box (☑) beside the ID, then press the <Delete> button to delete the group.

### Port-Based VLAN Configuration

Add a VLAN

ID

Add

VLAN Configuration List

	ID	Description	Member
<input type="radio"/>	1	Default	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
<input checked="" type="radio"/>	2	dg	19,20

Modify Delete Refresh

Fig. 4-9 Port-Based VLAN Configuration

## 4-2-6. PoE

Power Over Ethernet (PoE) technology allows IP telephones, wireless LAN access points, and other powered devices (PDs) to receive power and transfer data over existing LAN cabling.

### Function name:

PoE Configuration

### Function description:

In PoE Port Management function, user can configure the settings about PoE.

The switch complies with IEEE 802.3af protocol and be capable of detecting automatically that whether the device linked to the port on the switch is PD (Powered Device) or not. The switch also manage the power supplement based on the Class of the PD, and it will stop supplying the power once the power required by the PD exceeds the Class, Short Circuit or over temperature occurs.

### PoE Configuration

Port No	Status	State	Priority	Power(W)	Current(mA)	Class	Delay Time (0~300; 0:Disable)
1	Normal	Enable	Normal	0.0	0	0	0 Second(s)
2	Normal	Enable	Normal	0.0	0	0	0 Second(s)
3	Normal	Enable	Normal	0.0	0	0	0 Second(s)
4	Normal	Enable	Normal	0.0	0	0	0 Second(s)
5	Normal	Enable	Normal	0.0	0	0	0 Second(s)
6	Normal	Enable	Normal	0.0	0	0	0 Second(s)
7	Normal	Enable	Normal	0.0	0	0	0 Second(s)
8	Normal	Enable	Normal	0.0	0	0	0 Second(s)
9	Normal	Enable	Normal	0.0	0	0	0 Second(s)
10	Normal	Enable	Normal	0.0	0	0	0 Second(s)
11	Normal	Enable	Normal	0.0	0	0	0 Second(s)
12	Normal	Enable	Normal	0.0	0	0	0 Second(s)
13	Normal	Enable	Normal	0.0	0	0	0 Second(s)
14	Normal	Enable	Normal	0.0	0	0	0 Second(s)
15	Normal	Enable	Normal	0.0	0	0	0 Second(s)
16	Normal	Enable	Normal	0.0	0	0	0 Second(s)
17	Normal	Enable	Normal	0.0	0	0	0 Second(s)
18	Normal	Enable	Normal	0.0	0	0	0 Second(s)
19	Normal	Enable	Normal	0.0	0	0	0 Second(s)
20	Normal	Enable	Normal	0.0	0	0	0 Second(s)

Fig. 3-16

**Parameter description:**

Status:

Include "Normal" or "Active" two kinds of status. The former means the port is ready to link and supply the power to the PD at any time. The latter means the port is in the condition of supplying the power.

State:

"Enable" means the manager allows the power supplied to the PD is legal while the port linked to the PD; "Disable" means the port does not own PoE function.

Priority:

Three options are offered for the user to choose, including Normal, Low and High. Default is Normal. The switch will stop supplying the power to the port based on the order of the priority Low→Normal→High in case total power required by all PDs linked to the switch exceeds the power limit. As the ports have the same priority, then the switch will cease the power supplement from the port with the highest port id (12→1).

Power(W):

The power is consumed by the port.

Current(mA):

The current is supplied to the PD by the port.

Class:

The Class of the PD linked to the port of the switch.

Delay time:

The Delay time is using for set the time period for PD PoE enable time delay period. It is a solution to avoid rush current to cause shorter PD. The available time period is from 0 to 300 seconds and 0 means disable the function.

**Function name:**

PoE Status

**Function description:**

Display the information about the PoE status.

**PoE Status**

Vmain	48.3 V
Imain	0.00 A
Pconsume	0.0 W
Power Limit	380 W
Temperature	37 'C / 98 'F

Port No	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Port On																								
AC Disconnect Port Off																								
DC Disconnect Port Off																								
Overload Port Off																								
Short Circuit Port Off																								
Over Temp. Protection																								
Power Management Port Off																								

Refresh

Fig. 3-15

**Parameter description:**

Vmain:

The volt is supplied by the PoE.

Imain:

The sum of the current that every port supplies.

Pconsume:

The sum of the power that every port supplies.

Power Limit:

The maximal power that the switch can supply (Read Only).

Temperature:

The temperature of the chip on PoE.

Port No:

Port number.

Port On:

Show whether the port is supplying the power to the PD or not.

AC Disconnect Port Off:

Port is turned off due to the AC Disconnect function.

DC Disconnect Port Off:

Port is turned off due to the DC Disconnect function.

**Overload Port Off:**

The switch will stop supplying the power to the port due to the power required by the PD that is linked to the port on the switch exceeds the Class setting of the PD.

**Short Circuit Port Off:**

The switch will stop supplying the power to the port if it detects that the PD linked to the port is short circuit.

**Over Temp. Protection:**

The port of the switch will be disabled due to fast transient rise in temperature to 240°C or slow rise in temperature to 200°C.

**Power Management Port Off:**

Due to total power required by all PDs linked to the switch exceeds the power limit, so the switch stops supplying the power to this port after referring to the information of the priority.

**Function name:**

PoE Auto Checking:

**Function description:**

The function is using for PD auto checking. It can allow user to control the PoE function by using the ping command, in order to turn on or off any PD which connect with port assign.

**PoE Auto Checking**

Ping Check:

Port No	Ping IP Address	Interval Time (10~120 seconds)	Retry Time (1~5)	Failure Log	Failure Action	Reboot Time (3~255 seconds)
1	0.0.0.0	30	3	error=0 total=0	Nothing	15
2	0.0.0.0	30	3	error=0 total=0	Nothing	15
3	0.0.0.0	30	3	error=0 total=0	Nothing	15
4	0.0.0.0	30	3	error=0 total=0	Nothing	15
5	0.0.0.0	30	3	error=0 total=0	Nothing	15
6	0.0.0.0	30	3	error=0 total=0	Nothing	15
7	0.0.0.0	30	3	error=0 total=0	Nothing	15
8	0.0.0.0	30	3	error=0 total=0	Nothing	15
9	0.0.0.0	30	3	error=0 total=0	Nothing	15
10	0.0.0.0	30	3	error=0 total=0	Nothing	15
11	0.0.0.0	30	3	error=0 total=0	Nothing	15
12	0.0.0.0	30	3	error=0 total=0	Nothing	15
13	0.0.0.0	30	3	error=0 total=0	Nothing	15
14	0.0.0.0	30	3	error=0 total=0	Nothing	15
15	0.0.0.0	30	3	error=0 total=0	Nothing	15
16	0.0.0.0	30	3	error=0 total=0	Nothing	15

**Parameter description:**

Ping Check:

To scroll and select the Enable or Disable Ping Check function.

Port No.:

To display the Port Index, the maximum is 24.

Ping IP Address:

To set up the PD's IP address which you need to check it is alive.

Interval Time:

To set up the spacing interval time to do ping check, the default value is 30 seconds. The available range is 10 to 120 seconds.

Retry Time:

To set up the number of times for switch to check PD is alive. The default

is 3. The available range is 1 to 5.

**Failure Log:**

To display the PD's Ping result and log. Note down "Ping Check" a result of movement after starting. The error means switch to ping the PD is failure or total means total switch to do ping frequency.

**Failure Action:**

To set up when PD is failure and switch action command. The values are "Nothing" and "Reboot Remote PD".

Nothing: The switch detects that PD occurs failure and do nothing.

Reboot Remote PD: The switch detect that PD occurs failure and then reboot it.

**Reboot Time:**

The switch ping check PD failure "P.O.E" restarts the buffer time of switch. The default is 15 seconds. The available range is 3 to 255 seconds..

**Function name:**

PoE Scheduling

**Function description:**

The function provides user to appoint date and time, Enable or Disable PoE function, switch can with according to the time when is set up, carry on the designated movements. Web Smart Switch NTP only supports IP address for NTP server, no support domain name for NTP server.

**PoE Scheduling**

Schedule on: Port 01  
Schedule mode: Disable

Select all   **Copy Scheduling**   **Paste**

Hour\Day	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00	<input checked="" type="checkbox"/>						
01	<input checked="" type="checkbox"/>						
02	<input checked="" type="checkbox"/>						
03	<input checked="" type="checkbox"/>						
04	<input checked="" type="checkbox"/>						
05	<input checked="" type="checkbox"/>						
06	<input checked="" type="checkbox"/>						
07	<input checked="" type="checkbox"/>						
08	<input checked="" type="checkbox"/>						
09	<input checked="" type="checkbox"/>						
10	<input checked="" type="checkbox"/>						
11	<input checked="" type="checkbox"/>						
12	<input checked="" type="checkbox"/>						
13	<input checked="" type="checkbox"/>						
14	<input checked="" type="checkbox"/>						
15	<input checked="" type="checkbox"/>						
16	<input checked="" type="checkbox"/>						
17	<input checked="" type="checkbox"/>						
18	<input checked="" type="checkbox"/>						
19	<input checked="" type="checkbox"/>						
20	<input checked="" type="checkbox"/>						
21	<input checked="" type="checkbox"/>						
22	<input checked="" type="checkbox"/>						
23	<input checked="" type="checkbox"/>						

**Apply**

Note: The PoE Scheduling will be disabled automatically when the NTP sync time server failure happened.

Fig. 3-15-2

***Parameter description:***

Schedule on:

It provide user to set which port will action the PoE Scheduling function.

Schedule mode:

To set the schedule mode with Enable or Disable. The default is Disable.

Select all:

To select all date and time to enable the PoE function.

Hour/ Day:

To evoke what time to enable the PoE function.

Sunday ~ Saturday:

To set up the enable PoE function Date.

***Note: The PoE Scheduling will be disabled automatically when NTP sync time server failure happened.***

## 4-2-7. Aggregation

The Aggregation (Port Trunking) Configuration is used to configure the settings of Link Aggregation. You can bundle ports by same speed, MAC, and full duplex to be a single logical port, thus the logical port can aggregate the bandwidth of these ports. This means you can apply your current Ethernet equipments to build the bandwidth aggregation. For example, if three Fast Ethernet ports are aggregated into a logical port, then this logical port's bandwidth would be as three times high as a single Fast Ethernet port's.

### **Function name:**

Aggregation Configuration

### **Function description:**

Display the current setup of Aggregation Trunking. With this function, user is allowed to add a new trunking group or modify the members of an existed trunking group.

### **Aggregation/Trunking Configuration**

Group\Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Normal	<input checked="" type="radio"/>																							
Group 1	<input type="radio"/>																							
Group 2	<input type="radio"/>																							
Group 3	<input type="radio"/>																							
Group 4	<input type="radio"/>																							
Group 5	<input type="radio"/>																							
Group 6	<input type="radio"/>																							
Group 7	<input type="radio"/>																							
Group 8	<input type="radio"/>																							

Fig. 4-10 Aggregation/Trunking Configuration

### **Parameter description:**

Normal:

Set up the ports that do not join any aggregation trunking group.

Group 1~8:

Group the ports you choose together. Up to 12 ports can be selected for each group.

## 4-2-8. LACP

Smart Web Switch supports link aggregation IEEE802.3ad standard. The standard describes Link Aggregate Control Protocol (LACP) which dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the "standby" ports become operational without user intervention.

### **Function name:**

LACP Port Configuration

### **Function description:**

Enable or disable LACP protocol, user is allowed to set the aggregation key value.

### **LACP Port Configuration**

Port	Protocol Enabled	Key Value (0~255)
1	<input type="checkbox"/>	auto
2	<input type="checkbox"/>	auto
3	<input type="checkbox"/>	auto
4	<input type="checkbox"/>	auto
5	<input type="checkbox"/>	auto
6	<input type="checkbox"/>	auto
7	<input type="checkbox"/>	auto
8	<input type="checkbox"/>	auto
9	<input type="checkbox"/>	auto
10	<input type="checkbox"/>	auto
11	<input type="checkbox"/>	auto
12	<input type="checkbox"/>	auto
13	<input type="checkbox"/>	auto
14	<input type="checkbox"/>	auto
15	<input type="checkbox"/>	auto
16	<input type="checkbox"/>	auto
17	<input type="checkbox"/>	auto
18	<input type="checkbox"/>	auto
19	<input type="checkbox"/>	auto
20	<input type="checkbox"/>	auto
21	<input type="checkbox"/>	auto
22	<input type="checkbox"/>	auto
23	<input type="checkbox"/>	auto
24	<input type="checkbox"/>	auto

Apply

Refresh

Fig. 4-11 LACP Port Configuration

***Parameter description:***

Protocol Enabled:

Just tick the check box () to enable LACP protocol then press the **<Apply>** button to apply.

Key Value:

It's key for an aggregation. This must be an integer value between 1 and 255 or auto select by switch.

## 4-2-9. RSTP

RSTP detects and resolves network loops, and provides backup links between switches, bridges and routers. The protocol allows a switch to communicate with other RSTP compliant switches, and to ensure only one path existing between two stations in your network environment.

The switch allows you to create multiple STP configurations and assign ports to a specific tree.

### **Function name:**

RSTP System Configuration

### **Function description:**

This screen is used to display the RSTP system configuration and set the need of parameters.

### **RSTP System Configuration**

System Priority	32768	▼
Hello Time	2	
Max Age	20	
Forward Delay	15	
Force version	RSTP	▼

Fig. 4-12-1 LACP Port Configuration

### **Parameter description:**

System Priority:

System priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box.

The lower the numeric value you assign, the higher the priority for this system.

Default: 32768

Hello Time:

This is the time interval in seconds between BPDU configuration message generations by the root switch. The allowed range is 1 to 10 seconds.

Default: 2

Max Age:

This is the maximum time a switch can wait without receiving a BPDU before attempting to reconfigure. The allowed range is 6 to 40 seconds.

Default: 20

Forward Delay:

This is the maximum time (in seconds) a switch will wait before changing states. The general rule:  $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$

Default: 15

Force version:

Select RSTP or STP protocol from the drop-down list box.

**Function name:**

RSTP Port Configuration

**Function description:**

Enable or disable RSTP protocol on the ports that are selected and set path cost.

**RSTP Port Configuration**

Port	Protocol Enabled	Edge	Path Cost (1~200000000)
Aggregations	<input type="checkbox"/>		
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
11	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
12	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
13	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
14	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
15	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
16	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
17	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
18	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
19	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
20	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
21	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
22	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
23	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
24	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto

Fig. 4-12-2 RSTP Configuration

**Parameter description:**

Protocol Enabled:

Just tick the check box () beside the port x to enable RSTP protocol, then press the **<Apply>** button to apply.

Edge:

Just tick the check box () beside the port x to enable edge function.

Path Cost:

Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost, user can select auto or set the range from 1 to 200000000.

## 4-2-10. 802.1X

802.1x port-based network access control provides a method to restrict users to access network resources via authenticating user's information. This restricts users from gaining access to the network resources through a 802.1x-enabled port without authentication. If a user wishes to touch the network through a port under 802.1x control, he (she) must firstly input his (her) account name for authentication and waits for gaining authorization before sending or receiving any packets from a 802.1x-enabled port.

Before the devices or end stations can access the network resources through the ports under 802.1x control, the devices or end stations connected to a controlled port send the authentication request to the authenticator, the authenticator pass the request to the authentication server to authenticate and verify, and the server tell the authenticator if the request get the grant of authorization for the ports.

According to IEEE802.1x, there are three components implemented. They are Authenticator, Supplicant and Authentication server shown in Fig. 4-13.

### Supplicant:

It is an entity being authenticated by an authenticator. It is used to communicate with the Authenticator PAE (Port Access Entity) by exchanging the authentication message when the Authenticator PAE request to it.

### Authenticator:

An entity facilitates the authentication of the supplicant entity. It controls the state of the port, authorized or unauthorized, according to the result of authentication message exchanged between it and a supplicant PAE. The authenticator may request the supplicant to re-authenticate itself at a configured time period. Once start re-authenticating the supplicant, the controlled port keeps in the authorized state until re-authentication fails.

A port acting as an authenticator is thought to be two logical ports, a controlled port and an uncontrolled port. A controlled port can only pass the packets when the authenticator PAE is authorized, and otherwise, an uncontrolled port will unconditionally pass the packets with PAE group MAC address, which has the value of 01-80-c2-00-00-03 and will not be forwarded by MAC bridge, at any time.

### Authentication server:

A device provides authentication service, through EAP, to an authenticator by using authentication credentials supplied by the supplicant to determine if the supplicant is authorized to access the network resource.

The overview of operation flow for the Fig. 4-13 is quite simple. When Supplicant PAE issues a request to Authenticator PAE, Authenticator and Supplicant exchanges authentication message. Then, Authenticator passes the request to RADIUS server to verify. Finally, RADIUS server replies if the request is granted or denied.

While in the authentication process, the message packets, encapsulated by Extensible Authentication Protocol over LAN (EAPOL), are exchanged between an authenticator PAE and a supplicant PAE. The Authenticator exchanges the message to authentication server using EAP encapsulation. Before successfully authenticating, the supplicant can only touch the authenticator to perform authentication message exchange or access the network from the uncontrolled port.

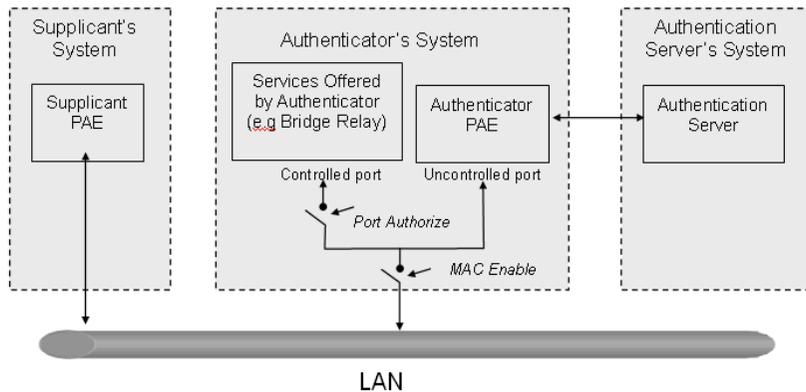


Fig. 4-13

In the Fig. 4-14, this is the typical configuration, a single supplicant, an authenticator and an authentication server. B and C is in the internal network, D is Authentication server running RADIUS, switch at the central location acts Authenticator connecting to PC A and A is a PC outside the controlled port, running Supplicant PAE. In this case, PC A wants to access the services on device B and C, first, it must exchange the authentication message with the authenticator on the port it connected via EAPOL packet. The authenticator transfers the supplicant's credentials to Authentication server for verification. If success, the authentication server will notice the authenticator the grant. PC A, then, is allowed to access B and C via the switch. If there are two switches directly connected together instead of single one, for the link connecting two switches, it may have to act two port roles at the end of the link: authenticator and supplicant, because the traffic is bi-directional.

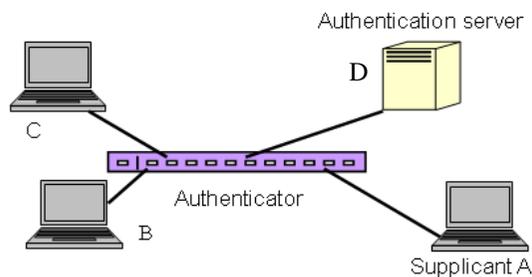


Fig. 4-14

The Fig. 4-15 shows the procedure of 802.1x authentication. There are steps for the login based on 802.1x port access control management. The protocol used in the right side is EAPOL and the left side is EAP.

1. At the initial stage, the supplicant A is unauthenticated and a port on switch acting as an authenticator is in unauthorized state. So the access is blocked in this stage.
2. Initiating a session. Either authenticator or supplicant can initiate the message exchange. If supplicant initiates the process, it sends EAPOL-start packet to the authenticator PAE and authenticator will immediately respond EAP-Request/Identity packet.
3. The authenticator always periodically sends EAP-Request/Identity to the supplicant for requesting the identity it wants to be authenticated.
4. If the authenticator doesn't send EAP-Request/Identity, the supplicant will initiate EAPOL-Start the process by sending to the authenticator.
5. And next, the Supplicant replies an EAP-Response/Identity to the authenticator. The authenticator will embed the user ID into Radius-Access-Request command and send it to the authentication server for confirming its identity.
6. After receiving the Radius-Access-Request, the authentication server sends Radius-Access-Challenge to the supplicant for asking for inputting user password via the authenticator PAE.
7. The supplicant will convert user password into the credential information, perhaps, in MD5 format and replies an EAP-Response with this credential information as well as the specified authentication algorithm (MD5 or OTP) to Authentication server via the authenticator PAE. As per the value of the type field in message PDU, the authentication server knows which algorithm should be applied to authenticate the credential information, EAP-MD5 (Message Digest 5) or EAP-OTP (One Time Password) or other else algorithm.
8. If user ID and password is correct, the authentication server will send a Radius-Access-Accept to the authenticator. If not correct, the authentication server will send a Radius-Access-Reject.
9. When the authenticator PAE receives a Radius-Access-Accept, it will send an EAP-Success to the supplicant. At this time, the supplicant is authorized and the port connected to the supplicant and under 802.1x control is in the authorized state. The supplicant and other devices connected to this port can access the network. If the authenticator receives a Radius-Access-Reject, it will send an EAP-Failure to the supplicant. This means the supplicant is failed to authenticate. The port it connected is in the unauthorized state, the supplicant and the devices connected to this port won't be allowed to access the network.
10. When the supplicant issue an EAP-Logoff message to Authentication server, the port you are using is set to be

unauthorized.

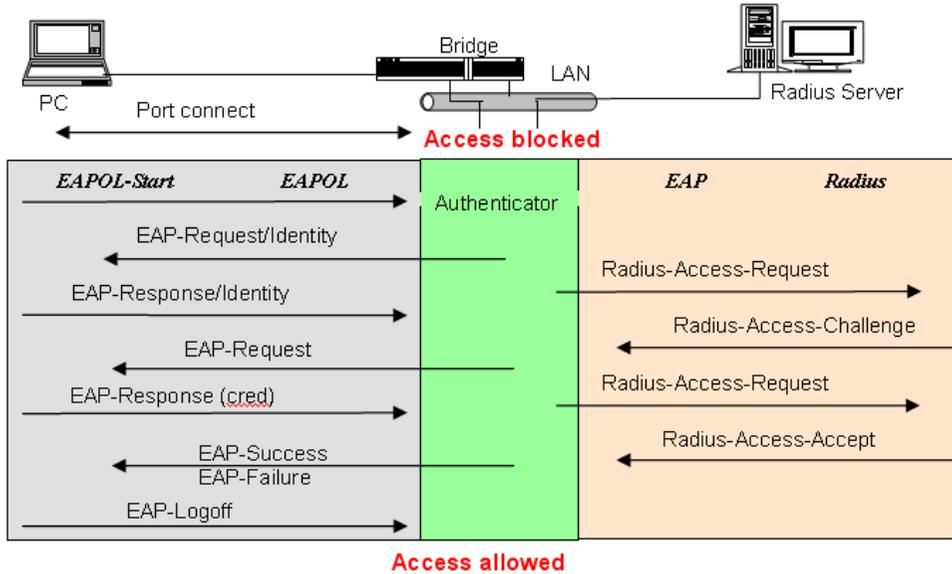


Fig. 4-15

The 802.1X “Enabled” is the type of authentication supported in the switch. In this mode, for the devices connected to this port, once a supplicant is authorized, the devices connected to this port can access the network resource through this port.

802.1x Port-based Network Access Control function supported by the switch is little bit complex, for it just support basic “Enabled” mode, which can distinguish the device’s MAC address and its VID. The following table is the summary of the combination of the authentication status and the port status versus the status of port mode, set in 802.1x Port mode, port control state, set in 802.1x port setting. Here Entry Authorized means MAC entry is authorized.

Port Mode	Port Control	Authentication	Port Status
Disable	Don't Care	Don't Care	Port Uncontrolled
Enabled	Auto	Successful	Port Authorized
Enabled	Auto	Failure	Port Unauthorized
Enabled	ForceUnauthorized	Don't Care	Port Unauthorized
Enabled	ForceAuthorized	Don't Care	Port Authorized

**Function name:**

802.1X Configuration

**Function description:**

This function is used to configure the global parameters for RADIUS authentication in 802.1x port security application.

## 802.1X Configuration

Mode:	Enabled ▾
RADIUS IP	0.0.0.0
RADIUS UDP Port	1812
RADIUS Secret	

Port	Admin State	Port State			
1	Force Authorized ▾	Link Down	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
2	Force Authorized ▾	Link Down	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
3	Force Authorized ▾	Link Down	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
4	Force Authorized ▾	Link Down	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
5	Force Authorized ▾	Link Down	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
6	Force Authorized ▾	Link Down	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
7	Force Authorized ▾	Authorized	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
8	Force Authorized ▾	Link Down	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
9	Force Authorized ▾	Link Down	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
10	Force Authorized ▾	Link Down	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
11	Force Authorized ▾	Link Down	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
12	Force Authorized ▾	Link Down	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>

----- continue -----

23	Force Authorized ▾	Link Down	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
24	Force Authorized ▾	Link Down	<a href="#">Re-authenticate</a>	<a href="#">Force Reinitialize</a>	<a href="#">Statistics</a>
			<a href="#">Re-authenticate All</a>	<a href="#">Force Reinitialize All</a>	

Parameters

[Apply](#) [Refresh](#)

Fig. 4-16 802.1X Configuration

### Parameter description:

Mode:

Enable or disable 802.1X function.

RADIUS IP:

RADIUS server IP address for authentication.

Default: 0.0.0.0

RADIUS UDP Port:

The port number to communicate with RADIUS server for the authentication service. The valid value ranges 1-65535.

Default port number is 1812.

RADIUS Secret:

The secret key between authentication server and authenticator. It is a string with the length 1 – 15 characters. The character string may contain upper case, lower case and 0-9. It is character sense. It is not allowed for putting a blank between any two characters.

Default: None

Admin State:

This is used to set the operation mode of authorization. There are three type of operation mode supported, Force Unauthorized, Force Authorized, Auto.

- Force Unauthorized:

The controlled port is forced to hold in the unauthorized state.

- Force Authorized:

The controlled port is forced to hold in the authorized state.

- Auto:

The controlled port is set to be in authorized state or unauthorized state depends on the result of the authentication exchange between the authentication server and the supplicant.

Default: Force Authorized

Port State:

Show the port status of authorization.

Re-authenticate:

Specify if subscriber has to periodically re-enter his or her username and password to stay connected to the port.

Re-authenticate All:

Re-authenticate for all ports in at once.

Force Reinitialize:

Force the subscriber has to reinitialize connected to the port.

Force Reinitialize All:

Force Reinitialize for all ports in at once.

**Statistics:**

Choose the port which you want to show of 802.1X statistics, the screen include Authenticator counters, backend Authenticator counters, dot1x MIB counters and Other statistics.

Press the **<Refresh>** button will fresh the screen and see the newer counters.

**802.1X Statistics for Port 1**

<b>Refresh</b>							
<a href="#">Port 1</a>	<a href="#">Port 2</a>	<a href="#">Port 3</a>	<a href="#">Port 4</a>	<a href="#">Port 5</a>	<a href="#">Port 6</a>	<a href="#">Port 7</a>	<a href="#">Port 8</a>
<a href="#">Port 9</a>	<a href="#">Port 10</a>	<a href="#">Port 11</a>	<a href="#">Port 12</a>	<a href="#">Port 13</a>	<a href="#">Port 14</a>	<a href="#">Port 15</a>	<a href="#">Port 16</a>
<a href="#">Port 17</a>	<a href="#">Port 18</a>	<a href="#">Port 19</a>	<a href="#">Port 20</a>	<a href="#">Port 21</a>	<a href="#">Port 22</a>	<a href="#">Port 23</a>	<a href="#">Port 24</a>
<b>Authenticator counters</b>							
authEntersConnecting	5		authEapLogoffsWhileConnecting	0			
authEntersAuthenticating	0		authAuthSuccessesWhileAuthenticating	0			
authAuthTimeoutsWhileAuthenticating	3		authAuthFailWhileAuthenticating	0			
authAuthEapStartsWhileAuthenticating	0		authAuthEapLogoffWhileAuthenticating	0			
authAuthReauthsWhileAuthenticated	0		authAuthEapStartsWhileAuthenticated	0			
authAuthEapLogoffWhileAuthenticated	0						
<b>Backend Authenticator counters</b>							
backendResponses	0		backendAccessChallenges	0			
backendOtherRequestsToSupplicant	4		backendAuthSuccesses	0			
backendAuthFails	0						
<b>dot1x MIB counters</b>							
dot1xAuthEapolFramesRx	0		dot1xAuthEapolFramesTx	7			
dot1xAuthEapolStartFramesRx	0		dot1xAuthEapolLogoffFramesRx	0			
dot1xAuthEapolRespIdFramesRx	0		dot1xAuthEapolRespFramesRx	0			
dot1xAuthEapolReqIdFramesTx	4		dot1xAuthEapolReqFramesTx	0			
dot1xAuthInvalidEapolFramesRx	0		dot1xAuthEapLengthErrorFramesRx	0			
dot1xAuthLastEapolFrameVersion	0		dot1xAuthLastEapolFrameSource				
<b>Other statistics</b>							
Last Supplicant identity							

Fig. 4-17 802.1X Statistics

**Function name:**

802.1x Parameters

**Function description:**

In here, user can enable or disable Reauthentication function and specify how often a client has to re-enter his or her username and password to stay connected to the port.

## 802.1X Parameters

<b>Reauthentication Enabled</b>	<input type="checkbox"/> <b>Enabled</b>
<b>Reauthentication Period</b> [ 1 - 3600 seconds ]	3600
<b>EAP timeout</b> [ 1 - 255 seconds ]	30

Apply
Refresh

Fig. 4-18 802.1X Parameters

***Parameter description:***

Reauthentication Enabled:

Choose whether regular authentication will take place in this port.

Default: disable

Reauthentication Period (1-65535 s):

A non-zero number seconds between the periodic re-authentication of the supplicant.

Default: 3600

EAP timeout ((1-255 s):

A timeout condition in the exchange between the authenticator and the supplicant. The valid range: 1 –255.

Default: 30 seconds

## 4-2-11 IGMP Snooping

### Function name:

IGMP Snooping Configuration

### Function description:

IGMP Snooping lets administrators configure a switch to constrain multicast traffic by listening to Internet Group Management Protocol (IGMP). After finishing the settings, please press **<Apply>** button to start up the function.

#### IGMP Configuration

IGMP Enabled	<input type="checkbox"/>
Router Ports	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="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24 <input type="checkbox"/>
Unregistered IPMC Flooding enabled	<input checked="" type="checkbox"/>

VLAN ID	IGMP Snooping Enabled	IGMP Querying Enabled
---	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Fig. 4-19 IGMP Configuration

### Parameter description:

IGMP Enabled:

Just tick the check box () to enable this function.

Default: disable

Router Ports:

Just tick the check box () beside the port x to enable router ports, then press the **<Apply>** button to start up.

Default: none

Unregistered IGMP Flooding enabled:

Just tick the check box () to enable this function.

Default: enable

VLAN ID:

At the IGMP Enable mode being selected, it will list the VLAN ID number.

IGMP Snooping Enabled:

After IGMP Enabled function start up then user can tick the check box () to enable this function.

Default: enable

IGMP Querying Enabled:

After IGMP Enabled function start up then user can tick the check box () to enable this function.

Default: enable

## 4-2-12. Mirror Configuration

### **Function name:**

Mirror Configuration

### **Function description:**

Mirror Configuration is provided to monitor the traffic in the network. This switch supports one-port mirror multi-ports. For example, we assume that Port A and Port B are Source Ports, and Port C is Mirror Port respectively, thus, the traffic passing through Port A and Port B will be copied to Port C for monitor purpose.

The screenshot displays the 'Mirroring Configuration' interface. It features a table with 13 rows, each representing a port from 1 to 13. The table has two columns: 'Port' and 'Mirror Source'. Each 'Mirror Source' cell contains an unchecked checkbox. Below the table is a '-----Continue-----' text. At the bottom, there is a 'Mirror Port' section with a dropdown menu currently set to 'Disabled'. Below this are two buttons: 'Apply' and 'Refresh'.

Port	Mirror Source
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="checkbox"/>
11	<input type="checkbox"/>
12	<input type="checkbox"/>
13	<input type="checkbox"/>

-----Continue-----

Mirror Port: Disabled

Apply Refresh

Fig. 4-20 Mirror ports configuration

### **Parameter description:**

Source Port:

Set up the port for being monitored. Just tick the check box (☑) beside the port x and valid port is Port 1~24.

Mirror Port:

Use the drop-down menu to select a mirror port.

## 4-2-13. QoS(Quality of Service) Configuration

The switch offers powerful QoS function. This function supports VLAN-tagged priority that can make precedence of 8 priorities, and DSCP(Differentiated Services Code Point) on Layer 3 of network framework.

### **Function name:**

QoS Configuration

### **Function description:**

While setting QoS function, please select QoS Mode in drop-down menu at first. Then you can use 802.1p Priority and DSCP Priority functions. In this function, you can enable/disable QoS Mode and set Priority Control, such as: 802.1p and DSCP. The switch only supports Strict Priority. High priority queue is always passed first.



Fig. 4-21 QoS Configuration

### **Function name:**

802.1p QoS Mode

### **Function description:**

This function will affect the priority of VLAN tag. Based on priority of VLAN tag, it can arrange 0~7 priorities, priorities can map to 4 queues of the switch (low, normal, medium, high) and possess different bandwidth distribution according to your weight setting.

### **Parameter description:**

Prioritize Traffic

Five Prioritize Traffic values are provided: Custom, All Low Priority, All Normal Priority, All Medium Priority, and All High Priority.

The QoS setting would apply to all ports on the switch if one of the following values is selected: All Low Priority, All Normal Priority, All Medium Priority, or All High Priority.

Port Number

When Custom is selected for Prioritize Traffic, you may assign specific Port Number for 802.1p Configuration.

802.1p Configuration:

Each Priority can select any of Queue. In Default, Priority 0 is mapping to Queue normal, Priority 1 is mapping to Queue low, Priority 2 is mapping to Queue low, Priority 3 is mapping to Queue normal, Priority 4 is mapping to Queue medium, Priority 5 is mapping to Queue medium, Priority 6 is mapping to Queue high, and Priority 7 is mapping to Queue high.

### QoS Configuration

QoS Mode	802.1p						
Prioritise Traffic	Custom						
Port Number	Port 1						

802.1p Configuration							
802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority
0	low	1	low	2	normal	3	normal
4	medium	5	medium	6	high	7	high

Apply Cancel

Fig. 4-22 802.1p Setting

**Function name:**

DSCP QoS Mode

**Function description:**

In the late 1990s, the IETF redefined the meaning of the 8-bit SERVICE TYPE field to accommodate a set of differentiated services (DS). Under the differentiated services interpretation, the first six bits comprise a codepoint, which is sometimes abbreviated DSCP, and the last two bits are left unused.

DSCP can form total 64 (0~63) kinds of Traffic Class based on the arrangement of 6-bit field in DSCP of the IP packet. In the switch, user is allowed to set up these 64 kinds of Class that belong to any of queue (low, normal, medium, high).

**Parameter description:**

**Prioritize Traffic**

Five Prioritize Traffic values are provided: Custom, All Low Priority, All Normal Priority, All Medium Priority, and All High Priority.

The QoS setting would apply to all ports on the switch if one of the following values is selected: All Low Priority, All Normal Priority, All Medium Priority, or All High Priority.

**Port Number**

When Custom is selected for Prioritize Traffic, you may assign specific Port Number for DSCP Configuration.

DSCP Configuration:

64 kinds of priority traffic as mentioned above, user can set up any of Queue (low, normal, medium, high). In default, Priority 0~63 are mapping to Queue high.

### QoS Configuration

QoS Mode	DSCP
Prioritise Traffic	All High Priority
Port Number	Port 1

DSCP Configuration	
DSCP Value(0..63)	Priority
	high
All others	high

**Apply** **Cancel**

Fig. 4-23 DSCP Setting

## 4-2-14. Filter

### **Function name:**

Filter Configuration

### **Function description:**

This function lets administrators easily set management source IP addresses to the ports on the switch. After completing the settings, please press **<Apply>** button to make this function take effect.

Port	Source IP Filter			DHCP Server Allowed
	Mode	IP Address	IP Mask	
1	Disabled ▾			<input checked="" type="checkbox"/>
2	Disabled ▾			<input checked="" type="checkbox"/>
3	Disabled ▾			<input checked="" type="checkbox"/>
4	Disabled ▾			<input checked="" type="checkbox"/>
5	Disabled ▾			<input checked="" type="checkbox"/>
6	Disabled ▾			<input checked="" type="checkbox"/>
7	Disabled ▾			<input checked="" type="checkbox"/>
8	Disabled ▾			<input checked="" type="checkbox"/>
9	Disabled ▾			<input checked="" type="checkbox"/>
10	Disabled ▾			<input checked="" type="checkbox"/>
11	Disabled ▾			<input checked="" type="checkbox"/>
12	Disabled ▾			<input checked="" type="checkbox"/>
13	Disabled ▾			<input checked="" type="checkbox"/>

Fig. 4-24 Filter Configuration

### **Parameter description:**

Source IP Filter:

Mode:

There are three types of mode in this drop-down menu. Default is disabled.

Disabled:

Allow all IP Address login to this switch and manage it.

Static:

Just allow the IP Address which set by administrator to login to this switch and manage it..

DHCP:

Allow the IP Address get from DHCP server can login to this switch and manage it.

**Note: If you choose this mode only an DHCP client could be package forwarding on the port.**

IP Address:

Setting up the IP Address, it can be one IP Address or a LAN.

IP Mask:

Setting up the IP Subnet Mask related with the IP Address.

DHCP Server Allowed:

Just tick the check box () under the port x to allow the DHCP Server on this port and valid port is Port 1~24.

Default: enable

## 4-2-15. Rate Limit

### Function name:

Ingress and Egress Bandwidth Setting

### Function description:

Ingress and Egress Bandwidth Setting function are used to set up the limit of Ingress or Egress bandwidth for each port.

### Rate Limit Configuration

Traffic Rate Unit		Ingress		Egress	
Port					
1	No Limit				
2	No Limit				
3	No Limit				
4	No Limit				
5	No Limit				
6	No Limit				
7	No Limit				
8	No Limit				
9	No Limit				
10	No Limit				
11	No Limit				
12	No Limit				

-----Continue-----

Rate Limit Configuration		Ingress		Egress	
Port					
1	No Limit				
2	No Limit				
3	No Limit				
4	No Limit				
5	No Limit				
6	No Limit				
7	No Limit				
8	No Limit				
9	No Limit				
10	No Limit				
11	No Limit				
12	No Limit				

Fig. 4-25 Rate Limit Configuration

***Parameter description:***

**Ingress:**

Set up the limit of Ingress bandwidth (Range: 128Kb, 512Kb, 1M, 10M and 32M) for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~24 ranges is from Rate1 to 29.

Default: No Limit

**Egress:**

Set up the limit of Egress bandwidth (Range: 128Kb, 512Kb, 1M, 10M and 32M) for the port you choose. Outgoing traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~24 ranges is from Rate1 to 29.

Default: No Limit

## 4-2-16. Storm Control

### Function name:

Storm Control

### Function description:

Storm Control is used to block unnecessary multicast and broadcast frames that reduce switch's performance. When the function is enabled and Storm Control rate settings are detected as exceeded, the unnecessary frames would be dropped.

#### Storm Control Configuration

Storm Control Number of frames per second	
ICMP Rate	No Limit
Learn Frames Rate	1k
Broadcast Rate	2k
Multicast Rate	4k
Flooded unicast Rate	8k
	16k
	32k
	64k
	128k
	256k
	512k
	1024k
	No Limit

Fig.4-26 Storm Control Configuration

### Parameter description:

#### ICMP Rate:

To enable the ICMP Storm capability. User can use drop-down menu to select number of frames. Default is No Limit. The setting range is 1k~1024k per second.

#### Learn Frames Rate:

To enable the Learn Frames Storm capability. User can use drop-down menu to select number of frames. Default is No Limit. The setting range is 1k~1024k per second.

#### Broadcast Rate:

To enable the Broadcast Storm capability. User can use drop-down menu to select number of frames. Default is No Limit. The setting range is 1k~1024k per second.

#### Multicast Rate:

To enable the Multicast Storm capability. User can use drop-down menu to select number of frames. Default is No Limit. The setting range is 1k~1024k per second.

#### Flooded unicast Rate:

To enable the Flooded unicast Storm capability. User can use drop-down menu to select number of frames. Default is No Limit. The setting range is 1k~1024k per second.

### NOTE:

After completing the function's setting, press **<Apply>** button to have this function taken effect.

## 4-2-17. SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. It is a protocol used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP "Enable", SNMP agent will be started up. If the field SNMP is set "Disable", SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

### **Function name:**

SNMP Configuration

### **Function description:**

This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click **<Apply>** button, the setting takes effect.

### **SNMP Configuration**

SNMP enabled	<input checked="" type="checkbox"/>
SNMP Trap destination	0.0.0.0
SNMP Get Community	public
SNMP Set Community	private
SNMP Trap Community	public

System Event	<input checked="" type="checkbox"/> Cold Boot	<input checked="" type="checkbox"/> Warm Boot
TP and Fiber Port Event	<input checked="" type="checkbox"/> Link Up	Link Up Counter 1
	<input checked="" type="checkbox"/> Link Down	Link Down Counter 0

Fig. 4-27 SNMP Configuration

### **Parameters description:**

SNMP enable:

The term SNMP enable here is used for the activation or de-activation of SNMP. Default is "Disable".

Get/Set/Trap Community:

Community name is used as password for authenticating if the

requesting network management unit belongs to the same community group. If they both don't have the same community name, they don't belong to the same group. Hence, the requesting network management unit can not access the device with different community name via SNMP protocol; If they both have the same community name, they can talk each other.

Community name is user-definable with a maximum length of 15 characters and is case sensitive. There is not allowed to put any blank in the community name string. Any printable character is allowable.

The community name for each function works independently. Each function has its own community name. Say, the community name for Read only works for Read function and can't be applied to other function such as Write and Trap.

Default SNMP function: Disable

Default community name for Get: public

Default community name for Set: private

Default community name for Trap: public

System Event:

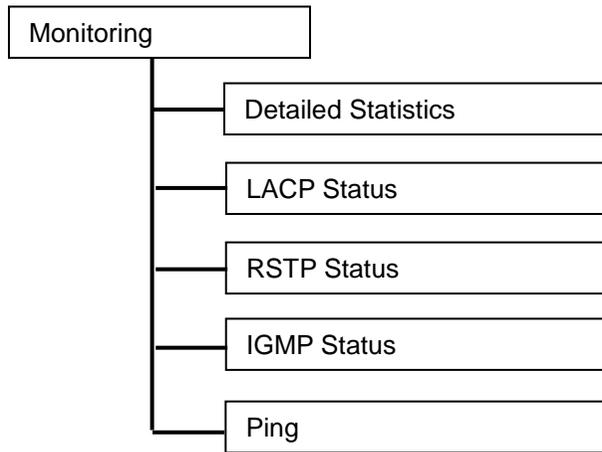
The System Event trap enable here is used for the "Cold Boot" or "Warm Boot" of system Event. Default is "Disable".

TP and Fiber Port Event:

The TP and Fiber Port Event trap enable here is used for the "Link Up" or "Link Down" of system Event. Default is "Disable".

### 4-3. Monitoring

There are six functions contained in the monitoring function.



### 4-3-1. Detailed Statistics

**Function name:**

Detailed Statistics

**Function description:**

Display the detailed counting number of each port's traffic. In the Fig. 4-26, the window can show all counter information each port at one time.

Statistics for Port 1																											
Clear		Refresh		Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port 9	Port 10	Port 11	Port 12	Port 13	Port 14	Port 15	Port 16	Port 17	Port 18	Port 19	Port 20	Port 21	Port 22	Port 23	Port 24
Receive Total												Transmit Total															
Rx Packets	33215											Tx Packets	21520														
Rx Octets	3390475											Tx Octets	5121779														
Rx High Priority Packets	-											Tx High Priority Packets	-														
Rx Low Priority Packets	-											Tx Low Priority Packets	-														
Rx Broadcast	-											Tx Broadcast	-														
Rx Multicast	-											Tx Multicast	-														
Rx Broad- and Multicast	1021											Tx Broad- and Multicast	0														
Rx Error Packets	0											Tx Error Packets	0														
Receive Size Counters												Transmit Size Counters															
Rx 64 Bytes	-											Tx 64 Bytes	-														
Rx 65-127 Bytes	-											Tx 65-127 Bytes	-														
Rx 128-255 Bytes	-											Tx 128-255 Bytes	-														
Rx 256-511 Bytes	-											Tx 256-511 Bytes	-														
Rx 512-1023 Bytes	-											Tx 512-1023 Bytes	-														
Rx 1024- Bytes	-											Tx 1024- Bytes	-														
Receive Error Counters												Transmit Error Counters															
Rx CRC/Alignment	-											Tx Collisions	-														

Fig. 4-29 Detailed Statistics for each port

**Parameter description:**

Rx Packets:

The counting number of the packet received.

Rx Octets:

Total received bytes.

Rx High Priority Packets:

Number of Rx packets classified as high priority.

Rx Low Priority Packets:

Number of Rx packets classified as low priority.

Rx Broadcast:

Show the counting number of the received broadcast packet.

Rx Multicast:

Show the counting number of the received multicast packet.

Rx Broad- and Multicast:

Show the counting number of the received broadcast with multicast packet.

Rx Error Packets:

Show the counting number of the received error packets.

Tx Packets:

The counting number of the packet transmitted.

TX Octets:

Total transmitted bytes.

Tx High Priority Packets:

Number of Tx packets classified as high priority.

Tx Low Priority Packets:

Number of Tx packets classified as low priority.

Tx Broadcast:

Show the counting number of the transmitted broadcast packet.

Tx Multicast:

Show the counting number of the transmitted multicast packet.

Tx Broad- and Multicast:

Show the counting number of the transmitted broadcast with multicast packet.

Tx Error Packets:

Show the counting number of the received error packets.

Rx 64 Bytes:

Number of 64-byte frames in good and bad packets received.

Rx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets received.

Rx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets received.

Rx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets received.

Rx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets received.

Rx 1024-Bytes:

Number of 1024-max\_length-byte frames in good and bad packets received.

Tx 64 Bytes:

Number of 64-byte frames in good and bad packets transmitted.

Tx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets transmitted.

Tx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets transmitted.

Tx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets transmitted.

Tx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets transmitted.

Tx 1024-Bytes:

Number of 1024-max\_length-byte frames in good and bad packets transmitted.

Rx CRC/Alignment:

Number of Alignment errors and CRC error packets received.

Rx Undersize:

Number of short frames (<64 Bytes) with valid CRC.

Rx Oversize:

Number of long frames(according to max\_length register) with valid CRC.

Rx Fragments:

Number of short frames (< 64 bytes) with invalid CRC.

Rx Jabber:

Number of long frames(according to max\_length register) with invalid CRC.

Rx Drops:

Frames dropped due to the lack of receiving buffer.

Tx Collisions:

Number of collisions transmitting frames experienced.

Tx Drops:

Number of frames dropped due to excessive collision, late collision, or frame aging.

Tx Overflow:

Number of frames dropped due to the lack of transmitting buffer.

## 4-3-2. LACP Status

### Function name:

LACP Status

### Function description:

Display LACP status. Fig. 4-30 illustrates that LACP Status window can show LACP information and status for all ports in the same time.

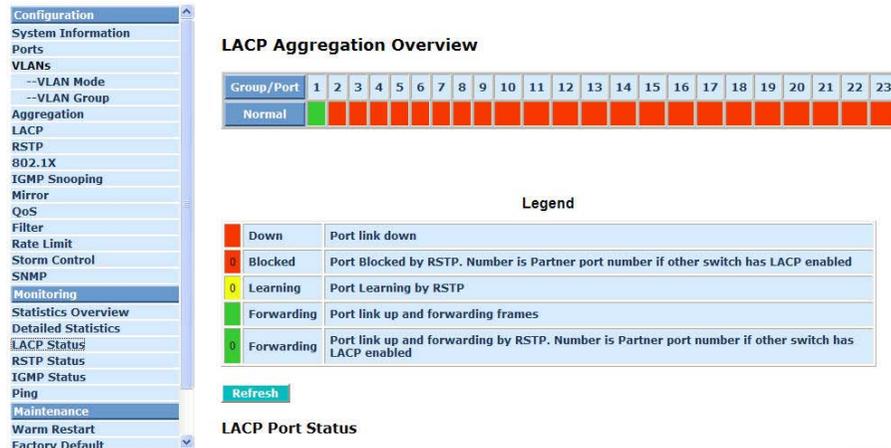


Fig. 4-30 LACP Status

### Parameter description:

LACP Aggregation Overview:

Show the group/port status. Default will set to red sign for port link down, user can check legend table below for all reference.

LACP Port Status:

Group/Port:

Show the port number.

Normal : as Legend.

### 4-3-3. RSTP Status

**Function name:**

RSTP Status

**Function description:**

Display RSTP status. Fig. 4-28 shows you that RSTP window can present VLAN bridge information and the status of all ports.

**RSTP VLAN Bridge Overview**

VLAN Id	Bridge Id	Hello Time	Max Age	Fwd Delay	Topology	Root Id
1	32769:00-a0-57-15-2a-f2	2	20	15	Steady	This switch is Root!

**Refresh**

**RSTP Port Status**

Port/Group	Vlan Id	Path Cost	Edge Port	P2p Port	Protocol	Port State
Port 1						Non-STP
Port 2						Non-STP
Port 3						Non-STP
Port 4						Non-STP
Port 5						Non-STP
Port 6						Non-STP
Port 7						Non-STP
Port 8						Non-STP
Port 9						Non-STP

Fig. 4-31 RSTP Status

**Parameter description:**

RSTP VLAN Bridge Overview:

VLAN Id:

Show the VLAN ID.

Bridge Id:

Show this switch's current bridge priority setting and bridge ID which stands for the MAC address of this switch.

Hello Time:

Show the current hello time of the root bridge. Hello time is a time interval specified by root bridge, used to request all other bridges periodically sending hello message every "hello time" seconds to the bridge attached to its designated port.

Max Age:

Show the root bridge's current max age time.

Fwd Delay:

Show the root bridge's forward delay time.

Topology:

Show the root bridge's spanning tree topology.

Root Id:

Show root bridge ID of this network segment. If this switch is a root bridge, the "This switch is Root" will show this switch's bridge ID.

#### 4-3-4. IGMP Status

**Function name:**

IGMP Status

**Function description:**

Display IGMP status. In Fig. 4-29, the window shows VLAN ID for each multicast group.

#### IGMP Status

VLAN ID	Querier	Queries transmitted	Queries received	v1 Reports	v2 Reports	v3 Reports	v2 Leaves
---	Idle	0	0	0	0	0	0

#### IGMP Status

Page:1

VLAN ID	IP Address	Ports
---	No active groups	---

Refresh	First Page	Prev Page	Next Page
---------	------------	-----------	-----------

Fig. 4-32 IGMP Status

**Parameter description:**

VLAN Id:

Show VLAN Id for each multicast group.

Querier:

Show the group membership queries status.

Queries transmitted:

To count the group membership queries transmitted.

Queries received:

To count the group membership queries received.

V1 Reports:

When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The host then sets a timer, with a value less than the *Max Response Time* field in the query, for each group to which it belongs. It Calculate the number of times of IGMPV1 report.

V2 Reports:

When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The host then sets a timer, with a value less than the *Max Response Time* field in the query, for each group to which it belongs. It Calculate the number of times of IGMPV2 report.

#### V3 Reports:

When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The host then sets a timer, with a value less than the *Max Response Time* field in the query, for each group to which it belongs. It Calculate the number of times of IGMPV3 report.

#### V2 Leaves:

When a host leaves a group, it sends a leave group membership message to multicast routers on the network, it show the leaves number.

### 4-3-5. Ping Status

**Function name:**

Ping Status

**Function description:**

To set up target IP address for ping function and display ping status. In Fig. 4-30, the window shows the ping information.

#### Ping Parameters

Target IP address	<input type="text"/>
Count	1 ▾
Time Out (in secs)	1 ▾

Apply

Ping Results	
Target IP address	0.0.0.0
Status	Test complete
Received replies	0
Request timeouts	0
Average Response Time (in ms)	0

Refresh

Fig. 4-33 Ping

**Parameter description:**

Ping Parameters:

Target IP address:

Set up a Target IP address to ping.

Count:

Use drop-down menu to set number of echo requests to send. Four type of number can choose, there are 1, 5, 10 and 20.

Default: 1

Time Out (in secs):

Use drop-down menu to set number of echo requests time out in second. Four type numbers can choose, there are 1,5,10 and 20.

Default: 1

**NOTE:** All the functions should press **<Apply>** button to start up after you set up the parameters.

Ping Results:

Target IP address:

Show the active target IP address.

Status:

Show the result of the ping status.

Received replies:

Show the received replies number of times.

Request timeouts:

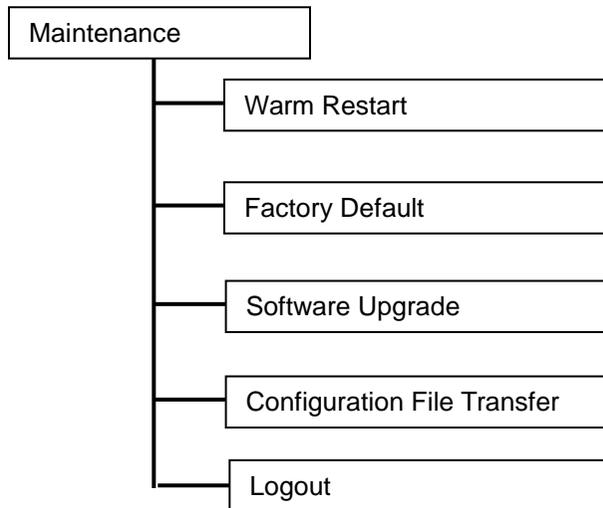
Show the timeout of request.

Average Response times (In ms):

Show the average response time in milliseconds.

## 4-4. Maintenance

There are five functions contained in the maintenance function.



### 4-4-1. Warm Restart

Web Smart Switch offers many approaches to reboot your switch, such as: power up, hardware reset and software reset. You can press RESET button in the front panel of your switch to reset the device and to retrieve default settings. After upgrading software, you have to reboot the device to have new configuration take effect. The function being discussed here is software reset.

**Function name:**

Warm Restart

**Function description:**

Reboot the switch. Reboot takes the same effect as the RESET button on the front panel of the switch. Press **<Yes>** button to confirm warm restart function and it will take around thirty (30) seconds to complete the system boot.

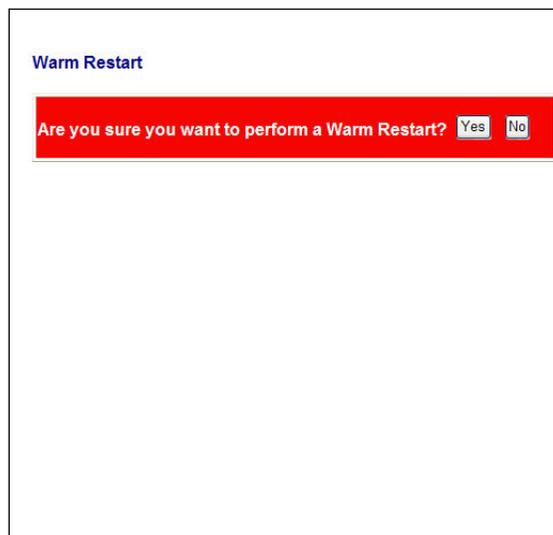


Fig. 4-34 Warm Restart

## 4-4-2. Factory Default

### **Function name:**

Factory Default

### **Function description:**

Factory Default provides the function to retrieve default settings and replace current configuration. Except the IP address setting, all settings will be restored to the factory default values when “Factory Default” function is performed. If you want to restore all configurations including the IP address setting to the factory default, please press the “RESET” button on the front panel.

Note for “RESET” button:

You must press the “RESET” button over 3 seconds to restore the factory default setting.

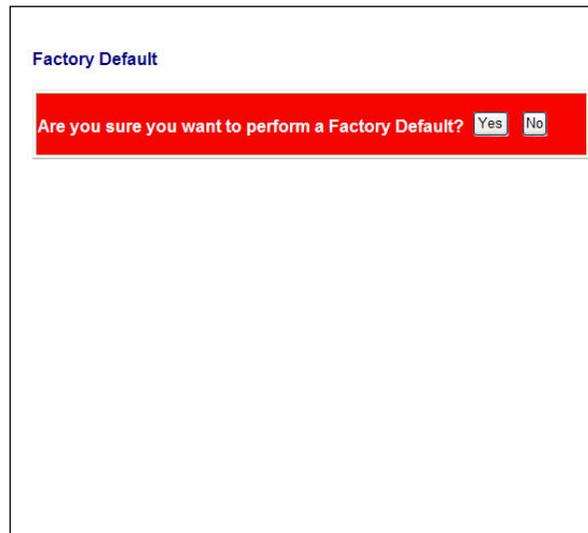


Fig. 4-35

### 4-4-3. Software Upgrade

**Function name:**

Software Upgrade

**Function description:**

You can just click Browse button to retrieve the file you want in your system to upgrade your switch.



Fig. 4-36 Software Upgrade

## 4-4-4. Configuration File Transfer

**Function name:**

Configuration File Transfer

**Function description:**

You can backup your switch's configuration file into your computer folder in case accident happens. In addition, uploading backup configuration file into a new or a crashed switch can save much time and avoid mistakes.

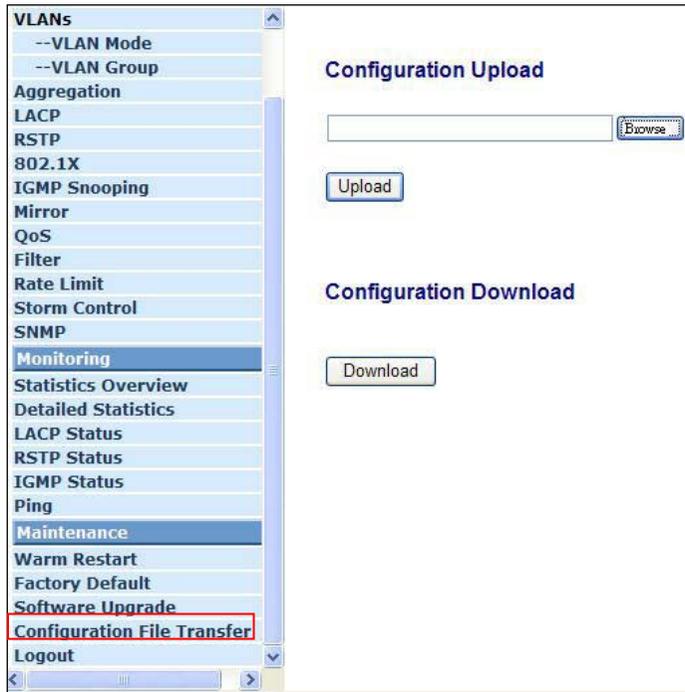


Fig. 4-37 Configuration Upload/Download

#### 4-4-5. Logout

In addition to auto logout function we just mentioned in system configuration section, the switch also allows administrators to logout manually by Logout function.

**Function name:**

Logout

**Function description:**

The switch allows you to logout the system to prevent other users from the system without the permission. If you do not logout and exit the browser, the switch will automatically have you logout. Besides this manually logout and implicit logout, you can set up the parameter of Auto Logout Timer in system configuration function to explicitly ON/OFF this logout function.



Fig. 4-38

**Parameter description:**

Auto/Manual Logout:

If no action and no key is stroke as well in any function screen more than the minutes you set up in Auto Logout Timer, the switch will have you logout automatically. Or press the **<Logout>** button in Logout function to exit the system manually.

# 5. Maintenance

## 5-1. Resolving No Link Condition

The possible causes for a no link LED status are as follows:

- The attached device is not powered on
- The cable may not be the correct type or is faulty
- The installed building premise cable is faulty
- The port may be faulty

## 5-2. Q&A

1. Computer A can connect to Computer B, but cannot connect to Computer C through the 24-Port GbE Web Smart PoE Switch.
  - ✓ The network device of Computer C may fail to work. Please check the link/act status of Computer C on the LED indicator. Try another network device on this connection.
  - ✓ The network configuration of Computer C may be something wrong. Please verify the network configuration on Computer C.
2. The uplink connection function fails to work.
  - ✓ The connection ports on another must be connection ports. Please check if connection ports are used on that 24-Port GbE Web Smart PoE Switch.
  - ✓ Please check the uplink setup of the 24-Port GbE Web Smart PoE Switch to verify the uplink function is enabled.
3. The console interface cannot appear on the console port connection.
  - ✓ 24-Port GbE Web Smart PoE Switch has no console port, so you cannot use console interface to connect with 24-Port GbE Web Smart PoE Switch.
4. How to configure the 24-Port GbE Web Smart Switch.
  - ✓ User can use IE browser program in window series of computer to control the web smart functions in 24-Port GbE Web Smart PoE Switch. First, choose any port in 24-Port GbE Web Smart PoE Switch. Then, use IE and type default IP address, 192.168.1.1, to connect to 24 Gigabit with RJ45 network line. Finally, the login screen will appear at once.

# Appendix A

## Technical Specifications

### *Features*

- 20 (10/100/1000Mbps) Gigabit Ethernet (TP) switching ports are compliant with IEEE802.3, 802.3u, 802.3z, 802.3ab and 802.3af.
- 4 Gigabit TP/(100/1000M) SFP fiber are dual media ports with auto detected function.
- Non-blocking store-and-forward shared-memory Web-Smart switched.
- Supports auto-negotiation for configuring speed, duplex mode.
- Supports 802.3x flow control for full-duplex ports.
- Supports collision-based and carrier-based backpressure for half-duplex ports.
- Any ports can be in disable mode, force mode or auto-polling mode.
- Supports Head of Line (HOL) blocking prevention.
- Supports broadcast storm filtering.
- Web-based management provides the ability to completely manage the switch from any web browser.
- Supports Port-based VLAN and Tag-based (IEEE802.1Q) VLAN.
- Auto-aging with programmable inter-age time.
- Supports 802.1p Class of Service with 2-level priority queuing.
- Supports port trunking with flexible load distribution and failover function.
- Supports port sniffer function
- Programmable maximum Ethernet frame length of range from 1518Bytes to 12.2KB jumbo frame.
- Efficient self-learning and address recognition mechanism enables forwarding rate at wire speed.
- Support IEEE802.3af Power over Ethernet and By supplying the power mid-span

## Hardware Specifications

- **Standard Compliance:** IEEE802.3/802.3ab / 802.3z / 802.3u / 802.3x/ 802.3af
- **Network Interface:**

Configuration	Mode	Connector	Port
10/100/1000Mbps Gigabit TP	NWay	TP (RJ-45)	1 - 24
1000Base-SX Gigabit Fiber	1000 FDX	*SFP	21,22,23,24 (Option)
1000Base-LX Gigabit Fiber	1000 FDX	*SFP	21,22,23,24 (Option)
1000Base-LX Single Fiber WDM (BiDi)	1000 FDX	*SFP	21,22,23,24 (Option)
100Base-FX Fibert	100 FX	SFP	21,22,23,24 (Option)

\*Port 21,22,23, 24 are TP/ (100/1000M) SFP fiber dual media ports with auto detected function

\*Optional SFP module supports LC or BiDi SC transceiver

- **Transmission Mode:** 10/100Mbps support full or half duplex  
1000Mbps support full duplex only
- **Transmission Speed:** 10/100/1000Mbps for TP  
100/1000M for Fiber
- **Full Forwarding/Filtering Packet Rate:** PPS (packets per second)

Forwarding Rate	Speed
1,488,000PPS	1000Mbps
148,800PPS	100Mbps
14,880PPS	10Mbps

- **MAC Address and Self-learning:** 8K MAC address
- **Buffer Memory:** Embedded 500 KB frame buffer
- **Flow Control:** IEEE802.3x compliant for full duplex  
Backpressure flow control for half duplex
- **Cable and Maximum Length:**

<b>TP</b>	Cat. 5 UTP cable, up to 100m
<b>1000Base-SX</b>	Up to 220/275/500/550m, which depends on Multi-Mode Fiber type
<b>1000Base-LX</b>	Single-Mode Fiber, up to 10/30/50Km
<b>1000Base-LX WDM (BiDi)</b>	Single-Mode Single Fiber, up to 20Km
<b>100Base-FX</b>	Multi-mode Fiber, up to 2Km
<b>100Base-FX</b>	Single-mode Fiber, up to 20Km

▪ **Diagnostic LED:**

System LED : Power  
 Per Port LED:  
   10/100/1000M TP Port 1 to 24 : LINK/ACT, 10/100/1000Mbps  
   PoE Port 1 to 24 : PoE  
   100/1000M SFP Fiber Port 21to24 : SFP(LINK/ACT)

▪ **Power Requirements** : AC Line

Voltage : 100~240 VAC  
 Frequency : 50~60 Hz  
 Consumption : 185 W  
                   : 25W for main board

- **Ambient Temperature** : 0° to 40°C
- **Humidity** : 10% to 90%
- **Dimensions** : 44(H) × 442(W) × 246.5(D) mm
- **Comply with FCC Part 15 Class A & CE Mark Approval**

**Management Software Specifications**

<b>System Configuration</b>	Auto-negotiation support on 10/100/1000Base-TX ports, Web browser can set transmission speed (10/100/1000Mbps) and operation mode (Full/Half duplex) on each port, enable/disable any port, set VLAN group, set Trunk Connection.
<b>Networking Convergence Algorithm</b>	IEEE802.1D Spanning Tree IEEE802.1w Rapid Spanning Tree
<b>VLAN Function</b>	Port-Base / 802.1Q-Tagged, allowed up to 16 active VLANs in one switch.
<b>Trunk Function</b>	Ports trunk connections allowed
<b>Quality of Service (QoS)</b>	Referred as Class of Service (CoS) by the IEEE 802.1P standard Four queues per port
<b>Power over Ethernet</b>	IEEE 802.3af compliant Supports 24-port up to 7.7 watts Endpoint with 48VDC power through RJ-45 pin 1,2,3,6 Auto detect powered device and consumption levels Supports per port power consumption monitoring Smart feature for PD on/off, PD detection, power level, PD status and power feeding priority Supports per port power priority setting.
<b>Network Management</b>	Web browser support based on HTTP Server

Note: Any specification is subject to change without notice.