



GEL-2460

24-Port L2 Managed Gigabit Ethernet Switch, 2 Ports SFP/RJ45 Combo

User Manual

V1.0

Digital Data Communications Asia Co., Ltd.

<http://www.level1.com>

The information in this document is subject to change without notice. Unless the explicit written permission of Digital Data Communications 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, Digital Data Communications Corporation, (hereinafter called "LevelOne") 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, LevelOne 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 LevelOne.

All defective Products must be returned to LevelOne 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. LevelOne will not accept collect shipments or those returned without an RMA number.

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

EXCLUSIONS. The warranty as mentioned above does not apply to the following conditions, in LevelOne's judgment, it contains (1) customer does not comply with the manual instructions offered by LevelOne 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 LevelOne 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 excused 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 LevelOne 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.

LEVELONE 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 LEVELONE 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 LevelOne 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 Digital Data Communications Corporation ("LevelOne"):

- (1) To use the LevelOne'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 LevelOne.
- (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 LevelOne's software or hardware products. Without the prior written consent of LevelOne, 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. LevelOne and/or its licensors retain all title and ownership in both the Software and its related documentation, including any revisions made by LevelOne. 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 LevelOne'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 LevelOne 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. LevelOne 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 LevelOne, then LevelOne will replace the media. LevelOne 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 LevelOne 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 LevelOne or the authorized agents. The maximum liability of LevelOne 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 LEVELONE AND ITS LICENSORS MAKE NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION. LEVELONE AND ITS LICENSORS DISCLAIM ALL OTHER WARRANTIES, INCLUSIVE OF WITHOUT LIMITATION, IMPLIED WARRANTIES OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. FURTHER, LEVELONE 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 LEVELONE 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 LEVELONE, EVEN IF LEVELONE HAS BEEN NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE. IN NO EVENT SHALL THE LIABILITY OF LEVELONE IN CONNECTION WITH THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO LEVELONE FOR THE LICENSE.

TERM AND TERMINATION. The License is effective until terminated; however, all of the restrictions in regard to LevelOne'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 LevelOne'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 LevelOne'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 LEVELONE AND LICENSEE.



Chapter 1	Product Overview	1
1.1	Key Features	1
1.2	Technical Specification	2
1.3	Physical Characteristics	3
1.3.1	Front Panel	3
1.3.2	Rear Panel	5
Chapter 2	Hardware Installation	6
2.1	Installation Requirements	6
2.2	Installing the Switch	6
2.2.1	Installing the Switch in a 19-inch Rack	6
2.2.2	Installing the Switch on a Level Surface	7
2.3	Connecting Network Devices	7
2.4	Connecting the Power	8
Chapter 3	Logging in to the Switch	9
3.1	Configuring Your Computer	9
3.2	Logging in to the Switch	10
3.3	Introduction to Web UI	12
3.3.1	Web UI Layout	12
3.3.2	Introduction to Menu Items	13
3.3.3	Description of Common BLevelOneons	15
3.3.4	Web UI Idle Timeout	16
Chapter 4	Start Menu	17
4.1	Setup Wizard	17
4.1.1	Running the Setup Wizard	17
4.1.2	Password Settings	18
4.1.3	IP Address Settings	18
4.1.4	Switch Type Settings	19
4.1.5	Link Aggregation Group Settings	20
4.1.6	Port Mirroring Settings	21
4.2	Summary Statistics	23
4.3	Restart	24
Chapter 5	Status	25
5.1	System Information	25
5.2	Summary Statistics	26
5.3	Port Statistics	26
5.3.1	Port Traffic Chart	27
5.3.2	Port Details	28
Chapter 6	Basic	29

6.1	Setup Wizard.....	29
6.2	System Settings	29
6.3	Port Settings.....	31
6.4	Port Mirroring.....	33
Chapter 7	Advanced	35
7.1	VLAN.....	35
7.1.1	VLAN Mode Settings.....	35
7.1.2	Port-based VLAN	35
7.1.3	Tag-based VLAN.....	38
7.2	RSTP.....	43
7.2.1	RSTP Status	43
7.2.2	RSTP Settings	46
7.3	LACP.....	48
7.3.1	Introduction to LACP	48
7.3.2	LACP Status	49
7.3.3	LACP Settings.....	50
7.4	Link Aggregation.....	52
7.4.1	Introduction to Link Aggregation.....	52
7.4.2	LAG Settings.....	52
7.4.3	LAG List	54
7.5	QoS.....	55
7.5.1	Disabling QoS.....	55
7.5.2	802.1p Priority Settings.....	55
7.5.3	Port-based Priority Settings	56
7.6	SNMP.....	58
Chapter 8	Linkage.....	59
8.1	Linkage Management.....	59
8.1.1	Remote Switch Discovery List.....	59
8.1.2	Remote Switch Management - Single Switch	61
8.1.3	Remote Switch Management - Batch Operation	70
8.1.4	Configuration Examples for Remote Switch Management.....	71
8.1.5	Linkage Configuration	75
8.1.6	Linkage Log	76
8.1.7	Network Topology	76
Chapter 9	Security	79
9.1	Security Log	79
9.2	Rate Limiting	80
9.2.1	Storm Control.....	80
9.2.2	Rate Limiting.....	80
9.3	IP Address Filtering	82
9.3.1	Introduction to DHCP Snooping.....	82

9.3.2	IP Filtering Settings	83
9.4	IP/MAC Binding	84
9.4.1	IP/MAC Binding.....	84
9.4.2	The Operation Principle of IP/MAC Binding	84
9.4.3	IP/MAC Binding Settings.....	85
9.4.4	IP/MAC Binding List	86
9.5	MAC/Port Binding.....	88
9.5.1	Dynamic MAC Address Table.....	88
9.5.2	Static MAC/Port Binding	88
9.5.3	MAC/Port Binding Settings.....	89
9.5.4	MAC/Port Binding List.....	90
9.6	Access Restriction.....	92
Chapter 10	Administration	93
10.1	System Time.....	93
10.2	Configuration	95
10.3	Firmware Upgrade.....	96
10.4	Restart.....	97
10.5	Help.....	97
Appendix A	Contact Information	98
Appendix B	Figure Index.....	99
Appendix C	Table Index.....	102

Chapter 1 Product Overview

Thanks for choosing the GEL-2460 24-Port Intelligent Managed Gigabit Switch from levelone technologies co. ltd.

The GEL-2460 is a 24-Port, layer 2 wire-speed, intelligentmanaged gigabit switch. It offers 24 x 10/100/1000M auto-negotiation ports with 2 SFP combo ports. All RJ-45 ports support auto MDI/MDI-X.

The GEL-2460 provides non-blocking wire-speed performance on all ports, making it ideal for use at the core of large networks, in data centers and areas of high traffic volume such as internet cafes and libraries.

The switch operates in both port speed and duplex mode, featuring auto-negotiation to enhance operability. The device also supports Jumbo frame, configurable to a maximum frame size of 1518-9600 bytes, as well as store-and-forward switching and SNMP, along with a host of other features.

1.1 Key Features

- Complies with IEEE802.3ab, IEEE802.3ad, IEEE802.3z and IEEE802.1p standards
- Supports store-and-forward switching method
- Provides non-blocking wire-speed switching performance on all ports
- All RJ-45 ports support auto MDI/MDI-X
- All RJ-45 ports support auto-negotiation for port speed and duplex mode
- Supports the port speed and duplex mode settings
- Supports Full/Half duplex transfer mode for 10 and 100Mbps and Full duplex transfer mode for 1000Mbps
- Any port can be enabled or disabled as desired
- Supports Jumbo frame, configurable maximum frame size (1518-9600 bytes)
- Supports MAC address auto-learning
- Supports MAC address auto-aging with configurable aging time (default: 300s)
- Supports MAC address table management
- Supports static MAC/Port binding

- Supports port-based VLAN
- Supports IEEE 802.1Q tag-based VLAN
- Supports shared VLAN
- Supports static link aggregation
- Supports Link Aggregation Control Protocol (LACP)
- Supports ARP spoofing prevention
- Supports port mirroring, user-defined mirroring port and mirrored port(s)
- Supports IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- Supports Simple Management Network Protocol (SNMPv1 and SNMPv2c)
- Supports IEEE 802.1p priority
- Supports port-based priority
- Supports linkage management, network topology discovery
- Supports summary traffic statistics and detailed traffic statistics for each port
- Supports port-based rate limiting
- Supports broadcast storm control
- Supports security log
- Provides the Web User Interface (Web UI)
- Provides the Command Line Interface (CLI) which can be accessed through the console port
- Prevents concurrent logins from different computers
- Supports password change
- Supports online firmware upgrade
- Supports factory default settings restore
- Supports configuration backup and restore

1.2 Technical Specification

Item	Specification
Dimension (L x W x H)	440mm x 230mm x 44mm
Ports	24 10/100/1000M RJ-45 Ports + 2 Gigabit SFP Combo Ports

Network Cables	<ul style="list-style-type: none"> • 10Base-T: UTP/STP Category 3, 4, 5 • 100Base-TX: UTP/STP Category 5 • 1000Base-T: UTP/STP Category 5e, 6
	<ul style="list-style-type: none"> • Multi-mode: 50/125µm multi-mode fiber, with LC connector, 550m transmission distance • Single-mode short-distance: 9/125µm single-mode fiber, with LC connector, transmission distance 10Km • Single-mode middle-distance: 9/125µm single-mode fiber, with LC connector, transmission distance 40Km • Single-mode long-distance: 9/125µm single-mode fiber, with LC connector, transmission distance 70Km
Power Supply	100V~240V AC, 50/60Hz
Power Consumption	30W, MAX
Operating Temperature	32° to 104° F (0° to 40° C)
Storage Temperature	-40° to 158° F (-40° to 70° C)
Operating Humidity	10% to 90% relative humidity, non-condensing
Storage Humidity	5% to 90% relative humidity, non-condensing

Table 1-1 Technical Specification

1.3 Physical Characteristics

1.3.1 Front Panel

As shown in Figure 1-1, the front panel of the GEL-2460 Switch contains the LEDs, 24 10/100/1000M RJ-45 ports, 2 Gigabit SFP combo ports, a Reset bLevelOneon, and a Console port. Therein, the two SFP ports (SFP1 and SFP2) are shared with RJ-45 Port 23 and Port 24 respectively. The SFP port has priority over the corresponding RJ-45 port. That is, when an SFP port is active, the corresponding RJ-45 port is disabled.



Figure 1-1 Front Panel of GEL-2460

 **Note**

The product pictures shown in Figure 1-1 and Figure 1-2 are for reference only. For details, please prevail in kind.

1. LEDs

LED	Full Name	Status and Description
PWR	Power LED	The LED lights steady when the power is being supplied to the Switch.
SYS	System LED	The LED flashes slowly when the Switch is operating properly. The LED will extinguish or light steady if a fault has occurred in the Switch.
Link/Act	RJ-45 Port Status LED	The LED lights steady when a link between the corresponding port and another device is detected. The LED flashes when the corresponding port is sending or receiving data.
1000M	RJ-45 Port Speed LED	The LED lights steady when another device is connected to the corresponding port and a 1000Mbps link is established between them.
SFP	SFP Port Status LED	The LED lights steady when a link between the corresponding port and another device is detected. The LED flashes when the corresponding port is sending or receiving data.

Table 1-2 Description of LEDs on the Front Panel

2. Reset BLevelOneon

If you forgot the administrator password, you need to use the Reset bLevelOneon to reset the Switch to factory default settings. The operation is as follows: While the Switch is powered on, use a pin or paper clip to press and hold the Reset bLevelOneon for more than 5 seconds, and then release the bLevelOneon. After that, the Switch will restart with factory default settings.

3. Console Port

You can access and manage the Switch through the console port.

1.3.2 Rear Panel

As shown in Figure 1-2, the three-pronged power connector is located on the rear panel of the Switch.



Figure 1-2 Rear Panel of the Switch

Chapter 2 Hardware Installation

2.1 Installation Requirements

Before you install the Switch, observe the following guidelines:

- Make sure that the Switch is powered off.
- Make sure that the workbench or rack is level and stable.
- Do not place heavy objects on the Switch.
- Make sure that there is proper heat dissipation and adequate ventilation around the Switch.
- Position the Switch in a dry environment
- Position the Switch out of direct sunlight and away from sources of heat and ignition
- Position the Switch away from sources of electrical noise, such as high power radio transmitters, radar stations, and so on.

2.2 Installing the Switch

You can install the Switch in a 19-inch standard rack; or on a level surface such as a desktop or shelf if you don't have a 19-inch standard rack.

2.2.1 Installing the Switch in a 19-inch Rack

To install the Switch in a 19-inch rack (see Figure 2-1), follow these steps:

- Step 1** Attach the two L-shaped brackets to the sides of the Switch with the supplied screws and secure them tightly.
- Step 2** Position the Switch into the rack and use the supplied screws to secure it in the rack.



Figure 2-1 Installing the Switch in a Rack

2.2.2 Installing the Switch on a Level Surface

To install the Switch on a level surface (such as a desktop or shelf), follow these steps:

- Step 1** Place the Switch upside down on a sturdy, flat surface with a power outlet nearby.
- Step 2** Remove the adhesive backing from the supplied rubber feet. Attach the four rubber feet to the four round recessed areas on the bottom of the Switch.
- Step 3** Turn the Switch over to make it right side up on the flat surface.

2.3 Connecting Network Devices

To connect network devices to the GEL-2460 Switch, follow these steps:

- Step 1** Make sure all devices you will connect to the Switch are powered off.
- Step 2** Connect a standard network cable from an available port on the Switch to a PC or other network device.
- Step 3** Repeat step 2 to connect rest network devices.

Note

All RJ-45 ports on the Switch support auto MDI/MDI-X feature. This means that you can use either a crossover cable or straight-through cable to connect a device to the Switch.

2.4 Connecting the Power

The GEL-2460 Switch will work with AC power in the range 100-240V AC, 50-60Hz. To prevent the Switch from working abnormally or being damaged, make sure that the power supply and connectivity are normal, and the power outlet is grounded properly before powering on the Switch.

The GEL-2460 Switch does not have an on/off switch. To supply power to the Switch, follow these steps:

- Step 1** Connect one end of the power cord to the power connector on the rear panel of the Switch. Then plug the other end of the power cord to a grounded three-prong AC power outlet.
- Step 2** Verify that the power LED (PWR) is lit, indicating that the Switch is powered on. If not, check to make sure that the power cord is correctly plugged in and the power outlet is good.

After the Switch is powered on, it will enter the self-test phase. During this phase, you can verify that the Switch starts up properly and the network connections are operational by checking the LED states, as described in Table 1-2.

Chapter 3 Logging in to the Switch

You can configure and manage the Switch through an intuitive and easy-to-use Web UI. Before configuring the Switch via Web UI, you need to properly install and configure TCP/IP properties on the computer that you use to administer the Switch.

3.1 Configuring Your Computer

To configure the Switch via Web UI, you need to assign your computer an IP address on the same subnet as the Switch. The Switch's default IP address is 192.168.1.1 with a subnet mask of 255.255.255.0.

Here we describe how to set a static IP address in Windows XP. The steps are as follows:

- Step 1** Click **Start > Settings > Control Panel**.
- Step 2** Double-click **Network Connections** icon.
- Step 3** Right-click the **Local Area Connection** icon and select **Properties**.
- Step 4** On the **General** tab, click the **Internet Protocol (TCP/IP)** item, and then click the **Properties** button.
- Step 5** Select the **Use the following IP address** radio button, enter 192.168.1.x (x is between 2 and 254, including 2 and 254) in the **IP address** text box, and 255.255.255.0 in the **Subnet mask** text box.

3.2 Logging in to the Switch

If you have Microsoft Windows or Linux operating system installed on your computer, you can configure the Switch through the Web browser (such as Internet Explorer and Firefox). If you use Internet Explorer, version 5.0 or higher is required.

To login to the Switch, do the following: Open a Web browser, enter the Switch's IP address (the default is **192.168.1.1**) in the address bar, and then press **<Enter>** key, see Figure 3-1.

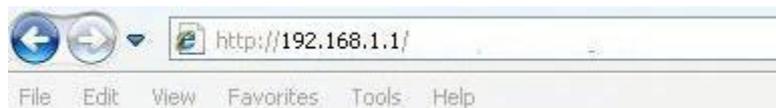


Figure 3-1 Entering IP address in the Address Bar

A login screen prompts you for your user name and password, see Figure 3-2. When you first login to the Switch, you should use the default administrator account: Enter **admin** as the username and password (the default username and password both are **admin**), and then click **OK**.



Figure 3-2 Login Screen

If your username and password are correct, it will display the homepage shown in Figure 3-3.

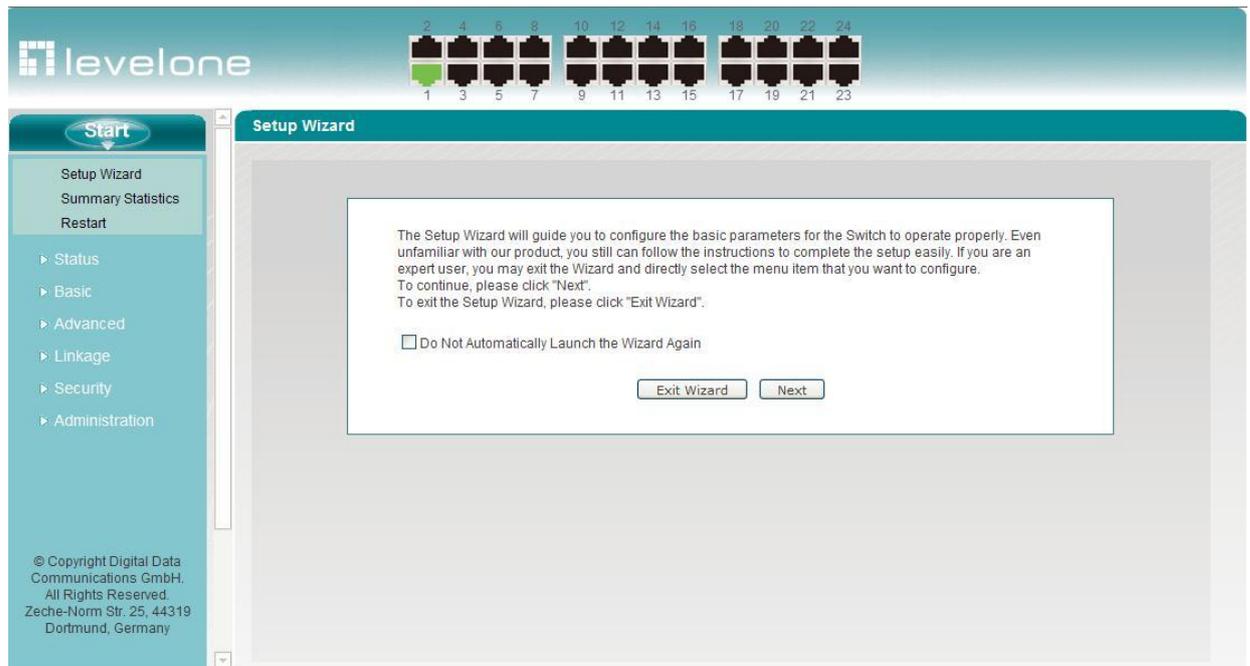


Figure 3-3 Homepage - Setup Wizard

3.3 Introduction to Web UI

3.3.1 Web UI Layout

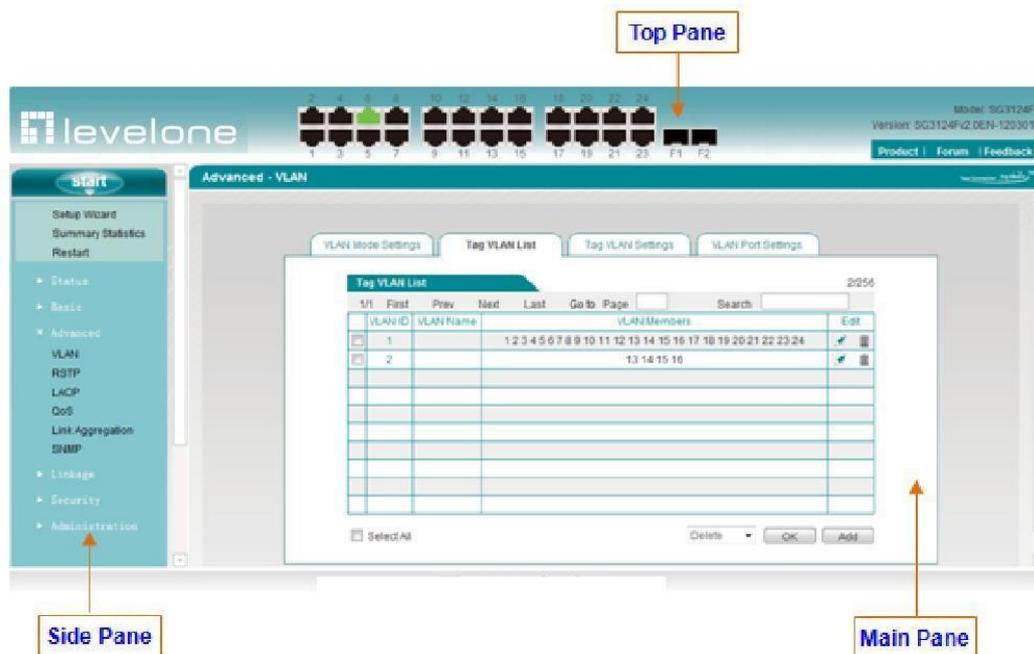


Figure 3-4 Web UI Layout

Each page of the Switch's Web UI consists of four panes:

1. **Top Pane:** It displays the LEVELONE logo, port graphics, model and version, and three shortcut icons.
 - 1) **LEVELONE Logo:** Click to link to the homepage of the LEVELONE website.
 - 2) **Port Graphics:** It displays the current status of the switch ports.
The background color of each port icon indicates the port status.
 - Black: The port is enabled, but the link is down.
 - Green: The port is enabled, and the link is up.
 - Grey: The port is disabled.
 If you hold your cursor over a port icon, it will pop up a label displaying the port status information. If a port is up, you can click the port icon to view its detailed traffic statistics.
 - 3) **Model and Version:** They display the product model and firmware version of the Switch.

- 4) **Short Icons:** They are used for fast link to the corresponding pages on the website of Digital Data Communications Asia Co., Ltd.
- **Product:** Click to link to the products page of the LEVELONE website to find more products.
 - **Forum:** Click to link to the forum homepage of the LEVELONE website to participate in product discussions.
 - **Feedback:** Click to link to send us your feedback by E-mail.
2. **Main Pane:** It is the location where you can configure each feature of the Switch, view configuration, status and statistics.
3. **Side Pane:** It displays the two-level main menu bar (i.e., navigation bar).

3.3.2 Introduction to Menu Items

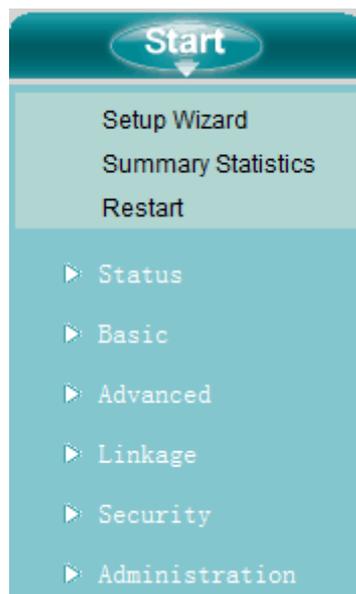


Figure 3-5 Main Menu Bar

As shown in Figure 3-5, the two-level main menu bar contains seven first level menu items, which include **Start**, **Status**, **Basic**, **Advanced**, **Linkage**, **Security** and **Administration**. You can click a first level menu item to reveal its submenu items, click again to hide them. Each second level menu item serves as a link to one Web page. The following table lists all of the first level menu items together with their submenu items, and the feature description. Using this table, you can quickly find the features you want to configure.

First Level Menu	Second Level Menu	Feature Description

Start	Setup Wizard	It guides you to quickly configure the basic features of the Switch.
	Summary Statistics	It displays summary traffic statistics on a port-by-port basis.
	Restart	It allows you to restart the Switch.
Status	System Information	It displays system resources usage information and basic system information.
	Summary Statistics	It displays summary traffic statistics on a port-by-port basis.
	Port Statistics	It displays the real-time traffic chart and detailed traffic statistics for each port.
Basic	Setup Wizard	It guides you to quickly configure the basic features of the Switch.
	System Settings	It allows you to enable or disable DHCP relay agent, DHCP client, ARP spoofing defense, configure IP address, subnet mask, CPU VLAN ID, MAC address aging time, system name and password.
	Port Settings	It allows you to configure and view basic information per port, including status, speed/duplex mode, maximum frame, port protection, etc.
	Port Mirroring	It allows you to choose one mirroring port, and one or more mirrored ports.
Advanced	VLAN	It allows you to configure VLAN (Virtual Local Area Network) including port-based VLAN and 802.1Q VLAN.
	RSTP	It allows you to configure RSTP (Rapid Spanning-Tree Protocol).
	LACP	It allows you to configure LACP (Link Aggregation Control Protocol).
	Link Aggregation	It allows you to configure static link aggregation groups.
	QoS	It allows you configure 802.1p priority and port-based priority.
	SNMP	It allows you to configure SNMP service.
Linkage	Linkage Management	It allows you to view and manage the remote switches in the same broadcast domain.
	Linkage Configuration	It displays the configuration files retrieved from the remote switches.
	Linkage Log	It displays the log messages of the local Switch and remote switches.

	Network Topology	It displays the network topology of the switches in the same broadcast domain, which support topology discovery protocol.
Security	Security Log	It displays security log messages.
	Rate Limiting	It allows you to set the maximum bandwidth for ingress traffic and egress traffic on each port.
	IP Filtering	It allows you to configure IP filtering and DHCP snooping.
	IP/MAC Binding	It allows you to configure IP/MAC bindings to prevent ARP spoofing attacks.
	MAC/Port Binding	It allows you to configure MAC/Port bindings, that is, static MAC addresses.
	Access Restriction	It allows you to enable device access restriction, and specify a range of computers that are exempt from the restriction.
Administration	System Time	It allows you to set the system date and time manually or automatically.
	Configuration	It allows you to backup and restore the system configuration, and reset the Switch to factory default settings
	Firmware Upgrade	It allows you to upgrade firmware.
	Restart	It allows you to restart the Switch.
	Help	It displays the basic online help information.

Table 3-1 Description of Menu Items

3.3.3 Description of Common BLevelOneons

The following table describes the commonly used bLevelOneons in the Web UI.

BLevelOneon Name	Description
Save	Click to save your changes.
Cancel	Click to revert to the last saved settings.
Refresh	Click to display the latest information on the page.
Delete	Click to delete the selected entry(ies).

Clear	Click to clear all the statistics on the page.
Help	Click to open the online help page to display the related help information.

Table 3-2 Description of Common BLevelOneons

3.3.4 Web UI Idle Timeout

The Web UI idle timeout is 300 seconds. The purpose of the idle timeout is for security. If you logs in and forgets to log out, the system will automatically log you out after 300 seconds of inactivity.

Chapter 4 Start Menu

The **Start** menu item is the first one under the top-level menu. It provides links to several commonly used pages including **Setup Wizard**, **Summary Statistics** and **Restart**.

4.1 Setup Wizard

The **Setup Wizard** will guide you to quickly configure the basic features of the Switch, which include password, IP address, switch type, link aggregation group and port mirroring settings.

4.1.1 Running the Setup Wizard

As mentioned earlier, the first page of the **Setup Wizard** appears immediately after your first login, see the following figure.

The Setup Wizard will guide you to configure the basic parameters for the Switch to operate properly. Even unfamiliar with our product, you still can follow the instructions to complete the setup easily. If you are an expert user, you may exit the Wizard and directly select the menu item that you want to configure. To continue, please click "Next". To exit the Setup Wizard, please click "Exit Wizard".

Do Not Automatically Launch the Wizard Again

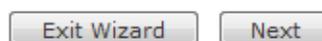


Figure 4-1 Running the Setup Wizard

- ◆ **Do Not Automatically Launch the Wizard Again:** If you select this check box, the system won't automatically launch the **Setup Wizard** the next time you login to the Switch. Else, the system will still launch the **Setup Wizard** automatically.
- ▶ **Exit Wizard:** Click to exit the **Setup Wizard**. The changes you have made in the **Setup Wizard** will be discarded.
- ▶ **Next:** Click to go to the next page of the **Setup Wizard**.

4.1.2 Password Settings

The Switch's default password is **admin**. To ensure security, it is strongly recommended that you change the default password, remember your new password and keep it safe. Once changed, you should use the new password to login to the Switch in the future.

Password	•••••
Confirm Password	•••••

Figure 4-2 Setup Wizard - Password Settings

- ◆ **Password:** It specifies the password (case sensitive) you use to login to the Switch.
- ◆ **Confirm Password:** You should re-enter the password.
- ▶ **Next:** Click to go to the next page of the **Setup Wizard**.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Exit:** Click to exit the **Setup Wizard**.
- ▶ **Help:** Click to view the related help information.

✔ Note

The password must be at most 11 characters long, and it cannot include the following characters: percent sign (%), single quotation mark ('), double quotation mark ("), backslash (\), and space.

4.1.3 IP Address Settings

<input type="checkbox"/>	Enable DHCP Client
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
System Name	

Figure 4-3 Setup Wizard - IP Address Settings

- ◆ **Enable DHCP Client:** It allows you enable or disable DHCP client. If you select the check box to enable DHCP client, the Switch will automatically obtain an IP address, subnet mask and default gateway address from a DHCP server available on your LAN. Else, you need to manually configure them for the Switch.
- ◆ **IP Address and Subnet Mask:** They specify the IP address and subnet mask of the Switch. You can use this IP address to access and manage the Switch. To facilitate management, please assign the Switch an IP address within your LAN subnet in most cases.
- ◆ **Default Gateway:** It specifies the IP address of the default gateway on your LAN.
- ◆ **System Name:** It specifies the name of the Switch.
- ▶ **Back:** Click to go back to the previous page of the **Setup Wizard**.
- ▶ **Next:** Click to go to the next page of the **Setup Wizard**.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Exit:** Click to exit the **Setup Wizard**.
- ▶ **Help:** Click to view the related help information.

4.1.4 Switch Type Settings

In this page, you can choose the type of the Switch, see Figure 4-4. In terms of physical placement, there are edge switches and core switches.

Edge Switch	<input checked="" type="radio"/>
Core Switch	<input type="radio"/>

Figure 4-4 Setup Wizard - Switch Type Settings

- ◆ **Edge Switch:** An edge switch (also called an access switch) is located at the edge of the network. The edge switch is connected to end-user hosts.
- ◆ **Core Switch:** A core switch is located in the core of the network and serves to interconnect edge switches.
- ▶ **Back:** Click to go back to the previous page of the **Setup Wizard**.
- ▶ **Next:** Click to go to the next page of the **Setup Wizard**.

- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Exit:** Click to exit the **Setup Wizard**.
- ▶ **Help:** Click to view the related help information.

 **Note**

The next page of the **Setup Wizard** depends on the specific type. If you choose the **Edge Switch**, the next page is **Setup Wizard - Link Aggregation Group** page. Else, the next page is **Setup Wizard - Port Mirroring** page.

4.1.5 Link Aggregation Group Settings

If you choose **Edge Switch** in the **Setup Wizard - Switch Type Settings** page, the **Setup Wizard - Link Aggregation Group** page will appear, see Figure 4-5. Else, this page will not appear.

This page provides a predefined LAG (Link Aggregation Group) that contains Port 23 and Port 24. You can enable or disable the predefined LAG. Please go to the **Advanced > Link Aggregation** to configure other LAGs if needed.



The image shows a rectangular button with the text "Enable LAG (Port 23, 24)" on the left and a small, empty square checkbox on the right.

Note: This page provides a typical configuration of LAG. The change made here will not affect the other LAGs.

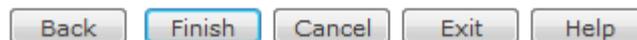


Figure 4-5 Setup Wizard - Link Aggregation Group (Edge Switch)

- ◆ **Enable LAG (Port 23, 24):** It allows you to enable or disable the predefined LAG that contains Port 23 and Port 24. If you want to enable the predefined LAG, please select the check box.
- ▶ **Back:** Click to go back to the previous page of the **Setup Wizard**.
- ▶ **Finish:** Click to save the changes you have made in the **Setup Wizard**.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Exit:** Click to exit the **Setup Wizard**.
- ▶ **Help:** Click to view the related help information.

 **Note**

Do not forget to click the **Finish** button to save the changes you have made in

the **Setup Wizard**, else these changes will be discarded.

4.1.6 Port Mirroring Settings

If you choose **Core Switch** in the **Setup Wizard - Switch Type Settings** page, the **Setup Wizard - Port Mirroring** page will appear, see Figure 4-6. Else, this page will not appear.

Port mirroring allows an administrator to mirror and monitor network traffic. It copies the traffic from the specified ports to another port where the traffic can be monitored with an external network analyzer. Then the administrator can perform traffic monitoring, performance analysis and fault diagnosis.

On the Switch, any port can act as the mirroring port, which is used to capture traffic of another port. As traffic can be captured from more than one port simultaneously, you can have one mirroring port and several other ports being monitored.

Mirroring Port

Note: Please select the mirrored ports (e.g., uplink port) as required. Select All

Port	Mirrored Port	Port	Mirrored 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"/>

Figure 4-6 Setup Wizard - Port Mirroring (Core Switch)

- ◆ **Mirroring Port:** It specifies the capture port that will mirror the traffic of the mirrored port(s).

- ◆ **Port:** It indicates the port number.
- ◆ **Mirrored Port:** It specifies the port whose traffic will be mirrored. You can choose one or more mirrored ports.
- ◆ **Select All:** It is used to select or clear all the **Mirrored Port** check boxes, except the check box for the **Mirroring Port**.
- ▶ **Back:** Click to go back to the previous page of the **Setup Wizard**.
- ▶ **Finish:** Click to save the changes you have made in the **Setup Wizard**.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Exit:** Click to exit the **Setup Wizard**.
- ▶ **Help:** Click to view the related help information.

**Note**

Do not forget to click the **Finish** button to save the changes you have made in the **Setup Wizard**, else these changes will be discarded.

4.2 Summary Statistics

This page displays summary traffic statistics on a port-by-port basis, which include the number of transmitted/received bytes, packets, non-unicast packets, and so on. You can use the statistics to monitor and analyze the system status.

Port	Tx Bytes	Tx Packets	Rx Bytes	Rx Packets	Tx Non-Unicast	Rx Non-Unicast	ARP Spoofing
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	1966669	4713	1700277	12078	5	6957	0
7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0

Figure 4-7 Summary Statistics

- ◆ **Port:** It displays the port number.
- ◆ **Tx Bytes:** It displays the total number of bytes transmitted by the port.
- ◆ **Tx Packets:** It displays the total number of packets transmitted by the port.
- ◆ **Rx Bytes:** It displays the total number of bytes received by the port.
- ◆ **Rx Packets:** It displays the total number of packets received by the port.
- ◆ **Tx Non-Unicast:** It displays the number of broadcast and multicast packets transmitted by the port.
- ◆ **Rx Non-Unicast:** It displays the number of broadcast and multicast packets received by the port.
- ◆ **ARP Spoofing:** It displays the number of ARP spoofing packets transmitted or received by the port.
- ▶ **Clear:** Click to clear all traffic statistics in this page.
- ▶ **Refresh:** Click to view the latest traffic statistics in this page.

4.3 Restart

(Note: The Restart process will take approximately 1 minute to complete.)

Figure 4-8 Restart the Switch

- ▶ **Restart:** Click to restart the Switch.

If you click the **Restart** button, the system will pop up a prompt dialog box (see Figure 4-9). Then you can click **OK** to restart the Switch, or click **Cancel** to cancel the operation.

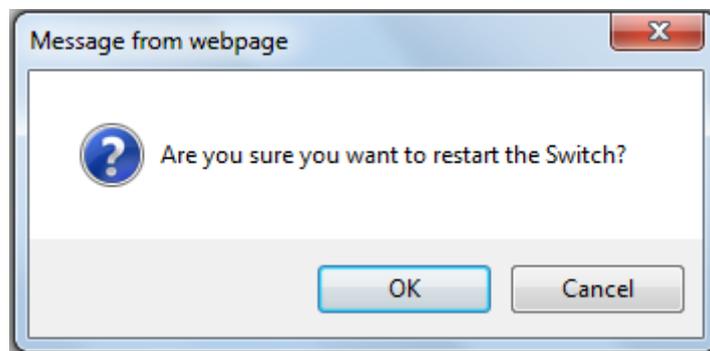


Figure 4-9 Prompt Dialog Box - Restart the Switch

 **Note**

Restarting the Switch will disconnect all the connections, so please do it with caution.

Chapter 5 Status

5.1 System Information

In the **Status > System Information** page, you can view system resources usage information including CPU usage, memory usage and, and basic system information including current system time, system up time, serial number and firmware version, and so on.

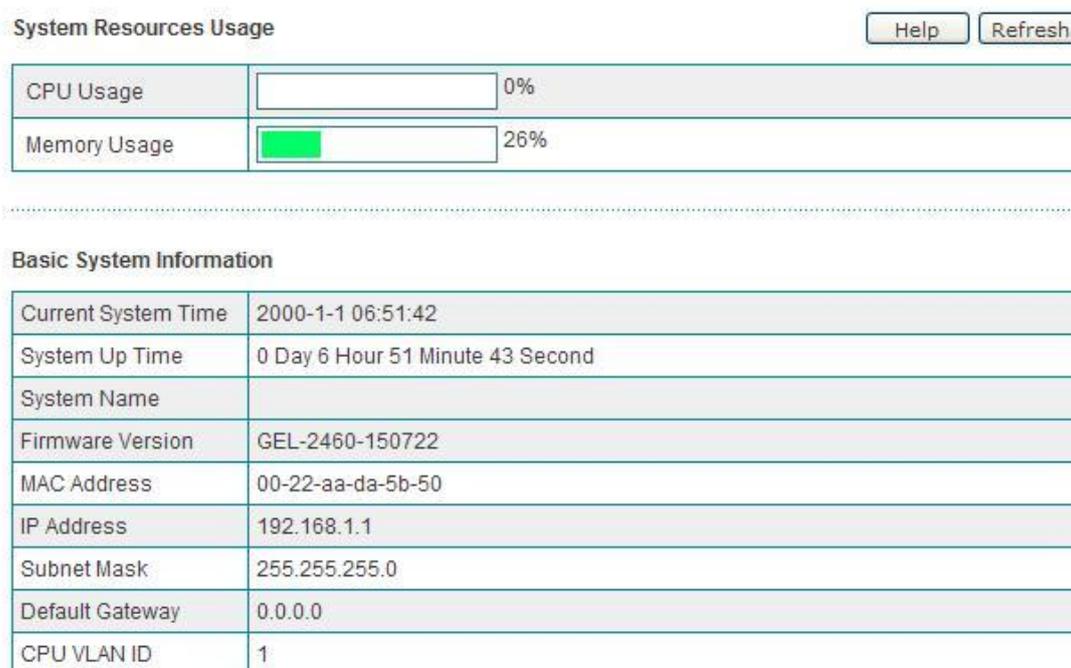


Figure 5-1 System Information

- ◆ **CPU Usage:** It displays the current CPU usage.
- ◆ **Memory Usage:** It displays the current memory usage.
- ◆ **Current System Time:** It displays the current system date (YYYY-MM-DD) and time (HH:MM:SS).
- ◆ **System Up Time:** It displays the elapsed time (in days, hours, minutes and seconds) since the Switch was last started.
- ◆ **System Name:** It displays the name of the Switch, which is configured in the **Basic >**

System Settings page.

- ◆ **Firmware Version:** It displays the version of the current firmware installed on the Switch.
- ◆ **MAC Address:** It displays the base MAC address of the Switch.
- ◆ **IP Address, Subnet Mask and Default Gateway:** They display the current IP address, subnet mask and default gateway address of the Switch.
- ◆ **CPU VLAN ID:** It displays the native VLAN ID of the Switch.



Note

1. The **CPU Usage**, **Memory Usage** and **USB Disk Usage** are displayed as a status bar and percentage value. The color of the status bar indicates the usage percentage for each resource.
 - When the percentage is below 1%, the bar is blank.
 - When the percentage is between 1% and 50% (below 50%), the color is green.
 - When the percentage is between 50% and 70% (below 70%), the color is yellow.
 - When the percentage is equal to or above 70%, the color is red.
2. The **CPU Usage** and **Memory Usage** indicate the load of the Switch. When the usage percentages are all relatively low, the Switch still has the ability to process more tasks. When they are all very high, the Switch is nearly under the full load. In this case, the network delays may occur if the Switch processes new tasks.

5.2 Summary Statistics

Please refer to **Section 4.2 Summary Statistics** for detailed information.

5.3 Port Statistics

This section describes the **Status > Port Statistics** page, which includes **Port Traffic** and **Port Details**.

5.3.1 Port Traffic Chart

In the **Status > Port Statistics** page, you can select the **Port Traffic** tab to view the real-time traffic chart for each port.

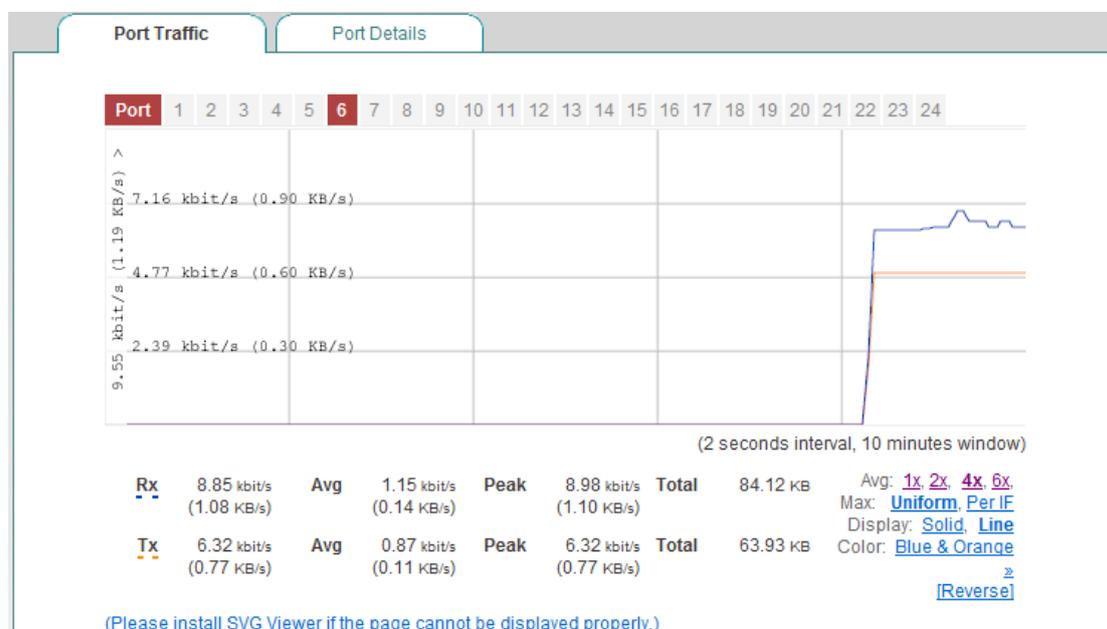


Figure 5-2 Port Traffic Chart

- ◆ **Rx:** It indicates the real-time rate of ingress traffic on the selected port, which is calculated every two seconds.
- ◆ **Tx:** It indicates the real-time rate of egress traffic on the selected port, which is calculated every two seconds.
- ◆ **Avg:** It indicates the average rate of ingress/egress traffic on the selected port since this page was last opened.
- ◆ **Peak:** It indicates the maximum rate of ingress/egress traffic on the selected port since this page was last opened.
- ◆ **Total:** It indicates the total ingress/egress traffic on the selected port since this page was last opened.
- ◆ **Avg: 1x, 2x, 4x, 6x:** It specifies the number of samples to average, or no averaging.
- ◆ **Max:** It determines that the charts are scaled uniformly to the max traffic value of all ports or individually per port.
- ◆ **Display:** It allows you to change the type of chart displayed. The options are **Line** and **Solid**.
 - **Line:** Select this option to display a line chart. The chart includes two lines with

different colors, which represent the real-time Rx rate and Tx rate respectively.

- **Solid:** Select this option to display an area chart. The area chart is like the line chart except that the area between the axis the plot line is solid.
- ◆ **Color:** It specifies the colors of the two lines (or filled areas), such as red, blue, black, etc.
- ◆ **Reverse:** Click to toggle the colors of the two lines (or filled areas).
- ▶ **Port:** You can select a port number at the top to view the traffic chart for that port.



Note

1. The rate chart can only show the rate and traffic information in the last ten minutes. Each time you open this page, the rate chart starts anew.
2. If the SVG Viewer plug-in isn't installed on your web browser, the port traffic chart cannot be displayed properly. Please click the **(Please install SVG Viewer if the page cannot be displayed properly.)** hyperlink to download and install the SVG Viewer to view the traffic chart.

5.3.2 Port Details

In the **Status > Port Statistics** page, you can select the **Port Details** tab to view the detailed traffic statistics for each port. You can select a port number to display detailed traffic statistics for that port. Please refer to **Section 4.2 Summary Statistics** for detailed description of the parameters.

Chapter 6 Basic

6.1 Setup Wizard

Please refer to **Section 4.1 Setup Wizard** for detailed information.

6.2 System Settings

In this page, you can configure DHCP relay agent, DHCP client, IP address, subnet mask, default gateway, CPU VLAN ID, MAC address aging time, password, and so on, see Figure 6-1.

System Settings		Save	Cancel	Help
Enable DHCP Relay Agent	<input type="checkbox"/>			
Enable DHCP Client	<input type="checkbox"/>			
IP Address	<input type="text" value="192.168.1.1"/>			
Subnet Mask	<input type="text" value="255.255.255.0"/>			
Default Gateway	<input type="text" value="0.0.0.0"/>			
CPU VLAN ID	<input type="text" value="1"/>			
MAC Address Aging Time(s)	<input type="text" value="300"/>			
System Name	<input type="text"/>			
Password	<input type="password" value="*****"/>			
Confirm Password	<input type="password" value="*****"/>			
ARP Spoofing Prevention	<input type="checkbox"/>			

Figure 6-1 System Settings

- ◆ **Enable DHCP Relay Agent:** It allows you enable or disable DHCP relay agent. If you select the check box to enable DHCP relay agent, the Switch can forward DHCP

messages between DHCP servers and clients.

- ◆ **Enable DHCP Client:** It allows you enable or disable DHCP client. If you select the check box to enable DHCP client, the Switch will automatically obtain an IP address, subnet mask and default gateway address from a DHCP server available on your LAN. Else, you need to manually configure them for the Switch.
- ◆ **IP Address and Subnet Mask:** They specify the IP address and subnet mask of the Switch. You can use this IP address to access and manage the Switch. To facilitate management, please assign the Switch an IP address within your LAN subnet in most cases.
- ◆ **Default Gateway:** It specifies the IP address of the default gateway on your LAN.
- ◆ **CPU VLAN ID:** It specifies the native VLAN ID of the Switch.
- ◆ **MAC Address Aging Time:** It specifies the aging time of dynamically learned MAC addresses in the MAC address table. If a dynamic MAC address remains inactive (neither used nor updated) for the specified amount of time, it is removed from the address table. In most cases, please leave the default value.
- ◆ **System Name:** It specifies the name of the Switch.
- ◆ **Password:** It specifies the password (case sensitive) you use to login to the Switch. The default value is **admin**.
- ◆ **Confirm Password:** You should re-enter the password.
- ◆ **ARP Spoofing Prevention:** It allows you to enable or disable ARP spoofing prevention. If you select the check box to enable this feature, it will effectively protect the Switch against ARP spoofing attacks.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.



Note

1. To ensure security, it is strongly recommended that you change the default password, remember your new password and keep it safe. If you forgot your password, you need to use the **Reset** button to reset the Switch to factory default settings, and then use the default password to login to the Switch.
2. In this page, you can either manually change the Switch IP parameters (IP address, subnet mask and default gateway) as required, or enable DHCP client to make the Switch automatically obtain them from a DHCP server available on your LAN.

6.3 Port Settings

In the **Basic > Port Settings** page, you can view the link status of each port, configure the name, port speed and duplex mode, maximum frame, flow control, enable or disable port protection and MAC address learning for each port.

Global Settings Mode

Port	Port Name	Link Status	Mode	Maximum Frame	Flow Control	Port Protection	Disable Learning
1	<input type="text"/>	Down	Auto	1518	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	Down	Auto	1518	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	Down	Auto	1518	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	Down	Auto	1518	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="text"/>	Down	Auto	1518	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="text"/>	100fdx	Auto	1518	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 6-2 Port Settings

- ◆ **Global Settings:** It is used to configure all ports at a time. For example, if you set the **Mode** to **1000M/Full** here, all ports' **Mode** will be set to **1000M/Full** automatically.
- ◆ **Port:** It indicates the port number.
- ◆ **Port Name:** It allows you to specify a meaningful name for the port to facilitate management.
- ◆ **Link Status:** It indicates the port link status. If the port is disabled, not connected, or experiencing a network error, it will display **Down**. If the port is working properly, it will display its current speed and duplex mode. In addition, the green border means that the port is operating at 100Mbps, and the orange border means that the port is operating at 1000Mbps.
- ◆ **Mode:** It specifies the port speed and duplex mode. The options are **Auto**, **10M/HDX**, **10M/FDX**, **100M/HDX**, **100M/FDX**, **1000M/FDX**, and **Disabled**. The default value is **Auto**, which means the port will auto negotiate the speed and duplex mode with the remote port on the link. If you want to disable a port, please select **Disabled**.
- ◆ **Maximum Frame:** It specifies the maximum frame size supported by the port. The valid range is from 1518 to 9600 bytes.
- ◆ **Flow Control:** It allows you to enable or disable flow control on the port. If you want to enable flow control on the port, please select the check box.
- ◆ **Port Protection:** It allows you to enable or disable port protection on the port. If you

select the check box to enable port protection on a port, the port will no longer learn any new MAC address, and only forward the packets whose destination MAC addresses have been added to the **MAC/Port Binding List**. Else, the port will learn MAC address and forward the packets as usual.

◆ **Disable Learning:** It allows you to enable or disable MAC address learning on the port. If you select the check box to disable MAC address learning on a port, the packets received on that port will be flooded to all other ports.

▶ **Save:** Click to save your changes.

▶ **Cancel:** Click to revert to the last saved settings.

▶ **Help:** Click to view the related help information.



Note

1. If no MAC address is added to the **MAC/Port Binding List**, enabling port protection on all ports will make you unable to access and manage the Switch.
2. If you select the **Disable Learning** check box on multiple or all ports, it will seriously degrade the network performance, so please do it with caution.
3. To use flow control feature properly, both the local port and remote port on the link should support and enable it. In addition, LACP and flow control cannot be enabled on a port at the same time. If you enable LACP on a port, the system will automatically disable flow control on the port.

6.4 Port Mirroring

Port mirroring allows an administrator to mirror and monitor network traffic. It copies the traffic from the specified ports to another port where the traffic can be monitored with an external network analyzer. Then the administrator can perform traffic monitoring, performance analysis and fault diagnosis.

On the Switch, any port can act as the mirroring port, which is used to capture traffic of another port. As traffic can be captured from more than one port simultaneously, you can have one mirroring port and several other ports being monitored.

Mirroring Port

Select All Note: Please select the mirrored ports (e.g., uplink port) as required.

Port	Mirrored Port	Port	Mirrored 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"/>

Figure 6-3 Port Mirroring

- ◆ **Mirroring Port:** It specifies the capture port that will mirror the traffic of the mirrored port(s).
- ◆ **Port:** It indicates the port number.
- ◆ **Mirrored Port:** It specifies the port whose traffic will be mirrored. You can choose one or more mirrored ports.
- ◆ **Select All:** It is used to select or clear all the **Mirrored Port** check boxes, except the check box for the **Mirroring Port**.

- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.

 **Note**

1. A port can't act as the mirroring port and mirrored port at the same time.
2. A LAG member port can't act as the mirroring port.

Chapter 7 Advanced

7.1 VLAN

A VLAN (Virtual Local Area Network) is a group of devices that form a logical LAN segment, that is, a broadcast domain. The members on the same VLAN can communicate with each other. The traffic will not disturb among different VLANs, that is, any traffic (unicast, broadcast or multicast) within a VLAN doesn't flow to another VLAN. This feature can help simplify network management, enhance network security, and improve network performance.

7.1.1 VLAN Mode Settings

The Switch supports port-based VLAN and IEEE 802.1Q tag-based VLAN. To configure VLAN on the Switch, firstly you need to choose the **VLAN Mode** in the **Advanced > VLAN > VLAN Mode Settings** page, see Figure 7-1.



Figure 7-1 VLAN Mode Settings

- ◆ **VLAN Mode:** It specifies the VLAN mode that you want to enable on the Switch. The options are **VLAN Disabled**, **Port VLAN**, and **TAG VLAN**. If you want to disable VLAN on the Switch, please leave the default value of **VLAN Disabled**.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.

7.1.2 Port-based VLAN

Port-based VLAN allows you to group the switch ports into multiple VLANs. Ports on the

same VLAN can communicate with each other, but they are unable to communicate with ports on different VLANs. End-user hosts become members in a VLAN based on the switch port to which they are connected.

To enable port-based VLAN on the Switch, select **Port VLAN** from the **VLAN Mode** drop-down list in the **Advanced > VLAN > VLAN Mode Settings** page, and then click the **Save** button, see Figure 7-2.

VLAN Mode

Figure 7-2 Enabling Port-based VLAN

7.1.2.1 Port-based VLAN Settings

In the **Advanced > VLAN** page, you can select the **Port VLAN Settings** tab to create port-based VLANs, see Figure 7-3.

VLAN ID VLAN Name Add Modify

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

Select All

Figure 7-3 Port-based VLAN Settings

- ◆ **VLAN ID:** It specifies a number used to identify the port-based VLAN. It must be between 1 and 24.
- ◆ **VLAN Name:** It allows you to specify a meaningful name for the port-based VLAN to facilitate management.
- ◆ **Members:** It allows you to choose one or more ports as the members of the port-based VLAN. Select a check box to add a port to the VLAN, or clear the check box to remove the port from the VLAN.
- ◆ **Add:** Keep the **Add** radio button selected when adding a new port-based VLAN.
- ◆ **Modify:** Keep the **Modify** radio button selected when modifying a configured port-based VLAN.
- ◆ **Select All:** It is used to select or clear the check boxes for all ports.

VLANs, you can view them in the **Port VLAN List**.

- ▶ **Modify a Port-based VLAN:** To modify a configured port-based VLAN, click its **VLAN ID** hyperlink or  icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- ▶ **Delete Port-based VLAN(s):** There are two ways to delete port-based VLANs.
 1. To delete a port-based VLAN, directly click its  icon.
 2. To delete more than one port-based VLAN at a time, select the leftmost check boxes of the VLANs that you want to delete, and then click the **Delete** button.



Note

You can edit VLAN 1 (the default VLAN), but you cannot delete it.

7.1.2.3 An Configuration Example for Port-based VLAN

In this example, it is required that Port 1 and Port 2 can communicate with each other, Port 2 and Port 3 also can communicate with each other, but Port 1 and Port 3 cannot.

The configuration steps are as follows:

Step 1 Modify VLAN 1 to make it contain only Port 1 and Port 2.

Step 2 Add a new VLAN (VLAN 2) that contains only Port 2 and Port 3.

7.1.3 Tag-based VLAN

The 802.1Q tag-based VLAN add a tag to the header of the packets to classify their VLANs. An 802.1Q tag-based VLAN is a group of ports located anywhere on the network, acting as part of the same physical segment. On the Switch, you can manually assign the ports to multiple VLANs, and then configure VLAN parameters for each port. When a tagged frame arrives at a port, the Switch uses the VLAN ID contained in the tag of the frame to identify the port broadcast domain. When an untagged frame arrives at a port, the Switch assigns the port's PVID to the frame.

To enable tag-based VLAN on the Switch, select **TAG VLAN** from the **VLAN Mode** drop-down list in the **Advanced > VLAN > VLAN Mode Settings** page, and then click the **Save** button, see Figure 7-5.



Figure 7-5 Enabling Tag-based VLAN

7.1.3.1 Tag-based VLAN Settings

In the **Advanced > VLAN** page, you can select the **Tag VLAN Settings** tab to create tag-based VLANs, see Figure 7-6.

VLAN ID VLAN Name Add Modify

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

Select All

Figure 7-6 Tag-based VLAN Settings

- ◆ **VLAN ID:** It specifies a number used to identify the tag-based VLAN. It must be between 1 and 4094.
- ◆ **VLAN Name:** It allows you to specify a meaningful name for the port-based VLAN to facilitate management.
- ◆ **Members:** It allows you to choose one or more ports as the members of the tag-based VLAN. Select a check box to add a port to the VLAN, or clear the check box to remove the port from the VLAN.
- ◆ **Add:** Keep the **Add** radio button selected when adding a new tag-based VLAN.
- ◆ **Modify:** Keep the **Modify** radio button selected when modifying a configured tag-based VLAN.
- ◆ **Select All:** It is used to select or clear the check boxes for all ports.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.

Note

1. On the Switch, the default VLAN is VLAN 1. And all switch ports are members of

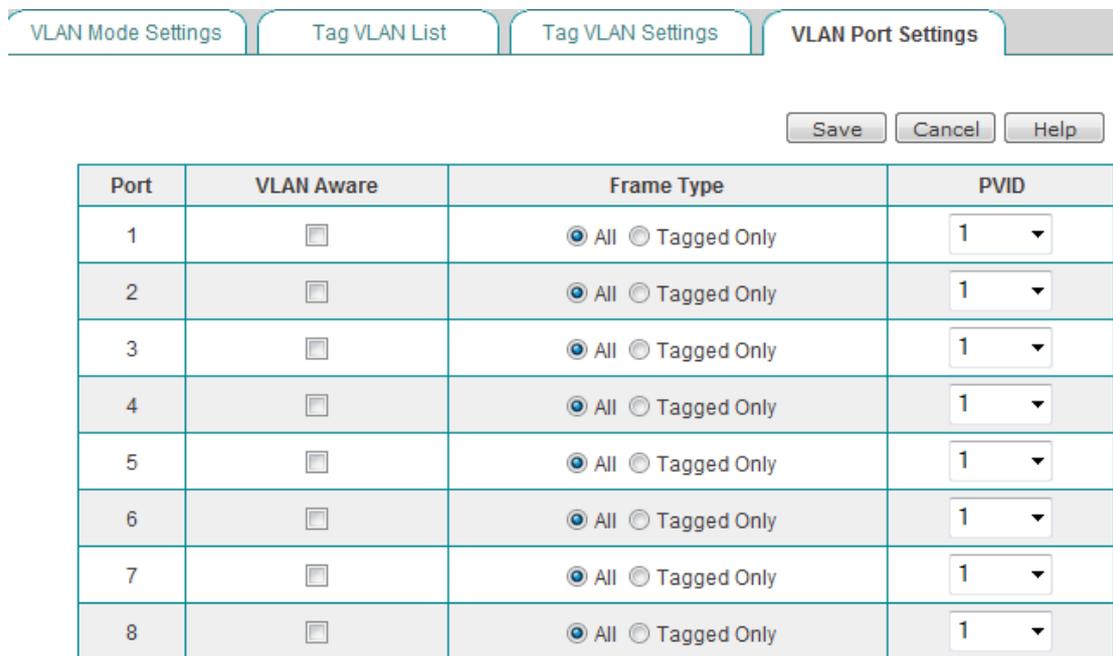
boxes of the VLANs that you want to delete, and then click the **Delete** button.

 **Note**

You can edit VLAN 1 (the default VLAN), but you cannot delete it.

7.1.3.3 Tag-based VLAN Port Settings

In the **Advanced > VLAN** page, you can select the **VLAN Port Settings** tab to configure VLAN parameters for each port, see Figure 7-8.



Port	VLAN Aware	Frame Type	PVID
1	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1
2	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1
3	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1
4	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1
5	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1
6	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1
7	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1
8	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1

Figure 7-8 VLAN Port Settings

- ◆ **Port:** It indicates the port number.
- ◆ **VLAN Aware:** It allows you to enable or disable VLAN awareness mode for the port. If you select the check box to enable VLAN awareness mode for a port, the port will distinguish between tagged frames and untagged frames, and handle them differently. Else, the port will ignore VLAN tags.
- ◆ **Frame Type:** It specifies the type of frames the port accepts. The options are **All** and **Tagged Only**.
 - **All:** It indicates that the port accepts both tagged and untagged frames.
 - **Tagged Only:** It indicates that the port accepts only tagged frames, and drops untagged frames.
- ◆ **PVID:** It specifies the VLAN ID that will be assigned to untagged frames received on

the port (when **VLAN Aware** is enabled). If you want to change the port's default PVID, you must create a tag-based VLAN that includes the port, and then choose that tag-based VLAN's ID (VID) as the port's PVID. If a port belongs to two or more tag-based VLANs, you can choose one of those VIDs as the PVID.

- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.

7.1.3.4 An Configuration Example for Tag-based VLAN

In this example, a business uses a HiPER Router to access the Internet. A SG3214F Switch's Port 1 is connected to the Router's LAN Port 1, PC1 (management host) is connected to the Router's LAN Port 5, and PC2 is connected to the Switch's Port 2. Neither PC1 nor PC2 can receive tagged frames. It is required that PC2 and PC1 can communicate with each other, but all other PCs cannot communicate with PC1.

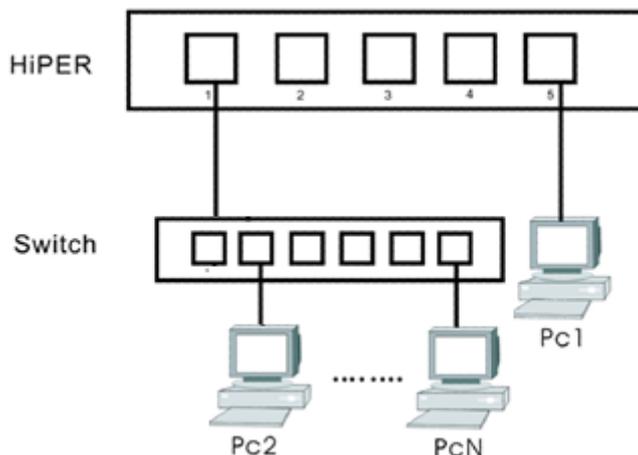


Figure 7-9 Network Topology – Tag-based VLAN Configuration Example

The configuration steps are as follows:

- Step 1** On the HiPER Router, add a new tag-based VLAN: VLAN ID is 2, and port members are Port 1 and Port 5.
- Step 2** On the GEL-2460 Switch, add a new tag-based VLAN: VLAN ID is 2, and port members are Port 1 and Port 2.

7.2 RSTP

The Spanning Tree Protocol (STP) is a link layer network protocol that detects and eliminates loops in a bridged or switched network. Using STP, the bridges can communicate with each other to discover physical loops in the network, and create a tree structure of loop-free leaves and branches that spans the entire Layer 2 network, leaving a single active path between any two network nodes. In addition, STP also provides path redundancy to improve network reliability: if an active path fails, the protocol automatically reconfigures the network to activate another path.

The Rapid Spanning Tree Protocol (RSTP) is an improved version of STP, which provides faster spanning tree convergence after a topology change.

7.2.1 RSTP Status

7.2.1.1 RSTP Bridge Overview



VLAN ID	Bridge ID	Hello Time	Max Age	Forward Delay	Topology	Root ID
2	32770:00-22-AA-AB-34-7B	2	20	15	Steady	32770:00-22-AA-AB-34-7B

Figure 7-10 RSTP Bridge Overview

- ◆ **VLAN ID:** It displays the VLAN ID associated with the RSTP Bridge.
- ◆ **Bridge ID:** It displays the Switch's Bridge ID (BID), which consists of the bridge priority and MAC address of the Switch.
- ◆ **Hello Time:** It displays the **Hello Time** configured in the **Advanced > RSTP > RSTP Settings** page.
- ◆ **Max Age:** It displays the **Max Age** configured in the **Advanced > RSTP > RSTP Settings** page.
- ◆ **Forward Delay:** It displays the **Forward Delay** configured in the **Advanced > RSTP > RSTP Settings** page.
- ◆ **Topology:** It indicates if the RSTP topology is steady or undergoing reconfiguration.
 - **Steady:** It indicates that the RSTP topology is steady.
 - **Changing:** It indicates that the RSTP topology is undergoing reconfiguration.

- ◆ **Root ID:** It indicates the **Bridge ID** of the currently elected root bridge.
- ▶ **Help:** Click to view the related help information.
- ▶ **Refresh:** Click to view the latest RSTP bridge status information.

7.2.1.2 RSTP Port Status

RSTP Port Status

Port	Path Cost	Edge Port	Protocol	Port State	Port	Path Cost	Edge Port	Protocol	Port State
1				Disabled	2				Disabled
3				Disabled	4				Disabled
5				Disabled	6				Disabled
7				Disabled	8				Disabled
9				Disabled	10				Disabled
11				Disabled	12				Disabled
13				Disabled	14				Disabled
15				Disabled	16				Disabled
17				Disabled	18				Disabled
19				Disabled	20				Disabled
21				Disabled	22				Disabled
23				Disabled	24				Disabled

Figure 7-11 RSTP Port Status

- ◆ **Port:** It indicates the port number.
- ◆ **Path Cost:** It displays the current port path cost. The lower the path cost, the faster the port.
- ◆ **Edge Port:** It indicates whether the port is an edge port or non-edge port.
 - **yes:** It indicates that the port is an edge port.
 - **no:** It indicates that the port is a non-edge port.
- ◆ **Protocol:** It displays the current running protocol, RSTP or STP.
- ◆ **Port State:** It displays the current RSTP state of the port. There are five states:
 - **Disabled:** It indicates that the port is not participating in RSTP. This can occur when the port is disabled, the port link is down, or RSTP is disabled on the port.
 - **Blocking:** It indicates that the port is currently blocked. In this state, the port can receive and process BPDUs, but it cannot forward user frames.

- **Listening:** It indicates that the port is listening for a BPDU from neighboring bridge(s) in order to determine the new topology. In this state, the port still cannot forward user frames.
 - **Learning:** It indicates that the port is in the learning state. In this state, the port still cannot forward user frames; however, the Switch can learn the MAC addresses of frames that the port receives, and add them to the MAC table.
 - **Forwarding:** It indicates that the port is in the forwarding state. In this state, the port can forward the user frames and learn new MAC addresses.
- ▶ **Help:** Click to view the related help information.
- ▶ **Refresh:** Click to view the latest RSTP port status information.

7.2.2 RSTP Settings

7.2.2.1 RSTP Bridge Settings



RSTP Bridge Settings			
Priority	32768	Hello Time	2
Max Age	20	Forward Delay	15

Figure 7-12 RSTP Bridge Settings

- ◆ **Priority:** It specifies the RSTP bridge priority. Each switch has a unique Bridge ID (BID) that consists of the bridge priority and its MAC address. The Switch with the lowest BID is elected as the root bridge. The range is 0 to 65535. The smaller the number, the higher the priority.
- ◆ **Hello Time:** It specifies the time interval between configuration BPDUs sent by the root bridge. The default value is 2 seconds.
- ◆ **Max Age:** It specifies the amount of time that a bridge stores a BPDU before discarding it. If this timer expires before the port receives a new BPDU, the port transitions to the listening state. The default value is 20 seconds.
- ◆ **Forward Delay:** It specifies the amount of time that a bridge remains in the listening and learning states before forwarding packets. The default value is 15 seconds.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.

7.2.2.2 RSTP Port Settings

RSTP Port Settings

Global Settings Path Cost: auto means auto-generated.

Port	RSTP	Edge Port	Path Cost	Port	RSTP	EdgePort	Path Cost
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>
9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>
11	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	12	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>
13	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	14	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>
15	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	16	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>
17	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	18	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>
19	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	20	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>
21	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	22	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>
23	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	24	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>

Figure 7-13 RSTP Port Settings

- ◆ **Global Settings:** It is used to configure all ports at a time.
- ◆ **Port:** It indicates the port number.
- ◆ **RSTP:** It allows you to enable or disable RSTP on the port. If you want to enable RSTP on the port, please select the check box.
- ◆ **Edge Port:** It specifies whether the port is an edge port or non-edge port. An edge port is directly connected to an end-user host (that is, it is not connected to any bridge), and it can go directly to the forwarding state without any delay. If you want to set the port as an edge port, please select the check box.
- ◆ **Path Cost:** It specifies the port contribution to the root path cost. The lower the path cost, the faster the port. If you want to use the default cost generated by the system, please leave the default value of **auto**.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.

7.3 LACP

7.3.1 Introduction to LACP

Link Aggregation Control Protocol (LACP) is part of IEEE 802.3ad which is used to bundle several physical ports together to form a single logical channel, known as a Link Aggregation Group (LAG) or bundle. LACP allows two switches to exchange Link Aggregation Control Protocol Data Units (LACPDUs) to negotiate a LAG automatically. An LACP-enabled port sends LACPDUs to tell the remote system about its system priority, system MAC address, port priority, port number and operational key. Then the remote system compares the received information with the information received on other ports to choose member ports for a LAG. This allows the two systems to reach agreement about whether a port can join or leave a dynamic LAG.

There are two link aggregation modes: dynamic and static. With dynamic LACP aggregation, the system can create/delete dynamic LAGs automatically; however, you cannot add/delete member ports into/from a dynamic LAG. Only the ports with the same basic configuration, speed and duplex mode can be aggregated to the same dynamic LAG. In addition, the system can create a dynamic LAG that contains only a single port, which is called single port aggregation. In a dynamic LAG, LACP is enabled and running on all the member ports.

In a dynamic LAG, a port can be in selected or standby state. Both selected ports and standby ports can transmit and receive LACPDUs; however, only selected ports can forward user packets.

A dynamic LAG can contain a limited number of ports. If the number of the member ports exceeds the maximum number of ports allowed in a LAG, the local system will negotiate with remote system to set aggregation state of each member port as follows:

1. Compare the System ID (System Priority + MAC Address). First compare the system priorities. If they are the same, compare the MAC addresses. The system with the smaller system ID wins out.
2. Compare the Port ID (Port Priority + Port Number) of the ports on the system with the smaller system ID. First compare the port priorities. If two or more ports have the same port priorities, compare their port numbers. The ports with smaller Port IDs are selected as selected ports, while others as standby ports.
3. In a dynamic LAG, the selected port with the least port number acts as the master port, while other selected ports act as the slave ports.

7.3.2 LACP Status

LACP Settings LACP Status

LACP Aggregation Overview Help Refresh

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
Default																								

LACP Port Status

Port	Protocol Active	Partner Port	Oper Key	Port	Protocol Active	Partner Port	Oper Key
1	No			2	No		
3	No			4	No		
5	No			6	No		
7	No			8	No		
9	No			10	No		
11	No			12	No		
13	No			14	No		
15	No			16	No		
17	No			18	No		
19	No			20	No		
21	No			22	No		
23	No			24	No		

Help Refresh

Figure 7-14 LACP Status

- ◆ **Group:** It displays the ID of each dynamic LAG. The **Default** group is used to display the ports in the negotiating phase (0 means that the corresponding port is in the negotiating phase). Once a LAG is formed successfully, a new row is created to display the LAG's port members on the local Switch and partner switch. If a port on the local Switch is a member of the LAG, the partner port number will appear in the same column.
- ◆ **Port:** It displays the port number on the local Switch.
- ◆ **Protocol Active:** It indicates if LACP is enabled and running on the port. If LACP is enabled and running on the port, it displays **Yes**. Else, it displays **No**.
- ◆ **Partner Port:** It displays the port number on the partner switch.
- ◆ **Oper Key:** It displays the current operational value of the key for the aggregation port. When aggregating ports, the system automatically assigns each port an operational

key based on its aggregation capability. All ports in a LAG share the same operational key.

- ▶ **Help:** Click to view the related help information.
- ▶ **Refresh:** Click to view the latest LACP status information.

7.3.3 LACP Settings

To configure a dynamic LAG, you only need to enable LACP on the ports that you want to join the LAG automatically, and then click the **Save** button. Only the ports with the same basic settings, speed and duplex mode can be aggregated to the same dynamic LAG.

For example, if you want to aggregate Port 2, 3, 4 and 5 on the local GEL-2460 Switch and those on the remote switch together to form a dynamic LAG, you only need to enable LACP on Port 2, 3, 4 and 5 respectively, and leave their **Admin Key** at the default value of **auto**, see Figure 7-15. If the remote switch is another vendor's product, you can configure LACP in a similar fashion.

LACP Settings
LACP Status

Global Settings
Enable LACP
 Admin Key: auto means auto-generated.
Save
Cancel
Help

Port	Enable LACP	Admin Key	Port	Enable LACP	Admin Key
1	<input type="checkbox"/>	auto	2	<input checked="" type="checkbox"/>	auto
3	<input checked="" type="checkbox"/>	auto	4	<input checked="" type="checkbox"/>	auto
5	<input checked="" 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 checked="" type="checkbox"/>	auto

Save
Cancel
Help

Figure 7-15 LACP Settings

- ◆ **Port:** It indicates the port number.
- ◆ **Enable LACP:** It allows you to enable or disable LACP on the port. If you want to enable LACP on the port, please select the check box.
- ◆ **Admin Key:** It specifies the administrative value of the key for the aggregation port. The administrative key is used to identify each link aggregation group (LAG). A LAG will only be formed between ports having the same administrative key. The **Admin Key** is a number between 1 and 255, or auto. If you want the Switch to set this key automatically, please leave the default value of **auto**.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.

**Note**

LACP and flow control cannot be enabled on a port at the same time. If you enable LACP on a port, the system will automatically disable flow control on the port.

7.4 Link Aggregation

The above section mainly describes how to use LACP to configure dynamic LAGs in the **Advanced > LACP** page. This section mainly describes how to manually configure static LAGs in the **Advanced > Link Aggregation** page.

7.4.1 Introduction to Link Aggregation

Link aggregation provides a means to combine multiple switch ports together to form a higher-bandwidth single logical link, known as a Link Aggregation Group (LAG), whose total bandwidth is approximately the sum of the individual switch ports. For example, there is a 100Mbps switch device, a LAG containing two ports will have 200Mbps bandwidth, and a LAG containing four ports will have 400Mbps bandwidth.

Link aggregation provides a higher performance logical link, as well as providing a fault-tolerant link between two devices. If one of the physical links in the LAG goes down, traffic is dynamically and transparently reassigned to the other physical links. Besides, link aggregation offers load balancing across multiple physical links.

In general, link aggregation achieves cascade connection between two devices, and provides bundled high-bandwidth by expensing the number of ports. Then it can improve network speed, break network bottleneck, and significantly improve network performance.

7.4.2 LAG Settings

In the **Advanced > Link Aggregation** page, you can add, view, modify and delete static LAGs.

LAG List

LAG Settings

LAG ID
LAG Name

Add
Modify

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

Figure 7-16 LAG Settings

- ◆ **LAG ID:** It specifies a number used to identify the LAG. The Switch supports up to 24 LAGs.
- ◆ **LAG Name:** It allows you to specify a meaningful name for the LAG to facilitate management.
- ◆ **Members:** It allows you to choose one or more ports as the members of the LAG. Select a check box to add a port to the LAG, or clear the check box to remove the port from the LAG. A port can belong to only one LAG.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.

**Note**

1. All ports in a LAG must have the same port settings (except **Port Name**) which are configured in the **Basic > Port Settings** page, and must have the same port speed and duplex mode.
2. All ports in a LAG must belong to the same VLAN, and must have the same tag VLAN port settings (configured in the **Advanced > VLAN > VLAN Port Settings** page) if you enable tag-based VLAN on the Switch.
3. A LAG can't contain the mirroring port.
4. If LACP or RSTP is enabled on a port, the port cannot be added to any LAG.
5. All ports in a LAG must have the same rate limiting settings which are configured in the **Security > Rate Limiting** page.

7.4.3 LAG List

The screenshot displays the 'Link Aggregation List' interface. At the top, there are two tabs: 'LAG List' and 'LAG Settings'. Below the tabs is a header for 'Link Aggregation' with a page indicator '0/24'. The main area contains a table with the following columns: 'LAG ID', 'LAG Name', 'LAG Members', and 'Edit'. Above the table, there are navigation controls including '0/0', 'First', 'Prev', 'Next', 'Last', 'Go to Page', a search box, and a 'Search' button. Below the table, there is a 'Select All' checkbox and two buttons: 'Add' and 'Delete'.

Figure 7-17 Link Aggregation List

- ▶ **Add a LAG:** To add a new LAG, first click the **Add** button or select the **LAG Settings** tab to go to the setup page, next configure it, lastly click the **Save** button.
- ▶ **View LAG(s):** When you have configured one or more LAGs, you can view them in the **Link Aggregation List**.
- ▶ **Modify a LAG:** To modify a configured LAG, click its **LAG ID** hyperlink or  icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- ▶ **Delete LAG(s):** There are two ways to delete LAGs.
 1. To delete a LAG, directly click its  icon.
 2. To delete more than one LAG at a time, select the leftmost check boxes of the LAGs that you want to delete, and then click the **Delete** button.

7.5 QoS

Quality of Service (QoS) is a technology which uses various mechanisms to decrease the negative effects of network congestion to improve network performance. For example, using QoS can guarantee a required delay and packet dropping probability to various real-time applications (video, audio, etc.) when network congestion occurs.

The Switch supports 802.1p and port-based QoS with four priority levels, which include low, normal, medium and high priority. The Switch uses the priority level to determine the order in which packets are forwarded. More specifically, high-priority packets are forwarded preferentially, next medium-priority packets are forwarded, and so on.

7.5.1 Disabling QoS

To disable QoS on the Switch, select **QoS Disabled** from the **QoS Mode** drop-down list, and then click the **Save** button, see Figure 7-18.



Figure 7-18 Disabling QoS

7.5.2 802.1p Priority Settings

IEEE 802.1p standard provides a mechanism for implementing QoS at the MAC level. Ethernet packets can have an optional 4-byte 802.1p VLAN tag which contains a 3-bit priority field. This 3-bit priority field carries one of eight 802.1p priority values (0-7), which are defined in IEEE 802.1p to support QoS traffic classes. On the Switch, it allows you to map each of the eight 802.1p values to one of the four priority levels: low, normal, medium or high. This ensures that time-sensitive application traffic will get preferential treatment when network congestion occurs.

To enable IEEE 802.1p priority on the Switch, select **802.1p** from the **QoS Mode** drop-down list in the **Advanced > QoS** page, and then click the **Save** button, see Figure 7-19.

QoS Mode Global Priority

802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority
0	Normal	1	Low	2	Low	3	Normal
4	Medium	5	Medium	6	High	7	High

Figure 7-19 802.1p Priority Settings

- ◆ **QoS Mode:** It specifies the QoS mode that you want to enable on the Switch. The options are **QoS Disabled**, **802.1p** and **Port-based Priority**. Here please select **802.1p**.
- ◆ **Global Priority:** It is used to set all 802.1p values to the same priority level.
- ◆ **802.1p Value:** It indicates the 802.1p priority value. There are eight 802.1p priority values (0-7).
- ◆ **Priority:** It specifies the priority level to which the 802.1p value is mapped. There are four priority levels: **Low**, **Normal**, **Medium** and **High**.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.

7.5.3 Port-based Priority Settings

Port-based QoS allows you to set priority level for each port. The packets received on a port have the same priority level as that port. The Switch supports four priority levels: low, normal, medium and high. The Switch uses the priority level to determine the order in which packets received on each port are forwarded. More specifically, packets received from the high-priority ports are forwarded preferentially, next packets received from the medium-priority ports are forwarded, and so on.

To enable port-based priority on the Switch, select **Port-based Priority** from the **QoS Mode** drop-down list in the **Advanced > QoS** page, and then click the **Save** button. See Figure 7-20.

QoS Mode Global Priority

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

Figure 7-20 Port-based Priority Settings

- ◆ **QoS Mode:** It specifies the QoS mode that you want to enable on the Switch. The options are **QoS Disabled**, **802.1p** and **Port-based Priority**. Here please select **Port-based**.
- ◆ **Global Priority:** It is used to set all ports to the same priority level.
- ◆ **Port:** It indicates the port number.
- ◆ **Priority:** It specifies the priority level for each port. There are four priority levels: **Low**, **Normal**, **Medium** and **High**.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.

7.6 SNMP

SNMP (Simple Network Management Protocol) is an application layer protocol for collecting information about devices on the network. SNMP feature can help you to remotely monitor, configure, and troubleshoot the Switch.

If you enable the SNMP agent on the Switch, you can use an SNMP manager to retrieve the Switch's configuration and status information, and modify its configuration. Besides, you can configure the Switch to send traps to the SNMP manager when particular events occur, such as system restart, link down, link up, and so on.

SNMP

Enable SNMP	<input type="checkbox"/>
SNMP Trap Host	<input type="text" value="0.0.0.0"/>
SNMP Read Community Name	<input type="text" value="uTt22aA"/>
SNMP Write Community Name	<input type="text" value="22AaUT"/>
SNMP Trap Community Name	<input type="text" value="public"/>

Figure 7-21 SNMP Settings

- ◆ **Enable SNMP:** It allows you enable or disable SNMP agent. If you select the check box to enable SNMP agent on the Switch, the SNMP settings will take effect. Else, they will be of no effect.
- ◆ **SNMP Trap Host:** It specifies the IP address of the host that receives SNMP traps. The default is 0.0.0.0, which means that the Switch won't send traps to any host.
- ◆ **SNMP Read Community Name:** It specifies the community name used for read-only access to the Switch. Using this community name, your SNMP manager can retrieve the configuration and status information of the Switch.
- ◆ **SNMP Write Community Name:** It specifies the community name used for read-write access to the Switch. Using this community name, your SNMP manager can modify the configuration of the Switch.
- ◆ **SNMP Trap Community Name:** It specifies the community name used when the Switch sends traps.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.

Chapter 8 Linkage

8.1 Linkage Management

The Switch provides linkage management feature to discover and manage the remote switches in the same broadcast domain. It can get the basic information of the remote switches in the same broadcast domain by sending broadcast packets. And it allows you to manage and configure those discovered switches via the local Switch, including port management, network security management, and system administration. In addition, it allows you to perform linkage batch operation to uniformly configure a group of discovered switches, including security binding, restart, reset defaults, retrieve configuration, distribute configuration, and retrieve logs.

8.1.1 Remote Switch Discovery List

In the **Linkage > Linkage Management** page, you can click the **Discover Switch** button to discover the remote switches on your network, and view them in the **Remote Switch Discovery List**, see the following figure.

Remote Switch Discovery List									3/24
1/1	First	Prev	Next	Last	Go to Page	Search			
	Name	Model	Serial Number	IP Address	MAC Address	Port	Password	Admin	
<input type="checkbox"/>	UTT-4	SG3124F	11460052	192.168.16.254	00-22-aa-ae-dd-d4	8	<input type="text"/>	Admin	
<input type="checkbox"/>	UTT-2	SG3124F	135465874	192.168.16.252	00-22-aa-13-0b-92	8	<input type="text"/>	Admin	
<input type="checkbox"/>	UTT-1	SG3124F	11500034	192.168.16.251	00-22-aa-af-7a-02	8	<input type="text"/>	Admin	

Select All

Figure 8-1 Remote Switch Discovery List

- ◆ **Name:** It displays the name of the remote switch.
- ◆ **Mode:** It displays the mode of the remote switch.

- ◆ **Serial Number:** It displays the internal serial number (SN) of the remote switch.
- ◆ **IP Address:** It displays the IP address of the remote switch. You can click the **IP Address** hyperlink to login to the remote switch directly.
- ◆ **MAC Address:** It displays the MAC address of the remote switch.
- ◆ **Port:** It displays the local Switch's port to which the remote switch is connected.
- ◆ **Password:** It specifies the login password of the remote switch. Please enter the correct password, otherwise you cannot manage and configure the switch.
- ◆ **Global Password:** It is used to enter the password for all the remote switches at a time. If you want to configure several remote switches having the same password, you can directly enter the password in this text box, instead of entering passwords one by one.
- ◆ **Admin:** Click to open the remote switch management page to manage and configure the selected remote switch, including **Port Management**, **Network Security Management** and **System Administration**.
 - **Port Management:** It includes **Port Settings**, **Port-based VLAN**, and **Link Aggregation**.
 - **Network Security Management:** It includes **Port Mirroring**, **Rate Limiting** and **Retrieve Logs**.
 - **System Administration:** It includes **System Info**, **System Settings**, **Restart**, **Reset Defaults**, **Retrieve Config** and **Distribute Config**.
- ▶ **Discover Switch:** Click to scan and discover the switches in the same broadcast domain as the local Switch. Once a compatible switch is discovered, the local Switch will automatically add the discovered switch information into the **Remote Switch Discovery List**.
- ▶ **Batch Operate:** To configure more than one remote switch at a time, enter the passwords of the remote switches you want to configure, and then select the leftmost check boxes of them, lastly click the **Batch Operate** button to go to the batch management page to uniformly configure them.
- ▶ **Help:** Click to view the related help information.

**Note**

1. So far, the Switch cannot discover the switches from other companies. And it can only discover the same model of switches from Digital Data Communications Asia Co., Ltd.
2. To configure a remote switch, please enter the correct password. Otherwise the settings will not take effect, and you will be prompted that the operation failed due to a wrong password. By default, the password of the LEVELONE's switches is **admin**.

- The Switch can only discover the switches in the same broadcast domain. That is, the Switch in a VLAN cannot discover any switch in other VLANs.

8.1.2 Remote Switch Management - Single Switch

To manage a remote switch in the **Remote Switch Discovery List**, please enter its password, and then click its **Admin** hyperlink to open the page shown in Figure 8-2.

Remote Switch Information

System Name	UTT-4	Model	SG3124F
Serial Number	11460052	IP Address	192.168.16.254
MAC Address	00-22-aa-ae-dd-d4	Firmware Version	SG3124Fv2.0EN-120301

Remote Switch Management

Port Management					
Port Settings	Port-based VLAN		Link Aggregation		
Network Security Management					
Port Mirroring	Rate Limiting		Retrieve Logs		
System Administration					
System Info	System Settings	Restart	Reset Defaults	Retrieve Config	Distribute Config

Figure 8-2 Remote Switch Management - Single Switch

In this page, you can view some specific information about the selected remote switch, such as **System Name**, **Model**, **Serial Number**, **IP Address**, and so on. You also can configure the remote switch as required. The following sections will describe the features that you can configure.

8.1.2.1 Port Management

8.1.2.1.1 Port Settings

You can click the **Port Settings** hyperlink to open the page shown in Figure 8-3. In this page, you can view port status and configure port parameters of the selected remote switch. Please refer to **Section 6.3 Port Settings** for detailed information. Note that don't forget to click the **Save** button to save any changes.

Global Settings Mode Auto

Port	Port Name	Link Status	Mode	Maximum Frame	Flow Control	Port Protection	Disable Learning
1	<input type="text"/>	Down	Auto <input type="button" value="v"/>	<input type="text" value="1518"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	Down	Auto <input type="button" value="v"/>	<input type="text" value="1518"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	Down	Auto <input type="button" value="v"/>	<input type="text" value="1518"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	Down	Auto <input type="button" value="v"/>	<input type="text" value="1518"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="text"/>	Down	Auto <input type="button" value="v"/>	<input type="text" value="1518"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="text"/>	1Gfdx	Auto <input type="button" value="v"/>	<input type="text" value="1518"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 8-3 Remote Switch Management - Port Settings

8.1.2.1.2 Port-based VLAN

You can click the **Port-based VLAN** hyperlink to open the page shown in Figure 8-4. In this page, you can configure port-based VLAN of the selected remote switch. Please refer to **Section 7.1.2 Port-based VLAN** for detailed information. Note that don't forget to click the **Save** button to save any changes.

Port VLAN List Port VLAN Settings

VLAN ID VLAN Name Add Modify

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

Select All

Figure 8-4 Remote Switch Management - Port-based VLAN

Note

If the selected remote switch's **VLAN Mode** is set to **VLAN Disabled** or **TAG VLAN**, then when you click the **Port-based VLAN** hyperlink, a dialog box will pop up asking you if you are sure you want to change to **Port VLAN** mode.

8.1.2.1.3 Link Aggregation

You can click the **Link Aggregation** hyperlink to open the page shown in Figure 8-5. In this page, you can configure link aggregation of the selected remote switch. Please refer to **Section 7.4 Link Aggregation** for detailed information. Note that don't forget to click

the **Save** bLevelOneon to save any changes.

LAG List
LAG Settings

LAG ID

LAG Name

Add Modify

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

Figure 8-5 Remote Switch Management - Link Aggregation

8.1.2.2 Network Security Management

8.1.2.2.1 Port Mirroring

You can click the **Port Mirroring** hyperlink to open the page shown in Figure 8-6. In this page, you can configure port mirroring of the selected remote switch. Please refer to **Section 6.4 Port Mirroring** for detailed information. Note that don't forget to click the **Save** bLevelOneon to save any changes.

Mirroring Port

Select All

Note: Please select the mirrored ports (e.g., uplink port) as required.

Port	Mirrored Port	Port	Mirrored 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"/>

Figure 8-6 Remote Switch Management - Port Mirroring

8.1.2.2.2 Rate Limiting

You can click the **Rate Limiting** hyperlink to open the page shown in Figure 8-7. In this page, you can configure rate limiting of the selected remote switch. Please refer to **Section 9.2 Rate Limiting** for detailed information. Note that don't forget to click the **Save** bLevelOneon to save any changes.

Storm Control (Packets/Second) Save Cancel Help Back

ICMP Rate	No Limit ▾	Broadcast Rate	No Limit ▾
Multicast Rate	No Limit ▾	Unknown Unicast Rate	No Limit ▾

Rate Limiting Granularity 128 kbps ▾ Save Cancel Help Back

Port	Ingress Rate	Egress Rate	Port	Ingress Rate	Egress Rate
1	No Limit ▾	No Limit ▾	2	No Limit ▾	No Limit ▾
3	No Limit ▾	No Limit ▾	4	No Limit ▾	No Limit ▾
5	No Limit ▾	No Limit ▾	6	No Limit ▾	No Limit ▾
7	No Limit ▾	No Limit ▾	8	No Limit ▾	No Limit ▾
9	No Limit ▾	No Limit ▾	10	No Limit ▾	No Limit ▾
11	No Limit ▾	No Limit ▾	12	No Limit ▾	No Limit ▾
13	No Limit ▾	No Limit ▾	14	No Limit ▾	No Limit ▾
15	No Limit ▾	No Limit ▾	16	No Limit ▾	No Limit ▾
17	No Limit ▾	No Limit ▾	18	No Limit ▾	No Limit ▾
19	No Limit ▾	No Limit ▾	20	No Limit ▾	No Limit ▾
21	No Limit ▾	No Limit ▾	22	No Limit ▾	No Limit ▾
23	No Limit ▾	No Limit ▾	24	No Limit ▾	No Limit ▾

Save Cancel Help Back

Figure 8-7 Remote Switch Management - Rate Limiting

8.1.2.2.3 Retrieve Logs

You can click the **Retrieve Logs** hyperlink to retrieve log messages from the selected remote switch, see Figure 8-8.

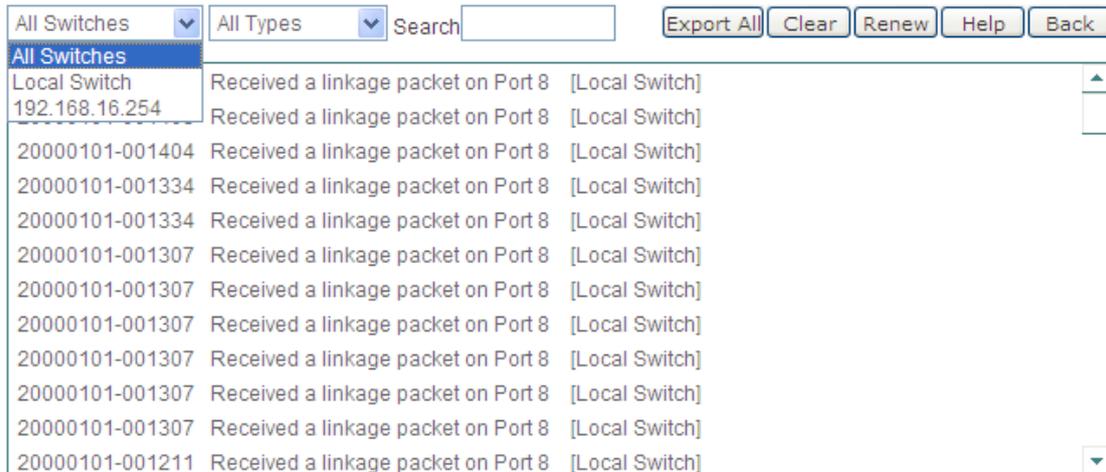


Figure 8-8 Remote Switch Management - Retrieve Logs

- ◆ The First Drop-down List: It allows you to select the switch(es) whose log messages you want to view. The options are **All Switches**, **Local Switch**, the IP address of each remote switch (e.g., 192.168.16.254 shown in the above figure).
- ◆ The Second Drop-down List: It allows you to select the type of log messages to be displayed. The options are **All**, **ARP Spoofing**, **MAC Move**, **Linkage** and **Other**.
- ◆ **Search:** Enter the keyword you want to search for in this text box, and then press **<Enter>** key to view all the matched log messages.
- ▶ **Export All:** Click to export and save all the current log messages to a text file on your local PC.
- ▶ **Clear:** Click to clear all the current log messages of the selected switch(es).
- ▶ **Renew:** Click to retrieve log messages of the selected remote switch(es) again.
- ▶ **Help:** Click to view the related help information.
- ▶ **Back:** Click to go back to the previous page.

8.1.2.3 System Administration

8.1.2.3.1 System Info

You can click the **System Info** hyperlink to open the page shown in Figure 8-9. In this page, you can view the system resources usage information and basic system information of the remote selected switch. Please refer to **Section 5.1 System Information** for detailed information.

System Resources Usage		Help	Refresh
CPU Usage	<input type="text" value="0"/>	0%	
Memory Usage		26%	

Basic System Information	
Current System Time	2000-1-1 06:51:42
System Up Time	0 Day 6 Hour 51 Minute 43 Second
System Name	
Firmware Version	GEL-2460-150722
MAC Address	00-22-aa-da-5b-50
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
CPU VLAN ID	1

Figure 8-9 Remote Switch Management - System Info

8.1.2.3.2 System Settings

You can click the **System Settings** hyperlink to open the page shown in Figure 8-10. In this page, you can configure system settings of the selected remote switch. Please refer to **Section 6.2 System Settings** for detailed information. Note that don't forget to click the **Save** bLevelOneon to save any changes.

System Settings		Save	Cancel	Help
Enable DHCP Relay Agent	<input type="checkbox"/>			
Enable DHCP Client	<input type="checkbox"/>			
IP Address	<input type="text" value="192.168.1.1"/>			
Subnet Mask	<input type="text" value="255.255.255.0"/>			
Default Gateway	<input type="text" value="0.0.0.0"/>			
CPU VLAN ID	<input type="text" value="1"/>			
MAC Address Aging Time(s)	<input type="text" value="300"/>			
System Name	<input type="text"/>			
Password	<input type="password" value="•••••"/>			
Confirm Password	<input type="password" value="•••••"/>			
ARP Spoofing Prevention	<input type="checkbox"/>			

local Switch's configuration to the selected remote switch, please select this option, see the following figure.

Local Configuration File Linkage Configuration File
 Distribution Mode

<input type="checkbox"/> System Settings	<input type="checkbox"/> VLAN Settings	<input type="checkbox"/> Link Aggregation
<input type="checkbox"/> Port Settings	<input type="checkbox"/> Rate Limiting	<input type="checkbox"/> IP/MAC Binding

Figure 8-12 Remote Switch Management - Distribute Config (Local Configuration File)

- ◆ **Distribution Mode:** There are two distribution modes.
 - **Partially Override:** In this mode, you can manually select one or more configuration items to distribute to the selected remote switch.
 - **Fully Override:** In this mode, the local configuration file will fully override the existing configuration of the selected remote switch, except IP address information.
- ◆ **System Settings:** If you want to distribute system settings to the selected remote switch, please select this check box.
- ◆ **VLAN:** If you want to distribute VLAN settings to the selected remote switch, please select this check box.
- ◆ **Link Aggregation:** If you want to distribute link aggregation settings to the selected remote switch, please select this check box.
- ◆ **Port Settings:** If you want to distribute port settings to the selected remote switch, please select this check box.
- ◆ **Rate Limiting:** If you want to distribute rate limiting settings to the selected remote switch, please select this check box.
- ◆ **IP/MAC Binding:** If you want to distribute IP/MAC binding settings to the selected remote switch, please select this check box.

 **Note**

1. In **Fully Override** mode, it will not change the IP address of the selected remote switch.
2. For **System Settings**, only the values of the following parameters can be distributed: **Enable DHCP Relay Agent**, **Enable DHCP Client** and **MAC Address Aging Time**.
3. If you choose **Fully Override** mode to distribute configuration, you need to restart the selected remote switch for the new configuration to take effect. However, in **Partially Override** mode, the new configuration will take effect immediately after distributing.

➤ Linkage Configuration File

It refers to the configuration file of a remote switch, which is retrieved through the **Retrieve Config** operation. If you select this option, you need to select a configuration file you want to distribute in the **Configuration File List**, see the following figure.

The **Distribution Mode** is the same as that of the **Local Configuration File**.

Local Configuration File Linkage Configuration File

Configuration File List 2/24

1/1 First Prev Next Last Go to Page Search

Select a File	Configuration File Name	Creation Time
<input checked="" type="radio"/>	configSG3124F_00-22-AA-AE-DD-D4_20000101_001642.txt	20000101-00:16:42
<input type="radio"/>	configSG3124F_00DD-D4_20120229_154058.txt	20120229-15:41:10

Distribution Mode ▼

<input type="checkbox"/> System Settings	<input type="checkbox"/> VLAN Settings	<input type="checkbox"/> Link Aggregation
<input type="checkbox"/> Port Settings	<input type="checkbox"/> Rate Limiting	<input type="checkbox"/> IP/MAC Binding

Figure 8-13 Remote Switch Management - Distribute Config (Linkage Configuration File)

- ▶ **Reset Defaults:** Click to reset the selected remote switches to factory default settings.
- ▶ **Retrieve Config:** Click to retrieve the configuration files of the selected remote switches.
- ▶ **Distribute Config:** Click to distribute configuration to the selected remote switches.
- ▶ **Retrieve Logs:** Click to retrieve log messages from the selected remote switches.

**Note**

If there is only one MAC address learned on a port of a selected remote switch, it will automatically set that port's IP filtering mode to **Static IP** (in the **Security > IP Filtering** page) after performing the **Security Binding** operation.

8.1.4 Configuration Examples for Remote Switch Management

8.1.4.1 Example 1 - Single Switch

1. Requirements

In this example (see Figure 8-16), there are four GEL-2460 switches in a company's LAN, which include SW251, SW252, SW253 and SW254. Now the administrator wants to remotely manage the other switches through the SW254.

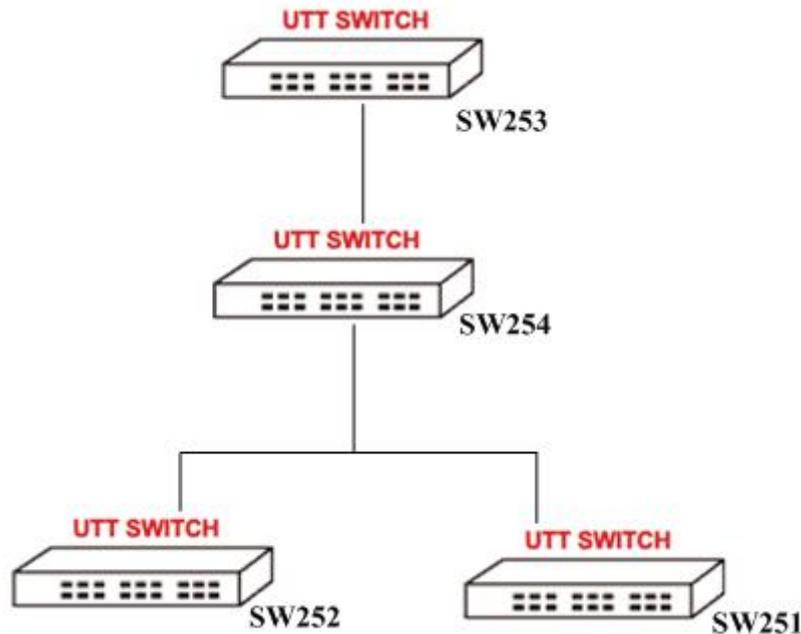


Figure 8-16 Network Topology - Remote Switch Management (Single Switch)

The network environment is as follows:

- 1) The SW254's IP address is 192.168.16.250, administrator user name and password both are admin.
- 2) The SW251's Port 1 is connected to the SW254's Port 1.
- 3) There are two VLANs on the SW251: VLAN 1 (member ports: Port 1-5) and VLAN 2 (member ports: Port 6-10).
- 4) On the SW251, rate limiting is enabled on all ports.
- 5) The SW253 is a new switch.
- 6) The SW253's Port 1 is connected to the SW254's Port3.

The administrator wants to make the following configurations:

- 1) On the SW251, Port 11-20 can communicate with VLAN 1, but cannot communicate with VLAN 2.
- 2) Change the **Egress Rate** and **Ingress Rate** of the SW251's Port 1 to **No Limit**.
- 3) Retrieve the configuration file and log messages of the SW251.
- 4) Make the SW253 have the same configuration as the SW251.

2. Configuration Steps

Step 1 Login to the SW254.

Step 2 Go to the **Linkage > Linkage Management** page, and then click the **Discover**

- Switch** bLevelOneon to discover the other switches. In the **Remote Switch Discovery List**, enter the password of the SW251, and click its **Admin** hyperlink to open the remote switch management page to configure the SW251.
- Step 3** Click the **Port-based VLAN** hyperlink, add a new VLAN (VLAN 3) that contains Port 1-5, 11-20, and then click the **Save** bLevelOneon.
- Step 4** Click the **Rate Limiting** hyperlink, set the Port 1's **Egress Rate** and **Ingress Rate** to **No Limit**, and then click the **Save** bLevelOneon.
- Step 5** Click the **Retrieve Logs** hyperlink to retrieve the log messages of the SW251. Then you can view the log messages of the SW251 and SW254.
- Step 6** Click the **Retrieve Config** hyperlink to retrieve the configuration file of the SW251. Then you can view the retrieved configuration file in the **Configuration File List**.
- Step 7** In the **Remote Switch Discovery List**, enter the password of the SW253, and click its **Admin** hyperlink to open the remote switch management page to configure the SW253.
- Step 8** Click the **Distribute Config** hyperlink to open the distribute configuration page.
- Step 9** Select the **Linkage Configuration File** radio box, and select the configuration file of the SW251 in the **Configuration File List**.
- Step 10** Select **Fully Override** from the **Distribution Mode** drop-down list, and then click the **Distribute** bLevelOneon to distribute the selected configuration file to the SW253.
- Step 11** After distributing, click the **Restart** bLevelOneon to restart the SW253 for the new configuration to take effect.

8.1.4.2 Example 2 - Batch Operation

1. Requirements

In this example (see Figure 8-17), there are four GEL-2460 switches in a company's LAN, which include SW251, SW252, SW253 and SW254. Now the administrator wants to remotely manage all the other switches through the SW254.

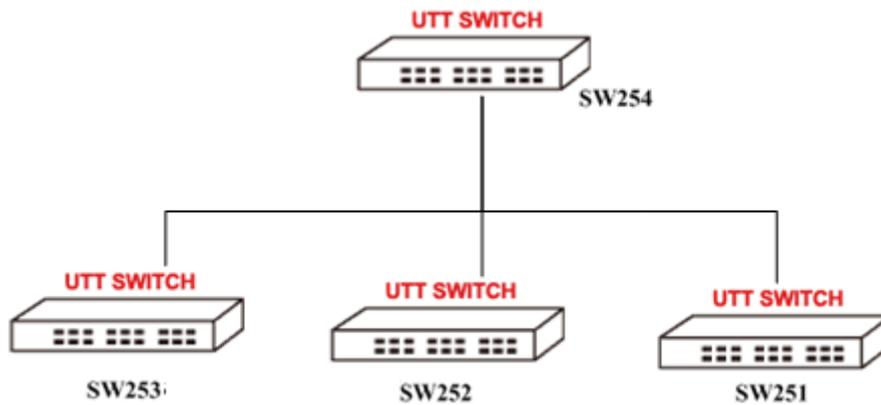


Figure 8-17 Network Topology - Remote Switch Management (Batch Operation)

The administrator wants to make the following configurations:

- 1) Change the passwords of all the other switches to the same new password.
- 2) Perform the MAC/Port binding operation for all the other switches.
- 3) Retrieve the configuration files of all the other switches.
- 4) Distribute the system settings of the SW254 to all the other switches.

2. Configuration Steps

Step 1 Login to the SW254.

Step 2 Go to the **Linkage > Linkage Management** page, and then click the **Discover Switch** bLevelOneon to discover other switches. In the **Remote Switch Discovery List**, select the **Select All** check box, enter the passwords of the SW251, SW252 and SW253 respectively (if they have the same password, you can directly enter the password in the **Global Password** text box), and then click the **Batch Operate** bLevelOneon to go to the batch management page to configure them.

Step 3 Enter the new password in the **Password** and **Confirm Password** text boxes, and then click the **Change Password** bLevelOneon.

Step 4 Click the **Security Binding** hyperlink, and then click the **OK** bLevelOneon in the confirmation dialog box.

Step 5 Click the **Retrieve Config** hyperlink to retrieve the configuration files of the SW251, SW252 and SW253. Then you can view the retrieved configuration files in the **Configuration File List**, and click the **Download** bLevelOneon to download each configuration file to your local PC respectively.

Step 6 Click the **Distribute Config** hyperlink to open the distribute configuration page. Select the **Local Configuration File** radio box, select **Partially Override** from the **Distribution Mode** drop-down list, select the **System Settings** check box,

8.1.6 Linkage Log

In the **Linkage > Linkage Log** page, you can view the log messages of the local Switch and remote switches, see Figure 8-19. The log messages of the remote switches are retrieved through the **Retrieve Logs** operation.

The log messages are listed in reverse chronological order of creation (i.e., most recent at the top).

The screenshot shows the Linkage Log interface. At the top, there are two dropdown menus: 'All Switches' and 'All Types', followed by a 'Search' text box. To the right are three buttons: 'Export All', 'Clear', and 'Help'. Below these controls is a list of log messages, each with a timestamp, a description, and a source identifier. The messages are as follows:

20000101-001933	Received a linkage packet on Port 8	[Local Switch]
20000101-001933	Received a linkage packet on Port 8	[Local Switch]
20000101-001933	Received a linkage packet on Port 8	[Local Switch]
20000101-001614	Received a linkage packet on Port 8	[Local Switch]
20000101-001612	Received a linkage packet on Port 8	[Local Switch]
20000101-001612	Received a linkage packet on Port 8	[Local Switch]
20000101-001610	Received a linkage packet on Port 8	[Local Switch]
20000101-001538	Received a linkage packet on Port 8	[Local Switch]
20000101-001538	Received a linkage packet on Port 8	[Local Switch]
20000101-001531	Received a linkage packet on Port 8	[Local Switch]
20000101-001531	Received a linkage packet on Port 8	[Local Switch]
20000101-001510	Received a linkage packet on Port 8	[Local Switch]

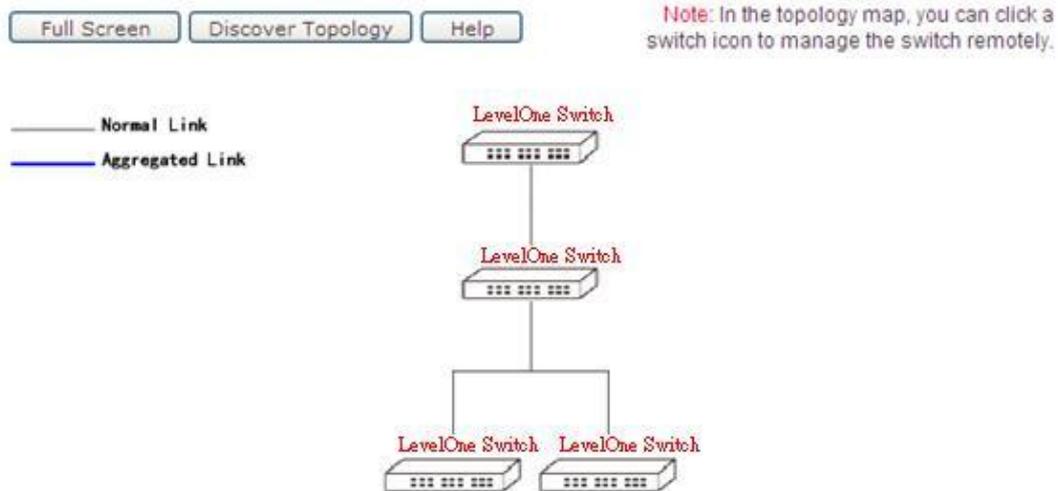
Figure 8-19 Linkage Log

- ◆ The First Drop-down List: It allows you to select the switch(es) whose log messages you want to view. The options are **All Switches**, **Local Switch**, the IP address of each remote switch.
- ◆ The Second Drop-down List: It allows you to select the type of log messages to be displayed. The options are **All**, **ARP Spoofing**, **MAC Move**, **Linkage** and **Other**.
- ◆ **Search:** Enter the keyword you want to search for in this text box, and then press **<Enter>** key to view all the matched log messages.
- ▶ **Export All:** Click to export and save all the current log messages to a text file on your local PC.
- ▶ **Clear:** Click to clear all the current log messages of the selected switch(es).
- ▶ **Help:** Click to view the related help information.

8.1.7 Network Topology

In the **Linkage > Network Topology** page, you can click the **Discover Topology** bLevelOneon to discover switches in the same broadcast domain, which support topology

discovery protocol; and display their network topology.



[\(Please install SVG Viewer if the page cannot be displayed properly.\)](#)

Figure 8-20 Network Topology

To remotely manage a switch shown in the topology map, please click the switch icon, and then enter its password in the dialog box shown in Figure 8-21.

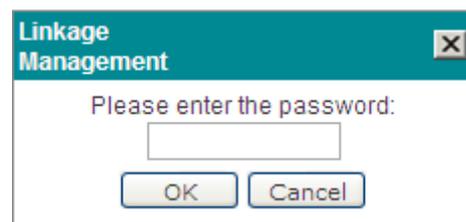


Figure 8-21 Network Topology - Password Input Dialog Box

If you hold your cursor over a switch icon, it will pop up a label which displays the switch information, such as IP address, MAC address, active ports count, etc., see Figure 8-22.

```
IP: 192.168.16.251
MAC: 00-22-AA-AF-7A-02
Model: SG3124F
Parent Node Port: 21
This Node Port: 15
active ports count: 1
```

Figure 8-22 Network Topology - Viewing the Switch Information in the Topology Map

- ◆ **IP:** It displays the IP address of this switch.
- ◆ **MAC:** It displays the MAC address of this switch.
- ◆ **Mode:** It displays the mode of this switch.

- ◆ **Parent Node Port:** It displays the uplink switch's port to which this switch is connected.
- ◆ **This Node Port:** It displays this switch's port to which the uplink switch is connected.
- ◆ **Active Ports Count:** It displays the total number of active ports on this Switch.
- ◆ **Security Alert:** It indicates that alert events have occurred in this switch, such as ARP attack, too high memory usage, etc. You can view the detailed information in its Security Log.
- ◆ **Parent Node Aggregation:** If a LAG (Link Aggregation Group) exists between this switch and the uplink switch, it will display the LAG member ports on the uplink switch.
- ◆ **This Node Aggregation:** If a LAG (Link Aggregation Group) exists between this switch and the uplink switch, it will display the LAG member ports on this switch.

**Note**

1. For the local Switch (that is, the switch you are currently logged into), it will display only the IP address and MAC address.
2. For the local Switch, it won't display security alert information even if the alert events occur.

Chapter 9 Security

9.1 Security Log

In the **Security > Security log** page, you can view various types of security log messages, such as system startup, ARP spoofing, MAC move, and so on.

The log messages are listed in reverse chronological order of creation (i.e., most recent at the top).

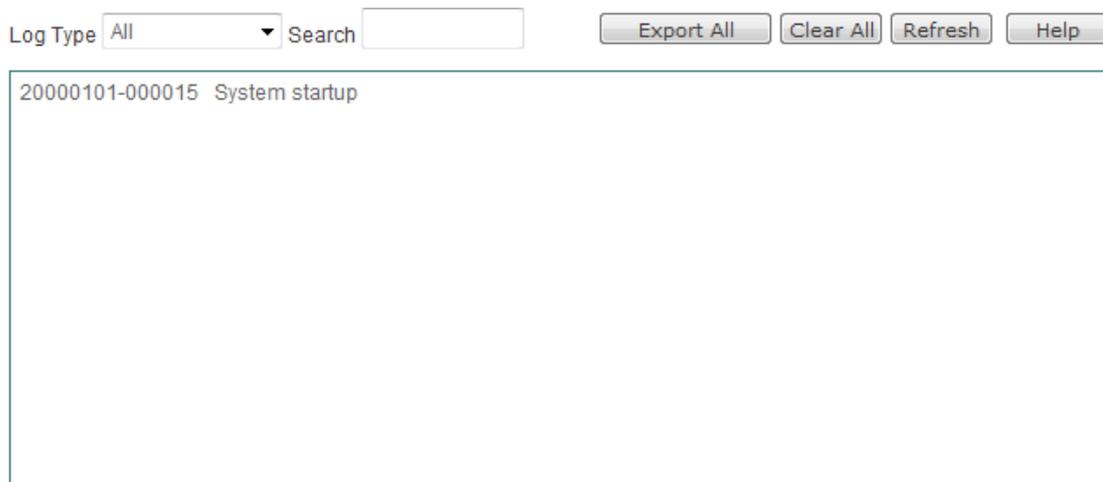


Figure 9-1 Security Log

- ◆ **Log Type:** It specifies the type of log messages to be displayed. There are five options: **All**, **ARP Spoofing**, **MAC Move**, **Linkage** and **Other**.
- ◆ **Search:** Enter the keyword you want to search for in this text box, and then press **<Enter>** key to view all the matched log messages.
- ▶ **Export All:** Click to export and save all the current log messages to a text file on your local PC.
- ▶ **Clear All:** Click to clear all the current log messages.
- ▶ **Refresh:** Click to view the latest log messages.
- ▶ **Help:** Click to view the related help information.

9.2 Rate Limiting

In the **Security > Rate Limiting** page, you can configure the storm control and rate limiting features.

9.2.1 Storm Control

Storm control allows you to limit the amount of ICMP packets, broadcast packets, multicast packets and unknown unicast packets accepted and forwarded by the Switch respectively. This feature can be used to optimize network performance effectively.

Storm Control (Packets/Second) Save Cancel Help

ICMP Rate	No Limit ▾	Broadcast Rate	No Limit ▾
Multicast Rate	No Limit ▾	Unknown Unicast Rate	No Limit ▾

Figure 9-2 Storm Control

- ◆ **ICMP Rate:** It specifies the maximum rate (packets per second) at which ICMP packets are forwarded.
- ◆ **Broadcast Rate:** It specifies the maximum rate (packets per second) at which broadcast packets are forwarded.
- ◆ **Multicast Rate:** It specifies the maximum rate (packets per second) at which the multicast packets are forwarded.
- ◆ **Unknown Unicast Rate:** It specifies the maximum rate (packets per second) at which unknown unicast packets are forwarded.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.

9.2.2 Rate Limiting

Rate limiting allows you to set the maximum bandwidth for ingress traffic and egress traffic on each port.

Rate Limiting Granularity

Port	Ingress Rate	Egress Rate	Port	Ingress Rate	Egress Rate
1	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>	2	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>
3	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>	4	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>
5	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>	6	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>
7	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>	8	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>
9	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>	10	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>
11	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>	12	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>
13	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>	14	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>
15	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>	16	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>
17	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>	18	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>
19	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>	20	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>
21	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>	22	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>
23	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>	24	<input type="text" value="No Limit"/>	<input type="text" value="No Limit"/>

Figure 9-3 Rate Limiting

- ◆ **Granularity:** It specifies the granularity for rate limiting. It is a global parameter which applies to all ports. The available egress/ingress rates are integer multiples of the selected granularity.
- ◆ **Port:** It indicates the port number.
- ◆ **Ingress Rate:** It specifies the maximum rate (kilobits per second) of ingress traffic on the port.
- ◆ **Egress Rate:** It specifies the maximum rate (kilobits per second) of egress traffic on the port.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.

9.3 IP Address Filtering

9.3.1 Introduction to DHCP Snooping

The Switch supports DHCP snooping to prevent DHCP spoofing attacks. DHCP spoofing attacks occur when an attacker masquerades as a valid DHCP server to reroute traffic to his machine, by advertising itself as the default gateway or DNS server. More specifically, let's assume that one or more valid DHCP servers are present on your local network. The danger is that an attacker can place a rogue DHCP server on the network. If the rogue server answers DHCP requests more quickly than the valid DHCP server, it will assign the false IP addresses and other TCP/IP configuration parameters to all DHCP clients in the network.

DHCP snooping is a feature that blocks DHCP responses from ports that don't have valid DHCP servers associated with them. The Switch allows you to set each port as a trusted port or an untrusted port. Trusted ports forward any received DHCP messages, while untrusted ports discard the DHCP responses from DHCP servers. So that your local computers can only obtain IP addresses from the DHCP servers connected to trusted ports. In conclusion, to prevent DHCP spoofing, you only need to designate the ports connecting to the valid DHCP servers as trusted ports, and all other ports as untrusted ports.

9.3.2 IP Filtering Settings

Global Settings Mode Disabled

Port	Allowed IP Addresses			DHCP Snooping Trust
	Mode	IP Address	Subnet Mask	
1	Static IP <input type="text" value="Static IP"/>	<input type="text" value="192.168.16.1"/>	<input type="text" value="255.255.255.255"/>	<input checked="" type="checkbox"/>
2	Disabled <input type="text" value="Disabled"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
3	Disabled <input type="text" value="Disabled"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
4	Disabled <input type="text" value="Disabled"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
5	Disabled <input type="text" value="Disabled"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
6	Disabled <input type="text" value="Disabled"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
7	Disabled <input type="text" value="Disabled"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
8	Disabled <input type="text" value="Disabled"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>

Figure 9-4 IP Address Filtering

- ◆ **Port:** It indicates the port number.
- ◆ **Mode:** It specifies the mode of IP filtering. The options are **Disabled**, **Static IP** and **DHCP**.
 - **Disabled:** It means that IP address filtering is disabled on the port. This option is selected by default.
 - **Static IP:** It means that only the hosts in the subnet specified by **IP Address** and **Subnet Mask** can communicate with the Switch via the port.
 - **DHCP:** It means that the Switch will record the source IP address of the first DHCP packet received on the port, and only the host that has obtained this IP address can communicate with the Switch via the port.
- ◆ **IP Address** and **Subnet Mask:** If you select **Static IP** from the **Mode** drop-down list on a port, you need to specify the allowed IP subnet of the port.
- ◆ **DHCP Snooping Trust:** It determines whether a port is a DHCP snooping trusted port or an untrusted port. If you want to set the port as a trusted port, please select the check box. Please refer to **Section 9.3.1 Introduction to DHCP Snooping** for detailed information.

9.4 IP/MAC Binding

In the **Security > IP/MAC Binding** page, you can configure IP/MAC bindings to effectively prevent ARP spoofing attacks.

9.4.1 IP/MAC Binding

The Switch provides IP/MAC binding feature to implement user identification. Using the IP/MAC address pair as a unique user identity, you can protect the Switch and your network against IP spoofing attacks. IP spoofing attack refers to that a computer attempts to use another trusted computer's IP address to communicate with the Switch. The computer's IP address can easily be changed to a trusted address, but MAC address cannot easily be changed as it is added to the Ethernet card at the factory.

9.4.2 The Operation Principle of IP/MAC Binding

For the sake of convenience, we firstly introduce several related terms including legal user, illegal user and undefined user.

- **Legal User:** A legal user's IP and MAC address pair matches an IP/MAC binding.
- **Illegal User:** An illegal user's IP address or MAC address is the same as that of an IP/MAC binding, but not both.
- **Undefined User:** An undefined user's IP address and MAC address both are different from any IP/MAC binding. The undefined users are all the users except legal and illegal users.

It allows the legal users to communicate with the Switch, and denies the illegal users. And the parameter of **Allow Undefined LAN PCs** determines whether it allows the undefined users to communicate with the Switch, that is, it will allow them if the **Allow Undefined LAN PCs** check box is selected, else block them.

When receiving a packet, the Switch will firstly determine the sender's identity by comparing the packet with the IP/MAC bindings in the **IP/MAC Binding List**, and then process the packet according to the sender's identity. The details are as follows:

1. If the sender is a legal user, the packet will be allowed to pass, and then be further processed by other function modules.
2. If the sender is an illegal user, the packet will be dropped immediately to prevent IP spoofing.

3. If the sender is an undefined user, there are two cases:
 - 1) If the **Allow Undefined LAN PCs** check box is selected, the packet will be allowed to pass, and then be further processed by other function modules.
 - 2) Else, the packet will be dropped immediately.

9.4.3 IP/MAC Binding Settings

IP/MAC Binding Settings

Subnet /

	<input checked="" type="radio"/> Add <input type="radio"/> Modify
Host Name	<input type="text"/>
IP Address	<input type="text"/>
MAC Address	<input type="text"/>
Description	<input type="text"/>

<==>

All Ports

Figure 9-5 IP/MAC Binding Settings

- ◆ **Host Name:** It indicates the host name of the local computer. It is read-only.
- ◆ **IP Address:** It specifies the IP address to be bound.
- ◆ **MAC Address:** It specifies the MAC address to be bound.
- ◆ **Description:** It specifies the description of the IP/MAC binding.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.
- ◆ **Subnet:** It specifies the subnet you want to scan. The default is the Switch's IP address and subnet mask.
- ▶ **Scan:** If you click the **Scan** button, the Switch will immediately scan the specified subnet, learn and display dynamic ARP information (that is, IP and MAC address pairs) in the list box.
- ▶ **<==>:** Select an IP/MAC address pair (e.g., 192.168.16.140 00-e0-4c-19-03-2d) in the list box, and then double-click it or click the **<==>** button, the selected IP address and MAC address will be displayed in the corresponding text boxes. Then click the **Save** button to add the selected IP/MAC address pair to the **IP/MAC**

Binding List.

- ▶ **Bind:** Select a port number from the drop-down list first, and then click the **Bind** button to bind the IP/MAC address pairs associated with that port. In addition, you can select **All Ports** and click the **Bind** button to bind all IP/MAC address pairs in the list box.



Note

If a computer's IP and MAC address pair has been added into the **IP/MAC Binding List**, the IP/MAC address pair will not be displayed in the list box after you perform the scan operation.

9.4.4 IP/MAC Binding List

The screenshot displays the 'IP/MAC Binding List' interface. At the top, there are two tabs: 'IP/MAC Binding List' (selected) and 'IP/MAC Binding Settings'. Below the tabs, there is a header bar with 'IP/MAC Binding List' on the left and '1/512' on the right. The main area contains a table with the following columns: Host Name, IP Address, MAC Address, Port, Description, and Edit. The first row of the table has the following data: Host Name (empty), IP Address (1.1.1.1), MAC Address (00-AA-22-11-22-33), Port (empty), Description (empty), and Edit (with edit and delete icons). Below the table, there are several controls: a 'Select All' checkbox, a checked 'Allow Undefined LAN PCs' checkbox, a 'Save' button, a 'Delete' button with a dropdown arrow, an 'OK' button, and an 'Add' button.

Figure 9-6 IP/MAC Binding List

- ◆ **Allow Undefined LAN PCs:** It allows or blocks the undefined local computers from communicating with the Switch. If you want to allow the undefined local computers to communicate with the Switch, select the check box.
- ▶ **Save:** Click to save your changes.
- ▶ **Add an IP/MAC Binding:** To add a new IP/MAC binding, first click the **Add** button or select the **IP/MAC Binding Settings** tab to go to the setup page, next configure it, lastly click the **Save** button.
- ▶ **View IP/MAC Binding(s):** When you have configured one or more IP/MAC bindings,

you can view them in the **IP/MAC Binding List**.

- ▶ **Modify an IP/MAC Binding:** To modify a configured IP/MAC binding, click its  icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- ▶ **Delete IP/MAC Binding(s):** There are three ways to delete IP/MAC bindings.
 1. To delete an IP/MAC binding, directly click its  icon.
 2. To delete more than one IP/MAC binding at a time, select the leftmost check boxes of the IP/MAC bindings you want to delete, and then select **Delete** from the drop-down list in the lower right corner of the list, lastly click the **OK** button.
 3. To delete all the IP/MAC bindings at a time, select **Delete All** from the drop-down list in the lower right corner of the list, and then click the **OK** button.



Note

If you want to clear the **Allow Undefined LAN PCs** check box to block the undefined local computers from communicating with the Switch, please make sure that you have added the IP/MAC address pair of the computer that you use to administer the Switch into the **IP/MAC Binding List**. Otherwise you cannot access the Switch from that computer.

9.5 MAC/Port Binding

9.5.1 Dynamic MAC Address Table

Each switch maintains a MAC address table to forward frames effectively. The MAC address table records MAC addresses associated with each port. The switch dynamically builds the address table by learning the source MAC address of the frames received. Initially, the MAC address table is empty. When the switch receives a frame from a host, the switch forwards the frame to all ports except the one which received the frame, and records the frame's source MAC address (that is, the host's MAC address) and the port that received the frame in the address table. The switch then forwards any future frames destined for this MAC address directly to this port instead of flooding all ports.

The switch uses an aging mechanism. If a dynamically learned MAC address remains inactive for a specific amount of time (defined by **MAC Address Aging Time**), it is removed from the address table.

9.5.2 Static MAC/Port Binding

You can also manually add static MAC address entries to the MAC address table if desired. A static MAC address is bound to its assigned port, and it cannot be learned on another port until the address is removed. In addition, a static address doesn't age and must be manually removed.

On the GEL-2460 Switch, static MAC address is also called MAC/Port binding. If a computer's MAC address is bound to a port of the Switch, the computer must be connected to that port in order to communicate with the Switch. If the computer is connected to another port, in order that the computer is able to communicate with the Switch, you need to delete the corresponding MAC/Port binding entry or modify the binding entry's port number.

9.5.3 MAC/Port Binding Settings

MAC/Port Binding Settings

MAC/Port Binding Settings

Scan

	<input checked="" type="radio"/> Add <input type="radio"/> Modify
Host Name	<input type="text"/>
MAC Address	<input type="text"/>
Port	<input type="text"/>
Description	<input type="text"/>

Save Cancel Help

All Ports Binding

Figure 9-7 MAC/Port Settings

- ◆ **Host Name:** It indicates the host name of the local computer. It is read-only.
- ◆ **MAC Address:** It specifies the MAC address to be bound.
- ◆ **Port:** It specifies the port to be bound. The range is 1 to 24.
- ◆ **Description:** It specifies the description of the MAC/Port binding.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.
- ▶ **Scan:** Click to display the dynamically learned MAC addresses and their associated ports in the list box.
- ▶ **<==:** Select a MAC/Port entry (e.g., 4 00-26-c7-50-11-22) in the list box, and then double-click it or click the **<==** button. The selected MAC address and port number will be displayed in the corresponding text boxes. Then click the **Save** button to add the selected MAC/Port entry to the **MAC/Port Binding List**.
- ▶ **Bind:** Select a port number from the drop-down list first, and then click the **Bind** button to bind the MAC addresses learned on the port to it. In addition, you can select **All Ports** and then click the **Bind** button to bind all dynamically learned MAC addresses to their associated ports.

Note

If a MAC address has been bound to a port of the Switch, the MAC address will not be displayed in the list box after you perform the scan operation.

If a computer's MAC address is bound to a port of the Switch, the computer must be connected to that port in order to communicate with the Switch. If the computer connected to another port, in order that the computer is able to communicate with the Switch, you need to delete the corresponding MAC/Port binding entry or modify the binding entry's port number.

9.6 Access Restriction

In this page, you can enable device access restriction, and specify a range of local computers that are exempt from the restriction. In other words, those specified computers can access and manage the Switch, but all other computers cannot. For example, as shown in Figure 9-9 Device Access Restriction Settings, only the local computers in the address range of 192.168.16.20 through 192.168.16.100 can access and manage the Switch.



Enable Device Access Restriction

Start IP Address

End IP Address

Figure 9-9 Device Access Restriction Settings

- ◆ **Enable Device Access Restriction:** It allows you to enable or disable device access restriction. If you want to enable device access restriction, please select the check box.
- ◆ **Start IP Address and End IP Address:** They specify a range of IP addresses. After you enable device access restriction, only the local computers in the specified address range can access and manage the Switch.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.

 **Note**

1. If you want to enable device access restriction, please make sure that your computer's IP address is within the range specified by the **Start IP Address** and **End IP Address**. Otherwise you cannot access the Switch from that computer.
2. If both **Start IP Address** and **End IP Address** are set to 0.0.0.0, the system will automatically disable device access restriction.

Chapter 10 Administration

10.1 System Time

To ensure that the time-related functions work well, you should synchronize the system clock.

You can manually configure the system time or enable SNTP (Synchronize with SNTP Server) to automatically synchronize the system time from a designated SNTP server on the Internet. It is suggested that you choose SNTP to automatically synchronize time in most cases.

Current System Time Date 2012-3-2 Time 20:21:38

Time Zone UTC+0800 (Beijing, Chongqing, Hongkong, Urumchi) ▼

Set Time Manually 2012 ▼ Year 3 ▼ Month 2 ▼ Date 20:21:38

Synchronize with SNTP Server

SNTP Server 1 IP Address * 192.43.244.18

SNTP Server 2 IP Address * 129.6.15.28

SNTP Server 3 IP Address 0.0.0.0

Note: To ensure that SNTP operates properly, you should select the correct time zone.

Figure 10-1 System Time Settings

- ◆ **Current System Time:** It displays the current system date (YYYY-MM-DD) and time (HH:MM:SS).
- ◆ **Time Zone:** It specifies the time zone for your local time. To ensure that SNTP operates properly, you must select the correct time zone.
- ◆ **Set Time Manually:** If you want to set the date (YYYY-MM-DD) and time (HH:MM:SS) for the Switch manually, select this radio button.

- ◆ **Synchronize with SNTP Server:** If you want the Switch to automatically synchronize the system clock from a designated SNTP server on the Internet, select this radio button.
- ◆ **SNTP Server 1 IP Address ~ SNTP Server 3 IP Address:** It allows you to configure up to three SNTP servers on the Switch. The Server 1 is the primary server (the default value is 192.43.244.18), and the Server 2 is the first backup server (the default value is 129.6.15.28), and the Server 3 is the second backup server (the default value is 0.0.0.0).
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Help:** Click to view the related help information.

**Note**

For more information about SNTP, or to find an SNTP server with which you can synchronize the system clock, please refer to <http://www.ntp.org>.

10.2 Configuration

Backup Configuration to Local PC

Restore Configuration

Reset to Factory Defaults before Restore

Select a Configuration File

Reset to Factory Defaults

Note: 1) The reset operation will clear all custom settings, so you'd better backup the current configuration before resetting.
2) After performing the restore or reset operation, please restart the Switch for the changes to take effect.

Figure 10-2 Configuration Backup and Restore

- ▶ **Save:** Click to export and save the Switch's current configuration to a text file on your local computer.
- ◆ **Reset to Factory Defaults before Restore:** If you select this check box, it will reset the Switch to factory default settings before importing the configuration file; else import the file directly.
- ◆ **Select a Configuration File:** Click the **Browse** button to choose an appropriate configuration file or enter the file path and name in the text box.
- ▶ **Restore:** Click to import the selected configuration file. It will overwrite the current configuration on the Switch with the new configuration.
- ▶ **Reset:** To reset the Switch to factory default settings, click the **Reset** button, and then restart the Switch.

 **Note**

1. The reset operation will clear all of the Switch's custom settings. It is strongly recommended that you backup the current configuration before resetting.
2. After performing the reset operation, you must manually restart the Switch in order for the default settings to take effect.

10.3 Firmware Upgrade

Current Firmware Version

Select a Firmware File

Restart after Upgrade

Please select the appropriate firmware file according to the product model. You'd better go to Administration > Configuration page to backup the Switch's current configuration before upgrade.

To avoid any unrecoverable error, Do NOT turn off the power during upgrading.

Figure 10-3 Firmware Upgrade

- ◆ **Current Firmware Version:** It displays the version of the current firmware installed on the Switch.
- ◆ **Select a Firmware File:** Click the **Browse** button to choose the firmware file you want to upgrade or enter the file path and name in the text box.
- ◆ **Restart after Upgrade:** After the upgrade is complete, the Switch will automatically restart in order for the new firmware to take effect.
- ▶ **Upgrade:** After you choose the firmware file, click the **Upgrade** button to renew the Switch's firmware.



Note

1. Before you upgrade the firmware, please click the **Download Firmware** hyperlink to download the latest firmware from the website of levelone technologies co. ltd.
2. It is suggested that you reset the Switch to factory default settings before upgrade.
3. It is strongly suggested that you upgrade the firmware when the Switch is under light load.
4. To avoid any unexpected error or unrecoverable hardware damage, do not power off the Switch during upgrading.
5. Don't leave the current page during upgrading.
6. After the upgrade is complete, the Switch will automatically restart in order for the new firmware to take effect, without human intervention.

10.4 Restart

Please refer to **Section 4.3 Restart** for detailed information.

10.5 Help

The **Administration > Help** page provides the basic online help information.

Appendix A Contact Information

If you have any questions regarding the operation or installation of the GEL-2460 Switch, please contact us in any of the following ways.

- **Technical Support Phone:** +886-0800-011-110
- **LEVELONE Forum:** <http://www.level1.com/>
- **E-mail:** support@level1.com

Appendix B Figure Index

Figure 1-1 Front Panel of GEL-2460.....	3
Figure 1-2 Rear Panel of the Switch	5
Figure 2-1 Installing the Switch in a Rack	7
Figure 3-1 Entering IP address in the Address Bar	10
Figure 3-2 Login Screen	10
Figure 3-3 Homepage - Setup Wizard	11
Figure 3-4 Web UI Layout.....	12
Figure 3-5 Main Menu Bar	13
Figure 4-1 Running the Setup Wizard.....	17
Figure 4-2 Setup Wizard - Password Settings	18
Figure 4-3 Setup Wizard - IP Address Settings.....	19
Figure 4-4 Setup Wizard - Switch Type Settings.....	19
Figure 4-5 Setup Wizard - Link Aggregation Group (Edge Switch)	20
Figure 4-6 Setup Wizard - Port Mirroring (Core Switch).....	21
Figure 4-7 Summary Statistics.....	23
Figure 4-8 Restart the Switch.....	24
Figure 4-9 Prompt Dialog Box - Restart the Switch.....	24
Figure 5-1 System Information.....	25
Figure 5-2 Port Traffic Chart.....	27
Figure 6-1 System Settings.....	29
Figure 6-2 Port Settings	31
Figure 6-3 Port Mirroring.....	33
Figure 7-1 VLAN Mode Settings	35
Figure 7-2 Enabling Port-based VLAN.....	36
Figure 7-3 Port-based VLAN Settings.....	36
Figure 7-4 Port-based VLAN List	37
Figure 7-5 Enabling Tag-based VLAN.....	39
Figure 7-6 Tag-based VLAN Settings.....	39
Figure 7-7 Tag-based VLAN List	40
Figure 7-8 VLAN Port Settings.....	41
Figure 7-9 Network Topology – Tag-based VLAN Configuration Example	42
Figure 7-10 RSTP Bridge Overview.....	43

Figure 7-11 RSTP Port Status.....	44
Figure 7-12 RSTP Bridge Settings.....	46
Figure 7-13 RSTP Port Settings.....	47
Figure 7-14 LACP Status	49
Figure 7-15 LACP Settings	51
Figure 7-16 LAG Settings.....	53
Figure 7-17 Link Aggregation List	54
Figure 7-18 Disabling QoS.....	55
Figure 7-19 802.1p Priority Settings.....	56
Figure 7-20 Port-based Priority Settings	57
Figure 7-21 SNMP Settings	58
Figure 8-1 Remote Switch Discovery List	59
Figure 8-2 Remote Switch Management - Single Switch	61
Figure 8-3 Remote Switch Management - Port Settings.....	62
Figure 8-4 Remote Switch Management - Port-based VLAN.....	62
Figure 8-5 Remote Switch Management - Link Aggregation.....	63
Figure 8-6 Remote Switch Management - Port Mirroring.....	64
Figure 8-7 Remote Switch Management - Rate Limiting.....	64
Figure 8-8 Remote Switch Management - Retrieve Logs	65
Figure 8-9 Remote Switch Management - System Info.....	66
Figure 8-10 Remote Switch Management - System Settings.....	67
Figure 8-11 Remote Switch Management - Configuration File List	67
Figure 8-12 Remote Switch Management - Distribute Config (Local Configuration File)	68
Figure 8-13 Remote Switch Management - Distribute Config (Linkage Configuration File)	69
Figure 8-14 Remote Switch Discovery List	70
Figure 8-15 Remote Switch Management - Batch Management.....	70
Figure 8-16 Network Topology - Remote Switch Management (Single Switch)	72
Figure 8-17 Network Topology - Remote Switch Management (Batch Operation)	74
Figure 8-18 Configuration File List.....	75
Figure 8-19 Linkage Log	76
Figure 8-20 Network Topology	77
Figure 8-21 Network Topology - Password Input Dialog Box	77
Figure 8-22 Network Topology - Viewing the Switch Information in the Topology Map	77
Figure 9-1 Security Log.....	79
Figure 9-2 Storm Control.....	80
Figure 9-3 Rate Limiting.....	81
Figure 9-4 IP Address Filtering.....	83

Figure 9-5 IP/MAC Binding Settings 85

Figure 9-6 IP/MAC Binding List..... 86

Figure 9-7 MAC/Port Settings 89

Figure 9-8 MAC/Port Binding List..... 90

Figure 9-9 Device Access Restriction Settings..... 92

Figure 10-1 System Time Settings 93

Figure 10-2 Configuration Backup and Restore 95

Figure 10-3 Firmware Upgrade 96

Appendix C Table Index

Table 1-1 Technical Specification	3
Table 1-2 Description of LEDs on the Front Panel	4
Table 3-1 Description of Menu Items.....	15
Table 3-2 Description of Common BLevelOneons	16