



GEL-2461

24-Port L2 Managed Gigabit Ethernet Switch, 16 Ports SFP

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 REPECT TO THE SOFTWARE AND DOCUMENTAITON. LEVELONE AND ITS LICENSORS DISCLAIM ALL OTHER WARRANTIES, INCLUSIVE OF WITHOUT LIMITATION, IMPLIED WARRANTIES OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. 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 DOCUMENTAITON 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.



Table of Contents

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	4
Chapter 2 Hardware Installation	5
2.1 Installation Requirements	5
2.2 Installing the Switch	5
2.2.1 Installing the Switch in a 19-inch Rack	5
2.2.2 Installing the Switch on a Level Surface	6
2.3 Connecting Network Devices	6
2.4 Connecting the Power	7
Chapter 3 Logging in to the Switch	8
3.1 Configuring Your Computer	8
3.2 Logging in to the Switch	8
3.3 Introduction to Web UI	9
3.3.1 Introduction to Menu Items	9
3.3.2 Description of Common Buttons	11
3.3.3 Web UI Idle Timeout	11
Chapter 4 Setup Wizard	12
4.1 Password Settings	12
4.2 IP Address Settings	13
4.3 Switch Type Settings	13
4.4 Link Aggregation Group Settings	14
4.5 Security Binding	15
4.6 Port Mirroring Settings	15
Chapter 5 Status	18
5.1 Summary Statistics	18
5.2 Port Statistics	19
5.3 RSTP Status	19

5.3.1	RSTP Bridge Overview	19
5.3.2	RSTP Port Status	20
5.4	LACP Status.....	21
5.4.1	LACP Aggregation Overview.....	21
5.4.2	LACP Port Status.....	22
Chapter 6	Basic	23
6.1	Setup Wizard.....	23
6.2	System Settings.....	23
6.3	Port Settings.....	26
6.4	Port Mirroring.....	27
Chapter 7	Advanced	29
7.1	VLAN.....	29
7.1.1	VLAN Mode Settings.....	29
7.1.2	Port-based VLAN.....	29
7.1.3	Tag-based VLAN.....	32
7.2	RSTP.....	36
7.2.1	RSTP Bridge Settings.....	36
7.2.2	RSTP Port Settings	37
7.3	LACP.....	38
7.3.1	Introduction LACP	38
7.3.2	LACP Settings	39
7.4	QoS.....	40
7.4.1	Disabling QoS	40
7.4.2	802.1p Priority Settings	40
7.4.3	Port-based Priority Settings	41
7.5	Link Aggregation	42
7.5.1	Introduction to Link Aggregation	42
7.5.2	Link Aggregation Settings	43
7.6	Linkage Management	44
Chapter 8	Security	47
8.1	Security Log.....	47
8.2	MAC/PORT Binding	48
8.2.1	Dynamic MAC Address Table.....	48
8.2.2	Static MAC/PORT Binding	48
8.2.3	MAC/PORT Binding Settings	49
8.2.4	MAC/PORT Binding List.....	50
8.3	Rate Limiting.....	51
8.3.1	Storm Control	51
8.3.2	Rate Limiting.....	52
8.4	IP Filtering.....	53

8.4.1	Introduction to DHCP Snooping	53
8.4.2	IP Filtering Settings	54
8.5	IP/MAC Binding.....	54
8.5.1	IP/MAC Binding	55
8.5.2	The Operation Principle of IP/MAC Binding.....	55
8.5.3	IP/MAC Binding Settings.....	56
8.5.4	IP/MAC Binding List	57
8.6	Access Restriction	58
Chapter 9	Administration	59
9.1	Configuration.....	59
9.2	Firmware Upgrade	60
9.3	Restart.....	61
9.4	Exit.....	61
Appendix A	Contact Information.....	62
Appendix B	Figure Index.....	63
Appendix C	Table Index.....	65

Chapter 1 Product Overview

Thanks for choosing the GEL-2461 24-Port Intelligent Managed Gigabit Switch from levelone technologies co. ltd.

GEL-2461 is a 24-Port Managed Gigabit Switch, providing secure and intelligent edge connectivity.

The device is a Layer 2 wire-speed Ethernet switch, perfect for deployments in small and medium businesses, branch offices, and for running essential business services. GEL-2461 offers 8 x 10/100/1000M auto-negotiation ports and 16 SFP combo ports. All RJ-45 ports support auto MDI/MDI-X, with SNMP and Full/Half duplex transfer mode for 10 and 100Mbps ports as well as Full duplex transfer mode for 1000Mbps ports. Supports Jumbo frame, MAC address auto-learning and a host of other features such as security logs and detailed traffic statistics for each port..

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
- 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	8 10/100/1000M RJ-45 Ports + 16 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-2461 Switch contains the LEDs, 8 10/100/1000M RJ-45 ports, 16 Gigabit SFP combo ports, a Reset button, and a Console port.



Figure 1-1 Front Panel of GEL-2461



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	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	Port Speed LED	The LED lights steady when another device is connected to the corresponding port and a 1000Mbps link is established between them.

Table 1-2 Description of LEDs on the Front Panel

2. Reset Button

If you forgot the administrator password, you need to use the Reset button 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 button for more than 5 seconds, and then release the button. 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-2461 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-2461 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-2461 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 192.168.16.x (x is between 2 and 253, including 2 and 253) 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.

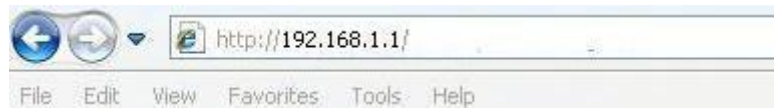


Figure 3-1 Entering IP address in the Address Bar

When you login to the Switch, the default password is **admin**, click **OK**. See Figure 3-2.



Figure 3-2 Login Screen

3.3 Introduction to Web UI

3.3.1 Introduction to Menu Items

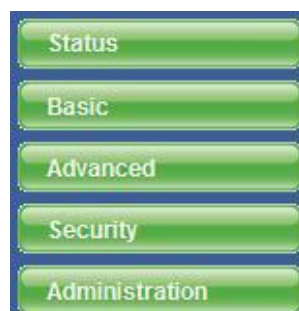


Figure 3-3 Main Menu Bar

As shown in Figure 3-3, the two-level main menu bar contains seven first level menu items, which include **Status**, **Basic**, **Advanced**, **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
Status	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.
	RSTP Status	It displays the RSTP status.
	LACP Status	It displays LACP aggregation overview and each port status.
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).
	QoS	It allows you configure 802.1p priority and port-based priority.
	Link Aggregation	It allows you to configure static link aggregation groups.
	Linkage Management	It allows you to view and manage the remote switches in the same broadcast domain.
Security	Security Log	It displays security log messages.
	MAC/PORT Binding	It allows you to configure MAC/Port bindings, that is, static MAC addresses.
	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.
	Access Restriction	It allows you to enable device access restriction, and specify a range of computers that are exempt from the restriction.
Administration	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.
	Exit	Exit the web configuration interface.

Table 3-1 Description of Menu Items

3.3.2 Description of Common Buttons

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

Button 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.

Table 3-2 Description of Common Buttons

3.3.3 Web UI Idle Timeout

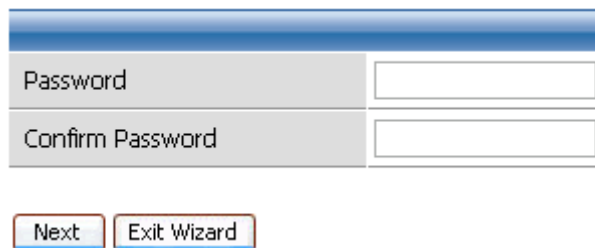
The Web UI idle timeout is 300 seconds. The purpose of the idle timeout is for security. If you logs in and forgets to log out, the system will automatically log you out after 300 seconds of inactivity.

Chapter 4 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 Password Settings

The Switch's default password is blank. To ensure security, it is strongly recommended that you set the 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	<input type="text"/>
Confirm Password	<input type="text"/>

Figure 4-1 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.



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.

4.2 IP Address Settings

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

Figure 4-2 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.

4.3 Switch Type Settings

In this page, you can choose the type of the Switch, see Figure 4-3. In terms of physical placement, there are edge switches and core switches.

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

Figure 4-3 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.

4.4 Link Aggregation Group Settings

This page provides a predefined LAG (Link Aggregation Group).When you choose **Edge Switch** in the **Setup Wizard – Switch Type Settings**, this page provides a predefined LAG that only contains Port 23 and Port 24, see Figure 4-5. You can enable or disable the predefined LAG.

1. Enable LAG(Port1 Port2)	<input type="checkbox"/>
2. Enable LAG(Port3 Port4)	<input type="checkbox"/>
3. Enable LAG(Port5 Port6)	<input type="checkbox"/>
4. Enable LAG(Port7 Port8)	<input type="checkbox"/>
5. Enable LAG(Port9 Port10)	<input type="checkbox"/>
6. Enable LAG(Port11 Port12)	<input type="checkbox"/>
7. Enable LAG(Port13 Port14)	<input type="checkbox"/>
8. Enable LAG(Port15 Port16)	<input type="checkbox"/>

Note: If you configure LAG here, it will clear the LAGs already configured.

Figure 4-4 Setup Wizard – LAG (Core Switch)

Enable LAG (Port 23, 24)	<input type="checkbox"/>
--------------------------	--------------------------

Note: If you configure LAG here, it will clear the LAGs already configured.

Figure 4-5 Setup Wizard - LAG (Edge Switch)

- ◆ **Enable LAG:** It allows you to enable or disable the predefined LAG. If you want to enable the predefined LAG, please select the check box.

 **Note**

If you configure LAG here, it will clear the LAGs already configured.

4.5 Security Binding

If you choose **Edge Switch** in the **Setup Wizard - Switch Type Settings** page, after setting the **LAG**, the **Setup Wizard – Security Binding** page will appear, see Figure 4-7. Else, this page will not appear.

View All Ports

Port	Link Status	IP/MAC/PORT Binding	IP Address	MAC Address
9	1000FDX	<input type="checkbox"/>	192.168.16.126	6c-62-6d-e9-6d-13
16	100FDX	<input type="checkbox"/>	192.168.16.1	00-22-aa-b8-cd-07

Figure 4-6 Setup Wizard – Security Binding (Edge Switch)

- ◆ **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.
- ◆ **IP/MAC/PORT Binding:** Select the check box to bind the IP/MAC address pairs associated with the port.
- ◆ **IP Address and MAC Address:** It displays the host's IP address and MAC address which on the switch port.
- ◆ **View All Ports:** It displays all ports.

 **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.

4.6 Port Mirroring Settings

If you choose **Core Switch** in the **Setup Wizard - Switch Type Settings** page, after setting the **LAG**, the **Setup Wizard - Port Mirroring** page will appear, see Figure 4-7. 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.



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 checked="" type="checkbox"/>	24	<input checked="" type="checkbox"/>

Select All

Figure 4-7 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**.



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.

Chapter 5 Status

5.1 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	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0
9	507029	1103	362855	1146	101	24	0
10	55891	79	24565	213	0	112	0
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0
16	449768	1295	15647194	18829	279	4755	0
17	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0

Figure 5-1 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.

5.2 Port Statistics

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 5.1 Summary Statistics** for detailed description of the parameters.

5.3 RSTP Status

5.3.1 RSTP Bridge Overview

Bridge ID	Hello Time	Max Age	Forward Delay	Topology	Root ID
32768:00-22-aa-23-fb-6e	2	20	15	Steady	32768:00-22-aa-23-fb-6e

[RSTP Settings](#)

Figure 5-2 RSTP Bridge Overview

- ◆ **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** page.
- ◆ **Max Age:** It displays the **Max Age** configured in the **Advanced > RSTP** page.
- ◆ **Forward Delay:** It displays the **Forward Delay** configured in the **Advanced > RSTP** 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.
- ▶ **RSTP Setting:** Click to go to the **Advanced > RSTP** page.

5.3.2 RSTP Port Status

RSTP Port Status

Port	Path Cost	Edge Port	Protocol	Port Status
Port 1				Disabled
Port 2				Disabled
Port 3				Disabled
Port 4				Disabled

Figure 5-3 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.

5.4 LACP Status

5.4.1 LACP Aggregation Overview

LACP Aggregation Overview

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																0								

Refresh

[LACP Settings](#)

Figure 5-4 LACP Aggregation Overview

- ◆ **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.
- ▶ **LACP Settings:** Click to go to the **Advanced > LACP** page.

5.4.2 LACP Port Status

LACP Port Status

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	yes	0	2

Figure 5-5 LACP Port Status

- ◆ **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.

Chapter 6 Basic

6.1 Setup Wizard

Please refer to **Section 4 Setup Wizard** for detailed information.

6.2 System Settings

In the **Basic > System Settings** page, you can view the basic system information of the switch(see Figure 6-1), configure DHCP relay agent, DHCP client, IP address, subnet mask, default gateway, VLAN ID, MAC address aging time, password, and so on, see Figure 6-2.

MAC Address	00-22-aa-44-12-31
Firmware Version	GEL-2461-150803
System Up Time	1day, 2hour, 29minute, 26second
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	0.0.0.0
Lease Left	0 secs

Figure 6-1 System Information

- ◆ **MAC Address:** It displays the base MAC address of the Switch.
- ◆ **Serial Number:** It displays the internal serial number (SN) of the Switch, which may be different from the SN found on the label at the bottom of the Switch.
- ◆ **Firmware Version:** It displays the version of the current firmware installed on the Switch.
- ◆ **System Up Time:** It displays the elapsed time (in days, hours, minutes and seconds) since the Switch was last started.
- ◆ **IP Address, Subnet Mask and Default Gateway:** They display the current IP

address, subnet mask and default gateway address of the Switch.

- ◆ **DHCP Server:** It displays the DHCP Server's IP address of the Switch.
- ◆ **Lease Left:** It displays the time remaining until the current IP address lease expires.

System Date	2009 <input type="button" value="v"/> Year 01 <input type="button" value="v"/> Month 02 <input type="button" value="v"/> Day
System Time	02 : 40 : 01
Enable DHCP Relay Agent	<input type="checkbox"/>
Enable DHCP Client	<input type="checkbox"/>
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
CPU VLAN ID	1
MAC Address Aging Time(s)	300
System Name	
Password	•••••
Confirm Password	•••••
ARP Spoofing Prevention	<input type="checkbox"/>
Enable SNMP	<input type="checkbox"/>
SNMP Trap Host	0.0.0.0
SNMP Read Community Name	read
SNMP Write Community Name	write
SNMP Trap Community Name	public

Figure 6-2 System Settings

- ◆ **System Date:** It specifies the current system date.
- ◆ **System Time:** It specifies the current system time.
- ◆ **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(s):** 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 blank.
- ◆ **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.
- ◆ **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.

**Note**

1. To ensure security, it is strongly recommended that you set the 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.
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 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	Link Status	Mode	Maximum Frame	Flow Control	Port Protection	Disable Learning	ARP Trusted Port
1	Down	Auto	1518	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	Down	Auto	1518	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	Down	Auto	1518	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	Down	Auto	1518	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	Down	Auto	1518	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	Down	Auto	1518	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	Down	Auto	1518	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	Down	Auto	1518	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	1000FDX	Auto	1518	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	Down	Auto	1518	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	Down	Auto	1518	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	Down	Auto	1518	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	Down	Auto	1518	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	Down	Auto	1518	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	Down	Auto	1518	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16	100FDX	Auto	1518	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 6-3 Port Settings

- ◆ **Global Settings:** It is used to configure all ports at a time. For example, if you set the **Mode** to **1000M/FDX** here, all ports' Mode will be set to **1000M/FDX** automatically.
- ◆ **Port:** It indicates the port number.
- ◆ **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.
- ◆ **ARP Trusted Port:** After you enable ARP spoofing prevention in **Basic > System Settings** page, the Switch will take protection measure if the number of received ARP packets exceeds the threshold. However, you can set a port as an ARP trusted port that is exempt from this restriction.



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

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

Select All

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"/>

Figure 6-4 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**.



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** page, see Figure 7-1.

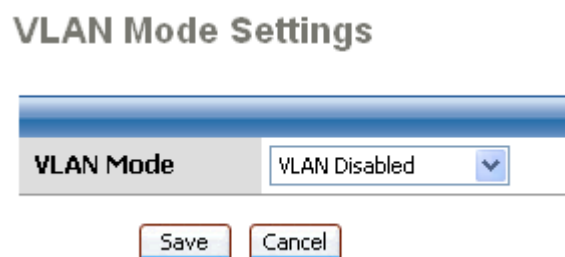


Figure 7-1 VLAN Mode Settings

- ◆ **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**.

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, and then click the **Save** button.

7.1.2.1 Port-based VLAN Settings

In the **Advanced > VLAN** page, you can create port-based VLANs, see Figure 7-2.

Port VLAN

Add Modify

VLAN ID(1-24)

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

Figure 7-2 Port-based VLAN Settings

- ◆ **VLAN ID:** It specifies a number used to identify the port-based VLAN. It must be between 1 and 24.
- ◆ **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 the VLAN ID from the **Port VLAN List**.



Note

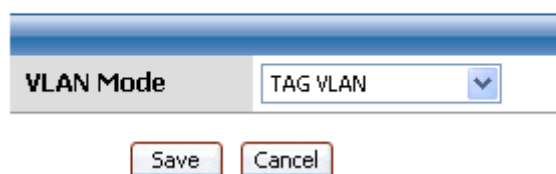
1. On the Switch, the default VLAN is VLAN 1. And all switch ports are members of VLAN 1 by default.
2. A port-based VLAN can contain one or more ports.
3. A port can belong to one or more port-based VLANs.
4. All ports in a LAG must belong to the same port-based VLAN.
5. The Switch supports up to 24 port-based VLANs.

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 and then click the **Save** button, see Figure 7-4.

VLAN Mode Settings



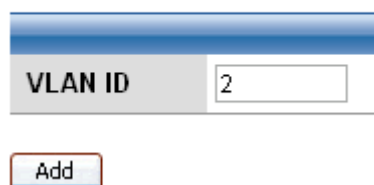
The screenshot shows a web interface titled "VLAN Mode Settings". It features a dropdown menu labeled "VLAN Mode" with "TAG VLAN" selected. Below the dropdown are two buttons: "Save" and "Cancel".

Figure 7-4 Enabling Tag-based VLAN

7.1.3.1 Tag-based VLAN Settings

In the **Advanced > VLAN** page, you can create tag-based VLANs, see Figure 7-5.

Add a VLAN



The screenshot shows a web interface titled "Add a VLAN". It features a text input field labeled "VLAN ID" containing the number "2". Below the field is an "Add" button.

Figure 7-5 Tag-based VLAN Settings

- ◆ **VLAN ID:** It specifies a number used to identify the tag-based VLAN. It must be between 1 and 4094.
- ▶ **Add:** Click the **Add** button to add a new tag-based VLAN and then go to the **VLAN Settings** page to select the VLAN's member.

VLAN Settings

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

Select All

Figure 7-6 Tag-based VLAN Settings

- ◆ **Port:** It indicates the port number.
- ◆ **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.

 **Note**

1. On the Switch, the default VLAN is VLAN 1. And all switch ports are members of VLAN 1 by default.
2. A tag-based VLAN can contain one or more ports.
3. A port can belong to one or more tag-based VLANs.
4. All ports in a LAG must belong to the same tag-based VLAN.

7.1.3.2 Tag-based VLAN List

In the **Advanced > VLAN** page, you can select the **Tag VLAN List** tab to view and edit **Tag VLAN List**, see Figure 7-7.

Tag VLAN List

1	2
<input type="radio"/>	<input checked="" type="radio"/>

Figure 7-7 Tag-based VLAN List

- ▶ **Modify:** To modify a configured tag-based VLAN, select a **VLAN ID**, then click **Modify** button.
- ▶ **Delete:** To delete a tag-based VLAN, select a **VLAN ID**, then click **Delete** button.
- ▶ **Delete All:** To delete all tag-based VLAN at a time.
- ▶ **Port Settings:** Click it to go to the **VLAN Port Settings** page to configure VLAN parameters for each port, see Figure 7-8.



Note

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

7.1.3.3 VLAN Port Settings

VLAN Port Settings

Port	VLAN Aware	Frame Type	PVID
Port 1	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1 <input type="button" value="v"/>
Port 2	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1 <input type="button" value="v"/>
Port 3	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1 <input type="button" value="v"/>
Port 4	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1 <input type="button" value="v"/>

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.

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 GEL-2461 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.

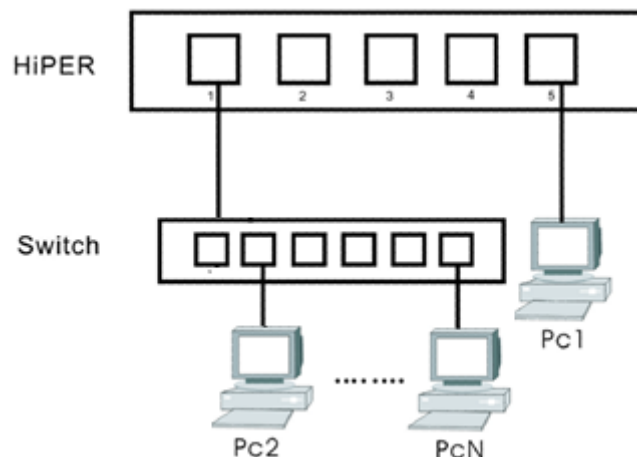


Figure 7-9 Network Topology – Tag-based VLAN Configuration Example

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-2461 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 Bridge Settings

RSTP Settings

Priority	32768 ▾
Hello Time	2
Max Age	20
Forward Delay	15

[View RSTP Status](#)

Figure 7-10 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.
- ▶ **View RSTP Status:** Click to go to the **Status> RSTP Status** page

7.2.2 RSTP Port Settings

RSTP Port Settings

Port	RSTP	Edge Port	Path Cost
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto

Figure 7-11 RSTP Port Settings

- ◆ **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**.

7.3 LACP

7.3.1 Introduction 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.

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-2461 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 7-12. If the remote switch is another vendor's product, you can configure LACP in a similar fashion.

7.3.2 LACP Settings

LACP Port Settings

[View LACP Status](#)

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

Figure 7-12 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**.
- ◆ **View lACP Status:** Click to go to the **Status > LACP Status** page



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 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.

7.4.1 Disabling QoS

To disable QoS on the Switch, select **QoS Disabled** from the **QoS Mode** drop-down list in the **Advanced > Qos** page, and then click the **Save** button, see Figure 7-13.

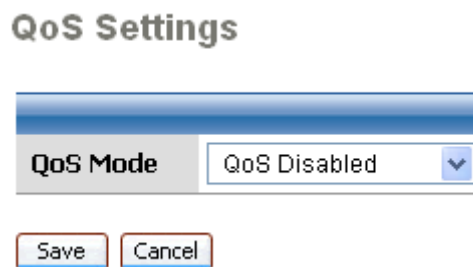


Figure 7-13 Disabling QoS

7.4.2 802.1p Priority Settings

IEEE 802.1p standard provides a mechanism for implementing QoS at the MAC level. Ethernet packets can have an optional 4-byte 802.1 Q 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.

QoS Settings

QoS Mode	802.1p
Global Priority	All Low

802.1p Settings

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

Save Cancel

Figure 7-14 802.1p 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**.

7.4.3 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.

QoS Settings

QoS Mode	Port-based Priority ▼
Global Priority	All Low ▼

Port-based Priority

Port	Priority
1	Low ▼
2	Low ▼
3	Low ▼
4	Low ▼

Figure 7-15 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**.

7.5 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.

7.5.1 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.

7.5.2 Link Aggregation Settings

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

Link Aggregation

LAG\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
None	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 7-16 LAG Settings

- ◆ **LAG:** It specifies a number used to identify the LAG. The Switch supports up to 24 LAGs.
- ◆ **Port:** 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.



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.

- ◆ **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 remote switch.
- ◆ **Remote Operation:** Including IP Settings, Rate Limiting, Port Protection, IP/PORT Banding, MAC/PORT Binding, Save Settings, Check MAC Address. Select the Remote Operation from the drop down list first, then click the **Go** Button to open the remote switch management page to manage and configure the selected remote switch.
 - **IP Settings:** To configure the IP Address, Subnet Mask and Default Gateway of the remote switch.
 - **Rate Limiting:** To configure the maximum rate of ingress/egress traffic on the ports of the remote switch.
 - **Port Protection:** To enable the Port Protection on the ports of the remote switch.
 - **IP/PORT Binding:** To banding the IP/PORT of the remote switch.
 - **MAC/PORT Binding:** To banding the MAC/PORT of the remote switch.
 - **Save Settings:** Save the remote switch's current configuration to a CFG file on your local computer.
 - **Check MAC Address:** To view the MAC Address of the remote switch.
- ◆ **Security Log:** Click the **Check** button can view the security log of the remote switch.
- ◆ **Active Ports Counts:** It dispalys the active ports counts of the remote switch. Click the Count you can view the Ports Status of the remote switch.
- ▶ **Discover Switch:** Click to scan and discover the switches in the same broadcast domain as the local Switch.
- ▶ **Distribute Security Settings:** Click to distribute security to the selected remote switches, including system time, MAC/PORT binding, IP/MAC binding (Remote switches must be enable ARP Spoofing Prevention), default gateway (The IP address of remote switches and default gateway must be on the same subnet).
- ▶ **Secure Binding:** Select the leftmost check boxes of the **Remotes Switch Discovery List**, then click **OK** button to binding the MAC/PORT, MAC/PORT of the remote swithc.
- ▶ **Reset Device:** Select the leftmost check boxes of the **Remote Switch Discovery List**, then click **OK** button to restart the remote switch.
- ▶ **Reset to Factory Defaults:** Select the leftmost check boxes of the **Remote Switch Discovery List**, then click **OK** button to reset the remote switch to factory default settings.

**Note**

1. So far, the Switch cannot discover the switches from other companies. And it can only discover the same model of switches from UTT Technologies 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.
3. 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.
4. **Distributie Security Settings** operation doesn't require password of the remote switch.

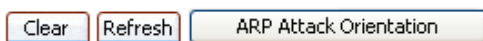
Chapter 8 Security

8.1 Security Log

In the **Security > Security log** page, you can view various types of security log messages, such as 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).

Security Log



[2009/01/01-00:24:33] Received a linkage discover packet from 00-22-aa-ab-34-58

[2009/01/01-00:10:05] Received a linkage discover packet from 00-22-aa-ab-34-58

[2009/01/01-00:05:54] Received a linkage discover packet from 00-22-aa-ab-34-58

Figure 8-1 Security Log

- ◆ **ARP Attack Orientation:** Orientation the current ARP attacks.
- ▶ **Clear:** Click to clear all the current log messages.
- ▶ **Refresh:** Click to view the latest log messages.

8.2 MAC/PORT Binding

8.2.1 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.

8.2.2 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-2461 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.

8.2.3 MAC/PORT Binding Settings

MAC/PORT Binding

The screenshot shows a configuration window titled "MAC/PORT Binding". At the top, there are radio buttons for "Add" (selected) and "Modify". Below this, there are two text input fields: "MAC Address *" containing "00-22-AA-B8-CD-07" and "Port *" containing "16". To the right of these fields is a list box containing two entries: "Port: 16 00-22-AA-B8-CD-07" and "Port: 9 6C-62-6D-E9-6D-13". A button with the symbol "<<--" is positioned between the form and the list box. At the bottom of the window, there are buttons for "Save", "Cancel", "Jump to Port Settings", a dropdown menu labeled "Please se", and "Scan Network".

Figure 8-2 MAC/Port Settings

- ◆ **MAC Address:** It specifies the MAC address to be bound.
- ◆ **Port:** It specifies the port to be bound. The range is 1 to 24.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Scan Network:** Select a port number from the drop-down list first, then click the **Scan Network** button, the list box will display the dynamically learned MAC addresses and their associated ports.
- ▶ **<==:** 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**.

✓ 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.

- ▶ **Bind All IP/MAC/PORT:** To binding all the dynamically learned IP Address, MAC addresses and their associated port, and it should configure the Gateway Address.
- ▶ **Delete All IP/MAC/PORT:** To delete all IP/MAC/PORT bindings.
- ▶ **Disable Port Protection on all Ports:** To disable port protection on all ports.

 **Note**

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.

8.3 Rate Limiting

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

8.3.1 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



Storm Control (Packets/Second)





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

Figure 8-4 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.

8.3.2 Rate Limiting

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

Rate Limiting

Port	Egress Rate	Ingress Rate
1	No Limit	No Limit
2	No Limit	No Limit
3	No Limit	No Limit
4	No Limit	No Limit

Figure 8-5 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.

8.4 IP Filtering

8.4.1 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.

8.4.2 IP Filtering Settings

IP Filtering Settings

Port	Allowed IP Addresses			DHCP Snooping Trust
	Mode	IP Address	Subnet Mask	
1	Static IP <input type="button" value="v"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>
2	DHCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	Disabled <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	Disabled <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Figure 8-6 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.

8.5 IP/MAC Binding

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

8.5.1 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.

8.5.2 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.

8.5.3 IP/MAC Binding Settings

IP/MAC Binding Settings

The screenshot shows a web-based configuration interface for IP/MAC binding. On the left, there is a form with two input fields: 'IP Address *' containing '192.168.16.1' and 'MAC Address *' containing '00-22-aa-b8-cd-07'. Above these fields are radio buttons for 'Add' (selected) and 'Modify'. To the right of the form is a list box containing two entries: '192.168.16.1 00-22-aa-b8-cd-07' and '192.168.16.126 6c-62-6d-e9-6d-13'. A '<<--' button is positioned between the form and the list box. Below the form are 'Save' and 'Cancel' buttons. Below the list box are a 'Please Se...' dropdown menu and a 'Scanning Network' button.

Figure 8-7 IP/MAC Binding Settings

- ◆ **IP Address:** It specifies the IP address to be bound.
- ◆ **MAC Address:** It specifies the MAC address to be bound.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ◆ **Subnet Network:** Select a port number from the drop-down list first, then click the **Subnet Network** button, the Switch will immediately scan the specified port(s), 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., 192.168.16.1 00-22-aa-ae-dd-d6) 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**.

✓ 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.

 **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.

8.6 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 8-9 Device Access Restriction Settings, only the local computers in the address range of 192.168.1.20 through 192.168.1.100 can access and manage the Switch.



Access Restriction	
Start IP Address *	192.168.1.20
End IP Address *	192.168.1.100
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 8-9 Device Access Restriction Settings

- ◆ **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.

 **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 9 Administration

9.1 Configuration

The image shows three distinct sections of a web interface. The first section, titled 'Configuration Update', contains a text input field followed by a 'Browse...' button, and an 'Update' button below it. The second section, titled 'Backup Configuration', contains a single 'Backup' button. The third section, titled 'Reset to Factory Defaults', contains a single 'Reset' button.

Figure 9-1 Configuration Backup and Restore

- ◆ **Configuration Update:** Click the **Browse** button to choose an appropriate configuration file or enter the file path and name in the text box, then click **Update** button.
- ◆ **Backup Configuration:** Click **Backup** button to export and save the Switch's current configuration to a CFG file on your local computer.
- ◆ **Reset to Factory Defaults:** To reset the Switch to factory default settings, click the **Reset** button.

 **Note**

The reset operation will clear all of the Switch's custom settings. It is strongly recommended that you backup the current configuration before resetting.

9.2 Firmware Upgrade

Firmware Upgrade



The screenshot shows a web interface for firmware upgrade. At the top, the title "Firmware Upgrade" is displayed. Below the title is a text input field. To the right of the input field is a button labeled "Browse...". Below the input field is a button labeled "upgrade".

Figure 9-2 Firmware Upgrade

- ◆ **Firmware Upgrade:** Click the **Browse** button to choose the firmware file you want to upgrade or enter the file path and name in the text box.
- ▶ **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 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.

9.3 Restart

Click the **Restart**, you can restart the switch.

9.4 Exit

Click the **Exit**, you can exit the web configuration interface.

Appendix A Contact Information

If you have any questions regarding the operation or installation of the GEL-2461 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-2461	3
Figure 1-2 Rear Panel of the Switch	4
Figure 2-1 Installing the Switch in a Rack	6
Figure 3-1 Entering IP address in the Address Bar	9
Figure 3-2 Login Screen	9
Figure 3-3 Main Menu Bar	9
Figure 4-1 Setup Wizard - Password Settings.....	12
Figure 4-2 Setup Wizard - IP Address Settings.....	13
Figure 4-3 Setup Wizard - Switch Type Settings	13
Figure 4-4 Setup Wizard – LAG (Core Switch).....	14
Figure 4-5 Setup Wizard - LAG (Edge Switch).....	14
Figure 4-6 Setup Wizard – Security Binding (Edge Switch)	15
Figure 4-7 Setup Wizard - Port Mirroring (Core Switch)	16
Figure 5-1 Summary Statistics	18
Figure 5-2 RSTP Bridge Overview	19
Figure 5-3 RSTP Port Status	20
Figure 5-4 LACP Aggregation Overview	21
Figure 5-5 LACP Port Status.....	22
Figure 6-1 System Information	23
Figure 6-2 System Settings	24
Figure 6-3 Port Settings	26
Figure 6-4 Port Mirroring	28
Figure 7-1 VLAN Mode Settings.....	29
Figure 7-2 Port-based VLAN Settings.....	30
Figure 7-3 Port-based VLAN List.....	31
Figure 7-4 Enabling Tag-based VLAN	32
Figure 7-5 Tag-based VLAN Settings.....	32
Figure 7-6 Tag-based VLAN Settings.....	33
Figure 7-7 Tag-based VLAN List	34
Figure 7-8 VLAN Port Settings	34
Figure 7-9 Network Topology – Tag-based VLAN Configuration Example	35
Figure 7-10 RSTP Bridge Settings.....	36
Figure 7-11 RSTP Port Settings	37
Figure 7-12 LACP Settings	39
Figure 7-13 Disabling QoS	40
Figure 7-14 802.1p Priority Settings	41
Figure 7-15 Port-based Priority Settings.....	42
Figure 7-16 LAG Settings.....	43

Figure 7-17 Remote Switch Discovery List.....	44
Figure 9-1 Security Log	47
Figure 9-2 MAC/Port Settings	49
Figure 9-3 MAC/Port Binding List.....	50
Figure 9-4 Storm Control.....	52
Figure 9-5 Rate Limiting.....	52
Figure 9-6 IP Address Filtering	54
Figure 9-7 IP/MAC Binding Settings	56
Figure 9-8 IP/MAC Binding List.....	57
Figure 9-9 Device Access Restriction Settings	58
Figure 10-1 Configuration Backup and Restore	59
Figure 10-2 Firmware Upgrade.....	60

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	11
Table 3-2 Description of Common Buttons	11