



. . . c o n n e c t i n g   y o u r   b u s i n e s s

# LANCOM GS-2124

# LANCOM GS-2124

© 2009 LANCOM Systems GmbH, Wuerselen (Germany). All rights reserved.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from LANCOM Systems. We reserve the right to make any alterations that arise as the result of technical development.

Windows®, Windows Vista™, Windows NT® and Microsoft® are registered trademarks of Microsoft, Corp.

The LANCOM Systems logo, LCOS and the name LANCOM are registered trademarks of LANCOM Systems GmbH. All other names or descriptions used may be trademarks or registered trademarks of their owners.

Subject to change without notice. No liability for technical errors or omissions.

Products from LANCOM Systems include software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org>).

Products from LANCOM Systems include cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).

Products from LANCOM Systems include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from LANCOM Systems contain the LZMA SDK developed by Igor Pavlov.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

[www.lancom.eu](http://www.lancom.eu)

Wuerselen, April 2009

# Preface

## Thank you for your confidence in us!

LANCOM Switches are ideally suited to small, medium-sized and performance networks in business environments.

The LANCOM GS-2124 switch features 20 Fast-Ethernet and four combo ports (TP/SFP), it integrates perfectly into LANCOM's Advanced Routing and Forwarding and it supports up to 256 active VLANs. It uses bandwidth control to prioritize the data traffic according to predefined criteria (e.g. voice data or certain ports).

The LANCOM Switch can be managed with the clearly structured Webconfig and is supported by the LANCOM Management Tools (LANconfig and LANmonitor).

## This documentation was created by ...

... several members of our staff from a variety of departments in order to ensure you the best possible support when using your LANCOM product.

Should you find any errors, or if you would like to suggest improvements, please do not hesitate to send an e-mail directly to:

[info@lancom.eu](mailto:info@lancom.eu)



Our online services [www.lancom.eu](http://www.lancom.eu) are available to you around the clock if you have any questions on the content in this manual, or if you require any further support. The area 'Support' will help you with many answers to frequently asked questions (FAQs). Furthermore, the knowledgebase offers you a large reserve of information. The latest drivers, firmware, utilities and documentation are constantly available for download.

In addition, LANCOM Support is available. For telephone numbers and contact addresses for LANCOM Support, please refer to the enclosed leaflet or the LANCOM Systems Web site.

**Information symbols**



Very important instructions. Failure to observe these may result in damage.



Important instruction that should be observed.



Additional information that may be helpful but is not essential.

# Contents

<b>1 Introduction</b>	<b>9</b>
1.1 Key Features in the Device	9
1.2 Just what can your LANCOM Switch do?	10
<b>2 Installation</b>	<b>13</b>
2.1 Package content	13
2.2 System requirements	13
2.3 Status displays and interfaces	14
2.3.1 Connectors, LEDs and buttons on the LANCOM GS-2124	14
2.3.2 Connectors on rear of the LANCOM GS-2124	15
2.4 Mounting and connecting up the LANCOM Switch	15
2.5 Software installation	16
2.5.1 Starting the software setup	16
2.5.2 Which software should I install?	17
<b>3 Configuring and monitoring the LANCOM Switch</b>	<b>18</b>
3.1 Configuration options	18
3.1.1 Starting WEBconfig	18
3.1.2 Starting the Command Line Interface over the network	20
3.1.3 Starting the Command Line Interface over the serial connection	20
3.2 Which configuration does the device use?	21
3.3 Save/Restore	22
3.3.1 Factory Defaults	23
3.3.2 Save Start	23
3.3.3 Save User	24
3.3.4 Restore User	24
3.4 Export/ Import Configuration File	25
3.5 Monitoring the LANCOM Switch with LANmonitor	25
3.5.1 Ethernet port status	25

<b>4 Operation of Web-based Management</b>	<b>27</b>
4.1 Web Management Home Overview	28
4.2 System: Basic Config	31
4.2.1 System Information	31
4.3 Account	33
4.3.1 Time	33
4.3.2 IP Configuration	36
4.3.3 Loop Detection	38
4.3.4 Management Policy	39
4.3.5 System Log	42
4.3.6 Virtual Stack	43
4.3.7 System: Port	45
4.3.8 Configuration	46
4.3.9 Port Status	48
4.3.10 Simple Counter	51
4.3.11 Detail Counter	52
4.4 Security: MAC	55
4.4.1 Mac Address Table	55
4.4.2 Static Filter	57
4.4.3 Static Forward	58
4.4.4 MAC Alias	59
4.4.5 MAC Table	60
4.5 Security: VLAN	61
4.5.1 VLAN Mode	61
4.5.2 Tag-based Group	62
4.5.3 Port-based Group	64
4.5.4 Ports	67
4.5.5 Port Isolation	68
4.5.6 Management VLAN	69
4.6 Security: ACL	69
4.6.1 Ports	70
4.6.2 Rate Limiters	71
4.6.3 Access Control List	72
4.6.4 Wizard	87
4.7 Security: IP MAC Binding	88
4.8 Security: DHCP Snooping	90
4.8.1 DHCP Snooping State	90
4.8.2 DHCP Snooping Entry	91

4.8.3	DHCP Snooping Client	93
4.9	Security: 802.1x Configuration	94
4.9.1	Server	98
4.9.2	Port Configuration	100
4.9.3	Status	103
4.9.4	Statistics	104
4.10	Security: Mirror	105
4.11	Configuration: GVRP	106
4.11.1	Config	107
4.11.2	Counter	109
4.11.3	Group	111
4.12	Configuration: QoS (Quality of Service) Configuration	112
4.12.1	Ports	113
4.12.2	Qos Control List	114
4.12.3	Rate Limiters	117
4.12.4	Storm Control	118
4.12.5	Wizard	119
4.13	Configuration: Trunk	121
4.13.1	Port	123
4.13.2	Aggregator View	126
4.13.3	Hash Method	127
4.13.4	LACP System Priority	128
4.14	Configuration: STP	128
4.14.1	STP Status	129
4.14.2	Configuration	131
4.14.3	Port	133
4.15	Configuration: MSTP	135
4.15.1	Status	136
4.15.2	Region Config	136
4.15.3	Instance View	137
4.16	Configuration: Multicast	143
4.16.1	IGMP Mode	143
4.16.2	Proxy	144
4.16.3	Snooping	145
4.16.4	IGMP Group Membership	145
4.17	Management: Alarm Configuration	147
4.17.1	Events	147
4.17.2	Email	148



4.18 Management: Diagnostics	149
4.18.1 Diag	149
4.18.2 Ping	150
4.19 Management: Maintenance	150
4.19.1 Reset device	150
4.19.2 Firmware upgrade	151
4.20 Management: SNMP	152
4.21 Logout	154
<b>5 Operation of CLI Management</b>	<b>155</b>
5.1 CLI Management	155
5.1.1 Login	155
5.2 Commands of CLI	156
5.2.1 Global Commands of CLI	156
5.2.2 4-2-2. Local Commands of CLI	162
<b>6 Appendix</b>	<b>274</b>
6.1 Performance data and specifications	274
6.2 Connector wiring	275
6.2.1 LAN interface 10/100Base-TX	275
6.3 Declaration of conformity	275

# 1 Introduction

The LANCOM Switch models LANCOM GS-2124 are managed layer-2 switches with 20 Gigabit ports (for twisted pair cable – TP) and four Gigabit dual media ports with TP/SFP, which meets the IEEE 802.3/u/x/z Gigabit, Fast Ethernet and Ethernet specifications

The switch can be managed through RS-232 serial port via directly connection, or through Ethernet port using Telnet or Web-based management unit, associated with SNMP agent. With the SNMP agent, the network administrator can logon the switch to monitor, configure and control each port's activity in a friendly way.

The overall network management is enhanced and the network efficiency is also improved to accommodate high bandwidth applications. In addition, the switch features comprehensive and useful function such as QoS (Quality of Service), Spanning Tree, VLAN, Port Trunking, Bandwidth Control, Port Security, SNMP/RMON and IGMP Snooping capability via the intelligent software. It is suitable for both metro-LAN and office application.

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

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

## 1.1 Key Features in the Device

### ■ QoS:

Support Quality of Service by the IEEE 802.1P standard. There are two priority queue and packet transmission schedule using Weighted Round Robin (WRR). User-defined weight classification of packet priority can be based on either VLAN tag on packets or user-defined port priority.

### ■ Spanning Tree:

Support IEEE 802.1D, IEEE 802.1w (RSTP: Rapid Spanning Tree Protocol) standards.

### ■ VLAN:

Support Port-based VLAN and IEEE802.1Q Tag VLAN. Support 256 active VLANs and VLAN ID 1~4094.

- **Port Trunking:**  
Support static port trunking and port trunking with IEEE 802.3ad LACP.
- **Bandwidth Control:**  
Support ingress and egress per port bandwidth control.
- **Port Security:**  
Support allowed, denied forwarding and port security with MAC address.
- **SNMP/RMON:**  
SNMP agent and RMON MIB. In the device, SNMP agent is a client software which is operating over SNMP protocol used to receive the command from SNMP manager (server site) and echo the corresponded data, i.e. MIB object. Besides, SNMP agent will actively issue TRAP information when happened.  
  
RMON is the abbreviation of Remote Network Monitoring and is a branch of the SNMP MIB.  
  
The device supports MIB-2 (RFC 1213), Bridge MIB (RFC 1493), RMON MIB (RFC 1757)-statistics Group 1,2,3,9, Ethernet-like MIB (RFC 1643), Ethernet MIB (RFC 1643) and so on.
- **IGMP Snooping:**  
Support IGMP version 2 (RFC 2236): The function IGMP snooping is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoid wasting the bandwidth while IP multicast packets are running over the network.

## 1.2 Just what can your LANCOM Switch do?

LANCOM GS-2124	
Hardware	
Supports 20-port 10/100/1000 Mbps TP ports and auto MDIX function	✓
4 Gigabit dual media ports(TP/SFP)	✓
On-line pluggable fiber transceiver modules	✓
256KB packet buffer and 128KB control memory	✓
Maximal packet length can be up to 1536 bytes	✓

LANCOM GS-2124	
Full-duplex flow control (IEEE802.3x) and half-duplex backpressure	✓
<b>Sstatus LEDs</b>	
System: Power	✓
TP Port 1-24: LINK/ACT, SPD	✓
SFP-Ports 21,22,23,24: LINK/ACT, SPD, SFP	✓
<b>PoE support</b>	
PoE with 48VDC power through RJ-45 pin 1, 2, 3, 6.	
Powered Device(PD) auto detection and classification.	
PoE-PSE status and activity LED indicator.	
<b>Management</b>	
Concisely the status of port and easily port configuration	✓
Per port traffic monitoring counters	✓
Port mirror function	✓
Static trunk function	✓
802.1Q VLAN with 256 entries.	✓
DHCP Broadcasting Suppression to avoid network suspended or crashed	✓
Trap event while monitored events happened	✓
Default configuration which can be restored to overwrite the current configuration which is working on via web browser and CLI	✓
5 kinds of QoS, are as follows, MAC Priority, 802.1p Priority, IP TOS Priority, and DiffServ DSCP Priority.	✓
Built-in web-based management and CLI management, providing a more convenient UI for the user	✓
Rapid Spanning Tree (802.1w RSTP)	✓
802.1x port security on a VLAN	✓
SNMP access can be disabled and prevent from illegal SNMP access	✓
Ingress, Non-unicast and Egress Bandwidth rating management	✓
The trap event and alarm message can be transferred via e-mail and mobile phone short message	✓

LANCOM GS-2124	
Diagnostics to let administrator knowing the hardware status	✓
External loopback test to check if the link is ok	✓
HTTP for firmware upgrade, system log upload and config file import/export	✓
Remote boot the device through user interface and SNMP	✓
Network time synchronization and daylight saving	✓
120 event log records in the main memory and display on the local console	✓
<b>Options</b>	
LANCOM SFP Transceiver: Item no. 61556 LANCOM SFP-SX-LC1 Item no. 61557 LANCOM SFP-LX-LC1	✓

## 2 Installation

This chapter will assist you to quickly install hardware and software. First, check the package contents and system requirements. The device can be installed and configured quickly and easily if all prerequisites are fulfilled.

### 2.1 Package content

Before beginning with the installation, please check that nothing is missing from your package. Along with the LANCOM Switch the box should contain the following accessories:

	LANCOM GS-2124
Power cord	✓
19" adapter (2 pieces) and mounting materials	✓
Serial configuration cable	✓
LANCOM CD	✓
Printed documentation	✓

Should anything be missing, please take up immediate contact to your dealer or to the address on the delivery note supplied with your device.

### 2.2 System requirements

Computers that connect to a LANCOM must meet the following minimum requirements:

- Operating system that supports TCP/IP, e.g. Windows Vista™, Windows XP, Windows Millennium Edition (Me), Windows 2000, Windows 98, Linux, BSD Unix, Apple Mac OS, OS/2.
- Access to the LAN via the TCP/IP protocol.



The LANtools also require a Windows operating system. A web browser under any operating system provides access to WEBconfig.

## 2.3 Status displays and interfaces

### Meanings of the LEDs

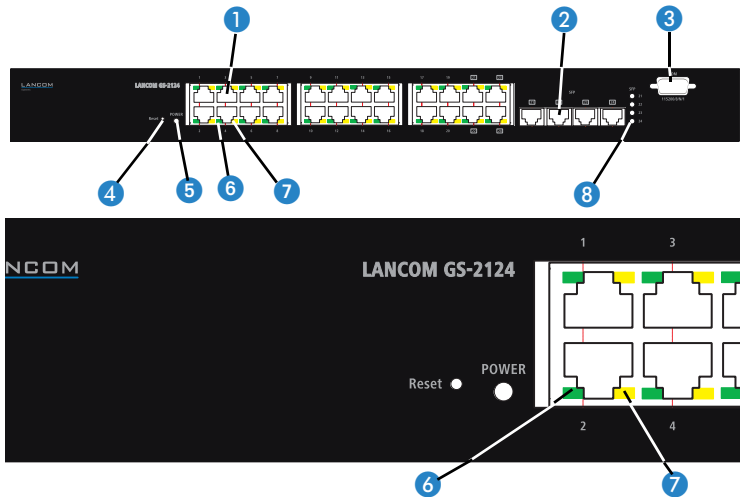
The following section describes the meaning of the LEDs.



Please be aware that LANmonitor shows far more information about the status of the LANCOM Switch than the LEDs '→ Monitoring the LANCOM switch with LANmonitor'.

### 2.3.1 Connectors, LEDs and buttons on the LANCOM GS-2124

Located on the front of the device are connectors for different cabled types, light-emitting diodes (LEDs) that provide information on device status, and also a button.



- |   |                  |  |
|---|------------------|--|
| 1 | TP connectors    | Connectors for twisted-pair cables.                      |
| 2 | SFP connectors   | Connectors for small form-factor pluggable (SFP) cables. |
| 3 | Serial connector | Connector for serial configuration cable.                |
| 4 | Reset            | Button to re-start the system.                           |
| 5 | POWER LED        | Constant green when power is supplied to the device.     |

- 6 LINK / ACT LED Port 1 to 24
  - Constant green when the network connection is established to the connected device.
  - Blinks during data transfer.
  - Off if no network connection can be established to the connected device.
- 7 10/100/1000 Mbps LED
  - Constant green when the 1000 Mbps mode is active.
  - Constant orange when the 100 Mbps mode is active.
  - Off when the 10 Mbps is active.
- 8 SFP (LINK/ACT) LED
  - Constant green when the network connection is established to the connected device.
  - Blinks during data transfer.
  - Off if no network connection can be established to the connected device.

### 2.3.2 Connectors on rear of the LANCOM GS-2124

The following connectors are located on the rear of the device.



- 1 Connector for the power supply cable.

## 2.4 Mounting and connecting up the LANCOM Switch

Installing the LANCOM Switch involves the following steps:


- 1 **Mounting** – The device is designed for mounting in an available 19" unit in a server cabinet. If necessary fix the rubber pads to the underside of the device to prevent any scratching to other equipment.

! Ensure that the device has sufficient ventilation to prevent damage from excessive heat build-up.


- 2 **LAN connection** – Connect the network devices to the ports of the LANCOM Switch by means of a suitable twisted-pair cable (TP cable). The connectors automatically detect the available data transfer speeds and the pin assignment (autosensing).



---

 Use only standard TP cables of category CAT 5 or better with a maximum length of 100 m to ensure the best possible transfer of data. Cross-over cables can be used thanks to the auto-sensing function.

---

 If optical connections are to be used, additional modules can be purchased as accessories.

---

**③ Configuration via serial ports** – In order to configure the LANCOM Switch directly, connect the serial configuration cable (supplied) to the COM port of the device. Connect the other end of this cable to an available COM port (RS 232) on a PC. Instructions on carrying out a configuration via the serial interface and on entering relevant parameters via a terminal program are available under → 'Starting the Command Line Interface via serial connection' in the following chapter.


**④ Supply power and switch on** – Supply power to the device by means of the IEC power cable.

**⑤ Ready for operation?** – After a brief self-test, the power LED lights up continuously. Green LAN-LINK LEDs show which LAN connectors are being used for a connection.

## 2.5 Software installation

The following section describes the installation of the Windows-compatible system software LANtools, as supplied.

---


 You may skip this section if you use your LANCOM Switch exclusively with computers running operating systems other than Windows.

---

### 2.5.1 Starting the software setup

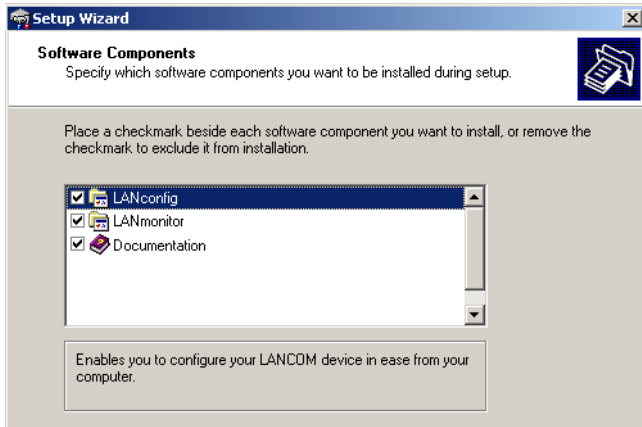
Place the product CD into your drive. The setup program will start automatically.

---

 If the setup does not start automatically, run AUTORUN.EXE in the root directory of the LANCOM CD.

---

In Setup, select **Install software**. The following selection menus will appear on screen:



## 2.5.2 Which software should I install?

- **LANconfig** is the Windows configuration program for all LANCOM devices. LANconfig searches for all LANCOM devices in your network. You can use this to start the Web-based configuration of a LANCOM Switch.
- With **LANmonitor** you can use a Windows computer to monitor all of your LANCOM devices. This program displays all important status information for a LANCOM Switch, such as link status or port PoE state.
- With **Documentation** you copy the documentation files onto your PC.

Select the appropriate software options and confirm your choice with **Next**. The software is installed automatically.

## 3 Configuring and monitoring the LANCOM Switch

### 3.1 Configuration options

There are two different methods of configuring the device.

- By means of a graphical user interface or via a browser (WEBconfig). This option is only available if you have network access to the device's IP address from your computer.

Instructions for configuring the device with WEBconfig are available in the chapter "Web-based configuration".

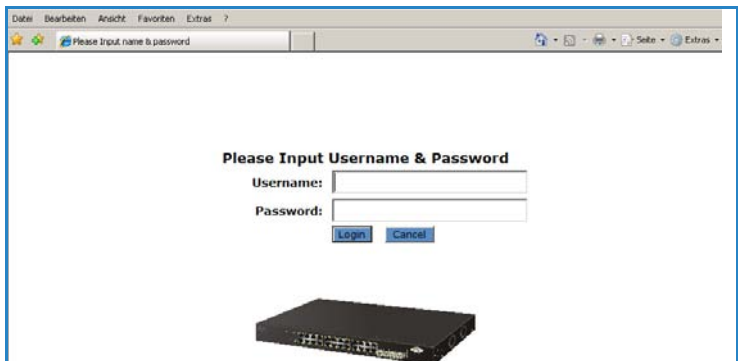
- Text-orientated configuration via a console (Command Line Interface – CLI): This method of configuration, which requires a program such as Telnet, Hyperterminal, or similar, can be conducted over a network connection or with a direct connection via serial interface (RS-232).

Instructions for configuring the device with CLI are available in the chapter "Command line interface".

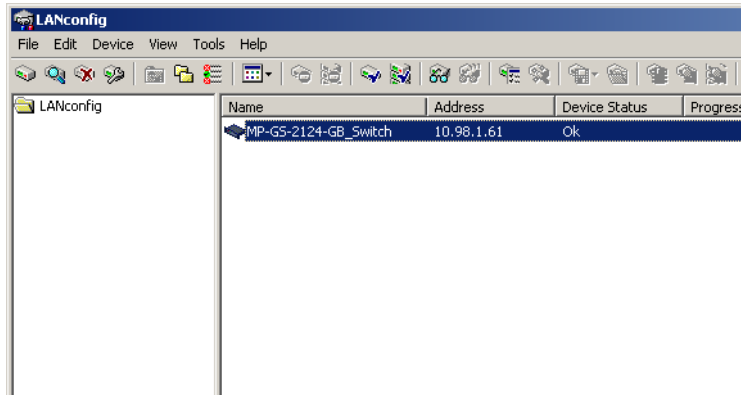
#### 3.1.1 Starting WEBconfig

There are two ways of starting the configuration by browser:

- If you know the device's IP address, simply enter this into the address line in the browser. The factory settings for accessing the device are: User name "admin", password "admin".



- If you do not have the device's IP number, LANconfig can be used to search for it. To start LANconfig click on **Start ▶ Programs ▶ LANCOM ▶ LANconfig**.



LANconfig automatically searches for all available devices in your network. Any available LANCOM devices will be displayed in the list, including the LANCOM Switch. Double-click on this entry to start the browser automatically with the correct IP address.

### What is the IP address of my LANCOM Switch?

The current IP address of the LANCOM Switch after being switched on depends on the network constellation.

**Networks with DHCP server** – In its factory settings, the LANCOM Switch is set for auto DHCP mode, meaning that it searches for a DHCP server to assign it an IP address, subnet mask and gateway address. The assigned IP address can only be determined by using the appropriate tools or via the DHCP server. If the DHCP server is a LANCOM device, the IP address of the LANCOM Switch can be read out from the DHCP table. If this is the case, the LANCOM Switch can be accessed from any network computer that receives its IP address from the same DHCP server.

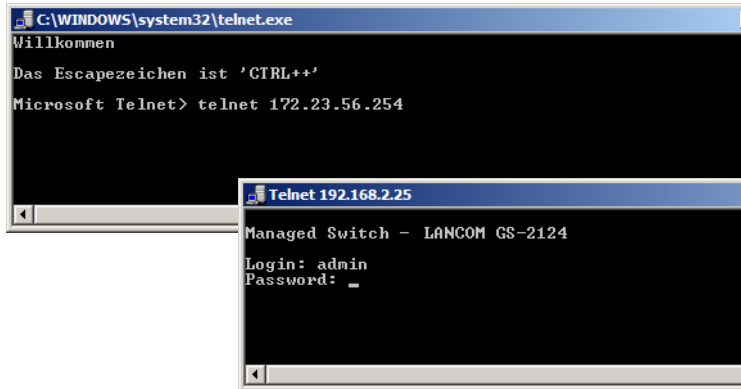
**Network without a DHCP server** – If no DHCP server is present in the network, the LANCOM Switch automatically adopts the address "172.23.56.250".

If this is the case, the LANCOM Switch can be accessed from any network computer with its IP address set to the address range "172.23.56.x".

### 3.1.2 Starting the Command Line Interface over the network

If you know the device's IP address (see section above) and the LANCOM Switch is accessible from your computer via the network, then you can use the command line interface via the network.

- 1 To do this, start a console such as Telnet and enter the device's IP address as the target.
- 2 Log on with user name and password (default: admin, admin).



### 3.1.3 Starting the Command Line Interface over the serial connection

If you do not know the IP address of the device, you can use the command line interface via a serial connection.

- 1 Use the serial configuration cable to connect the LANCOM Switch to the configuration computer (→ "Mounting and connecting up the LANCOM Switch').
- 2 Start a terminal program on the configuration computer, such as Hyperterminal under Windows. Use the following parameters for the connection:
  - Baud rate: 115200
  - Stop bits: 1
  - Data bits: 8
  - Parity: N
  - Flow control: None


- 3 Log on with user name and password (default: admin, admin).

## 3.2 Which configuration does the device use?

The switch supports four different configurations: The start configuration, the current working configuration, the user configuration and the default configuration.


- 1 Start configuration

At the system start, the device takes the parameters from the start configuration and copies these to the working configuration. On shipping, the start configuration is the same as the default configuration.

- 
-  To change the start configuration, the altered parameters have to be saved as the start configuration.


- 2 Working configuration:

This is the currently active configuration in the device. It can be changed at any time. All changes to the configuration are saved here. Each time you make changes and press <Apply>, the changes are stored to the working configuration.

- 
-  The changes to the working configuration are **not** automatically adopted for the start configuration. They have to be saved specifically as the start or user configuration. If you do not save the changes to your working configuration, they will be lost and the previous start configuration will be active when you start the system the next time.

- 3 User configuration:

This configuration exists for specific requirements or for making backups. You can save any state of the working configuration as a user configuration and restore this state later or with the function "Restore user configuration".

- 
-  If the start configuration is defective and the the device is not available via network, you use the serial configuration interface and the Command Line Interface to reload a functional start configuration.

- 4 Default configuration

This is the default configuration and it cannot be altered. The web user interface has the following options to restore the switch to its default setting.

- With the function "restore default configuration included default IP address" you can reset the switch to the factory default settings (including the administrator's password and the auto DHCP setting).
- With the function "restore default configuration without changing current IP address" you can reset the switch to the factory default settings, but without changing the IP address. You can access the switch at its last IP address.
- With the serial configuration interface you can reset the switch to the factory default setting, without knowing the current administrator's password. To do this you have to set up a serial connection to the device as described in → 'Start Command Line Interface via serial connection'. In the terminal program, before you enter the username press CTRL+Z, enter "RESET" as the username and the MAC address (without blank characters) as the password.



This action starts the reset process and all settings will be reset to the factory default state, including the administrator's password and the auto DHCP setting.

### 3.3 Save/Restore

The switch supports three copies of configuration, including the default configuration, working configuration and user configuration for your configuration management. All of them are listed and described below respectively.

#### ■ Default Configuration:

This is ex-factory setting and cannot be altered. In Web UI, two restore default functions are offered for the user to restore to the default setting of the switch. One is the function of "Restore Default Configuration including default IP address", the IP address will restore to default "192.168.1.1" as you use it. The other is the function of "Restore Default Configuration without changing current IP address", the IP address will keep the same one that you had saved before by performing this function.

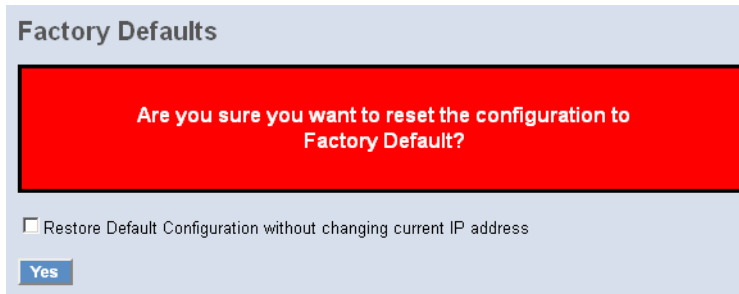
#### ■ Working Configuration:

It is the configuration you are using currently and can be changed any time. The configurations you are using are saved into this configuration file. This is updated each time as you press <Apply> button.

## ■ User Configuration:

It is the configuration file for the specified or backup purposes and can be updated while having confirmed the configuration. You can retrieve it by performing Restore User Configuration.

### 3.3.1 Factory Defaults

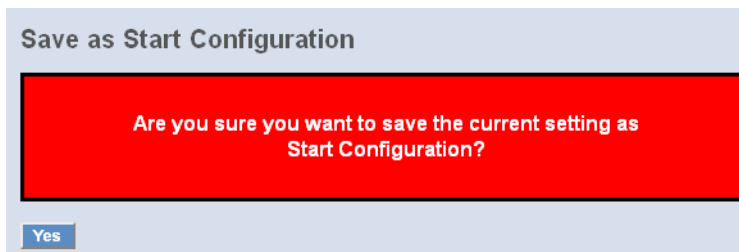


The screenshot shows a web interface titled "Factory Defaults". A large red box contains the text: "Are you sure you want to reset the configuration to Factory Default?". Below this box, there is a checkbox labeled "Restore Default Configuration without changing current IP address" which is currently unchecked. At the bottom left of the dialog, there is a blue button labeled "Yes".

## ■ Restore Default Configuration (includes default IP address)

Restore Default Configuration function can retrieve ex-factory setting to replace the start configuration. And the IP address of the switch will also be restored to 192.168.1.1.

### 3.3.2 Save Start



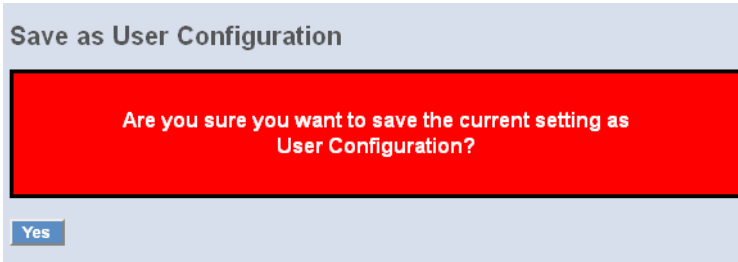
The screenshot shows a web interface titled "Save as Start Configuration". A large red box contains the text: "Are you sure you want to save the current setting as Start Configuration?". Below this box, there is a blue button labeled "Yes".

## ■ Save As Start Configuration

Save the current configuration as a start configuration file in flash memory.

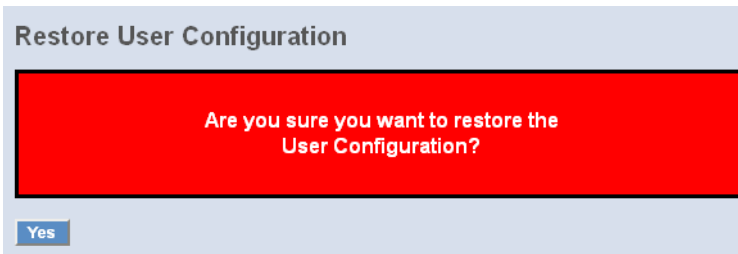


### 3.3.3 Save User



- Save As User Configuration  
Save the current configuration as a user configuration file in flash memory.

### 3.3.4 Restore User



- Restore User Configuration  
Restore User Configuration function can retrieve the previous confirmed working configuration stored in the flash memory to update start configuration. When completing to restore the configuration, the system's start configuration is updated and will be changed its system settings after rebooting the system.

## 3.4 Export/ Import Configuration File

The screenshot displays a configuration panel with three main sections:

- Export Configuration File:** Features a dropdown menu set to 'Current' and an 'Export' button.
- Import Start Configuration File:** Includes a text input field, a 'Durchsuchen...' (Browse) button, and an 'Import' button.
- Import User Configuration File:** Includes a text input field, a 'Durchsuchen...' (Browse) button, and an 'Import' button.

### ■ Config File

With this function, user can back up or reload the configuration files of Save As Start or Save As User via TFTP.

### ■ Parameter:

#### Export File Path:

Export Start: Export Save As Start's config file stored in the flash.

Export User-Conf: Export Save As User's config file stored in the flash.

#### Import File Path:

Import Start: Import Save As Start's config file stored in the flash.

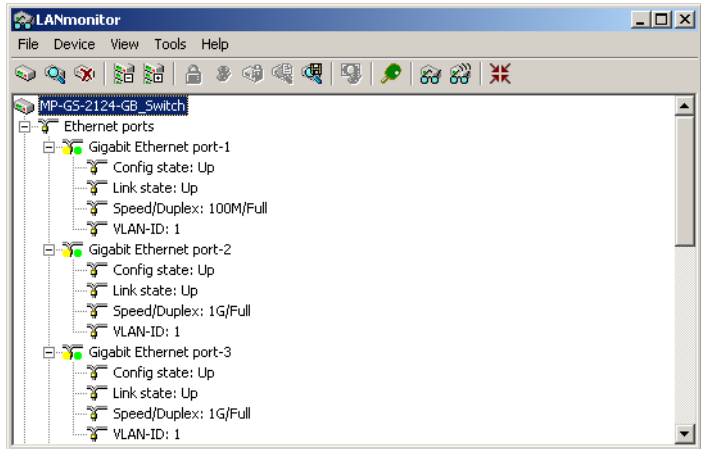
Import User-Conf: Import Save As User's config file stored in the flash.

## 3.5 Monitoring the LANCOM Switch with LANmonitor

The current state of the device and all ports can be monitored using the LEDs on the front panel. With LANmonitor the devices can be observed from any workstation without being able to see the LEDs. Besides the status information provided by the LEDs the LANmonitor provides further important information on the ports.

### 3.5.1 Ethernet port status

LANmonitor displays the current status of all of the device's Ethernet ports. This includes monitoring of the state as configured by the admin (config state) and the actual state (link state) of the port. Each port is displayed with two colored symbols in LANmonitor:



- The left icon shows the config state:
  - Gray: The port is deactivated in the configuration
  - Yellow: The port is activated in the configuration
- The right-hand icon shows the link state:
  - Gray: No active network device is connected to the port
  - Green: A network device is connected to the port and active

Apart from the status, LANmonitor displays the VLAN ID for each port and the detected data rate at active ports connected to active network devices.

## 4 Operation of Web-based Management

This chapter instructs you how to configure and manage the LANCOM GS-2124 through the web user interface it supports. With this facility, you can easily access and monitor through any one port of the switch all the status of the switch, including MIBs status, each port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, even illegal access record and so on.

The default values of the managed switch are listed in the table below:

LANCOM GS-2124	
IP Address	172.23.56.250
Subnet Mask	255.255.255.0
Default Gateway	172.23.56.254
Default DNS-Server	172.23.56.254
Username	admin
Password	admin

After the managed switch has been finished configuration in the CLI via the switch's serial interface, you can browse it. For instance, type `http://192.168.1.1` in the address row in a browser, it will show the following screen and ask you to input username and password in order to login and access. The default username and password are both "admin". For the first time to use, please enter the default username and password, then click the <Login> button. The login process now is completed.

In this login menu, you have to input the complete username and password respectively, the switch will not give you a shortcut to username automatically. This looks inconvenient, but safer.

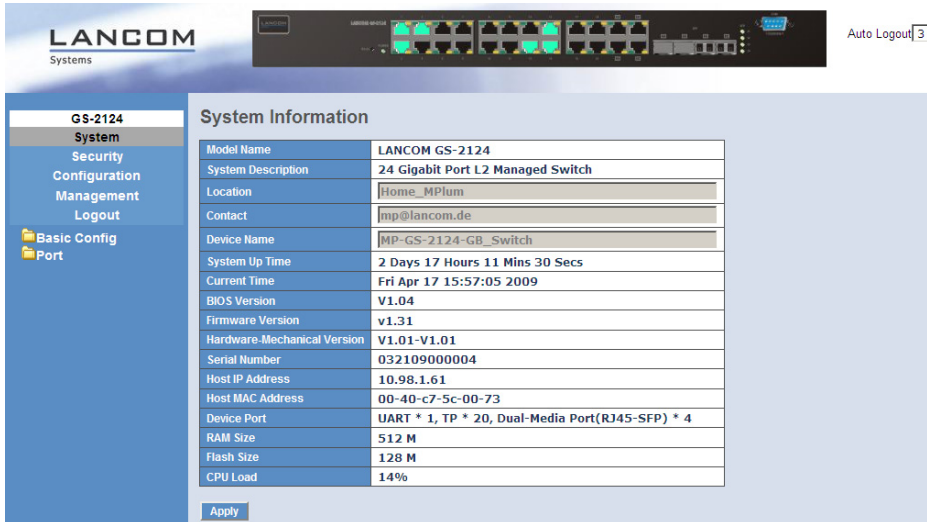
In the switch, it supports a simple user management function allowing only one administrator to configure the system at the same time. If there are two or more users using administrator's identity, the switch will allow the only one who logs in first to configure the system. The rest of users, even with administrator's identity, can only monitor the system. For those who have no administrator's identity, can only monitor the system. There are only a maximum of three users able to login simultaneously in the switch.

To optimize the display effect, we recommend you use Microsoft IE 6.0 above, Netscape V7.1 above or FireFox V1.00 above and have the resolution 1024x768. The switch supported neutral web browser interface.



## 4.1 Web Management Home Overview

After you login, the switch shows you the system information. This page is default and tells you the basic information of the system, including "Model Name", "System Description", "Location", "Contact", "Device Name", "System Up Time", "Current Time", "BIOS Version", "Firmware Version", "Hardware-Mechanical Version", "Serial Number", "Host IP Address", "Host MAC Address", "Device Port", "RAM Size" and "Flash Size". With this information, you will know the software version used, MAC address, serial number, how many ports good and so on. This is helpful while malfunctioning.



**GS-2124**  
System  
Security  
Configuration  
Management  
Logout  
Basic Config  
Port

Auto Logout 3

### System Information

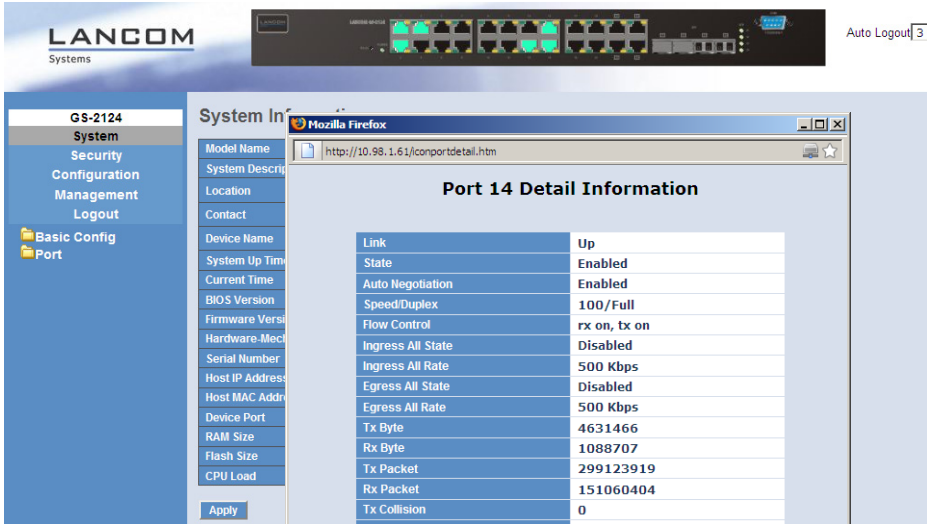
Model Name	LANCOM GS-2124
System Description	24 Gigabit Port L2 Managed Switch
Location	Home_MPLum
Contact	mp@lancom.de
Device Name	MP-GS-2124-GB_Switch
System Up Time	2 Days 17 Hours 11 Mins 30 Secs
Current Time	Fri Apr 17 15:57:05 2009
BIOS Version	V1.04
Firmware Version	v1.31
Hardware.Mechanical Version	V1.01-V1.01
Serial Number	032109000004
Host IP Address	10.98.1.61
Host MAC Address	00-40-c7-5c-00-73
Device Port	UART * 1, TP * 20, Dual-Media Port(RJ45-SFP) * 4
RAM Size	512 M
Flash Size	128 M
CPU Load	14%

Apply

## The Information of Page Layout

On the top side, it shows the front panel of the switch. In the front panel, the linked ports will display green; as to the ports, which are link off, they will be dark. For the optional modules, the slot will show only a cover plate if no module exists and will show a module if a module is present. The image of module depends on the one you inserted. The same, if disconnected, the port will show just dark, if linked, green.

In this device, there are clicking functions on the panel provided for the information of the ports. These are very convenient functions for browsing the information of a single port. When you click on the front panel of the port, an information window for the port will pop up.



The figure shows the basic information of the clicked port. With this, you'll see the information about the port status, traffic status and bandwidth rating for egress and ingress respectively.

On the right-top corner, there is a pull-down list for Auto Logout. For the sake of security, we provide auto-logout function to protect you from illegal user as you are leaving. If you do not choose any selection in Auto Logout list, it means you turn on the Auto Logout function and the system will be logged out automatically when no action on the device 3 minutes later. If OFF is chosen, the screen will keep as it is. Default is ON.

On the left side, the main menu tree for web is listed in the page. They are hierarchical menu. Open the function folder, a sub-menu will be shown. The functions of each folder are described in its corresponded section respectively. When clicking it, the function is performed.

## 4.2 System: Basic Config

### 4.2.1 System Information

System Information	
Model Name	LANCOM GS-2124
System Description	24 Gigabit Port L2 Managed Switch
Location	Home_MPlus
Contact	imp@lancom.de
Device Name	MP-GS-2124-GB_Switch
System Up Time	5 Days 22 Hours 6 Mins 34 Secs
Current Time	Thu Mar 26 13:21:57 2009
BIOS Version	V1.04
Firmware Version	v1.29
Hardware-Mechanical Version	V1.01-V1.01
Serial Number	032109000004
Host IP Address	10.98.1.61
Host MAC Address	00-40-c7-5c-00-73
Device Port	UART * 1, TP * 20, Dual-Media Port(RJ45-SFP) * 4
RAM Size	512 M
Flash Size	128 M
CPU Load	14%

Apply

- System Information:
  - Shows the basic system information.
- Parameter:
  - Model name:
    - The model name of this device.
  - System Description: As it is, this tells what this device is. Here, it is "L2 Plus Managed Switch" .
  - Location:
    - Basically, it is the location where this switch is put. User-defined.
  - Contact:
    - For easily managing and maintaining device, you may write down the contact person and phone here for getting help soon. You can configure this parameter through the device's user interface or SNMP.
  - Device name:
    - The name of the switch. User-defined. Default is LANCOM GS-2124.



- System up time:  
The time accumulated since this switch is powered up. Its format is day, hour, minute, second.
- Current time:  
Show the system time of the switch. Its format: day of week, month, day, hours : minutes : seconds, year. For instance, Tue Apr 20 23:25:58 2005.
- BIOS version:  
The version of the BIOS in this switch.
- Firmware version:  
The firmware version in this switch.
- Hardware-Mechanical version:  
The version of Hardware and Mechanical. The figure before the hyphen is the version of electronic hardware; the one after the hyphen is the version of mechanical.
- Serial number:  
The number is assigned by the manufacturer.
- Host IP address:  
The IP address of the switch.
- Host MAC address:  
It is the Ethernet MAC address of the management agent in this switch.
- Device Port:  
Show all types and numbers of the port in the switch.
- RAM size:  
The size of the DRAM in this switch.
- Flash size:  
The size of the flash memory in this switch.

## 4.3 Account

### Account Configuration

Account Name	Authorization
admin	Admin
guest	Guest

In this function, only administrator can create, modify or delete the username and password. Administrator can modify other guest identities' password without confirming the password but it is necessary to modify the administrator-equivalent identity. Guest-equivalent identity can modify his password only. Please note that you must confirm administrator/guest identity in the field of Authorization in advance before configuring the username and password. Only one administrator is allowed to exist and unable to be deleted. In addition, up to 4 guest accounts can be created.

- The default setting for user account is:

Username: admin

Password: admin

### 4.3.1 Time

### System Time Setting

Current Time	Thu Mar 26 13:24:35 2009			
<input checked="" type="radio"/> Manual	Year	2009 (2000~2036)	Month	3 (1~12)
	Day	26 (1~31)	Hour	13 (0~23)
	Minute	24 (0~59)	Second	35 (0~59)
<input type="radio"/> NTP	<input type="radio"/> 209.81.9.7(USA) <input type="radio"/> 137.189.8.174(HK) <input type="radio"/> 133.100.9.2(JP) <input type="radio"/> 131.188.3.222(Germany) <input checked="" type="radio"/> 10.98.1.33		Time Zone <input type="text" value="GMT+1:00"/>	
Daylight Saving	<input type="text" value="2"/>			
Daylight Saving Start	Mth	3	Day	28
	Hour	1		
Daylight Saving End	Mth	10	Day	28
	Hour	2		
<input type="button" value="Apply"/>				

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple and you just input "Year", "Month", "Day", "Hour", "Minute" and "Second" within the valid value range indicated in each item. If you input an invalid value, for example, 61 in minute, the switch will clamp the figure to 59.

NTP is a well-known protocol used to synchronize the clock of the switch system time over a network. NTP, an internet draft standard formalized in RFC 1305, has been adopted on the system is version 3 protocol. The switch provides four built-in NTP server IP addresses resided in the Internet and an user-defined NTP server IP address. The time zone is Greenwich-centered which uses the expression form of GMT+/- xx hours.

■ Time

Set the system time by manual input or set it by syncing from Time servers. The function also supports daylight saving for different area's time adjustment.

■ Parameter:

Current Time:

Shows the current time of the system.

Manual:

This is the function to adjust the time manually. Filling the valid figures in the fields of Year, Month, Day, Hour, Minute and Second respectively and press <Apply> button, time is adjusted. The valid figures for the parameter Year, Month, Day, Hour, Minute and Second are >=2000, 1-12, 1-31, 0-23, 0-59 and 0-59 respectively. Input the wrong figure and press <Apply> button, the device will reject the time adjustment request. There is no time zone setting in Manual mode.

Default: Year = 2000, Month = 1, Day = 1, Hour = 0, Minute = 0, Second = 0

NTP:

NTP is Network Time Protocol and is used to sync the network time based Greenwich Mean Time (GMT). If use the NTP mode and select a built-in NTP time server or manually specify an user-defined NTP server as well as Time Zone, the switch will sync the time in a short after pressing <Apply> button. Though it synchronizes the time automatically, NTP does not update the time periodically without user's processing.

Time Zone is an offset time off GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and updated NTP time to come out the local time, otherwise, you will not be able to get the correct time. The switch supports configurable time zone from -12 to +13 step 1 hour.

Default Time zone: +8 Hrs.

□ Daylight Saving:

Daylight saving is adopted in some countries. If set, it will adjust the time lag or in advance in unit of hours, according to the starting date and the ending date. For example, if you set the day light saving to be 1 hour. When the time passes over the starting time, the system time will be increased one hour after one minute at the time since it passed over. And when the time passes over the ending time, the system time will be decreased one hour after one minute at the time since it passed over.

The switch supports valid configurable day light saving time is -5 ~ +5 step one hour. The zero for this parameter means it need not have to adjust current time, equivalent to in-act daylight saving. You don't have to set the starting/ending date as well. If you set daylight saving to be non-zero, you have to set the starting/ending date as well; otherwise, the daylight saving function will not be activated.

Default for Daylight Saving: 0.

The following parameters are configurable for the function Daylight Saving and described in detail.

Day Light Saving Start :

This is used to set when to start performing the day light saving time.

Mth: Range is 1 ~ 12; Default: 1

Day: Range is 1 ~ 31; Default: 1

Hour: Range is 0 ~ 23; Default: 0

Day Light Saving End: This is used to set when to stop performing the daylight saving time.

Mth: Range is 1 ~ 12; Default: 1

Day: Range is 1 ~ 31; Default: 1

Hour: Range is 0 ~ 23; Default: 0

## 4.3.2 IP Configuration

### IP Configuration

DHCP Setting	<input checked="" type="checkbox"/> Enable
IP Address	<input type="text" value="10.98.1.61"/>
Current IP Address	<b>10.98.1.61</b>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="10.98.1.33"/>
Current Gateway	<b>10.98.1.33</b>
DNS Server	<input type="text" value="Auto"/> <input type="text" value="10.98.1.33"/>

IP configuration is one of the most important configurations in the switch. Without the proper setting, network manager will not be able to manage or view the device. The switch supports both manual IP address setting and automatic IP address setting via DHCP server. When IP address is changed, you must reboot the switch to have the setting taken effect and use the new IP to browse for web management and CLI management.

### ■ IP Configuration

Set IP address, subnet mask, default gateway and DNS for the switch.

### ■ Parameter:

#### DHCP Setting:

DHCP is the abbreviation of Dynamic Host Configuration Protocol. Here DHCP means a switch to turn ON or OFF the function.

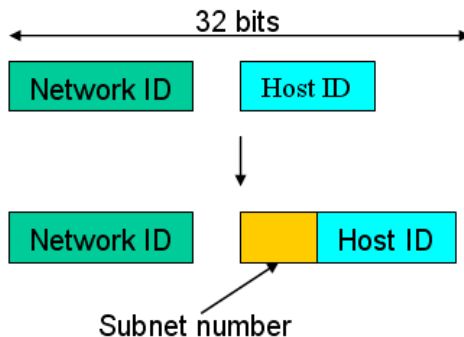
The switch supports DHCP client used to get an IP address automatically if you set this function "Enable". When enabled, the switch will issue the request to the DHCP server resided in the network to get an IP address. If DHCP server is down or does not exist, the switch will issue the request and show IP address is under requesting, until the DHCP server is up. Before getting an IP address from DHCP server, the device will not continue booting procedures. If set this field "Disable", you'll have to input IP address manually. For more details about IP address and DHCP, please see the Section 2-1-5 "IP Address Assignment" in this manual.

Default: Disable

- IP address:  
Users can configure the IP settings and fill in new values if users set the DHCP function "Disable". Then, click <Apply> button to update. When DHCP is disabled, Default: 192.168.1.1 If DHCP is enabled, this field is filled by DHCP server and will not allow user manually set it any more.

- Subnet mask:  
The subnet mask divides the IP address in two parts, one for the network and one for the device. The part of the network denotes the network of the computer. Only computer in the same network are able to communicate with each other. With devices of other networks can only be communicate through a router. The part of the device denotes the single device in a network. The address of the device within a network needs to be unambiguously.

For more information, please also see the Section "IP Address Assignment" in this manual. Default: 255.255.255.0



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

Default: 192.168.1.254

□ DNS:

It is Domain Name System used to serve the translation between IP address and name address.

The switch supports DNS client function to re-route the mnemonic name address to DNS server to get its associated IP address for accessing Internet. User can specify a DNS IP address for the switch. With this, the switch can translate a mnemonic name address into an IP address.

There are two ways to specify the IP address of DNS. One is fixed mode, which manually specifies its IP address, the other is dynamic mode, which is assigned by DHCP server while DHCP is enabled. DNS can help you easily remember the mnemonic address name with the meaningful words in it. Default is no assignment of DNS address.

Default: 0.0.0.0

### 4.3.3 Loop Detection

#### Loop Detection

##### Detection Port

Port No																							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
<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"/>

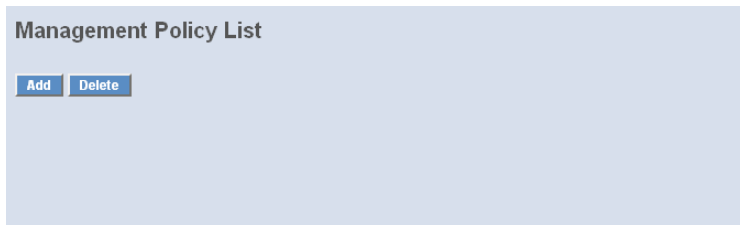
##### Locked Port

Port No																							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
<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"/>

The loop detection is used to detect the presence of traffic. When switch receives packet's(looping detection frame) MAC address the same as oneself from port, show Loop detection happens. The port will be locked when it received the looping detection frames. If you want to resume the locked port, please find out the looping path and take off the looping path, then select the resume the locked port and click on "Resume" to turn on the locked ports.

- Loop Detection
  - Display whether switch open Loop detection.
- Parameter:
  - Port No:
    - Display the port number. The number is 1 - 24.
  - Detection Port - Enable:
    - When Port No is chosen, and enable port' s Loop detection, the port can detect loop happens. When Port-No is chosen, enable port' s Loop detection, and the port detects loop happen, port will be Locked. If Loop did not happen, port maintains Unlocked.
  - Locked Port - Resume:
    - When Port No is chosen, enable port' s Loop detection, and the port detects loop happen, the port will be Locked. When choosing Resume, port locked will be opened and turned into unlocked. If not choosing Resume, Port maintains locked.

#### 4.3.4 Management Policy



Through the management security configuration, the manager can do the strict setup to control the switch and limit the user to access this switch.

The following rules are offered for the manager to manage the switch:

- 1 When no lists exists, then it will accept all connections.

Accept

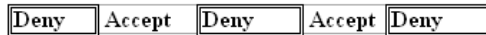
---

- 2 When only "accept lists" exist, then it will deny all connections, excluding the connection inside of the accepting range.

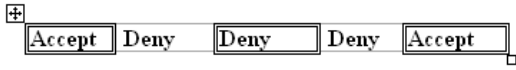




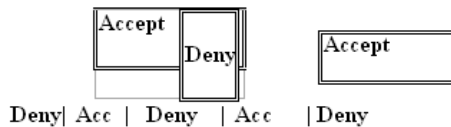
- 3 When only “deny lists” exist, then it will accept all connections, excluding the connection inside of the denying range.



- 4 When both “accept and deny” lists exist, then it will deny all connections, excluding the connection inside of the accepting range.



- 5 When both “accept and deny” lists exist, then it will deny all connections, excluding the connection inside of the accepting range and NOT inside of the denying range at the same time.



#### ■ Management Security Configuration

The switch offers Management Security Configuration function. With this function, the manager can easily control the mode that the user connects to the switch. According to the mode, users can be classified into two types: Those who are able to connect to the switch (Accept) and those who are unable to connect to the switch (Deny). Some restrictions also can

be placed on the mode that the user connect to the switch, for example, we can decide that which VLAN VID is able to be accepted or denied by the switch, the IP range of the user could be accepted or denied by the switch, the port that the user is allowed or not allowed to connect with the switch, or the way of controlling and connecting to the switch via Http, Telnet or SNMP.

### Management Security Configuration

Name	VID	IP Range
<input style="width: 100%; height: 100%;" type="text"/>	<input checked="" type="radio"/> Any <input type="radio"/> Custom <input style="width: 50px;" type="text"/>	<input checked="" type="radio"/> Any <input type="radio"/> Custom <input style="width: 100px;" type="text"/> -- <input style="width: 100px;" type="text"/>

Incoming Port	Access Type	Action
<input checked="" type="radio"/> Any <input type="radio"/> Custom 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. <input type="checkbox"/> 6. <input type="checkbox"/> 7. <input type="checkbox"/> 8. <input type="checkbox"/> 9. <input type="checkbox"/> 10. <input type="checkbox"/> 11. <input type="checkbox"/> 12. <input type="checkbox"/> 13. <input type="checkbox"/> 14. <input type="checkbox"/> 15. <input type="checkbox"/> 16. <input type="checkbox"/> 17. <input type="checkbox"/> 18. <input type="checkbox"/> 19. <input type="checkbox"/> 20. <input type="checkbox"/> 21. <input type="checkbox"/> 22. <input type="checkbox"/> 23. <input type="checkbox"/> 24. <input type="checkbox"/> 25. <input type="checkbox"/> 26. <input type="checkbox"/>	<input checked="" type="radio"/> Any <input type="radio"/> Custom <input type="checkbox"/> Http <input type="checkbox"/> Telnet <input type="checkbox"/> SNMP	<input type="radio"/> Deny <input checked="" type="radio"/> Accept

Edit/Create
Delete

■ Parameter:

- Name:  
A name is composed of any letter (A-Z, a-z) and digit (0-9) with maximal 8 characters.
- VID:  
The switch supports two kinds of options for managed valid VLAN VID, including "Any" and "Custom". Default is "Any". When you choose "Custom", you can fill in VID number. The valid VID range is 1~4094.
- IP Range:  
The switch supports two kinds of options for managed valid IP Range, including "Any" and "Custom". Default is "Any". In case that "Custom" had been chosen, you can assigned effective IP range. The valid range is 0.0.0.0~255.255.255.255.
- Incoming Port:  
The switch supports two kinds of options for managed valid Port Range, including "Any" and "Custom". Default is "Any". You can select

the ports that you would like them to be worked and restricted in the management security configuration if "Custom" had been chosen.

□ Access Type:

The switch supports two kinds of options for managed valid Access Type, including "Any" and "Custom". Default is "Any". "Http", "Telnet" and "SNMP" are three ways for the access and managing the switch in case that "Custom" had been chosen.

□ Action:

The switch supports two kinds of options for managed valid Action Type, including "Deny" and "Accept". Default is "Deny". When you choose "Deny" action, you will be restricted and refused to manage the switch due to the "Access Type" you choose. However, while you select "Accept" action, you will have the authority to manage the switch.

□ Edit/Create:

A new entry of Management Security Configuration can be created after the parameters as mentioned above had been setup and then press <Edit/Create> button. Of course, the existed entry also can be modified by pressing this button.

□ Delete:

Remove the existed entry of Management Security Configuration from the management security table.

### 4.3.5 System Log

The System Log provides information about system logs, including information when the device was booted, how the ports are operating, when users logged in, when sessions timed out, as well as other system information.

**System Log**

No	Time	Desc
1	Thu Mar 26 13:21:53 2009	Login [guest]
2	Thu Mar 26 13:04:00 2009	Login [guest]
3	Thu Mar 26 10:49:05 2009	Login [guest]
4	Thu Mar 26 10:43:52 2009	Login [guest]
5	Thu Mar 26 10:33:07 2009	Login [guest]
6	Thu Mar 26 10:29:28 2009	Login [guest]
7	Wed Mar 25 16:02:45 2009	Login [guest]
8	Wed Mar 25 15:57:59 2009	Login [guest]
9	Wed Mar 25 15:40:33 2009	Login [guest]
10	Wed Mar 25 15:06:22 2009	Login [guest]
11	Wed Mar 25 14:47:17 2009	Login [guest]
12	Wed Mar 25 14:34:55 2009	Login [guest]

### ■ System Log

The Trap Log Data is displaying the log items including all SNMP Private Trap events, SNMP Public traps and user logs occurred in the system. In the report table, No., Time and Events are three fields contained in each trap record.

### ■ Parameter:

- No:  
Display the order number that the trap happened.
- Time:  
Display the time that the trap happened.
- Desc:  
Displays a description event recorded in the System Log.
- Clear:  
Clear log data.

## 4.3.6 Virtual Stack

### ■ Virtual Stack

Virtual Stack Management(VSM) is the group management function. Through the proper configuration of this function, switches in the same LAN will be grouped automatically. And among these switch, one switch will be a master machine, and the others in this group will become the slave devices.

VSM offers a simple centralized management function. It is not necessary to remember the address of all devices, manager is capable of managing

the network with knowing the address of the Master machine. Instead of SNMP or Telnet UI, VSM is only available in Web UI. While one switch become the Master, two rows of buttons for group device will appear on the top of its Web UI. By pressing these buttons, user will be allowed to connect the Web UI of the devices of the group in the same window without the login of these device.

The most top-left button is only for Master device. The background color of the button you press will be changed to represent that the device is under your management.

Note: It will remove the grouping temporarily in case that you login the switch via the console.

The device of the group will be shown as station address ( the last number of IP Address) + device name on the button (e.g. 196\_LANCOM GS-2124), otherwise it will show " ---- " if no corresponding device exists.

Once the devices join the group successfully, then they are merely able to be managed via Master device, and user will fail to manage them via telnet/console/web individually.

Up to 16 devices can be grouped for VSM, however, only one Master is allowed to exist in each group. For Master redundancy, user may configure more than two devices as Master device, however, the Master device with the smaller MAC value will be the Master one. All of these 16 devices can become Master device and back up with each other .

### Virtual Stack Configuration

State	Disable ▾
Role	Slave ▾
Group ID	default

Apply

**Note: You should logout every time you have changed the state of Virtual Stack.**

- Parameter:
  - State:
    - It is used for the activation or de-activation of VSM. Default is Enable.

- Role:  
The role that the switch would like to play in virtual stack. Two types of roles, including master and slave are offered for option. Default is Master.
- Group ID:  
It is the group identifier (GID) which signs for VSM. Valid letters are A-Z, a-z, 0-9, " - " and " \_ " characters. The maximal length is 15 characters.

### 4.3.7 System: Port

This section contains the descriptions of the Port configuration, Port Status, Simple Counter and Detail Counter for port monitoring and management. Each of them will be described in detail orderly in the following section.

## 4.3.8 Configuration

Port Configuration						
Port	Media	Speed	Flow Control	Maximum Frame	Excessive Collision Mode	Description
1	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	Uplink zum LANCOM 1823
2	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	zum Server 10.98.1.43
3	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	Uplink GB PoE Switch > 10.98.1
4	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
5	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
6	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
7	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
8	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
9	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
10	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
11	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
12	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
13	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
14	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	dLAN Schlafzimmer 10.98.1.46
15	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	oAP310 10.98.1.38
16	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	dm600 10.98.1.47
17	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
18	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
19	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
20	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
21	TP	Auto	<input checked="" type="checkbox"/>	9600	Discard	
22	SFP	Auto				
23	SFP	Auto				
24	SFP	Auto				

**Apply**

Port Configuration is applied to change the setting of each port. In this configuration function, you can set/reset the following functions.

- Port Configuration

It is used to set each port's operation mode. The switch supports 3 parameters for each port. They are State, Speed/Duplex and Flow Control.

- Parameter

- Speed/Duplex:

Set the speed and duplex of the port. In speed, 10, 100 and 1000 MBit/s baud rate is available for Ethernet at the ports 1-24. If the media at the SFP-ports 21, 22, 23 and/or 24 is 1Gbps fiber, it is always 1000Mbps and the duplex is full only. If the media is TP, the Speed/Duplex is comprised of the combination of speed mode, 10/

100/1000Mbps, and duplex mode, full duplex and half duplex. The following table summarized the function the media supports.

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

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

□ Flow Control:

There are two modes to choose in flow control, including Symmetric and Asymmetric. If flow control is set Symmetric, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. When it is set Asymmetric, this will let the receiving port care the PAUSE frame from transmitting device(s), but it doesn't send PAUSE frame. This is one-way flow control.

Default: Symmetric.

□ Maximum Frame:

This module offer 1518~9600 (Bytes) length to make the long packet.

□ Excessive Collision Mode:

There are two modes to choose when excessive collision happen in half-duplex condition as below:

**Discard:** The "Discard" mode determines whether the MAC drop frames after an excessive collision has occurred. If set, a frame is dropped after excessive collisions. This is IEEE Std 802.3 half-duplex flow control operation.

**Restart:** The "Restart" mode determines whether the MAC retransmits frames after an excessive collision has occurred. If set, a frame is not dropped after excessive collisions, but the backoff sequence is restarted. This is a violation of IEEE Std 802.3, but is useful in non-dropping half-duplex flow control operation.



### 4.3.9 Port Status

#### Port Status

Port	Link	Speed	Flow Control		Description	Media
			Rx	Tx		
1	up	100fdx	√	√	Uplink zum LANCOM 1823	TP
2	up	1Gfdx	√	√	zum Server 10.98.1.43	TP
3	up	1Gfdx	X	X	Uplink GB PoE Switch > 10.98.1.62	TP
4	down	down	X	X		TP
5	down	down	X	X		TP
6	down	down	X	X		TP
7	down	down	X	X		TP
8	down	down	X	X		TP
9	down	down	X	X		TP
10	down	down	X	X		TP
11	down	down	X	X		TP
12	down	down	X	X		TP
13	down	down	X	X		TP
14	up	100fdx	√	√	dLAN Schlafzimmer 10.98.1.46	TP
15	up	100fdx	√	√	OAP310 10.98.1.38	TP
16	up	100fdx	X	X	dm600 10.98.1.47	TP
17	down	down	X	X		TP
18	down	down	X	X		TP
19	down	down	X	X		TP
20	down	down	X	X		TP
21	down	down	X	X		TP
22	down	down	X	X		TP
23	down	down	X	X		TP
24	down	down	X	X		TP

The function Port Status gathers the information of all ports' current status and reports it by the order of port number, media, link status, port state, Auto-Negotiation status, speed/duplex, Rx Pause and Tx Pause. An extra media type information for the module ports 21, 22, 23 and 24 is also offered.

#### ■ Port Status

Report the latest updated status of all ports in this switch. When any one of the ports in the switch changes its parameter displayed in the page, it will be automatically refreshed the port current status about every 5 seconds.

#### ■ Parameter:

##### Port No:

Display the port number. The number is 1 – 24.

##### Media:

Show the media type adopted in all ports. The Ports 21, 22, 23 and 24 are optional modules, which support either fiber or UTP media with either Gigabit Ethernet (1000Mbps) or 10/100Mbps Fast Ethernet port. They may have different media types and speed. Especially,

fiber port has comprehensive types of connector, distance, fiber mode and so on. The switch describes the module ports with the following page.

□ Link:

Show that if the link on the port is active or not. If the link is connected to a working-well device, the Link will show the link "Up"; otherwise, it will show "Down". This is determined by the hardware on both devices of the connection.

No default value.

□ State:

Show that the communication function of the port is "Enabled" or "Disabled". When it is enabled, traffic can be transmitted and received via this port. When it is disabled, no traffic can be transferred through this port. Port State is configured by user.

Default: Enabled.

□ Auto Nego.:

Show the exchange mode of Ethernet MAC. There are two modes supported in the switch. They are auto-negotiation mode "Enabled" and forced mode "Disabled". When in "Enabled" mode, this function will automatically negotiate by hardware itself and exchange each other the capability of speed and duplex mode with other site which is linked, and comes out the best communication way. When in "Disabled" mode, both parties must have the same setting of speed and duplex, otherwise, both of them will not be linked. In this case, the link result is "Down".

Default: Enabled

□ Speed / Duplex:

Display the speed and duplex of all port. There are three speeds 10Mbps, 100Mbps and 1000Mbps supported for TP media, and the duplex supported is half duplex and full duplex. If the media is 1Gbps fiber, it is 1000Mbps supported only. The status of speed/duplex mode is determined by 1) the negotiation of both local port and link partner in "Auto Speed" mode or 2) user setting in "Force" mode. The local port has to be preset its capability.

Default: None, depends on the result of the negotiation.

- Rx Pause:  
The way that the port adopts to process the PAUSE frame. If it shows "on", the port will care the PAUSE frame; otherwise, the port will ignore the PAUSE frame.

Default: None

- Tx Pause:  
It decides that whether the port transmits the PAUSE frame or not. If it shows "on", the port will send PAUSE frame; otherwise, the port will not send the PAUSE frame.

Default: None.

- Parameter of SFP ports:

- Connector Type:  
Display the connector type, for instance, UTP, SC, ST, LC and so on.
- Fiber Type:  
Display the fiber mode, for instance, Multi-Mode, Single-Mode.
- Tx Central Wavelength:  
Display the fiber optical transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm and so on.
- Baud Rate:  
Display the maximum baud rate of the fiber module supported, for instance, 10M, 100M, 1G and so on.
- Vendor OUI:  
Display the Manufacturer's OUI code which is assigned by IEEE.
- Vendor Name:  
Display the company name of the module manufacturer.
- Vendor P/N:  
Display the product name of the naming by module manufacturer.
- Vendor Rev (Revision):  
Display the module revision.
- Vendor SN (Serial Number):  
Show the serial number assigned by the manufacturer.
- Date Code:  
Show the date this module was made.

- Temperature:  
Show the current temperature of module.
- Vcc:  
Show the working DC voltage of module.
- Mon1(Bias) mA:  
Show the Bias current of module.
- Mon2(TX PWR):  
Show the transmit power of module.
- Mon3(RX PWR):  
Show the receiver power of module.

### 4.3.10 Simple Counter

Port Statistics Overview										Auto-refresh <input type="checkbox"/>	Refresh	Clear
#	Packets		Bytes		Errors		Drops					
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit				
1	16267179	12099616	15155825112	2931467884	246	0	246	0				
2	5104210	7415085	2260606921	7864373317	0	0	0	0				
3	477554	1551601	69489750	905182762	0	0	0	0				
4	0	0	0	0	0	0	0	0				
5	0	0	0	0	0	0	0	0				
6	0	0	0	0	0	0	0	0				
7	0	0	0	0	0	0	0	0				
8	0	0	0	0	0	0	0	0				
9	0	0	0	0	0	0	0	0				
10	0	0	0	0	0	0	0	0				
11	3713014	5420036	1083072850	6486441238	0	0	0	4				
12	0	0	0	0	0	0	0	0				
13	0	0	0	0	0	0	0	0				
14	8087339	2746758	1031732803	350401436	0	0	0	0				
15	1601531	2843855	461282165	1437049234	1	0	1	0				
16	1580029	2708987	130597568	314423594	0	0	0	0				
17	0	0	0	0	0	0	0	0				
18	0	0	0	0	0	0	0	0				
19	0	0	0	0	0	0	0	0				
20	0	0	0	0	0	0	0	0				
21	0	0	0	0	0	0	0	0				
22	0	0	0	0	0	0	0	0				
23	0	0	0	0	0	0	0	0				
24	0	0	0	0	0	0	0	0				

The function of Simple Counter collects any information and provides the counting about the traffic of the port, no matter the packet is good or bad.

In the following figure, the window can show all ports' counter information at the same time. Each data field has 20-digit long. If the counting is overflowing, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The valid range is 3 to 10 seconds. The

Refresh Interval is used to set the update frequency. Default update time is 3 seconds.

- Function name: Simple Counter
- Function Description: Display the summary counting of each port's traffic, including Tx Byte, Rx Byte, Tx Packet, Rx Packet, Tx Collision and Rx Error Packet.
- Parameters Description:
  - Tx Byte: Total transmitted bytes.
  - Rx Byte: Total received bytes.
  - Tx Packet: The counting number of the packet transmitted.
  - Rx Packet: The counting number of the packet received.
  - Tx Collision: Number of collisions transmitting frames experienced.
  - Rx Error Packet: Number of bad packets received.

### 4.3.11 Detail Counter

Detailed Port Statistics Port 1			
		Port 1 ▾	Auto-refresh <input type="checkbox"/>
		<input type="button" value="Refresh"/>	<input type="button" value="Clear"/>
Receive Total		Transmit Total	
Rx Packets	16267917	Tx Packets	1209967
Rx Octets	15155694011	Tx Octets	2931533716
Rx Unicast	15213715	Tx Unicast	12000603
Rx Multicast	103694	Tx Multicast	60367
Rx Broadcast	950062	Tx Broadcast	38777
Rx Pause	0	Tx Pause	60077
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	1060608	Tx 64 Bytes	5793400
Rx 65-127 Bytes	3084194	Tx 65-127 Bytes	4229839
Rx 128-255 Bytes	1634836	Tx 128-255 Bytes	256611
Rx 256-511 Bytes	242656	Tx 256-511 Bytes	111882
Rx 512-1023 Bytes	372356	Tx 512-1023 Bytes	298771
Rx 1024-1526 Bytes	9873262	Tx 1024-1526 Bytes	1409464
Rx 1527- Bytes	5	Tx 1527- Bytes	0
Receive Error Counters		Transmit Error Counters	
Rx Drops	246	Tx Drops	0
Rx CRC/Alignment	246	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		

The function of Detail Counter collects any information and provides the counting about the traffic of the port, no matter the packet is good or bad.

In the following figure the window can show only one port counter information at the same time. To see another port's counter, you have to pull down the list of Select, then you will see the figures displayed about the port you had chosen.

Each data field has 20-digit long. If the counting is overflow, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The valid range is 3 to 10 seconds. The Refresh Interval is used to set the update frequency. Default update time is 3 seconds.

■ Detail Counter

Display the detailed counting number of each port's traffic. The window can show all counter information of each port at one time.

■ Parameter:

- Rx Packets:  
The counting number of the packet received.
- Rx Octets:  
Total received bytes.
- Rx Errors:  
Number of bad packets received.
- Rx Unicast Packets:  
Show the counting number of the received unicast packet.
- Rx Broadcast Packets:  
Show the counting number of the received broadcast packet.
- Rx Multicast Packets:  
Show the counting number of the received multicast packet.
- Rx Pause Packets:  
Show the counting number of the received pause packet.
- Tx Collisions:  
Number of collisions transmitting frames experienced.
- Tx Single Collision:  
Number of frames transmitted that experienced exactly one collision.
- Tx Multiple Collision:  
Number of frames transmitted that experienced more than one collision.
- Tx Drop Packets:  
Number of frames dropped due to excessive collision, late collision, or frame aging.

- Tx Deferred Transmit:  
Number of frames delayed to transmission due to the medium is busy.
- Tx Late Collision:  
Number of times that a collision is detected later than 512 bit-times into the transmission of a frame.
- Tx Excessive Collision:  
Number of frames that are not transmitted because the frame experienced 16 transmission attempts.
- Packets 64 Octets:  
Number of 64-byte frames in good and bad packets received.
- Packets 65-127 Octets:  
Number of 65 ~ 127-byte frames in good and bad packets received.
- Packets 128-255 Octets:  
Number of 128 ~ 255-byte frames in good and bad packets received.
- Packets 256-511 Octets:  
Number of 256 ~ 511-byte frames in good and bad packets received.
- Packets 512-1023 Octets:  
Number of 512 ~ 1023-byte frames in good and bad packets received.
- Packets 1024- 1522 Octets:  
Number of 1024-1522-byte frames in good and bad packets received.
- Tx Packets:  
The counting number of the packet transmitted.
- TX Octets:  
Total transmitted bytes.
- Tx Unicast Packets:  
Show the counting number of the transmitted unicast packet.
- Tx Broadcast Packets:  
Show the counting number of the transmitted broadcast packet.
- Tx Multicast Packets:  
Show the counting number of the transmitted multicast packet.
- Tx Pause Packets:  
Show the counting number of the transmitted pause packet.

- Rx FCS Errors:  
Number of bad FSC packets received.
- Rx Alignment Errors:  
Number of Alignment errors packets received.
- Rx Fragments:  
Number of short frames (< 64 bytes) with invalid CRC.
- Rx Jabbers:  
Number of long frames(according to max\_length register) with invalid CRC.
- Rx Drop Packets:  
Frames dropped due to the lack of receiving buffer.
- Rx Undersize Packets:  
Number of short frames (<64 Bytes) with valid CRC.
- Rx Oversize Packets:  
Number of long frames(according to max\_length register) with valid CRC.

## 4.4 Security: MAC

MAC Table Configuration gathers many functions, including MAC Table Information, MAC Table Maintenance, Static Forward, Static Filter and MAC Alias, which cannot be categorized to some function type. They are described below.

### 4.4.1 Mac Address Table

#### MAC Address Table Configuration

**Aging Configuration**

<b>Age time</b>	300	seconds.
<b>Disable automatic aging</b>	<input type="checkbox"/>	

**MAC Table Learning**

	Port Members																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
<b>Auto</b>	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒
<b>Disable</b>	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒
<b>Secure</b>	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒



## ■ MAC Address Table Information

This function can allow the user to set up the processing mechanism of MAC Table. An idle MAC address exceeding MAC Address Age-out Time will be removed from the MAC Table. The range of Age-out Time is 10-1000000 seconds, and the setup of this time will have no effect on static MAC addresses.

In addition, the learning limit of MAC maintenance is able to limit the amount of MAC that each port can learn.

## ■ Parameter:

## □ Aging Time:

Delete a MAC address idling for a period of time from the MAC Table, which will not affect static MAC address. Range of MAC Address Aging Time is 10-1000000 seconds. The default Aging Time is 300 seconds.

## □ Disable automatic aging:

Stop the MAC table aging timer, the learned MAC address will not age out automatically

## □ Auto:

Enable this port MAC address dynamic learning mechanism.

## □ Disable:

Disable this port MAC address dynamic learning mechanism, only support static MAC address setting.

## □ Secure:

Disable this port MAC address dynamic learning mechanism and copy the dynamic learning packets to CPU

## □ Save:

Save MAC Address Table configuration

## □ Reset:

Reset MAC Address Table configuration

## 4.4.2 Static Filter

Static Filter

MAC						VID	Alias			
00	-	40	-	C7	-	D6	-	00	-	02

Apply

No	MAC	VID	Alias
----	-----	-----	-------

Delete

### ■ Static Filter

Static Filter is a function that denies the packet forwarding if the packet's MAC Address is listed in the filtering Static Filter table. User can very easily maintain the table by filling in MAC Address, VID (VLAN ID) and Alias fields individually. User also can delete the existed entry by clicking <Delete> button.

### ■ Parameter:

- MAC:  
It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example,  
00 - 40 - C7 - D6 - 00 - 02
- VID:  
VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.
- Alias:  
MAC alias name you assign.

### 4.4.3 Static Forward

Static Forward

MAC	Port No	VID	Alias
- - - - -			

Apply

No	MAC	Port	VID	Alias

Delete

#### ■ Static Forward

Static Forward is a function that allows the user in the static forward table to access a specified port of the switch. Static Forward table associated with a specified port of a switch is set up by manually inputting MAC address and its alias name.

When a MAC address is assigned to a specific port, all of the switch's traffic sent to this MAC address will be forwarded to this port.

For adding a MAC address entry in the allowed table, you just need to fill in four parameters: MAC address, associated port, VID and Alias. Just select the existed MAC address entry you want and click <Delete> button, you also can remove it.

#### ■ Parameter:

- MAC:  
It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example,  
00 - 40 - C7 - D6 - 00 - 01
- Port No:  
Port number of the switch. It is 1 ~24.
- VID:  
VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.

- Alias:  
MAC alias name you assign.

#### 4.4.4 MAC Alias

MAC Alias	
MAC	Alias
00 - 00 - 00 - 00 - 00 - 00	

Apply

No	MAC	Alias
----	-----	-------

Delete

- MAC Alias
 

MAC Alias function is used to let you assign MAC address a plain English name. This will help you tell which MAC address belongs to which user in the illegal access report. At the initial time, it shows all pairs of the existed alias name and MAC address.

There are three MAC alias functions in this function folder, including MAC Alias Add, MAC Alias Edit and MAC Alias Delete. You can click <Create/Edit> button to add/modify a new or an existed alias name for a specified MAC address, or mark an existed entry to delete it. Alias name must be composed of A-Z, a-z and 0-9 only and has a maximal length of 15 characters.
- Parameter:
  - MAC Address:
 

It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example,

00 - 40 - C7 - D6 - 00 - 01

- Alias:  
MAC alias name you assign.

Note: If there are too many MAC addresses learned in the table, we recommend you inputting the MAC address and alias name directly.

#### 4.4.5 MAC Table

**MAC Table Information**

Port	<input checked="" type="checkbox"/> 01 <input checked="" type="checkbox"/> 02 <input checked="" type="checkbox"/> 03 <input checked="" type="checkbox"/> 04 <input checked="" type="checkbox"/> 05 <input checked="" type="checkbox"/> 06 <input checked="" type="checkbox"/> 07 <input checked="" type="checkbox"/> 08 <input checked="" type="checkbox"/> 09 <input checked="" type="checkbox"/> 10 <input checked="" type="checkbox"/> 11 <input checked="" type="checkbox"/> 12 <input checked="" type="checkbox"/> 13 <input checked="" type="checkbox"/> 14 <input checked="" type="checkbox"/> 15 <input checked="" type="checkbox"/> 16 <input checked="" type="checkbox"/> 17 <input checked="" type="checkbox"/> 18 <input checked="" type="checkbox"/> 19 <input checked="" type="checkbox"/> 20 <input checked="" type="checkbox"/> 21 <input checked="" type="checkbox"/> 22 <input checked="" type="checkbox"/> 23 <input checked="" type="checkbox"/> 24
	<input checked="" type="checkbox"/> Select/Unselect All
Search	MAC: ?? - ?? - ?? - ?? - ?? - ?? VID: ?

Alias	MAC Address	Port	VID

- Dynamic MAC Table  
Display the static or dynamic learning MAC entry and the state for the selected port.
- Parameter:
  - Type:  
Dynamic or Static.
  - VLAN:  
VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.
  - MAC address:  
Display the MAC address of one entry you selected from the searched MAC entries table.
  - Port:  
The port that exists in the searched MAC Entry.
  - Refresh:  
Refresh function can help you to see current MAC Table status.
  - Clear:  
To clear the selected entry.

- Previous Page:  
Move to the previous page.
- Next Page:  
Move to the next page.

## 4.5 Security: VLAN

The switch supports Tag-based VLAN (802.1q) and Port-based VLAN. Support 256 active VLANs and VLAN ID 1~4094. VLAN configuration is used to partition your LAN into small ones as your demand. Properly configuring it, you can gain not only improving security and increasing performance but greatly reducing VLAN management.

### 4.5.1 VLAN Mode



The screenshot shows a web-based configuration interface for VLAN Mode. At the top, the title 'VLAN Mode' is displayed. Below the title, there is a dropdown menu labeled 'VLAN Mode' with 'Tag-based' selected. Below the dropdown menu, there is an 'Apply' button.

#### ■ VLAN Mode Setting

The VLAN Mode Selection function includes five modes: Port-based, Tag-based, Metro Mode, Double-tag and Disable, you can choose one of them by pulling down list and selecting an item. Then, click <Apply> button, the settings will take effect immediately.

#### ■ Parameter:

- VLAN Mode:

Port-based:

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

name. This switch can support up to maximal 24 port-based VLAN groups.

Tag-based:

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

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

## 4.5.2 Tag-based Group

**Tag-Based VLAN Memberships Configuration**

IGMP-A: IGMP Aware    P-VLAN: Private VLAN    GVRP-P: GVRP Propagation

VLAN Name					Port Members																
Del	VID	IGMP-A	P-VLAN	GVRP-P	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
				Default																	
	1	Disable	Disable	Disable	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

### ■ Tag-based Group Configuration

It shows the information of existed Tag-based VLAN Groups, You can also easily create, edit and delete a Tag-based VLAN group by pressing <Add>, <Edit> and <Delete> function buttons. User can add a new VLAN group by inputting a new VLAN name and VLAN ID.

### ■ Parameter:

#### VLAN Name:

The name defined by administrator is associated with a VLAN group. Valid letters are A-Z, a-z, 0-9, " - " and " \_ " characters. The maximal length is 15 characters.

#### VLAN ID:

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

- IGMP Proxy:  
IGMP proxy enables the switch to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts. This switch can be set IGMP function "Enable" or "Disable" by VLAN group. If the VLAN group IGMP proxy is disabled, the switch will stop the exchange of IGMP messages in the VLAN group members. If the VLAN group IGMP proxy is enabled, the switch will support the exchange of IGMP messages in the VLAN group members and follow up IGMP proxy router port configuration, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP. You enable IGMP on the interfaces that connect the system to its hosts that are farther away from the root of the tree. These interfaces are known as downstream interfaces. Please refer to 3-15-1 for detail IGMP Proxy function description.
- Member Port:  
This is used to enable or disable if a port is a member of the new added VLAN, "Enable" means it is a member of the VLAN. Just tick the check box ( ) beside the port x to enable it.
- Add new VLAN:  
Please click on <Add new VLAN> to create a new Tag-based VLAN. Input the VLAN name as well as VID, configure the SYM-VLAN function and choose the member by ticking the check box beside the port No., then, press the <Apply> button to have the setting taken effect.
- Delete Group:  
Just press the <Delete> button to remove the selected group entry from the Tag-based group table.

Note: If you need to use PVLAN ( Private VLAN) have a look at the section "Port Isolation"



### 4.5.3 Port-based Group

VLAN Name		Port Members																			
Delete	Group	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	Default	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	1																				

#### ■ Port-based Group Configuration

Function Description: It shows the information of the existed Port-based VLAN Groups. You can easily create, edit and delete a Port-based VLAN group by pressing <Add>, <Edit> and <Delete> function buttons. User can add a new VLAN group by inputting a new VLAN name.

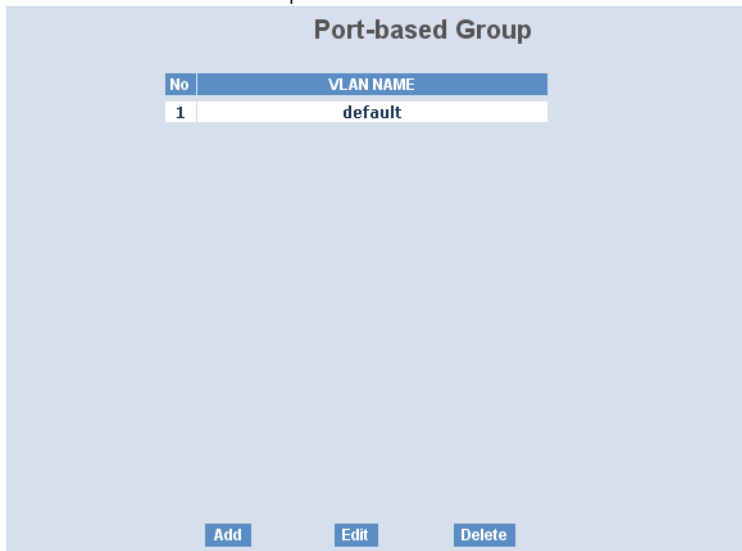
#### ■ Parameter:

##### VLAN Name:

The name defined by administrator is associated with a VLAN group. Valid letters are A-Z, a-z, 0-9, " - " and " \_ " characters. The maximal length is 15 characters.

Member Port:

This is used to enable or disable if a port is a member of the new added VLAN, "Enable" means it is a member of the VLAN. Just tick the check box beside the port x to enable it.



**Port-based Group**

No	VLAN NAME
1	default

 Add a new VLAN:

Create a new Port-based VLAN. Input the VLAN name and choose the member by ticking the check box beside the port No., then, press the <Apply> button to have the setting taken effect.

**Chapter 4: Operation of Web- based Management** Delete Group:

Just press the <Delete> button to remove the selected group entry from the Port-based group table.



**Port-based Group**

No	VLAN NAME
1	default
2	VLAN-2

Add Edit Delete

## 4.5.4 Ports

**VLAN Port Configuration**

Tag Identifier: 0x8100

Port #	VLAN Aware	Ingress Filtering	Frame Type	PVID	Role	Untag VID	Double Tag
1	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
2	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
3	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
4	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
5	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
6	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
7	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
8	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
9	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
10	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
11	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
12	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
13	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
14	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
15	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
16	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
17	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
18	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
19	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
20	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
21	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
22	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
23	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable
24	<input type="checkbox"/>	<input type="checkbox"/>	All	1	Access	0	Disable

Apply

### ■ VLAN Port Configuration

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

### ■ Parameter:

- Port 1-24:  
Port number.
- VLAN Aware:  
Based on IEEE 802.1Q VLAN tag to forward packet

- Ingress Filtering:  
Discard other VLAN group packets, only forward this port joined VLAN group packets
- Frame Type:  
All: Forward all tagged and untagged packets  
Tagged: Forward tagged packets only and discard untagged packets
- PVID:  
This PVID range will be 1-4094. Before you set a number x as PVID, you have to create a Tag-based VLAN with VID x. For example, if port x receives an untagged packet, the switch will apply the PVID (assume as VID y) of port x to tag this packet, the packet then will be forwarded as the tagged packet with VID y.
- Role:  
This is an egress rule of the port. Here you can choose Access, Trunk or Hybrid. Trunk means the outgoing packets must carry VLAN tag header. Access means the outgoing packets carry no VLAN tag header. If packets have double VLAN tags, one will be dropped and the other will still be left. As to Hybrid, it is similar to Trunk, and both of them will tag-out. When the port is set to Hybrid, its packets will be untagged out if the VID of the outgoing packets with tag is the same as the one in the field of Untag VID of this port.
- Untag VID:  
Valid range is 1~4094. It works only when Role is set to Hybrid.

## 4.5.5 Port Isolation

**Port Isolation Configuration**

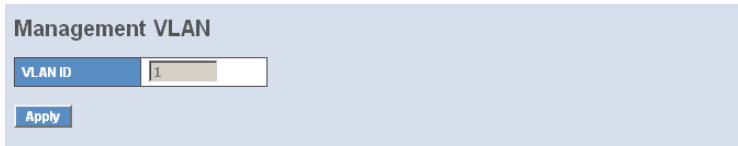
Port Number																							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input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

If you need to use PVLAN ( Private VLAN) function on Switch you need to do the following:

- ① Create a VLAN as primary VLAN and the VLAN ID is 2 and evoke the Private VLAN to enable Private VLAN service.

- 2 Assign port member to the VLAN2
- 3 You need to assign these ports for member of port isolation.
- 4 Press the "Save" to complete the PVLAN configuration process.

#### 4.5.6 Management VLAN



Management VLAN

VLAN ID 1

Apply

- Management VLAN  
To assign a specific VLAN for management purpose.
- Parameter:
  - VID:  
Specific Management VLAN ID.

### 4.6 Security: ACL

The LANCOM GS-2124 switch access control list (ACL) is probably the most commonly used object in the IOS. It is used for packet filtering but also for selecting types of traffic to be analyzed, forwarded, or influenced in some way. The ACLs are divided into EtherTypes. IPv4, ARP protocol, MAC and VLAN parameters etc. Here we will just go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port, the policy number is 1-8, however, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

## 4.6.1 Ports

### ACL Ports Configuration

Port #	Policy ID	Action	Rate Limiter ID	Port Copy	Counter
1	1	Permit	Disabled	Disabled	16154955
2	1	Permit	Disabled	Disabled	5086192
3	1	Permit	Disabled	Disabled	472983
4	1	Permit	Disabled	Disabled	0
5	1	Permit	Disabled	Disabled	0
6	1	Permit	Disabled	Disabled	0
7	1	Permit	Disabled	Disabled	0
8	1	Permit	Disabled	Disabled	0
9	1	Permit	Disabled	Disabled	0
10	1	Permit	Disabled	Disabled	0
11	1	Permit	Disabled	Disabled	3699263
12	1	Permit	Disabled	Disabled	0
13	1	Permit	Disabled	Disabled	0
14	1	Permit	Disabled	Disabled	1723284
15	1	Permit	Disabled	Disabled	1598931
16	1	Permit	Disabled	Disabled	1566794
17	1	Permit	Disabled	Disabled	0
18	1	Permit	Disabled	Disabled	0
19	1	Permit	Disabled	Disabled	0
20	1	Permit	Disabled	Disabled	0
21	1	Permit	Disabled	Disabled	0
22	1	Permit	Disabled	Disabled	0
23	1	Permit	Disabled	Disabled	0
24	1	Permit	Disabled	Disabled	0

Apply

#### ■ ACL Port Configuration

The switch ACL function support up to 128 Access Control Entries (ACEs), using the shared 128 ACEs for ingress classification. You can create an ACE and assign this ACE for each port with <Any> or assign this ACE for a policy or assign this ACE for a port. There are 8 policies, each port can select one of policy, then decides which of the following actions would take according to the packet's IPv4, EtherType, ARP Protocol, MAC Parameters and VLAN parameters:

- Packet Deny or Permit
- Rate Limiter (Unit: pps)
- Port Copy (1 - 24)

#### ■ Parameter:

- Port #:
  - Port number: 1~24

- Policy ID:  
Policy ID range:1~8
- Action:  
Permit or Deny forwarding the met ACL packets
- Rate Limiter ID:  
Disabled: Disable Rate Limitation  
Rate Limiter ID Range: 1~16. To select one of rate limiter ID for this port, it will limit met ACL packets by rate limiter ID configuration.
- Port Copy:  
Disabled: Disable to copy the met ACL packets to specific port.  
Port number: 1~24. Copy the met ACL packets to the selected port.
- Counter:  
The counter will increase from initial value 0, when this port received one of the met ACL packet the counter value will increase +1

## 4.6.2 Rate Limiters

**ACL Rate Limiter Configuration**

Rate Limiter ID	Rate (pps)
1	1K
2	16K
3	512
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1
16	1

- ACL Rate Limiter Configuration  
There are 16 rate limiter ID. You can assign one of the limiter ID for each port. The rate limit configuration unit is Packet Per Second (pps).



## ■ Chapter 4: Operation of Web-based Management

### ■ Parameter:

- Rate Limiter ID:

ID Range: 1~16

- Rate(pps):

1 / 2 / 4 / 8 / 16 / 32 / 64 / 128 / 256 / 512 / 1K / 2K / 4K / 8K / 16K / 32K / 64K / 128K / 256K / 512K / 1024K

## 4.6.3 Access Control List

Access Control List Configuration						Auto-refresh <input type="checkbox"/>	Refresh	Clear
Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Counters			
Any	ARP	Deny	1	Disabled	142			
Any	ARP	Permit	1	Disabled	40903			
Any	ARP	Permit	3	Disabled	0			
Any	ARP	Permit	1	Disabled	0			
Any	ARP	Permit	Any	Disabled	107469			
Any	undefined	Deny	Any	Disabled	0			
Any	EType	Deny	Any	Disabled	0			
Any	IPv4/DHCP Client (Out)	Permit	Any	Disabled	411			
Any	IPv4/DHCP Server (Out)	Permit	Any	Disabled	34255			
Any	IPv4/Other	Permit	Any	Disabled	26374			
Any	IPv4 DIP:0.0.0.0	Permit	Any	Disabled	18			
Any	undefined	Permit	Any	Disabled	0			
Any	EType	Permit	Any	Disabled	0			

### ■ ACL Rate Limiter Configuration

The switch ACL function support up to 128 Access Control Entries (ACEs), using the shared 128 ACEs for ingress classification. You can create an ACE and assign this ACE for each port with <Any> or assign this ACE for a policy or assign this ACE for a port. There are 8 policies, each port can select one of policy, then decides which of the Permit/Deny, Rate Limitation and Port Copy actions would take according to the ACL configuration packet's IPv4, EtherType, ARP Protocol, MAC Parameters and VLAN parameters.

### ■ Parameter description:

- Ingress Port:

Configurable Range: Any / Policy 1-8 / Port 1-24

Any: Apply this ACE rule for each port ingress classification

Policy 1-8: Apply this ACE rule for specific policy

Port 1-24: Apply this ACE rule for specific port ingress classification

## ■ Parameter:

## □ Frame Type:

Range: Any / Ethernet Type / ARP / IPv4

Any: It is including all frame type

Ethernet Type: It is including all Ethernet frame type

ARP: It is including all ARP protocol frame type

IPv4: It is including all IPv4 protocol frame type

## ■ ACE Configuration

The switch ACL function support up to 128 Access Control Entries (ACEs), using the shared 128 ACEs for ingress classification. You can create an ACE and assign this ACE for each port with <Any> or assign this ACE for a policy or assign this ACE for a port. There are 8 policies, each port can select one of policy, then decides which of the Permit/Deny, Rate Limitation and Port Copy actions would take according to the ACL configuration packet's IPv4, EtherType, ARP Protocol, MAC Parameters and VLAN parameters.

## ■ Parameter:

## □ Ingress Port:

Range: Any / Policy 1-8 / Port 1-24

Any: Apply this ACE rule for each port ingress classification

Policy 1-8: Apply this ACE rule for specific policy

Port 1-24: Apply this ACE rule for specific port ingress classification

## □ IP Protocol Filter:

Range: Any / Ethernet Type / ARP / IPv4

Any: It is including all frame type

Ethernet Type: It is including all Ethernet frame type

ARP: It is including all ARP protocol frame type

IPv4: It is including all IPv4 protocol frame type

- MAC Parameters: (When Frame Type = Any)
  - DMAC Filter: Range: Any / MC / BC / UC
    - Any: It is including all destination MAC address
    - MC: It is including all Multicast MAC address
    - BC: It is including all Broadcast MAC address
    - UC: It is including all Unicast MAC address
- MAC Parameters: (When Frame Type = Ethernet Type)
  - SMAC Filter:
    - Range: Any / Specific
    - Any: It is including all source MAC address
    - Specific: It is according to SMAC Value specific the source MAC address
  - DMAC Filter:
    - Range: Any / MC / BC / UC / Specific
    - Any: It is including all destination MAC address
    - MC: It is including all Multicast MAC address
    - BC: It is including all Broadcast MAC address
    - UC: It is including all Unicast MAC address
    - Specific: It is according to DMAC Value specific the destination MAC address

- MAC Parameters: (When Frame Type = ARP)
  - SMAC Filter:
    - Range: Any / Specific
    - Any: It is including all source MAC address
    - Specific: It is according to SMAC Value specific the source MAC address
  - DMAC Filter:
    - Range: Any / MC / BC / UC
    - Any: It is including all destination MAC address
    - MC: It is including all Multicast MAC address
    - BC: It is including all Broadcast MAC address
    - UC: It is including all Unicast MAC address
- MAC Parameters: (When Frame Type = IPv4)
  - DMAC Filter:
    - Range: Any / MC / BC / UC
    - Any: It is including all destination MAC address
    - MC: It is including all Multicast MAC address
    - BC: It is including all Broadcast MAC address
    - UC: It is including all Unicast MAC address
- Ether Type Parameters: (When Frame Type = Ethernet Type)
  - EtherType Filter:
    - Range: Any / Specific
    - Any: It is including all Ethernet frame type
    - Specific: It is according to specific Ethernet Type Value.
  - Ethernet Type Value:
    - The Ethernet Type Range: 0x600-0xFFFF

## □ ARP Parameters: (When Frame Type = ARP)

## ARP/RARP:

Range: Any / ARP / RARP / Other

Any: Including all ARP/RARP protocol frame types

ARP: Including all ARP protocol frame types

RARP: Including all RARP frame types

Other: Including other frame types except ARP/RARP protocol

## Request/Reply:

Range: Any / Request / Reply

Any: Including all ARP/RARP Request and Reply

Request: Including all ARP/RARP request frames

Reply: Including all ARP/RARP reply frames

## Sender IP Filter:

Range: Any / Host / Network

Any: Including all sender IP address

Host: Only one specific sender host IP address

Network: A specific IP subnet segment under the sender IP mask

Sender IP Address: Default: 192.168.1.1

Sender IP Mask: Default: 255.255.255.0

## Target IP Filter:

Range: Any / Host / Network

Any: Including all target IP address

Host: Only one specific target host IP address

Network: A specific IP subnet segment under the target IP mask

Target IP Address: Default: 192.168.1.254

Target IP Mask: Default: 255.255.255.0

## ARP SMAC Match:

Range: Any / 0 / 1

Any: Both 0 and 1

0: The ingress ARP frames where the source MAC address is not

equal SMAC under MAC parameter setting

1: The ingress ARP frames where the source MAC address is equal SMAC address under MAC parameter setting

RARP DMAC Match:

Range: Any / 0 / 1

Any: Both 0 and 1

0: The ingress RARP frames where the Destination MAC address is not equal DMAC address under MAC parameter setting

1: The ingress RARP frames where the Destination MAC address is equal DMAC address under MAC parameter setting

IP/Ethernet Length:

Range: Any / 0 / 1

Any: Both 0 and 1

0: The ingress ARP/PARP frames where the Hardware size is not equal "0x6" or the Protocol size is not equal "0x4"

1: The ingress ARP/PARP frames where the Hardware size is equal "0x6" and the Protocol size is "0x4"

IP:

Range: Any / 0 / 1

Any: Both 0 and 1

0: The ingress ARP/PARP frames where Protocol type is not equal "0x800"

1: The ingress ARP/PARP frames where Protocol type is equal "0x800"

Ethernet:

Range: Any / 0 / 1

Any: Both 0 and 1

0: The ingress ARP/PARP frames where Hardware type is not equal "0x100"

1: The ingress ARP/PARP frames where Hardware type is equal "0x100"

- IP Parameters: (When Frame Type = IPv4 and IP Protocol Filter = Any)  
IPTTL: (Time To Live)

How many routers a datagram can pass through. Each router decrements this value by 1 until it reaches 0 when the datagram is discarded. This keeps misrouted datagrams from remaining on the Internet forever

Range: Any / Non-zero / Zero

Any: Including all conditions for IPTTL

Non-Zero: Including IPTTL is Non-Zero

Zero: Including IPTTL is zero

- IP Fragment: (IP Fragmentation Flag)

Controls datagram fragmentation together with the identification field. The flags indicate whether the datagram may be fragmen-

ted, whether the datagram is fragmented, and whether the current fragment is the final one.

Range: Any / Yes / No

Any: Including all IP fragment case

Yes: The ingress frame is fragmented packet

No: The ingress frames is not fragmented packet

IP Option:

A list of optional specifications for security restrictions, route recording, and source routing. Not every datagram specifies an options field.

Range: Any / Yes / No

Any: Including all IP option case

Yes: The ingress frame is specified IP options

No: The ingress frame is not specified IP options

SIP Filter: (SIP Source IP Address)

Range: Any / Host / Network

Any: Including all source IP address

Host: Only one specific source host IP address

Network: A specific IP subnet segment under the source IP mask

SIP Address: Default: 192.168.1.1

SIP Mask: Default: 255.255.255.0

DIP Filter: (DIP Destination IP Address)

Range: Any / Host / Network

Any: Including all destination IP address

Host: Only one specific destination host IP address

Network: A specific IP subnet segment under the destination IP mask

DIP Address: Default: 192.168.1.254

DIP Mask: Default: 255.255.255.0



- IP Parameters: (Frame Type = IPv4 and IP Protocol Filter = ICMP)
  - ICMP Type Filter:
    - Range: Any / Specific
    - Any: Including all types of ICMP type values
    - Specific: According to following ICMP type value setting for ingress classification
  - ICMP Type Value: Range: 0-255
  - ICMP Code Filter:
    - Range: Any / Specific
    - Any: Including all of ICMP code values
    - Specific: According to following ICMP code value setting for ingress classification
  - ICMP Code Value: Range: 0-255

- IP Parameters: (Frame Type = IPv4 and IP Protocol Filter = UDP)

Source Port Filter:

Range: Any / Specific / Range

Any: Including all UDP source ports

Specific: According to following Source Port No. setting for ingress classification.

Range: According to following Source Port Range setting for ingress classification.

Source Port No.: Range: 0-65535

Source Port Range.: Range: 0-65535

Dest. Port Filter:

Range: Any / Specific / Range

Any: Including all UDP destination ports

Specific: According to following Dest. Port No. setting for ingress classification

Range: According to following Dest. Port Range setting for ingress classification

Dest. Port No.: (Destination Port Number)

Range: 0-65535

Dest. Port Range.: (Destination Port Range)

Range: 0-65535

- IP Parameters: (Frame Type = IPv4 and IP Protocol Filter = TCP)

Source Port Filter:

Range: Any / Specific / Range

Any: Including all TCP source ports

Specific: According to following Source Port No. setting for ingress classification

Range: According to following Source Port Range setting for ingress classification

Source Port No.: Range: 0-65535

Source Port Range.: Range: 0-65535

Dest. Port Filter:

Range: Any / Specific / Range

Any: Including all TCP destination ports

Specific: According to following Dest. Port No. setting for ingress classification

Range: According to following Dest. Port Range setting for ingress classification

Dest. Port No.: Range: 0-65535

Dest. Port Range.: Range: 0-65535

TCP FIN:

TCP Control Bit FIN: Means No more data from sender

Range: Any / 0 / 1

Any: Including all TCP FIN case

0: The TCP control bit FIN is 0

1: The TCP control bit FIN is 1

TCP SYN:

TCP Control Bit SYN: Means Synchronize sequence numbers

Range: Any / 0 / 1

Any: Including all TCP SYN case

0: The TCP control bit SYN is 0

1: The TCP control bit SYN is 1

**TCP RST:**

TCP Control Bit RST: Means Reset the connection

Range: Any / 0 / 1

Any: Including all TCP RST case

0: The TCP control bit RST is 0

1: The TCP control bit RST is 1

**TCP PSH:**

TCP Control Bit PSH: Means Push Function

Range: Any / 0 / 1

Any: Including all TCP PSH case

0: The TCP control bit PSH is 0

1: The TCP control bit PSH is 1

**TCP ACK:**

TCP Control Bit ACK: Means Acknowledgment field significant

Range: Any / 0 / 1

Any: Including all TCP ACK case

0: The TCP control bit ACK is 0

1: The TCP control bit ACK is 1

**TCP URG:**

TCP Control Bit URG: Means Urgent Pointer field significant

Range: Any / 0 / 1

Any: Including all TCP URG case

0: The TCP control bit URG is 0

1: The TCP control bit URG is 1

**IP Protocol Value:**

The IP Protocol Value is TCP options may occupy space at the end of the TCP header and are a multiple of 8 bits in length. Currently defined options include (kind indicated in octal):

0 - End of option list

1 - No-Operation

Range: Any / 0 / 1

Any: Including all IP protocol value case

0: The IP protocol value is 0

1: The IP protocol value is 1

- IP Parameters: (Frame Type = IPv4 and IP Protocol Filter = Other)

IP Protocol Value: Default: 255

IPTTL: (Time To Live)

How many routers a datagram can pass through. Each router decrements this value by 1 until it reaches 0 when the datagram is discarded. This keeps misrouted datagrams from remaining on the Internet forever

Range: Any / Non-zero / Zero

Any: Including all conditions for IPTTL

Non-Zero: Including IPTTL is Non-Zero

Zero: Including IPTTL is zero

- IP Fragment: (IP Fragmentation Flag)

Controls datagram fragmentation together with the identification field. The flags indicate whether the datagram may be fragmen-

ed, whether the datagram is fragmented, and whether the current fragment is the final one.

Range: Any / Yes / No

Any: Including all IP fragment case

Yes: The ingress frame is fragmented packet

No: The ingress frames is not fragmented packet

IP Option:

A list of optional specifications for security restrictions, route recording, and source routing. Not every datagram specifies an options field.

Range: Any / Yes / No

Any: Including all IP option case

Yes: The ingress frame is specified IP options

No: The ingress frame is not specified IP options

SIP Filter: (SIP Source IP Address)

Range: Any / Host / Network

Any: Including all source IP address

Host: Only one specific source host IP address

Network: A specific IP subnet segment under the source IP mask

SIP Address: Default: 192.168.1.1

SIP Mask: Default: 255.255.255.0

DIP Filter: (DIP Destination IP Address)

Range: Any / Host / Network

Any: Including all destination IP address

Host: Only one specific destination host IP address

Network: A specific IP subnet segment under the destination IP mask

DIP Address: Default: 192.168.1.254

DIP Mask: Default: 255.255.255.0

## □ VLAN Parameters:

## VLAN ID Filter:

Range: Any / Specific

Any: Including all VLAN IDs

Specific: According to following VLAN ID and Tag Priority setting for ingress classification

## VLAN ID:

Range: 1-4094

Tag Priority:

Range: Any / 0-7

Any: Including all Tag Priority values

0-7: The Tag Priority Value is one of number (0-7)

## Action Parameters:

When the ingress frame meet above ACL ingress classification rule you can do the following actions:

## Action:

Range: Permit / Deny

Permit: Permit the met ACL ingress classification rule packets forwarding to other ports on the switch

Deny: Discard the met ACL ingress classification rule packets

## Rate Limiter:

Range: Disabled / 1-16

Disable: Disable Rate Limiter function

1-16: Apply the Rate Limiter Number setting for met ACL ingress rule packets

## Port Copy:

Range: Disabled / 1-24

Disable: Disable the Port Copy function

1-24: The packets will be copied to the selected port when they met ACL ingress rule.

## 4.6.4 Wizard

**Welcome to the ACL Configuration Wizard!**

**Please select an action:**

**Set up Policy Rules**  
Set up the default policy rules for Client ports, Server ports, Network ports, and Guest ports.

**Set up Port Policies**  
Group ports into several types according to different ACL policies.

**Set up Typical Network Application Rules**  
Set up the specific ACL for different typical network application access control.

To continue, click Next.

---

[Next >](#)

### ■ Wizard

The wizard function is provide 4 type of typical application for user easy to configure their application with ACL function.

### ■ Parameter:

- Please select an Action:  
Set up Policy Rules / Set up Port Policies / Set up Typical Network Application Rules / Set up Source MAC and Source IP Binding
- Next:  
Click on <Next> to confirm current setting and go to next step automatically.
- Cancel:  
Cancel current setting back to top layer in the ACL wizard function
- Back:  
Click on <Back> to back to previous step
- Wizard Again:  
Click on <Wizard Again> the UI will back to top layer in the wizard function
- Finish:  
Click in <Finish> to finish the ACL Wizard setting, it will according the selection items to change the related parameters, then you have to click on <Apply> to confirm the all changed parameters setting.



- Parameter:
  - Common Server:  
DHCP / DNS / FTP / HTTP / IMAP / NFS / POP3 / SAMBA / SMTP / TELNET / TFTP
  - Instant Messaging:  
Google Talk / MSN Messenger / Yahoo Messenger
  - User Definition:  
Ethernet Type / UDP Port / TCP Port
  - Others:  
TCP Port / ICMP / Multicast IP Stream / NetBIOS / Ping Request / Ping Reply / SNMP / SNMP Traps
  - Ingress Port:  
Any / Policy1-8 / Port1-24
  - Action:  
Permit / Deny
  - Rate Limiter ID:  
Disabled / 1-16
- Parameter:
  - Port #:  
1-24
  - Binding Enabled:  
Use the switch ACL function to support IP/MAC Binding function, the maximum is up to 128 entries.
  - Source MAC Address:  
xx-xx-xx-xx-xx-xx (For example: 00-40-c7-00-00-01)
  - Source IP Address:  
xxx.xxx.xxx.xxx (For example: 192.168.1.100)

## 4.7 Security: IP MAC Binding

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC binding is to restrict the access to a switch to a number of authorized users. Only

the authorized client can access the Switch's port by checking the pair of IP-MAC. Addresses and port number with the pre-configured database. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet.

### IP MAC Binding Configuration

**State**

**Trust Port**

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

**Apply**

MAC	IP	Port No	VID
- . - . - .		1	

**Add**

No	MAC	IP	Port	VID

**Delete**

#### ■ IP MAC Binding Configuration

The switch has client and server two classes of IP-MAC Binding table. The maximum number of IP-MAC binding client table is 512 entries. The maximum number of IP-MAC Binding server table is 64 entries. The creation of authorized users can be manually. The function is global, this means a user can enable or disable the function for all ports on the switch.

#### ■ Parameters:

- **State:**  
Disabled / Enabled
- **Time Interval:**  
Range: 10 / 20 / 30. Time interval is for ARP echo, the switch will according to server table entries to send ARP echo.
- **Server/Client:**  
The maximum number of IP-MAC binding client table is 512 entries.  
The maximum number of IP-MAC Binding server table is 64 entries.

- MAC:  
Six-byte MAC Address: xx-xx-xx-xx-xx-xx (For example: 00-40-c7-00-00-01)
- IP:  
Four-byte IP Address: xxx.xxx.xxx.xxx (For example: 192.168.1.100)
- Port No:  
Port no.: 1-24
- VID:  
VLAN ID: 1-4094
- Add:  
Input MAC, IP, Port and VID, then click on <Add> to create a new entry into the IP MAC Binding table
- Delete:  
Select one of entry from the table, then click on <Delete> to delete this entry.

IP MAC Binding Dynamic Entry

No	MAC	IP	Port	VID

Delete

## 4.8 Security: DHCP Snooping

### 4.8.1 DHCP Snooping State

DHCP Snooping State

DHCP Snooping

Apply

### ■ DHCP Snooping State

The addresses assigned to DHCP clients on unsecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping. DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.

### ■ Parameter:

#### DHCP Snooping state:

The parameter which set to disabled or enabled the DHCP snooping function on the switch, the default is Disabled.

Note: To click " Apply" when you finish the configuration.

## 4.8.2 DHCP Snooping Entry

### DHCP Snooping Entry

VID	Trust Port 1	Trust Port 2	Server IP	Option 82	Action
<input type="button" value="Delete"/>					
VID	<input type="text"/>	Trust Port 1	<input type="text" value="Disable"/>	Trust Port 2	<input type="text" value="Disable"/>
Server IP	<input type="text"/>	Option 82	<input type="text" value="Disable"/>	Action	<input type="text" value="Keep"/>
<input type="button" value="Add"/>					
VID	<input type="text" value="0"/>	Trust Port 1	<input type="text" value="Disable"/>	Trust Port 2	<input type="text" value="Disable"/>
Server IP	<input type="text" value="0.0.0.0"/>	Option 82	<input type="text" value="Disable"/>	Action	<input type="text" value="Keep"/>
<input type="button" value="Apply"/>					

### ■ DHCP Snooping Entry

DHCP snooping Entry allows a switch to add the an trust DHCP server and 2 trust port the DHCP snooping available entry. This information can be useful in tracking an IP address back to a physical port and enable or disable the DHCP Option 82.

- Parameter:
  - VID:
 

When DHCP snooping is enabled, and enabled on the specified VLAN, DHCP packet filtering will be performed on any un-trusted ports within the VLAN. It set a available VLAN ID to enable the DHCP snooping on VLAN interface.
  - Trust Port 1:
 

If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a trusted por. It set a trust port 1. available port from 0 to 24. 0 is disabled.
  - Trust port 2:
 

It set a trust port 2. available port from 0 to 24. 0 is disabled.
  - Trust VID:
 

It set a trust VLAN ID. available VID from 1 to 4094.
  - Server IP:
 

It set a trust DHCP Server IP address for DHCP Snooping.
  - Option 82:
 

It set the DHCP Option 82 function on the switch, default is Disable.
  - Action:
 

It set the switch when received a client DHCP request packet then action for filtering. available action: keep/ drop / replace.

Note: Filtering rules are implemented as follows:

- If the DHCP snooping is disabled, all DHCP packets are forwarded.
- If DHCP snooping is enabled and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a trusted port.
- If DHCP snooping is enabled and also enabled on the VLAN where the DHCP packet is received, but the port is not trusted, it is processed as follows:
 

If the DHCP packet is a reply packet from a DHCP server, the packet is dropped.

If the DHCP packet is from a client, such as a DISCOVER, REQUEST INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled. However, if MAC address verifi-

cation is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.

If the DHCP packet is not a recognizable type, it is dropped.

- If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
- If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and un-trusted ports in the same VLAN.

### 4.8.3 DHCP Snooping Client

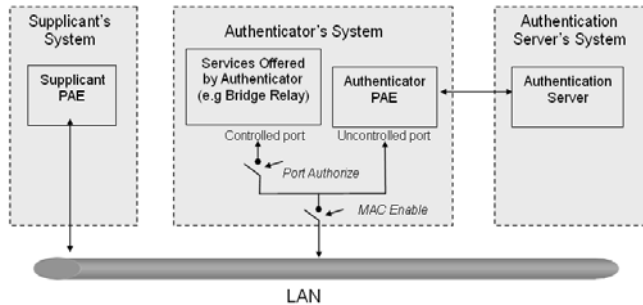
DHCP Snooping Client				
MAC	VID	Port	IP	Lease
<a href="#">Delete</a>				

- DHCP Snooping Client  
To show the DHCP snooping client.
- Parameter:
  - MAC:  
To show the DHCP snooping client's MAC address.
  - VID:  
To show the DHCP snooping client's VLAN ID.
  - Port:  
To show the DHCP snooping client's port.
  - IP:  
To show the DHCP snooping client's IP address.
  - Lease:  
To show the DHCP snooping client's lease.

## 4.9 Security: 802.1x Configuration

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

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



According to IEEE802.1x, there are three components implemented. They are Authenticator, Supplicant and Authentication server.

### ■ Supplicant:

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

### ■ Authenticator:

An entity facilitates the authentication of the supplicant entity. It controls the state of the port, authorized or unauthorized, according to the result of authentication message exchanged between it and a supplicant PAE. The authenticator may request the supplicant to re-authenticate itself at

a configured time period. Once start re-authenticating the supplicant, the controlled port keeps in the authorized state until re-authentication fails.

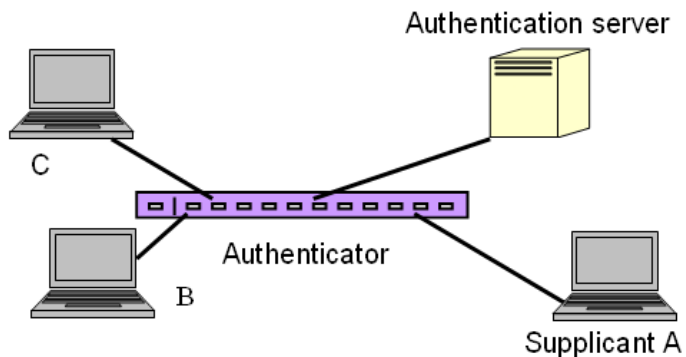
A port acting as an authenticator is thought to be two logical ports, a controlled port and an uncontrolled port. A controlled port can only pass the packets when the authenticator PAE is authorized, and otherwise, an uncontrolled port will unconditionally pass the packets with PAE group MAC address,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

■ Authentication server:

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

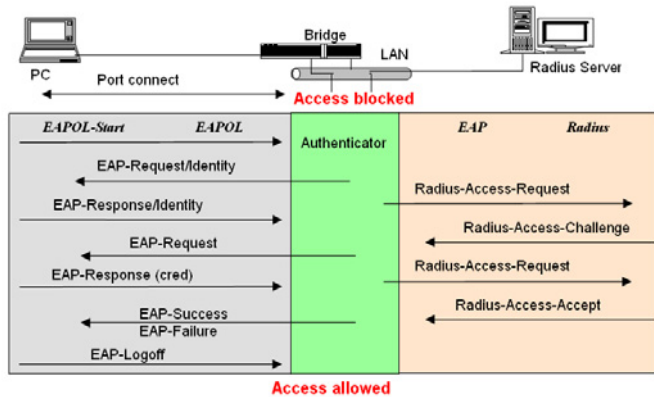
The overview of operation flow for the following figure is quite simple. When Supplicant PAE issues a request to Authenticator PAE, Authenticator and Supplicant exchanges authentication message. Then, Authenticator passes the request to RADIUS server to verify. Finally, RADIUS server replies if the request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

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





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



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

- 1 At the initial stage, the supplicant A is unauthenticated and a port on switch acting as an authenticator is in unauthorized state. So the access is blocked in this stage.
- 2 Initiating a session. Either authenticator or supplicant can initiate the message exchange. If supplicant initiates the process, it sends EAPOL-start packet to the authenticator PAE and authenticator will immediately respond EAP-Request/Identity packet.

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

Only MultiHost 802.1X is the type of authentication supported in the switch. In this mode, for the devices connected to this port, once a supplicant is

authorized, the devices connected to this port can access the network resource through this port.

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

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

## 4.9.1 Server

### 802.1X Server Configuration

Authentication Server	
Server IP Address 1	192.168.1.1
UDP Port	1812
Server IP Address 2	192.168.1.1
UDP Port	1812
Secret Key	Radius
Accounting Server	
Server IP Address 1	192.168.1.1
UDP Port	1813
Server IP Address 2	192.168.1.1
UDP Port	1813
Secret Key	Radius

### ■ 802.1X Server Configuration

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

## ■ Parameter:

## □ Authentication Server

Server IP Server:

Server IP address for authentication.

Default: 192.168.1.1

UDP Port:

Default port number is 1812.

Secret Key:

The secret key between authentication server and authenticator. It is a string with the length 1 - 31 characters. The character string may contain upper case, lower case and 0-9. It is character sense. It is not allowed for putting a blank between any two characters.

Default: Radius

## □ Accounting Server

Server IP Server:

Server IP address for authentication.

Default: 192.168.1.1

UDP Port:

Default port number is 1812.

Secret Key:

The secret key between authentication server and authenticator. It is a string with the length 1 - 31 characters. The character string may contain upper case, lower case and 0-9. It is character sense. It is not allowed for putting a blank between any two characters.

Default: Radius

## 4.9.2 Port Configuration

### 802.1X Port Configuration

<b>Port</b>	Port 1
<b>Mode</b>	Disabled
<b>Port Control</b>	Auto
<b>reAuthMax</b>	2 (1-10)
<b>txPeriod</b>	30 (1-65535 sec)
<b>quietPeriod</b>	60 (0-65535 sec)
<b>reAuthEnabled</b>	ON
<b>reAuthPeriod</b>	120 (1-65535 sec)
<b>maxReq</b>	2 (1-10)
<b>suppTimeout</b>	30 (1-255 sec)
<b>server Timeout</b>	30 (1-255 sec)

### ■ 802.1X Port Configuration

This function is used to configure the parameters for each port in 802.1X port security application. Refer to the following parameters description for details.

Parameter:

- **Port:**  
It is the port number to be selected for configuring its associated 802.1X parameters which are Port control, reAuthMax, txPeriod, Quiet Period, reAuthEnabled, reAuthPeriod, max. Request, suppTimeout, serverTimeout and Controlled direction.
- **Mode:**  
Range: Disable / Normal / Advanced / Clientless  
 Disable: Disable IEEE 802.1X for this port.  
 Normal: All clients under this port will be authorized when one of the client do 802.1X authentication successfully.  
 Advanced: Each clients under this port have to do 802.1X authentication by himself.  
 Clientless: The clients don't need to install 802.1X client function, that means the client PC (for example WINDOW XP) does not need to enable 802.1X client function also can do 802.1X authentication. But the network maintainer need to configure the Radius server using each client's MAC address for Radius account ID and password.

- Port Control:  
This is used to set the operation mode of authorization. There are three type of operation mode supported, ForceUnauthorized, ForceAuthorized, Auto.  
ForceUnauthorized: The controlled port is forced to hold in the unauthorized state.  
ForceAuthorized: The controlled port is forced to hold in the authorized state.  
Auto: The controlled port is set to be in authorized state or unauthorized state depends on the result of the authentication exchange between the authentication server and the supplicant.  
Default: Auto
- reAuthMax(1-10):  
The number of authentication attempt that is permitted before the port becomes unauthorized.  
Default: 2
- txPeriod(1-65535 s):  
A time period to transmitted EAPOL PDU between the authenticator and the supplicant.  
Default: 30
- Quiet Period(0-65535 s):  
A period of time during which we will not attempt to access the supplicant.  
Deafult: 60 seconds
- reAuthEnabled:  
Choose whether regular authentication will take place in this port.  
Default: ON
- reAuthPeriod(1-65535 s):  
A non-zero number seconds between the periodic re-authentication of the supplicant.  
Default: 3600

- max. Request(1-10):  
The maximum of number times that the authenticator will retransmit an EAP Request to the supplicant before it times out the authentication session. The valid range: 1 - 10.  
Default: 2 times
- suppTimeout(1-65535 s):  
A timeout condition in the exchange between the authenticator and the supplicant. The valid range: 1 -65535.  
Default: 30 seconds.
- serverTimeout(1-65535 s):  
A timeout condition in the exchange between the authenticator and the authentication server. The valid range: 1 -65535.  
Default: 30 seconds

### 4.9.3 Status

**802.1X Status**

Port	Mode	Status
1	Disable	-
2	Disable	-
3	Disable	-
4	Disable	-
5	Disable	-
6	Disable	-
7	Disable	-
8	Disable	-
9	Disable	-
10	Disable	-
11	Disable	-
12	Disable	-
13	Disable	-
14	Disable	-
15	Disable	-
16	Disable	-
17	Disable	-
18	Disable	-
19	Disable	-
20	Disable	-
21	Disable	-
22	Disable	-
23	Disable	-
24	Disable	-

**Refresh**

- **802.1X Status**  
Show the each port IEEE 802.1X authentication current operating mode and status.
- **Parameter:**
  - Port:**  
Port number: 1-24
  - Mode:**  
Show this port IEEE 802.1X operating mode: There are four modes Disable, Normal, Advance and Clientless
  - Status:**  
Show this port IEEE 802.1X security current status: Authorized or Unauthorized



## 4.9.4 Statistics

802.1X Port Statistics Port 1	
Port 1 <input type="checkbox"/> Auto-refresh <input type="button" value="Refresh"/> <input type="button" value="Clear"/>	
<b>Authenticator Counters</b>	
authEntersConnecting	0
authEapLogoffsWhileConnecting	0
authEntersAuthenticating	0
authAuthSuccessesWhileAuthenticating	0
authAuthTimeoutsWhileAuthenticating	0
authAuthFailWhileAuthenticating	0
authAuthEapStartsWhileAuthenticating	0
authAuthEapLogoffWhileAuthenticating	0
authAuthReauthsWhileAuthenticated	0
authAuthEapStartsWhileAuthenticated	0
authAuthEapLogoffWhileAuthenticated	0
<b>Backend Authenticator Counters</b>	
backendResponses	0
backendAccessChallenges	0
backendOtherRequestsToSupplicant	0
backendAuthSuccesses	0
backendAuthFails	0
<b>802.1X MIB Counters</b>	
dot1xAuthEapolFramesRx	0
dot1xAuthEapolFramesTx	0
dot1xAuthEapolStartFramesRx	0
dot1xAuthEapolLogoffFramesRx	0
dot1xAuthEapolRespIdFramesRx	0
dot1xAuthEapolRespFramesRx	0
dot1xAuthEapolReqIdFramesTx	0
dot1xAuthEapolReqFramesTx	0
dot1xAuthInvalidEapolFramesRx	0
dot1xAuthEapLengthErrOfFramesRx	0
dot1xAuthLastEapolFrameVersion	0
dot1xAuthLastEapolFrameSource	00-00-00-00-00-00

### ■ 802.1X Port Statistics Port1

Show the IEEE 802.1X authentication related counters for manager monitoring authenticator status.

#### ■ Parameter:

- Port:  
Port Number: 1-24
- Auto - refresh:  
Refresh the authenticator counters in the web UI automatically
- Refresh:  
Click on the <Refresh> to update the authenticator counters in the web UI
- Clear:  
Click on the <Clear> to clear all authenticator counters in the web UI

## 4.10 Security: Mirror

### Mirror Configuration

Port to mirror to: Disabled ▾

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

Apply

### ■ Mirror Configuration

Mirror Configuration is to monitor the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.

Note: When configure the mirror function, you should avoid setting a port to be a sniffer port and aggregated port at the same time. It will cause something wrong.

### ■ Parameter:

- Port to mirror to:  
Range: Disabled / Port 1-24  
Set the monitoring port.

- Port #:  
Range: 1-24  
Select the monitored ports.
- Source Enable:  
The source enable means the monitored port ingress traffic will be copied to monitoring port.
- Destination Enable:  
The destination enable means the monitored port egress traffic will be copied to monitoring port.

## 4.11 Configuration: GVRP

GVRP (Generic VLAN Registration Protocol) is an application based on Generic Attribute Registration Protocol (GARP), mainly used to automatically and dynamically maintain the group membership information of the VLANs. The GVRP offers the function providing the VLAN registration service through a GARP application. It makes use of GARP Information Declaration (GID) to maintain the ports associated with their attribute database and GARP Information Propagation (GIP) to communicate among switches and end stations. With GID information and GIP, GVRP state machine maintain the contents of Dynamic VLAN Registration Entries for each VLAN and propagate these information to other GVRP-aware devices to setup and update their knowledge database, the set of VLANs associated with currently active members, and through which ports these members can be reached.

In GVRP Configuration function folder, there are three functions supported, including GVRP Config, GVRP Counter and GVRP Group explained below.

## 4.11.1 Config

**GVRP Configuration**

GVRP State:

Port	Join Time	Leave Time	LeaveAll Time	Default Applicant Mode	Default Registrar Mode	Restricted Mode
1	20	60	1000	Normal	Normal	Disabled
2	20	60	1000	Normal	Normal	Disabled
3	20	60	1000	Normal	Normal	Disabled
4	20	60	1000	Normal	Normal	Disabled
5	20	60	1000	Normal	Normal	Disabled
6	20	60	1000	Normal	Normal	Disabled
7	20	60	1000	Normal	Normal	Disabled
8	20	60	1000	Normal	Normal	Disabled
9	20	60	1000	Normal	Normal	Disabled
10	20	60	1000	Normal	Normal	Disabled
11	20	60	1000	Normal	Normal	Disabled
12	20	60	1000	Normal	Normal	Disabled
13	20	60	1000	Normal	Normal	Disabled
14	20	60	1000	Normal	Normal	Disabled
15	20	60	1000	Normal	Normal	Disabled
16	20	60	1000	Normal	Normal	Disabled
17	20	60	1000	Normal	Normal	Disabled
18	20	60	1000	Normal	Normal	Disabled
19	20	60	1000	Normal	Normal	Disabled
20	20	60	1000	Normal	Normal	Disabled
21	20	60	1000	Normal	Normal	Disabled
22	20	60	1000	Normal	Normal	Disabled
23	20	60	1000	Normal	Normal	Disabled
24	20	60	1000	Normal	Normal	Disabled

### ■ GVRP Config

In the function of GVRP Config, it is used to configure each port's GVRP operation mode, in which there are seven parameters needed to be configured described below.

### ■ Parameter:

#### □ GVRP State Setting:

This function is simply to let you enable or disable GVRP function. You can pull down the list and click the <Downward> arrow key to choose "Enable" or "Disable". Then, click the <Apply> button, the system will take effect immediately.

#### □ Join Time:

Used to declare the Join Time in unit of centisecond. Valid time range: 20–100 centisecond, Default: 20 centisecond.

- Leave Time:  
Used to declare the Leave Time in unit of centisecond. Valid time range: 60 –300 centisecond, Default: 60 centisecond.
- Leave All Time:  
A time period for announcement that all registered device is going to be de-registered. If someone still issues a new join, then a registration will be kept in the switch. Valid range: 1.000-5.000 unit time, Default: 1.000 unit time.
- Default Applicant Mode:  
The mode here means the type of participant. There are two modes, normal participant and non-participant, provided for the user's choice.
  - Normal:  
It is Normal Participant. In this mode, the switch participates normally in GARP protocol exchanges. The default setting is Normal.
  - Non-Participant:  
It is Non-Participant. In this mode, the switch does not send or reply any GARP messages. It just listens messages and reacts for the received GVRP BPDU (Bridge Protocol Data Unit).
- Default Registrar Mode:  
The mode here means the type of Registrar. There are three types of parameters for registrar administrative control value, normal registrar, fixed registrar and forbidden registrar, provided for the user's choice.
  - Normal:  
It is Normal Registration. The Registrar responds normally to incoming GARP messages. The default setting is Normal.
  - Fixed:  
It is Registration Fixed. The Registrar ignores all GARP messages, and all members remain in the registered (IN) state.
  - Forbidden:  
It is Registration Forbidden. The Registrar ignores all GARP messages, and all members remain in the unregistered (EMPTY) state.

□ Restricted Mode:

This function is used to restrict dynamic VLAN be created when this port received GVRP PDU (Protocol Data Unit). There are two modes, disable and enable, provided for the user's choice.

Disabled:

In this mode, the switch dynamic VLAN will be created when this port received GVRP PDU. The default setting is Normal.

Enabled:

In this mode, the switch does not create dynamic VLAN when this port received GVRP PDU. Except received dynamic VLAN message of the GVRP PDU is an existed static VLAN in the switch, this port will be added into the static VLAN members dynamically.

## 4.11.2 Counter

**GVRP Counter**

Select Port

Counter Name	Received	Transmitted
Total GVRP Packets	0	0
Invalid GVRP Packets	0	0
LeaveAll message	0	0
JoinEmpty message	0	0
JoinIn message	0	0
LeaveEmpty message	0	0
Empty message	0	0

■ GVRP Counter

All GVRP counters are mainly divided into Received and Transmitted two categories to let you monitor the GVRP actions. Actually, they are GARP packets.

## ■ Parameter:

## □ Received:

## Total GVRP Packets:

Total GVRP BPDU is received by the GVRP application.

## Invalid GVRP Packets:

Number of invalid GARP BPDU is received by the GARP application.

## LeaveAll Message Packets:

Number of GARP BPDU with Leave All message is received by the GARP application.

## JoinEmpty Message Packets:

Number of GARP BPDU with Join Empty message is received by the GARP application.

## JoinIn Message Packets:

Number of GARP BPDU with Join In message is received by the GARP application.

## LeaveEmpty Message Packets:

Number of GARP BPDU with Leave Empty message is received by the GARP application.

## Empty Message Packets:

Number of GARP BPDU with Empty message is received by the GARP application.

- Transmitted:
  - Total GVRP Packets:
    - Total GARP BPDU is transmitted by the GVRP application.
  - Invalid GVRP Packets:
    - Number of invalid GARP BPDU is transmitted by the GVRP application.
  - LeaveAll Message Packets:
    - Number of GARP BPDU with Leave All message is transmitted by the GARP application.
  - JoinEmpty Message Packets:
    - Number of GARP BPDU with Join Empty message is transmitted by the GARP application.
  - JoinIn Message Packets:
    - Number of GARP BPDU with Join In message is transmitted by the GARP application.
  - LeaveEmpty Message Packets:
    - Number of GARP BPDU with Leave Empty message is transmitted by the GARP application.
  - Empty Message Packets:
    - Number of GARP BPDU with Empty message is transmitted by the GARP application.

### 4.11.3 Group

GVRP VLAN Group Information	
VID	Member Port
<a href="#">Edit Administrative Control</a>	

- GVRP Group VLAN Information
  - To show the dynamic group member and their information.
- Parameter:
  - VID:
    - VLAN identifier. When GVRP group creates, each dynamic VLAN group owns its VID. Valid range is 1 ~ 4094.



- Member Port:  
Those are the members belonging to the same dynamic VLAN group.
- Edit Administrative Control:  
When you create GVRP group, you can use Administrative Control function to change Applicant Mode and Registrar Mode of GVRP group member.

## 4.12 Configuration: QoS (Quality of Service) Configuration

The switch support four QoS queues per port with strict or weighted fair queuing scheduling. There are 24 QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges.

High flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class.

The switch support advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frame. A super priority queue with dedicated memory and strict highest priority in the arbitration. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

## 4.12.1 Ports

**Port QoS Configuration**

Number of Classes

Port	Default Class	QCL	User Priority	Queuing Mode	Queue Weighted (Low:Normal:Medium:High)			
1	Low	1	0	Strict Priority	1	2	4	8
2	Low	1	0	Strict Priority	1	2	4	8
3	Low	1	0	Strict Priority	1	2	4	8
4	Low	1	0	Strict Priority	1	2	4	8
5	Low	1	0	Strict Priority	1	2	4	8
6	Low	1	0	Strict Priority	1	2	4	8
7	Low	1	0	Strict Priority	1	2	4	8
8	Low	1	0	Strict Priority	1	2	4	8
9	Low	1	0	Strict Priority	1	2	4	8
10	Low	1	0	Strict Priority	1	2	4	8
11	Low	1	0	Strict Priority	1	2	4	8
12	Low	1	0	Strict Priority	1	2	4	8
13	Low	1	0	Strict Priority	1	2	4	8
14	Low	1	0	Strict Priority	1	2	4	8
15	Low	1	0	Strict Priority	1	2	4	8
16	Low	1	0	Strict Priority	1	2	4	8
17	Low	1	0	Strict Priority	1	2	4	8
18	Low	1	0	Strict Priority	1	2	4	8
19	Low	1	0	Strict Priority	1	2	4	8
20	Low	1	0	Strict Priority	1	2	4	8
21	Low	1	0	Strict Priority	1	2	4	8
22	Low	1	0	Strict Priority	1	2	4	8
23	Low	1	0	Strict Priority	1	2	4	8
24	Low	1	0	Strict Priority	1	2	4	8

### ■ Port QoS Configuration

To configure each port QoS behavior. Four QoS queue per port with strict or weighted fair queuing scheduling. There are 24 QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges.

### ■ Parameter:

- Number of Classes:

1 / 2 / 4

- Port:

User can choose the port (1~24) respectively with Priority Class on Per Port Priority function.

- **Default Class:**  
User can set up High Priority or Low Priority for each port respectively.  
Low / Normal / Medium / High
- **QCL:**  
The number of QCL rule 1~24, each port have to apply one of the QCL rule for QoS behavior
- **User priority:**  
The user priority value 0~7 (3 bits) is used as an index to the eight QoS class values for VLAN tagged or priority tagged frames.
- **Queuing Mode:**  
There are two Scheduling Method, Strict Priority and Weighted Fair. Default is Strict Priority. After you choose any of Scheduling Method, please click Apply button to be in operation.
- **Queue Weighted:**  
There are four queues per port and four classes weighted number (1 / 2 / 4 / 8) for each queues, you can select the weighted number when the scheduling method be set to "Weighted Fair" mode.

#### 4.12.2 Qos Control List

##### QoS Control List Configuration

QCE Type	Type Value	Traffic Class

##### ■ Qos Control List Configuration

The switch support four QoS queues per port with strict or weighted fair queuing scheduling. There are 24 QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ether Type, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges.

QCE Configuration: The QCL consists of 12 QoS Control Entries (QCEs) that are searched from the top of the list to the bottom of the list for a match. The first matching QCE determines the QoS classification of the frame. The QCE ordering is therefore important for the resulting QoS classification algorithm. If no matching QCE is found, the default QoS class is used in the port QoS configuration.

- Parameter:
  - QCL#:
    - QCL number : 1~24
  - QCE Type:
    - Ethernet Type / VLAN ID / UDP/TCP Port / DSCP / ToS / Tag Priority
  - Ethernet Type Value:
    - The configurable range is 0x600~0xFFFF. Well known protocols already assigned EtherType values. The commonly used values in the EtherType field and corresponding protocols are listed below:

Ethertype (Hexadecimal)	Protocol
0x0800	IP, Internet Protocol
0x0801	X.75 Internet
0x0802	NBS Internet
0x0803	ECMA Internet
0x0804	Chaosnet
0x0805	X.25 Level 3
0x0806	ARP, Address Resolution Protocol.
0x0808	Frame Relay ARP [RFC1701]
0x6559	Raw Frame Relay [RFC1701]
0x8035	DRARP, Dynamic RARP. RARP, Reverse Address Resolution Protocol.
0x8037	Novell Netware IPX
0x809B	EtherTalk (AppleTalk over Ethernet)
0x80D5	IBM SNA Services over Ethernet
0x 80F3	AARP, AppleTalk Address Resolution Protocol.
0x8100	IEEE Std 802.1Q - Customer VLAN Tag Type.
0x8137	IPX, Internet Packet Exchange.
0x 814C	SNMP, Simple Network Management Protocol.
0x86DD	IPv6, Internet Protocol version 6.
0x880B	PPP, Point-to-Point Protocol.
0x 880C	GSMP, General Switch Management Protocol.

Ethertype (Hexadecimal)	Protocol
0x8847	MPLS, Multi-Protocol Label Switching (unicast).
0x8848	MPLS, Multi-Protocol Label Switching (multicast).
0x8863	PPPoE, PPP Over Ethernet (Discovery Stage).
0x8864	PPPoE, PPP Over Ethernet (PPP Session Stage).
0x88BB	LWAPP, Light Weight Access Point Protocol.
0x88CC	LLDP, Link Layer Discovery Protocol.
0x8E88	EAPOL, EAP over LAN.
0x9000	Loopback (Configuration Test Protocol)
0xFFFF	reserved.

- VLAN ID:  
The configurable VID range: 1~4094
- UDP/TCP Port:  
To select the UDP/TCP port classification method by Range or Specific.  
UDP/TCP Port Range:  
The configurable ports range: 0~65.535  
You can refer to following UDP/TCP port-numbers information.  
<http://www.iana.org/assignments/port-numbers>  
UDP/TCP Port No.:  
The configurable specific port value: 0~65.535
- DSCP Value:  
The configurable DSCP value: 0~63
- Traffic Class:  
Low / Normal / Medium / High

### 4.12.3 Rate Limiters

**Rate Limit Configuration**

Port #	Ingress Enabled	Ingress Rate	Ingress Unit	Egress Enabled	Egress Rate	Egress Unit
1	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
2	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
3	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
4	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
5	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
6	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
7	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
8	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
9	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
10	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
11	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
12	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
13	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
14	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
15	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
16	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
17	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
18	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
19	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
20	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
21	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
22	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
23	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
24	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs

**Apply**

#### ■ Rate Limit Configuration

Each port includes an ingress policer, and an egress shaper, which can limit the bandwidth of received and transmitted frames. Ingress policer or egress shaper operation is controlled per port in the Rate Limit Configuration.

#### ■ Parameter:

- Port #: Port number.
- Policer Enabled: Policer enabled to limit ingress bandwidth by policer rate.

## ■ Chapter 4: Operation of Web-based Management

- **Policer Rate:**  
The configurable policer rate range:  
500 Kbps ~ 1000000 Kbps  
1 Mbps ~ 1000 Mbps
- **Policer Unit:**  
There are two units for ingress policer rate limit: kbps / Mbps
- **Shaper Enabled:**  
Shaper enabled to limit egress bandwidth by shaper rate.
- **Shaper Rate:**  
The configurable shaper rate range:  
500 Kbps ~ 1000000 Kbps  
1 Mbps ~ 1000 Mbps
- **Shaper Unit:**  
There are two units for egress shaper rate limit: kbps / Mbps

### 4.12.4 Storm Control

#### Storm Control Configuration

Frame Type	Status	Rate (pps)
Flooded unicast	<input type="checkbox"/>	1
Multicast	<input type="checkbox"/>	1
Broadcast	<input type="checkbox"/>	1

[Apply](#)

- **Storm Control Configuration**  
The switch support storm ingress policer control function to limit the Flooded, Multicast and Broadcast to prevent storm event happen.
- **Parameter:**
  - **Frame Type:**  
There three frame types of storm can be controlled: Flooded unicast / Multicast / Broadcast
  - **Status:**  
Enable/Disable Selection: a checkmark in the box means enabled, no checkmark in the box means disabled

- Rate(pps):  
Refer to the following rate configurable value list, the unit is Packet Per Second (pps).  
1 / 2 / 4 / 8 / 16 / 32 / 64 / 128 / 256 / 512 / 1K / 2K / 4K / 8K / 16K / 32K / 64K / 128K / 256K / 512K / 1024K

### 4.12.5 Wizard

**Welcome to the QCL Configuration Wizard!**

**Please select an action:**

- Set up Port Policies**  
Group ports into several types according to different QCL policies.
- Set up Typical Network Application Rules**  
Set up the specific QCL for different typical network application quality control.
- Set up TOS Precedence Mapping**  
Set up the traffic class mapping to the precedence part of TOS (3 bits) when receiving IPv4/IPv6 packets.
- Set up VLAN Tag Priority Mapping**  
Set up the traffic class mapping to the user priority value (3 bits) when receiving VLAN tagged packets.

To continue, click Next.

[Next >](#)

#### ■ Wizard

The QCL configuration Wizard is targeted on user can easy to configure the QCL rules for QoS configuration. The wizard provide the typical network application rules, user can apply these application easily.

#### ■ Parameter:

- Please select an Action:  
User need to select one of action from following items, then click on <Next> to finish QCL configuration:  
Set up Port Policies  
Set up Typical Network Application Rules  
Set up TOS Precedence Mapping  
Set up VLAN Tag Priority Mapping
- Next:  
Go to next step.



- Cancel:  
Abort current configuration back to previous step.
- Back:  
Back to previous screen.
- QCL ID:  
QoS Control List (QCL): 1~24
- Port Member:  
Port Member: 1~24
- Wizard Again:  
Click on the <Wizard Again> , back to QCL Configuration Wizard.
- Finish:  
When you click on <Finish>, the parameters will be set according to the wizard configuration and shown on the screen, then ask you to click on <Apply> for changed parameters confirmation.
- Audio and Video:  
QuickTime 4 Server / MSN Messenger Phone / Yahoo Messenger Phone / Napster / Real Audio
- Games:  
Blizzard Battlenet (Diablo2 and StarCraft) / Fighter Ace II / Quake2 / Quake3 / MSN Game Zone
- User Definition:  
Ethernet Type / VLAN ID / UDP/TCP Port / DSCP  
Ethernet Type Value: Type Range: 0x600~0xFFFF  
VLAN ID: VLAN ID Range: 1~4094  
UDP/TCP Port: Two Mode: Range / Specific  
UDP/TCP Port Range: Port Range: 0~65535  
UDP/TCP Port No.: Port Range: 0~65535  
DSCP Value: DSCP Value Range: 0~63
- QCL ID:  
QCL ID Range: 1~24
- Traffic Class:  
There are four classes: Low / Normal / Medium / High

- QCL #:
  - QoS Control List (QCL): 1~24
- QCL ID:
  - QoS Control List (QCL): 1~24
- TOS Precedence 0~7 Class:
  - Low / Normal / Medium / High
- QCL ID:
  - QoS Control List (QCL): 1~24
- Tag Priority 0~7 Class:
  - Low / Normal / Medium / High

### 4.13 Configuration: Trunk

The Port Trunking Configuration is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipments to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port has.

The switch supports two kinds of port trunking methods:

#### 1 LACP:

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP GroupID (1~3) to form a logic "trunked port". The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a "trunk group" (also called aggregator). LACP is safer than the other trunking method - static trunk.

The switch LACP does not support the followings:

- Link Aggregation across switches
- Aggregation with non-IEEE 802.3 MAC link
- Operating in half-duplex mode
- Aggregate the ports with different data rates

#### 2 Static Trunk:

Ports using Static Trunk as their trunk method can choose their unique Static GroupID (also 1~3, this Static groupID can be the same with another LACP groupID) to form a logic "trunked port". The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregate together to form a "logic trunked port". Using Static Trunk on both end of a link is strongly recommended. Please also note that low speed links will stay in "not ready" state when using static trunk to aggregate with high speed links.

As to system restrictions about the port aggregation function on the switch, in the management point of view, the switch supports maximum 3 trunk groups for LACP and additional 3 trunk groups for Static Trunk. But in the system capability view, only 3 "real trunked" groups are supported. An LACP trunk group with more than one ready member-ports is a "real trunked" group. An LACP trunk group with only one or less than one ready member-ports is not a "real trunked" group. Any Static trunk group is a "real trunked" group.

Per Trunking Group supports a maximum of 12 ready member-ports. Please note that some decisions will automatically be made by the system while you are configuring your trunking ports. Some configuration examples are listed below:

- ① 12 ports have already used Static Trunk Group ID 1, the 13th port willing to use the same Static Trunk Group ID will be automatically set to use the "None" trunking method and its Group ID will turn to 0. This means the port won't aggregate with other ports.
- ② 14 ports all use LACP Trunk Group ID 1 at most 12 ports can aggregate together and transit into the ready state.
- ③ A port using the "None" trunking method or Group ID 0 will be automatically set to use the "None" trunking method with Group ID 0.

### 4.13.1 Port

#### Trunk Port Setting/Status

Port	Trunk Port Setting			Trunk Port Status	
	Method	Group	Active LACP	Aggr	Status
1	None	0	Active	1	Ready
2	None	0	Active	2	Ready
3	None	0	Active	3	Ready
4	None	0	Active	4	---
5	None	0	Active	5	---
6	None	0	Active	6	---
7	None	0	Active	7	---
8	None	0	Active	8	---
9	None	0	Active	9	---
10	None	0	Active	10	---
11	None	0	Active	11	---
12	None	0	Active	12	---
13	None	0	Active	13	---
14	None	0	Active	14	Ready
15	None	0	Active	15	Ready
16	None	0	Active	16	Ready
17	None	0	Active	17	---
18	None	0	Active	18	---
19	None	0	Active	19	---
20	None	0	Active	20	---
21	None	0	Active	21	---
22	None	0	Active	22	---
23	None	0	Active	23	---
24	None	0	Active	24	---

Apply/Refresh

- Trunk Port Setting/Status  
Port setting/status is used to configure the trunk property of each and every port in the switch system.
- Parameter:
  - Port:  
Port Number: 1-24

- Method:

This determines the method a port uses to aggregate with other ports.

None: A port does not want to aggregate with any other port should choose this default setting.

LACP: A port use LACP as its trunking method to get aggregated with other ports also using LACP.

Static: A port use Static Trunk as its trunking method to get aggregated with other ports also using Static Trunk.
- Group:

Ports choosing the same trunking method other than "None" must be assigned a unique Group number (i.e. Group ID, valid value is from 1 to 8) in order to declare that they wish to aggregate with each other.
- Active LACP:

This field is only referenced when a port's trunking method is LACP.

Active:

An Active LACP port begins to send LACPDU to its link partner right after the LACP protocol entity started to take control of this port.

Passive:

A Passive LACP port will not actively send LACPDU out before it receives an LACPDU from its link partner.
- Aggtr:

Aggtr is an abbreviation of "aggregator". Every port is also an aggregator, and its own aggregator ID is the same as its own Port No. We can regard an aggregator as a representative of a trunking group. Ports with same Group ID and using same trunking method will have the opportunity to aggregate to a particular aggregator port. This aggregator port is usually the port with the smallest Port No. within the trunking group.
- Status:

This field represents the trunking status of a port which uses a trunking method other than "None". It also represents the management link status of a port which uses the "None" trunking method. "---" means "not ready".

### Trunk Port Setting/Status [Setting Rule](#)

Port	Trunk Port Setting			Trunk Port Status	
	Method	Group	Active LACP	Aggtr	Status
1	None ▾	0 ▾	Active ▾	1	---
2	None ▾	0 ▾	Active ▾	2	Ready
3	None ▾	0 ▾	Active ▾	3	---
4	None ▾	0 ▾	Active ▾	4	---
5	None ▾	0 ▾	Active ▾	5	---
6	None ▾	0 ▾	Active ▾	6	---
7	None ▾	0 ▾	Active ▾	7	---
8	None ▾	0 ▾	Active ▾	8	---
9	None ▾	0 ▾	Active ▾	9	---
10	None ▾	0 ▾	Active ▾	10	---
11	None ▾	0 ▾	Active ▾	11	---

## 4.13.2 Aggregator View

Aggregator	Method	Member Ports	Ready Ports
1	None	1	1
2	None	2	2
3	None	3	3
4	None	4	
5	None	5	
6	None	6	
7	None	7	
8	None	8	
9	None	9	
10	None	10	
11	None	11	
12	None	12	
13	None	13	
14	None	14	14
15	None	15	15
16	None	16	16
17	None	17	
18	None	18	
19	None	19	
20	None	20	
21	None	21	
22	None	22	
23	None	23	
24	None	24	

Refresh LACP Detail

### ■ Aggregator view

To display the current port trunking information from the aggregator point of view.

### ■ Parameter:

#### □ Aggregator:

It shows the aggregator ID (from 1 to 26) of every port. In fact, every port is also an aggregator, and its own aggregator ID is the same as its own Port No..

#### □ Method:

Show the method a port uses to aggregate with other ports.

- Member Ports:  
Show all member ports of an aggregator (port).
- Ready Ports:  
Show only the ready member ports within an aggregator (port).

**Aggregator View**

Aggregator	Method	Member Ports	Ready Ports
1	None	1	
2	None	2	2
3	None	3	
4	None	4	
5	None	5	
6	None	6	
7	None	7	
8	None	8	
9	None	9	
10	None	10	
11	None	11	
12	None	12	
13	None	13	
14	None	14	
15	None	15	

### 4.13.3 Hash Method

**Aggregation Mode Configuration**

Hash Code Contributors	
Source MAC Address	<input checked="" type="checkbox"/>
Destination MAC Address	<input type="checkbox"/>
IP Address	<input checked="" type="checkbox"/>
TCP/UDP Port Number	<input checked="" type="checkbox"/>

**Apply**

DA+SA, DA and SA are three Hash methods offered for the Link Aggregation of the switch. Packets will decide the path to transmit according to the mode of Hash you choose.

Default: DA and SA



#### 4.13.4 LACP System Priority

### LACP System Priority

<b>System Priority</b>	32768 (1~65535)
<input type="button" value="Apply"/>	

#### ■ LACP System Priority

It is used to set the priority part of the LACP system ID. LACP will only aggregate together the ports whose peer link partners are all on a single system. Each system supports LACP will be assigned a globally unique System Identifier for this purpose. A system ID is a 64-bit field comprising a 48-bit MAC Address and 16-bit priority value.

#### ■ Parameter:

##### System Priority:

The System Priority can be set by the user. Its range is from 1 to 65.535. Default: 32.768

### 4.14 Configuration: STP

The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in switched networks. When STP is enabled, ensure that only one path is active between any two nodes on the network at a time. User can enable Spanning Tree Protocol on switch's web management and then set up other advanced items. We recommend that you enable STP on all switches to ensure a single active path on the network.

### 4.14.1 STP Status

STP Status	
STP State	Disabled
Bridge ID	00:40:C7:5C:00:73
Bridge Priority	32768
Designated Root	00:40:C7:5C:00:73
Designated Priority	32768
Root Port	0
Root Path Cost	0
Current Max. Age(sec)	20
Current Forward Delay(sec)	15
Hello Time(sec)	2
STP Topology Change Count	0
Time Since Last Topology Change(sec)	0

#### ■ STP Status

In the Spanning Tree Status, user can read 12 parameters to know STP current status. The 12 parameters' description is listed in the following table.

#### ■ Parameter:

- STP State:  
Show the current STP Enabled / Disabled status. Default is "Disabled".
- Bridge ID:  
Show switch's bridge ID which stands for the MAC address of this switch.
- Bridge Priority:  
Show this switch's current bridge priority setting. Default is 32.768.
- Designated Root:  
Show root bridge ID of this network segment. If this switch is a root bridge, the "Designated Root" will show this switch's bridge ID.
- Designated Priority:  
Show the current root bridge priority.
- Root Port:  
Show port number connected to root bridge with the lowest path cost.

- Root Path Cost:  
Show the path cost between the root port and the designated port of the root bridge.
- Current Max. Age:  
Show the current root bridge maximum age time. Maximum age time is used to monitor if STP topology needs to change. When a bridge does not receive a hello message from root bridge until the maximum age time is counted down to 0, the bridge will treat the root bridge malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges.  
  
All bridges in the LAN will re-learn and determine which the root bridge is. Maximum Age time is assigned by root bridge in unit of seconds. Default is 20 seconds.
- Current Forward Delay:  
Show the current root bridge forward delay time. The value of Forward Delay time is set by root. The Forward Delay time is defined as the time spent from Listening state moved to Learning state or from Learning state moved to Forwarding state of a port in bridge.
- Hello Time:  
Show the current hello time of the root bridge. Hello time is a time interval specified by root bridge, used to request all other bridges periodically sending hello message every "hello time" seconds to the bridge attached to its designated port.
- STP Topology Change Count:  
STP Topology Change Count expresses the time spent in unit of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once the STP change is converged, the Topology Change count will be reset to 0. The figures showing in the screen may not be the exact time it spent but very close to, because the time is eclipsing.
- Time Since Last Topology Change:  
Time Since Last Topology Change is the accumulated time in unit of seconds the STP has been since the last STP Topology Change was made. When Topology Change is initiated again, this counter will be reset to 0. And it will also count again once STP topology Change is completed.

## 4.14.2 Configuration

### STP Configuration

Spanning Tree Protocol	Disable ▾
Bridge Priority (0-61440)	32768 ▾
Hello Time (1-10 sec)	2
Max. Age (6-40 sec)	20
Forward Delay (4-30 sec)	15
Force Version	RSTP ▾

**Note:**  $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$   
 $\text{Max Age} \geq 2 * (\text{Hello Time} + 1)$

Apply

**Note:** You will lose connection with this device for a while if you enable STP.

The STP, Spanning Tree Protocol, actually includes RSTP. In the Spanning Tree Configuration, there are six parameters open for the user to configure as user's idea. Each parameter description is listed below.

### ■ STP Configuration

User can set the following Spanning Tree parameters to control STP function enable/disable, select mode RSTP/STP and affect STP state machine behavior to send BPDU in this switch. The default setting of Spanning Tree Protocol is "Disable".

### ■ Parameter:

- Spanning Tree Protocol:  
Set 802.1W Rapid STP function Enable / Disable. Default is "Disable"
- Bridge Priority:  
The lower the bridge priority is, the higher priority it has. Usually, the bridge with the highest bridge priority is the root. If you want to have the LANCOM Switch as root bridge, you can set this value lower than that of bridge in the LAN. The valid value is 0 ~ 61.440. The default is 32.768.
- Hello Time:  
Hello Time is used to determine the periodic time to send normal BPDU from designated ports among bridges. It decides how long a bridge should send this message to other bridge to tell I am alive.

When the LANCOM Switch is the root bridge of the LAN, for example, all other bridges will use the hello time assigned by this switch to communicate with each other. The valid value is 1 ~ 10 in unit of second. Default is 2 seconds.

□ Max. Age:

When the LANCOM Switch is the root bridge, the whole LAN will apply this figure set by this switch as their maximum age time. When a bridge received a BPDU originated from the root bridge and if the message age conveyed in the BPDU exceeds the Max. Age of the root bridge, the bridge will treat the root bridge malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges. All bridges in the LAN will re-calculate and determine who the root bridge is. The valid value of Max. Age is 6 ~ 40 seconds. Default is 20 seconds.

□ Forward Delay:

You can set the root bridge forward delay time. This figure is set by root bridge only. The forward delay time is defined as the time spent from Listening state moved to Learning state and also from Learning state moved to Forwarding state of a port in bridge. The forward delay time contains two states, Listening state to Learning state and Learning state to Forwarding state. It assumes that forward delay time is 15 seconds, then total forward delay time will be 30 seconds. This has much to do with the STP convergent time which will be more than 30 seconds because some other factors. The valid value is 4 ~ 30 seconds, default is 15 seconds.

□ Force Version:

Two options are offered for the user's choosing STP algorithm. One is RSTP and the other is STP. If STP is chosen, RSTP will run as a legacy STP. The switch supports RSTP (802.1w) which is backward compatible with STP (802.1d).

### 4.14.3 Port

#### STP Port Configuration

Port No	Port Status	Path Cost Status	Configured Path Cost	Priority	Admin Port Type	Admin Point To Point
1	FORWARDING	2000000	0	128	Normal	Auto
2	FORWARDING	2000000	0	128	Normal	Auto
3	FORWARDING	2000000	0	128	Normal	Auto
4	FORWARDING	2000000	0	128	Normal	Auto
5	FORWARDING	2000000	0	128	Normal	Auto
6	FORWARDING	2000000	0	128	Normal	Auto
7	FORWARDING	2000000	0	128	Normal	Auto
8	FORWARDING	2000000	0	128	Normal	Auto
9	FORWARDING	2000000	0	128	Normal	Auto
10	FORWARDING	2000000	0	128	Normal	Auto
11	FORWARDING	2000000	0	128	Normal	Auto
12	FORWARDING	2000000	0	128	Normal	Auto
13	FORWARDING	2000000	0	128	Normal	Auto
14	FORWARDING	2000000	0	128	Normal	Auto
15	FORWARDING	2000000	0	128	Normal	Auto
16	FORWARDING	2000000	0	128	Normal	Auto
17	FORWARDING	2000000	0	128	Normal	Auto
18	FORWARDING	2000000	0	128	Normal	Auto
19	FORWARDING	2000000	0	128	Normal	Auto
20	FORWARDING	2000000	0	128	Normal	Auto
21	FORWARDING	2000000	0	128	Normal	Auto
22	FORWARDING	2000000	0	128	Normal	Auto
23	FORWARDING	2000000	0	128	Normal	Auto
24	FORWARDING	2000000	0	128	Normal	Auto



#### ■ STP Port Setting

In the STP Port Setting, one item selection and five parameters settings are offered for user's setup. User can disable and enable each port by selecting each Port Status item. User also can set "Path Cost" and "Priority" of each port by filling in the desired value and set "Admin Edge Port" and "Admin Point To Point" by selecting the desired item.

## ■ Parameter:

## □ Port Status:

It displays the current state of a port. We cannot manually set it because it displays the status only. There are three possible states. (according to 802.1w specification)

“Discarding State” indicates that this port can neither forward packets nor contribute learning knowledge.

Notice: Three other states (“disable state”, “blocking state” and “listening state”) defined in the 802.1d specification are now all represented as “discarding state”.

“Learning state” indicates this port can now contribute its learning knowledge but cannot forward packets still.

“Forwarding state” indicates this port can both contribute its learning knowledge and forward packets normally.

## □ Path Cost Status:

It is the contribution value of the path through this port to Root Bridge. STP algorithm determines a best path to Root Bridge by calculating the sum of path cost contributed by all ports on this path. A port with a smaller path cost value would become the Root Port more possibly.

## □ Configured Path Cost:

The range is 0 – 200.000.000. In the switch, if path cost is set to be zero, the STP will get the recommended value resulted from auto-negotiation of the link accordingly and display this value in the field of Path Cost Status. Otherwise, it may show the value that the administrator set up in Configured Path Cost and Path Cost Status.

802.1w RSTP recommended value: (Valid range: 1 – 200.000.000)

10 Mbps : 2.000.000

100 Mbps : 200.000

1 Gbps : 20.000

Default : 0

## □ Priority:

Priority here means Port Priority. Port Priority and Port Number are mixed to form the Port ID. Port IDs are often compared in order to

determine which port of a bridge would become the Root Port. The range is 0 – 240. Default is 128.

□ Admin Edge Port:

If user selects “Yes”, this port will be an edge port. An Edge Port is a port connected to a device that knows nothing about STP or RSTP. Usually, the connected device is an end station. Edge Ports will immediately transit to forwarding state and skip the listening and learning state because the edge ports cannot create bridging loops in the network. This will expedite the convergence. When the link on the edge port toggles, the STP topology keeps unchanged. Unlike the designate port or root port though, an edge port will transit to a normal spanning-tree port immediately if it receives a BPDU. Default: No

□ Admin Point To Point:

Say a port is a point-to-point link, from RSTP’s view, if it is in full-duplex mode but is shared link if it is in half-duplex mode. RSTP fast convergence can only happen on point-to-point links and on edge ports. This can expedite the convergence because this will have the port fast transitioned to forwarding state.

There are three parameters, Auto, True and False, used to configure the type of the point-to-point link. If configure this parameter to be Auto, it means RSTP will use the duplex mode resulted from the auto-negotiation. In today’s switched networks, most links are running in full-duplex mode. For sure, the result may be half-duplex, in this case, the port will not fast transit to Forwarding state. If it is set as True, the port is treated as point-to-point link by RSTP and unconditionally transitioned to Forwarding state. If it is set as False, fast transition to Forwarding state will not happen on this port. Default: Auto

□ M Check:

Migration Check. It forces the port sending out an RSTP BPDU instead of a legacy STP BPDU at the next transmission. The only benefit of this operation is to make the port quickly get back to act as an RSTP port. Click <M Check> button to send a RSTP BPDU from the port you specified.

## 4.15 Configuration: MSTP

The implementation of MSTP is according to IEEE 802.1Q 2005 Clause 13 - Multiple Spanning Tree Protocol. MSTP allows frames assigned to different



VLANs to follow separate paths, each based on an independent Multiple Spanning Tree Instance (MSTI), within Multiple Spanning Tree (MST) Regions composed of LANs and or MST Bridges. Proper configuration of MSTP in an 802.1Q VLAN environment can ensure a loop-free data path for a group of VLANs within an MSTI. Redundant path and load balancing in VLAN environment is also achieved via this feature. A spanning tree instance called CIST (Common and Internal Spanning Tree) always exists. Up to 64 more spanning tree instances (MSTIs) can be provisioned.

### 4.15.1 Status

#### MSTP State

<b>Multiple Spanning Tree Protocol</b>	Disable ▾
<b>Force Version</b>	MSTP ▾

**Apply**

- **MSTP State**  
To enable or disable MSTP. And to select a version of Spanning Tree protocol which MSTP should operate on.
- **Parameter:**
  - Multiple Spanning Tree Protocol:  
Disabled / Enabled
  - Force Version:  
STP / RSTP / MSTP

### 4.15.2 Region Config

#### MSTP Region Config

<b>Region Name (0~32 characters)</b>	mstpRegion1
<b>Revision Level (0-65535)</b>	0

**Apply**

- **MSTP Region Config**  
To configure the basic identification of a MSTP bridge. Bridges participating in a common MST region must have the same Region Name and Revision Level.

- Parameter:
  - Region Name:
    - 0-32 characters.(A variable length text string encoded within a fixed field of 32 octets , conforming to RFC 2271's definition of SnmpAdminString.)
  - Revision Level:
    - 0-65.535

### 4.15.3 Instance View

MSTP Instance Config	
Instance ID	Corresponding Vlans
0	1-4094

Edit MSTI/Vlan
Del MSTI
Del All MSTI

Instance Config
Port Config
Instance Status
Port Status

- MSTP Instance Config
 

Providing an MST instance table which include information (VLAN membership of a MSTI ) of all spanning instances provisioned in the particular MST region which the bridge belongs to. Through this table, additional MSTP configuration data can be applied and MSTP status can be retrieved.
- Parameter:
  - Instance ID:
    - Every spanning tree instance need to have a unique instance ID within 0~4095. Instance 0 (CIST) always exists and can not be deleted. Additional spanning instances (MSTIs) can be added or deleted. At least one VLAN must be provisioned for an MSTI to declare the need for the MSTI to be existent.

- Corresponding VLANs:  
0-4095.  
Multiple VLANs can belong to an MSTI. All VLANs that are not provisioned through this will be automatically assigned to Instance 0(CIST).
- Edit MSTI / VLAN:  
See Figure. To add an MSTI and provide its VLAN members or modify VLAN members for a specific MSTI.
- Del MSTI:  
To delete an MSTI.
- Del All MSTI:  
Deleting all provisioned MSTIs at a time.
- Instance Configuration:  
See Figure. To provision spanning tree performance parameters per instance.
- Port Config:  
See Figure. To provision spanning tree performance parameters per instance per port.
- Instance Status:  
See Figure. To show the status report of a particular spanning tree instance.
- Port Status:  
See Figure. To show the status report of all ports regarding a specific spanning tree instance.
- VLAN Mapping:  
VID STRING
- VID STRING Example:  
2.5-7.100-200.301.303.1000-1500 (Valid VID Range:1-4094)
- Priority:  
The priority parameter used in the CIST(Common and Internal Spanning Tree) connection.  
0 / 4096 / 8192 / 12288 / 16384 / 20480 / 24576 / 28672 / 32768 / 36864 / 40960 / 45056 / 49152 / 53248 / 57344 / 61440

- MAX. Age:  
6-40sec. The same definition as in the RSTP protocol.
- Forward Delay:  
4-30sec. The same definition as in the RSTP protocol.
- MAX. Hops:  
6-40sec. It's a new parameter for the multiple spanning tree protocol. It is used in the internal spanning tree instances. "CIST Remaining Hops" or "MSTI Remaining Hops" in the Spanning tree protocol message would decrease by one when the message is propagated to the neighboring bridge. If the Remaining Hops in a message is zero, the message (BPDU) would be regarded as invalid. Max Hops is used to specify the initial value of the Remaining Hops for Regional Root Bridge (Either CIST Regional Root or MSTI Regional Root)
- Port:  
1-24
- Path Cost:  
1 - 200,000,000.  
  
The same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.
- Priority:  
0 / 16 / 32 / 48 / 64 / 80 / 96 / 112 / 128 / 144 / 160 / 176 / 192 / 208 / 224 / 240  
  
The same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.
- Hello Time:  
1 / 2. In contrast with RSTP, Hello Time in MSTP is a per port setting for the CIST.
- Admin Edge:  
Yes / No. The same definition as in the RSTP specification for the CIST ports.
- Admin P2P:  
Auto / True / False. The same definition as in the RSTP specification for the CIST ports.

- **Restricted Role:**  
Yes / No. If "Yes" causes the Port not to be selected as Root Port for the CIST or any MSTI, even it has the best spanning tree priority vector. Such a Port will be selected as an Alternate Port after the Root Port has been selected. This parameter is "No" by default. If set, it can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.
- **Restricted TCN:**  
Yes / No. If "Yes" causes the Port not to propagate received topology change notifications and topology changes to other Ports. This parameter is "No" by default. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator. or the status of MAC operation for the attached LANs transitions frequently.
- **Mcheck:**  
The same definition as in the RSTP specification for the CIST ports.
- **MSTP State:**  
MSTP protocol is Enable or Disable.
- **Force Version:**  
It shows the current spanning tree protocol version configured.
- **Bridge Max Age:**  
It shows the Max Age setting of the bridge itself.
- **Bridge Forward Delay:**  
It shows the Forward Delay setting of the bridge itself.
- **Bridge Max Hops:**  
It shows the Max Hops setting of the bridge itself.
- **Instance Priority:**  
Spanning tree priority value for a specific tree instance(CIST or MSTI).

- Bridge Mac Address:  
The Mac Address of the bridge itself.
- CIST ROOT PRIORITY:  
Spanning tree priority value of the CIST root bridge.
- CIST ROOT MAC:  
Mac Address of the CIST root bridge.
- CIST EXTERNAL ROOT PATH COST:  
Root path cost value from the point of view of the bridge's MST region.
- CIST ROOT PORT ID:  
The port ID of the bridge's root port. In MSTP, peer port of a root port may reside in different MST region or in the same MST region. The first case indicates that the root port's owner is the CIST regional root bridge.
- CIST REGIONAL ROOT PRIORITY:  
Spanning tree priority value of the CIST regional root bridge. Note that CIST Regional Root bridge is different from CIST Root bridge. One exception is that when a bridge belonging to an MST region happens to be the root bridge of the CST (Common Spanning Tree). An MST Region in the CST can be regarded as a common RSTP bridge. The IST (Internal Spanning Tree) and MSTIs are transparent to bridges outside this region.
- CIST REGIONAL ROOT MAC:  
Mac Address of the CIST regional root bridge.
- CIST INTERNAL ROOT PATH COST:  
Root path cost value from the point of view of the bridges inside the IST.
- CIST CURRENT MAX AGE:  
Max Age of the CIST Root bridge.
- CIST CURRENT FORWARD DELAY:  
Forward Delay of the CIST Root bridge.
- TIME SINCE LAST TOPOLOGY CHANGE (SECS):  
Time Since Last Topology Change is the elapsed time in unit of seconds for a bunch of "Topology Change and(or) Topology Change

Notification receiving" to occur. When new series of Topology Changes occur again, this counter will be reset to 0.

- TOPOLOGY CHANGE COUNT(SECs):  
The per spanning tree instance Topology Change Count expresses the time spent in unit of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once there is no topology change occurring and no more topology change notification received, the Topology Change count will be reset to 0.
- Port No:  
1-24
- Status:  
The forwarding status. Same definition as of the RSTP specification  
Possible values are "FORWARDING" , "LEARNING" , "DISCARDING"
- Status:  
The role that a port plays in the spanning tree topology. Possible values are "dsbl"(disable port) , "alt"(alternate port) , "bkup"(backup port) , "ROOT"(root port) , "DSGN"(designated port) , "MSTR"(master port). The last 3 are possible port roles for a port to transit to FORWARDING state
- Path Cost:  
Display currently resolved port path cost value for each port in a particular spanning tree instance.
- Priority:  
Display port priority value for each port in a particular spanning tree instance.
- Hello:  
Per port Hello Time display. It takes the following form: Current Hello Time/Hello Time Setting
- Oper. Edge:  
Whether or not a port is an Edge Port in reality.
- Oper. P2P:  
Whether or not a port is a Point-to-Point Port in reality.
- Restricted Role:  
Same as mentioned in "Port Config".

- Restricted Tcn:  
Same as mentioned in "Port Config"

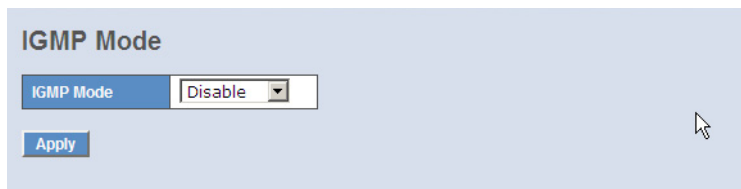
## 4.16 Configuration: Multicast

The function, IGMP Snooping, is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping can not tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch supported IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance.

### 4.16.1 IGMP Mode



Select the IGMP operating mode IGMP for multicast.

#### ■ Parameter Description

- IGMP Mode
  - Disable: Set "Disable" mode to disable IGMP function.
  - Proxy: Set "Proxy" to enable the IGMP Proxy for multicast pakets.
  - Snooping: Set "Snooping" to enable the IGMP Snooping for multicast pakets.



## 4.16.2 Proxy

IGMP proxy enables the switch to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The switch acts as a proxy for its hosts.

You enable IGMP proxy on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

### IGMP Proxy Configuration

General Query Interval	125	(seconds: 1 ~ 3600)
General Query Response Timeout	11	(seconds: 1 ~ 25)
General Query Max Response Time	10	(seconds: 1 ~ 25)
Last Member Query Count	2	(times: 1 ~ 16)
Last Member Query Interval	3	(seconds: 1 ~ 25)
Last Member Query Max Response Time	1	(seconds: 1 ~ 25)

Router Ports															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
<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"/>

#### ■ Parameter

- General Query Interval: :  
To set the switch send general query period time. (Available : 1~3600 secs)
- General Query Response Timeout :  
To set the switch determine the client living time. (Available : 1~25 secs)
- General Query Max Response Time :  
To set the max response code value of the general query packet . (Available : 1~25 secs)
- Last Member Query Count :  
To set the frequency. When Switch received IGMP leave then switch send specific query frequency. (Available : 1~16 secs)
- Last Member Query Interval :  
To set the frequency what the Switch send specific query period time. (Available : 1~25 secs)

- Last Member Query Max Response Time :  
To set the max response code value in the specific query packet (Available : 1~25 secs)
- Update Interval of Router Port :  
To set the period time what interface ever received IGMP query packet. (Available : 1~3600 secs)
- Router Ports:  
To set the interface what connect to IGMP Router, and it is the switch what it send/receive IGMP report/leave port. Router ports may be only or more than one.
- Apply:  
To save all configuration.

### 4.16.3 Snooping

#### IGMP snooping Configuration

Host Time Out  (seconds: 1 ~ 65535)

Fast Leave															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
<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"/>

Router Ports															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
<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"/>

Here you can enable the IGMP snooping for certain ports.

- Parameter description
  - Fast Leave: These ports are monitored by the switch for IGMP messages from hosts, which are leaving a multicast group.
  - Router Ports: These ports are monitored by the switch for IGMP messages from routers.

### 4.16.4 IGMP Group Membership

To show the IGMP group members information, the you can edit the parameters for IGMP groups and members in the web user interface.

### IGMP Group Membership

Index	Group Address	VLAN ID	Port Members															
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
			<a href="#">Previous Page</a>			<a href="#">Next Page</a>			<a href="#">Refresh</a>									

- Parameter
  - IGMP Group Membership:  
To display current built-up multicast group entry.
  - Previous Page:  
To display previous page context.
  - Next Page:  
To display next page context.
  - Refresh:  
To Update multicast group membership.

## 4.17 Management: Alarm Configuration

### 4.17.1 Events

#### Trap Events Configuration

Email Select/Unselect All

Trap Select/Unselect All

Event	Email	Trap
Cold Start	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Warm Start	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Link Down	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Link Up	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Authentication Failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Login	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Logout	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Module Inserted	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Module Removed	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Dual Media Swapped	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Looping Detected	<input checked="" type="checkbox"/>	<input type="checkbox"/>
STP Disabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>
STP Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>

#### ■ Events Configuration

The Trap Events Configuration function is used to enable the switch to send out the trap information while pre-defined trap events occurred. The switch offers 22 different trap events to users for switch management. The trap information can be sent out in three ways, including email, mobile phone SMS (short message system) and trap. The message will be sent while users tick (ž) the trap event individually on the web page shown as below.

#### ■ Parameter:

- Trap:  
Cold Start, Warm Start, Link Down, Link Up, Authentication Failure, User login, User logout
- STP:  
STP Topology Changed, STP Disabled, STP Enabled

- LACP:  
LACP Disabled, LACP Enabled, LACP Member Added, LACP Port Failure
- GVRP:  
GVRP Disabled, GVRP Enabled
- VLAN:  
Port-based VLAN Enabled, Tag-based VLAN Enabled
- Module Swap:  
Module Inserted, Module Removed, Dual Media Swapped

## 4.17.2 Email

Alarm Configuration	
Mail Server	10.1.1.1
User Name	
Password	*****
Sender	
Email Address 1	mp@lancom.de
Email Address 2	
Email Address 3	
Email Address 4	
Email Address 5	
Email Address 6	

### ■ Email/SMS Configuration

Alarm configuration is used to configure the persons who should receive the alarm message via either email or SMS, or both. It depends on your settings. An email address or a mobile phone number has to be set in the web page of alarm configuration. Then, user can read the trap information from the email or the mobile phone. This function provides 6 email addresses and 6 mobile phone numbers at most. The 22 different trap events will be sent out to SNMP Manager when trap event occurs. After ticking trap events, you can fill in your desired email addresses and mobile phone numbers. Then, please click <Apply> button to complete the alarm configuration. It will take effect in a few seconds.

Note: SMS may not work in your mobile phone system. It is customized for different systems.

- Parameter:
  - Email:
    - Mail Server: the IP address of the server transferring your email.
    - Username: your username on the mail server.
    - Password: your password on the mail server.
    - Email Address 1 – 6: email address that would like to receive the alarm message.
  - SMS:
    - SMS Server: the IP address of the server transferring your SMS.
    - Username: your username in ISP.
    - Password: your username in ISP.
    - Mobile Phone 1-6: the mobile phone number that would like to receive the alarm message.

## 4.18 Management: Diagnostics

These are functions for device self-diagnostics. Each of them will be described in detail orderly in the following sections.

### 4.18.1 Diag

Diagnostics	
EEPROM Test	OK
UART Test	OK
DRAM Test	OK
Flash Test	OK
<a href="#">Run</a>	

- Diagnostics
 

Diagnostics function provides a set of basic system diagnosis. It let users know that whether the system is health or needs to be fixed. The basic system check includes EEPROM test, UART test, DRAM test and Flash test.

## 4.18.2 Ping

**ICMP Ping**

IP Address

Ping size

**Start**

### ■ Ping Test

Ping Test function is a tool for detecting if the target device is alive or not through ICMP protocol which abounds with report messages. The switch provides Ping Test function to let you know that if the target device is available or not. You can simply fill in a known IP address and then click <Ping> button. After a few seconds later, the switch will report you the pinged device is alive or dead in the field of Ping Result.

### ■ Parameter:

- IP Address:  
An IP address with the version of v4, e.g. 192.168.1.1.
- Default Gateway:  
IP address of the default gateway.

## 4.19 Management: Maintenance

This chapter will introduce the reset and firmware upgrade function for the firmware upgrade and key parameters change system maintenance requirements.

### 4.19.1 Reset device

**Warm Restart**

**Are you sure you want to perform a Warm Restart?**

**Yes**

We offer you many ways to reset the device, including power up, hardware reset and software reset. You can press the RESET button in the front panel to reset the switch. After upgrading software, changing IP configuration or

changing VLAN mode configuration, you must reboot to have the new configuration taken in effect. Here we are discussing the software reset for rebooting in the main menu.

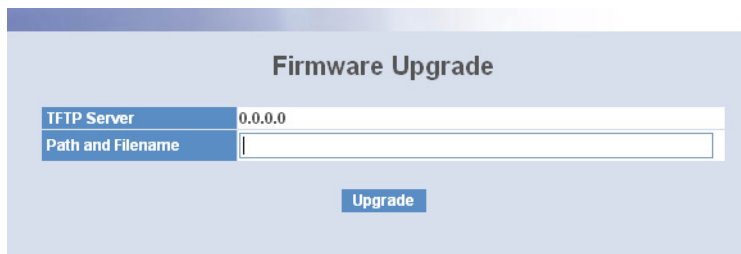
## 4.19.2 Firmware upgrade



Software upgrade tool is used to help upgrade the software function in order to fix or improve the function. The switch provides a TFTP client for software upgrade. This can be done through Ethernet.

### ■ Software upload

Click on <Browse> to select a specific LANCOM GS-2124 firmware file from the Web management PC, then click on <Upload> to confirm the upgrade firmware action. The new firmware will be uploaded into the switch and write into flash memory. You have to reboot the switch for new firmware take effect after the firmware upgrade successfully.





## 4.20 Management: SNMP

### SNMP Configuration

SNMP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable					
Get Community	<input type="text" value="public"/>					
Set Community	<input type="text" value="private"/>	<input type="button" value="Disable"/>				
Trap Host 1 IP Address	<input type="text" value="0.0.0.0"/>	<input type="text" value="162"/>	Community	<input type="text" value="public"/>		
Trap Host 2 IP Address	<input type="text" value="0.0.0.0"/>	<input type="text" value="162"/>	Community	<input type="text" value="public"/>		
Trap Host 3 IP Address	<input type="text" value="0.0.0.0"/>	<input type="text" value="162"/>	Community	<input type="text" value="public"/>		
Trap Host 4 IP Address	<input type="text" value="0.0.0.0"/>	<input type="text" value="162"/>	Community	<input type="text" value="public"/>		
Trap Host 5 IP Address	<input type="text" value="0.0.0.0"/>	<input type="text" value="162"/>	Community	<input type="text" value="public"/>		
Trap Host 6 IP Address	<input type="text" value="0.0.0.0"/>	<input type="text" value="162"/>	Community	<input type="text" value="public"/>		

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

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

### ■ SNMP Configuration

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

### ■ Parameter:

#### SNMP:

The term SNMP here is used for the activation or de-activation of SNMP.

Default is Enable.



If the SNMP support is deactivated, LANmonitor can not show information about the LANCOM Switch.

□ Get/Set/Trap Community:

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

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

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

Default SNMP function : Enable

Default community name for GET: public

Default community name for SET: private

Default community name for Trap: public

Default Set function : Enable

Default trap host IP address: 0.0.0.0

Default port number :162

□ Trap:

In the switch, there are 6 trap hosts supported. Each of them has its own community name and IP address; is user-definable. To set up a trap host means to create a trap manager by assigning an IP address to host the trap message. In other words, the trap host is a network management unit with SNMP manager receiving the trap message from the managed switch with SNMP agent issuing the trap message. 6 trap hosts can prevent the important trap message from being lost.

For each public trap, the switch supports the trap event Cold Start, Warm Start, Link Down, Link Up and Authentication Failure Trap. They can be enabled or disabled individually in the menu alarm > events. For the configuration of the traps use the function alarm and events. When enabled, the corresponded trap will actively send a trap message to the trap host when a trap happens. If all public traps are disabled, no public trap message will be sent. The Enterprise (no. 6) trap is classified as private trap. It is listed in the Trap Alarm Configuration function folder.

Default for all public traps: Enable.

## 4.21 Logout



You can manually logout by performing Logout function. In the switch, it provides another way to logout. You can configure it to logout automatically.

### ■ Logout

The switch allows you to logout the system to prevent other users from the system without the permission. If you do not logout and exit the browser, the switch will automatically have you logout. Besides this manually logout and implicit logout, you can pull down the <Auto Logout> list at the right-top corner to explicitly ON/OFF this logout function.

### ■ Parameter:

#### Auto Logout:

If it is "ON", and no action and no key is stroke as well in any function screen more than 3 minutes, the switch will have you logout automatically. Default is ON.

## 5 Operation of CLI Management

### 5.1 CLI Management

Refer to Chapter 2 for basic installation. The following description is the brief of the network connection.

- Locate the correct DB-9 null modem cable with female DB-9 connector. Null modem cable comes with the management switch. Refer to the Appendix B for null modem cable configuration.
- Attach the DB-9 female connector to the male DB-9 serial port connector on the Management board.
- Attach the other end of the DB-9 cable to an ASCII terminal emulator or PC Com-1, 2 port. For example, PC runs Microsoft Windows HyperTerminal utility.
- At "Com Port Properties" Menu, configure the parameters as below: (see the next section)

Baud rate	115200
Stop bits	1
Data bits	8
Parity	N
Flow control	none

#### 5.1.1 Login

The command-line interface (CLI) is a text-based interface. User can access the CLI through either a direct serial connection to the device or a Telnet session. The default values of the managed switch are listed below:

Username: admin

Password: admin

After you login successfully, the prompt will be shown as "#" if you are the first login person and your authorization is administrator; otherwise it may show "\$". See the following two figures. The former means you behave as an administrator and have the access right of the system. As to the latter, it means you behave as a guest and are only allowed to view the system without the permission to do any setting for this switch.

## 5.2 Commands of CLI

```

Telnet 10.98.1.61
Managed Switch - LANCOM GS-2124
Login: guest
Password: *****
LANCOM GS-2124$ ?
 802.1X          Enter into 802.1X mode
 account        Enter into account mode
 acl            Enter into acl mode
 alarm          Enter into alarm mode
 autologout     Change autologout time
 config-file    Enter into config file mode
 dhcp_snooping Enter into dhcp snooping mode
 diagnostics    Enter into diagnostics mode
 gvrp           Enter into gvrp mode
 ip             Enter into ip mode
 ip_mac_binding Enter into ip mac binding mode
 loop-detection Enter into Loop Detection(LD) mode
 mac            Enter into mac mode
 mirror        Enter into mirror mode
 mstp          Enter into mstp mode
 multicast      Enter into multicast mode
 policy        Enter into Management Policy mode
 port          Enter into port mode
 qos           Enter into qos mode
 snmp          Enter into snmp mode
 stp           Enter into stp mode
 system        Enter into system mode
 time          Enter into time mode
 traplog       Enter into trap log mode
 ..(q to quit)

 trunk          Enter into trunk mode
 vlan           Enter into vlan mode
 vs             Enter into virtual stack mode

```

### 5.2.1 Global Commands of CLI

#### ■ end

□ Syntax:

end

□ Description:

Back to the top mode.

When you enter this command, your current position would move to the top mode. If you use this command in the top mode, you are still in the position of the top mode.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L# alarm

```
GS-2124L(alarm)# events
```

```
GS-2124L(alarm-events)# end
```

```
GS-2124L#
```

### ■ exit

Syntax:

```
exit
```

Description:

Back to the previous mode.

When you enter this command, your current position would move back to the previous mode. If you use this command in the top mode, you are still in the position of the top mode.

Argument:

None.

Possible value:

None.

Example:

```
GS-2124L# trunk
```

```
GS-2124L(trunk)# exit
```

```
GS-2124L#
```

### ■ help

Syntax:

```
help
```

Description:

To show available commands.

Some commands are the combination of more than two words. When you enter this command, the CLI would show the complete commands. Besides, the command would help you classify the commands between the local commands and the global ones.

Argument:

None.

Possible value:

None.

Example:

```
GS-2124L# ip
```

```
GS-2124L(ip)# help
```

```
Commands available:
```

```
-----<< Local commands >>-----
```

```
set ip          Set ip,subnet mask and gateway
```

```
set dns        Set dns
```

```
enable dhcp    Enable DHCP, and set dns auto or manual
```

```
disable dhcp  Disable DHCP
```

```
show          Show IP Configuration
```

```
-----<< Global commands >>-----
```

```
exit          Back to the previous mode
```

```
end           Back to the top mode
```

```
help         Show available commands
```

```
history      Show a list of previously run commands
```

```
logout       Logout the system
```

```
save start   Save as start config
```

```
save user    Save as user config
```

```
restore default Restore default config
```

```
restore user Restore user config
```

## ■ history

□ Syntax:

```
history [#]
```

□ Description:

To show a list of previous commands that you had ever run.

When you enter this command, the CLI would show a list of commands which you had typed before. The CLI supports up to 256 records. If no argument is typed, the CLI would list total records up to 256. If optional argument is given, the CLI would only show the last numbers of records, given by the argument.

□ Argument:

[#]: show last number of history records. (optional)

- Possible value:

[#]: 1, 2, 3, ..., 256

- Example:

GS-2124L(ip)# history

Command history:

0. trunk

1. exit

2. GS-2124L# trunk

3. GS-2124L(trunk)# exit

4. GS-2124L#

5. ?

6. trunk

7. exit

8. alarm

9. events

10. end

11. ip

12. help

13. ip

14. history

GS-2124L(ip)# history 3

Command history:

13. ip

14. history

15. history 3

GS-2124L(ip)#

## ■ **logout**

- Syntax:

logout

- Description:



When you enter this command via Telnet connection, you would logout the system and disconnect. If you connect the system through direct serial port with RS-232 cable, you would logout the system and be back to the initial login prompt when you run this command.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L# logout

### ■ **restore default**

□ Syntax:

restore default

□ Description:

When you use this function in CLI, the system will show you the information "Do you want to restore the default IP address?(y/n)". If you choose Y or y, the IP address will restore to default "192.168.1.1". If you choose N or n, the IP address will keep the same one that you had saved before.

If restoring default successfully, the CLI would prompt if reboot immediately or not. If you press Y or y, the system would reboot immediately; otherwise, it would be back to the CLI system. After restoring default configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would reset to factory default.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L# restore default

Restoring ...

Restore Default Configuration Successfully

Press any key to reboot system.

■ **restore user**

## □ Syntax:

restore user

## □ Description:

To restore the startup configuration as user defined configuration. If restoring default successfully, the CLI would prompt if reboot immediately or not. If you press Y or y, the system would reboot immediately; others would back to the CLI system. After restoring user-defined configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would replace as user defined one.

## □ Argument:

None.

## □ Possible value:

None.

## □ Example:

```
GS-2124L# restore user
```

```
Restoring ...
```

```
Restore User Configuration Successfully
```

```
Press any key to reboot system.
```

■ **save start**

## □ Syntax:

save start

## □ Description:

To save the current configuration as the start one. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH. If you want the configuration still works after rebooting, save the configuration using the command 'save stat'.

## □ Argument:

None.

## □ Possible value:

None.

## □ Example:

```
GS-2124L# save start
```

Saving start...

Save Successfully

GS-2124L#

#### ■ **save user**

□ Syntax:

save user

□ Description:

To save the current configuration as the user-defined configuration. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH as user-defined configuration.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L# save user

Saving user...

Save Successfully

GS-2124L#

## 5.2.2 4-2-2. Local Commands of CLI

### 802.1X

#### ■ **set maxReq**

□ Syntax:

set maxReq <port-range> <vlaue>

□ Description:

The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session.

□ Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<value>: max-times , range 1-10

- Possible value:  
<port range> : 1 to 24  
<value>: 1-10, default is 2

- Example:  
GS-2124L(802.1X)# set maxReq 2 2

### ■ set mode

- Syntax:  
set mode <port-range> <mode>

- Description:  
To set up the 802.1X authentication mode of each port.

- Argument:  
<port range> : syntax 1,5-7, available from 1 to 24  
<mode>: set up 802.1X mode

0:disable the 802.1X function  
1:set 802.1X to Multi-host mode

- Possible value:  
<port range> : 1 to 24  
<mode>: 0 or 1

- Example:  
GS-2124L(802.1X)# set mode 2 1  
GS-2124L(802.1X)#

### ■ set port-control

- Syntax:  
set port-control <port-range> <unauthorized| authorized| auto>

- Description:  
To set up 802.1X status of each port.

- Argument:  
<port range> : syntax 1,5-7, available from 1 to 24  
<authorized> : Set up the status of each port

0:ForceUnauthorized  
1:ForceAuthorized

2:Auto

□ Possible value:

<port range> : 1 to 24

<authorized> : 0, 1 or 2

□ Example:

GS-2124L(802.1X)# set port-control 2 2

### ■ set quietPeriod

□ Syntax:

set quietPeriod <port-range> <value>

□ Description:

A timer used by the Authenticator state machine to define periods of time during when it will not attempt to acquire a Supplicant.

□ Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<value> : timer , range 0-65535

□ Possible value:

<port range> : 1 to 24

<value> : 0-65535, default is 60

□ Example:

GS-2124L(802.1X)# set quietPeriod 2 30

### ■ set reAuthEnabled

□ Syntax:

set reAuthEnabled <port-range> <on | off >

□ Description:

A constant that define whether regular reauthentication will take place on this port.

□ Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<on | off > :

0:OFF Disable reauthentication

1:ON Enable reauthentication

□ Possible value:

<port range> : 1 to 24

< on | off |> : 0 or 1, default is 1

□ Example:

```
GS-2124L(802.1X)# set reAuthEnabled 2 1
```

### ■ set reAuthMax

□ Syntax:

```
set reAuthMax <port-range> <value>
```

□ Description:

The number of reauthentication attempts that are permitted before the port becomes Unauthorized.

□ Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<value> : max. value , range 1-10

□ Possible value:

<port range> : 1 to 24

<value> : 1-10, default is 2

□ Example:

```
GS-2124L(802.1X)# set reAuthMax 2 2
```

### ■ set reAuthPeriod

□ Syntax:

```
set reAuthPeriod <port-range> <value>
```

□ Description:

A constant that defines a nonzero number of seconds between periodic reauthentication of the supplicant.

□ Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<value> : timer , range 1-65535

□ Possible value:

<port range> : 1 to 24

<value> : 1-65535, default is 3600

□ Example:

```
GS-2124L(802.1X)# set reAuthPeriod 2 3600
```

■ **set serverTimeout**

## □ Syntax:

set serverTimeout <port-range> <value>

## □ Description:

A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.

## □ Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<value> : timer , range 1-65535

## □ Possible value:

<port range> : 1 to 24

<value> : 1-65535, default is 30

## □ Example:

```
GS-2124L(802.1X)# set serverTimeout 2 30
```

■ **set auth-server**

## □ Syntax:

set auth-server <ip-address> <udp-port> <secret-key>

## □ Description:

To configure the settings related with 802.1X Radius Server.

## □ Argument:

<ip-address> : the IP address of Radius Server

<udp-port> : the service port of Radius Server(Authorization port)

<secret-key> : set up the value of secret-key, and the length of secret-key is

from 1 to 31

## □ Possible value:

<udp-port > : 1~65535, default is 1812

## □ Example:

```
GS-2124L(802.1X)# set auth-server 192.168.1.115 1812 WinRadius
```

**■ set suppTimeout**

## □ Syntax:

set suppTimeout <port-range> <value>

## □ Description:

A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.

## □ Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<value> : timer , range 1-65535

## □ Possible value:

<port range> : 1 to 24

<value> : 1-65535, default is 30

## □ Example:

```
GS-2124L(802.1X)# set suppTimeout 2 30
```

**■ set txPeriod**

## □ Syntax:

set txPeriod <port-range> <value>

## □ Description:

A timer used by the Authenticator PAE state machine to determine when an EAPOL PDU is to be transmitted

## □ Argument:

<port range> : syntax 1,5-7, available from 1 to 24

<value> : timer , range 1-65535

## □ Possible value:

<port range> : 1 to 24

<value> : 1-65535, default is 30

## □ Example:

```
GS-2124L(802.1X)# set txPeriod 2 30
```

**■ show status**

## □ Syntax:



show status

- Description:

To display the mode of each port.

- Argument:

None

- Possible value:

None

- Example:

GS-2124L(802.1X)# show status

Port	Mode
1	Disable
2	Multi-host
3	Disable
4	Disable
5	Disable
6	Disable

=====

1	Disable
2	Multi-host
3	Disable
4	Disable
5	Disable
6	Disable

### ■ show port-config

- Syntax:

show port-config <port-range>

- Description:

To display the parameter settings of each port.

- Argument:

<port range> : syntax 1,5-7, available from 1 to 24

- Possible value:

<port range> : 1 to 24

- Example:

GS-2124L(802.1X)# show port-config 1, 2

port 1) Mode : Disabled

port control : Auto

```

reAuthMax : 2
txPeriod : 30
Quiet Period : 60
reAuthEnabled : ON
reAuthPeriod : 120
max. Request : 2
suppTimeout : 30
serverTimeout : 30
port 2) Mode : Disabled
port control : Auto
reAuthMax : 2
txPeriod : 30
Quiet Period : 60
reAuthEnabled : ON
reAuthPeriod : 120
max. Request : 2
suppTimeout : 30
serverTimeout : 30

```

### ■ show statistics

□ Syntax:

```
show statistics <#>
```

□ Description:

To display the statistics of each port.

□ Argument:

<#> syntax 1,5-7, available from 1 to 24

□ Possible value:

<#> 1 to 24

:

### ■ show server

□ Syntax:

show server

□ Description:

Show the Radius server configuration

□ Argument:

None

□ Possible value:

None

□ Example:

GS-2124L(802.1X)# show server

Authentication Server

---

IP Address: 192.168.1.1

UDP Port : 1812

Secret Key : Radius

Accounting Server

---

IP Address: 192.168.1.1

UDP Port : 1812

Secret Key : Radius

### ° account

#### ■ add

□ Syntax:

add <name>

□ Description:

To create a new guest user. When you create a new guest user, you must type in password and confirm password.

□ Argument:

<name> : new account name

□ Possible value:

A string must be at least 5 character.

□ Example:

```
GS-2124L(account)# add aaaaa
```

```
Password:
```

```
Confirm Password:
```

```
GS-2124L(account)#
```

### ■ del

- Syntax:

```
del <name>
```

- Description:

To delete an existing account.

- Argument:

<name> : existing user account

- Possible value:

None.

- Example:

```
GS-2124L(account)# del aaaaa
```

```
Account aaaaa deleted
```

### ■ modify

- Syntax:

```
modify <username>
```

- Description:

To change the username and password of an existing account.

- Argument:

<name> : existing user account

- Possible value:

None.

- Example:

```
GS-2124L(account)# modify aaaaa
```

```
username/password: the length is from 5 to 15.
```

```
Current username (aaaaa):bbbb
```

```
New password:
```

```
Confirm password:
```

Username changed successfully.

Password changed successfully.

■ **show**

□ Syntax:

show

□ Description:

To show system account, including account name and identity.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L(account)# show

Account Name	Identity
-----	
admin	Administrator
guest	guest

° **acl**

■ **ace**

□ Syntax:

ace <index>

□ Description:

To display the ace configuration.

□ Argument:

<index> : the access control rule index value

□ Possible value:

None.

□ Example:

GS-2124L(acl)# ace 2

index: 2

rule: switch

vid: any  
 tag\_prio: any  
 dmac: any  
 frame type: arp  
 arp type: Request/Reply (opcode): any  
 source ip: any  
 destination ip: any  
 ARP flag  
 ARP SMAC Match: any  
 RARP DMAC Match: any  
 IP/Ethernet Length: any  
 IP: any  
 Ethernet: any  
 action: 1  
 rate limiter: 0  
 copy port: 0

■ **action**

□ Syntax:

action <port> <permit|deny> <rate\_limiter> <port copy>

□ Description:

To set the access control per port as packet filter action rule.

□ Argument:

<port> : 1-24

<permit/deny>: permit: 1, deny: 0

<rate\_limiter>: 0-16 (0:disable)

<port copy> : 0-24 (0:disable)

□ Possible value:

<port> : 1-24

<permit/deny>: 0-1

<rate\_limiter>: 0-16

<port copy> : 0-24

- Example:

```
GS-2124L(ac1)# action 5 0 2 2
```

```
GS-2124L(ac1)# show
```

```
port policy id action rate limiter port copy counter a class map
```

```
.. .. i-i- i- i- ..
5 1 deny 2 2
23 1 permit 0 0 0
24 1 permit 0 0 0
rate limiter rate(pps)
```

```
-----
1 1
2 1
3 1
4 1
5 1
```

```
i-i- i-i-
```

```
GS-2124L(ac1)#
```

### ■ delete

- Syntax:

```
delete <index>
```

- Description:

To delete the ACE ( Access Control Entry) configuration on the switch.

- Argument:

<index> : the access control rule index value

- Possible value:

None.

- Example:

```
GS-2124L(ac1)# delete 1
```

```
GS-2124L(ac1)#
```

**■ move**

- Syntax:

move <index1> <index2>

- Description:

To move the ACE ( Access Control Entry) configuration between index1 and index2..

- Argument:

None.

- Possible value:

None.

- Example:

FGS-2924(account)# move 1 2

**■ policy**

- Syntax:

policy <policy> <ports>

- Description:

To set acl port policy on switch

- Argument:

<policy> : 1-8

<ports> : 1-24

- Possible value:

<policy> : 1-8

<ports> : 1-24

- Example:

GS-2124L(acl)# policy 3 10

GS-2124L(acl)#

**■ ratelimiter**

- Syntax:

ratelimiter <id> <rate>

- Description:



To set access control rule with rate limiter on switch

□ Argument:

<id> : 1-16

<rate> : 1,2,4,8,16,32,64,128,256,512,1000,2000, 4000,8000,  
16000,32000,64000,128000,256000,512000,1024000

□ Possible value:

<id> : 1-16

<rate> : 1,2,4,8,16,32,64,128,256,512,1000,2000, 4000,8000,  
16000,32000,64000,128000,256000,512000,1024000

□ Example:

GS-2124L(acl)# ratelimiter 3 16000

GS-2124L(acl)#

## ■ set

□ Syntax:

set [<index>] [<next index>]

[switch | (port <port>) | (policy <policy>)]

[<vid>] [<tag\_prio>] [<dmac\_type>]

[(any) |

(etype [<etype>] [<smac>]) |

(arp [<arp type>] [<opcode>]

(any | [<source ip>] [<source ip mask>])

(any | [<destination ip>] [<destination ip mask>])

[<source mac>] [<arp smac match flag>]

[<raro dmac match flag>] [<ip/ethernet length flag>]

[<ip flag>] [<ethernet flag>]) |

(ip [(<source ip> <source ip mask>) | any]

[(<destination ip> <destination ip mask>) | any]

[<ip ttl>] [<ip fragment>] [<ip option>]

[(icmp <icmp type> <icmp code>) |

(udp <source port range> <destination port range>) |

(tcp <source port range> <destination port range>]

```

    <tcp fin flag> <tcp syn flag> <tcp rst flag>
    <tcp psh flag> <tcp ack flag> <tcp urg flag> |
    (other <ip protocol value>) |
    (any)]
  ]
  [<action>] [<rate limiter>] [<port copy>]

```

- Description:

To set access control entry on switch

- Argument:

- Possible value:

- Example:

## ■ show

- Syntax:

show

- Description:

To show all access control entry setting on switch

- Argument:

none

- Possible value:

none

- Example:

GS-2124L(acl)# show

```
port policy id action rate limiter port copy counter a class map
```

```
.. .. i-i- i- i- ..
```

```
5 1 deny 2 2
```

```
23 1 permit 0 0 0
```

```
24 1 permit 0 0 0
```

```
rate limiter rate(pps)
```

```

-----
1      1
2      1
3      1
4      1
5      1

```

```

i-i-   i-i-
GS-2124L(ac)#

```

### ° alarm

```
<<email>>
```

#### ■ del mail-address

□ Syntax:

```
del mail-address <#>
```

□ Description:

To remove the configuration of E-mail address.

□ Argument:

<#>: email address number, range: 1 to 6

□ Possible value:

<#>: 1 to 6

□ Example:

```
GS-2124L(alarm-email)# del mail-address 2
```

#### ■ del server-user

□ Syntax:

```
del server-user
```

□ Description:

To remove the configuration of server, user account and password.

□ Argument:

None.

□ Possible value:

None.

□ Example:  
GS-2124L(alarm-email)# del server-user

#### ■ set mail-address

□ Syntax:  
set mail-address <#> <mail address>

□ Description:  
To set up the email address.

□ Argument:  
<#>:email address number, range: 1 to 6  
<mail address>:email address

□ Possible value:  
<#>: 1 to 6

□ Example:  
GS-2124L(alarm-email)# set mail-address 1 abc@mail.abc.com

#### ■ set server

□ Syntax:  
set server <ip>

□ Description:  
To set up the IP address of the email server.

□ Argument:  
<ip>:email server ip address or domain name

□ Possible value:  
None.

□ Example:  
GS-2124L(alarm-email)# set server 192.168.1.6

#### ■ set user

□ Syntax:  
set user <username>

□ Description:  
To set up the account and password of the email server.

□ Argument:  
<username>: email server account and password

- Possible value:

None.

- Example:

GS-2124L (alarm-email)# set user admin

### ■ show

- Syntax:

show

- Description:

To display the configuration of e-mail.

- Argument:

None.

- Possible value:

None.

- Example:

GS-2124L(alarm-email)# show

Mail Server : 192.168.1.6

Username : admin

Password : \*\*\*\*\*

Email Address 1: abc@mail.abc.com

Email Address 2:

Email Address 3:

Email Address 4:

Email Address 5:

Email Address 6:

<<events>>

### ■ del all

- Syntax:

del all <range>

- Description:

To disable email, sms and trap of events.

- Argument:

<range>:del the range of events, syntax 1,5-7

□ Possible value:

<range>: 1~24

□ Example:

GS-2124L(alarm-events)# del all 1-3

### ■ del email

□ Syntax:

del email <range>

□ Description:

To disable the email of the events.

□ Argument:

<range>:del the range of email, syntax 1,5-7

□ Possible value:

<range>: 1~24

□ Example:

GS-2124L(alarm-events)# del email 1-3

### ■ del trap

□ Syntax:

del trap <range>

□ Description:

To disable the trap of the events.

□ Argument:

<range>:del the range of trap, syntax 1,5-7

□ Possible value:

<range>: 1~24

□ Example:

GS-2124L(alarm-events)# del trap 1-3

### ■ set all

□ Syntax:

set all <range>

□ Description:

To enable email, sms and trap of events.

- Argument:  
<range>:set the range of events, syntax 1,5-7
- Possible value:  
<range>: 1~24
- Example:  
GS-2124L(alarm-events)# set all 1-3

### ■ set email

- Syntax:  
set email <range>
- Description:  
To enable the email of the events.
- Argument:  
<range>:set the range of email, syntax 1,5-7
- Possible value:  
<range>: 1~24
- Example:  
GS-2124L(alarm-events)# set email 1-3

### ■ set trap

- Syntax:  
set trap <range>
- Description:  
To enable the trap of the events.
- Argument:  
<range>:set the range of trap, syntax 1,5-7
- Possible value:  
<range>: 1~24
- Example:  
GS-2124L(alarm-events)# set trap 1-3

### ■ show

- Syntax:  
show
- Description:

To display the configuration of alarm event.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L(alarm-events)# show

Events	Email SMS Trap
-----	
1 Cold Start	v
2 Warm Start	v
3 Link Down	v
4 Link Up	v
5 Authentication Failure	v
6 Login	
7 Logout	
8 Module Inserted	
9 Module Removed	
10 Dual Media Swapped	
11 Looping Detected	
12 STP Disabled	
13 STP Enabled	
14 STP Topology Changed	
15 LACP Disabled	
16 LACP Enabled	
17 LACP Member Added	
18 LACP Aggregates Port Failure	
19 GVRP Disabled	
20 GVRP Enabled	
21 VLAN Disabled	



- 22 Port-based Vlan Enabled
- 23 Tag-based Vlan Enabled
- 24 IP MAC Binding Enabled
- 25 IP MAC Binding Disabled
- 26 IP MAC Binding Client Authenticate error
- 27 IP MAC Binding Server Authenticate error

### ■ show (alarm)

- Syntax:

show

- Description:

The Show for alarm here is used to display the configuration of Events, or E-mail.

- Argument:

None.

- Possible value:

None.

- Example:

GS-2124L(alarm)# show events

GS-2124L(alarm)# show email

### ° autologout

autologout

- Syntax:

autologout <time>

- Description:

To set up the timer of autologout.

- Argument:

<time>: range 1 to 3600 seconds, 0 for autologout off, current setting is 180 seconds.

- Possible value:

<time>: 0,1-3600

- Example:

```
GS-2124L# autologout 3600
Set autologout time to 3600 seconds
```

### ° config-file

#### ■ export

- Syntax:

```
export <current | user> < ip address>
```

- Description:

[To run the](#) export function.

- Argument:

< Usage> set up current or user

< ip address> the TFTP server ip address

- Possible value:

none

- Example:

```
GS-2124L(config-file)# export current 192.168.1.63
```

Export successful\_

#### ■ import

- Syntax:

```
import <current | user> < ip address>
```

- Description:

To run the [im](#)port start function.

- Argument:

None

- Possible value:

None

- Example:

```
GS-2124L(config-file)# import current 192.168.1.63
```

Import successful\_

### ° firmware

#### ■ Upgrade

- Syntax:

upgrade <ip\_address> <file\_path>

## □ Description:

To set up the image file that will be upgraded.

## □ Argument:

< ip address> : TFTP server ip address

<filepath>: upgrade file path

## □ Possible value:

< ip address> : TFTP server ip address

<filepath>: upgrade file path

## □ Example:

```
GS-2124L(firmware)# upgrade 192.168.2.4 fgs2924R_GS-2124L_v2.03.img
```

## ° gvrp

## ■ set state

## □ Syntax:

set state < 0 | 1>

## □ Description:

To disable/ enable the gvrp function.

## □ Argument:

0 : disable the gvrp function

1 : enable the gvrp function

## □ Possible value:

0 : disable the gvrp function

1 : enable the gvrp function

## □ Example:

```
GS-2124L(gvrp)# set state 1
```

## ■ group applicant

## □ Syntax:

group applicant <vid> <port> < 0 | 1>

## □ Description:

To enter any of gvrp group for changing gvrp group setting. You can change the applicant or registrar mode of existing gvrp group per port.

- Argument:

<vid>: enter which gvrp group you had created, using value is vid.  
Available range: 1 to 4094

<port>: 1 to 24

< 0 | 1 > :

- Possible value:

<vid>: 1~4094

<port>: 1 to 24

- Example:

```
GS-2124L(gvrp)# group applicant 2 5 0
```

GVRP group information

Current Dynamic Group Number: 1

VID	Member	Port
-----		
2	5	

### ■ set applicant

- Syntax:

```
set applicant <port> < 0 | 1 >
```

- Description:

To set default applicant mode for each port.

- Argument:

<port>: port range, syntax 1,5-7, available from 1 to 24

<0>: set applicant as normal mode

<1>: set applicant as non-participant mode

- Possible value:

<port>: 1 to 24

< 0 | 1 >: normal or non-participant

- Example:

```
GS-2124L(gvrp)# set applicant 1-10 non-participant
```

### ■ set registrar

- Syntax:

```
set registrar <port> < 0 | 1 | 2 >
```

## □ Description:

To set default registrar mode for each port.

## □ Argument:

<port>: port range, syntax 1,5-7, available from 1 to 24

<0>: set registrar as normal mode

<1>: set registrar as fixed mode

<2>: set registrar as forbidden mode

## □ Possible value:

<range>: 1 to 24

< 0 | 1 | 2>: normal or fixed or forbidden

## □ Example:

```
GS-2124L(gvrp)# set registrar 1-5 fixed
```

■ **set restricted**

## □ Syntax:

```
set restricted <port> <0 | 1 | 2>
```

## □ Description:

To set the restricted mode for each port.

## □ Argument:

<port>: port range, syntax 1,5-7, available from 1 to 24

<0>: set restricted normal

<1>: set restricted fixed

<2>: set restricted forbidden

## □ Possible value:

<port>: 1 to 24

< 0 | 1 | 2>: normal, fixed or forbidden

## □ Example:

```
GS-2124L(gvrp)# set restricted 1-10 1
```

```
GS-2124L(gvrp)# show config
```

```
GVRP state: Enable
```

```
Port Join Time Leave Time LeaveAll Time Applicant Registrar Restricted
```

```

-----
-
1  20  60  1000  Normal  Normal  Enable
2  20  60  1000  Normal  Normal  Enable
3  20  60  1000  Normal  Normal  Enable
4  20  60  1000  Normal  Normal  Enable
5  20  60  1000  Normal  Normal  Enable
6  20  60  1000  Normal  Normal  Enable
7  20  60  1000  Normal  Normal  Enable
8  20  60  1000  Normal  Normal  Enable
9  20  60  1000  Normal  Normal  Enable
10 20  60  1000  Normal  Normal  Enable
      :
      :
      :
22 20  60  1000  Normal  Normal  Disable
23 20  60  1000  Normal  Normal  Disable
24 20  60  1000  Normal  Normal  Disable

```

### ■ set timer

#### □ Syntax:

```
set timer <port> <JoinTime> <leaveTime> <leaveAllTime>
```

#### □ Description:

To set gvrp join time, leave time, and leaveall time for each port.

#### □ Argument:

<port> : port range, syntax 1,5-7, available from 1 to 24

<JoinTime>: join timer, available from 20 to 100

<LeaveTime>: leave timer, available from 60 to 300

<LeaveAllTime>: leaveall timer, available from 1000 to 5000

Leave Time must equal double Join Time at least.

#### □ Possible value:

<port> : 1 to 24

<JoinTime>: 20 to 100  
 <LeaveTime>: 60 to 300  
 <LeaveAllTime>: 1000 to 5000

□ Example:

```
GS-2124L(gvrp)# set timer 2-8 25 80 2000
```

■ **show**

□ Syntax:

```
show
```

□ Description:

To display the gvrp configuration.

□ Argument:

None

□ Possible value:

None

□ Example:

```
GS-2124L(gvrp)# show
```

```
GVRP state: Enable
```

```
Port Join Time Leave Time LeaveAll Time Applicant Registrar Restricted
```

```
-----
```

```
-
```

1	20	60	1000	Normal	Normal	Disable
2	25	80	2000	Normal	Normal	Disable
3	25	80	2000	Normal	Normal	Disable
4	25	80	2000	Normal	Normal	Disable
5	25	80	2000	Normal	Normal	Disable
6	25	80	2000	Normal	Normal	Disable
7	25	80	2000	Normal	Normal	Disable
8	25	80	2000	Normal	Normal	Disable
				:		
				:		
23	20	60	1000	Normal	Normal	Disable

24 20 60 1000 Normal Normal Disable

### ■ counter

- Syntax:

counter <port>

- Description:

To display the counter number of the port.

- Argument:

<port>: port number

- Possible value:

<port>: available from 1 to 24

- Example:

```
GS-2124L(gvrp)# counter 2
```

Received

Total GVRP Packets : 0

Invalid GVRP Packets : 0

LeaveAll message : 0

JoinEmpty message : 0

JoinIn message : 0

LeaveEmpty message : 0

Empty message : 0

Transmitted

Total GVRP Packets : 0

Invalid GVRP Packets : 0

LeaveAll message : 0

JoinEmpty message : 0

JoinIn message : 0

LeaveEmpty message : 0

Empty message : 0

### ■ group grpinfo

- Syntax:

group grpinfo <vid>



- Description:  
To show the gvrp group.
- Argument:  
<vid>: To set the vlan id from 1 to 4094
- Possible value:  
<vid>: 1 to 4094
- Example:  
GS-2124L(gvrp)# group grpinfo 2  
GVRP group information  
VID Member Port  
-----

### ° hostname

#### ■ hostname

- Syntax:  
hostname <name>
- Description:  
To set up the hostname of the switch.
- Argument:  
<name>: hostname, max. 40 characters.
- Possible value:  
<name>: hostname, max. 40 characters.
- Example:  
GS-2124L# hostname Company  
Company#

### ° igmp

#### ■ set drp

- Syntax:  
set drp <port >
- Description:  
Set router ports to disable.
- Argument:

<port >: syntax 1,5-7, available from 1 to 24

□ Possible value:

<port >: 1 to 24

□ Example:

```
GS-2124L(igmp)# set drp 1-10
```

### ■ set erp

□ Syntax:

```
set erp <port>
```

□ Description:

Set router ports to enable

□ Argument:

<port>: syntax 1,5-7, available from 1 to 24

□ Possible value:

<port>: 1 to 24

□ Example:

```
GS-2124L(igmp)# set erp 1
```

### ■ set flood

□ Syntax:

```
set flood <state>
```

□ Description:

To set up disable / enable unregister ipmc flooding.

□ Argument:

<state>: 0:disable, 1:enable

□ Possible value:

<state>: 0, or 1

□ Example:

```
GS-2124L(igmp)# set flood 1
```

### ■ show gm

□ Syntax:

```
show gm
```

□ Description:

To display group membership.

- Argument:

None.

- Possible value:

None.

- Example:

GS-2124L(igmp)# show gm

### ■ **show igmpp**

- Syntax:

show igmpp

- Description:

To display igmp proxy setting

- Argument:

None.

- Possible value:

None.

- Example:

GS-2124L(igmp)# show igmpp

### ◦ IP

#### ■ **disable dhcp**

- Syntax:

disable dhcp

- Description:

To disable the DHCP function of the system.

- Argument:

None

- Possible value:

None

- Example:

GS-2124L(ip)# disable dhcp



#### ■ **enable dhcp**

- Syntax:

enable dhcp <manual|auto>

□ Description:

To enable the system DHCP function and set DNS server via manual or auto mode.

□ Argument:

<manual|auto> : set dhcp by using manual or auto mode.

□ Possible value:

<manual|auto> : manual or auto

□ Example:

GS-2124L(ip)# enable dhcp manual

### ■ set dns

□ Syntax:

set dns <ip>

□ Description:

To set the IP address of DNS server.

□ Argument:

<ip> : dns ip address

□ Possible value:

168.95.1.1

□ Example:

GS-2124L (ip)# set dns 168.95.1.1

### ■ set ip

□ Syntax:

set ip <ip> <mask> <gateway>

□ Description:

To set the system IP address, subnet mask and gateway.

□ Argument:

<ip> : ip address

<mask> : subnet mask

<gateway> : default gateway

□ Possible value:

<ip> : 192.168.1.2 or others

<mask> : 255.255.255.0 or others

<gateway> : 192.168.1.253 or others

□ Example:

```
GS-2124L(ip)# set ip 192.168.1.2 255.255.255.0 192.168.1.253
```

## ■ show

□ Syntax:

show

□ Description:

To display the system's DHCP function state, IP address, subnet mask, default gateway, DNS mode, DNS server IP address and current IP address.

□ Argument:

None

□ Possible value:

None

□ Example:

```
GS-2124L(ip)# show
```

```
DHCP          : Disable
```

```
IP Address    : 192.168.2.237
```

```
Current IP Address : 192.168.2.237
```

```
Subnet mask   : 255.255.255.0
```

```
Gateway       : 192.168.2.252
```

```
DNS Setting   : Manual
```

```
DNS Server    : 168.95.1.1
```

## ° ip\_mac\_binding

### ■ set entry

□ Syntax:

```
set entry < 0 | 1> < mac> < ip> < port no> < vid>
```

□ Description:

To set ip mac binding entry

- Argument:

< 0 | 1 > : 0 : Client , 1: Server

<mac> : mac address

< ip > : ip address

< port > : syntax 1,5-7, available from 1 to 24

< vid > : vlan id, 1 to 4094

- Possible value:

< 0 | 1 > : 0 : Client , 1: Server

<mac> : format: 00-02-03-04-05-06

< ip > : ip address

< port > : 1 to 24

< vid > : 1 to 4094

- Example:

```
GS-2124L(ip_mac_binding)# set entry 1 00-11-2f-de-7b-a9 192.168.2.2
1 1
```

### ■ delete ip

- Syntax:

delete ip < 0 | 1 > <ip>

- Description:

Delete ip mac binding entry by ip.

- Argument:

<0 | 1> : 0 : client, 1: server

<ip> : ip address

- Possible value:

None

- Example:

```
GS-2124L(ip_mac_binding)# delete ip 1 192.168.2.2
```

### ■ set state

- Syntax:

show

- Description:

To display the mac alias entry.

□ Argument:

None

□ Possible value:

None

□ Example:

```
GS-2124L(mac-table-alias)# show
```

MAC Alias List

MAC Address	Alias
-------------	-------

-----

1) 00-02-03-04-05-06 aaa

2) 00-33-03-04-05-06 ccc

3) 00-44-33-44-55-44 www

### ° loop-detection

#### ■ disable

□ Syntax:

disable <#>

□ Description:

To disable switch ports the loop detection function.

□ Argument:

<#> : set up the range of the ports to search for, syntax 1,5-7, available form 1 to 24

□ Possible value:

<#> :1 to 24

□ Example:

```
GS-2124L(loop-detection)# disable 1-24
```

```
GS-2124L(loop-detection)# show
```

Detection Port	Locked Port
----------------	-------------

Port Status	Port Status
-------------	-------------

-----

1 Disable	1 Normal
-----------	----------

2 Disable	2 Normal
-----------	----------

3 Disable	3 Normal
4 Disable	4 Normal
5 Disable	5 Normal
6 Disable	6 Normal
7 Disable	7 Normal
8 Disable	8 Normal

i-i-i-

■ **enable**

□ Syntax:

enable &lt;#&gt;

□ Description:

To enable switch ports the loop detection function.

□ Argument:

&lt;#&gt; : set up the range of the ports to search for, syntax 1,5-7, available form 1 to 24

□ Possible value:

&lt;#&gt; :1 to 24

□ Example:

GS-2124L(loop-detection)# enable 1-24

GS-2124L(loop-detection)# show

Detection Port      Locked Port

Port Status        Port Status

-----

1 Enable	1 Normal
2 Enable	2 Normal
3 Enable	3 Normal
4 Enable	4 Normal
5 Enable	5 Normal
6 Enable	6 Normal
7 Enable	7 Normal
8 Enable	8 Normal



i-i-i-i-

■ **Resume**

□ Syntax:

resume &lt;#&gt;

□ Description:

To resume locked ports on switch.

□ Argument:

&lt;#&gt; : set up the range of the ports to search for, syntax 1,5-7, available form 1 to 24

□ Possible value:

&lt;#&gt; :1 to 24

□ Example:

GS-2124L (loop-detection)# resume 1-24

GS-2124L (loop-detection)# show

Detection Port	Locked Port
Port Status	Port Status

-----

1 Enable	1 Normal
2 Enable	2 Normal
3 Enable	3 Normal
4 Enable	4 Normal
5 Enable	5 Normal
6 Enable	6 Normal
7 Enable	7 Normal
8 Enable	8 Normal

i-i-i-i-

■ **Resume**

□ Syntax:

resume &lt;#&gt;

□ Description:

To resume locked ports on switch.

- Argument:

<#> : set up the range of the ports to search for, syntax 1,5-7, available form 1 to 24

- Possible value:

<#> :1 to 24

- Example:

```
GS-2124L (loop-detection)# resume 1-24
```

```
GS-2124L (loop-detection)# show
```

Detection Port	Locked Port
Port Status	Port Status

-----

1 Enable	1 Normal
2 Enable	2 Normal
3 Enable	3 Normal
4 Enable	4 Normal
5 Enable	5 Normal
6 Enable	6 Normal
7 Enable	7 Normal
8 Enable	8 Normal

i-i-i-i-

### ■ show

- Syntax:

show

- Description:

To display loop detection configure.

- Argument:

None

- Possible value:

None

- Example:

```
GS-2124L (loop-detection)# show
```

Detection Port	Locked Port
Port Status	Port Status
-----	
1 Enable	1 Normal
2 Enable	2 Normal
3 Enable	3 Normal
4 Enable	4 Normal
5 Enable	5 Normal
6 Enable	6 Normal
7 Enable	7 Normal
8 Enable	8 Normal
i-i-i-i-	

## ° Mac

## ■ &lt;&lt;alias&gt;&gt;

## ■ del

□ Syntax:

del &lt;mac&gt;

□ Description:

To del mac alias entry.

□ Argument:

&lt;mac&gt; : set up the MAC format: xx-xx-xx-xx-xx-xx

□ Possible value:

&lt;mac&gt; : set up the MAC format: xx-xx-xx-xx-xx-xx

□ Example:

GS-2124L(mac-alias)# set 23-56-r5-55-3f-03 test3

GS-2124L(mac-alias)# show

MAC Alias

No	MAC	Alias
=====		
1	23-56-00-55-3F-03	test3

```

2 23-56-00-55-EF-03 test13
3 23-56-00-55-EF-33 test1
GS-2124L(mac-alias)# del 23-56-00-55-3F-03
GS-2124L(mac-alias)# show
MAC Alias
No      MAC      Alias
=====
1 23-56-00-55-EF-03 test13
2 23-56-00-55-EF-33 test1

```

■ **set**

## □ Syntax:

```
set <mac> <alias>
```

## □ Description:

To set mac alias entry.

## □ Argument:

<mac> : mac address, xx-xx-xx-xx-xx-xx

<alias> : mac alias name, max 15 characters

## □ Possible value:

<mac> : set up the MAC format: xx-xx-xx-xx-xx-xx

<alias> : mac alias name, max 15 characters

## □ Example:

```
GS-2124L(mac-alias)# set 23-56-r5-55-3f-03 test3
```

```
GS-2124L(mac-alias)# show
```

```
MAC Alias
```

```
No      MAC      Alias
=====
```

```

1 23-56-00-55-3F-03 test3
2 23-56-00-55-EF-03 test13
3 23-56-00-55-EF-33 test1

```

■ **show**

## □ Syntax:

show

□ Description:

To display mac alias entry.

□ Argument:

None

□ Possible value:

none

□ Example:

GS-2124L(mac-alias)# show

MAC Alias

No	MAC	Alias
----	-----	-------

=====

1	23-56-00-55-3F-03	test3
---	-------------------	-------

2	23-56-00-55-EF-03	test13
---	-------------------	--------

3	23-56-00-55-EF-33	test1
---	-------------------	-------

■ <<mac-table>>

■ flush

□ Syntax:

flush

□ Description:

To del dynamic mac entry.

□ Argument:

none

□ Possible value:

none

□ Example:

GS-2124L(mac-mac-table)# flush

GS-2124L(mac-mac-table)# show

No	Type	VLAN	MAC	Port Members
----	------	------	-----	--------------

-----  
-----

```

1          Static          1  FF-FF-FF-FF-FF-FF
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,1
8,19,20,21,22,23,24,

```

### ■ show

- Syntax:

show

- Description:

To show all mac table informaion.

- Argument:

none

- Possible value:

none

- Example:

GS-2124L(mac-mac-table)# show

```

No  Type  VLAN      MAC          Port Members
-----
1          Static          1  FF-FF-FF-FF-FF-FF
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,1
8,19,20,21,22,23,24,

```

### ■ <<maintenance>>

#### ■ set age-time

- Syntax:

set age-time <#>

- Description:

To set mac table age out time of dynamic learning mac.

- Argument:

<#>: age-timer in seconds, 0, 10 1000000. The value zero disables aging

- Possible value:

<#>: 0, 10 to 1000000.

- Example:

GS-2124L(mac-table-maintain)# set age-time 300

```
GS-2124L(mac-maintenance)# show
E api_ai 26/vtss_
Aging Configuration:   Enter into sta
Age time: 300mode
MAC Table Learning
Port  Learning Mode-<< Global commands >
2    Auto
3    Auto
4    Auto
5    Auto
6    Auto
7    Auto
8    Auto
9    Auto
10   Auto
11   Auto
12   Auto
13   Auto
14   Auto
15   Auto
16   Auto
17   Auto
18   Auto
19   Auto
20   Auto
21   Auto
22   Auto
23   Auto
24   Auto
```

■ **set learning**

## □ Syntax:

```
set learning <range> <auto|disable|secure>
```

## □ Description:

To set mac table learning.

## □ Argument:

<range syntax> : 1,5-7, available from 1 to 24

<auto >: auto learning

<disable >: disable learning

<secure >: learn frames are discarded

## □ Possible value:

<range syntax> : 1,5-7, available from 1 to 24

<auto >: auto learning

<disable >: disable learning

<secure >: learn frames are discarded.

## □ Example:

```
GS-2124L(mac-table-maintain)# set learning 1-24 auto
```

```
GS-2124L(mac-maintenance)# show
```

```
E api_ai 26/vtss_
```

```
Aging Configuration:   Enter into sta
```

```
Age time: 300mode
```

```
MAC Table Learning
```

```
Port  Learning Mode-<< Global commands >
```

```
2    Auto
```

```
3    Auto
```

```
4    Auto
```

```
5    Auto
```

```
6    Auto
```

```
7    Auto
```

```
8    Auto
```

```
9    Auto
```



- 10 Auto
- 11 Auto
- 12 Auto
- 13 Auto
- 14 Auto
- 15 Auto
- 16 Auto
- 17 Auto
- 18 Auto
- 19 Auto
- 20 Auto
- 21 Auto
- 22 Auto
- 23 Auto
- 24 Auto

■ **show**

- Syntax:

show

- Description:

To display mac table maintenance

- Argument:

Noneq

- Possible value:

None

- Example:

```
GS-2124L(mac-maintenance)# show
```

```
1 Static
```

```
Aging Configuration:FF 1,2,3,4,5,6,7,8,9
```

```
Age time: 3004,15,16,17,1
```

```
MAC Table Learning
```

```
Port Learning Mode
```

2 Auto  
3 Auto  
4 Auto  
5 Auto  
6 Auto  
7 Auto  
8 Auto  
9 Auto  
10 Auto  
11 Auto  
12 Auto  
13 Auto  
14 Auto  
15 Auto  
16 Auto  
17 Auto  
18 Auto  
19 Auto  
20 Auto  
21 Auto  
22 Auto  
23 Auto  
24 Auto

■ <<static-mac>>

■ add

□ Syntax:

add <mac> <port> <vid> [alias]

□ Description:

To add the static mac entry.

□ Argument:

<mac> : mac address, format: 00-02-03-04-05-06

<port> : 0-24. The value "0" means this entry is filtering entry  
 <vid> : vlan id. 0, 1-4094. VID must be zero if vlan mode is not tag-based  
 [alias] : mac alias name, max. 15 characters

□ Possible value:

<mac> : mac address

<port> : 0-24

<vid> : 0, 1-4094

[alias] : mac alias name

□ Example:

```
GS-2124L(mac-static-mac)# add 00-02-03-04-05-06 3 0 aaa
```

```
GS-2124L(mac-static-mac)#
```



### ■ del

□ Syntax:

```
del <mac> <vid>
```

□ Description:

To del the static mac entry.

□ Argument:

<mac> : mac address, format: 00-02-03-04-05-06

<vid> : vlan id. 0, 1-4094. VID must be zero if vlan mode is not tag-based

□ Possible value:

<mac> : mac address

<vid> : 0, 1-4094

□ Example:

```
GS-2124L(mac-static-mac)# del 00-02-03-04-05-06 0
```

```
GS-2124L(mac-static-mac)#
```

### ■ show filter

□ Syntax:

```
show filter
```

□ Description:

To display the static filtering mac entry.

- Argument:

None

- Possible value:

None

- Example:

```
GS-2124L(mac-static-mac)# show filter
```

```
Static Filtering Etnry: (Total 1 item(s))
```

```
1) mac: 00-33-03-04-05-06, vid: -, alias: ccc
```

```
GS-2124L(mac-static-mac)#
```

### ■ show forward

- Syntax:

```
show forward
```

- Description:

To display the static forwarding mac entry.

- Argument:

None

- Possible value:

None

- Example:

```
GS-2124L(mac-static-mac)# show forward
```

```
Static Forwarding Etnry: (Total 1 item(s))
```

```
1) mac: 00-02-03-04-05-06, port: 3, vid: -, alias: aaa
```

```
GS-2124L(mac-static-mac)#
```

### ° mirror

#### ■ set mirror

- Syntax:

```
set mirror < #>
```

- Description:

To set mirror port and enable/disable mirror function

- Argument:

<#>: port, available from 1 to 24 and 0.

1 to 24: available port number

0: disable mirror function

□ Possible value:

<#>: 1 to 24

□ Example:

```
GS-2124L(mirror)# set mirror 2
```

### ■ set monitor-destination

□ Syntax:

```
set monitor-destination <range>
```

□ Description:

To set monitor destination port. The packets sent by this port will be copied to the monitoring port.

□ Argument:

<range>: the port that is chosen for monitored port of the mirror function, syntax 1,5-7, available from 1 to 24

□ Possible value:

<range>: 1 to 24

□ Example:

```
GS-2124L(mirror)# set monitor-destination 2-15
```

```
GS-2124L(mirror)# show
```

2	V
3	V
4	V
5	V
6	V
7	V
8	V
9	V
10	V
11	V
12	V

13	V
14	V
15	V
16	
17	
18	

EN

### ■ set monitor-source

- Syntax:

```
set monitor-source <range>
```

- Description:

To set up the monitoring port of the mirror function. User can observe the packets that the monitored port received via this port.

- Argument:

<range>: the monitoring port that is chosen for the mirror function. Only one port is allowed to configure, available from 1 to 24

- Possible value:

<range>:1 to 24

- Example:

```
GS-2124L(mirror)# set monitor-source 18
```

```
GS-2124L(mirror)# show
```

```
Port to mirror to: 1
```

Port	Source Enable	Destination Enable
------	---------------	--------------------

2		V
---	--	---

3		V
---	--	---

4		V
---	--	---

5		V
---	--	---

6		V
---	--	---

7		V
---	--	---

8		V
---	--	---

9		V
---	--	---

```

10                V
11                V
12                V
13                V
14                V
15                V

```

```
16
```

```
17
```

```
18          V
```

```
19
```

```
20
```

```
21
```

```
22
```

```
23
```

```
24
```

```
GS-2124L(mirror)#
```

■ **show**

□ Syntax:

```
show
```

□ Description:

To display the setting status of mirror configuration.

□ Argument:

None

□ Possible value:

None

□ Example:

```
GS-2124L(mirror)# show
```

```
Port to mirror to: 1
```

```
Port  Source Enable  Destination Enable
```

```
2                V
```

```
3                V
```

4		V
5		V
6		V
7		V
8		V
9		V
10		V
11		V
12		V
13		V
14		V
15		V
16		
17		
18	V	
19		
20		
21		
22		
23		
24		

GS-2124L(mirror)#

## ° mstp

## ■ disable

Syntax:

disable

Description:

To disable mstp function.

Argument:

None



- Possible value:

None

- Example:

GS-2124L (mstp)# disable

#### ■ enable

- Syntax:

enable

- Description:

To enable mstp function.

- Argument:

None

- Possible value:

None

- Example:

GS-2124L (mstp)# enable

#### ■ migrate-check

- Syntax:

migrate-check <port-range>

- Description:

To force the port to transmit RST BPDUs.

- Argument:

Usage: migrate-check <port range>

- port range syntax: 1,5-7, available from 1 to 24

- Possible value:

Usage: migrate-check <port range>

- port range syntax: 1,5-7, available from 1 to 24

- Example:

GS-2124L (mstp)# migrate-check 1-2

#### ■ set config

- Syntax:

set config <Max Age><Forward Delay><Max Hops>

- Description:

To set max age,forward delay,max hops.

□ Argument:

<Max Age> : available from 6 to 40. Recommended value is 20

<Forward Delay(sec)> : available from 4 to 30. Recommended value is 15

<Max Hops> : available from 6 to 40. Recommended value is 20

□ Possible value:

<Max Age> : available from 6 to 40. Recommended value is 20

<Forward Delay(sec)> : available from 4 to 30. Recommended value is 15

<Max Hops> : available from 6 to 40. Recommended value is 20

□ Example:

```
GS-2124L(mstp)# set config 20 15 20
```

```
GS-2124L(mstp)#
```

#### ■ set msti-vlan

□ Syntax:

```
set msti-vlan <instance-id><vid-string>
```

□ Description:

To map Vlan ID(s) to an MSTI

□ Argument:

<instance-id> : MSTI id available from 1 to 4095

□ <vid-string> : syntax example: 2.5-7.100-200

□ Possible value:

<instance-id> : available from 1 to 4094

□ Example:

```
GS-2124L(mstp)# set msti-vlan 2 2.5
```

msti 2 had been successfully created and(or)

vlan(s) have been added to map to this msti.

```
GS-2124L(mstp)#
```

#### ■ set p-cost

□ Syntax:

```
set p-cost <instance_id> <port range> <path cost>
```

□ Description:

To set port path cost per instance

- Argument:
- <port range> syntax: 1,5-7, available from 1 to 24  
<path cost> : 0, 1-200000000. The value zero means auto status
- Possible value:  
<port range> : available from 1 to 24  
<path cost> : The value zero means auto status, 0-2000000000
- Example:  
GS-2124L(mstp)# set p-cost 2 8-10 0  
GS-2124L(mstp)#

### ■ set p-edge

- Syntax:  
set p-edge <port range> <admin edge>
- Description:  
To set per port admin edge
- Argument:
- <port range> syntax: 1,5-7, available from 1 to 24  
<admin edge> : 0->non-edge port,1->edge ports
- Possible value:
- <port range> syntax: 1,5-7, available from 1 to 24  
<admin edge> : 0->non-edge port,1->edge ports
- Example:  
GS-2124L(mstp)# set p-edge 10-12 0  
GS-2124L(mstp)#

### ■ set p-hello

- Syntax:  
set p-hello <port range> <hello time>
- Description:  
To set per port hello time
- Argument:
- <port range> : syntax: 1,5-7, available from 1 to 24  
<hello time> : only 1~2 are valid values
- Possible value:

□ <port range> : syntax: 1,5-7, available from 1 to 24  
 <hello time> : only 1~2 are valid values

□ Example:

```
GS-2124L(mstp)# set p-hello 5-10 1
```

```
GS-2124L(mstp)#
```

### ■ set p-p2p

□ Syntax:

```
set p-p2p <port range> <admin p2p>
```

□ Description:

To set per port admin p2p

□ Argument:

□ <port range> syntax: 1,5-7, available from 1 to 24  
 <admin p2p> : Admin point to point, <auto|true|false>

□ Possible value:

□ <port range> syntax: 1,5-7, available from 1 to 24  
 <admin p2p> : Admin point to point, <auto|true|false>

□ Example:

```
GS-2124L(mstp)# set p-p2p 8-10 auto
```

```
GS-2124L(mstp)#
```

### ■ set priority

□ Syntax:

```
set priority <instance-id><Instance Priority>
```

□ Description:

To set instance priority

□ Argument:

<instance-id> : 0->CIST; 1-4095->MSTI

<Instance Priority> : must be a multiple of 4096,available from 0 to 61440

□ Possible value:

<instance-id> : 0->CIST; 1-4095->MSTI

<Instance Priority> : 0 to 61440

□ Example:

```
GS-2124L(mstp)# set priority 0 4096
GS-2124L(mstp)# enable
MSTP started
GS-2124L(mstp)# show instance 0
mstp status : enabled
force version : 3
instance id: 0
bridge max age : 20
bridge forward delay : 15
bridge max hops : 20
instance priority : 4096
bridge mac : 00:40:c7:5e:00:09
CIST ROOT PRIORITY : 4096
CIST ROOT MAC : 00:40:c7:5e:00:09
CIST EXTERNAL ROOT PATH COST : 0
CIST ROOT PORT ID : 0
CIST REGIONAL ROOT PRIORITY : 4096
CIST REGIONAL ROOT MAC : 00:40:c7:5e:00:09
CIST INTERNAL ROOT PATH COST : 0
CIST CURRENT MAX AGE : 20
CIST CURRENT FORWARD DELAY : 15
TIME SINCE LAST TOPOLOGY CHANGE(SECS) : 2
TOPOLOGY CHANGE COUNT(SECS) : 0
GS-2124L(mstp)#
```

■ **set r-role**

- Syntax:  
set r-role <port range> <restricted role>
- Description:  
To set per port restricted role
- Argument:

□ <port range> syntax: 1,5-7, available from 1 to 24

<restricted role> : 0->>false,1->True

□ Possible value:

<port range> : 1 to 24

<restricted role> : 0->>false,1->True

□ Example:

```
GS-2124L(mstp)# set r-role 8-12 1
```

```
GS-2124L(mstp)# set r-role 13-16 0
```

```
GS-2124L(mstp)# show ports 0
```

```
=====
==Operational== ==Restricted==
PortPortStatus Role Path Cost Pri Hello Edge- Port P2P Role Tcn
=====
=====
1 FORWARDING DSGN 200000 128 2/2 V
2 DISCARDING dsbl 2000000 128 2/2 V
3 DISCARDING dsbl 2000000 128 2/2 V
4 DISCARDING dsbl 2000000 128 2/2 V
5 FORWARDING DSGN 200000 128 2/2 V V
6 DISCARDING dsbl 2000000 128 2/2 V
7 FORWARDING DSGN 20000 128 2/2 V V
8 DISCARDING dsbl 2000000 128 2/2 V V
9 DISCARDING dsbl 2000000 128 2/2 V V
10 DISCARDING dsbl 2000000 128 2/2 V V
11 DISCARDING dsbl 2000000 128 2/2 V V
12 DISCARDING dsbl 2000000 128 2/2 V V
13 DISCARDING dsbl 2000000 128 2/2 V
14 DISCARDING dsbl 2000000 128 2/2 V
15 DISCARDING dsbl 2000000 128 2/2 V
16 DISCARDING dsbl 2000000 128 2/2 V
17 DISCARDING dsbl 2000000 128 2/2 V
```

```

18 DISCARDING dsbl 2000000 128 2/2 V
19 DISCARDING dsbl 2000000 128 2/2 V
20 DISCARDING dsbl 2000000 128 2/2 V
21 DISCARDING dsbl 2000000 128 2/2 V
22 DISCARDING dsbl 2000000 128 2/2 V
23 DISCARDING dsbl 2000000 128 2/2 V
24 DISCARDING dsbl 2000000 128 2/2 V
GS-2124L(mstp)#

```

■ **set r-tcn**

□ Syntax:

```
set r-tcn <port range> <restricted tcn>
```

□ Description:

To set per port restricted tcn

□ Argument:

□ &lt;port range&gt; syntax: 1,5-7, available from 1 to 24

```
<restricted tcn> : 0->>false,1->True
```

□ Possible value:

```
<port range> : 1 to 24
```

```
<restricted tcn> : 0->>false,1->True
```

□ Example:

```
GS-2124L(mstp)# set r-tcn 9-10 1
```

```
GS-2124L(mstp)# set r-tcn 14-20 1
```

```
GS-2124L(mstp)# show pconf 0
```

```

Port Path Cost Priority Hello Edge-Port P2P Role Tcn
system      Enter in

```

```

=====
=====... (q to quit)

```

```

2    0 128 2 true auto false false
3    0 128 2 true auto false true
4    0 128 2 true auto false true
5    0 128 2 true auto false false

```

```

6    0 128 2 true auto false false
7    0 128 2 true auto false false
8    0 128 2 true auto true false
9    0 128 2 true auto true true
10   0 128 2 true auto true true
11   0 128 2 true auto true false
12   0 128 2 true auto true false
13   0 128 2 true auto false false
14   0 128 2 true auto false true
15   0 128 2 true auto false true
16   0 128 2 true auto false true
17   0 128 2 true auto true true
18   0 128 2 true auto true true
19   0 128 2 true auto true true
20   0 128 2 true auto true true
21   0 128 2 true auto true false
22   0 128 2 true auto true false
23   0 128 2 true auto true false
24   0 128 2 true auto true false

```

GS-2124L(mstp)#

### ■ set region-name

□ Syntax:

```
set region-name <string>
```

□ Description:

To set mstp region name(0~32 bytes)

□ Argument:

```
<string> :a null region name
```

□ Possible value:

```
<string> :1-32
```

□ Example:

```
GS-2124L(mstp)# set region-name test2
```



```
GS-2124L(mstp)# show region-info
```

```
Name : test2
```

```
Revision : 0
```

```
Instances : 0
```

```
GS-2124L(mstp)#
```

#### ■ set revision-level

- Syntax:

```
set rev <revision-level>
```

- Description:

```
To set mstp revision-level(0~65535)
```

- Argument:

```
<revision-level> :0~65535
```

- Possible value:

```
<revision-level> :0~65535
```

- Example:

```
GS-2124L(mstp)# set revision-level 30000
```

```
GS-2124L(mstp)# show region-info
```

```
Name : test2
```

```
Revision : 30000
```

```
Instances : 0
```

```
GS-2124L(mstp)#
```

#### ■ set version

- Syntax:

```
set version <stp|rstp|mstp>
```

- Description:

```
To set force-version
```

- Argument:

```
<revision-level> :0~65535
```

- Possible value:

```
<revision-level> :0~65535
```

- Example:

```
GS-2924(mstp)# set version mstp
```

■ **show instance**

□ Syntax:

```
show instance <instance-id>
```

□ Description:

To show instance status

□ Argument:

```
<instance-id> :0->CIST;1-4095->MSTI
```

□ Possible value:

```
<instance-id> :0->CIST;1-4095->MSTI
```

□ Example:

```
GS-2124L(mstp)# show instance 0
```

```
mstp status : enabled
```

```
force version : 2
```

```
instance id: 0
```

```
bridge max age : 20
```

```
bridge forward delay : 15
```

```
bridge max hops : 20
```

```
instance priority : 4096
```

```
bridge mac : 00:40:c7:5e:00:09
```

```
CIST ROOT PRIORITY : 4096
```

```
CIST ROOT MAC : 00:40:c7:5e:00:09
```

```
CIST EXTERNAL ROOT PATH COST : 0
```

```
CIST ROOT PORT ID : 0
```

```
CIST REGIONAL ROOT PRIORITY : 4096
```

```
CIST REGIONAL ROOT MAC : 00:40:c7:5e:00:09
```

```
CIST INTERNAL ROOT PATH COST : 0
```

```
CIST CURRENT MAX AGE : 20
```

```
CIST CURRENT FORWARD DELAY : 15
```

```
TIME SINCE LAST TOPOLOGY CHANGE(SECS) : 2569
```

```
TOPOLOGY CHANGE COUNT(SECS) : 0
```

GS-2124L(mstp)#

■ **show pconf**

□ Syntax:

show pconf <instance-id>

□ Description:

To show port configuration

□ Argument:

instance-id:0->CIST;1-4095->MSTI

□ Possible value:

<instance-id> :0->CIST;1-4095->MSTI

□ Example:

GS-2124L(mstp)# show pconf 0

set	r-role	Se						
2	0	128	2	true	auto	false	false	
3	0	128	2	true	auto	false	true	
4	0	128	2	true	auto	false	true	
5	0	128	2	true	auto	false	false	
6	0	128	2	true	auto	false	false	
7	0	128	2	true	auto	false	false	
8	0	128	2	true	auto	true	false	
9	0	128	2	true	auto	true	true	
10	0	128	2	true	auto	true	true	
11	0	128	2	true	auto	true	false	
12	0	128	2	true	auto	true	false	
13	0	128	2	true	auto	false	false	
14	0	128	2	true	auto	false	true	
15	0	128	2	true	auto	false	true	
16	0	128	2	true	auto	false	true	
17	0	128	2	true	auto	true	true	
18	0	128	2	true	auto	true	true	
19	0	128	2	true	auto	true	true	

```

20    0 128 2 true auto true true
21    0 128 2 true auto true false
22    0 128 2 true auto true false
23    0 128 2 true auto true false
24    0 128 2 true auto true false

```

```
GS-2124L(mstp)#
```

### ■ show ports

□ Syntax:

```
show ports <instance-id>
```

□ Description:

To show port status

□ Argument:

```
instance-id:0->CIST;1-4095->MSTI
```

□ Possible value:

```
<instance-id> :0->CIST;1-4095->MSTI
```

□ Example:

```
GS-2124L(mstp)# show ports 0
```

### ■ show region-info

□ Syntax:

```
show region-info
```

□ Description:

To show region config

□ Argument:

none

□ Possible value:

none

□ Example:

```
GS-2124L(mstp)# show region-info
```

```
Name : test2
```

```
Revision : 30000
```

```
Instances : 0
```

```
GS-2124L(mstp)#
```

### ■ show vlan-map

□ Syntax:

```
show vlan-map <instance-id>
```

□ Description:

To show vlan mapping of an instance

□ Argument:

```
<nstance-id> :0->CIST;1-4095->MSTI
```

□ Possible value:

```
<instance-id> :0->CIST;1-4095->MSTI
```

□ Example:

```
GS-2124L(mstp)# show vlan-map 0
```

```
instance 0 has those vlans :
```

```
0-4095
```

```
GS-2124L(mstp)#
```

### ° policy

#### ■ add

□ Syntax:

```
add [name <value>] [ip <value>] [port <value>] [type <value>] action  
<value>
```

□ Description:

To add a new management policy entry.

□ Argument:

```
Synopsis: add name George ip 192.168.1.1-192.168.1.90 port 2-5,8
```

```
type h,s action a
```

```
Synopsis: add name Mary ip 192.168.2.1-192.168.2.90 action deny
```

□ Possible value:

None

□ Example:

```
GS-2124L(policy)# add name Mary ip 192.168.3.1-192.168.3.4 action  
deny
```

```
GS-2124L(policy)# show
```

- 1) Name : george      IP Range : 192.168.1.1-192.168.1.90  
 Action : Accept      Access Type : HTTP SNMP  
 Port : 2 3 4 5 8
- 2) Name : rule1      IP Range : 192.168.2.1-192.168.2.30  
 Action : Deny      Access Type : HTTP TELENT SNMP  
 Port : 11 12 13 14 15
- 3) Name : Mary      IP Range : 192.168.3.1-192.168.3.4  
 Action : Deny      Access Type : Any  
 Port : Any

GS-2124L(policy)#

■ **delete**

Syntax:

delete <index>

Description:

To add a new management policy entry.

Argument:

<index> : a specific or range management policy entry(s)

e.g. delete 2,3,8-12

Possible value:

<index> : a specific or range management policy entry(s)

Example:

GS-2124L(policy)# add name rule2 ip 192.168.4.23-192.168.4.33 port 6-8 type s,t

action d

GS-2124L(policy)# show

- 1) Name : rule1      IP Range : 192.168.4.5-192.168.4.22  
 Action : Deny      Access Type : HTTP TELENT SNMP  
 Port : 2 3 4 5
- 2) Name : rule2      IP Range : 192.168.4.23-192.168.4.33  
 Action : Deny      Access Type : TELENT SNMP  
 Port : 6 7 8

```

GS-2124L(policy)# delete 2
GS-2124L(policy)# show
  1) Name   : rule1       IP Range   : 192.168.4.5-192.168.4.22
     Action : Deny       Access Type : HTTP TELENT SNMP
     Port   : 2 3 4 5
GS-2124L(policy)#

```

■ **show**

□ Syntax:

show

□ Description:

To show management policy list.

□ Argument:

none

□ Possible value:

none

□ Example:

```

GS-2124L(policy)# show
  1) Name   : rule1       IP Range   : 192.168.4.5-192.168.4.22
     Action : Deny       Access Type : HTTP TELENT SNMP
     Port   : 2 3 4 5
  2) Name   : rule2       IP Range   : 192.168.4.23-192.168.4.33
     Action : Deny       Access Type : TELENT SNMP
     Port   : 6 7 8

```

° **port**■ **clear counter**

□ Syntax:

clear counter

□ Description:

To clear all ports' counter (include simple and detail port counter) information.

□ Argument:

None

□ Possible value:

None

□ Example:

GS-2124L(port)# clear counter

### ■ set description

□ Syntax:

set description <port-range> <description>

□ Description:

To set port description

□ Argument:

<port range> syntax : 1,5-7, available from 1 to 24

<description> : set port description, max 47 characters

□ Possible value:

<port range> : 1 to 24

<description> : max 47 characters

□ Example:

GS-2124L(port)# set description 3-8 salesdepartment

GS-2124L(port)# show config

```
Speed/ Flow Maximum ExcessiveSynopsis: add name George ip
192.168.1.1-
```

```
Port Duplex Control Frame Collision Description
```

```
type
```

```
2 Auto Disabled 9600 Discard
3 Auto Disabled 9600 Discard salesdepartment
4 Auto Disabled 9600 Discard salesdepartment
5 Auto Disabled 9600 Discard salesdepartment
6 Auto Disabled 9600 Discard salesdepartment
7 Auto Disabled 9600 Discard salesdepartment
8 Auto Disabled 9600 Discard salesdepartment
9 Auto Disabled 9600 Discard
```



■ **set excessive-collision**

## □ Syntax:

```
set excessive-collision <port-range> <discard|restart>
```

## □ Description:

To set port description

## □ Argument:

<port range> syntax : 1,5-7, available from 1 to 24

## □ Possible value:

<port range> : 1 to 24

## □ Example:

```
GS-2124L(port)# set excessive-collision 6-10 restart
```

```
GS-2124L(port)# show config
```

```
Speed/ Flow Maximum Excessive
```

```
Port Duplex Control Frame Collision Description a list of previously run
command set priority
```

-----

DISCAR

```
2 Auto Disabled 9600 Discard
3 Auto Disabled 9600 Discard salesdepartment
4 Auto Disabled 9600 Discard salesdepartment
5 Auto Disabled 9600 Discard salesdepartment
6 Auto Disabled 9600 Restart salesdepartment
7 Auto Disabled 9600 Restart salesdepartment
8 Auto Disabled 9600 Restart salesdepartment
9 Auto Disabled 9600 Restart
10 Auto Disabled 9600 Restart
11 Auto Disabled 9600 Discard
```

■ **set flow-control**

## □ Syntax:

```
set flow-control <port-range> <enable|disable>
```

## □ Description:

To set per-port flow control

- Argument:

<port-range>: syntax 1,5-7, available from 1 to 24

- Possible value:

<port-range>: 1 ~ 24

- Example:

```
GS-2124L(port)# set flow-control 3-10
```

```
GS-2124L(port)# show config
```

```
1 Auto   Disabled 9600  Discard
2 Auto   Disabled 9600  Discard
3 Auto   Enabled  9600  Discard salesdepartment
4 Auto   Enabled  9600  Discard salesdepartment
5 Auto   Enabled  9600  Discard salesdepartment
6 Auto   Enabled  9600  Restart salesdepartment
7 Auto   Enabled  9600  Restart salesdepartment
8 Auto   Enabled  9600  Restart salesdepartment
9 Auto   Enabled  9600  Restart
10 Auto  Enabled  9600  Restart
11 Auto  Disabled 9600  Discard
12 Auto  Disabled 9600  Discard
```

### ■ set max-frame

- Syntax:

```
set max-frame <port-range> <value>
```

- Description:

To set per-port maximum frame size

- Argument:

<port range> syntax : 1,5-7, available from 1 to 24

<value> : Allowed value are 1518-9600 bytes.

- Possible value:

<port range> syntax : 1 to 24

<value> : 1518-9600 bytes.

- Example:

```
GS-2124L(port)# set max-frame 3-6 1518
```

```
GS-2124L(port)# show config
```

```

Speed/  Flow  Maximum Excessiveommands
2 Auto   Disabled 9600   Discard
3 Auto   Enabled  1518   Discard salesdepartment
4 Auto   Enabled  1518   Discard salesdepartment
5 Auto   Enabled  1518   Discard salesdepartment
6 Auto   Enabled  1518   Restart salesdepartment
7 Auto   Enabled  9600   Restart salesdepartment
8 Auto   Enabled  9600   Restart salesdepartment
9 Auto   Enabled  9600   Restart
10 Auto  Enabled  9600   Restart
11 Auto  Disabled 9600   Discard

```

### ■ set speed



- Syntax:

```
set <speed> <port-range>
<disable|auto|1Gfull|100full|100half|10full|10half
```

- Description:

To set port capability.

- Argument:

<port-range>:syntax 1,5-7, available from 1 to 24

<port-speed>:

auto: set auto-negotiation mode

10half: set speed/duplex 10M Half

10full: set speed/duplex 10M Full

100half: set speed/duplex 100M Half

100full: set speed/duplex 100M Full

1Gfull: set speed/duplex 1G Full

- Possible value:

<port-range>: 1 to 24

```
<port-speed>: auto, 10half, 10full, 100half, 100full, 1Gfull
```

□ Example:

```
GS-2124L(port)# set speed 3 auto
```

```
GS-2124L(port)# show status
```

```
Speed/
```

```
Port Link Duplex Rx Pause Tx Pause Description
```

```
-----
 1 Up 100M/Full Disabled Disabled
 2 Down Down Disabled Disabled
 3 Up 100M/Full Disabled Disabled
 4 Down Down Disabled Disabled
 5 Down Down Disabled Disabled
 6 Down Down Disabled Disabled
 7 Up 1G/Full Disabled Disabled
 8 Down Down Disabled Disabled
 9 Down Down Disabled Disabled
```

### ■ show config

□ Syntax:

```
show config
```

□ Description:

To display the each port's configuration information.

□ Argument:

None.

□ Possible value:

None.

□ Example:

```
GS-2124L(port)# show config
```

```
Speed/ Flow Maximum Excessive
```

```
Port Duplex Control Frame Collision Description
```

```
-----
 1 Auto Disabled 9600 Discard
```

2	1G/Full	Disabled	9600	Discard
3	Auto	Disabled	9600	Discard
4	1G/Full	Disabled	9600	Discard
5	1G/Full	Disabled	9600	Discard
6	Auto	Disabled	9600	Discard
7	Auto	Disabled	9600	Discard
8	Auto	Disabled	9600	Discard
9	Auto	Disabled	9600	Discard
10	Auto	Disabled	9600	Discard
11	Auto	Disabled	9600	Discard
12	Auto	Disabled	9600	Discard

■ **show detail-counter**

- Syntax:

```
show detail-counter <port>
```

- Description:

To display the display detail port counter.

- Argument:

<port>: port, available from 1 to 24

- Possible value:

<port>:1 ~ 24

- Example:

```
GS-2124L (port)# show detail-counter 3
```

Rx Multicast	6	Tx Multicast	641
Rx Broadcast	94	Tx Broadcast	5251
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	

---

Rx 64 Bytes	7381	Tx 64 Bytes	4351
Rx 65-127 Bytes	291	Tx 65-127 Bytes	2342
Rx 128-255 Bytes	118	Tx 128-255 Bytes	605
Rx 256-511 Bytes	53	Tx 256-511 Bytes	1081

Rx 512-1023 Bytes	33	Tx 512-1023 Bytes	144
Rx 1024-1526 Bytes	28	Tx 1024-1526 Bytes	11453
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Error Counters		Transmit Error Counters	

```

-----
Rx Drops          0 Tx Drops          0
Rx CRC/Alignment  0 Tx Late/Exc. Coll.  0
Rx Undersize      0
Rx Oversize       0
Rx Fragments      0
Rx Jabber         0

```

### ■ show sfp

- Syntax:

```
show sfp <port>
```

- Description:

To display the SFP module information.

- Argument:

<port>: SFP port of the switch, available from 1, 24

- Possible value:

<port>: 1- 24,

- Example:

```
GS-2124L(port)# show sfp 11
```

Port 11 SFP information

```

-----
Connector Type    : SFP - Unknown or unspecified
Fiber Type        : Reserved
Tx Central Wavelength : 0
Baud Rate         : 1G
Vendor OUI        : 00:00:00
Vendor Name       : FIBERXON INC.
Vendor PN         : FTM-C012R-LC

```

```

Vendor Rev      : 10
Vendor SN      : PP220052901281
Date Code     : 051012
Temperature    : none
Vcc           : none
Mon1 (Bias) mA : none
Mon2 (TX PWR) : none
Mon3 (RX PWR) : none
GS-2124L(port)#
Port 23 SFP information

```

```

-----
Connector Type  : SFP - LC
Fiber Type     : Multi-mode (MM)
Tx Central Wavelength : 850
Baud Rate      : 1G
Vendor OUI     : 00:40:c7
Vendor Name    : APAC Opto
Vendor PN      : KM28-C3S-TC-N
Vendor Rev     : 0000
Vendor SN      : 5425010708
Date Code     : 050530
Temperature    : none
Vcc           : none
Mon1 (Bias) mA : none
Mon2 (TX PWR) : none
Mon3 (RX PWR) : none

```

■ **show simple-counter**

- Syntax:  
show simple-counter
- Description:

To display the summary counting of each port's traffic.

□ Argument:

None.

□ Possible value:

None.

□ Example:

```
GS-2124L (port)# show simple-counter
```

```
set max-frame      Set per-port maximum frame size
```

13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0

```
GS-2124L(port)#
```

#### ■ show status

□ Syntax:

```
show status
```

□ Description:

To display the port's current status.

□ Argument:

None.

□ Possible value:

None.

□ Example:



```

GS-2124L(port)# show status
      Speed/1G/Full  Disable
Port Link Duplex  Rx Pause Tx Pause  Description
 3 Auto   Disabled 9600   Discard
 2 Down Down   Disabled Disabled
 3 Up   100M/Full Disabled Disabled
 4 Down Down   Disabled Disabled
 5 Down Down   Disabled Disabled
 6 Down Down   Disabled Disabled
 7 Up   1G/Full Disabled Disabled
 8 Down Down   Disabled Disabled
 9 Down Down   Disabled Disabled
10 Down Down   Disabled Disabled
11 Up   Null/Half Disabled Disabled
12 Down Down   Disabled Disabled
13 Down Down   Disabled Disabled
14 Down Down   Disabled Disabled
15 Down Down   Disabled Disabled
16 Down Down   Disabled Disabled
17 Down Down   Disabled Disabled
18 Down Down   Disabled Disabled
19 Down Down   Disabled Disabled
20 Down Down   Disabled Disabled
21 Down Down   Disabled Disabled
22 Down Down   Disabled Disabled
23 Down Down   Disabled Disabled
24 Down Down   Disabled Disabled
GS-2124L(port)#

```

## ° qos

## ■ &lt;&lt;ports&gt;&gt;



## ■ set class

- Syntax:

set class <#>

- Description:

To set number of classes.

- Argument:

#: Number of classes, available 1, 2, 4

- Possible value:

<#>: 1,2,4

- Example:

GS-2124L(qos-ports)# set class 2

GS-2124L(qos-ports)#

## ■ set port

- Syntax:

set port <range> <default class> <qcl> <user priority> <queuing mode>  
<lo

w queue weighted> <normal queue weighted> <medium queue  
weighted> <high queue we  
ighted>

- Description:

To set port information.

- Argument:

<range syntax>: 1,5-7, available from 1 to 24

<default class option>: low | normal | medium | high

<qcl> : available from 1 to 24

<user priority>: available from 0 to 7

<queuing mode>: strict | weighted

<low queue weighted>: 1 / 2 / 4 / 8

<normal queue weighted>: 1 / 2 / 4 / 8

<medium queue weighted> : 1 / 2 / 4 / 8

<high queue weighted>: 1 / 2 / 4 / 8

□ Possible value:

<range syntax>: 1 to 24

<default class option>: low | normal | medium | high

<qcl> : 1 to 24

<user priority>: 0 to 7

<queuing mode>: strict | weighted

<low queue weighted>: 1 / 2 / 4 / 8

<normal queue weighted>: 1 / 2 / 4 / 8

<medium queue weighted> : 1 / 2 / 4 / 8

<high queue weighted>: 1 / 2 / 4 / 8

□ Example:

```
GS-2124L(qos-ports)# set port 2 medium 1 3 weithted 2 2 2 2
```

```
GS-2124L(qos-ports)# show
```

```
 2 Medium    1    3    Weighted Fair  2 / 2 / 2 / 2
```

```
 3 Low      1    0    Strict Priority 1 / 2 / 4 / 8
```

```
 4 Low      1    0    Strict Priority 1 / 2 / 4 / 8
```

```
 5 Low      1    0    Strict Priority 1 / 2 / 4 / 8
```

```
 6 Low      1    0    Strict Priority 1 / 2 / 4 / 8
```

```
 7 Low      1    0    Strict Priority 1 / 2 / 4 / 8
```

```
 8 Low      1    0    Strict Priority 1 / 2 / 4 / 8
```

```
 9 Low      1    0    Strict Priority 1 / 2 / 4 / 8
```

```
10 Low      1    0    Strict Priority 1 / 2 / 4 / 8
```

```
11 Low      1    0    Strict Priority 1 / 2 / 4 / 8
```

```
12 Low      1    0    Strict Priority 1 / 2 / 4 / 8
```

```
13 Low      1    0    Strict Priority 1 / 2 / 4 / 8
```

```
14 Low      1    0    Strict Priority 1 / 2 / 4 / 8
```

```
jKjKjK
```

```
GS-2124L(qos-ports)#
```

■ **show**

## □ Syntax:

show

## □ Description:

To show port information.

## □ Argument:

none

## □ Possible value:

none

## □ Example:

GS-2124L(qos-ports)# show

Number of Classes:2

2 Medium 1 3 Weighted Fair 2 / 2 / 2 / 2

3 Low 1 0 Strict Priority 1 / 2 / 4 / 8

4 Low 1 0 Strict Priority 1 / 2 / 4 / 8

5 Low 1 0 Strict Priority 1 / 2 / 4 / 8

6 Low 1 0 Strict Priority 1 / 2 / 4 / 8

7 Low 1 0 Strict Priority 1 / 2 / 4 / 8

8 Low 1 0 Strict Priority 1 / 2 / 4 / 8

9 Low 1 0 Strict Priority 1 / 2 / 4 / 8

10 Low 1 0 Strict Priority 1 / 2 / 4 / 8

&lt;&lt;qcl&gt;&gt;

■ **set**

## □ Syntax:

set &lt;dscp&gt; &lt;tos&gt; &lt;tagpriority&gt; &lt;qce type&gt; &lt;value&gt; &lt;class&gt;

## □ Description:

To add the QCE entry in the specific QCL

## □ Argument:

&lt;dscp&gt;: dscp field, syntax 1,5-7, available from 0 to 63

&lt;tos&gt; : tos priority , available from 1 to 8

&lt;tagpriority&gt; : tag priority, available from 1 to 8

<qce type> : ethernet

<value> : 0xffff0

<class> : high

□ Possible value:

<dscp>: dscp field, syntax 1,5-7, available from 0 to 63

<tos> : tos priority , available from 1 to 8

<tagpriority> : tag priority, available from 1 to 8

<qce type> : ethernet

<value> : 0xffff0

<class> : high

□ Example:

```
GS-2124L(qos-qcl)# set 2 0 3 ethernet 0xffff0 high
```

```
GS-2124L(qos-qcl)# show 2 1
```

```
QCE Type:      Ethernet Type
```

```
Ethernet Type Value:0xffff0
```

```
Traffic Class:  High
```

```
GS-2124L(qos-qcl)#
```

#### ■ move

□ Syntax:

```
move <qcl> <qce> <new qce>
```

□ Description:

To move up the specific QCE entry in the specific QCL

□ Argument:

<qcl> : the qcl number, available from 1 to 24.

<qce> : the original qce number, available from 1 to 12.

<new qce> : the new qce number, available from 1 to 12.

□ Possible value:

<qcl> : available from 1 to 24.

<qce> : available from 1 to 12.

<new qce> : available from 1 to 12.

□ Example:

GS-2124L(qos-qcl)# move 2 1 1

### ■ delete

□ Syntax:

delete <qcl> <qce range>

□ Description:

To delete the specific QCE entry in the specific QCL.

□ Argument:

<qcl> : the qcl number, available from 1 to 24.

<qce range> : 1,5-7, available from 1 to 12

□ Possible value:

<qcl> : available from 1 to 24.

<qce range> : available from 1 to 12

□ Example:

GS-2124L(qos-qcl)# delete 2 1

<<rate>>

### ■ set

□ Syntax:

set <range> <policer enabled> <rate> <unit> <shaper enabled> <rate>  
<unit>

□ Description:

To set rate limit configuration

□ Argument:

<range syntax> : 1,5-7, available from 1 to 24

<policer enabled> : 1 means enable and 0 means disable

<rate>: allowed values are 500kbps-1Gkps

<unit>: 'k' means kbps and 'm' means mbps

<shaper enabled>: 1 means enable and 0 means disable

<rate>: allowed values are 500kbps-1Gkps

<unit>: 'k' means kbps and 'm' means mbps

□ Possible value:

□ range syntax: 1,5-7, available from 1 to 24

policer enabled: 1 means enable and 0 means disable

rate: allowed values are 500kbps-1Gkps

unit: 'k' means kbps and 'm' means mbps

shaper enabled: 1 means enable and 0 means disable

rate: allowed values are 500kbps-1Gkps

unit: 'k' means kbps and 'm' means mbps

□ Example:

```
GS-2124L(qos-rate)# set 2 1 1000 m 1 1000 m
```

```
GS-2124L(qos-rate)# show
```

2	V	1000	Mbps	V	1000	Mbps
3		500	kbps		500	kbps
4		500	kbps		500	kbps
5		500	kbps		500	kbps
6		500	kbps		500	kbps
7		500	kbps		500	kbps
8		500	kbps		500	kbps
9		500	kbps		500	kbps
10		500	kbps		500	kbps

■ << storm >>

■ set broadcast

■

□ Syntax:

```
set broadcast <status> <rate>
```

□ Description:

To set broadcast storm control configuration

□ Argument:

<status> : 1 means enable and 0 means disable

<rate> : 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k

, 256k, 512k

□ Possible value:

<status> : 1 means enable and 0 means disable

<rate> : 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k, 512k

□ Example:

```
GS-2124L(qos-storm)# set broadcast 1 512
```

```
GS-2124L(qos-storm)# show
```

```
Frame Type   Status   Rate(Packet Per Second)
```

```
-----
Flooded unicast      1
Multicast             1
Broadcast            V   512
```

### ■ set multicast

□ Syntax:

```
set multicast <status> <rate>
```

□ Description:

To set multicast storm control configuration

□ Argument:

<status> : 1 means enable and 0 means disable

<rate> : 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k, 512k

□ Possible value:

<status> : 1 means enable and 0 means disable

<rate> : 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k, 512k

□ Example:

```
GS-2124L(qos-storm)# set multicast 1 64
```

```
GS-2124L(qos-storm)# show
```

```
Frame Type   Status   Rate(Packet Per Second)
```

```
-----
```



```

Flooded unicast    1
Multicast    V    64
Broadcast    V    512

```

### ■ set unicast

#### □ Syntax:

```
set unicast <status> <rate>
```

#### □ Description:

To set flooded unicast storm control configuration

#### □ Argument:

<status> : 1 means enable and 0 means disable

<rate> : 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k

, 256k, 512k

#### □ Possible value:

<status> : 1 means enable and 0 means disable

<rate> : 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k

, 256k, 512k

#### □ Example:

```
GS-2124L(qos-storm)# set unicast 1 128
```

```
GS-2124L(qos-storm)# show
```

```
Frame Type    Status    Rate(Packet Per Second)
```

```
-----
```

```
Flooded unicast V    128
```

```
Multicast    V    64
```

```
Broadcast    V    512
```

### ■ show

#### □ Syntax:

```
show
```

#### □ Description:

To show storm control configuration

□ Argument:

none

□ Possible value:

none

□ Example:

GS-2124L(qos-storm)# show

Frame Type	Status	Rate(Packet Per Second)
-----		
Flooded unicast	V	128
Multicast	V	64
Broadcast	V	512

#### ° reboot

##### ■ reboot

□ Syntax:

reboot

□ Description:

To reboot the system.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L# reboot

#### ° snmp

##### ■ <<disable>>

□ Syntax:

disable set-ability

disable snmp

□ Description:

The Disable here is used for the de-activation of snmp or set-community.

- Argument:

None.

- Possible value:

None.

- Example:

GS-2124L(sntp)# disable snmp

GS-2124L(sntp)# disable set-ability

### ■ <<enable>>

- Syntax:

enable set-ability

enable snmp

- Description:

The Enable here is used for the activation snmp or set-community.

- Argument:

None.

- Possible value:

None.

- Example:

GS-2124L(sntp)# enable snmp

GS-2124L(sntp)# enable set-ability

### ■ <<set>>

- Syntax:

set get-community <community>

set set-community <community>

set trap <#> <ip> [port] [community]

- Description:

The Set here is used for the setup of get-community, set-community, trap host ip, host port and trap-community.

- Argument:

<#>: trap number

<ip>: ip address or domain name

<port>: trap port

<community>:trap community name

□ Possible value:

<#>: 1 to 6

<port>:1~65535

□ Example:

```
GS-2124L(snmp)# set get-community public
```

```
GS-2124L(snmp)# set set-community private
```

```
GS-2124L(snmp)# set trap 1 192.168.1.1 162 public
```

### ■ show

□ Syntax:

show

□ Description:

The Show here is to display the configuration of SNMP.

□ Argument:

None.

□ Possible value:

None.

□ Example:

```
GS-2124L(snmp)# show
```

```
SNMP      : Enable
```

```
Get Community: public
```

```
Set Community: private [Enable]
```

```
Trap Host 1 IP Address: 192.168.1.1 Port: 162 Community: public
```

```
Trap Host 2 IP Address: 0.0.0.0 Port: 162 Community: public
```

```
Trap Host 3 IP Address: 0.0.0.0 Port: 162 Community: public
```

```
Trap Host 4 IP Address: 0.0.0.0 Port: 162 Community: public
```

```
Trap Host 5 IP Address: 0.0.0.0 Port: 162 Community: public
```

```
Trap Host 6 IP Address: 0.0.0.0 Port: 162 Community: public
```

### ° stp

#### ■ MCheck

□ Syntax:

MCheck <range>

□ Description:

To force the port to transmit RST BPDUs.

□ Argument:

<range>: syntax 1,5-7, available from 1 to 24

□ Possible value:

<range>: 1 to 24

□ Example:

GS-2124L(stp)# Mcheck 1-8

disable

□ Syntax:

disable

□ Description:

To disable the STP function.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L(stp)# disable

enable

□ Syntax:

enable

□ Description:

To enable the STP function.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L(stp)# enable

■ **set config**

## □ Syntax:

set config <Bridge Priority> <Hello Time> <Max. Age> <Forward Delay>

## □ Description:

To set up the parameters of STP.

## □ Argument:

<Bridge Priority>: priority must be a multiple of 4096, available from 0 to 61440.

<Hello Time>: available from 1 to 10.

<Max. Age>: available from 6 to 40.

<Forward Delay>: available from 4 to 30.

Note:  $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$

$\text{Max Age} \geq 2 * (\text{Hello Time} + 1)$

## □ Possible value:

<Bridge Priority>: 0 to 61440

<Hello Time>: 1 to 10

<Max. Age>: 6 to 40

<Forward Delay>: 4 to 30

## □ Example:

GS-2124L(stp)# set config 61440 2 20 15

■ **set port**

## □ Syntax:

set port <range> <path cost> <priority> <edge\_port> <admin p2p>

## □ Description:

To set up the port information of STP.

## □ Argument:

<range>: syntax 1,5-7, available from 1 to 24

<path cost>: 0, 1-20000000. The value zero means auto status

<priority>: priority must be a multiple of 16, available from 0 to 240

<edge\_port> : Admin Edge Port, <yes|no>

<admin p2p>: Admin point to point, <auto|true|false>

- Possible value:  
<range>: 1 to 24  
<path cost>: 0, 1-200000000  
<priority>: 0 to 240  
<edge\_port>: yes / no  
<admin p2p>: auto / true / false

- Example:  
GS-2124L(stp)# set port 1-16 0 128 yes auto

### ■ set version

- Syntax:  
set version <stp|rstp>
- Description:  
To set up the version of STP.
- Argument:  
<stp|rstp>:stp / rstp
- Possible value:  
<stp|rstp>:stp / rstp
- Example:  
GS-2124L(stp)# set version rstp\_

### ■ show config

- Syntax:  
show config
- Description:  
To display the configuration of STP.
- Argument:  
None.
- Possible value:  
None.
- Example:  
GS-2124L(stp)# show config  
STP State Configuration :  
Spanning Tree Protocol : Enabled

Bridge Priority (0-61440) : 61440

Hello Time (1-10 sec) : 2

Max. Age (6-40 sec) : 20

Forward Delay (4-30 sec) : 15

Force Version : RSTP

### ■ show port

□ Syntax:

show port

□ Description:

To display the port information of STP.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L# stp

GS-2124L(stp)# show port

Port Port Status Path Cost Priority Admin Edge Port Admin Point To Point

Port	Port	Status	Path	Cost	Priority	Admin	Edge	Port	Admin	Point To Point
1	DISCARDING	2000000	128	No	Auto					
2	DISCARDING	2000000	128	No	Auto					
3	DISCARDING	2000000	128	No	Auto					
4	DISCARDING	2000000	128	No	Auto					
5	DISCARDING	2000000	128	No	Auto					
6	DISCARDING	2000000	128	No	Auto					
7	DISCARDING	2000000	128	No	Auto					
8	DISCARDING	2000000	128	No	Auto					
9	DISCARDING	2000000	128	No	Auto					
10	DISCARDING	2000000	128	No	Auto					
11	DISCARDING	2000000	128	No	Auto					



12	DISCARDING	2000000	128	No	Auto
13	DISCARDING	2000000	128	No	Auto
14	DISCARDING	2000000	128	No	Auto
15	DISCARDING	2000000	128	No	Auto
16	DISCARDING	2000000	128	No	Auto
17	DISCARDING	2000000	128	No	Auto
18	DISCARDING	2000000	128	No	Auto
19	DISCARDING	2000000	128	No	Auto
20	DISCARDING	2000000	128	No	Auto
21	DISCARDING	2000000	128	No	Auto
22	DISCARDING	2000000	128	No	Auto
...(q to quit)					
23	DISCARDING	2000000	128	No	Auto
24	DISCARDING	2000000	128	No	Auto

■ **show status**

□ Syntax:

show status

□ Description:

To display the status of STP.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L(stp)# show status

STP Status :

STP State : Enabled

Bridge ID : 00:40:C7:D8:09:1D

Bridge Priority : 61440

Designated Root : 00:40:C7:D8:09:1D

Designated Priority : 61440

```

Root Port                : 0
Root Path Cost           : 0
Current Max. Age(sec)    : 20
Current Forward Delay(sec) : 15
Hello Time(sec)          : 2
STP Topology Change Count : 0
Time Since Last Topology Change(sec) : 848_

```

### ° system

#### ■ set contact

□ Syntax:

```
set contact <contact string>
```

□ Description:

To set the contact description of the switch.

□ Argument:

<contact>:string length up to 40 characters.

□ Possible value:

<contact>: A, b, c, d, ... ,z and 1, 2, 3, .... etc.

□ Example:

```
GS-2124L(system)# set contact Taipei
```

#### ■ set device-name

□ Syntax:

```
set device-name <device-name string>
```

□ Description:

To set the device name description of the switch.

□ Argument:

<device-name>: string length up to 40 characters.

□ Possible value:

<device-name>: A, b, c, d, ... ,z and 1, 2, 3, .... etc.

□ Example:

```
GS-2124L(system)# set device-name CR-2600
```

■ **set location**

## □ Syntax:

```
set location <location string>
```

## □ Description:

To set the location description of the switch.

## □ Argument:

<location>: string length up to 40 characters.

## □ Possible value:

<location>: A, b, c, d, ..., z and 1, 2, 3, .... etc.

## □ Example:

```
GS-2124L(system)# set location Taipei
```

■ **show**

## □ Syntax:

```
show
```

## □ Description:

To display the basic information of the switch.

## □ Argument:

None.

## □ Possible value:

None.

## □ Example:

```
GS-2124L(system)# show
```

```
Model Name           : GS-2124L
```

```
System Description   : L2 Managed Switch
```

```
Location             :
```

```
Contact              :
```

```
Device Name          : GS-2124L
```

```
System Up Time       : 0 Days 0 Hours 4 Mins 14 Secs
```

```
Current Time         : Tue Jan 17 16:28:46 2006
```

```
BIOS Version         : v1.05
```

```
Firmware Version     : v2.08
```

Hardware-Mechanical Version : v1.01-v1.01  
 Serial Number : 030C02000003  
 Host IP Address : 192.168.1.1  
 Host MAC Address : 00-40-c7-e7-00-10  
 Device Port : UART \* 1, TP \* 22, Dual-Media Port(RJ45/SFP) \* 2  
 RAM Size : 16 M  
 Flash Size : 2 M

### ° traplog

#### ■ clear

Syntax:

#### clear

Description:

To clear trap log.

Argument:

none

Possible value:

none

Example:

GS-2124L(traplog)# clear

GS-2124L(traplog)# show

No	time	desc
-----		

#### ■ show

Syntax:

#### show

Description:

To display the trap log.

Argument:

None.

Possible value:

None.

## □ Example:

```
GS-2124L(tftp)# show
```

```
2 Mon Mar 17 15:18:38 2008gvrp mode> <qce type> .
```

```
    Dual Media Swapped [Port:1][SwapTo:TP]ge hostnamexit/ 4 / 8
```

```
3 Mon Mar 17 15:18:38 2008nto igmp mode, available from
```

```
    Link Up [Port:1]Enter into ip mode
```

```
6 Mon Mar 17 15:18:38 2008
```

```
    Dual Media Swapped [Port:5][SwapTo:TP]
```

```
7 Mon Mar 17 15:18:38 2008
```

```
    Link Up [Port:5]
```

```
8 Mon Mar 17 15:18:48 2008
```

```
    Login [admin]
```

## ° time

## ■ set daylightsaving

## □ Syntax:

```
set daylightsaving <hr> <MM/DD/HH> <mm/dd/hh>
```

## □ Description:

To set up the daylight saving.

## □ Argument:

hr : daylight saving hour, range: -5 to +5

MM : daylight saving start Month (01-12)

DD : daylight saving start Day (01-31)

HH : daylight saving start Hour (00-23)

mm : daylight saving end Month (01-12)

dd : daylight saving end Day (01-31)

hh : daylight saving end Hour (00-23)

## □ Possible value:

hr : -5 to +5

MM : (01-12)

DD : (01-31)

HH : (00-23)

mm : (01-12)

dd : (01-31)

hh : (00-23)

□ Example:

```
GS-2124L(time)# set daylightsaving 3 10/12/01 11/12/01
```

Save Successfully

### ■ set manual

□ Syntax:

```
set manual <YYYY/MM/DD> <hh:mm:ss>
```

□ Description:

To set up the current time manually.

□ Argument:

YYYY : Year (2000-2036)      MM : Month (01-12)

DD : Day (01-31)      hh : Hour (00-23)

mm : Minute (00-59)      ss : Second (00-59)

□ Possible value:

YYYY : (2000-2036)      MM : (01-12)

DD : (01-31)      hh : (00-23)

mm : (00-59)      ss : (00-59)

□ Example:

```
GS-2124L(time)# set manual 2004/12/23 16:18:00
```

### ■ set ntp

□ Syntax:

```
set ntp <ip> <timezone>
```

□ Description:

To set up the current time via NTP server.

□ Argument:

<ip>: ntp server ip address or domain name

<timezone>: time zone (GMT), range: -12 to +13

□ Possible value:

<timezone>: -12,-11...,0,1...,13

□ Example:

```
GS-2124L(time)# set ntp clock.via.net 8
```

```
Synchronizing...(1)
```

```
Synchronization success
```

### ■ show

□ Syntax:

```
show
```

□ Description:

To show the time configuration, including "Current Time", "NTP Server", "Timezone", "Daylight Saving", "Daylight Saving Start" and "Daylight Saving End"

□ Argument:

None.

□ Possible value:

None.

□ Example:

```
GS-2124L(time)# show
```

```
Current Time: Thu Thu 14 15:04:03 2005
```

```
NTP Server: 209.81.9.7
```

```
Timezone: GMT+8:00
```

```
Day light Saving: 0 Hours
```

```
Day light Saving Start: Mth: 1 Day: 1 Hour: 0
```

```
Day light Saving End : Mth: 1 Day: 1 Hour: 0
```

```
GS-2124L(time)#
```

### ° trunk

#### ■ del trunk

□ Syntax:

```
del trunk <port-range>
```

□ Description:

To delete the trunking port.

- Argument:  
<port-range>: port range, syntax 1,5-7, available from 1 to 24
- Possible value:  
<port-range>: 1 to 24
- Example:  
GS-2124L(trunk)# del trunk 1



### ■ set priority

- Syntax:  
set priority <range>
- Description:  
To set up the LACP system priority.
- Argument:  
<range>: available from 1 to 65535.
- Possible value:  
<range>: 1 to 65535, default: 32768
- Example:  
GS-2124L(trunk)# set priority 33333



### ■ set trunk

- Syntax:  
set trunk <port-range> <method> <group> <active LACP>
- Description:  
To set up the status of trunk, including the group number and mode of the trunk as well as LACP mode.
- Argument:  
<port-range> : port range, syntax 1,5-7, available from 1 to 24  
<method>:  
static : adopt the static link aggregation  
lacp : adopt the dynamic link aggregation- link aggregation control protocol  
<group>: 1-8.  
<active LACP>:



active : set the LACP to active mode  
 passive : set the LACP to passive mode

□ Possible value:

<port-range> : 1 to 24

<method>: static / lacp

<group>: 1-8.

<active LACP>: active /passive

□ Example:

```
GS-2124L(trunk)# set trunk 1-4 lacp 1 active
```

### ■ show aggtr-view

□ Syntax:

```
show aggtr-view
```

□ Description:

To display the aggregator list.

□ Argument:

None.

□ Possible value:

None.

□ Example:

```
GS-2124L(trunk)# show aggtr-view
```

```
Aggregator 1) Method: None
```

```
    Member Ports: 1
```

```
    Ready Ports: 1
```

```
Aggregator 2) Method: LACP
```

```
    Member Ports: 2
```

```
    Ready Ports:
```

```
                :
```

### ■ show lacp-detail

□ Syntax:

```
show lacp-detail <aggtr>
```

□ Description:

To display the detailed information of the LACP trunk group.

□ Argument:

<aggr>: aggregator, available from 1 to 24

□ Possible value:

<aggr>: 1 to 24

□ Example:

GS-2124L(trunk)# show lacp-detail 2

Aggregator 2 Information:

Actor		Partner	
System Priority	MAC Address	System Priority	MAC Address
32768	00-40-c7-e8-00-02	32768	00-00-00-00-00-00
Port	Key	Port	Key
2	257	2	0

### ■ show lacp-priority

□ Syntax:

show lacp-priority

□ Description:

To display the value of LACP Priority.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L(trunk)# show lacp-priority

LACP System Priority : 32768

### ■ show status

□ Syntax:

show status

## □ Description:

To display the aggregator status and the settings of each port.

## □ Argument:

None.

## □ Possible value:

None.

## □ Example:

GS-2124L(trunk)# show status

```

                Trunk Port Setting      Trunk Port Status
-----
port  Method  Group  Active LACP  Aggtregator  Status
=====
1     None    0     Active  1     Ready
2     LACP    1     Active  2     ---
3     LACP    1     Active  3     ---
4     LACP    1     Active  4     ---
5     LACP    1     Active  5     ---
6     LACP    1     Active  6     ---
7     LACP    1     Active  7     ---
:
19    None    0     Active  19    ---
20    None    0     Active  20    ---
21    None    0     Active  21    ---
22    None    0     Active  22    ---
23    None    0     Active  23    ---
24    None    0     Active  24    ---

```

## ° vlan

## ■ del port-group

## □ Syntax:

del port-group <name>

- Description:

To delete the port-based vlan group.

- Argument:

<name>: which vlan group you want to delete.

- Possible value:

<name>: port-vlan name

- Example:

```
GS-2124L(vlan)# del port-group VLAN-2
```

### ■ del tag-group

- Syntax:

```
del tag-group <vid>
```

- Description:

To delete the tag-based vlan group.

- Argument:

<vid>: which vlan group you want to delete, available from 1 to 4094

- Possible value:

<vid>: 1 to 4094

- Example:

```
GS-2124L(vlan)# del tag-group 2
```

```
disable drop-untag
```

- Syntax:

```
disable drop-untag <range>
```

- Description:

Don't drop the untagged frames.

- Argument:

<range> : which port(s) you want to set, syntax 1,5-7, available from 1 to 24

- Possible value:

<range>: 1 to 24

- Example:

```
GS-2124L(vlan)# disable drop-untag 5-10
```

```
disable sym-vlan
```

- Syntax:  
disable sym-vlan <range>
- Description:  
To drop frames from the non-member port.
- Argument:  
<range>: which port(s) you want to set, syntax 1,5-7, available from 1 to 24
- Possible value:  
<range>: 1 to 24
- Example:  
GS-2124L(vlan)# disable sym-vlan 5-10  
enable drop-untag
- Syntax:  
enable drop-untag <range>
- Description:  
To drop the untagged frames.
- Argument:  
<range>: which port(s) you want to set, syntax 1,5-7, available from 1 to 24
- Possible value:  
<range>: 1 to 24
- Example:  
GS-2124L(vlan)# enable drop-untag 5-10  
enable sym-vlan
- Syntax:  
enable sym-vlan <range>
- Description:  
To drop frames from the non-member port.
- Argument:  
<range> : which port(s) you want to set, syntax 1,5-7, available from 1 to 24
- Possible value:

<range>: 1 to 24

□ Example:

```
GS-2124L(vlan)# enable sym-vlan 5-10
```

### ■ set mode

□ Syntax:

```
set mode <disable|port|tag|metro|double-tag> [up-link]
```

□ Description:

To switch VLAN mode, including disable, port-based, tag-based, metro and double-tag modes.

□ Argument:

<disable>: vlan disable

<tag>: set tag-based vlan

<port>: set port-based vlan

<metro>: set metro mode vlan

<double-tag>: enable Q-in-Q function

<up-link>: syntax 1,5-7, available from 23 to 24, only for metro mode vlan

□ Possible value:

<disable|port|tag|metro|double-tag>: disable,port,tag,metro,double-tag

[up-link]: 23 or 24 or "23,24"

□ Example:

```
GS-2124L(vlan)# set mode port
```

### ■ set port-group

□ Syntax:

```
set port-group <name> <range>
```

□ Description:

To add or edit a port-based VLAN group.

□ Argument:

<name>: port-vlan name

<range>: syntax 1,5-7, available from 1 to 24

□ Possible value:

<range>: 1 to 24

- Example:

```
GS-2124L(vlan)# set port-group VLAN-1 2-5,6,15-13
```

### ■ set port-role

- Syntax:

```
set port-role <range> <access|trunk|hybrid> [vid]
```

- Description:

To set egress rule: configure the port roles.

- Argument:

<range> :which port(s) you want to set, syntax 1,5-7, available from 1 to 24

<access>: Do not tag frames

<trunk>: Tag all frames

<hybrid>: Tag all frames except a specific VID

<vid>: untag-vid for hybrid port

- Possible value:

<range>: 1 to 24

<vid>: 1 to 4094

- Example:

```
GS-2124L(vlan)# set port-role 5 hybrid 6
```

### ■ set pvid

- Syntax:

```
set pvid <range> <pvid>
```

- Description:

To set the pvid of vlan.

- Argument:

<range>: which port(s) you want to set PVID(s), syntax 1,5-7, available from

1 to 24

<pvid>: which PVID(s) you want to set, available from 1 to 4094

- Possible value:

<range>: 1 to 24

<pvid>: 1 to 4094

- Example:

```
GS-2124L(vlan)# set pvid 3,5,6-8 5
```

### ■ set tag-group

- Syntax:

```
set tag-group <vid> <name> <range> <#>
```

- Description:

To add or edit the tag-based vlan group.

- Argument:

<vid>: vlan ID, range from 1 to 4094

<name>: tag-vlan name

<range>: vlan group members, syntax 1,5-7, available from 1 to 24

<#>: sym/asym vlan setting. 1: symmetric vlan, 0: asymmetric vlan

- Possible value:

<vid>: 1 to 4094

<range>: 1 to 24

<#>: 0 or 1

- Example:

```
GS-2124L(vlan)# set tag-group 2 VLAN-2 2-5,6,15-13 0
```

### ■ show group

- Syntax:

```
show group
```

- Description:

To display the vlan mode and vlan group.

- Argument:

None.

- Possible value:

None.

- Example:

```
GS-2124L(vlan)# show group
```

Vlan mode is double-tag.

1) Vlan Name : default

Vlan ID : 1



Sym-vlan : Disable

Member : 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

2) Vlan Name : VLAN-2

Vlan ID : 2

Sym-vlan : Disable

Member : 2 3 4 5 6 13 14 15

### ■ show port

□ Syntax:

show port

□ Description:

To display pvid, ingress/egress rule.

□ Argument:

None.

□ Possible value:

None.

□ Example:

GS-2124L(vlan)# show pvid

Port	PVID	Rule1	Rule2	Port Rule	Untag Vid
1	1	Disable	Disable	Access	-
2	1	Disable	Disable	Access	-
3	5	Disable	Disable	Access	-
4	1	Disable	Disable	Access	-
5	5	Enable	Disable	Hybrid	6
6	5	Enable	Disable	Access	-
7	5	Enable	Disable	Access	-
8	5	Enable	Disable	Access	-
9	1	Enable	Disable	Access	-
10	1	Enable	Disable	Access	-
11	1	Disable	Disable	Access	-

-----

1	1	Disable	Disable	Access	-
2	1	Disable	Disable	Access	-
3	5	Disable	Disable	Access	-
4	1	Disable	Disable	Access	-
5	5	Enable	Disable	Hybrid	6
6	5	Enable	Disable	Access	-
7	5	Enable	Disable	Access	-
8	5	Enable	Disable	Access	-
9	1	Enable	Disable	Access	-
10	1	Enable	Disable	Access	-
11	1	Disable	Disable	Access	-

```
                :  
                :  
23  1  Disable  Disable  Access  -  
24  1  Disable  Disable  Access  -
```

## 6 Appendix

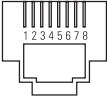
### 6.1 Performance data and specifications

LANCOM GS-2124		
Performance	Switching technology	Store and forward with latency less than 5 µs
	MAC addresses	Support of max 8K MAC addresses
	Throughput	max. 48 Gbps on the backplane
	Virtual Stacking Management (VSM)	Supports stacking of up to 16 devices, several switches can be managed via one ip address
	VLAN	Port based and IEEE 802.1q tag based VLAN with up to 4096 VLAN and up to 256 active VLANs; Supports ingress and egress packet filter in port based VLAN
LAN protocols	Link Aggregation Control Protocol (LACP)	Max 12 groups, max 16 member per group, supports DA, SA and DA+SA MAC based trunking with automatic failover
	Multicasting	Supports IGMP snooping including active and passive mode
	GVRP/GARP	802.1q with GVRP/GARP
	Spanning Tree Protokoll (STP) / Rapid STP / Multiple STP	802.1d/1w/1s
Interfaces	Ethernet ports	20 ports 10/100/1000 Mbps ethernet, 4 Combo ports TP/SFP 10/100/1000 Mbps
	Serial interface	Serial configuration interface
Power supply		Internal power supply unit (110–230 V, 50-60 Hz)
Housing		Robust metal housing, 19" 1U (440 x 44 x 209 mm) with removable mounting brackets, network connectors on the front
CE		CE conformity according to EN 55022, EN 55024, EN 60950
Environment		Temperature range 0–40°C; humidity 5–90%; non-condensing
Accessories		<ul style="list-style-type: none"> <li>■ 1000Base-SX SFP module, LANCOM SFP-SX-LC1, item no. 61556</li> <li>■ 1000Base-LX SFP module, LANCOM SFP-LX-LC1, item no. 61557</li> </ul>
Service		5 years
Support		via Hotline and Internet

## 6.2 Connector wiring

### 6.2.1 LAN interface 10/100Base-TX

8-pin RJ45 sockets (ISO 8877, EN 60603-7)

Connector	Pin	Line
	1	T+
	2	T-
	3	R+
	4	PoE/G
	5	PoE/G
	6	R-
	7	PoE/ -48 V
	8	PoE/ -48 V

EN

## 6.3 Declaration of conformity



LANCOM Systems herewith declares that the devices of the type described in this documentation are in agreement with the basic requirements and other relevant regulations of the 1995/5/EC directive.

The CE declarations of conformity for your device are available in the appropriate product area on the LANCOM Systems web site ([www.lancom.eu](http://www.lancom.eu)).