



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

LANCOM GS-1224 LANCOM GS-1224P

LANCOM GS-1224
LANCOM GS-1224P

© 2011 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 7® 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).

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

Wuerselen, Juli 2011

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-1224 switch features 24 Gigabit-Ethernet and four combo ports (TP/SFP), it integrates perfectly into LANCOM's Advanced Routing and Forwarding and it supports up to 24 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).

Furthermore the LANCOM GS-1224P switch supports Power-over-Ethernet for connected network devices. The overall power output of 185 Watts from the PoE supply can be flexibly divided between the ports.

Model variants

This documentation is intended for LANCOM Switch users. The following models are available:

- The LANCOM GS-1224 without PoE support.
- The LANCOM GS-1224P with PoE support.

Passages applying only to certain models are identified either in the text itself or by a comment in the margin.

Otherwise the documentation refers to all models collectively as the LANCOM Switch series.

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



Our online services 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

Model
restrictions

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

1 Introduction	7
1.1 Key Features in the Device	7
1.2 Just what can your LANCOM Switch do?	8
2 Installation	10
2.1 Package content	10
2.2 System requirements	10
2.3 Status displays and interfaces	10
2.3.1 Connectors, LEDs and buttons on the LANCOM GS-1224	11
2.3.2 Connectors on the back of the LANCOM GS-1224	12
2.4 Mounting and connecting up the LANCOM Switch	12
2.5 Software installation	13
2.5.1 Starting the software setup	13
2.5.2 Which software should I install?	14
3 Configuring and monitoring the LANCOM Switch	15
3.1 Configuration with WEBconfig	15
3.2 Back up and reload the configuration	16
3.3 Monitoring the LANCOM Switch with LANmonitor	17
3.3.1 Ethernet port status	17

4	Operation of Web-based Management	18
4.1	Web Management Home Overview	18
4.2	Configuration	20
4.2.1	System Configuration	20
4.2.2	Port Configuration	23
4.2.3	PoE	24
4.2.4	VLAN Mode Configuration	27
4.2.5	VLAN Group Configuration	30
4.2.6	Aggregation	34
4.2.7	LACP	35
4.2.8	RSTP	36
4.2.9	802.1x Configuration	38
4.2.10	IGMP Snooping	46
4.2.11	Mirror Configuration	47
4.2.12	QoS (Quality of Service) Configuration	48
4.2.13	Filter	51
4.2.14	Rate Limit	52
4.2.15	Storm Control	53
4.2.16	SNMP	54
4.3	Monitoring	56
4.3.1	Detailed Statistics	56
4.3.2	LACP Status	60
4.3.3	RSTP Status	61
4.3.4	IGMP Status	62
4.3.5	Ping Status	63
4.4	Maintenance	64
4.4.1	Warm Restart	64
4.4.2	Factory Default	65
4.4.3	Software Upgrade	65
4.4.4	Configuration File Transfer	65
4.4.5	Logout	66
5	Appendix	67
5.1	Performance data and specification	67
5.2	Connector wiring	69
5.2.1	Ethernet interface 10BASE-T/100BASE-TX/1000BASE-T	69
5.3	CE-declarations of conformity	69

1 Introduction

The LANCOM GS-1224 is a websmart layer-2 switch with 20 Gigabit ports (for twisted pair cable – TP) and four Gigabit dual media ports with TP/SFP, which meets the IEEE 802.3 Gigabit, Fast Ethernet and Ethernet specifications.

The LANCOM Switches can be configured through WEBconfig.

The overall network management is enhanced and the network efficiency is also improved to accommodate high bandwidths. 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 and IGMP Snooping capability via the intelligent software. It is suitable for both metro-LAN and office application.

The LANCOM GS-1224P switch also complies with IEEE 802.3af, its advanced auto-sensing algorithm enables providing power devices (PD) discovery, classification, current limit, and other necessary functions. It also supports high safety with short circuit protection and power-out auto-detection to PD.

The 10/100/1000 Mbps TP-Ports are standard Ethernet ports that meets all IEEE 802.3/u/x/z (Gigabit and Fast Ethernet) specifications.

The 1000 Mbps SFP Fiber transceiver are Gigabit Ethernet ports that fully complies with all IEEE 802.3z and 1000Base-SX/LX standards. The 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 IEEE 802.1q Tag VLAN. Support 24 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.
- Power saving:
The switch can detect inactive links and deactivate the power supply for the corresponding ports
- SNMP:
SNMP agent. In the device, SNMP agent is a client software which is operating over SNMP protocol used to receive the command from SNMP manager (server site) and echo the corresponded data, i.e. MIB object. Besides, SNMP agent will actively issue TRAP information when happened.

The device supports MIB II (RFC1213), Bridge MIB (RFC1493), Interface Group MIB (RFC2863).
- 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-1224	LANCOM GS-1224P
Hardware		
Supports 20-port 10/100/1000 Mbps TP ports and auto MDIX function	✓	✓
4 Gigabit dual media ports(TP/SFP)	✓	✓
Hot-Plugging for SFP modules	✓	✓
400KB packet buffer	✓	✓
Support of Jumbo frames (maximum 9600 bytes)	✓	✓
Full-duplex flow control (IEEE 802.3x)	✓	✓

	LANCOM GS-1224	LANCOM GS-1224P
Status LEDs		
System: Power	✓	✓
TP Port 1-24: LINK/ACT, SPD	✓	✓
SFP-Ports 21,22,23,24: LINK/ACT, SPD, SFP	✓	✓
PoE support		
PoE with 48 V DC power through RJ-45 pin 1, 2, 3, 6.		✓
Powered Device(PD) auto detection and classification.		✓
PoE-PSE status and activity LED indicator.		✓
Management		
Concisely the status of port and easily port configuration	✓	✓
Per port traffic monitoring counters	✓	✓
Port mirror function	✓	✓
Static trunk function	✓	✓
IEEE 802.1q VLAN	✓	✓
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	✓	✓
Types of QoS: IEEE 802.1p Priority and DiffServ DSCP Priority.	✓	✓
Rapid Spanning Tree (IEEE 802.1w RSTP)	✓	✓
IEEE 802.1X port security on a VLAN	✓	✓
SNMP access can be disabled and prevent from illegal SNMP access	✓	✓
Bandwidth rating management	✓	✓
HTTP for firmware upgrade and config file import/export	✓	✓
Remote boot through WEBconfig	✓	✓
Options		
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-1224	LANCOM GS-1224P
Power cord	✓	✓
19" adapter (2 pieces) and mounting materials	✓	✓
LANCOM data medium (CD/DVD)	✓	✓
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 with TCP/IP support, such as Windows, 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

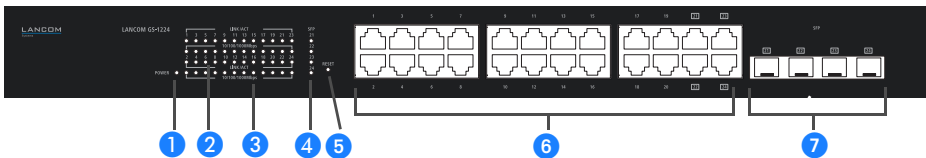
The following section describes the meaning of the LEDs.



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-1224

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



- | | |
|--|---|
| <p>1 POWER LED</p> | <p>Constant green when power is supplied to the device.</p> |
| <p>2 LINK / ACT LED
Port 1 to 24</p> | <ul style="list-style-type: none"> ■ Constant green when the network connection is established to the connected device. ■ Flashes during data transfer. ■ Off if no network connection can be established to the connected device. |
| <p>3 10/100/1000
Mbps LED</p> | <ul style="list-style-type: none"> ■ 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. |
| <p>4 SFP (LINK/ACT)
LED</p> | <ul style="list-style-type: none"> ■ Constant green when the network connection is established to the connected device. ■ Flashes during data transfer. ■ Off if no network connection can be established to the connected device. |
| <p>5 Reset</p> | <p>Button to reset the system. If you press the button longer than three seconds, all settings will be reset to default (factory setting).</p> |
| <p>6 TP connectors</p> | <p>Connectors for twisted-pair cables.</p> |
| <p>7 SFP connectors</p> | <p>Connectors for small form-factor pluggable (SFP) modules.</p> |



The device starts after the reset in an unconfigured mode and **all** settings will get lost. Therefore you should save the actual configuration **before** you reset the device!

2.3.2 Connectors on the back of the LANCOM GS-1224

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



LANCOM GS-1224

- 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).


ℹ Use only standard TP cables of category CAT 5e 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.

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

- ③ **Supply power and switch on** – Supply power to the device by means of the IEC power cable.
- ④ **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.

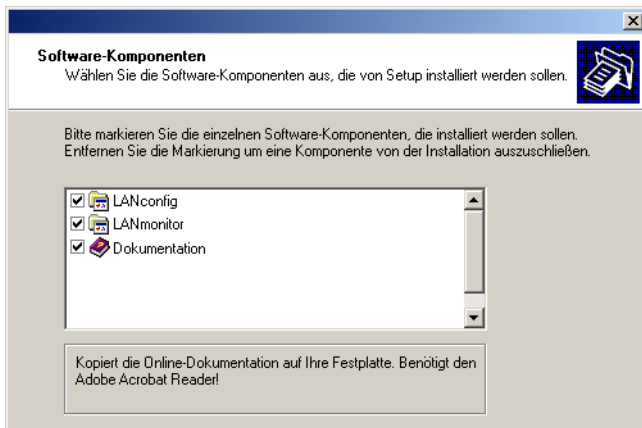
 You may skip this section if you use your LANCOM Switch exclusively with computers running operating systems other than Windows.

2.5.1 Starting the software setup

Place the supplied data medium (CD/DVD) 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 data medium.

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.

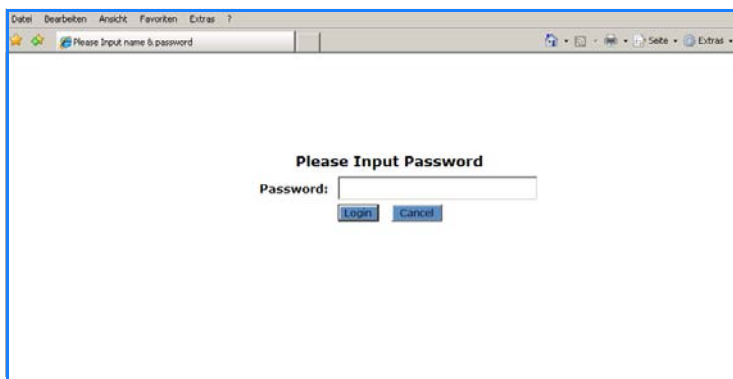
3 Configuring and monitoring the LANCOM Switch

3.1 Configuration with WEBconfig

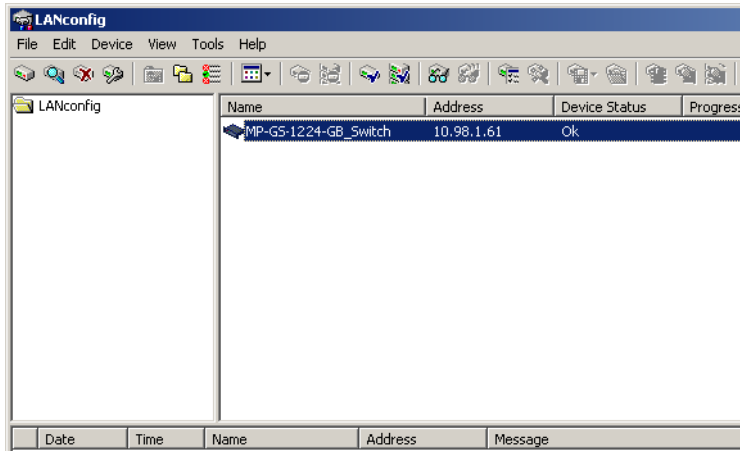
The configuration is done over a graphical user interface via a browser (WEBconfig). Instructions for configuring the device with WEBconfig are available in the chapter "Web-based configuration".

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 password for accessing the device is "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 subnetwork.

Network without a DHCP server – If no DHCP server is present in the network, the LANCOM Switch waits about 5 minutes and then 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".

3.2 Back up and reload the configuration

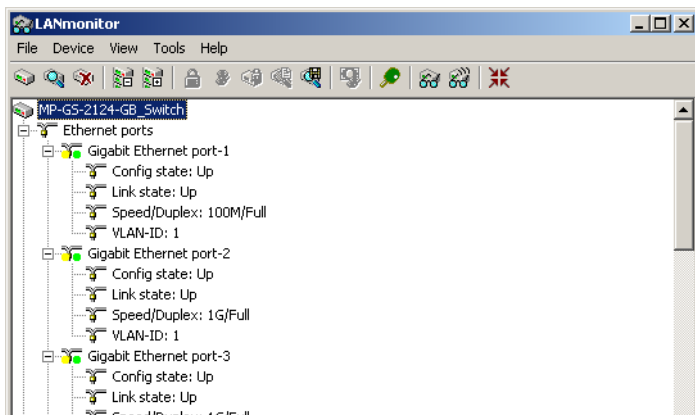
With this function you can back up or reload your current configuration for safety reasons. This backup can be uploaded into a new or defective device.

3.3 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.

3.3.1 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

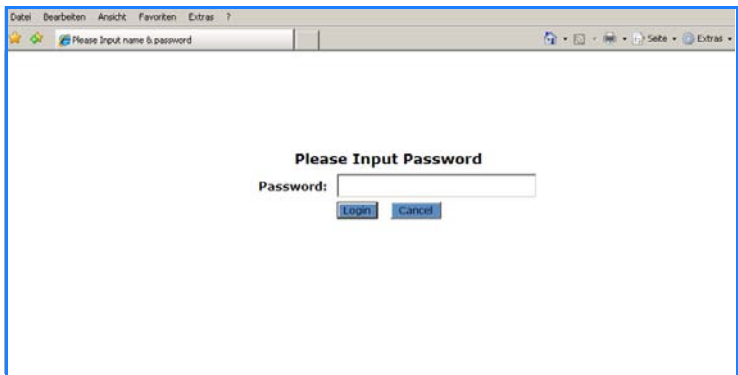
4 Operation of Web-based Management

This chapter instructs you how to configure and manage the switch through the web user interface (WEBconfig). With this facility, you can easily access and monitor through any one port of the switch all the status of the switch.

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

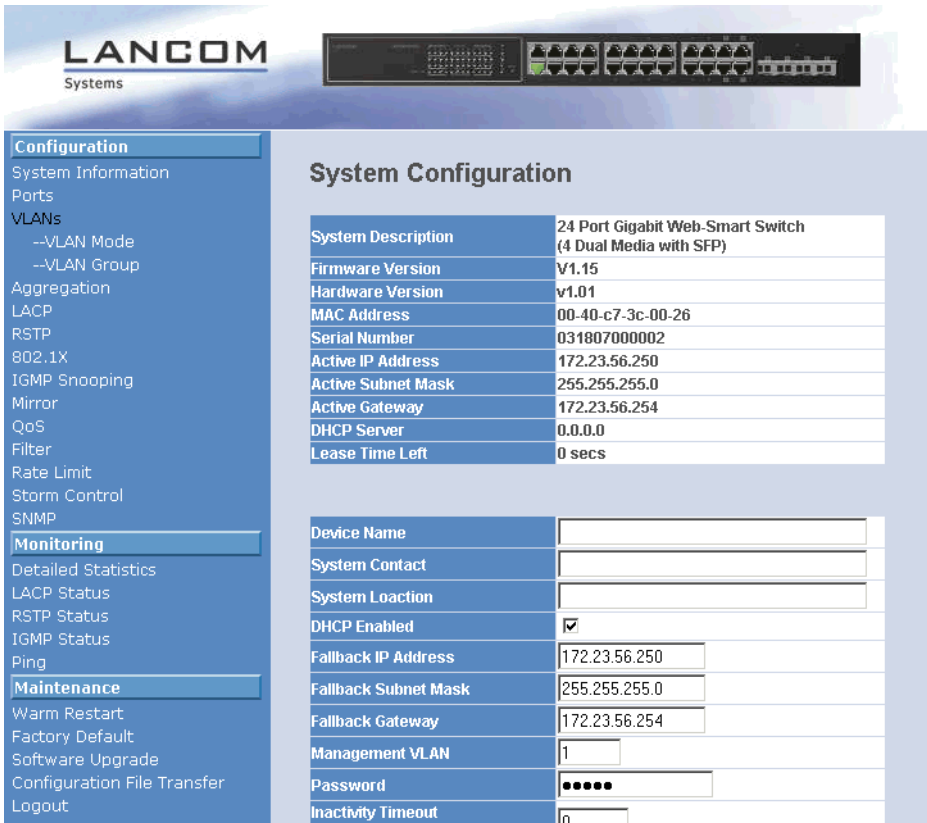
LANCOM GS-1224/ GS-1224P	
IP Address	172.23.56.250
Subnet Mask	255.255.255.0
Default Gateway	172.23.56.254
Password	admin

Web Smart Switch supports a simplified user management function which allows only one administrator to configure the switch at one time. Fill in the IP address in the address row in a browser to start WEBconfig. The default password is "admin".



4.1 Web Management Home Overview

After login, System Information will be displayed as the following screenshot illustrates:



LANCOM
Systems

Configuration

- System Information
- Ports
- VLANs
 - VLAN Mode
 - VLAN Group
- Aggregation
- LACP
- RSTP
- 802.1X
- IGMP Snooping
- Mirror
- QoS
- Filter
- Rate Limit
- Storm Control
- SNMP

Monitoring

- Detailed Statistics
- LACP Status
- RSTP Status
- IGMP Status
- Ping

Maintenance

- Warm Restart
- Factory Default
- Software Upgrade
- Configuration File Transfer
- Logout

System Configuration

System Description	24 Port Gigabit Web-Smart Switch (4 Dual Media with SFP)
Firmware Version	V1.15
Hardware Version	v1.01
MAC Address	00-40-c7-3c-00-26
Serial Number	031807000002
Active IP Address	172.23.56.250
Active Subnet Mask	255.255.255.0
Active Gateway	172.23.56.254
DHCP Server	0.0.0.0
Lease Time Left	0 secs

Device Name	<input type="text"/>
System Contact	<input type="text"/>
System Location	<input type="text"/>
DHCP Enabled	<input checked="" type="checkbox"/>
Fallback IP Address	<input type="text" value="172.23.56.250"/>
Fallback Subnet Mask	<input type="text" value="255.255.255.0"/>
Fallback Gateway	<input type="text" value="172.23.56.254"/>
Management VLAN	<input type="text" value="1"/>
Password	<input type="password" value="*****"/>
Inactivity Timeout	<input type="text" value="0"/>

The Information of Page Layout

The top part of the information page shows the front panel of the switch. Linked ports are displayed in green color, and ports without link in black.

The ports for the optional SFP modules show a demonstration of the module, if it is installed. Ports without installed SFP modules show covered plates.

On the left side, the main menu tree for web management is listed on the page. According to the function name in bold, all functions can be divided into three parts: Configuration, Monitoring and Maintenance. The functions of each folder are described in its corresponded section respectively. When clicking it, the function is performed.

4.2 Configuration

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

4.2.1 System Configuration

In the system configuration you can define the basic parameter for the configuration and the operation of the device. The switch supports manual IP address setting and further address information via DHCP or the manual setting of a fixed IP address.

System Configuration

System Description	24 Port Gigabit Web-Smart Switch (4 Dual Media with SFP)
Firmware Version	V1.14
Hardware Version	v1.01
MAC Address	00-40-c7-3c-00-25
Serial Number	031807000001
Active IP Address	10.1.80.137
Active Subnet Mask	255.255.0.0
Active Gateway	10.1.1.11
DHCP Server	0.0.0.0
Lease Time Left	0 secs

Device Name	<input type="text" value="LANCOM GS-1224"/>
DHCP Enabled	<input type="checkbox"/>
Fallback IP Address	<input type="text" value="10.1.80.137"/>
Fallback Subnet Mask	<input type="text" value="255.255.0.0"/>
Fallback Gateway	<input type="text" value="10.1.1.11"/>
Management VLAN	<input type="text" value="1"/>
Password	<input type="password" value="••••"/>
Inactivity Timeout (0, 60-10000 Secs)	<input type="text" value="0"/>

Parameter:

- System Description:
The simple description of this switch.
- Firmware Version:
The firmware version of this switch.

- **Hardware Version:**
The hardware version of this switch.
- **MAC Address:**
It is the Ethernet MAC address of the management agent in this switch.
- **Serial Number:**
The serial number assigned by the manufacturer.
- **Active IP Address:**
Shows the active IP address of this switch.
- **Active Subnet Mask:**
Shows the active subnet mask of this switch.
- **Active Gateway:**
Shows the active gateway of this switch.
- **DHCP Server:**
Shows the IP address of the DHCP server.
- **Lease Time Left:**
Show the lease time left of DHCP client.
- **Device Name:**
Set a special name for this switch. Up to 16 characters are allowed in this parameter. Any alphanumeric character and zero are acceptable.
Default: no default
- **DHCP Enabled:**
You can enable the automatic delivery of an IP address and activate further address information via DHCP.
Default: enabled
- **Fallback IP Address:**
Fill in an IP address, which is used by the device, if DHCP is disabled or the DHCP server is not accessible.
Default: 172.23.56.250
- **Fallback Subnet Mask:**
Fill in a subnet mask, which is used by the device, if DHCP is disabled or the DHCP server is not accessible.
Default: 255.255.255.0

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

- **Fallback Gateway:**
Fill in a gateway, which is used by the device, if DHCP is disabled or the DHCP server is not accessible.
Default: 172.23.56.254
- **Management VLAN:**
Shows the ID of the management VLAN.
- **Password:**
Set a password for this switch. Up to 16 characters are allowed in this parameter. Any alphanumeric character is acceptable.
Default: admin
- **Inactivity Timeout(secs):**
Set the auto-logout timer. The valid value is 0-60 in the unit of minute and a decimal point is not allowed. The value 0 means auto-logout timer is disabled.
Default: 0

4.2.2 Port Configuration

Here you can configure the individual ports.

Port Configuration

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

Power Saving Enable

TP Ports

Port	Link	Mode	Flow Control	Flow Control Status
1	Down	Auto Speed ▼	<input type="checkbox"/>	disabled
2	Down	Auto Speed ▼	<input type="checkbox"/>	disabled
3	Down	Auto Speed ▼	<input type="checkbox"/>	disabled
4	Down	Auto Speed ▼	<input type="checkbox"/>	disabled
5	Down	Auto Speed ▼	<input type="checkbox"/>	disabled
6	Down	Auto Speed ▼	<input type="checkbox"/>	disabled
7	Down	Auto Speed ▼	<input type="checkbox"/>	disabled
8	Down	Auto Speed ▼	<input type="checkbox"/>	disabled

Fiber Ports

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

Parameter:

- **Enable Jumbo Frames:**
Jumbo frames are not standardized and oversized frames. This function support jumbo frames of up to 9600 bytes.
Default: disable
- **Power Saving Mode:**
This function supports Power Saving, to deactivate automatically the power supply for the ports with inactive links. Select: Enable/ Disable.
Default: enable
- **Link:**
Shows link status of this port.

Chapter 4: Operation of Web-based Management

Mode:

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

Medium	NWay	Speed	Duplex
Twisted Pair	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1 Gbit-Faser	ON/OFF	1000M	Full

Flow Control:

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

Default: Disable

Flow Control status:

To display the Flow control status.

4.2.3 PoE

LANCOM GS-1224P
only

PoE Status

Displays the information about the PoE status.

PoE Status																								
Vmain	48.4 V																							
Imain	0 A																							
Pconsume	0 W																							
Power Limit	185 W																							
Temperature	35 °C / 95 °F																							
Port No	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	
Port On																								
AC Disconnect Port Off																								
DC Disconnect Port Off																								
Overload Port Off																								
Short Circuit Port Off																								
Over Temp. Protection																								
Power Management Port Off																								

- Parameter:
 - Vmain: The voltage supplied by the switch.
 - Imain: The sum of the current that every port supplies.
 - Pconsume: The sum of the power that every port supplies.
 - Power Limit: The maximal power that the switch can supply (Read Only).
 - Temperature: The PoE temperature.
 - Port No: Port number.
 - Port On: Shows whether the port is supplying the power to the powered device or not.
 - AC Disconnect Port Off: Port is turned off due to the AC Disconnect function.
 - DC Disconnect Port Off: Port is turned off due to the DC Disconnect function.
 - Overload Port Off: The switch will stop supplying the power to the port due to the power required by the powered device that is linked to the port on the switch exceeding the Class setting of the powered device.
 - Short Circuit Port Off: The switch will stop supplying the power to the port if it detects that the powered device linked to the port is short circuit.
 - Over Temp. Protection: The PoE will be disabled when the temperature on chip will rise to 150°C.
 - Power Management Port Off: Due to total power required by all powered devices linked to the switch exceeds the power limit, so the switch stops supplying the power to this port after referring to the information of the priority.

PoE Configuration

In the PoE Port Management the PoE settings can be configured.

The switch complies with IEEE 802.3af protocol and is capable of detecting automatically whether the device linked to the port on the switch is a PoE capable device or not. The switch also manages the power supplement based on the Class of the powered device, and it will stop supplying

the power once the power required by the powered device exceeds the Class, Short Circuit or over temperature occurs.

PoE Configuration

Port No	Status	State	Priority	Power(W)	Current(mA)	Class
1	Normal	Enable	Normal	0	0	0
2	Normal	Enable	Normal	0	0	0
3	Normal	Enable	Normal	0	0	0
4	Normal	Enable	Normal	0	0	0
5	Normal	Enable	Normal	0	0	0
6	Normal	Enable	Normal	0	0	0
7	Normal	Enable	Normal	0	0	0
8	Normal	Enable	Normal	0	0	0
9	Normal	Enable	Normal	0	0	0
10	Normal	Enable	Normal	0	0	0
11	Normal	Enable	Normal	0	0	0
12	Normal	Enable	Normal	0	0	0
13	Normal	Enable	Normal	0	0	0
14	Normal	Enable	Normal	0	0	0
15	Normal	Enable	Normal	0	0	0
16	Normal	Enable	Normal	0	0	0
17	Normal	Enable	Normal	0	0	0
18	Normal	Enable	Normal	0	0	0

■ Parameter:

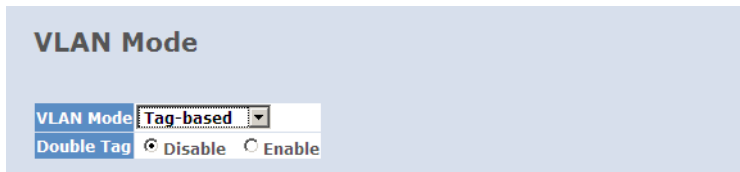
- Status: The status is either "Normal" or "Active". The former means the port is ready to link and supply the power to the powered device at any time. The latter means the port is currently supplying power.
- State: "Enable" allows power supply while a device is linked to the port; "Disable" means the port does not support PoE functions.
- Priority: Choices are "Normal", "Low" and "High". The former being the default choice. In case the power required by all linked devices exceeds the maximum available power, the switch will cut power to the devices with the lowest priority. If ports have the same priority, the switch will stop the power supply to the port with the highest port id.
- Power(W): The power consumed by the port.
- Current(mA): The current supplied by the port.
- Class: The class of the powered device linked to the port of the switch.

4.2.4 VLAN Mode Configuration

The switch supports Tag-based VLAN (802.1q) and Port-based VLAN. Its VLAN mode supports 24 active VLANs and the available VLAN ID range is from 1~4094. VLAN configuration is used to divide a LAN into smaller ones. With proper configuration you can not only gain improved security and increased performance but greatly reduced VLAN management.

■ VLAN Mode Setting

The VLAN Mode Selection function includes four modes: Port-based, Tag-based and Metro mode.



Parameter:

■ VLAN Mode:

Port-based:

A port-based VLAN defines its members by port. Any packet coming in or going out from any port of a port-based VLAN will be accepted. No filtering criterion applies in a port-based VLAN, the only criterion is the physical connection to a member port. For example in a port-based VLAN with the member ports 1, 2, 3 and 4, the ports 1, 2, 3 and 4 can communicate with each other, but port 5 can not communicate with them. Each port-based VLAN is identified with an ID (1 to 4094) and you can capture further information about the VLAN in a description. This switch supports up to maximal 24 port-based VLANs.

As soon as the VLAN mode is set on "port-based", the display automatically changes to the configuration of the port-based VLAN groups.

Port-Based VLAN Configuration

Add a VLAN

ID

Add

VLAN Configuration List

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

Modify **Delete** **Refresh**

Tag-based:

A tag-based VLAN identifies its member by VLAN-ID. If there are any more rules in ingress or egress filtering lists, this rule determines if the packet will be forwarded or not. The switch supports standard of 802.1q.

Each tag-based VLAN you set up must get a VLAN name and VLAN ID. A valid VLAN ID is 1 up to 4094. You can create up to 24 Tag VLAN groups.

As soon as the VLAN mode is set on "tag-based", the setting double-tag mode will be offered. If the double-tag mode is activated all packets (tagged or untagged) will get a VLAN tag. Packets which have already an "inner" tag will get in addition an "outer" tag. Internet service provider use this function for additionally tagging in their own network of customers VLAN tagged data streams.

If the double-tag mode is activated, you can select the ports on which the doubled VLAN tags should be used.

VLAN Mode

VLAN Mode	Tag-based ▾
Double Tag	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Up-link Port	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/>
	9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/>
	17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24 <input type="checkbox"/>

After confirmation of the tag-based VLAN mode, the display automatically changes to the configuration of the tag-based VLAN groups.

Tag-Based VLAN Configuration

Add a VLAN

VLAN ID

VLAN Configuration List

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

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

- Metro Mode:**
The Metro mode is a quick method to configure port-based VLANs. Metro mode can be activated for the ports 21, 22, 23 and 24. This option is usually used to get a comfortable uplink to the metro ethernet environment.

VLAN Mode

VLAN Mode

Up-link Port 21 22 23 24

After confirmation of the Metro mode the display changes to the configuration of the port-based VLAN groups. At the same time for **all ports without metro mode support** a VLAN group is set up. This VLAN group contains the respective port and the ports **with** metro mode support. Ports can be deleted manually from certain groups if needed.

Port-Based VLAN Configuration

Add a VLAN

ID

VLAN Configuration List

	ID	Description	Member
<input type="radio"/>	1	Default1	1,21,22,23
<input type="radio"/>	2	Default2	2,21,22,23
<input type="radio"/>	3	Default3	3,21,22,23
<input type="radio"/>	4	Default4	4,21,22,23

4.2.5 VLAN Group Configuration

Shows the information of VLAN Groups, and allows administrators to maintain them by modifying and deleting each VLAN group.

The display differs depending on the current VLAN mode:

- If you are in port-based VLAN or in metro mode, it will just show the ID and the descriptions of the existing members.
- If you are in tag-based VLAN, it will show the ID and the descriptions of the existing members. Additionally you can define further options for each port.

The switch can store the configuration of port-based VLAN and tag-based VLAN separately.

General functions

- Add:
Adds a new port-based or tag-based VLAN.
- Modify:
Click on **Modify** to edit the selected VLAN.
- Delete:
Click on **Delete** to remove the selected VLAN.

Tag-Based VLAN Configuration

Add a VLAN

VLAN ID

Add

VLAN Configuration List

Port Config

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

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

Modify
Delete
Refresh

VLAN group configuration

Parameter:

- ID (VLAN ID):
ID of the VLAN group (1 to 4094). The packet forwarding is based on this ID.
- Member:
Select the member ports of the VLAN group.

VLAN Setup

Description

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

VLAN Port Configuration

In tag-based mode you can define further settings for each port. Please click the **Port Config** button in the list of tag-based VLAN group.

Tag-Based VLAN Configuration

Add a VLAN

VLAN ID

VLAN Configuration List

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

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

Parameter:

- Ingress Filtering enabled:

If the filter for incoming packets is activated, packets on this port are forwarded only, if the port is member of the corresponding VLAN group. Packets with other VLAN tags are discarded.
- Packet Type:
 - All: Forwards all packets (tagged and untagged).
 - Tagged Only: Forwards tagged packets only and discards untagged packets.
- Role:

Defines the rules for outgoing packets.

 - Access: Packets on this port are forwarded untagged. If double tags are detected, the outer tag will be removed. This option is generally used if end devices are connected to the port.
 - Trunk: Packets on this port are forwarded using the current tag.
 - Hybrid: Similar to trunk, packets on this port are forwarded using the current tag. If the current tag matches the "Untagged VLAN ID", the tag will be removed.
- Untagged VLAN ID:

Active only if the role is set to hybrid. This value (from 1 to 4094) defines the tag, which will be removed from outgoing packets.
- PVID (Port VLAN ID):

This VLAN ID from 1 to 4094 is used to tag incoming packets for forwarding. Only VLAN IDs which are defined in the list of tag-based VLAN groups can be used as Port VLAN ID.

VLAN Per Port Configuration

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

4.2.6 Aggregation

The Aggregation (Port Trunking) Configuration is used to configure the settings of Link Aggregation. You can bundle more than one port by 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.

Aggregation/Trunking Configuration

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

Apply

Refresh

The Aggregation Configuration displays the current setup of Aggregation Trunking. With this function you can add a new trunking group or modify the members of an existing trunking group.

Parameter:

- Normal:
Set up the ports that do not join any aggregation trunking group.
- Group 1-8:
Groups the ports you choose together. Up to 12 ports can be selected for each group.



The aggregation groups has to be set up one after each other. Group 2 will remain inactive until the ports for group 1 are selected and the settings are stored with **Apply**.

4.2.7 LACP

Smart Web Switch supports "Link Aggregation Control Protocol" (LACP). LACP is a standard network protocol IEEE 802.3ad which dynamically creates and manages trunk groups.

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

LACP Port Configuration

Port	Protocol Enabled	Key Value (0~255)
1	<input type="checkbox"/>	auto
2	<input type="checkbox"/>	auto
3	<input type="checkbox"/>	auto
4	<input type="checkbox"/>	auto

Parameter:

- Protocol Enabled:
Just tick the check box to enable LACP protocol then press **Apply**.
- Key Value:
It's a key for an aggregation. This must be an integer value between 1 and 255 or auto select by switch.

4.2.8 RSTP

Rapid Spanning Tree protocol (RSTP) detects and resolves network loops, respectively in case of need (breakdown of a connection) to activate it again. The protocol allows a switch to communicate with other RSTP compliant switches and to ensure, that only one path exists between two end points in your network.

Parameter:

■ System Priority:

System priority is used to determine the root switch, thus the root of the spanning tree. The switch with the highest priority (lowest numeric value) becomes the root switch. If all switches have the same priority, the switch with the lowest MAC address will become the root switch. Select a value from the drop-down list box. (The lower the numeric value you assign, the higher the priority for this system.)

Default: 32768

■ Hello Time:

Hello Time is the time interval, in which the switch tells the following devices in the spanning tree, with a "hello packet", that it is still active. If for example the LANCOM Switch is the root switch of the LAN, all other bridges will use the hello time assigned by this switch to communicate with each other. The allowed range is 1-10 second.

Default: 2 seconds

■ Max. Age:

If there are no "hello packets" for a certain time, a device in the spanning tree assumes a change in the structure. In this case all connections in the network need to be established again.

Maximum Age is the maximum time a switch can wait without receiving a "hello packet" before attempting to reconfigure. During this time of reconfiguration, all STP-capable devices in the network send only administration packets, but no reference data of the connected devices.

The valid value of Max. Age is 6 - 40 seconds.

Default: 20 seconds

■ Forward Delay:

Forward delay time is the maximum time (in seconds) a switch waits before changing its state.

For example the time a bridge port needs, to move from "Listening state" to "Learning state" or from "Learning state" to "Forwarding state". The general rule is:

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

Default: 15 seconds

■ Force Version:

For the STP algorithm you can select between two options in the dropdown list: RSTP or STP. Rapid Spanning Tree Protocol (RSTP) is an extension of STP and reduces the needed time for the new organisation of a network after structure changed.

RSTP Port Configuration

Enable or disable RSTP protocol on the ports that are selected. Decide if the Port should be an edge port and set path costs.

Parameter:

■ Protocol Enabled:

Just tick the check box beside the port x to enable RSTP protocol, then press **Apply**.

■ Edge:

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.

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

■ Path Cost:

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

RSTP System Configuration

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

RSTP Port Configuration

Port	Protocol Enabled	Edge	Path Cost (1~20000000)
Aggregations	<input type="checkbox"/>		
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto

4.2.9 802.1x 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 IEEE 802.1x, 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.

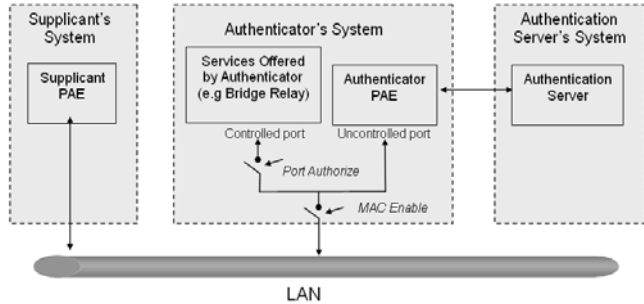
A port acting as an authenticator is thought to be two logical ports, a controlled port and an uncontrolled port. A controlled port can only pass the packets when the authenticator PAE is authorized, and otherwise, an uncontrolled port will unconditionally pass the packets with PAE group MAC address,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

■ **Authentication server:**

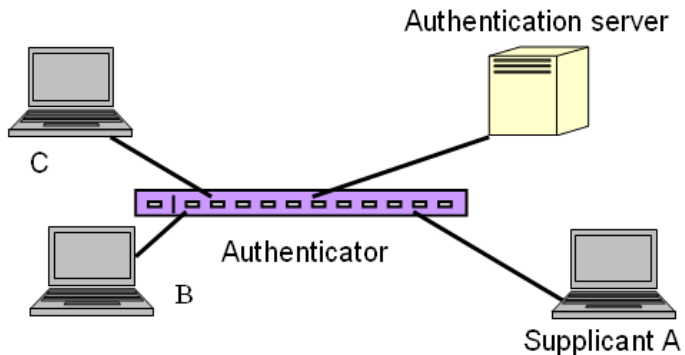
A device provides authentication service, through EAP, to an authenticator by using authentication credentials supplied by the supplicant to determine if the supplicant is authorized to access the network resource.

The overview of operation flow for the following figure is quite simple. When the Supplicant PAE issues a request to the Authenticator PAE, Authenticator and Supplicant PAE exchange authentication messages. Then, the Authenticator passes the request to the RADIUS server to verify. Finally, the 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 the authentication server by using EAP encapsulation. Before successfully authenticating, the supplicant can only reach the authenticator to perform authentication message exchange or access the network from the uncontrolled port.



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

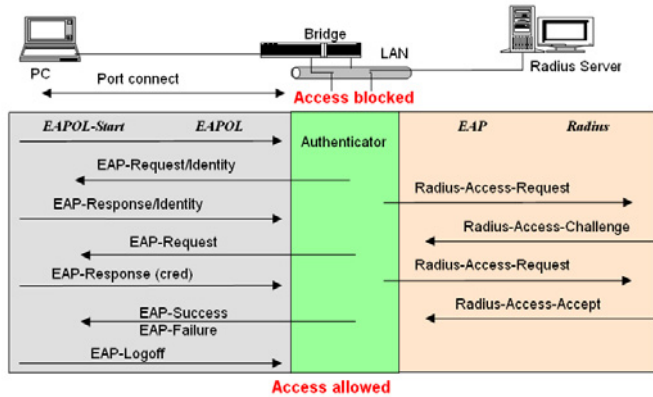


The following figure shows the procedure of 802.1x authentication. There are steps for the login based on 802.1x port access control management. The protocol used in the right side is EAPOL and the left side is EAP.

- 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 an EAPOL-start packet to the authenticator PAE and the authenticator will immediately respond with an EAP-Request/Identity packet.
- 3 The authenticator sends periodically an EAP-Request/Identity to the supplicant requesting the identity that needs to be authenticated.
- 4 If the authenticator doesn't send EAP-Request/Identity, the supplicant will initiate the process by sending the EAPOL-Start to the authenticator.
- 5 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 a RADIUS-Access-Challenge to the supplicant to ask for the user password via the authenticator PAE.
- 7 The supplicant converts the user password into the credential information, in MD5 format and replies an EAP-Response with this credential information as well as the specified authentication algorithm (MD5 or OTP) to the authentication server via the authenticator PAE. As per the value of the type field in the 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 algorithms.
- 8 If user ID and password are 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 has failed to authenticate. The port it is connected to 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 issues an EAP-Logoff message to the authentication server, the port used is set to unauthorized.



The 802.1X "enabled" is the type of authentication supported by the switch. In this mode, the devices connected to this port, once a supplicant is authorized, can access the network resources through this port.

The 802.1x Port-based Network Access Control function supported by the switch is more complex, it just supports 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	Force Unauthorized	Don't Care	Port Unauthorized
Multihost	Force Authorized	Don't Care	Port Authorized

Configuration

The 802.1X Server Configuration is used to configure the global parameters for RADIUS authentication in 802.1X port security application.

Parameter:

- **Mode:**
Enable or disable 802.1X function.
- **RADIUS IP:**
RADIUS server IP address for authentication.
Default: 0.0.0.0
- **RADIUS UDP Port:**
The port number to communicate with a RADIUS server for the authentication service. The valid value ranges 1-65535.
Default port number is 1812.
- **RADIUS Secret:**
The secret key between authentication server and authenticator. It is a string with the length of 1 - 15 characters. The character string may contain upper case, lower case and 0-9. It is character sense. It is not allowed to put a blank between any two characters.
Default: None
- **Admin State:**
This is used to set the operation mode of authorization. There are three types of operation modes supported: Force Unauthorized, Force Authorized, Auto.
 - **Force Unauthorized:**
The controlled port is forced to hold in the **unauthorized state**, no matter which EAP negotiation between authenticator and supplicant takes place.

- Force Authorized:
The controlled port is forced to hold in the **authorized state**, no matter which EAP negotiation between authenticator and supplicant takes place.
- Auto:
If the port is set to be in authorized or unauthorized state depends on the result of the authentication exchange between the authenticator and supplicant.

Default: Force Authorized

- Port State:
Shows the port status of authorization.
- Re-authenticate:
Using this function all devices connected to this port will have to re-authenticate with username and password when the reauthentication period expires.
- Re-authenticate All:
Re-authenticate for all ports at once.
Using this function forces the devices connected **to all ports** to re-authenticate with username and password when the reauthentication period expires.
- Force Reinitialize:
Using this function forces all devices connected to this port to re-authenticate with username and password **immediately**.
- Force Reinitialize All:
Using this function forces the devices connected **to all ports** to re-authenticate with username and password **immediately**.

802.1X Configuration

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

Port	Admin State	Port State			
1	Auto ▾	802.1X Disabled	Re-authenticate	Force Re-initialise	Statistics
2	Force Authorised ▾	802.1X Disabled	Re-authenticate	Force Re-initialise	Statistics
3	Force Authorised ▾	802.1X Disabled	Re-authenticate	Force Re-initialise	Statistics
4	Force Authorised ▾	802.1X Disabled	Re-authenticate	Force Re-initialise	Statistics
5	Force Authorised ▾	802.1X Disabled	Re-authenticate	Force Re-initialise	Statistics

Statistics

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

802.1X Statistics for Port 1

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

Authenticator counters			
authEntersConnecting	0	authEapLogoffsWhileConnecting	0
authEntersAuthenticating	0	authAuthSuccessesWhileAuthenticating	0
authAuthTimeoutsWhileAuthenticating	0	authAuthFailWhileAuthenticating	0
authAuthEapStartsWhileAuthenticating	0	authAuthEapLogoffWhileAuthenticating	0
authAuthReauthsWhileAuthenticated	0	authAuthEapStartsWhileAuthenticated	0
authAuthEapLogoffWhileAuthenticated	0		
Backend Authenticator counters			
backendResponses	0	backendAccessChallenges	0
backendOtherRequestsToSupplicant	0	backendAuthSuccesses	0
backendAuthFails	0		
dot1x MIB counters			
dot1xAuthEapolFramesRx	0	dot1xAuthEapolFramesTx	0
dot1xAuthEapolStartFramesRx	0	dot1xAuthEapolLogoffFramesRx	0

Parameters

You can enable or disable the reauthentication function and specify how often a client has to reenter his or her username and password to stay connected to the port.

802.1X Parameters

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

Parameter:

- Reauthentication Enabled:
Choose whether regular authentication will take place in this port.
Default: Disable
- Reauthentication Period (1-65535 s):
You can define the time period (in seconds), after a supplicant has to authenticate again. The time period can not be zero.
Default: 3600 seconds
- EAP timeout (1-255 s):
A timeout condition in the exchange between the authenticator and the supplicant. Valid range: 1 -255.
Default: 30 seconds

4.2.10 IGMP Snooping

IGMP Snooping lets administrators configure a switch to constrain multicast traffic on certain ports.

Parameter:

- IGMP Enabled:
Here you can enable the IGMP function.
Default: disable
- Router Ports:
A Port is a router port, if a router is connected which handles multicast routing. Enable here the corresponding ports.
Default: none

- Unregistered IGMP Flooding enabled:
Allows multicats flooding, while the multicast traffic is not registered in the multicast table.
Default: enable
- VLAN ID:
With the IGMP Enable mode being selected, it will list the VLAN ID number.
- IGMP Snooping Enabled:
If this function is enabled, the switch can handle IGMP-requests in the network and learns the membership of certain multicast groups if necessary.
Default: enable
- IGMP Querying Enabled:
If this function is enabled, the switch can distribute IGMP-requests in the network.
Default: enable

IGMP Configuration

IGMP Enabled	<input type="checkbox"/>																							
Router Ports	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>	6 <input type="checkbox"/>	7 <input type="checkbox"/>	8 <input type="checkbox"/>	9 <input type="checkbox"/>	10 <input type="checkbox"/>	11 <input type="checkbox"/>	12 <input type="checkbox"/>	13 <input type="checkbox"/>	14 <input type="checkbox"/>	15 <input type="checkbox"/>	16 <input type="checkbox"/>	17 <input type="checkbox"/>	18 <input type="checkbox"/>	19 <input type="checkbox"/>	20 <input type="checkbox"/>	21 <input type="checkbox"/>	22 <input type="checkbox"/>	23 <input type="checkbox"/>	24 <input type="checkbox"/>
Unregistered IPMC Flooding enabled	<input checked="" type="checkbox"/>																							

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

Apply
Refresh

4.2.11 Mirror Configuration

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

Parameter:

- Source Port:
Sets the port for monitoring. Just tick the check box beside the port x. Valid ports are port 1-24.
- Mirror Port:
Use the drop-down menu to select a mirror port
The value "disabled" (default) deactivates this function.

Mirroring Configuration

Port	Mirror Source
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>

Mirror Port

4.2.12 QoS (Quality of Service) Configuration

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

- QoS Configuration
While setting QoS function, please select the QoS Mode in drop-down menu at first. Then you can use 802.1p Priority and DSCP Priority functions. In this function, you can enable/disable QoS Mode and set Priority Control, such as: 802.1p and DSCP. The switch only supports Strict Priority. High priority queue is always passed first.
- 802.1p QoS Mode
This function will affect the priority of VLAN tags. Based on priority of VLAN tags, it can arrange 0~7 priorities, priorities can map to 4 queues of the switch (low, normal, medium, high) and possess different bandwidth distribution according to your weight setting.

Parameter:

- **Prioritize Traffic**
Five Prioritize Traffic values are provided: Custom, All Low Priority, All Normal Priority, All Medium Priority, and All High Priority.
The QoS setting would apply to all ports on the switch if one of the following values is selected: All Low Priority, All Normal Priority, All Medium Priority, or All High Priority.
- **Port Number**
When Custom is selected to prioritize traffic, you may assign a specific Port Number for 802.1p Configuration.
- **802.1p Configuration**
Each Priority can select any of the Queues. In Default, Priority 0 is mapping to Queue normal, Priority 1 is mapping to Queue low, Priority 2 is mapping to Queue low, Priority 3 is mapping to Queue normal, Priority 4 is mapping to Queue medium, Priority 5 is mapping to Queue medium, Priority 6 is mapping to Queue high, and Priority 7 is mapping to Queue high.

QoS Configuration

QoS Mode	802.1p
Prioritise Traffic	Custom
Port Number	Port 1

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

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

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

Parameter:

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

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

- Port Number**
When Custom is selected for Prioritize Traffic, you may assign a specific Port Number for DSCP Configuration.
- 802.1p Configuration**
64 kinds of priority traffic as mentioned above, can be set up for any Queue (low, normal, medium, high). In default, Priority 0-63 are mapping to Queue high.

QoS Configuration

QoS Mode: **DSCP**

Prioritise Traffic: **All High Priority**

Port Number: **Port 1**

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

Apply **Cancel**

4.2.13 Filter

The filter configuration lets administrators assign certain IP addresses or subnets to ports on the switch, from which a login on the switch for configuration is allowed.

Filter Configuration

Port	Source IP Filter			DHCP Server Allowed
	Mode	IP Address	IP Mask	
1	Disabled ▾	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
2	Disabled ▾	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
3	Disabled ▾	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>

Parameter:

■ Source IP Filter:

Mode:

There are three types of modes in this drop-down menu.

Default: Disabled.

Disabled:

Allows all IP Addresses to login and manage the switch.

Static:

Allows the IP Addresses set by the administrator to login and manage the switch.

DHCP:

Allows the IP Address distributed by the DHCP to login and manage the switch.

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

IP Address:

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

IP Mask:

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

■ DHCP Server Allowed:

Just tick the check box under the port x to allow the DHCP Server on this port.

Default: allowed

4.2.14 Rate Limit

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

Rate Limit Configuration

Traffic Rate Unit: 128 Kbps

Port	Ingress	Egress
1	Rate 4 512 kbps	Rate 2 256 kbps
2	Rate 10 1280 kbps	Rate 2 256 kbps
3	No Limit No Limit	No Limit No Limit
4	No Limit No Limit	No Limit No Limit
5	No Limit No Limit	No Limit No Limit
6	No Limit No Limit	No Limit No Limit
7	No Limit No Limit	No Limit No Limit
8	No Limit No Limit	No Limit No Limit
9	No Limit No Limit	No Limit No Limit

Parameter:

- Traffic Rate Unit

Select the data rate as basis for the rate limit. Possible values from 128 Kbps to 32 Mbps.

- Ingress:

Set up the limit of Ingress bandwidth for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set up in the Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid values are multiples (0 to 31) of the traffic rate unit. The resulting limit is shown on the right next to the drop down box.

Default: No Limit

- Egress:

Set up the limit of Egress bandwidth for the port you choose. Outgoing traffic will be discarded if the rate exceeds the value you set up in the Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid values are multiples (0 to 31) of the traffic rate unit. The resulting limit is shown on the right next to the drop down box.

Default: No Limit

4.2.15 Storm Control

Storm Control is used to block unnecessary multicast and broadcast frames that reduce the switch's performance. When the function is enabled and values of storm control are exceeded, multicast and broadcast frames will be dropped.

Storm Control Configuration

Storm Control	Number of frames per second
ICMP Rate	No Limit
Learn Frames Rate	No Limit
Broadcast Rate	No Limit
Multicast Rate	No Limit
Flooded unicast Rate	No Limit

Apply Refresh

1k
2k
4k
8k
16k
32k
64k
128k
256k
512k
1024k
No Limit

Parameter:

■ ICMP Rate:

Enables the ICMP Storm capability. The setting range is 1k-1024k per second. If the amount of ICMP packets reaches this value, ICMP packets will be dropped.

Default: No Limit

■ Learn Frames Rate:

To enable the Learn Frames Storm capability. User can use the drop-down menu to select the number of frames. The setting range is 1k~1024k per second.

Default: No Limit

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

4.2.16 SNMP

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. 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 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** and the setting takes effect.

SNMP Configuration	
SNMP enabled	<input checked="" type="checkbox"/>
SNMP Trap destination	0.0.0.0
SNMP Get Community	public
SNMP Set Community	private
SNMP Trap Community	public
System Event	<input checked="" type="checkbox"/> Cold Boot <input checked="" type="checkbox"/> Warm Boot
TP and Fiber Port Event	<input checked="" type="checkbox"/> Link Up Link Up Counter 1
	<input checked="" type="checkbox"/> Link Down Link Down Counter 0
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>	

Parameter:

■ **SNMP enable:**

Enables or disables SNMP.

Default: Enabled

■ **Get/Set/Trap Community:**

The 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 cannot access the device with a different community name via the SNMP protocol; If they both have the same community name, they can talk to each other.

The community name is user-definable variable 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 READ only works for the READ function and can't be applied to other functions such as WRITE or TRAP.

Default SNMP function : enable

Default community name for Get: public

Default community name for Set: private

Default community name for Trap: public

■ System Event:

Select the events for which an SNMP-Trap should be send (Cold Boot and/or Warm Boot).

Default: Enable

■ TP and Fiber Port Event:

Select the events on the ports for which an SNMP-Trap should be send (Link Up and/or Link Down).

4.3 Monitoring

There are five functions contained in the monitoring function: Detailed Statistics, LACP Status, RSTP Status, IGMP Status and Ping Status.

4.3.1 Detailed Statistics

Displays the detailed counting number of each port's traffic. All counter information for one port are shown at one time. Click on a port in the upper screen to show the values of this port. You can activate up to five receive statistics and five transmit statistics at the same time. Confirm your selection with a click on **Apply**. With **Refresh** you can update the table.

Statistics for Port 19

	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7
	Port 9	Port 10	Port 11	Port 12	Port 13	Port 14	Port 15
	Port 17	Port 18	Port 19	Port 20	Port 21	Port 22	Port 23
	Receive Total			Transmit Total			
Rx Octets	107575921			Tx Octets			
<input checked="" type="checkbox"/> Rx Packets	1294405			<input checked="" type="checkbox"/> Tx Packets			
<input checked="" type="checkbox"/> Rx High Priority Packets	1294406			<input checked="" type="checkbox"/> Tx High Priority Packets			
<input checked="" type="checkbox"/> Rx Low Priority Packets	0			<input checked="" type="checkbox"/> Tx Low Priority Packets			
<input checked="" type="checkbox"/> Rx Broadcast	1044233			<input checked="" type="checkbox"/> Tx Broadcast			
<input checked="" type="checkbox"/> Rx Multicast	177216			<input checked="" type="checkbox"/> Tx Multicast			
<input type="checkbox"/> Rx Broad- and Multicast	-			<input type="checkbox"/> Tx Broad- and Multicast			
<input type="checkbox"/> Rx Error Packets	-			<input type="checkbox"/> Tx Error Packets			
	Receive Size Counters			Transmit Size Count			
<input type="checkbox"/> Rx 64 Bytes	-			<input type="checkbox"/> Tx 64 Bytes			
<input type="checkbox"/> Rx 65-127 Bytes	-			<input type="checkbox"/> Tx 65-127 Bytes			
<input type="checkbox"/> Rx 128-255 Bytes	-			<input type="checkbox"/> Tx 128-255 Bytes			
<input type="checkbox"/> Rx 256-511 Bytes	-			<input type="checkbox"/> Tx 256-511 Bytes			
<input type="checkbox"/> Rx 512-1023 Bytes	-			<input type="checkbox"/> Tx 512-1023 Bytes			
<input type="checkbox"/> Rx 1024- Bytes	-			<input type="checkbox"/> Tx 1024- Bytes			
	Receive Error Counters			Transmit Error Count			
<input type="checkbox"/> Rx CRC/Aligment	-			<input type="checkbox"/> Tx Collisions			
<input type="checkbox"/> Rx Undersize	-			<input type="checkbox"/> Tx Drops			
<input type="checkbox"/> Rx Oversize	-						
<input type="checkbox"/> Rx Fragments	-						
<input type="checkbox"/> Rx Jabber	-						
<input type="checkbox"/> Rx Drops	-						

Parameter:

- Rx Packets:
The number of packets received.
- Rx Octets:
Total received bytes.
- Rx High Priority Packets:
Number of Rx packets classified as high priority.
- Rx Low Priority Packets:
Number of Rx packets classified as low priority.
- Rx Broadcast:
Shows the number of the received broadcast packets.

- Rx Multicast:
Shows the number of received multicast packets.
- Rx Broad- and Multicast:
Shows the number of received broadcasts with multicast packets.
- Rx Error Packets:
Shows the number of received error packets.
- Tx Packets:
The number of packets transmitted.
- Tx Octets:
Total transmitted bytes.
- Tx High Priority Packets:
Number of Tx packets classified as high priority.
- Tx Low Priority Packets:
Number of Tx packets classified as low priority.
- Tx Broadcast:
Shows the number of transmitted broadcast packets.
- Tx Multicast:
Shows the number of transmitted multicast packets.
- Tx Broad- and Multicast:
Shows the number of transmitted broadcasts with multicast packets.
- Tx Error Packets:
Shows the number of received error packets.
- Rx 64 Bytes:
Number of 64-byte frames in good and bad packets received.
- Rx 65-127 Bytes:
Number of 65 ~ 126-byte frames in good and bad packets received.
- Rx 128-255 Bytes:
Number of 127 ~ 255-byte frames in good and bad packets received.
- Rx 256-511 Bytes:
Number of 256 ~ 511-byte frames in good and bad packets received.
- Rx 512-1023 Bytes:
Number of 512 ~ 1023-byte frames in good and bad packets received.

- Rx 1024-Bytes:
Number of 1024-max_length-byte frames in good and bad packets received.
- Tx 64 Bytes:
Number of 64-byte frames in good and bad packets transmitted.
- Tx 65-127 Bytes:
Number of 65 ~ 126-byte frames in good and bad packets transmitted.
- Tx 128-255 Bytes:
Number of 127 ~ 255-byte frames in good and bad packets transmitted.
- Tx 256-511 Bytes:
Number of 256 ~ 511-byte frames in good and bad packets transmitted.
- Tx 512-1023 Bytes:
Number of 512 ~ 1023-byte frames in good and bad packets transmitted.
- Tx 1024-Bytes:
Number of 1024-max_length-byte frames in good and bad packets transmitted.
- Rx CRC/Alignment:
Number of Alignment errors and CRC error packets received. A cyclic redundancy check (CRC) checks an inspection value for data, to detect errors in the transmitting process and the storage.
- Rx Undersize:
Number of short frames (<64 Bytes) with valid CRC.
- Rx Oversize:
Number of long frames (according to max_length register) with valid CRC.
- Rx Fragments:
Number of short frames (< 64 bytes) with invalid CRC.
- Rx Jabber:
Number of long frames (according to max_length register) with invalid CRC.
- Rx Drops:
Frames dropped due to the lack of receiving buffer.
- Tx Collisions:
Number of collisions transmitting frames experienced.

■ Chapter 4: Operation of Web-based Management

- Tx Drops:
Number of frames dropped due to excessive collision, late collision, or frame aging.
- Tx Overflow:
Number of frames dropped due to the lack of transmitting buffer.






4.3.2 LACP Status

The LACP Status window shows LACP information and status for all ports at the same time. Within the IEEE specification the Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel.

LACP Aggregation Overview

Group/Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
Normal																									

Legend

	Down	Port link down
	Blocked	Port Blocked by RSTP. Number is Partner port number if other switch has LACP enabled
	Learning	Port Learning by RSTP
	Forwarding	Port link up and forwarding frames
	Forwarding	Port link up and forwarding by RSTP. Number is Partner port number if other switch has

Parameter:

- LACP Aggregation Overview:
Shows the group/port status. Default will set to red sign for “port link down”. Please check legend table below for all references.
- LACP Port Status:
Group/Port: Shows the port number.
Normal: See Legend.

4.3.3 RSTP Status

RSTP Status shows the present VLAN bridge information and the status of all ports.

RSTP VLAN Bridge Overview

VLAN Id	Bridge Id	Hello Time	Max Age	Fwd Delay	Topology	Root Id
1	32769:00-40-c7-3c-00-25	2	20	15	Steady	This switch is Root!

[Refresh](#)

RSTP Port Status

Port/Group	Vlan Id	Path Cost	Edge Port	P2p Port	Protocol	Port State
Port 1						Non-STP
Port 2						Non-STP
Port 3						Non-STP
Port 4						Non-STP

Parameter:

- VLAN ID:
Shows VLAN ID.
- Bridge ID:
Shows bridge priority setting and bridge ID of the switch, which stands for the MAC address of this switch.
- Hello Time:
Shows the current hello time of the root bridge.
- Max. Age:
Shows the current root bridge maximum age time.
- Forward Delay:
Shows the current root bridge forward delay time.
- Topology:
Shows the root bridge's spanning tree topology.
- Root ID:
Shows Root bridge ID of this network segment. If this switch is a root bridge the text: "This switch is Root" will appear.

4.3.4 IGMP Status

Internet Group Management Protocol (IGMP) is used to snoop the status of IP multicast groups and display its associated information in both tagged VLAN and non-tagged VLAN networks. When IGMP snooping is enabled in the switch it analyzes all IGMP packets between hosts connected to the switch and multicast router in the network. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host's port number to the multicast list for that group. When the switch hears an IGMP Leave, it removes the host's port from the table entry.

IGMP Status shows the VLAN ID for each multicast group.

IGMP Status

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

IGMP Status

Page:1

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

Refresh First Page Prev Page Next Page

Parameter:

- VLAN ID:
Shows VLAN ID for each multicast group.
- Querier:
Shows the group membership queries status.
- Queries transmitted:
Shows the number of group membership queries transmitted.
- Queries received:
Shows the number of group membership queries received.
- V1 Reports:
When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The

host then sets a timer, with a value less than the Max Response Time field in the query, for each group to which it belongs. It calculates the number of times of IGMPV1 report.

- V2 Reports: See V1.
- V3 Reports: See V1.
- V2 Leaves:

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

4.3.5 Ping Status

Sets up target IP address for ping function and display ping status.

Ping test function is a tool for detecting if the target device is alive or not through the ICMP protocol which abounds with report messages. The switch provides the ping test function to let you know if the target device is available or not. Fill in an IP address and click **Apply**. The result will show if the target device is available. You can update the table with a click on **Refresh**.

Ping Parameters

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

Apply

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

Refresh

Parameter:

- Ping Parameter:
 - Target IP address:
Target IP address to ping.

- Count:
Use the drop-down menu to set the number of echo requests to send.
Four type of number are possible: 1, 5, 10 and 20.
Default: 1
- Time Out (in secs):
Use the drop-down menu to set the number of echo requests time out in second. Four type numbers are possible: 1, 5, 10 and 20.
Default: 1
NOTE: You need to press **Apply** to start after you set the parameters.

- Ping Results:
 - Target IP address:
Shows the active target IP address.
 - Status:
Shows the result of the ping status.
- Received replies:
Shows the received replies number of times.
- Request timeouts:
Shows the timeout of request.
- Average Response times (In ms):
Shows the average response time in milliseconds.

4.4 Maintenance

In this section the functions are described for maintaining the switch.

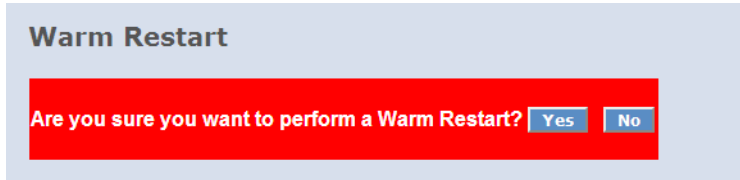
4.4.1 Warm Restart

Warm restart provides the function to restart the device.



After upgrading software, you must restart the switch to have the new configuration taken in effect.

- Warm restart: Press **Yes** to confirm warm restart function. It will take around 30 seconds to complete the system boot.



4.4.2 Factory Default

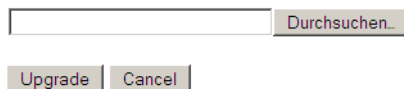
Factory default provides the function to retrieve default settings and replace current configuration. Except the IP address setting, all settings will be restored to the factory default values when "Factory Default" function is performed. If you want to restore all configurations including the IP address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



4.4.3 Software Upgrade

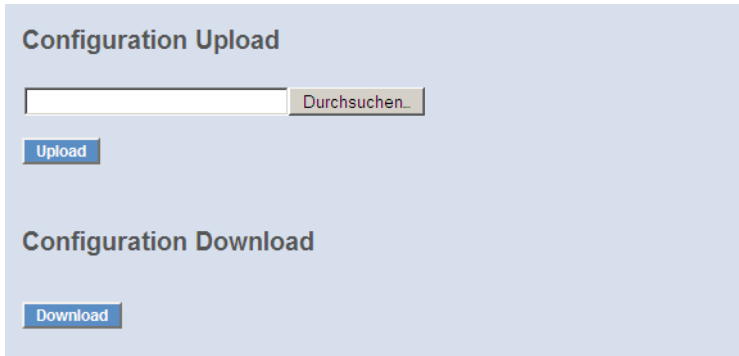
You can just click the browse button to retrieve the file you want in your system to upgrade your switch.

Software Upgrade



4.4.4 Configuration File Transfer

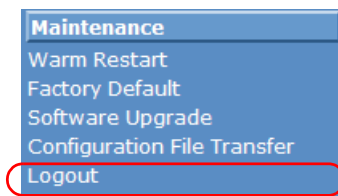
You can backup your switch's configuration file into your computer folder in case accident happens. In addition, uploading backup configuration file into a new or a crashed switch can save much time and avoid mistakes.



4.4.5 Logout

The switch allows you to log out of the system to prevent other users from using the system without permission. There are three possibilities to log out or be logged out.

- Auto Logout: If Auto Logout is ON and no action/no key stroke is done for the time (in minutes) you set up in the Auto Logout Timer, the switch will log you out automatically.
- Implicit Logout: If you do not log out and exit the browser, the switch will automatically log you out.
- Logout Function: The switch allows administrators to log out manually by Logout function.



5 Appendix

5.1 Performance data and specification

	LANCOM GS-1224	LANCOM GS-1224P
Performance	Switching technology	Store and forward with latency less than 5 µs
	MAC addresses	Support of maximal 8K MAC addresses
	Throughput	maximal 48 Gbps on the backplane
	VLAN	Port based and IEEE 802.1q tag based VLAN with up to 4096 VLAN and up to 24 active VLANs; Supports ingress and egress packet filter in port based VLAN
LAN protocols	Link Aggregation Control Protocol (LACP)	Maximal 12 groups, max 8 member per group, supports DA, SA and DA+SA MAC based trunking with automatic failover
	Multicasting	Supports IGMP snooping
	Spanning Tree Protokoll (STP) / Rapid STP	802.1d/1w
802.3af Features	Ports	24x 802.3af PoE ports
	Power	185 Watt total power with dynamic load balancing on all ports (i.e. up to 15.4 watt for 12 ports or 7.7 watt für 24 ports)
	Priorisation	Supports port based priority and PoE status setting
	Status information	Monitoring via LED, displaying the actual power consumption per port in web interface
Interfaces	Ethernet ports	24 ports 10/100/1000 Mbps ethernet, 4 Combo ports TP/SFP 10/100/1000 Mbps
Power supply		Internal power supply unit (110–230 V, 50-60 Hz)
Housing		Robust metal housing, 19" 1HE (440 x 44,2 x 170 mm) with removable mounting brackets, network connectors on the front
Standards		CE conformity according to EN 55022, EN 55024, EN 60950
Environment/ Temperature		Temperature range 0–40°C; humidity 5–90%; non-condensing

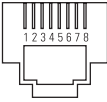
■ Chapter 5: Appendix

	LANCOM GS-1224	LANCOM GS-1224P
Accessories		<ul style="list-style-type: none"> ■ 1000Base-SX SFP module, LANCOM SFP-SX-LC1, item no. 61556 ■ 1000Base-LX SFP module, LANCOM SFP-LX-LC1, item no. 61557
Service		5 years
Support		Via Hotline and Internet

5.2 Connector wiring

5.2.1 Ethernet interface 10BASE-T/100BASE-TX/1000BASE-T

8-pin RJ45 sockets (ISO 8877, EN 60603-7)

Connector	Pin	Fast Ethernet	Gigabit Ethernet
	1	T+	BI_DA+
	2	T-	BI_DA-
	3	R+	BI_DB+
	4	PoE/G	BI_DC+
	5	PoE/G	BI_DC-
	6	R-	BI_DB-
	7	PoE/ -48 V	BI_DD+
	8	PoE/ -48 V	BI_DD-

5.3 CE-declarations 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 can be found on the relevant product page on the LANCOM Web site (www.lancom.eu).

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Germany

E-Mail: info@lancom.eu

Internet www.lancom.eu