

Lantech

IES-5208DF Series

8 10/100TX + 2 100/1000FX Dual Speed Fiber L2⁺ Industrial
Managed Switch w/ITU G.8032 Ring

User Manual



IP-67



IP-43

Dec. 2013

Important Notice

Lantech Communications Global, Inc. reserves the right to modify the equipment, its specification or this manual without prior notice, in the interest of improving performance, reliability, or servicing. At the time of publication all data is correct for the operation of the equipment at the voltage and/or temperature referred to. Performance *data* indicates typical values related to the particular product.

No part of this documentation or information supplied may be divulged to any third party without the express written consent of Lantech Communications Global Inc. Products offered may contain software which is proprietary to Lantech Communications Global Inc. The offer or supply of these products and services does not include or infer any transfer of ownership.

Interference Issues

This Equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a commercial or industrial installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions.

FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Content

Chapter 1 Introduction	1
Hardware Features	1
Software Features	4
Chapter 2 Hardware Description.....	8
2.1 Physical Dimension.....	8
2.2 IP Protection	9
2.3 LED Indicators	12
Chapter 3 Hardware Installation	13
Chapter 4 Network Application.....	17
ITU G.8032 Scheme	17
Ring Coupling	17
Multiple Rings.....	18
Dual Homing.....	18
Chain.....	18
Chapter 5 Console Management.....	21
5.1 Connecting to the Console Port.....	21
5.2 Login in the Console Interface.....	21
Chapter 6 Web-Based Management	23
6.1 About Web-based Management.....	23
6.2 Preparing for Web Management	23
6.3 System Login	24
6.4 System.....	25
6.4.1 System Identification Configuration.....	25
6.4.2 Switch Information	26

6.4.3 IP configuration.....	26
6.4.4 DHCP server.....	28
6.4.5 System Time	29
6.4.6 SNMP Configuration	33
6.4.7 Fault Relay Configuration	34
6.4.8 Digital Input/Output.....	36
6.5 Event & Log.....	38
6.5.1 View Logs	38
6.5.2 Events	39
6.5.3 Actions	39
6.5.4 Event Action Map	42
6.6 Ports.....	45
6.6.1 Device Settings.....	45
6.6.2 Status	46
6.6.3 Statistics	46
6.6.4 Mirroring.....	47
6.6.5 Rate Limiting	48
6.6.6 Loop Protection.....	49
6.7 Power over Ethernet.....	50
6.8 Topology.....	51
6.9 QoS.....	54
6.9.1 QoS Policy	54
6.10 Security	56
6.10.1 MAC Address Tables.....	56
6.10.2 Access Control List.....	57
6.10.3 IEEE 802.1X Radius Server	58
6.10.4 IP Security	59
6.11 VLAN.....	60

6.11.1 802.1Q VLAN Config	60
6.11.2 Status.....	62
6.12 MVR	63
6.12 LLDP	64
6.12.1 LLDP Configuration	64
6.12.2 LLDP Neighbor	65
6.12.3 LLDP Statistics	67
6.13 CDP	70
6.13.1 CDP Configuration Device Settings	70
6.13.2 CDP Port Configuration	71
6.13.3. CDP Status	71
6.14 IGMP Snooping	73
6.14.1 IGMP Snooping Configuration.....	74
6.14.2 IGMP Snooping Status	75
6.15 MSTP	77
6.15.1. MSTP Global Configuration	77
6.15.2 How to enable MSTP	78
6.15.3 CIST Settings.....	80
6.15.3.1 Bridge configuration	80
6.15.3.2 Port.....	80
6.15.4. MSTP MSTI Settings	81
6.15.5. MSTP Bridges Status	82
6.15.6. Bridge status of all ports	83
6.16 Aggregation.....	84
6.16.1. Aggregation Configuration.....	84
6.16.2 LACP Port Status	85
6.17 PTP IEEE 1588 v2.....	86

6.18 G.8032 ERPS	88
6.18.1. G.8032 Ethernet Ring Protection Configuration	88
6.18.2 How to set ERPS G.8032	89
6.19 Dual Homing.....	92
6.20 Maintenance	94
6.20.1 Save Configuration	94
6.20.2 Config backup/restore	94
6.20.3 Restart device	95
6.20.4 Firmware Upgrade	96
6.20.5 Diagnostics	96
Appendix —Command Line mode	98

Chapter 1 Introduction

Lantech IES-5408DF (IP67/IP43) series is a high performance L2⁺ IP67/IP43 industrial Gigabit uplink switch with 8x10/100TX + 2 100/1000FX Dual Speed Fiber by M12 connectors which provides L2 wire speed and advanced security function. It delivers ITU G.8032 ring recovery less than 50ms, comprehensive QoS, , IGMPv1/v2/v3 & routing, QinQ (double tag VLAN) , MVR (multicast VLAN registration) , LACP link aggregation and advanced security including ACL, TACAS+*, SSH/SSL, DHCP Option 82*which are important features required in large network. It also supports Cisco Discovery Protocol (CDP) and LLDP for Ciscoworks to detect the switch info to be shown on L2 map topology. The user friendly UI, innovative auto topology drawing and topology demo makes IES-5408DF (IP67/IP43) much easier to get hands-on.

Hardware Features

Standard	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX IEEE802.3z Gigabit fiber IEEE802.3x Flow Control and Back Pressure IEEE802.3ad Port trunk with LACP IEEE802.1d Spanning Tree IEEE802.1w Rapid Spanning Tree IEEE802.1s Multiple Spanning Tree IEEE 802.3ad Link Aggregation Control Protocol (LACP) IEEE 802.1AB Link Layer Discovery Protocol (LLDP) IEEE 802.1X User Authentication (Radius) IEEE802.1p Class of Service IEEE802.1Q VLAN Tag
Switch Architecture	Back-plane (Switching Fabric): 5.6Gbps Packet throughput ability (Full-Duplex): 13.8Mpps @64bytes

Transfer Rate	14,880pps for Ethernet port 148,800pps for Fast Ethernet port 1,488,000pps for Gigabit Ethernet port
MAC Address	16K MAC address table
Connector	10/100TX: 8 x M12 4-pole type D-Coded connector 100/1000FX Dual Speed Fiber: 2 x LC connector Power Input: 1 x M12 5-pole A-coded connector Relay Contact: 1 x M12 5-pole A-coded connector RS-232 connector: 1 x M12 5-pole A-coded connector
Network Cable	10Base-T: 2-pair UTP/STP Cat. 3, 4, 5 cable EIA/TIA-568 100-ohm (100m) 100Base-TX: 2-pair UTP/STP Cat. 5/ 5E cable EIA/TIA-568 100-ohm (100m)
Optical Fiber	<p>Giga:</p> Multi-mode: 50/125um~62.5/125um Single mode: 9/125um Available distance: 0.5km (Multi-mode)/10km (Single-mode) Wavelength: 1310nm (Multi-mode/Single-mode) <p>100M:</p> Multi-mode: 50/125um~62.5/125um Single mode: 9/125um Available distance: 2km (Multi-mode)/30km (Single-mode) Wavelength: 1310nm (Multi-mode/Single-mode) <p>Characteristics:</p> Min. TX Output: -9 dBm Max. TX Output: -3 dBm RX Sensitivity: -24 dBm (@1.25Gbps); -29 dBm (@125Mbps) RX Saturation Level: -3 dBm The optical power is launched into a 9/125μm single-mode fiber

Protocol	CSMA/CD
LED	Per unit: Power 1 (Green), Power 2 (Green), P-Fail (Red) Ethernet port: Link/Activity (Green), Speed (Green); Giga-T: Link/Activity (Green)
DI/DO	1 Digital Input(DI): Level 0: -30~2V/Level1: 10~30V Max. input current:8mA 1 Digital Output(DO): open collector to 40VDC, 200mA
Power Supply	Standard model: 12~48VDC (9.2 to 68 VDC) -48VDC is available for single power input
Power Consumption	Max. 10W
Operating Humidity	5% to 95% (Non-condensing)
Operating Temperature	-40°C ~ 75°C
Storage Temperature	-40°C ~ 85°C
Case Dimension	Aluminum case. IP-67, 215 (W) x 200 (D) x 84.4 (H) mm Aluminum case. IP-43, 203 (W) x 187(D) x 84.4 (H) mm
Installation	DIN rail** and wall mount ear
EMI	FCC Class A, CE EN61000-4-2, CE EN61000-4-3, CE EN-61000-4-4, CE EN61000-4-5, CE EN61000-4-6, CE EN61000-4-8, CE EN61000-4-11, CE EN61000-4-12, CE EN61000-6-2, CE EN61000-6-4
Stability Testing	IEC60068-2-32 (Free fall), IEC60068-2-27 (Shock), IEC60068-2-6 (Vibration)

Software Features

Management	SNMP v1 v2c, v3/ Web/Telnet/CLI
SNMP MIB	RFC 1215 Traps MIB, RFC 1213 MIBII, RFC 1157 SNMP MIB, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC 1643 EtherLike, RFC 1757 RMON, RSTP MIB, Private MIB, LLDP MIB
ITU G.8032	Support ITU G.8032 v2 for Ring protection in less than 10ms for self-heal recovery < 256 switches ; Support various ring/chain topologies Ring covers data & multicast* packets
User friendly UI	<ul style="list-style-type: none"> ● Auto topology drawing ● Topology demo ● Auto configuration for G.8032*
Port Trunk with LACP	LACP Port Trunk: 4 Trunk groups/Maximum 4 trunk members Load balancing through LACP to distribute load*
LLDP	Supports LLDP to allow switch to advise its identification and capability on the LAN
CDP	Cisco Discovery Protocol for topology mapping
VLAN	Port Based VLAN IEEE 802.1Q Tag VLAN (256 entries)/ VLAN ID (Up to 4K, VLAN ID can be assigned from 1 to 4096.)

	GVRP (256 Groups)*, GMRP*, MVRP (Multi VLAN Registration), QinQ*
Network Security	<p>Support 10 IP addresses that have permission to access the switch management and to prevent unauthorized intruder.</p> <p>802.1X access control for port based and MAC based authentication/MAC-IP-Port binding</p> <p>Management access control with priority *</p> <p>256 Policy based Access Control List*</p> <p>SSL/ SSH for Management</p> <p>TACACS+ for Authentication*</p>
SMTP/Text SMS	Supports SMTP Server and 6 e-mail accounts for receiving event alert; can send SMS text alert via mobile
Spanning Tree	Supports IEEE802.1d Spanning Tree and IEEE802.1w Rapid Spanning Tree, IEEE802.1s Multiple Spanning Tree
Quality of Service	The quality of service determined by port, Tag and IPv4 Type of service, IPv4 Different Service
Class of Service	Supports IEEE802.1p class of service, per port provides 4 priority queues
IP Security	Supports 10 IP addresses that have permission to access the switch management and to prevent unauthorized intruder.
Login Security	Supports IEEE802.1X Authentication/RADIUS
Port Mirror	Support 3 mirroring types: "RX, TX and Both packet"

IGMP	Support IGMP snooping v1,v2,v3; Supports IGMP static route 256 multicast groups and IGMP query
Multicast VLAN Registration*	MVR enables multicast packets go through VLAN for VOD application
Bandwidth Control	Support ingress packet filter and egress packet limit. The egress rate control supports all of packet type. Ingress filter packet type combination rules are Broadcast/Multicast/Flooded Uni-cast packet, Broadcast/Multicast packet, Broadcast packet only and all types of packet. The packet filter rate can be set an accurate value through the pull-down menu for the ingress packet filter and the egress packet limit.
RTC	Built-in Real Time Clock to keep track of time always
Flow Control	Supports Flow Control for Full-duplex and Back Pressure for Half-duplex
System Log	Supports System log record and remote system log server
SMTP	Supports SMTP Server and 6 e-mail accounts for receiving event alert
Relay Alarm	Provides one relay output for port breakdown, power fail Alarm Relay current carry ability: 1A @ DC24V
SNMP Trap	1. Topology Change 2. Power Trap 3. MAC-Violation
DHCP	Provides DHCP Client/ DHCP Server/ Port and IP Binding

DNS	Provides DNS client feature and supports Primary and Secondary DNS server
SNTP	Supports SNTP to synchronize system clock in Internet
Firmware Update	Supports TFTP firmware update, TFTP backup and restore.
Configuration Upload/Download	Supports text configuration file for system quick installation;
ifAlias	Each port allows an alphabetic string of 128-byte assigned as its own unique name via the SNMP or CLI interface

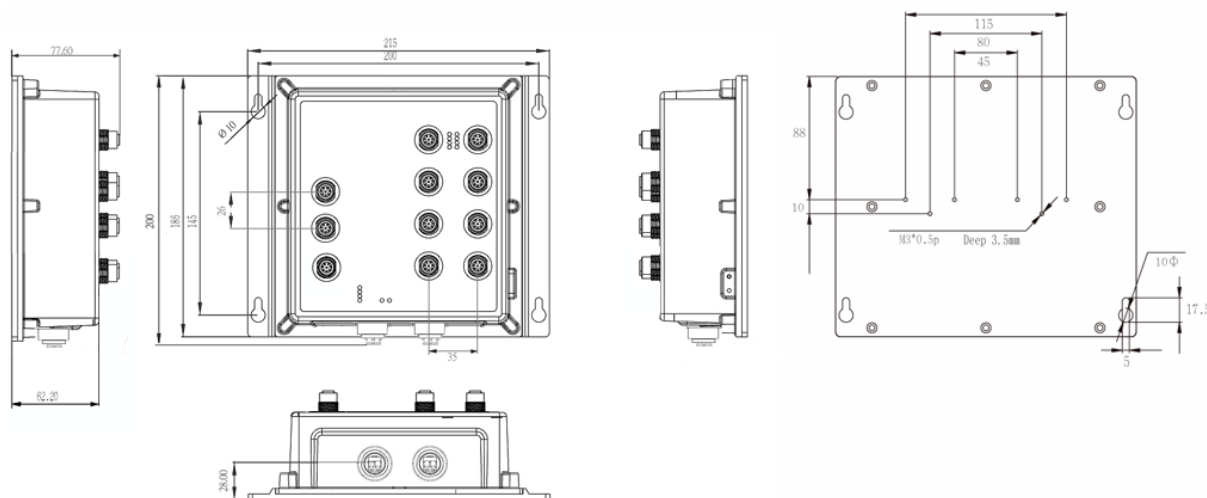
Chapter 2 Hardware Description

In this paragraph, it will describe the Industrial switch's hardware spec, port, cabling information, and wiring installation.

2.1 Physical Dimension

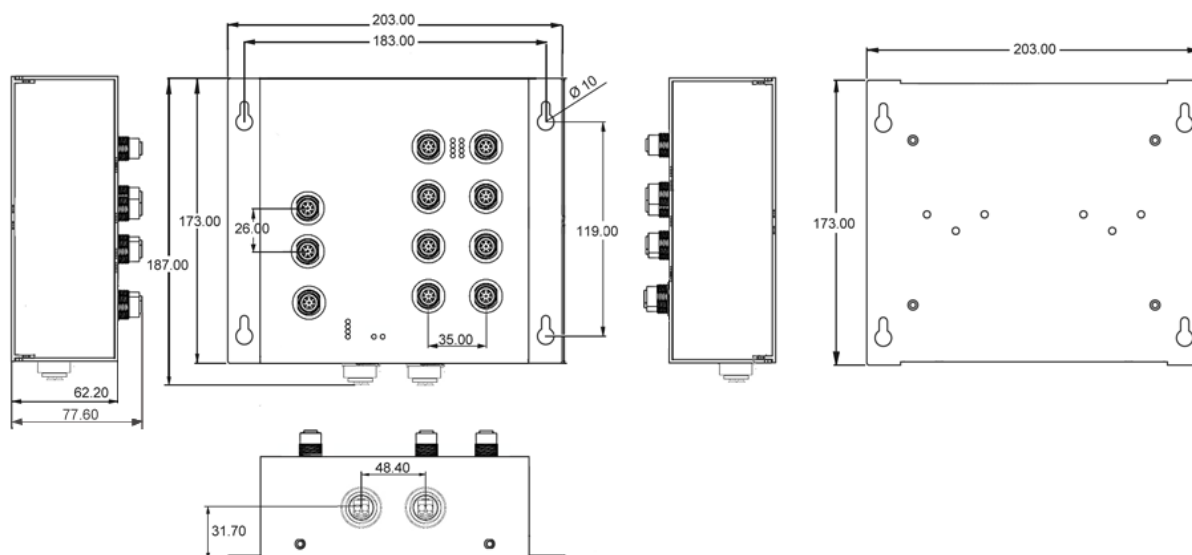
Aluminium case. IP-67,

215 (W) x 200 (D) x 84.4 (H) mm



Aluminium case. IP-43,

203 (W) x 187(D) x 84.4 (H) mm



2.2 IP Protection

The **IP Code, Ingress Protection Rating**, sometimes also interpreted as **International Protection Rating**, classifies and rates the degree of protection provided against the intrusion (including body parts such as hands and fingers), dust, accidental contact, and water in *mechanical casings* and with electrical enclosures. It is published by the International Electrotechnical Commission (IEC)

Solid particle protection

The first digit indicates the level of protection that the enclosure provides against access to hazardous parts (e.g., electrical conductors, moving parts) and the ingress of solid foreign objects.

Level	Object size protected against	Effective against
0	—	No protection against contact and ingress of objects
1	>50 mm	Any large surface of the body, such as the back of a hand, but no protection against deliberate contact with a body part
2	>12.5 mm	Fingers or similar objects
3	>2.5 mm	Tools, thick wires, etc.
4	>1 mm	Most wires, screws, etc.
5	Dust protected	Ingress of dust is not entirely prevented, but it must not enter in sufficient quantity to interfere with the satisfactory operation of the equipment; complete protection against contact
6	Dust tight	No ingress of dust; complete protection against contact

Liquid ingress protection

The second digit indicates the level of protection that the enclosure provides against harmful ingress of water.

Level	Protected against	Testing for	Details
0	Not protected	—	—
1	Dripping water	Dripping water (vertically falling drops) shall have no harmful effect.	Test duration: 10 minutes Water equivalent to 1 mm rainfall per minute
2	Dripping water when tilted up to 15°	Vertically dripping water shall have no harmful effect when the enclosure is tilted at an angle up to 15° from its normal position.	Test duration: 10 minutes Water equivalent to 3 mm rainfall per minute
3	Spraying water	Water falling as a spray at any angle up to 60° from the vertical shall have no harmful effect.	Test duration: 5 minutes Water volume: 0.7 litres per minute Pressure: 80–100 kPa
4	Splashing of water	Water splashing against the enclosure from any direction shall have no harmful effect.	Test duration: 5 minutes Water volume: 10 litres per minute Pressure: 80–100 kPa
5	Water jets	Water projected by a nozzle (6.3 mm) against enclosure from any direction shall have no harmful effects.	Test duration: at least 15 minutes Water volume: 12.5 litres per minute Pressure: 30 kPa at distance of 3 m
6	Powerful	Water projected in powerful	Test duration: at least

	water jets	jets (12.5 mm nozzle) against the enclosure from any direction shall have no harmful effects.	3 minutes Water volume: 100 litres per minute Pressure: 100 kPa at distance of 3 m
7	Immersion up to 1 m	Ingress of water in harmful quantity shall not be possible when the enclosure is immersed in water under defined conditions of pressure and time (up to 1 m of submersion).	Test duration: 30 minutes Immersion at depth of at least 1 m measured at bottom of device, and at least 15 cm measured at top of device
8	Immersion beyond 1 m	The equipment is suitable for continuous immersion in water under conditions which shall be specified by the manufacturer. Normally, this will mean that the equipment is hermetically sealed. However, with certain types of equipment, it can mean that water can enter but only in such a manner that it produces no harmful effects.	Test duration: continuous immersion in water Depth specified by manufacturer
9	Powerful high temperature water jets	Protected against close-range high pressure, high temperature spray downs.	—

2.3 LED Indicators

The diagnostic LEDs that provide real-time information of system and optional status are located on the front panel of the industrial switch. The following table provides the description of the LED status and their meanings for the switch.

LED	Color	Status	Meaning
R.M	Green	On	The switch unit is owner switch of ITU-Ring
		Off	The switch is not owner switch
PWR1	Green	On	Power 1 is active
		Off	Power 1 is inactive
PWR2	Green	On	Power 2 is active
		Off	Power 2 is inactive
FAULT	Red	On	Power or port failure
		Off	No failure
P1 ~ P8	Link/Ack	On	A network device is detected.
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached
P9 ~ P10	Link/Ack	On	A network device is detected.
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached.

Chapter 3 Hardware Installation

3.1 Hardware installation

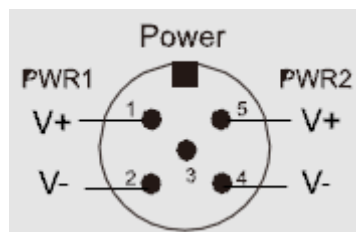
3.1.1 Unpack switch and check the accessory with packing list

3.1.2 Mount the switch on desired position

3.1.3 Connect the M12 connector of power input. The Power supply voltage for IES-5208DF series is connected via a 5-pin M12 connector and supplied with by an external power supply unit.

■ Voltage of Power Input

With IES-5208DF series standard models, the voltage of power input can use 12/24/48VDC and -48VDC.

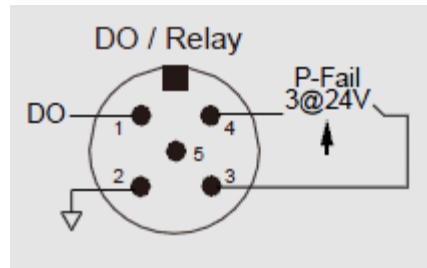


Pin assignment of Power input

■ Redundant Power Input

The power input can be supported redundantly. The supply voltage is electrically isolated from the housing.

Note: With single power supply of the mains voltage, the device will report a power failure. You can disable this power fail event via web browser.



Pin assignment of alarm relay

A break in contact is reported via the relay contact :

- The failure of at least one of the two supply voltages.
- The break link status of at least one switch port.

3.1.4 Fitting the device, grounding

Install the system in a dry and clean area to protect the switch to get exposed with dirt.

Plug the connector to the power supply plug then turn on the power supply.

■ Ground

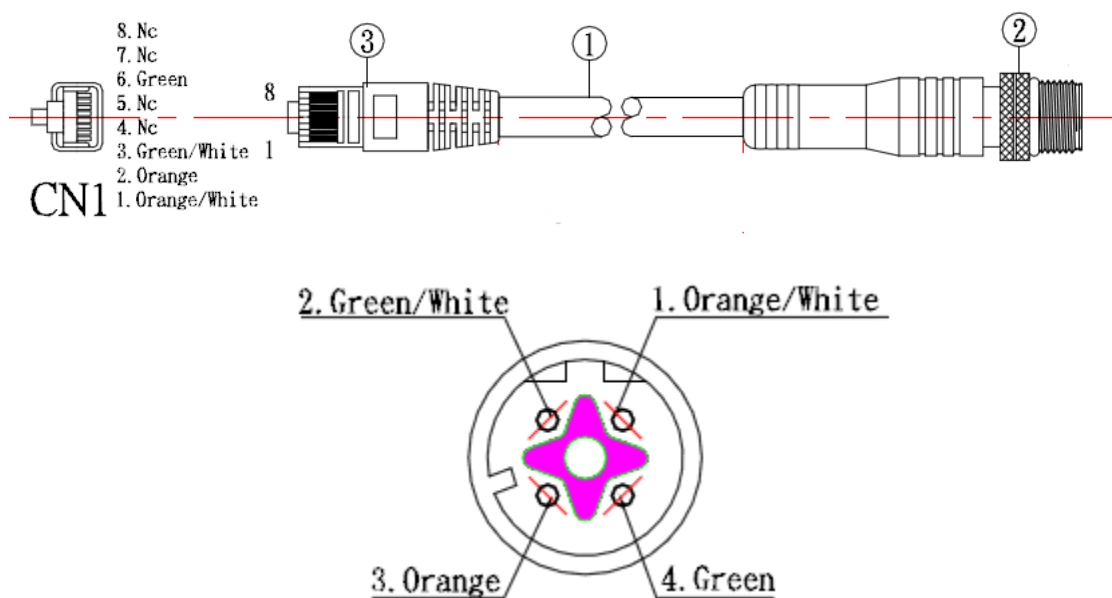
The chassis is grounded via a separate ground nut (M3).

Use toothed locking washers for a good electrical connection.

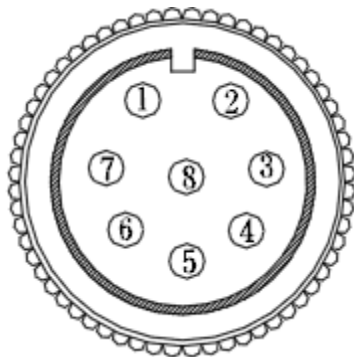


Ground screw of IES-5208DF switch

3.1.5 Connect the M12 connector with RJ-45 data cable, ports are not used shall be capped that comes with the package to insulate the surrounding.



Pin assignment of M12 10/100Tx network connector

	Gnd	Shell
	Brown	8
	Brown/White	7
	Green	6
	Blue/White	5
	Blue	4
	Green/White	3
	Orange	2
	Orange/White	1
	Wire Color	CN. 2

Pin assignment of M12 10/100/100T network connector

3.1.6 Check the status of LED, make sure the switch was in working status.

Note:

- The protection class IP67/IP43 is only achieved when bolted together.
- The other components attaching to the system have to meet with the IP67/IP43 protection class in order to reach the whole system IP 67/IP43 protection.
- Empty ports must be sealed with the protective caps supplied.

Chapter 4 Network Application

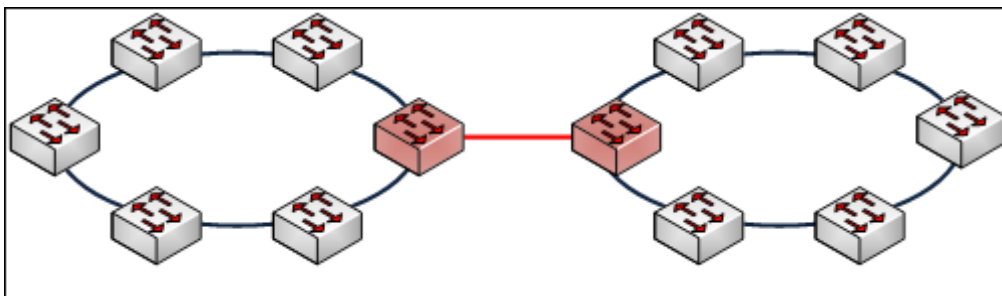
ITU G.8032 Scheme

Lantech G.8032 protocol is following ITU (International Telecommunication Unit) G.8032 v2 draft. The benefits of G.8032 are:

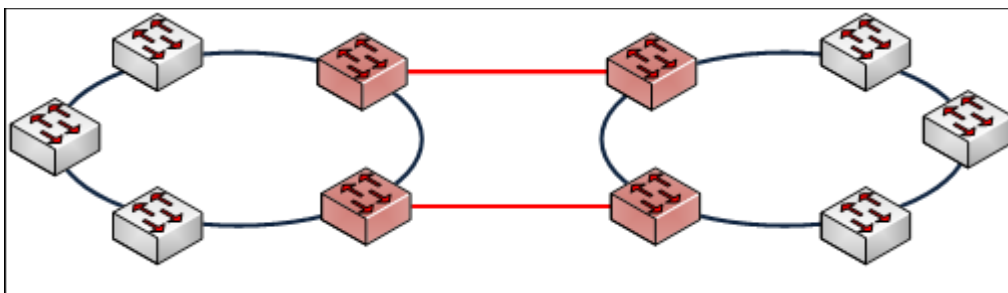
1. <50ms recovery time when failover
2. G.8032 has defined the protocol scheme, parameters, functions, test measures to be unified that the users can evaluate the possible network infrastructure without literally testing each brand in large scale.

Ring Coupling

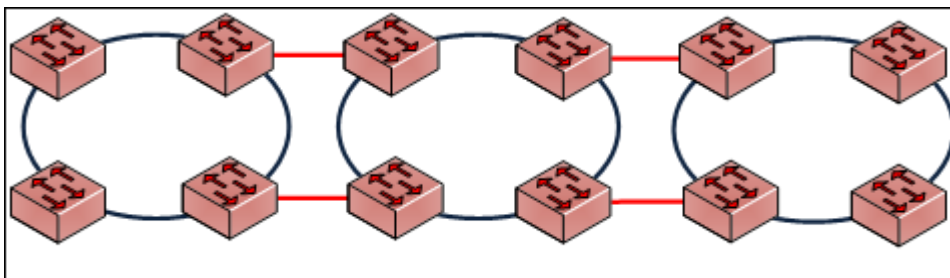
1-1. Single Coupling



1-2. Redundant Coupling

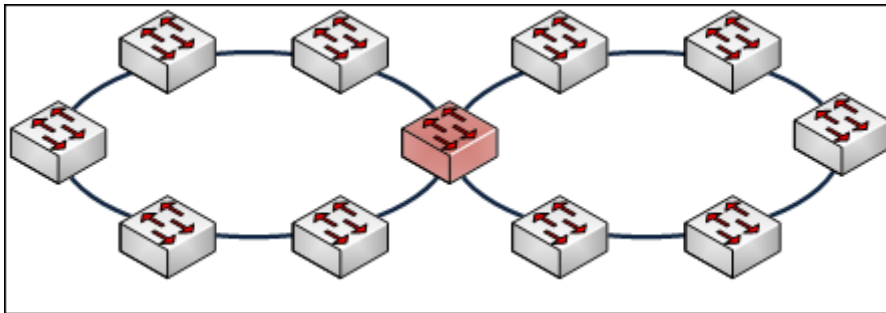


1-3. Redundant Coupling with Multiple Rings

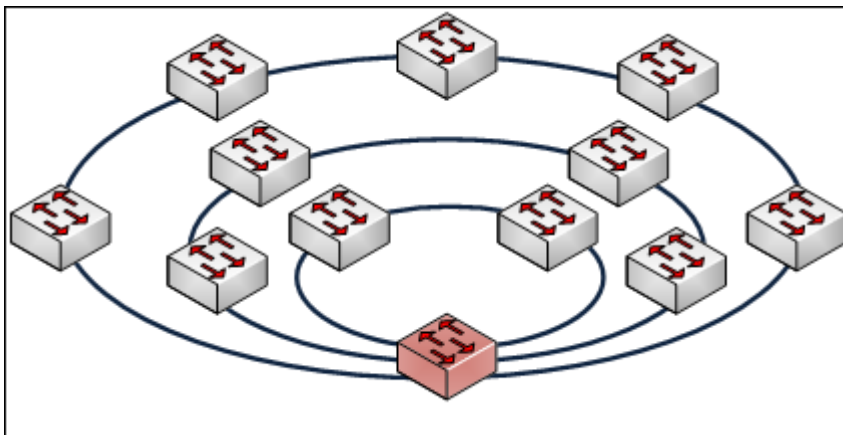


Multiple Rings

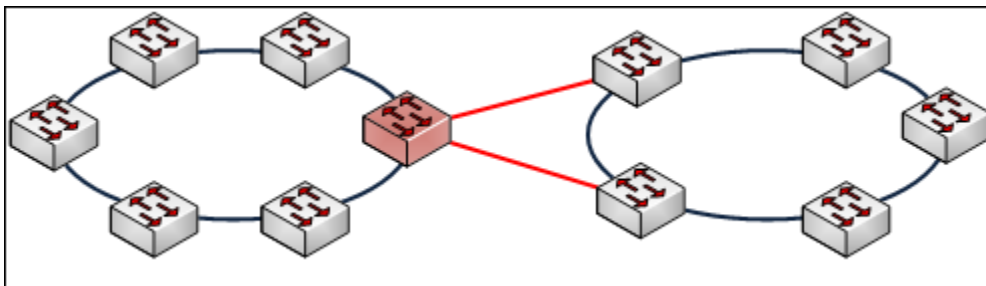
1-4. Dual Rings



1-5. Multiple Rings

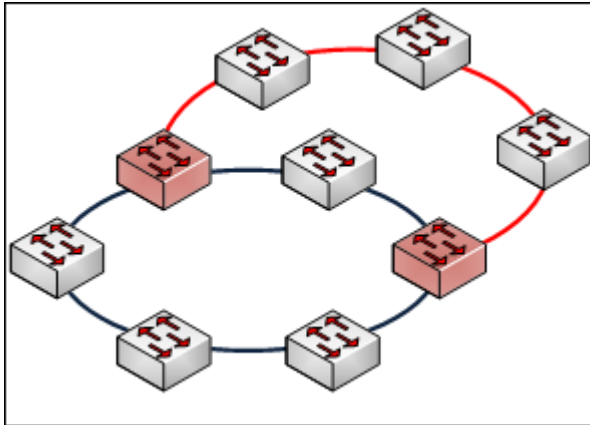


Dual Homing

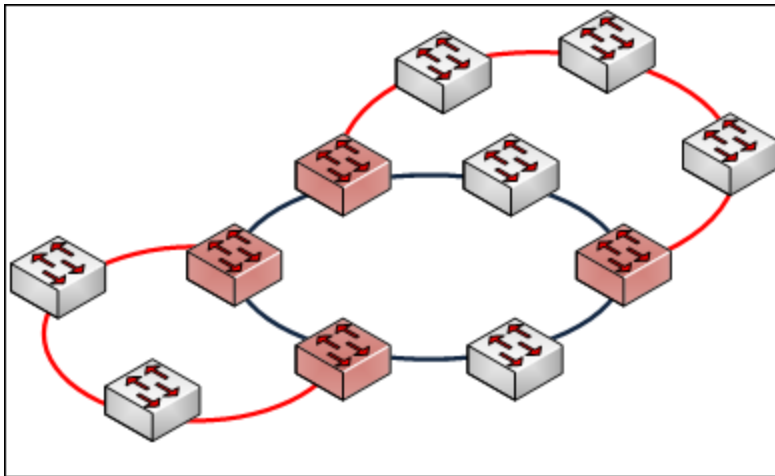


Chain

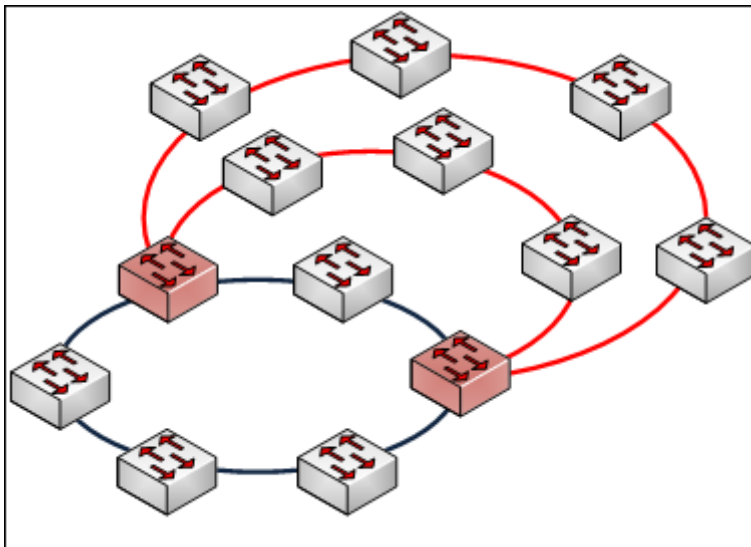
1-6. Single Chain



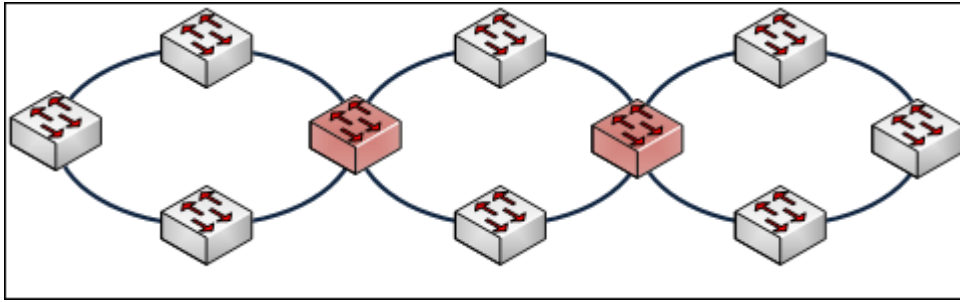
1-7. Multiple Chains



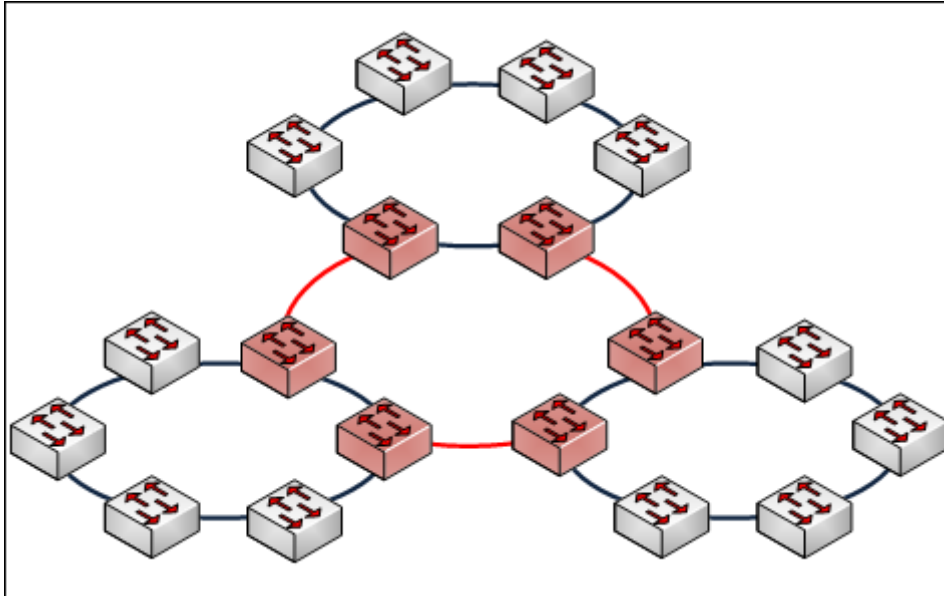
1-8. Multiple Chains Share Common Ends



1-9. Cascade Chain



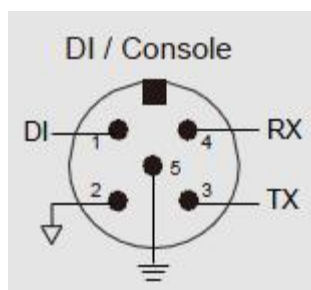
1-10. Chain in Chain



Chapter 5 Console Management

5.1 Connecting to the Console Port

The supplied cable which one end is M12 5-pole connector and the other end is RS-232 connector. Attach the end of RS-232 connector to PC or terminal and the other end of M12 connector to the console port of the switch. The connected terminal or PC must support the terminal emulation program.



5.2 Login in the Console Interface

When the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program or **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

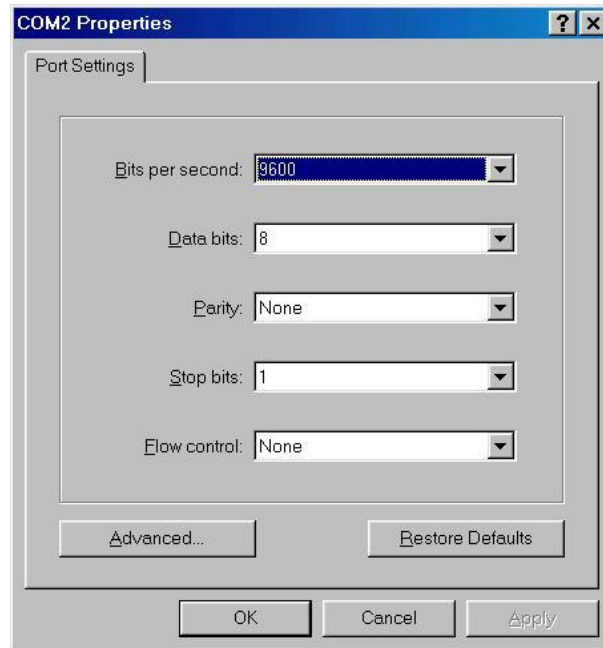
Baud Rate:115200 bps

Data Bits: 8

Parity: none

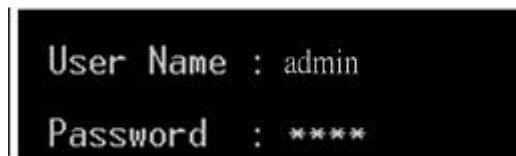
Stop Bit: 1

Flow control: None



The settings of communication parameters

Having finished the parameter settings, click '**OK**'. When the blank screen shows up, press Enter key to have the login prompt appears. Key in '**admin**' (default value) for both User name and Password (use **Enter** key to switch), then press Enter and the Main Menu of console management appears. Please see below figure for login screen.



Console login interface

Chapter 6 Web-Based Management

This section introduces the configuration and functions of the Web-Based management.

6.1 About Web-based Management

There is an embedded HTML web site residing in flash memory on CPU board of the switch, which offers advanced management features and allows users to manage the switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 6.0 or later version. And, it is applied for Java Applets for reducing network bandwidth consumption, enhance access speed and present an easy viewing screen.

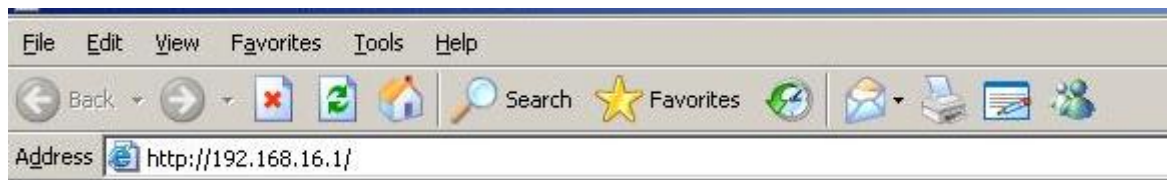
6.2 Preparing for Web Management

Before using the web management, install the industrial switch on the network and make sure that any one of the PCs on the network can connect with the industrial switch through the web browser. The industrial switch default value of IP, subnet mask, username and password are listed as below:

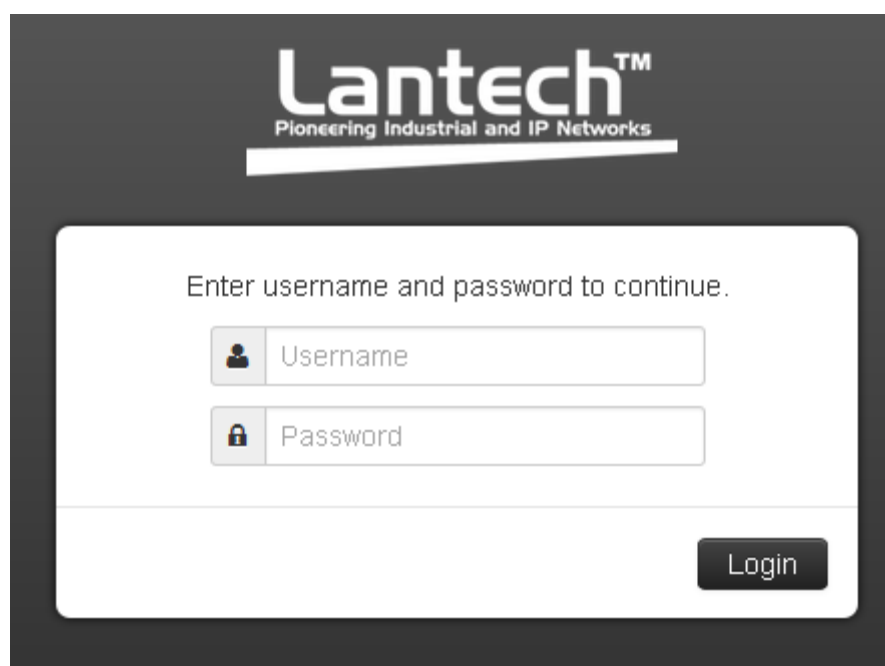
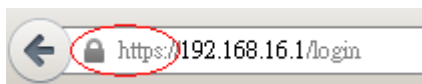
- IP Address: **192.168.16.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.16.254**
- User Name: **admin**
- Password: **admin**

6.3 System Login

1. Launch the Internet Explorer on the PC(the switch also support Mozilla and Chrome browser).
2. Key in “http://” + “the IP address of the switch”, and then Press “**Enter**”.



3. The login screen will appear right after
4. Key in the user name and password. The default user name and password are the same as ‘**admin**’.
5. Press **Enter** or click the **OK** button, and then the home screen of the Web-based management appears.
6. The switch also support SSL security login, if you need SSL to protect your access account of switch, please key in “https//” + “ the IP address of switch “, and press “Enter”

A screenshot of the Lantech login screen. The background is dark gray. At the top, the Lantech logo is displayed in white, with the tagline 'Pioneering Industrial and IP Networks' below it. In the center, there is a white rounded rectangle containing the text 'Enter username and password to continue.' Below this text are two input fields: 'Username' and 'Password'. The 'Username' field has a user icon on the left, and the 'Password' field has a lock icon on the left. At the bottom right of the white rectangle is a dark gray button with the text 'Login' in white.

6.4 System

6.4.1 System Identification Configuration

Name:

An administratively assigned name for this managed switch. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first or last character must not be a minus sign. The allowed string length is 0 to 255.

Description:

Display the description of switch. The allowed string length is 0 to 255.

Location:

The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Contact:

The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

.

System Identification Configuration

Name:	<input type="text" value="The Switch"/>
Description:	<input type="text" value="Current used"/>
Location:	<input type="text" value="Taiwan Taipei"/>
Contact:	<input type="text" value="Engineer"/>

Apply

6.4.2 Switch Information

User can find the system name, description, location and contact personnel to identify the switch. The version table below is a read-only field to show the basic information of the switch.

System Information

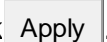
Identification	
Name	The Switch
Description	Current used
Location	Taiwan Taipei
Contact	Engineer

Information	
Device Time	2013年11月5日 下午 04:38:22
Up Time	2263
Software Version	V3.34
Kernel Version	57292a0b
MAC Address	28:60:46:a0:04:f5
Hardware Model	IES-5408DFT
Hardware Description	2 10/100/1000T +2 100/1000 SFP + 8 10/100TX L2+ Industrial Managed Switch

6.4.3 IP configuration

The switch is a network device which needs to be assigned an IP address for being

identified on the network. Users can select a method of assigning IP address to the switch.

- **DHCP Client:** Enable or disable the DHCP client function. When DHCP client function is enabled, the switch will obtain an IP address from the network DHCP server automatically. The default IP address will be replaced by the assigned IP address from the DHCP server. After the user clicks **Apply**, a popup dialog shows up to inform the user that when the DHCP client is enabled, the current IP will lose and user should find the new IP obtained from the DHCP server.
- **IP Address:** Assign a static IP address to the switch from the subnet address range that the network is using. If DHCP client function is enabled, this switch is configured as a DHCP client. The network DHCP server will assign the IP address to the switch and the switch displays it in this column. The default IP is 192.168.1.88 or the user can choose an IP address manually when DHCP Client is disabled.
- **Subnet Mask:** Assign the subnet mask of the IP address. If DHCP client function is disabled, the user has to assign the subnet mask in this column field.
- **Gateway:** Assign the network gateway for the switch. If DHCP client function is disabled, the user has to assign the gateway in this column field. The default gateway is 192.168.1.254.
- **DNS Server IP:** Assign the primary DNS IP address.
- And then, click .

DHCP client: ☐

IP Address:

IPv6 Address:

Network Mask:

Default Gateway:

DNS Server IP:


6.4.4 DHCP server

DHCP is the abbreviation of Dynamic Host Configuration Protocol that is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

The system provides the DHCP server function. Having enabled the DHCP server function, the switch system will be configured as a DHCP server.

- **DHCP Server:** Enable or Disable the DHCP Server function. Enable—the switch will be the DHCP server on your local network.
- **IP Range(up):** Type in an IP address. Low IP address is the beginning of the dynamic IP range. For example, dynamic IP is in the range between 192.168.1.100 ~ 192.168.1.200. In contrast, 192.168.1.100 is the Low IP

address.

- **IP Range(down):** Type in an IP address. High IP address is the end of the dynamic IP range. For example, dynamic IP is in the range between 192.168.1.100 ~ 192.168.1.200. In contrast, 192.168.1.200 is the High IP address.
- **Subnet Mask:** Type in the subnet mask of the IP configuration.
- **Gateway:** Type in the IP address of the gateway in your network.
- **DNS:** Type in the Domain Name Server IP Address in your network.
- **Lease Time:** It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server doesn't know that the dynamic IP is idle.
- And then, click .

Enable DHCP Server ☒

IP Range	<input type="text" value="192.168.16.100"/> <input type="text" value="192.168.16.200"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.16.254"/>
DNS	<input type="text" value="8.8.8.8"/>
Lease Time	<input type="text" value="86400"/>

6.4.5 System Time

SNTP (Simple Network Time Protocol) is a simplified version of NTP which is an Internet protocol used to synchronize the clocks of computers to a specified time reference. Because time usually just advances, the time on different node stations will be different. With the communicating programs running on those devices, it would cause time to jump forward and back, a non-desirable effect. Therefore, the switch provides comprehensive mechanisms to access national time and frequency dissemination services, organize the time-synchronization subnet and the local clock

in each participating subnet peer.

Daylight saving time (DST) is the convention of advancing clocks so that afternoons have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

- **Time zone:** Universal Time Coordinated. Set the switch location time zone. The following table lists the different location time zone for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am

Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

■ SNTP Client setting

▪ Time zone

This field is to select the Timezone which this switch is located

▪ Manual

Synchronize the time with the desktop which connect with switch.

▪ SNTP :

This is to enable/disable the SNTP service, enable the SNTP client is to use the service from SNTP server, the system time will follow the SNTP server, disable is to use local time without any SNTP server information, note that the network should be enabled to have system receive time information from SNTP server if it is enabled

▪ NTP Sever :

Set the SNTP server IP address. You can assign a local network time server's IP address or an internet time server's IP address.


- Click to have the configuration take effect.

Time Zone:	<input type="text" value="Select an Option"/>
Clock Source	<input type="text" value="SNTP"/>
	<input type="text" value="Manual"/>
Device Time	<input type="text" value="2013年05月31日下午 11:59:29"/>


NTP Server:	<input type="text" value="ntp.ubuntu.com"/>
-------------	---

6.4.6 SNMP Configuration

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

- **Agent Version:** Select the SNMP version (V1/V2c or V3) that you want to use. And then Click.  to switch to the selected SNMP version mode.

Here you can define the new community string set and remove the unwanted community string.

- **Community String:** Fill the name string.
- **Privilege:**Read only. Enables requests accompanied by this community string to display MIB-object information.
Read/write. Enables requests accompanied by this community string to display MIB-object information and to set MIB objects.
- Click. 

Community **Trap** V3 Users

Agent Version

String	Permission	
public	Read Only	×
private	Read/Write	×
Community String <small>Please enter a valid value.</small>	<input checked="" type="checkbox"/> Read Only	+

A trap manager is a management station that receives the SNMP trap messages generated by the switch. If no trap manager is defined, no traps will be issued. To define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version.

- **IP Address:** Enter the IP address of the trap manager.
- **Community:** Enter the community string for the trap station.
- **Version:** Select the SNMP trap version type—v1 or v2c.
- Click .
- To remove the community string, select the community string listed in the current manager's field and click .

Community **Trap** V3 Users

IP Address	Community	Version
<input type="text" value="IP address"/>	<input type="text" value="public"/>	<input type="text" value="v2c"/> v1 v2c


6.4.7 Fault Relay Configuration

The Fault Relay Alarm function provides the Power Failure and Port Link Down/Broken detection. With both power input 1 and power input 2 installed and the

check boxes of power 1/power 2 ticked, the FAULT LED indicator will then be possible to light up when any one of the power failures occurs. As for the Port Link Down/Broken detection, the FAULT LED indicator will light up when the port failure occurs; certainly the check box beside the port must be ticked first. Please refer to the segment of '**Wiring the Fault Alarm Contact**' for the failure detection.

- **Power Failure** : Tick the check box to enable the function of lighting up the **FAULT** LED on the panel when power fails.
- **Port Link Down/Broken** : Tick the check box to enable the function of lighting up **FAULT** LED on the panel when Ports' states are link down or broken.

Fault Relay Configuration

	Power Failure						
<input type="checkbox"/> Power 1 <input type="checkbox"/> Power 2							

	Port Link Down/Broken						
<input type="checkbox"/> Port 1 <input type="checkbox"/> Port 2 <input type="checkbox"/> Port 3 <input type="checkbox"/> Port 4 <input type="checkbox"/> Port 5 <input type="checkbox"/> Port 6 <input type="checkbox"/> Port 7							
<input type="checkbox"/> Port 8 <input type="checkbox"/> Port 9 <input type="checkbox"/> Port 10 <input type="checkbox"/> Port 11 <input type="checkbox"/> Port 12							

Apply

6.4.8 Digital Input/Output

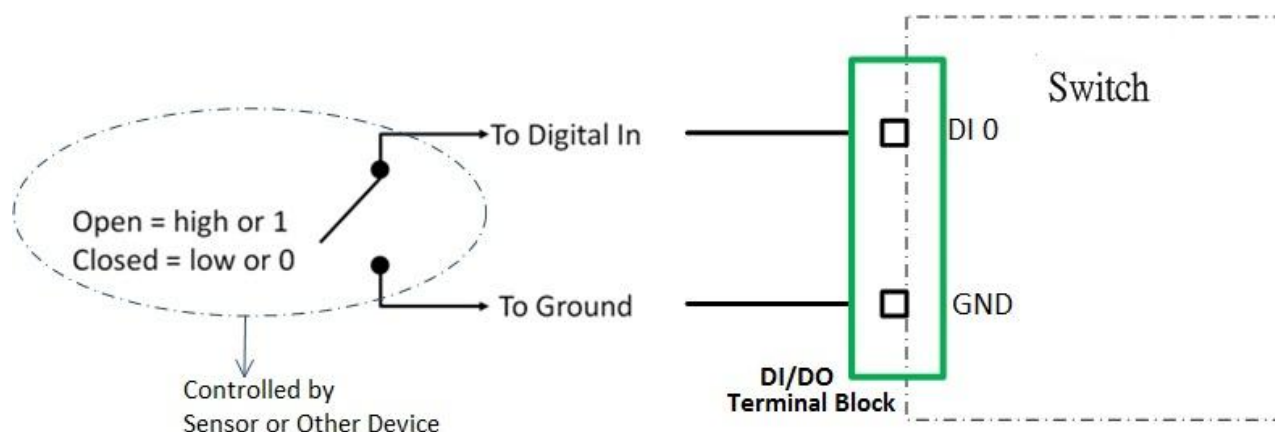
The IES-5208DF Industrial Switch contains two digital outputs and two digital inputs. Outputs are open-collector transistor switches that may be controlled by the host computer. They provide control signals, which can be applied to heaters, pumps, and other electrical equipment. The digital inputs may be read by the host computer and used to sense the state of a remote digital signal.

Digital Input

DIN 1	<input checked="" type="checkbox"/>	Both	
DIN 2	<input type="checkbox"/>	Both	
		High -> Low	
		Low -> High	

Digital Input Setting

- When **DI0/DI1** function is enabled; first Digital Input (DI0) and second Digital Input (DI1) will then be available respectively.
- **Digital Input:** Choose the transition type to trigger DI0/DI1.
 - **Low→High:** Having focused this radio button, DI0/DI1 will only report the status when the external device's voltage changes from low to high.
 - **High→Low:** Having focused this radio button, DI0/DI1 will only report the status when the external device's voltage changes from high to low.
 - **Both:** Having focused this radio button, DI0/DI1 will report both the status when the external device's voltage changes from high to low or low to high.
- **Event description:** Please fill in the description for the event.



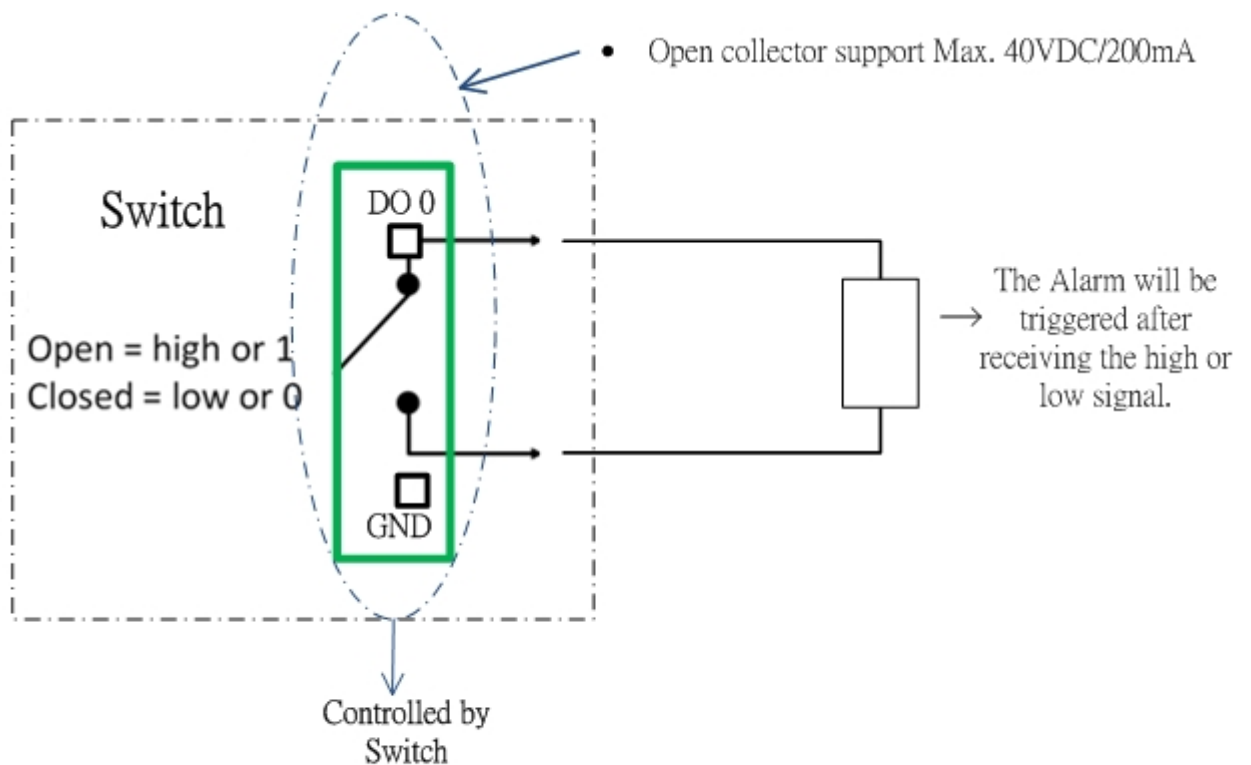
- High Status : keep in open Status or 10~30V DC(with External power)
- Low Status : Keep in close Status or -30~2V DC(with External power)

Digital Output

DOOUT 1 ☒ Low -> High
DOOUT 2 ☐ High -> Low
Low -> High

Digital Output Setting

- When **DO0/DO1** function is enabled; first Digital Output (DO0) and second Digital Output (DO1) will then be available respectively.
- **Condition:** Tick the check boxes to decide whether or not to send the events via digital output with the event about port fail or power fail or both.
- **Action:** Choose the transition type of DO0/DO1.
 - **Low→High:** When switch receive the event about port fail or power fail, DO0/DO1 will switch the output voltage from low to high.
 - **High→Low:** When switch receive the event about port fail or power fail, DO0/DO1 will switch the output voltage from high to low.



- Digital Output only support open collector design, if you want to connect DO with Alarm device, please use external power supply.

Digital Input/Output

Digital Input

DIN 1 ☐

Digital Output

DOUT 1 ☐

6.5 Event & Log


Logs

☒ Login ☒ Boot ☒ DDM ☒ DIN ☒ Link Change ☒ Power

Clear

🔗 22nd, 9:56:02 am	Link Change	Phyport(7).linkChg: down
🔗 22nd, 9:47:33 am	Link Change	Phyport(7).linkChg: up
🔗 22nd, 9:47:33 am	Link Change	Phyport(2).linkChg: up
🔗 22nd, 9:47:31 am	Boot	System Bootup
🔗 22nd, 9:47:08 am	Link Change	Phyport(2).linkChg: up
🔗 22nd, 9:46:59 am	Link Change	Phyport(2).linkChg: down
🔗 22nd, 9:46:43 am	Link Change	Phyport(2).linkChg: up
🔗 22nd, 9:46:41 am	Boot	System Bootup
🔗 22nd, 9:45:21 am	Link Change	Phyport(2).linkChg: up

6.5.1 View Logs

- This will show you the log in local interface, you can press  or F5 to refresh the web page and get the newest event log.

6.5.2 Events

Env Monitor Best

DDM Best

Environment Monitoring Event

Enable EnvMon Events: ☒

Voltage

0.00 V 20.00 V 50.00 V 100.0

Range: 30.00 V

Current

0.033 A 1.500 A

Range: 1.467 A

Power

1.0 W 29.8 W 50.0

Range: 28.8 W

Temperature

-50.0 °C -20.0 °C 69.0 °C 100.0 °C

Range: 89.0 °C

Apply

6.5.2.1 Environmental Monitoring Event

You can set the trigger range of each event in here, for example, when you set the blue bar in the range from 20V to 50V, if the voltage of power input was over 50VDC or lower than the 20VDC, it will trigger the event system.

6.5.3 Actions

Actions

Local Log Action

Remote SysLog Action

Email Action

SMS Action

SNMP Trap Action

DOut Action

☐ Save to Local

Apply

6.5.3.1 Local Log Action

Save to Local: Save log to local file

Local Log Action Remote Syslog Action

☐ Save to Local

6.5.3.2 Remote Syslog Action

Log to Remote Syslog Server: Save log to Syslog Server

Local Log Action Remote SysLog Action Email Action

☒ Log to Remote Syslog Server

Syslog Server: 0.0.0.0

Tag: node-event

Facility: user

Host Name: host

6.5.3.3 Email Action


Email Alert: Sent log via Email

Local Log Action Remote SysLog Action **Email Action** SMS Action SNMP Trap Action

☒ **Email Alert**

Subject:

Cloud SMTP: ☒

Receivers: 

Please enter at least one receiver

6.5.3.4 SMS Action

SMS Alert: Sent log via SMS service.

(The user must let the switch connect with internet and define the SMS server then the user can use this function)

(Currently the SMS service was offered by Lantech in Taiwan.)

Local Log Action Remote SysLog Action Email Action **SMS Action** SNMP Trap Action


☒ **SMS Alert**

The SMS alert service may charge usage fee in the future.

User ID:

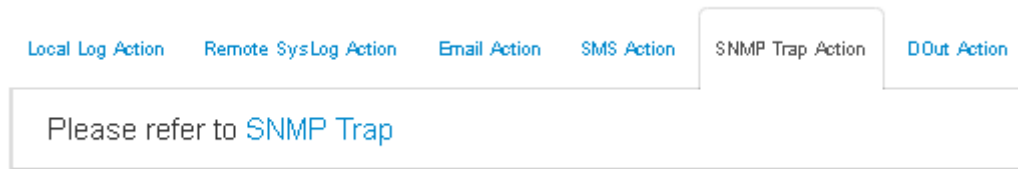
Password:

Sender Text:

Phone Numbers: 

6.5.3.5 SNMP Trap Action

SNMP Trap Action: The setting page of this function will be redirect to SNMP TRAP.

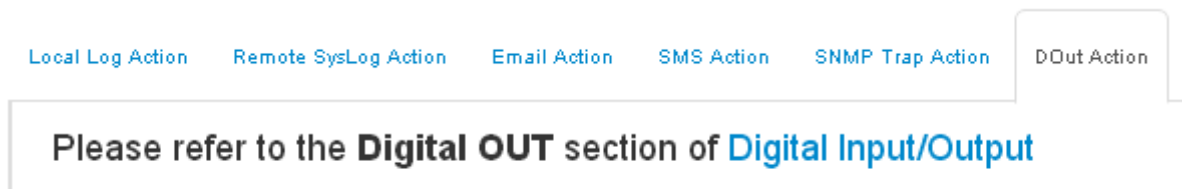


Local Log Action Remote SysLog Action Email Action SMS Action **SNMP Trap Action** DOut Action

Please refer to [SNMP Trap](#)

6.5.3.6 DOut Action

DOUT Action: The setting page of this function will be redirect to Digital Input/Output.

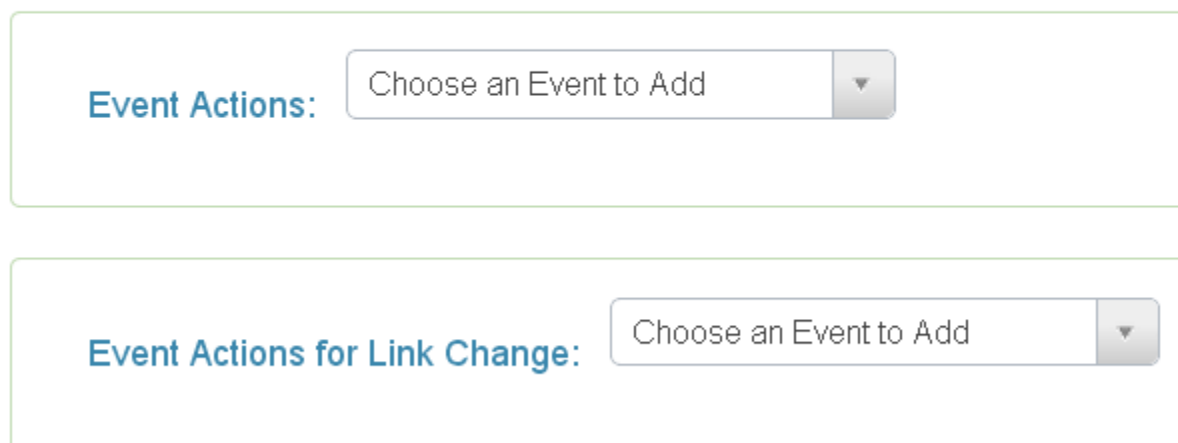


Local Log Action Remote SysLog Action Email Action SMS Action SNMP Trap Action **DOut Action**

Please refer to the **Digital OUT** section of [Digital Input/Output](#)

6.5.4 Event Action Map

Event Action Map

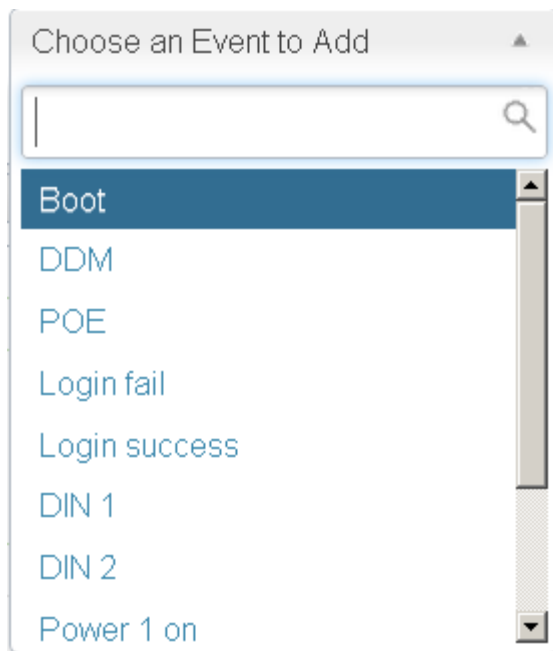


Event Actions: Choose an Event to Add ▼

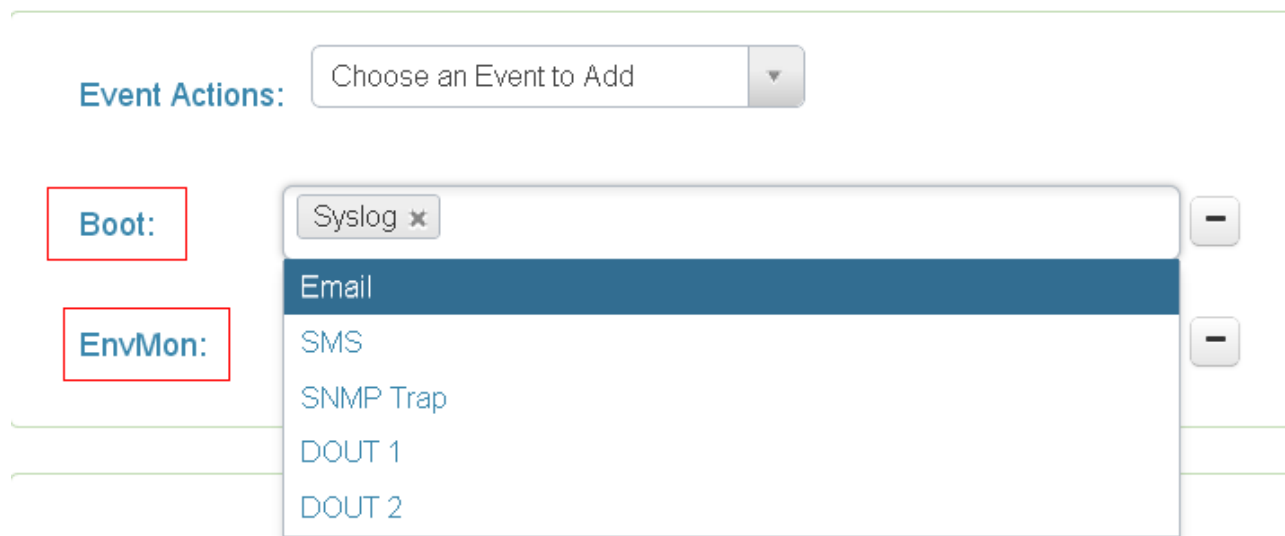
Event Actions for Link Change: Choose an Event to Add ▼

6.5.4.1 Event Actions:

- Choose the event which you want to active



B. You will find the event which you select will be display as below, then choose forwarding method to define how to forward this event to manager side.



C. You can set the forwarding method of port break event in here.

Event Actions for Link Change:

Apply

Choose an Event to Add



Port 1 up
Port 1 down
Port 2 up
Port 2 down
Port 3 up
Port 3 down
Port 4 up
Port 4 down



6.6 Ports

Device Settings

Port No.	Type	Description	Enabled	Flow Control	Speed
1	100TX	<input type="text" value="Port 1"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto <input type="button" value="v"/>
2	100TX	<input type="text" value="Port 2"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Auto <input type="button" value="v"/>

6.6.1 Device Settings

In Port control you can configure the settings of each port to control the connection parameters, and the status of each port is listed beneath.

- **Port No.:** The port number which you want to be configured.
- **Type:** Current port state.
- **Description:** Port description.
- **Enables:** enable/disable the switch port.
- **Flow Control:** Whether or not the receiving node sends feedback to the sending node is determined by this item. When enabled, once the device exceeds the input data rate of another device, the receiving device will send a PAUSE frame which halts the transmission of the sender for a specified period of time. When disabled, the receiving device will drop the packet if too much to process.
- **Speed:** It can be set as auto or set speed and negotiated way manually.
- Click to have the configuration take effect.

Port Status

Port No.	Type	Link	State	Speed	Flow Control
1	100TX	up	Enable	100 Full	Disable
2	100TX	down	Enable	N/A	N/A

6.6.2 Status

It will show you the status of port configuration setting.

Port Statistic

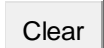
Port	Type	Link	State	TX Good	TX Bad	RX Good	RX Bad	TX Abort	Collision	Drop	RX BCAST	RX MCAST	TX MCAST
1	DSFP	Down	Enable	0	0	0	0	0	0	0	0	0	0
2	DSFP	Down	Enable	0	0	0	0	0	0	0	0	0	0
3	DSFP	Down	Enable	0	0	0	0	0	0	0	0	0	0
4	DSFP	Down	Enable	0	0	0	0	0	0	0	0	0	0

6.6.3 Statistics

The following chart provides the current statistic information which displays the real-time packet transfer status for each port. The user might use the information to plan and implement the network, or check and find the problem when the collision or heavy traffic occurs.

- **Port:** The port number.
- **Type:** Displays the current speed of connection to the port.
- **Link:** The status of linking—‘Up’ or ‘Down’.
- **State:** It’s set by Port Control. When the state is disabled, the port will not transmit or receive any packet.
- **Tx Good Packet:** The counts of transmitting good packets via this port.
- **Tx Bad Packet:** The counts of transmitting bad packets (including undersize [less than 64 octets], oversize, CRC Align errors, fragments and jabbers packets) via this port.
- **Rx Good Packet:** The counts of receiving good packets via this port.
- **Rx Bad Packet:** The counts of receiving good packets (including undersize [less

than 64 octets], oversize, CRC error, fragments and jabbers) via this port.

- **Tx Abort Packet:** The aborted packet while transmitting.
- **Packet Collision:** The counts of collision packet.
- **Packet Dropped:** The counts of dropped packet.
- **Rx Bcast Packet:** The counts of broadcast packet received.
- **Rx Mcast Packet:** The counts of multicast packet received.
- **Tx Mcast Packet:** The counts of multicast packet transmitted
- Click  button to clean all counts.

Port Mirroring

Direction	Destination	Mirror From
RX	<input type="text" value="Port 1"/>	<input type="text" value="Choose ports"/>
TX	<input type="text" value="Port 1"/>	<input type="text" value="Choose ports"/>



6.6.4 Mirroring

The Port mirroring is a method for monitor traffic in switched networks. Traffic through ports can be monitored by one specific port, which means traffic goes in or out monitored (source) ports will be duplicated into mirror (destination) port.

- **Destination :** You can set which switch port will be responsible for collecting the data which was duplicated from the source port.
- **Mirrpr From:** You can set which switch port will be duplicated then send to the destination port.

Note1 : All the duplicated data of the source port can be separated with RX and TX, if you want to collect multi-source ports at the same time, you can assign the Tx of one destination port to be responsible for collecting all the Tx data of source ports and assign another RX of destination port to be responsible for collecting all the Rx data of source ports.

- And then, click  button.

Rate Limiting

Port	Ingress	Egress
1	<div>Unicast Multicast Broadcast</div> <div>0 kbps 0%</div>	<div>0 kbps 0%</div>
2	<div>Unicast Multicast Broadcast</div> <div>0 kbps</div>	<div>0 kbps</div>

6.6.5 Rate Limiting

You can set up every port's bandwidth rate and frame limitation type.

All the ports support port egress rate control. For example, assume port 1 is 10Mbps, users can set its effective egress rate is 1Mbps, ingress rate is 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate

- Click Apply to apply the settings

6.6.6 Loop Protection

Loop Protection

Config

Status

Enable Loop Protection

☒

Interval

1

Shutdown

60

Apply

The loop Protection is used to detect the presence of traffic. When switch receives packet's (looping detection frame) MAC address the same as oneself from port, show Loop Protection happens. The port will be locked when it received the looping Protection frames.

■ Enable Loop Protection:

Control whether loop protections is enabled (as a whole). .

■ Interval:

The interval between each loop protection PDU sent on each port. valid values are 1 to 10 seconds.

■ Shutdown :

The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).

6.7 Power over Ethernet

The IES-5208DF switch doesn't support PoE function

Power over Ethernet Configuration

This device doesn't support POE.

6.8 Topology

This function can help user to build the network topology drawing automatically for the switches that are in closed looped and show the detail information of each switch node by clicking the icon. The topology view drawing can show the backup path with the dot line for overall picture, please remember to enable **LLDP** function before you use this function.

Topology Status

Warning!

Please [Enable LLDP](#) to see topology status

Topology Status

Text View

Graphic View

Demo

Nodes

MAC Address	IP
-------------	----

Links

From	To	Stat
------	----	------

Rings

|--|

Topology Status

■ Text View:

Display each switch in your network by text.

The Topology was build with the information from LLDP where can let you see the information from other switches.

■ Nodes:

show the information of each switch like MAC address and IP address.

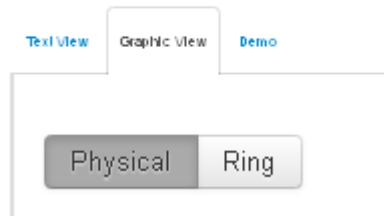
■ Links:

show the information of each connection .

■ Rings:

show the information from ITU-Ring function

Topology Status



■ Graphic View:

Display each switch connection in the network by graphic.

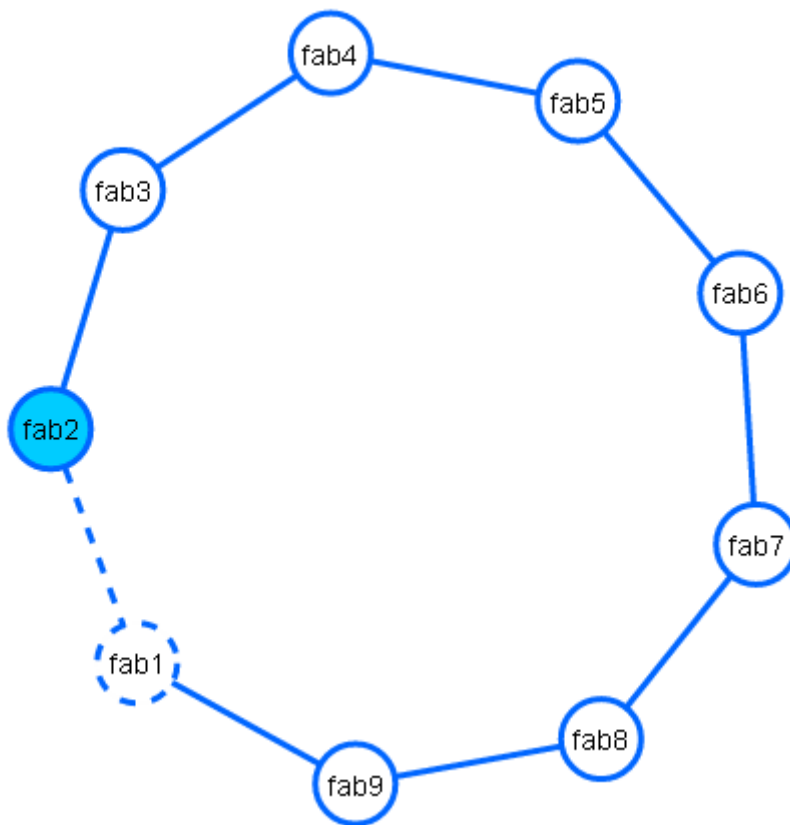
You can see the topology diagram which is assorted by the LLDP information.

■ Physical :

display the physical connection of network .

■ Ring :

Beside the physical connection, also show the information about ITU-Ring




■ **Demo:**


Demo display each topology in different connection.


6.9 QoS









QoS Configuration

 **QoS Policy:**

Use weighted fair queuing scheme ☒

Priority Type Disabled 

 **Weighted Fair Queue Ratio**

Traffic 0	Traffic 1	Traffic 2	Traffic 3	Traffic 4	Traffic 5	Traffic 6	Traffic 7
1 	1 	1 	1 	1 	1 	1 	1 

Apply

Quality of Service (QoS) is the ability to provide different priority to different applications, users or data flows, or to guarantee a certain level of performance to a data flow. QoS guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP or Video Teleconferencing, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication. In the absence of network congestion, QoS mechanisms are not required.

6.9.1 QoS Policy

■ Using the weight fair queue scheme

The switch will follow 8:4:2:1 rate to process priority queue from High to lowest queue. For example, while the system processing, 1 frame of the lowest queue, 2 frames of the low queue, 4 frames of the middle queue, and 8 frames of the high queue will be processed at the same time in accordance with the 8,4,2,1 policy rule.

■ Priority Type

There are 5 priority type selections available—**Port-based**, **TOS only**, **COS only**, **TOS first**, and **COS first**. Disable means no priority type is selected.

- **Port Base Priority**

Configure the priority level for each port. With the drop-down selection item of **Priority Type** above being selected as Port-based, this control item will then be available to set the queuing policy for each port.

- **Cos**

Set up the COS priority level. With the drop-down selection item of **Priority Type** above being selected as COS only/COS first, this control item will then be available to set the queuing policy for each port.

- **Tos**

ToS priority: the system provides 0~63 ToS priority level. Each level has 8 type of priority - 0~7. The default value is "1" priority for each level. When the IP packet is received, the system will check the ToS level value in the IP packet has received. For example: user set the ToS level 25 is 7. The port 1 is following the ToS priority policy only. When the packet received by port 1, the system will check the ToS value of the received IP packet. If the ToS value of received IP packet is 25(priority = 7), and then the packet priority will have highest priority.

Click  to have the configuration take effect.

6.10 Security

MAC Address Tables

Static MAC Addresses

MAC Filtering

All MAC Addresses

0 static MAC address entries

MAC Address	VLAN ID	Port No	
<div>MAC address</div> <div>Please enter a valid MAC address.</div>	1	Port 1	+

Apply

6.10.1 MAC Address Tables

Use the MAC address table to ensure the port security.

■ Static MAC Address

You can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add / modify / delete a static MAC address. MAC Address: Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity. VLAN ID : Entering the VLAN ID. Port No : pull down the selection menu to select the port number.

■ MAC Filtering

By filtering MAC address, the switch can easily filter pre-configure MAC address and reduce the un-safety. You can add and delete filtering MAC address. MAC Address: Enter the MAC address that you want to filter.

■ All MAC Addresses

you can view the port that connected device's MAC address and related device's MAC address.

6.10.2 Access Control List

The switch access control list (ACL) is probably the most commonly used object in the OSI layer 2 and 3. It is used for access filtering. The ACLs are divided into MAC and IP filtering.

6.10.2.1 ACL with Layer2 (MAC)

■ No:

The number of ACL record.

■ Port:

assign the port which you want to enable the ACL function.

■ Direction:

Let the switch check the destination address or source address of packet.

Address: assign the MAC address which you want to deny.

Mask: set the mask to filter the MAC range.

No	Port	Direction	Address	Mask	Action
1	Port 1	Source	00:00:00:00:00:00	ff:ff:ff:fe:00:00	Deny

6.10.2.2 ACL with Layer3 (IP)

■ No:

The number of ACL record.

■ Port:

assign the port which you want to enable the ACL function.

■ Direction:

let the switch check the destination address or source address of packet.

■ Address:

assign the IP address which you want to deny.

■ Mask:

set the mask to filter the IP range.

No	Port	Direction	Address	Mask	Action
1	Port 1	Source	192.168.16.1	255.255.255.0	Deny

6.10.3 IEEE 802.1X Radius Server

802.1X is an IEEE authentication specification which prevents the client from accessing a wireless access point or wired switch until it provides authority, like the user name and password that are verified by an authentication server (such as RADIUS server).

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

- **Server IP**

Assign the RADIUS Server IP address.

- **Server Port**

Set the UDP destination port for authentication requests to the specified RADIUS Server.

- **Shared Key**

Set an encryption key for using during authentication sessions with the specified RADIUS server. This key must match the encryption key used on the RADIUS Server.

- **NAS Identifier**

Set the identifier for the RADIUS client.

- **Enable on Ports**

Enable or disable 802.1x protocol.

IP Security

☐ Enable IP Security

Apply

6.10.4 IP Security

IP security function allows user to assign 20 specific IP addresses that have permission to access the switch through the web browser for the securing switch management.

■ Enable IP Security

When this option is in Enable mode, the Enable Web Server and Enable Telnet Server and Enable SSH Server check boxes will then be available.

■ Enable Web Server

When this check box is checked, the IP addresses among IP permit list will be allowed to access via web service.

■ Enable Telnet Server

When this check box is checked, the IP addresses among IP permit list will be allowed to access via telnet service.

■ Enable SSH Server

When this check box is checked, the IP addresses among IP permit list will be allowed to access via ssh service.

■ IP permit list

Assign up to 20 specific IP address. Only these 10 IP address can access and manage the switch through the Web browser

802.1Q VLAN Config

Help Log Messages admin

Management VLAN ID 0

Port No.	Link Type	PVID	Tagged VLANs
1	Access	1	
2	Access	1	
3	Access	1	
4	Access	1	
5	Access	1	

6.11 VLAN

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allow you to isolate network traffic, so only the members of the same VLAN will receive traffic from the ones of the same VLAN. Basically, creating a VLAN on a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

6.11.1 802.1Q VLAN Config

802.1Q VLAN Config

Management VLAN ID 0

Port No.	Link Type	PVID	Tagged VLANs
1	Access	1	
2	Access	1	
3	Access	1	
4	Access	1	
5	Access	1	
6	Access	1	
7	Access	1	
8	Access	1	

■ **Management VLAN ID:**

This will set which VLAN group can access the switch, the default “0” means all VLAN group, this limitation will not support port based VLAN.

■ **Link Type:**

There are 3 types of link type.

1. Access Link: A segment which provides the link path for one or more stations to the VLAN-aware device. An Access Port (untagged port), connected to the access link, has an untagged VID (also called PVID). After an untagged frame gets into the access port, the switch will insert a four-byte tag in the frame. The contents of the last 12-bit of the tag is untagged VID. When this frame is sent out through any of the access port of the same PVID, the switch will remove the tag from the frame to recover it to what it was. Those ports of the same untagged VID are regarded as the same VLAN group members.

Note: Because the access port doesn't have an understanding of tagged frame, the column field of Tagged VID is not available.

2. Trunk Link: A segment which provides the link path for one or more VLAN-aware devices (switches). A Trunk Port, connected to the trunk link, has an understanding of tagged frame, which is used for the communication among VLANs across switches. Which frames of the specified VIDs will be forwarded depends on the values filled in the Tagged VID column field. Please insert a comma between two VIDs.

Note:

A trunk port doesn't insert tag into an untagged frame, and therefore the untagged VID column field is not available.

It's not necessary to type '1' in the tagged VID. The trunk port will forward the frames of VLAN 1.

The trunk port has to be connected to a trunk/hybrid port of the other switch. Both the tagged VID of the two ports have to be the same.

3. Hybrid Link: A segment which consists of Access and Trunk links. The hybrid port has both the features of access and trunk ports. A hybrid port has a PVID belonging to a particular VLAN, and it also forwards the specified tagged-frames

for the purpose of VLAN communication across switches.

■ PVID

This column field is available when Link Type is set as Access Link and Hybrid Link. Assign a number in the range between 1 and 4094.

■ Tagged VID:

This column field is available when Link Type is set as Trunk Link and Hybrid Link. Assign a number in the range between 1 and 4094.

802.1Q VLAN Status

VLAN ID	Port Members
1	Port 1 U Port 2 U Port 3 U Port 4 U Port 5 U Port 6 U Port 7 U Port 8 U Port 9 U Port 10 U Port 11 T Port 12 T
2	Port 1 U Port 2 U Port 11 T Port 12 T
3	Port 1 U Port 11 T Port 12 T

6.11.2 Status

You can see the status of each VLAN group in here.

Multicast VLAN Registration

New MVR			
VLAN ID	Multicast Address	Port Members	Delete MVR
Apply			

6.12 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP join message to Switch A in order to join the appropriate multicast. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

■ VLAN ID

Specify the Multicast VLAN ID.

■ Multicast Addresses

Multicast Addresses of the group displayed.

■ Port Members

Ports under this group.

Multicast VLAN Registration

VLAN ID	Multicast Address	Port Members
		<div>Port 1 x</div>

Apply

LLDP Configuration

Enabled ☒

TX Interval(secs)

10

Port NO	Port ID	Mode
1	1	Both
2	2	Both

6.12 LLDP

Link Layer Discovery Protocol (LLDP) is defined in the IEEE802.1AB, it is an emerging standard which provides a solution for the configuration issues caused by expanding LANs. LLDP specifically defines a standard method for Ethernet network devices such as switches, routers and wireless LAN access points to advertise information about themselves to other nodes on the network and store the information they discover. LLDP runs on all 802 media. The protocol runs over the data-link layer only, allowing two systems running different network layer protocols to learn about each other.

6.12.1 LLDP Configuration

■ Enabled

Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbours.

■ Tx Interval

The switch periodically transmits LLDP frames to its neighbours for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds.

The LLDP port settings relate to the currently selected stack unit, as reflected by the page header.

■ Port No

The switch port number of the logical LLDP port.

■ Port Id

Enter characters to be id name for the logical LLDP port.

■ Mode

Select LLDP mode.

Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.

Tx only The switch will drop LLDP information received from neighbors, but will send out **LLDP information**.

Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors.

Both The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

LLDP Neighbor Information

Identification						
Local Port	Chassis ID	Port ID	Port Description	System Name	System Capability	Management Address

6.12.2 LLDP Neighbor

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The columns hold the following information:

■ Local Port

The port on which the LLDP frame was received.

■ Chassis ID

The **Chassis ID** is the identification of the neighbor's LLDP frames.

■ Remote Port ID

The **Remote Port ID** is the identification of the neighbor port.

■ Port Description

Port Description is the port description advertised by the neighbor unit.

■ System Name

System Name is the name advertised by the neighbour unit.

■ **System Capabilities**

System Capabilities describes the neighbour unit's capabilities. The possible capabilities are:

1. Other
2. Repeater
3. Bridge
4. WLAN Access Point
5. Router
6. Telephone
7. DOCSIS cable device
8. Station only
9. Reserved

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

■ **Management Address**

Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.

LLDP Neighbor Information

Total									
Neighbors Aged Out	Neighbors Add	Neighbors Delete	Frames Discarded	Frames Received In Error	Frames In	Frames Out	TLVs Discarded	TLVs Unrecognizeds	
0	0	0	0	0	0	0	0	0	

Ports									
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0

6.12.3 LLDP Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. **Total** are counters that refer to the whole stack, switch, while **Port** refer to per port counters for the currently selected switch.

6.12.3.1 Total

■ Neighbours Aged Out

Shows the number of entries deleted due to Time-To-Live expiring.

■ Neighbours Added

Shows the number of new entries added since switch reboot.

■ Neighbours Deleted

Shows the number of new entries deleted since switch reboot.

■ Frames Discarded

If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.

■ **Frames Received In Error**

The number of received LLDP frames containing some kind of error.

■ **Frames In**

The number of LLDP frames received on the port.

■ **Frames Out**

The number of LLDP frames transmitted on the port.

■ **TLVs Discarded**

Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

■ **TLVs Unrecognized**

The number of well-formed TLVs, but with an unknown type value.

■ **Ports**

The displayed table contains a row for each port. The columns hold the following information:

■ **Port**

The port on which LLDP frames are received or transmitted.

■ **Neighbors Aged Out**

Shows the number of entries deleted due to Time-To-Live expiring.

■ **Neighbors Added**

Shows the number of new entries added since switch reboot.

■ **Neighbors Deleted**

Shows the number of new entries deleted since switch reboot.

■ **Frames Discarded**

If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.

■ **Frames Received In Error**

The number of received LLDP frames containing some kind of error.

■ **Frames In**

The number of LLDP frames received on the port.

■ **Frames Out**

The number of LLDP frames transmitted on the port.

■ **TLVs Discarded**

Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

■ **TLVs Unrecognized**

The number of well-formed TLVs, but with an unknown type value.

6.13 CDP

The **Cisco Discovery Protocol (CDP)** is a proprietary data link layer protocol developed by Cisco. It is used to share information about other directly connected Cisco equipment, such as the OS version and IP address

CDP Configuration Device Settings

CDP Enable: ☒

CDP timer(secs)

CDP holdtime(secs)

Port	Enabled
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>
7	<input checked="" type="checkbox"/>

6.13.1 CDP Configuration Device Settings

■ CDP Enabled

Enabled the switch will send out CDP information, and will analyze CDP information received from neighbors.

■ Tx Interval(secs)

The switch periodically transmits CDP frames to its neighbours for having the network discovery information up-to-date. The interval between each CDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds.

■ Tx Holdtime(secs)

Each CDP frame contains information about how long the information in the CDP frame shall be considered valid. The holdtime between each CDP frame is determined by the **Tx Holdtime** value. Valid values are restricted to 5 - 32768 seconds.

6.13.2 CDP Port Configuration

■ Port

The switch port number of the logical CDP port.

■ Enabled

The switch will send out CDP information, and will analyze CDP information received from neighbors.

CDP Status

Statistics	
Total Packets Output	Total Packets Input
0	0

Clear

Neighbors						
Local Port NO	CDP Version	Ageout TTL	Device ID	Platform	Software Version	Addresses

6.13.3. CDP Status

■ Statistics

Total Packets Output

The number of CDP frames transmitted on the switch.

Total Packets Input

The number of CDP frames received on the switch.

■ Neighbors

The displayed table contains a row for each port on which an CDP neighbour is detected. The columns hold the following information:

Local Port

The port on which the CDP frame was received.

Version

Version is the CDP version advertised by the neighbor unit.

Ageout TTL

Ageout TTL is the ageout Time-To-Live advertised by the neighbor unit.

Device ID

The Device ID is the identification of the neighbor's CDP frames.

Platform

Platform is the description advertised by the neighbor unit.

Software Version

Software Version is the software version advertised by the neighbor unit.

Addresses

Addresses is the neighbour unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.

6.14 IGMP Snooping

The switch support IP multicast, you can enable IGMP protocol on web management's switch setting configuration page, then the IGMP snooping information displays. IP multicast addresses range are from 224.0.0.0 through 239.255.255.255.

IGMP Snooping Configuration

Global Configuration

- ☐ Enable Querier
- ☒ Enable Snooping
- ☒ Flood Well-known Multicast Traffic

VLAN Configuration

ID	Enable Querier	Enable Snooping
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Port Related Configuration

Port	Router Port	Fast Leave
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>

6.14.1 IGMP Snooping Configuration

Global Configuration

- ☐ Enable Querier
- ☒ Enable Snooping
- ☒ Flood Well-known Multicast Traffic

Port Related Configuration

Port	Router Port	Fast Leave
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>

6.14.1.1 Global Configuration

- **Enable Query:** enable or disable the IGMP query function. The IGMP query information will be displayed in IGMP status section.
- **Enable Snooping:** enable or disable the IGMP protocol.
- **Flood Well-known Multicast traffic:** let the switch know how to process the Multicast data stream which was unregistered with IGMP Query.
-

6.14.1.2 Port Related Configuration

■ Port

The switch port number of the logical port.

■ Router Port

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

■ Fast Leave

Enable the fast leave on the port.

IGMP Snooping Status

Statistics

VLAN ID	Status Querier	Querier Transmitted	Querier Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leave Received
0	true	0	0	0	0	0	0

Clear

IGMP Groups

false

Clear

6.14.2 IGMP Snooping Status

6.14.2.1 Statistics

■ VLAN ID

The VLAN ID of the entry.

■ Status Querior

Shows the Querior status is "ACTIVE" or "IDLE".

"DISABLE" denotes the specific interface is administratively disabled.

■ Queries Transmitted

The number of Transmitted Queries.

■ Queries Received

The number of Received Queries.

■ V1 Reports Received

The number of Received V1 Reports.

■ V2 Reports Received

The number of Received V2 Reports.

■ **V3 Reports Received**

The number of Received V3 Reports.

■ **V2 Leaves Received**

The number of Received V2 Leaves.

■ **IGMP Groups**

Entries in the IGMP Group Table are shown on this page.

■ **VLAN ID**

VLAN ID of the group.

■ **Multicast Addresses**

Group address of the group displayed.

■ **Port Members**

Ports under this group.

■ **Membership Interval**

The group hold aging out TTL

MSTP Global Configuration

Mode	<input type="text" value="MSTP"/>
Name	<input type="text" value="REGION1"/>
Revision	<input type="text" value="0"/>
Max Age	<input type="text" value="20"/>
Forward Delay	<input type="text" value="15"/>
Max Hops	<input type="text" value="20"/>

Apply

6.15 MSTP

The section describes that how to configure the Spanning Tree Bridge and STP System settings. It allows you to configure STP System settings are used by all STP Bridge instance in the Switch.

6.15.1. MSTP Global Configuration

■ Mode

Show the STP protocol version setting. Valid values are STP, RSTP and MSTP.

■ Name

The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

■ Revision

The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

■ Forward Delay

The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

■ Max Age

The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be $\leq (\text{FwdDelay}-1)*2$.

■ Maximum Hop Count

This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

6.15.2 How to enable MSTP

6.15.2.1 Enter MSTP → CIST Settings , press icon to enable MSTP

PS: (The default was disable with all ports)

The screenshot shows the network configuration interface. On the left is a sidebar menu with categories: QoS, Security, VLAN, MVR, LLDP, IGMP Snooping, CDP, MSTP, Aggregation, PTP, and G 8032 FRPS. The MSTP category is expanded, showing sub-items: Global Configuration, CIST Settings, MSTI Settings, Bridge Status, and Port Status. The main area displays the 'Port Configuration' table. Above the table, there is a 'Priority' field set to 32768 and a button labeled 'Enable STP on all ports' with a checkmark icon. The table has columns: Port NO, Enable STP, Path Cost, Priority, Edge Mode, and P2P Mode. All 10 ports are listed, with 'Enable STP' set to 'NO' for all.

Port NO	Enable STP	Path Cost	Priority	Edge Mode	P2P Mode
1	NO	0	128	Force Enabled	Force Enabled
2	NO	0	128	Force Enabled	Force Enabled
3	NO	0	128	Force Enabled	Force Enabled
4	NO	0	128	Force Enabled	Force Enabled
5	NO	0	128	Force Enabled	Force Enabled
6	NO	0	128	Force Enabled	Force Enabled
7	NO	0	128	Force Enabled	Force Enabled
8	NO	0	128	Force Enabled	Force Enabled
9	NO	0	128	Force Enabled	Force Enabled
10	NO	0	128	Force Enabled	Force Enabled

6.15.2.2 Check the status of STP, all ports should display “Yes”

- Security
- VLAN
- MVR
- LLDP
- IGMP Snooping
- CDP
- MSTP**
 - Global Configuration
 - CIST Settings
 - MSTI Settings
 - Bridge Status
 - Port Status
- Aggregation
- PTP
- G 8032 ERPS

Port Configuration

Disable STP on all ports

Port NO	Enable STP	Path Cost	Priority	Edge Mode	P2P Mode
1	YES	0	128	Force Enabled	Force Enabled
2	YES	0	128	Force Enabled	Force Enabled
3	YES	0	128	Force Enabled	Force Enabled
4	YES	0	128	Force Enabled	Force Enabled
5	YES	0	128	Force Enabled	Force Enabled
6	YES	0	128	Force Enabled	Force Enabled
7	YES	0	128	Force Enabled	Force Enabled
8	YES	0	128	Force Enabled	Force Enabled
9	YES	0	128	Force Enabled	Force Enabled
10	YES	0	128	Force Enabled	Force Enabled

6.15.2.3 Remember to press “Apply”

6.15.1.4 Save setting

CIST Settings

Bridge Configuration

VLANs Unmapped VLANs are mapped to the CIST here.

Priority

Port Configuration

Port NO	Enable STP	Path Cost	Priority	Edge Mode	P2P Mode
Port 1	YES	0	128	Force Enabled	Force Enabled
Port 2	YES	0	128	Force Enabled	Force Enabled
Port 3	YES	0	128	Force Enabled	Force Enabled
Port 4	YES	0	128	Force Enabled	Force Enabled

6.15.3 CIST Settings

■ 6.15.3.1 Bridge configuration

VLANs Mapped

The list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Bridge Priority

Control the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

■ 6.15.3.2 Port

Port No

The switch port number of the logical STP port.

Enabled STP

Control whether STP is enabled on this switch port.

Path Cost

Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority

Control the port priority. This can be used to control priority of ports having identical port cost. (See above).

edge_mode

Control whether the oper Edge flag should start as being set or cleared. (The initial oper Edge state when a port is initialized). Control whether the bridge should enable automatic edge detection on the bridge port. This allows oper Edge to be derived from whether BPDU's are received on the port or not.

p2p_mode

Description: Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

MSTP MSTI Settings

Instance NO	VLANs	Priority
<div>Add</div>		

6.15.4. MSTP MSTI Settings

■ Instance No

VLANs

The list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Priority

Control the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

MSTP Bridges Status

NO	Bridge ID	Root ID	Root Port	Root Cost	Topology State
CIST 0	32768-	32768-	0	0	

6.15.5. MSTP Bridges Status

■ Instance

The Bridge Instance. ex: CIST, MSTI1, ...

■ Bridge ID

The Bridge ID of this Bridge instance.

■ Root ID

The Bridge ID of the currently elected root bridge.

■ Root Port

The switch port currently assigned the root port role.

■ Root Cost

Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

■ Topology State

The current state of the Topology Change Flag of this Bridge instance.

■ Topology Change Last

The time since last Topology Change occurred.

Bridge status of all ports

Port 1	Port 2	Port 3
as Designated/FORWARDING in CIST	as Disabled/BLOCKING in CIST	as Disabled/BLOCKING in CIST
Port 4	Port 5	Port 6
as Disabled/BLOCKING in CIST	as Disabled/BLOCKING in CIST	as Disabled/BLOCKING in CIST
Port 7	Port 8	Port 9
as Designated/FORWARDING in CIST	as Disabled/BLOCKING in CIST	as Disabled/BLOCKING in CIST
Port 10	Port 11	Port 12
as Disabled/BLOCKING in CIST	as Disabled/BLOCKING in CIST	as Disabled/BLOCKING in CIST

6.15.6. Bridge status of all ports

■ Port

The switch port number of the logical STP port.

■ Role

The current STP port role of the port. The port role can be one of the following values:
AlternatePort BackupPort RootPort DesignatedPort Disabled.

■ State

The current STP port state of the port. The port state can be one of the following values: Discarding Learning Forwarding.

Aggregation Configuration

Group Configuration:

Trunking Group	Enable LACP Dynamic Trunking	Port Members
1	<input type="checkbox"/>	Select Some Options
2	<input type="checkbox"/>	Select Some Options
3	<input type="checkbox"/>	Select Some Options
4	<input type="checkbox"/>	Select Some Options
5	<input type="checkbox"/>	Select Some Options
6	<input type="checkbox"/>	Select Some Options

6.16 Aggregation

Port trunking is the combination of several ports or network cables to expand the connection speed beyond the limits of any one single port or network cable. Link Aggregation Control Protocol (LACP), which is a protocol running on layer 2, provides a standardized means in accordance with IEEE 802.3ad to bundle several physical ports together to form a single logical channel. All the ports within the logical channel or so-called logical aggregator work at the same connection speed and LACP operation requires full-duplex mode.

6.16.1. Aggregation Configuration

- **Trunking Group :**

There are 6 trunk groups to be selected.

- **Enable LACP Dynamic Trunking:**

Enable LACP with the dedicated trunking group.

- **Port member:** This column field allows the user to choose the total number of active port up to four. With **LACP**, e.g. you assign four ports to be the members of a trunk group whose work ports column field is set as two; the exceed ports

are standby/redundant ports and can be aggregated if working ports fail.

LACP Group Status

Trunking Group	LACP	System ID	Port Members
----------------	------	-----------	--------------

6.16.2 LACP Port Status

You can check the setting of Port aggregation in Status.

■ Trunking Group

Number of trunking group

■ LACP

'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.

■ System ID

The ID of each Trunking group

■ Port Members

Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

PTP Configuration

Enable on	<input type="text" value="select ports to enable PTP"/>
Domain:	<input type="text" value="0"/>
Priority 1:	<input type="text" value="255"/>
Priority 2:	<input type="text" value="255"/>
Announce Interval:	<input type="text" value="1"/>
Announce Interval Timeout:	<input type="text" value="2"/>
Sync Interval:	<input type="text" value="1"/>
Delay Request Interval:	<input type="text" value="1"/>

6.17 PTP IEEE 1588 v2

The **Precision Time Protocol (PTP)** is a protocol used to synchronize clocks throughout a network where achieves clock accuracy in the 1us range, making it suitable for measurement and control systems. IEEE 1588 v2 is designed for local systems requiring accuracies beyond those attainable using NTP. It is also designed for applications that cannot bear the cost of a GPS receiver at each node, or for which GPS signals are inaccessible.

- **Enable on:**

Select which port you want to enable PTP function.

- **Domain:**

Set the PTP domain

■ **Priority1:**

Specify the **priority1** value to override the default criteria (clock quality, clock class, etc.) for best master clock selection. Lower values take precedence. The range for both is from 0 to 255., The default is 255

■ **Priority2:**

Specify a **priority2** value to be used as a tie-breaker between two devices that are otherwise equally matched in the default criteria. For example, you can use priority2 value to give a specific switch priority over other identical switches. The range for both is from 0 to 255. The default is 255.

■ **Announce Interval:**

Specify the time for sending announce messages. The range is 0 to 4 seconds. The default is 1 (2 seconds).

■ **Announce Interval Timeout:**

specify the time for announcing timeout messages. The range is 2 to 10 seconds. The default is 2 (4 seconds).

■ **Sync Interval:**

enter the time for sending synchronization messages. The range is -1 second to 1 second. The default is 1 second.

■ **Delay Request Interval:**

specify the time recommended to the member devices to send delay request messages when the port is in the master state. The range is -1 second to 6 seconds. The default is 1 (2 seconds).

6.18 G.8032 ERPS

G.8032 Ethernet Ring Protection

ID	Enabled	Role	Type	Ring Port 0	Ring Port 1	Node Failure Protection	
----	---------	------	------	-------------	-------------	-------------------------	--

Apply

ERPS specifies protection switching mechanisms and a protocol for Ethernet layer network rings. Ethernet Rings can provide wide-area multipoint connectivity more economically due to their reduced number of links. The mechanisms and protocol defined in this recommendation achieve highly reliable and stable protection and never form loops, which would fatally affect network operation and service availability.

6.18.1. G.8032 Ethernet Ring Protection Configuration

ID	Enabled	Role	Type	Ring Port 0	Ring Port 1	Node Failure Protection
1	Disabled	None	Major	Port 1	Port 2	NO

The G.8032 Ethernet Ring Protection Switch instances are configured here.

■ ID

The ID of the created Protection group

■ Enabled

Enable/Disable the G.8032 ERP.

■ Role

It can be either RPL owner or RPL Neighbor.

■ Type

Type of Protection ring. It can be either major ring or sub-ring.

■ Ring Port 0

This will create a Port 0 of the switch in the ring.

■ Ring Port 1

This will create "Ring Port 1" of the switch in the Ring.

■ Node Failure Protection

This option can prevent the event that all switch in the same ITU ring reboot together then the ITU Ring will fail.

Ring Status


ID	State	Role	Ring Port 0	Ring Port 1
----	-------	------	-------------	-------------

6.18.2 How to set ERPS G.8032

- Make sure you have disabled the MSTP/RSTP protocol.
- Press “+” icon to add one ring with G.8032 protocol.
-

PS: in this case, we will use the port9 and port10 of each switch to build a ring.



G.8032 Ethernet Ring Protection

ID	Enabled	Role	Type	Ring Port 0	Ring Port 1	
1	Disabled	None	Sub	Port 1	Port 2	

Apply

- Enter edit mode

G.8032 Ethernet Ring Protection

ID	Enabled	Role	Type	Ring Port 0	Ring Port 1	
1	Disabled	None	Sub	Port 1	Port 2	 

Apply

- There are 3 **roles** in the ring of G.8032, “**owner**”, “**neighbour**” and “**none**”, remember 3 roles are very important things during the setting procedure:
- **The port 0 of “owner” switch must connect with the “neighbour” switch.**
- **After enabling the ring of G8032, the port0 of owner switch will be blocked at first.**

To be safe, we suggest to finish all the settings of G8032 before connecting physically if the user is not familiar with the ring G8032 function.

- The setting of owner switch
(Because we only have single ring, so we set the type as Major)

ID	Enabled	Role	Type	Ring Port 0	Ring Port 1	+
Editing Ring Instance 0						
ID	1					
Ring Enabled	<input checked="" type="checkbox"/>					
Role	Owner					
Type	Major					
Port 0	Port 9					
Port 1	Port 10					
						<div> <div>Cancel</div> <div>Save</div> </div>

Apply

- The setting of neighbour switch

ID	Enabled	Role	Type	Ring Port 0	Ring Port 1	+
Editing Ring Instance 0						
ID	1					
Ring Enabled	<input checked="" type="checkbox"/>					
Role	Neighbour					
Type	Major					
Port 0	Port 9					
Port 1	Port 10					
						<div> <div>Cancel</div> <div>Save</div> </div>

- The setting of none switch

ID	Enabled	Role	Type	Ring Port 0	Ring Port 1	
Editing Ring Instance 0						
ID	1					
Ring Enabled	<input checked="" type="checkbox"/>					
Role	None					
Type	Major					
Port 0	Port 9					
Port 1	Port 10					
						<input type="button" value="Cancel"/> <input type="button" value="Save"/>

6.19 Dual Homing

Dual-Homing

ID	Enabled	Role	Port	
<input type="button" value="+"/>				
<input type="button" value="Apply"/>				

This function was designed to connect ITU-Ring with the other 3rd party switches while maintaining redundant path.

ID	Enabled	Role	Port	
Editing Dual-Homing Instance 1				
ID	1			
Enabled	<input type="checkbox"/>			
Role	Primary			
Port	Port 1			

- **ID:**
the ID of Dual Homing connection
- **Enable:**
enable the Dual Homing function of this port
- **Role:**
there should be 2 connections between RSTP with ITU-Ring, one set Primary, the other set Secondary
- **Port:**
The port which connect to the switch which running RSTP protocol.

6.20 Maintenance

6.20.1 Save Configuration

Save setting of switch

System Config Save

Save

6.20.2 Config backup/restore

■ Settings Backup

You can download the backup configuration of the switch.

■ Settings Restore

You can copy the backup configuration of the switch to the startup configuration on this page. The new startup configuration is not available immediately, which means that restart the switch is necessary.

■ Reset to default

You can reset the configuration of the switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no res

Config Backup/Restore

Settings Backup

Click button to download current settings

Download settings

Settings Restore

Select the file previously backup to restore

Select File

Reset to default

Click button to reset to default settings

Restore to default

Keep IP & Account



Restart is necessary.

6.20.3 Restart device

Reboot the switch with selected firmware.

Maintaince Reboot

Active Firmware

Firmware 1

Firmware 1

Firmware 2

Restart Device

6.20.4 Firmware Upgrade

Update the switch with the firmware file which on your desktop.

Firmware Upgrade

Select the firmware file to upload

Select File

6.20.5 Diagnostics

■ PING

Address: Set the IP address which you want to ping

Count: Set the times of Ping

Packet Size: set the size of Ping packet.

Ping

ARP Table

Address

192.168.9.1

Send!

Count

4

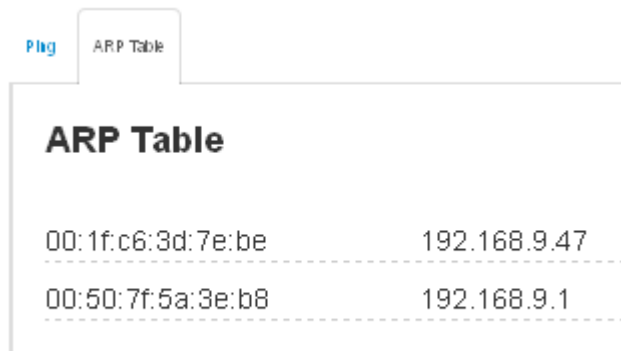
Packet Size

64

PING 192.168.9.1 (192.168.9.1): 64 data bytes
72 bytes from 192.168.9.1: seq=0 ttl=255 time=8.048 ms
72 bytes from 192.168.9.1: seq=1 ttl=255 time=0.429 ms
72 bytes from 192.168.9.1: seq=2 ttl=255 time=0.420 ms
72 bytes from 192.168.9.1: seq=3 ttl=255 time=0.417 ms
--- 192.168.9.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.417/2.328/8.048 ms

■ ARP Table

You can find the MAC address of each IP you have ping via this switch in here.



ARP Table	
00:1f:c6:3d:7e:be	192.168.9.47
00:50:7f:5a:3e:b8	192.168.9.1

Appendix —Command Line mode

Except the web access mode, the Lantech switch also support Telnet access and console access mode, to compare the web access mode, both the Telnet and console only support command line user interface, all these commands are shown as below:

1. Access via console port

When the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program or **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

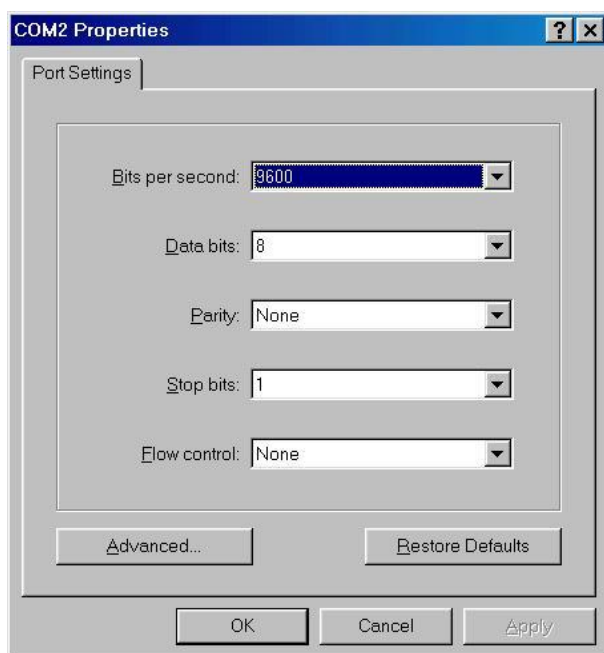
Baud Rate:115200 bps

Data Bits: 8

Parity: none

Stop Bit: 1

Flow control: None



The settings of communication parameters

Having finished the parameter settings, click '**OK**'. When the blank screen shows up, press Enter key to have the login prompt appears. First you need to key in '**admin**' (default value) for both User name and Password (use **Enter** key to switch), then press

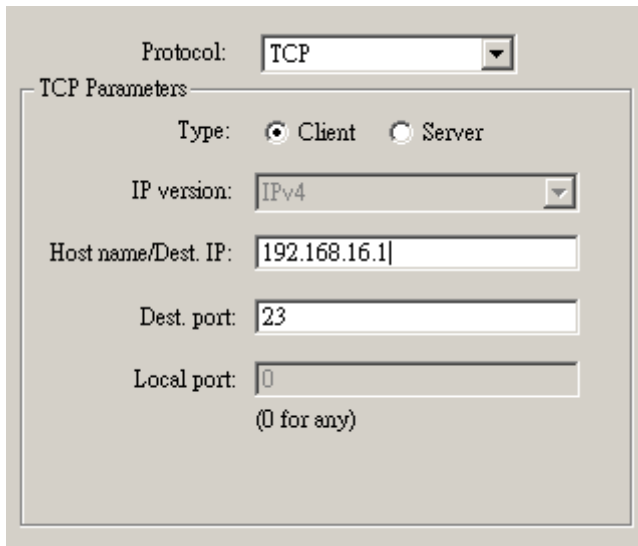
Enter and the Main Menu of console management appears. Please see below figure for login screen.

```
Lantech 2013  
  
login: cli  
Last login: Fri Jun 21 06:15:11 on pts/0  
Login : admin  
Password :  
cur_login = admin  
  
Welcome to Command Line Interface.  
>_
```

Notice: if you forgot the password, you can access the switch via console port and input `lantech /lantech` to restore the password to default.

2. Access via Telnet

Use Telnet utility to access switch IP and make sure the socket was set as 23, all the commands under Telnet mode were the same as the Console mode.



The image shows a configuration window for a Telnet connection. At the top, there is a 'Protocol:' dropdown menu set to 'TCP'. Below this is a section titled 'TCP Parameters'. Inside this section, there are several fields: 'Type:' with radio buttons for 'Client' (selected) and 'Server'; 'IP version:' with a dropdown menu set to 'IPv4'; 'Host name/Dest. IP:' with a text box containing '192.168.16.1'; 'Dest. port:' with a text box containing '23'; and 'Local port:' with a text box containing '0'. Below the 'Local port:' field, there is a note '(0 for any)'.

3. Commands

3.1 System

Command: system

Parameter: N/A

Description: Enter the system mode

Example:

```

>system
Available Commands:
System Configuration
System Contact [<contact>]
System Name [<name>]
System Location [<location>]
System Description [<description>]
System DHCPClient [enable]
System DHCPServer [enable]
System DHCPStatus
System NetStatus
System NetSettingIPv4
System NetSettingIPv6
System Reboot
System RestoreDefault
System Log
System Save
System Ping [<IpAddr>]
System Arp
System Memory
System ConfigAccess [enable]
System Upgrade [URL]
SYSTEM>_

```

3.1.1 Command: system> configuration

Parameter: N/A

Description: show the information of switch

Example:

```

SYSTEM>configuration
SYSTEM>
SystemName : IES-5408DSFP
SystemDescription : 4 1000 SFP +
SystemLocation : 13
SystemContact :
SystemTimeZoneOffset : 0
OID : 1.3.6.1.4.1.37072.302.2.3
MacAddr : 00:11:22:33:44:81
SystemDate : Fri Jun 21 2013 15:
SystemUptime : 77141
SoftwarekernelVersion : 39c48cd6
SoftwareVersion : V3.27

```

3.1.2 Command: system > Contact

Parameter: N/A

Description: display or fix the contact information

Example: if I want to change the contact windows to jacky@lantechcom.tw

```
SYSTEM>contact jacky@lantechcom.tw
SYSTEM>
SystemContact : jacky@lantechcom.tw
```

3.1.3 Command: system > name

Parameter: N/A

Description: display or fix the system name

Example:

```
SYSTEM>name
SYSTEM>
SystemName : IES-5408DSFP
SYSTEM>name IGS-5400-2P
SYSTEM>
SystemName : IGS-5400-2P
```

3.1.4 Command: system > location

Parameter: N/A

Description: display or fix the location

Example:

```
SYSTEM>location
SYSTEM>
SystemLocation : 13
SYSTEM>location Taiwan
SYSTEM>
SystemLocation : Taiwan
```

3.1.5 Command: system > description

Parameter: N/A

Description: display or fix the system description

Example:

```
SYSTEM>
SystemDescription : switch
SYSTEM>description industrial
SYSTEM>
SystemDescription : industrial
```

3.1.6 Command: system > DHCPclient

Parameter: enable/disable

Description: enable or disable DHCP client

Example:

```
SYSTEM>dhcpclient enable
SYSTEM>
DHCP Client enable: 0
SYSTEM>dhcpclient disable
SYSTEM>
DHCP Client enable: 1
```

3.1.7 Command: system > DHCP server

Parameter: [enable|disable]→ enable or disable DHCP server

[<range_low>]/[<range_high>]→ set the IP range

[<netmask>]→ set submask

[<gateway>]→ set gateway

[<dns>]→ set DNS server

[<lease_time>]→ set the lease time of released IP

Example:

```
SYSTEM>DHCPserver
SYSTEM>
DHCP Server enable: true
DHCP Server range_low: 192.168.9.100
DHCP Server range_high: 192.168.9.200
DHCP Server netmask: 255.255.255.0
DHCP Server gateway: 192.168.16.254
DHCP Server dns: 8.8.8.8
DHCP Server lease_time: 86400
```

3.1.8 Command system > DHCPstatus

Parameter: N/A

Description: show the information of DHCP client

Example:

```

SYSTEM>DHCPstatus
SYSTEM>
MacAddress                IpAddress
-----
00:1f:c6:3d:7e:25        192.168.9.101

```

3.1.9 Command: system > netstatus

Parameter: N/A

Description: show the status about IP address

Example:

```

SYSTEM>netstatus
SYSTEM>
IpAddr : 192.168.16.1
Netmask : 255.255.255.0
GatewayIp :
DnsIp : 168.95.1.1

```

3.1.10 Command: system > netsettingIPv4

Parameter: [<IpAddr>]→ set IP address

[<netmask>]→ set netmask

[<gatewayip>]→ set gateway

[<dnsip>]→ set DNS server

Description: set the IP detail of switch

Example:

```

SYSTEM>netsettingIPv4
SYSTEM>
IpAddr : 192.168.16.1
Netmask : 255.255.255.0
GatewayIp : 192.168.9.1
DnsIp : 168.95.1.1

```

3.1.11 Command: system > netsettingIPv6

Parameter: N/A

Description: set the IP address of IPv6

Example:

```

SYSTEM>netsettingIPv6
SYSTEM>
IpAddrv6 : 2001:0db8:0:f101::3

```

3.1.12 Command: system > reboot

Parameter: N/A

Description: reboot the switch

Example:

```
SYSTEM>reboot
SYSTEM>System Reboot after 1 sec

Broadcast message from root (Fri Jun 21 17
The system is going down for reboot NOW!
```

3.1.13 Command: system > restoredefault

Parameter: keep_none → restore all setting

keep_all → restore all but keep original IP address and account

keep_ip → restore all but keep original IP address

keep_account → restore all but keep original account

Description: restore the setting of switch to factory default

Example:

```
SYSTEM>restoredefault ?
Invalid parameter:?
Syntax:System RestoreDefault [keep_none | keep_all | keep_ip | keep_account]
```

3.1.14 Command: system > log

Parameter: N/A

Description: display the event log

Example:

```
Fri, 21 Jun 2013 03:40:27 GMT linkchg
Fri, 21 Jun 2013 05:37:26 GMT linkchg
Fri, 21 Jun 2013 05:37:40 GMT boot
Fri, 21 Jun 2013 06:04:23 GMT auth
Fri, 21 Jun 2013 06:15:20 GMT auth
```

3.1.15 Command: system > save

Parameter: N/A

Description: save the fixed setting

Example:


```
SYSTEM>save
SYSTEM>
System save success!!
```

3.1.16 Command: system > ping

Parameter: N/A

Description: ping the IP address

Example:

```
SYSTEM>ping 192.168.16.1
SYSTEM>host 192.168.16.1 is alive
```

3.1.17 Command: system > arp

Parameter: N/A

Description: resolve the IP address to MAC address

Example:

```
SYSTEM>arp
SYSTEM>
IpAddress                      MacAddress
-----                      -
192.168.16.66                  00:1f:c6:3d:7e:25
```

3.1.18 Command: system > memory

Parameter: N/A

Description: display the status of used switch memory

Example:

```
SYSTEM>memory
SYSTEM>
Type                      Size(kb)
-----                      -
MemTotal                  239540
MemFree                   173664
```

3.1.19 Command: system > configaccess

Parameter: [export|import] → export or import the setting of switch
 [URL] → set the destination which save/load the setting file, support both the TFTP and FTP protocol.

Description: export or import the setting of switch

Example:

```
SYSTEM>configaccess export ftp://192.168.16.66
```

3.1.20 Command: system > upgrade

Parameter: [URL] → set the source of firmware file, support TFTP and FTP and HTTP protocol.

Description: update switch firmware

Example:

```
SYSTEM>upgrade tftp:192.168.16.1  
Please wait for upgrade
```

3.2 LLDP

Command: LLDP

Parameter: N/A

Description: Enter the LLDP mode

Example:

```
>lldp  
Available Commands:  
LLDP Configuration [<port_list>]  
LLDP Enabled [enable|disable]  
LLDP Mode [<port_list>] [enabledRx  
LLDP Interval [<interval>]  
LLDP Timetolive [<tvl>]  
LLDP Info [<port_list>]  
LLDP Statistics [clear]  
LLDP>_
```

3.2.1 Command: LLDP > configuration

Parameter: N/A

Description: display the LLDP information

Example:

```

LLDP>configuration
LLDP>
Interval: 10
Port      Mode
-----
1         enabledRxTx
2         enabledRxTx
3         enabledRxTx
4         enabledRxTx
5         enabledRxTx
6         enabledRxTx
7         enabledRxTx
8         enabledRxTx
9         enabledRxTx
10        enabledRxTx
11        enabledRxTx
12        enabledRxTx

```

3.2.2 Command: LLDP > enabled

Parameter: N/A

Description: enable LLDP protocol

Example:

```

LLDP>enabled
LLDP>
Enabled: true

```

3.2.3 Command: LLDP > mode

Parameter: [<port_list>]→display LLDP information of the dedicated port

[enabledRxTx]→ enable Tx and Rx of LLDP function with dedicated port

[enabledTxOnly]→ enable Tx only of LLDP function with dedicated port

[enabledRxOnly]→ enable Rx only of LLDP function with dedicated port

[disabled]→ disable LLDP function with dedicated

Description: enable LLDP function of each port

Example:

```
LLDP>mode
LLDP>
Port      Mode
-----
1         enabledRxTx
2         enabledRxTx
3         enabledRxTx
4         enabledRxTx
5         enabledRxTx
6         enabledRxTx
7         enabledRxTx
```

3.2.4 Command: LLDP > interval

Parameter: N/A

Description: set the interval time of LLDP

Example:

```
LLDP>interval 10
LLDP>
Interval: 10
```

3.2.5 Command: LLDP > timetolive

Parameter: N/A

Description: display the alive time of LLDP information.

Example:

```
LLDP>timetolive
LLDP>
Time to live : 15
```

3.2.6 Command: LLDP > info

Parameter: N/A

Description: display the LLDP information of neighbor port

Example:

```
LLDP>info
LLDP>
Localport          ChassisID          PortID  PortDescription  SystemName
-----
```

3.2.7 Command: LLDP > statistics

Parameter: N/A

Description: display the detail information of LLDP settings

Example:

```
LLDP>statistics
LLDP>
Total LLDP traffic statistics
Total entries added : 0
Total entries deleted : 0
Total entries aged : 0
Total frames out : 6127
Total frames in : 0
Total frames received in error : 0
Total frames discarded : 0
Total TLVs discarded : 0
Total TLVs unrecognized : 0
Localport          FramesIn          FramesOut
-----
```

1	0	55
2	0	55
3	0	55
4	0	55

3.3 Port

Command: port

Parameter: N/A

Description: Enter the port mode

Example:

```

>port
Available Commands:
Port Configuration [<port_list>]
Port Status [<port_list>]
Port Enabled [<port_list>] [enable|disable]
Port Description [<port_list>] [string]
Port Speed [<port_list>] [10hdx|10fdx|100hdx|100fdx]
Port FlowControl [<port_list>] [enable|disable]
Port IngressRate [<port_list>] [<rate> kbps]
Port EgressRate [<port_list>] [<rate> kbps]
Port Statistics [clear]

```

3.3.1 Command: port > configuration

Parameter: N/A

Description: display the setting of each port

Example:

```

PORT>configuration
PORT>

```

Port	enabled	Description	Speed	Conf	Flow Control	Conf
1	true	Port 1	auto		auto	
2	true	Port 2	auto		auto	
3	true	Port 3	auto		auto	
4	true	Port 4	auto		auto	
5	true	Port 5	auto		auto	
6	true	Port 6	auto		auto	
7	true	Port 7	auto		auto	
8	true	Port 8	auto		auto	

3.3.2 Command: port > status

Parameter: N/A

Description: display the connection status of each port

Example:

```

PORT>status
PORT>

```

Port	Group ID	Type	Link	State	Speed
1	-1	100TX	down	enable	N/A
2	-1	100TX	down	enable	N/A
3	-1	100TX	down	enable	N/A
4	-1	100TX	up	enable	100
5	-1	100TX	down	enable	N/A
6	-1	100TX	down	enable	N/A
7	-1	100TX	down	enable	N/A
8	-1	100TX	down	enable	N/A
9	-1	DSFP	down	enable	N/A

3.3.3 Command: port > enabled

Parameter: [<port_list>]→ choose which port you want to enable or disable
[enable|disable]→ enable/disable

Description: enable or disable switch port

Example:

```

PORT>enable
PORT>

```

Port	Enabled
1	true
2	true
3	true
4	true
5	true
6	true
7	true

3.3.4 Command: port > description

Parameter: N/A

Description: display the description of each port

Example:

```

PORT>description
PORT>
Port      Description
-----
1         Port 1
2         Port 2
3         Port 3
4         Port 4
5         Port 5

```

3.3.5 Command: port > speed

Parameter: N/A

Description: display the speed of each port

Example:

```

PORT>speed
PORT>
Port      Speed Conf
-----
1         auto
2         auto
3         auto
4         auto
5         auto

```

3.3.6 Command: port > flowcontrol

Parameter: [<port_list>]→ choose which port you want to enable or disable
[enable|disable]→ enable/disable

Description: enable or disable flow control function of each port

Example:


```

PORT>flowcontrol
PORT>
Port      FlowControl Conf
-----
1         true
2         true
3         true
4         true
5         true
6         true
7         true

```

3.3.7 Command: port > Ingressrate

Parameter: [<port_list>]→ choose which port you want to set the ingress rate
 [<rate> kbps]→set the ingress rate of these packet as below

- ◆ broadcast
- ◆ multicast
- ◆ unicast
- ◆ broad_uni
- ◆ broad_multi
- ◆ multi_uni
- ◆ uni_broad_multi

Description: set the ingress rate of the dedicated port with specified packet

Example:

```

PORT>ingressrate
PORT>
Port      Ingress Rate      Ingress Type
-----
1         0
2         0
3         0
4         0

```

3.3.8 Command: port > egressrate

Parameter: [<port_list>] → choose which port you want to set the ingress rate

[<rate> kbps] → set the ingress rate

Description: set the egress rate of the dedicated port

Example:

```
PORT>egress
PORT>
Port      Egress Rate
-----
1         0
2         0
3         0
4         0
```

3.3.9 Command: port > statistics

Parameter: N/A

Description: display the detail information of port statistics

Example:

```
PORT>statistics
PORT>
ports :
Txgoodbyte :
Txgoodpkts :
Txmcpkts :
Txbrdepkts :
Txerr :
Txucpkts :
Txmultiplepkts :
Txdeferredpkts :
Rxgoodbyte :
Rxbadbyte :
Rxgoodpkts :
Rxbadpkts :
Rxbrdepkts :
Rxmcpkts :
Rxmacerror :
Rxbadfc :
Rxucpkts :
Rxunrecognt r :
Rxgoodfc :
64byte_ :
```