



IES-P3073GC

Industrial Managed Ethernet Switch

User Manual

Version 3.0

Jan, 2014



COPYRIGHT NOTICE

Copyright © 2014 ORing Industrial Networking Corp.

All rights reserved.

No part of this publication may be reproduced in any form without the prior written consent of ORing Industrial Networking Corp.

TRADEMARKS



is a registered trademark of ORing Industrial Networking Corp.

All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

WARRANTY

ORing warrants that all ORing products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). ORing will repair or replace products found by ORing to be defective within this warranty period, with shipment expenses apportioned by ORing and the distributor. This warranty does not cover product modifications or repairs done by persons other than ORing-approved personnel, and this warranty does not apply to ORing products that are misused, abused, improperly installed, or damaged by accidents.

Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

DISCLAIMER

Information in this publication is intended to be accurate. ORing shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ORing reserves the right to revise the contents of this publication without notice.

CONTACT INFORMATION

ORing Industrial Networking Corp.

3F., NO.542-2, Jhongjheng Rd., Sindian District, New Taipei City 231, Taiwan, R.O.C.

Tel: + 886 2 2218 1066 // Fax: + 886 2 2218 1014

Website: www.oring-networking.com

Technical Support

E-mail: support@oring-networking.com

Sales Contact

E-mail: sales@oring-networking.com (Headquarters)

sales@oring-networking.com.cn (China)



Table of Content

Getting Started.....	5
1.1 About IES-P3073GC.....	5
1.2 Software Features	5
1.3 Hardware Specifications	6
Hardware Overview.....	7
2.1 Front Panel.....	7
2.1.1 Ports and Connectors	7
2.1.2 LED.....	8
2.2 Rear Panel	8
Hardware Installation	9
3.1 DIN-rail Installation	9
3.2 Wall Mounting.....	10
3.3 Wiring.....	11
3.3.1 Grounding	12
3.3.2 Fault Relay	12
3.3.3 Redundant Power Inputs	12
3.4 Connection.....	13
3.4.1 Cables.....	13
3.4.2 SFP.....	15
3.4.3 O-Ring/O-Chain.....	16
Redundancy.....	19
4.1 O-Ring.....	19
4.1.1 Introduction	19
4.1.2 Configurations.....	19
4.2 Open-Ring.....	21
4.2.1 Introduction	21
4.2.2 Configurations.....	21
4.3 O-Chain.....	22
4.3.1 Introduction	22
4.3.2 Configurations.....	22
4.4 MRP.....	23
4.4.1 Introduction	23
4.4.2 Configurations.....	23



- 4.5 STP/RSTP/MSTP 24
 - 4.5.1 STP/RSTP..... 24
 - 4.5.2 MSTP 28
- 4.6 Fast Recovery..... 32
- Management 33**
- 5.1 Basic Settings..... 34
 - 5.1.1 System Information..... 34
 - 5.1.2 Admin & Password 35
 - 5.1.3 IP Settings..... 36
 - 5.1.4 Time Settings..... 37
 - 5.1.5 LLDP..... 39
 - 5.1.6 Modbus TCP 40
 - 5.1.7 Backup/Restore..... 41
 - 5.1.8 Firmware Update..... 42
- 5.2 Multicast..... 43
 - 5.2.1 IGMP Snooping 43
 - 5.2.2 MVR..... 44
 - 5.2.3 Static Multicast Filtering..... 45
- 5.3 Port Setting 45
 - 5.3.1 Port Control..... 46
 - 5.3.2 Port Status..... 46
 - 5.3.3 Port Alias..... 47
 - 5.3.4 Rate Limit..... 47
 - 5.3.5 Port Trunk..... 48
 - 5.3.6 Loop Guard 49
 - 5.3.7 VLAN..... 49
- 5.4 Traffic Prioritization 52
 - 5.4.1 QoS Policy 52
 - 5.4.2 Port-base priority..... 54
 - 5.4.3 COS/802.1p..... 54
 - 5.4.4 TOS/DSCP..... 55
- 5.5 DHCP Server..... 55
 - 5.5.1 Basic Settings..... 56
 - 5.5.2 Client List 57
 - 5.5.3 Port and IP Bindings..... 57
 - 5.5.4 DHCP Relay Agent 57
- 5.6 SNMP..... 58



5.6.1	SNMP Agent.....	59
5.6.2	SNMP Trap.....	60
5.6.3	SNMPV3	61
5.6.4	Security.....	63
5.6.5	IP Guard.....	68
5.6.6	Warning.....	70
5.7	Monitor and Diag.....	73
5.7.1	System Event Log	73
5.7.2	MAC Address Table.....	74
5.7.3	Ping.....	80
5.7.4	Save Configuration	81
5.7.5	Factory Default.....	81
5.7.6	System Reboot.....	81
	Command Line Interface Management.....	82

Getting Started

1.1 About IES-P3073GC



The IES-P3073GC is a powerful managed industrial switch designed for extreme temperatures, dusty environments and high humidity. With IEC61850 compliance, the switch is especially ideal for power substation applications. Featuring seven 10/100Base-T(X) RJ-45 fast Ethernet ports and three Gigabit combo ports (10/100/1000Base-T(X) RJ-45 & 100/1000Base-X SFP Ports), the IES-P3073GC can be managed centrally via web browsers, TELNET, Console or other third-party SNMP software as well as ORing's proprietary Open-Vision management utility. With complete support for Ethernet redundancy protocols such as O-Ring (recovery time < 30ms over 250 units of connection) and MSTP (RSTP/STP compatible), the switch can protect your mission-critical applications from network interruptions or temporary malfunctions with its fast recovery technology. Boasting a wide operating temperature from -40°C to 70°C, the switch can meet the demanding requirements of power substations and rolling stock applications.

1.2 Software Features

- Supports O-Ring (recovery time < 30ms over 250 units of connection) and MSTP(RSTP/STP compatible) for Ethernet redundancy
- Supports Open-Ring to interoperate with other vendors' ring technology in open architecture
- Supports O-Chain to allow multiple redundant network rings
- Supports standard IEC 62439-2 MRP (Media Redundancy Protocol) function
- Supports STP/RSTP/MSTP
- Support PTP Client (Precision Time Protocol) clock synchronization
- Supports Modbus / TCP protocol
- Supports IGMP v2/v3 (IGMP snooping support) to filter multicast traffic
- Supports Port Trunking for easy bandwidth management
- Supports SMTP client
- Supports RMON for traffic monitoring
- Supports DDM (Digital Diagnostic Monitoring) function
- Support LLDP protocol
- Locks ports to prevent access from unauthorized MAC address
- Supports multiple notifications for incidents such as Syslog, e-mail, SNMP trap, and relay output



- Supports management via Web-based interfaces, Telnet, Console (CLI), and Windows utility (Open-Vision)

1.3 Hardware Specifications

- 7 x 10/100Base-T(X)
- 3 x 10/100/1000Base-T(X) Gigabit Ethernet ports (combo)
- 3 x 100/1000Base-X SFP ports (combo)
- 1 x Console Port
- Redundant DC power inputs
- IEC 61850-3 and IEEE 1613 compliance
- Din-rail and wall-mounting available
- Operating Temperature: -40 to 85°C
- Storage Temperature: -40 to 85°C
- Operating Humidity: 5% to 95%, non-condensing
- Casing: IP-30
- Dimensions: 96.4 (W) x 145.5 (D) x 154 (H)mm

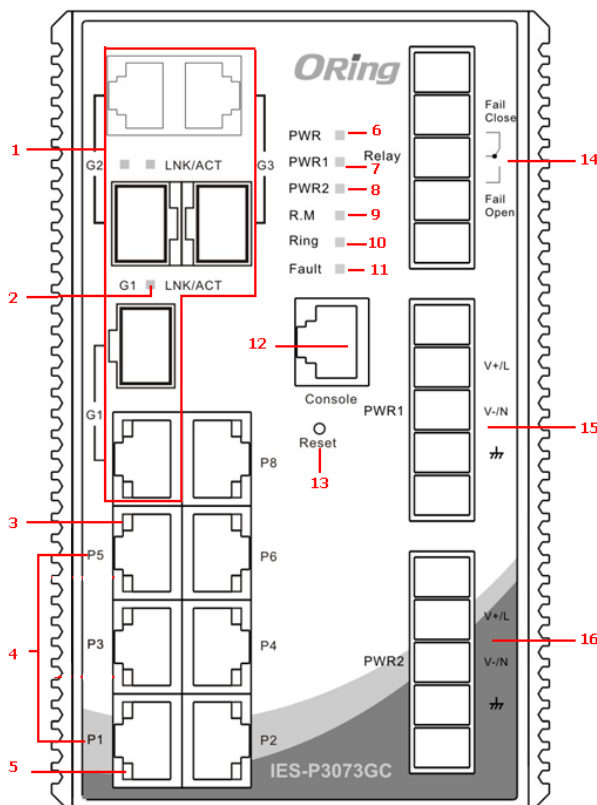
Hardware Overview

2.1 Front Panel

2.1.1 Ports and Connectors

The IES-P3073GC series provide the following ports on the front panel. The Ethernet ports on the switch use RJ-45 connectors and the SFP module slots.

Port	Description
Copper port	7 x 10/100Base-T(X) ports
Gigabit combo port	3 x 10/100/1000Base-T(X) RJ-45 + 100/1000Base-X SFP ports
Console port	1 x console port
Reset button	1 x reset button. Press the button for 3 seconds to reset and 5 seconds to return to factory default.



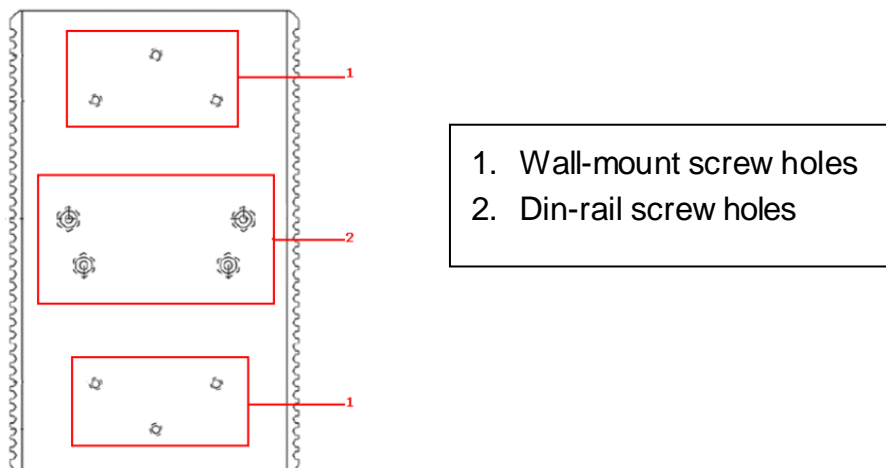
1. 100Base FX/1000Base X combo ports
2. LNK/ACT LED for Gigabit LAN ports
3. LNK status LED for Ethernet LAN ports
4. Ethernet LAN ports
5. ACT status LED for LAN ports
6. Power LED
7. PW1 LED
8. PW2 LED
9. R.M status LED
10. Ring status LED
11. Fault indicator
12. Console port
13. Reset button
14. Fault relay
15. PWR 1 terminals

2.1.2 LED

LED	Color	Status	Description
PWR	Green	On	DC power on
PW1	Green	On	DC power module 1 activated
PW2	Green	On	DC power module 2 activated
R.M	Green	On	System running in Ring Master mode
Ring	Green	On	System running in Ring mode
		Blinking	Ring structure is broken (i.e. part of the ring is disconnected)
Fault	Amber	On	Faulty relay (power failure or port malfunctioning)
10/100Base-T(X) Fast Ethernet ports			
LNK/ACT	Green	On	Ethernet links connected
		Blinking	Transmitting data
Full Duplex	Amber	On	Port works in full duplex mode
SFP Combo ports			
LNK/ACT	Green	On	Ethernet links connected
		Blinking	Transmitting data

2.2 Rear Panel

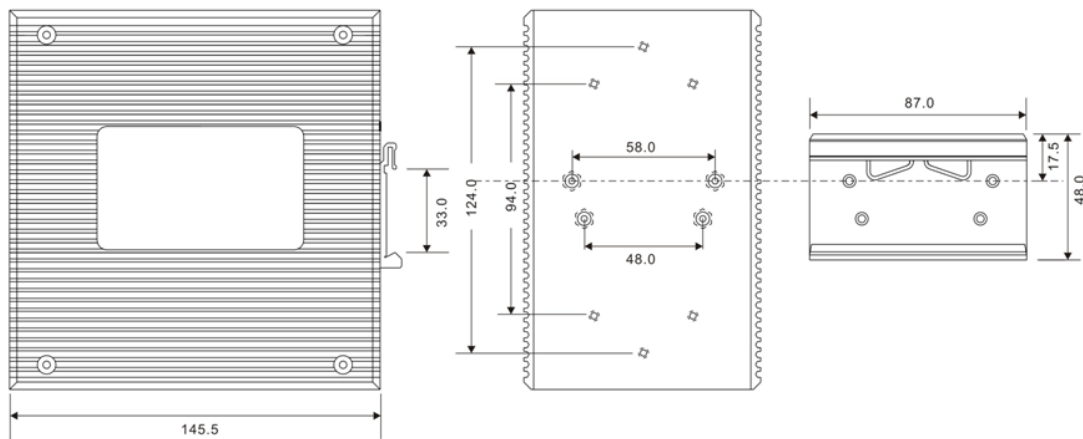
On the rear panel of the switch sit three sets of screw holes. The two sets placed in triangular patterns on both ends of the rear panel are used for wall-mounting (red boxes in the figure below) and the set of four holes in the middle are used for Din-rail installation (blue box in the figure below). For more information on installation, please refer to [23.1 Din-rail Installation](#).



Hardware Installation

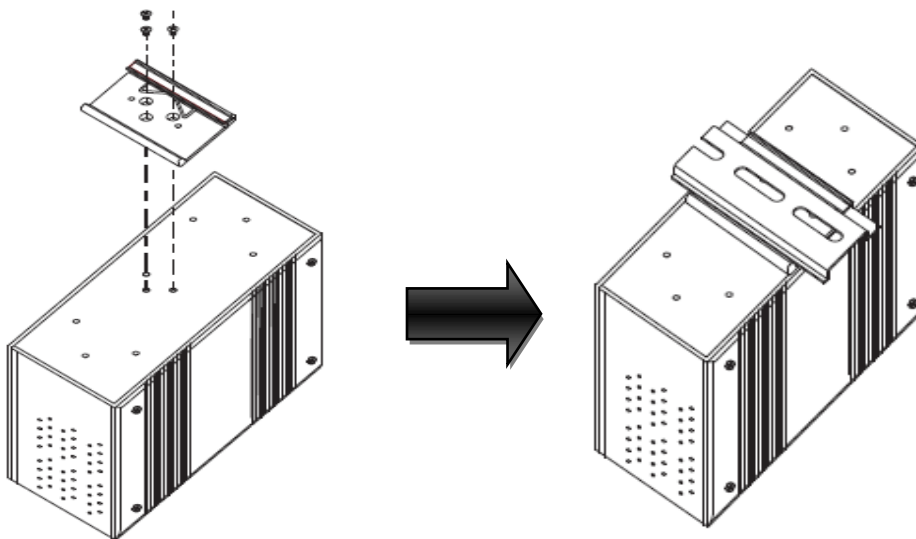
3.1 DIN-rail Installation

The device comes with a DIN-rail kit to allow you to fasten the switch to a DIN-rail in any environments.



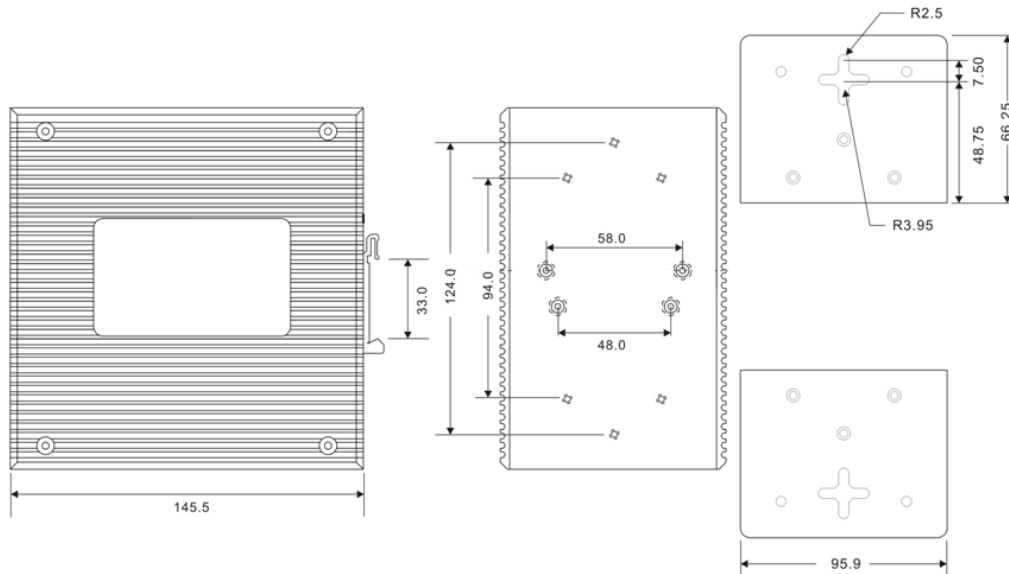
DIN-rail Kit Measurement

Installing the switch on the DIN-rail is easy. First, screw the Din-rail kit onto the back of the switch, right in the middle of the back panel. Then slide the switch onto a DIN-rail from the Din-rail kit and make sure the switch clicks into the rail firmly.



3.2 Wall Mounting

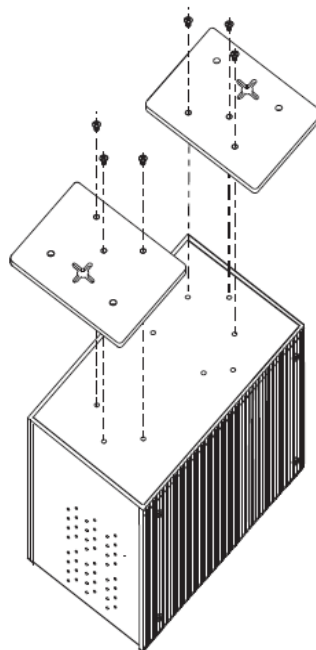
Besides Din-rail, the switch can be fixed to the wall via a wall mount panel, which can be found in the package.



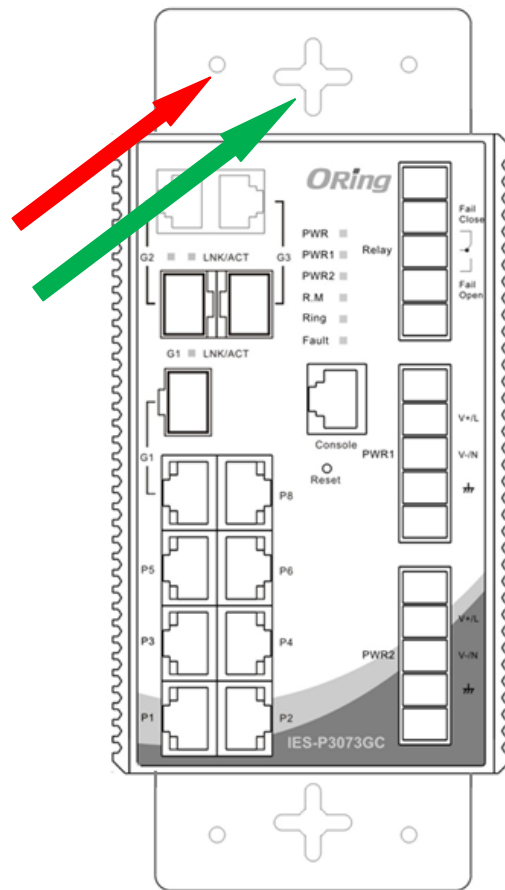
Wall-Mount Kit Measurement

To mount the switch onto the wall, follow the steps:

1. Screw the two pieces of wall-mount kits onto both ends of the rear panel of the switch. A total of six screws are required, as shown below.



2. Use the switch, with wall mount plates attached, as a guide to mark the correct locations of the four screws.
3. Insert screws through the round screw holes (the red arrow as below) on the sides or through the cross-shaped aperture (the green arrow as below) in the middle of the plate and fasten the screw to the wall with a screwdriver.
4. If the screw goes through the cross-shaped aperture, slide the switch down before tightening the screw.



Note: Instead of screwing the screws in all the way, leave about 2 mm to allow room for sliding the wall mount panel between the wall and the screws.

3.3 Wiring



WARNING

Do not disconnect modules or wires unless power has been switched off or the area is known to be non-hazardous. The devices may only be connected to the supply voltage shown on the type plate.



ATTENTION

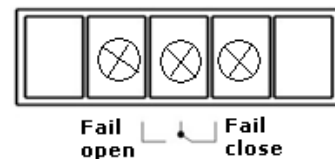
1. Be sure to disconnect the power cord before installing and/or wiring your switches.
2. Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.
3. If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.
4. Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.
5. Do not run signal or communications wiring and power wiring through the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.
6. You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring sharing similar electrical characteristics can be bundled together.
7. You should separate input wiring from output wiring.
8. It is advised to label the wiring to all devices in the system.

3.3.1 Grounding

Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screw on the power module to the grounding surface prior to connecting devices.

3.3.2 Fault Relay

The switch provides fail open and fail close options for you to form relay circuits based on your needs. If you want the relay device to start operating at power failure, attach the two wires to COM and fail close to form a close circuit, vice versa. The relay contact of the 2-pin terminal block connector will respond to user-configured events according to the wiring.

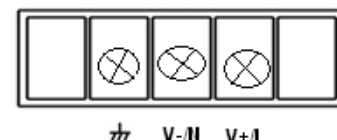


3.3.3 Redundant Power Inputs

The switch has two sets of power inputs, power input 1 and power input 2, which sit on the front panel along with LAN ports. Follow the steps below to wire redundant power inputs.

Step 1: insert the negative/positive wires into the V-/V+ terminals, respectively.

Step 2: to keep the wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.



3.4 Connection

3.4.1 Cables

10/100/1000BASE-T(X) Pin Assignments

The IES-P3073GC series have standard Ethernet ports. According to the link type, the switch uses CAT 3, 4, 5, 5e UTP cables to connect to any other network devices (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications:

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45
1000BASE-TX	Cat. 5/Cat. 5e 100-ohm UTP	UTP 100 m (328ft)	RJ-45

With 10/100Base-T(X) cables, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

10/100 Base-T(X) RJ-45 Pin Assignments :

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

1000 Base-T RJ-45 Pin Assignments :

Pin Number	Assignment
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-

6	BI_DB-
7	BI_DD+
8	BI_DD-

The IES-P3073GC series switches support auto MDI/MDI-X operation. You can use a cable to connect the switch to a PC. The table below shows the 10/100Base-T(X) MDI and MDI-X port pin outs.

10/100 Base-T(X) MDI/MDI-X Pin Assignments:

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

1000Base-T(X) MDI/MDI-X Pin Assignments:

Pin Number	MDI port	MDI-X port
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

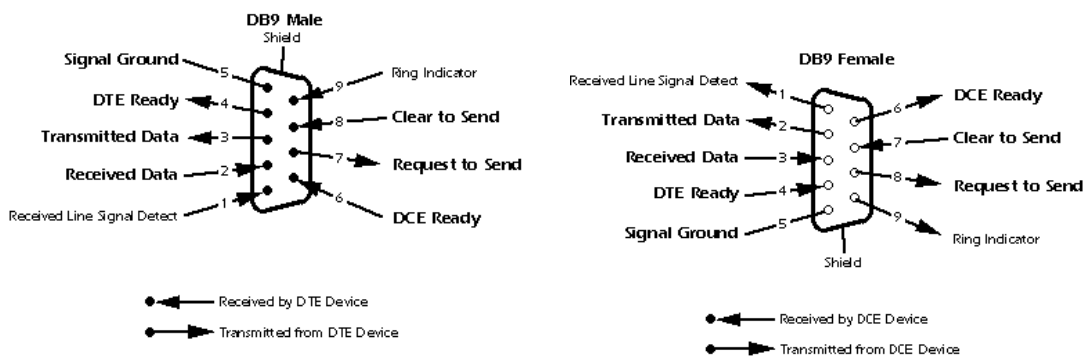
Note: “+” and “-” signs represent the polarity of the wires that make up each wire pair.

RS-232 console port wiring

The IES-P3073GC series can be managed via console ports using a RS-232 cable which can be found in the package. You can connect the port to a PC via the RS-232 cable with a DB-9 female connector. The DB-9 female connector of the RS-232 cable should be connected the PC while the other end of the cable (RJ-45 connector) should be connected to the console port

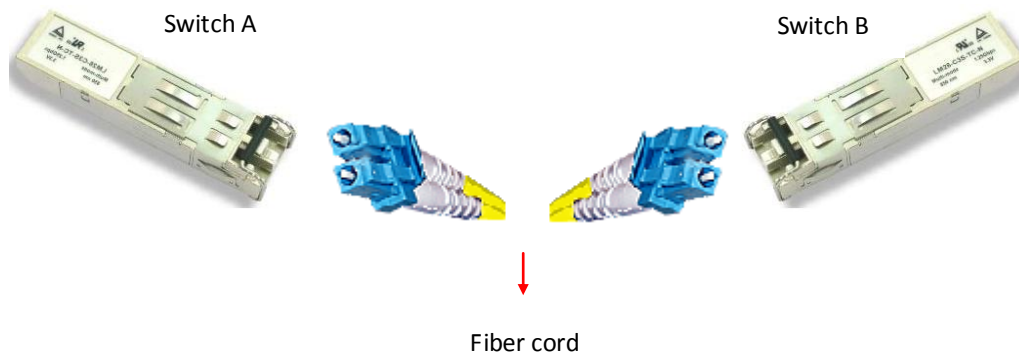
of the switch.

PC pin out (male) assignment	RS-232 with DB9 female connector	DB9 to RJ 45
Pin #2 RD	Pin #2 TD	Pin #2
Pin #3 TD	Pin #3 RD	Pin #3
Pin #5 GD	Pin #5 GD	Pin #5



3.4.2 SFP

The switch provides three combo ports which consist of three SFP transceivers paired with three Gigabit Ethernet ports, allowing you to connect to fiber networks for longer transmission distances. You can choose appropriate SFP transceivers based on your needs as they are hot swappable. SFP transceivers are available in multi- or single-mode with LC connectors. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.

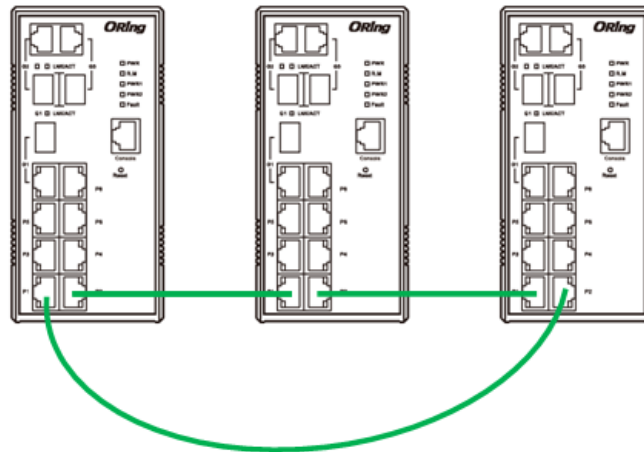


3.4.3 O-Ring/O-Chain

O-Ring

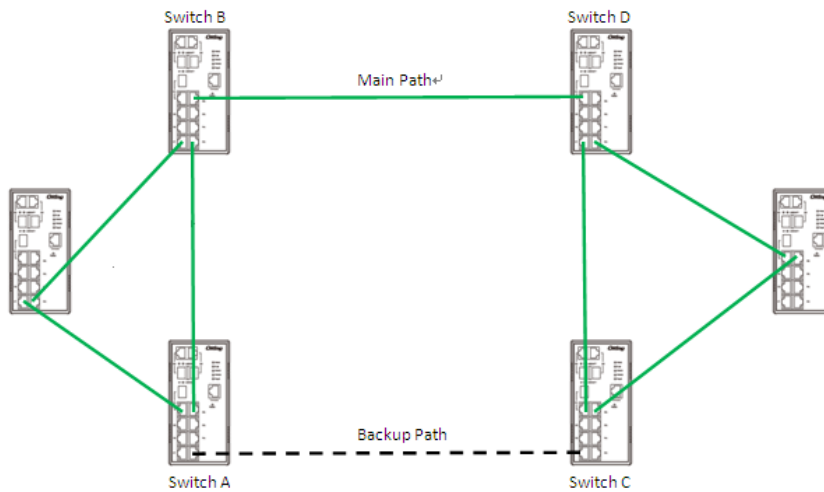
You can connect three or more switches to form a ring topology to gain network redundancy capabilities through the following steps.

1. Connect each switch to form a daisy chain using an Ethernet cable.
2. Set one of the connected switches to be the master and make sure the port setting of each connected switch on the management page corresponds to the physical ports connected. For information about the port setting, please refer to [4.1.2 Configurations](#).
3. Connect the last switch to the first switch to form a ring topology.



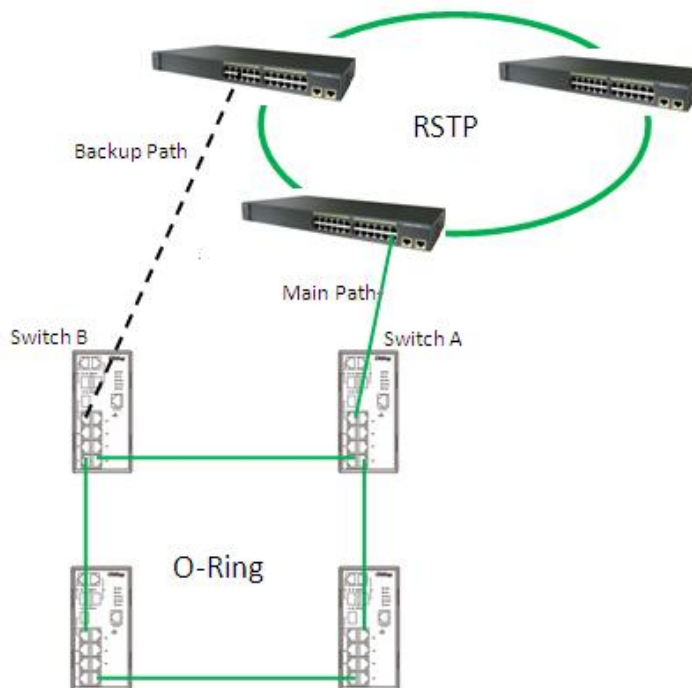
Coupling Ring

If you already have two O-Ring topologies and would like to connect the rings, you can form them into a coupling ring. All you need to do is select two switches from each ring to be connected, for example, switch A and B from Ring 1 and switch C and D from ring 2. Decide which port on each switch to be used as the coupling port and then link them together, for example, port 1 of switch A to port 2 of switch C and port 1 of switch B to port 2 of switch D. Then, enable Coupling Ring option by checking the checkbox on the management page and select the coupling ring in correspondance to the connected port. For more information on port setting, please refer to [4.1.2 Configurations](#). Once the setting is completed, one of the connections will act as the main path while the other will act as the backup path.



Dual Homing

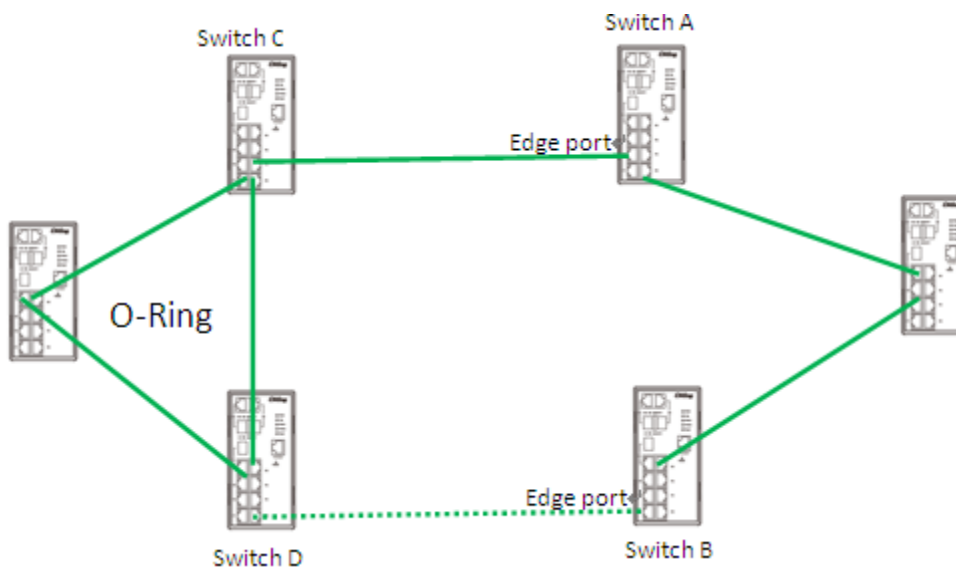
If you want to connect your ring topology to a RSTP network environment, you can use dual homing. Choose two switches (Switch A & B) from the ring for connecting to the switches in the RSTP network (core switches). The connection of one of the switches (Switch A or B) will act as the primary path, while the other will act as the backup path that is activated when the primary path connection fails.



O-Chain

When connecting multiple O-Rings to meet your expansion demand, you can create an O-Chain topology through the following steps.

1. Select two switches from the chain (Switch A & B) that you want to connect to the O-Ring and connect them to the switches in the ring (Switch C & D).
2. In correspondence to the port connected to the ring, configure an edge port for both of the connected switches in the chain by checking the box in the management page (see [4.1.2 Configurations](#)).
3. Once the setting is completed, one of the connections will act as the main path, and the other as the back up path.



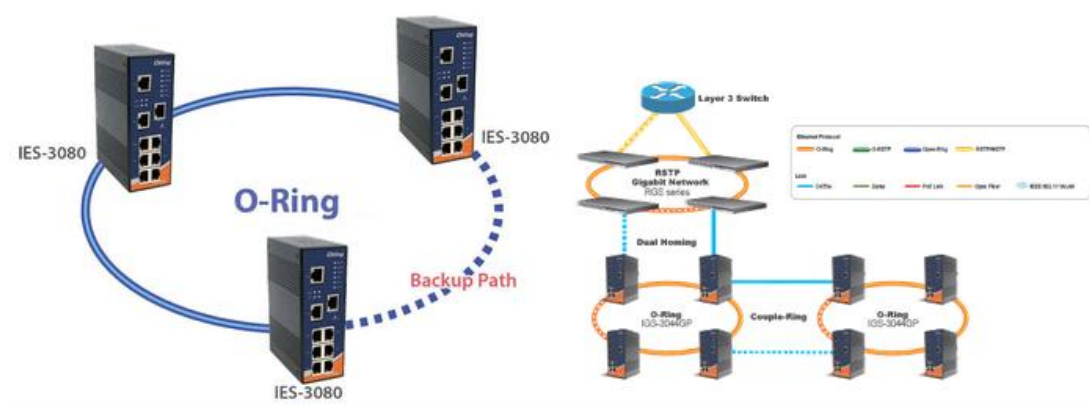
Redundancy

Redundancy for minimized system downtime is one of the most important concerns for industrial networking devices. Hence, ORing has developed proprietary redundancy technologies including O-Ring and Open-Ring featuring faster recovery time than existing redundancy technologies widely used in commercial applications, such as STP, RSTP, and MSTP. ORing's proprietary redundancy technologies not only support different networking topologies, but also assure the reliability of the network.

4.1 O-Ring

4.1.1 Introduction

O-Ring is ORing's proprietary redundant ring technology, with recovery time of less than 30 milliseconds (in full-duplex Gigabit operation) or 10 milliseconds (in full-duplex Fast Ethernet operation) and up to 250 nodes. The ring protocols identify one switch as the master of the network, and then automatically block packets from traveling through any of the network's redundant loops. In the event that one branch of the ring gets disconnected from the rest of the network, the protocol automatically readjusts the ring so that the part of the network that was disconnected can reestablish contact with the rest of the network. The O-Ring redundant ring technology can protect mission-critical applications from network interruptions or temporary malfunction with its fast recover technology.



4.1.2 Configurations

O-Ring supports three ring topologies: **Ring Master**, **Coupling Ring**, and **Dual Homing**. You can configure the settings in the interface below.

O-Ring

<input checked="" type="checkbox"/>	Enable Ring	
<input type="checkbox"/>	Enable Ring Master	
	1st Ring Port	Port.01 <input type="button" value="v"/> LINKDOWN
	2nd Ring Port	Port.02 <input type="button" value="v"/> LINKDOWN
<input type="checkbox"/>	Enable Couple Ring	
	Couple Port	Port.03 <input type="button" value="v"/> LINKDOWN
<input type="checkbox"/>	Enable Dual Homing	
	Homing Port	Port.05 <input type="button" value="v"/> LINKDOWN

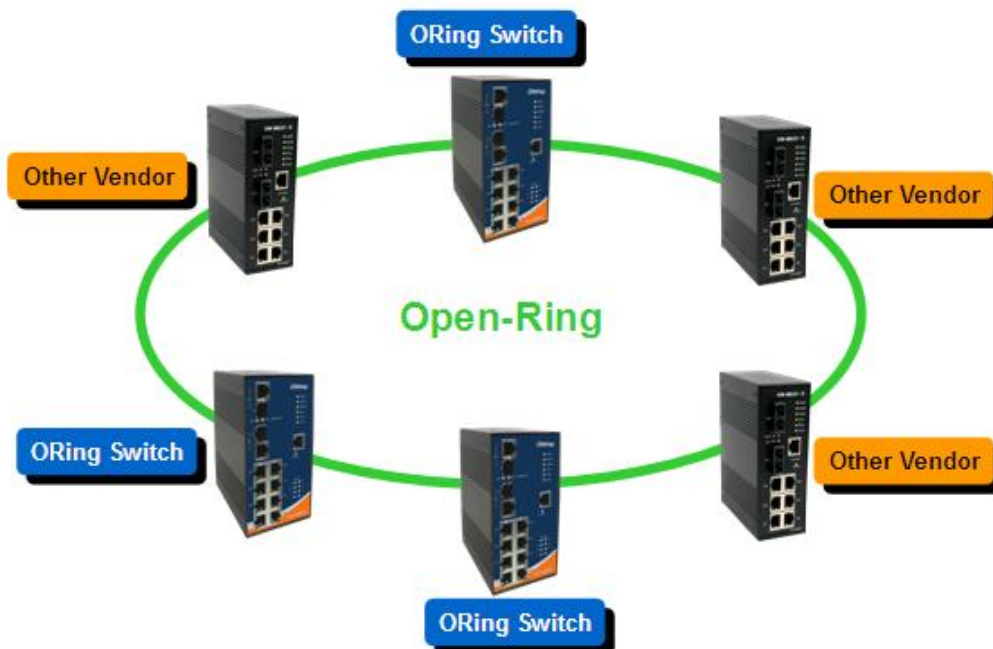
Label	Description
Enable Ring	Check to enable O-Ring topology.
Enable Ring Master	Only one ring master is allowed in a ring. However, if more than one switches are set to enable Ring Master , the switch with the lowest MAC address will be the active ring master and the others will be backup masters.
1st Ring Port	The primary port when the switch is ring master
2nd Ring Port	The backup port when the switch is ring master
Enable Coupling Ring	Check to enable Coupling Ring . Coupling Ring can divide a big ring into two smaller rings to avoid network topology changes affecting all switches. It is a good method for connecting two rings.
Couple Port	Ports for connecting multiple rings. A coupling ring needs four switches to build an active and a backup link. Links formed by the coupling ports will run in active/backup mode.
Enable Dual Homing	Check to enable Dual Homing . When Dual Homing is enabled, the ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work in active/backup mode, and connect each ring to the normal switches in RSTP mode.
Apply	Click to activate the configurations.

Note: due to heavy loading, setting one switch as ring master and coupling ring at the same time is not recommended.

4.2 Open-Ring

4.2.1 Introduction

Open-Ring is a technology developed by ORing to enhance ORing switches' interoperability with other vendors' products. With this technology, you can add any ORing switches to the network based on other ring technologies.



4.2.2 Configurations

Open-Ring

<input checked="" type="checkbox"/> Enable	
Vender	MOXX ▼
1st Ring Port	Port.01 ▼
2nd RingPort	Port.02 ▼

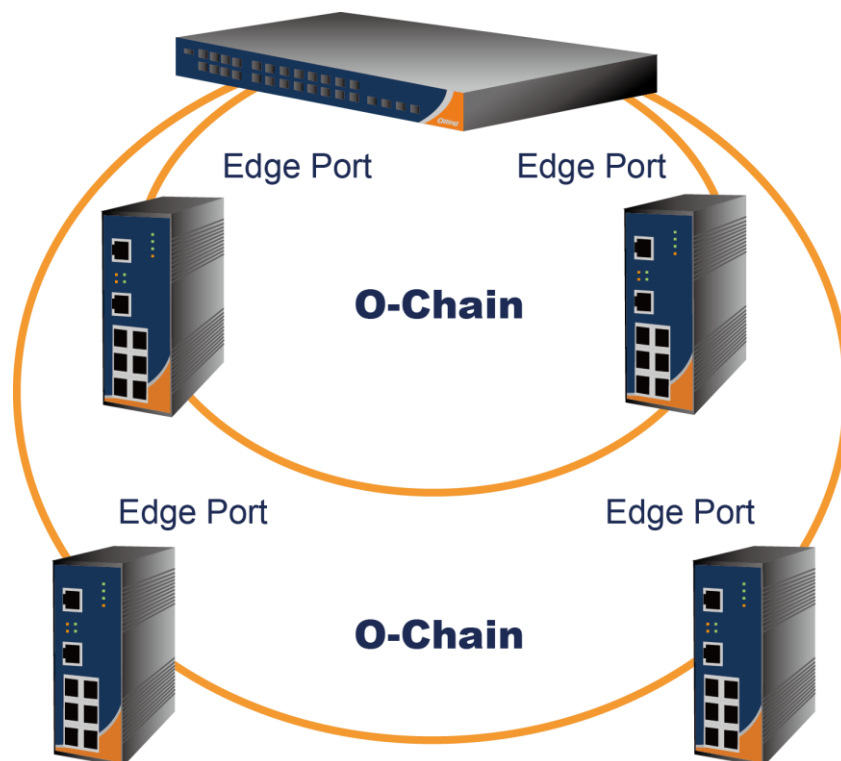
Label	Description
Enable	Check to enable Open-Ring topology
Vender	Choose the vendors that you want to join in their rings
1st Ring Port	The first port to connect to the ring
2nd Ring Port	The second port to connect to the ring

4.3 O-Chain

4.3.1 Introduction

O-Chain is ORing's revolutionary network redundancy technology which enhances network redundancy for any backbone networks, providing ease-of-use and maximum fault-recovery swiftness, flexibility, compatibility, and cost-effectiveness in a set of network redundancy topologies. The self-healing Ethernet technology designed for distributed and complex industrial networks enables the network to recover in less than 30 milliseconds (in full-duplex Gigabit operation) or 10 milliseconds (in full-duplex Fast Ethernet operation) for up to 250 switches if at any time a segment of the chain fails.

O-Chain allows multiple redundant rings of different redundancy protocols to join and function together as a large and the most robust network topologies. It can create multiple redundant networks beyond the limitations of current redundant ring technologies.



4.3.2 Configurations

O-Chain is very easy to configure and manage. Only one edge port of the edge switch needs to be defined. Other switches beside them just need to have O-Chain enabled.

O-Chain

<input checked="" type="checkbox"/> Enable			
	Uplink Port	Edge Port	State
1st	Port.01	<input type="checkbox"/>	Linkdown
2nd	Port.02	<input type="checkbox"/>	Forwarding

Apply

Label	Description
Enable	Check to enable O-Chain function
1st Ring Port	The first port connecting to the ring
2nd Ring Port	The second port connecting to the ring
Edge Port	An O-Chain topology must begin with edge ports. The ports with a smaller switch MAC address will serve as the backup link and RM LED will light up.

4.4 MRP

4.4.1 Introduction

MRP (Media Redundancy Protocol) is an industry standard for high-availability Ethernet networks. MRP allowing Ethernet switches in ring configuration to recover from failure rapidly to ensure seamless data transmission. A MRP ring (IEC 62439) can support up to 50 devices and will enable a back-up link in 80ms (adjustable to max. 200ms/500ms).

4.4.2 Configurations

MRP

<input checked="" type="checkbox"/> Enable			
<input type="checkbox"/>	<input type="checkbox"/> Manager		<input type="checkbox"/> React on Link Change
1st Ring Port	G1		Linkdown
2nd Ring Port	G2		Forwarding
<input type="checkbox"/> Force Speed/Duplex for 100BASE-TX			

Apply



Label	Description
Enable	Enables the MRP function
Manager	Every MRP topology needs a MRP manager. One MRP topology can only have a Manager. If two or more switches are set to be Manager, the MRP topology will fail.
React on Link Change (Advanced mode)	Faster mode. Enabling this function will cause MRP topology to converge more rapidly. This function only can be set in MRP manager switch.
1st Ring Port	Chooses the port which connects to the MRP ring
2nd Ring Port	Chooses the port which connects to the MRP ring
Force Speed / Duplex for 100BASE-TX	By default, this is in auto-negotiation mode. Enabling this function will automatically change the default to Full mode.(this function is used in combination with Hirschmann's switch as the MRP ring port speed/duplex of Hirschmann's switches are always in Full mode)

4.5 STP/RSTP/MSTP

4.5.1 STP/RSTP

STP (Spanning Tree Protocol), and its advanced versions RSTP (Rapid Spanning Tree Protocol) and MSTP (Multiple Spanning Tree Protocol), are designed to prevent network loops and provide network redundancy. Network loops occur frequently in large networks as when two or more paths run to the same destination, broadcast packets may get in to an infinite loop and hence causing congestion in the network. STP can identify the best path to the destination, and block all other paths. The blocked links will stay connected but inactive. When the best path fails, the blocked links will be activated. Compared to STP which recovers a link in 30 to 50 seconds, RSTP can shorten the time to 5 to 6 seconds. In other words, RSTP provides faster spanning tree convergence after a topology changes. The switch supports STP and will auto detect the connected device running on STP or RSTP protocols.

RSTP Repeater

A repeater can pass a BPDU packet directly from one RSTP device to another as if the two devices are connected.

RSTP-Repeater

<input type="checkbox"/> Enable		
	Uplink Port	RSTP Edge Port
1st	Port.01 ▾	<input type="checkbox"/>
2nd	Port.02 ▾	<input type="checkbox"/>

Label	Description
Enable	Check to enable RSTP Repeater
1st Ring Port	The first port connecting to the RSTP network
2nd Ring Port	The second port connecting to the RSTP network
Edge Port	Only the edge device (connected to RSTP device) needs to specify edge port. The user must specify the edge port according to topology of network.

RSTP Bridge Setting

RSTP - Bridge Setting

RSTP Mode	Enable ▾
Priority (0-61440)	32768
Max Age (6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15

Priority must be a multiple of 4096.
 $2 * (\text{Forward Delay Time} - 1)$ should be greater than or equal to the Max Age.
The Max Age should be greater than or equal to $2 * (\text{Hello Time} + 1)$.

Label	Description
RSTP mode	You must enable or disable RSTP function before configuring the related parameters.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the

	value changes, you must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule
Max Age Time(6-40)	The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. The valid value is between 6 through 40.
Hello Time (1-10)	The time interval a switch sends out the BPDU packet to check RSTP current status. The time is measured in seconds and the valid value is between 1 through 10.
Forwarding Delay Time (4-30)	The time of a port waits before changing from RSTP learning and listening states to forwarding state. The valid value is between 4 through 30.
Apply	Click to apply the configurations.

NOTE: the calculation of the MAX Age, Hello Time, and Forward Delay Time is as follows:
 $2 \times (\text{Forward Delay Time value} - 1) \geq \text{Max Age value} \geq 2 \times (\text{Hello Time value} + 1)$

The following pages show the information of the root bridge, including its port status.

Root Bridge Information

Bridge ID	8000001E94011E7A
Root Priority	32768
Root Port	ROOT
Root Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15

RSTP - Port Setting

Port	Path Cost (1-200000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non Stp
Port.01					
Port.02					
Port.03	200000	128	auto	true	false
Port.04					
Port.05					

priority must be a multiple of 16

Apply Help

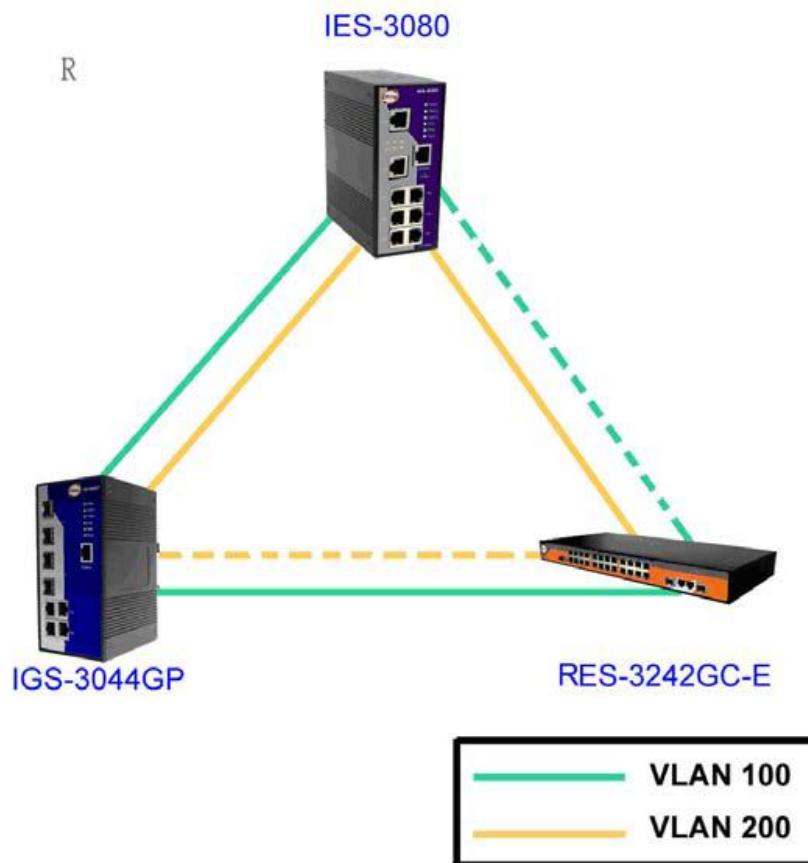
Port Status

Port	Path Cost	Port Priority	Oper P2P	Oper Edge	Stp Neighbor	State	Role
Port.01	200000	128	True	True	False	Disabled	Disabled
Port.02	200000	128	True	True	False	Disabled	Disabled
Port.03	200000	128	True	True	False	Disabled	Disabled
Port.04	200000	128	True	True	False	Disabled	Disabled
Port.05	200000	128	True	True	False	Disabled	Disabled

Label	Description
Path Cost (1-200000000)	The path cost incurred by the port. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range of valid values is 1 to 200000000.
Port Priority (0-240)	Decide which port should be blocked by priority in the LAN. The valid value is between 0 and 240, and must be a multiple of 16
Oper P2P	Configures the port connects to a point-to-point LAN rather than a shared medium. This can be configured automatically or set to true or false manually. True means P2P enabling. False means P2P disabling. Transiting to forwarding state is faster for point-to-point LANs than for shared media.
Oper Edge	A flag indicating whether the port is connected directly to edge devices or not (no bridges attached). Transiting to the forwarding state is faster for edge ports (operEdge set to true) than other ports.
STP Neighbor	The port uses mathematical calculations according to STP. True means not included in mathematical calculations, and False means contained in mathematical calculations according to STP.
State	Determines the STP state of the port
Role	When enabled, the port will not be selected as root port for CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an alternate port after the root port has been selected. If set, spanning trees will lose connectivity. It can be set by a network administrator to prevent bridges outside a core region of the network from influencing the active spanning tree topology because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
Apply	Click to apply the configurations.

4.5.2 MSTP

Since the recovery time of STP and RSTP takes seconds, which is unacceptable in industrial applications, MSTP was developed. The technology supports multiple spanning trees within a network by grouping and mapping multiple VLANs into different spanning-tree instances, known as MSTIs, to form individual MST regions. Each switch is assigned to an MST region. Hence, each MST region consists of one or more MSTP switches with the same VLANs, at least one MST instance, and the same MST region name. Therefore, switches can use different paths in the network to effectively balance loads.



Bridge Settings

This page allows you to examine and change the configurations of current MSTI ports. A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before MSTI port configuration options are displayed.

MSTP - Bridge Setting

MSTP Enable	Enable <input type="button" value="v"/>
Force Version	MSTP <input type="button" value="v"/>
Configuration Name	MSTP_SWITCH
Revision Level (0-65535)	0
Priority (0-61440)	32768
Max Age Time (6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15
Max Hops (1-40)	20

Priority must be a multiple of 4096.
 $2 * (\text{Forward Delay Time} - 1)$ should be greater than or equal to the Max Age.
 The Max Age should be greater than or equal to $2 * (\text{Hello Time} + 1)$.

Label	Description
MSTP Enable	Enables or disables MSTP function.
Force Version	Forces a VLAN bridge that supports RSTP to operate in an STP-compatible manner.
Configuration Name	The name which identifies the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configurations in order to share spanning trees for MSTIs (intra-region). The name should not exceed 32 characters.
Revision Level (0-65535)	Revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, you must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.
Max Age Time(6-40)	The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. The valid value is between 6 through 40.
Hello Time (1-10)	The time interval a switch sends out the BPDU packet to check RSTP current status. The time is measured in seconds and the valid value is between 1 through 10.

Forwarding Delay Time (4-30)	The time of a port waits before changing from RSTP learning and listening states to forwarding state. The valid value is between 4 through 30.
Max Hops (1-40)	An additional parameter for those specified for RSTP. A single value applies to all STP within an MST region (the CIST and all MSTIs) for which the bridge is the regional root.
Apply	Click to apply the configurations.

Bridge Port

MSTP - Bridge Port

Port No.	Priority (0-240)	Path Cost (1-200000000, 0:Auto)	Admin P2P	Admin Edge	Admin Non Stp
Port.01 <input type="button" value="▲"/> Port.02 <input type="button" value="□"/> Port.03 <input type="button" value="▼"/> Port.04 <input type="button" value="▲"/> Port.05 <input type="button" value="▼"/>	128	0	auto ▼	true ▼	false ▼

priority must be a multiple of 16

Label	Description
Port No.	The number of port you want to configure
Priority (0-240)	Decide which port should be blocked by priority in the LAN. The valid value is between 0 and 240, and must be a multiple of 16.
Path Cost (1-200000000)	The path cost incurred by the port. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range of valid values is 1 to 200000000.
Admin P2P	Configures whether the port connects to a point-to-point LAN rather than a shared medium. This can be configured automatically or set to true or false manually. True means P2P enabling. False means P2P disabling. Transitioning to forwarding state is faster for point-to-point LANs than for shared media.
Admin Edge	Specify whether this port is an edge port or a nonedge port. An edge port is not connected to any other bridge. Only edge ports and point-to-point links can rapidly transition to forwarding state. To configure the port as an edge port, set the port to True.
Admin Non STP	The port includes the STP mathematic calculation. True is not

	including STP mathematic calculation, false is including the STP mathematic calculation.
Apply	Click to apply the configurations.

Instance Setting

This page allows you to change the configurations of current MSTI bridge instance.

MSTP - Instance Setting

Instance	State	VLANs	Priority (0-61440)
1 <input type="button" value="v"/>	Enable <input type="button" value="v"/>	<input type="text" value="1-4094"/>	<input type="text" value="32768"/>

Priority must be a multiple of 4096.

Label	Description
Instance	Set the instance from 1 to 15
State	Enables or disables the instance
VLANs	The VLAN which is mapped to the MSTI. A VLAN can only be mapped to one MSTI. An unused MSTI will be left empty (ex. without any mapped VLANs).
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, you must reboot the switch. The value must be a multiple of 4096 according to the protocol standard
Apply	Click to apply the configurations.

Port Priority

This page allows you to change the configurations of current MSTI bridge instance priority.

MSTP - Instance Port

Instance: CIST

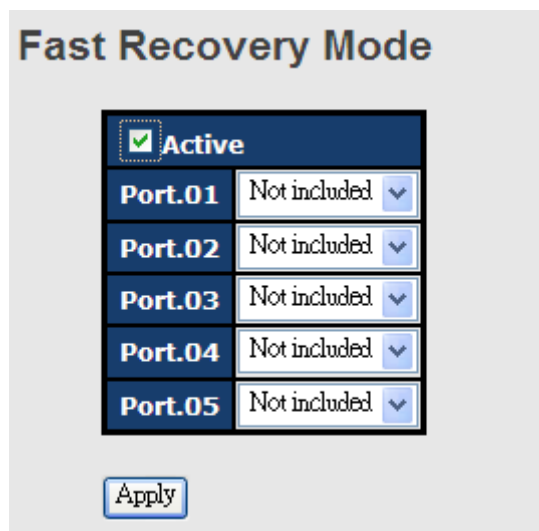
Port	Priority (0-240)	Path Cost (1-200000000, 0:Auto)
<input type="button" value="v"/> Port.01 <input type="button" value="v"/> Port.02 <input type="button" value="v"/> Port.03 <input type="button" value="v"/> Port.04 <input type="button" value="v"/> Port.05	<input type="text" value="128"/>	<input type="text" value="0"/>

Priority must be a multiple of 16

Label	Description
Instance	The bridge instance. CIST is the default instance, which is always active.
Port	The port number which you want to configure.
Priority (0-240)	Decides the priority of ports to be blocked in the LAN. The valid value is between 0 and 240, and must be a multiple of 16
Path Cost (1-20000000)	The path cost incurred by the port. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range of valid values is 1 to 200000000.
Apply	Click to apply the configurations.

4.6 Fast Recovery

Fast recovery mode can be set to connect multiple ports to one or more switches, thereby providing redundant links. Fast recovery mode supports 5 priorities. Only the first priority will be the active port, and the other ports with different priorities will be backup ports.



Label	Description
Active	Activate fast recovery mode
Port.01 - 05	Ports can be set to 5 priorities. Only the port with the highest priority will be the active port. 1st Priority is the highest.
Apply	Click to activate the configurations.

Management

The switch can be controlled via a built-in web server which supports Internet Explorer (Internet Explorer 5.0 or above versions) and other Web browsers such as Chrome. Therefore, you can manage and configure the switch easily and remotely. You can also upgrade firmware via a Web browser. The Web management function not only reduces network bandwidth consumption, but also enhances access speed and provides a user-friendly viewing screen.

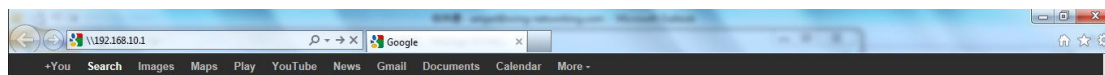
Note: By default, IE5.0 or later version do not allow Java applets to open sockets. You need to modify the browser setting separately in order to enable Java applets for network ports.

Management via Web Browser

Follow the steps below to manage your switch via a Web browser

System Login

1. Launch an Internet Explorer.
2. Type `http://` and the IP address of the switch. Press **Enter**.



3. A login screen appears.
4. Type in the username and password. The default username and password is **admin**.
5. Press **Enter** or click **OK**, the management page appears.



Note: you can use the following default values:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

Default Gateway: **192.168.10.254**



User Name: **admin**

Password: **admin**

After logging in, you will see the information of the switch as below.

System Information

System Name	IES-P3073GC
System Description	Industrial IEC 61850-3 10-port managed Ethernet switch with 7x10/100Base-T(X) and 3xGigabit combo ports, SFP socket
System Location	
System Contact	
SNMP OID	1.3.6.1.4.1.25972.100.0.0.133
Firmware Version	v1.01
Kernel Version	v3.08
MAC Address	00-22-3B-0A-0E-FD
System Uptime	0 Day(s) 0 Hour(s) 0 Min(s) 38 Sec(s)

On the right hand side of the management interface shows links to various settings. Clicking on the links will bring you to individual configuration pages.

5.1 Basic Settings

The Basic Settings page allows you to configure the basic functions of the switch.

5.1.1 System Information

This page shows the general information of the switch.

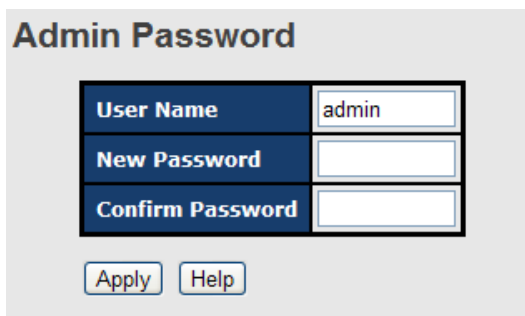
System Setting

System Name	IES-P3073GC
System Description	Industrial IEC 61850-3 10-port managed Ethernet switch with 7x10/100Base-T(X) a
System Location	
System Contact	

Label	Description
System Name	An administratively assigned name for the managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string consisting of alphabets (A-Z, a-z), digits (0-9), and minus sign (-). Space is not allowed to be part of the name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
System Description	Description of the device
System Location	The physical location of the node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and only ASCII characters from 32 to 126 are allowed.
System 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 only ASCII characters from 32 to 126 are allowed.
System Timezone offset(minutes)	Provides the time-zone offset from UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.2 Admin & Password

This page allows you to configure the system password required to access the web pages or log in from CLI.

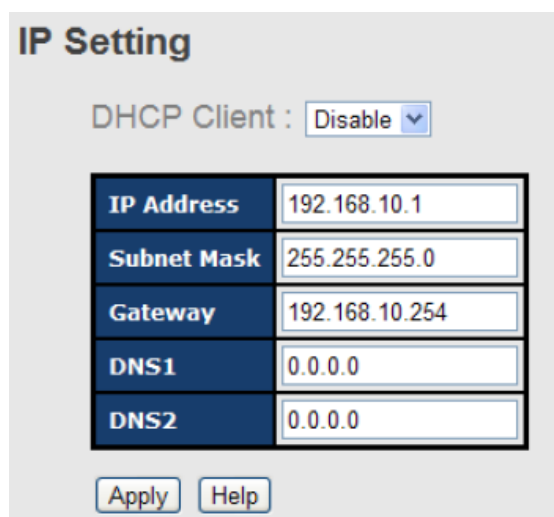


Label	Description
User name	The account name you use to log into the system (the default is admin)

New Password	The new system password. The allowed string length is 0 to 31, and only ASCII characters from 32 to 126 are allowed.
Confirm password	Re-type the new password.
Apply	Click to activate the configurations.

5.1.3 IP Settings

This page allows you to configure IP information for the switch. You can configure the settings manually by disabling DHCP Client. After inputting the values, click **Apply** and the new values will be applied.



IP Setting

DHCP Client :

IP Address	<input type="text" value="192.168.10.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.10.254"/>
DNS1	<input type="text" value="0.0.0.0"/>
DNS2	<input type="text" value="0.0.0.0"/>

Label	Description
DHCP Client	Enables or disables the DHCP client. If DHCP fails or the configured IP address is zero, DHCP will retry. If DHCP retry fails, DHCP will stop trying and the configured IP settings will be used.
IP Address	Assigns the IP address of the network in use. If DHCP client function is enabled, you do not need to assign the IP address. The network DHCP server will assign an IP address to the switch and it will be displayed in this column. The default IP is 192.168.10.1 .
Subnet Mask	Assigns the subnet mask of the IP address. If DHCP client function is enabled, you do not need to assign the subnet mask.
Gateway	Assign the network gateway for the switch. The default gateway is 192.168.10.254.
DNS1	Assign the primary DNS IP address
DNS2	Assign the secondary DNS IP address
Apply	Click to apply the changes

5.1.4 Time Settings

This page allows you to configure SNTP and system clock.

System Clock

The system clock synchronizes the tasks in a computer, like loading data before manipulating it.

Time Setting

System Clock

System Clock	Thu Jan 01 1970 00:39:12 GMT+0800 (台北標準時間)		
System Date (YYYY/MM/DD)	2012	Jun	22
System Time (hh:mm:ss)	15	: 43	: 42

Label	Description
System clock	Shows the current system time. The time stamp could be assigned manually configuration or automatically by a SNTP server.
System Date	Specifies the year, month and day of the system clock (YYYY/MM/DD). Year: 2006-2015. Month: Jan-Dec. Day:1-31(28)
System Time	Specify the hour, minute and second of the system clock (hh:mm:ss). Hour:0-24, Minute:0-59, Second:0-59

SNTP

SNTP (Simple Network Time Protocol) is a protocol able to synchronize the time on your system to the clock on the Internet. It will synchronize your computer system time with a server that has already been synchronized by a source such as a radio, satellite receiver or modem.

SNTP Client :

UTC Timezone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
SNTP Server Address	0.0.0.0

Daylight Saving Time :

Daylight Saving Period	2012 Jun 22 07 ~
Daylight Saving Offset	0 (hours)



Label	Description
SNTP Client	Enables or disables SNTP function to retrieve the time from a SNTP server.
UTC Time zone	Selects the time zone for the switch according to its location
SNTP Sever Address	Enters the SNTP server IP address which you would like to use for time synchronization.
Daylight Saving Time	Enables or disables daylight saving time function. When it is enabled, you need to configure the daylight saving time period.
Daylight Saving Period	Configures the beginning and ending time for the daylight saving option. The values will vary each year.
Daylight Saving Offset	Configures the offset time.
Apply	Click to apply the changes

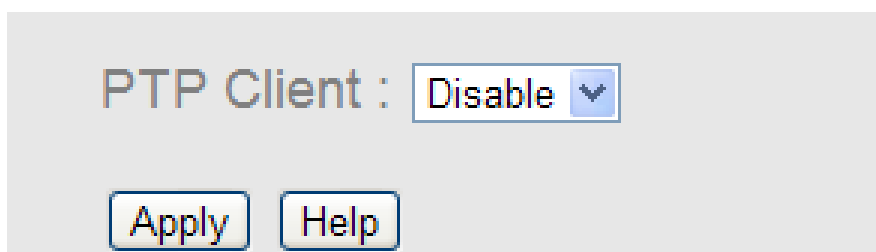
The following table lists different location time zones for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11 am
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	+1 hour	1 pm

Winter		
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	+10 hours	10 pm
Standard GST Guam Standard, USSR Zone 9		
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

PTP Client

The Precision Time Protocol (PTP) is a time-transfer protocol defined in the IEEE 1588-2002 standard that allows precise synchronization of networks (e.g., Ethernet). Accuracy within the nanosecond range can be achieved with this protocol when using hardware generated timestamps.



Label	Description
PTP Client	Enables or disables PTP Client

5.1.5 LLDP

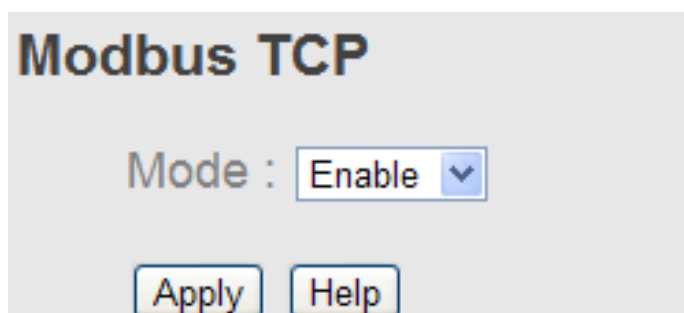
LLDP (Link Layer Discovery Protocol) provides a method for networked devices to receive and/or transmit their information to other connected devices on the network that are also using the protocols, and to store the information that is learned about other devices. This page allows you to examine and configure current LLDP port settings.



Label	Description
LLDP Protocol	Enables or disables LLDP function.
LLDP Interval	The interval of resending LLDP (30 seconds by default)
Apply	Click to apply the configurations.
Help	Shows help file.
Neighbor info table	Shows neighbor device info, including system name, MAC address, and IP address.

5.1.6 Modbus TCP

Modbus TCP uses TCP/IP and Ethernet to carry the data of the Modbus message structure between compatible devices. The protocol is commonly used in SCADA systems for communications between a human-machine interface (HMI) and programmable logic controllers. This page enables you to enable and disable Modbus TCP support of the switch.



Label	Description
Mode	Enables or disables Modbus TCP function

Auto Provision

Auto Provision allows you to update switch firmware automatically. You can put the firmware or configuration file on a TFTP server. When you reboot the switch, it will upgrade firmware automatically. Before updating, make sure you have your TFTP server ready and the firmware image and configuration files are on the TFTP server.

Auto Provision

Auto install configuration file from TFTP server?

TFTP Server IP Address	192.168.10.66
Configuration File Name	data.bin

Auto install firmware image file from TFTP server?

TFTP Server IP Address	192.168.10.66
Firmware File Name	image.bin

5.1.7 Backup/Restore

You can save current values from the switch to a TFTP server, and restore the switch to the settings by going to the TFTP restore configuration page.

The following page allows you to save the existing configurations as a backup file to a TFTP server.

Backup Configuration

To TFTP Server

TFTP Server IP Address	192.168.10.2
Backup File Name	data.bin

To Local PC

The following page allows you to restore the system to previous configurations from a TFTP server.

Restore Configuration

From TFTP Server

TFTP Server IP Address	192.168.10.2
Restore File Name	data.bin

From Local PC

Label	Description
TFTP Server IP Address	The IP address of the TFTP where you put the configuration file or where you want to restore the switch to previous settings.
Backup File Name	The name of the configuration file you want to save as.
Restore File Name	The name of the configuration file you want to use for the switch.
Backup	Click to back up the configurations.
To Local PC	You can save the configuration file to your PC instead of a TFTP server.
Restore	Click to restore the configurations.
Form Local PC	You can use the file stored on a local PC instead of from the TFTP server. Click Browse to locate the file you want to use for update, and then click Restore .

5.1.8 Firmware Update

This page allows you to update the firmware of the switch. Before updating, make sure you have your TFTP server ready and the firmware file is on the TFTP server. Enter the IP address of the TFTP server you want to connect to and the firmware file name, and then click upgrade to start upgrading. You can also choose the firmware file from your PC.

Upgrade Firmware

From TFTP Server

TFTP Server IP	192.168.10.2
Firmware File Name	image.bin

From Local PC

5.2 Multicast

5.2.1 IGMP Snooping

IGMP (Internet Group Management Protocol) snooping monitors the IGMP traffic between hosts and multicast routers. The switch uses what IGMP snooping learns to forward multicast traffic only to interfaces that are connected to interested receivers. This conserves bandwidth by allowing the switch to send multicast traffic to only those interfaces that are connected to hosts that want to receive the traffic, instead of flooding the traffic to all interfaces in the VLAN. This page allows you to set up IGMP snooping configurations.

IGMP Snooping

IGMP Snooping :

IGMP Query Mode:

IGMP Snooping Table

IP Address	VLAN ID	Member Port
230.0.0.20	1	Port.07

Label	Description
IGMP Snooping	Check to enable global IGMP snooping
IGMP Query Mode	Configures the switch to be the IGMP querier. Only one IGMP querier is allowed in an IGMP application. Auto will select the switch with the lowest IP address as the querier.
Apply	Click to apply the configurations.
Help	Shows help file.

5.2.2 MVR

MVR (Multicast VLAN registration) enables hosts that are not part of a multicast VLAN to receive multicast streams from the multicast VLAN. As a result, the multicast VLAN can be shared across the network and there is no need to send duplicate multicast streams to each requesting VLAN in the network.

MVR

MVR Mode:

MVR VLAN:

Port	Type	Immediate Leave
Port.01	Inactive	<input type="checkbox"/>
Port.02	Inactive	<input type="checkbox"/>
Port.03	Inactive	<input type="checkbox"/>
Port.04	Inactive	<input type="checkbox"/>
Port.05	Inactive	<input type="checkbox"/>
Port.06	Inactive	<input type="checkbox"/>
Port.07	Inactive	<input type="checkbox"/>

Label	Description
MVR Mode	Enables or disables MVR
MVR VLAN	The number of MVR VLANs
Type	Indicates the MVR type of the port. Inactive means the port is not participating in any MVR groups.
Immediate Leave	Check to enables immediate leave function. Immediate leave reduces the length of time it takes the switch to stop forwarding multicast traffic when the last member host on the interface leaves the group.

5.2.3 Static Multicast Filtering

Static multicast filtering provides a method for users to configure multicast group memberships manually. The function enables end devices to receive multicast traffic only if they register to join specific multicast groups. With static multicast filtering, network devices only forward multicast traffic to the ports connected to registered end devices. The function allows you to control the multicast traffic precisely.

Static Multicast Filtering

Multicast IP Address :

Member Ports :

Port.01 Port.02 Port.03 Port.04
 Port.05 Port.06 Port.07 G1
 G2 G3

	IP Address	Member Ports
<input type="checkbox"/>	230.0.0.6	Port.04, Port.05

Label	Description
Multicast IP Address	Assigns a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255
Member Ports	Check the box next to the port number to include them as member ports in the specific multicast group.
Add	Click to add the ports to the IP multicast list
Delete	Deletes an entry from the table
Help	Shows help file.

5.3 Port Setting

Port Setting allows you to manage individual ports of the switch, including speed/duplex, flow control, and security.

5.3.1 Port Control

Port Control

Port No.	State	Speed/Duplex	Flow Control	Security
Port.01	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.02	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.03	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.04	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.05	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.06	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.07	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
G1	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
G2	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
G3	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼

Auto Detect 100/1000 SFP
Enable ▼

Label	Description
Port NO.	The number of the port to be configured.
State	Enables or disables the port.
Speed/Duplex	Available values include auto-negotiation , 100-full , 100-half , 10-full , or 10-half
Flow Control	Supports symmetric and asymmetric modes to avoid packet loss when congestion occurs
Security	Enabling port security will disable MAC address learning in this port. Thus only the frames with MAC addresses in the port security list will be forwarded, otherwise will be discarded.
Auto Detect 100/1000	Automatically detects SFP port speed (100M / 1000M)
Apply	Click to apply the configurations

5.3.2 Port Status

This page shows the status of the each port in terms of its state, speed/duplex, and flow

control.

Port Status

Port No.	Type	Link	State	Speed/Duplex	Flow Control
Port.01	100TX	Down	Enable	N/A	N/A
Port.02	100TX	Down	Enable	N/A	N/A
Port.03	100TX	Down	Enable	N/A	N/A
Port.04	100TX	Down	Enable	N/A	N/A

5.3.3 Port Alias

This page provides alias IP address configuration. Some devices might have more than one IP addresses. You could specify other IP addresses here.

Port Alias

Port No.	Port Alias
Port.01	
Port.02	
Port.03	
Port.04	
Port.05	

5.3.4 Rate Limit

This page allows you to define the rate limits applied to a port, including incoming and outgoing traffic.

Rate Limit

Port No.	Ingress Limit Frame Type	Ingress	Egress
Port.01	All	0 kbps	0 kbps
Port.02	All	0 kbps	0 kbps
Port.03	All	0 kbps	0 kbps
Port.04	All	0 kbps	0 kbps
Port.05	All	0 kbps	0 kbps

Label	Description
Ingress Limit Frame Type	Valid values include All , Broadcast only , Broadcast/Multicast and Broadcast/Multicast/Flooded Unicast .
Ingress	The transmission rate for incoming traffic
Egress	The transmission rate for outgoing traffic
Apply	Click to activate the configurations.

5.3.5 Port Trunk

A port trunk is a group of ports that have been grouped together to function as one logical path. This method provides an economical way for you to increase the bandwidth between the switch and another networking device. In addition, it is useful when a single physical link between the devices is insufficient to handle the traffic load. This page allows you to configure the aggregation hash mode and the aggregation group.

Port Trunk - Setting

Port No.	Group ID	Type
Port.01	None	Static
Port.02	None	Static
Port.03	None	Static
Port.04	None	Static
Port.05	None	Static
Port.06	None	Static
Port.07	None	Static
G1	None	Static
G2	None	Static
G3	None	Static

802.3ad LACP Work Ports

Group ID	Work Ports
Trunk1	max
Trunk2	max
Trunk3	max
Trunk4	max
Trunk5	max

Label	Description
Group ID	Indicates the ID of each aggregation group. None means no aggregation. Only one group ID is valid per port.
Type	The switch supports two types of link aggregation; static and 802.3ad LACP. Static trunks are manually configured, while LACP-configured ports will automatically negotiate a trunk with LACP-configured ports on another device.

Work Ports	The total number of active ports in a dynamic trunk group. The default value of works ports is Max . In a dynamic trunk group, if the number of work ports is lower than the number of members of the trunk group, the exceed ports are standby/redundant ports and can be aggregated if working ports fail. If it is a static trunk group, the number of work ports must equal the total number of group member ports.
Apply	Click to activate the configurations.

Port Trunk - Status

Group ID	Trunk Member	Type
Trunk 1	N/A	Static
Trunk 2	N/A	Static
Trunk 3	N/A	Static
Trunk 4	N/A	Static
Trunk 5	N/A	Static

Label	Description
Group ID	Indicates the ID of each aggregation group. None means no aggregation. Only one group ID is valid per port.
Trunk Member	Lists members of a specific trunk group.
Type	Indicates the type of the port trunk

5.3.6 Loop Guard

This feature prevents loop attack. When receiving loop packets, the port will be disabled automatically, preventing the loop attack from affecting other network devices.

Loop Guard

Port No.	Active	Port State
Port.01	<input type="checkbox"/>	Enable
Port.02	<input type="checkbox"/>	Enable
Port.03	<input type="checkbox"/>	Enable

Label	Description
Active	Check to enable Loop Guard
Port Status	Indicates the enabled/disabled status of the port.

5.3.7 VLAN

VLAN Setting - IEEE 802.1Q

A VLAN (Virtual LAN) is a logical LAN based on a physical LAN with links that does not consist of a physical (wired or wireless) connection between two computing devices but is implemented using methods of network virtualization. A VLAN can be created by partitioning a physical LAN into multiple logical LANs using a VLAN ID. You can assign switch ports to a VLAN and add new VLANs in this page.

VLAN Setting

VLAN Operation Mode :

GVRP Mode :

Management VLAN ID :

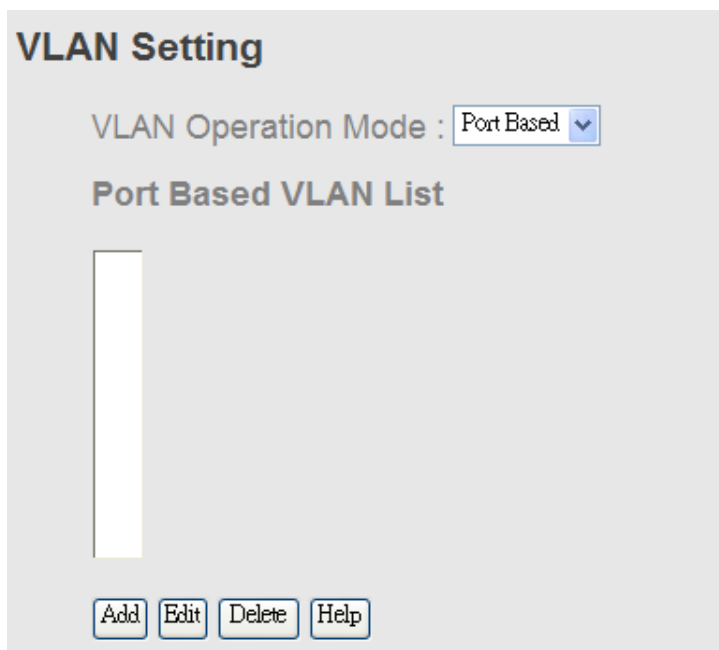
Port VLAN Setting

Port No.	Link Type	PVID	Untagged VIDs	Tagged VIDs
Port.01	Access	1	1	
Port.02	Access	1	1	
Port.03	Access	1	1	

Label	Description
VLAN Operation Mode	Available options include Disable , Port Base , and 802.1Q
GVRP Mode	GVRP is a GARP application that provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. With GVRP, the switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q trunk ports.
Management VLAN ID	The VLAN ID for the entry.
Link type	Three link types are available: Access Link: An access link connects a VLAN-unaware device to the port of a VLAN-aware bridge. All frames on access links must be implicitly tagged (untagged). Trunk Link: All the devices connected to a trunk link, including workstations, must be VLAN-aware. All frames on a trunk link must have a special header attached. Hybrid Link: The combination of Access Link and Trunk Link.

	<p>This is a link where both VLAN-aware and VLAN-unaware devices are attached. It can have both tagged and untagged frames, but all the frames for a specific VLAN must be either tagged or untagged.</p> <p>Hybrid(QinQ) Link: Allows one more VLAN tag in an original VLAN frame.</p>
Untagged VID	Set the port default VLAN ID for untagged devices that connect to the port. The range is 1 to 4094.
Tagged VIDs	Set the tagged VIDs to carry different VLAN frames to other switch.
Apply	Click to set the configurations.

VLAN Setting – Port based



Label	Description
VLAN Operation Mode	Available options include Disable , Port Base , and 802.1Q
Add	Click to start adding a VLAN
Edit	Edits existing VLANs
Delete	Deletes existing VLANs
Help	Shows help file.

VLAN Setting

VLAN Operation Mode : Port Based ▾

Group Name:

VLAN ID:

Port.01
Port.02
Port.03
Port.04
Port.05
Port.06
Port.07
G1
G2
G3

Label	Description
VLAN Operation Mode	Available options include Disable , Port Base , and 802.1Q
Group Name	The name of the VLAN that you want to change settings.
VLAN ID	The number of the VLAN
Add	Select ports from the left column and clicks Add to include them to the VLAN group
Remove	Remove ports from the VLAN group
Apply	Click to apply the configurations
Help	Shows help file.

5.4 Traffic Prioritization

With traffic prioritization schemes, the switch can transmit data based on its importance, thereby ensuring mission-critical applications, such as VoIP and video teleconferencing, have sufficient bandwidth for transmission when the network is congested.

QoS (Quality of Service) is a method to achieve efficient bandwidth utilization between devices by prioritizing frames according to individual requirements and transmit the frames based on their importance. Frames in higher priority queues receive a bigger slice of bandwidth than those in a lower priority queue.

5.4.1 QoS Policy

Policing is a traffic regulation mechanism for limiting the rate of traffic streams, thereby

controlling the maximum rate of traffic sent or received on an interface. When the traffic rate exceeds the configured maximum rate, policing drops or remarks the excess traffic. This page allows you to configure QoS policies for the switch.

Policy

QoS Mode : Disable ▼

QoS Policy :

Use an 8,4,2,1 weighted fair queuing scheme
 Use a strict priority scheme

Apply
Help

Label	Description
QOS Mode	Available modes include: Disable: disables the mode Port-base: the output priority is determined by ingress port. COS only: the output priority is determined by COS only. TOS only: the output priority is determined by TOS only. COS first: the output priority is determined by COS and TOS, but COS first. TOS first: the output priority is determined by COS and TOS, but TOS first.
QOS policy	Using the 8,4,2,1 weight fair queue scheme: the output queues will use an 8:4:2:1 ratio to transmit packets from the highest to lowest queue. For example: 8 high queue packets, 4 middle queue packets, 2 low queue packets, and the one lowest queue packets are transmitted in one turn. Use the strict priority scheme: when traffic arrives at the device, traffic on the highest priority queue will be transmitted first, followed by traffic on lower priorities. If there is always some content in the highest priority queue, then the other packets in the rest of queues will not be sent until the highest priority queue is empty.
Apply	Click to apply the configurations
Help	Shows help file.

5.4.2 Port-base priority

Port-based Priority

Port No.	Priority
Port.01	Lowest
Port.02	Lowest
Port.03	Lowest
Port.04	Lowest
Port.05	Lowest
Port.06	Lowest
Port.07	Lowest
Port.08	Lowest

Label	Description
Priority	Assigns a port to a priority queue. Four priority queues are available: High , Middle , Low , and Lowest .
Apply	Click to apply the configurations
Help	Shows help file.

5.4.3 COS/802.1p

COS (Class of Service), also known as 802.1p, is a parameter for differentiating the types of payloads contained in the packet to be transmitted. CoS operates only on 802.1Q VLAN Ethernet at Layer 2, while other QoS mechanisms operate at the Layer 3 or use a local QoS tagging system that does not modify the actual packet. COS supports up to 7 priorities and 4 priority queues: High, Middle, Low, and Lowest. When an ingress packet has no VLAN tag, the default priority value will be used.

COS/802.1p		COS Port Default	
COS	Priority	Port No.	COS
0	Lowest	Port.01	0
1	Lowest	Port.02	0
2	Low	Port.03	0
3	Low	Port.04	0
4	Middle	Port.05	0
5	Middle	Port.06	0
6	High	Port.07	0
7	High		

Label	Description
Priority	Assigns a port to a priority queue. Four priority queues are available: High, Middle, Low, and Lowest.
Apply	Click to apply the configurations
Help	Shows help file.

5.4.4 TOS/DSCP

TOS (Type of Service) is a field in the IP header of a packet. It is used by Differentiated Services and is called the DSCP (Differentiated Services Code Point). The output priority of a packet can be determined by this field and the supported priority value ranges from 0 to 63. DSCP supports four priority queues: High, Middle, Low, and Lowest.

TOS/DSCP

DSCP	0	1	2	3	4	5	6	7
Priority	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
DSCP	8	9	10	11	12	13	14	15
Priority	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
DSCP	16	17	18	19	20	21	22	23
Priority	Low ▾	Low ▾	Low ▾	Low ▾	Low ▾	Low ▾	Low ▾	Low ▾
DSCP	24	25	26	27	28	29	30	31
Priority	Low ▾	Low ▾	Low ▾	Low ▾	Low ▾	Low ▾	Low ▾	Low ▾
DSCP	32	33	34	35	36	37	38	39
Priority	Middle ▾	Middle ▾	Middle ▾	Middle ▾	Middle ▾	Middle ▾	Middle ▾	Middle ▾
DSCP	40	41	42	43	44	45	46	47
Priority	Middle ▾	Middle ▾	Middle ▾	Middle ▾	Middle ▾	Middle ▾	Middle ▾	Middle ▾
DSCP	48	49	50	51	52	53	54	55
Priority	High ▾	High ▾	High ▾	High ▾	High ▾	High ▾	High ▾	High ▾
DSCP	56	57	58	59	60	61	62	63
Priority	High ▾	High ▾	High ▾	High ▾	High ▾	High ▾	High ▾	High ▾

Label	Description
Priority	Assigns a port to a priority queue. Four priority queues are available: High, Middle, Low, and Lowest.
Apply	Click to apply the configurations
Help	Shows help file.

5.5 DHCP Server

The switch provides DHCP server functions. By enabling DHCP, the switch will become a DHCP server and dynamically assigns IP addresses and related IP information to network

clients.

5.5.1 Basic Settings

This page allows you to set up DHCP settings for the switch. You can check the **Enabled** checkbox to activate the function. Once the box is checked, you will be able to input information in each column.

DHCP Server - Basic Setting

DHCP Server :

Low IP Address	<input type="text" value="192.168.10.2"/>
High IP Address	<input type="text" value="192.168.10.200"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.10.254"/>
DNS	<input type="text" value="0.0.0.0"/>
Lease Time (sec)	<input type="text" value="604800"/>

Label	Description
DHCP Server	Enables or disables DHCP server function. When enabled, the switch will become the DHCP server on your local network.
Low IP Address	The beginning of the dynamic IP address range. The lowest IP address in the range is considered the start IP address. For example, if the range is from 192.168.1.100 to 192.168.1.200, 192.168.1.100 will be the start IP address.
High IP Address	The end of the dynamic IP address range. The highest IP address in the range is considered the end IP address. For example, if the range is from 192.168.1.100 to 192.168.1.200, 192.168.1.200 will be the end IP address
Subnet Mask	The subnet mask for the dynamic IP assign range
Gateway	The gateway of your network
DNS	The DNS IP of your network
Lease Time (sec)	The length of time that the client may use the IP address it has been assigned. The time is measured in seconds.
Apply	Click to apply the configurations

5.5.2 Client List

When DHCP server functions are activated, the switch will collect DHCP client information and display it in the following table.

DHCP Server - Client List

IP addr	Client ID	Type	Status	Lease
192.168.10.2	00:1E:94:3A:04:B0	dynamic	DHCPOffer	604798

5.5.3 Port and IP Bindings

You can assign a specific IP address within the dynamic IP range to a specific port. When a device is connected to the port and requests for dynamic IP assigning, the switch will assign the IP address that has previously been assigned to the connected device.

DHCP Server - Port and IP Binding

Port	IP
Port.01	192.168.10.123
Port.02	0.0.0.0
Port.03	0.0.0.0
Port.04	0.0.0.0
Port.05	0.0.0.0

5.5.4 DHCP Relay Agent

The DHCP relay agent relays DHCP messages between clients and servers for DHCP on different subnet domain. DHCP relay agent use Option 82 to insert specific information into a request that is being forwarded to a DHCP server, and according to Option 82 to remove the specific information from a reply packets when forwarding server DHCP packets to a DHCP client.

DHCP Relay Agent

Mode :

DHCP Server IP Address

1st Server IP	<input type="text" value="0.0.0.0"/>	VID	<input type="text" value="1"/>
2nd Server IP	<input type="text" value="0.0.0.0"/>	VID	<input type="text" value="1"/>
3rd Server IP	<input type="text" value="0.0.0.0"/>	VID	<input type="text" value="1"/>
4th Server IP	<input type="text" value="0.0.0.0"/>	VID	<input type="text" value="1"/>

DHCP Option 82 Remote ID

Type	<input type="text" value="IP"/>
Value	<input type="text" value="192.168.10.1"/>
Display	<input type="text" value="COA80A01"/>

DHCP Option 82 Circuit-ID Table

Port No.	Circuit-ID	Option 82
Port.01	000400010001	<input type="checkbox"/>
Port.02	000400010002	<input type="checkbox"/>
Port.03	000400010003	<input type="checkbox"/>
Port.04	000400010004	<input type="checkbox"/>
Port.05	000400010005	<input type="checkbox"/>
Port.06	000400010006	<input type="checkbox"/>

Label	Description
DHCP Relay	Enable/Disable DHCP Relay Agent.
DHCP Server IP Address and VID	Specify the IP address and VID of DHCP server. Keep "0.0.0.0" means server is inactive.
DHCP Option 82 Remote ID	"Option 82 Remote ID" provides a identifier for the remote server. There are 4 types supported: IP, MAC, Client-ID, and Other.
DHCP Option 82 Circuit-ID Table	"Option 82 Circuit-ID" encodes an agent-local identifier of the circuit from which a DHCP client-to-server packet was received. It is intended for use by agents in relaying DHCP responses back to the proper circuit.
Apply	Click " Apply " to set the configurations.

5.6 SNMP

SNMP (Simple Network Management Protocol) is a protocol for managing devices on IP networks. It is mainly used network management systems to monitor the operational status of

networked devices. In an event-triggered situation, traps and notifications will be sent to administrators.

5.6.1 SNMP Agent

An SNMP agent will receive and process requests, send responses to the manager, and send traps when an event occurs. The following page allows you to configure the SNMP agent for the switch.

SNMP - Agent Setting

SNMP Agent Version SNMPV1/V2c ▼

Apply

SNMP V1/V2c Community

Community String	Privilege
<input style="width: 90%;" type="text" value="public"/>	Read Only ▼
<input style="width: 90%;" type="text" value="private"/>	Read and Write ▼
<input style="width: 90%;" type="text"/>	Read Only ▼
<input style="width: 90%;" type="text"/>	Read Only ▼

Apply

Label	Description
SNMP Agent Version	The column shows the version of the SNMP agent used by the switch. Three SNMP versions are supported, including SNMP V1 , SNMP V2c , and SNMP V3 . SNMP V1/SNMP V2c agents use a community string to authenticate the SNMP management station and SNMP agent. SNMP V3 requires MD5 or DES authentication which will encrypt data for higher data security.
Community String	The default community string that provides monitoring or read capability is often public . The default management or write community string is often private . Do not leave the community string to public on any of your SNMP agents. Since anyone with SNMP manager software installed on his/her PC can make changes to your SNMP agents, this will expose your SNMP agent to any SNMP management station.

Privilege	<p>Choose the appropriate access level from the dropdown list.</p> <p>Read Only: The community string can only read the values of MIB objects.</p> <p>Write Only: The community string can read and write the values of MIB objects.</p> <p>Read and Write: The community string can read and write the values of MIB objects and send MIB object values for a trap and inform messages.</p>
Apply	Click to apply the configurations

5.6.2 SNMP Trap

SNMP traps are event reports sent to a list of managers configured to receive event notifications when an error occurs. SNMP traps provide the value of one or more instances of management information. A trap manager is a management station that receives traps. If no trap manager is defined, no traps will be issued. You can create a trap manager by entering the IP address of the station and a community string.

SNMP - Trap Setting

Trap Server Setting

Server IP	<input style="width: 90%;" type="text"/>
Community	<input style="width: 90%;" type="text"/>
Trap Version	<input checked="" type="radio"/> V1 <input type="radio"/> V2c

Trap Server Profile

Server IP	Community	Trap Version
(none)		

Label	Description
Server IP	The IP address of the server to receive traps
Community	The community string for authentication



Trap Version	The trap version. V1 and V2c are supported.
Add	Click to add the trap sever to the trap server profile.
Trap Server Profile	Shows a list of trap servers, including their community strings and trap versions.
Remove	Click to remove a trap server from the profile

5.6.3 SNMPV3

Unlike SNMP v1 and v2 which uses community strings for authentication, SNMP v3 uses username/password authentication, along with an encryption key. Therefore, SNMPv3 provides greater security features for authentication, privacy, and access control. The switch supports SNMP v3 which can be configured in the following page.

NMP - SNMPv3 Setting

SNMPv3 Engine ID: f465000003001e940a002b

Context Table

Context Name :

User Table

Current User Profiles : <input type="button" value="Remove"/>	New User Profile : <input type="button" value="Add"/>	
(none)	User ID:	<input type="text"/>
	Authentication Password:	<input type="text"/>
	Privacy Password:	<input type="text"/>

Group Table

Current Group content : <input type="button" value="Remove"/>	New Group Table: <input type="button" value="Add"/>	
(none)	Security Name (User ID):	<input type="text"/>
	Group Name:	<input type="text"/>

Current Access Tables :	New Access Table :	
Remove	Add	
(none)	Context Prefix:	<input type="text"/>
	Group Name:	<input type="text"/>
	Security Level:	<input type="radio"/> NoAuthNoPriv. <input type="radio"/> AuthNoPriv. <input type="radio"/> AuthPriv.
	Context Match Rule	<input type="radio"/> Exact <input type="radio"/> Prefix
	Read View Name:	<input type="text"/>
	Write View Name:	<input type="text"/>
	Notify View Name:	<input type="text"/>

MIBView Table

Current MIBTables :	New MIBView Table :	
Remove	Add	
(none)	View Name:	<input type="text"/>
	SubOid-Tree:	<input type="text"/>
	Type:	<input type="radio"/> Excluded <input type="radio"/> Included

Note:
 Any modification of SNMPv3 tables might cause MIB accessing rejection. Please take notice of the causality between the tables before you modify these tables.

Label	Description
Context Table	Context is a collection of management information accessible by a SNMP entity and is stored in the context table. You can assign a context name to the context table and click Apply to change the name.
User Table	<p>You can manage existing and add new user profiles in this section. In Current User Profiles, select an entry you want to remove and click Remove. In New User Profiles, specify the following information of a new entry:</p> <p>User ID: the username of the user</p> <p>Authentication Password: the authentication password for the user</p> <p>Privacy Password: the private password for the user</p> <p>Click Add after inputting the information.</p>
Group Table	You can manage existing and add new group content in this section. In Current Group Content, select an entry you want to remove and click Remove . In New Group Table, specify the following information for a new entry:

	<p>Security Name (User ID): the name of the user to be added to the table.</p> <p>Group Name: the name of the group</p> <p>Click Add after inputting the information.</p>
<p>Access Table</p>	<p>The Access table lists the access rights and restrictions of the various groups. 1. You can manage existing and add new tables in this section. In Current Access Tables, select an entry you want to remove and click Remove. In New Access Table, specify the following information for a new entry:</p> <p>Context Prefix: the context name of the user as defined in the context table.</p> <p>Group Name: set up the group.</p> <p>Security Level: the security level of the user</p> <p>Context Match Rule: the rule for matching context</p> <p>Read View Name: the read view name provided for the v3 user</p> <p>Write View Name: the write view name provided for the v3 user.</p> <p>Notify View Name: the notify view name provided for the v3 user.</p> <p>Click Add after inputting the information.</p>
<p>MIBview Table</p>	<p>You can configure MIB views for users and groups by entering the OID number of the MIB view. A MIB view consists of a family of view subtrees which may be individually included in or (occasionally) excluded from the view. Each view subtree is defined by a combination of an OID subtree together with a bit string mask. The view table is indexed by the view name and subtree OID values.</p> <p>In New MIBview Table, enter the following information:</p> <p>ViewName: the name of the view</p> <p>Sub-Oid Tree: fill in the Sub OID.</p> <p>Type: select the type as excluded or included.</p> <p>Click Add after inputting the information.</p>

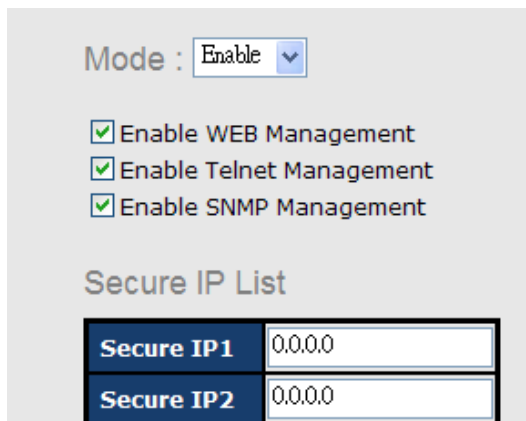
5.6.4 Security

The switch supports five security functions: IP security, port security, MAC blacklist, static MAC Forwarding, and 802.1x protocol.

IP Security

By setting up a secure IP list, only IP addresses in the list can manage the switch according to

the management mode you have specified (WEB, Telnet, SNMP, etc.).



Mode : ▾

Enable WEB Management
 Enable Telnet Management
 Enable SNMP Management

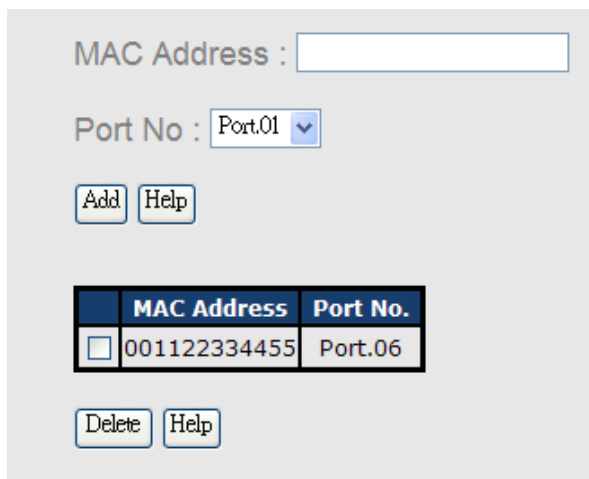
Secure IP List

Secure IP1	<input type="text" value="0.0.0.0"/>
Secure IP2	<input type="text" value="0.0.0.0"/>

Label	Description
Mode	Indicates IP security mode. Enables or disables IP security functions.
Enable WEB Management	Check to enable WEB management
Enable Telnet Management	Check to enable Telnet management
Enable SNMP Management	Check to enable MPSN management
Apply	Click to apply the configurations.
Help	Shows help file.

Static MAC Forwarding

You can use static MAC addresses to provide port security for the switch. With this method, only the frames with the MAC addresses in this list will be forwarded, otherwise will be discarded.



MAC Address :

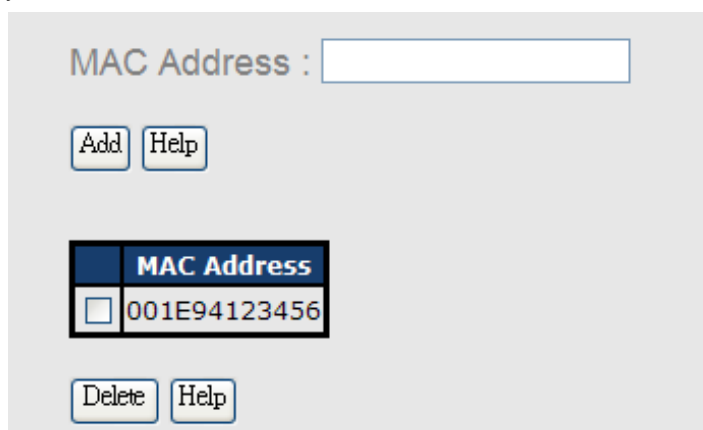
Port No : ▾

	MAC Address	Port No.
<input type="checkbox"/>	001122334455	Port.06

Label	Description
MAC Address	Enter a MAC address for a specific port.
Port NO.	Select a switch port
Add	Add the MAC address and port information.
Delete	Deletes an entry
Help	Shows help file

MAC Blacklist

You can block specific devices from network access by creating a MAC blacklist. MAC blacklists will prevent traffic from forwarding to specific MAC addresses in the list. Any frames forwarding to the MAC addresses in this list will be discarded. As a result, the target device will never receive any frame.



MAC Address :

	MAC Address
<input type="checkbox"/>	001E94123456

Label	Description
MAC Address	Enter a MAC address for a specific port.
Port NO.	Select a switch port
Add	Add the MAC address and port information.
Delete	Delete an entry
Help	Shows help file

802.1x

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more backend servers (RADIUS) determine whether the user is allowed access to the network.

In an 802.1X network environment, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the

authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames which encapsulate EAP PDUs. Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible as it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) does not need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding the result to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note: in an environment where two backend servers are enabled, the server timeout is configured to X seconds (using the authentication configuration page), and the first server in the list is currently down (but not considered dead), if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, it will never be authenticated because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. Since the server has not failed (because the X seconds have not expired), the same server will be contacted when the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

802.1x - Radius Server

Radius Server Setting

802.1x Protocol	Enable
Radius Server IP	192.168.16.3
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

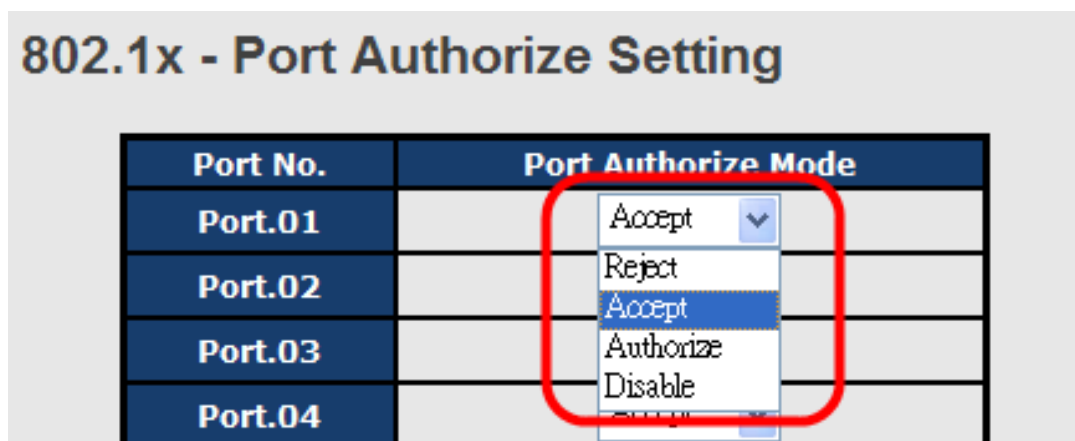
Advanced Setting

Quiet Period	60
TX Period	30
Supplicant Timeout	30
Server Timeout	30
Max Requests	2
Re-Auth Period	3600

Apply Help

Label	Description
802.1x Protocol	Enables or disables 802.1X Radius server
Radius Server IP	IP address of the authentication server
Server Port	The UDP port number used by the authentication server to authenticate
Accounting Port	The number of the UDP port that the RADIUS server uses for accounting requests.
Shared Key	A key shared between the switch and authentication server
NAS, Identifier	A string used to identify the switch.
Quiet Period	The time interval between authentication failure and the start of a new authentication attempt.
Tx Period	The time that the switch waits for response to an EAP request/identity frame from the client before resending the request.
Supplicant Timeout	The period of time the switch waits for a supplicant respond to an EAP request.
Server Timeout	The period of time the switch waits for a Radius server respond to an authentication request.
Max Requests	The maximum number of times to retry sending packets to the supplicant.
Re-Auth Period	The period of time after which clients connected must be re-authenticated
Apply	Click to apply the configurations
Help	Shows help file

The 802.1x authorized mode of each port can be set in the following dialog:



802.1x - Port Authorize State

Port No.	Port Authorize State
Port.01	Accept
Port.02	Accept
Port.03	Accept
Port.04	Accept
Port.05	Accept
Port.06	Accept
Port.07	Accept
G1	Accept
G2	Accept
G3	Accept

Label	Description
Port Authorize Mode	Reject: force the port to be unauthorized Accept: force the port to be authorized Authorize: the state of the port is determined by the outcome of the 802.1x authentication Disable: the port will not participate in the 802.1x portocol
Apply	Click to apply the configurations
Help	Shows help file

5.6.5 IP Guard

Port Setting

This page allows you to configure IP guard functions for each port, an intelligent and user-friendly IP security method. It protects the network from unknown IP (IPs not in the allowed list) attack. Unauthorized IP traffic will be blocked.

Port No.	Mode
Port.01	Monitor <input type="button" value="v"/>
Port.02	Security <input type="button" value="v"/>
Port.03	Disabled <input type="button" value="v"/>
Port.04	Disabled <input type="button" value="v"/>

Label	Description
Mode	Disabled: disables the function Monitor: scans the IP information of the connected device before implementing further actions Security: performs security actions without scanning the information of the connected device
Apply	Click to apply the configurations
Help	Shows help file

Allow List

By creating an allow list, traffic from the IP addresses in the list will be allowed.

IP Guard - Allow List

Delete	IP	MAC	Port	Status
<input type="checkbox"/>	192.168.10.66	001E94112547	G1	Active ▼

IP	MAC	Port	Status
<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	Port.01 ▼	Active ▼

Label	Description
IP	IP address of the allowed entry
MAC	MAC address of the allowed entry
Port	Port number of the allowed entry
Status	The option allows you to block suspicious IP traffic. Active: allows the IP traffic. Suspend: blocks the IP traffic.
Delete	Check to delete an entry

Super-IP List

A super-IP list enables you to give full access to the switch to the user you specify. Devices with the IP addresses listed in the table will be able to manage the switch disregarding the rule you have set.

IP Guard - Super-IP List

IP Address :

Super-IP List

IP Address

Monitor List

You can create a monitor list to monitor IP traffic of individual ports automatically.

IP Guard - Monitor List

Add to Allow List	IP	MAC	Port	Time
<input type="checkbox"/>	192.168.10.66	001E94988989	Port.08	19700103 19:20

Label	Description
IP	IP address of the port
MAC	MAC address of the port
Port	The port number you want to monitor
Time	The time when the entry is logged.
Add to Allow List	Check to add the entry to the allow list

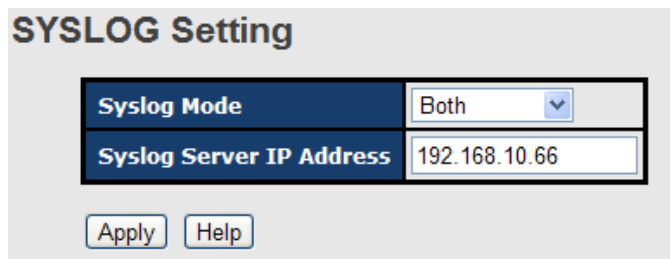
5.6.6 Warning

The switch supports several alerting methods, including SYSLOG, e-mail, and fault relay. These methods enable you to monitor switch status remotely. When an event occurs, the system will send an alert to your appointed servers.

SYSLOG Setting

SYSLOG is a protocol that allows a device to send event notification messages across IP networks to event message collectors. It permits separation of the software that generates

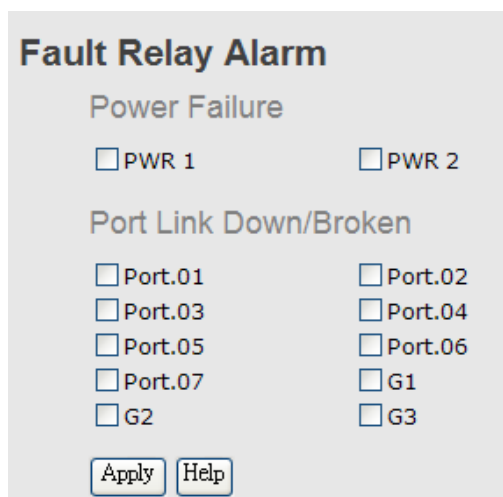
messages from the system that stores them and the software that reports and analyzes them. As Syslog messages are UDP-based, the sender and receiver will not be aware of it if the packet is lost due to network disconnection and no UDP packet will be resent.



Label	Description
Syslog Mode	Disable: disables SYSLOG Client Only: logs in to a local system Server Only: logs in to a remote SYSLOG server Both: logs in to a local and remote server.
SYSLOG Server IP Address	The IP address of the remote SYSLOG server
Apply	Click to apply the configurations
Help	Shows help file

Fault Relay

When any selected fault event happens, the Fault LED on the switch panel will light up and the electric relay will signal at the same time. You can set the switch to trigger alarms when power fails or ports are disconnected.



SMTP Setting

SMTP (Simple Mail Transfer Protocol) is a protocol for transmitting e-mails across the Internet. By setting up SMTP alert, the device will send a notification e-mail when a user-defined event occurs.

SMTP Setting

E-mail Alert: Enable

SMTP Server IP Address :	<input type="text" value="192.168.10.66"/>
Mail Subject :	<input type="text" value="Automated Email Alert"/>
Sender :	<input type="text" value="test mail"/>
<input type="checkbox"/> Authentication	
Rcpt e-mail Address 1 :	<input type="text" value="test@192.168.10.66"/>
Rcpt e-mail Address 2 :	<input type="text"/>
Rcpt e-mail Address 3 :	<input type="text"/>
Rcpt e-mail Address 4 :	<input type="text"/>

Label	Description
E-mail Alert	Enables or disables transmission of system warnings by e-mail
SMTP Server IP Address	The IP address of the SMTP server to receive the notification e-mail
Mail Subject	Subject of the mail
Sender	The email account to send the alert
Authentication	<ul style="list-style-type: none"> ■ Username: the authentication username ■ Password: the authentication password ■ Confirm Password: re-enter password
Recipient E-mail Address	The recipient's e-mail address. A mail allows for 6 recipients.
Apply	Click to activate the configurations
Help	Shows help file

Event Selection

The device supports both SYSLOG and SMTP alerts. Check the corresponding box to enable the system event warning method you want. Please note that the checkboxes will gray out if SYSLOG or SMTP is disabled.

Event Selection

System Event

Event Type	Syslog	SMTP
Device cold start	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device warm start	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Authentication failure	<input type="checkbox"/>	<input checked="" type="checkbox"/>
O-Ring topology change	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Port Event

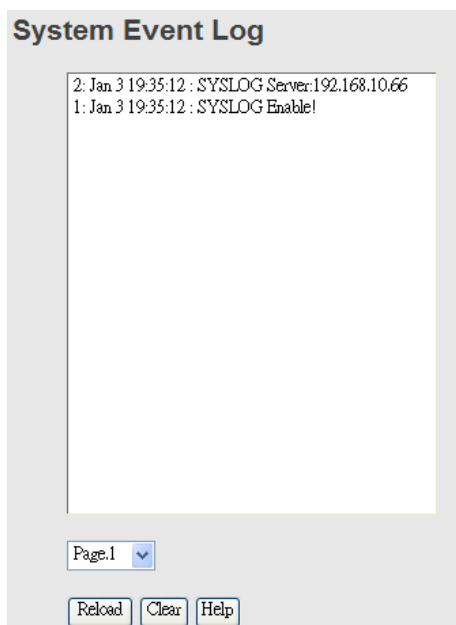
Port	Syslog	SMTP
Port.01	Link Down <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.02	Disable <input type="button" value="v"/>	Link Up & Link Down <input type="button" value="v"/>

Label	Description
Device cold start	Sends alerts when you restart the device using the power button on your PC.
Device warm start	Sends alerts when you restart the device using the Reset button or software.
Authentication Failure	Sends alerts when SNMP authentication fails
O-Ring topology change	Sends alerts when O-Ring topology changes
Port Event	<p>Sends alerts when the port meets a specified condition. Available options include:</p> <ul style="list-style-type: none"> ■ Disable: disables alert function ■ Link Up: sends alerts when port is connected ■ Link Down: sends alerts when port is not connected ■ Link Up & Link Down: sends alerts when port is connected and disconnected
Apply	Click to apply the configurations
Help	Shows help file

5.7 Monitor and Diag

5.7.1 System Event Log

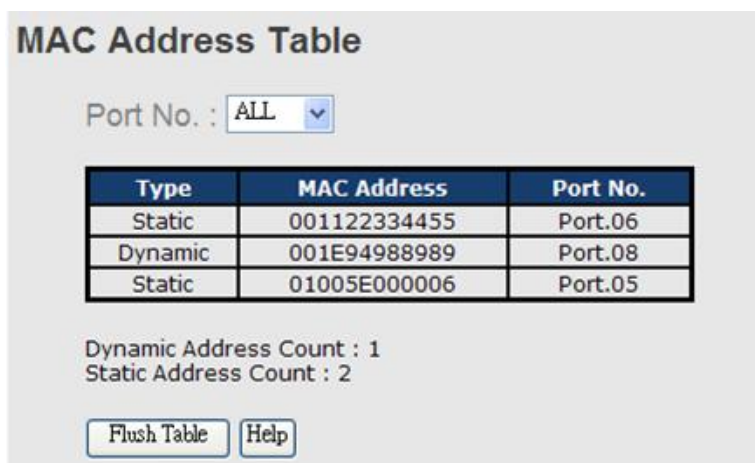
If a system log client is enabled, the system event log will be shown in this table.



Label	Description
Page	The page number of the selected LOG
Reload	Click to refresh the information in this page
Clear	Clear log
Help	Shows help file

5.7.2 MAC Address Table

A MAC address table is a table in a network switch that maps MAC addresses to ports. The switch uses the table to determine which port the incoming packet should be forwarded to. Entries in a MAC address table fall into two types: dynamic and static entries. Entries in a static MAC table are added or removed manually and cannot age out by themselves. Entries in a dynamic MAC table will age out after a configured aging time. Such entries can be added by learning or manual configuration.



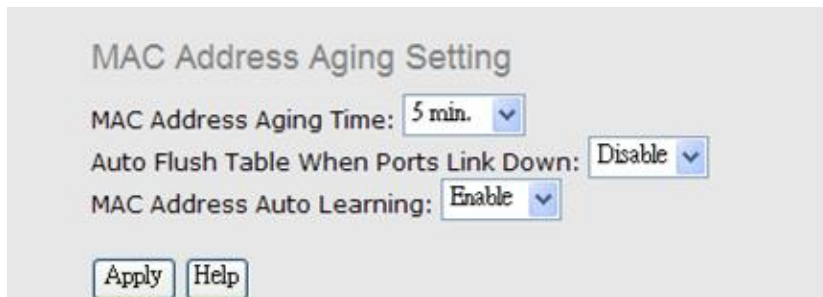
Label	Description
Port NO. :	Shows all MAC addresses mapped to a selected port in the table
Flush Table	Clears all MAC addresses in the table
Help	Shows help file.

Aging Configuration

Aging enables the switch to track only active MAC addresses on the network and flush out MAC addresses that are no longer used, thereby keeping the table current. You can configure aging time by entering a value in the **MAC Address Aging Time** box. Note that aging time must be a multiple of 15.

MAC Table Learning

The switch can add the address and port on which the packet was received to the MAC table if the address does not exist in the table by examining the source address of each packet received on a port. This is called learning. It allows the MAC table to expand dynamically. If the learning mode for a given port is grayed out, it means another module is in control of the mode, and thus the user cannot change the configurations. An example of such a module is MAC-Based authentication under 802.1X.



The screenshot shows a configuration window titled "MAC Address Aging Setting". It contains three dropdown menus: "MAC Address Aging Time" set to "5 min.", "Auto Flush Table When Ports Link Down" set to "Disable", and "MAC Address Auto Learning" set to "Enable". At the bottom, there are "Apply" and "Help" buttons.

Label	Description
MAC Address Aging Time	The time of an entry stays valid in the table
Auto Flush Table When Ports Link Down	Clears the MAC table automatically when ports are disconnected
MAC Address Auto Learning	Enables or disables MAC learning function
Apply	Click to apply the configurations.

Port Overview

This page provides an overview of general traffic statistics for all switch ports.

Port Overview

Port No.	Type	Link	State	TX Good Packet	TX Bad Packet	RX Good Packet	RX Bad Packet	TX Abort Packet	Packet Collision
Port.01	100TX	Down	Forwarding	0	0	0	0	0	0
Port.02	100TX	Down	Forwarding	0	0	0	0	0	0
Port.03	100TX	Down	Forwarding	0	0	0	0	0	0
Port.04	100TX	Down	Forwarding	0	0	0	0	0	0

Label	Description
Type	Shows port speed and media type.
Link	Shows port link status
State	Shows port status
TX GOOD Packet	The number of good packets sent by this port
TX Bad Packet	The number of bad packets sent by this port
RX GOOD Packet	The number of good packets received by this port
RX Bad Packet	The number of bad packets received by this port
TX Abort Packet	The number of packets aborted by this port
Packet Collision	The number of times a collision is detected by this port
Clear	Clears all counters
Help	Shows help file

Port Counter

The displayed counters include the total number for receive and transmit, the size for receive and transmit, and the errors for receive and transmit.

Port No. :

InGoodOctetsLo	InGoodOctetsHi	InBadOctets	OutFCSErr
0	0	0	0
InUnicasts	Deferred	InBroadcasts	InMulticasts
0	0	0	0
Octets64	Octets127	Octets255	Octets511
0	0	0	0
Octets1023	OctetsMax	OutOctetsLo	OutOctetsHi
0	0	0	0
OutUnicasts	Excessive	OutMulticasts	OutBroadcasts
0	0	0	0
Single	OutPause	InPause	Multiple
0	0	0	0
Undersize	Fragments	Oversize	Jabber
0	0	0	0
InMACRcvErr	InFCSErr	Collisions	Late
0	0	0	0



Label	Description
InGoodOctetsLo	The lower 32-bits of the 64-bit InGoodOctets counter. This field indicates the total length of all good Ethernet frames received.
InGoodOctetsHi	The upper 32-bits of the 64-bit InGoodOctets counter. This field indicates the total length of all good Ethernet frames received.
InBadOctets	The total length of all bad Ethernet frames received.
OutFCSErr	The number of frames transmitted with an invalid FCS. Whenever a frame is modified during transmission (e.g., to add or remove a tag), the frame's original FCS is inspected before a new FCS is added to a modified frame. If the original FCS is invalid, the new FCS is made invalid too and this counter is incremented.
InUnicasts	The number of good frames received that have a Unicast destination MAC address.
Deferred	The total number of successfully transmitted frames without collision but are delayed because the medium is busy during the first attempt. This counter is applicable in half-duplex only.
InBroadcasts	The number of good frames received that have a Broadcast destination MAC address.
InMulticasts	The number of good frames received that have a Multicast destination MAC address.
Octets64	Total frames received (and/or transmitted) with a length of exactly 64 octes, including those with errors.
Octets127	Total frames received (and/or transmitted) with a length of between 65 and 127 octes, including those with errors.
Octets255	Total frames received (and/or transmitted) with a length of between 128 and 255 octes, including those with errors.
Octets511	Total frames received (and/or transmitted) with a length of between 256 and 511 octes, including those with errors.
Octets1023	Total frames received (and/or transmitted) with a length of between 512 and 1023 octes, including those with errors.
OctetsMax	Total frames received (and/or transmitted) with a length of between 1024 and MaxSize octes, including those with errors.
OutOctetsLo	The lower 32-bit of the 64-bit OutOctets counter. This field indicates the total length of all Ethernet frames sent from this MAC address.
OutOctetsHi	The upper 32-bit of the 64-bit OutOctets counter. This field indicates the total length of all Ethernet frames sent from this MAC



	address.
OutUnicasts	The number of frames sent with an Unicast destination MAC address.
Excessive	The number frames dropped in the transmitted MAC address because the frame experiences 16 consecutive collisions. This counter is applicable in half-duplex only and only when DiscardExcessive is one.
OutBroadcasts	The number of good frames sent with a Broadcast destination MAC address
Single	The total number of successfully transmitted frames that experiences exactly one collision. This counter is applicable in half-duplex only.
OutPause	The number of good Flow Control frames sent
InPause	The number of good Flow Control frames received
Multiple	The total number of successfully transmitted frames that experience more than one collision. This counter is applicable in half-duplex only.
Undersize	Total frames received with a length of less than 64 octets but with a valid FCS
Fragments	Total frames received with a length of more than 64 octets and with an invalid FCS
Oversize	Total frames received with a length of more than MaxSize octets but with a valid FCS
Jabber	Total frames received with a length of more than MaxSize octets but with an invalid FCS
InMACRcvErr	Total frames received with an RxErr signal from the PHY
InFCSErr	Total frames received with a CRC error not counted in Fragments, Jabber or RxErr.
Collisions	The number of frames for which one or more collisions occurred when the frames were sent, including single, multiple, excessive, or late collisions. This counter is applicable in half-duplex only.
Late	When a collision is detected by a station after it has sent the 512th bit of its frame, it is counted as a late collision. This counter is applicable in half-duplex only.

Port Monitoring

The switch supports several types of port monitoring including TX (egress) only, RX (ingress)

only, and both TX/RX monitoring. TX monitoring sends any data that egress out checked TX source ports to a selected TX destination port as well. RX monitoring sends any data that ingress in checked RX source ports out to a selected RX destination port as well as sending the frame where it normally would have gone. Note that keep all source ports unchecked in order to disable port monitoring.

Port Monitoring

Port No.	Destination Port		Source Port	
	RX	TX	RX	TX
Port.01	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.02	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.03	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.04	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>

Label	Description
Destination Port	The port will receive a copied frame from source port for monitoring purpose.
Source Port	Check to monitor specific ports
TX	The frames transmitted by a port
RX	The frames received by a port
Apply	Click to activate the configurations.
Clear	Clears all checked boxes (disable the function)
Help	Shows help file

Traffic Monitoring

By enabling traffic monitoring function, the switch will send out an SYSLOG event notification or SMTP e-mail when the traffic becomes too large.

Traffic Monitor

Port No.	Monitored-Counter	Time-Interval (1~300s)	Increasing-Quantity
Port.01	RX Octet	3	1000
Port.02	RX Broadcast	3	1000
Port.03	RX Multicast	3	1000
Port.04	RX Unicast	3	1000
Port.05	RX Non-Unicast	3	1000
Port.06	Disable	3	1000

Label	Description
Monitored-Counter	Monitor the incoming traffic by bandwidth or number of packets. Available options include: RX Octet: calculates the total bandwidth consumed by incoming traffic RX Broadcast: calculates the number of broadcast packets RX Multicast: calculates the number of multicast packets RX Unicast: calculates the number of unicast packets RX Non-Unicast: calculates the total number of multicast and broadcast packets Disable: disables the function
Time-Interval	Sets the time interval of counting
Increasing Quantity	- Specify a threshold for the counter. When the result of calculation exceeds the value, an alert will be issued.
Event Alarm	Specifies alarm type (SYSLOG or SMTP)

5.7.3 Ping

This command sends ICMP echo request packets to another node on the network. Using the ping command, you can see if another site on the network can be reached.

Ping

IP Address :

Ping Log

Pinging 192.168.10.66: seq 1 sent...
Reply seq 1 from 192.168.10.66

Pinging 192.168.10.66: seq 2 sent...
Reply seq 2 from 192.168.10.66

Pinging 192.168.10.66: seq 3 sent...
Reply seq 3 from 192.168.10.66

Pinging 192.168.10.66: seq 4 sent...
Reply seq 4 from 192.168.10.66

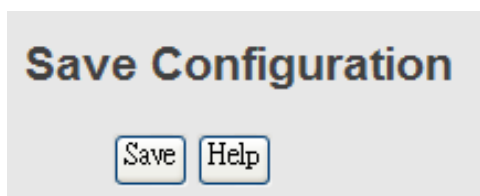
Ping complete: sent 4, received 4

After you press **Active**, four ICMP packets will be transmitted, and the sequence number and roundtrip time will be displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

Label	Description
IP Address	Enter the IP address that you want to detect
Active	Click to send ICMP packets

5.7.4 Save Configuration

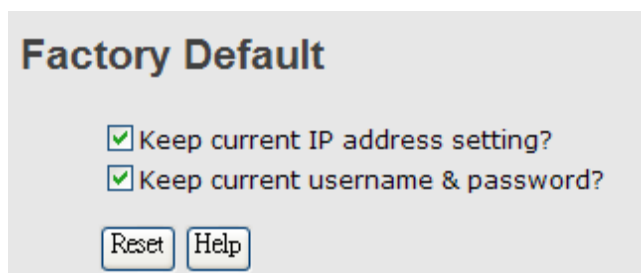
Click **Save Configuration** whenever you change a configuration to save current configurations; otherwise, the changes you make will be lost when the power is off or system is reset.



Label	Description
Save	Saves all configurations
Help	Shows help file

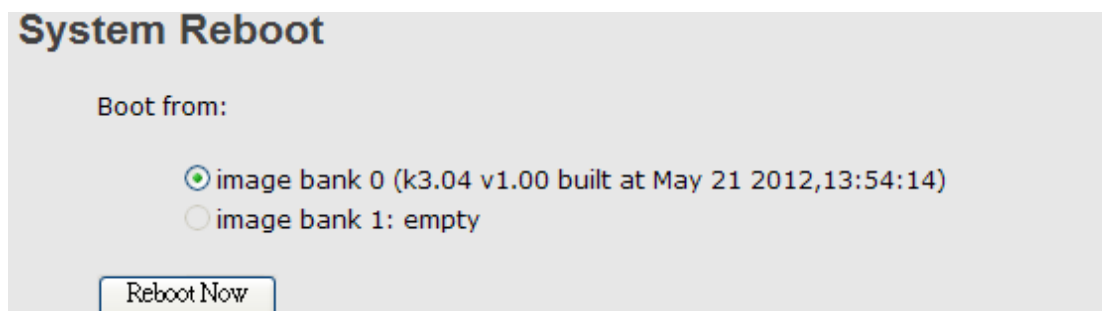
5.7.5 Factory Default

This function is to force the switch back to the original factory settings. You can decide to keep current IP address settings or username/password by checking in the boxes.



5.7.6 System Reboot

You can reset the stack switch on this page. After reset, the system will boot normally as if you have powered on the devices.



Command Line Interface Management

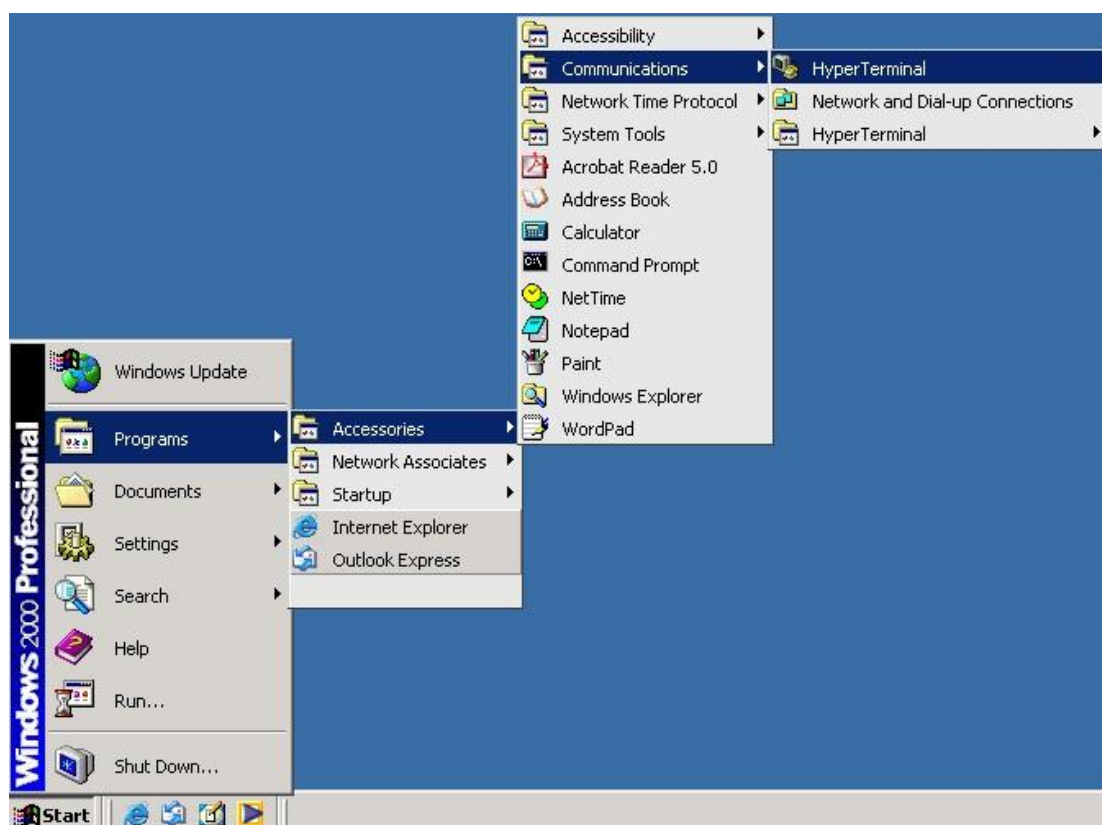
Besides Web-based management, the switch also supports CLI management. You can use console or telnet to manage the switch by CLI.

CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

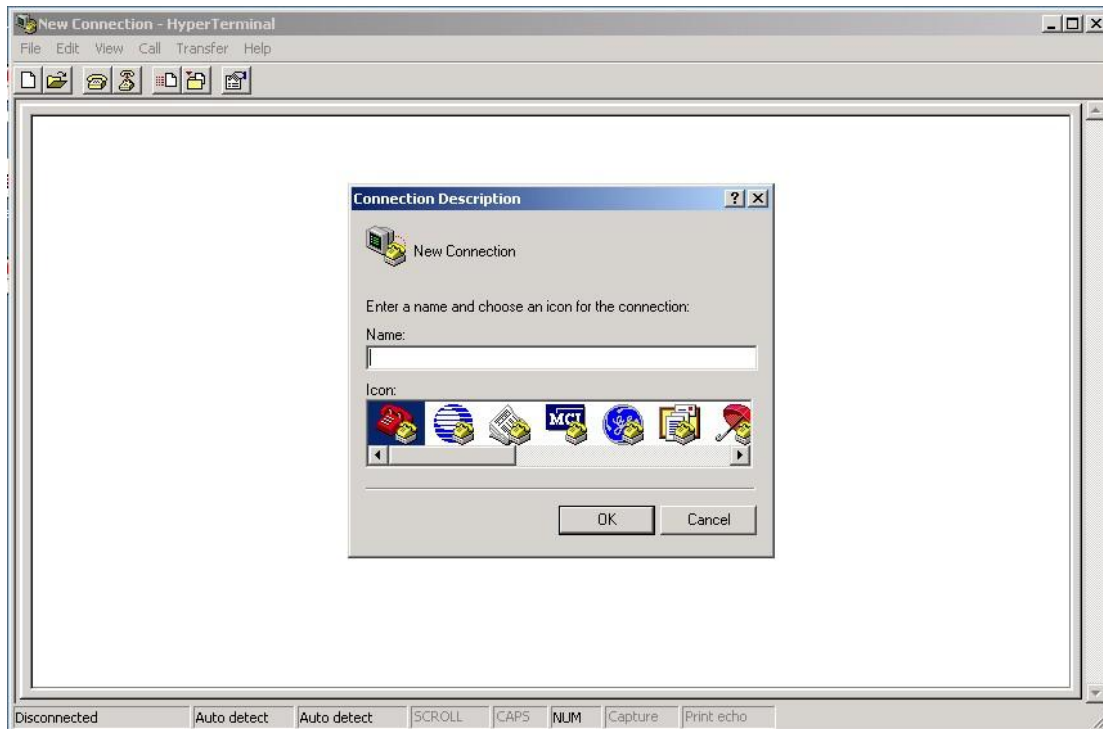
Before configuring RS-232 serial console, connect the RS-232 port of the switch to your PC Com port using a RJ45 to DB9-F cable.

Follow the steps below to access the console via RS-232 serial cable.

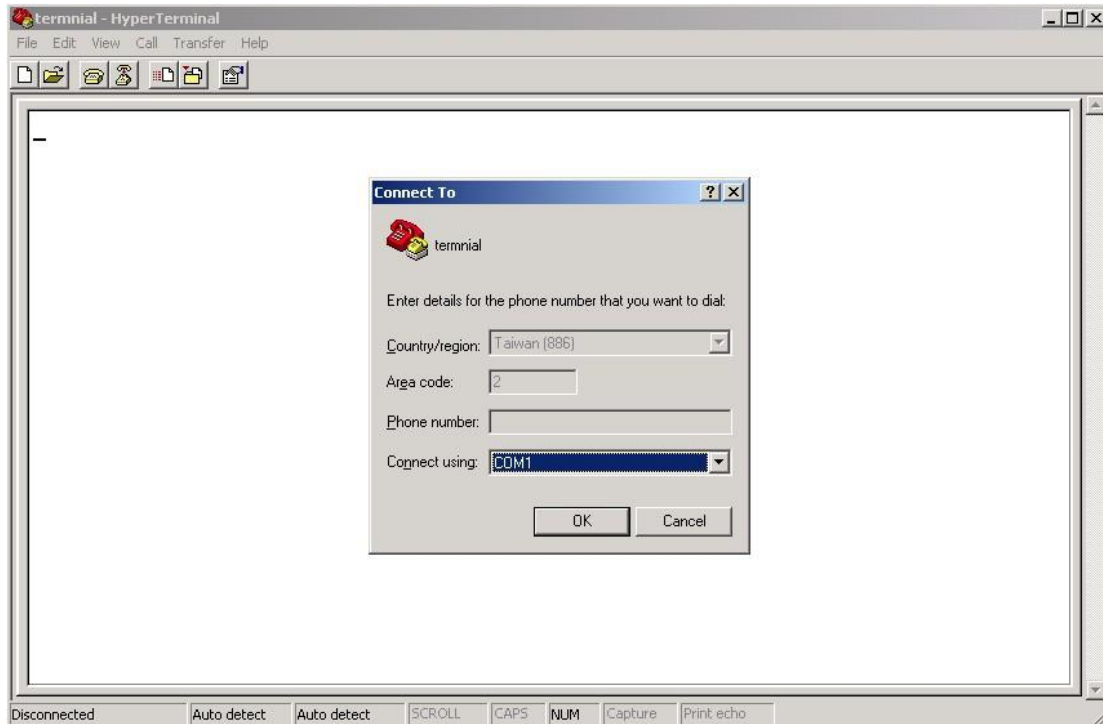
Step 1: On Windows desktop, click on **Start -> Programs -> Accessories -> Communications -> Hyper Terminal**



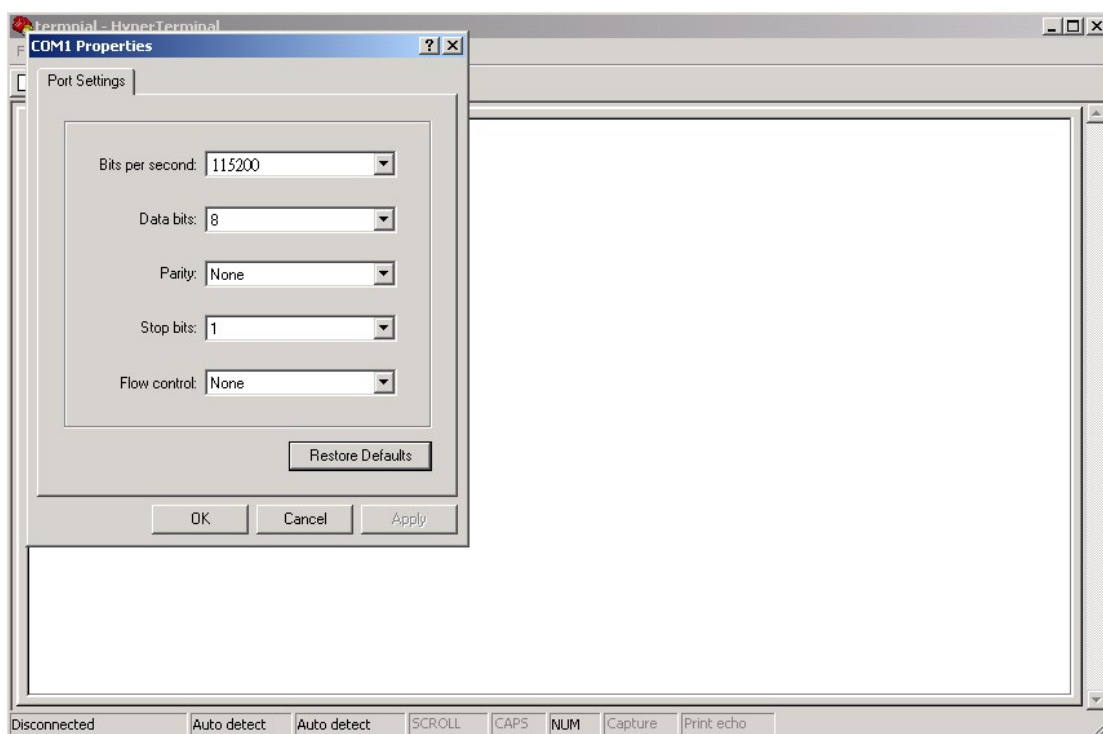
Step 2. Input a name for the new connection.



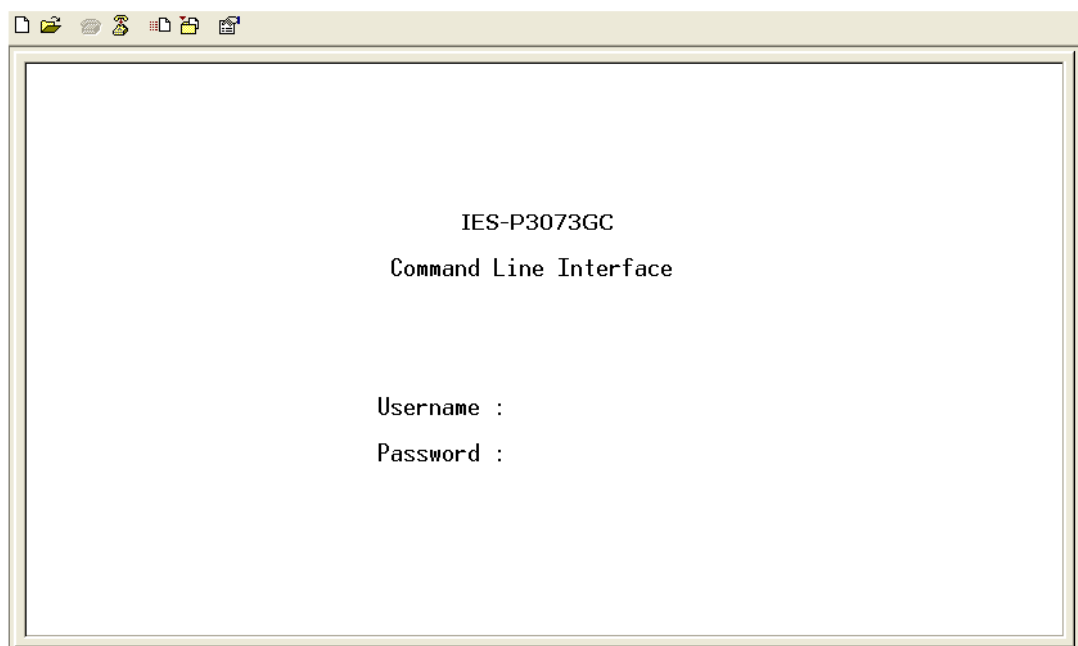
Step 3. Select a COM port in the drop-down list.



Step 4. A pop-up window that indicates COM port properties appears, including bits per second, data bits, parity, stop bits, and flow control.



Step 5. The console login screen will appear. Use the keyboard to enter the Username and Password (same as the password for Web browsers), then press **Enter**.



CLI Management by Telnet

You can use **TELNET** to configure the switch. The default values are:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

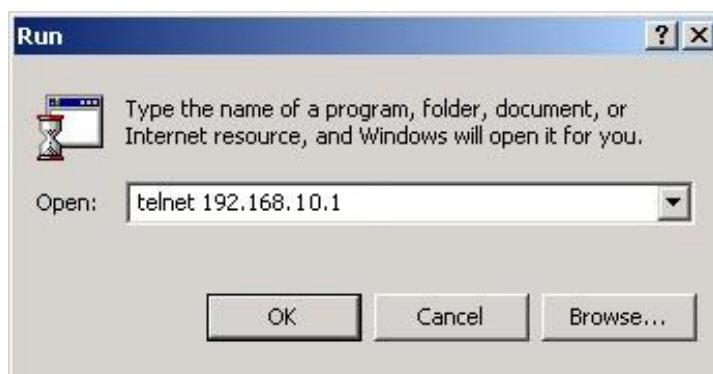
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

Follow the steps below to access console via Telnet.

Step 1. Telnet to the IP address of the switch from the **Run** window by inputting commands (or from the MS-DOS prompt) as below.



Step 2. The Login screen will appear. Use the keyboard to enter the Username and Password (same as the password for Web browser), and then press **Enter**.





System

System>	Configuration [all] [<port_list>]
	Reboot
	Restore Default [keep_ip]
	Contact [<contact>]
	Name [<name>]
	Location [<location>]
	Description [<description>]
	Password <password>
	Username [<username>]
	Timezone [<offset>]
	Log [<log_id>] [all info warning error] [clear]

IP

IP>	Configuration
	DHCP [enable disable]
	Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]
	Ping <ip_addr_string> [<ping_length>]
	SNTP [<ip_addr_string>]

Port

port>	Configuration [<port_list>] [up down]
	Mode [<port_list>] [auto 10hdx 10fdx 100hdx 100fdx 1000fdx sfp_auto_ams]
	Flow Control [<port_list>] [enable disable]
	State [<port_list>] [enable disable]
	MaxFrame [<port_list>] [<max_frame>]
	Power [<port_list>] [enable disable actiphy dynamic]
	Excessive [<port_list>] [discard restart]
	Statistics [<port_list>] [<command>] [up down]
	VeriPHY [<port_list>]
	SFP [<port_list>]

MAC

MAC>	Configuration [<port_list>]
	Add <mac_addr> <port_list> [<vid>]
	Delete <mac_addr> [<vid>]

	Lookup <mac_addr> [<vid>]
	Agetime [<age_time>]
	Learning [<port_list>] [auto disable secure]
	Dump [<mac_max>] [<mac_addr>] [<vid>]
	Statistics [<port_list>]
	Flush

VLAN

VLAN>	Configuration [<port_list>]
	PVID [<port_list>] [<vid> none]
	FrameType [<port_list>] [all tagged untagged]
	IngressFilter [<port_list>] [enable disable]
	tx_tag [<port_list>] [untag_pvid untag_all tag_all]
	PortType [unaware c-port s-port s-custom-port] [<port_list>]
	EtypeCustomSport [<etype>]
	Add <vid> <name> [<ports_list>]
	Forbidden Add <vid> <name> [<port_list>]
	Delete <vid> <name>
	Forbidden Delete <vid> <name>
	Forbidden Lookup [<vid>] [(name <name>)]
	Lookup [<vid>] [(name <name>)] [combined static nas all]
	Name Add <name> <vid>
	Name Delete <name>
	Name Lookup [<name>]
Status [<port_list>] [combined static nas mstp all conflicts]	

Private VLAN

PVLAN>	Configuration [<port_list>]
	Add <pvlan_id> [<port_list>]
	Delete <pvlan_id>
	Lookup [<pvlan_id>]
	Isolate [<port_list>] [enable disable]

Security

Security >	Switch Switch security setting
------------	--

	Network Network security setting
	AAA Authentication, Authorization and Accounting setting

Security Switch

Security/switch>	Password <password>
	Auth Authentication
	SSH Secure Shell
	HTIPS Hypertext Transfer Protocol over Secure Socket Layer
	RMON Remote Network Monitoring

Security Switch Authentication

Security/switch/auth>	Configuration
	Method [console telnet ssh web] [none local radius] [enable disable]

Security Switch SSH

Security/switch/ssh>	Configuration
	Mode [enable disable]

Security Switch HTTPS

Security/switch/ssh>	Configuration
	Mode [enable disable]

Security Switch RMON

Security/switch/rmon>	Statistics Add <stats_id> <data_source>
	Statistics Delete <stats_id>
	Statistics Lookup [<stats_id>]
	History Add <history_id> <data_source> [<interval>] [<buckets>]
	History Delete <history_id>
	History Lookup [<history_id>]
	Alarm Add <alarm_id> <interval> <alarm_variable> [absolute delta]<rising_threshold> <rising_event_index> <falling_threshold> <falling_event_index>



	[rising falling both]
	Alarm Delete <alarm_id>
	Alarm Lookup [<alarm_id>]

Security Network

Security/Network>	Psec	Port Security Status
	NAS	Network Access Server (IEEE 802.1X)
	ACL	Access Control List
	DHCP	Dynamic Host Configuration Protocol

Security Network Psec

Security/Network/Psec>	Switch [<port_list>]
	Port [<port_list>]

Security Network NAS

Security/Network/NAS>	Configuration [<port_list>]
	Mode [enable disable]
	State [<port_list>] [auto authorized unauthorized macbased]
	Reauthentication [enable disable]
	ReauthPeriod [<reauth_period>]
	EapolTimeout [<eapol_timeout>]
	Agetime [<age_time>]
	Holdtime [<hold_time>]
	Authenticate [<port_list>] [now]
Statistics [<port_list>] [clear eapol radius]	

Security Network ACL

Security/Network/ACL>	Configuration [<port_list>]
	Action [<port_list>] [permit deny]
	[<rate_limiter>][<port_redirect>] [<mirror>] [<logging>]
	[<shutdown>]
	Policy [<port_list>] [<policy>]
	Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]
Add [<ace_id>] [<ace_id_next>][<port_list>] [(policy <policy> <policy_bitmask>)] [<tagged>] [<vid>]	
[<tag_prio>] [<dmac_type>][<etype <etype>] [<smac>]	

	[<dmac>] (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>]) [permit deny] [<rate_limiter>] [<port_redirect>] [<mirror>] [<logging>] [<shutdown>]
	Delete <ace_id>
	Lookup [<ace_id>]
	Clear
	Status [combined static loop_protect dhcp ptp ipmc conflicts]
	Port State [<port_list>] [enable disable]

Security Network DHCP

Security/Network/DHCP>	Configuration
	Mode [enable disable]
	Server [<ip_addr>]
	Information Mode [enable disable]
	Information Policy [replace keep drop]
	Statistics [clear]

Security Network AAA

Security/Network/AAA>	Configuration
	Timeout [<timeout>]
	Deadtime [<dead_time>]
	RADIUS [<server_index>] [enable disable] [<ip_addr_string>] [<secret>] [<server_port>]
	ACCT_RADIUS [<server_index>] [enable disable] [<ip_addr_string>] [<secret>] [<server_port>]
	Statistics [<server_index>]

STP

STP>	Configuration
	Version [<stp_version>] Non-certified release, v
	Txhold [<holdcount>]lt 15:15:15, Dec 6 2007
	MaxAge [<max_age>]
	FwdDelay [<delay>]
	bpduFilter [enable disable]
	bpduGuard [enable disable]
	recovery [<timeout>]
	CName [<config-name>] [<integer>]
	Status [<msti>] [<port_list>]
	Msti Priority [<msti>] [<priority>]
	Msti Map [<msti>] [clear]
	Msti Add <msti> <vid>
	Port Configuration [<port_list>]
	Port Mode [<port_list>] [enable disable]
	Port Edge [<port_list>] [enable disable]
	Port AutoEdge [<port_list>] [enable disable]
	Port P2P [<port_list>] [enable disable auto]
	Port RestrictedRole [<port_list>] [enable disable]
	Port RestrictedTcn [<port_list>] [enable disable]
	Port bpduGuard [<port_list>] [enable disable]
	Port Statistics [<port_list>]
	Port Mcheck [<port_list>]
	Msti Port Configuration [<msti>] [<port_list>]
	Msti Port Cost [<msti>] [<port_list>] [<path_cost>]
Msti Port Priority [<msti>] [<port_list>] [<priority>]	

Aggr

Aggr>	Configuration
	Add <port_list> [<aggr_id>]
	Delete <aggr_id>
	Lookup [<aggr_id>]
	Mode [smac dmac ip port] [enable disable]

LACP

LACP>	Configuration [<port_list>]
	Mode [<port_list>] [enable disable]
	Key [<port_list>] [<key>]
	Role [<port_list>] [active passive]
	Status [<port_list>]
	Statistics [<port_list>] [clear]

LLDP

LLDP>	Configuration [<port_list>]
	Mode [<port_list>] [enable disable]
	Statistics [<port_list>] [clear]
	Info [<port_list>]

PoE

PoE>	Configuration [<port_list>]
	Mode [<port_list>] [disabled poe poe+]
	Priority [<port_list>] [low high critical]
	Mgmt_mode [class_con class_res al_con al_res lldp_res lldp_con]
	Maximum_Power [<port_list>] [<port_power>]
	Status
	Primary_Supply [<supply_power>]

QoS

QoS>	DSCP Map [<dscp_list>] [<class>] [<dpl>]
	DSCP Translation [<dscp_list>] [<trans_dscp>]
	DSCP Trust [<dscp_list>] [enable disable]
	DSCP Classification Mode [<dscp_list>] [enable disable]
	DSCP Classification Map [<class_list>] [<dpl_list>] [<dscp>]
	DSCP EgressRemap [<dscp_list>] [<dpl_list>] [<dscp>]
	Storm Unicast [enable disable] [<packet_rate>]

	Storm Multicast [enable disable] [<packet_rate>]
	Storm Broadcast [enable disable] [<packet_rate>]
	QCL Add [<qce_id>] [<qce_id_next>] [<port_list> [<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type> [(etype [<etype>]) (LLC [<DSAP>] [<SSAP>] [<control>]) (SNAP [<PID>]) (ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment> [<sport>] [<dport>]) (ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport> [<dport>])] [<class>] [<dp>] [<classified_dscp>]
	QCL Delete <qce_id>
	QCL Lookup [<qce_id>]
	QCL Status [combined static conflicts]
	QCL Refresh

Mirror

Mirror>	Configuration [<port_list>]
	Port [<port> disable]
	Mode [<port_list>] [enable disable rx tx]

Dot1x

Dot1x>	Configuration [<port_list>]
	Mode [enable disable]
	State [<port_list>] [macbased auto authorized unauthorized]
	Authenticate [<port_list>] [now]
	Reauthentication [enable disable]
	Period [<reauth_period>]
	Timeout [<eapol_timeout>]
	Statistics [<port_list>] [clear eapol radius]
	Clients [<port_list>] [all <client_cnt>]
	Agetime [<age_time>]



	Holdtime [<hold_time>]
--	------------------------

IGMP

IGMP>	Configuration [<port_list>]
	Mode [enable disable]
	State [<vid>] [enable disable]
	Querier [<vid>] [enable disable]
	Fastleave [<port_list>] [enable disable]
	Router [<port_list>] [enable disable]
	Flooding [enable disable]
	Groups [<vid>]
	Status [<vid>]

ACL

ACL>	Configuration [<port_list>]
	Action [<port_list>] [permit deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]
	Policy [<port_list>] [<policy>]
	Rate [<rate_limiter_list>] [<packet_rate>]
	Add [<ace_id>] [<ace_id_next>] [switch (port <port>) (policy <policy>)] [<vid>] [<tag_prio>] [<dmac_type>] [(etype [<etype>] [<smac>] [<dmac>]) (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])] [permit deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]
	Delete <ace_id>
	Lookup [<ace_id>]



	Clear
--	-------

Mirror

Mirror>	Configuration [<port_list>]
	Port [<port> disable]
	Mode [<port_list>] [enable disable rx tx]

Config

Config>	Save <ip_server> <file_name>
	Load <ip_server> <file_name> [check]

Firmware

Firmware>	Load <ip_addr_string> <file_name>
-----------	-----------------------------------

SNMP

SNMP>	Trap Inform Retry Times [<retries>]
	Trap Probe Security Engine ID [enable disable]
	Trap Security Engine ID [<engineid>]
	Trap Security Name [<security_name>]
	Engine ID [<engineid>]
	Community Add <community> [<ip_addr>] [<ip_mask>]
	Community Delete <index>
	Community Lookup [<index>]
	User Add <engineid> <user_name> [MD5 SHA] [<auth_password>] [DES] [<priv_password>]
	User Delete <index>
	User Changekey <engineid> <user_name> <auth_password> [<priv_password>]
	User Lookup [<index>]
	Group Add <security_model> <security_name> <group_name>
	Group Delete <index>
	Group Lookup [<index>]
	View Add <view_name> [included excluded] <oid_subtree>



	View Delete <index>
	View Lookup [<index>]
	Access Add <group_name> <security_model> <security_level> [<read_view_name>] [<write_view_name>]
	Access Delete <index>
	Access Lookup [<index>]

Firmware

Firmware>	Load <ip_addr_string> <file_name>
-----------	-----------------------------------

PTP

PTP>	Configuration [<clockinst>]
	PortState <clockinst> [<port_list>] [enable disable internal]
	ClockCreate <clockinst> [<devtype>] [<twostep>] [<protocol>] [<oneway>] [<clockid>] [<tag_enable>] [<vid>] [<prio>]
	ClockDelete <clockinst> [<devtype>]
	DefaultDS <clockinst> [<priority1>] [<priority2>] [<domain>]
	CurrentDS <clockinst>
	ParentDS <clockinst>
	Timingproperties <clockinst> [<utcoffset>] [<valid>] [<leap59>] [<leap61>] [<timetrac>] [<freqtrac>] [<ptptimescale>] [<timesource>]
	PTP PortDataSet <clockinst> [<port_list>] [<announceintv>] [<announceto>] [<syncintv>] [<delaymech>] [<minpdelayreqintv>] [<delayasymmetry>] [<ingressLatency>]
	LocalClock <clockinst> [update show ratio] [<clockratio>]
	Filter <clockinst> [<def_delay_filt>] [<period>] [<dist>]
	Servo <clockinst> [<displaystates>] [<ap_enable>] [<ai_enable>] [<ad_enable>] [<ap>] [<ai>] [<ad>]
	SlaveTableUnicast <clockinst>
	UniConfig <clockinst> [<index>] [<duration>] [<ip_addr>]
	ForeignMasters <clockinst> [<port_list>]
	EgressLatency [show clear]
	MasterTableUnicast <clockinst>
	ExtClockMode [<one_pps_mode>] [<ext_enable>] [<clockfreq>]

	[<vcxo_enable>]
	OnePpsAction [<one_pps_clear>]
	DebugMode <clockinst> [<debug_mode>]
	Wireless mode <clockinst> [<port_list>] [enable disable]
	Wireless pre notification <clockinst> <port_list>
	Wireless delay <clockinst> [<port_list>] [<base_delay>] [<incr_delay>]

Loop Protect

	Configuration
	Mode [enable disable]
	Transmit [<transmit-time>]
	Shutdown [<shutdown-time>]
Loop Protect>	Port Configuration [<port_list>]
	Port Mode [<port_list>] [enable disable]
	Port Action [<port_list>] [shutdown shut_log log]
	Port Transmit [<port_list>] [enable disable]
	Status [<port_list>]

IPMC

	Configuration [igmp]
	Mode [igmp] [enable disable]
	Flooding [igmp] [enable disable]
	VLAN Add [igmp] <vid>
	VLAN Delete [igmp] <vid>
IPMC>	State [igmp] [<vid>] [enable disable]
	Querier [igmp] [<vid>] [enable disable]
	Fastleave [igmp] [<port_list>] [enable disable]
	Router [igmp] [<port_list>] [enable disable]
	Status [igmp] [<vid>]
	Groups [igmp] [<vid>]
	Version [igmp] [<vid>]

Fault

Fault>	Alarm PortLinkDown [<port_list>] [enable disable]
	Alarm PowerFailure [pwr1 pwr2 pwr3] [enable disable]

Event

Event>	Configuration
	Syslog SystemStart [enable disable]
	Syslog PowerStatus [enable disable]
	Syslog SnmpAuthenticationFailure [enable disable]
	Syslog RingTopologyChange [enable disable]
	Syslog Port [<port_list>] [disable linkup linkdown both]
	SMTP SystemStart [enable disable]
	SMTP PowerStatus [enable disable]
	SMTP SnmpAuthenticationFailure [enable disable]
	SMTP RingTopologyChange [enable disable]
	SMTP Port [<port_list>] [disable linkup linkdown both]

DHCP Server

DHCP Server>	Mode [enable disable]
	Setup [<ip_start>] [<ip_end>] [<ip_mask>] [<ip_router>]
	[<ip_dns>] [<ip_tftp>] [<lease>] [<bootfile>]

Ring

Ring>	Mode [enable disable]
	Master [enable disable]
	1stRingPort [<port>]
	2ndRingPort [<port>]
	Couple Mode [enable disable]
	Couple Port [<port>]
	Dualhoming Mode [enable disable]
	Dualhoming Port [<port>]

Chain

Chain>	Configuration
	Mode [enable disable]
	1stUplinkPort [<port>]
	2ndUplinkPort [<port>]
	EdgePort [1st 2nd none]



RCS

RCS>	Mode [enable disable]
	Add [<ip_addr>] [<port_list>] [web_on web_off] [telnet_on telnet_off] [snmp_on snmp_off]
	Del <index>
	Configuration

FastRecovery

FastRecovery>	Mode [enable disable]
	Port [<port_list>] [<fr_priority>]

SFP

SFP>	syslog [enable disable]
	temp [<temperature>]
	Info

DeviceBinding

Devicebinding>	Mode [enable disable]
	Port Mode [<port_list>] [disable scan binding shutdown]
	Port DDOS Mode [<port_list>] [enable disable]
	Port DDOS Sensibility [<port_list>] [low normal medium high]
	Port DDOS Packet [<port_list>] [rx_total rx_unicast rx_multicast rx_broadcast tcp udp]
	Port DDOS Low [<port_list>] [<socket_number>]
	Port DDOS High [<port_list>] [<socket_number>]
	Port DDOS Filter [<port_list>] [source destination]
	Port DDOS Action [<port_list>] [do_nothing block_1_min block_10_mins block shutdown only_log reboot_device]
	Port DDOS Status [<port_list>]
	Port Alive Mode [<port_list>] [enable disable]
	Port Alive Action [<port_list>] [do_nothing link_change shutdown only_log reboot_device]
	Port Alive Status [<port_list>]
	Port Stream Mode [<port_list>] [enable disable]
	Port Stream Action [<port_list>] [do_nothing only_log]

	Port Stream Status [<port_list>]
	Port Addr [<port_list>] [<ip_addr>] [<mac_addr>]
	Port Alias [<port_list>] [<ip_addr>]
	Port DeviceType [<port_list>] [unknown ip_cam ip_phone ap pc plc nvr]
	Port Location [<port_list>] [<device_location>]
	Port Description [<port_list>] [<device_description>]

MRP

MRP>	Configuration
	Mode [enable disable]
	Manager [enable disable]
	React [enable disable]
	1stRingPort [<mrp_port>]
	2ndRingPort [<mrp_port>]
	Parameter MRP_TOPchgT [<value>]
	Parameter MRP_TOPNRmax [<value>]
	Parameter MRP_TSTshortT [<value>]
	Parameter MRP_TSTdefaultT [<value>]
	Parameter MRP_TSTNRmax [<value>]
	Parameter MRP_LNKdownT [<value>]
	Parameter MRP_LNKupT [<value>]
	Parameter MRP_LNKNRmax [<value>]

Modbus

Modbus>	Status
	Mode [enable disable]



Technical Specifications

ORing Switch Model	IES-P3073GC-LV (Preliminary)	IES-P3073GC-HV
Physical Ports		
10/100 Base-T(X) Port in RJ45 Auto MDI/MDIX	7	
Gigabit combo Ports with 10/100/1000Base-T(X) and 100/1000Base-X SFP Port	3	
Technology		
Ethernet Standards	IEEE 802.3 for 10Base-T IEEE 802.3u for 100Base-TX and 100Base-FX IEEE 802.3z for 1000Base-X IEEE 802.3ab for 1000Base-T IEEE 802.3x for Flow control IEEE 802.3ad for LACP (Link Aggregation Control Protocol) IEEE 802.1D for STP (Spanning Tree Protocol) IEEE 802.1p for COS (Class of Service) IEEE 802.1Q for VLAN Tagging IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol) IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol) IEEE 802.1x for Authentication IEEE 802.1AB for LLDP (Link Layer Discovery Protocol)	
MAC Table	8192 MAC addresses	
Priority Queues	4	
Processing	Store-and-Forward	
Switch Properties	Switching latency: 7 us Switching bandwidth: 7.4Gbps Max. Number of Available VLANs: 4096 IGMP multicast groups: 1024 Port rate limiting: User Define	
Security Features	Enable/disable ports, MAC based port security Port based network access control (802.1x) VLAN (802.1Q) to segregate and secure network traffic Supports Q-in-Q VLAN for performance & security to expand the VLAN space Radius centralized password management SNMP v1/v2c/v3 encrypted authentication and access security	
Software Features	STP/RSTP/MSTP (IEEE 802.1D/w/s) Redundant Ring (O-Ring) with recovery time less than 10ms over 250 units TOS/Diffserv supported Quality of Service (802.1p) for real-time traffic VLAN (802.1Q) with VLAN tagging and GVRP supported IGMP Snooping for multicast filtering Port configuration, status, statistics, monitoring, security SNTP for synchronizing of clocks over network Support PTP Client (Precision Time Protocol) clock synchronization DHCP Server / Client support Port Trunk support MVR (Multicast VLAN Registration) support Modbus TCP	
Network Redundancy	O-Ring Open-Ring O-Chain MRP STP / RSTP / MSTP	
Warning / Monitoring System	Relay output for fault event alarming Syslog server / client to record and view events Include SMTP for event warning notification via email Event selection support	
RS-232 Serial Console Port	RS-232 in RJ45 connector with console cable. 9600bps, 8, N, 1	



LED Indicators		
Power Indicator	Green : Power LED x 3	
R.M. Indicator	Green : Indicate system operated in O-Ring master mode	
Fault Indicator	Amber : Indicate unexpected event occurred	
10/100Base-T(X) RJ45 Port Indicator	Green for port Link/Act. Amber for Duplex/Collision	
10/100/1000Base-T(X) RJ45 Port Indicator	Green for port Link/Act. Amber for 100Mbps indicator	
100/1000Base-X SFP Port Indicator	Green for port Link/Act.	
Fault contact		
Relay	Relay output to carry capacity of 1A at 24VDC	
Power		
Redundant Input Power	TBD (Preliminary)	Dual power inputs. 85~264VAC/88~373VDC on dual 3-pin terminal block
Power Consumption (Typ.)	TBD (Preliminary)	12 Watts
Overload Current Protection	Present	
Reverse Polarity Protection	Present on terminal block	
Physical Characteristic		
Enclosure	IP-30	
Dimension (W x D x H)	TBD (Preliminary)	96.4 (W) x 145.5 (D) x 154 (H)mm 3.8 (W) x 5.73 (D) x 6.06 (H)inch
Weight (g)	TBD (Preliminary)	1935 g
Environmental		
Storage Temperature	-40 to 85°C (-40 to 185°F)	
Operating Temperature	-40 to 85°C (-40 to 185°F)	
Operating Humidity	5% to 95% Non-condensing	
Regulatory approvals		
Power Automation	IEC 61850-3, IEEE 1613	
EMI	FCC Part 15, CISPR (EN55022) class A, EN50155 (EN50121-3-2, EN55011, EN50121-4)	
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11	
Shock	IEC60068-2-27	
Free Fall	IEC60068-2-32	
Vibration	IEC60068-2-6	
Safety	EN 60950-1	
Warranty		
	5 years	