



IES-A3 Series

Industrial Managed Ethernet Switch

User Manual

Drawing Number: IES-A3 Series
Version 3.0
January, 2014

www.oring-networking.com

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

ORing 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 542-2 Zhongzheng Road, Xindian District, New Taipei City 231 Taiwan

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	6
1.1 About IES-A3 Series.....	6
1.2 Software Features	6
1.3 Hardware Features.....	6
Hardware Overview.....	8
2.1 Front Panel.....	8
2.2 Front Panel LEDs	10
2.3 Top Panel	11
2.4 Rear Panel	12
Hardware Installation.....	12
3.1 DIN-rail Installation	13
3.2 Wall Mounting.....	14
3.3 Wiring.....	17
3.3.1 Grounding	17
3.3.2 Redundant Power Inputs.....	17
3.4 Connection	18
3.4.1 Ethernet Cables.....	18
3.4.2 Fibers.....	19
3.4.3 RS-232 Console Port.....	20
3.4.4 O-Ring.....	21
Management	23
4.1 System Information.....	24
4.2 Front Panel.....	25
4.3 Basic Setting	26
4.3.1 Switch Setting	26
4.3.2 Admin Password	26
4.3.3 IP Setting	27
4.3.4 Time Setting.....	28
4.3.5 LLDP.....	31
4.3.6 Auto Provision.....	31
4.3.7 Backup & Restore	31
4.3.8 Upgrade Firmware.....	32
4.4 Multicast.....	33

4.4.1	IGMP Snooping.....	33
4.4.2	Multicast Filter.....	33
4.5	Port Setting.....	34
4.5.1	Port Control.....	35
4.5.2	Port Status.....	35
4.5.3	Port Alias.....	36
4.5.4	Rate Limit.....	36
4.5.5	Port Trunk.....	37
4.6	Redundancy.....	38
4.6.1	O-Ring.....	38
4.6.2	Open-Ring.....	40
4.6.3	RSTP.....	41
4.6.4	MSTP.....	43
4.7	VLAN.....	47
4.7.1	VLAN Setting.....	47
4.8	Traffic Prioritization.....	50
4.8.1	QoS Policy.....	50
4.8.2	Port-base Priority.....	51
4.8.3	COS/802.1p.....	52
4.8.4	TOS/DSCP.....	52
4.9	DHCP Server.....	53
4.9.1	Setting.....	53
4.9.2	Client List.....	54
4.9.3	Port and IP bindings.....	55
4.10	SNMP.....	55
4.10.1	Agent Setting.....	55
4.10.2	Trap Setting.....	57
4.11	Security.....	58
4.11.1	IP Security.....	58
4.11.2	Port Security.....	59
4.11.3	MAC Blacklist.....	59
4.11.4	802.1x.....	60
4.12	Warning.....	63
4.12.1	SYSLOG Setting.....	63
4.12.2	SMTP Setting.....	63
4.12.3	Event Selection.....	64
4.13	Monitor and Diag.....	66

4.13.1	System Event Log	66
4.13.2	MAC Address Table	66
4.13.3	Ping	69
4.14	Save Configuration.....	70
4.14.1	Factory Default	70
4.14.2	System Reboot.....	70
Command Line Interface Management		72
Technical Specifications		97

Getting Started

1.1 About IES-A3 Series

The IES-A3 series are powerful managed industrial Ethernet switches designed for harsh environments, especially oil & gas applications where security requirements are extremely demanding. The series can be managed via web browsers, TELNET, Console or other third-party SNMP software as well as ORing's proprietary management utility Open-Vision. The user-friendly and powerful interface of Open-Vision allows you to easily configure and monitor multiple switches at the same time.

1.2 Software Features

- Supports O-Ring (Recovery time < 10ms over 250 units connection)
- Supports Ring Coupling, Dual Homing over O-Ring and standard STP/RSTP/MSTP
- Supports SNMPv1/v2c/v3 & RMON & Port base/802.1Q VLAN Network Management
- Enable/disable ports, MAC based port security
- Port based network access control (802.1x)
- VLAN (802.1Q) to segregate and secure network traffic
- Radius centralized password management
- SNMPv3 encrypted authentication and access security
- Quality of Service (802.1p) for real-time traffic
- VLAN (802.1Q) with double tagging and GVRP supported
- IGMP Snooping for multicast filtering
- Port configuration, status, statistics, mirroring, security
- Remote Monitoring (RMON)
- Supports event notification by e-mail and SNMP traps
- Supports management via Web-based interfaces, Telnet, Console (CLI), and Windows utility (Open-Vision)

1.3 Hardware Features

- 10/100/1000Base-T(X) Gigabit Ethernet port
- 10/100Base-T(X) Ethernet port
- 100Base-FX Fiber port for FX series model
- 1000Base-X Fiber port for GF series model
- Console Port
- Redundant two DC power inputs on terminal block
- Wide Operating Temperature: -40 to 70oC

- Storage Temperature: -40 to 85oC
- Operating Humidity: 5% to 95%, non-condensing
- Casing: IP-30
- Dimensions(W x D x H) : 52 mm(W)x 106 mm(D)x 144 mm(H)

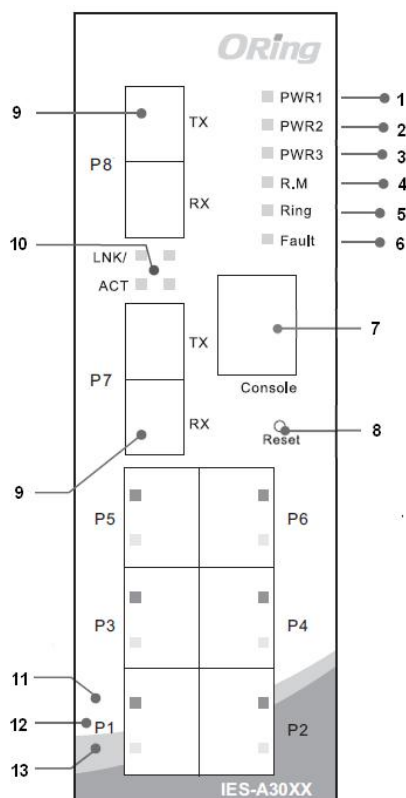
Hardware Overview

2.1 Front Panel

The following table describes the features on the IES-A3 series:

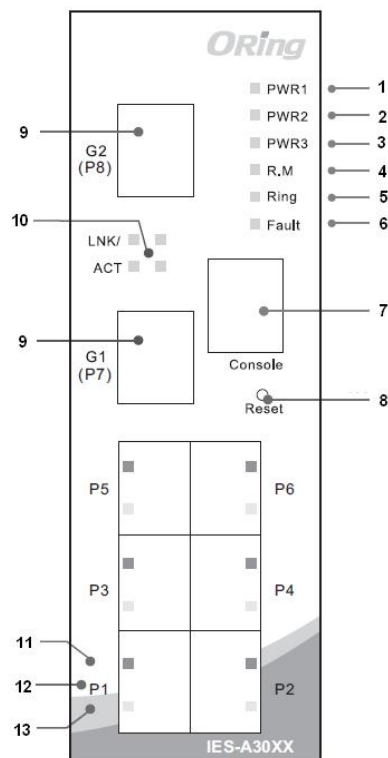
Port	Description
10/100 RJ-45 fast Ethernet ports	6 10/100Base-T(X) RJ-45 fast Ethernet ports supporting auto-negotiation. Default Setting: Speed: auto Duplex: auto Flow control: disable
Gigabit RJ-45 port	2 10/100/1000Base-TX Giga ports for IES-A3062GT
Fiber port	2 1000Base-X for IES-A3062GF Series 2 100Base-FX for IES-A3062FX Series
Console	Use RS-232 to RJ-45 cable to manage switch.
Reset	Press the reset button for 2 to 3 seconds to reset the switch or 5 seconds to reset the switch to Factory Default .

IES-A3 optical fiber series model



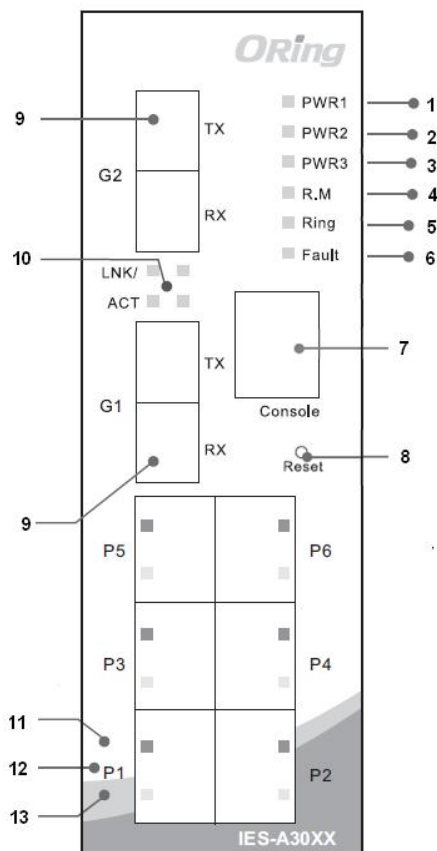
- | | |
|------------------------------|----------------------------------------|
| 1. LED for PWR1 | 9. 100BaseFX fiber port |
| 2. LED for PWR2 | 10. LED for fiber port link/act status |
| 3. LED for PWR3 | 11. LNK/ACT LED for LAN port |
| 4. LED for R.M (Ring master) | 12. 10/100Base-T(X) Ethernet ports |
| 5. LED for Ring status | 13. Full duplex LED for LAN port |
| 6. LED for fault relay | 14. Model names: |
| 7. Console port (RJ-45) | IES-A3062FX-MM-SC/IES-A3062FX-SS-SC |
| 8. Reset button | |

IES-A3 copper port series model



- | | |
|------------------------------|----------------------------------------------------------------------------------------------------|
| 1. LED for PWR1 | 8. Reset button |
| 2. LED for PWR2 | 9. 10/100/1000Base-T(X) Ethernet port (IES-A3062GT);
10/100Base-T(X) Ethernet ports (IES-A3080) |
| 3. LED for PWR3 | 10. LED for G1/G2 (IES-A3062GT) or P7/P8 LAN
(ES-A3080) port status |
| 4. LED for R.M (Ring master) | 11. LNK/ACT LED for LAN port |
| 5. LED for Ring status | 12. 10/100Base-T(X) Ethernet ports |
| 6. LED for fault relay | 13. Full duplex LED for LAN port |
| 7. Console port (RJ-45) | 14. Model names: IES-A3080/IES-A3062GT |

IES-A3 Gigabit optical fiber series model



- | | |
|------------------------------|----------------------------------------|
| 1. LED for PWR1 | 9. 1000Base-X optical fiber port |
| 2. LED for PWR2 | 10. LED for fiber port link/act status |
| 3. LED for PWR3 | 11. LNK/ACT LED for LAN port |
| 4. LED for R.M (Ring master) | 12. 10/100Base-T(X) Ethernet ports |
| 5. LED for Ring status | 13. Full duplex LED for LAN port |
| 6. LED for fault relay | 14. Model names: |
| 7. Console port (RJ-45) | IES-A3062GF-MM-SC/IES-A3062GF-SS-SC |
| 8. Reset button | |

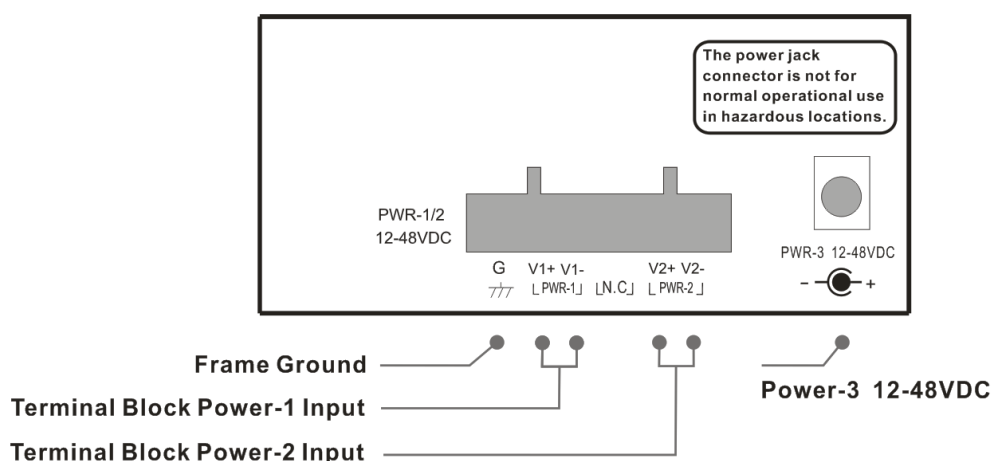
2.2 Front Panel LEDs

LED	Color	Status	Description
PWR1	Green	On	DC power module 1 activated
PWR2	Green	On	DC power module 2 activated
R.M	Green	On	Port running as O-Ring Master
Ring	Green	On	O-Ring enabled
		Slowly blinking	O-Ring topology has problems

		Fast blinking	O-Ring works normally
Fault	Amber	On	Faulty relay (power failure or port malfunctioning)
10/100Base-T(X) Fast Ethernet ports			
LNK / ACT	Green	On	Ports are linked
		Blinking	Transmitting data
Full Duplex	Amber	On	Ports running in full duplex mode
Gigabit Ethernet ports			
ACT	Green	On	Ports are linked
		Blinking	Transmitting data
LNK	Amber	On	Ports are linked
Fiber ports			
ACT	Green	On	Ports are linked
		Blinking	Transmitting data
LNK	Amber	On	Ports are linked
Fiber ports			
LNK / ACT	Green	On	Ports are linked
		Blinking	Transmitting data

2.3 Top Panel

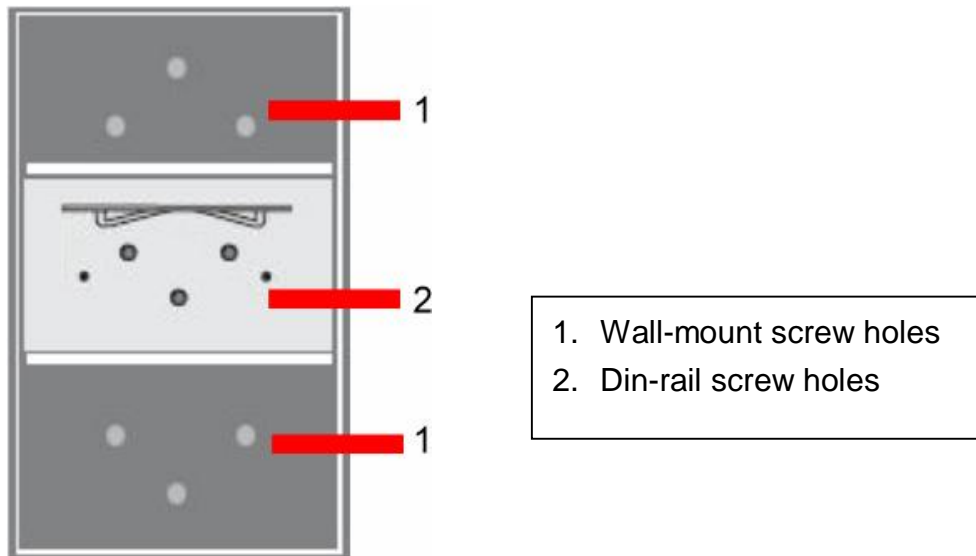
Below are the top panel components of IES-A3 series:



WARNING – POWER JACK CONNECTOR NOT FOR USE IN HAZARDOUS LOCATIONS. SEE INSTALLATION INSTRUCTIONS

2.4 Rear Panel

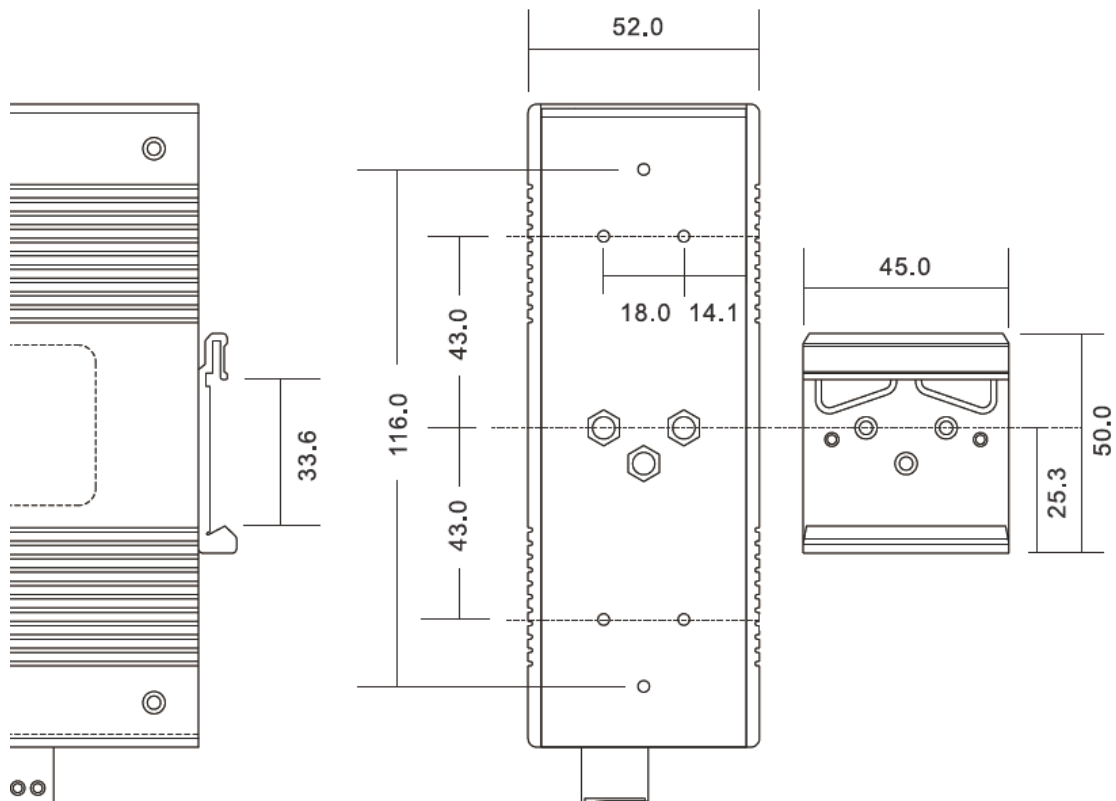
On the rear panel of the switch sit three sets of screw holes. The two sets placed in triangular patterns on top and bottom of the rear panel are used for wall-mounting and the set of four holes in the middle are used for Din-rail installation. For more information on installation, please refer to [錯誤! 找不到參照來源。 Din-rail Installation](#).



Hardware Installation

3.1 DIN-rail Installation

The series can be fastened to a DIN-rail using a DIN-rail kit which can be found in the package.



Din-rail Kit Measurement

Installing the switch on the DIN-rail is easy. Simply follow the steps below.

Step 1: Screw the DIN-rail kit to the back of the switch.

Step 2: Slant the switch and mount the metal spring to the DIN-rail.

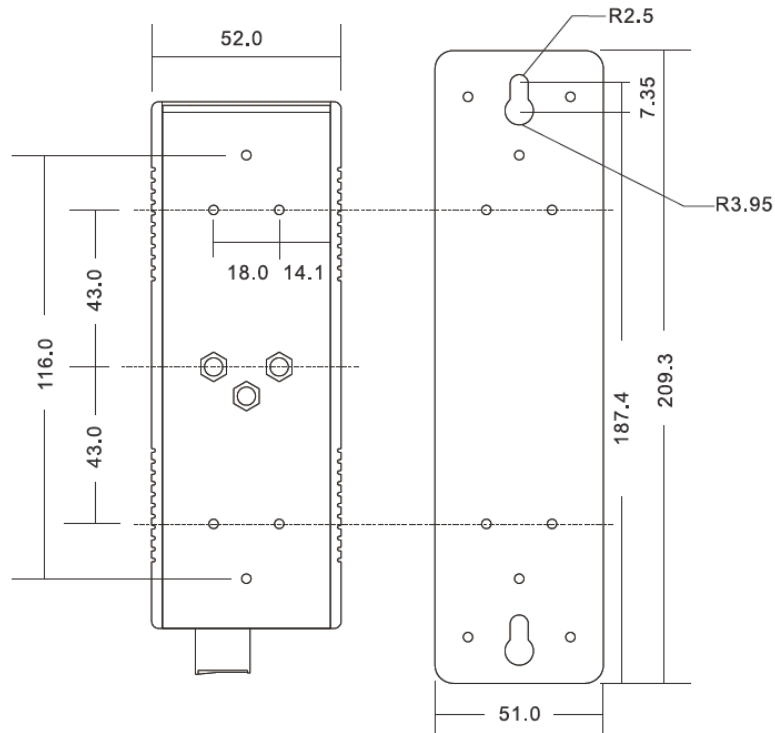


Step 2: Push the switch toward the DIN-rail until you hear a “click” sound.



3.2 Wall Mounting

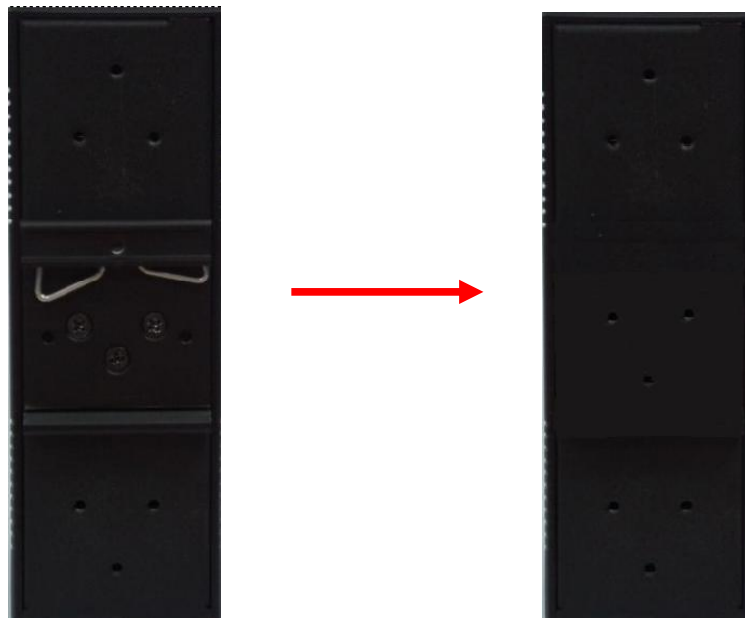
The series can also be fixed to the wall via a wall mount panel, which can be found in the package.



Wall-Mount Kit Measurement

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

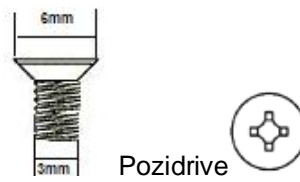
Step 1: Remove DIN-rail kit.



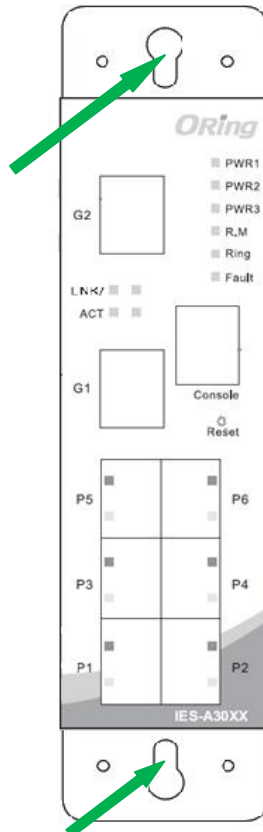
Step 2: Use the 6 screws found in the package to attach the wall mount kit to the switch, as shown below:



Below are the screw specifications. To protect the switch from any damage, the screws should not be larger than the size used in the IES-A3 series switches.



Step 3: Mount the switch to the wall by inserting screws through the holes of the wall-mount kit.



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 Redundant Power Inputs

The switch has two sets of power inputs, power input 1 and power input 2, which sit on the terminal block. 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 Ethernet Cables

The IES-A3 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 (328ft)	RJ-45
100BASE-TX	Cat.5 100-ohm UTP	UTP 100 m (328ft)	RJ-45
1000BASE-TX	Cat.5/Cat.5e 100-ohm UTP	UTP 100 m (328ft)	RJ-45

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

With 10/100/1000BASE-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 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-A3 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-TX and 1000Base-T MDI and MDI-X port pin outs.

10/100 Base-TX MDI/MDI-X pins 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

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

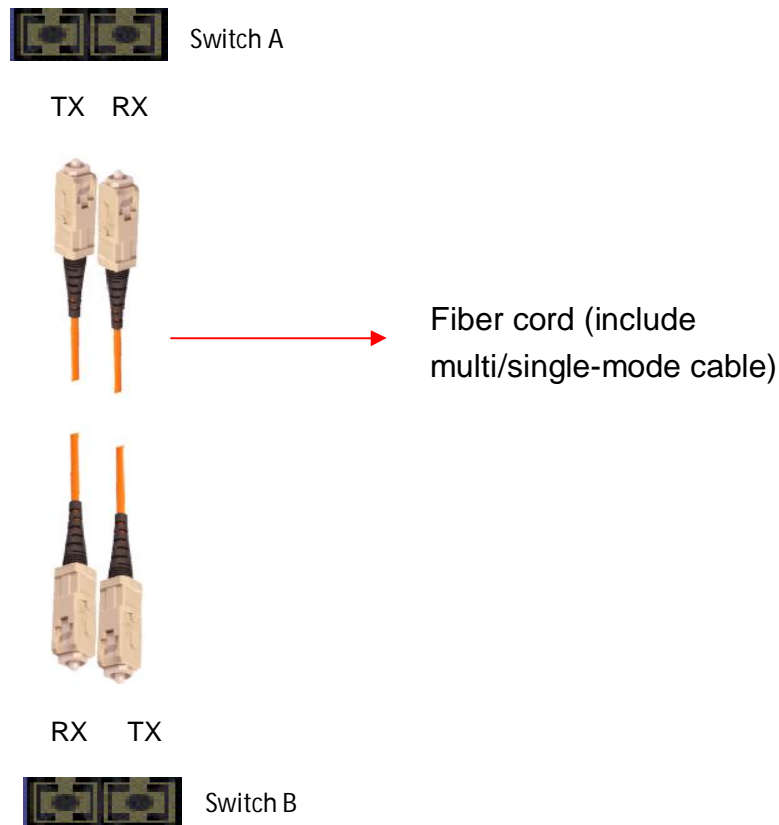
1000 Base-T MDI/MDI-X pins assignments

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.

3.4.2 Fibers

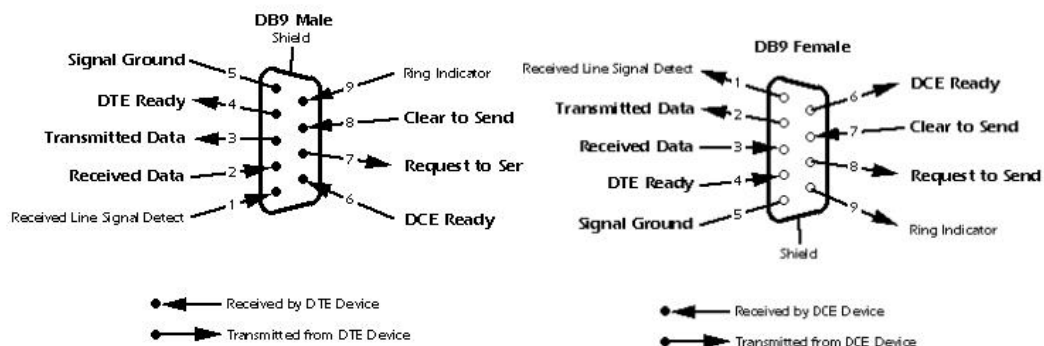
The IES-A3 optical fiber series provide optical fiber functions to extend transmission distances; the optical fiber ports support multi-mode or single-mode with SC connectors. Remember that the TX port of Switch A should be connected to the RX port of Switch B.



3.4.3 RS-232 Console Port

The IES-A3 series switches can be managed via a console port using a RS-232 (DB-9 to RJ-45) cable which can be found in the package. You can connect the port to a PC using the RS-232 cable with the DB-9 female connector connecting to the PC and the RJ-45 connector connecting 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

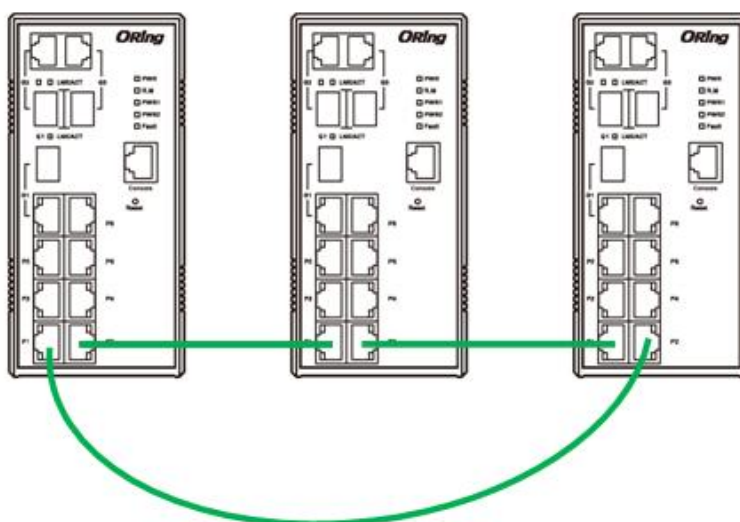


3.4.4 O-Ring

O-Ring

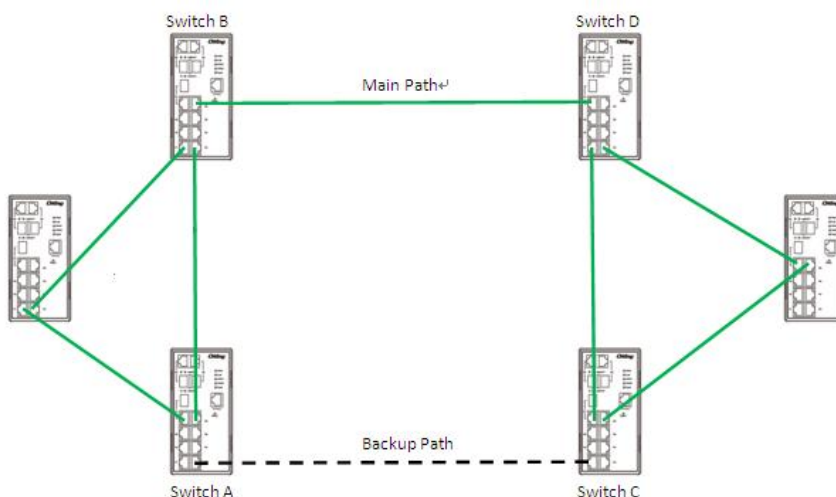
You can connect three or more switches to form a ring topology to gain network redundancy capabilities through the following steps.

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 [錯誤! 找不到參照來源。 Configurations](#).
3. Connect the last switch to the first switch to form a ring topology.



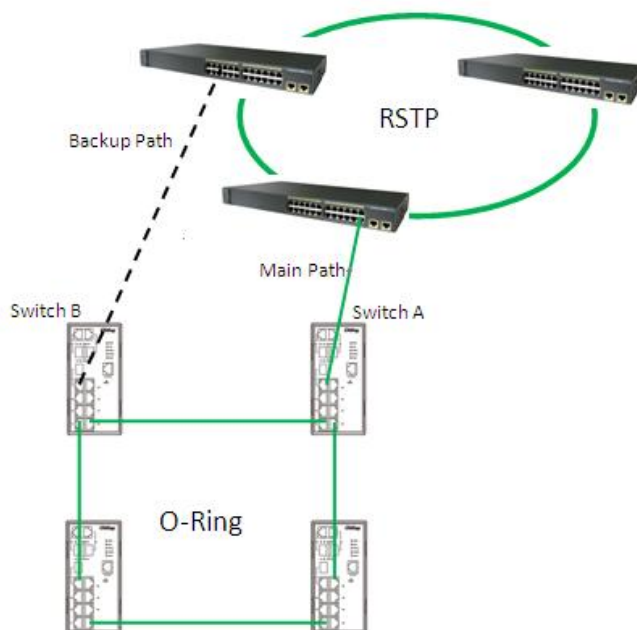
Coupling Ring

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 [錯誤! 找不到參照來源。 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.



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**

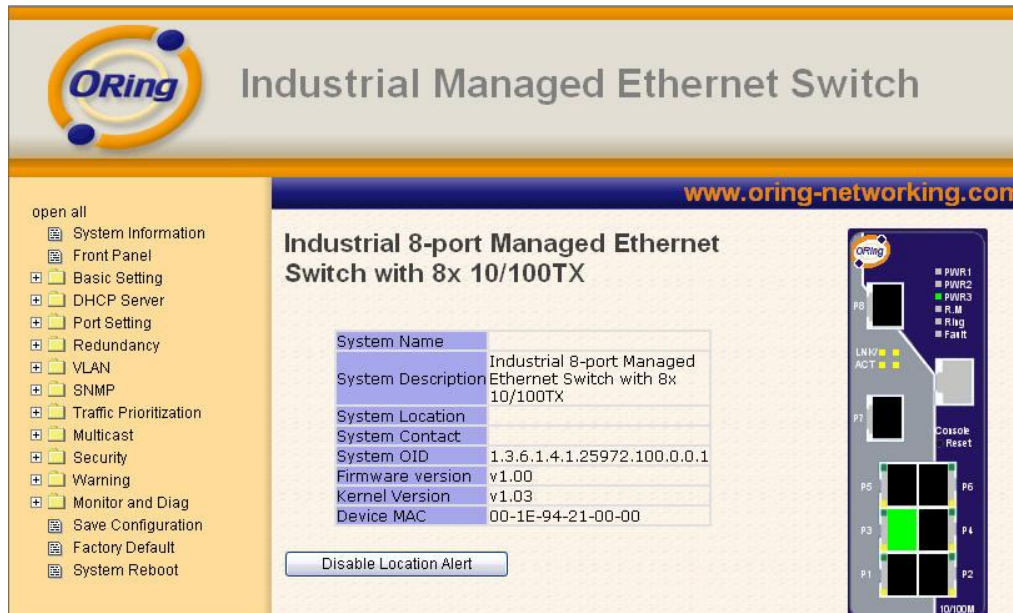
Subnet Mask: **255.255.255.0**

Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

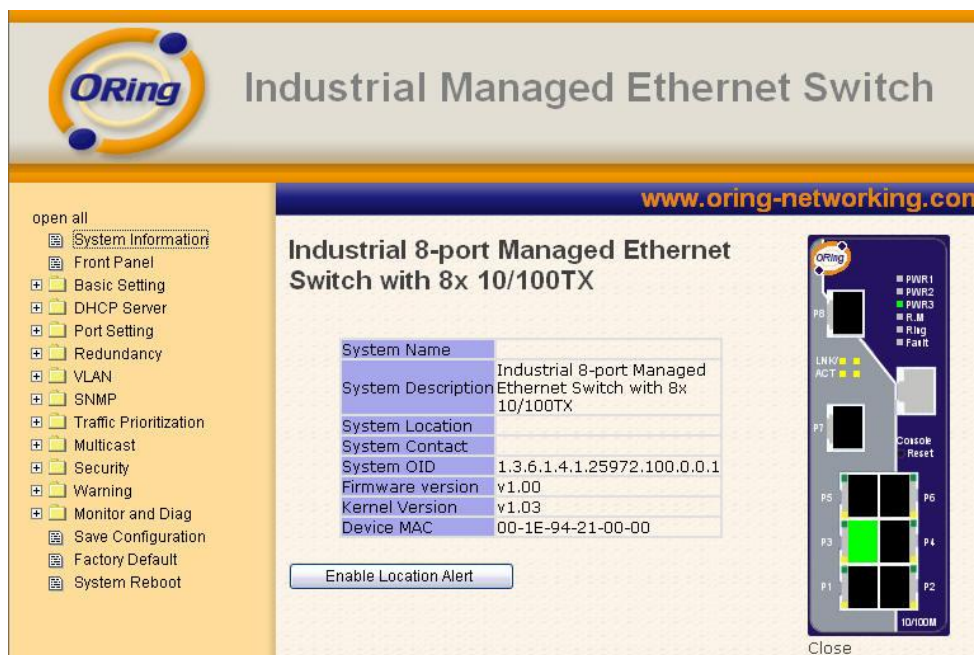
After logging in, you will see the information of the switch as below.



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.

4.1 System Information

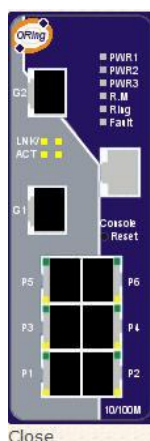
This page shows the general information of the switch.



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.
SNMP OID	Shows the OID of the SNMP message
Firmware Version	Shows the version of the current firmware
Kernel Version	Shows the version of the current kernel
MAC Address	Show the MAC address of the device
System Uptime	Shows the period of time since the system starts operation
Enable Location Alert	Check to enable location alert function
Help	Shows Help file

4.2 Front Panel

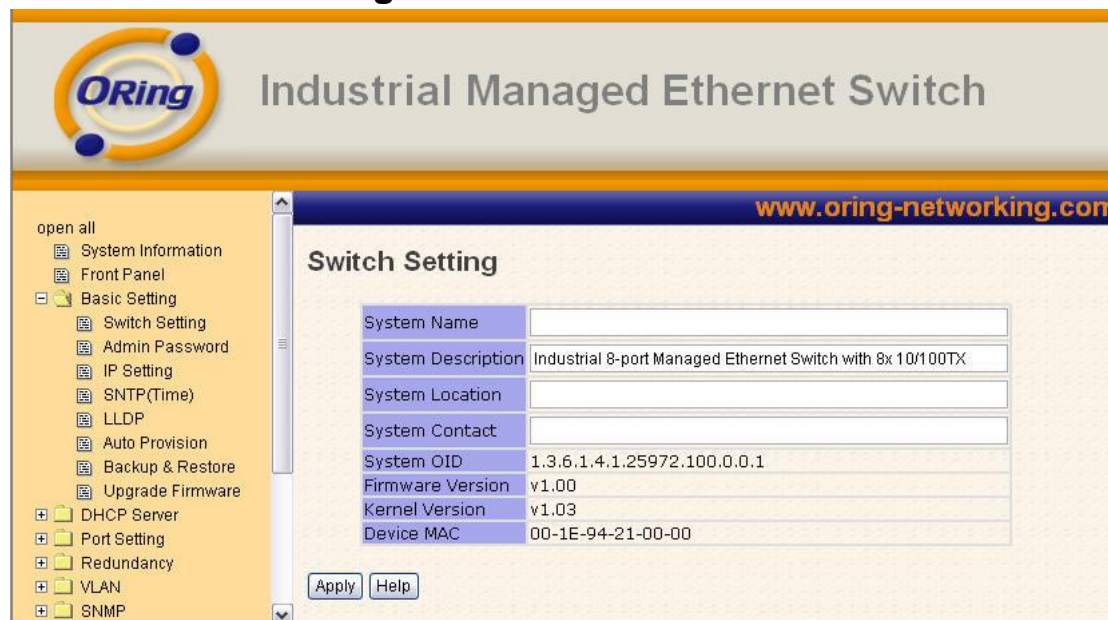
On the right hand side shows a picture of the front panel of the device which LED indication corresponding to the physical device. Click **Close** to close the image.



4.3 Basic Setting

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

4.3.1 Switch Setting



Label	Description
System Name	Assigns the name of switch. The maximum length is 64 bytes
System Description	Description of the device
System Location	Assigns physical switch location. The maximum length is 64 bytes
System Contact	Information of the contact person or organization
System OID	Displays the switch's OID information
Firmware Version	Displays the switch's firmware version
Kernel Version	Displays the kernel software version
MAC Address	Displays the unique hardware address assigned by manufacturer (default)

4.3.2 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.

4.3.3 IP Setting

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.

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

4.3.4 Time Setting

This page allows you to configure SNTP and system clock.

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.

Label	Description
SNTP Client	Enables or disables SNTP function to retrieve the time from a SNTP server.
Daylight Saving Time	Enables or disables daylight saving time function. When it is enabled, you need to configure the daylight saving time period.
UTC Timezone	Selects the time zone for the switch according to its location

SNTP Sever IP Address	Enters the SNTP server IP address which you would like to use for time synchronization.
Current System Time	Shows the current time of the system
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 Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

PTP Client

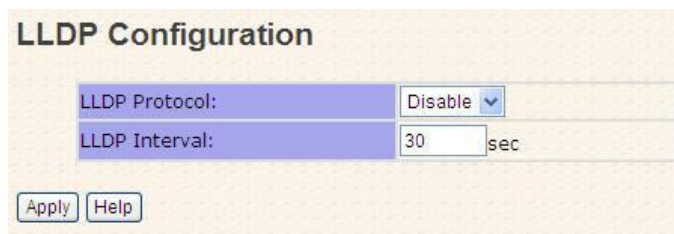
The Precision Time Protocol (PTP) is a time-transfer protocol defined in the IEEE 1588-2002 standard that allows precise synchronization of networks (e.g., Ethernet). Accuracy within the nanosecond range can be achieved with this protocol when using hardware generated timestamps.



Label	Description
PTP Client	Enables or disables PTP Client

4.3.5 LLDP

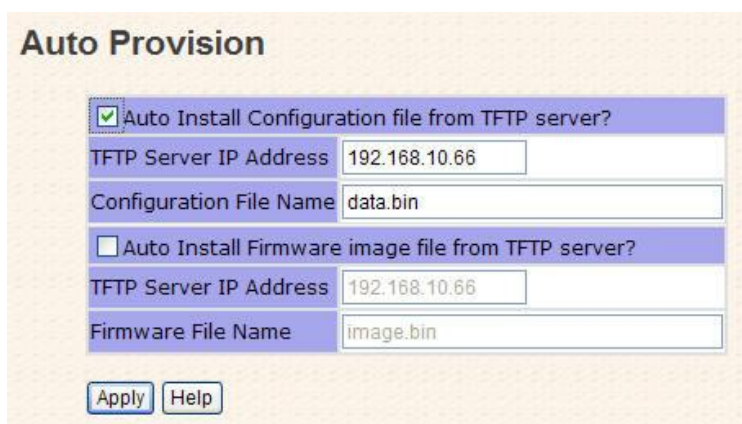
LLDP (Link Layer Discovery Protocol) provides a method for networked devices to receive and/or transmit their information to other connected devices on the network that are also using the protocols, and to store the information that is learned about other devices. This page allows you to examine and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

4.3.6 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.



4.3.7 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 restore the system to previous configurations from a TFTP server or save the existing configurations as a backup file to a TFTP server.

Backup & Restore

Restore Configuration

TFTP Server IP Address: 192.168.10.66

Restore File Name: data.bin

Restore Help

Backup Configuration

TFTP Server IP Address: 192.168.10.66

Backup File Name: data.bin

Backup Help

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.
Restore	Click to restore the configurations.

4.3.8 Upgrade Firmware

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

TFTP Server IP: 192.168.10.66

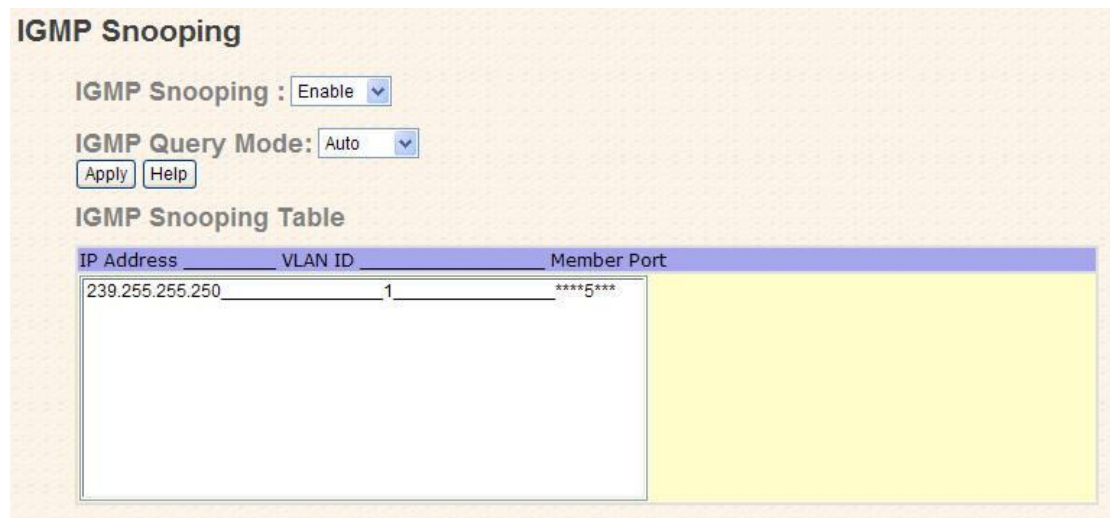
Firmware File Name: image.bin

Upgrade Help

4.4 Multicast

4.4.1 IGMP Snooping

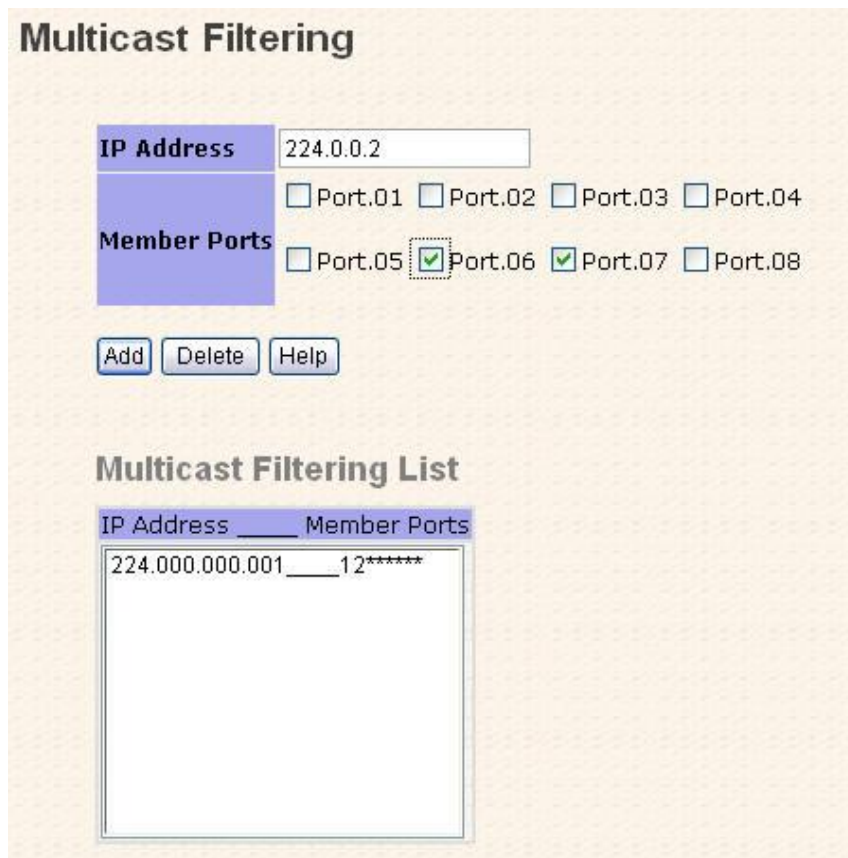
IGMP (Internet Group Management Protocol) snooping monitors the IGMP traffic between hosts and multicast routers. The switch uses what IGMP snooping learns to forward multicast traffic only to interfaces that are connected to interested receivers. This conserves bandwidth by allowing the switch to send 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.



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.
IGMP Snooping Table	Shows a list of current IP multicast
Apply	Click to apply the configurations.
Help	Shows help file.

4.4.2 Multicast Filter

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.



Label	Description
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.

4.5 Port Setting

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

4.5.1 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
G1	Enable	AutoNegotiation	Symmetric	Disable
G2	Enable	AutoNegotiation	Symmetric	Disable

Apply Help

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.
Apply	Click to apply the configurations

4.5.2 Port Status

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

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
Port.05	100TX	UP	Enable	100 Full	Disable
Port.06	100TX	Down	Enable	N/A	N/A
G1	1000TX	Down	Enable	N/A	N/A
G2	1000TX	Down	Enable	N/A	N/A

4.5.3 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	<input type="text"/>
Port.02	<input type="text"/>
Port.03	<input type="text"/>
Port.04	<input type="text"/>
Port.05	<input type="text"/>
Port.06	<input type="text"/>
G1	<input type="text"/>
G2	<input type="text"/>

4.5.4 Rate Limit

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

Rate Limiting

	Ingress Limit Frame Type	Ingress	Egress
Port.01	All <input type="text"/>	0 kbps	0 kbps
Port.02	All <input type="text"/>	0 kbps	0 kbps
Port.03	All <input type="text"/>	0 kbps	0 kbps
Port.04	All <input type="text"/>	0 kbps	0 kbps
Port.05	All <input type="text"/>	0 kbps	0 kbps
Port.06	All <input type="text"/>	0 kbps	0 kbps
G1	All <input type="text"/>	0 kbps	0 kbps
G2	All <input type="text"/>	0 kbps	0 kbps

Rate range is from 100 kbps to 102400 kbps (i.e. 100Mbps) for mega-ports, or 256000 kbps (i.e. 250Mbps) for giga-ports. Zero means no limit.

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.

4.5.5 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	Trunk 1	Static
Port.02	Trunk 1	Static
Port.03	None	Static
Port.04	None	Static
Port.05	None	Static
Port.06	None	Static
G1	None	Static
G2	None	Static

Note: the types should be the same for all member ports in a group.

Apply Help

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.
Apply	Click to activate the configurations.

Port Trunk - Status

Group ID	Trunk Member	Type
Trunk 1	1, 2	Static
Trunk 2		Static
Trunk 3		Static
Trunk 4		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

4.6 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

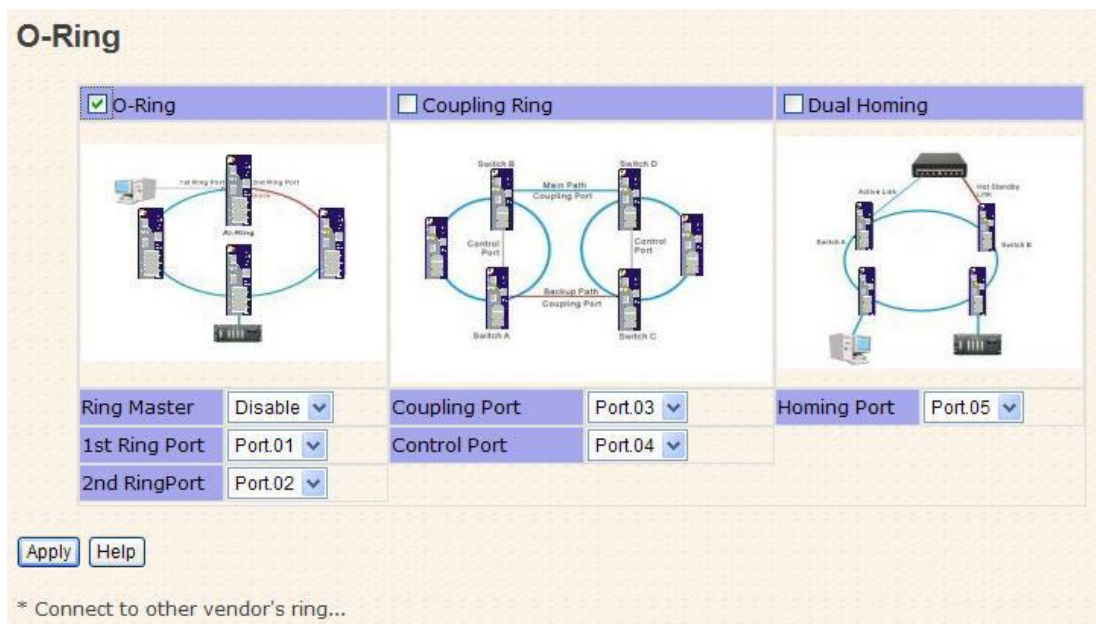
4.6.1 O-Ring

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.



Configuration

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



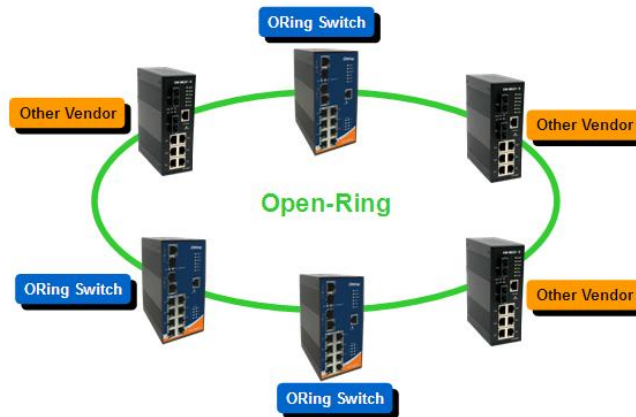
Label	Description
O-Ring	Check to enable O-Ring topology.
Ring Master	Only one ring master is allowed in a ring. However, if more than one switches are set to enable Ring Master , the switch with the lowest MAC address will be the active ring master and the others will be backup masters.
1st Ring Port	The primary port when the switch is ring master
2nd Ring Port	The backup port when the switch is ring master
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.
Coupling 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.
Control Port	Set a port as control port to link to the control port of the switch in the same ring. The control port is used to transmit control signals.
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.
Homing Port	Assigns a port as home port which will be used as a backup port in the ring.
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.

4.6.2 Open-Ring

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.



Configuration

O-Ring

<input checked="" type="checkbox"/> O-Ring	<input type="checkbox"/> Coupling Ring	<input type="checkbox"/> Dual Homing
Ring Master: Disable	Coupling Port: Port.03	Homing Port: Port.05
1st Ring Port: Port.01	Control Port: Port.04	
2nd RingPort: Port.02		

Apply Help

* Connect to other vendor's ring..

By clicking **Connect to other vendor's ring.....**, you will join the ring built by other vendors.

Open-Ring

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

Apply

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

4.6.3 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.

Setting

RSTP Setting

RSTP Mode Enable ▾

Bridge Configuration

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

Port Configuration

Port	Path Cost (1-200000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non STP
1	200000	128	Auto ▾	True ▾	False ▾
2	200000	128	Auto ▾	True ▾	False ▾
3	200000	128	Auto ▾	True ▾	False ▾
4	200000	128	Auto ▾	True ▾	False ▾
5	200000	128	Auto ▾	True ▾	False ▾
6	200000	128	Auto ▾	True ▾	False ▾
7	200000	128	Auto ▾	True ▾	False ▾
8	200000	128	Auto ▾	True ▾	False ▾

Apply Help

Label	Description
RSTP mode	Enables or disables RSTP mode.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest priority is selected as the root. If more than one bridges have the same priority, the one with the lowest MAC address will be selected. 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 STP configuration messages before attempting a reconfiguration. The valid value is between 6 and 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 and 10.
Forward 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 and 30.
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 20000000.
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.
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.

RSTP Information

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

RSTP Information

Root Bridge Information

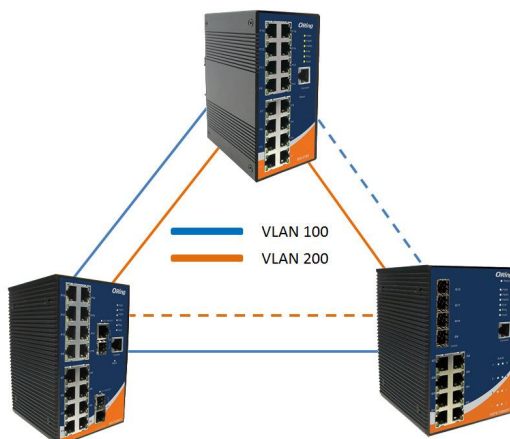
Bridge ID	0080001123455789
Root Priority	32768
Root Port	Root
Root Path Cost	0
Max Age Time	20
Hello Time	2
Forward Delay Time	15

Port Information

Port	Path Cost	Port Priority	OperP2P	OperEdge	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	Forwarding	Designated
Port.06	200000	128	True	True	False	Disabled	Disabled
G1	20000	128	True	True	False	Disabled	Disabled
G2	20000	128	True	True	False	Disabled	Disabled

4.6.4 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.



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 Setting

MSTP Enable	Disable ▾
Force Version	MSTP ▾
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*(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*(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.
Forward 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.

MSTP Port

Port No.	Priority (0-240)	Path Cost (1-200000000, 0:Auto)	Admin P2P	Admin Edge	Admin Non Stp
Port.01					
Port.02					
Port.03	128	0	auto	true	false
Port.04					
Port.05					

priority must be a multiple of 16

Apply Help

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.

MSTP Instance

Instance	State	VLANs	Priority (0-61440)
1	Enable	1-4094	32768

Priority must be a multiple of 4096.

Apply Help

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)
Port.01		
Port.02		
Port.03	128	0
Port.04		
Port.05		

Priority must be a multiple of 16

Apply Help

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 (1-200000000)	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.
Apply	Click to apply the configurations.

4.7 VLAN

4.7.1 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 Configuration

VLAN Operation Mode :

GVRP Mode :

Management Vlan ID :

VLAN Configuration

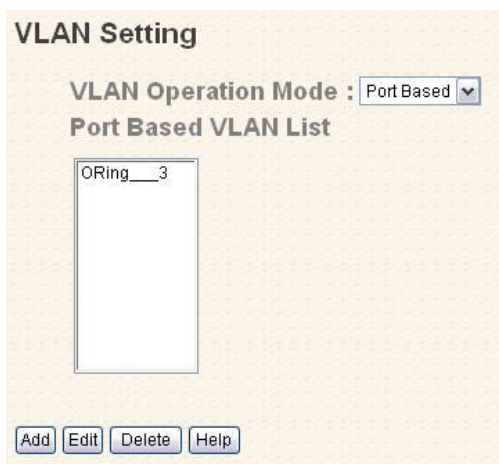
Port No.	Link Type	Untagged VID	Tagged VIDs
Port.03	Access	<input type="text" value="1"/>	<input type="text"/>
Port.04	Access	<input type="text" value="1"/>	<input type="text"/>
Port.05	Access	<input type="text" value="1"/>	<input type="text"/>
Port.06	Access	<input type="text" value="1"/>	<input type="text"/>
G1	Access	<input type="text" value="1"/>	<input type="text"/>
G2	Access	<input type="text" value="1"/>	<input type="text"/>
Trunk.1	Access	<input type="text" value="1"/>	<input type="text"/>

Note: Use the comma to separate the multiple tagged VLANs.
E.g., 2,3,4 means joining the Tagged VLAN 2,3 and 4.

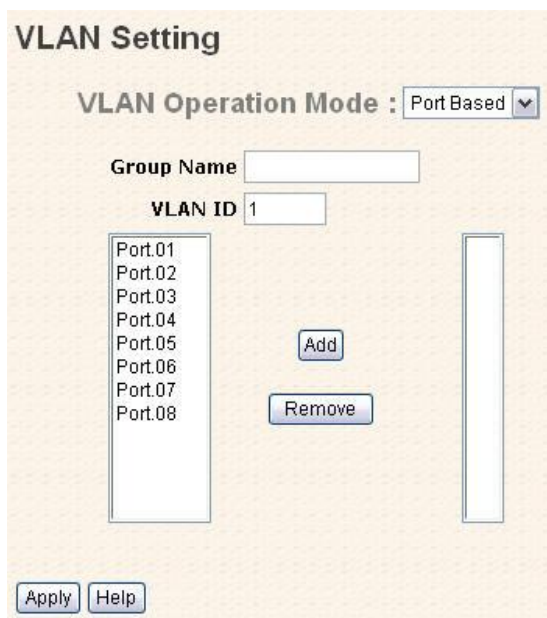
Label	Description
VLAN Operation Mode	Available options include Disable , Port Base , and 802.1Q
GVRP Mode	GVRP is a GARP application that provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. With GVRP, the switch can exchange VLAN configuration information with 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	<p>Three link types are available:</p> <p>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).</p> <p>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.</p> <p>Hybrid Link: The combination of Access Link and Trunk Link. 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.

Port Based

Packets can only be sent to members in the same VLAN group. All unselected ports will be treated as belonging to another single VLAN. If port-based VLAN is enabled, the VLAN-tagging is ignored.



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.



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.

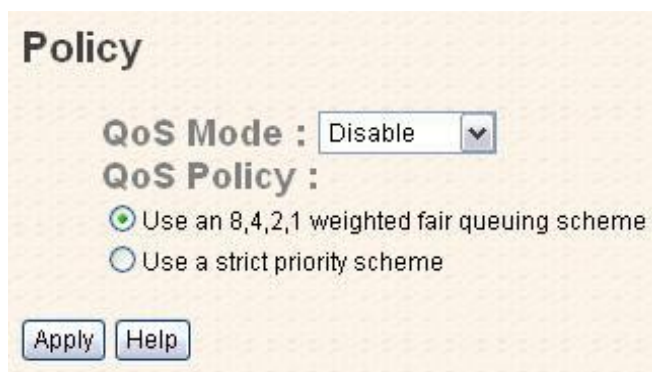
4.8 Traffic Prioritization

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.

4.8.1 QoS Policy

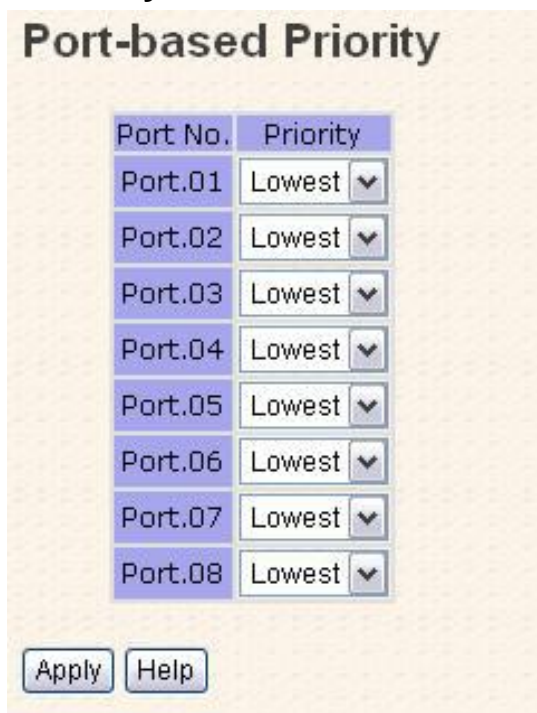
Policing is a traffic regulation mechanism for limiting the rate of traffic streams, thereby controlling the maximum rate of traffic sent or received on an interface. When the traffic rate exceeds the configured maximum rate, policing drops or remarks the excess traffic. This page allows you to configure QoS policies for the switch.



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

	<p>COS first.</p> <p>TOS first: the output priority is determined by COS and TOS, but TOS first.</p>
QOS policy	<p>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.</p> <p>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.</p>
Apply	Click to apply the configurations
Help	Shows help file.

4.8.2 Port-base Priority

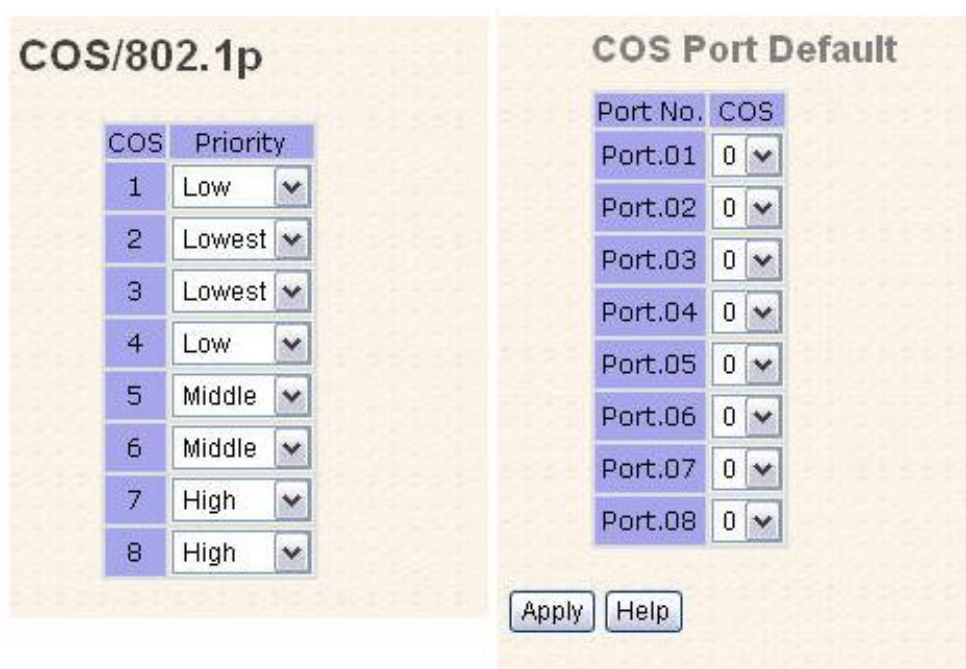


Label	Description
Priority	Assigns a port to a priority queue. Four priority queues are available: High , Middle , Low , and Lowest .

Apply	Click to apply the configurations
Help	Shows help file.

4.8.3 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.



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.

4.8.4 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 ▾

Apply Help

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.

4.9 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.

4.9.1 Setting

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.



Label	Description
DHCP Server	Enables or disables DHCP server function. When enabled, the switch will become the DHCP server on your local network.
Start 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.
End 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 (Hour)	The length of time that the client may use the IP address it has been assigned. The time is measured in hours.
Apply	Click to apply the configurations

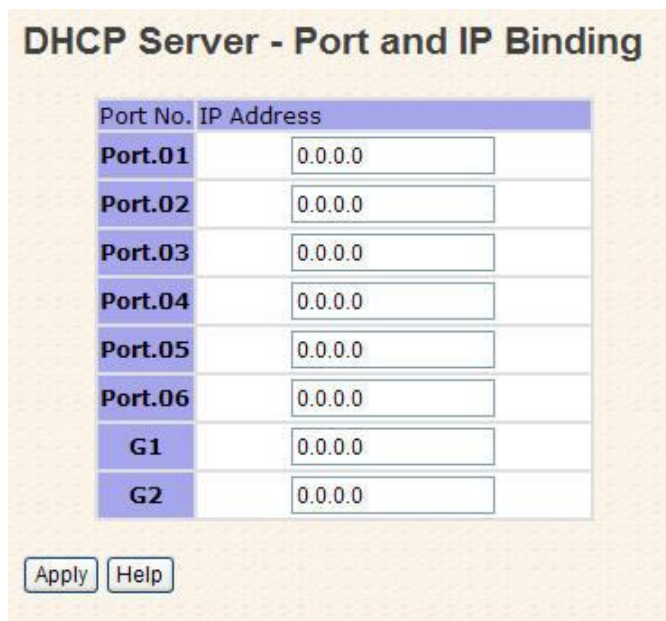
4.9.2 Client List

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



4.9.3 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.



4.10SNMP

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.

4.10.1 Agent Setting

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

SNMP V1/V2c Community

Community String	Privilege
public	Read Only
private	Read and Write
	Read Only
	Read Only

SNMPv3 User

User Name	<input type="text"/>
Auth Password	<input type="text"/>
Privacy Password	<input type="text"/>

Current SNMPv3 User Profile

User Name	Auth. Password	Priv. Password

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	Choose the appropriate access level from the dropdown list. Read Only: The community string can only read the values of MIB objects.

	<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>
SNMPv3User	<p>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.</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>
Apply	Click to apply the configurations

4.10.2 Trap Setting

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.



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

4.11 Security

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

4.11.1 IP Security

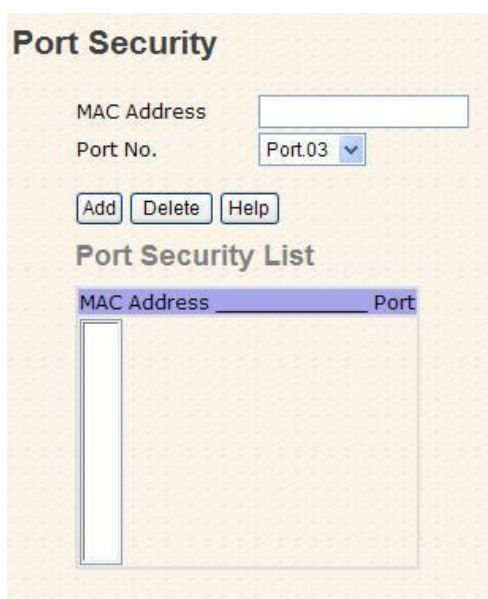
By setting up a secure IP list, only IP addresses in the list can manage the switch according to the management mode you have specified (WEB, Telnet, SNMP, etc.).

Label	Description
IP Security Mode	Indicates IP security mode. Enables or disables IP security

		functions.
Enable Management	WEB	Check to enable WEB management
Enable Management	Telnet	Check to enable Telnet management
Enable Management	SNMP	Check to enable MPSN management
Apply		Click to apply the configurations.
Help		Shows help file.

4.11.2 Port Security

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.

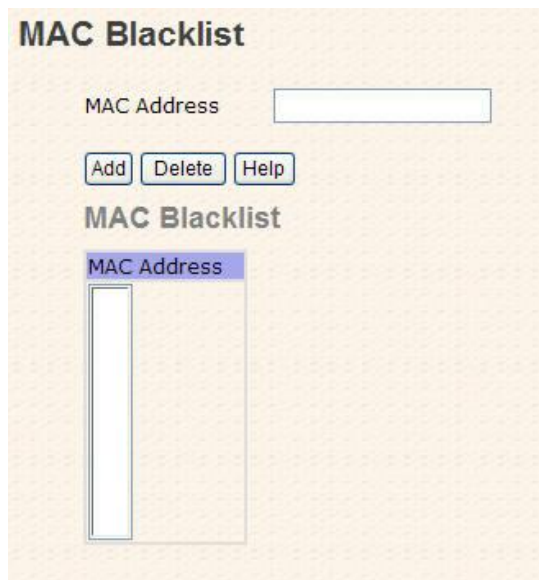


Label	Description
MAC Address	Enter a MAC address for a specific port.
Port NO.	Select a switch port
Add	Add the MAC address and port information.
Delete	Deletes an entry
Help	Shows help file

4.11.3 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.



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

4.11.4 802.1x

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	Disable ▼
Radius Server IP	192.168.16.3
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

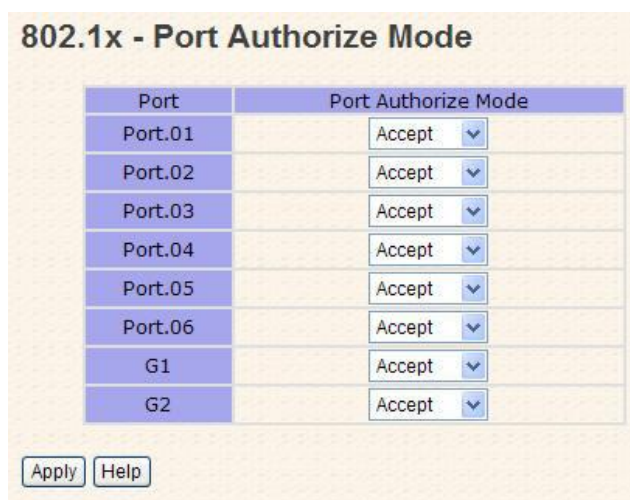
Advanced Setting

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

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:



Label	Description
Port Authorize Mode	Reject: force the port to be unauthorized Accept: force the port to be authorized

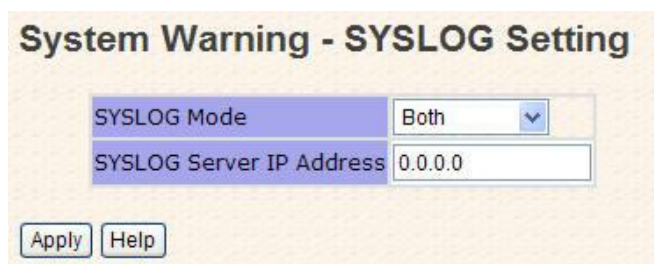
	<p>Authorize: the state of the port is determined by the outcome of the 802.1x authentication</p> <p>Disable: the port will not participate in the 802.1x portocol</p>
Apply	Click to apply the configurations
Help	Shows help file

4.12 Warning

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

4.12.1 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	<p>Disable: disables SYSLOG</p> <p>Client Only: logs in to a local system</p> <p>Server Only: logs in to a remote SYSLOG server</p> <p>Both: logs in to a local and remote server.</p>
SYSLOG Server IP Address	The IP address of the remote SYSLOG server
Apply	Click to apply the configurations
Help	Shows help file

4.12.2 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.

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

4.12.3 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.

System Warning - Event Selection

System Event

Event	SYSLOG	SMTP
System Cold Start	<input type="checkbox"/>	<input type="checkbox"/>
Power Status	<input type="checkbox"/>	<input type="checkbox"/>
SNMP Authentication Failure	<input type="checkbox"/>	<input type="checkbox"/>
O-Ring Topology Change	<input type="checkbox"/>	<input type="checkbox"/>

Port Event

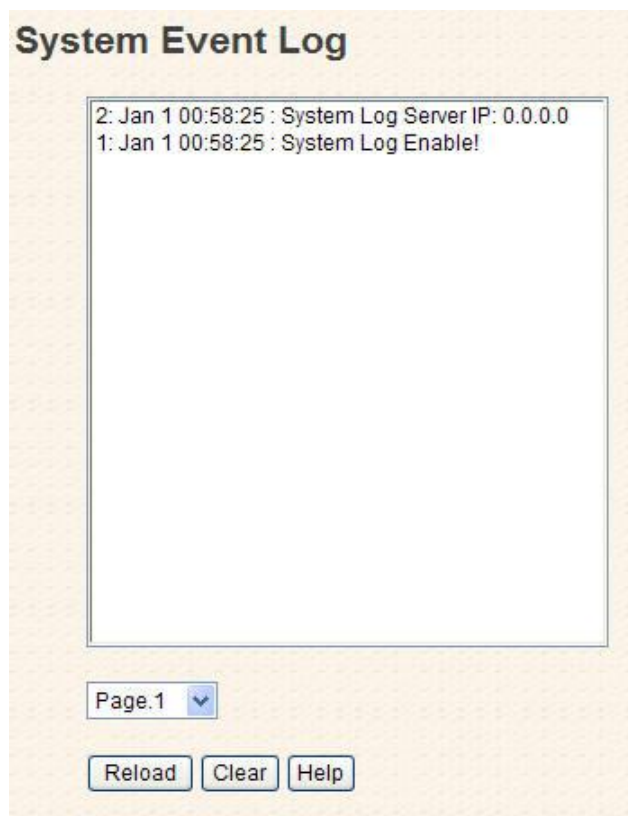
Port No.	SYSLOG	SMTP
Port.01	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.02	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.03	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.04	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.05	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.06	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
G1	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
G2	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>

Label	Description
System Cold Start	Sends alerts when you restart the device using the power button on your PC.
Power Status	Sends alerts when power is up or down.
SNMP Authentication Failure	Sends alerts when SNMP authentication fails
O-Ring Topology Chang	Sends alerts when O-Ring topology changes
Port Event SYSLOG/SNMP	<p>Sends alerts when a 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

4.13 Monitor and Diag

4.13.1 System Event Log

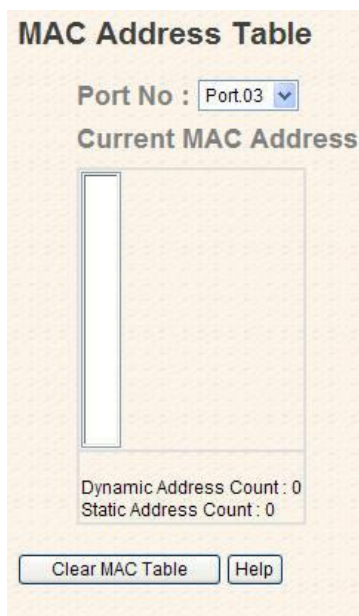
If a system log client is enabled, the system event log will be shown in this table.



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

4.13.2 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 table
Clear MAC 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.



Label	Description
MAC Address Table Aging Time	Sets the aging time for a MAC address table. The valid value ranges from 0 to 3825 and the default setting is 300 secs.
Auto Flush MAC Address Table When ports Link Down	Check to enable this function. Once enabled, the system will clear the MAC address table automatically when a port is disconnected.

Apply	Click to activate the configurations
Help	Shows help file

Port Statistics

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

Port Statistics

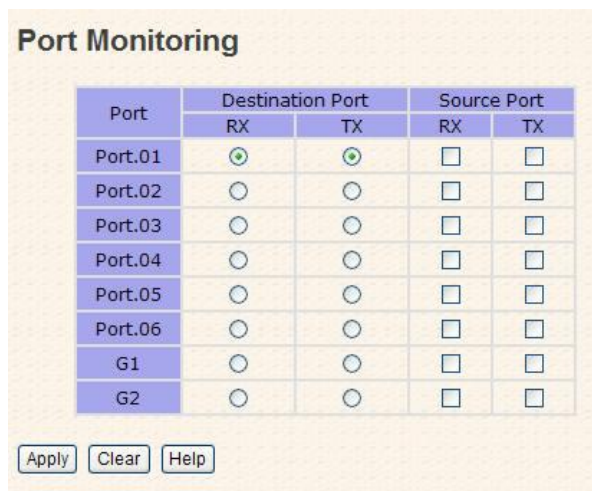
Port	Type	Link	State	TX Good Packet	TX Bad Packet	RX Good Packet	RX Bad Packet	TX Abort Packet	Packet Collision
Port.01	100TX	Down	Enable	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0
Port.05	100TX	Up	Enable	11430	0	22683	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0
G1	1000TX	Down	Enable	0	0	0	0	0	0
G2	1000TX	Down	Enable	0	0	0	0	0	0

Clear Help

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 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.



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

4.13.3 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.

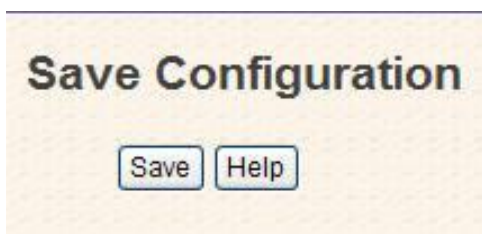


Label	Description
IP Address	Enter the IP address that you want to detect
Active	Click to send ICMP packets

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.

4.14 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

4.14.1 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.



4.14.2 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.

System Reboot

Please click **[Reboot]** button to restart switch device.

Reboot

Command Line Interface Management

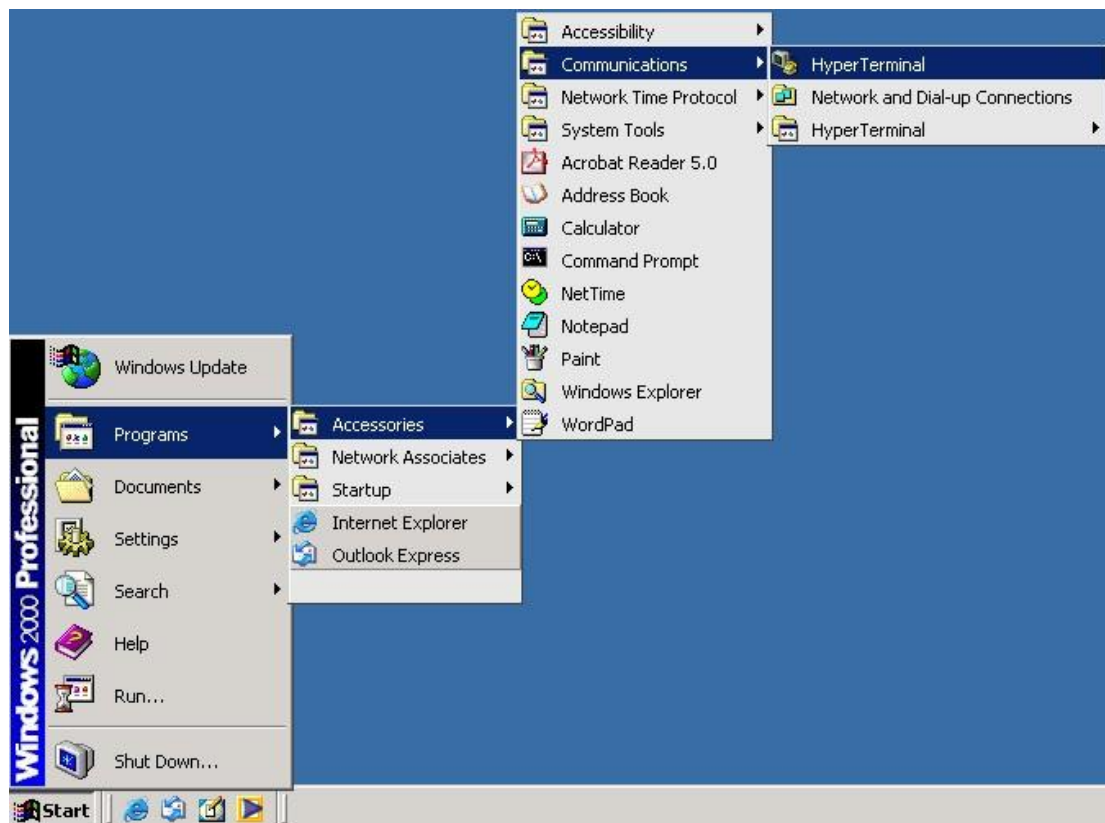
Besides Web-based management, the switch also supports CLI management. You can use console or telnet to manage the switch by CLI.

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

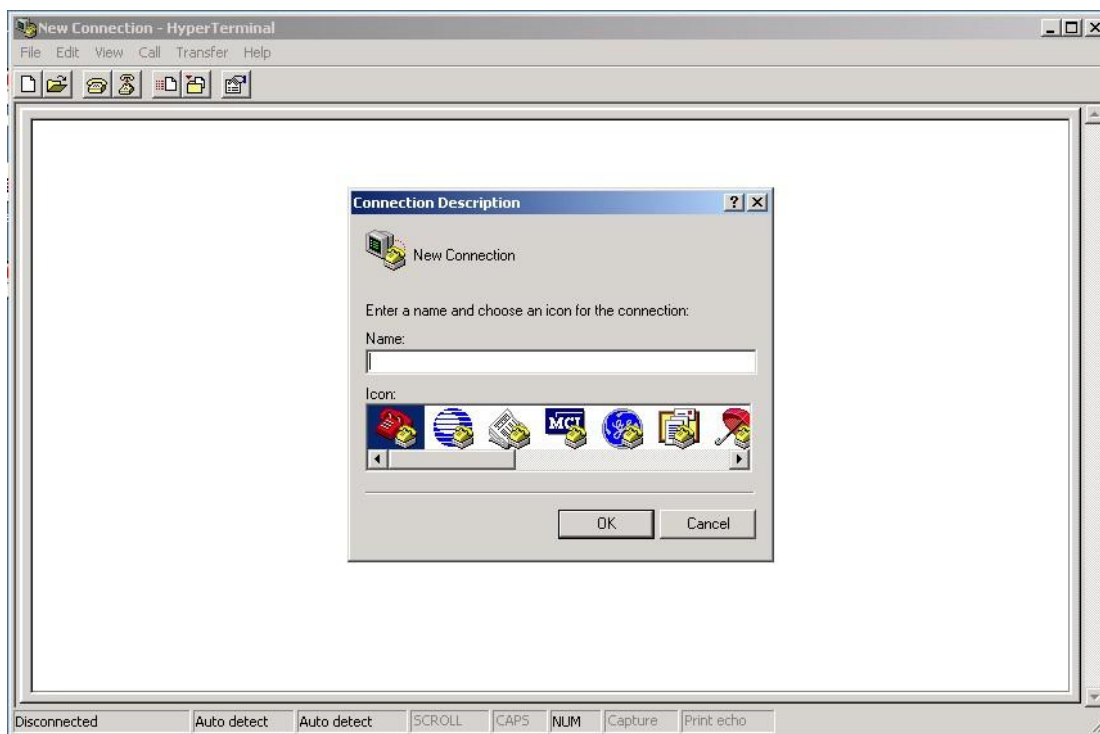
Before configuring RS-232 serial console, connect the RS-232 port of the switch to your PC Com port using a RJ45 to DB9-F cable.

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

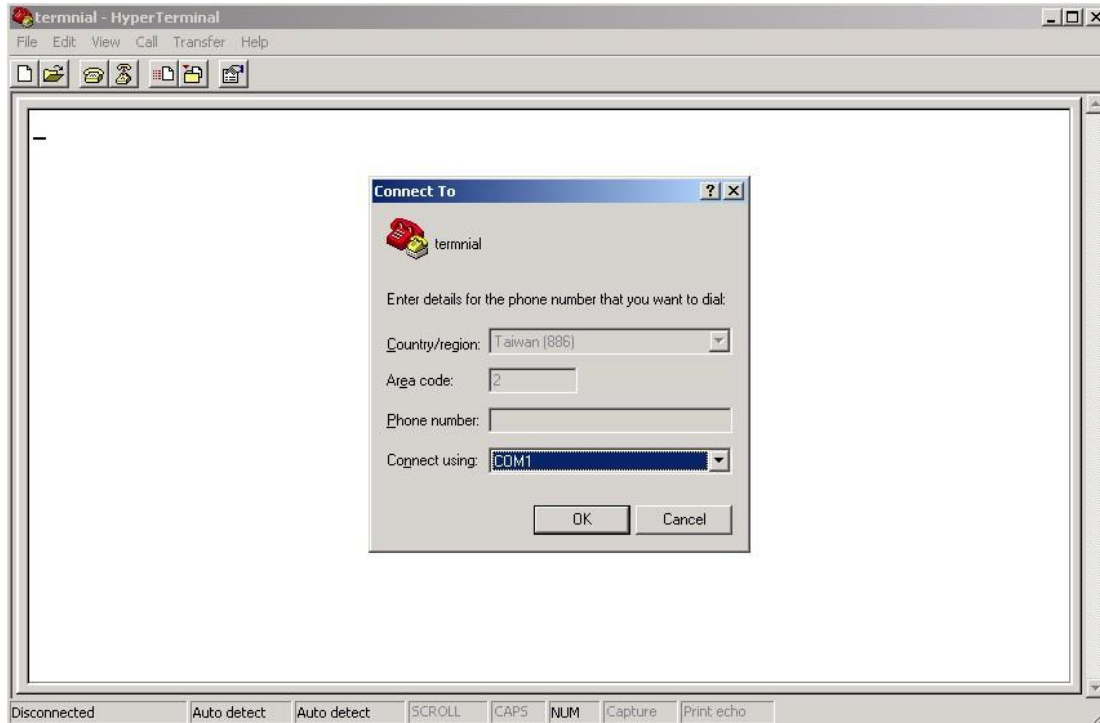
Step 1: On Windows desktop, click on **Start -> Programs -> Accessories -> Communications -> Hyper Terminal**



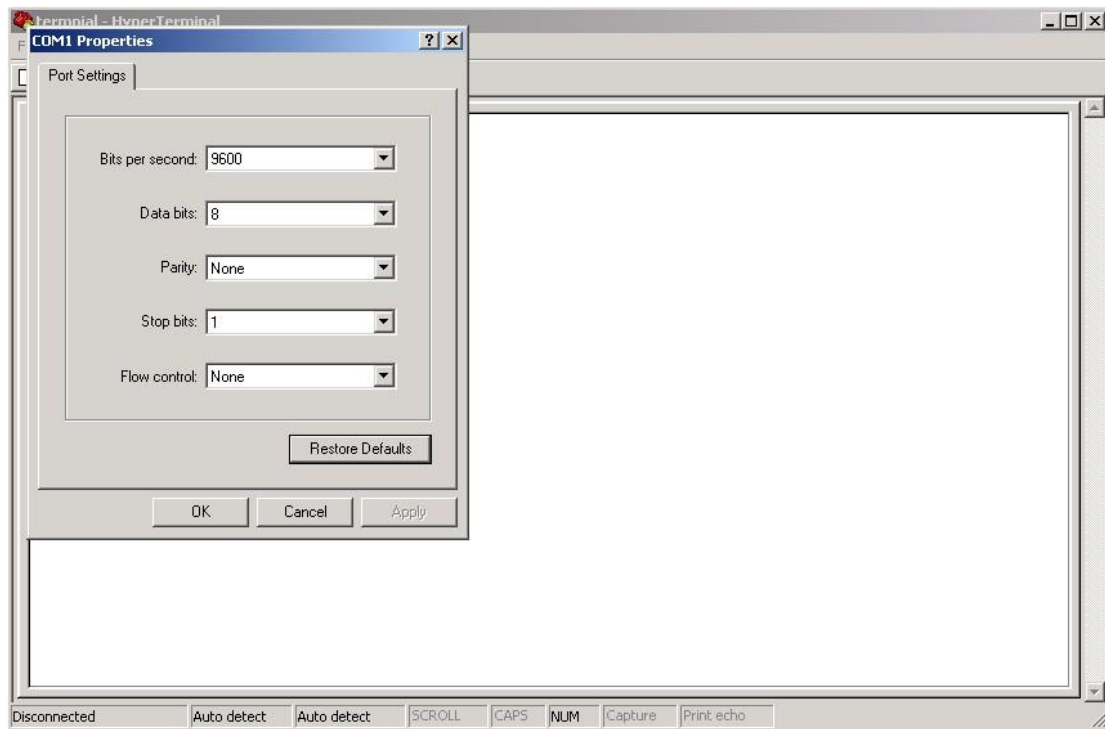
Step 2: Input a name for the new connection.



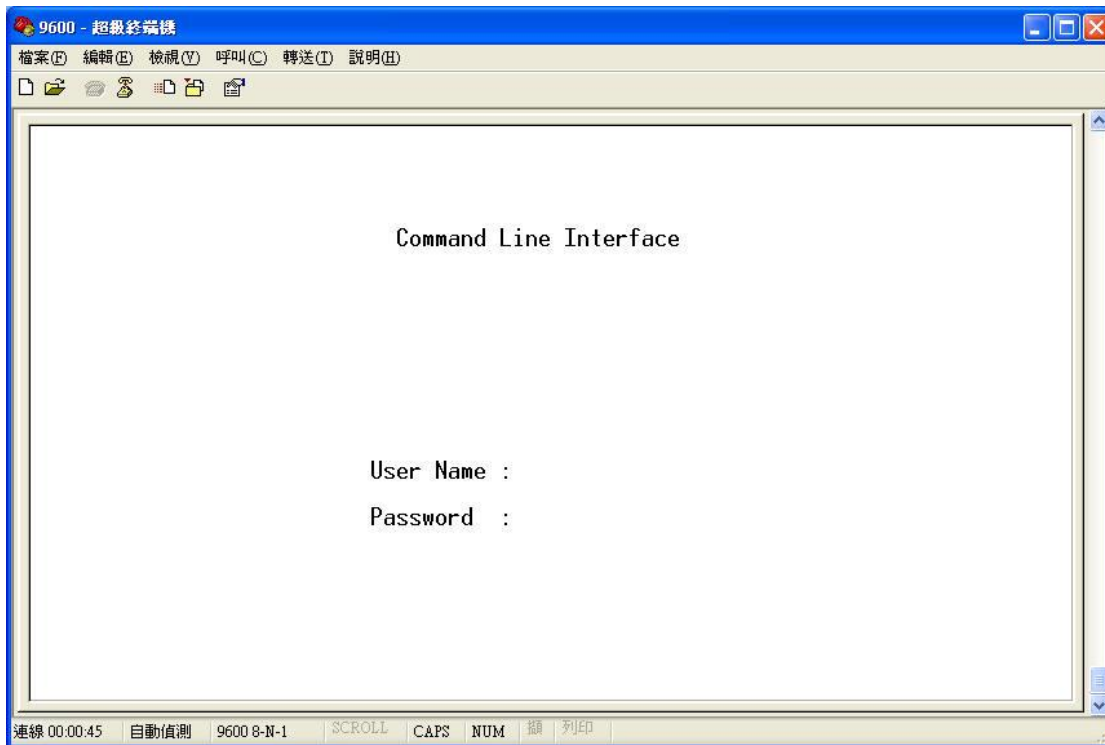
Step 3: Select a COM port in the drop-down list.



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**

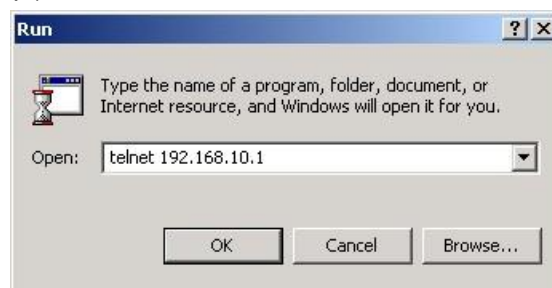
Default Gateway: **192.168.10.254**

User Name: **admin**

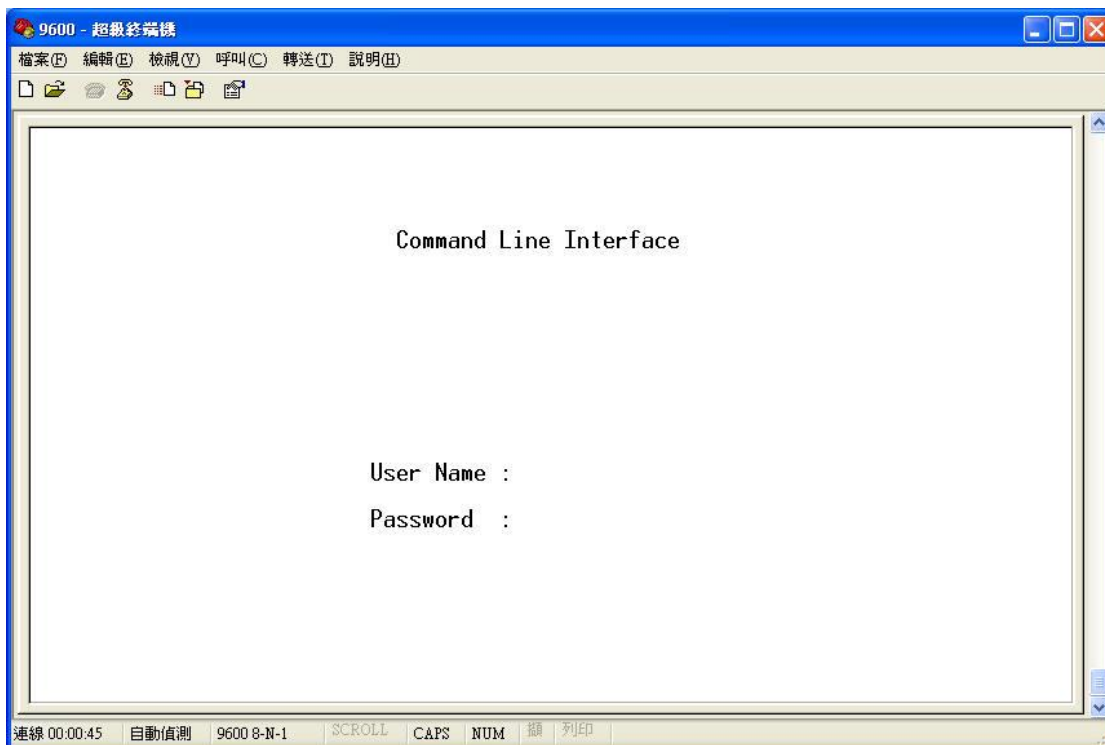
Password: **admin**

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**.



Commands Level

Modes	Access Method	Prompt	Exit Method	About This Model
User EXEC	Begin a session with your switch.	switch>	Enter logout or quit .	The user command available at the level of user is the subset of those available at the privileged level. Use this mode to <ul style="list-style-type: none"> • Enter menu mode. • Display system information.
Privileged EXEC	Enter the enable command while in user EXEC mode.	switch#	Enter disable to exit.	The privileged command is advance mode Privileged this mode to <ul style="list-style-type: none"> • Display advance function status • save configures
Global configuration	Enter the configure command while in privileged EXEC mode.	switch(configuration)#	To exit to privileged EXEC mode, enter exit or end	Use this mode to configure parameters that apply to your Switch as a whole.
VLAN database	Enter the vlan database command while in privileged EXEC mode.	switch(vlan)#	To exit to user EXEC mode, enter exit .	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the interface command (with a specific interface) while in global configuration mode	switch(configuration-if)#	To exit to global configuration mode, enter exit . To exist privileged EXEC mode or end .	Use this mode to configure parameters for the switch and Ethernet ports.

Symbol of Command Level.

Mode	Symbol of Command Level
User EXEC	E
Privileged EXEC	P
Global configuration	G
VLAN database	V
Interface configuration	I

6.1 Commands Set List—System Commands Set

IES-A3080 / IES-A3062 SERIES Commands	Level	Description	Example
show config	E	Show switch configuration	switch>show config
show terminal	P	Show console information	switch#show terminal
write memory	P	Save your configuration into permanent memory (flash rom)	switch#write memory
system name [System Name]	G	Configure system name	switch(config)#system name xxx
system location [System Location]	G	Set switch system location string	switch(config)#system location xxx
system description [System Description]	G	Set switch system description string	switch(config)#system description xxx
system contact [System Contact]	G	Set switch system contact window string	switch(config)#system contact xxx
show system-info	E	Show system information	switch>show system-info
ip address [Ip-address] [Subnet-mask] [Gateway]	G	Configure the IP address of switch	switch(config)#ip address 192.168.1.1 255.255.255.0 192.168.1.254
ip dhcp	G	Enable DHCP client function of switch	switch(config)#ip dhcp
show ip	P	Show IP information of	switch#show ip

		switch	
no ip dhcp	G	Disable DHCP client function of switch	switch(config)#no ip dhcp
reload	G	Halt and perform a cold restart	switch(config)#reload
default	G	Restore to default	Switch(config)#default
admin username [Username]	G	Changes a login username. (maximum 10 words)	switch(config)#admin username xxxxxx
admin password [Password]	G	Specifies a password (maximum 10 words)	switch(config)#admin password xxxxxx
show admin	P	Show administrator information	switch#show admin
dhcpserver enable	G	Enable DHCP Server	switch(config)#dhcpserver enable
dhcpserver lowip [Low IP]	G	Configure low IP address for IP pool	switch(config)# dhcpserver lowip 192.168.1.1
dhcpserver highip [High IP]	G	Configure high IP address for IP pool	switch(config)# dhcpserver highip 192.168.1.50
dhcpserver subnetmask [Subnet mask]	G	Configure subnet mask for DHCP clients	switch(config)#dhcpserver subnetmask 255.255.255.0
dhcpserver gateway [Gateway]	G	Configure gateway for DHCP clients	switch(config)#dhcpserver gateway 192.168.1.254
dhcpserver dnsip [DNS IP]	G	Configure DNS IP for DHCP clients	switch(config)# dhcpserver dnsip 192.168.1.1
dhcpserver leasetime [Hours]	G	Configure lease time (in hour)	switch(config)#dhcpserver leasetime 1
dhcpserver ipbinding [IP address]	I	Set static IP for DHCP clients by port	switch(config)#interface fastEthernet 2 switch(config-if)#dhcpserver ipbinding 192.168.1.1
show dhcpserver configuration	P	Show configuration of DHCP server	switch#show dhcpserver configuration
show dhcpserver clients	P	Show client entries of DHCP server	switch#show dhcpserver clinets
show dhcpserver ip-binding	P	Show IP-Binding information of DHCP server	switch#show dhcpserver ip-binding

no dhcpserver	G	Disable DHCP server function	switch(config)#no dhcpserver
security enable	G	Enable IP security function	switch(config)#security enable
security http	G	Enable IP security of HTTP server	switch(config)#security http
security telnet	G	Enable IP security of telnet server	switch(config)#security telnet
security ip [Index(1..10)] [IP Address]	G	Set the IP security list	switch(config)#security ip 1 192.168.1.55
show security	P	Show the information of IP security	switch#show security
no security	G	Disable IP security function	switch(config)#no security
no security http	G	Disable IP security of HTTP server	switch(config)#no security http
no security telnet	G	Disable IP security of telnet server	switch(config)#no security telnet

6.2 Commands Set List—Port Commands Set

IES-A3080 / IES-A3062 SERIES Commands	Level	Description	Example
interface fastEthernet [Portid]	G	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex [full half]	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
speed [10 100 1000 auto]	I	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100

		can't be set to 1000 if the port isn't a giga port..	
flowcontrol mode [Symmetric Asymmetric]	I	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion.	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol mode Asymmetric
no flowcontrol	I	Disable flow control of interface	switch(config-if)#no flowcontrol
security enable	I	Enable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#security enable
no security	I	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
bandwidth type all	I	Set interface ingress limit frame type to "accept all frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to "accept broadcast, multicast, and flooded unicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to "accept broadcast and multicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast
bandwidth type broadcast-only	I	Set interface ingress limit frame type to "only accept broadcast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only
bandwidth in [Value]	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth in 100

		or to 256000 kbps for giga ports, and zero means no limit.	
bandwidth out [Value]	I	Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth out 100
show bandwidth	I	Show interfaces bandwidth control	switch(config)#interface fastEthernet 2 switch(config-if)#show bandwidth
state [Enable Disable]	I	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#interface fastEthernet 2 switch(config-if)#state Disable
show interface configuration	I	show interface configuration status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface configuration
show interface status	I	show interface actual status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface status
show interface accounting	I	show interface statistic counter	switch(config)#interface fastEthernet 2 switch(config-if)#show interface accounting

no accounting	I	Clear interface accounting information	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting
----------------------	----------	----------------------------------------	----------------------------------------------------------------------------

6.3 Commands Set List—Trunk command set

IES-A3080 / IES-A3062 SERIES Commands	Level	Description	Example
aggregator priority [1to65535]	G	Set port group system priority	switch(config)#aggregator priority 22
aggregator activityport [Port Numbers]	G	Set activity port	switch(config)#aggregator activityport 2
aggregator group [GroupID] [Port-list] lacp workp [Workport]	G	Assign a trunk group with LACP active. [GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	switch(config)#aggregator group 1 1-4 lacp workp 2 or switch(config)#aggregator group 2 1,4,3 lacp workp 3
aggregator group [GroupID] [Port-list] nolacp	G	Assign a static trunk group. [GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#aggregator group 1 2-4 nolacp or switch(config)#aggregator group 1 3,1,2 nolacp
show aggregator	P	Show the information of trunk group	switch#show aggregator

no aggregator lacp [GroupID]	G	Disable the LACP function of trunk group	switch(config)#no aggregator lacp 1
no aggregator group [GroupID]	G	Remove a trunk group	switch(config)#no aggregator group 2

6.4 Commands Set List—VLAN command set

IES-A3080 / IES-A3062 SERIES Commands	Level	Description	Example
vlan database	P	Enter VLAN configure mode	switch#vlan database
vlan [8021q gvrp]	V	To set switch VLAN mode.	switch(vlan)# vlanmode 802.1q or switch(vlan)# vlanmode gvrp
no vlan [VID]	V	Disable vlan group(by VID)	switch(vlan)#no vlan 2
no gvrp	V	Disable GVRP	switch(vlan)#no gvrp
IEEE 802.1Q VLAN			
vlan 8021q port [PortNumber] access-link untag [UntaggedVID]	V	Assign a access link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 802.1q port 3 access-link untag 33
vlan 8021q port [PortNumber] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 8021q port 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q port 3 trunk-link tag 3-20
vlan 8021q port [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)# vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q port 3 hybrid-link untag 5 tag 6-8
vlan 8021q aggregator [TrunkID] access-link untag [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)#vlan 8021q aggregator 3 access-link untag 33

vlan 8021q aggregator [TrunkID] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VLAN by trunk group	switch(vlan)#vlan 8021q aggregator 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q aggregator 3 trunk-link tag 3-20
vlan 8021q aggregator [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for VLAN by trunk group	switch(vlan)# vlan 8021q aggregator 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q aggregator 3 hybrid-link untag 5 tag 6-8
show vlan [VID] or show vlan	V	Show VLAN information	switch(vlan)#show vlan 23

6.5 Commands Set List—Spanning Tree command set

IES-A3080 / IES-A3062 SERIES Commands	Level	Description	Example
spanning-tree enable	G	Enable spanning tree	switch(config)#spanning-tree enable
spanning-tree priority [0to61440]	G	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
spanning-tree max-age [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it	switch(config)# spanning-tree max-age 15

		recomputed the Spanning Tree Protocol (STP) topology.	
spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
spanning-tree forward-time [seconds]	G	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)# spanning-tree forward-time 20
stp-path-cost [1to200000000]	I	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20

		cost when selecting an interface to place into the forwarding state.	
stp-path-priority [Port Priority]	I	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-path-priority 127
stp-admin-p2p [Auto True False]	I	Admin P2P of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-p2p Auto
stp-admin-edge [True False]	I	Admin Edge of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-edge True
stp-admin-non-stp [True False]	I	Admin NonSTP of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-non-stp False
Show spanning-tree	E	Display a summary of the spanning-tree states.	switch>show spanning-tree
no spanning-tree	G	Disable spanning-tree.	switch(config)#no spanning-tree

6.6 Commands Set List—QoS command set

IES-A3080 / IES-A3062 SERIES Commands	Level	Description	Example
qos policy [weighted-fair strict]	G	Select QOS policy scheduling	switch(config)#qos policy weighted-fair
qos prioritytype	G	Setting of QOS	switch(config)#qos prioritytype

[port-based cos-only tos-only cos-first tos-first]		priority type	
qos priority portbased [Port] [lowest low middle high]	G	Configure Port-based Priority	switch(config)#qos priority portbased 1 low
qos priority cos [Priority][lowest low middle high]	G	Configure COS Priority	switch(config)#qos priority cos 2 middle
qos priority tos [Priority][lowest low middle high]	G	Configure TOS Priority	switch(config)#qos priority tos 3 high
show qos	P	Display the information of QoS configuration	switch>show qos
no qos	G	Disable QoS function	switch(config)#no qos

6.7 Commands Set List—IGMP command set

IES-A3080 / IES-A3062 SERIES Commands	Level	Description	Example
igmp enable	G	Enable IGMP snooping function	switch(config)#igmp enable
igmp-query auto	G	Set IGMP query to auto mode	switch(config)#igmp-query auto
igmp-query force	G	Set IGMP query to force mode	switch(config)#igmp-query force
show igmp configuration	P	Displays the details of an IGMP configuration.	switch#show igmp configuration
show igmp multi	P	Displays the details of an IGMP snooping entries.	switch#show igmp multi
no igmp	G	Disable IGMP snooping function	switch(config)#no igmp
no igmp-query	G	Disable IGMP query	switch#no igmp-query

6.8 Commands Set List—MAC/Filter Table command set

IES-A3080 / IES-A3062 SERIES Commands	Level	Description	Example
<code>mac-address-table static hwaddr [MAC]</code>	I	Configure MAC address table of interface (static).	switch(config)#interface fastEthernet 2 switch(config-if)#mac-address-table static hwaddr 000012345678
<code>mac-address-table filter hwaddr [MAC]</code>	G	Configure MAC address table(filter)	switch(config)#mac-address-table filter hwaddr 000012348678
<code>show mac-address-table</code>	P	Show all MAC address table	switch#show mac-address-table
<code>show mac-address-table static</code>	P	Show static MAC address table	switch#show mac-address-table static
<code>show mac-address-table filter</code>	P	Show filter MAC address table.	switch#show mac-address-table filter
<code>no mac-address-table static hwaddr [MAC]</code>	I	Remove an entry of MAC address table of interface (static)	switch(config)#interface fastEthernet 2 switch(config-if)#no mac-address-table static hwaddr 000012345678
<code>no mac-address-table filter hwaddr [MAC]</code>	G	Remove an entry of MAC address table (filter)	switch(config)#no mac-address-table filter hwaddr 000012348678
<code>no mac-address-table</code>	G	Remove dynamic entry of MAC address table	switch(config)#no mac-address-table

6.9 Commands Set List—SNMP command set

IES-A3080 / IES-A3062 SERIES Commands	Level	Description	Example
<code>snmp agent-mode [v1v2c v3]</code>	G	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2c
<code>snmp-server host [IP address] community [Community-string]</code>	G	Configure SNMP server host information and community string	switch(config)#snmp-server host 192.168.10.50 community public trap-version v1 (remove)

trap-version [v1 v2c]			Switch(config)# no snmp-server host 192.168.10.50
snmp community-strings [Community-string] right [RO RW]	G	Configure the community string right	switch(config)#snmp community-strings public right RO or switch(config)#snmp community-strings public right RW
snmp snmpv3-user [User Name] password [Authentication Password] [Privacy Password]	G	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#snmp snmpv3-user test01 password AuthPW PrivPW
show snmp	P	Show SNMP configuration	switch#show snmp
show snmp-server	P	Show specified trap server information	switch#show snmp-server
no snmp community-strings [Community]	G	Remove the specified community.	switch(config)#no snmp community-strings public
no snmp snmpv3-user [User Name] password [Authentication Password] [Privacy Password]	G	Remove specified user of SNMPv3 agent. Privacy password could be empty.	switch(config)# no snmp snmpv3-user test01 password AuthPW PrivPW
no snmp-server host [Host-address]	G	Remove the SNMP server host.	switch(config)#no snmp-server 192.168.10.50

6.10 Commands Set List—Port Mirroring command set

IES-A3080 / IES-A3062 SERIES Commands	Level	Description	Example
monitor rx	G	Set RX destination port of monitor function	switch(config)#monitor rx
monitor tx	G	Set TX destination	switch(config)#monitor tx

		port of monitor function	
show monitor	P	Show port monitor information	switch#show monitor
monitor [RX TX Both]	I	Configure source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#monitor RX
show monitor	I	Show port monitor information	switch(config)#interface fastEthernet 2 switch(config-if)#show monitor
no monitor	I	Disable source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#no monitor

6.11 Commands Set List—802.1x command set

IES-A3080 / IES-A3062 SERIES Commands	Level	Description	Example
8021x enable	G	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiusip [IP address]	G	Use the 802.1x system radius IP global configuration command to change the radius server IP.	switch(config)# 8021x system radiusip 192.168.1.1
8021x system serverport [port ID]	G	Use the 802.1x system server port global configuration command to change the radius server port	switch(config)# 8021x system serverport 1815
8021x system accountport [port ID]	G	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# 8021x system accountport 1816
8021x system sharekey	G	Use the 802.1x	switch(config)# 8021x system

[ID]		system share key global configuration command to change the shared key value.	sharekey 123456
8021x system nasid [words]	G	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# 8021x system nasid test1
8021x misc quietperiod [sec.]	G	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# 8021x misc quietperiod 10
8021x misc txperiod [sec.]	G	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# 8021x misc txperiod 5
8021x misc supportimeout [sec.]	G	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# 8021x misc supportimeout 20
8021x misc servertimeout [sec.]	G	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#8021x misc servertimeout 20
8021x misc maxrequest [number]	G	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# 8021x misc maxrequest 3

8021x misc reauthperiod [sec.]	G	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# 8021x misc reauthperiod 3000
8021x portstate [disable reject accept authorize]	I	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch(config)#interface fastethernet 3 switch(config-if)#8021x portstate accept
show 8021x	E	Display a summary of the 802.1x properties and also the port sates.	switch>show 8021x
no 8021x	G	Disable 802.1x function	switch(config)#no 8021x

6.12 Commands Set List—TFTP command set

IES-A3080 / IES-A3062 SERIES Commands	Level	Description	Defaults Example
backup flash:backup_cfg	G	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#backup flash:backup_cfg
restore flash:restore_cfg	G	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)#restore flash:restore_cfg
upgrade flash:upgrade_fw	G	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file	switch(config)#upgrade lash:upgrade_fw

		name of image.	
--	--	----------------	--

6.13 Commands Set List—SYSLOG, SMTP, EVENT command set

IES-A3080 / IES-A3062 SERIES Commands	Level	Description	Example
systemlog ip [IP address]	G	Set System log server IP address.	switch(config)# systemlog ip 192.168.1.100
systemlog mode [client server both]	G	Specified the log mode	switch(config)# systemlog mode both
show systemlog	E	Display system log.	Switch>show systemlog
show systemlog	P	Show system log client & server information	switch#show systemlog
no systemlog	G	Disable systemlog function	switch(config)#no systemlog
smtp enable	G	Enable SMTP function	switch(config)#smtp enable
smtp serverip [IP address]	G	Configure SMTP server IP	switch(config)#smtp serverip 192.168.1.5
smtp authentication	G	Enable SMTP authentication	switch(config)#smtp authentication
smtp account [account]	G	Configure authentication account	switch(config)#smtp account User
smtp password [password]	G	Configure authentication password	switch(config)#smtp password
smtp rcptemail [Index] [Email address]	G	Configure Rcpt e-mail Address	switch(config)#smtp rcptemail 1 Alert@test.com
show smtp	P	Show the information of SMTP	switch#show smtp
no smtp	G	Disable SMTP function	switch(config)#no smtp
event device-cold-start [Systemlog SMTP Both]	G	Set cold start event type	switch(config)#event device-cold-start both
event	G	Set Authentication	switch(config)#event

authentication-failure [Systemlog SMTP Both]		failure event type	authentication-failure both
event O-Ring-topology-change [Systemlog SMTP Both]	G	Set s ring topology changed event type	switch(config)#event ring-topology-change both
event systemlog [Link-UP Link-Down Both]	I	Set port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#event systemlog both
event smtp [Link-UP Link-Down Both]	I	Set port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#event smtp both
show event	P	Show event selection	switch#show event
no event device-cold-start	G	Disable cold start event type	switch(config)#no event device-cold-start
no event authentication-failure	G	Disable Authentication failure event typ	switch(config)#no event authentication-failure
no event O-Ring-topology-change	G	Disable O-Ring topology changed event type	switch(config)#no event ring-topology-change
no event systemlog	I	Disable port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#no event systemlog
no event smpt	I	Disable port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#no event smpt
show systemlog	P	Show system log client & server information	switch#show systemlog

6.14 Commands Set List—SNTP command set

IES-A3080 / IES-A3062 SERIES Commands	Level	Description	Example
sntp enable	G	Enable SNTP function	switch(config)#sntp enable
sntp daylight	G	Enable daylight saving time, if SNTP function	switch(config)#sntp daylight

		is inactive, this command can't be applied.	
sntp daylight-period [Start time] [End time]	G	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# sntp daylight-period 20060101-01:01 20060202-01-01
sntp daylight-offset [Minute]	G	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight-offset 3
sntp ip [IP]	G	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp ip 192.169.1.1
sntp timezone [Timezone]	G	Set timezone index, use "show sntp timzezone" command to get more information of index number	switch(config)#sntp timezone 22
show sntp	P	Show SNTP information	switch#show sntp
show sntp timezone	P	Show index number of time zone list	switch#show sntp timezone
no sntp	G	Disable SNTP function	switch(config)#no sntp
no sntp daylight	G	Disable daylight saving time	switch(config)#no sntp daylight

6.15 Commands Set List—O-Ring command set

IES-A3080 / IES-A3062	Level	Description	Example
-----------------------	-------	-------------	---------

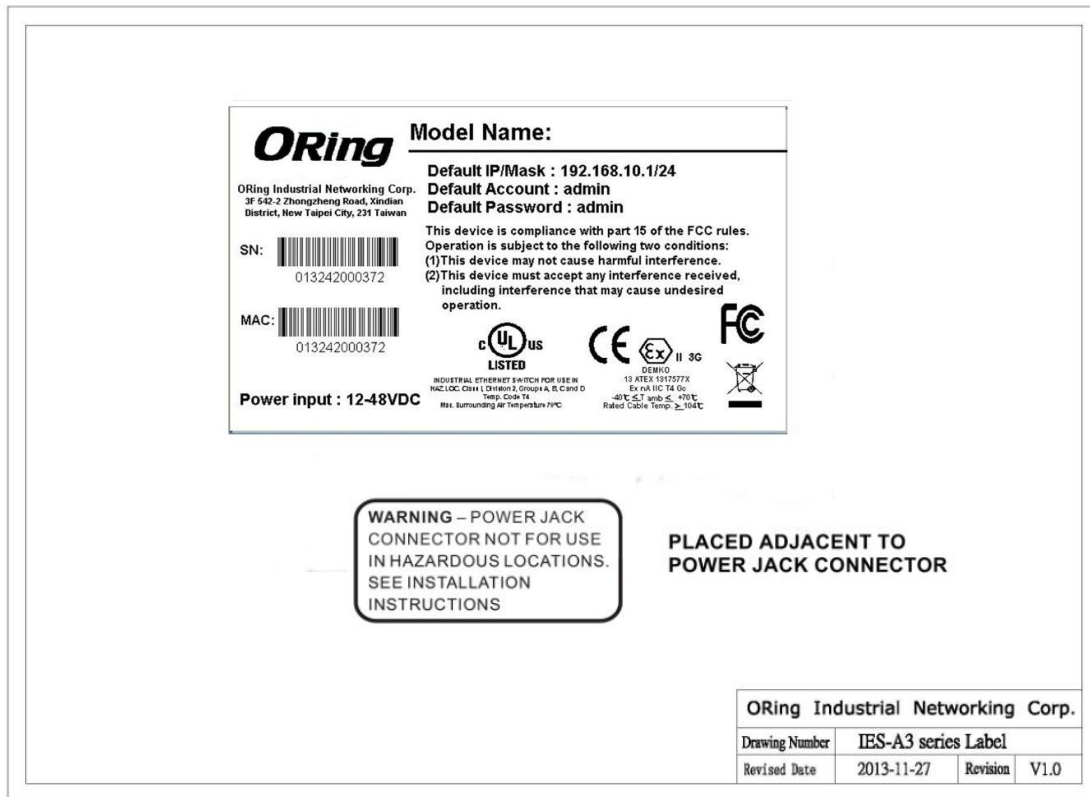
SERIES Commands			
Ring enable	G	Enable O-Ring	switch(config)# ring enable
Ring master	G	Enable ring master	switch(config)# ring master
Ring couplering	G	Enable couple ring	switch(config)# ring couplering
Ring dualhoming	G	Enable dual homing	switch(config)# ring dualhoming
Ring ringport [1st Ring Port] [2nd Ring Port]	G	Configure 1st/2nd Ring Port	switch(config)# ring ringport 7 8
Ring couplingport [Coupling Port]	G	Configure Coupling Port	switch(config)# ring couplingport 1
Ring controlport [Control Port]	G	Configure Control Port	switch(config)# ring controlport 2
Ring homingport [Dual Homing Port]	G	Configure Dual Homing Port	switch(config)# ring homingport 3
show Ring	P	Show the information of O-Ring	switch#show ring
no Ring	G	Disable O-Ring	switch(config)#no ring
no Ring master	G	Disable ring master	switch(config)# no ring master
no Ring couplering	G	Disable couple ring	switch(config)# no ring couplering
no Ring dualhoming	G	Disable dual homing	switch(config)# no ring dualhoming

Technical Specifications

Technology	
Ethernet Standards	802.3 - 10Base-T, 802.3u - 100Base-TX, 100Base-FX, 802.3z - 1000Base-LX/SX 802.3ab - 1000Base-TX, 802.3ad - Link Aggregation Control Protocol 802.3x - Flow Control 802.1D - Spanning Tree Protocol 802.1p - Class of Service, 802.1Q - VLAN Tagging 802.1w - Rapid Spanning Tree Protocol, 802.1X - Authentication 802.1ad - VLAN QinQ 802.1AB - LLDP 802.1s - MSTP
MAC addresses	8192
Priority Queues	4
Flow Control	IEEE 802.3x Flow Control and Back-pressure
Processing	Store-and-Forward
Interface	
RJ45 Ports	10/100Base-T(X), Auto MDI/MDI-X
Giga Fiber Ports	1000 Base-X (SC Connector) Multi-Mode: 0 to 550m, 850 nm (50/125 μ m to 62.5/125 μ m) Single-Mode: 0 to 10km, 1310 nm (9/125 μ m)
Giga Ports	10/100/1000 Base-T(X), Auto MDI/MDIX
Fiber Ports	100 Base-FX (SC Connector) Multi-Mode: 0 to 2 km, 1310 nm (50/125 μ m to 62.5/125 μ m) Single-Mode: 0 to 30km, 1310 nm (9/125 μ m)
LED Indicators	Per Unit : Power x 3(Green) RJ45 Ports:

	Per Port : Link/Activity(Green/Blinking Green), Full duplex(Amber) Giga/Fiber Ports: Per Port : Activity(Green), Link (Amber)
Power Requirements	
Power Input Voltage	PWR1/2: 12 to 48VDC in 7-pin Terminal Block PWR3: 12 to 48VDC in Power Jack (WARNING – POWER JACK CONNECTOR NOT FOR USE IN HAZARDOUS LOCATIONS. SEE INSTALLATION INSTRUCTIONS)
Reverse Polarity Protection	Present at terminal block
Electrical Ratings	
Rated Supply Input	12-48VDC
Maximum Surrounding Air Temperature	70 °C
Environmental	
Operating Temperature	-40 to 70 °C
Storage Temperature	-40 to 85 °C
Operating Humidity	5% to 95%, non-condensing
Mechanical	
Dimensions(W x D x H)	52 mm(W)x 106 mm(D)x 144 mm(H)
Casing	IP-30 protection
Regulatory Approvals	
Regulatory Approvals	FCC Part 15, CISPER (EN55022) class A
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	IEC 60068-2-27
Free Fall	IEC 60068-2-32
Vibration	IEC 60068-2-6
Warranty	5 years

Label



A. Condition of safe use:

1. Subject devices are to be installed in an ATEX Certified IP54 enclosure and accessible only by the use of a tool.
2. Subject devices are for use in an area of not more than pollution degree 2 in accordance with IEC 60664-1.
3. Provision shall be made to prevent the rated voltage being exceeded by the transient disturbances of more than 140% of the peak rated voltage.

B. Installation Instruction:

1. Cable temperature rating not less than 104°C
2. The terminal Block (J9) – Cat. No. 5EHDR-07P by Dinkle Eterprise Co., Ltd., rated 300 V, 15 A, 105°C, FW-1 mating with Cat. No. 5ESDV-07P by Dinkle Eterprise Co., Ltd., rated 300 V, 15 A, 105°C, FW-2, suitable for 28-12 AWG wire size, torque value 4.5 lb-in.

C. Standards:

IEC 60079-0 Ed.6, IEC 60079-15 Ed.4, EN 60079-0:2012, EN 60079-15:2010