

# Industrial Management Ethernet Switch

---

## IES-3160 User's Manual



**Version 1.3**  
**Feb, 2010.**



**ORing Industrial Networking Corp.**

4F., NO.3, Lane235, Baociao Rd.Sindian City,  
Taipei County 23145 Taiwan, R.O.C.

Tel: + 886 2 2918 3036

Fax: + 886 2 2918 3084

Website: [www.oring-networking.com](http://www.oring-networking.com)

E-mail: [support@oring-networking.com](mailto:support@oring-networking.com)



# Table of Content

<b>Getting to Know Your Switch</b> .....	<b>4</b>
1.1 About the IES-3160 Managed Industrial Switch.....	4
1.2 Software Features .....	4
1.3 Hardware Features.....	5
<b>Hardware Installation</b> .....	<b>6</b>
2.1 Installing Switch on DIN-Rail.....	6
2.1.1 Mount IES-3160 on DIN-Rail .....	6
2.2 Wall Mounting Installation.....	7
2.2.1 Mount IES-3160 Series on the wall.....	7
<b>Hardware Overview</b> .....	<b>9</b>
3.1 Front Panel .....	9
3.2 Front Panel LEDs .....	11
3.3 Top view Panel .....	11
3.4 Rear Panel.....	12
<b>Cables</b> .....	<b>13</b>
4.1 Ethernet Cables .....	13
4.1.1 10/100/100BASE-TX/10BASE-T Pin Assignments.....	13
4.1.2 100BASE-TX/10BASE-T Pin Assignments.....	14
4.2 Console Cable.....	15
<b>WEB Management</b> .....	<b>16</b>
5.1 Configuration by Web Browser .....	16
5.1.1 About Web-based Management .....	16
5.1.2 System Information .....	18
5.1.3 Front Panel.....	18
5.1.4 Basic setting.....	19
5.1.4.1 Switch Setting .....	19
5.1.4.2 Admin Password .....	20
5.1.4.3 IP Setting.....	20
5.1.4.4 SNTP (Time) .....	21
5.1.4.5 LLDP.....	24



- 5.1.4.6 Auto Provision ..... 24
- 5.1.4.7 Backup & Restore ..... 25
- 5.1.4.8 Upgrade Firmware ..... 26
- 5.1.5 DHCP Server ..... 26
  - 5.1.5.1 DHCP Server – Setting..... 26
  - 5.1.5.2 DHCP Server – Client List..... 27
  - 5.1.5.3 DHCP Server – Port and IP bindings ..... 28
- 5.1.6 Port Setting ..... 29
  - 5.1.6.1 Port Control..... 29
  - 5.1.6.2 Port Status ..... 30
  - 5.1.6.3 Port Alias..... 30
  - 5.1.6.4 Rate Limit ..... 31
  - 5.1.6.5 Port Trunk ..... 32
- 5.1.7 Redundancy ..... 34
  - 5.1.7.1 O-Ring..... 34
  - 5.1.7.2 Open-Ring ..... 35
  - 5.1.7.3 O-RSTP..... 36
  - 5.1.7.4 RSTP ..... 38
  - 5.1.7.5 MSTP ..... 41
- 5.1.8 VLAN..... 45
  - 5.1.8.1 VLAN Setting ..... 45
  - 5.1.8.2 VLAN Setting – Port Based ..... 48
- 5.1.9 SNMP ..... 49
  - 5.1.9.1 SNMP – Agent Setting ..... 50
  - 5.1.9.2 SNMP – Trap Setting ..... 51
- 5.1.10 Traffic Prioritization..... 52
- 5.1.11 Multicast ..... 57
  - 5.1.11.1 IGMP Snooping..... 57
  - 5.1.11.2 MVR ..... 58
  - 5.1.11.3 Multicast Filter ..... 58
- 5.1.12 Security ..... 60
  - 5.1.12.1 IP Security ..... 60
  - 5.1.12.2 Port Security..... 61
  - 5.1.12.3 MAC Blacklist ..... 62
  - 5.1.12.4 802.1x..... 62
- 5.1.13 Warning..... 66
  - 5.1.13.1 Fault Alarm ..... 66



- 5.1.13.2 System Alarm ..... 67
- 5.1.14 Monitor and Diag ..... 70
  - 5.1.14.1 MAC Address Table ..... 70
  - 5.1.14.2 MAC Address Aging ..... 71
  - 5.1.14.3 Port Statistics ..... 72
  - 5.1.14.4 Port Monitoring ..... 73
  - 5.1.14.5 System Event Log ..... 75
  - 5.1.14.6 Ping ..... 76
- 5.1.15 Save Configuration ..... 76
- 5.1.16 Factory Default ..... 77
- 5.1.17 System Reboot ..... 77

**Command Line Interface Management ..... 78**

- 6.1 About CLI Management ..... 78
- 6.2 Commands Set List—System Commands Set ..... 83
- 6.3 Commands Set List—Port Commands Set ..... 85
- 6.4 Commands Set List—Trunk command set ..... 88
- 6.5 Commands Set List—VLAN command set ..... 89
- 6.6 Commands Set List—Spanning Tree command set ..... 90
- 6.7 Commands Set List—QoS command set ..... 92
- 6.8 Commands Set List—IGMP command set ..... 93
- 6.9 Commands Set List—MAC/Filter Table command set ..... 94
- 6.10 Commands Set List—SNMP command set ..... 94
- 6.11 Commands Set List—Port Mirroring command set ..... 95
- 6.12 Commands Set List—802.1x command set ..... 96
- 6.13 Commands Set List—TFTP command set ..... 98
- 6.14 Commands Set List—SYSLOG, SMTP, EVENT command set ..... 99
- 6.15 Commands Set List—SNTP command set ..... 100
- 6.16 Commands Set List—O-Ring command set ..... 102

**Technical Specifications ..... 103**



# Getting to Know Your Switch

## 1.1 About the IES-3160 Managed Industrial Switch

The IES-3160 is powerful managed industrial switch with many features. The switch can work under wide temperature, dusty environment and humid condition. They can be managed by WEB, TELNET, Consol or other third-party SNMP software as well. Besides, the switch can be managed by a useful utility that we called Open-Vision. Open-Vision is powerful network management software. With its friendly and powerful interface, you can easily configure multiple switches at the same time, and monitor switches' status.

## 1.2 Software Features

- World's fastest Redundant Ethernet Ring (Recovery time < 10ms over 250 units connection)
- Supports Ring Coupling, Dual Homing over O-Ring
- Supports SNMPv1/v2/v3 & RMON & Port base/802.1Q VLAN Network Management
- Event notification by Email, SNMP trap and Relay Output
- Web-based ,Telnet, Console, CLI configuration
- 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
- RSTP (802.1w)
- 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)



## 1.3 Hardware Features

- Redundant two DC power inputs
- Wide Operating Temperature: -40 to 70°C
- Storage Temperature: -40 to 85°C
- Operating Humidity: 5% to 95%, non-condensing
- Casing: IP-30
- 10/100Base-T(X) Ethernet port
- Console Port
- Dimensions(W x D x H) :74.3 mm(W)x 109.2 mm( D )x 153.6 mm(H)

# Hardware Installation

## 2.1 Installing Switch on DIN-Rail

Each switch has a DIN-Rail kit on rear panel. The DIN-Rail kit helps switch to fix on the DIN-Rail. It is easy to install the switch on the DIN-Rail:

### 2.1.1 Mount IES-3160 on DIN-Rail

Step 1: Slant the switch and mount the metal spring to DIN-Rail.



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

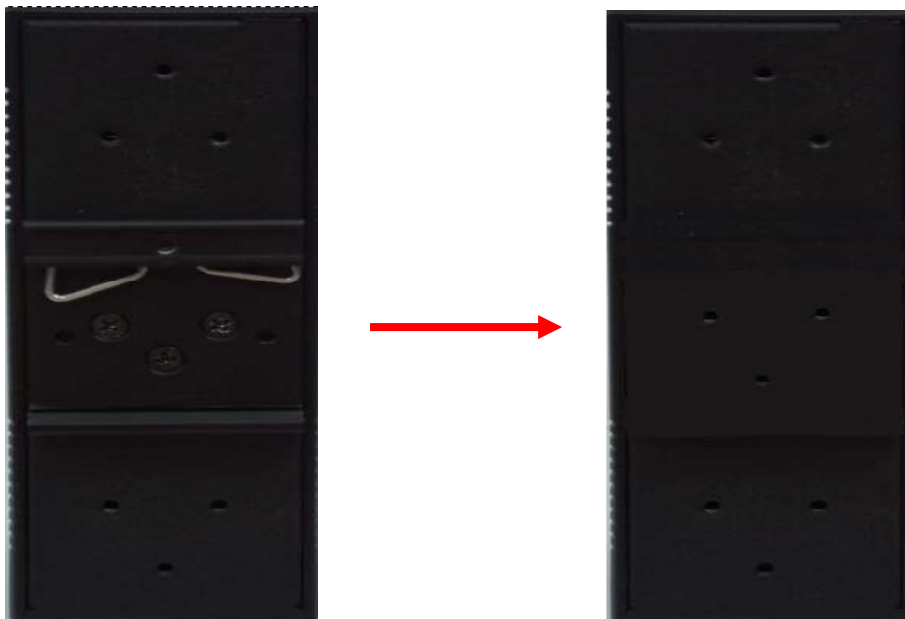


## 2.2 Wall Mounting Installation

Each switch has another installation method for users to fix the switch. A wall mount panel can be found in the package. The following steps show how to mount the switch on the wall.

### 2.2.1 Mount IES-3160 on the wall

Step 1: Remove DIN-Rail kit.

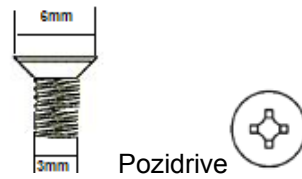


Step 2: Use 6 screws that can be found in the package to combine the wall mount panel. Just like the picture shows below:

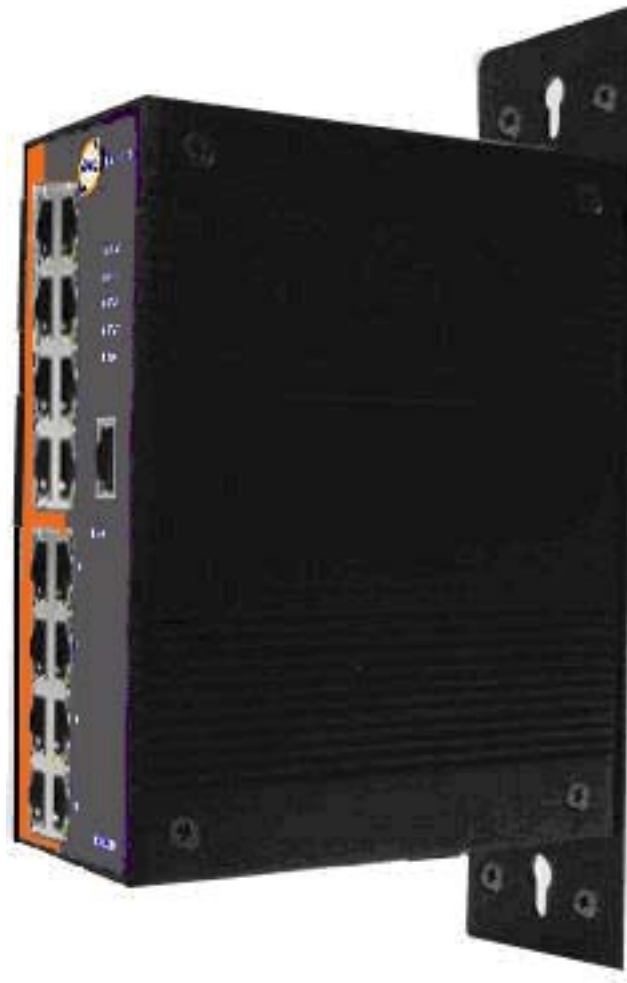




The screws specification shows in the following two pictures. In order to prevent switch from any damage, the screws should not larger than the size that used in IES-3160 switch.



Step 3: Mount the combined switch on the wall.





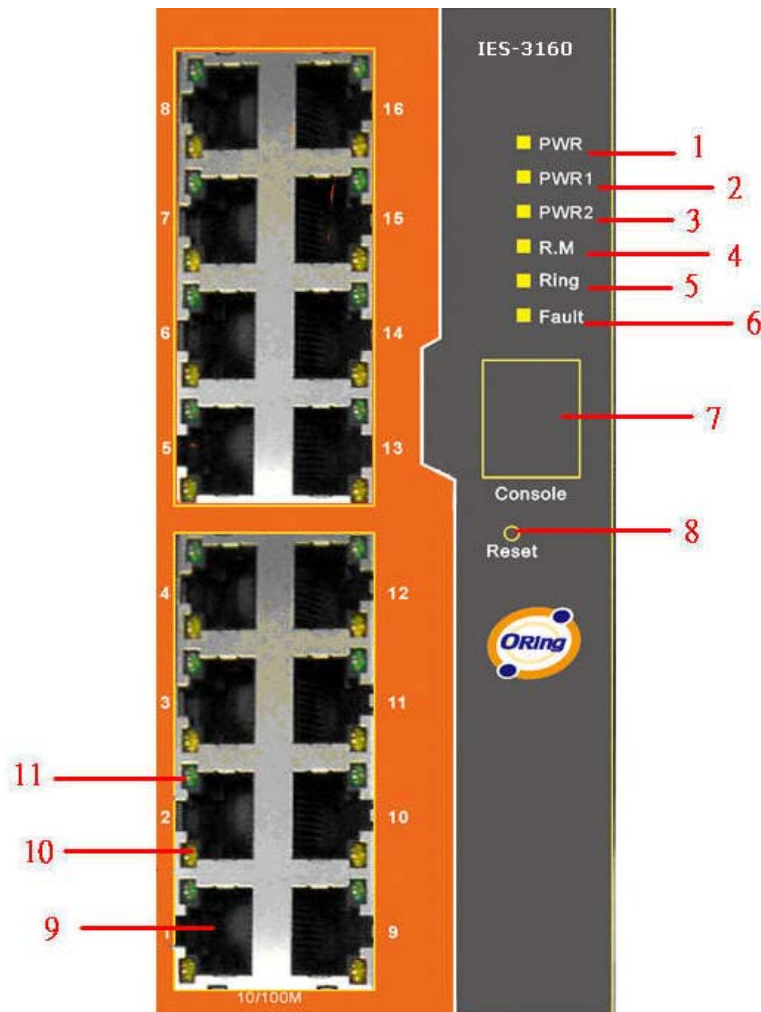
# Hardware Overview

## 3.1 Front Panel

The following table describes the labels that stick on the IES-3160.

Port	Description
<b>10/100 RJ-45 fast Ethernet ports</b>	16 10/100Base-T(X) RJ-45 fast Ethernet ports support auto-negotiation. Default Setting : Speed: auto Duplex: auto Flow control : disable
<b>Console</b>	Use RS-232 to RJ-45 connector to manage switch.
<b>Reset</b>	Push reset button 2 to 3 seconds to reset the switch. Push reset button 5 seconds to reset the switch into <b>Factory Default</b> .

## IES-3160



1. LED for PWR. When the PWR links, the green led will be light on.
2. LED for PWR1. When the PWR1 links, the green led will be light on.
3. LED for PWR2. When the PWR2 links, the green led will be light on.
4. LED for R.M (Ring master). When the LED light on, it means that the switch is the ring master of O-Ring.
5. LED for Ring. When the led light on, it means the O-Ring is activated.
6. LED for Fault Relay. When the fault occurs, the amber LED will be light on.
7. . Console port (RJ-45).
8. Reset button. Push the button 3 seconds for reset; 5 seconds for factory default.
9. 10/100Base-T(X) Ethernet ports.
10. LED for Ethernet ports speed.
11. LED for Ethernet ports link status.

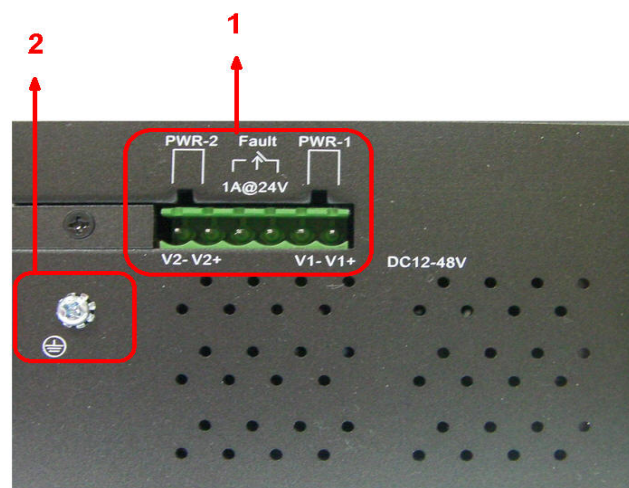
## 3.2 Front Panel LEDs

LED	Color	Status	Description
<b>PWR</b>	Green	On	DC power ready
<b>PW1</b>	Green	On	DC power module 1 activated.
<b>PW2</b>	Green	On	DC power module 2 activated.
<b>R.M</b>	Green	On	O-Ring Master.
<b>Fault</b>	Amber	On	Fault relay. Power failure or Port down/fail.
10/100Base-T(X) Fast Ethernet ports			
<b>LNK / ACT</b>	Green	On	Port link up.
		Blinking	Data transmitted.
<b>Full Duplex</b>	Amber	On	Port works under full duplex.

## 3.3 Top view Panel

The bottom panel components of IES-3160 are shown as below:

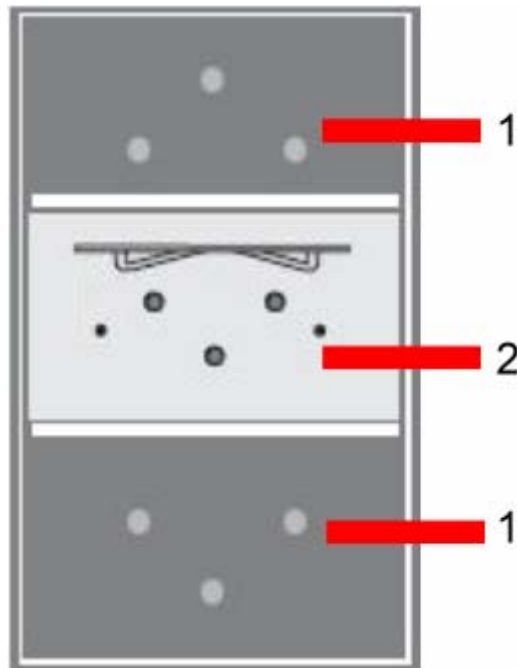
1. Terminal block includes: PWR1, PWR2 (48V DC)
2. Ground wire



### 3.4 Rear Panel

The components in the rear of IES-3160 are shown as below:

1. Screw holes for wall mount kit.
2. DIN-Rail kit





# Cables

## 4.1 Ethernet Cables

The IES-3160 switch has standard Ethernet ports. According to the link type, the switch use CAT 3, 4, 5, 5e UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

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

### 4.1.1 100BASE-TX/10BASE-T Pin Assignments

The IES-3160 switch have standard Ethernet ports. According to the link type, the switch use CAT 3, 4, 5, 5e UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

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



### 4.1.2 100BASE-TX/10BASE-T Pin Assignments

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

#### 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

The IES-3160 switch support auto MDI/MDI-X operation. You can use a straight-through cable to connect PC to switch. The following table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

#### MDI/MDI-X pins assignment

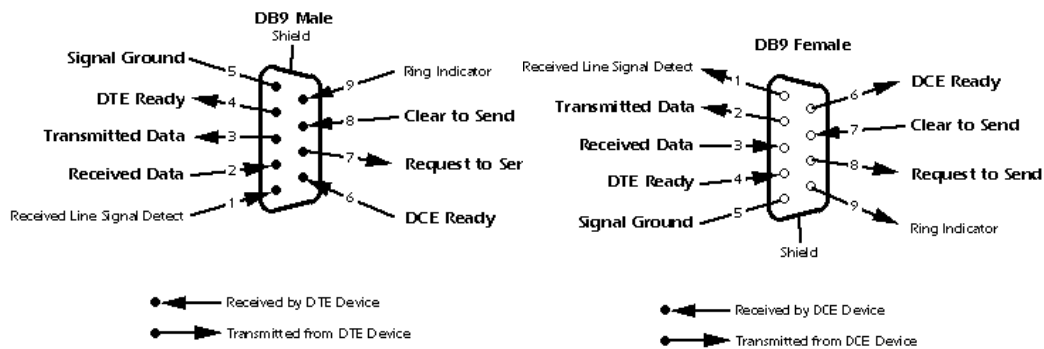
Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

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

## 4.2 Console Cable

IES-3160 switch can be management by console port. The DB-9 to RJ-45 cable can be found in the package. You can connect them to PC via a RS-232 cable with DB-9 female connector and the other end (RJ-45 connector) connects to console port of 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





# WEB Management



## 5.1 Configuration by Web Browser

This section introduces the configuration by Web browser.

### 5.1.1 About Web-based Management

An embedded HTML web site resides in flash memory on the CPU board. It contains advanced management features and allows you to manage the switch from anywhere on the network through a standard web browser such as Microsoft Internet Explorer.

The Web-Based Management function supports Internet Explorer 5.0 or later. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

**Note:** By default, IE5.0 or later version does not allow Java Applets to open sockets. You need to explicitly modify the browser setting in order to enable Java Applets to use network ports.

### Preparing for Web Management

The default value is as below:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

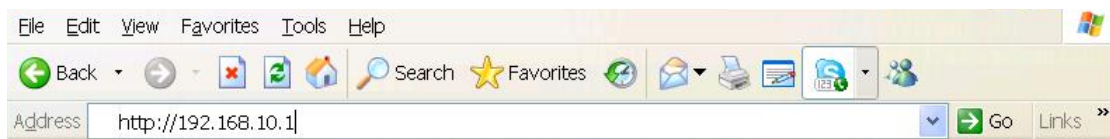
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

### System Login

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

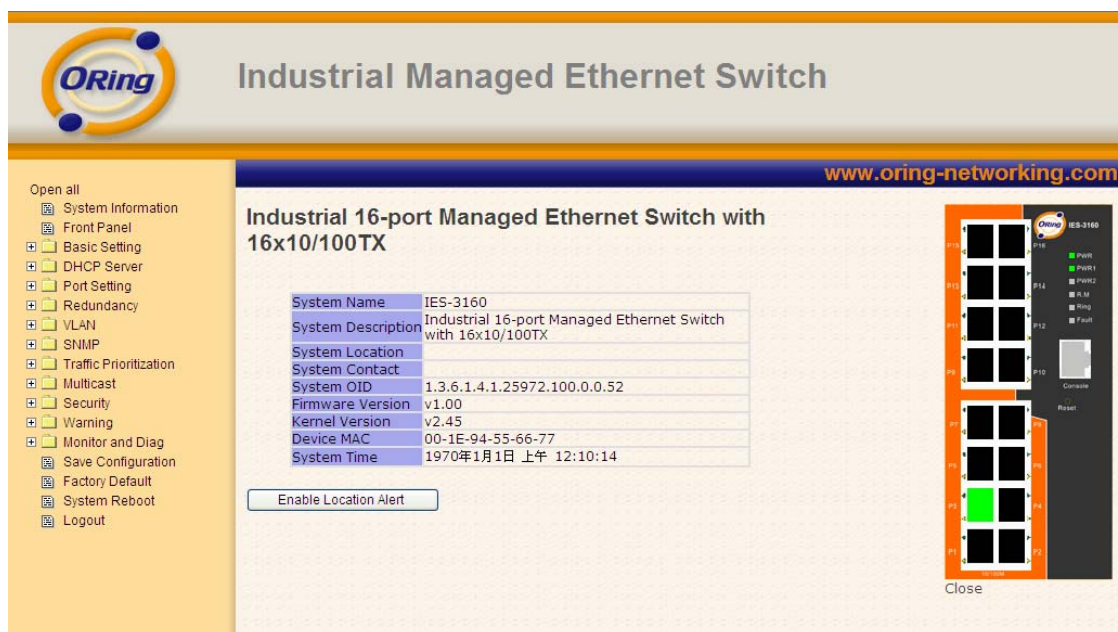


3. The login screen appears.
4. Key in the username and password. The default username and password is "admin".
5. Click "Enter" or "OK" button, then the main interface of the Web-based management appears.



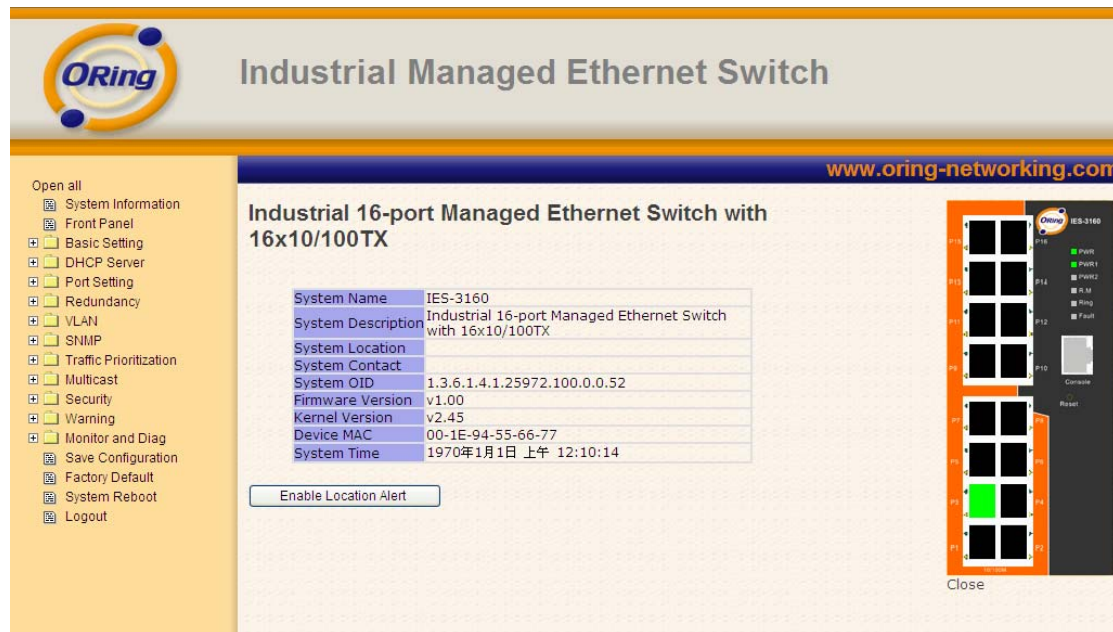
Login screen

## Main Interface



Main interface

### 5.1.2 System Information



System Information interface

### System Information

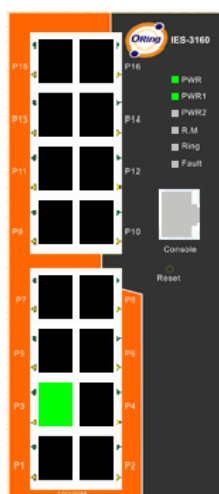
The system information will display the configuration of Basic Setting / Switch Setting page.

#### Enable Location Alert

When click  , PWR1 and PWR2 LEDs of the switch will start to flash together, and click  , the LEDs will stop flashing.

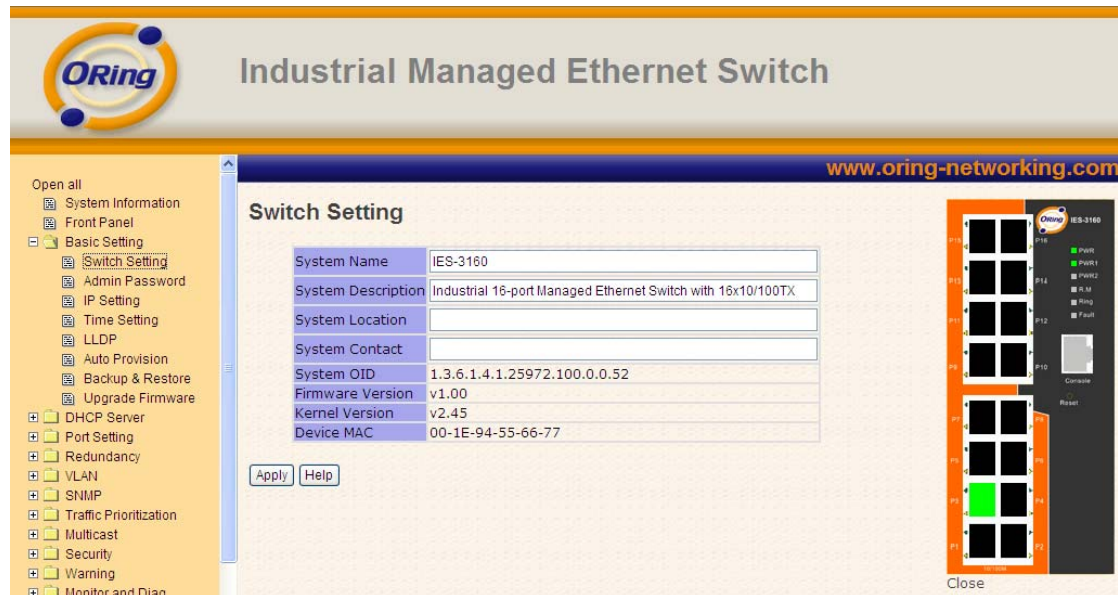
### 5.1.3 Front Panel

Show the panel of IES-3160. Click "Close" to close panel on web.



## 5.1.4 Basic setting

### 5.1.4.1 Switch Setting



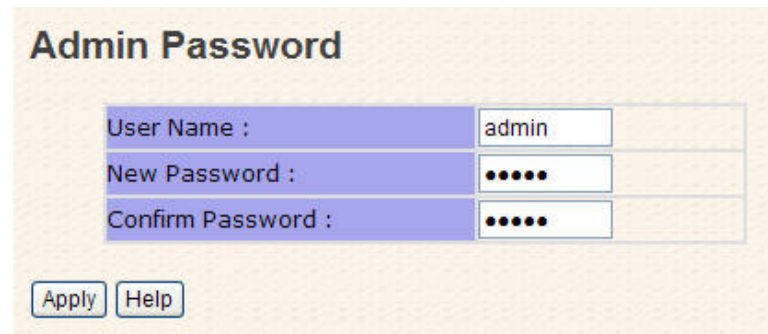
Switch setting interface

The following table describes the labels in this screen.

Label	Description
<b>System Name</b>	Assign the name of switch. The maximum length is 64 bytes
<b>System Description</b>	Display the description of switch.
<b>System Location</b>	Assign the switch physical location. The maximum length is 64 bytes
<b>System Contact</b>	Enter the name of contact person or organization
<b>System OID</b>	Display the switch's OID information
<b>Firmware Version</b>	Display the switch's firmware version
<b>Kernel Version</b>	Display the kernel software version
<b>MAC Address</b>	Display the unique hardware address assigned by manufacturer (default)

### 5.1.4.2 Admin Password

Change web management login username and password for the management security issue



The screenshot shows the 'Admin Password' configuration page. It features three input fields: 'User Name' with the value 'admin', 'New Password' with masked characters, and 'Confirm Password' with masked characters. Below the fields are 'Apply' and 'Help' buttons.

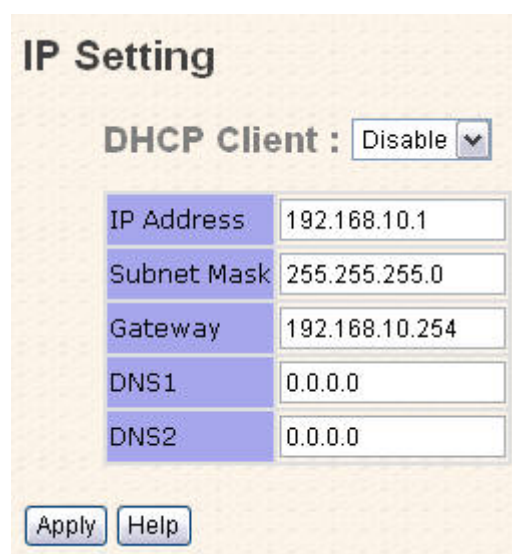
Admin Password interface

The following table describes the labels in this screen.

Label	Description
<b>User name</b>	Key in the new username (The default is “ <b>admin</b> ”)
<b>New Password</b>	Key in the new password (The default is “ <b>admin</b> ”)
<b>Confirm password</b>	Re-type the new password.
<b>Apply</b>	Click “ <b>Apply</b> ” to activate the configurations.

### 5.1.4.3 IP Setting

You can configure the IP Settings and DHCP client function through IP configuration.



The screenshot shows the 'IP Setting' configuration page. At the top, there is a 'DHCP Client' dropdown menu set to 'Disable'. Below it are five input fields: 'IP Address' (192.168.10.1), 'Subnet Mask' (255.255.255.0), 'Gateway' (192.168.10.254), 'DNS1' (0.0.0.0), and 'DNS2' (0.0.0.0). At the bottom are 'Apply' and 'Help' buttons.

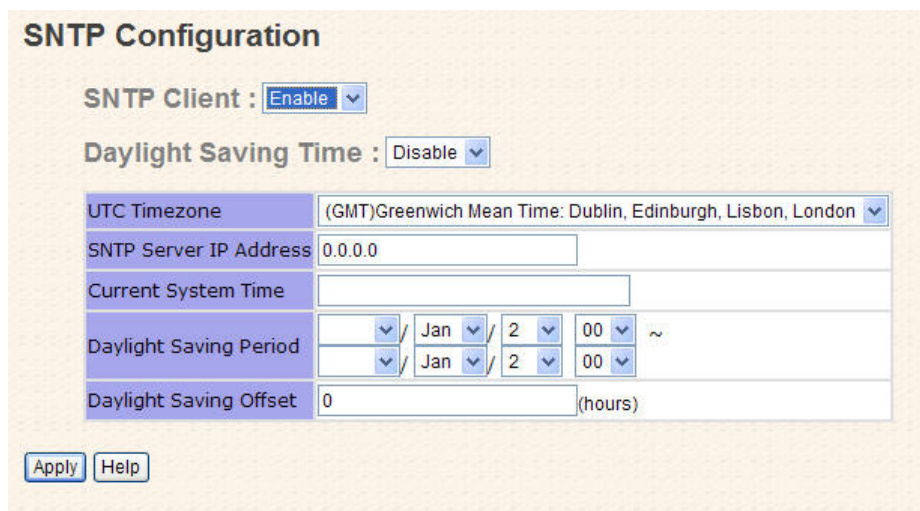
IP Configuration interface

The following table describes the labels in this screen.

Label	Description
<b>DHCP Client</b>	To enable or disable the DHCP client function. When DHCP client function is enabling, the switch will be assigned the IP address from the network DHCP server. The default IP address will be replaced by the IP address which the DHCP server has assigned. After clicking " <b>Apply</b> " button, a popup dialog shows up to inform when the DHCP client is enabling. The current IP will lose and you should find a new IP on the DHCP server.
<b>IP Address</b>	Assign the IP address that the network is using. If DHCP client function is enabling, you do not need to assign the IP address. The network DHCP server will assign the IP address for the switch and it will be display in this column. The default IP is 192.168.10.1
<b>Subnet Mask</b>	Assign the subnet mask of the IP address. If DHCP client function is enabling, you do not need to assign the subnet mask
<b>Gateway</b>	Assign the network gateway for the switch. The default gateway is 192.168.10.254
<b>DNS1</b>	Assign the primary DNS IP address
<b>DNS2</b>	Assign the secondary DNS IP address
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.

#### 5.1.4.4 SNTP (Time)

The SNTP (Simple Network Time Protocol) settings allow you to synchronize switch clocks in the Internet.



SNTP Configuration interface



The following table describes the labels in this screen.

Label	Description
<b>SNTP Client</b>	Enable or disable SNTP function to get the time from the SNTP server.
<b>Daylight Saving Time</b>	Enable or disable daylight saving time function. When daylight saving time is enabling, you need to configure the daylight saving time period.
<b>UTC Time zone</b>	Set the switch location time zone. The following table lists the different location time zone for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	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

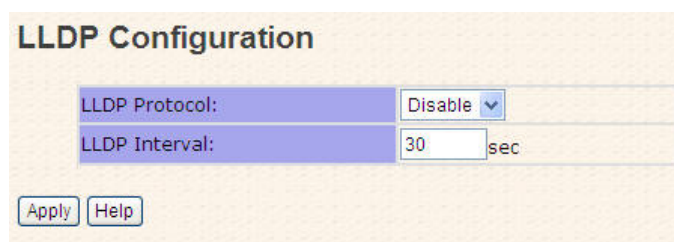
Label	Description
<b>SNTP Sever IP Address</b>	Set the SNTP server IP address.
<b>Daylight Saving</b>	Set up the Daylight Saving beginning time and Daylight Saving



<b>Period</b>	ending time. Both will be different each year.
<b>Daylight Saving Offset</b>	Set up the offset time.
<b>Switch Timer</b>	Display the switch current time.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.

#### 5.1.4.5 LLDP

LLDP (Link Layer Discovery Protocol) function allows the switch to advertise its information to other nodes on the network and store the information it discovers.



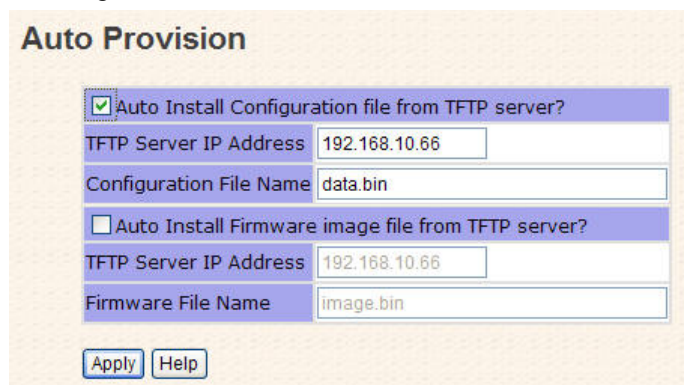
LLDP configuration interface

The following table describes the labels in this screen.

Label	Description
<b>LLDP Protocol</b>	" <b>Enable</b> " or " <b>Disable</b> " LLDP function.
<b>LLDP Interval</b>	The interval of resend LLDP (by default at 30 seconds)
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.
<b>Help</b>	Show help file.

#### 5.1.4.6 Auto Provision

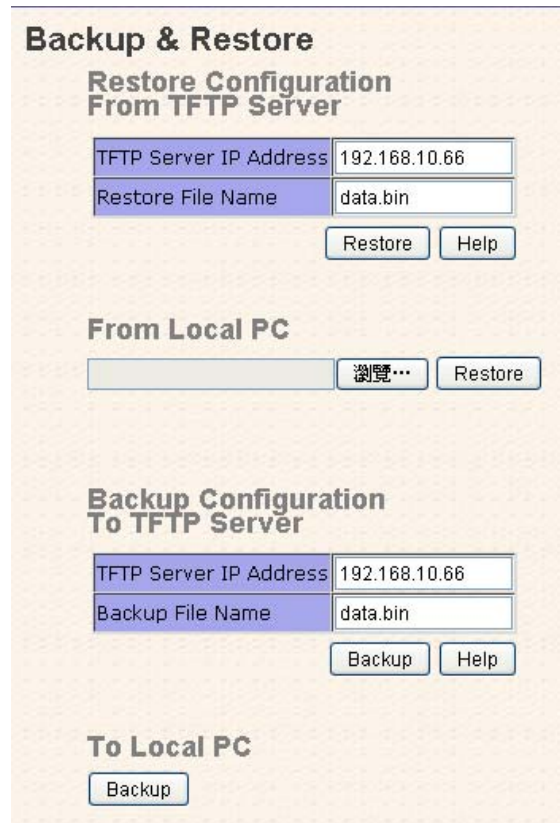
Auto Provision allows you to update the switch firmware automatically. You can put firmware or configuration file on TFTP server. When you reboot the switch, it will upgrade automatically. Before updating, make sure you have your TFTP server ready and the firmware image and configuration file is on the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



Auto Provision interface

### 5.1.4.7 Backup & Restore

You can save current configuration from the switch to TFTP server, or restore the configuration from TFTP server in this page.



The screenshot shows a web interface titled "Backup & Restore". It is divided into four main sections:

- Restore Configuration From TFTP Server:** Contains two input fields: "TFTP Server IP Address" (with value 192.168.10.66) and "Restore File Name" (with value data.bin). Below these are "Restore" and "Help" buttons.
- From Local PC:** Contains a file selection input field with a "瀏覽..." (Browse) button and a "Restore" button.
- Backup Configuration To TFTP Server:** Contains two input fields: "TFTP Server IP Address" (with value 192.168.10.66) and "Backup File Name" (with value data.bin). Below these are "Backup" and "Help" buttons.
- To Local PC:** Contains a single "Backup" button.

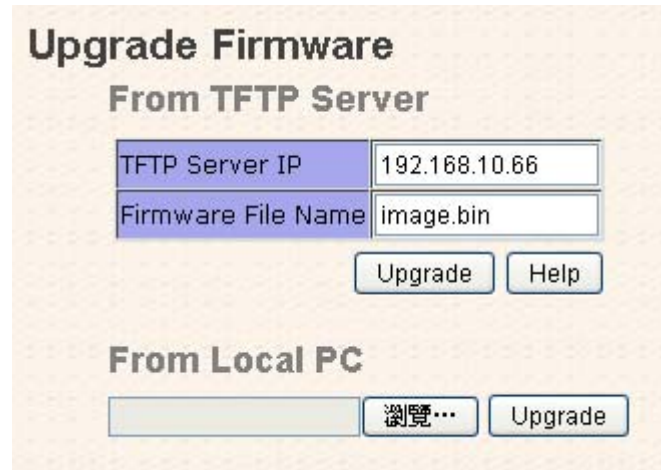
Backup & Restore interface

The following table describes the labels in this screen.

Label	Description
<b>TFTP Server IP Address</b>	Fill in the TFTP server IP
<b>Restore File Name</b>	Fill the file name.
<b>Restore</b>	Click " <b>restore</b> " to restore the configurations.
<b>Restore File Name</b>	Fill the file name.
<b>Restore</b>	Click " <b>restore</b> " to restore the configurations.
<b>Backup</b>	Click " <b>backup</b> " to backup the configurations.

### 5.1.4.8 Upgrade Firmware

Upgrade Firmware allows you to update the firmware of switch. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server.

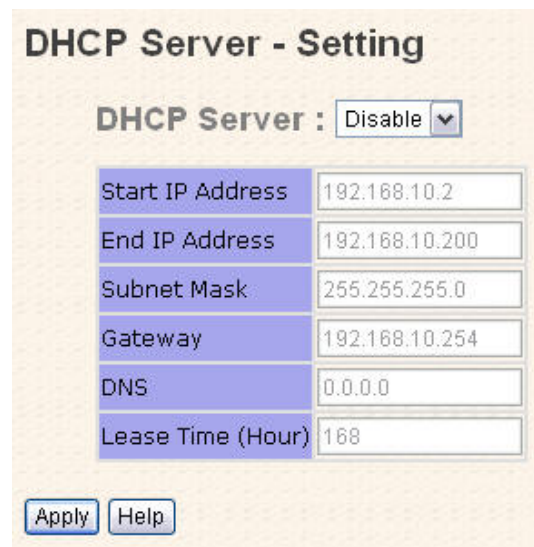


Update Firmware interface

## 5.1.5 DHCP Server

### 5.1.5.1 DHCP Server – Setting

The system provides with DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.



DHCP Server Configuration interface

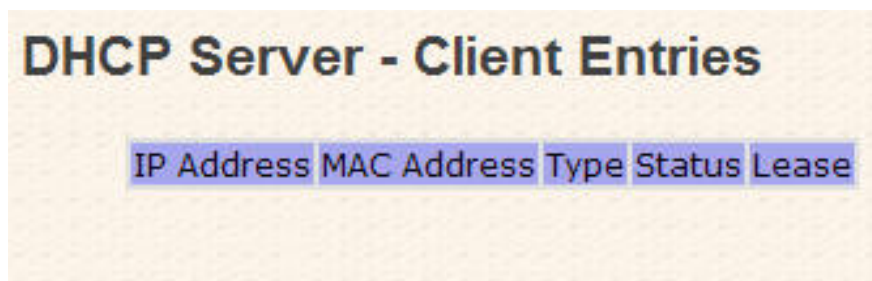
The following table describes the labels in this screen.

Label	Description
<b>DHCP Server</b>	Enable or Disable the DHCP Server function. Enable – the switch will be the DHCP server on your local network

<b>Start IP Address</b>	The dynamic IP assign range. Low IP address is the beginning of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 to 192.168.1.200. 192.168.1.100 will be the Start IP address.
<b>End IP Address</b>	The dynamic IP assign range. High IP address is the end of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 to 192.168.1.200. 192.168.1.200 will be the End IP address
<b>Subnet Mask</b>	The dynamic IP assign range subnet mask
<b>Gateway</b>	The gateway in your network.
<b>DNS</b>	Domain Name Server IP Address in your network.
<b>Lease Time (Hour)</b>	It is the period that system will reset the assigned dynamic IP to ensure the IP address is in used.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.

### 5.1.5.2 DHCP Server – Client List

When the DHCP server function is activated, the system will collect the DHCP client information and display in here.



DHCP Server Client Entries interface

### 5.1.5.3 DHCP Server – Port and IP bindings

You can assign the specific IP address which is in the assigned dynamic IP range to the specific port. When the device is connecting to the port and asks for dynamic IP assigning, the system will assign the IP address that has been assigned before in the connected device.

**DHCP Server - Port and IP Binding**

Port No.	IP Address
Port.01	<input type="text" value="0.0.0.0"/>
Port.02	<input type="text" value="0.0.0.0"/>
Port.03	<input type="text" value="0.0.0.0"/>
Port.04	<input type="text" value="0.0.0.0"/>
Port.05	<input type="text" value="0.0.0.0"/>
Port.06	<input type="text" value="0.0.0.0"/>
Port.07	<input type="text" value="0.0.0.0"/>
Port.08	<input type="text" value="0.0.0.0"/>
Port.09	<input type="text" value="0.0.0.0"/>
Port.10	<input type="text" value="0.0.0.0"/>
Port.11	<input type="text" value="0.0.0.0"/>
Port.12	<input type="text" value="0.0.0.0"/>
Port.13	<input type="text" value="0.0.0.0"/>
Port.14	<input type="text" value="0.0.0.0"/>
Port.15	<input type="text" value="0.0.0.0"/>
Port.16	<input type="text" value="0.0.0.0"/>

DHCP Server Port and IP Binding interface

## 5.1.6 Port Setting

### 5.1.6.1 Port Control

By this function, you can set the state, speed/duplex, flow control, and security of the port.

### Port Control

Port No.	State	Speed/Duplex	Flow Control	Security
Port.01	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.02	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.03	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.04	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.05	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.06	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.07	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.08	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.09	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.10	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.11	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.12	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.13	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.14	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.15	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼
Port.16	Enable ▼	AutoNegotiation ▼	Symmetric ▼	Disable ▼

Port Control interface

The following table describes the labels in this screen.

Label	Description
<b>Port NO.</b>	Port number for setting.
<b>Speed/Duplex</b>	You can set Auto-negotiation, 100 full, 100 half, 10 full or 10 half
<b>Flow Control</b>	Support symmetric and asymmetric mode to avoid packet loss when congestion occurred.
<b>Security</b>	Support port security function. When enable the function, the port will STOP learning MAC address dynamically.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.

### 5.1.6.2 Port Status

The following information provides the current port status information

Port Status					
Port No.	Type	Link	State	Speed/Duplex	Flow Control
Port.01	100TX	Down	Enable	N/A	N/A
Port.02	100TX	Down	Enable	N/A	N/A
Port.03	100TX	UP	Enable	100 Full	Enable
Port.04	100TX	Down	Enable	N/A	N/A
Port.05	100TX	Down	Enable	N/A	N/A
Port.06	100TX	Down	Enable	N/A	N/A
Port.07	100TX	Down	Enable	N/A	N/A
Port.08	100TX	Down	Enable	N/A	N/A
Port.09	100TX	Down	Enable	N/A	N/A
Port.10	100TX	Down	Enable	N/A	N/A
Port.11	100TX	Down	Enable	N/A	N/A
Port.12	100TX	Down	Enable	N/A	N/A
Port.13	100TX	Down	Enable	N/A	N/A
Port.14	100TX	Down	Enable	N/A	N/A
Port.15	100TX	Down	Enable	N/A	N/A
Port.16	100TX	Down	Enable	N/A	N/A

Port Status interface

### 5.1.6.3 Port Alias

The user can define the name of every Port. Can let user, convenient management every Port.

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"/>
Port.07	<input type="text"/>
Port.08	<input type="text"/>
Port.09	<input type="text"/>
Port.10	<input type="text"/>
Port.11	<input type="text"/>

### 5.1.6.4 Rate Limit

By this function, you can limit traffic of all ports, including broadcast, multicast and flooded Unicast. You can also set "Ingress" or "Egress" to limit traffic received or transmitted bandwidth.

#### Rate Limit

Port No.	Ingress Limit Frame Type	Ingress	Egress
Port.01	All	0 kbps	0 kbps
Port.02	All	0 kbps	0 kbps
Port.03	All	0 kbps	0 kbps
Port.04	All	0 kbps	0 kbps
Port.05	All	0 kbps	0 kbps
Port.06	All	0 kbps	0 kbps
Port.07	All	0 kbps	0 kbps
Port.08	All	0 kbps	0 kbps
Port.09	All	0 kbps	0 kbps
Port.10	All	0 kbps	0 kbps
Port.11	All	0 kbps	0 kbps
Port.12	All	0 kbps	0 kbps
Port.13	All	0 kbps	0 kbps
Port.14	All	0 kbps	0 kbps
Port.15	All	0 kbps	0 kbps
Port.16	All	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.

Rate Limit interface

The following table describes the labels in this screen.

Label	Description
<b>Ingress Limit Frame Type</b>	You can set "all", "Broadcast only", "Broadcast/Multicast" or "Broadcast/Multicast/Flooded Unicast" mode.
<b>Ingress</b>	The switch port received traffic.
<b>Egress</b>	The switch port transmitted traffic.
<b>Apply</b>	Click "Apply" to activate the configurations.



### 5.1.6.5 Port Trunk

#### Port Trunk – Setting

You can select static trunk or 802.3ad LACP to combine several physical links with a logical link to increase the bandwidth.

#### Port Trunk - Setting

Port No.	Group ID	Type
Port.01	None	Static
Port.02	None	Static
Port.03	None	Static
Port.04	None	Static
Port.05	None	Static
Port.06	None	Static
Port.07	None	Static
Port.08	None	Static
Port.09	None	Static
Port.10	None	Static
Port.11	None	Static
Port.12	None	Static
Port.13	None	Static
Port.14	None	Static
Port.15	None	Static
Port.16	None	Static

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

---

#### 802.3ad LACP Work Ports

Group ID	Work Ports
Trunk1	max
Trunk2	max
Trunk3	max
Trunk4	max
Trunk5	max
Trunk6	max
Trunk7	max
Trunk8	max

Port Trunk - Setting interface

The following table describes the labels in this screen.

Label	Description
<b>Group ID</b>	Select port to join a trunk group.
<b>Type</b>	Support static trunk and 802.3ad LACP
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.

### Port Trunk – Status

You can check the configuration of port trunk.



Group ID	Trunk Member	Type
Trunk 1		Static
Trunk 2		Static
Trunk 3		Static
Trunk 4		Static
Trunk 5		Static
Trunk 6		Static
Trunk 7		Static
Trunk 8		Static

Port Trunk - Status interface

## 5.1.7 Redundancy

### 5.1.7.1 O-Ring

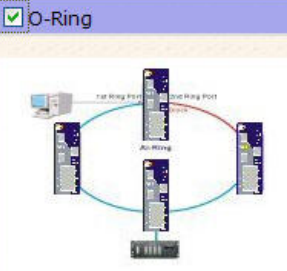
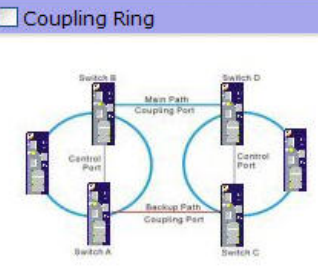

O-Ring is one of the most powerful Redundant Ring technologies in the world. The recovery time of O-Ring is less than 10 ms over 250 units of connections. It can reduce unexpected malfunction caused by network topology change. O-Ring technology supports three Ring topologies for network redundancy: O-Ring, Coupling Ring and Dual Homing.

### O-Ring

O-Ring

Coupling Ring

Dual Homing

Ring Master	Disable	Coupling Port	Port.03
1st Ring Port	Port.01	Control Port	Port.04
2nd RingPort	Port.02		

Apply
Help

\* Connect to other vendor's ring...

O-Ring interface

The following table describes the labels in this screen.

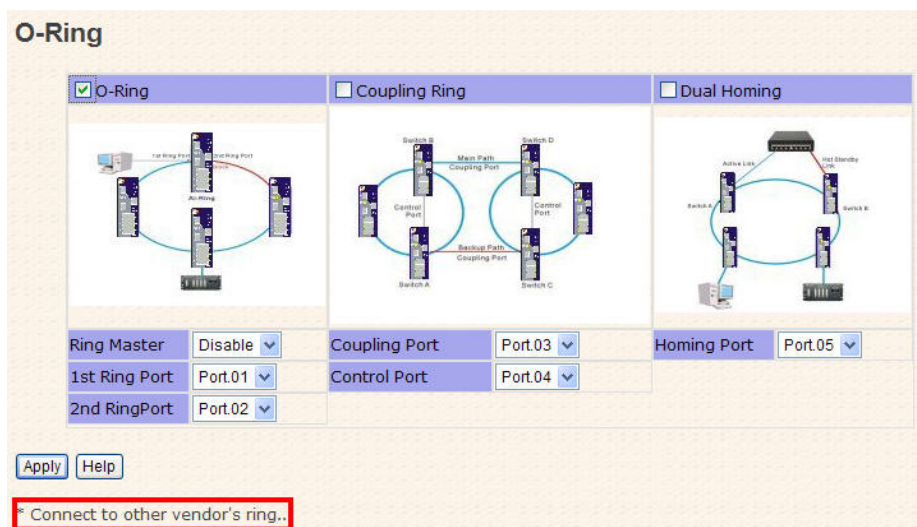
Label	Description
<b>O-Ring</b>	To enable O-Ring.
<b>Ring Master</b>	There should be one and only one Ring Master in a ring. However if there are two or more switches which set Ring Master to enable, the switch with the lowest MAC address will be the actual Ring Master and others will be Backup Masters.
<b>1<sup>st</sup> Ring Port</b>	The primary port, when this switch is configured in O-Ring.
<b>2<sup>nd</sup> Ring Port</b>	The backup port, when this switch is configured in O-Ring.
<b>Coupling Ring</b>	To enable Coupling Ring. Coupling Ring can be used to divide a big ring into two smaller Rings to avoid effecting all switches when network topology change. It is a good application for connecting two Rings.
<b>Coupling Port</b>	Set a port as coupling port to link to the Coupling Port of the switch in another ring. Coupling Ring need four switch to

	construct an active and a backup link. The coupled four ports of four switches will be operated at active/backup mode.
<b>Control Port</b>	Set a port as Control Port to link to the Control Port of the switch in the same ring. Control Port used to transmit control signals.
<b>Dual Homing</b>	To enable Dual Homing. By selecting Dual Homing mode, Ring will be connected to normal switches through two RSTP links (i.e., backbone Switch). The two links act as active/backup mode, and connect each Ring to the normal switches in RSTP mode.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.

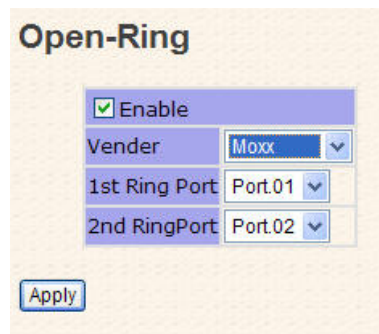
**Note:** It is not recommended to set one switch as a Ring Master and a Coupling Ring at the same time due to heavy load of system.

### 5.1.7.2 Open-Ring

Open-Ring technology can be applied for other vendor's proprietary ring. Thus, you can add switches of ORing into the network constructed by other ring technology and enable Open-Ring to co-operate with other vendor's managed switch.



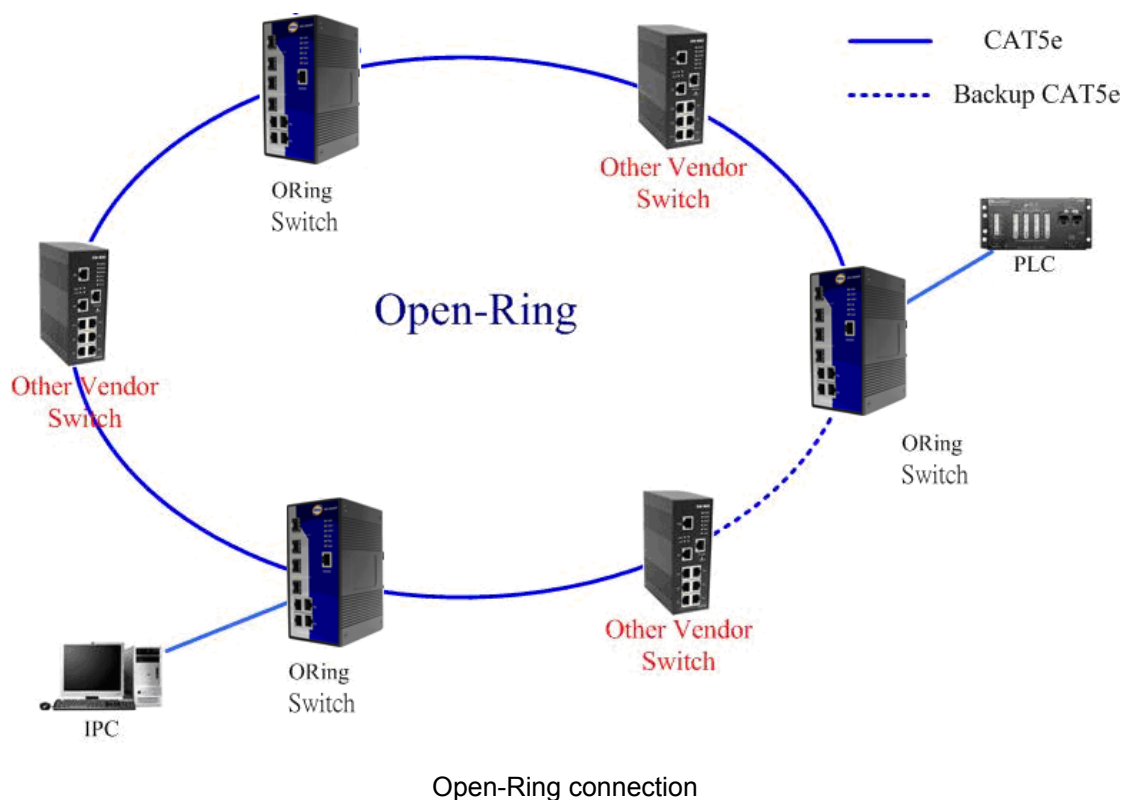
Click "Connect to other vendor's ring....." to join the ring constructed by other vendor.



Open-Ring interface

Label	Description
Enable	Enabling the Open-Ring function
Vender	Choosing the venders that you want to join to their ring
1 <sup>st</sup> Ring Port	Choosing the port which connect to the ring
2 <sup>nd</sup> Ring Port	Choosing the port which connect to the ring

The application of Open-Ring is shown as below.



### 5.1.7.3 O-RSTP

O-RSTP is proprietary redundant ring technology invented by ORing. Different from standard STP/RSTP, the recovery time of O-RSTP is less than 20ms and support more nodes of connection in a ring topology.

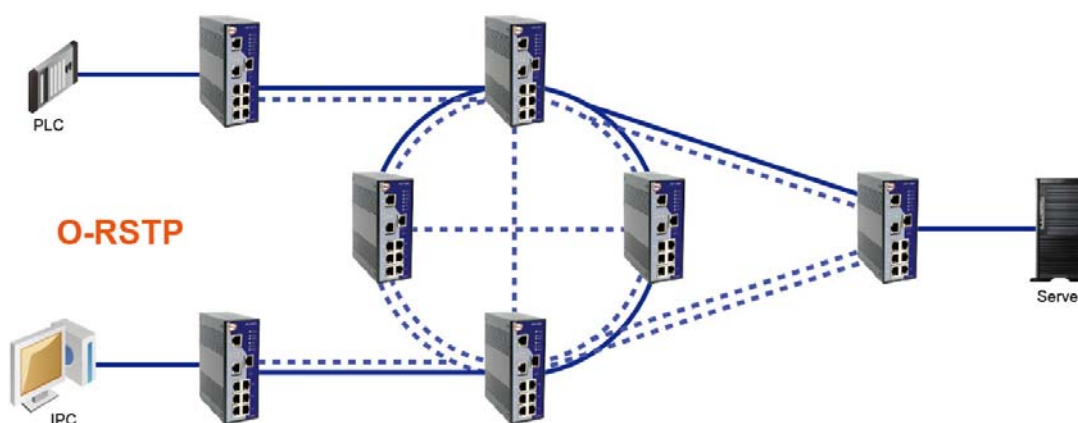
### O-RSTP

ROOT switch:

Port No.	Active	State
Port.01	<input type="checkbox"/>	INACTIVE
Port.02	<input type="checkbox"/>	INACTIVE
Port.03	<input type="checkbox"/>	INACTIVE
Port.04	<input type="checkbox"/>	INACTIVE
Port.05	<input type="checkbox"/>	INACTIVE
Port.06	<input type="checkbox"/>	INACTIVE
Port.07	<input type="checkbox"/>	INACTIVE
Port.08	<input type="checkbox"/>	INACTIVE
Port.09	<input type="checkbox"/>	INACTIVE
Port.10	<input type="checkbox"/>	INACTIVE
Port.11	<input type="checkbox"/>	INACTIVE
Port.12	<input type="checkbox"/>	INACTIVE
Port.13	<input type="checkbox"/>	INACTIVE
Port.14	<input type="checkbox"/>	INACTIVE
Port.15	<input type="checkbox"/>	INACTIVE
Port.16	<input type="checkbox"/>	INACTIVE
Port.17	<input type="checkbox"/>	INACTIVE
Port.18	<input type="checkbox"/>	INACTIVE

O-RSTP interface

The application of O-RSTP is shown as below.



O-RSTP connection

### 5.1.7.4 RSTP

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol (STP). It provides faster convergence of spanning tree after a topology change. The system also supports STP and the system will detect the connected device that is running STP or RSTP protocol automatically.

#### RSTP setting

You can enable/disable RSTP function, and set parameters for each port.

### RSTP Setting

**RSTP Mode:** Disable ▾

**Bridge Setting**

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

**Port Setting**

Port No.	Path Cost (1-200000000)	Priority (0-240)	P2P	Edge	Non STP
Port.01	200000	128	Auto ▾	true ▾	false ▾
Port.02	200000	128	Auto ▾	true ▾	false ▾
Port.03	200000	128	Auto ▾	true ▾	false ▾
Port.04	200000	128	Auto ▾	true ▾	false ▾
Port.05	200000	128	Auto ▾	true ▾	false ▾
Port.06	200000	128	Auto ▾	true ▾	false ▾
Port.07	200000	128	Auto ▾	true ▾	false ▾
Port.08	200000	128	Auto ▾	true ▾	false ▾
Port.09	200000	128	Auto ▾	true ▾	false ▾
Port.10	200000	128	Auto ▾	true ▾	false ▾
Port.11	200000	128	Auto ▾	true ▾	false ▾
Port.12	200000	128	Auto ▾	true ▾	false ▾
Port.13	200000	128	Auto ▾	true ▾	false ▾
Port.14	200000	128	Auto ▾	true ▾	false ▾
Port.15	200000	128	Auto ▾	true ▾	false ▾
Port.16	200000	128	Auto ▾	true ▾	false ▾
Port.17	200000	128	Auto ▾	true ▾	false ▾
Port.18	200000	128	Auto ▾	true ▾	false ▾

Apply
Help

RSTP Setting interface



The following table describes the labels in this screen.

Label	Description
<b>RSTP mode</b>	You must enable or disable RSTP function before configuring the related parameters.
<b>Priority (0-61440)</b>	A value used to identify the root bridge. The bridge with the lowest value with the highest priority and is selected as the root. If the value changes, you must restart the switch. The value must be multiple of 4096 according to the rule of the protocol.
<b>Max Age (6-40)</b>	The number of seconds for a bridge to wait without receiving Spanning-tree Protocol configuration messages before reconfiguration. Enter a value between 6 through 40.
<b>Hello Time (1-10)</b>	The time that controls switch sends out the BPDU (Bridge Protocol Data Unit) packet to check RSTP current status. Enter a value between 1 through 10.
<b>Forwarding Delay Time (4-30)</b>	The number of seconds a port to wait before changing from its learning/listening state to forwarding state. Enter a value between 4 through 30.
<b>Path Cost (1-200000000)</b>	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
<b>Priority (0-240)</b>	Decide which port should be blocked by setting the priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16
<b>Admin P2P</b>	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e., It is served by a point-to-point LAN segment), or it can be connected to two or more bridges (i.e., It is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True means P2P enabled. False means P2P disabled.
<b>Admin Edge</b>	The port directly connected to end stations, and it cannot create bridging loop in the network. To configure the port as an edge port, set the port to "True".
<b>Admin Non STP</b>	The port includes the STP mathematic calculation. STP algorithm is included for "True" setting, STP algorithm is not



	included for <b>“False”</b> setting.
<b>Apply</b>	Click <b>“Apply”</b> to activate the configurations.

**NOTE:** Follow the rule to configure the MAX Age, Hello Time, and Forward Delay Time:

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

## RSTP Information

Show RSTP algorithm result at this table.

www

### RSTP Information

#### Root Bridge Information

Bridge ID	0080001E94ABCDEF
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	Disabled	Disabled
Port.06	200000	128	True	True	False	Disabled	Disabled
Port.07	200000	128	True	True	False	Disabled	Disabled
Port.08	200000	128	True	True	False	Disabled	Disabled
Port.09	200000	128	True	True	False	Disabled	Disabled
Port.10	200000	128	True	True	False	Disabled	Disabled
Port.11	200000	128	True	True	False	Disabled	Disabled
Port.12	200000	128	True	True	False	Disabled	Disabled
Port.13	200000	128	True	True	False	Disabled	Disabled
Port.14	200000	128	True	True	False	Disabled	Disabled
Port.15	200000	128	True	True	False	Disabled	Disabled
Port.16	200000	128	True	True	False	Forwarding	Designated

RSTP Information interface

### 5.1.7.5 MSTP

Multiple Spanning Tree Protocol (MSTP) is a standard protocol base on IEEE 802.1s. The function is that several VLANs can be mapping to a reduced number of spanning tree instances because most networks do not need more than a few logical topologies. It supports load balancing scheme and the CPU is sparer than PVST (Cisco proprietary technology).

### MSTP Setting

<b>MSTP Enable</b>	Disable ▾
<b>Force Version</b>	MSTP ▾
<b>Configuration Name</b>	MSTP_SWITCH
<b>Revision Level (0-65535)</b>	0
<b>Priority (0-61440)</b>	32768
<b>Max Age Time (6-40)</b>	20
<b>Hello Time (1-10)</b>	2
<b>Forward Delay Time (4-30)</b>	15
<b>Max Hops (1-40)</b>	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).**

MSTP Setting interface

The following table describes the labels in this screen.

Label	Description
<b>MSTP Enable</b>	You must enable or disable MSTP function before configuring the related parameters.
<b>Force Version</b>	The Force Version parameter can be used to force a VLAN Bridge that supports RSTP to operate in an STP-compatible manner.
<b>Configuration Name</b>	The same MST Region must have the same MST configuration name.
<b>Revision Level (0-65535)</b>	The same MST Region must have the same revision level.
<b>Priority (0-61440)</b>	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 multiple of 4096 according to the protocol standard rule.
<b>Max Age Time(6-40)</b>	The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
<b>Hello Time (1-10)</b>	The setting follow the rule below to configure the MAX Age, Hello Time, and Forward Delay Time at controlled switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.  $2 \times (\text{Forward Delay Time value} - 1) \geq \text{Max Age value} \geq 2 \times (\text{Hello Time value} + 1)$
<b>Forwarding Delay Time (4-30)</b>	The number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.
<b>Max Hops (1-40)</b>	This parameter is additional to those specified for RSTP. A single value applies to all Spanning Trees within an MST Region (the CIST and all MSTIs) for which the Bridge is the Regional Root.
<b>Apply</b>	Click " <b>Apply</b> " to activate 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 ▼ Port.04 Port.05 ▼	128	0	auto ▼	true ▼	false ▼

priority must be a multiple of 16

Apply

### Port Information

Port	Priority	Path Cost		P2P		Edge		Admin Non Stp
		Admin	Oper	Admin	Oper	Admin	Oper	

MSTP Port interface



Label	Description
<b>Port No.</b>	Selecting the port that you want to configure.
<b>Priority (0-240)</b>	Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16
<b>Path Cost (1-200000000)</b>	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
<b>Admin P2P</b>	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. It is served by a point-to-point LAN segment), or it can be connected to two or more bridges (i.e. It is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True means P2P enabling. False means P2P disabling.
<b>Admin Edge</b>	Label
<b>Admin Non STP</b>	Label
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.

### MSTP Instance

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

Priority must be a multiple of 4096.

### Instance Information

Instance	VLANs	Priority	Regional Root Bridge ID	Path Cost	Root Port

MSTP Instance interface

Label	Description
<b>Instance</b>	Set the instance from 1 to 15
<b>State</b>	Enable or disable the instance
<b>VLANs</b>	Set which VLAN will belong which instance

<b>Proprietary (0-61440)</b>	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 multiple of 4096 according to the protocol standard rule.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.

### 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

### Instance Port Information

Port No.	Priority	Path Cost		State	Role
		Admin	Oper		

MSTP Instance Port interface

Label	Description
<b>Instance</b>	Set the instance's information except CIST
<b>Port</b>	Selecting the port that you want to configure.
<b>Priority (0-240)</b>	Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16
<b>Path Cost (1-200000000)</b>	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
<b>Apply</b>	Click " <b>Apply</b> " to set the configurations.



## 5.1.8 VLAN

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which allows you to isolate network traffic. Only the members of the same VLAN will receive the traffic from the other members. Basically, to create a VLAN from a switch is logically equivalent of separating a group of network devices. However, all the network devices are still plugged into the same switch physically.

This managed switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration of VLAN operation mode is at “**802.1Q**”.

### 5.1.8.1 VLAN Setting

Tagged-based VLAN is an IEEE 802.1Q specification standard, and it is possible to create a VLAN across devices from different switch vendors. IEEE 802.1Q VLAN uses a technique to insert a “tag” into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

You can create Tag-based VLAN, and enable or disable GVRP protocol. There are 256 VLAN groups available. Enable 802.1Q VLAN, all ports on the switch belong to default VLAN, VID is 1. The default VLAN cannot be deleted.

GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request by using the VID of a VLAN defined on the switch; the switch will automatically add that device to the existing VLAN.

## VLAN Setting

VLAN Operation Mode : 802.1Q GVRP Mode : Disable Management Vlan ID : 0 

### VLAN Configuration

Port No.	Link Type	Untagged VID	Tagged VIDs
Port.01	Access <input type="button" value="v"/>	1 <input type="text"/>	<input type="text"/>
Port.02	Access <input type="button" value="v"/>	1 <input type="text"/>	<input type="text"/>
Port.03	Access <input type="button" value="v"/>	1 <input type="text"/>	<input type="text"/>
Port.04	Access <input type="button" value="v"/>	1 <input type="text"/>	<input type="text"/>
Port.05	Access <input type="button" value="v"/>	1 <input type="text"/>	<input type="text"/>
Port.06	Access <input type="button" value="v"/>	1 <input type="text"/>	<input type="text"/>
Port.07	Access <input type="button" value="v"/>	1 <input type="text"/>	<input type="text"/>
Port.08	Access <input type="button" value="v"/>	1 <input type="text"/>	<input type="text"/>
Port.09	Access <input type="button" value="v"/>	1 <input type="text"/>	<input type="text"/>
Port.10	Access <input type="button" value="v"/>	1 <input type="text"/>	<input type="text"/>
Port.11	Access <input type="button" value="v"/>	1 <input type="text"/>	<input type="text"/>
Port.12	Access <input type="button" value="v"/>	1 <input type="text"/>	<input type="text"/>
Port.13	Access <input type="button" value="v"/>	1 <input type="text"/>	<input type="text"/>
Port.14	Access <input type="button" value="v"/>	1 <input type="text"/>	<input type="text"/>
Port.15	Access <input type="button" value="v"/>	1 <input type="text"/>	<input type="text"/>
Port.16	Access <input type="button" value="v"/>	1 <input type="text"/>	<input type="text"/>

Note: Use the comma to separate the multiple tagged VIDs.  
E.g., 2-4,6 means joining the Tagged VLAN 2, 3, 4 and 6.

VLAN Configuration – 802.1Q interface



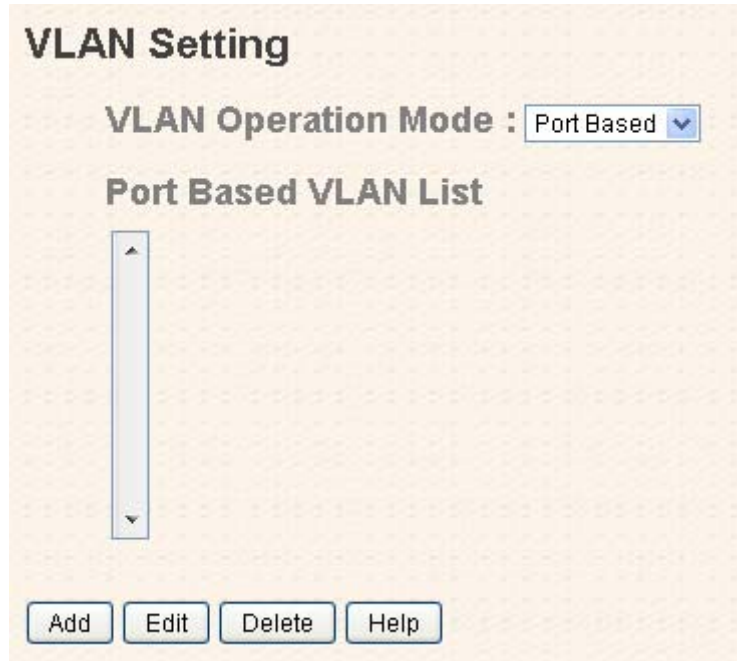
The following table describes the labels in this screen.

Label	Description
<b>VLAN Operation Mode</b>	Configure VLAN Operation Mode: disable, Port Base,802.1Q
<b>GVRP Mode</b>	Enable/Disable GVRP function.
<b>Management VLAN ID</b>	Management VLAN provide network administrator a secured VLAN to management Switch. Only the devices in the management VLAN can access the switch.
<b>Link type</b>	There are 3 types of link type: <b>Access Link:</b> single switch only, allows you to group ports by setting the same VID. <b>Trunk Link:</b> extended application of <b>Access Link</b> , allows you to group ports by setting the same VID with 2 or more switches. <b>Hybrid Link:</b> Both <b>Access Link</b> and <b>Trunk Link</b> are available. <b>Hybrid(QinQ) Link:</b> enable QinQ mode , allow you to insert one more VLAN tag in a original VLAN frame.
<b>Untagged VID</b>	Set the port default VLAN ID for untagged devices that connect to the port. The range is 1 to 4094.
<b>Tagged VIDs</b>	Set the tagged VIDs to carry different VLAN frames to other switch.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.



### 5.1.8.2 VLAN Setting – Port Based

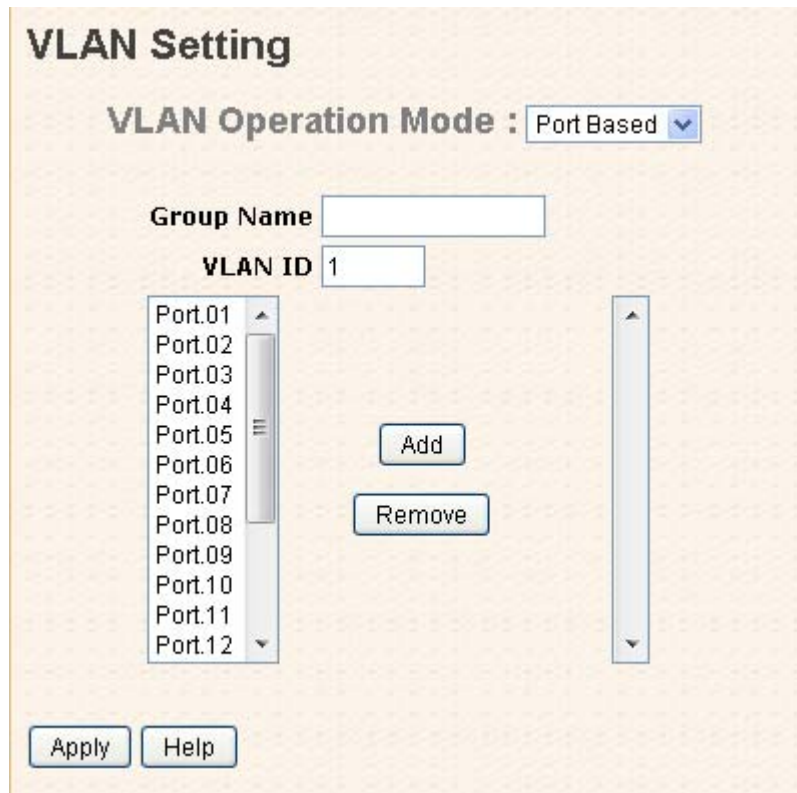
Traffic is forwarded to the member ports of the same vlan group. vlan port based startup, set in the same group of the port, can be a normal transmission packet, without restricting the types of packets.



VLAN Configuration – Port Base interface-1

The following table describes the labels in this screen.

Label	Description
<b>Add</b>	Click “ <b>add</b> ” to enter VLAN add interface.
<b>Edit</b>	Edit exist VLAN
<b>Delete</b>	Delete exist VLAN
<b>Help</b>	Show help file.



VLAN Configuration – Port Base interface-2

The following table describes the labels in this screen.

Label	Description
<b>Group Name</b>	VLAN name.
<b>VLAN ID</b>	Specify the VLAN ID
<b>Add</b>	Select port to join the VLAN group.
<b>Remove</b>	Remove port of the VLAN group
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.
<b>Help</b>	Show help file.

### 5.1.9 SNMP

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

### 5.1.9.1 SNMP – Agent Setting

You can set SNMP agent related information by Agent Setting Function.



SNMP Agent Setting interface

The following table describes the labels in this screen.

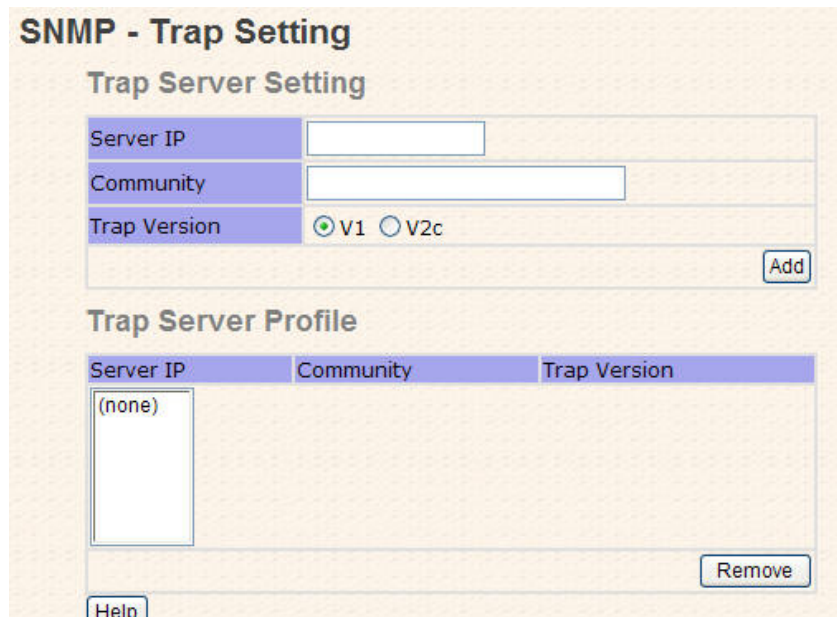
Label	Description
<b>SNMP agent Version</b>	Three SNMP versions are supported such as SNMP V1/SNMP V2c, and SNMP V3. SNMP V1/SNMP V2c agent use a community string match for authentication, that means SNMP servers access objects with read-only or read/write permissions with the community default string public/private. SNMP V3 requires an authentication level of MD5 or DES to encrypt data to enhance data security.
<b>SNMP V1/V2c Community</b>	SNMP Community should be set for SNMP V1/V2c. Four sets of "Community String/Privilege" are supported. Each Community String is maximum 32 characters. Keep empty to remove this



	Community string.
<b>SNMPv3User</b>	<p>If SNMP V3 agent is selected, the SNMPv3 you profiled should be set for authentication. The Username is necessary. The Auth Password is encrypted by MD5 and the Privacy Password which is encrypted by DES. There are maximum 8 sets of SNMPv3 User and maximum 16 characters in username, and password.</p> <p>When SNMP V3 agent is selected, you can:</p> <ol style="list-style-type: none"><li>1. Input SNMPv3 username only.</li><li>2. Input SNMPv3 username and Auth Password.</li><li>3. Input SNMPv3 username, Auth Password and Privacy Password, which can be different with Auth Password.</li></ol> <p>To remove a current user profile:</p> <ol style="list-style-type: none"><li>1. Input SNMPv3 user name you want to remove.</li><li>2. Click "<b>Remove</b>" button</li></ol>
<b>Current SNMPv3 User Profile</b>	Show all SNMPv3 user profiles.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.
<b>Help</b>	Show help file.

### 5.1.9.2 SNMP – Trap Setting

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will issue. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager and enter SNMP community strings and selects the SNMP version.



The image shows the 'SNMP - Trap Setting' web interface. It is divided into two main sections: 'Trap Server Setting' and 'Trap Server Profile'.  
 In the 'Trap Server Setting' section, there are three input fields: 'Server IP', 'Community', and 'Trap Version'. The 'Trap Version' field has two radio buttons, 'V1' (which is selected) and 'V2c'. An 'Add' button is located at the bottom right of this section.  
 The 'Trap Server Profile' section contains a table with three columns: 'Server IP', 'Community', and 'Trap Version'. The table currently has one row with '(none)' in the 'Server IP' column. A 'Remove' button is at the bottom right, and a 'Help' button is at the bottom left.

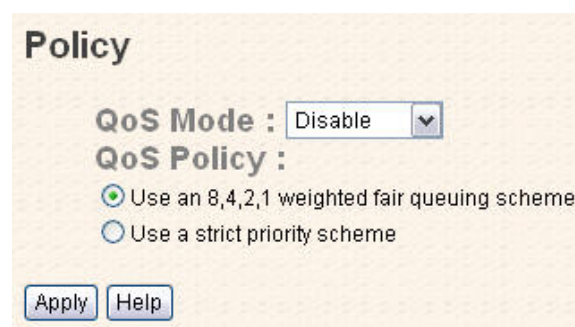
SNMP Trap Setting interface

The following table describes the labels in this screen.

Label	Description
<b>Server IP</b>	The server IP address to receive Trap
<b>Community</b>	Community for authentication
<b>Trap Version</b>	Trap Version supports V1 and V2c.
<b>Add</b>	Add trap server profile.
<b>Remove</b>	Remove trap server profile.
<b>Help</b>	Show help file.

### 5.1.10 Traffic Prioritization

Traffic Prioritization includes 3 modes: port base, 802.1p/COS, and TOS/DSCP. By traffic prioritization function, you can classify the traffic into four classes for differential network application. IES-3160 support 4 priority queues.



The image shows the 'Policy' web interface. It features a 'QoS Mode' dropdown menu currently set to 'Disable'. Below it is the 'QoS Policy' section with two radio buttons: 'Use an 8,4,2,1 weighted fair queuing scheme' (which is selected) and 'Use a strict priority scheme'. At the bottom, there are 'Apply' and 'Help' buttons.

Policy Setting interface



Label	Description
<b>QoS Mode</b>	<ul style="list-style-type: none"><li>■ <b>Port-base:</b> the output priority is determined by ingress port.</li><li>■ <b>COS only:</b> the output priority is determined by COS only.</li><li>■ <b>TOS only:</b> the output priority is determined by TOS only.</li><li>■ <b>COS first:</b> the output priority is determined by COS and TOS, but COS first.</li><li>■ <b>TOS first:</b> the output priority is determined by COS and TOS, but TOS first.</li></ul>
<b>QoS policy</b>	<ul style="list-style-type: none"><li>■ <b>Using the 8,4,2,1 weight fair queue scheme:</b> the output queues will follow 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.</li><li>■ <b>Use the strict priority scheme:</b> always the packets in higher queue will be transmitted first until higher queue is empty.</li></ul>
<b>Help</b>	Show help file.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.

### Port-based Priority

Port No.	Priority
Port.01	Lowest ▼
Port.02	Lowest ▼
Port.03	Lowest ▼
Port.04	Lowest ▼
Port.05	Lowest ▼
Port.06	Lowest ▼
Port.07	Lowest ▼
Port.08	Lowest ▼
Port.09	Lowest ▼
Port.10	Lowest ▼
Port.11	Lowest ▼
Port.12	Lowest ▼
Port.13	Lowest ▼
Port.14	Lowest ▼
Port.15	Lowest ▼
Port.16	Lowest ▼

Port-based Priority interface

Label	Description
<b>Port base Priority</b>	Assign Port with a priority queue. 4 priority queues can be assigned: High, Middle, Low, and Lowest.
<b>Help</b>	Show help file.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.

### COS/802.1p

COS	Priority
0	Low
1	Lowest
2	Lowest
3	Low
4	Middle
5	Middle
6	High
7	High

### COS Port Default

Port No.	COS
Port.01	0
Port.02	0
Port.03	0
Port.04	0
Port.05	0
Port.06	0
Port.07	0
Port.08	0
Port.09	0
Port.10	0
Port.11	0
Port.12	0
Port.13	0
Port.14	0
Port.15	0
Port.16	0

COS/802.1p interface



Label	Description
<b>COS/802.1p</b>	COS (Class Of Service) is well known as 802.1p. It describes that the output priority of a packet is determined by user priority field in 802.1Q VLAN tag. The priority value is supported 0 to 7. COS value map to 4 priority queues: High, Middle, Low, and Lowest.
<b>COS Port Default</b>	When an ingress packet has not VLAN tag, a default priority value is considered and determined by ingress port.
<b>Help</b>	Show help file.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.

**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 ▾

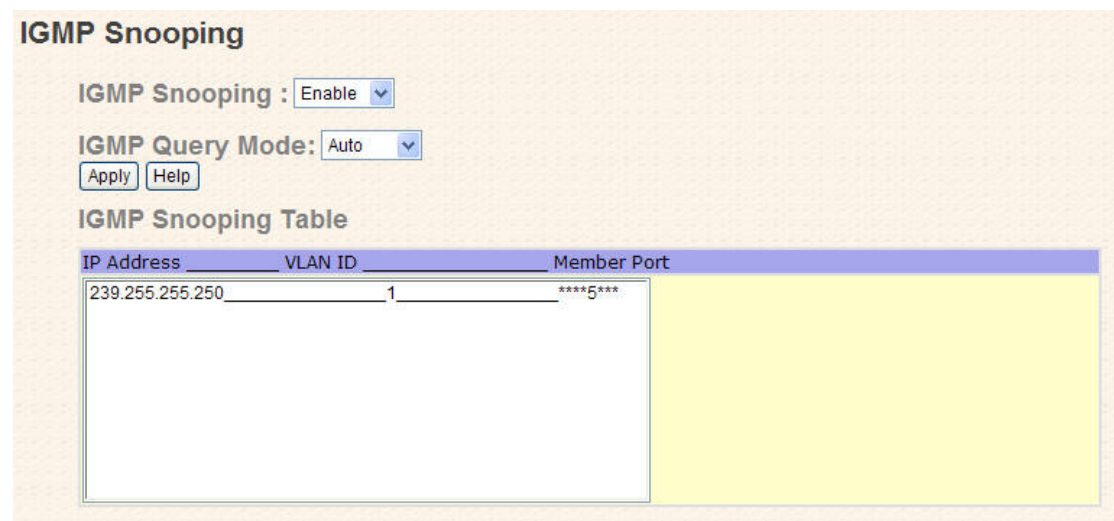
TOS/DSCP interface

Label	Description
<b>TOS/DSCP</b>	TOS (Type of Service) is a field in IP header of a packet. This TOS field is also used by Differentiated Services and is called the Differentiated Services Code Point (DSCP). The output priority of a packet can be determined by this field and the priority value is supported 0 to 63. DSCP value map to 4 priority queues: High, Middle, Low, and Lowest.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.
<b>Help</b>	Show help file.

## 5.1.11 Multicast

### 5.1.11.1 IGMP Snooping

Internet Group Management Protocol (IGMP) is used by IP hosts to register their dynamic multicast group membership. IGMP has 3 versions, IGMP v1, v2 and v3. Please refer to RFC 1112, 2236 and 3376. IGMP Snooping improves the performance of networks that carry multicast traffic. It provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic and reduces the amount of traffic on the Ethernet LAN.



**IGMP Snooping**

IGMP Snooping :  ▾

IGMP Query Mode:  ▾

**IGMP Snooping Table**

IP Address	VLAN ID	Member Port
239.255.255.250	1	****5***

IGMP Snooping interface

The following table describes the labels in this screen.

Label	Description
<b>IGMP Snooping</b>	Enable/Disable IGMP snooping.
<b>IGMP Query Mode</b>	Switch will be IGMP querier or not. There should exist one and the only one IGMP querier in an IGMP application. The "Auto" mode means that the querier is the one with lower IP address.
<b>IGMP Snooping Table</b>	Show current IP multicast list
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.
<b>Help</b>	Show help file.

### 5.1.11.2 MVR

**MVR**

MVR Mode:  ▾

MVR VLAN:

Port	Type	Immediate Leave
Port.01	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.02	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.03	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.04	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.05	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.06	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.07	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.08	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.09	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.10	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.11	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.12	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.13	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.14	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.15	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>
Port.16	<input type="text" value="Inactive"/> ▾	<input type="checkbox"/>

MVR interface

### 5.1.11.3 Multicast Filter

Multicast filtering is the system by which end stations only receive multicast traffic if they register to join specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end stations.

## Multicast Filtering

IP Address

Port.01    Port.02    Port.03    Port.04  
 Port.05    Port.06    Port.07    Port.08

Member Ports

Port.09    Port.10    Port.11    Port.12  
 Port.13    Port.14    Port.15    Port.16

### Multicast Filtering List

IP Address	Member Ports
<div style="border: 1px solid #ccc; width: 100%; height: 100%;"></div>	

Multicast Filtering interface

The following table describes the labels in this screen.

Label	Description
<b>IP Address</b>	Assign a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255
<b>Member Ports</b>	Tick the check box beside the port number to include them as the member ports in the specific multicast group IP address.
<b>Add</b>	Show current IP multicast list
<b>Delete</b>	Delete an entry from table
<b>Help</b>	Show help file.

## 5.1.12 Security

Five useful functions can enhance security of switch: IP Security, Port Security, MAC Blacklist, and MAC address Aging and 802.1x protocol.

### 5.1.12.1 IP Security

IP security can enable/disable remote management from WEB or Telnet or SNMP. Additionally, IP security can restrict remote management to some specific IP addresses. Only these secure IP addresses can manage this switch remotely.



IP Security interface

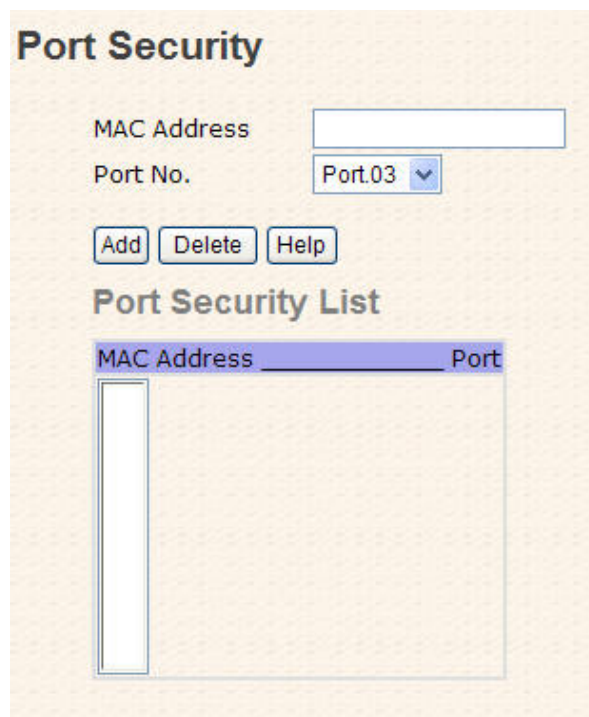
The following table describes the labels in this screen.

Label	Description
<b>IP security MODE</b>	Enable/Disable the IP security function.
<b>Enable WEB</b>	Mark the blank to enable WEB Management.

<b>Management</b>	
<b>Enable Telnet Management</b>	Mark the blank to enable Telnet Management.
<b>Enable SNMP Management</b>	Mark the blank to enable MPSN Management.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.
<b>Help</b>	Show help file.

### 5.1.12.2 Port Security

Port security is to add static MAC addresses to hardware forwarding database. If port security is enabled at **Port Control** page, only the frames with MAC addresses in this list will be forwarded, otherwise will be discarded.



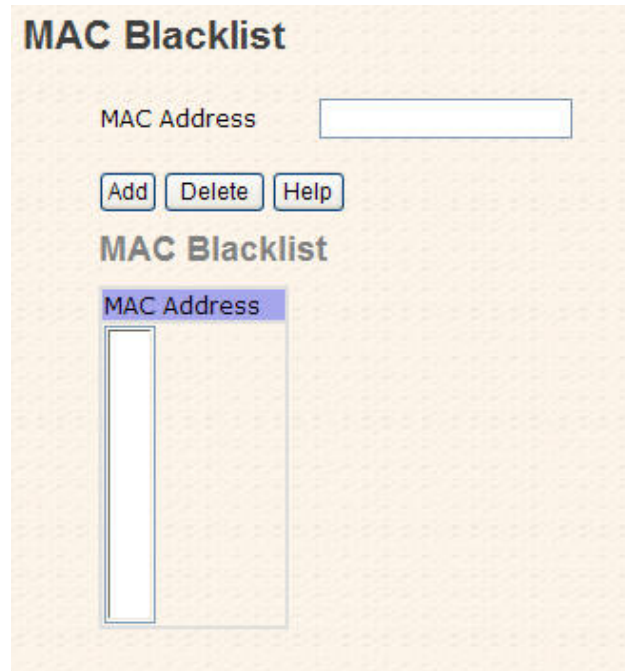
Port Security interface

The following table describes the labels in this screen.

Label	Description
<b>MAC Address</b>	Input MAC Address to a specific port.
<b>Port NO.</b>	Select port of switch.
<b>Add</b>	Add an entry of MAC and port information.
<b>Delete</b>	Delete the entry.
<b>Help</b>	Show help file.

### 5.1.12.3 MAC Blacklist

MAC Blacklist can eliminate the traffic forwarding to specific MAC addresses in list. Any frames forwarding to MAC addresses in this list will be discarded. Thus the target device will never receive any frame.



The screenshot shows a web interface for managing a MAC blacklist. At the top, there is a title "MAC Blacklist". Below the title is a text input field labeled "MAC Address". Underneath the input field are three buttons: "Add", "Delete", and "Help". Below the buttons is another title "MAC Blacklist" followed by a table. The table has a single header row labeled "MAC Address" and is currently empty.

MAC Blacklist interface

The following table describes the labels in this screen.

Label	Description
<b>MAC Address</b>	Input MAC Address to add to MAC Blacklist.
<b>Port NO.</b>	Select port of switch.
<b>Add</b>	Add an entry to Blacklist table.
<b>Delete</b>	Delete the entry.
<b>Help</b>	Show help file.

### 5.1.12.4 802.1x

#### 802.1x - Radius Server

802.1x makes the use of the physical access characteristics of IEEE802 LAN infrastructures in order to provide a authenticated and authorized devices attached to a LAN port. Please refer to IEEE 802.1X - Port Based Network Access Control.

### 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

802.1x Radius Server interface

The following table describes the labels in this screen.

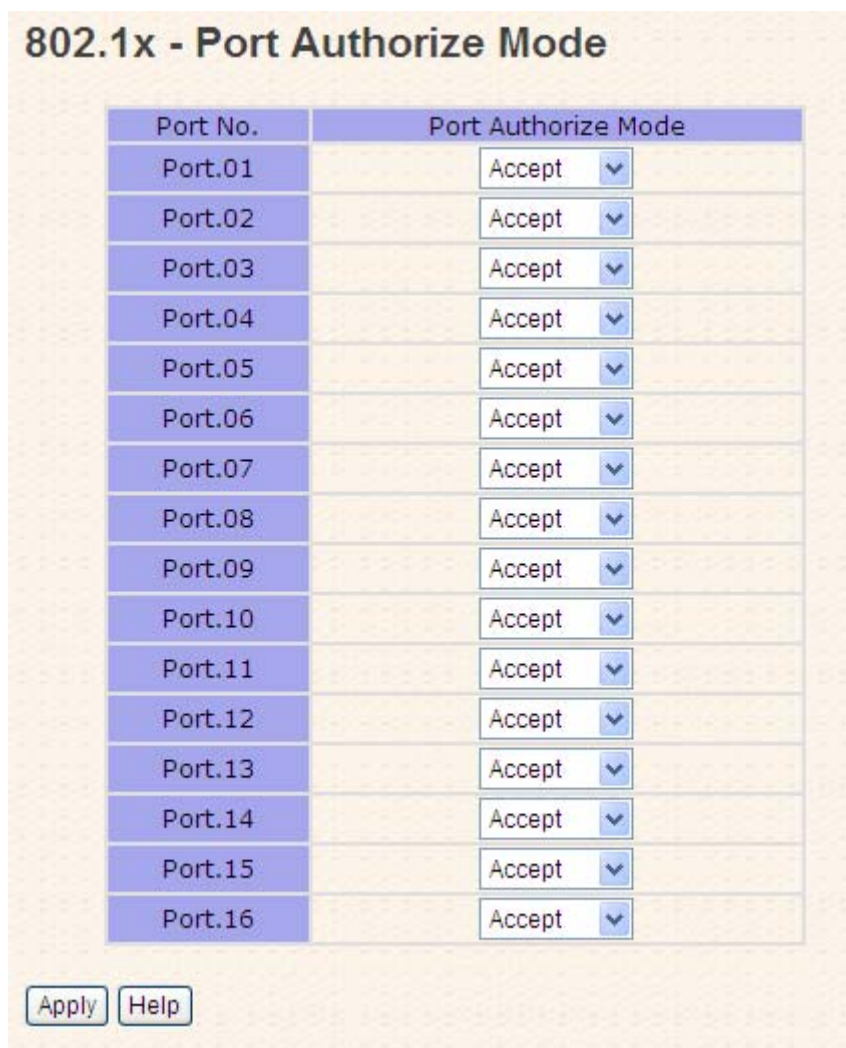
Label	Description
<b>Radius Server Setting</b>	
<b>Radius Server IP</b>	The IP address of the authentication server.
<b>Server port</b>	Set the UDP port number used by the authentication server to authenticate.
<b>Account port</b>	Set the UDP destination port for accounting requests to the specified Radius Server.
<b>Shared Key</b>	A key shared between this switch and authentication server.
<b>NAS, Identifier</b>	A string used to identify this switch.
<b>Advanced Setting</b>	
<b>Quiet Period</b>	Set the time interval between authentication failure and the start of a new authentication attempt.
<b>Tx Period</b>	Set the time that the switch can wait for response to an EAP request/identity frame from the client before resending the request.



<b>Supplicant Timeout</b>	Set the period of time the switch waits for a supplicant response to an EAP request.
<b>Server Timeout</b>	Set the period of time the switch waits for a Radius server response to an authentication request.
<b>Max Requests</b>	Set the maximum number of times to retry sending packets to the supplicant.
<b>Re-Auth Period</b>	Set the period of time after which clients connected must be re-authenticated.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.
<b>Help</b>	Show help file.

### 802.1x-Port Authorized Mode

Set the 802.1x authorized mode of each port.



Port No.	Port Authorize Mode
Port.01	Accept
Port.02	Accept
Port.03	Accept
Port.04	Accept
Port.05	Accept
Port.06	Accept
Port.07	Accept
Port.08	Accept
Port.09	Accept
Port.10	Accept
Port.11	Accept
Port.12	Accept
Port.13	Accept
Port.14	Accept
Port.15	Accept
Port.16	Accept

Apply Help

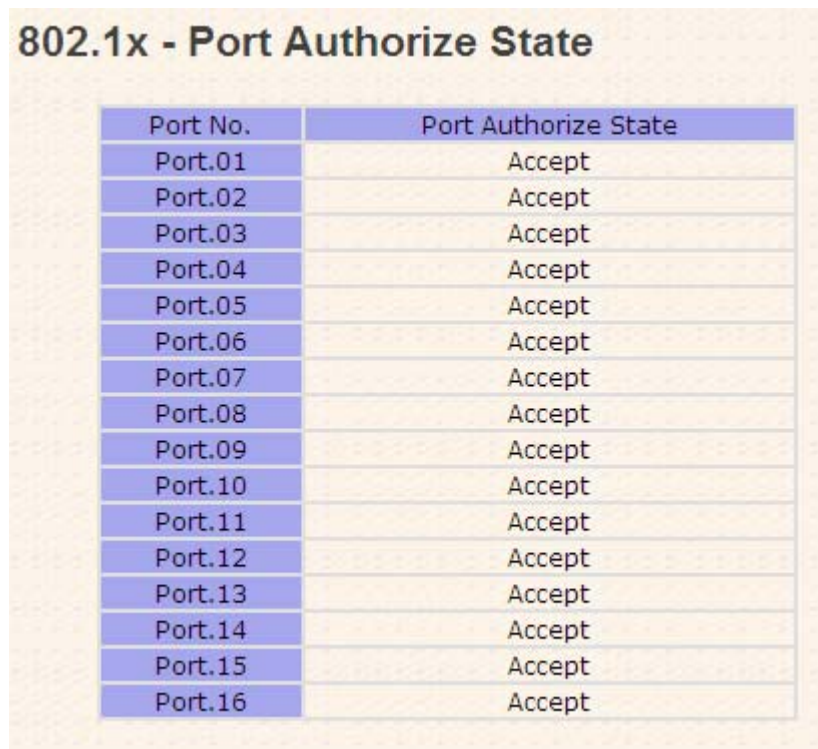
802.1x Port Authorize interface

The following table describes the labels in this screen.

Label	Description
<b>Port Authorized Mode</b>	<ul style="list-style-type: none"> <li>■ <b>Reject:</b> force this port to be unauthorized.</li> <li>■ <b>Accept:</b> force this port to be authorized.</li> <li>■ <b>Authorize:</b> the state of this port was determined by the outcome of the 802.1x authentication.</li> <li>■ <b>Disable:</b> this port will not participate in 802.1x.</li> </ul>
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.
<b>Help</b>	Show help file.

### 802.1x-Port Authorized State

Show 802.1x port authorized state.



**802.1x - Port Authorize State**

Port No.	Port Authorize State
Port.01	Accept
Port.02	Accept
Port.03	Accept
Port.04	Accept
Port.05	Accept
Port.06	Accept
Port.07	Accept
Port.08	Accept
Port.09	Accept
Port.10	Accept
Port.11	Accept
Port.12	Accept
Port.13	Accept
Port.14	Accept
Port.15	Accept
Port.16	Accept

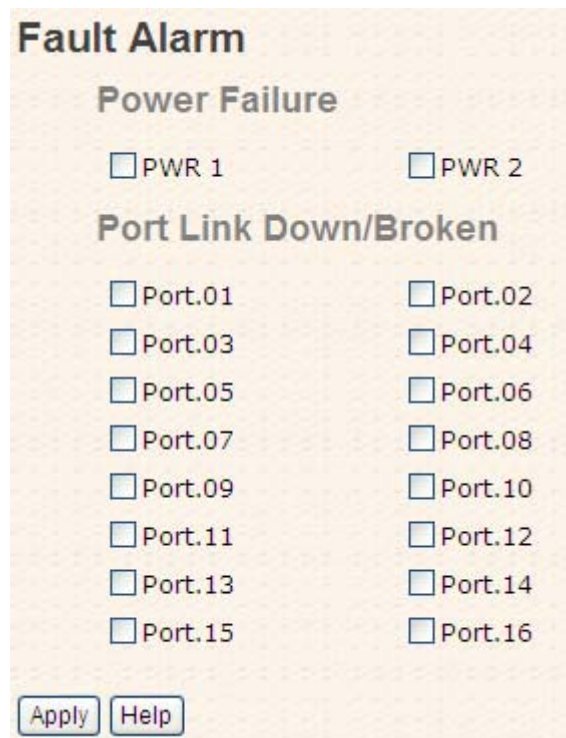
802.1x Port Authorize State interface

### 5.1.13 Warning

Warning function is very important for managing switch. You can manage switch by SYSLOG, E-MAIL, and Fault Relay. It helps you to monitor the switch status on remote site. When events occurred, the warning message will send to your appointed server, E-MAIL, or relay fault to switch panel.

#### 5.1.13.1 Fault Alarm

When any selected fault event is happened, the Fault LED in switch panel will light up and the electric relay will signal at the same time.



Fault Alarm interface

The following table describes the labels in this screen.

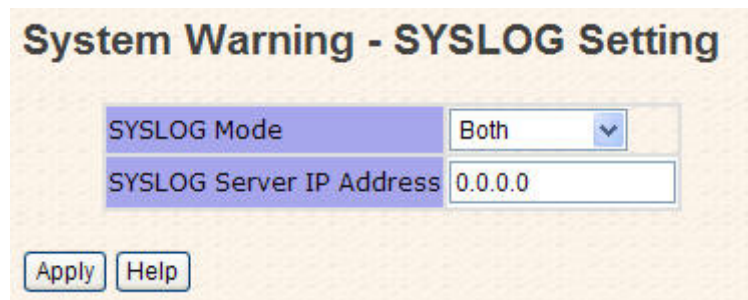
Label	Description
<b>Power Failure</b>	Mark the blank of PWR 1 or PWR 2 to monitor.
<b>Port Link Down/Broken</b>	Mark the blank of port 1 to port 16 to monitor.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.
<b>Help</b>	Show help file.

### 5.1.13.2 System Alarm

System alarm support two warning mode: 1. SYSLOG. 2. E-MAIL. You can monitor switch through selected system events.

#### System Warning – SYSLOG Setting

The SYSLOG is a protocol to transmit event notification messages across networks. Please refer to RFC 3164 - The BSD SYSLOG Protocol



System Warning – SYSLOG Setting interface

The following table describes the labels in this screen.

Label	Description
<b>SYSLOG Mode</b>	<ul style="list-style-type: none"> <li>■ <b>Disable:</b> disable SYSLOG.</li> <li>■ <b>Client Only:</b> log to local system.</li> <li>■ <b>Server Only:</b> log to a remote SYSLOG server.</li> <li>■ <b>Both:</b> log to both of local and remote server.</li> </ul>
<b>SYSLOG Server IP Address</b>	The remote SYSLOG Server IP address.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.
<b>Help</b>	Show help file.

#### System Warning – SMTP Setting

The SMTP is Short for Simple Mail Transfer Protocol. It is a protocol for e-mail transmission across the Internet. Please refer to RFC 821 - Simple Mail Transfer Protocol.

### System Warning - SMTP Setting

E-mail Alert :  ▾

#### SMTP Configuration

SMTP Server IP Address	<input type="text"/>
Sender E-mail Address	<input type="text"/>
Mail Subject	<input type="text"/>
<input type="checkbox"/> Authentication	
Recipient E-mail Address 1	<input type="text"/>
Recipient E-mail Address 2	<input type="text"/>
Recipient E-mail Address 3	<input type="text"/>
Recipient E-mail Address 4	<input type="text"/>
Recipient E-mail Address 5	<input type="text"/>
Recipient E-mail Address 6	<input type="text"/>

System Warning – SMTP Setting interface

The following table describes the labels in this screen.

Label	Description
<b>E-mail Alarm</b>	Enable/Disable transmission system warning events by e-mail.
<b>Sender E-mail Address</b>	The SMTP server IP address
<b>Mail Subject</b>	The Subject of the mail
<b>Authentication</b>	<ul style="list-style-type: none"> <li>■ <b>Username:</b> the authentication username.</li> <li>■ <b>Password:</b> the authentication password.</li> <li>■ <b>Confirm Password:</b> re-enter password.</li> </ul>
<b>Recipient E-mail Address</b>	The recipient's E-mail address. It supports 6 recipients for a mail.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.
<b>Help</b>	Show help file.

### System Warning – Event Selection

SYSLOG and SMTP are the two warning methods that supported by the system. Check the corresponding box to enable system event warning method you wish to choose. Please note that the checkbox can not be checked when SYSLOG or SMTP is disabled.

## System Warning - Event Selection

### System Event

Event	SYSLOG	SMTP
System Cold Start	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Power Status	<input type="checkbox"/>	<input type="checkbox"/>
SNMP Authentication Failure	<input checked="" type="checkbox"/>	<input type="checkbox"/>
O-Ring Topology Change	<input type="checkbox"/>	<input checked="" 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"/>
Port.07	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.08	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.09	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.10	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.11	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.12	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.13	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.14	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.15	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.16	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>

System Warning – Event Selection interface



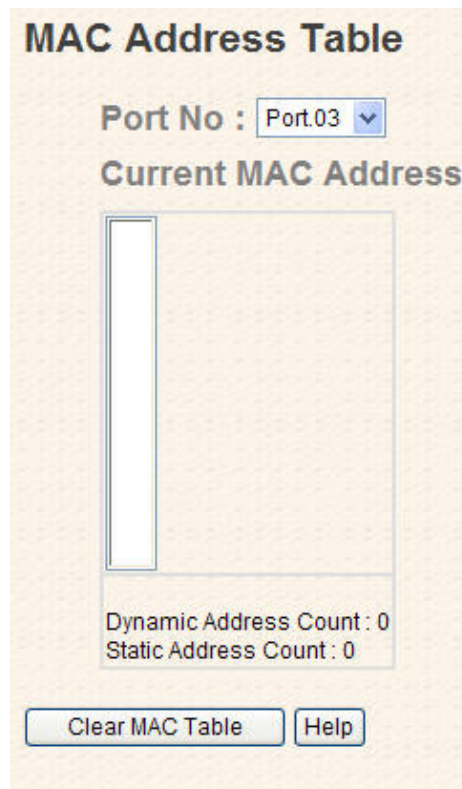
The following table describes the labels in this screen.

Label	Description
<b>System Event</b>	
<b>System Cold Start</b>	Alert when system restart
<b>Power Status</b>	Alert when a power up or down
<b>SNMP Authentication Failure</b>	Alert when SNMP authentication failure.
<b>O-Ring Topology Change</b>	Alert when O-Ring topology changes.
<b>Port Event SYSLOG / SMTP event</b>	<ul style="list-style-type: none"><li>■ <b>Disable</b></li><li>■ <b>Link Up</b></li><li>■ <b>Link Down</b></li><li>■ <b>Link Up &amp; Link Down</b></li></ul>
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.
<b>Help</b>	Show help file.

## 5.1.14 Monitor and Diag

### 5.1.14.1 MAC Address Table

Refer to IEEE 802.1 D Sections 7.9. The MAC Address Table, that is Filtering Database, supports queries by the Forwarding Process, as to whether a frame received by a given port with a given destination MAC address is to be forwarded through a given potential transmission port.



The image shows the 'MAC Address Table' configuration interface. At the top, it is titled 'MAC Address Table'. Below the title, there is a 'Port No.' dropdown menu currently set to 'Port.03'. Underneath is the label 'Current MAC Address' followed by a large, empty rectangular box intended for displaying MAC addresses. At the bottom of this box, it shows 'Dynamic Address Count : 0' and 'Static Address Count : 0'. Below the box are two buttons: 'Clear MAC Table' and 'Help'.

MAC Address Table interface

The following table describes the labels in this screen.

Label	Description
<b>Port NO. :</b>	Show all MAC addresses mapping to a selected port in table.
<b>Clear MAC Table</b>	Clear all MAC addresses in table
<b>Help</b>	Show help file.

#### 5.1.14.2 MAC Address Aging

You can set MAC Address aging timer, as time expired, the unused MAC will be cleared from MAC table. IES-3160 also support Auto Flush MAC Address Table When ports Link Down.



The image shows the 'MAC Address Aging' configuration interface. It is titled 'MAC Address Aging'. Below the title, there is a label 'MAC Address Table Aging Time: (0~3825)' followed by a text input field containing '300' and the unit 'secs'. Below this is a checkbox labeled 'Auto Flush MAC Address Table When Ports Link Down', which is currently unchecked. At the bottom are two buttons: 'Apply' and 'Help'.

MAC Address Aging interface





The following table describes the labels in this screen.

Label	Description
<b>MAC Address Table Aging Time</b>	Set the aging time for MAC table. The value is between 0 and 3825. Default setting is 300 secs.
<b>Auto Flush MAC Address Table When ports Link Down</b>	Enable this function,
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.
<b>Help</b>	Show help file.

### 5.1.14.3 Port Statistics

Port statistics show several statistics counters for all 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	Up	Enable	6528	0	10239	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0
Port.07	100TX	Down	Enable	0	0	0	0	0	0
Port.08	100TX	Down	Enable	0	0	0	0	0	0
Port.09	100TX	Down	Enable	0	0	0	0	0	0
Port.10	100TX	Down	Enable	0	0	0	0	0	0
Port.11	100TX	Down	Enable	0	0	0	0	0	0
Port.12	100TX	Down	Enable	0	0	0	0	0	0
Port.13	100TX	Down	Enable	0	0	0	0	0	0
Port.14	100TX	Down	Enable	0	0	0	0	0	0
Port.15	100TX	Down	Enable	0	0	0	0	0	0
Port.16	100TX	Down	Enable	0	0	0	0	0	0

Clear Help

Port Statistics interface

The following table describes the labels in this screen.

Label	Description
<b>Type</b>	Show port speed and media type.
<b>Link</b>	Show port link status.
<b>State</b>	Show ports enable or disable.



<b>TX GOOD Packet</b>	The number of good packets sent by this port.
<b>TX Bad Packet</b>	The number of bad packets sent by this port.
<b>RX GOOD Packet</b>	The number of good packets received by this port.
<b>RX Bad Packet</b>	The number of bad packets received by this port.
<b>TX Abort Packet</b>	The number of packets aborted by this port.
<b>Packet Collision</b>	The number of times a collision detected by this port.
<b>Clear</b>	Clear all counters.
<b>Help</b>	Show help file.

#### **5.1.14.4 Port Monitoring**

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

### Port Monitoring

Port	Destination Port		Source Port	
	RX	TX	RX	TX
Port.01	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.02	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.03	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.04	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.05	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.06	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.07	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.08	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.09	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.10	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.11	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.12	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.13	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.14	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.15	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.16	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>

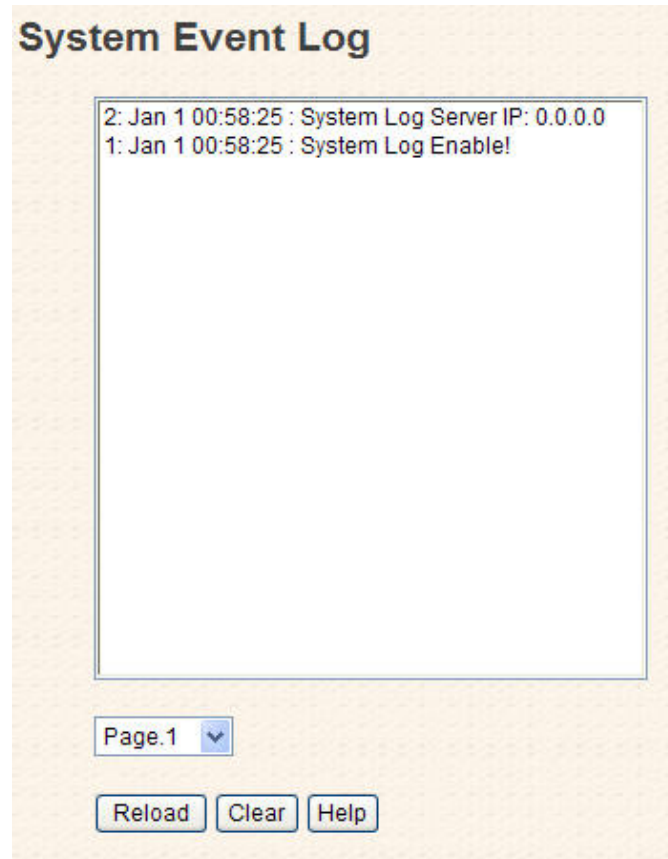
Port monitoring interface

The following table describes the labels in this screen.

Label	Description
<b>Destination Port</b>	The port will receive a copied frame from source port for monitoring purpose.
<b>Source Port</b>	The port will be monitored. Mark the blank of TX or RX to be monitored.
<b>TX</b>	The frames come into switch port.
<b>RX</b>	The frames receive by switch port.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.
<b>Clear</b>	Clear all marked blank.(disable the function)
<b>Help</b>	Show help file.

### 5.1.14.5 System Event Log

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



System event log interface

The following table describes the labels in this screen.

Label	Description
<b>Page</b>	Select LOG page.
<b>Reload</b>	To get the newest event logs and refresh this page.
<b>Clear</b>	Clear log.
<b>Help</b>	Show help file.

### 5.1.14.6 Ping

Ping function allows the switch to send ICMP packets to detect the remote notes.



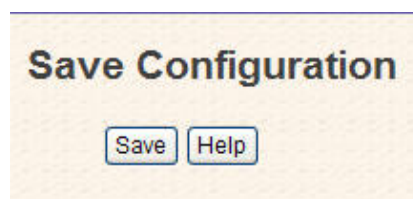
Ping interface

The following table describes the labels in this screen.

Label	Description
<b>IP Address</b>	Enter the IP address that you want to detect.
<b>Active</b>	Click "Active" to send ICMP packets

### 5.1.15 Save Configuration

If any configuration changed, "**Save Configuration**" should be clicked to save current configuration data to the permanent flash memory. Otherwise, the current configuration will be lost when power off or system reset.

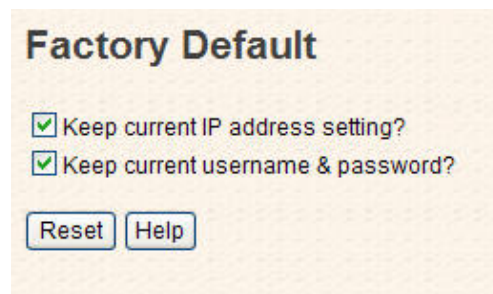


System Configuration interface

The following table describes the labels in this screen.

Label	Description
<b>Save</b>	Save all configurations.
<b>Help</b>	Show help file.

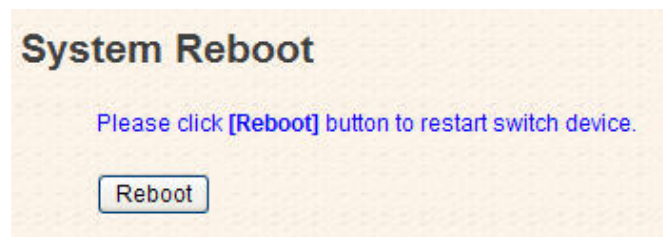
### 5.1.16 Factory Default



Factory Default interface

Reset switch to default configuration. Click **Reset** to reset all configurations to the default value. You can select “**Keep current IP address setting**” and “**Keep current username & password**” to keep current IP and username and password.

### 5.1.17 System Reboot



System Reboot interface

# Command Line Interface Management

## 6.1 About CLI Management

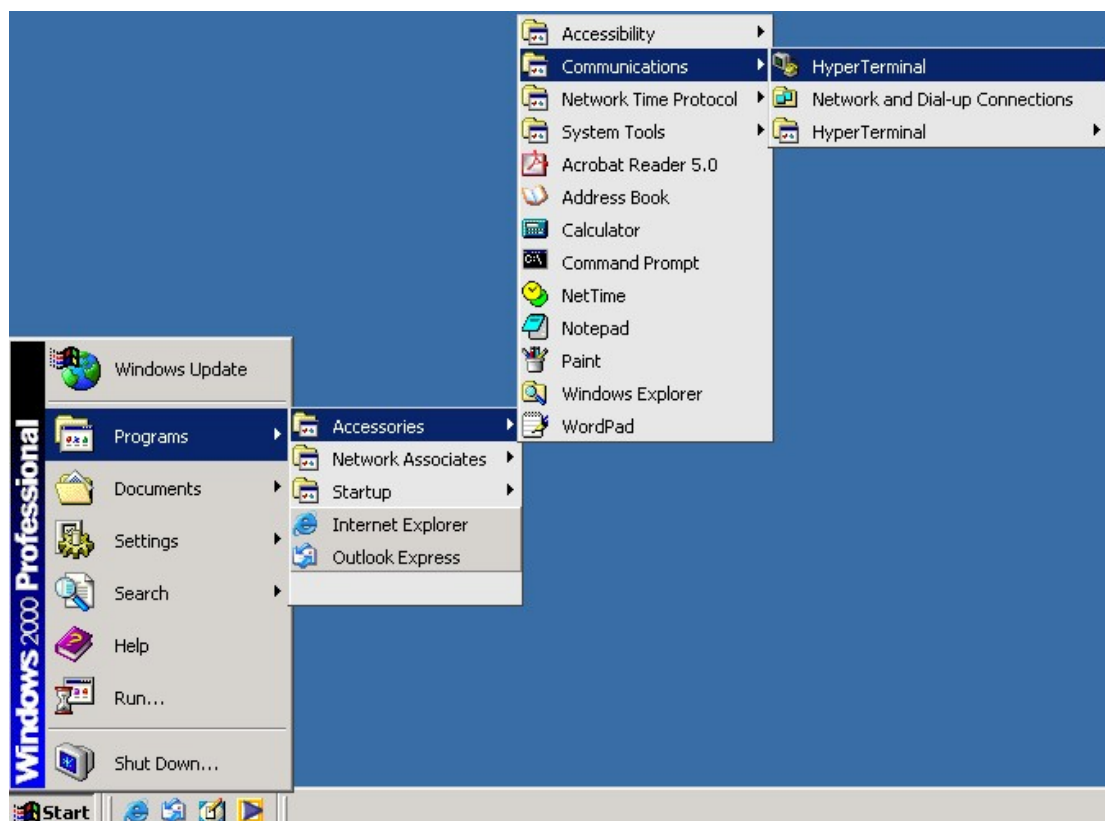
Besides WEB-base management, IES-3160 also support CLI management. You can use console or telnet to management switch by CLI.

### CLI Management by RS-232 Serial Console (9600, 8, none, 1, none)

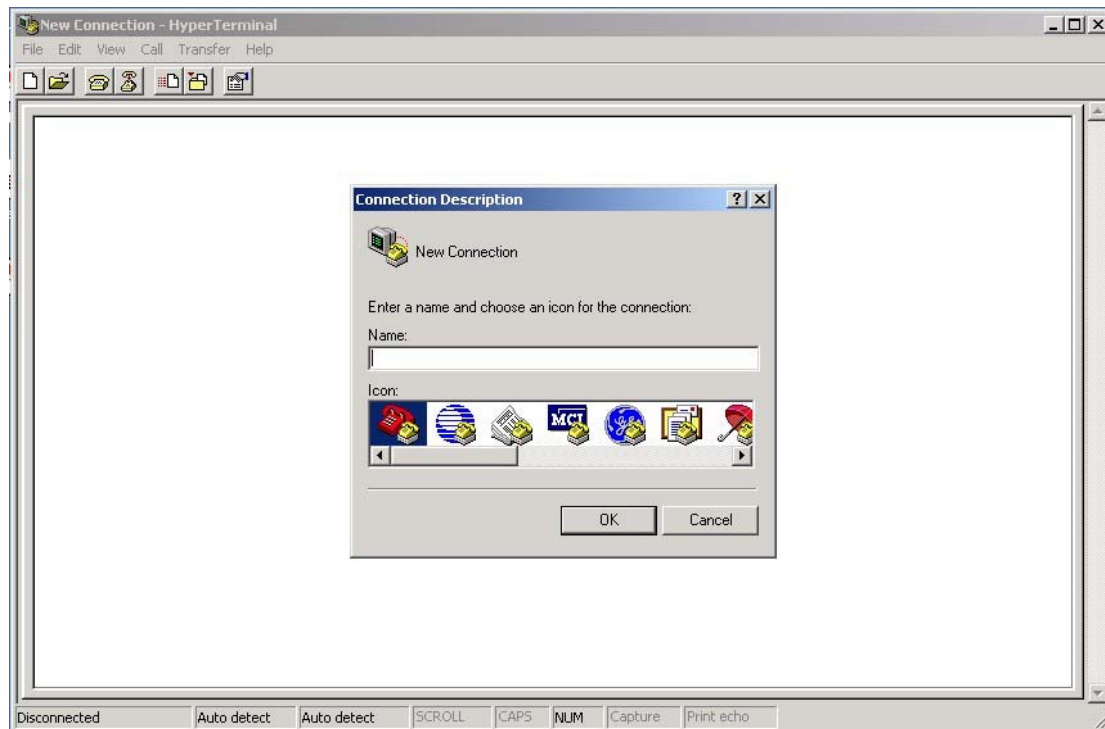
Before Configuring by RS-232 serial console, use an RJ45 to DB9-F cable to connect the Switches' RS-232 Console port to your PC's COM port.

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

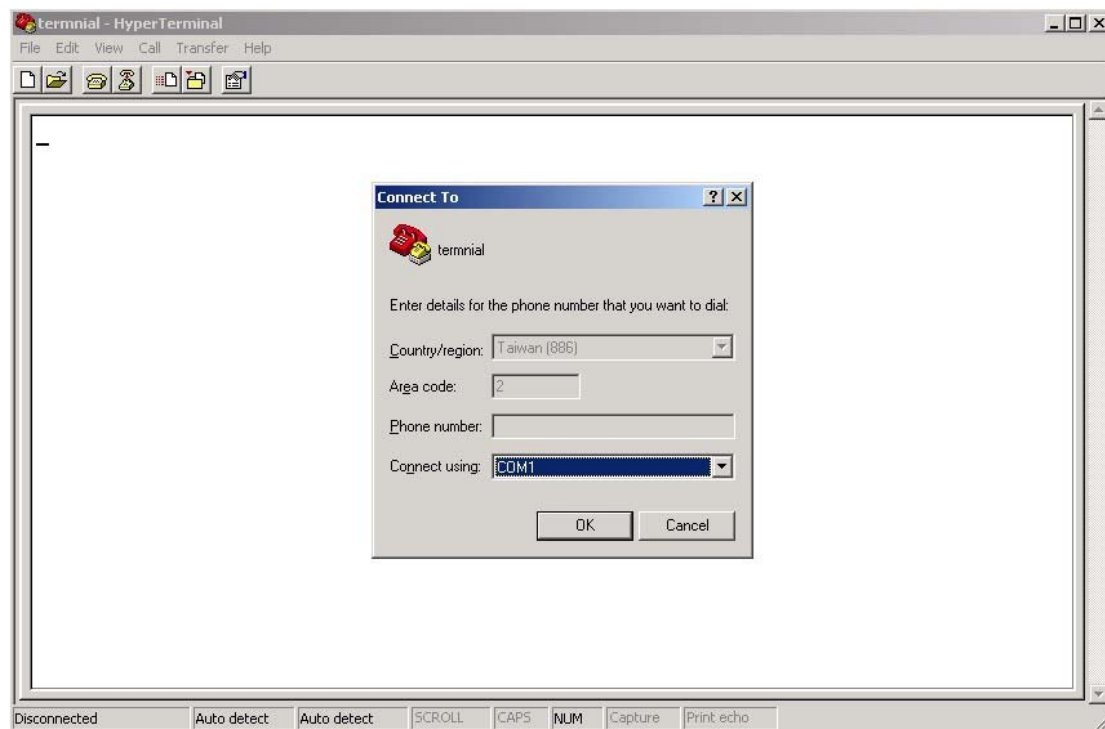
Step 1. From the Windows desktop, click on Start -> Programs -> Accessories -> Communications -> Hyper Terminal



### Step 2. Input a name for new connection

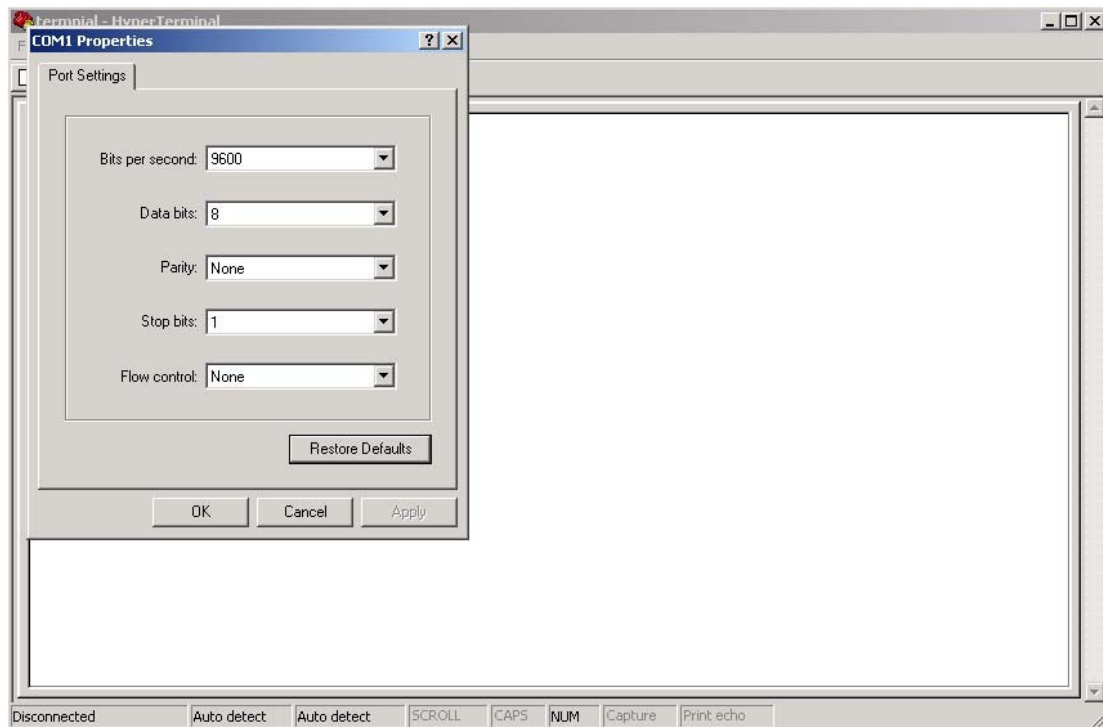


### Step 3. Select to use COM port number

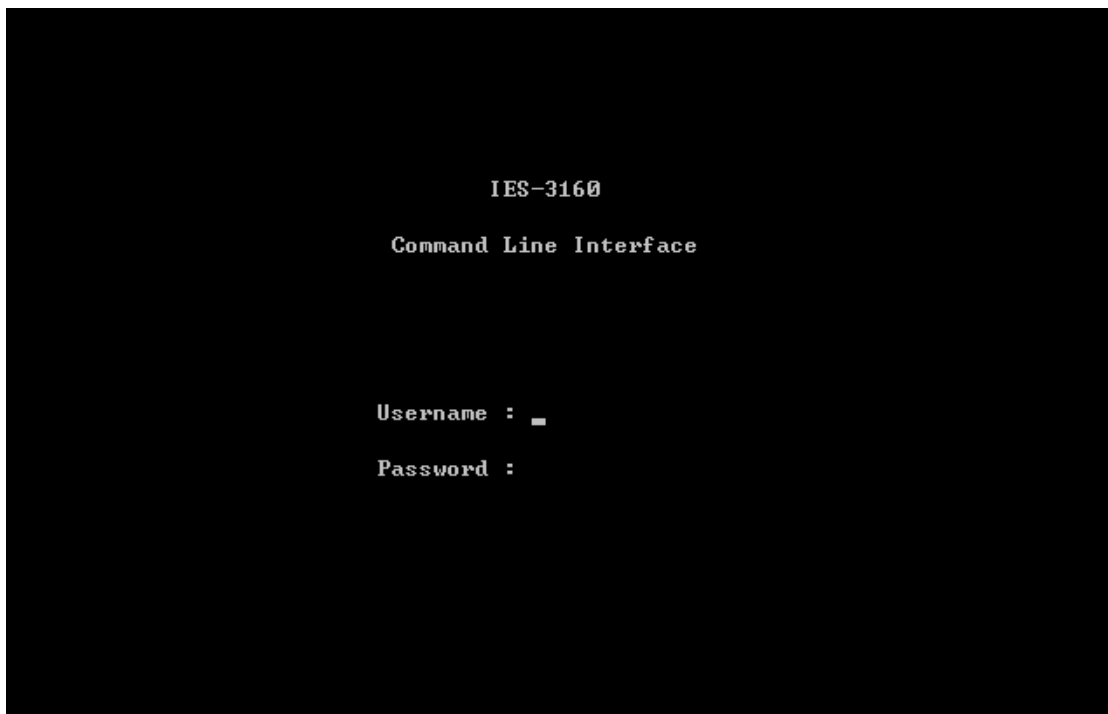




Step 4. The COM port properties setting, 9600 for Bits per second, 8 for Data bits, None for Parity, 1 for Stop bits and none for Flow control.



Step 5. The Console login screen will appear. Use the keyboard to enter the Username and Password (The same with the password for Web Browser), then press "Enter".



### CLI Management by Telnet

Users can use “TELNET” to configure the switches.

The default value is as below:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

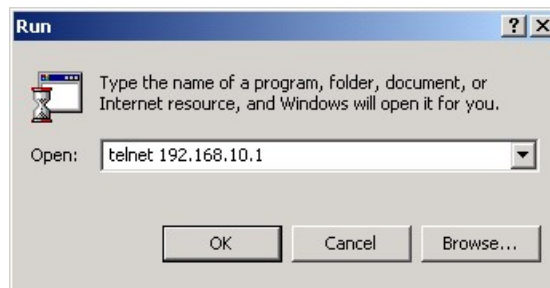
Default Gateway: **192.168.10.254**

User Name: **admin**

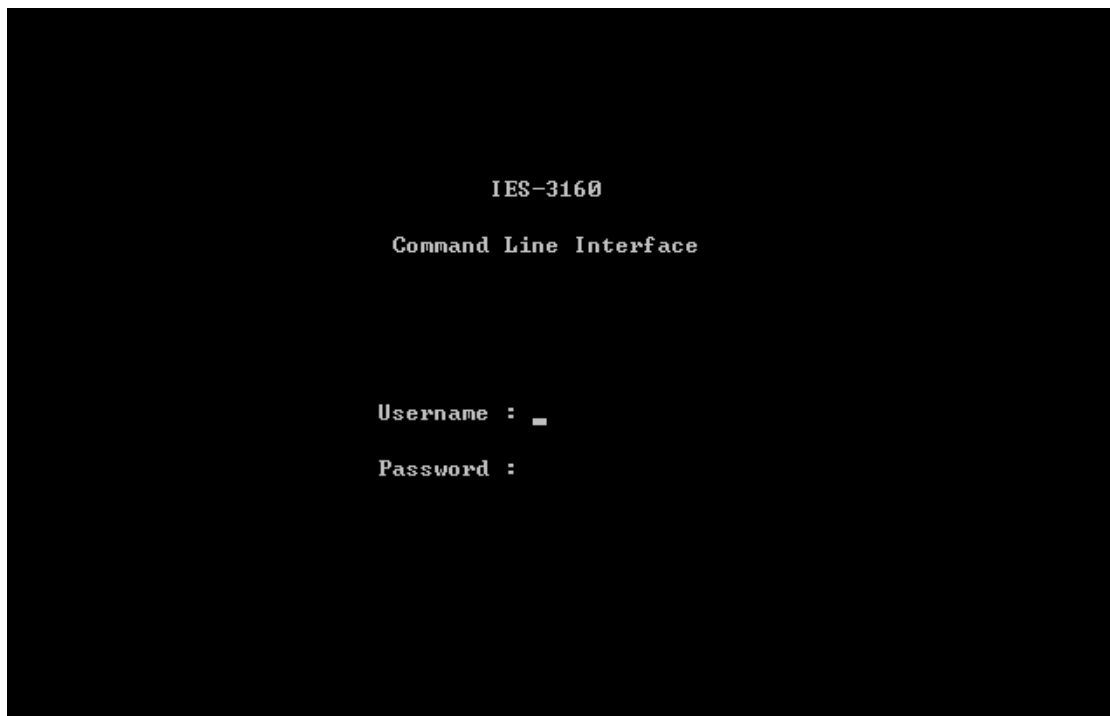
Password: **admin**

Follow the steps below to access the console via Telnet.

Step 1. Telnet to the IP address of the switch from the Windows “Run” command (or from the MS-DOS prompt) as below.



Step 2. The Login screen will appear. Use the keyboard to enter the Username and Password (The same with the password for Web Browser ), and then press “Enter”





**Commands Level**

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

**6.2 Commands Set List—System Commands Set**

IES-3160 Commands	Level	Description	Example
<b>show config</b>	E	Show switch configuration	switch>show config
<b>show terminal</b>	P	Show console information	switch#show terminal
<b>write memory</b>	P	Save your configuration into permanent memory (flash rom)	switch#write memory
<b>system name</b> [System Name]	G	Configure system name	switch(config)#system name xxx
<b>system location</b> [System Location]	G	Set switch system location string	switch(config)#system location xxx
<b>system description</b> [System Description]	G	Set switch system description string	switch(config)#system description xxx
<b>system contact</b> [System Contact]	G	Set switch system contact window string	switch(config)#system contact xxx
<b>show system-info</b>	E	Show system information	switch>show system-info
<b>ip address</b> [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
<b>ip dhcp</b>	G	Enable DHCP client function of switch	switch(config)#ip dhcp



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



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

### 6.3 Commands Set List—Port Commands Set

IES-3160 Commands	Level	Description	Example
<b>interface fastEthernet [Portid]</b>	<b>G</b>	Choose the port for modification.	switch(config)#interface fastEthernet 2
<b>duplex [full   half]</b>	<b>I</b>	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
<b>speed [10 100 1000 auto]</b>	<b>I</b>	Use the speed configuration command to specify the speed mode of operation for Fast	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100



		Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	
<b>flowcontrol mode</b> [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
<b>no flowcontrol</b>	I	Disable flow control of interface	switch(config-if)#no flowcontrol
<b>security enable</b>	I	Enable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#security enable
<b>no security</b>	I	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
<b>bandwidth type all</b>	I	Set interface ingress limit frame type to "accept all frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
<b>bandwidth type broadcast-multicast-flooded-unicast</b>	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
<b>bandwidth type broadcast-multicast</b>	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
<b>bandwidth type broadcast-only</b>	I	Set interface ingress limit frame type to "only accept broadcast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only
<b>bandwidth in</b> [Value]	I	Set interface input bandwidth. Rate Range is from 100	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth in 100



		<p>kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.</p>	
<p><b>bandwidth out</b> [Value]</p>	I	<p>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.</p>	<p>switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth out 100</p>
<p><b>show bandwidth</b></p>	I	<p>Show interfaces bandwidth control</p>	<p>switch(config)#interface fastEthernet 2 switch(config-if)#show bandwidth</p>
<p><b>state</b> [Enable   Disable]</p>	I	<p>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.</p>	<p>switch(config)#interface fastEthernet 2 switch(config-if)#state Disable</p>
<p><b>show interface configuration</b></p>	I	<p>show interface configuration status</p>	<p>switch(config)#interface fastEthernet 2 switch(config-if)#show interface configuration</p>
<p><b>show interface status</b></p>	I	<p>show interface actual status</p>	<p>switch(config)#interface fastEthernet 2 switch(config-if)#show interface status</p>
<p><b>show interface accounting</b></p>	I	<p>show interface statistic counter</p>	<p>switch(config)#interface fastEthernet 2 switch(config-if)#show interface</p>





			accounting
<b>no accounting</b>	<b>I</b>	Clear interface accounting information	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting

### 6.4 Commands Set List—Trunk command set

IES-3160 Commands	Level	Description	Example
<b>aggregator priority</b> [1to65535]	<b>G</b>	Set port group system priority	switch(config)#aggregator priority 22
<b>aggregator activityport</b> [Port Numbers]	<b>G</b>	Set activity port	switch(config)#aggregator activityport 2
<b>aggregator group</b> [GroupID] [Port-list] <b>lacp</b> <b>workp</b> [Workport]	<b>G</b>	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
<b>aggregator group</b> [GroupID] [Port-list] <b>nolacp</b>	<b>G</b>	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



<b>show aggregator</b>	<b>P</b>	Show the information of trunk group	switch#show aggregator
<b>no aggregator lacp</b> [GroupID]	<b>G</b>	Disable the LACP function of trunk group	switch(config)#no aggregator lacp 1
<b>no aggregator group</b> [GroupID]	<b>G</b>	Remove a trunk group	switch(config)#no aggregator group 2

## 6.5 Commands Set List—VLAN command set

IES-3160 Commands	Level	Description	Example
<b>vlan database</b>	<b>P</b>	Enter VLAN configure mode	switch#vlan database
<b>vlan</b> [8021q   gvrp]	<b>V</b>	To set switch VLAN mode.	switch(vlan)# vlanmode 802.1q or switch(vlan)# vlanmode gvrp
<b>no vlan</b> [VID]	<b>V</b>	Disable vlan group(by VID)	switch(vlan)#no vlan 2
<b>no gvrp</b>	<b>V</b>	Disable GVRP	switch(vlan)#no gvrp
<b>IEEE 802.1Q VLAN</b>			
<b>vlan 8021q port</b> [PortNumber] <b>access-link untag</b> [UntaggedVID]	<b>V</b>	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
<b>vlan 8021q port</b> [PortNumber] <b>trunk-link tag</b> [TaggedVID List]	<b>V</b>	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
<b>vlan 8021q port</b> [PortNumber] <b>hybrid-link untag</b> [UntaggedVID] <b>tag</b> [TaggedVID List]	<b>V</b>	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
<b>vlan 8021q aggregator</b> [TrunkID]	<b>V</b>	Assign a access link for VLAN by trunk	switch(vlan)#vlan 8021q aggregator 3 access-link untag 33



<b>access-link untag</b> [UntaggedVID]		group	
<b>vlan 8021q aggregator</b> [TrunkID] <b>trunk-link tag</b> [TaggedVID List]	<b>V</b>	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
<b>vlan 8021q aggregator</b> [PortNumber] <b>hybrid-link untag</b> [UntaggedVID] <b>tag</b> [TaggedVID List]	<b>V</b>	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
<b>show vlan</b> [VID] or <b>show vlan</b>	<b>V</b>	Show VLAN information	switch(vlan)#show vlan 23

## 6.6 Commands Set List—Spanning Tree command set

IES-3160 Commands	Level	Description	Example
<b>spanning-tree enable</b>	<b>G</b>	Enable spanning tree	switch(config)#spanning-tree enable
<b>spanning-tree priority</b> [0to61440]	<b>G</b>	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
<b>spanning-tree max-age</b> [seconds]	<b>G</b>	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	switch(config)# spanning-tree max-age 15



		from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	
<b>spanning-tree hello-time</b> [seconds]	<b>G</b>	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
<b>spanning-tree forward-time</b> [seconds]	<b>G</b>	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
<b>stp-path-cost</b> [1to200000000]	<b>I</b>	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,	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20



		spanning tree considers the path cost when selecting an interface to place into the forwarding state.	
<b>stp-path-priority</b> [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
<b>stp-admin-p2p</b> [Auto True False]	I	Admin P2P of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-p2p Auto
<b>stp-admin-edge</b> [True False]	I	Admin Edge of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-edge True
<b>stp-admin-non-stp</b> [True False]	I	Admin NonSTP of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-non-stp False
<b>Show spanning-tree</b>	E	Display a summary of the spanning-tree states.	switch>show spanning-tree
<b>no spanning-tree</b>	G	Disable spanning-tree.	switch(config)#no spanning-tree

## 6.7 Commands Set List—QoS command set

IES-3160 Commands	Level	Description	Example
<b>qos policy</b>	G	Select QOS policy	switch(config)#qos policy



[weighted-fair strict]		scheduling	weighted-fair
<b>qos prioritytype</b> [port-based cos-only tos-only cos-first tos-first]	<b>G</b>	Setting of QOS priority type	switch(config)#qos prioritytype
<b>qos priority portbased</b> [Port] [lowest low middle high]	<b>G</b>	Configure Port-based Priority	switch(config)#qos priority portbased 1 low
<b>qos priority cos</b> [Priority][lowest low middle high]	<b>G</b>	Configure COS Priority	switch(config)#qos priority cos 22 middle
<b>qos priority tos</b> [Priority][lowest low middle high]	<b>G</b>	Configure TOS Priority	switch(config)#qos priority tos 3 high
<b>show qos</b>	<b>P</b>	Display the information of QoS configuration	switch>show qos
<b>no qos</b>	<b>G</b>	Disable QoS function	switch(config)#no qos

### 6.8 Commands Set List—IGMP command set

IES-3160 Commands	Level	Description	Example
<b>igmp enable</b>	<b>G</b>	Enable IGMP snooping function	switch(config)#igmp enable
<b>igmp-query auto</b>	<b>G</b>	Set IGMP query to auto mode	switch(config)#igmp-query auto
<b>igmp-query force</b>	<b>G</b>	Set IGMP query to force mode	switch(config)#igmp-query force
<b>show igmp configuration</b>	<b>P</b>	Displays the details of an IGMP configuration.	switch#show igmp configuration
<b>show igmp multi</b>	<b>P</b>	Displays the details of an IGMP snooping entries.	switch#show igmp multi
<b>no igmp</b>	<b>G</b>	Disable IGMP snooping function	switch(config)#no igmp
<b>no igmp-query</b>	<b>G</b>	Disable IGMP query	switch#no igmp-query



## 6.9 Commands Set List—MAC/Filter Table command set

IES-3160 Commands	Level	Description	Example
<b>mac-address-table static hwaddr</b> [MAC]	I	Configure MAC address table of interface (static).	switch(config)#interface fastEthernet 2 switch(config-if)#mac-address-table static hwaddr 000012345678
<b>mac-address-table filter hwaddr</b> [MAC]	G	Configure MAC address table(filter)	switch(config)#mac-address-table filter hwaddr 000012348678
<b>show mac-address-table</b>	P	Show all MAC address table	switch#show mac-address-table
<b>show mac-address-table static</b>	P	Show static MAC address table	switch#show mac-address-table static
<b>show mac-address-table filter</b>	P	Show filter MAC address table.	switch#show mac-address-table filter
<b>no mac-address-table static hwaddr</b> [MAC]	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
<b>no mac-address-table filter hwaddr</b> [MAC]	G	Remove an entry of MAC address table (filter)	switch(config)#no mac-address-table filter hwaddr 000012348678
<b>no mac-address-table</b>	G	Remove dynamic entry of MAC address table	switch(config)#no mac-address-table

## 6.10 Commands Set List—SNMP command set

IES-3160 Commands	Level	Description	Example
<b>snmp agent-mode</b> [v1v2c   v3]	G	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2c
<b>snmp-server host</b> [IP address]	G	Configure SNMP server host	switch(config)#snmp-server host 192.168.10.50 community public



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

### 6.11 Commands Set List—Port Mirroring command set

IES-3160 Commands	Level	Description	Example
<b>monitor rx</b>	<b>G</b>	Set RX destination port of monitor	switch(config)#monitor rx





		function	
<b>monitor tx</b>	<b>G</b>	Set TX destination port of monitor function	switch(config)#monitor tx
<b>show monitor</b>	<b>P</b>	Show port monitor information	switch#show monitor
<b>monitor</b> [RX TX Both]	<b>I</b>	Configure source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#monitor RX
<b>show monitor</b>	<b>I</b>	Show port monitor information	switch(config)#interface fastEthernet 2 switch(config-if)#show monitor
<b>no monitor</b>	<b>I</b>	Disable source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#no monitor

### 6.12 Commands Set List—802.1x command set

IES-3160 Commands	Level	Description	Example
<b>8021x enable</b>	<b>G</b>	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
<b>8021x system radiusip</b> [IP address]	<b>G</b>	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
<b>8021x system serverport</b> [port ID]	<b>G</b>	Use the 802.1x system server port global configuration command to change the radius server port	switch(config)# 8021x system serverport 1815
<b>8021x system accountport</b> [port ID]	<b>G</b>	Use the 802.1x system account port global configuration command to change	switch(config)# 8021x system accountport 1816



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



		MAX requests.	
<b>8021x misc reauthperiod</b> [sec.]	<b>G</b>	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# 8021x misc reauthperiod 3000
<b>8021x portstate</b> [disable   reject   accept   authorize]	<b>I</b>	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
<b>show 8021x</b>	<b>E</b>	Display a summary of the 802.1x properties and also the port sates.	switch>show 8021x
<b>no 8021x</b>	<b>G</b>	Disable 802.1x function	switch(config)#no 8021x

### 6.13 Commands Set List—TFTP command set

IES-3160 Commands	Level	Description	Defaults Example
<b>backup flash:backup_cfg</b>	<b>G</b>	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
<b>restore flash:restore_cfg</b>	<b>G</b>	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



<b>upgrade</b> <b>flash:upgrade_fw</b>	<b>G</b>	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#upgrade lash:upgrade_fw
---	----------	--	---

### 6.14 Commands Set List—SYSLOG, SMTP, EVENT command set

IES-3160 Commands	Level	Description	Example
<b>systemlog ip</b> [IP address]	<b>G</b>	Set System log server IP address.	switch(config)# systemlog ip 192.168.1.100
<b>systemlog mode</b> [client server both]	<b>G</b>	Specified the log mode	switch(config)# systemlog mode both
<b>show systemlog</b>	<b>E</b>	Display system log.	Switch>show systemlog
<b>show systemlog</b>	<b>P</b>	Show system log client & server information	switch#show systemlog
<b>no systemlog</b>	<b>G</b>	Disable systemlog function	switch(config)#no systemlog
<b>smtp enable</b>	<b>G</b>	Enable SMTP function	switch(config)#smtp enable
<b>smtp serverip</b> [IP address]	<b>G</b>	Configure SMTP server IP	switch(config)#smtp serverip 192.168.1.5
<b>smtp authentication</b>	<b>G</b>	Enable SMTP authentication	switch(config)#smtp authentication
<b>smtp account</b> [account]	<b>G</b>	Configure authentication account	switch(config)#smtp account User
<b>smtp password</b> [password]	<b>G</b>	Configure authentication password	switch(config)#smtp password
<b>smtp rcptemail</b> [Index] [Email address]	<b>G</b>	Configure Rcpt e-mail Address	switch(config)#smtp rcptemail 1 <a href="mailto:Alert@test.com">Alert@test.com</a>
<b>show smtp</b>	<b>P</b>	Show the information of SMTP	switch#show smtp
<b>no smtp</b>	<b>G</b>	Disable SMTP	switch(config)#no smtp



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

### 6.15 Commands Set List—SNTP command set

IES-3160 Commands	Level	Description	Example
-------------------	-------	-------------	---------



<b>sntp enable</b>	<b>G</b>	Enable SNTP function	switch(config)#sntp enable
<b>sntp daylight</b>	<b>G</b>	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight
<b>sntp daylight-period</b> [Start time] [End time]	<b>G</b>	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
<b>sntp daylight-offset</b> [Minute]	<b>G</b>	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight-offset 3
<b>sntp ip</b> [IP]	<b>G</b>	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp ip 192.169.1.1
<b>sntp timezone</b> [Timezone]	<b>G</b>	Set timezone index, use "show sntp timzezone" command to get more information of index number	switch(config)#sntp timezone 22
<b>show sntp</b>	<b>P</b>	Show SNTP information	switch#show sntp
<b>show sntp timezone</b>	<b>P</b>	Show index number of time zone list	switch#show sntp timezone
<b>no sntp</b>	<b>G</b>	Disable SNTP function	switch(config)#no sntp
<b>no sntp daylight</b>	<b>G</b>	Disable daylight	switch(config)#no sntp daylight



		saving time	
--	--	-------------	--

## 6.16 Commands Set List—O-Ring command set

IES-3160 Commands	Level	Description	Example
<b>Ring enable</b>	<b>G</b>	Enable O-Ring	switch(config)# ring enable
<b>Ring master</b>	<b>G</b>	Enable ring master	switch(config)# ring master
<b>Ring couplering</b>	<b>G</b>	Enable couple ring	switch(config)# ring couplering
<b>Ring dualhoming</b>	<b>G</b>	Enable dual homing	switch(config)# ring dualhoming
<b>Ring ringport</b> [1st Ring Port] [2nd Ring Port]	<b>G</b>	Configure 1st/2nd Ring Port	switch(config)# ring ringport 7 8
<b>Ring couplingport</b> [Coupling Port]	<b>G</b>	Configure Coupling Port	switch(config)# ring couplingport 1
<b>Ring controlport</b> [Control Port]	<b>G</b>	Configure Control Port	switch(config)# ring controlport 2
<b>Ring homingport</b> [Dual Homing Port]	<b>G</b>	Configure Dual Homing Port	switch(config)# ring homingport 3
<b>show Ring</b>	<b>P</b>	Show the information of O-Ring	switch#show ring
<b>no Ring</b>	<b>G</b>	Disable O-Ring	switch(config)#no ring
<b>no Ring master</b>	<b>G</b>	Disable ring master	switch(config)# no ring master
<b>no Ring couplering</b>	<b>G</b>	Disable couple ring	switch(config)# no ring couplering
<b>no Ring dualhoming</b>	<b>G</b>	Disable dual homing	switch(config)# no ring dualhoming



# Technical Specifications

<b>Technology</b>	
Ethernet Standards	802.3 - 10Base-T, 802.3u - 100Base-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
<b>Interface</b>	
RJ45 Ports	10/100Base-T(X), Auto MDI/MDI-X
LED Indicators	Per Unit : Power x 3(Green) RJ45 Ports: Per Port : Link/Activity(Green/Blinking Green), Full duplex(Amber)
<b>Power Requirements</b>	
Power Input Voltage	PWR1/2: 12~8VDC on 6-pin Terminal Block
Reverse Polarity Protection	Present
Power Consumption	7.68 Watts
<b>Environmental</b>	
Operating Temperature	-40 to 70 °C
Storage Temperature	-40 to 85 °C
Operating Humidity	5% to 95%, non-condensing
<b>Mechanical</b>	





Dimensions(W x D x H)	74.3 mm(W)x 109.2 mm(D)x 153.6 mm(H)
Casing	IP-30 protection
<b>Regulatory Approvals</b>	
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
<b>Warranty</b>	5 years