Industrial
Management Ethernet Switch

IES-3240

User's Manual

Version 2.0
Jun, 2012

ORing Industrial Networking Corp.

3F., NO.542-2, Jhongjheng Rd., Sindian
Distric, New Taipei City 231, Taiwan, R.O.C.
Tel: + 886 2 2218 1066
Fax: + 886 2 2218 1014
Website: www.oring-networking.com
E-mail: support@oring-networking.com

Table of Content

Getting to Know Your Switch

1.1 About the IES-3240 Managed Industrial Switch

The IES-3240 is powerful managed industrial switch with many features. The switch can work under wide temperature, dusty environment and humid condition.

The IES-3240 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 : O-Ring (Recovery time < 10ms over 250 units connection)
- Supports Ring Coupling, Dual Homing over O-Ring technology
- Supports SNMPv1/v2c/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)
- Radius centralized password management
- 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

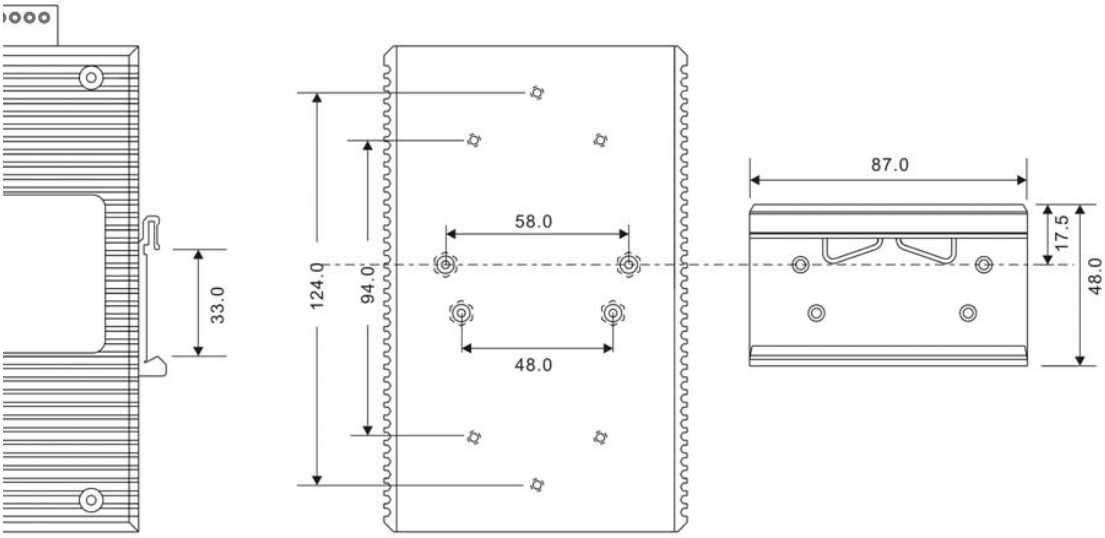
- Redundant two DC power inputs
- Wide Operating Temperature: -40 to 70^{o}C
- Storage Temperature: -40 to 85^{o}C
- Operating Humidity: 5% to 95%, non-condensing
- Casing: IP-30
- 10/100Base-T(X) Ethernet port
- Console Port
- Dimensions(W x D x H) : 96 mm(W)x 109.2 mm(D)x 153.6 mm(H)

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:

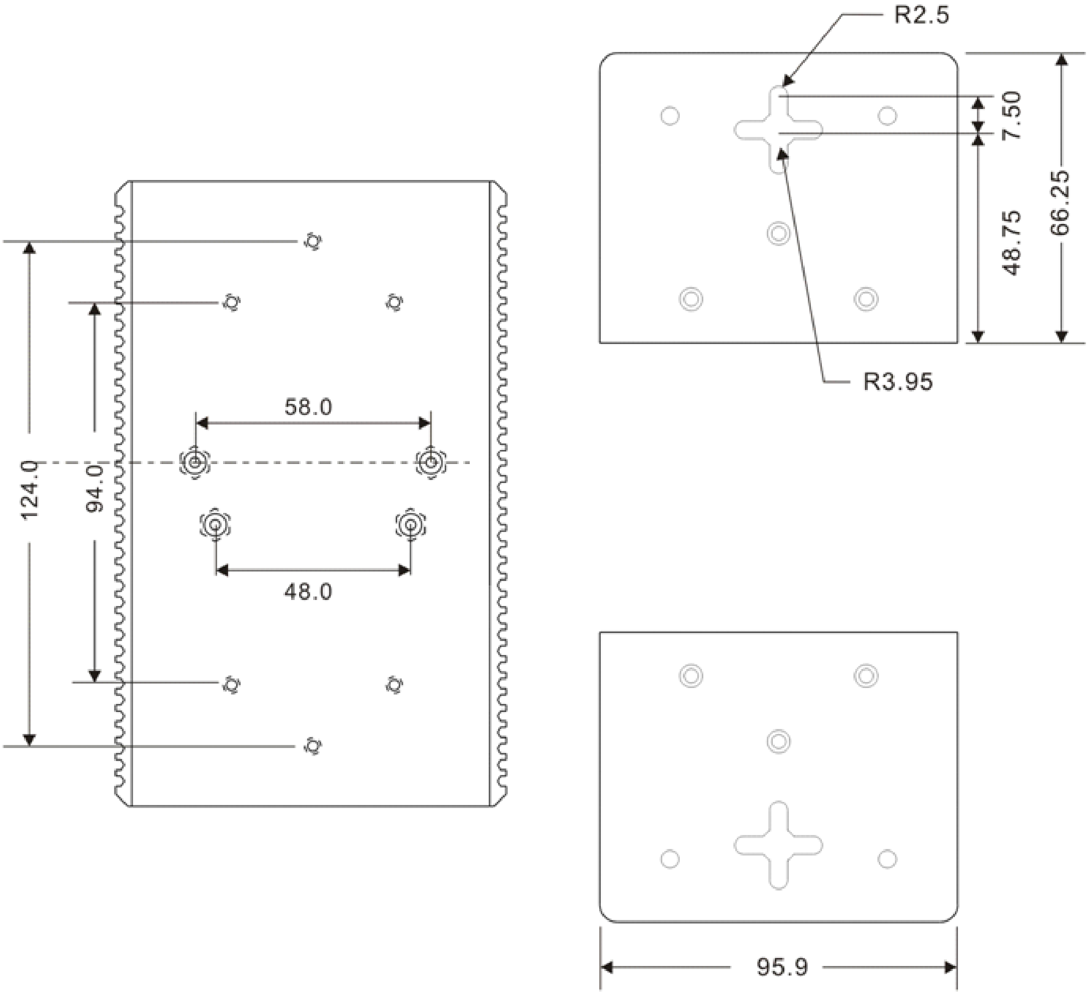
2.1.1 Mount IES-3240 on DIN-Rail



DIN-Rail Size

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:



Wall-Mounting size

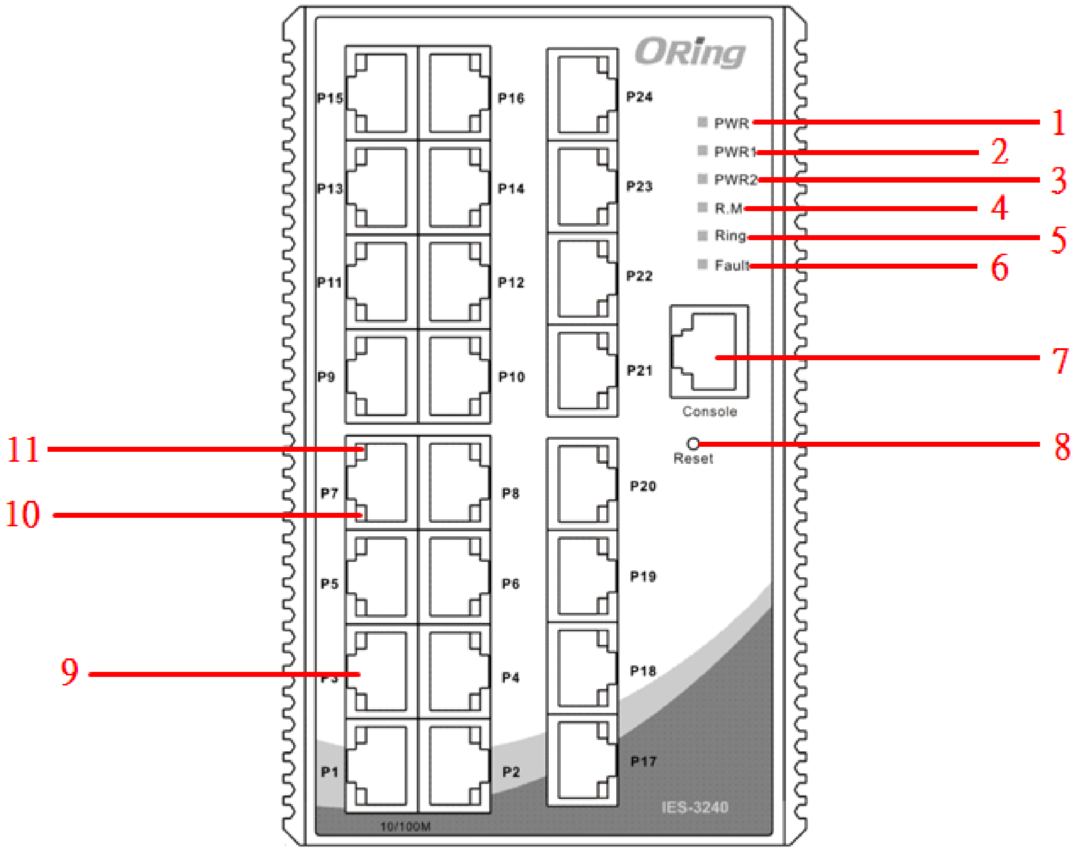
Hardware Overview

3.1 Front Panel

The following table describes the labels that stick on the IES-3240.

Port	Description
10/100 RJ-45 fast Ethernet ports	8 10/100Base-T(X) RJ-45 fast Ethernet ports support auto-negotiation. Default Setting : Speed: auto Duplex: auto Flow control : disable
Console	Use RS-232 to RJ-45 connecter to manage switch.
Reset	Push reset button 2 to 3 seconds to reset the switch. Push reset button 5 seconds to reset the switch into **Factory Default.**

IES-3240



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. Amber LED for Ethernet ports Duplex/Collision status.
11. Green LED for Ethernet ports Act/Link status.

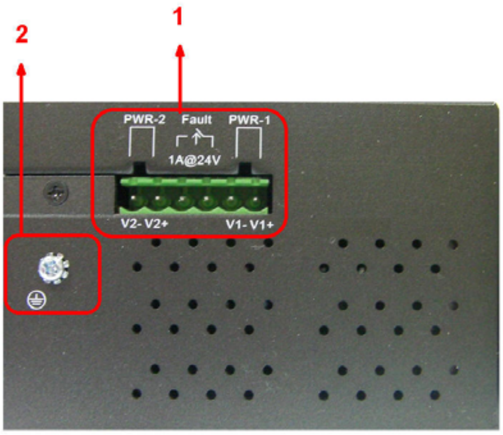
3.2 Front Panel LEDs

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

3.3 Top view Panel

The bottom panel components of IES-3240 are shown as below:

1. Terminal block includes: Dual 12~48VDC power inputs and one 1A@24V relay ouput
2. Ground wire



.

Cables

4.1 Ethernet Cables

The IES-3240 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

4.1.1 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-3240 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.

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

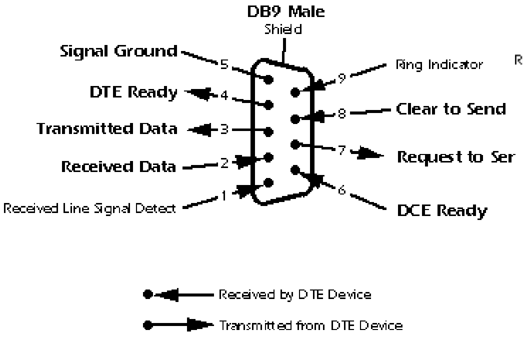
Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

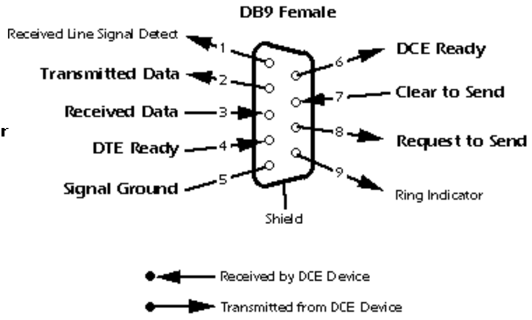
Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.

4.2 Console Cable

IES-3240 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

Warning!!!

While making any establishment and upgrading firmware, please remove physical loop connection first.

DO NOT power off equipment during firmware is upgrading!

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**

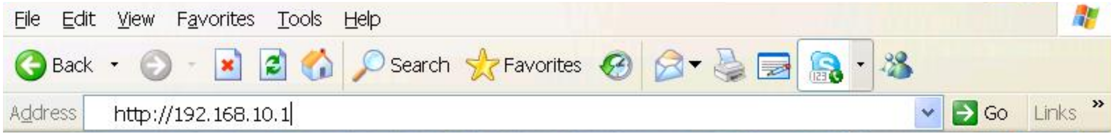
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

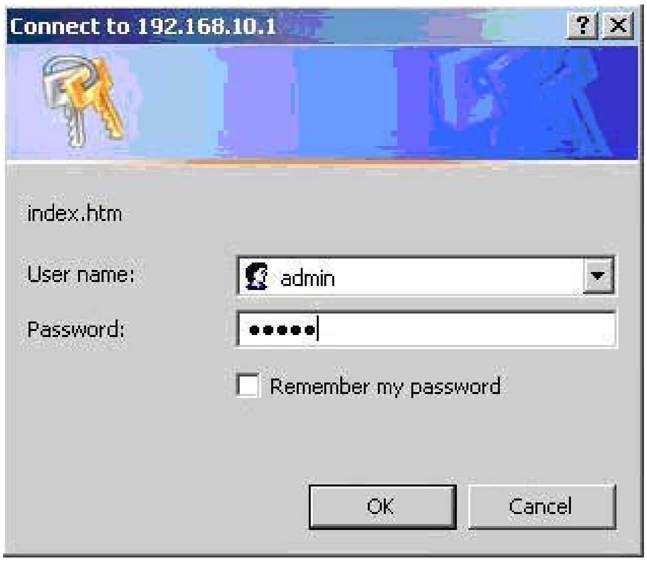
System Login

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



Address: http://192.168.10.1

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.


Connect to 192.168.10.1

index.htm

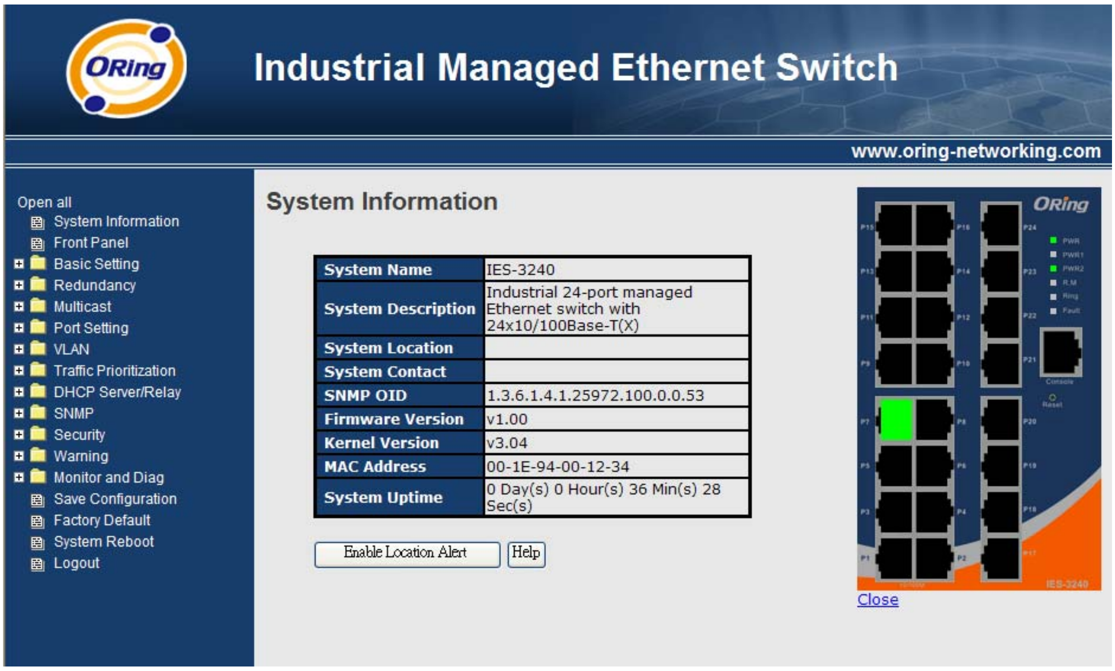
User name: admin

Password: •••••

☐ Remember my password

Login screen

Main Interface

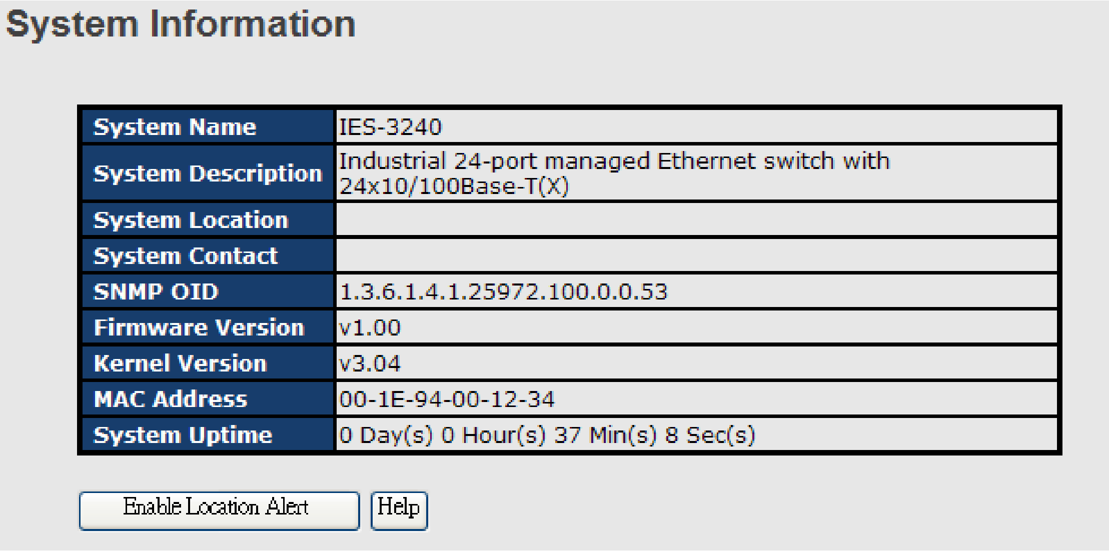


System Information

System Name	IES-3240
System Description	Industrial 24-port managed Ethernet switch with 24x10/100Base-T(X)
System Location	
System Contact	
SNMP OID	1.3.6.1.4.1.25972.100.0.0.53
Firmware Version	v1.00
Kernel Version	v3.04
MAC Address	00-1E-94-00-12-34
System Uptime	0 Day(s) 0 Hour(s) 36 Min(s) 28 Sec(s)

Main interface

5.1.2 System Information



System Information

System Name	IES-3240
System Description	Industrial 24-port managed Ethernet switch with 24x10/100Base-T(X)
System Location	
System Contact	
SNMP OID	1.3.6.1.4.1.25972.100.0.0.53
Firmware Version	v1.00
Kernel Version	v3.04
MAC Address	00-1E-94-00-12-34
System Uptime	0 Day(s) 0 Hour(s) 37 Min(s) 8 Sec(s)

System Information interface

System Information

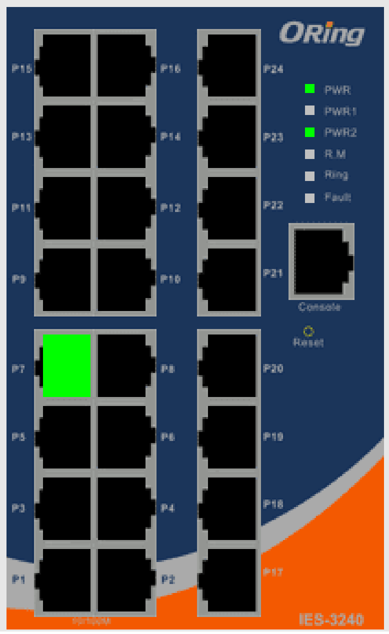
The system information will display the configuration of Basic Setting / Switch Setting page.

Enable Location Alert

When click Enable Location Alert, PWR1, PWR2 and PWR3 LEDs of the switch will start to flash together, and click Disable Location Alert , the LEDs will stop flashing.

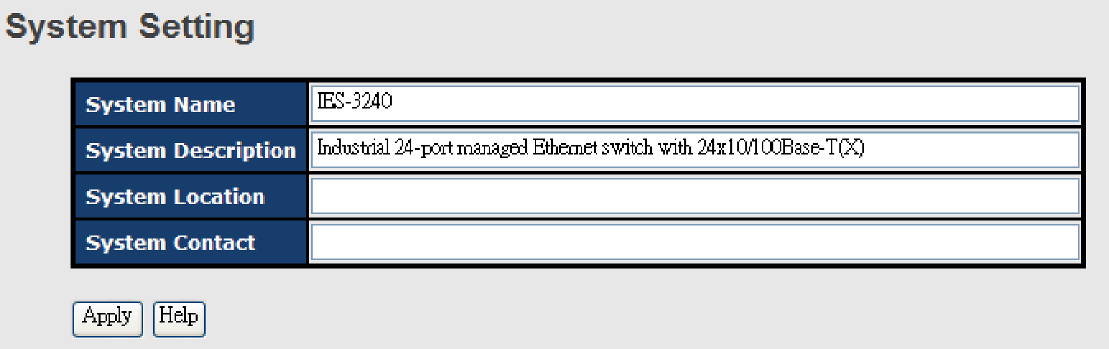
5.1.3 Front Panel

Show the panel of IES-3240. Click "**Close**" to close panel on web.



5.1.4 Basic setting

5.1.4.1 Switch Setting



System Setting

System Name	IES-3240
System Description	Industrial 24-port managed Ethernet switch with 24x10/100Base-T(X)
System Location	
System Contact	

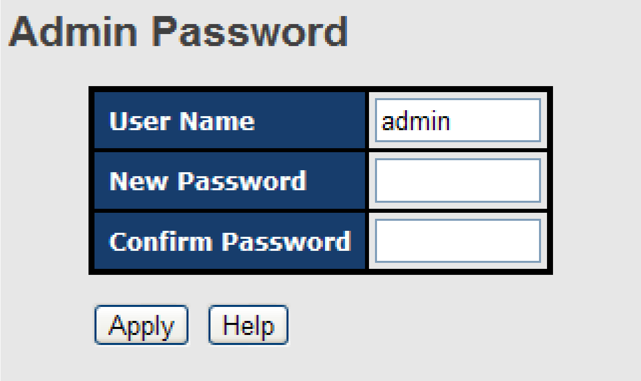
Switch setting interface

The following table describes the labels in this screen.

Label	Description
System Name	Assign the name of switch. The maximum length is 64 bytes
System Description	Display the description of switch.
System Location	Assign the switch physical location. The maximum length is 64 bytes
System Contact	Enter the name of contact person or organization

5.1.4.2 Admin Password

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



Admin Password

User Name	admin
New Password	
Confirm Password	

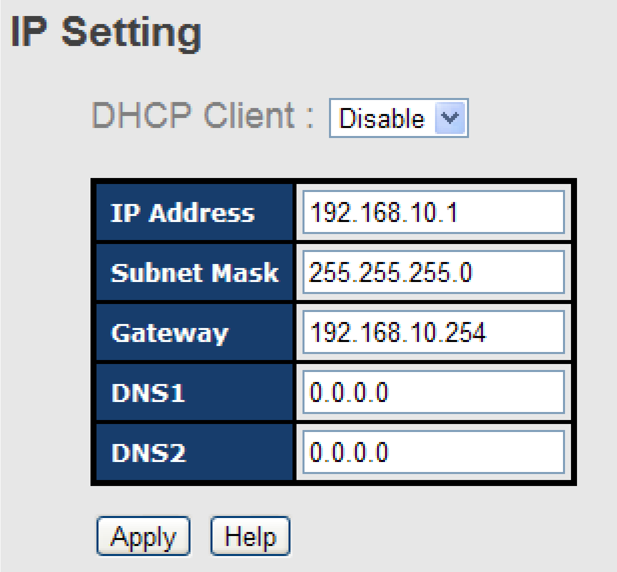
Admin Password interface

The following table describes the labels in this screen.

Label	Description
User name	Key in the new username (The default is "**admin**")
New Password	Key in the new password (The default is "**admin**")
Confirm password	Re-type the new password.
Apply	Click "**Apply**" to activate the configurations.

5.1.4.3 IP Setting

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



IP Setting

DHCP Client : Disable

IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway	192.168.10.254
DNS1	0.0.0.0
DNS2	0.0.0.0

IP Configuration interface

The following table describes the labels in this screen.

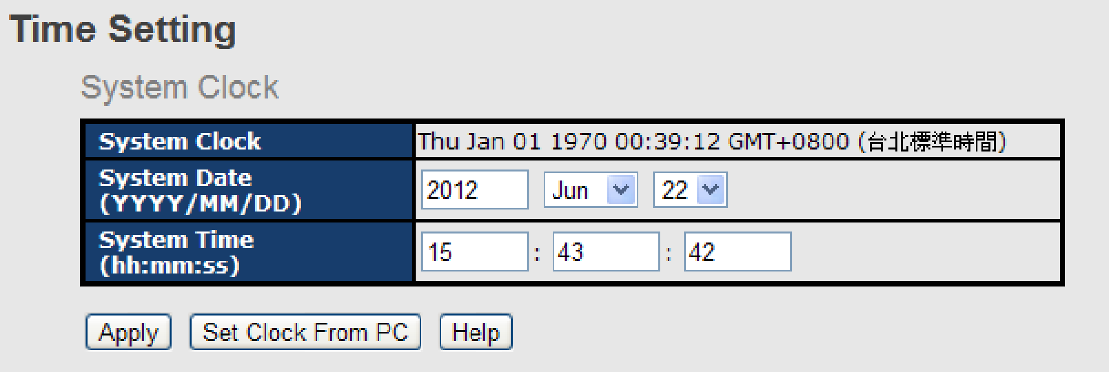
Label	Description
DHCP Client	To enable or disable the DHCP client function. When DHCP client function is enabling, the switch will be assigned the IP address from the network DHCP server. The default IP address will be replaced by the IP address which the DHCP server has assigned. After clicking "**Apply**" 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.
IP Address	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
Subnet Mask	Assign the subnet mask of the IP address. If DHCP client function is enabling, you do not need to assign the subnet mask
Gateway	Assign the network gateway for the switch. The default gateway is 192.168.10.254
DNS1	Assign the primary DNS IP address
DNS2	Assign the secondary DNS IP address
Apply	Click "**Apply**" to activate the configurations.

5.1.4.4 Time Setting

This page includes configurations of SNTP and system clock.

System Clock



Time Setting

System Clock

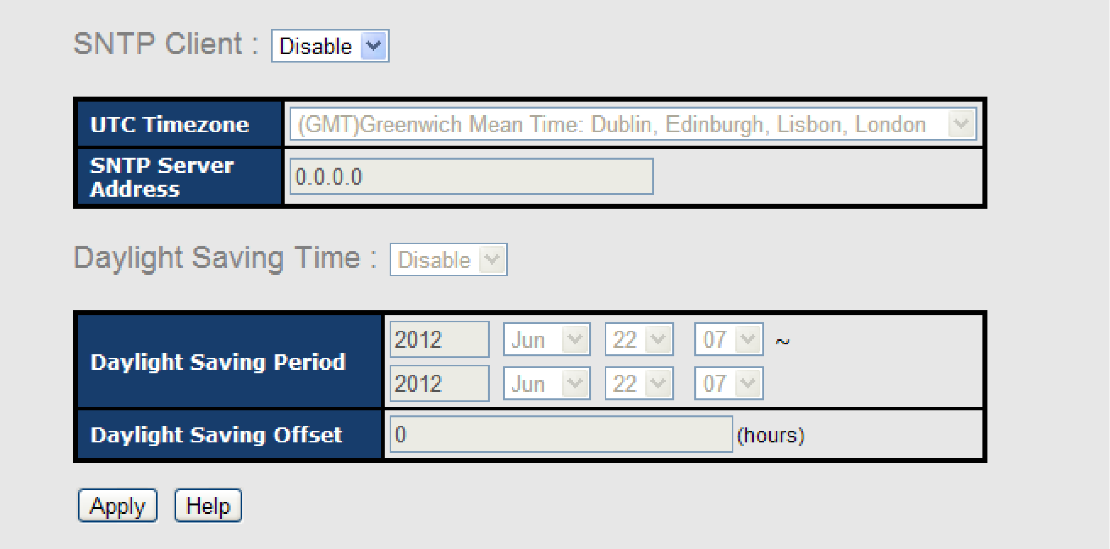
System Clock	Thu Jan 01 1970 00:39:12 GMT+0800 (台北標準時間)
System Date (YYYY/MM/DD)	2012 Jun 22
System Time (hh:mm:ss)	15 : 43 : 42

The following table describes the labels in this screen.

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

SNTP

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



SNTP Client : Disable

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

Daylight Saving Time : Disable

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

SNTP Configuration interface

The following table describes the labels in this screen.

Label	Description
SNTP Client	Enable or disable SNTP function to get the time from the SNTP server.
Daylight Saving Time	Enable or disable daylight saving time function. When daylight saving time is enabling, you need to configure the daylight saving time period.
UTC Time zone	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	-5 hours	7 am

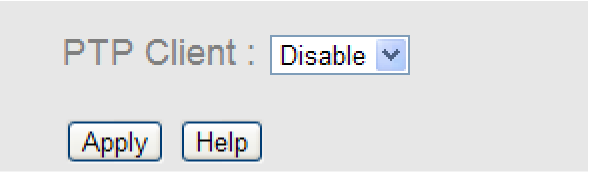
CDT - Central Daylight		
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	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	+10 hours	10 pm

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

Label	Description
SNTP Sever IP Address	Set the SNTP server IP address.
Daylight Saving Period	Set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different each year.
Daylight Saving Offset	Set up the offset time.
Switch Timer	Display the switch current time.
Apply	Click "**Apply**" to activate the configurations.

PTP Client

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

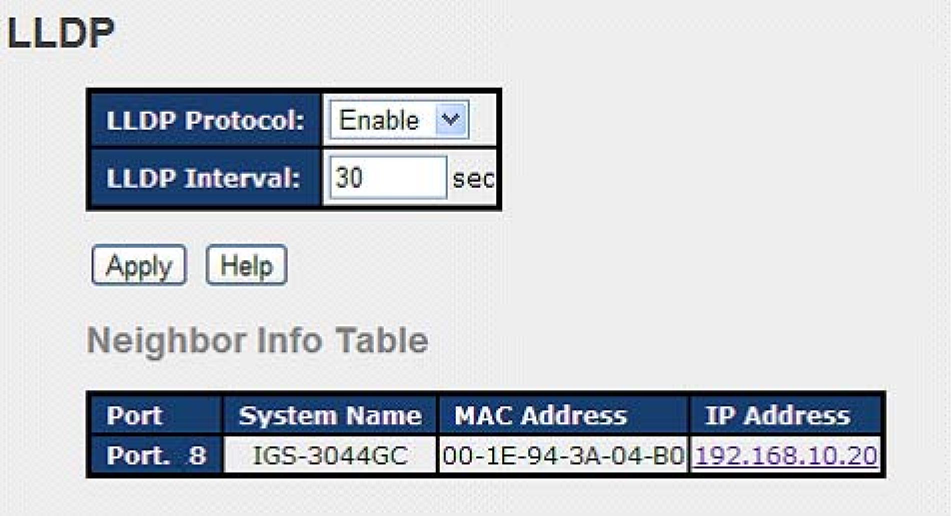


PTP Client : Disable

Label	Description
PTP Client	Enable / Disable PTP Client

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

LLDP Protocol: Enable

LLDP Interval: 30 sec

Neighbor Info Table

Port	System Name	MAC Address	IP Address
Port. 8	IGS-3044GC	00-1E-94-3A-04-B0	192.168.10.20

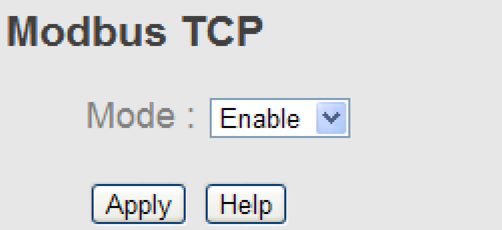
LLDP configuration interface

The following table describes the labels in this screen.

Label	Description
LLDP Protocol	"Enable" or "Disable" LLDP function.
LLDP Interval	The interval of resend LLDP (by default at 30 seconds)
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.
Neighbor info table	Can show neighbor device info .

5.1.4.6 Modbus TCP

Support Modbus TCP .(About Modbus please reference http://www.modbus.org/)



Modbus TCP

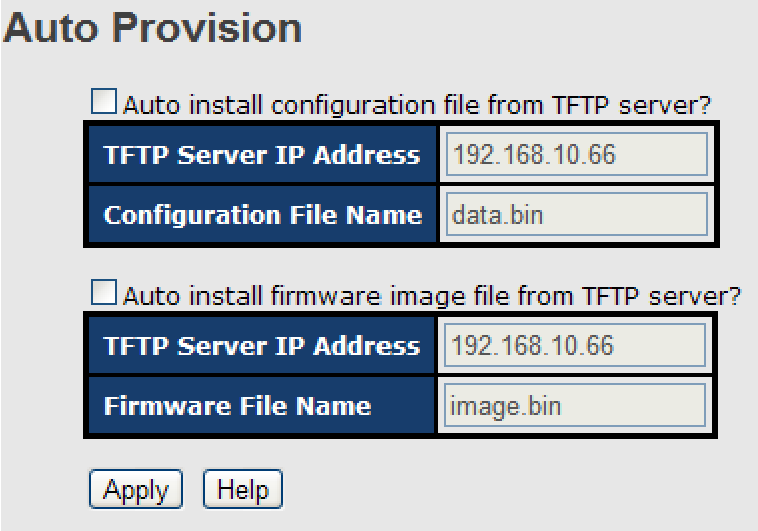
Mode : Enable

The following table describes the labels in this screen.

Label	Description
Mode	Enable or Disalble Modbus TCP function

5.1.4.7 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

□ Auto install configuration file from TFTP server?

TFTP Server IP Address	192.168.10.66
Configuration File Name	data.bin

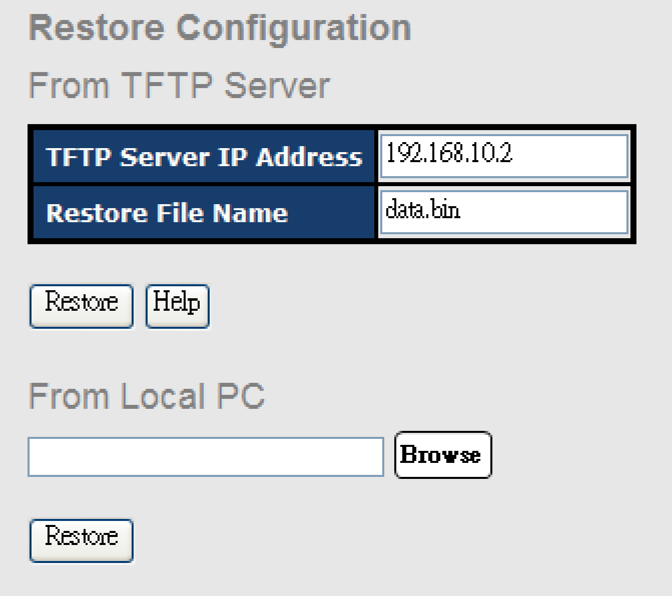
□ Auto install firmware image file from TFTP server?

TFTP Server IP Address	192.168.10.66
Firmware File Name	image.bin

Auto Provision interface

5.1.4.8 Backup & Restore

You can save current EEPROM value from the switch to TFTP server, then go to the TFTP restore configuration page to restore the EEPROM value.

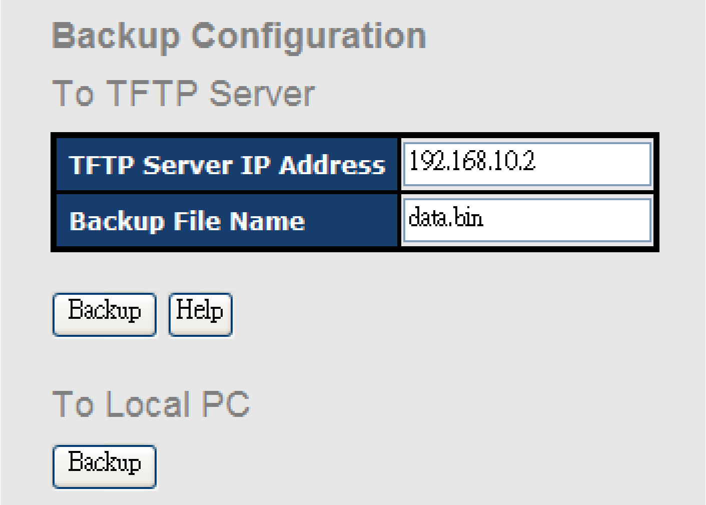


Restore Configuration

From TFTP Server

TFTP Server IP Address	192.168.10.2
Restore File Name	data.bin

From Local PC



Backup Configuration

To TFTP Server

TFTP Server IP Address	192.168.10.2
Backup File Name	data.bin

To Local PC

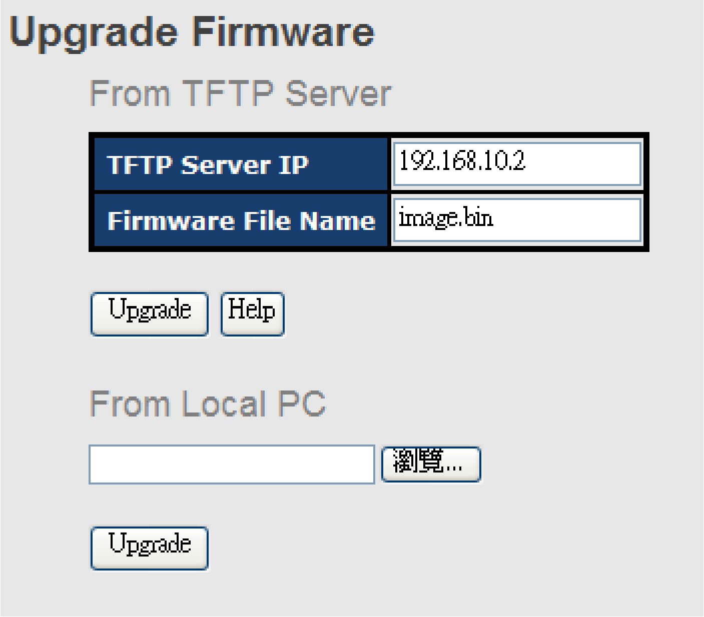
Backup & Restore interface

The following table describes the labels in this screen.

Label	Description
TFTP Server IP Address	Fill in the TFTP server IP
Restore File Name	Fill the file name.
Restore	Click "**restore**" to restore the configurations.
Form Local PC	User can select file restore , not need TFTP server .
Restore File Name	Fill the file name.
Restore	Click "**restore**" to restore the configurations.
Backup	Click "**backup**" to backup the configurations.
To Local PC	User can download config file to switch . not need TFTP server

5.1.4.9 Upgrade Firmware

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



Upgrade Firmware

From TFTP Server

TFTP Server IP	192.168.10.2
Firmware File Name	image.bin

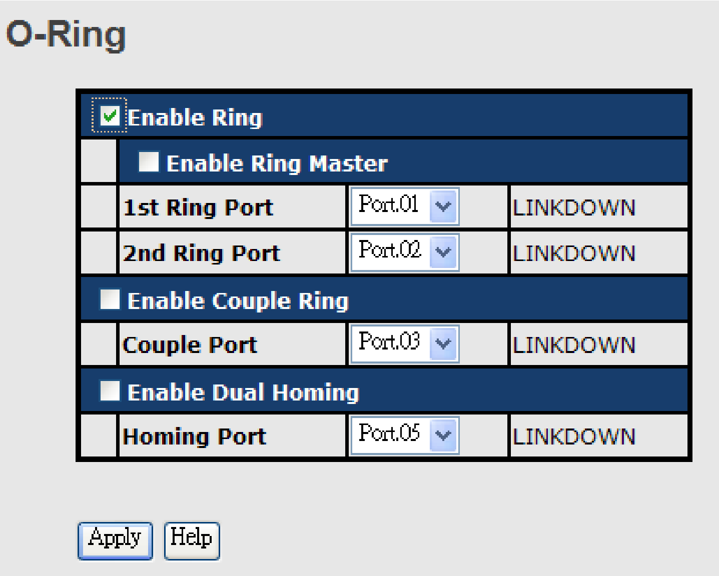
From Local PC

Update Firmware interface

5.1.1 Redundancy

5.1.1.1 O-Ring

O-Ring is the most powerful Ring in the world. The recovery time of O-Ring is less than 10 mS. It can reduce unexpected damage caused by network topology change. O-Ring supports three Ring topologies: O-Ring, Coupling Ring and Dual Homing.



O-Ring

☑ Enable Ring			
	□ Enable Ring Master		
	1st Ring Port	Port.01	LINKDOWN
	2nd Ring Port	Port.02	LINKDOWN
□ Enable Couple Ring			
	Couple Port	Port.03	LINKDOWN
□ Enable Dual Homing			
	Homing Port	Port.05	LINKDOWN

O-Ring interface

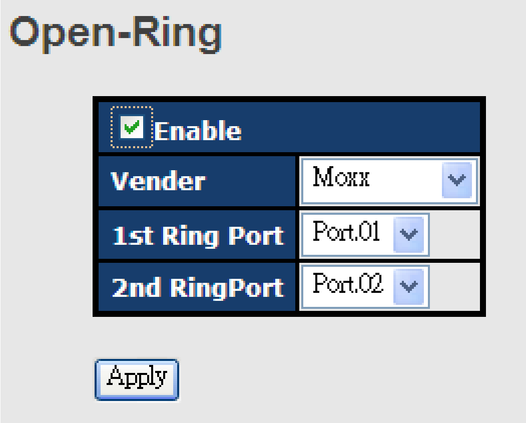
The following table describes the labels in this screen.

Label	Description
Enable Ring	Mark to enable Ring.
Enable Ring Master	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.
1st Ring Port	The primary port, when this switch is Ring Master.
2nd Ring Port	The backup port, when this switch is Ring Master.
Enable Coupling Ring	Mark 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.
Coupling Port	Link to Coupling Port of the switch in another ring. Coupling Ring need four switch to build an active and a backup link. Set a port as coupling port. The coupled four ports of four switches will be run at active/backup mode.
Control Port	Link to Control Port of the switch in the same ring. Control Port used to transmit control signals.
Enable Dual Homing	Mark to enable Dual Homing. By selecting Dual Homing mode, O-Ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work as active/backup mode, and connect each O-Ring to the normal switches in RSTP mode.
Apply	Click "Apply" to set the configurations.

Note: We don't suggest you to set one switch as a Ring Master and a Coupling Ring at the same time due to heavy load.

5.1.1.2 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.



Open-Ring

☑ Enable

Vender: Moxx

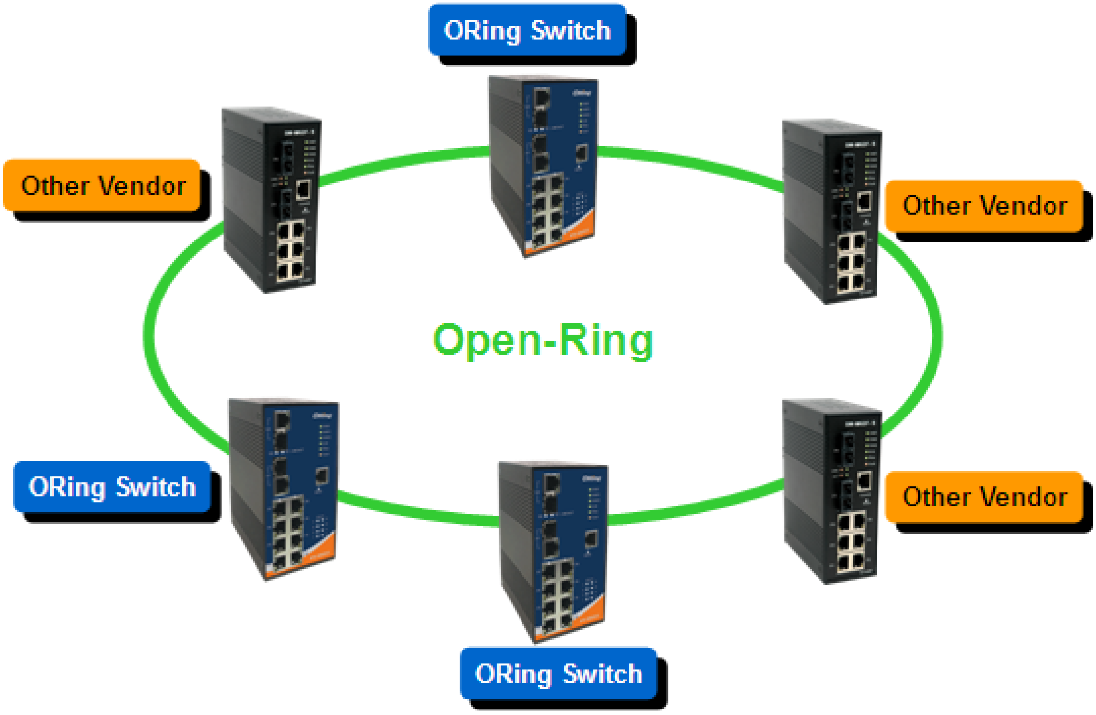
1st Ring Port: Port.01

2nd RingPort: Port.02

Open-Ring interface

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

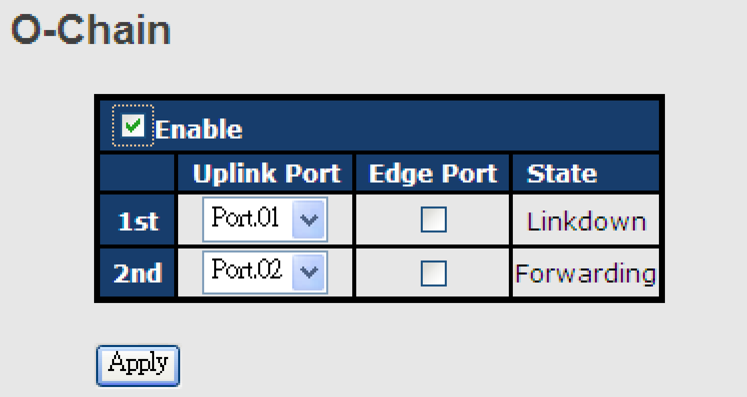
The application of Open-Ring is shown as below.



Open-Ring connection

5.1.1.3 O-Chain

O-Chain is the revolutionary network redundancy technology that provides the add-on network redundancy topology for any backbone network, providing ease-of-use while maximizing fault-recovery swiftness, flexibility, compatibility, and cost-effectiveness in one set of network redundancy topologies O-Chain allows multiple redundant network rings of different redundancy protocols to join and function together as a larger and more robust compound network topology, i.e. the creation of multiple redundant networks beyond the limitations of current redundant ring technology.

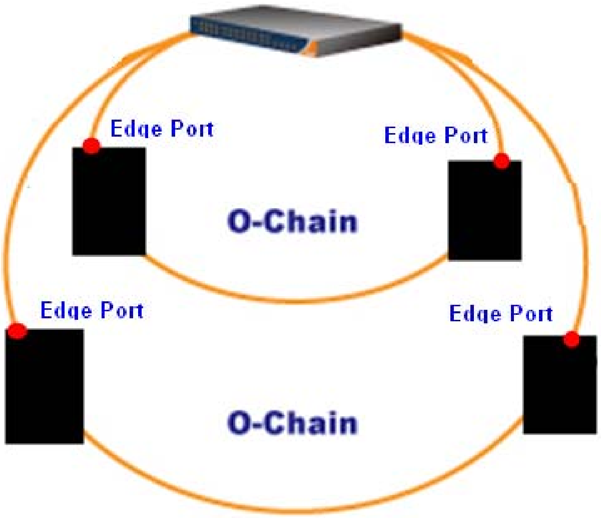


O-Chain

☑ Enable

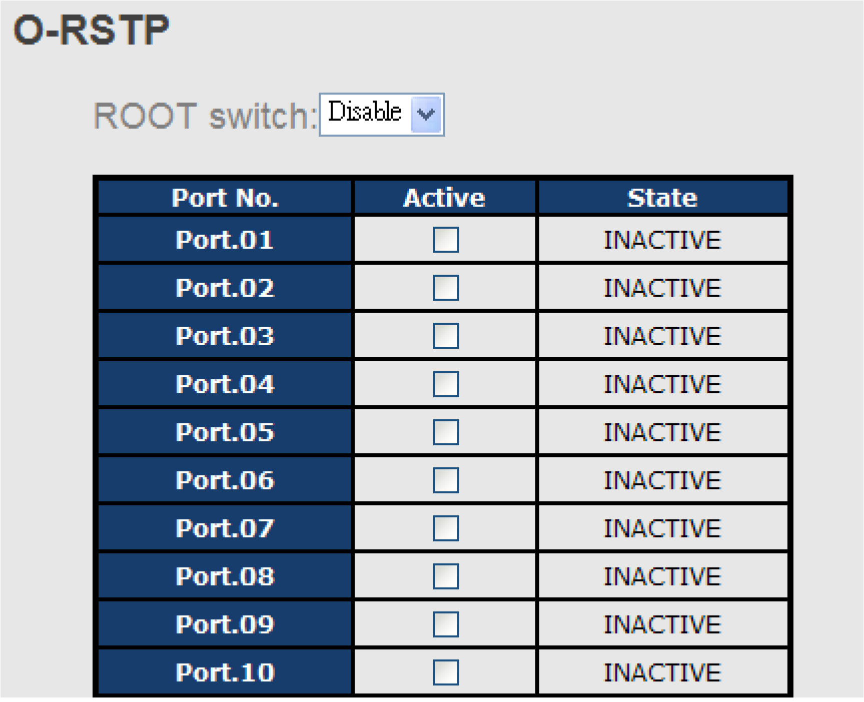
	Uplink Port	Edge Port	State
1st	Port.01	□	Linkdown
2nd	Port.02	□	Forwarding

Label	Description
Enable	Enabling the O-Chain function
1st Ring Port	Choosing the port which connect to the ring
2nd Ring Port	Choosing the port which connect to the ring
Edge Port	In the O-Chain application, the head and tail of two Switch Port, must start the Edge,MAC smaller Switch, Edge port will be the backup and RM LED Light.



5.1.1.4 O-RSTP

O-RSTP is proprietary redundant ring technology invented by O-Ring. Different from standard STP/RSTP, the recovery time of O-RSTP is less than 10ms and support more nodes of connection in a ring topology.



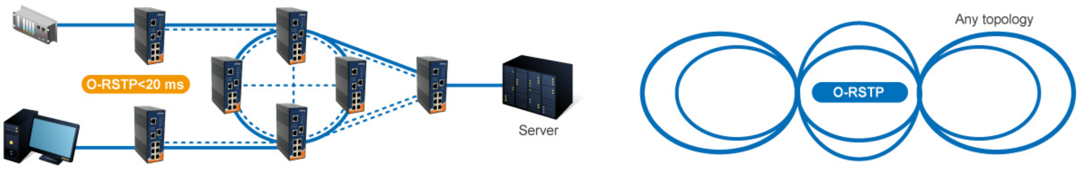
O-RSTP

ROOT switch: Disable

Port No.	Active	State
Port.01	□	INACTIVE
Port.02	□	INACTIVE
Port.03	□	INACTIVE
Port.04	□	INACTIVE
Port.05	□	INACTIVE
Port.06	□	INACTIVE
Port.07	□	INACTIVE
Port.08	□	INACTIVE
Port.09	□	INACTIVE
Port.10	□	INACTIVE

O-RSTP interface

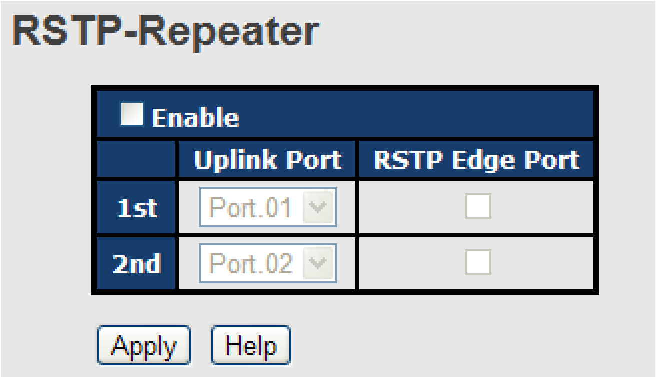
The application of O-RSTP is shown as below.



O-RSTP connection

5.1.1.5 RSTP – Repeater

RSTP-Repeater is a simple function , this function can direct pass RSTP BPDU packet , like two RSTP devices connected..



RSTP-Repeater

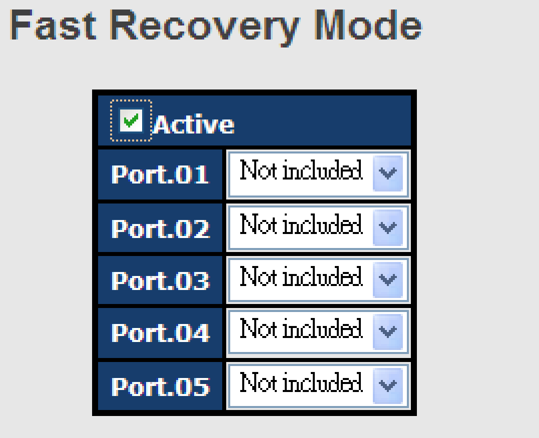
☐ Enable

	Uplink Port	RSTP Edge Port
1st	Port.01	☐
2nd	Port.02	☐

Label	Description
Enable	Check this box to enable RSTP-Repeater.
1st Ring Port	Choosing the port which connect to the RSTP
2nd Ring Port	Choosing the port which connect to the RSTP
Edge Port	Only the edge device (connected to RSTP device) needs to specify edge port. The user must specify the edge port according to topology of network.

5.1.1.6 Fast Recovery

The Fast Recovery Mode can be set to connect multiple ports to one or more switches. The IES-3240 with its fast recovery mode will provide redundant links. Fast Recovery mode supports 24 priorities, only the first priority will be the act port, the other ports configured with other priority will be the backup ports.



Fast Recovery Mode

☑ Active

Port.01	Not included
Port.02	Not included
Port.03	Not included
Port.04	Not included
Port.05	Not included

Fast Recovery Mode interface

The following table describes the labels in this screen.

Label	Description
Active	Activate the fast recovery mode.
port	Port can be configured as 24 priorities. Only the port with highest priority will be the active port. 1st Priority is the highest.
Apply	Click "**Apply**" to activate the configurations.

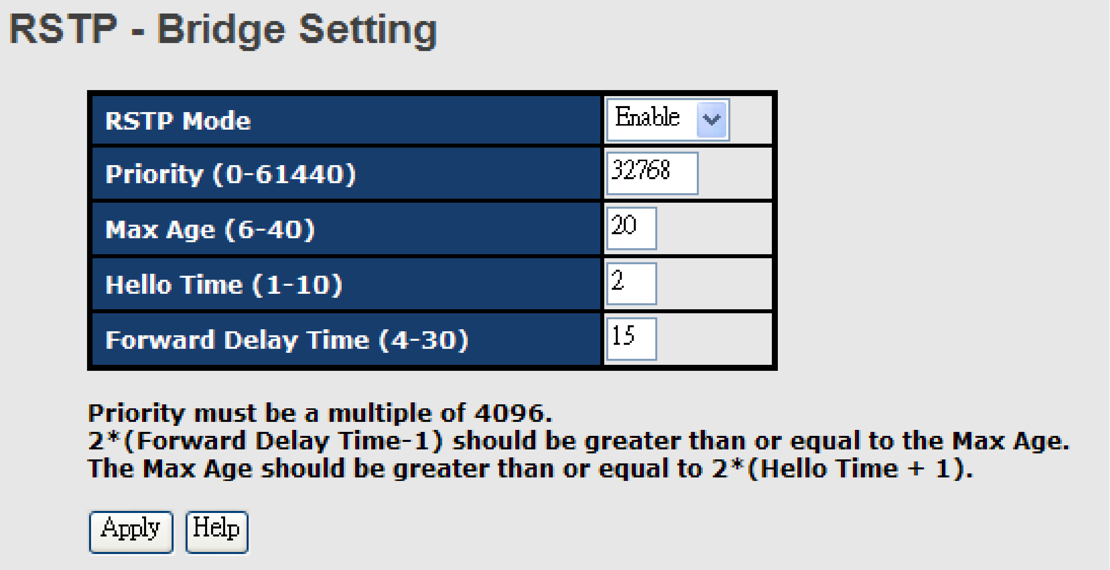
Note. If connect to PC then don't activate Fast Recovery mode at the port

5.1.1.7 RSTP

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

RSTP setting

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



RSTP - Bridge Setting

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

Priority must be a multiple of 4096.
2*(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).

RSTP Setting interface

The following table describes the labels in this screen.

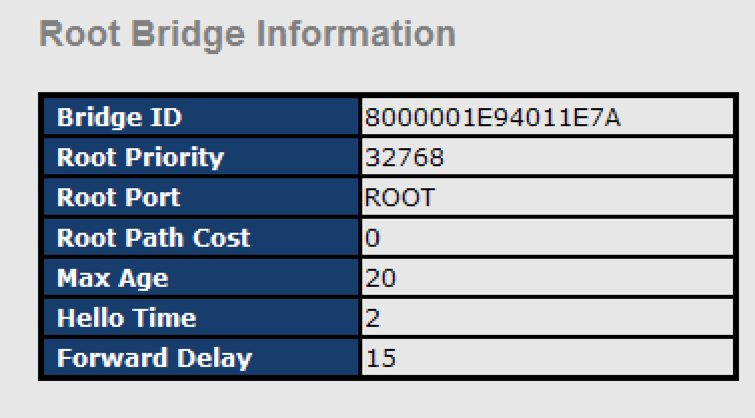
Label	Description
RSTP mode	You must enable or disable RSTP function before configuring the related parameters.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, You must reboot the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

	value must be multiple of 4096 according to the protocol standard rule.
Max Age Time(6-40)	The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
Hello Time (1-10)	The time that controls switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.
Forwarding Delay Time (4-30)	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.
Apply	Click "**Apply**" to set the configurations.

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

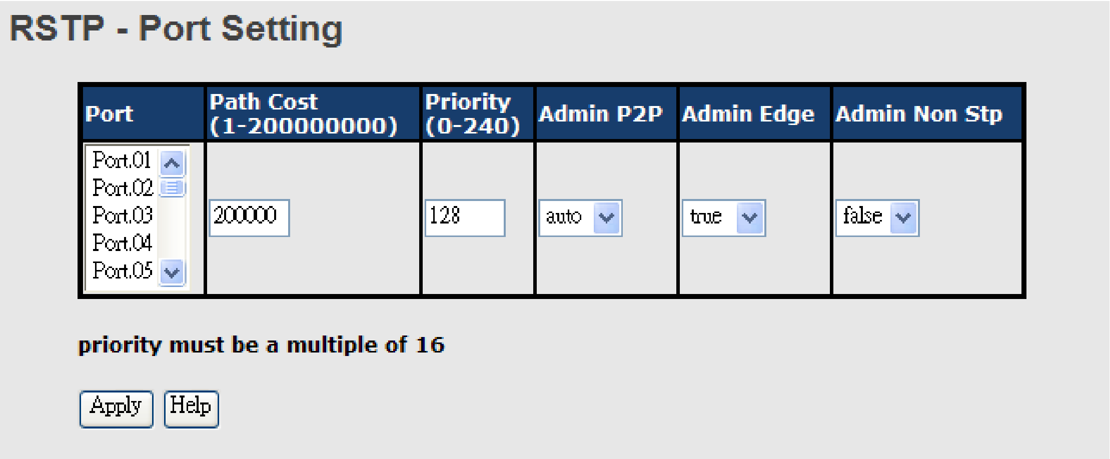
2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)

Show RSTP algorithm result at this table



Root Bridge Information

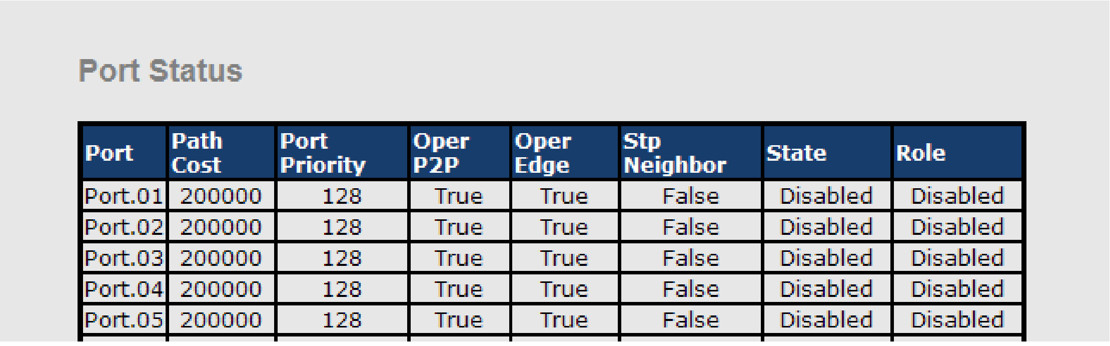
Bridge ID	8000001E94011E7A
Root Priority	32768
Root Port	ROOT
Root Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15



RSTP - Port Setting

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

priority must be a multiple of 16



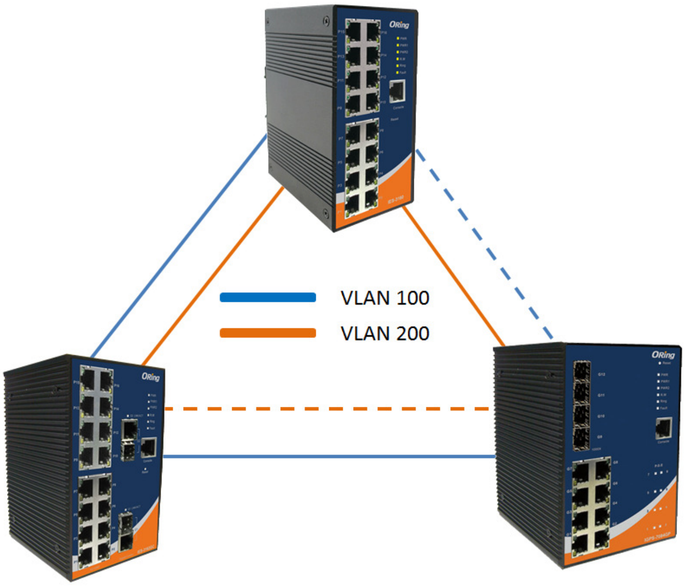
Port Status

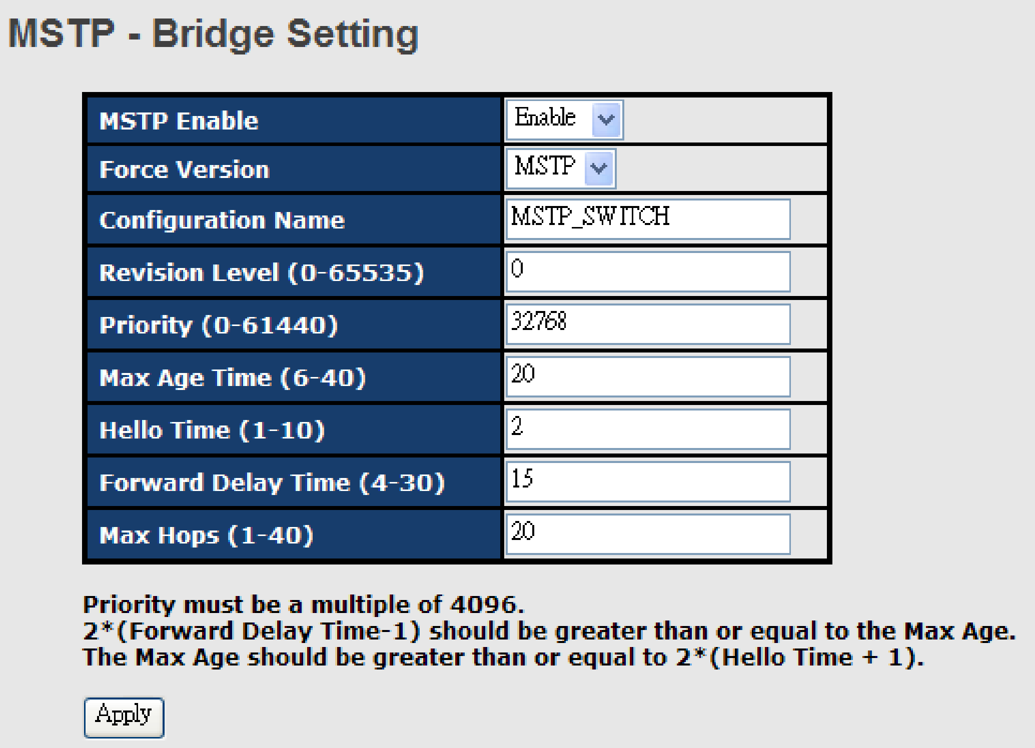
Port	Path Cost	Port Priority	Oper P2P	Oper Edge	Stp Neighbor	State	Role
Port.01	200000	128	True	True	False	Disabled	Disabled
Port.02	200000	128	True	True	False	Disabled	Disabled
Port.03	200000	128	True	True	False	Disabled	Disabled
Port.04	200000	128	True	True	False	Disabled	Disabled
Port.05	200000	128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

Label	Description
Path Cost (1-200000000)	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
Port Priority (0-240)	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
Admin P2P	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.
Admin Edge	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**".
Admin Non STP	The port includes the STP mathematic calculation. **True** is not including STP mathematic calculation. **False** is including the STP mathematic calculation.
Apply	Click "**Apply**" to set the configurations.

5.1.1.8 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 - Bridge Setting

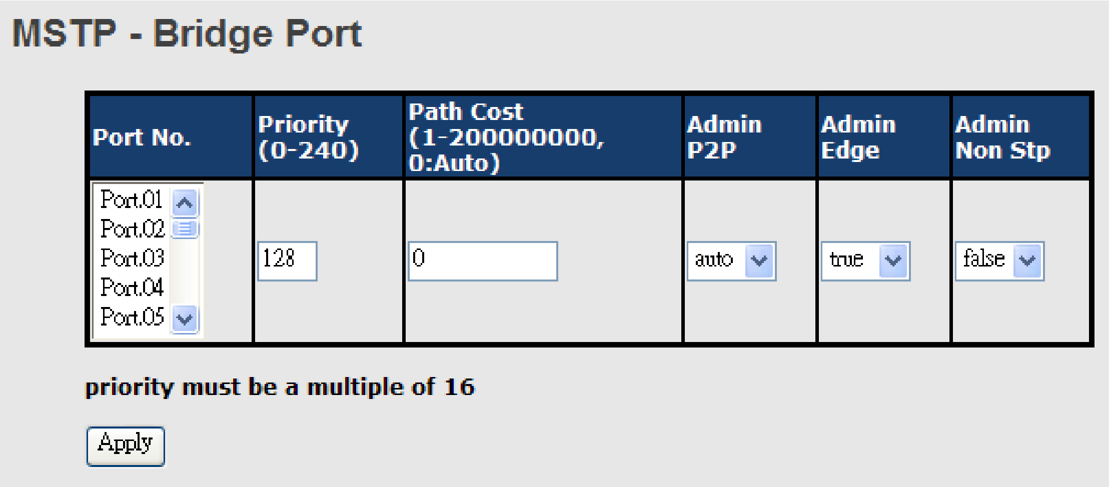
MSTP Enable	Enable
Force Version	MSTP
Configuration Name	MSTP_SWITCH
Revision Level (0-65535)	0
Priority (0-61440)	32768
Max Age Time (6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15
Max Hops (1-40)	20

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

MSTP Setting interface

The following table describes the labels in this screen.

Label	Description
MSTP Enable	You must enable or disable MSTP function before configuring the related parameters.
Force Version	The Force Version parameter can be used to force a VLAN Bridge that supports RSTP to operate in an STP-compatible manner.
Configuration Name	The same MST Region must have the same MST configuration name.
Revision Level (0-65535)	The same MST Region must have the same revision level.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, You must reboot the switch. The value must be multiple of 4096 according to the protocol standard rule.
Max Age Time(6-40)	The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
Hello Time (1-10)	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 x (Forward Delay Time value –1) ≥ Max Age value ≥ 2 x (Hello Time value +1)**
Forwarding Delay Time (4-30)	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.
Max Hops (1-40)	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.
Apply	Click "**Apply**" to activate the configurations.



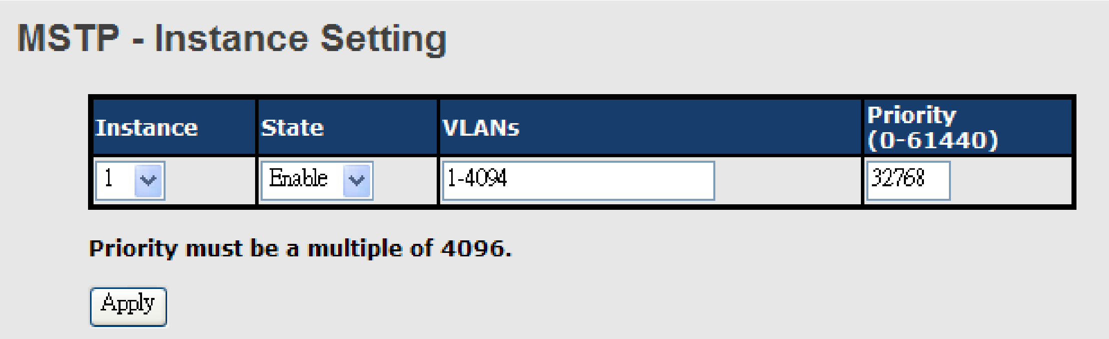
MSTP - Bridge Port

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

MSTP Port interface

Label	Description
Port No.	Selecting the port that you want to configure.
Priority (0-240)	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
Path Cost (1-200000000)	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
Admin P2P	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.
Admin Edge	Label
Admin Non STP	Label
Apply	Click "**Apply**" to activate the configurations.



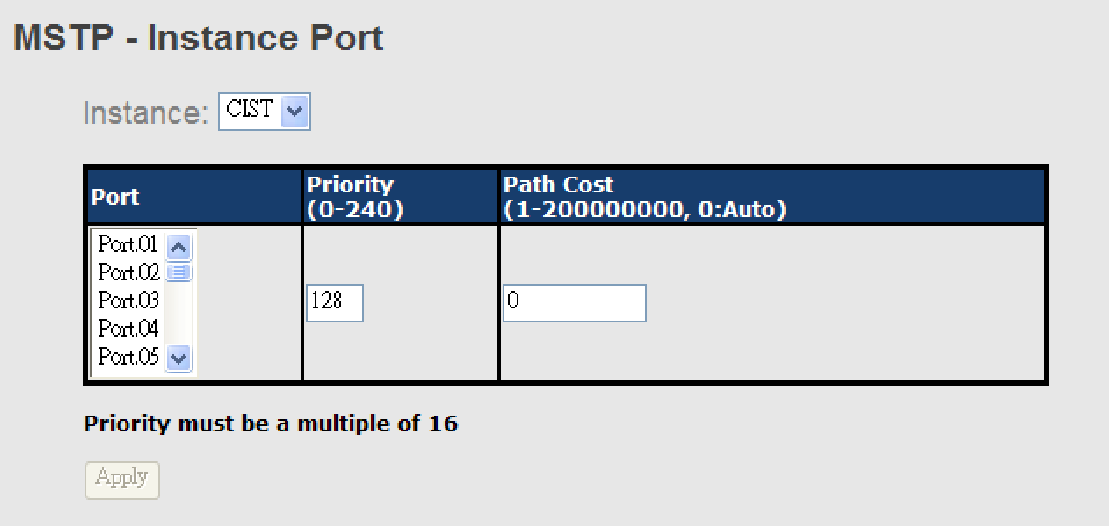
MSTP - Instance Setting

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

Priority must be a multiple of 4096.

MSTP Instance interface

Label	Description
Instance	Set the instance from 1 to 15
State	Enable or disable the instance
VLANs	Set which VLAN will belong which instance
Proprietary (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, You must reboot the switch. The value must be multiple of 4096 according to the protocol standard rule.
Apply	Click “**Apply**” 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 Port.04 Port.05	128	0

Priority must be a multiple of 16

MSTP Instance Port interface

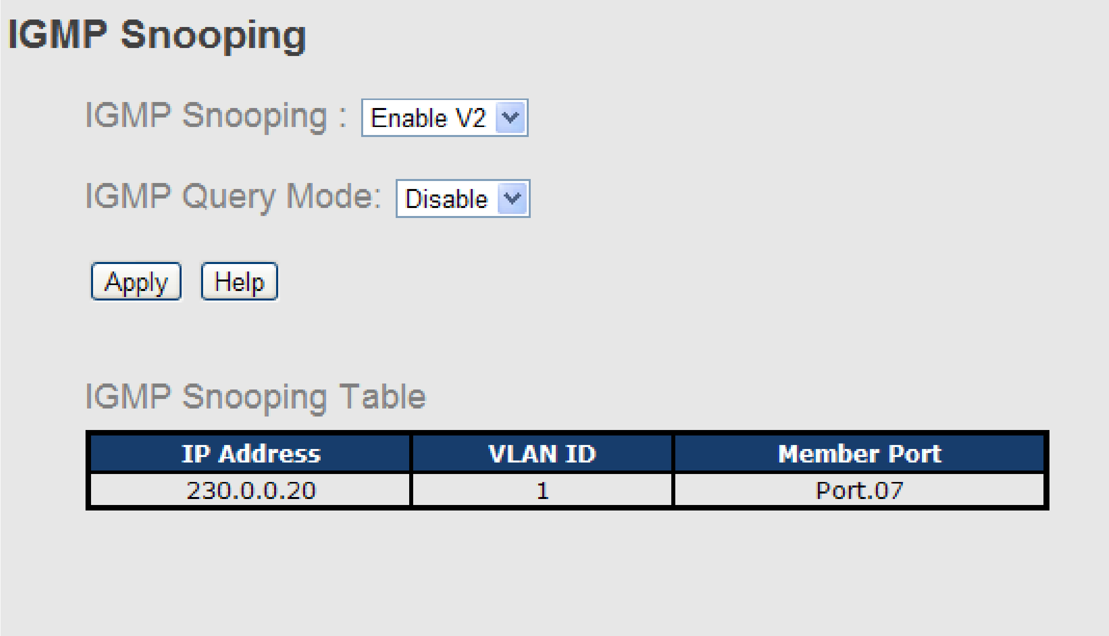
Label	Description
Instance	Set the instance’s information except CIST
Port	Selecting the port that you want to configure.
Priority (0-240)	Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple

	of 16
Path Cost (1-200000000)	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
Apply	Click "**Apply**" to set the configurations.

5.1.2 Multicast

5.1.2.1 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 : Enable V2

IGMP Query Mode: Disable

IGMP Snooping Table

IP Address	VLAN ID	Member Port
230.0.0.20	1	Port.07

IGMP Snooping interface

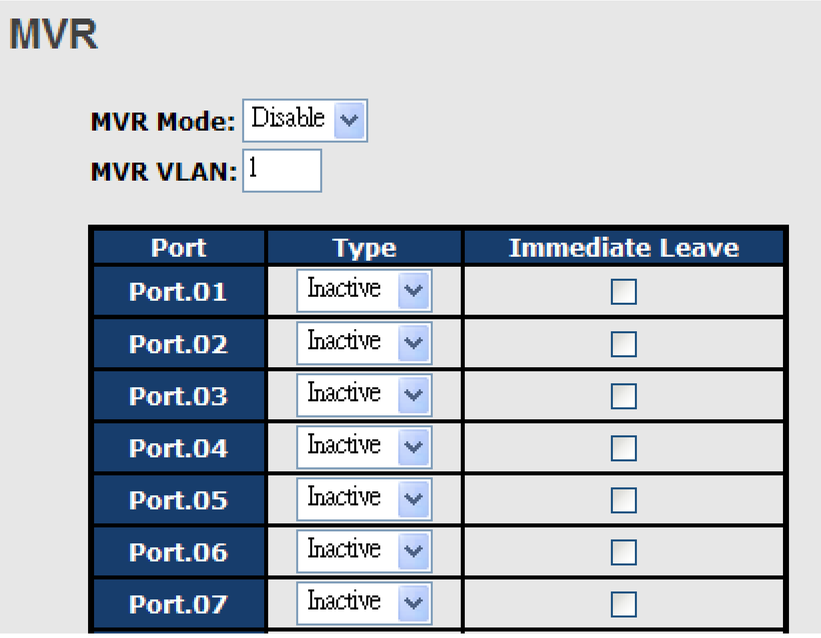
The following table describes the labels in this screen.

Label	Description
IGMP Snooping Table	Show current IP multicast list
IGMP Protocol	Enable/Disable IGMP snooping.

IGMP Query	Switch will be IGMP querier or not. There should exist one and only one IGMP querier in an IGMP application. The "Auto" mode means that the querier is the one with lower IP address.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.1.2.2 MVR

MVR Function can provide a different VLAN users to receive MVR Mode VLAN Multicast Packet.



MVR

MVR Mode: Disable

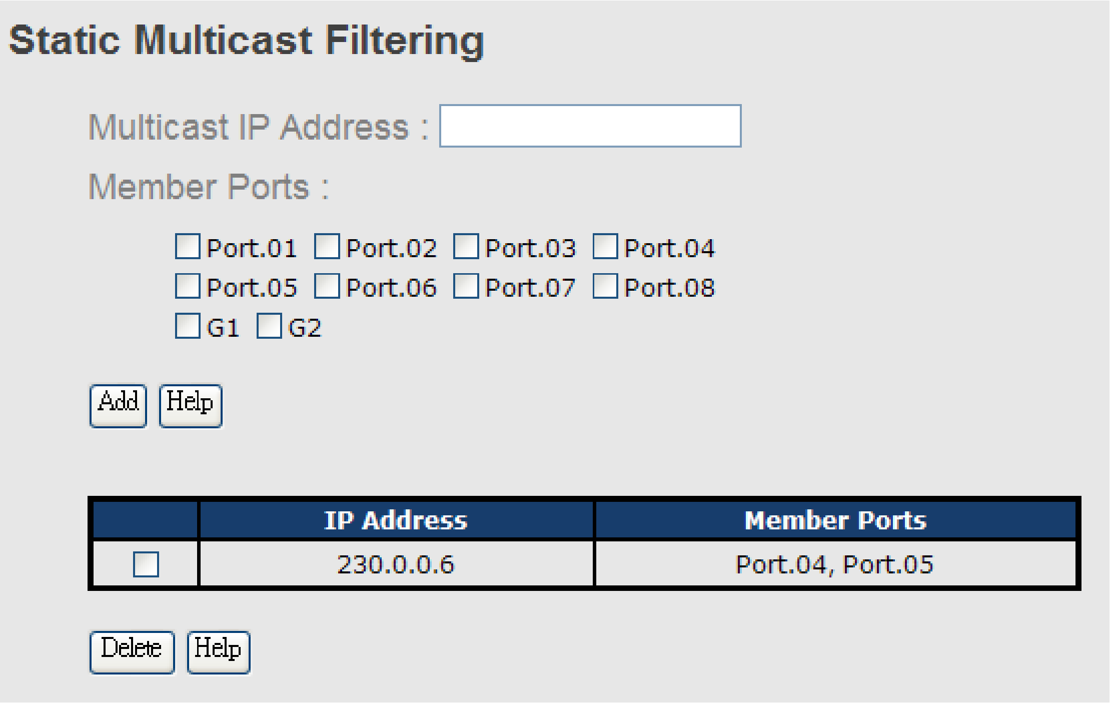
MVR VLAN: 1

Port	Type	Immediate Leave
Port.01	Inactive	□
Port.02	Inactive	□
Port.03	Inactive	□
Port.04	Inactive	□
Port.05	Inactive	□
Port.06	Inactive	□
Port.07	Inactive	□

Label	Description
MVR Mode	Enable or Disable MVR Mode
MVR VLAN	Setting MVR VLAN
TYPE	Setting Port Type to inactive、Receiver、Source
Immediate Leave	Enable or disable Immediate leave

5.1.2.3 Static Multicast Filtering

Static 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.



Static Multicast Filtering

Multicast IP Address :

Member Ports :

□ Port.01 □ Port.02 □ Port.03 □ Port.04
□ Port.05 □ Port.06 □ Port.07 □ Port.08
□ G1 □ G2

	IP Address	Member Ports
□	230.0.0.6	Port.04, Port.05

Multicast Filtering Interface

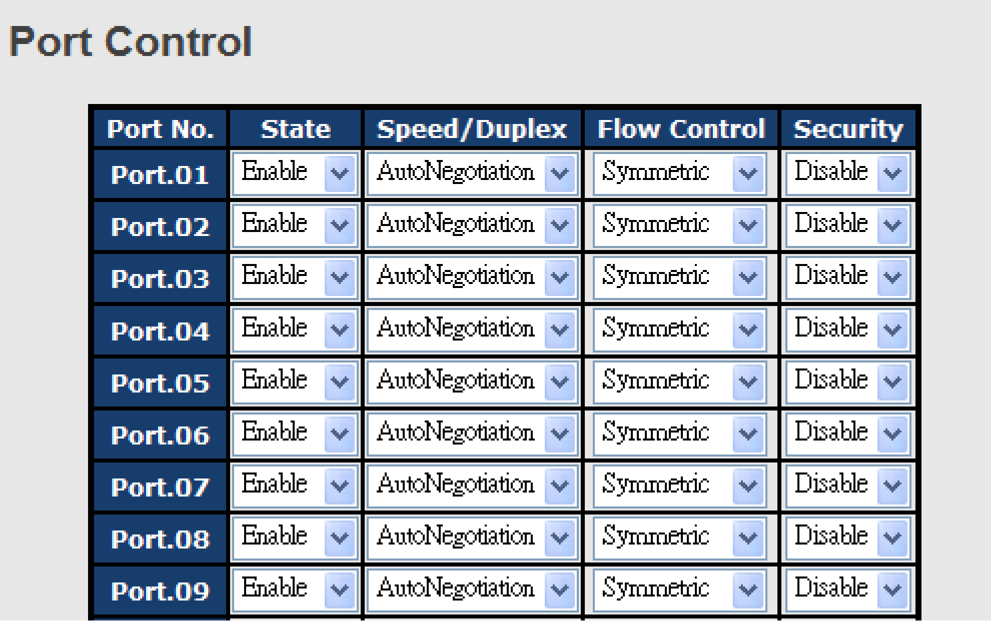
The following table describes the labels in this screen.

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

5.1.3 Port Setting

5.1.3.1 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

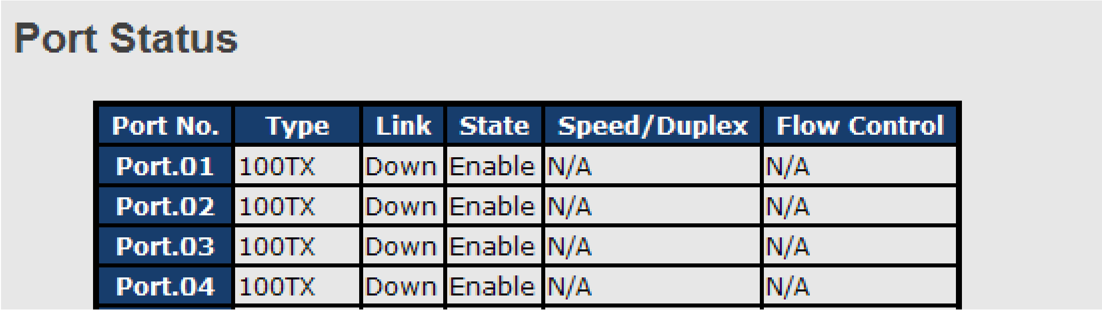
Port Control interface

The following table describes the labels in this screen.

Label	Description
Port NO.	Port number for setting.
State	Enable/Disable the port.
Speed/Duplex	You can set Auto-negotiation, 100-full, 100-half, 10-full, 10-half mode.
Flow Control	Support symmetric and asymmetric mode to avoid packet loss when congestion occurred.
Security	Enabled port security will disable MAC address learning in this port. Thus only the frames with MAC addresses in port security list will be forwarded, otherwise will be discarded.
Apply	Click "**Apply**" to activate the configurations.

5.1.3.2 Port Status

The following information provides the current port status information



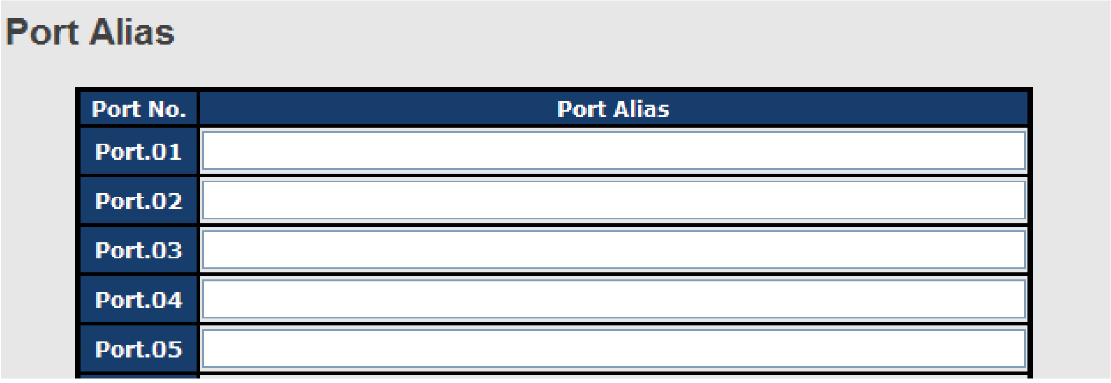
Port Status

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	Down	Enable	N/A	N/A
Port.04	100TX	Down	Enable	N/A	N/A

Port Status interface

5.1.3.3 Port Alias

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

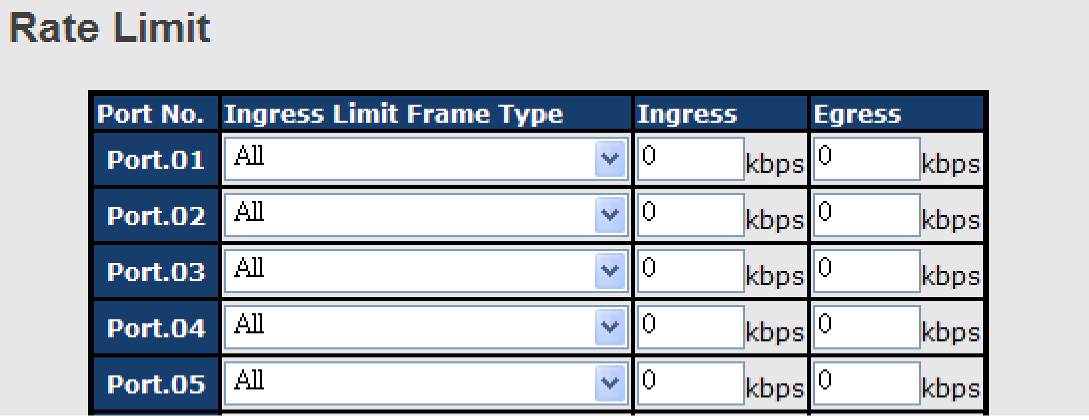


Port Alias

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

5.1.3.4 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

Rate Limit interface

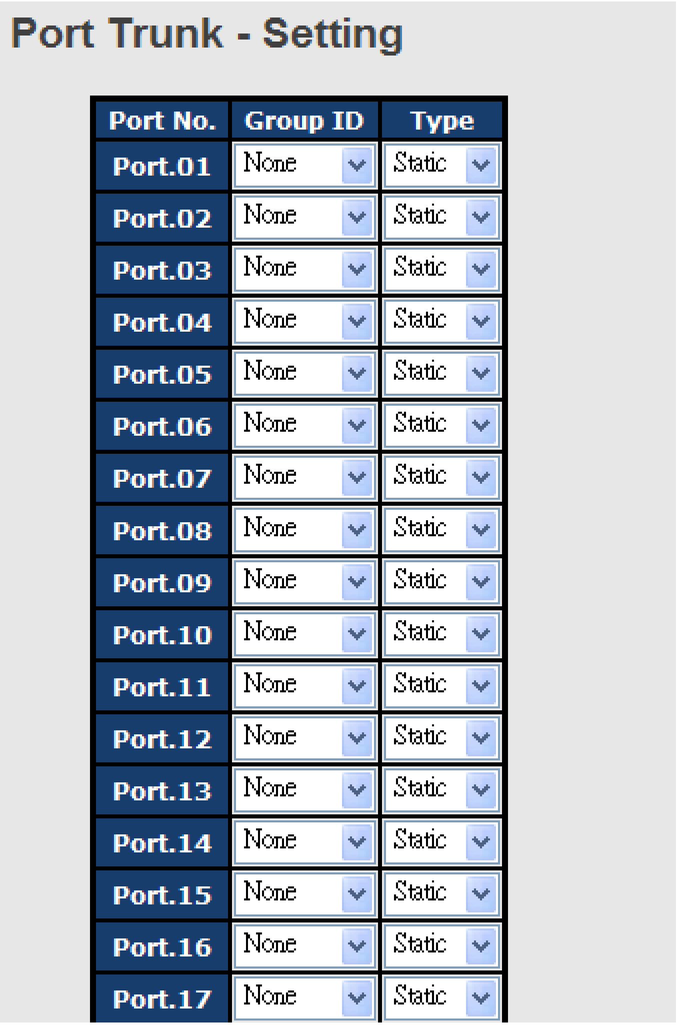
The following table describes the labels in this screen.

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

5.1.3.5 Port Trunk

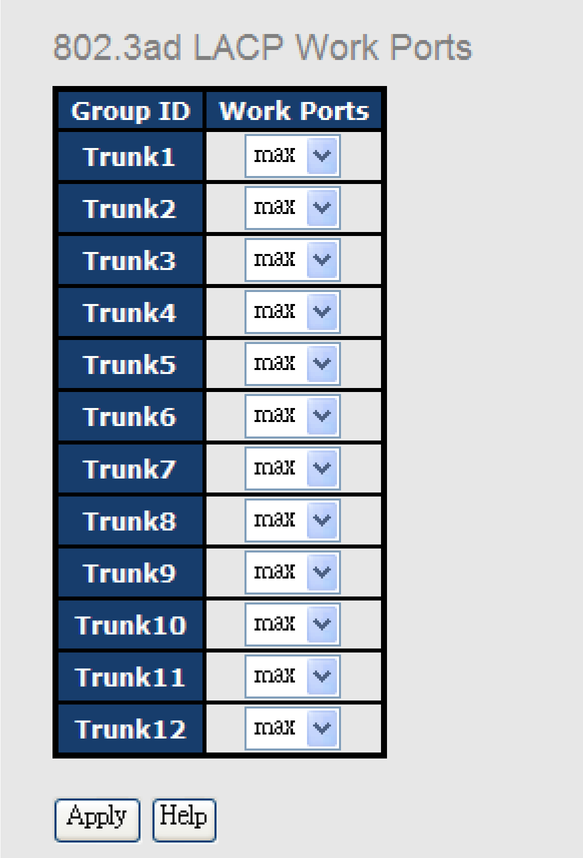
Port Trunk – Setting

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
Port.17	None	Static



802.3ad LACP Work Ports

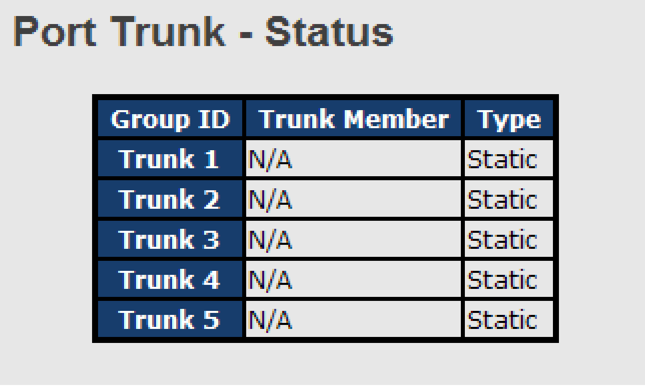
Group ID	Work Ports
Trunk1	max
Trunk2	max
Trunk3	max
Trunk4	max
Trunk5	max
Trunk6	max
Trunk7	max
Trunk8	max
Trunk9	max
Trunk10	max
Trunk11	max
Trunk12	max

Port Trunk - Setting interface

The following table describes the labels in this screen.

Label	Description
Group ID	Select port to join a trunk group.
Type	Support static trunk and 802.3ad LACP
Work Port	Select the number of active ports in dynamic group (LACP). The default value of works ports is maximum number of the group. If the number is not maximum number of ports, the other inactive ports in dynamic group will be suspended (no traffic). Once the active port is broken, the suspended port will be active automatically.
Apply	Click "**Apply**" to set the configurations.

Port Trunk – Status



Port Trunk - Status

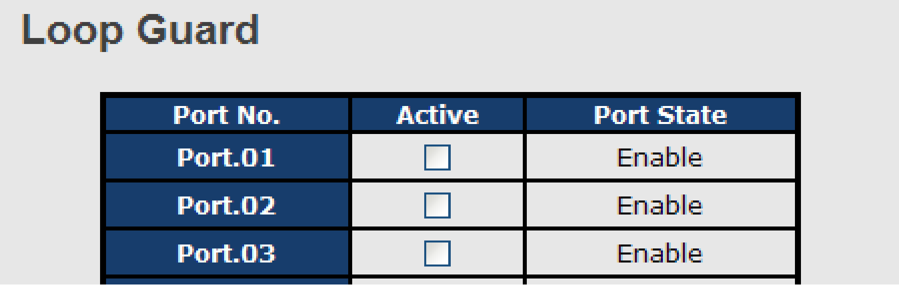
Group ID	Trunk Member	Type
Trunk 1	N/A	Static
Trunk 2	N/A	Static
Trunk 3	N/A	Static
Trunk 4	N/A	Static
Trunk 5	N/A	Static

Port Trunk - Status interface

Label	Description
Group Key	Trunk Group number
Port Member	Show Group port info

5.1.3.6 Loop Guard

This feature prevents the loop attack, When the port receives loop packet. This port will auto disable , prevent the "loop attack" affect other network devices



Loop Guard

Port No.	Active	Port State
Port.01	□	Enable
Port.02	□	Enable
Port.03	□	Enable

Label	Description
Active	Loop Guard Enable or Disable
Port Status	Port work status.

5.1.4 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 VLAN will receive traffic from the same members of VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

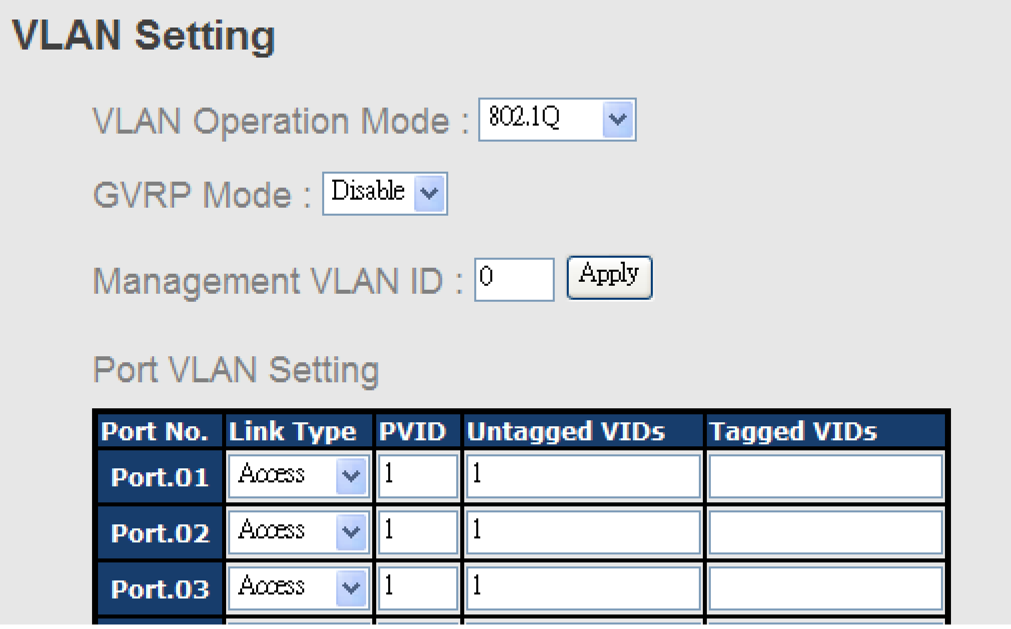
The switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration of VLAN operation mode is at "**802.1Q**".

5.1.4.1 VLAN Setting - IEEE 802.1Q

Tagged-based VLAN is an IEEE 802.1Q specification standard, and t is possible to create a VLAN across devices from different switch venders. 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 to provide configure. Enable 802.1Q VLAN, the 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

Port VLAN Setting

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

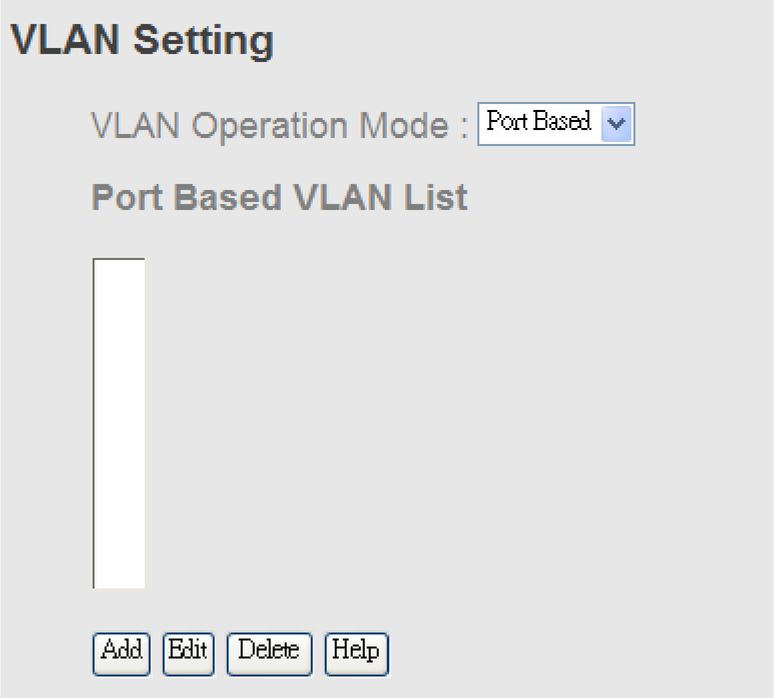
VLAN Configuration – 802.1Q interface

The following table describes the labels in this screen.

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

5.1.4.2 VLAN Setting – Port Based

Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.



VLAN Setting

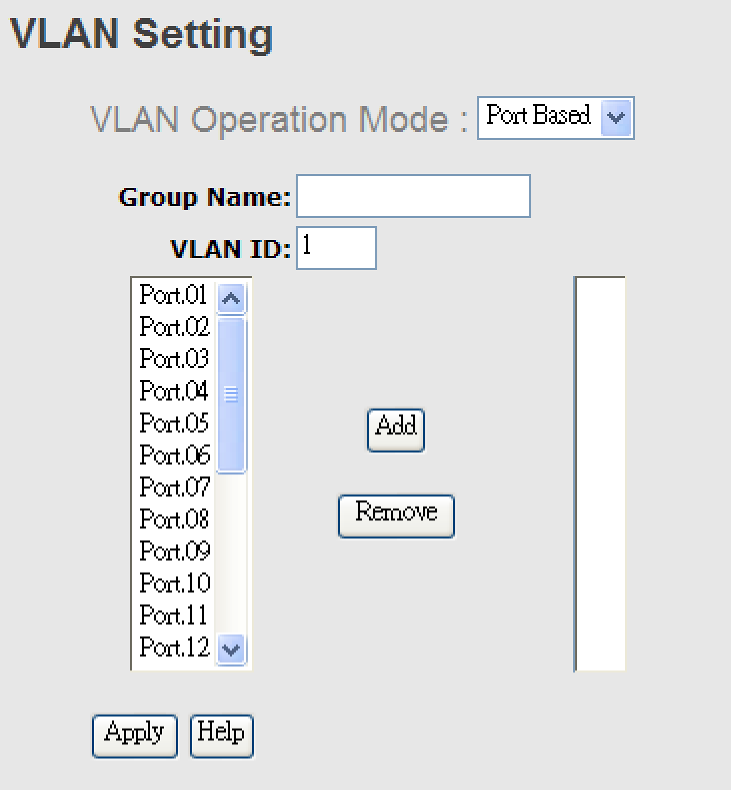
VLAN Operation Mode : Port Based

Port Based VLAN List

VLAN Configuration – Port Base interface-1

The following table describes the labels in this screen.

Label	Description
Add	Click "**add**" to enter VLAN add interface.
Edit	Edit exist VLAN
Delete	Delete exist VLAN
Help	Show help file.



VLAN Setting

VLAN Operation Mode : Port Based

Group Name:

VLAN ID: 1

VLAN Configuration – Port Base interface-2

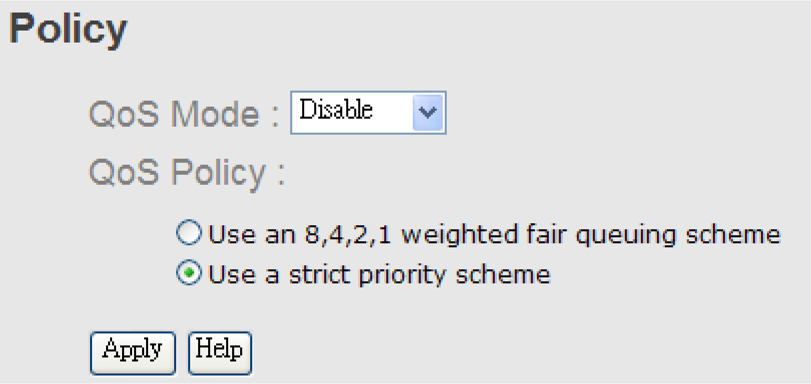
The following table describes the labels in this screen.

Label	Description
Group Name	VLAN name.
VLAN ID	Specify the VLAN ID
Add	Select port to join the VLAN group.
Remove	Remove port of the VLAN group
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.1.5 Traffic Priorilization

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.

5.1.5.1 Qos policy



Policy

QoS Mode : Disable

QoS Policy :

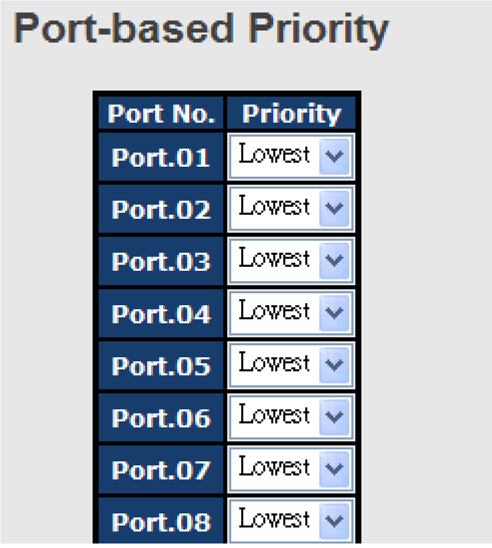
○ Use an 8,4,2,1 weighted fair queuing scheme
● Use a strict priority scheme

Traffic Prioritization interface

The following table describes the labels in this screen.

Label	Description
QOS Mode	■ **Port-base:** the output priority is determined by ingress port. ■ **COS only:** the output priority is determined by COS only. ■ **TOS only:** the output priority is determined by TOS only. ■ **COS first:** the output priority is determined by COS and TOS, but COS first. ■ **TOS first:** the output priority is determined by COS and TOS, but TOS first.
QOS policy	■ **Using the 8,4,2,1 weight fair queue scheme:** the output queues will 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. ■ **Use the strict priority scheme:** always the packets in higher queue will be transmitted first until higher queue is empty.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.1.5.2 Port-base priority



Port-based Priority

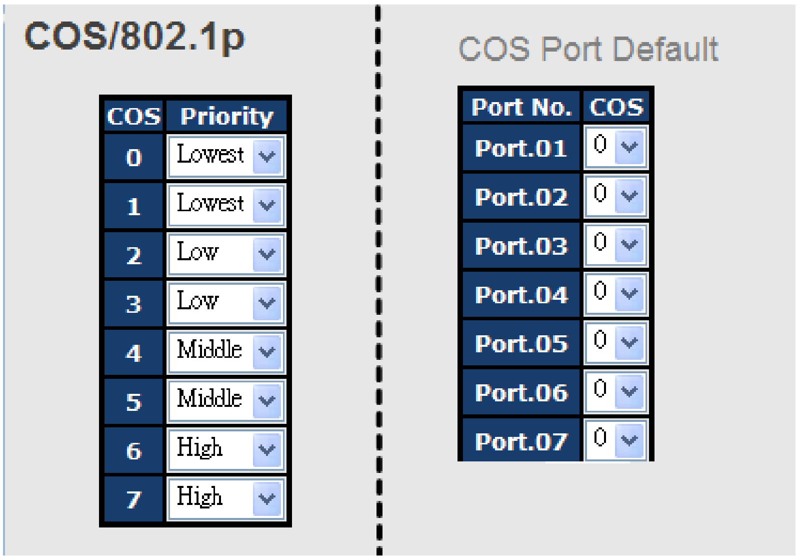
Port No.	Priority
Port.01	Lowest
Port.02	Lowest
Port.03	Lowest
Port.04	Lowest
Port.05	Lowest
Port.06	Lowest
Port.07	Lowest
Port.08	Lowest

Port-based Priority interface

The following table describes the labels in this screen

Port base Priority	Assign Port with a priority queue. 4 priority queues can be assigned: High, Middle, Low, and Lowest.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.1.5.3 COS/802.1p



COS/802.1p

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

COS Port Default

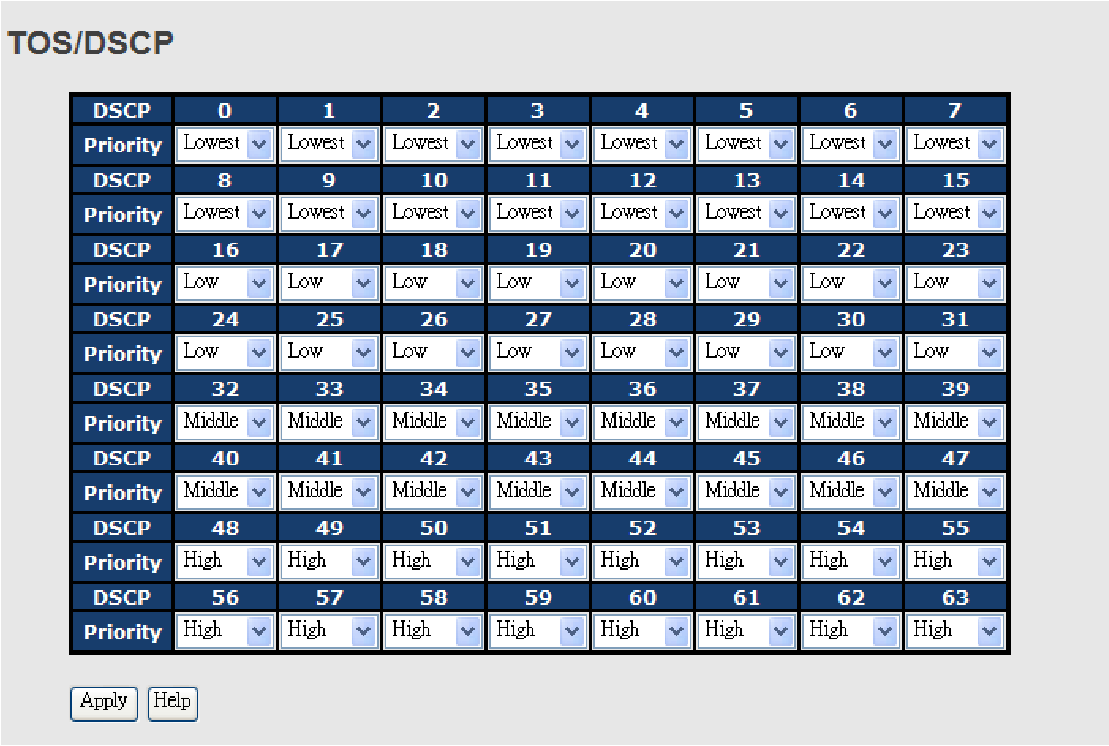
Port No.	COS
Port.01	0
Port.02	0
Port.03	0
Port.04	0
Port.05	0
Port.06	0
Port.07	0

COS/802.1p interface

The following table describes the labels in this screen

COS/802.1p	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 0to7.COS value map to 4 priority queues: High, Middle, Low, and Lowest.
COS Port Default	When an ingress packet has not VLAN tag, a default priority value is considered and determined by ingress port.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.1.5.4 TOS/DSCP



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

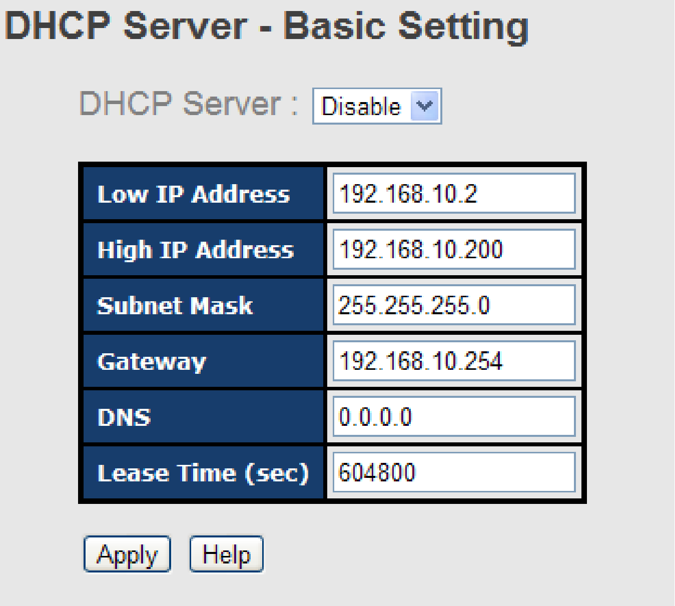
The following table describes the labels in this screen

TOS/DSCP	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 0to63. DSCP value map to 4 priority queues: High, Middle, Low, and Lowest.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.1.6 DHCP Server

5.1.6.1 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 - Basic Setting

DHCP Server : Disable

Low IP Address	192.168.10.2
High IP Address	192.168.10.200
Subnet Mask	255.255.255.0
Gateway	192.168.10.254
DNS	0.0.0.0
Lease Time (sec)	604800

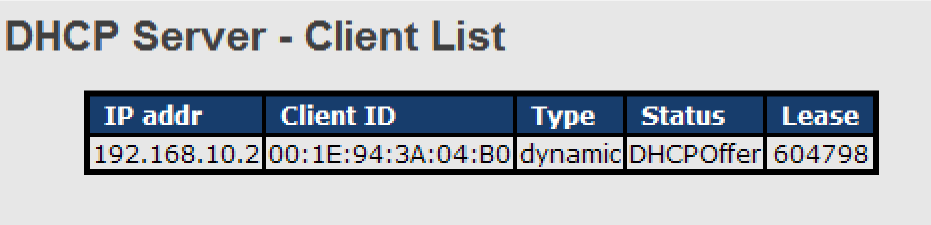
DHCP Server Configuration interface

The following table describes the labels in this screen.

Label	Description
DHCP Server	Enable or Disable the DHCP Server function. Enable – the switch will be the DHCP server on your local network
Start IP Address	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.
End IP Address	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
Subnet Mask	The dynamic IP assign range subnet mask
Gateway	The gateway in your network.
DNS	Domain Name Server IP Address in your network.
Lease Time (Hour)	It is the period that system will reset the assigned dynamic IP to ensure the IP address is in used.
Apply	Click "**Apply**" to set the configurations.

5.1.6.2 DHCP Server – Client List

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



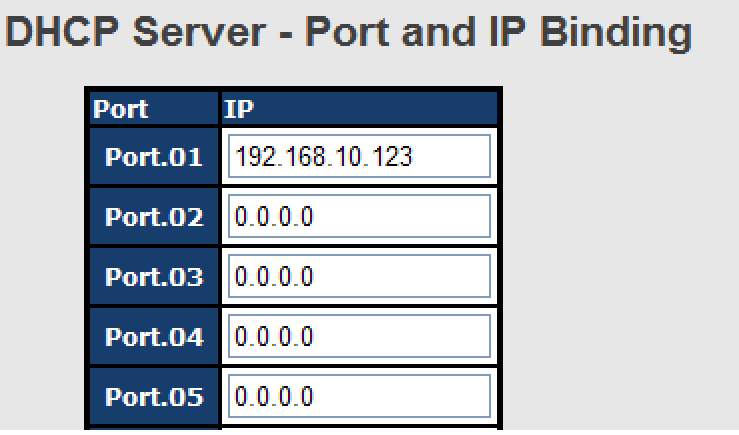
DHCP Server - Client List

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

DHCP Server Client Entries interface

5.1.6.3 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.



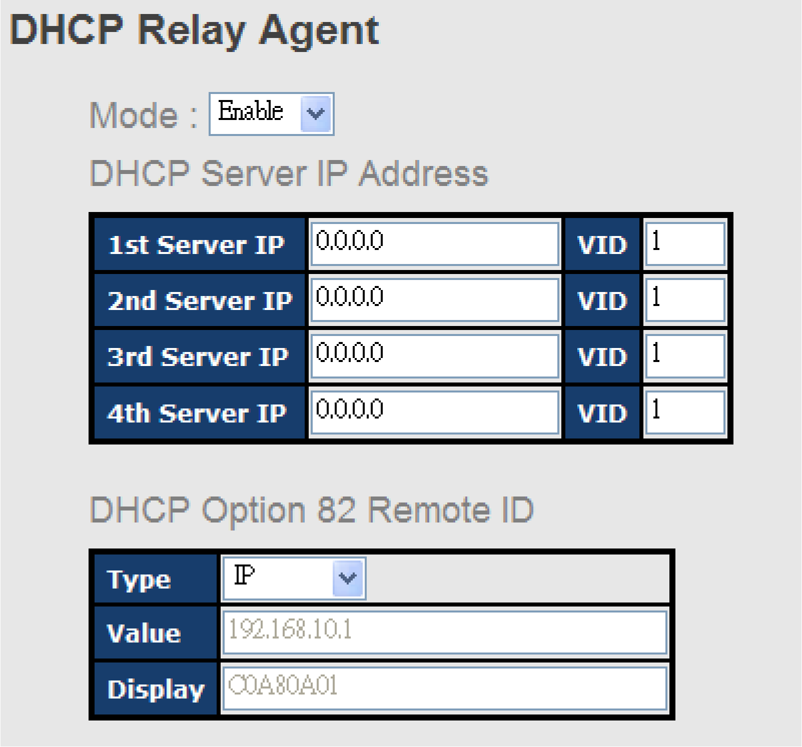
DHCP Server - Port and IP Binding

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

DHCP Server Port and IP Binding interface

5.1.6.4 DHCP Server –DHCP Relay Agent

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



DHCP Relay Agent

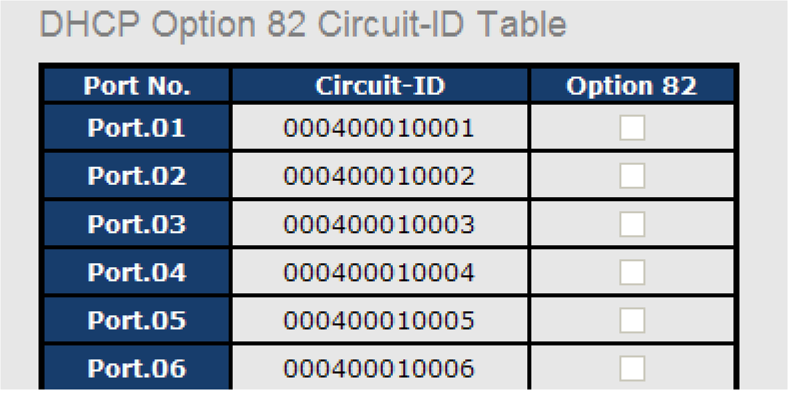
Mode : Enable

DHCP Server IP Address

1st Server IP	0.0.0.0	VID	1
2nd Server IP	0.0.0.0	VID	1
3rd Server IP	0.0.0.0	VID	1
4th Server IP	0.0.0.0	VID	1

DHCP Option 82 Remote ID

Type	IP
Value	192.168.10.1
Display	C0A80A01



DHCP Option 82 Circuit-ID Table

Port No.	Circuit-ID	Option 82
Port.01	000400010001	□
Port.02	000400010002	□
Port.03	000400010003	□
Port.04	000400010004	□
Port.05	000400010005	□
Port.06	000400010006	□

The following table describes the labels in this screen.

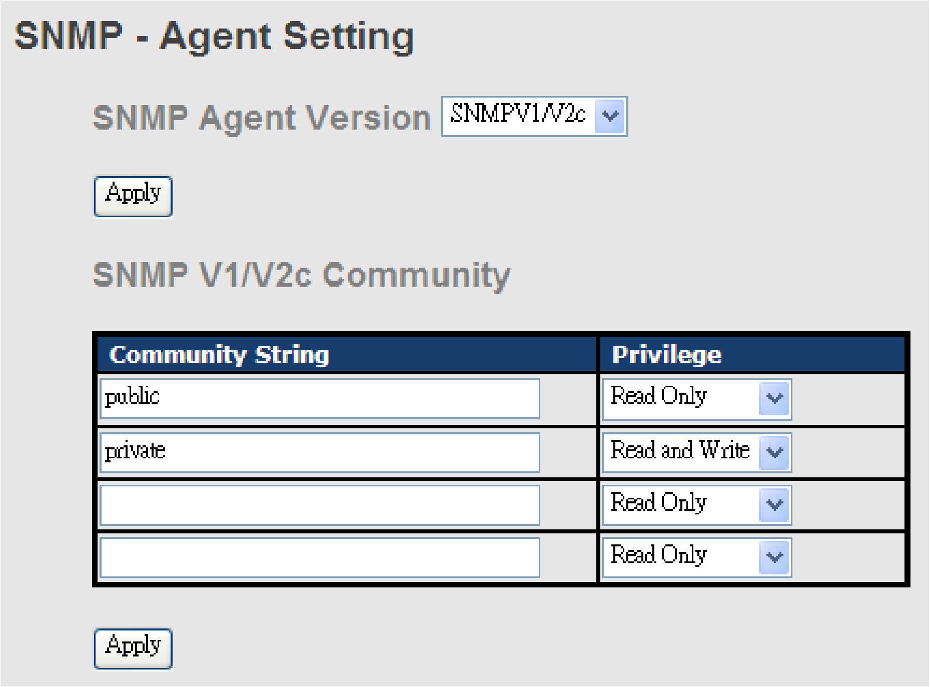
Label	Description
DHCP Relay	Enable/Disable DHCP Relay Agent.
DHCP Server IP Address and VID	Specify the IP address and VID of DHCP server. Keep "0.0.0.0" means server is inactive.
DHCP Option 82 Remote ID	"Option 82 Remote ID" provides a identifier for the remote server. There are 4 types supported: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

5.1.7 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.

5.1.7.1 SNMP – Agent Setting

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



SNMP - Agent Setting

SNMP Agent Version: SNMPV1/V2c

SNMP V1/V2c Community

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

SNMP – Agent setting interface

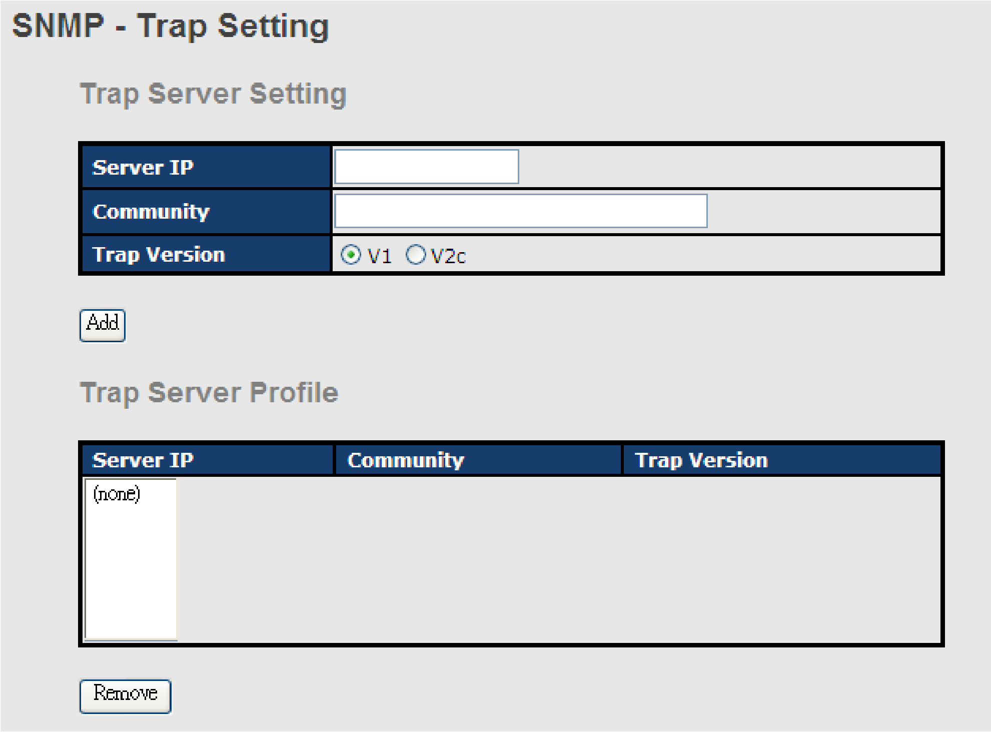
The following table describes the labels in this screen.

Label	Description
SNMP agent Version	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.
SNMP V1/V2c Community	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.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.7.2 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.



SNMP - Trap Setting

Trap Server Setting

Server IP	
Community	
Trap Version	● V1 ○ V2c

Trap Server Profile

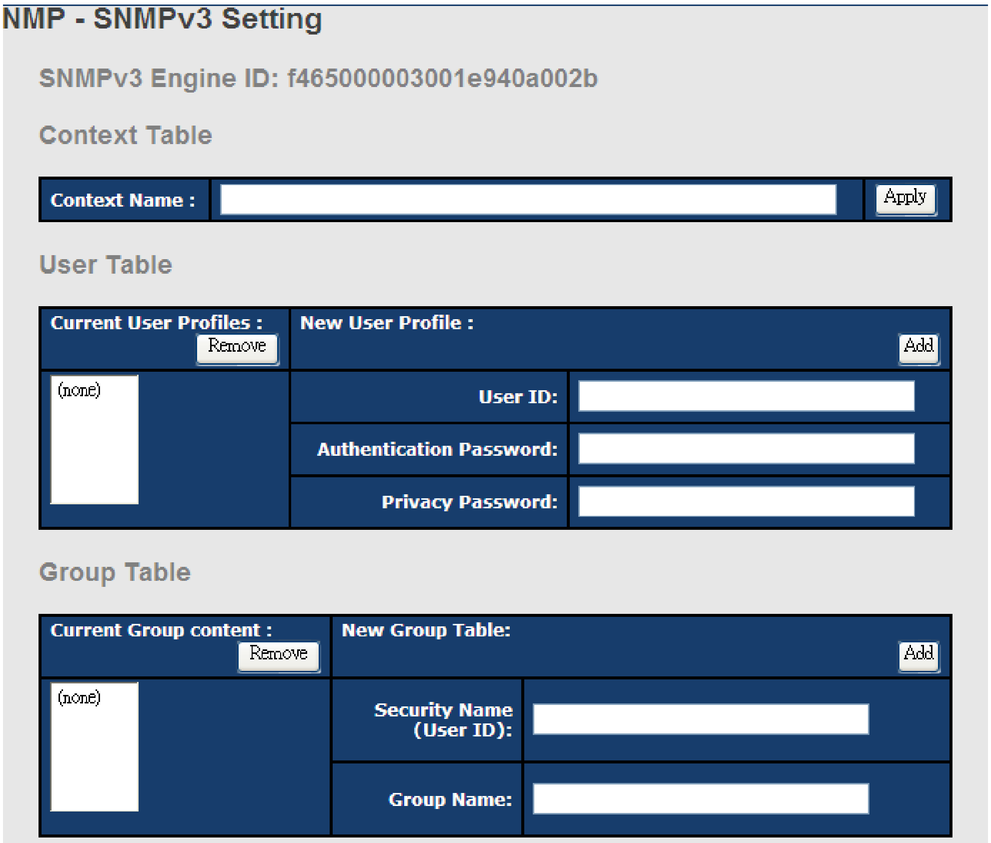
Server IP	Community	Trap Version
(none)		

SNMP –Trap Setting interface

The following table describes the labels in this screen.

Label	Description
Server IP	The server IP address to receive Trap
Community	Community for authentication
Trap Version	Trap Version supports V1 and V2c and V3
Add	Add trap server profile.
Remove	Remove trap server profile.
Help	Show help file.

5.1.7.3 SNMPV3



NMP - SNMPv3 Setting

SNMPv3 Engine ID: f465000003001e940a002b

Context Table

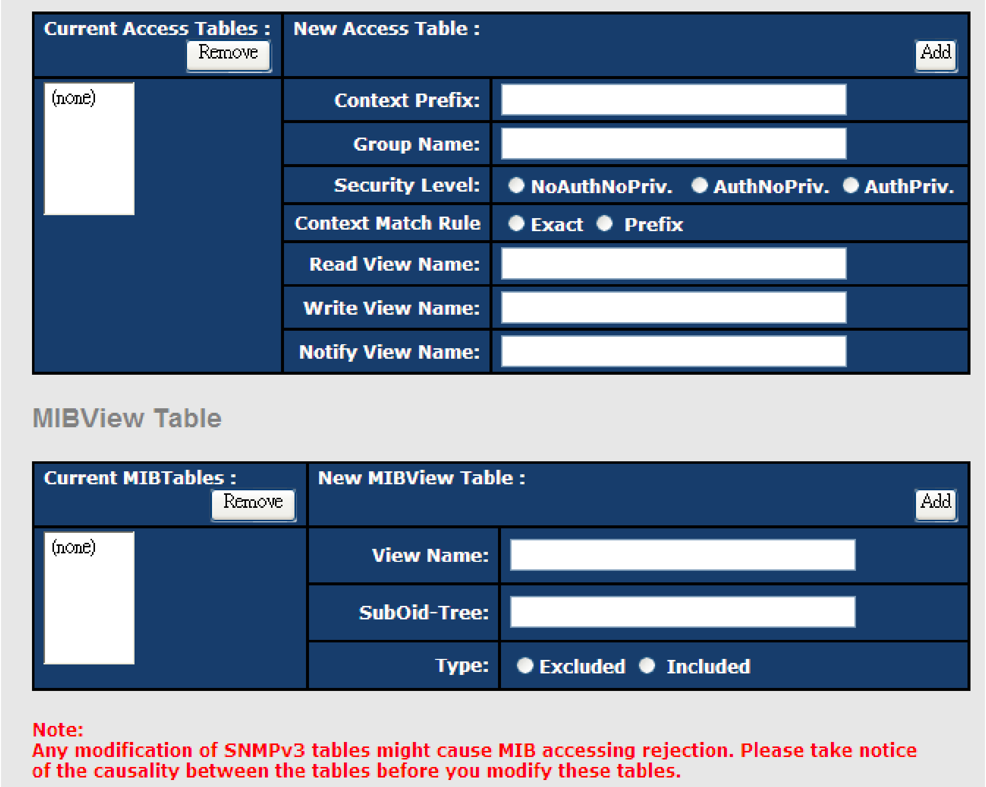
Context Name :		Apply

User Table

Current User Profiles : Remove	New User Profile : Add	
(none)	User ID:	
	Authentication Password:	
	Privacy Password:	

Group Table

Current Group content : Remove	New Group Table: Add	
(none)	Security Name (User ID):	
	Group Name:	



Current Access Tables : Remove	New Access Table : Add	
(none)	Context Prefix:	
	Group Name:	
	Security Level:	● NoAuthNoPriv. ● AuthNoPriv. ● AuthPriv.
	Context Match Rule	● Exact ● Prefix
	Read View Name:	
	Write View Name:	
	Notify View Name:	

MIBView Table

Current MIBTables : Remove	New MIBView Table : Add	
(none)	View Name:	
	SubOid-Tree:	
	Type:	● Excluded ● Included

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

The following table describes the labels in this screen

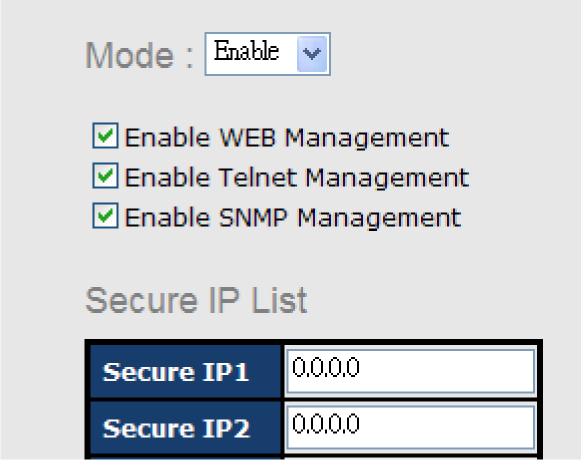
Label	Description
Context Table	Configure SNMP v3 context table. Assign the context name of context table. Click "Apply" to change context name
User Table	1. Configure SNMP v3 user table. 2. **User ID:** set up the user name. 3. **Authentication Password:** set up the authentication password. 4. **Privacy Password:** set up the private password. 5. Click "Add" to add context name. 6. Click "Remove" to remove unwanted context name.
Group Table	1. Configure SNMP v3 group table. 2. **Security Name (User ID):** assign the user name that you have set up in user table. 3. **Group Name:** set up the group name. 4. Click "Add" to add context name. 5. Click "Remove" to remove unwanted context name.
Access Table	1. Configure SNMP v3 access table. 2. **Context Prefix:** set up the context name. 3. **Group Name:** set up the group. 4. **Security Level:** select the access level. 5. **Context Match Rule:** select the context match rule. 6. **Read View Name:** set up the read view. 7. **Write View Name:** set up the write view. 8. **Notify View Name:** set up the notify view. 9. Click "Add" to add context name. 10. Click "Remove" to remove unwanted context name.
MIBview Table	1. Configure MIB view table. 2. **ViewName:** set up the name. 3. **Sub-Oid Tree:** fill the Sub OID. 4. **Type:** select the type – exclude or included. 5. Click "Add" to add context name. 6. Click "Remove" to remove unwanted context name.
Help	Show help file.

5.1.8 Security

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

5.1.8.1 Management Security

Only IP in the Secure IP List can manage the switch through your defined management mode. (WEB, Telnet, SNMP)



Mode : Enable

☑ Enable WEB Management
☑ Enable Telnet Management
☑ Enable SNMP Management

Secure IP List

Secure IP1	0.0.0.0
Secure IP2	0.0.0.0

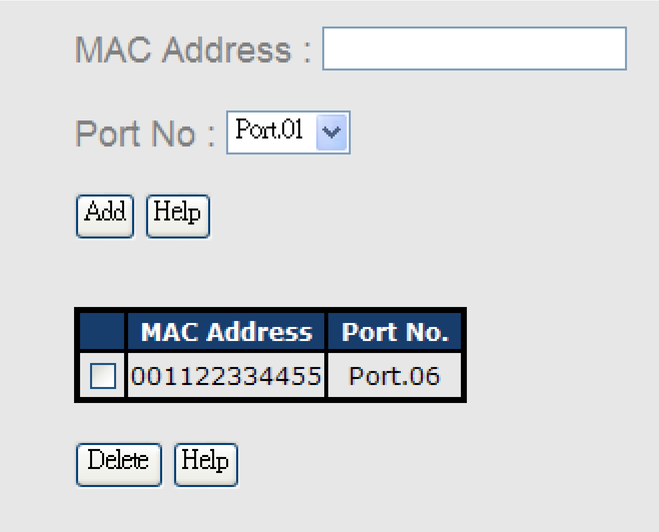
IP Security interface

The following table describes the labels in this screen.

Label	Description
IP security MODE	Enable/Disable the IP security function.
Enable WEB Management	Mark the blank to enable WEB Management.
Enable Telnet Management	Mark the blank to enable Telnet Management.
Enable SNMP Management	Mark the blank to enable MPSN Management.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.1.8.2 Static MAC Forwarding

Static MAC Forwarding 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.



MAC Address :

Port No : Port.01

	MAC Address	Port No.
□	001122334455	Port.06

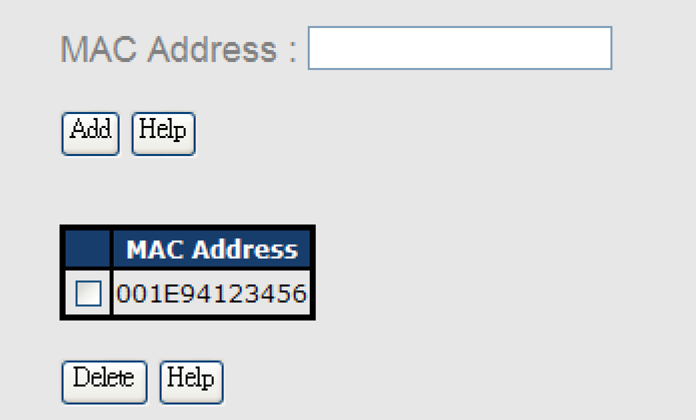
Port Security interface

The following table describes the labels in this screen.

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

5.1.8.3 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.



MAC Address :

	MAC Address
□	001E94123456

MAC Blacklist interface

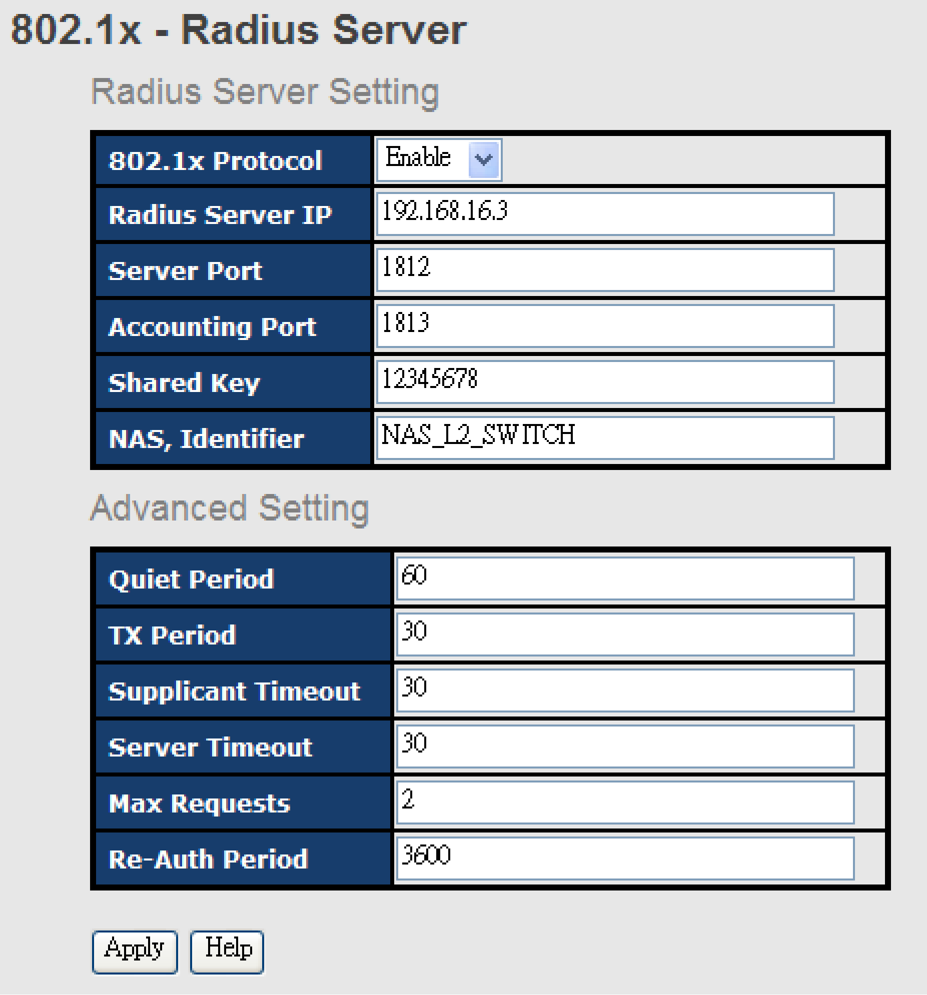
The following table describes the labels in this screen.

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

5.1.8.4 802.1x

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

Advanced Setting

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

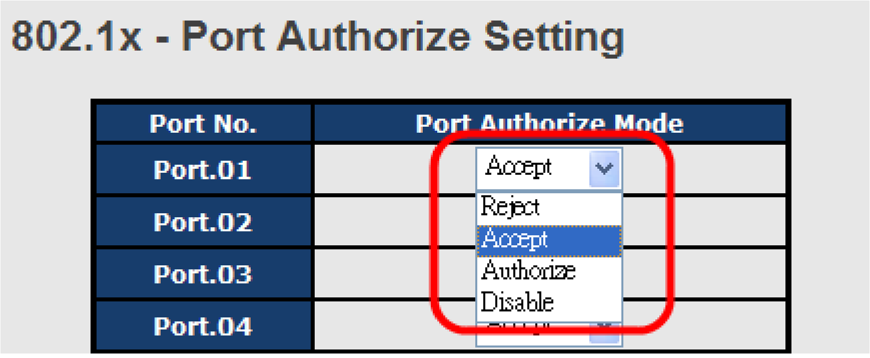
802.1x Radius Server interface

The following table describes the labels in this screen.

Label	Description
802.1x Portocol	Enable or Disable 802.1X Radius Server function .
Radius Server IP	The IP address of the authentication server.
Server port	Set the UDP port number used by the authentication server to authenticate.
Account port	Set the UDP destination port for accounting requests to the specified Radius Server.
Shared Key	A key shared between this switch and authentication server.
NAS, Identifier	A string used to identify this switch.
Advanced Setting	
Quiet Period	Set the time interval between authentication failure and the start of a new authentication attempt.
Tx Period	Set the time that the switch can wait for response to an EAP request/identity frame from the client before resending the request.
Supplicant Timeout	Set the period of time the switch waits for a supplicant response to an EAP request.
Server Timeout	Set the period of time the switch waits for a Radius server response to an authentication request.
Max Requests	Set the maximum number of times to retry sending packets to the supplicant.
Re-Auth Period	Set the period of time after which clients connected must be re-authenticated.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

802.1x-Port Authorized Mode

Set the 802.1x authorized mode of each port.



802.1x - Port Authorize Setting

Port No.	Port Authorize Mode
Port.01	Accept
Port.02	
Port.03	
Port.04	

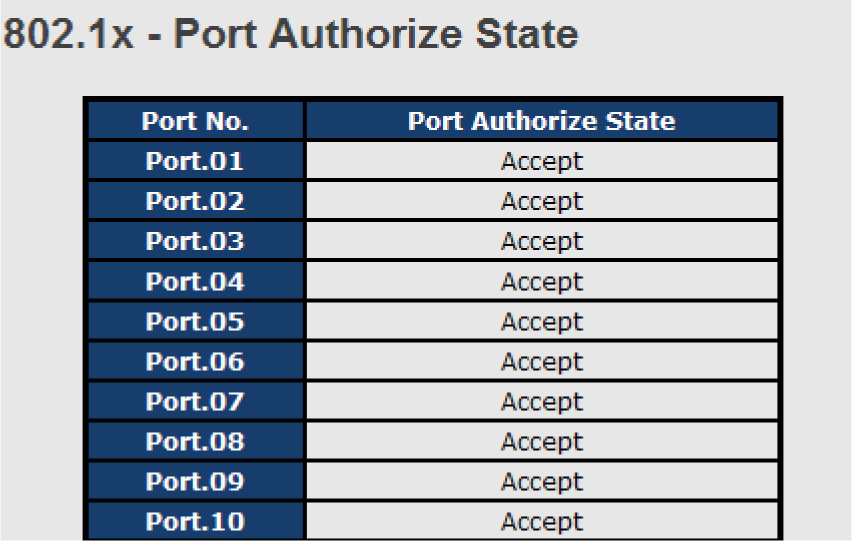
802.1x Port Authorize interface

The following table describes the labels in this screen.

Label	Description
Port Authorized Mode	■ **Reject:** force this port to be unauthorized. ■ **Accept:** force this port to be authorized. ■ **Authorize:** the state of this port was determined by the outcome of the 802.1x authentication. ■ **Disable:** this port will not participate in 802.1x.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

802.1x-Port Authorized Mode

Show 802.1x port authorized state.



802.1x - Port Authorize State

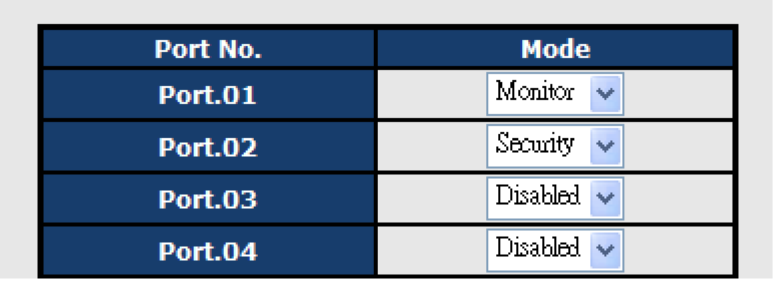
Port No.	Port Authorize State
Port.01	Accept
Port.02	Accept
Port.03	Accept
Port.04	Accept
Port.05	Accept
Port.06	Accept
Port.07	Accept
Port.08	Accept
Port.09	Accept
Port.10	Accept

802.1x Port Authorize State interface

5.1.8.5 IP Guard

IP Guard – Port Setting

This page allows you to configure port configuration of IP Guard. IP Guard is an intelligent and easy use function for IP security. It could protect the network from unknown IP(the IP not in allowed list) attack. The illegal IP traffic will be blocked.



Port No.	Mode
Port.01	Monitor
Port.02	Security
Port.03	Disabled
Port.04	Disabled

IP Guard – Port Setting State interface

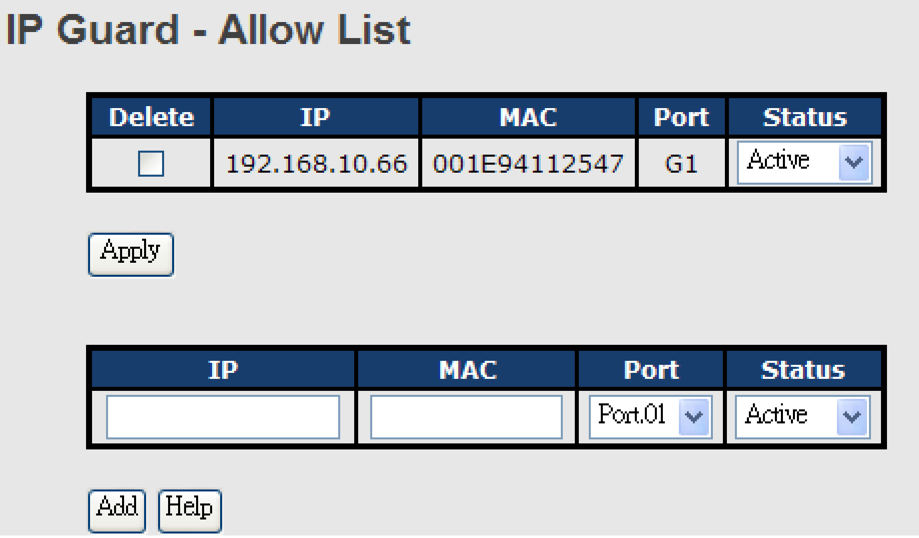
The following table describes the labels in this screen.

Label	Description
Mode	■ **Disable mode: function is totally disabled.** ■ **Monitor mode: function is disabled, but keeps monitor the IP traffic.** ■ **Security mode: function is enabled, the illegal IP taffic will be blocked.**
Apply	Click “**Apply**” to set the configurations.
Help	Show help file.

IP Guard – Allow List

IP Guard is an intelligent and easy use function for IP security. It could protect the network from unknown IP(the IP not in allowed list) attack. The illegal IP traffic will be blocked.

This page allows you to configure IP Guard allowed list. The IP traffic will be blocked, if it was not in allowed list



IP Guard - Allow List

Delete	IP	MAC	Port	Status
□	192.168.10.66	001E94112547	G1	Active

IP	MAC	Port	Status
		Port.01	Active

IP Guard – Allow List State interface

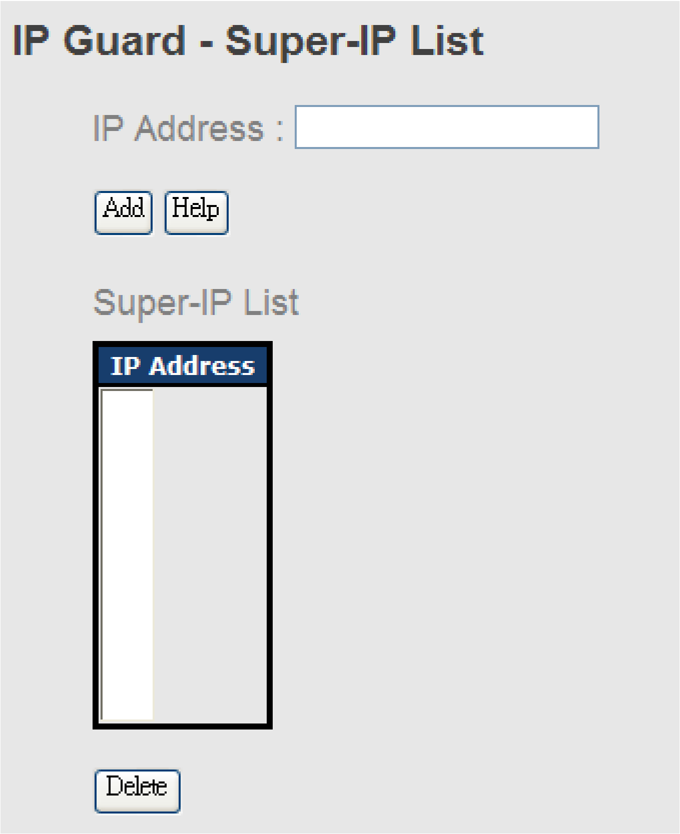
The following table describes the labels in this screen.

Label	Description
IP	IP address of the allowed entry.
MAC	MAC address of the allowed entry.
Port	Port number of the allowed entry.
Status	If you doubt some allowed IP traffic are abnormal, you could block the traffic use this field. Active: Allow the IP traffic. Suspend: Block the IP traffic.
Delete	If you want to delete the entry, please check this box and apply it.

IP Guard – Super-IP List

IP Guard is an intelligent and easy use function for IP security. It could protect the network from unknown IP(the IP not in allowed list) attack. The illegal IP traffic will be blocked.

This page allows you to configure IP Guard Super-IP list. Super-IP entry has a special priority, the IP has no limited of MAC address and port binding. Any IP traffic are allowed, when the IP is in the Super-IP list.


IP Guard - Super-IP List

IP Address :

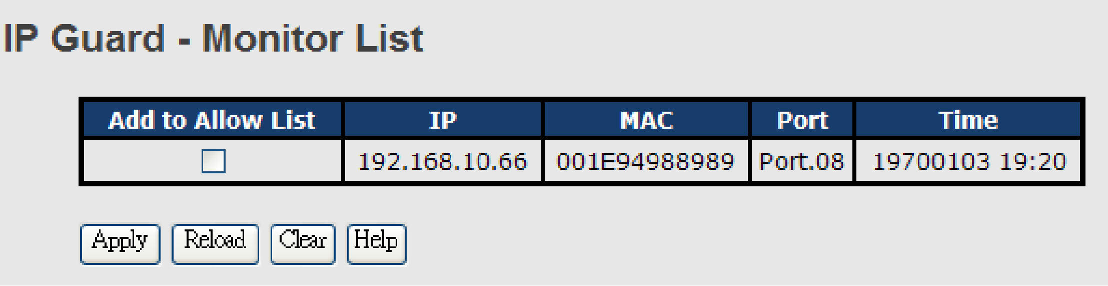
Super-IP List

IP Address

IP Guard – Super-IP List State interface

IP Guard – Super-IP List

IP Guard is an intelligent and easy use function for IP security. It could protect the network from unknown IP(the IP not in allowed list) attack. The illegal IP traffic will be blocked.



IP Guard - Monitor List

Add to Allow List	IP	MAC	Port	Time
□	192.168.10.66	001E94988989	Port.08	19700103 19:20

The following table describes the labels in this screen.

Label	Description
IP	IP address of entry.
MAC	MAC address of entry.
Port	Port number of entry.
Time	The logged time .
Add to Allow List	If you want to allow the IP traffic, please check this box and apply it.

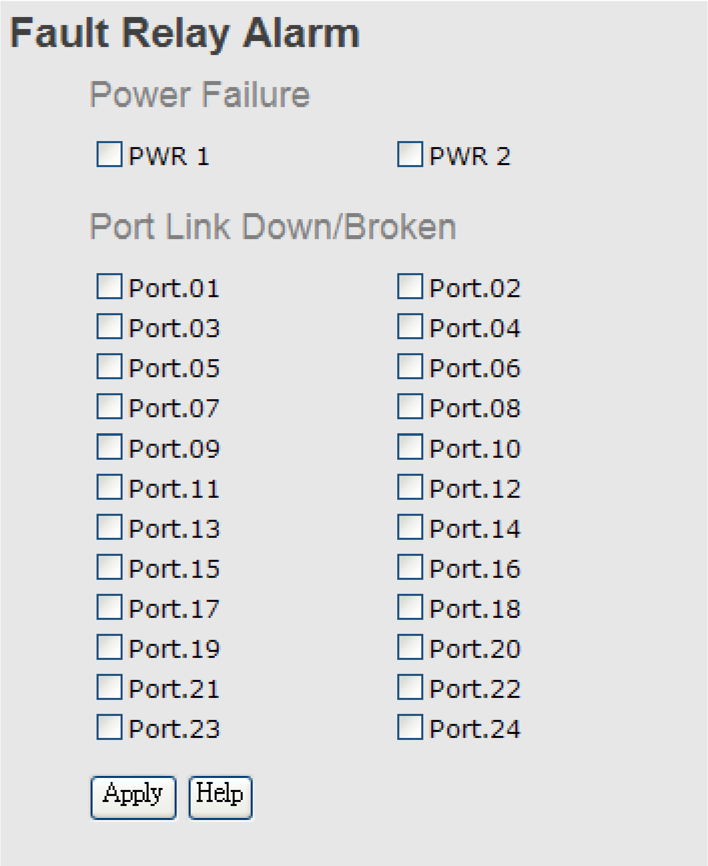
5.1.9 Warning

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.

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

Warning – Fault Relay 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 Relay Alarm

Power Failure

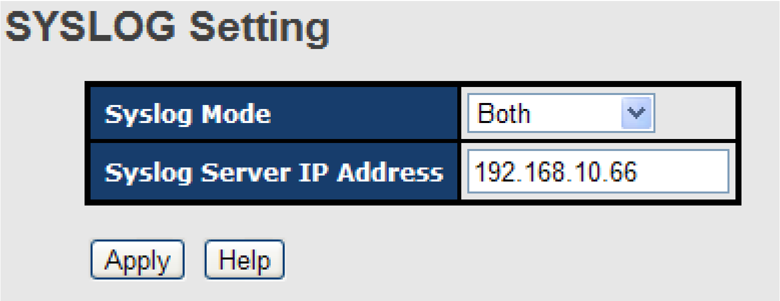
□ PWR 1 □ PWR 2

Port Link Down/Broken

□ Port.01	□ Port.02
□ Port.03	□ Port.04
□ Port.05	□ Port.06
□ Port.07	□ Port.08
□ Port.09	□ Port.10
□ Port.11	□ Port.12
□ Port.13	□ Port.14
□ Port.15	□ Port.16
□ Port.17	□ Port.18
□ Port.19	□ Port.20
□ Port.21	□ Port.22
□ Port.23	□ Port.24

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



SYSLOG Setting

Syslog Mode	Both
Syslog Server IP Address	192.168.10.66

System Warning – SYSLOG Setting interface

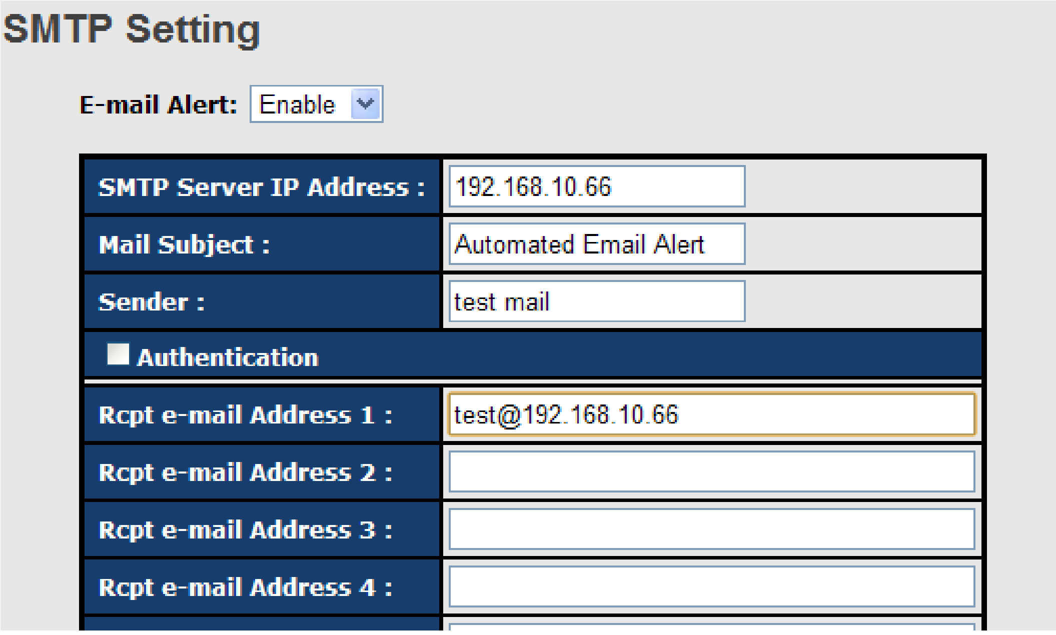
The following table describes the labels in this screen.

Label	Description
SYSLOG Mode	■ **Disable:** disable SYSLOG. ■ **Client Only:** log to local system. ■ **Server Only:** log to a remote SYSLOG server.

	■ **Both:** log to both of local and remote server.
SYSLOG Server IP Address	The remote SYSLOG Server IP address.
Apply	Click "**Apply**" to set the configurations.
Help	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.



SMTP Setting

E-mail Alert: Enable

SMTP Server IP Address :	192.168.10.66
Mail Subject :	Automated Email Alert
Sender :	test mail
□ Authentication	
Rcpt e-mail Address 1 :	test@192.168.10.66
Rcpt e-mail Address 2 :	
Rcpt e-mail Address 3 :	
Rcpt e-mail Address 4 :	

System Warning – SMTP Setting interface

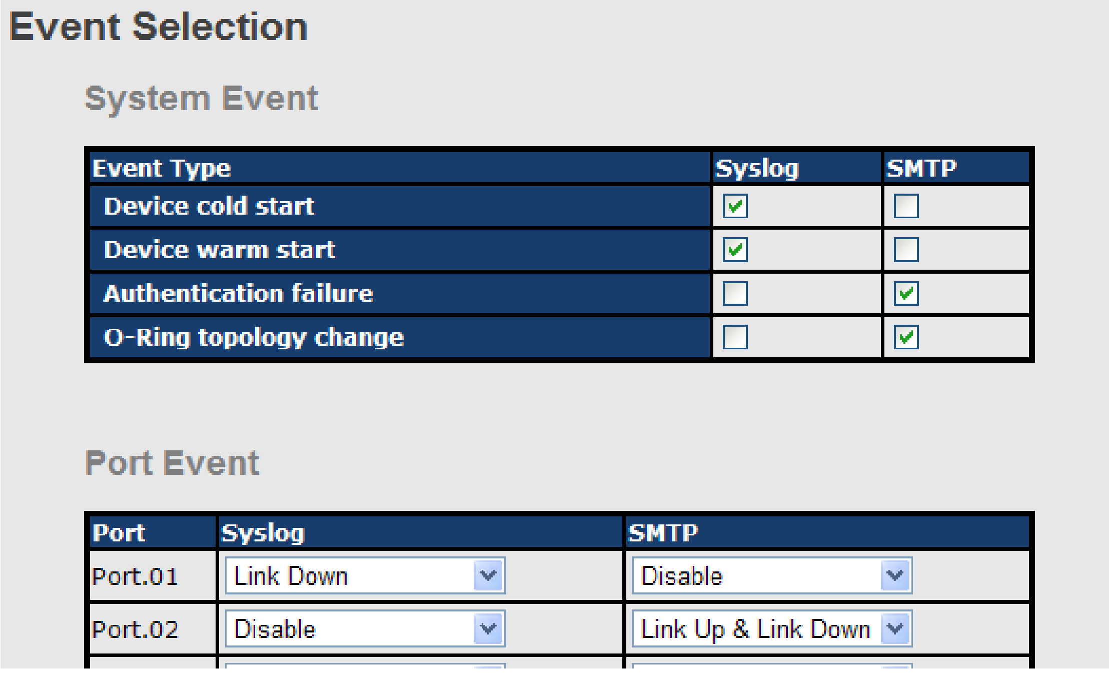
The following table describes the labels in this screen.

Label	Description
E-mail Alart	Enable/Disable transmission system warning events by e-mail.
SMTP Server IP Address	Setting up the mail server IP address
Mail Subject	The Subject of the mail
Sender	Set up the email account to send the alert.
Authentication	■ **Username:** the authentication username. ■ **Password:** the authentication password. ■ **Confirm Password:** re-enter password.

Recipient E-mail Address	The recipient's E-mail address. It supports 6 recipients for a mail.
Apply	Click "**Apply**" to set the configurations.
Help	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.



Event Selection

System Event

Event Type	Syslog	SMTP
Device cold start	☑	□
Device warm start	☑	□
Authentication failure	□	☑
O-Ring topology change	□	☑

Port Event

Port	Syslog	SMTP
Port.01	Link Down	Disable
Port.02	Disable	Link Up & Link Down

System Warning – Event Selection interface

The following table describes the labels in this screen.

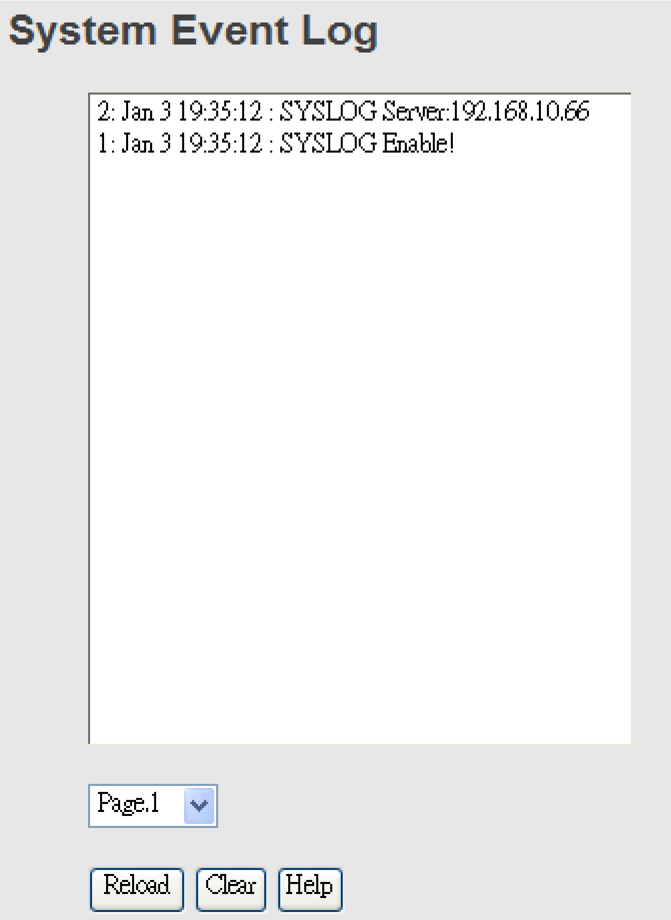
Label	Description
Device cold start	When the device executes cold start, the system will issue a log event.
Device warm start	When the device executes warm start, the system will issue a log event.
Authentication Failure	Alert when SNMP authentication failure.
O-Ring topology change	Alert when O-Ring topology changes.
Port Event	■ **Disable** ■ **Link Up**

	■ **Link Down** ■ **Link Up & Link Down**
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.1.10 Monitor and Diag

5.1.10.1 System Event Log

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


System Event Log

```
2: Jan 3 19:35:12 : SYSLOG Server:192.168.10.66
1: Jan 3 19:35:12 : SYSLOG Enable!
```

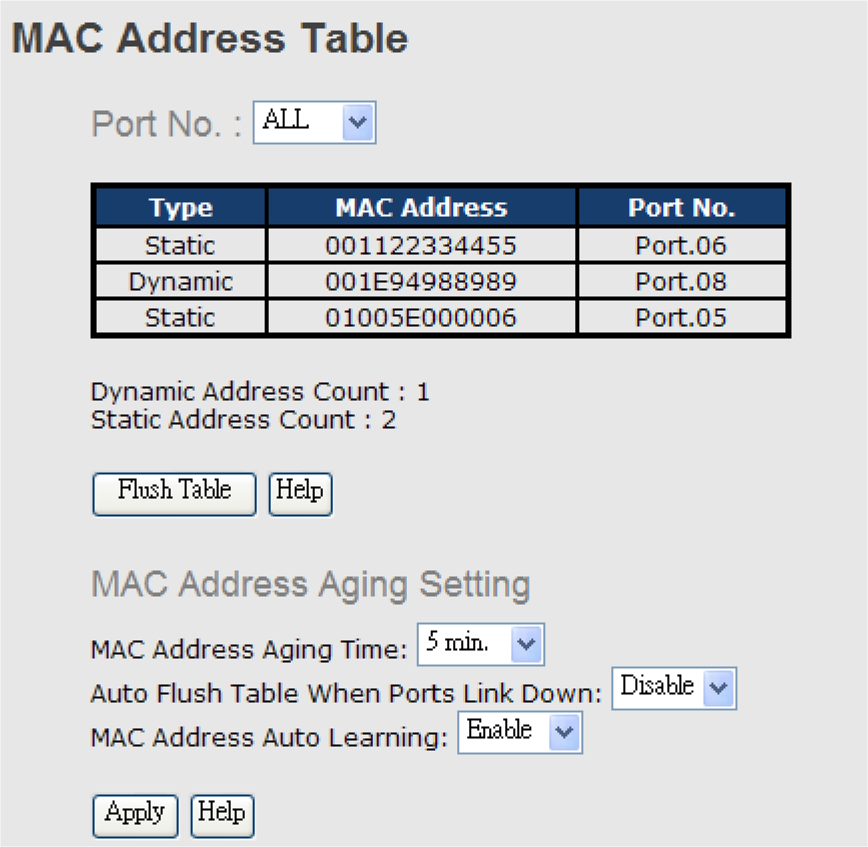
System event log interface

The following table describes the labels in this screen.

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

5.1.10.2 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.



MAC Address Table

Port No. : ALL

Type	MAC Address	Port No.
Static	001122334455	Port.06
Dynamic	001E94988989	Port.08
Static	01005E000006	Port.05

Dynamic Address Count : 1
Static Address Count : 2

MAC Address Aging Setting

MAC Address Aging Time: 5 min.
Auto Flush Table When Ports Link Down: Disable
MAC Address Auto Learning: Enable

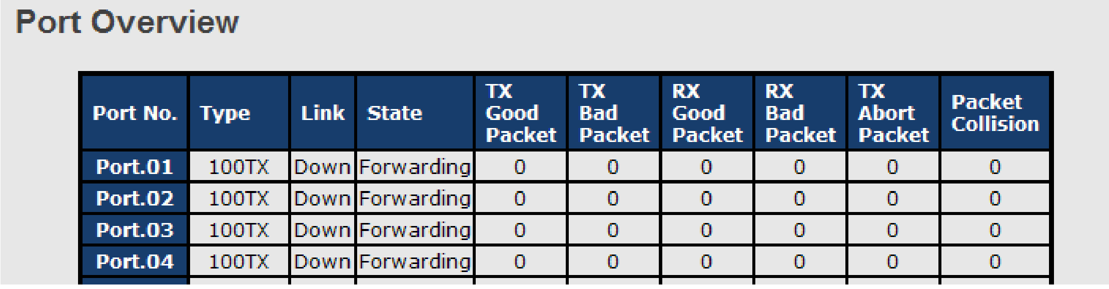
MAC Address Table interface

The following table describes the labels in this screen.

Label	Description
Port NO. :	Show all MAC addresses mapping to a selected port in table.
Flush MAC Table	Clear all MAC addresses in table
MAC Address Aging Time	Assign aging time MUST be multiple of 15.
Auto Flush Table When Ports Link Down	Enable this function , when port link down , switch will Flush MAC table.
MAC Address Auto Learning	Enable or Disable MAC Learning function .
Apply	Click “Apply” to set the configurations.

5.1.10.3 Port Overview

Port statistics show several statistics counters for all ports



Port Overview

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

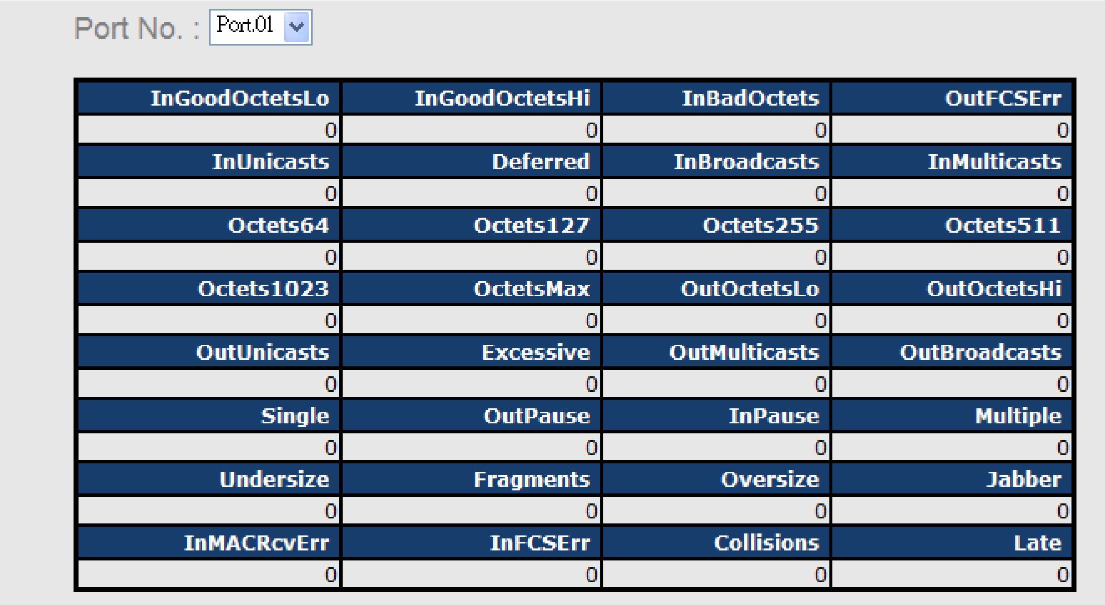
Port Overview interface

The following table describes the labels in this screen.

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

5.1.10.4 Port Counters

This page shows statistic counters for the port. The "Clear" button is to reset all counters to zero for all ports.



Port No. : Port.01

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

Port Counters interface

The following table describes the labels in this screen.

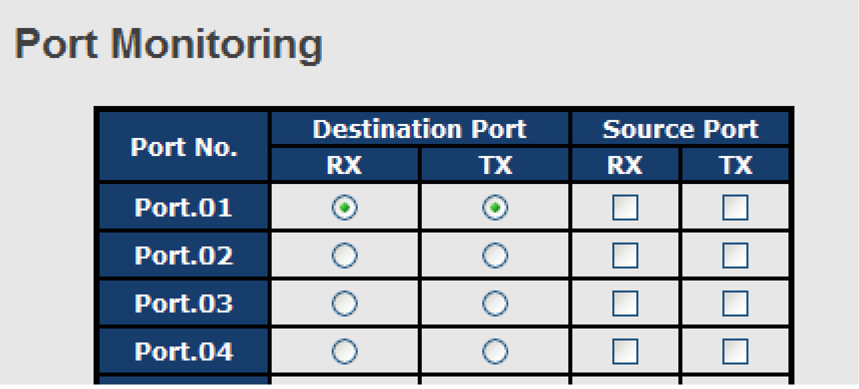
Label	Description
InGoodOctetsLo	The lower 32-bits of the 64-bit InGoodOctets counter. The sum of lengths of all good Ethernet frames received, that is frames that are not bad frames.
InGoodOctetsHi	The upper 32-bits of the 64-bit InGoodOctets counter. The sum of lengths of all good Ethernet frames received, that is frames that are not bad frames.
InBadOctets	The sum of lengths of all bad Ethernet frames received.
OutFCSErr	The number of frames transmitted with a invalid FCS. Whenever a frame is modified during transmission(e.g., to add or remove a tag) the frames's original FCS is inspected before a new FCS is added to a modified frame. If the original FCS is invalid, the new FCS is made invalid too and this counter is incremented.
InUnicasts	The number of good frames received that have a Unicast destination MAC address.
Deferred	The total number of successfully transmitted frames that experienced no collisions bu are delayed because the medium was busy during the first attempt. This counter is applicable in

	half-duplex only.
InBroadcasts	The number of good frames received that have a Broadcast destination MAC address.
InMulticasts	The number of good frames received that have a Multicast destnation MAC address.
Octets64	Total frames received (and/or transmitted) with a length of exactly 64 octes, include those with errors.
Octets127	Total frames received (and/or transmitted) with a length of between 65 and 127 octes in clusive, including those with error.
Octets255	Total frames received (and/or transmitted) with a length of between 128 and 255 octes in clusive, including those with error.
Octets511	Total frames received (and/or transmitted) with a length of between 256 and 511 octes in clusive, including those with error.
Octets1023	Total frames received (and/or transmitted) with a length of between 512 and 1023 octes in clusive, including those with error.
OctetsMax	Total frames received (and/or transmitted) with a length of between 1024 and MaxSize octes in clusive, including those with error.
OutOctetsLo	The lower 32-bit of the 64-bit OutOctets counter. The sum of lengths of all Ethernet frames sent from this MAC.
OutOctetsHi	The upper 32-bit of the 64-bit OutOctets counter. The sum of lengths of all Ethernet frames sent from this MAC.
OutUnicasts	The number of frames sent that have an Unicast destination MAC address.
Excessive	The number frames dropped in the transmit MAC because the frame experienced 16 consecutive collisions. This counter is applicable in half-duplex only and only of DiscardExcessive is one.
OutBroadcasts	The number of good frames sent that have a Broadcast destination MAC address.
Single	The total number of successfully transmitted frames that experienced exactly one collision. This counter is applicable in half-duplex only.
OutPause	The number of good Flow Control frames sent.
InPause	The number of good Flow Control frames received.
Multiple	The total number of successfully transmitted frames that experienced more than one collision. This counter is applicable in

	half-duplex only.
Undersize	Total frames received with a length of less than 64 octets but with a valid FCS.
Fragments	Total frames received with a length of more than 64 octets and with a invalid FCS.
Oversize	Total frames received with a length of more than MaxSize octets but with a valid FCS.
Jabber	Total frames received with a length of more than MaxSize octets but with an invalid FCS.
InMACRcvErr	Total frames received with an RxErr signal from the PHY.
InFCSErr	Total frames received with a CRC error not counted in Fragments, Jabber or RxErr.
Collisions	The number of collision events seen by MAC not including those conted in Single, Multiple, Excessive or Late. This counter is applicable in half-duplex only.
Late	The number of times a collision is detected later than 512 bits-times into the transmission of a frame. This counter is applicable in half-duplex only.

5.1.10.5 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 No.	Destination Port		Source Port	
	RX	TX	RX	TX
Port.01	◉	◉	□	□
Port.02	○	○	□	□
Port.03	○	○	□	□
Port.04	○	○	□	□

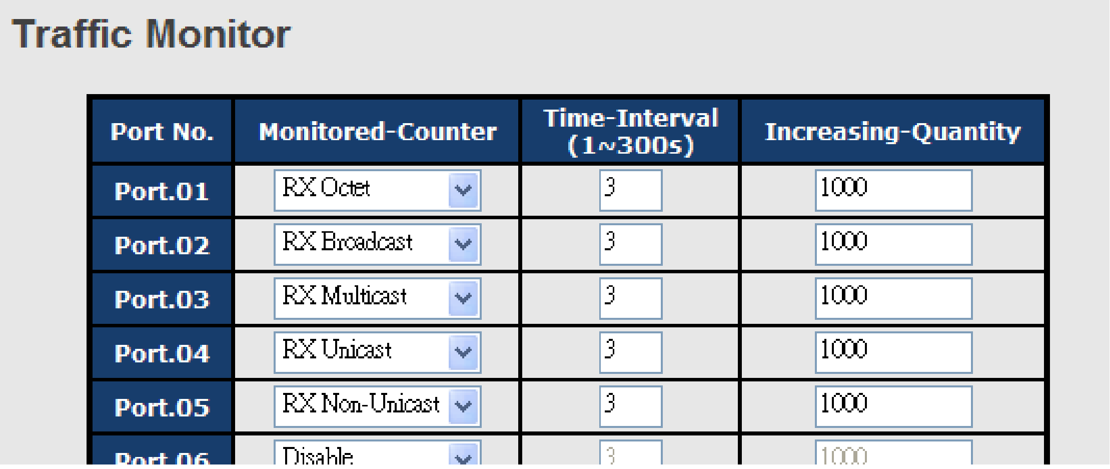
Port monitoring interface

The following table describes the labels in this screen.

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

5.1.10.6 Traffic Monitor

The function can monitor switch Traffic. If traffic is too large, Switch will sent SYSLOG Event or SMTP Mail . .



Traffic Monitor

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

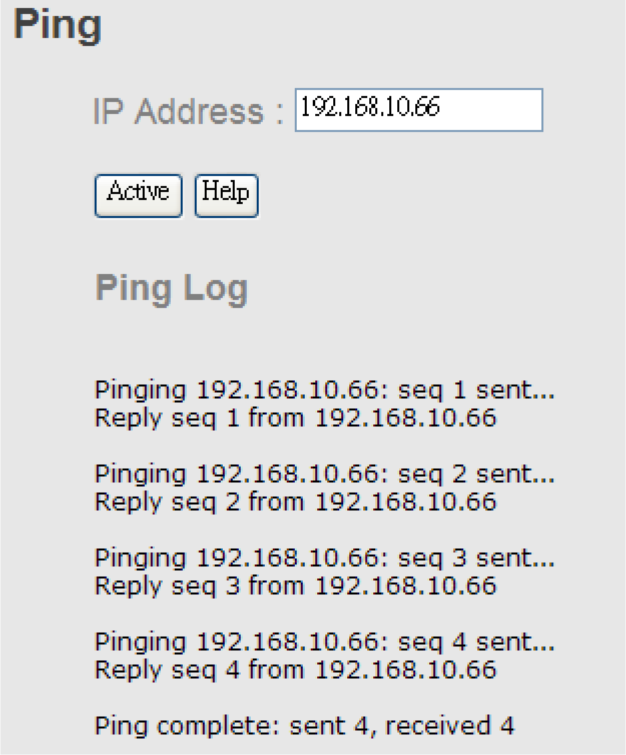
System event log interface

The following table describes the labels in this screen.

Label	Description
Monitored –Counter	Select monitor type .
Time-Interval	Setting Interval time .
Increasing – Quantity	Setting alarm Quantity
Event Alarm	Select alarm function (SYSLOG or SMTP)

5.1.10.7 Ping

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



IP Address : 192.168.10.66

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

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

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

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

Ping complete: sent 4, received 4
```

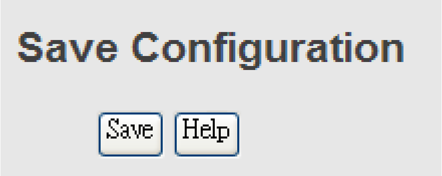
Ping interface

The following table describes the labels in this screen.

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

5.1.11 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.

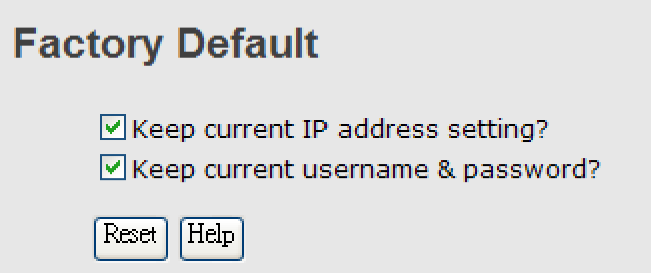


System Configuration interface

The following table describes the labels in this screen.

Label	Description
Save	Save all configurations.
Help	Show help file.

5.1.12 Factory Default



Factory Default

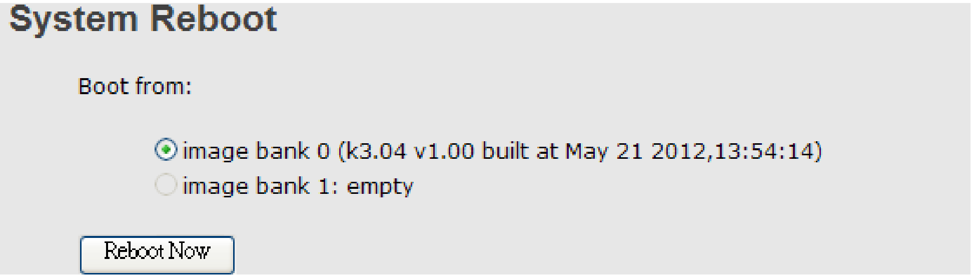
☑ Keep current IP address setting?

☑ Keep current username & password?

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.

5.1.13 System Reboot



System Reboot

Boot from:

● image bank 0 (k3.04 v1.00 built at May 21 2012,13:54:14)

○ image bank 1: empty

System Reboot interface

Command Line Interface Management

6.1 About CLI Management

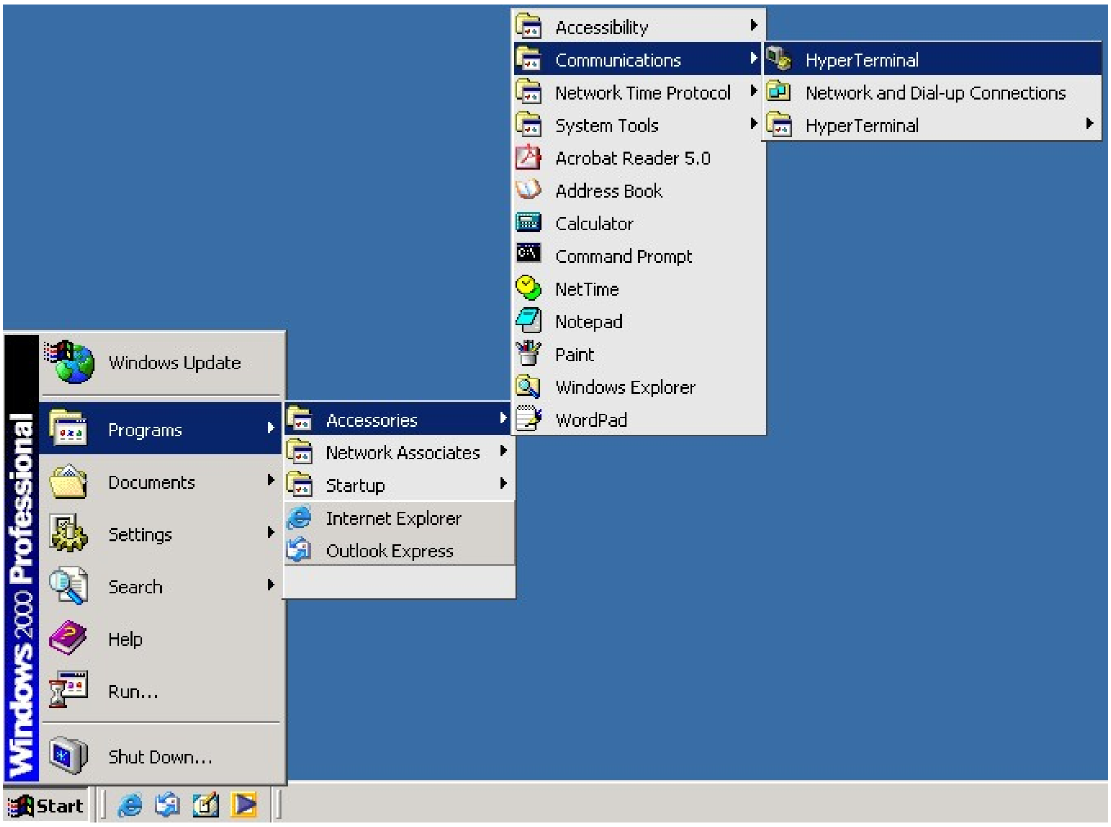
Besides WEB-based management, IES-3240 also supports CLI management. You can use console or telnet to management switch by CLI.

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

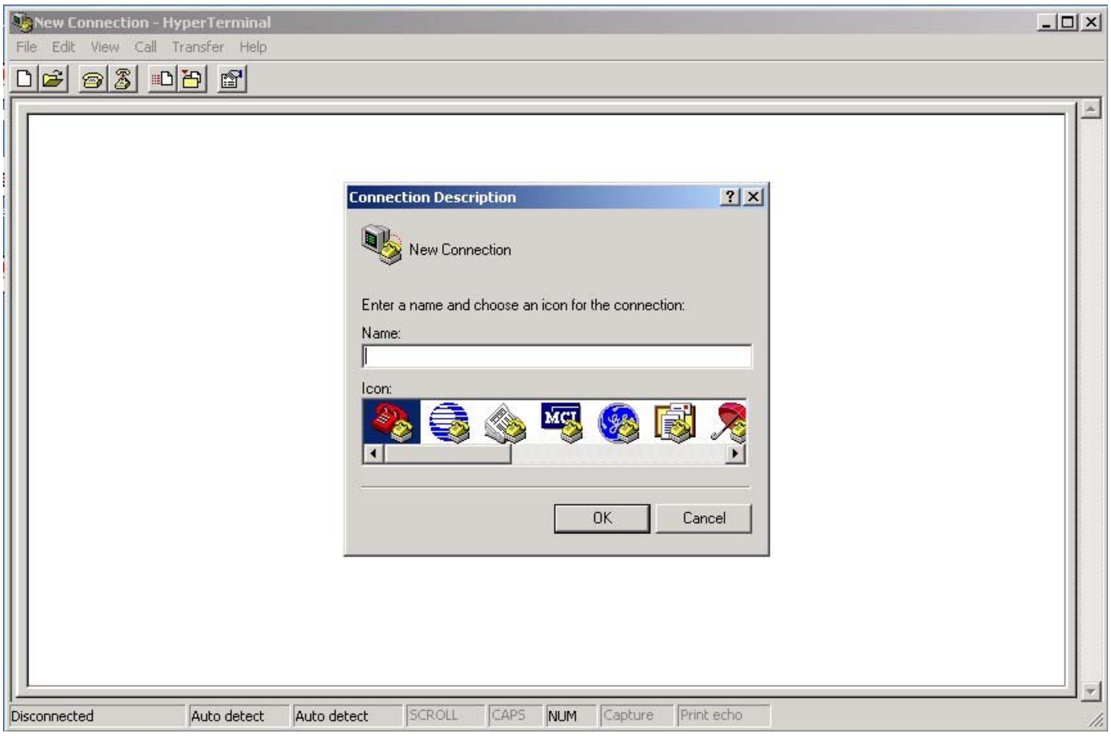
Before Configuring by RS-232 serial console, use an RJ45 to DB9-F cable to connect the Switches' RS-232 Console port to your PCs' COM port.

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



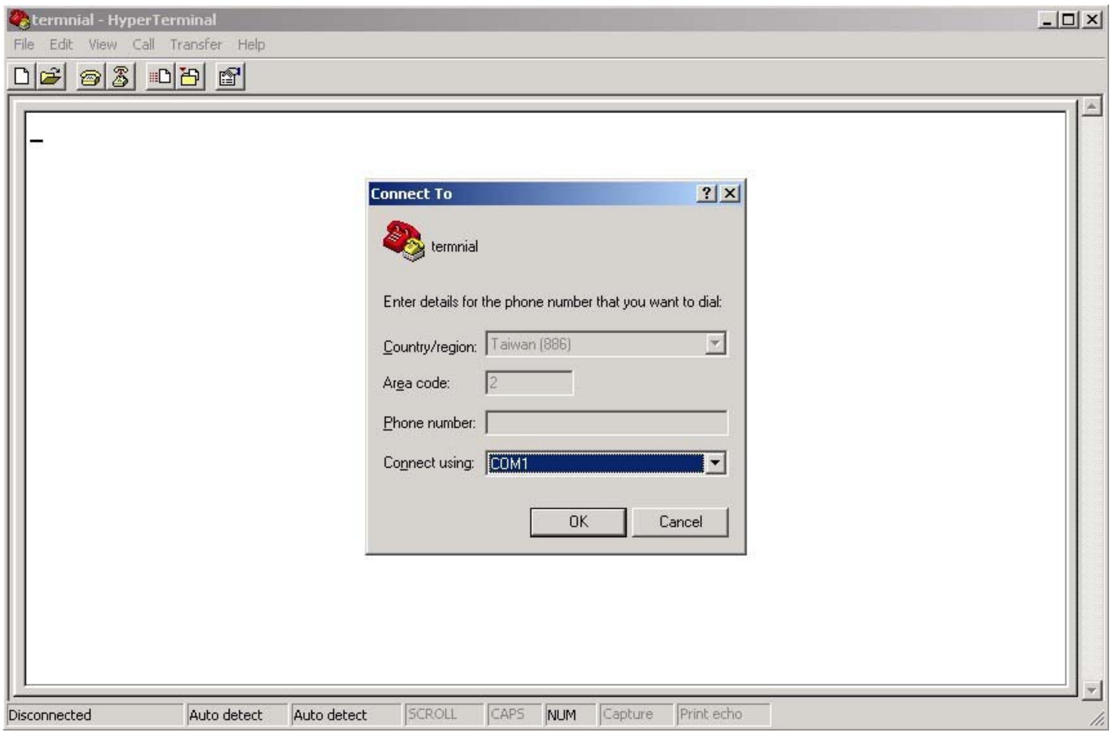
New Connection

Enter a name and choose an icon for the connection:

Name:

Icon:

Step 3. Select to use COM port number



termnial

Enter details for the phone number that you want to dial:

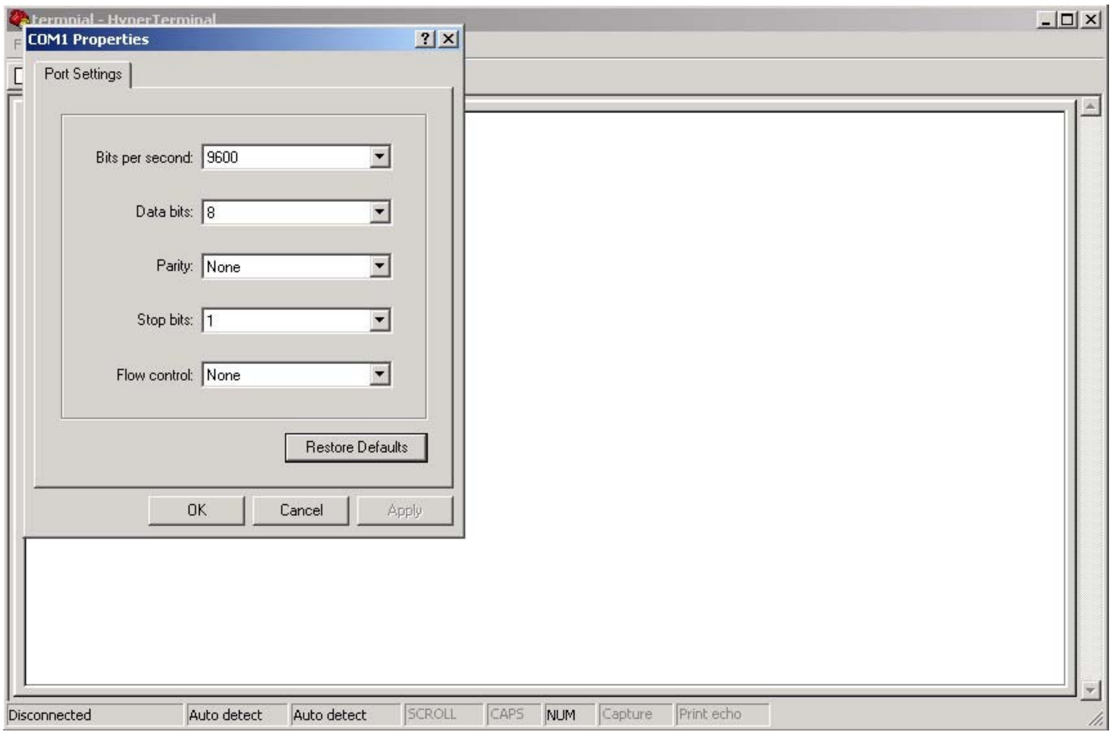
Country/region: Taiwan (886)

Area code: 2

Phone number:

Connect using: COM1

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.



COM1 Properties

Port Settings

Bits per second: 9600

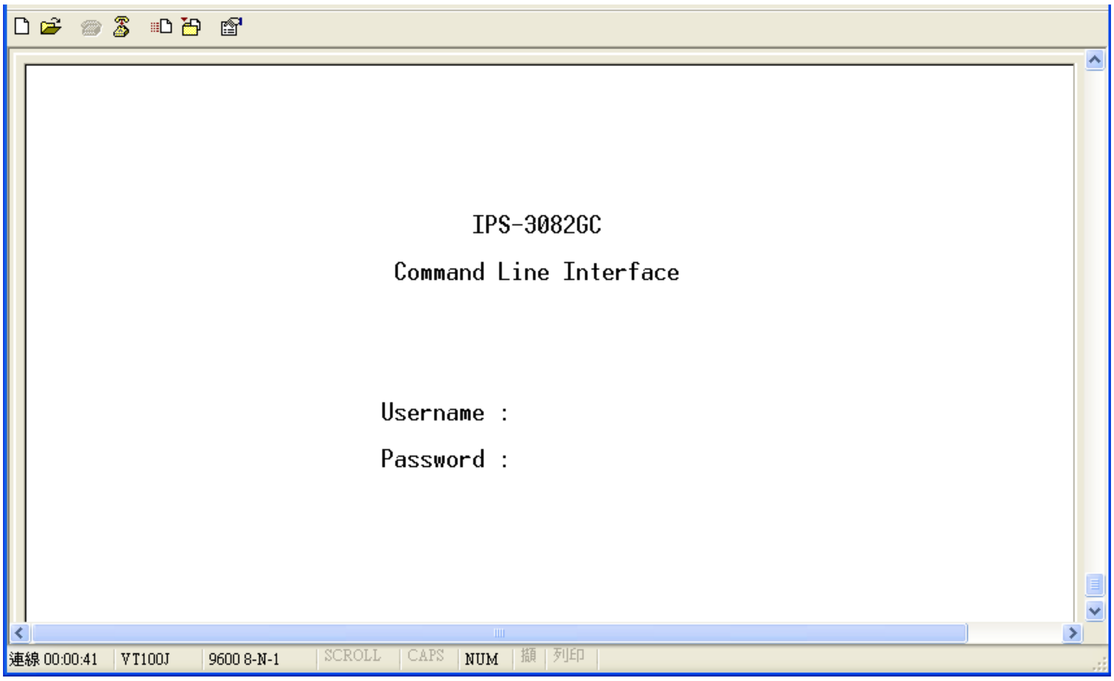
Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

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**”.



```
IPS-3082GC
Command Line Interface

Username :
Password :
```

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**

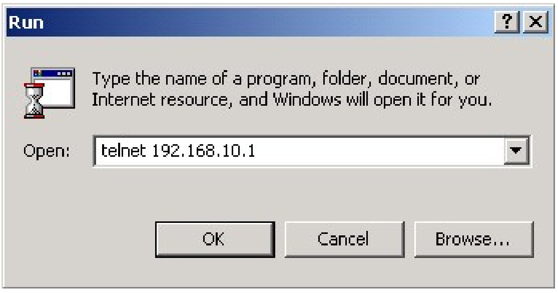
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

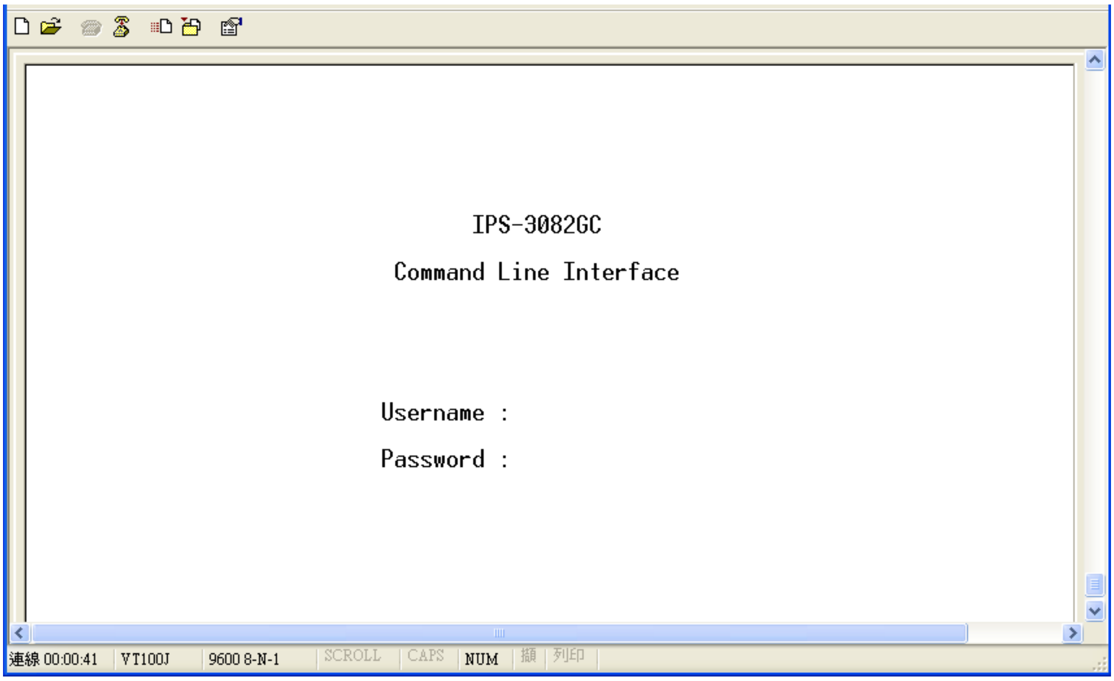
Follow the steps below to access the console via Telnet.

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


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

```
telnet 192.168.10.1
```

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**"



```
IPS-3082GC
Command Line Interface


Username :
Password :
```

Commands Level

Modes	**Access Method**	**Prompt**	**Exit Method**	**About This Model**
User EXEC	Begin a session with your switch.	switch>	Enter **logout** or **quit**.	The user command available at the level of user is the subset of those available at the privileged level. Use this mode to • Enter menu mode. • Display system information.
Privileged EXEC	Enter the **enable** command while in user EXEC mode.	switch#	Enter **disable** to exit.	The privileged command is advance mode Privileged this mode to • Display advance function status • save configures
Global configuration	Enter the **configure** command while in privileged EXEC mode.	switch(config)#	To exit to privileged EXEC mode, enter **exit** or **end**	Use this mode to configure parameters that apply to your Switch as a whole.
VLAN database	Enter the **vlan database** command while in privileged EXEC mode.	switch(vlan)#	To exit to user EXEC mode, enter **exit**.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the **interface** command (with a specific interface)while in global configuration mode	switch(config-if)#	To exit to global configuration mode, enter **exit.** To exist privileged EXEC mode or **end.**	Use this mode to configure parameters for the switch and Ethernet ports.

Symbol of Command Level.

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

6.2 Commands Set List—System Commands Set

IES-3240 Commands	Level	Description	Example
show config	**E**	Show switch configuration	switch>show config
show terminal	**P**	Show console information	switch#show terminal
write memory	**P**	Save your configuration into permanent memory (flash rom)	switch#write memory
system name **[System Name]**	**G**	Configure system name	switch(config)#system name xxx
system location **[System Location]**	**G**	Set switch system location string	switch(config)#system location xxx
system description **[System Description]**	**G**	Set switch system description string	switch(config)#system description xxx
system contact **[System Contact]**	**G**	Set switch system contact window string	switch(config)#system contact xxx
show system-info	**E**	Show system information	switch>show system-info
ip address **[Ip-address]** **[Subnet-mask]** **[Gateway]**	**G**	Configure the IP address of switch	switch(config)#ip address 192.168.1.1 255.255.255.0 192.168.1.254
ip dhcp	**G**	Enable DHCP client function of switch	switch(config)#ip dhcp

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

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

6.3 Commands Set List—Port Commands Set

IES-3240 Commands	Level	Description	Example
interface fastEthernet **[Portid]**	G	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex **[full | half]**	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
speed **[10|100|1000|auto]**	I	Use the speed configuration command to specify the speed mode of operation for Fast	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..	
flowcontrol mode **[Symmetric|Asymmetric]**	I	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion.	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol mode Asymmetric
no flowcontrol	I	Disable flow control of interface	switch(config-if)#no flowcontrol
security enable	I	Enable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#security enable
no security	I	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
bandwidth type all	I	Set interface ingress limit frame type to "accept all frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to "accept broadcast, multicast, and flooded unicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to "accept broadcast and multicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast
bandwidth type broadcast-only	I	Set interface ingress limit frame type to "only accept broadcast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only
bandwidth in **[Value]**	I	Set interface input bandwidth. Rate Range is from 100	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth in 100

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

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

6.4 Commands Set List—Trunk command set

IES-3240 Commands	Level	Description	Example
aggregator priority **[1to65535]**	G	Set port group system priority	switch(config)#aggregator priority 22
aggregator activityport **[Port Numbers]**	G	Set activity port	switch(config)#aggregator activityport 2
aggregator group **[GroupID] [Port-list]** **lacp** **workp** **[Workport]**	G	Assign a trunk group with LACP active. [GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	switch(config)#aggregator group 1 1-4 lacp workp 2 or switch(config)#aggregator group 2 1,4,3 lacp workp 3
aggregator group **[GroupID] [Port-list]** **nolacp**	G	Assign a static trunk group. [GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#aggregator group 1 2-4 nolacp or switch(config)#aggreator group 1 3,1,2 nolacp

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

6.5 Commands Set List—VLAN command set

IES-3240 Commands	**Level**	**Description**	**Example**
vlan database	**P**	Enter VLAN configure mode	switch#vlan database
vlan **[8021q | gvrp]**	**V**	To set switch VLAN mode.	switch(vlan)# vlanmode 802.1q or switch(vlan)# vlanmode gvrp
no vlan **[VID]**	**V**	Disable vlan group(by VID)	switch(vlan)#no vlan 2
no gvrp	**V**	Disable GVRP	switch(vlan)#no gvrp
IEEE 802.1Q VLAN			
vlan 8021q port **[PortNumber]** **access-link untag** **[UntaggedVID]**	**V**	Assign a access link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 802.1q port 3 access-link untag 33
vlan 8021q port **[PortNumber]** **trunk-link tag** **[TaggedVID List]**	**V**	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 8021q port 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q port 3 trunk-link tag 3-20
vlan 8021q port **[PortNumber]** **hybrid-link untag** **[UntaggedVID]** **tag** **[TaggedVID List]**	**V**	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)# vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q port 3 hybrid-link untag 5 tag 6-8
vlan 8021q aggreator **[TrunkID]**	**V**	Assign a access link for VLAN by trunk	switch(vlan)#vlan 8021q aggreator 3 access-link untag 33

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

6.6 Commands Set List—Spanning Tree command set

IES-3240 Commands	Level	Description	Example
spanning-tree enable	**G**	Enable spanning tree	switch(config)#spanning-tree enable
spanning-tree priority **[0to61440]**	**G**	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
spanning-tree max-age **[seconds]**	**G**	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message	switch(config)# spanning-tree max-age 15

		from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	
spanning-tree hello-time **[seconds]**	**G**	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
spanning-tree forward-time **[seconds]**	**G**	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)# spanning-tree forward-time 20
stp-path-cost **[1to200000000]**	**I**	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop,	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.	
stp-path-priority **[Port Priority]**	**I**	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-path-priority 127
stp-admin-p2p **[Auto|True|False]**	**I**	Admin P2P of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-p2p Auto
stp-admin-edge **[True|False]**	**I**	Admin Edge of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-edge True
stp-admin-non-stp **[True|False]**	**I**	Admin NonSTP of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-non-stp False
Show spanning-tree	**E**	Display a summary of the spanning-tree states.	switch>show spanning-tree
no spanning-tree	**G**	Disable spanning-tree.	switch(config)#no spanning-tree

6.7 Commands Set List—QoS command set

IES-3240 Commands	Level	Description	Example
qos policy **[weighted-fair|strict]**	G	Select QOS policy scheduling	switch(config)#qos policy weighted-fair
qos prioritytype **[port-based|cos-only|tos-only|cos-first|tos-first]**	G	Setting of QOS priority type	switch(config)#qos prioritytype
qos priority portbased **[Port]** **[lowest|low|middle|high]**	G	Configure Port-based Priority	switch(config)#qos priority portbased 1 low
qos priority cos **[Priority][lowest|low|middle|high]**	G	Configure COS Priority	switch(config)#qos priority cos 22 middle
qos priority tos **[Priority][lowest|low|middle|high]**	G	Configure TOS Priority	switch(config)#qos priority tos 3 high
show qos	P	Display the information of QoS configuration	switch>show qos
no qos	G	Disable QoS function	switch(config)#no qos

6.8 Commands Set List—IGMP command set

IES-3240 Commands	Level	Description	Example
igmp enable	G	Enable IGMP snooping function	switch(config)#igmp enable
Igmp-query auto	G	Set IGMP query to auto mode	switch(config)#Igmp-query auto
Igmp-query force	G	Set IGMP query to force mode	switch(config)#Igmp-query force
show igmp configuration	P	Displays the details of an IGMP configuration.	switch#show igmp configuration
show igmp multi	P	Displays the details of an IGMP snooping entries.	switch#show igmp multi
no igmp	G	Disable IGMP	switch(config)#no igmp

		snooping function	
no igmp-query	G	Disable IGMP query	switch#no igmp-query

6.9 Commands Set List—MAC/Filter Table command set

IES-3240 Commands	Level	Description	Example
mac-address-table static hwaddr **[MAC]**	I	Configure MAC address table of interface (static).	switch(config)#interface fastEthernet 2 switch(config-if)#mac-address-table static hwaddr 000012345678
mac-address-table filter hwaddr **[MAC]**	G	Configure MAC address table(filter)	switch(config)#mac-address-table filter hwaddr 000012348678
show mac-address-table	P	Show all MAC address table	switch#show mac-address-table
show mac-address-table static	P	Show static MAC address table	switch#show mac-address-table static
show mac-address-table filter	P	Show filter MAC address table.	switch#show mac-address-table filter
no mac-address-table static hwaddr **[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
no mac-address-table filter hwaddr **[MAC]**	G	Remove an entry of MAC address table (filter)	switch(config)#no mac-address-table filter hwaddr 000012348678
no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#no mac-address-table

6.10 Commands Set List—SNMP command set

IES-3240 Commands	Level	Description	Example
snmp agent-mode **[v1v2c | v3]**	G	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2c

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

6.11 Commands Set List—Port Mirroring command set

IES-3240 Commands	Level	Description	Example
monitor rx	G	Set RX destination port of monitor function	switch(config)#monitor rx
monitor tx	G	Set TX destination port of monitor function	switch(config)#monitor tx
show monitor	P	Show port monitor information	switch#show monitor
monitor **[RX|TX|Both]**	I	Configure source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#monitor RX
show monitor	I	Show port monitor information	switch(config)#interface fastEthernet 2 switch(config-if)#show monitor
no monitor	I	Disable source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#no monitor

6.12 Commands Set List—802.1x command set

IES-3240 Commands	Level	Description	Example
8021x enable	G	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiousip **[IP address]**	G	Use the 802.1x system radious IP global configuration command to change the radious server IP.	switch(config)# 8021x system radiousip 192.168.1.1
8021x system serverport **[port ID]**	G	Use the 802.1x system server port global configuration command to change the radious server port	switch(config)# 8021x system serverport 1815

8021x system accountport **[port ID]**	**G**	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# 8021x system accountport 1816
8021x system sharekey **[ID]**	**G**	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# 8021x system sharekey 123456
8021x system nasid **[words]**	**G**	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# 8021x system nasid test1
8021x misc quietperiod **[sec.]**	**G**	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# 8021x misc quietperiod 10
8021x misc txperiod **[sec.]**	**G**	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# 8021x misc txperiod 5
8021x misc supportimeout **[sec.]**	**G**	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# 8021x misc supportimeout 20
8021x misc servertimeout **[sec.]**	**G**	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#8021x misc servertimeout 20

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

6.13 Commands Set List—TFTP command set

IES-3240 Commands	Level	Description	Defaults Example
backup flash:backup_cfg	G	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#backup flash:backup_cfg
restore flash:restore_cfg	G	Get configuration from TFTP server and need	switch(config)#restore flash:restore_cfg

		to specify the IP of TFTP server and the file name of image.	
upgrade flash:upgrade_fw	G	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-3240 Commands	Level	Description	Example
systemlog ip **[IP address]**	G	Set System log server IP address.	switch(config)# systemlog ip 192.168.1.100
systemlog mode **[client|server|both]**	G	Specified the log mode	switch(config)# systemlog mode both
show systemlog	E	Display system log.	Switch>show systemlog
show systemlog	P	Show system log client & server information	switch#show systemlog
no systemlog	G	Disable systemlog functon	switch(config)#no systemlog
smtp enable	G	Enable SMTP function	switch(config)#smtp enable
smtp serverip **[IP address]**	G	Configure SMTP server IP	switch(config)#smtp serverip 192.168.1.5
smtp authentication	G	Enable SMTP authentication	switch(config)#smtp authentication
smtp account **[account]**	G	Configure authentication account	switch(config)#smtp account User
smtp password **[password]**	G	Configure authentication password	switch(config)#smtp password
smtp rcptemail **[Index] [Email address]**	G	Configure Rcpt e-mail Address	switch(config)#smtp rcptemail 1 Alert@test.com

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

6.15 Commands Set List—SNTP command set

IES-3240 Commands	Level	Description	Example
sntp enable	G	Enable SNTP function	switch(config)#sntp enable
sntp daylight	G	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight
sntp daylight-period **[Start time] [End time]**	G	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# sntp daylight-period 20060101-01:01 20060202-01-01
sntp daylight-offset **[Minute]**	G	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight-offset 3
sntp ip **[IP]**	G	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp ip 192.169.1.1
sntp timezone **[Timezone]**	G	Set timezone index, use "show sntp timzezone" command to get more information of index number	switch(config)#sntp timezone 22
show sntp	P	Show SNTP information	switch#show sntp
show sntp timezone	P	Show index number of time zone list	switch#show sntp timezone
no sntp	G	Disable SNTP	switch(config)#no sntp

		function	
no sntp daylight	**G**	Disable daylight saving time	switch(config)#no sntp daylight

6.16 Commands Set List—O-Ring command set

IES-3240 Commands	Level	Description	Example
Ring enable	**G**	Enable O-Ring	switch(config)# ring enable
Ring master	**G**	Enable ring master	switch(config)# ring master
Ring couplering	**G**	Enable couple ring	switch(config)# ring couplering
Ring dualhoming	**G**	Enable dual homing	switch(config)# ring dualhoming
Ring ringport **[1st Ring Port] [2nd Ring Port]**	**G**	Configure 1st/2nd Ring Port	switch(config)# ring ringport 7 8
Ring couplingport **[Coupling Port]**	**G**	Configure Coupling Port	switch(config)# ring couplingport 1
Ring controlport **[Control Port]**	**G**	Configure Control Port	switch(config)# ring controlport 2
Ring homingport **[Dual Homing Port]**	**G**	Configure Dual Homing Port	switch(config)# ring homingport 3
show Ring	**P**	Show the information of O-Ring	switch#show ring
no Ring	**G**	Disable O-Ring	switch(config)#no ring
no Ring master	**G**	Disable ring master	switch(config)# no ring master
no Ring couplering	**G**	Disable couple ring	switch(config)# no ring couplering
no Ring dualhoming	**G**	Disable dual homing	switch(config)# no ring dualhoming

Technical Specifications

ORing Switch Model	IES-3240
Physical Ports	
10/100 Base-T(X) Ports in RJ45 Auto MDI/MDIX	**24**
Technology	
Ethernet Standards	IEEE 802.3 for 10Base-T IEEE 802.3u for 100Base-TX IEEE 802.3x for Flow control IEEE 802.3ad for LACP (Link Aggregation Control Protocol) IEEE 802.1D for STP (Spanning Tree Protocol) IEEE 802.1p for COS (Class of Service) IEEE 802.1Q for VLAN Tagging IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol) IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol) IEEE 802.1x for Authentication IEEE 802.1AB for LLDP (Link Layer Discovery Protocol)
MAC Table	8192 MAC addresses
Priority Queues	4
Processing	Store-and-Forward
Switch Properties	Switching bandwidth: 4.8Gbps Max. Number of Available VLANs: 4096 IGMP multicast groups: 1024 Port rate limiting: User Define
Security Features	Enable/disable ports, MAC based port security Port based network access control (802.1x) VLAN (802.1Q) to segregate and secure network traffic Supports Q-in-Q VLAN for performance & security to expand the VLAN space Radius centralized password management SNMP V1/V2c/V3 encrypted authentication and access security
Software Features	STP/RSTP/MSTP (IEEE 802.1D/w/s) Redundant Ring (O-Ring) with recovery time less than 10ms over 250 units TOS/Diffserv supported Quality of Service (802.1p) for real-time traffic VLAN (802.1Q) with VLAN tagging and GVRP supported IGMP Snooping for multicast filtering Port configuration, status, statistics, monitoring, security SNTP for synchronizing of clocks over network Support **PTP Client** (Precision Time Protocol) clock synchronization DHCP Server / Client support Port Trunk support MVR (Multicast VLAN Registration) support
Network Redundancy	O-Ring Open-Ring O-RSTP STP RSTP MSTP
Warning / Monitoring System	Relay output for fault event alarming Syslog server / client to record and view events Include SMTP for event warning notification via email Event selection support
RS-232 Serial Console Port	RS-232 in RJ45 connector with console cable. 9600bps, 8, N, 1
LED indicators	
Power Indicator	Green : Power LED x 3
R.M. Indicator	Green : Indicate system operated in O-Ring master mode

Fault Indicator	Amber : Indicate unexpected event occurred
10/100Base-T(X) RJ45 Port Indicator	Green for port Link/Act. Amber for Duplex/Collision
Fault contact	
Relay	Relay output to carry capacity of 1A at 24VDC
Power	
Redundant Input power	Dual DC inputs. 12 ~ 48VDC on 6-pin terminal block
Power consumption (Typ.)	9.6 Watts
Overload current protection	Present
Reverse polarity protection	Present on terminal block
Physical Characteristic	
Enclosure	IP-30
Dimension (W x D x H)	96(W)x109.2(D)x153.6(H) mm (3.78 x 4.3 x 6.05 inch)
Weight (g)	1052 g
Environmental	
Storage Temperature	-40 to 85^{o}C (-40 to 185^{o}F)
Operating Temperature	-40 to 70^{o}C (-40 to 158^{o}F)
Operating Humidity	5% to 95% Non-condensing
Regulatory approvals	
EMI	FCC Part 15, CISPR (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	IEC60068-2-27
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6
Safety	EN60950-1
Warranty	5 years