IES-3082GC

Industrial Managed Ethernet Switch

User Manual

Version 1.0

Mar, 2013

COPYRIGHT NOTICE

TRADEMARKS

is a registered trademark of ORing Industrial Networking Corp.

All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

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

WARRANTY

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

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

DISCLAIMER

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

CONTACT INFORMATION

ORing Industrial Networking Corp.

3F., NO.542-2, Jhongjheng Rd., Sindian District, New Taipei City 23145, Taiwan, R.O.C.
Tel: + 886 2 2218 1066 // Fax: + 886 2 22181014
Website: www.oring-networking.com

Technical Support

E-mail: support@oring-networking.com

Sales Contact

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

Table of Content

Getting to Know Your Switch

1.1 About the IES-3082GC Managed Industrial Switch

The IES-3082GC is a powerful managed industrial switch designed for extreme temperatures, dusty environments and high humidity. With 8 X 10/100Base-T(X) and 2 x Gigabit combo ports, the IES-3082GC can be managed via web browsers, TELNET, Console or other third-party SNMP software as well as ORing's proprietary management utility Open-Vision. The user-friendly and powerful interface of Open-Vision allows you to easily configure and monitor multiple switches at the same time.

1.2 Software Features

- Supports O-Ring (Recovery time < 10ms over 250 units connection)
- Supports Ring Coupling, Dual Homing over O-Ring
- Supports SNMPv1/v2/v3 & RMON & Port base/802.1Q VLAN Network Management
- Event notification by email, SNMP trap, and relay output
- Web-based ,Telnet, Console (CLI) configuration
- Enable/disable ports, MAC based port security
- Port-based network access control (802.1x)
- Supports VLAN (802.1Q) to segregate and secure network traffic
- Radius centralized password management
- SNMPv3 encrypted authentication and access security
- RSTP (802.1w)
- Quality of Service (802.1p) for real-time traffic
- VLAN (802.1Q) with double tagging and GVRP supported
- IGMP snooping for multicast filtering
- Port configuration, status, statistics, mirroring, security
- Remote monitoring (RMON)

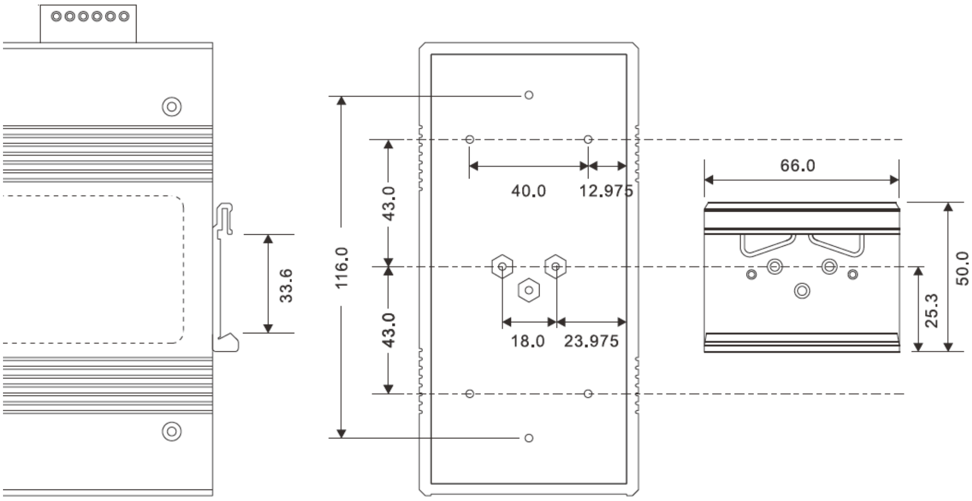
1.3 Hardware Features

- Dual 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
- 10/100/1000Base-T(X) Gigabit Ethernet port (in combo ports)
- 100/1000Base-X on SFP port (in combo ports)
- Console port
- Dimensions (W x D x H): 74.3 mm (W) x 109.2 mm (D) x 153.6 mm (H)

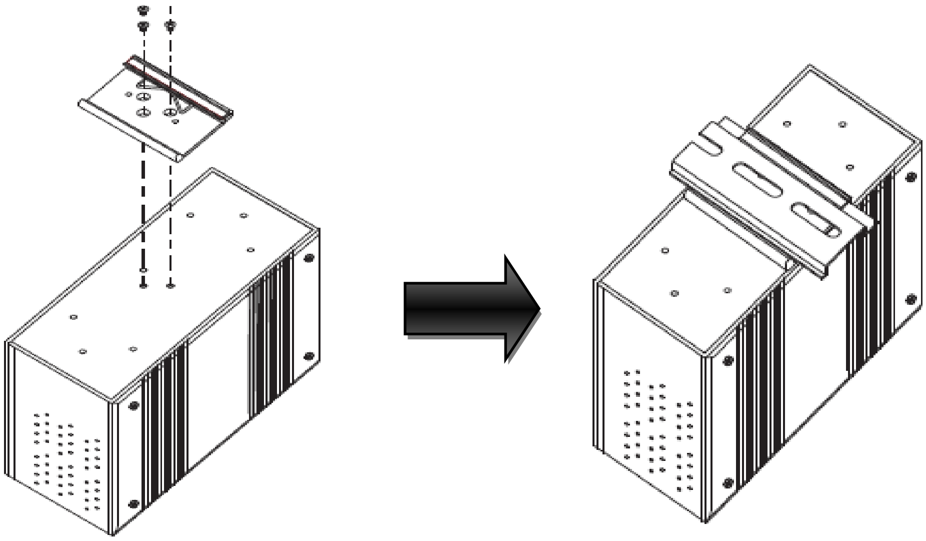
Hardware Installation

2.1 DIN-rail Installation

Each switch comes with a DIN-rail kit which can be installed on the rear panel. With the DIN-rail kit, the switch can be fixed on a DIN-rail. Installing the switch on the DIN-rail is easy. First, screw the Din-rail kit onto the back of the switch, right in the middle of the back panel. Then slide the switch onto a DIN-rail from the Din-rail kit and make sure the switch clicks into the rail firmly.

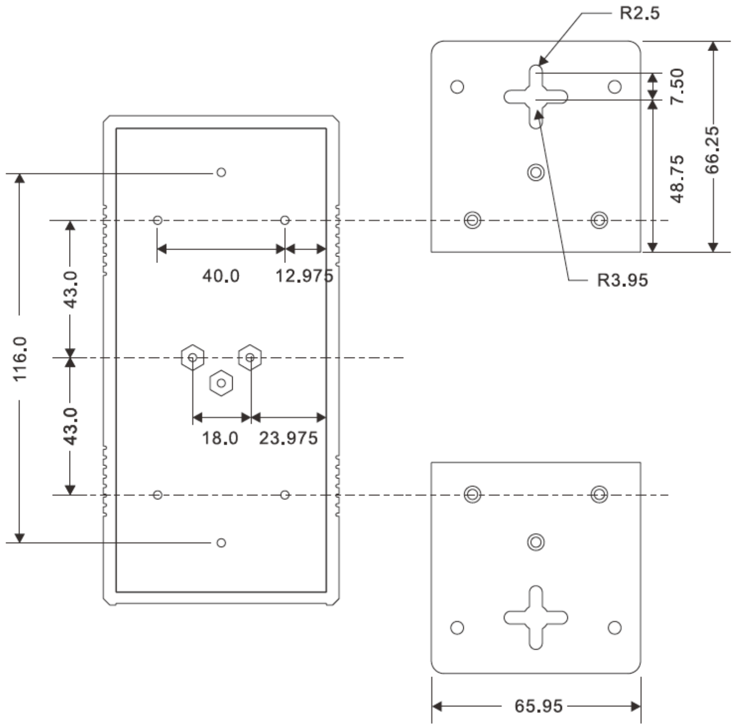


Din-rail Kit Measurement



2.2 Wall Mounting

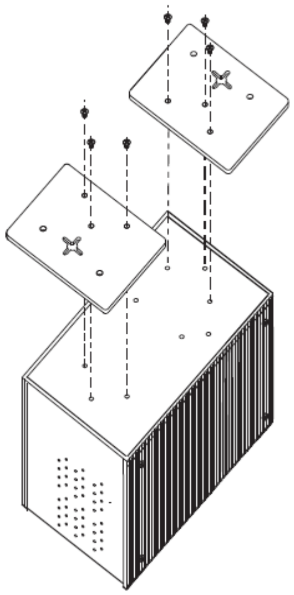
Besides Din-Rail, the switch can be fixed to the wall via a wall mount panel, which can be found in the package.



Wall-Mount Kit Measurement

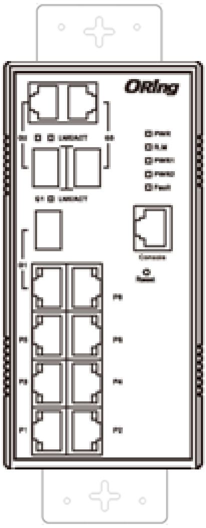
To mount the switch onto the wall, follow the steps:

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



2. Use the switch, with wall mount plates attached, as a guide to mark the correct locations of the four screws.

3. Insert four screw heads through the large parts of the keyhole-shaped apertures, and then slide the switch downwards. Tighten the four screws for added stability.



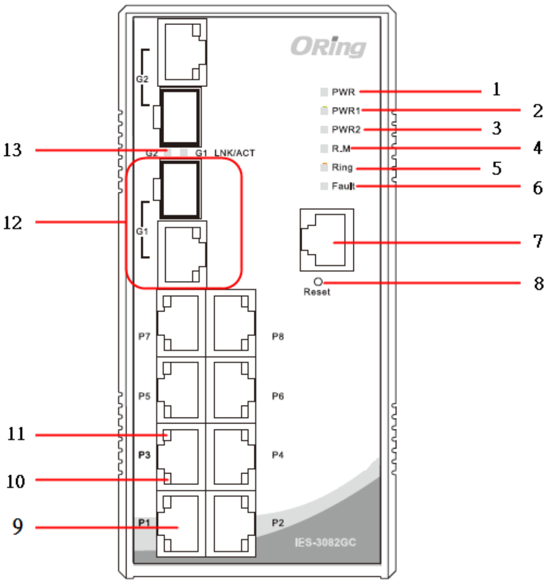
Note: Instead of screwing the screws in all the way, leave about 2 mm to allow room for sliding the wall mount panel between the wall and the screws.

Hardware Overview

3.1 Front Panel

IES-3082GC comes with the following ports on the front panel:

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
Gigabit RJ-45 ports	2x 10/100/1000Base-T(X) Gigabit ports (in combo ports)
SFP ports	2x 100/1000Base-X on SFP port (in combo ports)
Console	Use RS-232 to RJ-45 cable to manage switch.
Reset	Push reset button 2 to 3 seconds to reset the switch. Push reset button 5 seconds to return the switch to factory setting**.**



1. LED for PWR.
2. LED for PWR1.
3. LED for PWR2.
4. LED for R.M (Ring master).
5. LED for Ring.
6. LED for Fault Relay.
7. Console port (RJ-45).
8. Reset button.
9. 10/100Base-T(X) Ethernet ports.
10. LED indicating the speed of Ethernet ports
11. LED indicating the link status of Ethernet ports
12. 1000 COMBO ports with SFP
13. LED for SFP ports link/act status.

3.2 Front Panel LEDs

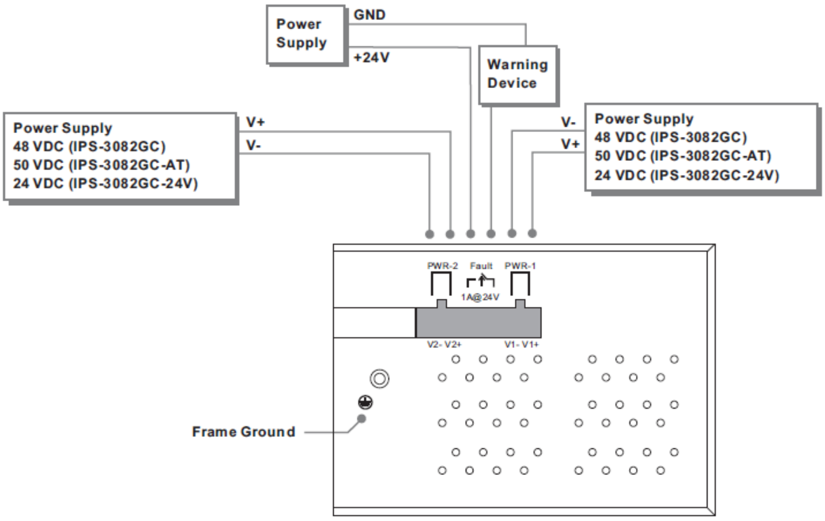
LED	Color	Status	Description
PWR	Green	On	DC power on
PW1	Green	On	DC power module 1 activated.
PW2	Green	On	DC power module 2 activated.
R.M	Green	On	O-Ring Master.
Ring	Green	On	O-Ring enabled.
		Slowly blinking	Ring structure is broken (i.e. part of the ring is disconnected)
		Fast blinking	Ring disabled
Fault	Amber	On	Faulty relay (power failure or port malfunctioning)
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.
Gigabit Ethernet ports			
ACT	Green	On	Port link up.
		Blinking	Data transmitted.
LNK	Amber	On	Port link up.
SFP ports			
LNK / ACT	Green	On	Port link up.
		Blinking	Data transmitted.

3.3 Top Panel

Below are the top panel components of IES-3082GC series:

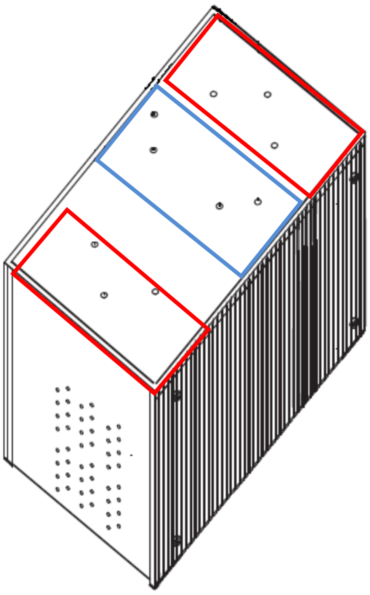
1. Terminal block

2. Ground wire



3.4 Rear Panel

On the rear panel of the switch sit three sets of screw holes. The two sets placed in triangular patterns on both ends of the rear panel are used for wall-mounting (red boxes in the figure below) and the set of four holes in the middle are used for Din-rail installation (blue box in the figure below).



Cables

4.1 Ethernet Cables

The IES-3082GC switch has standard Ethernet ports. According to the link type, the switch uses CAT 3, 4, 5,5e UTP cables to connect to any other network devices (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

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

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

With 1000/100BASE-TX/10BASE-T cables, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

10/100 Base-T RJ-45 Pin Assignments:

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

The IES-3082GC series switches support auto MDI/MDI-X operation. You can use a cable to connect the switch to a PC. The table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

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

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

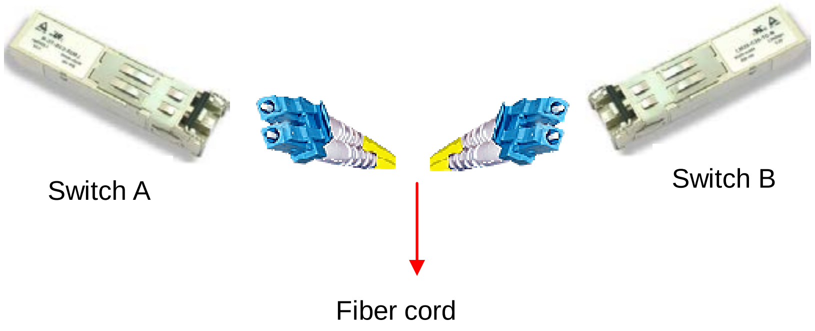
1000 Base-T MDI/MDI-X Pin Assignments:

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

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

4.2 SFP

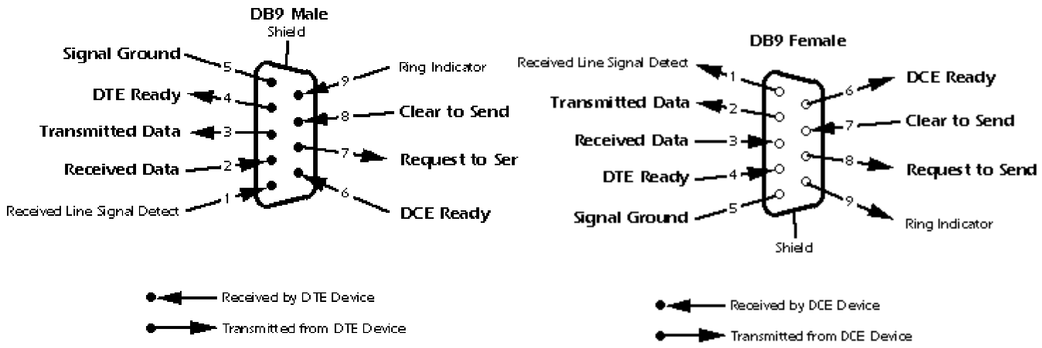
The switch comes with fiber optical ports that can connect to other devices using SFP modules. The fiber optical ports are in multi-mode (0 to 550M, 850 nm with 50/125 µm, 62.5/125 µm fiber) and single-mode with LC connectors. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.



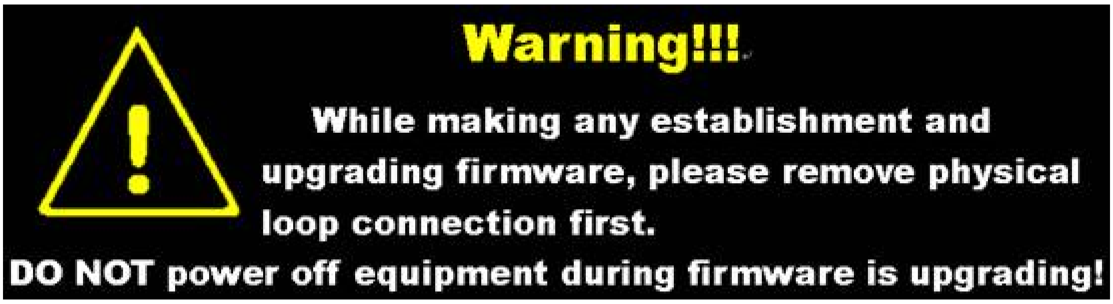
4.3 Console Cable

The IES-3082GC switch can be managed via console ports using a RS-232 cable which can be found in the package. You can connect the port to a PC via the RS-232 cable with a DB-9 female connector. The DB-9 female connector of the RS-232 cable should be connected the PC while the other end of the cable (RJ-45 connector) should be connected to the console port of the switch.

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



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

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

Note: By default, IE5.0 or later version 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

You can access the management page of the switch via the following default values:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

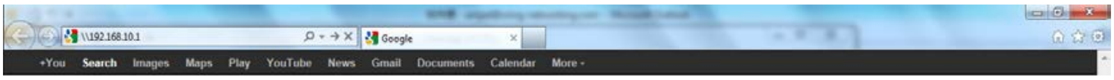
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

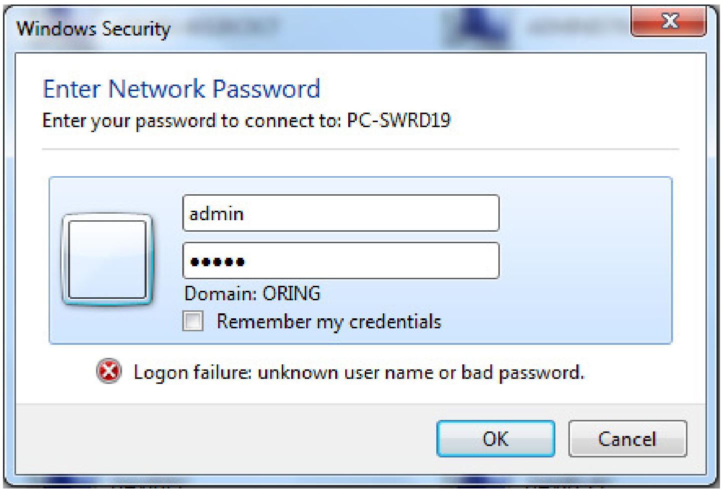
System Login

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



\\192.168.10.1

1. A login screen appears.
2. Type in the username and password. The default username and password is **admin**.
3. Click **Enter** or **OK** button, the management Web page appears.



Windows Security

Enter Network Password

Enter your password to connect to: PC-SWRD19

admin

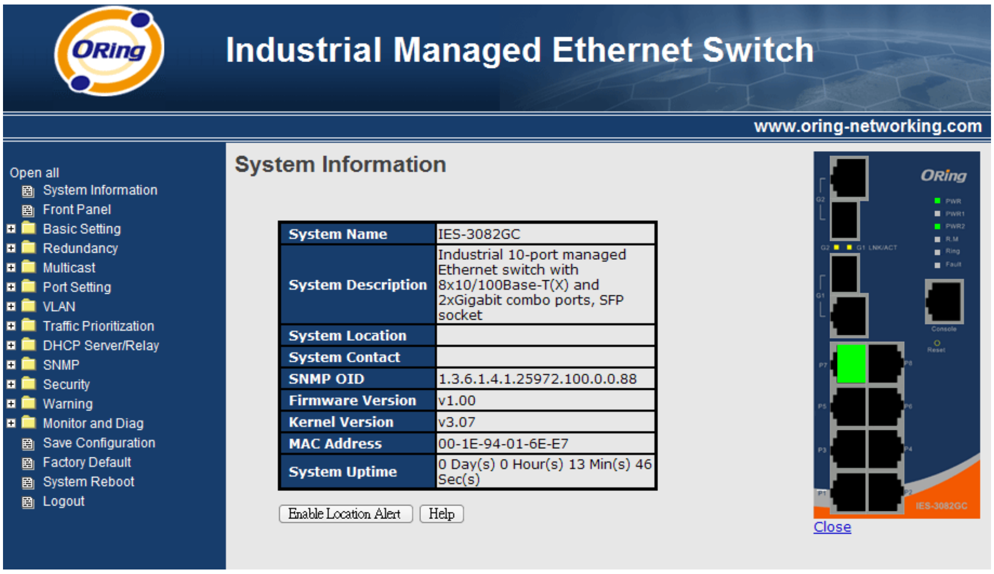
●●●●●

Domain: ORING

□ Remember my credentials

Logon failure: unknown user name or bad password.

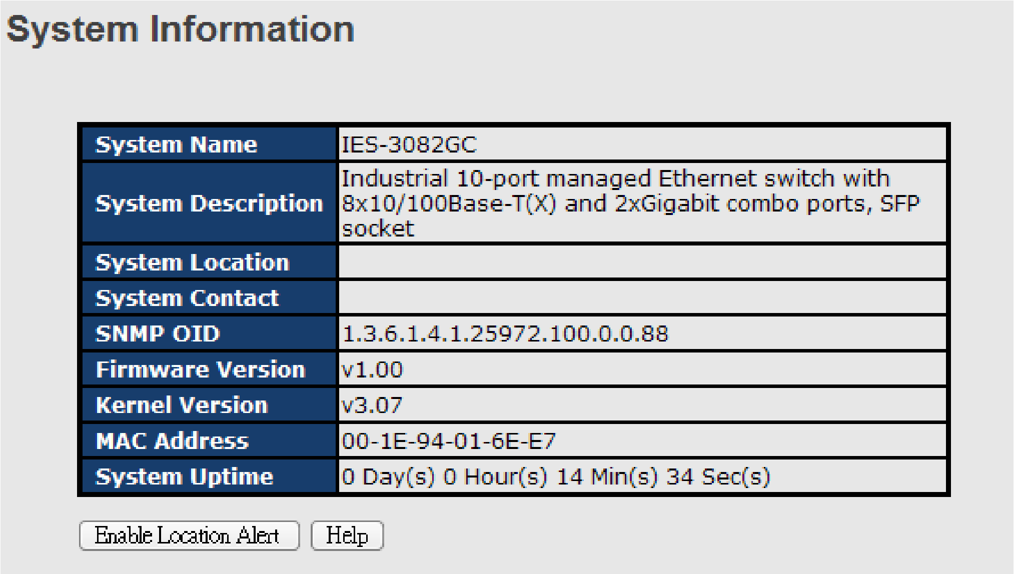
After logging in, you will see the screen below. On the right hand side of the management interface shows links to various settings. You can click on the links to access the configuration pages of different functions.



System Information

System Name	IES-3082GC
System Description	Industrial 10-port managed Ethernet switch with 8x10/100Base-T(X) and 2xGigabit combo ports, SFP socket
System Location	
System Contact	
SNMP OID	1.3.6.1.4.1.25972.100.0.0.88
Firmware Version	v1.00
Kernel Version	v3.07
MAC Address	00-1E-94-01-6E-E7
System Uptime	0 Day(s) 0 Hour(s) 13 Min(s) 46 Sec(s)

Click on the System Information on the right hand column will display the detailed information of the system, shown as below.



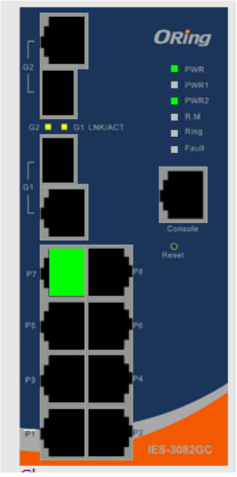
System Information

System Name	IES-3082GC
System Description	Industrial 10-port managed Ethernet switch with 8x10/100Base-T(X) and 2xGigabit combo ports, SFP socket
System Location	
System Contact	
SNMP OID	1.3.6.1.4.1.25972.100.0.0.88
Firmware Version	v1.00
Kernel Version	v3.07
MAC Address	00-1E-94-01-6E-E7
System Uptime	0 Day(s) 0 Hour(s) 14 Min(s) 34 Sec(s)

The system information will display the configuration of the basic setting / switch setting pages. When clicking **Enable Location Alert**, PWR1, PWR2 and PWR3 LEDs on the switch will start to flash together. When you click **Disable Location Alert**, the LEDs will stop flashing.

5.1.3 Front Panel Configuration

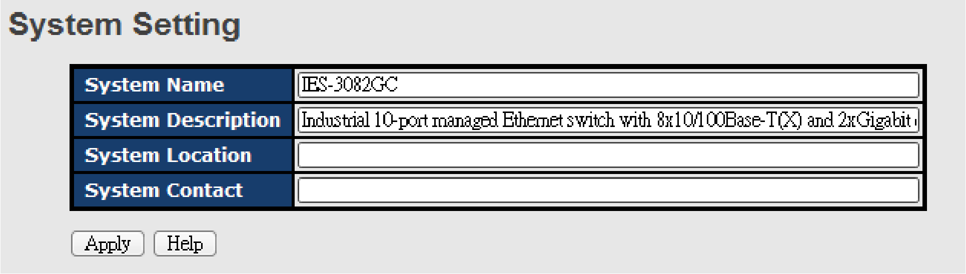
Click **Front Panel** to show the front panel configuration of the switch or click **Close** to close the page.



5.1.4 Basic Setting

Basic Settings allow you to configure the basic functions of the switch.

5.1.4.1 Switch Setting



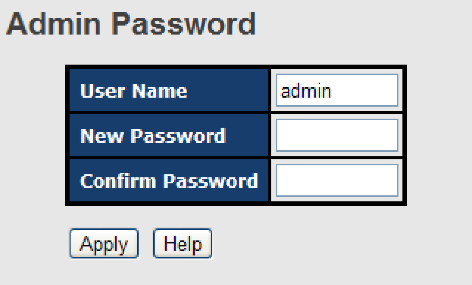
System Setting

System Name	IES-3082GC
System Description	Industrial 10-port managed Ethernet switch with 8x10/100Base-T(X) and 2xGigabit
System Location	
System Contact	

Label	Description
System Name	Assigns the name of switch. The maximum length is 64 bytes
System Description	Description of the device
System Location	Assigns physical switch location. The maximum length is 64 bytes
System Contact	Information of the contact person or organization

5.1.4.2 Admin Password

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



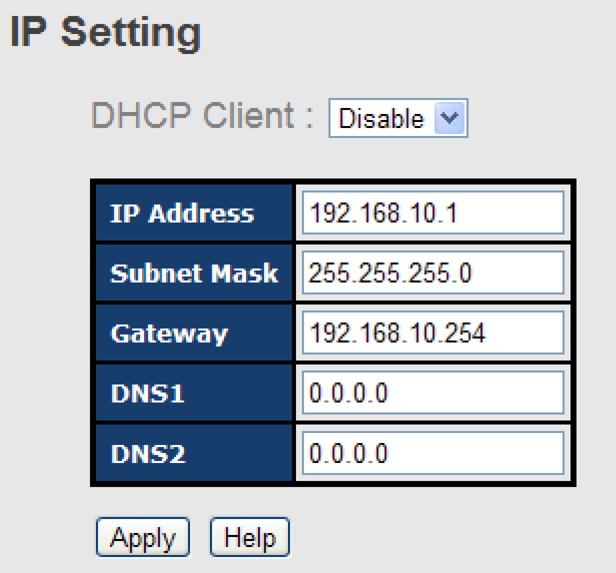
Admin Password

User Name	admin
New Password	
Confirm Password	

Label	Description
User name	The user name for operating the switch (default is **admin**)
New Password	The new system password (default is **admin**)
Confirm password	Re-type the new password
Apply	Click to save changes

5.1.4.3 IP Setting

You can configure IP information of the switch in this page.



IP Setting

DHCP Client : Disable

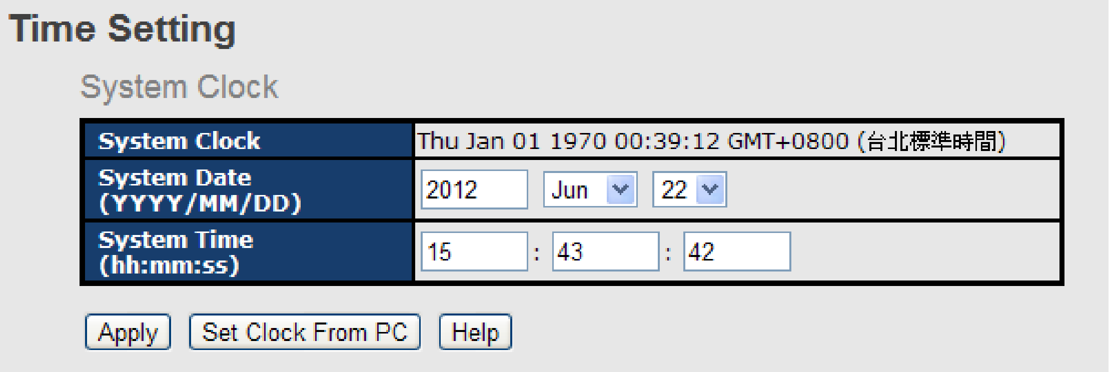
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway	192.168.10.254
DNS1	0.0.0.0
DNS2	0.0.0.0

Label	Description
DHCP Client	Enables or disables the DHCP client function. When DHCP client function is enabled, the switch will be assigned with an IP address by the network DHCP server. The default IP address will be replaced by the IP address assigned by the DHCP server. After clicking **Apply**, a popup dialog appears to inform when the DHCP client is enabled. The current IP will lose and you should find the new IP on the DHCP server.
IP Address	Assigns the IP address that the network is using. If DHCP client function is enabled, you do not need to assign the IP address. The network DHCP server will assign the IP address to the switch and it will be displayed in this column. The default IP is 192.168.10.1.
Subnet Mask	Assigns the subnet mask of the IP address. If DHCP client function is enabled, you do not need to assign the subnet mask
Gateway	Assigns the network gateway for the switch. The default gateway is 192.168.10.254
DNS1	Assigns the primary DNS IP address
DNS2	Assigns the secondary DNS IP address
Apply	Click to activate the configurations

5.1.4.4 Time Setting

This page includes configurations of SNTP and system clock.

System Clock



Time Setting

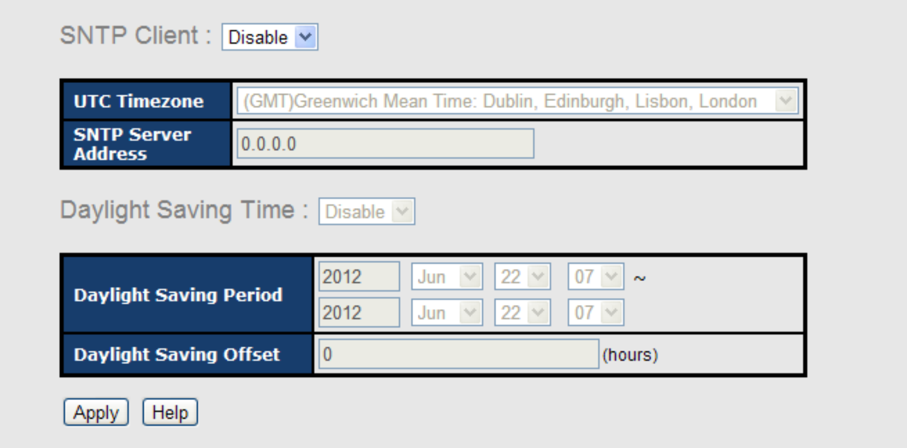
System Clock

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

Label	Description
System Clock	This field shows the current system timer. The time stamp could be assigned manually or by a SNTP server.
System Date	Specifies the year, month and day of system clock (YYYY/MM/DD). Year: 2006-2015. Month: Jan-Dec. Day:1-31(28)
System Time	Specifies 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)

Label	Description
SNTP Client	Enables or disables SNTP function to retrieve the time from the SNTP server.
Daylight Saving Time	Enables or disables daylight saving time function. When daylight saving time is enabled, you need to configure the daylight saving time period.
UTC Time zone	Sets the switch location time zone. The following table lists different location time zones for your reference.

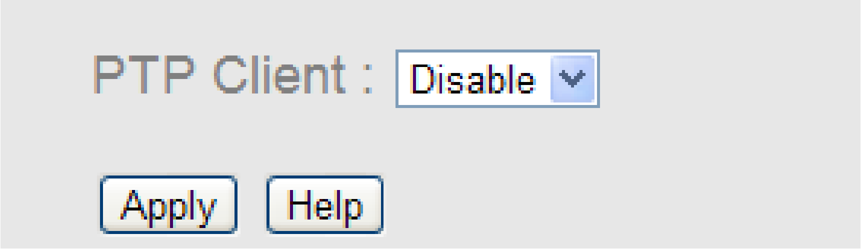
Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11 am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard	+12 hours	Midnight

NZT - New Zealand		

Label	Description
SNTP Sever IP Address	Sets SNTP server IP address.
Daylight Saving Period	Sets up the start and end time of daylight saving. Both will be different each year.
Daylight Saving Offset	Sets up the offset time
Switch Timer	Displays current time of the switch
Apply	Click 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.

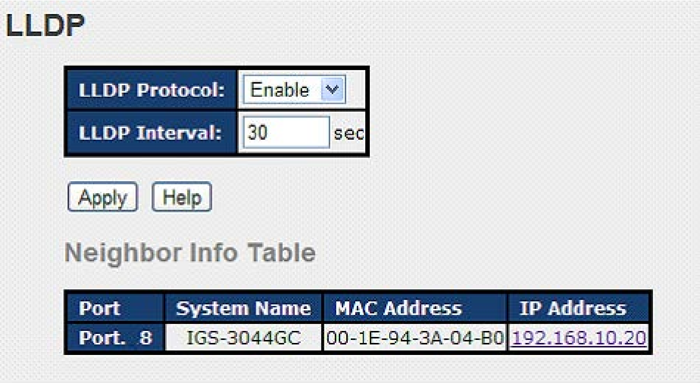


PTP Client : Disable

Label	Description
PTP Client	Enables or disables 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.



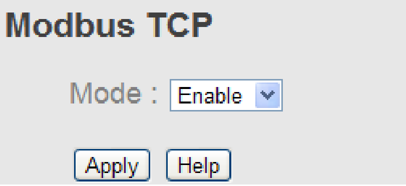
LLDP Protocol:	Enable
LLDP Interval:	30 sec

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

Label	Description
LLDP Protocol	Enables or disables LLDP function
LLDP Interval	The interval of resend LLDP (by default at 30 seconds)
Apply	Click to set the configurations
Help	Shows help file
Neighbor info table	Shows neighbor device infomation

5.1.4.6 Modbus TCP

This page shows Modbus TCP support of the switch. (For more information regarding Modbus, please visit http://www.modbus.org/)

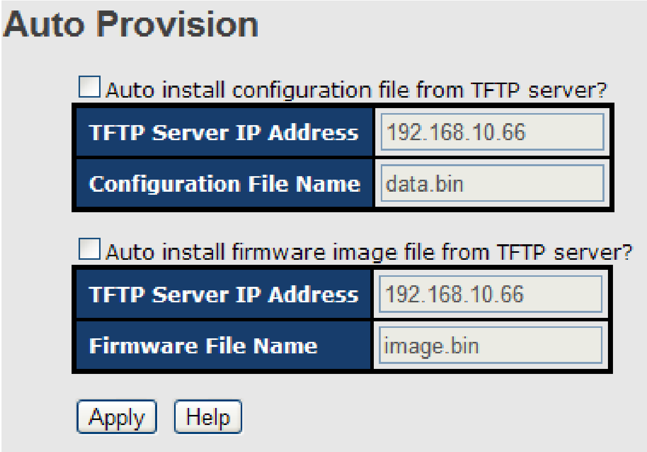


Mode : Enable

Label	Description
Mode	Enables or disables Modbus TCP function

5.1.4.7 Auto Provision

This page allows you to update switch firmware automatically. You can put firmware or configuration files on a 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 are on the TFTP server.



Auto Provision

□ Auto install configuration file from TFTP server?

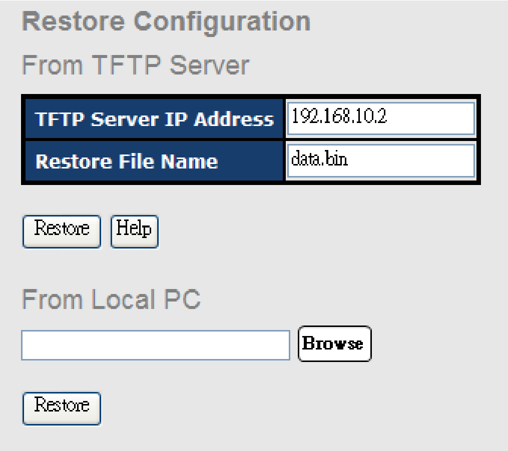
TFTP Server IP Address	192.168.10.66
Configuration File Name	data.bin

□ Auto install firmware image file from TFTP server?

TFTP Server IP Address	192.168.10.66
Firmware File Name	image.bin

5.1.4.8 Backup & Restore

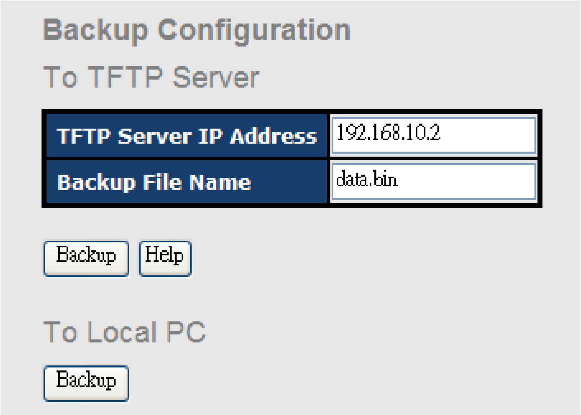
You can save current EEPROM value from the switch to a TFTP server, then go to the TFTP restore configuration page to restore the EEPROM value.



Restore Configuration

From TFTP Server

TFTP Server IP Address	192.168.10.2
Restore File Name	data.bin



Backup Configuration

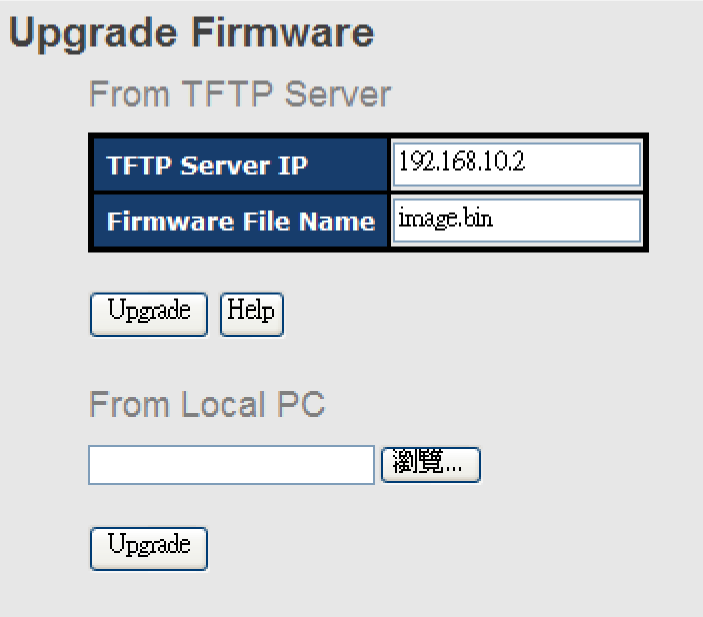
To TFTP Server

TFTP Server IP Address	192.168.10.2
Backup File Name	data.bin

Label	Description
TFTP Server IP Address	Types in TFTP server IP
Restore File Name	Types in the file name
Restore	Click to restore the configurations
Form Local PC	User can select the file from a local PC instead of a TFTP server
Restore File Name	Types in the file name
Restore	Click to restore the configurations
Backup	Click to back up the configurations
To Local PC	User can download config file to the switch without using a TFTP server

5.1.4.9 Upgrade Firmware

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



Upgrade Firmware

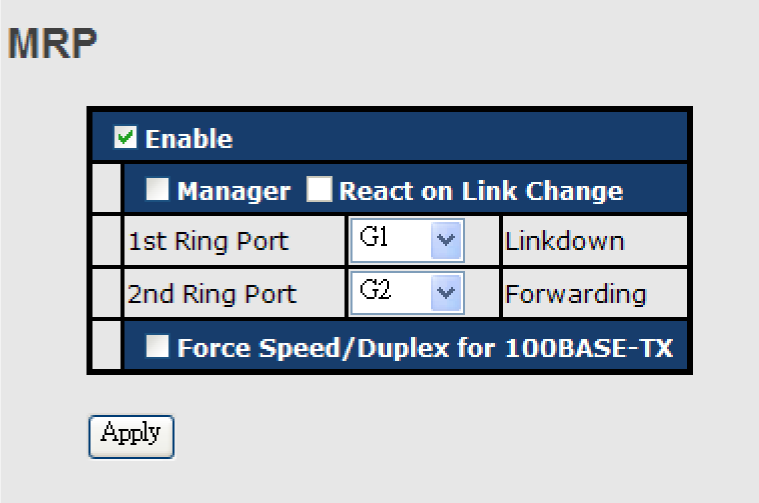
From TFTP Server

TFTP Server IP	192.168.10.2
Firmware File Name	image.bin

5.1.1 Redundancy

5.1.1.1 MRP

MRP (Media Redundancy Protocol) Ring (IEC 62439) can support up to 50 devices and will enable a back-up link in 80ms (adjustable to max. 200ms/500ms).



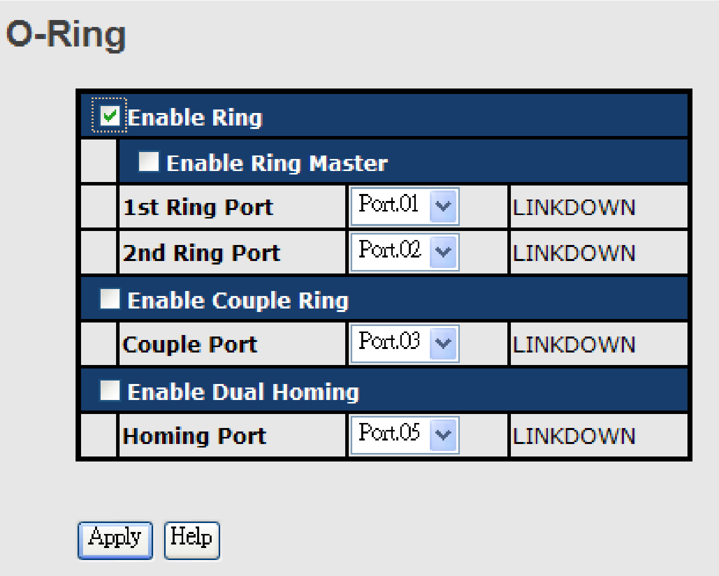
MRP

☑ Enable			
	☐ Manager ☐ React on Link Change		
	1st Ring Port	G1	Linkdown
	2nd Ring Port	G2	Forwarding
	☐ Force Speed/Duplex for 100BASE-TX		

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

5.1.1.2 O-Ring

O-Ring is ORing's proprietary redundant ring technology, with recovery time of less than 10 milliseconds and up to 250 nodes. It can reduce unexpected damage caused by network topology changes. O-Ring supports three Ring topologies: O-Ring, Coupling Ring and Dual Homing.



O-Ring

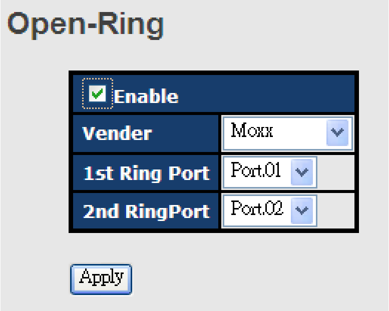
☑ Enable Ring			
	□ Enable Ring Master		
	1st Ring Port	Port.01	LINKDOWN
	2nd Ring Port	Port.02	LINKDOWN
□ Enable Couple Ring			
	Couple Port	Port.03	LINKDOWN
□ Enable Dual Homing			
	Homing Port	Port.05	LINKDOWN

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

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

5.1.1.3 Oen-Ring

Open-Ring technology can be applied to enable ORing's switches to work with other vendors' proprietary rings.



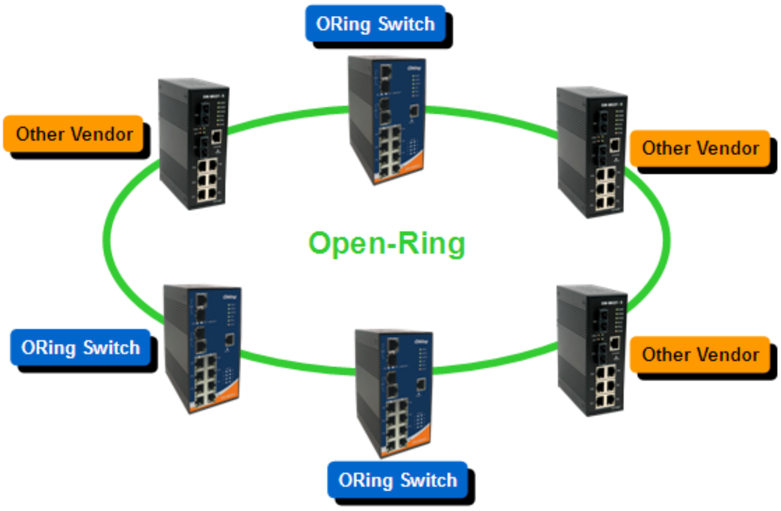
Open-Ring

☑ Enable

Vender	Moxx
1st Ring Port	Port.01
2nd RingPort	Port.02

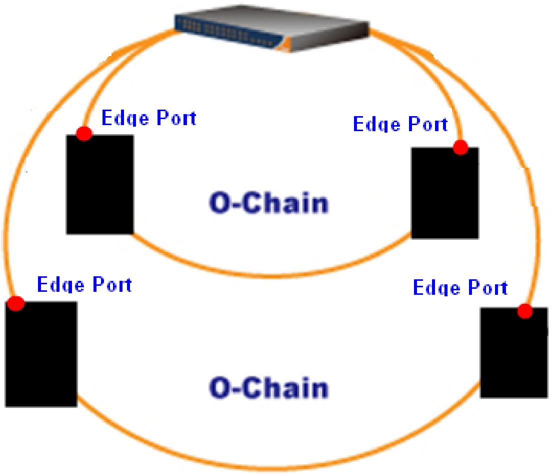
Label	Description
Enable	Enables Open-Ring function
Vender	Chooses the vendors that you want to join to their ring
1st Ring Port	Chooses the port which connects to the ring
2nd Ring Port	Chooses the port which connects to the ring

The application of Open-Ring is shown as below.

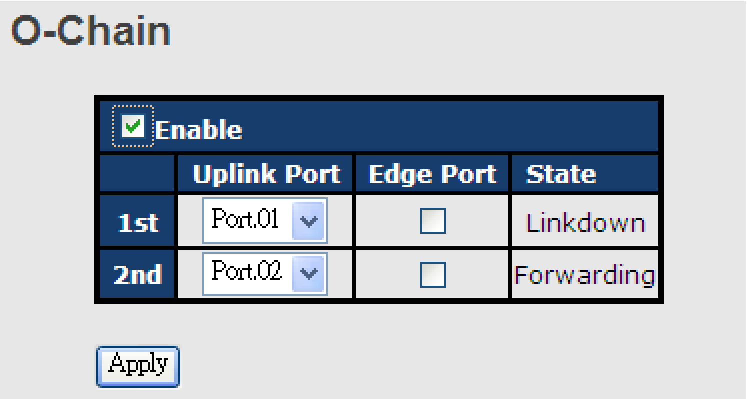


5.1.1.4 O-Chain

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



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



O-Chain

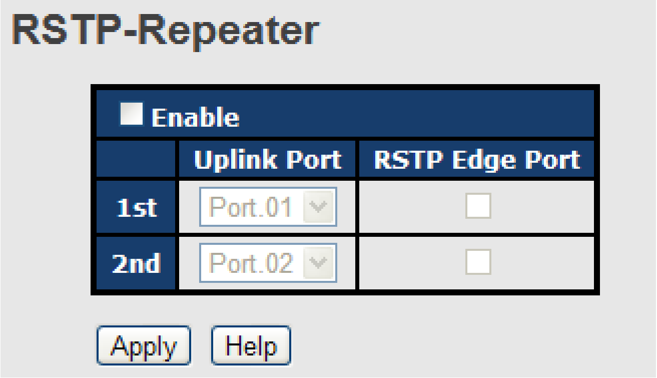
☑ Enable

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

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

5.1.1.5 RSTP – Repeater

RSTP-Repeater is a simple function which can directly pass RSTP BPDU packets. With this function, the devices will act as two RSTP devices connected.



RSTP-Repeater

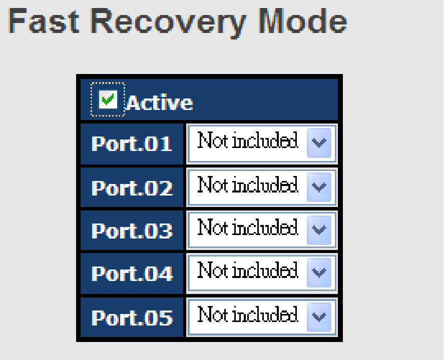
□ Enable

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

Label	Description
Enable	Checks to enable RSTP-Repeater
1st Ring Port	Chooses the port which connects to the RSTP
2nd Ring Port	Chooses the port which connects to the RSTP
Edge Port	Only the edge device (connects to RSTP device) needs to specify an edge port. The user must specify the edge port according to the network topology.

5.1.1.6 Fast Recovery

Fast recovery mode can be set to connect multiple ports to one or more switches. The IES-3082GC with fast recovery mode will provide redundant links. Fast recovery mode supports 10 priorities. Only the first priority will be the active port, and the other ports with different priorities will be 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

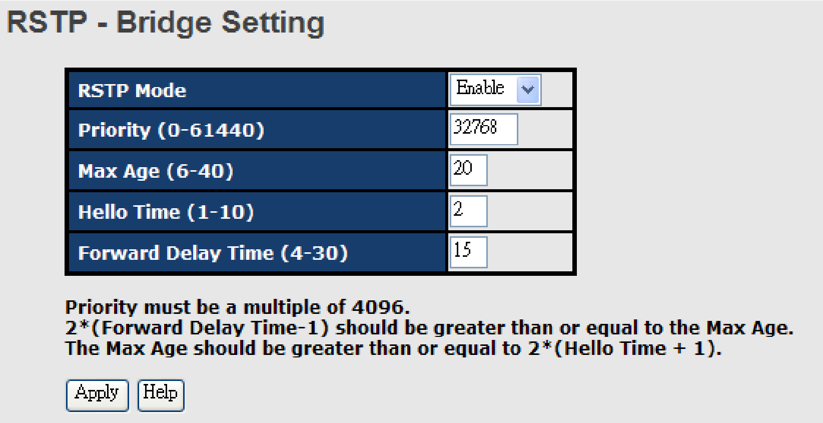
Label	Description
Active	Activates fast recovery mode
port	Ports can be set to 10 priorities. Only the port with the highest priority will be the active port. 1st Priority is the highest.
Apply	Click to activate the configurations

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 network topology is changed. The system also supports STP and will automatically detect the connected devices running STP or RSTP protocols.

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

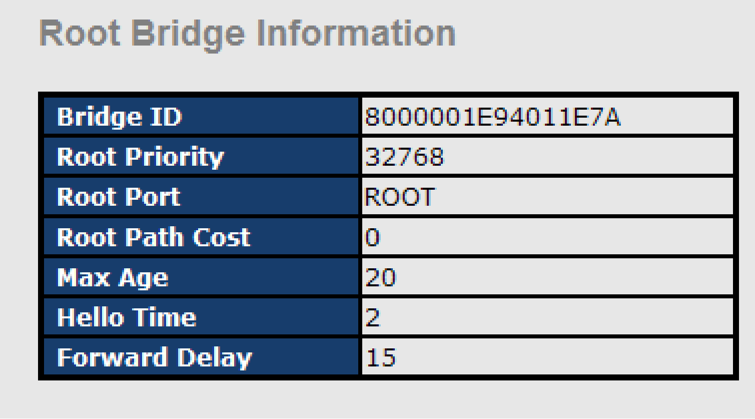
Priority must be a multiple of 4096.
2*(Forward Delay Time-1) should be greater than or equal to the Max Age.
The Max Age should be greater than or equal to 2*(Hello Time + 1).

Label	Description
RSTP mode	You must enable or disable RSTP function before configuring 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 to set the configurations

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

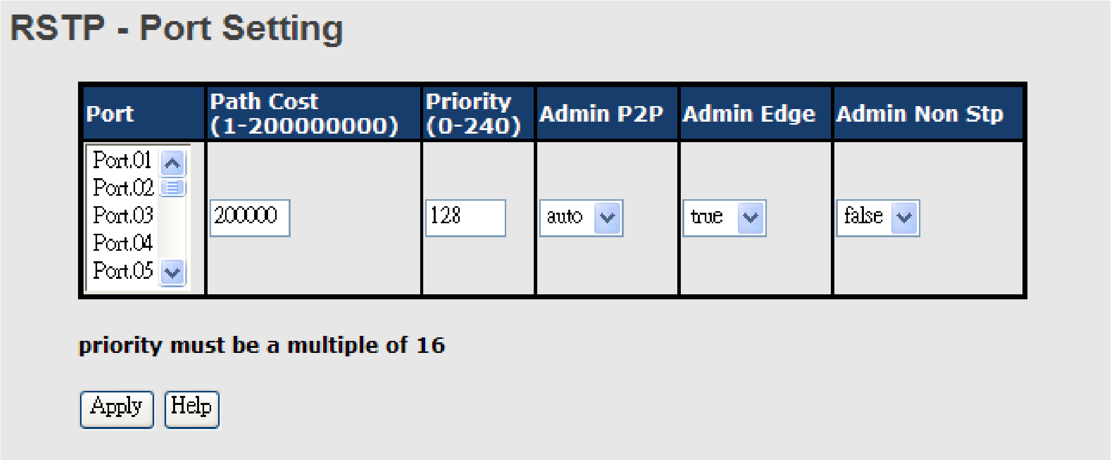
2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)

The following tablet shows RSTP algorithm results.



Root Bridge Information

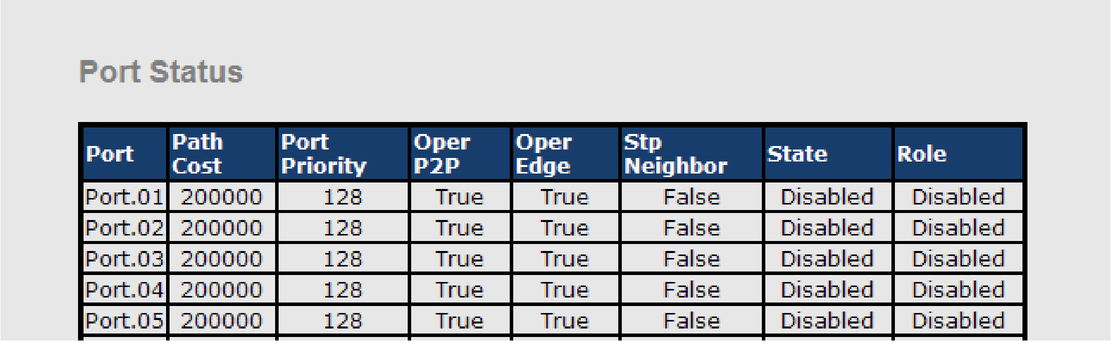
Bridge ID	8000001E94011E7A
Root Priority	32768
Root Port	ROOT
Root Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15



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

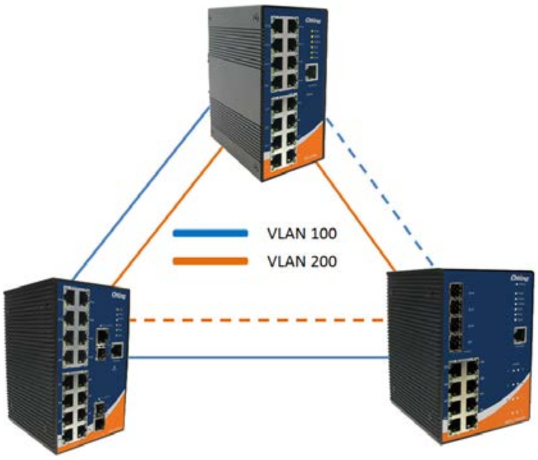
Port	Path Cost	Port Priority	Oper P2P	Oper Edge	Stp Neighbor	State	Role
Port.01	200000	128	True	True	False	Disabled	Disabled
Port.02	200000	128	True	True	False	Disabled	Disabled
Port.03	200000	128	True	True	False	Disabled	Disabled
Port.04	200000	128	True	True	False	Disabled	Disabled
Port.05	200000	128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

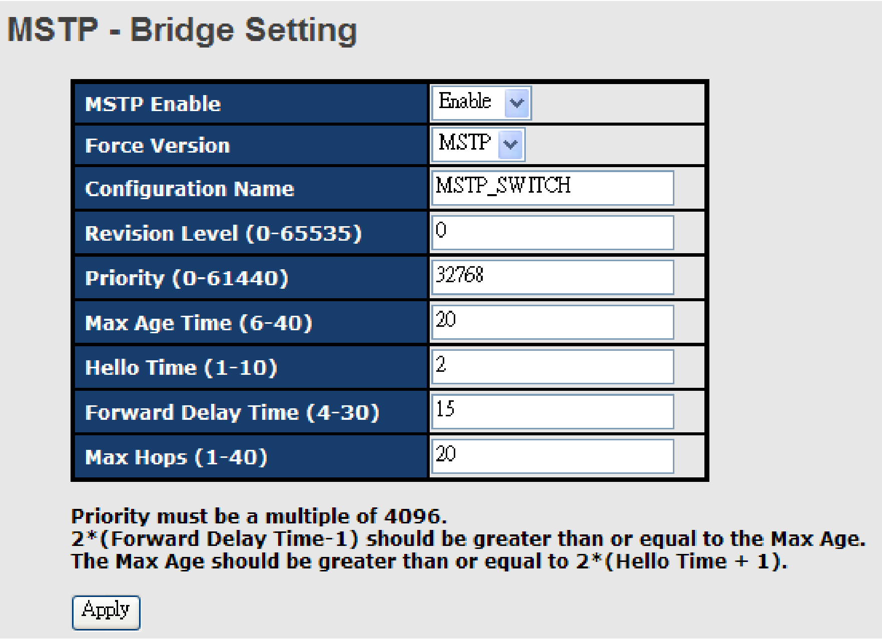
Label	Description
Path Cost (1-200000000)	The cost of the path to the other bridge. The range of valid values is 1 to 200000000.
Port Priority (0-240)	Configures the priority of the ports to be blocked in the LAN. The range of valid values is 0 to 240. The value of priority must be the multiple of 16
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 is 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	The port includes the STP mathematic calculation. **True** does not include

STP	STP mathematic calculation. **False** includes the STP mathematic calculation.
Apply	Click to activate the configurations

5.1.1.8 MSTP

Multiple Spanning Tree Protocol (MSTP) is a standard protocol base on IEEE 802.1s. The function allows several VLANs to be mapped to a reduced number of spanning tree instances because most networks only need a few logical topologies. It supports load balancing scheme and the CPU is sparer than PVST (Cisco proprietary technology).



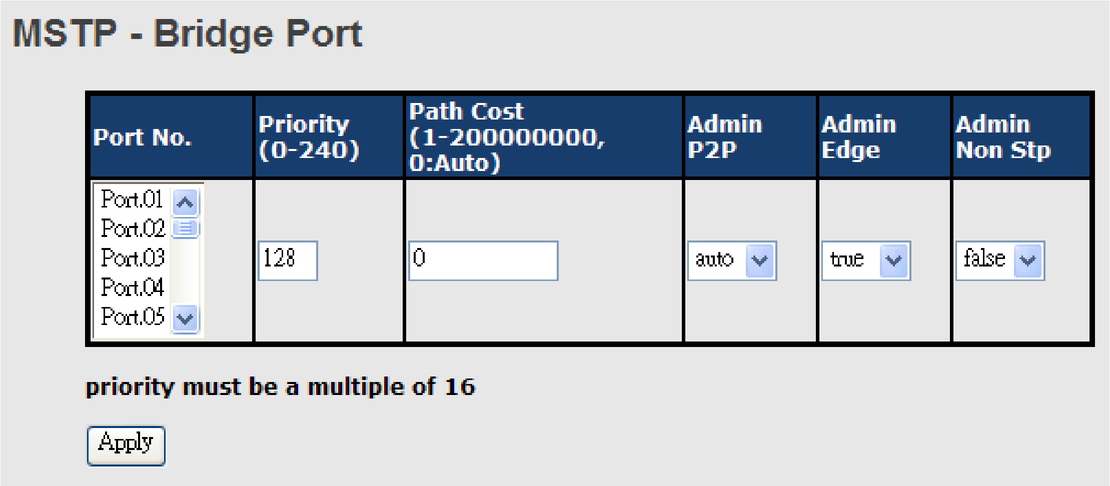


MSTP - Bridge Setting

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).

Label	Description
MSTP Enable	You must enable or disable MSTP function before configuring related parameters.
Force Version	The 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)	Follow the rule below to configure the MAX Age, Hello Time, and Forward Delay Time for the switch which sends out BPDU packets 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 to activate the configurations

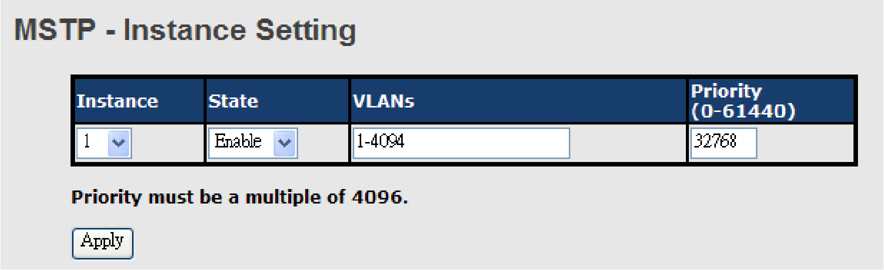


MSTP - Bridge Port

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

Label	Description
Port No.	Selects the port you want to configure
Priority (0-240)	Configures the priority of the ports to be blocked in the 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. 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 to activate the configurations.

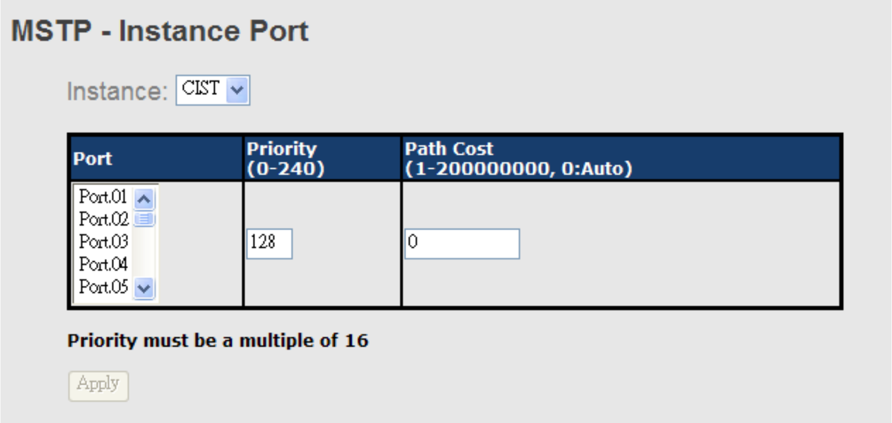


MSTP - Instance Setting

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

Priority must be a multiple of 4096.

Label	Description
Instance	Sets the instance from 1 to 15
State	Enables or disables the instance
VLANs	Sets 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 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

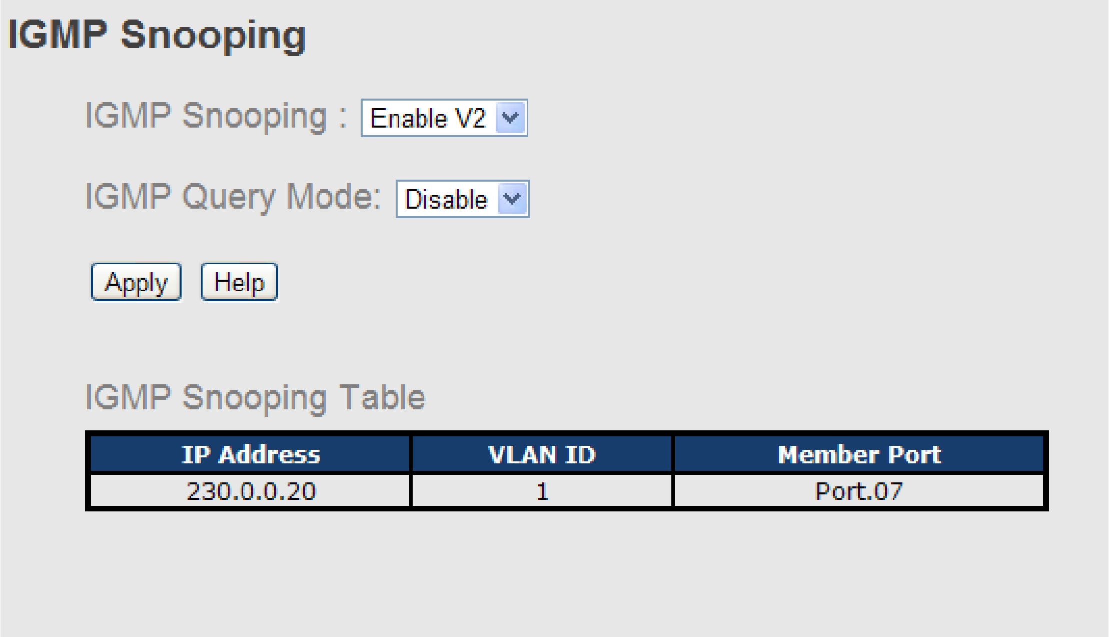
Priority must be a multiple of 16

Label	Description
Instance	Sets the instance's information except CIST
Port	Selects the port you want to configure
Priority (0-240)	Configures the priority of the ports to be blocked in the 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. Enter a number 1 through 200000000.
Apply	Click 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

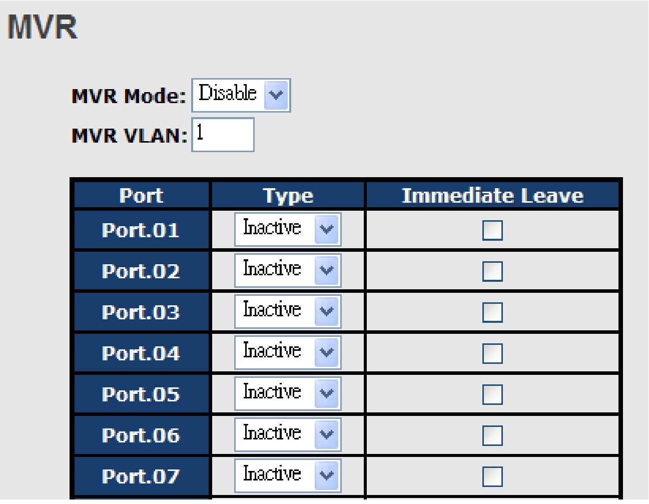
IGMP Snooping Table

IP Address	VLAN ID	Member Port
230.0.0.20	1	Port.07

Label	Description
IGMP Snooping Table	Shows current IP multicast list
IGMP Protocol	Enables or disables IGMP snooping
IGMP Query Mode	Configures the switch to be the IGMP querier. There must be one and only one IGMP querier in an IGMP application. **Auto** means the querier is the one with a lower IP address.
Apply	Click to activate the configurations
Help	Shows help file

5.1.2.2 MVR

MVR allows different VLAN users to receive VLAN Multicast packets in MVR mode.



MVR

MVR Mode: Disable

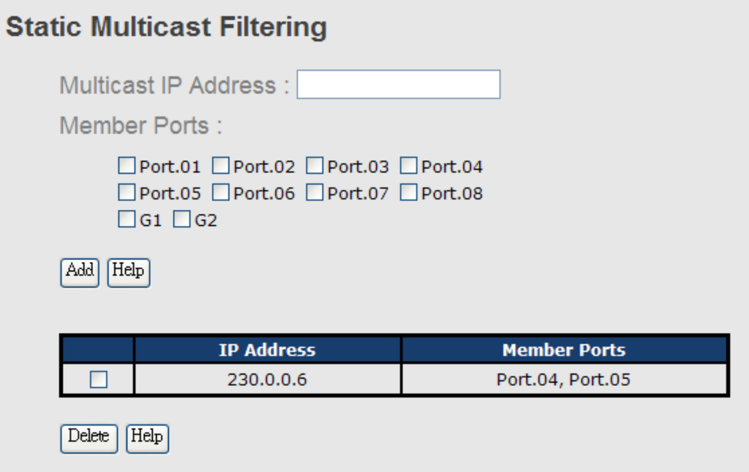
MVR VLAN: 1

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	Enables or disables MVR mode
MVR VLAN	Sets MVR VLAN
TYPE	Sets port type to **inactive**, **Receiver**, or **Source**
Immediate Leave	Enables or disables 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

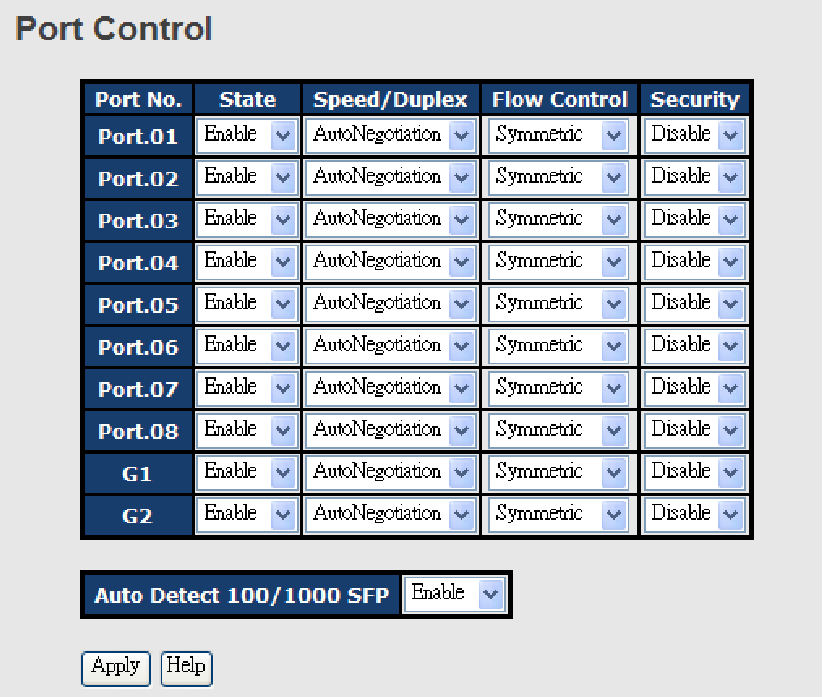
	IP Address	Member Ports
□	230.0.0.6	Port.04, Port.05

Label	Description
IP Address	Assigns 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	Shows current IP multicast list
Delete	Deletes an entry from table
Help	Shows help file.

5.1.3 Port Setting

5.1.3.1 Port Control

The function allows you to 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
G1	Enable	AutoNegotiation	Symmetric	Disable
G2	Enable	AutoNegotiation	Symmetric	Disable

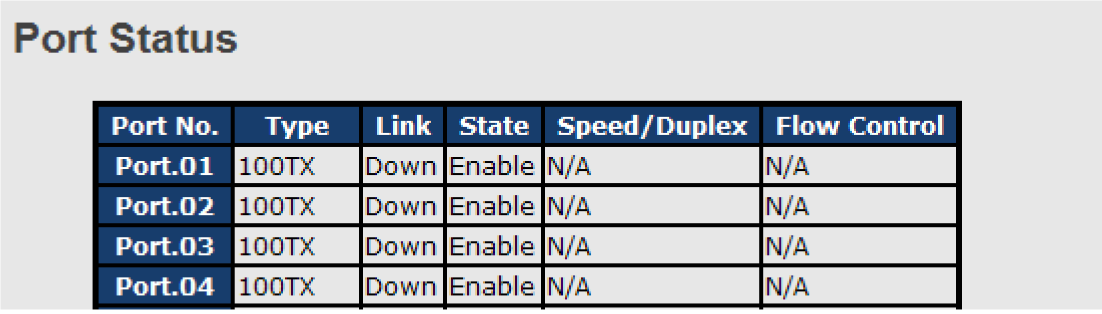
Auto Detect 100/1000 SFP: Enable

Label	Description
Port NO.	Port number for individual settings
State	Enables or disables the port
Speed/Duplex	You can set the value to **AutoNegotiation**, **100-full**, **100-half, 10-full**, or **10-half**.
Flow Control	Supports symmetric and asymmetric modes to avoid packet loss when congestion occurred
Security	Enabling port security will disable MAC address learning in this

	port. Thus only the frames with MAC addresses in the port security list will be forwarded, otherwise will be discarded.
Auto Detect 100/1000	Automatically detects SFP port's SFP module speed (100M / 1000M)
Apply	Click to activate the configurations.

5.1.3.2 Port Status

The following page provides the status information of the current port.

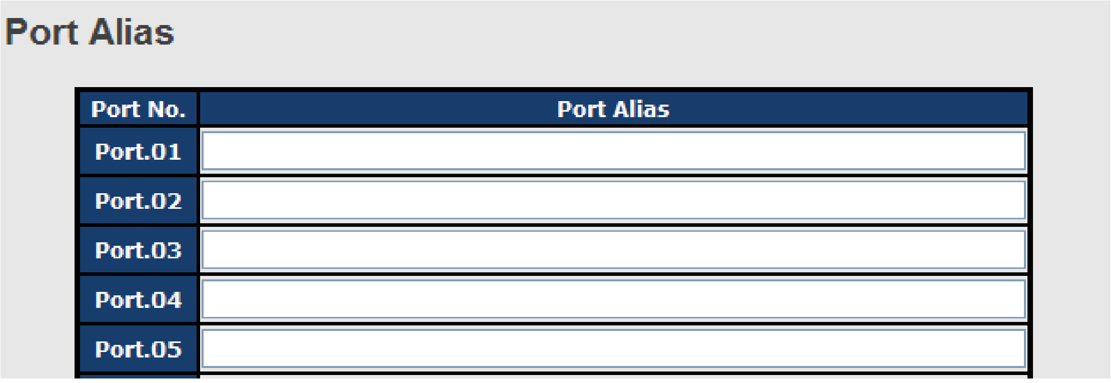


Port Status

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

5.1.3.3 Port Alias

Users can define the name of each port and manage each port easily in this page.

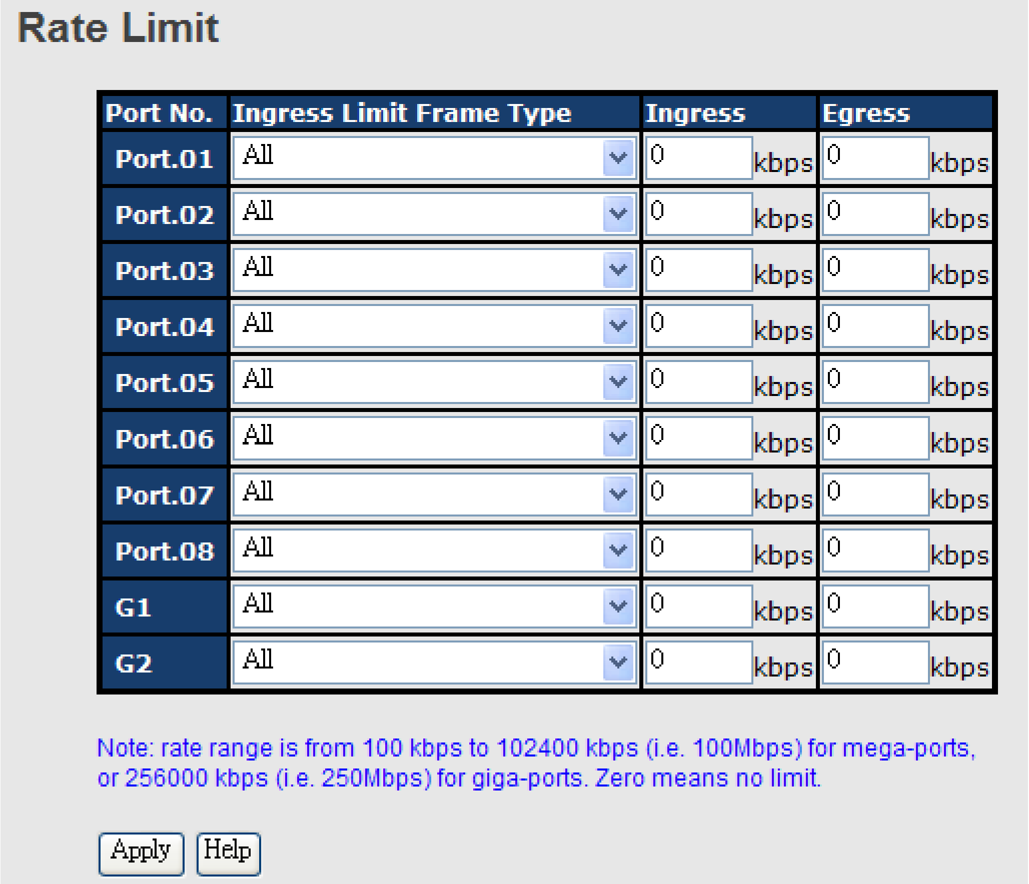


Port Alias

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

5.1.3.4 Rate Limit

This function allows you to limit traffic of all ports, including broadcast, multicast and flooded unicast. You can also set ingress or egress parameters to limit receiving or transmitting bandwidth.



Rate Limit

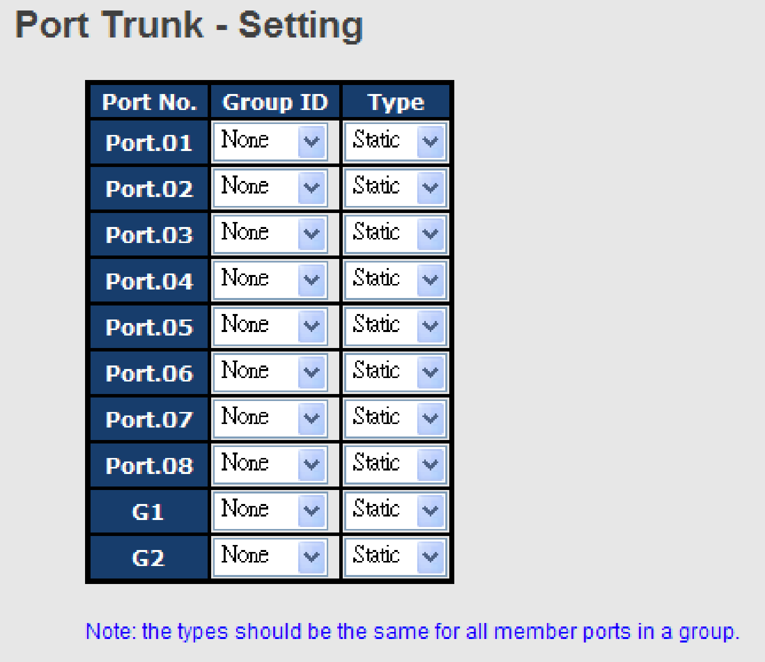
Port No.	Ingress Limit Frame Type	Ingress	Egress
Port.01	All	0 kbps	0 kbps
Port.02	All	0 kbps	0 kbps
Port.03	All	0 kbps	0 kbps
Port.04	All	0 kbps	0 kbps
Port.05	All	0 kbps	0 kbps
Port.06	All	0 kbps	0 kbps
Port.07	All	0 kbps	0 kbps
Port.08	All	0 kbps	0 kbps
G1	All	0 kbps	0 kbps
G2	All	0 kbps	0 kbps

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

Label	Description
Ingress Limit Frame Type	Available values include **all**, **Broadcast only**, **Broadcast/Multicast** and **Broadcast/Multicast/Flooded Unicast**
Ingress	Traffic received at the switch port
Egress	Traffic transmitted from the port
Apply	Click to activate the configurations

5.1.3.5 Port Trunking

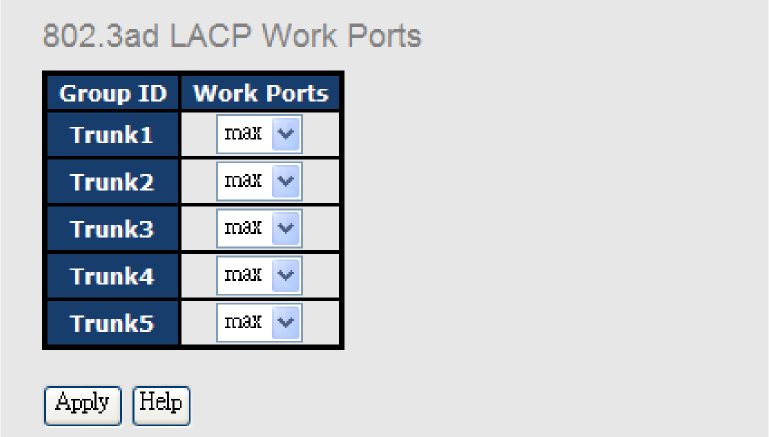
You can select static trunk or 802.3ad LACP to combine several physical links with a logical link to increase the bandwidth.



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
G1	None	Static
G2	None	Static

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

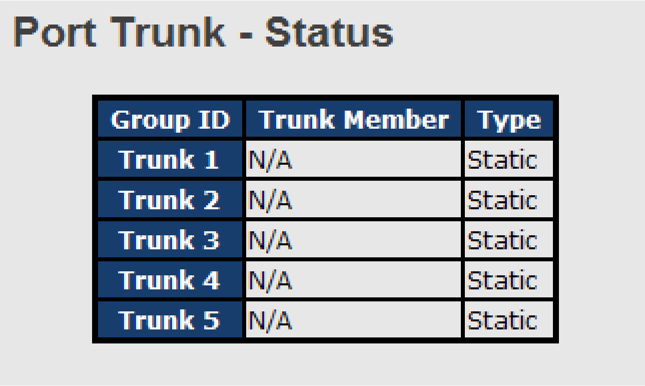


802.3ad LACP Work Ports

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

Label	Description
Group ID	Selects the ports to join a trunk group
Type	Supports static trunk and 802.3ad LACP
Work Port	Selects the number of active ports in dynamic group (LACP). The default value is the maximum number of the group. If the number is not the 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 to activate the configurations

Port Trunk – Status



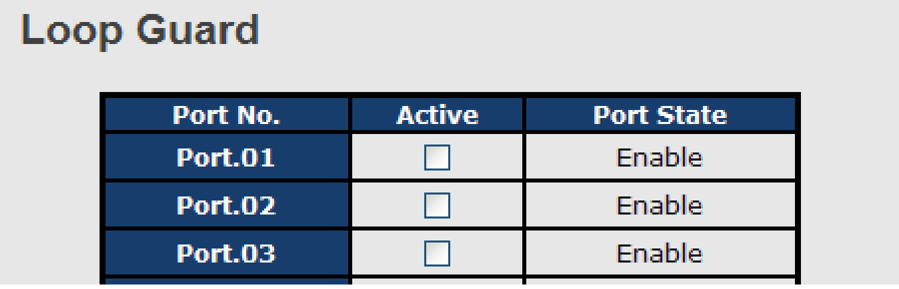
Port Trunk - Status

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

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

5.1.3.6 Loop Guard

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



Loop Guard

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

Label	Description
Active	Enables or disables loop guard
Port Status	Shows port work status

5.1.4 VLAN

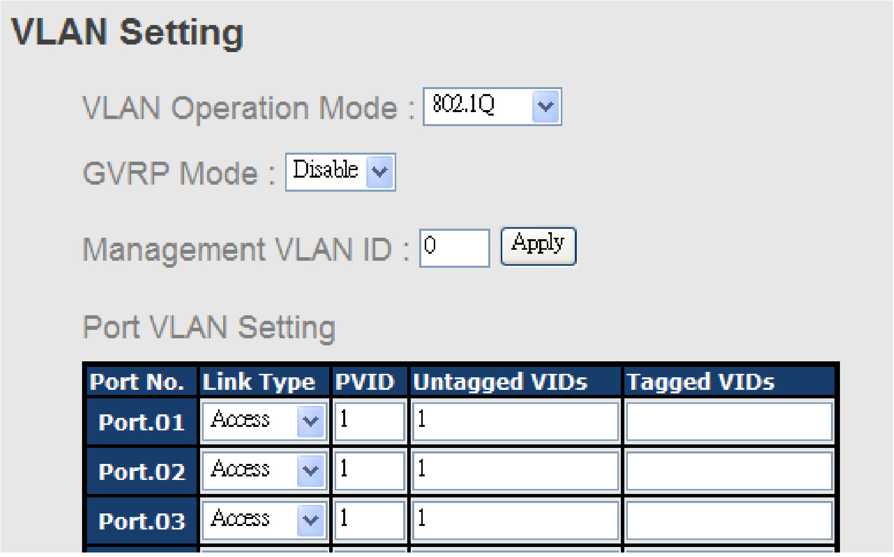
A Virtual LAN (VLAN) is logical network grouping that limits the broadcast domain, which allows you to isolate network traffic. Only the members of the VLAN will receive traffic from the same members of the VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically. The IES-3082GC 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 that can create a VLAN with devices provided by different switch vendors. IEEE 802.1Q VLAN will insert a “tag” which contains a VLAN Identifier (VID) for indicating VLAN numbers into the Ethernet frames.

You can create Tag-based VLAN and enable or disable GVRP protocol. You can configure up to 256 VLAN groups. When enabling 802.1Q VLAN, all ports on the switch will belong to default VLAN whose 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

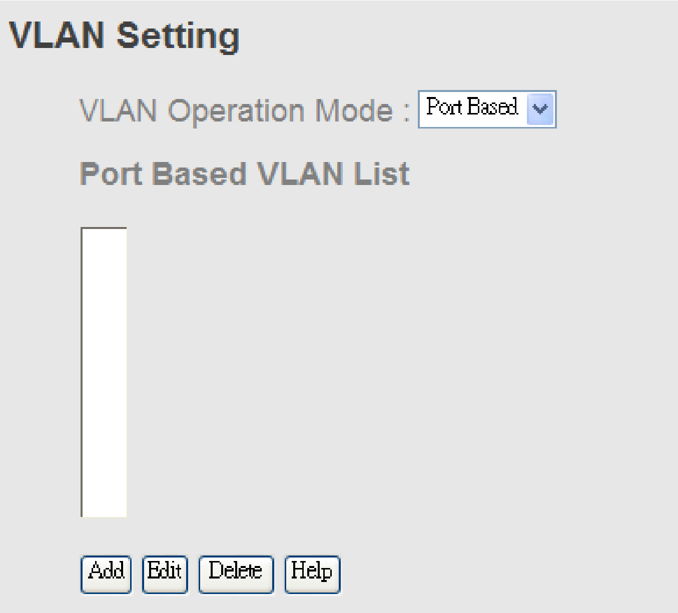
Port No.	Link Type	PVID	Untagged VIDs	Tagged VIDs
Port.01	Access	1	1	
Port.02	Access	1	1	
Port.03	Access	1	1	

Label	Description
VLAN Operation Mode	Configures VLAN operation mode. Available values inlcude **disable**, **Port Base**, and **802.1Q.**
GVRP Mode	Enables or disables GVRP function
Management VLAN ID	Management VLAN enables the network administrator to manage the switch in a secure VLAN environment. Only the devices in the management VLAN can access the switch.
Port	Selects the ports to be configured
Link type	There are three link types: **Access Link:** single switch only, allowing you to group ports by setting the same VID. **Trunk Link:** extended application of **Access Link**, allowing

	you to group ports by applying the same VID to 2 or more switches. **Hybrid Link:** Both **Access Link** and **Trunk Link** are available. **Hybrid (QinQ) Link:** enables QinQ mode, allowing you to insert one more VLAN tags in an original VLAN frame.
Untagged VID	Sets the port to default VLAN ID for untagged devices connected to the port. The range is 1 to 4094.
Tagged VIDs	Sets the tagged VIDs to carry different VLAN frames to other switch
Apply	Click to activate the configurations

5.1.4.2 VLAN Setting – Port Based

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

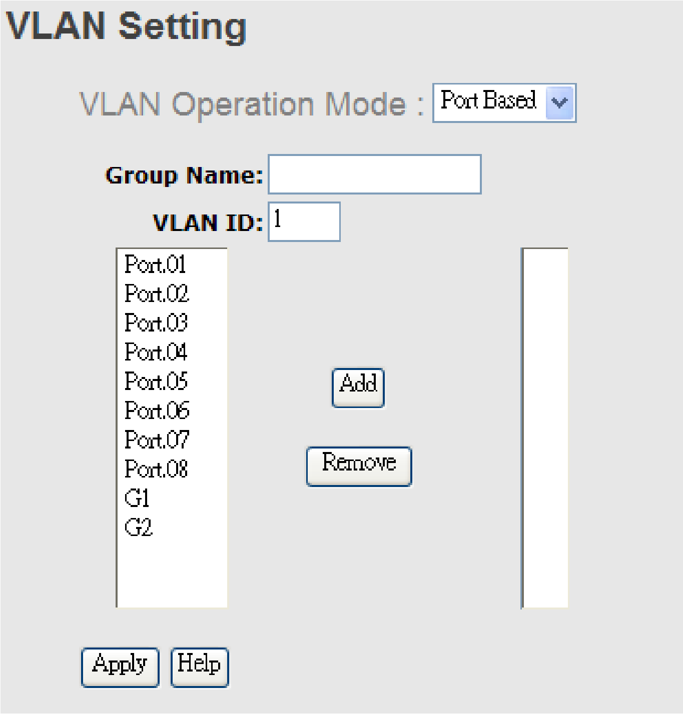


VLAN Setting

VLAN Operation Mode : Port Based

Port Based VLAN List

Label	Description
Add	Click to enter VLAN Add interface
Edit	Edits existing VLAN
Delete	Deletes existing VLAN
Help	Shows help file



VLAN Setting

VLAN Operation Mode : Port Based

Group Name:

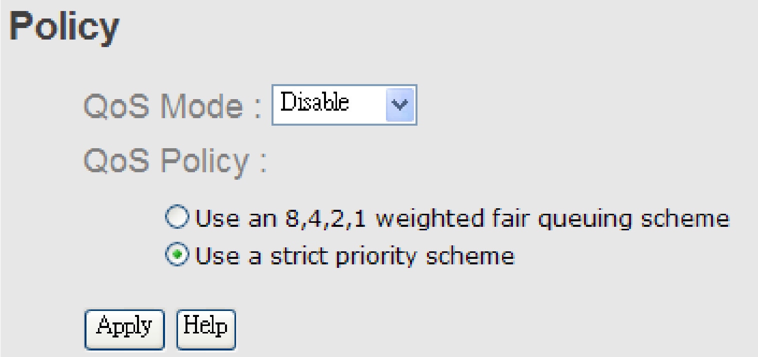
VLAN ID: 1

Label	Description
Group Name	VLAN name.
VLAN ID	Specifies the VLAN ID
Add	Selects ports to join the VLAN group
Remove	Removes ports from the VLAN group
Apply	Click to set the configurations.
Help	Shows help file

5.1.5 Traffic Prioritization

Traffic prioritization includes three modes: port base, 802.1p/COS, and TOS/DSCP. The function enables you to classify the traffic into four classes for differential network applications.

5.1.5.1 QoS Policy



Policy

QoS Mode : Disable

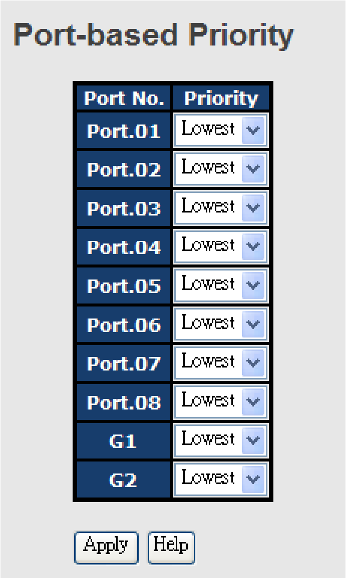
QoS Policy :

○ Use an 8,4,2,1 weighted fair queuing scheme

● Use a strict priority scheme

Label	Description
QOS Mode	■ **Port-base:** output priority is determined by ingress port. ■ **COS only:** output priority is determined by COS only. ■ **TOS only:** output priority is determined by TOS only. ■ **COS first:** output priority is determined by COS and TOS, but COS first. ■ **TOS first:** 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 transmit packets from the highest to lowest queue with a 8:4:2:1 ratio. For example: 8 high queue packets, 4 middle queue packets, 2 low queue packets, and one lowest queue packet are transmitted in one turn. ■ **Use the strict priority scheme:** always transmit packets in higher queue first until higher queue is empty.
Apply	Click to activate the configurations
Help	Shows help file.

5.1.5.2 Port-base Priority



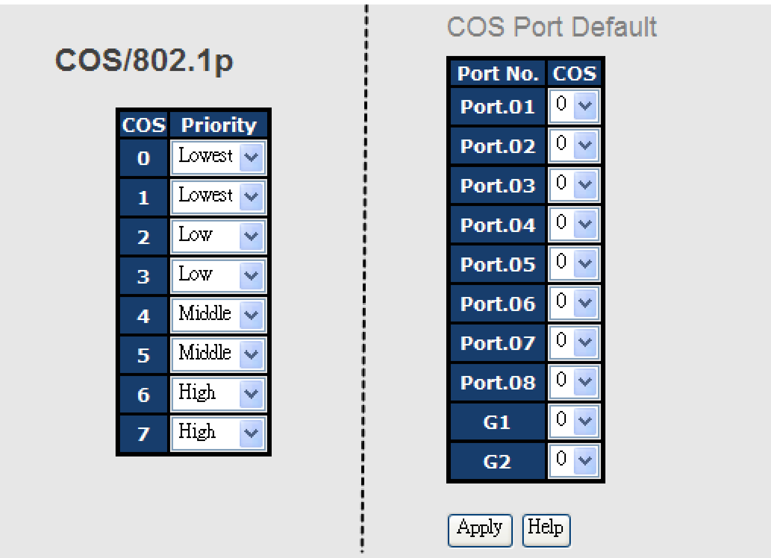
Port-based Priority

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
G1	Lowest
G2	Lowest

Port base Priority	Assigns ports with a priority queue. 4 priority queues can be assigned: **High**, **Middle**, **Low**, and **Lowest**.

Apply	Click to activate the configurations
Help	Shows help file

5.1.5.3 COS/802.1p



COS/802.1p

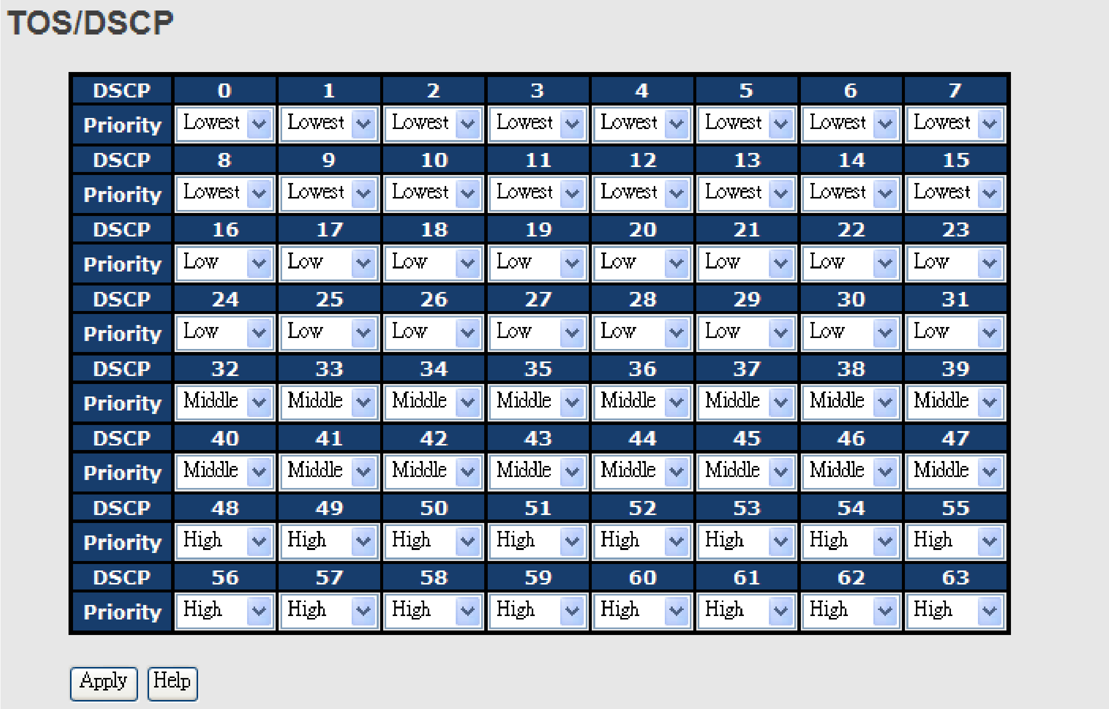
COS	Priority
0	Lowest
1	Lowest
2	Low
3	Low
4	Middle
5	Middle
6	High
7	High

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
Port.08	0
G1	0
G2	0

COS/802.1p	Known as 802.1p, CoS (Class of Service) will prioritize the output of a packet by the setting in 802.1Q VLAN tag. The priority value ranges from 0 to 7. CoS value maps to 4 priority queues: **High**, **Middle**, **Low**, and **Lowest**.
COS Port Default	When an ingress packet has no VLAN tag, a default priority value is considered and determined by ingress port.
Apply	Click to activate the configurations
Help	Shows help file

5.1.5.4 TOS/DSCP



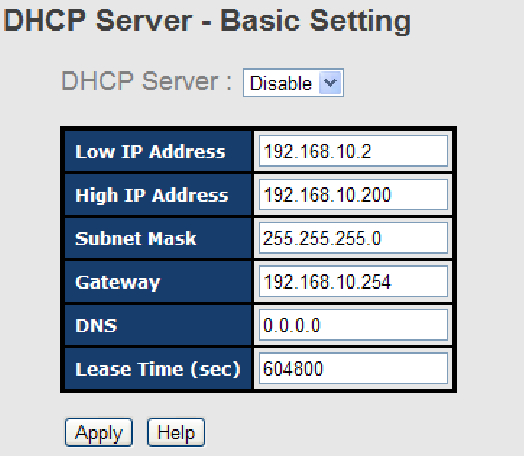
TOS/DSCP

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	ToS (Type of Service) is a field in the IP header of a packet. This ToS field is also used by Differentiated Services and is thus called Differentiated Services Code Point (DSCP). The output priority of a packet can be determined by this field and the priority value ranges from 0 to 63. DSCP value maps to 4 priority queues: **High**, **Middle**, **Low**, and **Lowest**.
Apply	Click to activate the configurations
Help	Shows help file

5.1.6 DHCP Server

5.1.6.1 Basic Setting



DHCP Server - Basic Setting

DHCP Server : Disable

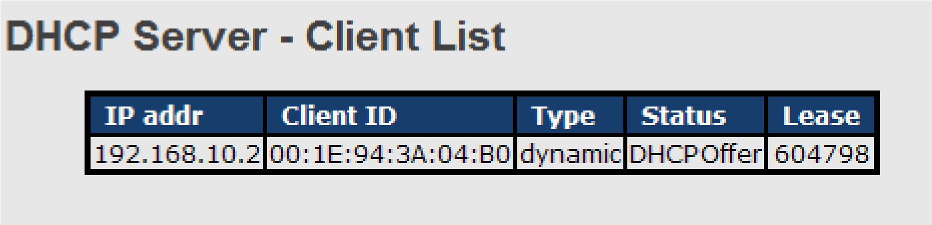
Low IP Address	192.168.10.2
High IP Address	192.168.10.200
Subnet Mask	255.255.255.0
Gateway	192.168.10.254
DNS	0.0.0.0
Lease Time (sec)	604800

The system provides DHCP server function which enables a switch to be a DHCP server when enabled.

Label	Description
DHCP Server	Enables or disables the DHCP server function. When enabled, the switch will be the DHCP server on your local network.
Start IP Address	The dynamic assignment range of IP addresses. The start IP address will be the smallest value. For example, if the dynamic 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 assignment range of IP addresses. The end IP address will be the largest value. For example: if the dynamic range is from 192.168.1.100 to 192.168.1.200, 192.168.1.200 will be the end IP address
Subnet Mask	Subnet mask for the dynamic assignment range of IP addresses
Gateway	Gateway in your network
DNS	The domain name server IP address in your network
Lease Time (Hour)	The period that system will reset the assigned dynamic IP to ensure the IP address is in use
Apply	Click to activate the configurations

5.1.6.2 DHCP Server – Client List

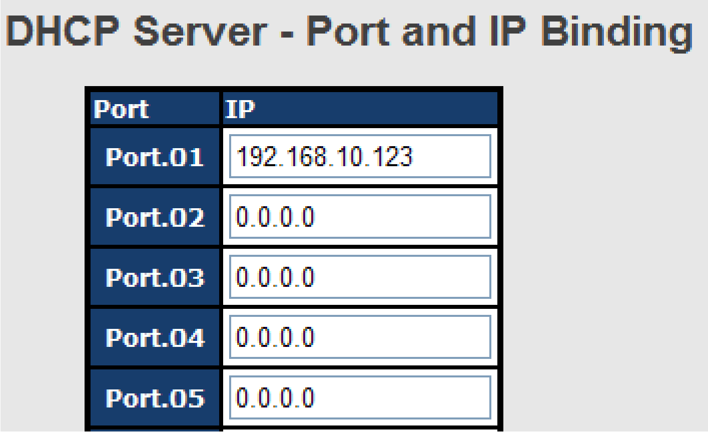
When the DHCP server function is activated, the system will collect the DHCP client information and display here.



DHCP Server - Client List

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

5.1.6.3 DHCP Server – Port and IP Bindings



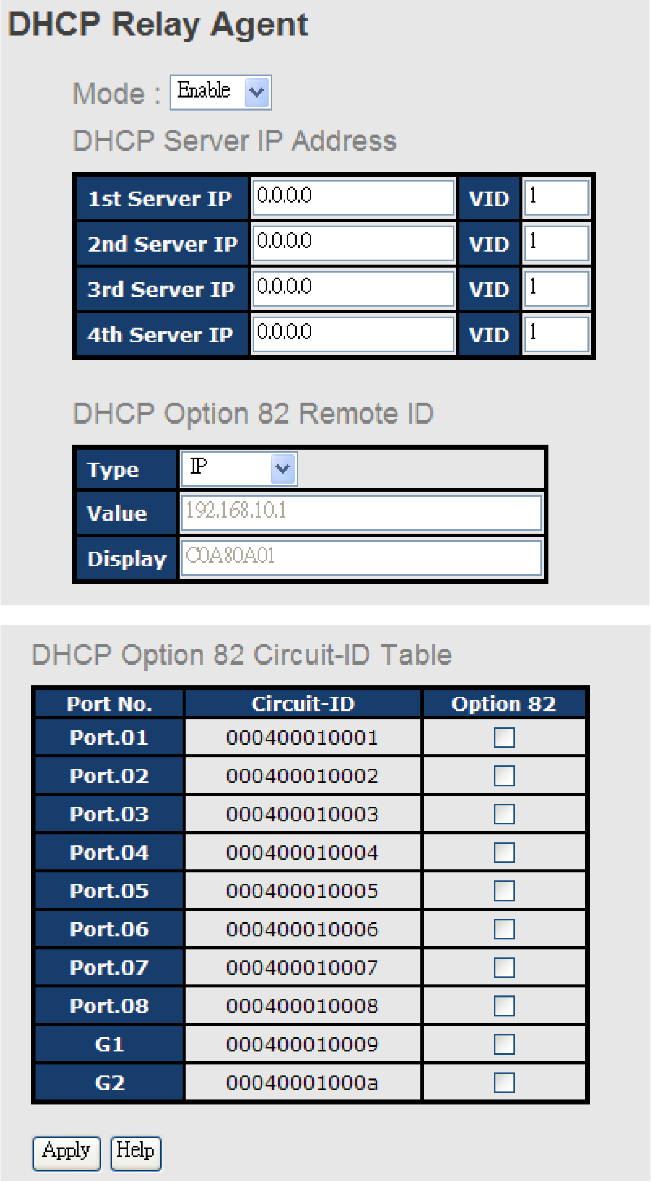
DHCP Server - Port and IP Binding

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

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

5.1.6.4 DHCP Server –DHCP Relay Agent

The DHCP relay agent relays DHCP messages between clients and servers on different subnet domains. DHCP relay agent use Option 82 to insert specific information into a request that is being forwarded to a DHCP server, and removes the specific information from a reply packet according to Option 82 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	□
Port.07	000400010007	□
Port.08	000400010008	□
G1	000400010009	□
G2	00040001000a	□

Label	Description
DHCP Relay	Enables or disables DHCP relay agent
DHCP Server IP Address and VID	Specifies IP address and VID of DHCP server. Keep **0.0.0.0** means the server is inactive.
DHCP Option 82 Remote ID	Provides a identifier for the remote server. Four types are supported: **IP**, **MAC**, **Client-ID**, and **Other**.

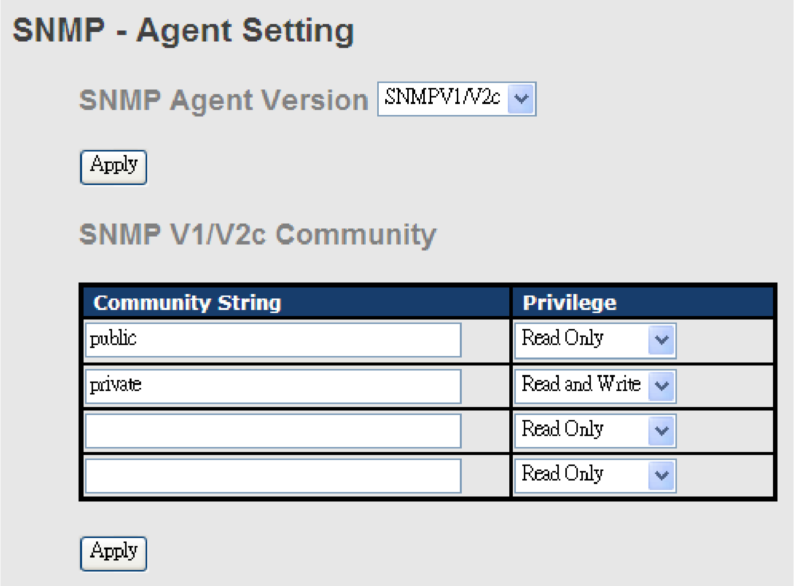
DHCP Option 82 Circuit-ID Table	Encodes an agent-local identifier of the circuit from which a DHCP client-to-server packet is received. It is intended for use by agents in relaying DHCP responses back to the proper circuit.
Apply	Click to activate the configurations.

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 via Agent Setting.



SNMP - Agent Setting

SNMP Agent Version: SNMPV1/V2c

SNMP V1/V2c Community

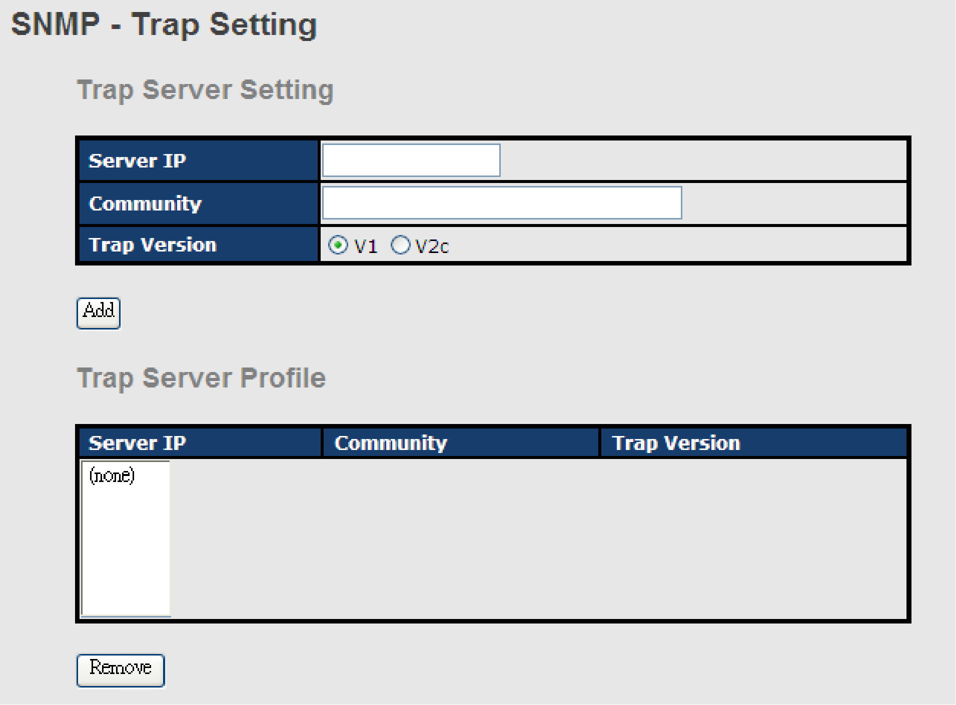
Community String	Privilege
public	Read Only
private	Read and Write
	Read Only
	Read Only

Label	Description
SNMP agent Version	Three SNMP versions are supported: SNMP V1/SNMP V2c, and SNMP V3. SNMP V1/SNMP V2c agent uses a community string match for authentication, meaning SNMP servers access objects with read-only or read/write permissions in line with the default community string (**public** or **private**). SNMP V3 requires an authentication level of MD5 or DES to encrypt data to enhance data security.
SNMP V1/V2c	SNMP community should be set for SNMP V1/V2c. Four sets of

Community	community string/privilege are supported. Each community string can support up to 32 characters. Leave the setting to empty to remove this community string.
Apply	Click to activate the configurations
Help	Shows help file

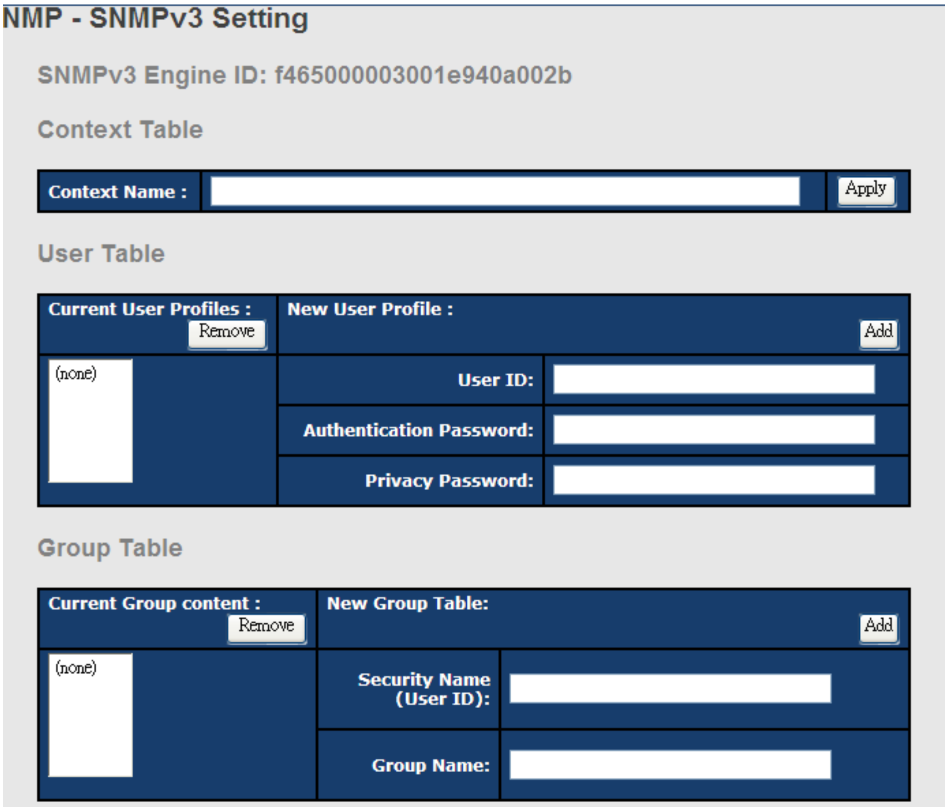
5.1.7.2 SNMP –Trap Setting

A trap manager is a management station that receives traps. Traps are system alerts generated by the switch. If no trap manager is defined, no traps will be issued. You can create a trap manager by entering the IP address of the station and a community string. You can define management stations as trap manager by entering a SNMP community string and selecting the SNMP version.



Label	Description
Server IP	The server IP address to receive traps
Community	Community strings for authentication
Trap Version	Supported trap versions
Add	Adds a trap server profile
Remove	Removes a trap server profile
Help	Shows help file

5.1.7.3 SNMPV3



NMP - SNMPv3 Setting

SNMPv3 Engine ID: f465000003001e940a002b

Context Table

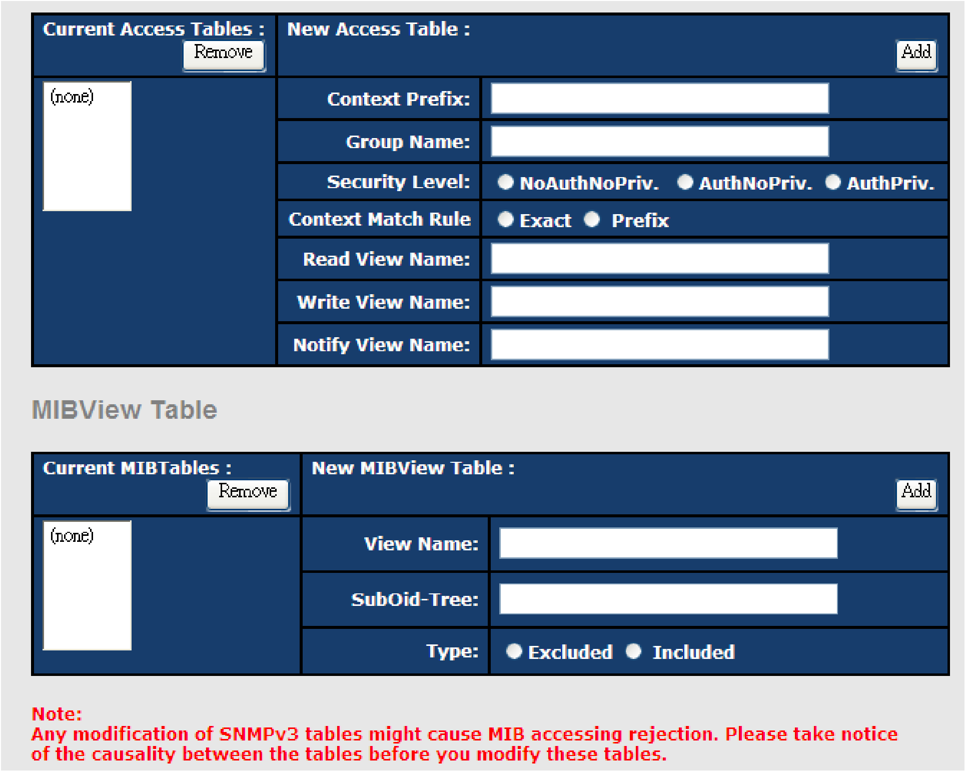
Context Name :		Apply

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.

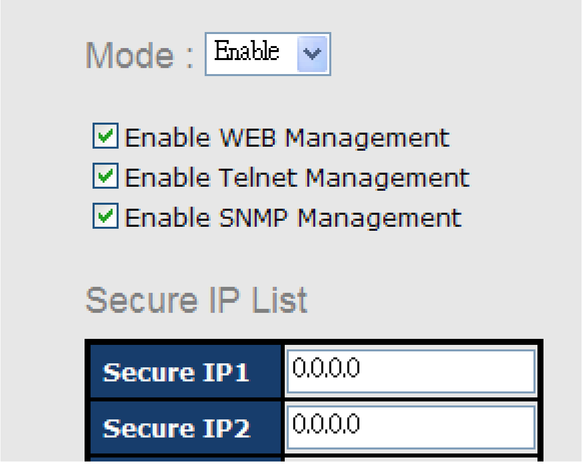
Label	Description
Context Table	Configures SNMP v3. Assigns the context name of a context table. Click **Apply** to change the context name.
User Table	**User ID:** sets up the user name. **Authentication Password**: sets up the authentication password. **Privacy Password**: sets up the private password Click **Add** to add context name. Click **Remove** to remove unwanted context name
Group Table	Configure SNMP v3 group table: **Security Name (User ID)**: assigns the user name that you have set up in user table **Group Name**: sets up the group name Click **Add** to add context name Click **Remove** to remove unwanted context name
Access Table	Configure SNMP v3 access table. **Context Prefix**: sets up the context name **Group Name**: sets up the group **Security Level**: selects the access level **Context Match Rule**: selects the context match rule **Read View Name**: sets up the read view **Write View Name**: sets up the write view **Notify View Name**: sets up the notify view Click **Add** to add context name Click **Remove** to remove unwanted context name
MIBview Table	Configures MIB view table **ViewName**: sets up the name **Sub-Oid Tree**: fills the Sub OID **Type**: selects **Excluded** or **Included** Click **Add** to add context name Click **Remove** to remove unwanted context name
Help	Shows help file

5.1.8 Security

You can enhance security of switch via the following settings: IP security, port security, MAC blacklist, and MAC address assigning and 802.1x protocol.

5.1.8.1 Management Security

Only the IP address 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

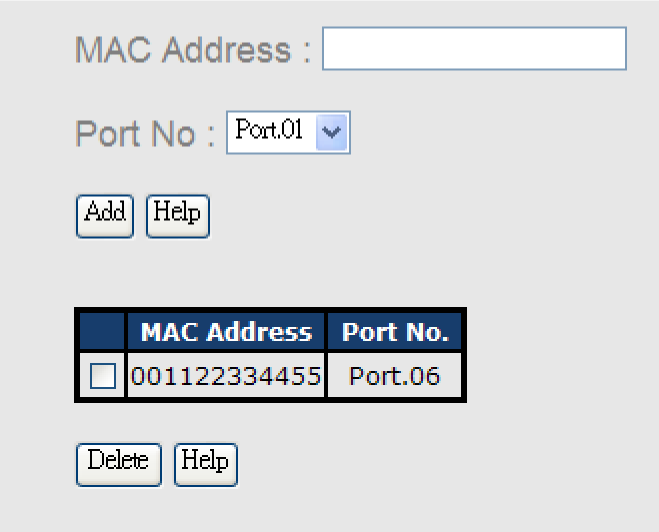
Secure IP List

Secure IP1	0.0.0.0
Secure IP2	0.0.0.0

Label	Description
IP security MODE	Enables and disables the IP security function
Enable WEB Management	Checks to enable WEB management
Enable Telnet Management	Checks to enable Telnet management
Enable SNMP Management	Checks to enable MPSN management.
Apply	Click to activate the configurations
Help	Shows help file

5.1.8.2 Static MAC Forwarding

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

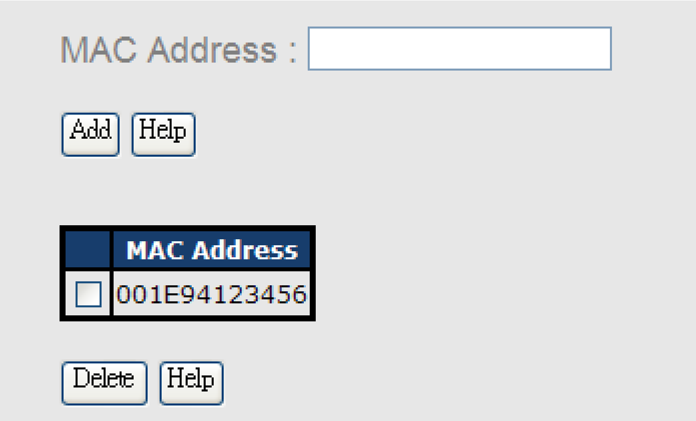


	MAC Address	Port No.
□	001122334455	Port.06

Label	Description
MAC Address	Inputs MAC address to a specific port
Port NO.	Selects ports
Add	Adds an entry of MAC address and port information
Delete	Deletes entry
Help	Shows help file

5.1.8.3 MAC Blacklist

MAC blacklist can stop traffic from being forwarded to specific MAC addresses in the list. Any frames forwarded to the MAC addresses in this list will be discarded. Thus the target device will not receive any frame.



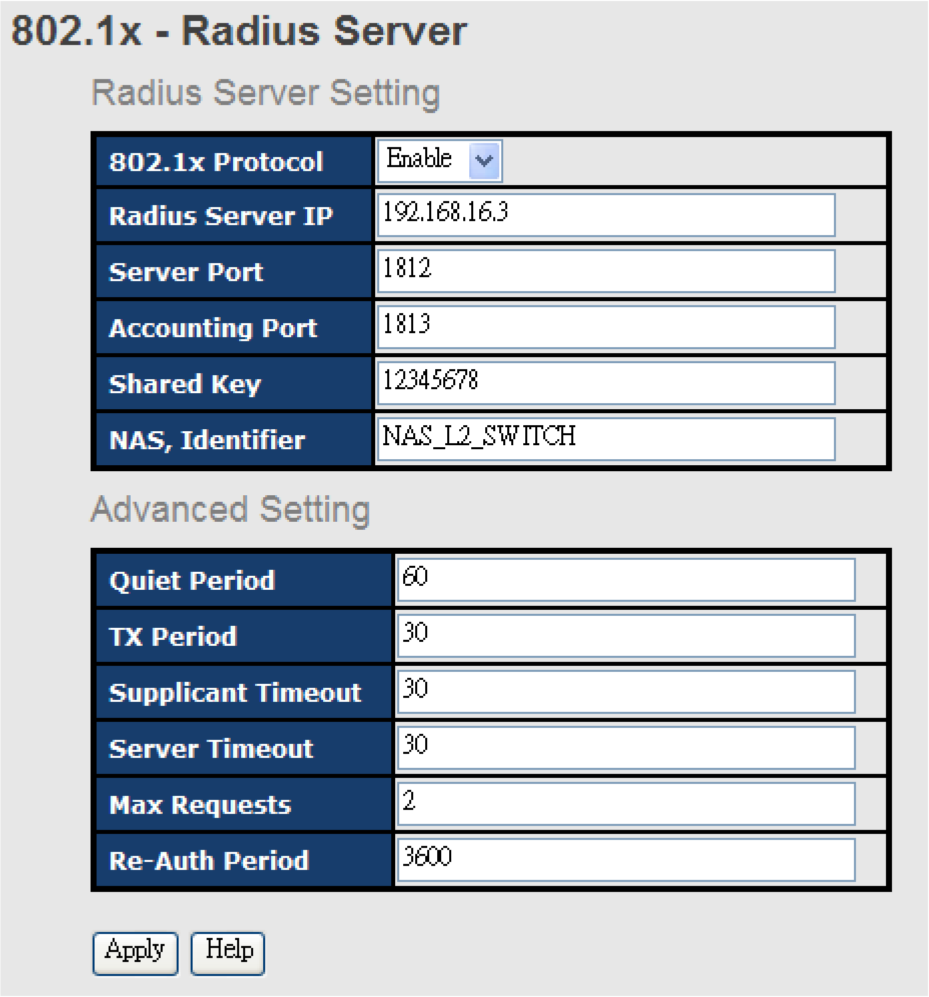
	MAC Address
□	001E94123456

Label	Description
MAC Address	Inputs MAC address to MAC blacklist
Port NO.	Selects ports
Add	Adds an entry to blacklist table
Delete	Deletes entry
Help	Shows help file

5.1.8.4 802.1x

802.1x - Radius Server

802.1x uses the physical access characteristics of the IEEE802 LAN infrastructure to authorize devices attached to a LAN port. Please refer to IEEE 802.1X - Port Based Network Access Control for more information.



802.1x - Radius Server

Radius Server Setting

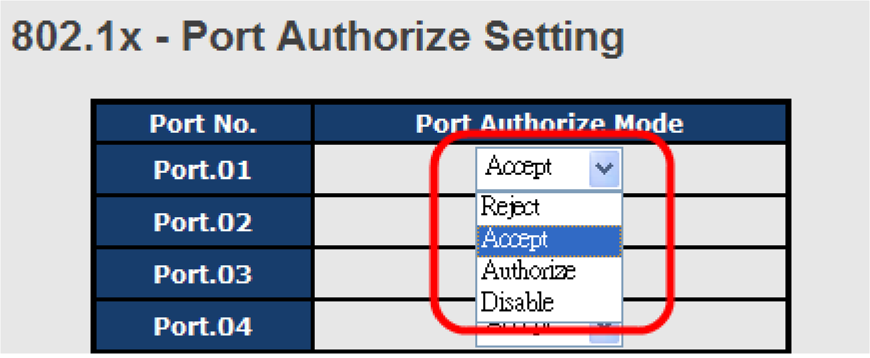
802.1x Protocol	Enable
Radius Server IP	192.168.16.3
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

Advanced Setting

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

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

802.1x Port Authorization Setting

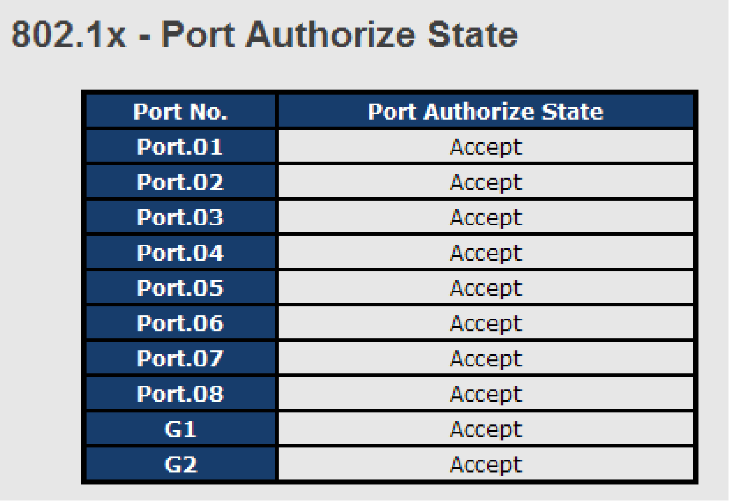


802.1x - Port Authorize Setting

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

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 is determined by the outcome of the 802.1x authentication. **Disable**: this port will not participate in 802.1x
Apply	Click to activate the configurations
Help	Shows help file

802.1x Port Authorization State



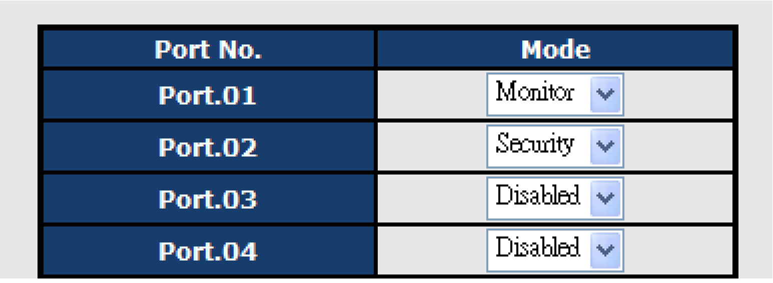
802.1x - Port Authorize State

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
G1	Accept
G2	Accept

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-to-use function for IP security. It protects the network from unknown IP (IPs which are not in the allowed list) attack. The illegal IP traffic will be blocked.

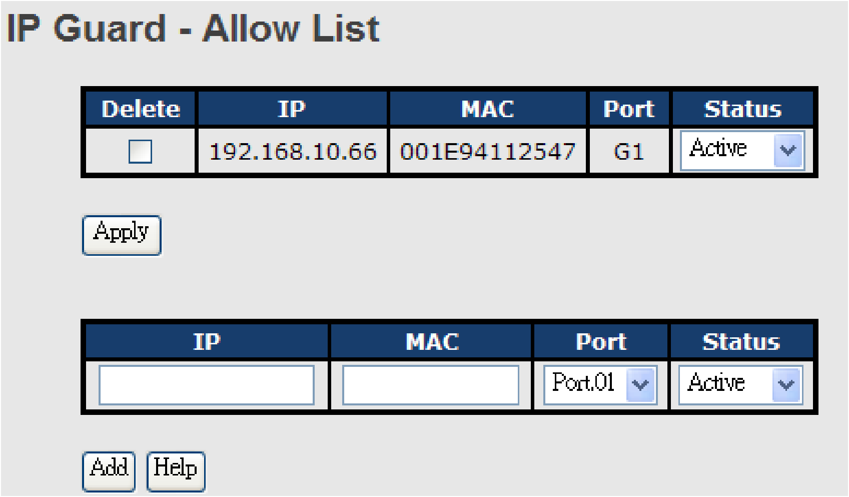


Port No.	Mode
Port.01	Monitor
Port.02	Security
Port.03	Disabled
Port.04	Disabled

Label	Description
Mode	**Disabled**: IP Guard is disabled **Monitor**: IP Guard is disabled, but IP traffic will be monitored constantly. **Security**: IP Guard is enabled and illegal IP traffic will be blocked.
Apply	Click to activate the configurations.
Help	Shows help file

IP Guard – Allow List

This page allows you to configure the IP Guard allowed list. IP traffic will be blocked if it is not in allowed list.



IP Guard - Allow List

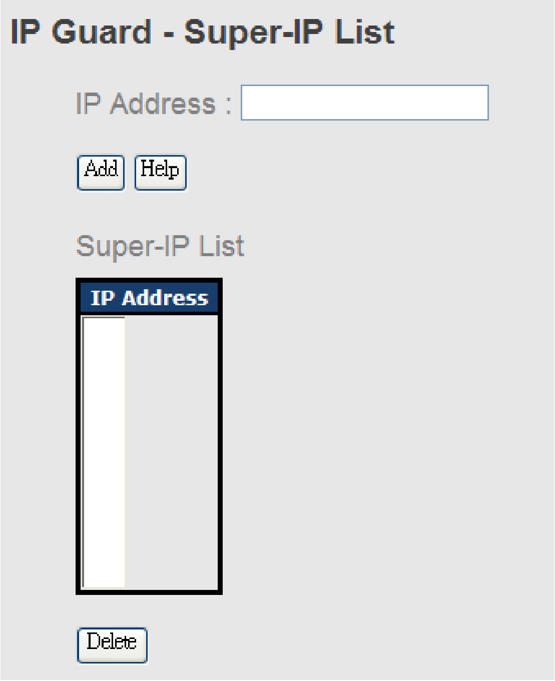
Delete	IP	MAC	Port	Status
□	192.168.10.66	001E94112547	G1	Active

IP	MAC	Port	Status
		Port.01	Active

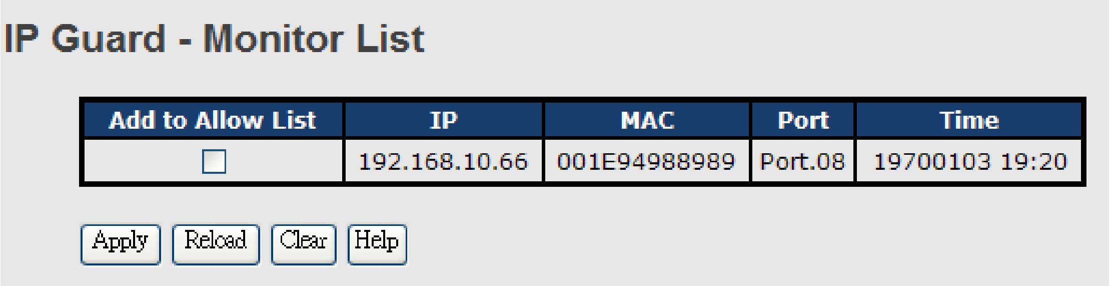
Label	Description
IP	IP address of the allowed entry
MAC	MAC address of the allowed entry
Port	Port number of the allowed entry
Status	If you suspect some allowed IP traffic to be abnormal, you can block the traffic in this field. Active: allow the IP traffic. Suspend: block the IP traffic.
Delete	If you want to delete the entry, please check this box and apply it.

IP Guard – Super-IP List

This page allows you to configure the IP Guard Super-IP list. Super-IP entry has a special priority; the IP has no limitation on MAC address and port binding. Any IP traffic is allowed as long as the IP is in the Super-IP list.



IP Guard – Monitor List


IP Guard - Monitor List

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

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

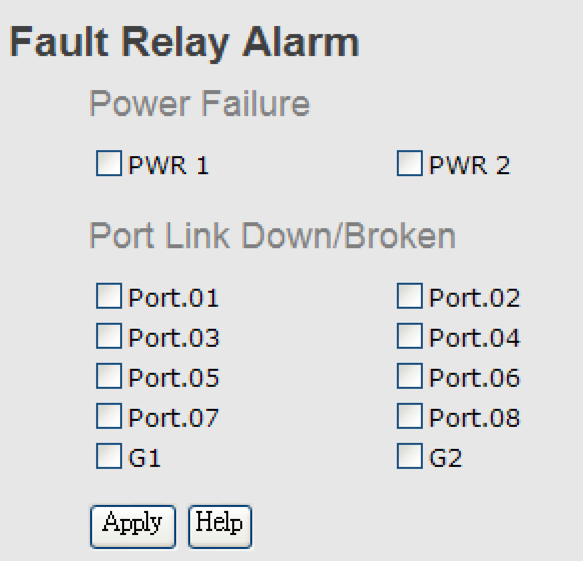
5.1.9 Warning

Warning function is very important for managing switches. You can manage a switch by SYSLOG, email, and fault relay. It helps you to monitor switch status on a remote site. When events occur, a warning message will be sent to your appointed server via email or the faulty relay function.

System alarm supports two warning mode, SYSLOG and email. You can monitor switches for selected system events.

Warning – Fault Relay Alarm

When any selected event happens, the Fault LED on the switch panel will light up and the electric relay will send out signals at the same time.



Fault Relay Alarm

Power Failure

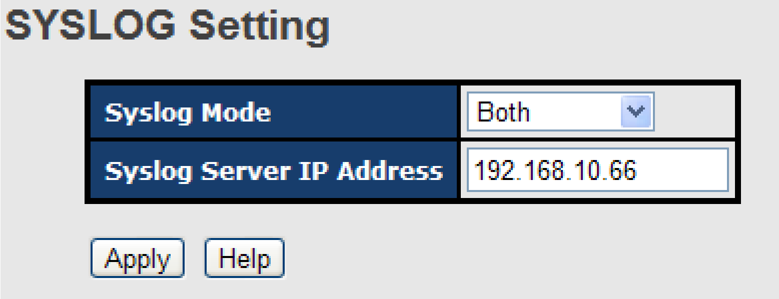
□ PWR 1 □ PWR 2

Port Link Down/Broken

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

System Warning – SYSLOG Setting

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



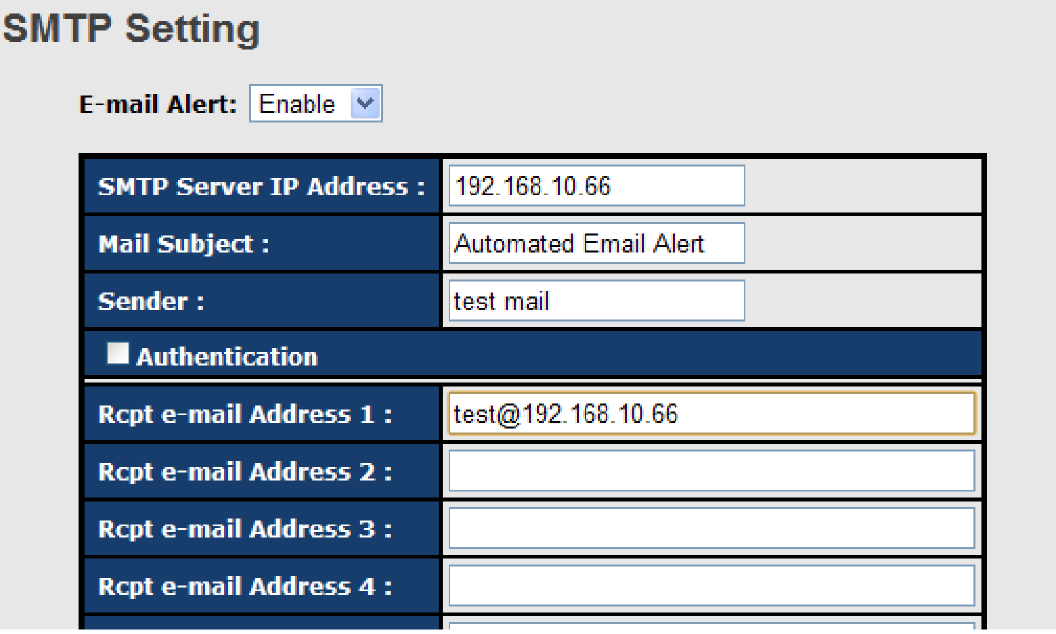
SYSLOG Setting

Syslog Mode	Both
Syslog Server IP Address	192.168.10.66

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

System Warning – SMTP Setting

SMTP (Simple Mail Transfer Protocol) is a protocol for transmitting e-mails across the Internet. Please refer to RFC 821 - Simple Mail Transfer Protocol for more information.



SMTP Setting

E-mail Alert: Enable

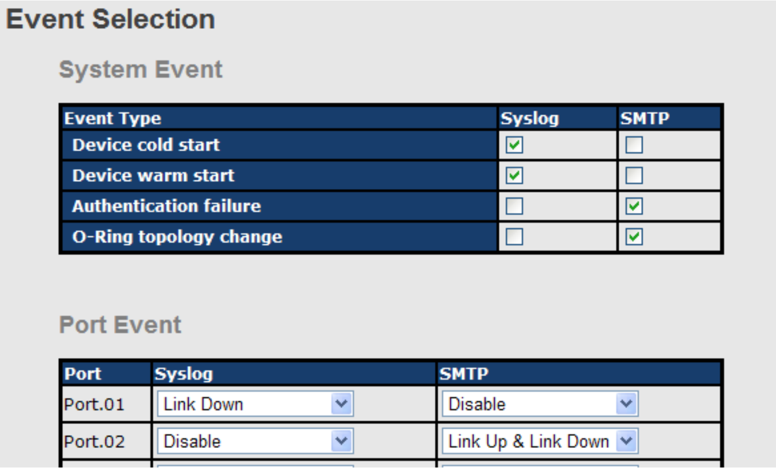
SMTP Server IP Address :	192.168.10.66
Mail Subject :	Automated Email Alert
Sender :	test mail
□ Authentication	
Rcpt e-mail Address 1 :	test@192.168.10.66
Rcpt e-mail Address 2 :	
Rcpt e-mail Address 3 :	
Rcpt e-mail Address 4 :	

Label	Description
E-mail Alert	Enables or disables system to send out warning e-mail during an event
SMTP Server IP Address	Configures mail server IP address
Mail Subject	Subject of the mail
Sender	Configures the email account for send the alert
Authentication	**Username**: authorized username **Password**: authorized password **Confirm Password**: re-enter password

Recipient E-mail Address	The recipient's email address. Up to six recipients are supported in a mail.
Apply	Click to activate the configurations
Help	Shows help file

System Warning – Event Selection

SYSLOG and SMTP are the two warning methods supported by the system. Check the corresponding box to enable the warning you want. Please note that the checkbox cannot 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

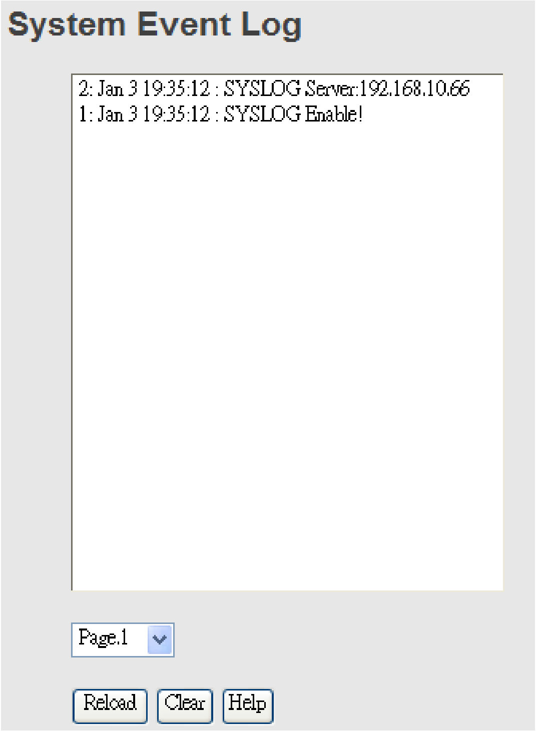
Port	Syslog	SMTP
Port.01	Link Down	Disable
Port.02	Disable	Link Up & Link Down

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	Alerts when SNMP authentication fails
O-Ring topology change	Alerts when O-Ring topology changes
Port Event	Available values include: **Disable**, **Link Up**, **Link Down**, and **Link Up & Link Down**
Apply	Click to activate the configurations
Help	Shows help file

5.1.10 Monitor and Diag

5.1.10.1 System Event Log

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

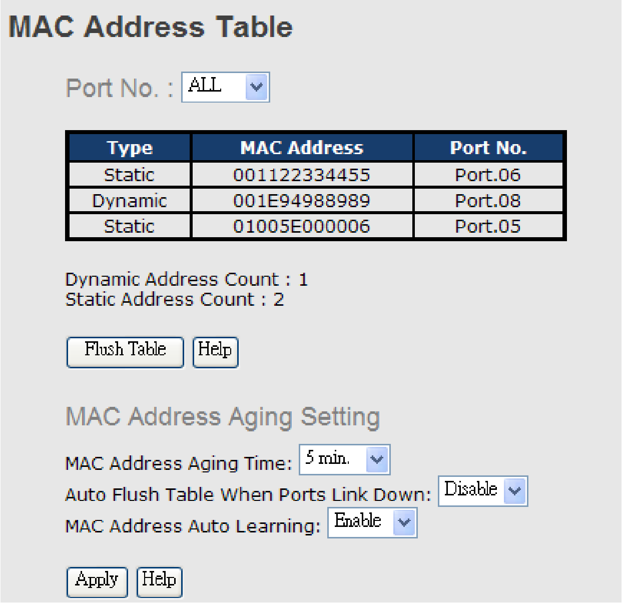


System Event Log

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

Label	Description
Page	Selects LOG page
Reload	Renews to show the newest event logs
Clear	Clear log
Help	Shows help file

5.1.10.2 MAC Address Table



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

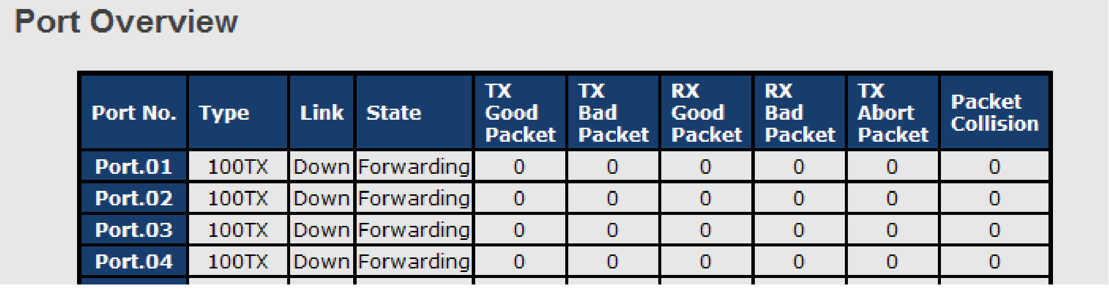
MAC Address Aging Setting

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

A MAC address table (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.

Label	Description
Port NO. :	Shows all MAC addresses mapped to a selected port in the table
Flush MAC Table	Clears all MAC addresses in the table
MAC Address Aging Time	Assigns aging time; the value MUST be multiple of 15.
Auto Flush Table When Ports Link Down	When enabled, the switch will flush MAC table when port link is down.
MAC Address Auto Learning	Enables or disables MAC learning function
Apply	Click to activate the configurations

5.1.10.3 Port Overview



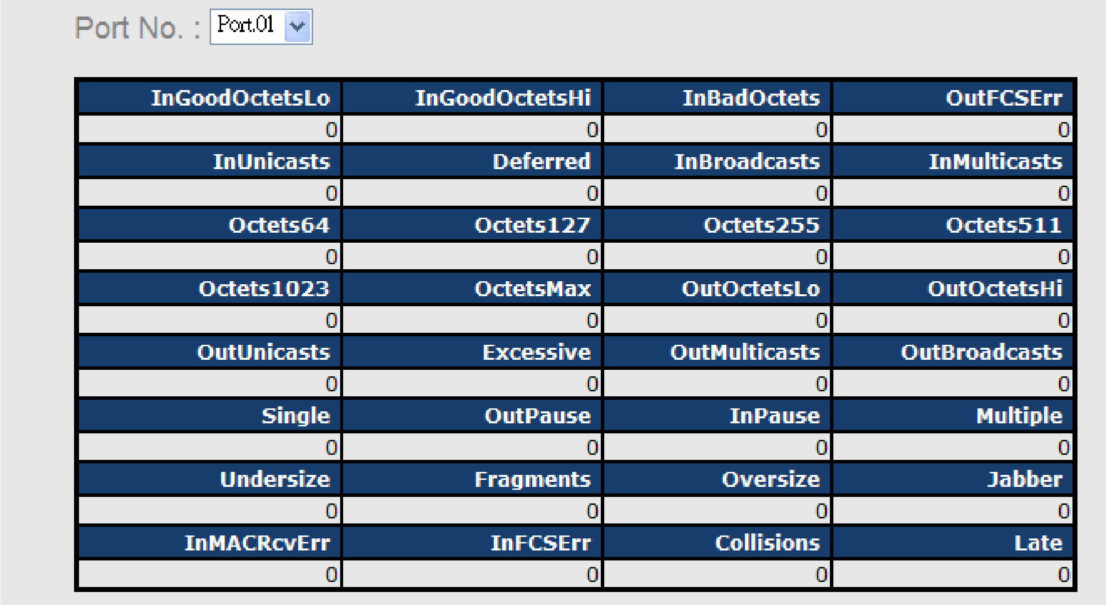
Port Overview

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

Label	Description
Type	Shows port speed and media type
Link	Shows port link status
State	Shows ports enabled or disabled
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	Clears all counters
Help	Shows help file

5.1.10.4 Port Counters

This page shows statistic counters for the port. The **Clear** button will reset all counters to zero.



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

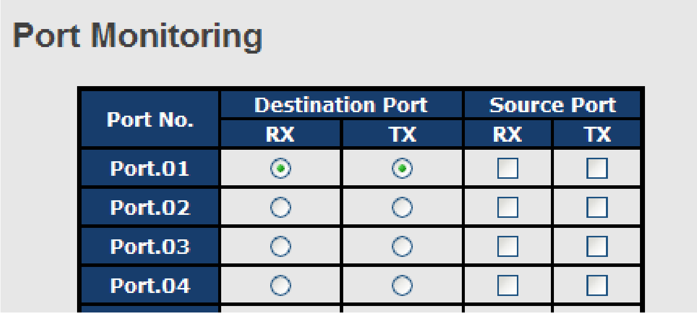
Label	Description
InGoodOctetsLo	The lower 32-bits of the 64-bit InGoodOctets counter. The sum of lengths of all good Ethernet frames received, that is frames that are not bad frames.
InGoodOctetsHi	The upper 32-bits of the 64-bit InGoodOctets counter. The sum of lengths of all good Ethernet frames received, 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

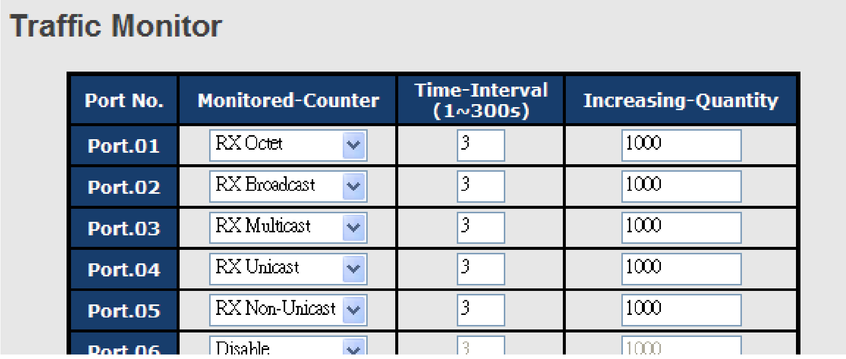
Port No.	Destination Port		Source Port	
	RX	TX	RX	TX
Port.01	◉	◉	□	□
Port.02	○	○	□	□
Port.03	○	○	□	□
Port.04	○	○	□	□

Label	Description
Destination Port	The port will receive a copied frame from source port for monitoring purpose.
Source Port	The port will be monitored. Check in the boxes to configure TX or RX to be monitored.

TX	The frames sent to the switch port
RX	The frames receive at the switch port
Apply	Click to activate the configurations.
Clear	Clear all marked blank (disable the function)
Help	Shows help file

5.1.10.6 Traffic Monitor

The function allows you to monitor switch traffic. If traffic is too large, the switch will sent SYSLOG events or SMTP mails.



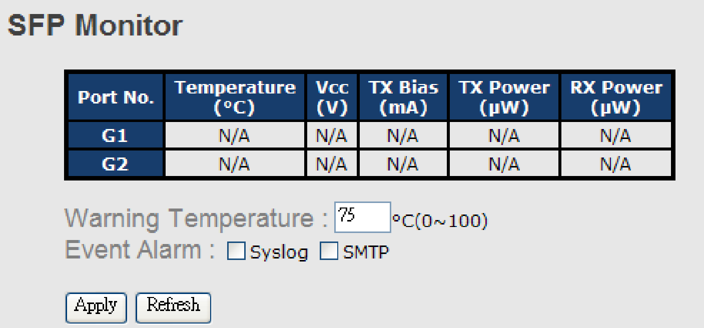
Traffic Monitor

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

Label	Description
Monitored –Counter	Selects monitor type
Time-Interval	Sets interval time
Increasing – Quantity	Sets alarm quantity
Event Alarm	Selects alarm function (SYSLOG or SMTP)

5.1.10.7 SFP Monitor

SFP modules with DDM (Digital Diagnostic Monitoring) function can measure the temperature of the apparatus, helping you monitor the status of connection and detect errors immediately. You can manage and set up event alarms through DDM Web interface.



SFP Monitor

Port No.	Temperature (°C)	Vcc (V)	TX Bias (mA)	TX Power (μW)	RX Power (μW)
G1	N/A	N/A	N/A	N/A	N/A
G2	N/A	N/A	N/A	N/A	N/A

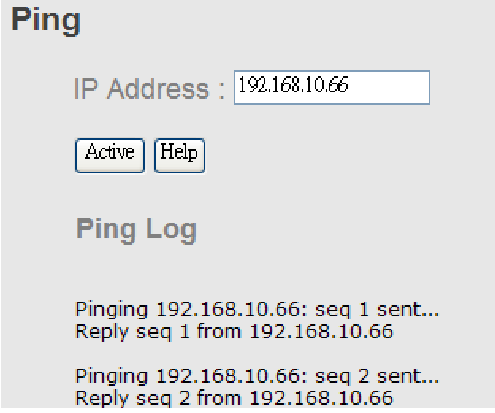
Warning Temperature : 75 °C(0~100)

Event Alarm : □ Syslog □ SMTP

Label	Description
Warning Temperature	Sets warning temperature
Event Alarm	Selects warning method (SYSLOG or SMTP)

5.1.10.8 Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.



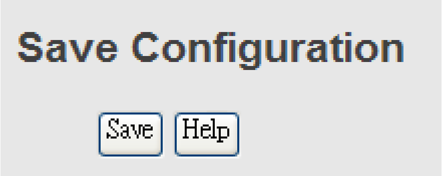
```
Pinging 192.168.10.66: seq 1 sent...
Reply seq 1 from 192.168.10.66

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

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

5.1.11 Save Configuration

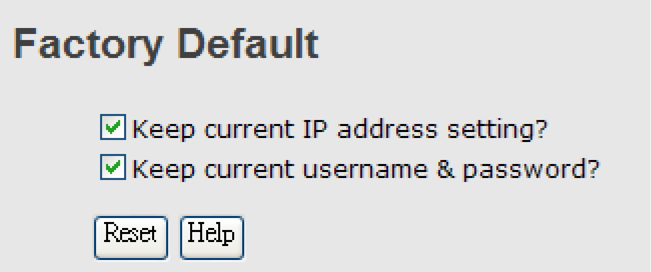
If any configuration is changed, you should click **Save** to save current configuration data to the permanent flash memory. Otherwise, the current configuration will be lost when power is off or system is reset.



Label	Description
Save	Saves all configurations
Help	Shows help file

5.1.12 Factory Default

Reset the switch to default configurations. 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.



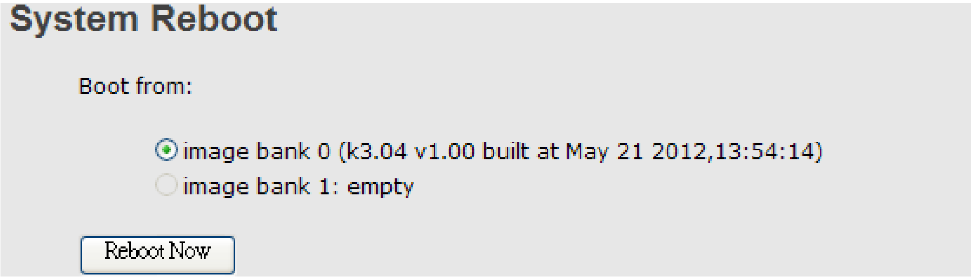
Factory Default

☑ Keep current IP address setting?

☑ Keep current username & password?

5.1.13 System Reboot

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



System Reboot

Boot from:

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

○ image bank 1: empty

Command Line Interface Management

6.1 About CLI Management

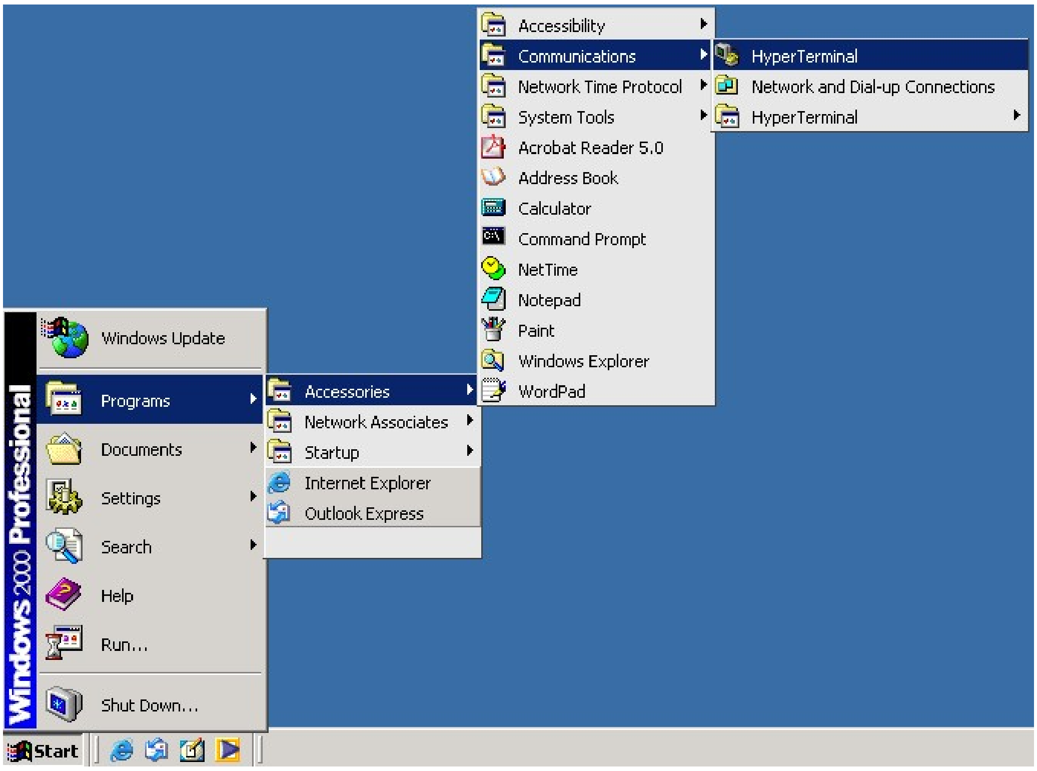
Besides Web-based management, the switch also supports CLI management. You can use console or telnet to manage the switch by CLI.

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

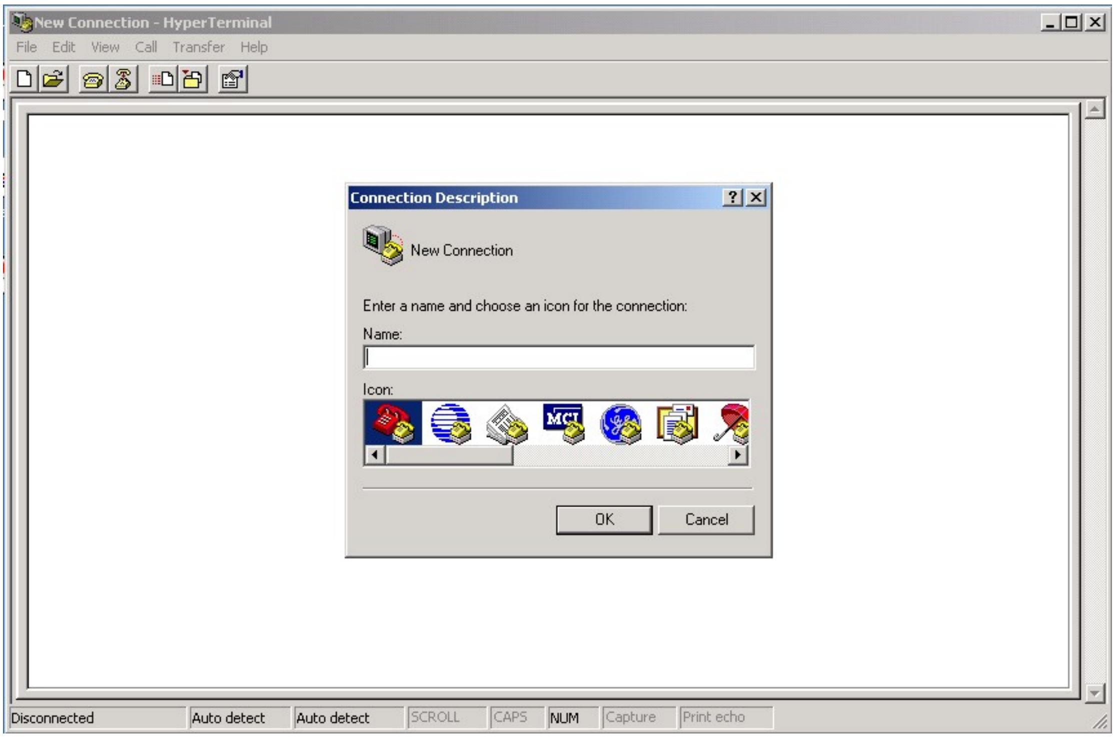
Before configuring RS-232 serial console, connect the RS-232 port of the switch to your PC Com port using a RJ45 to DB9-F cable.

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

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



Step 2. Input a name for new connection



New Connection - HyperTerminal

Connection Description

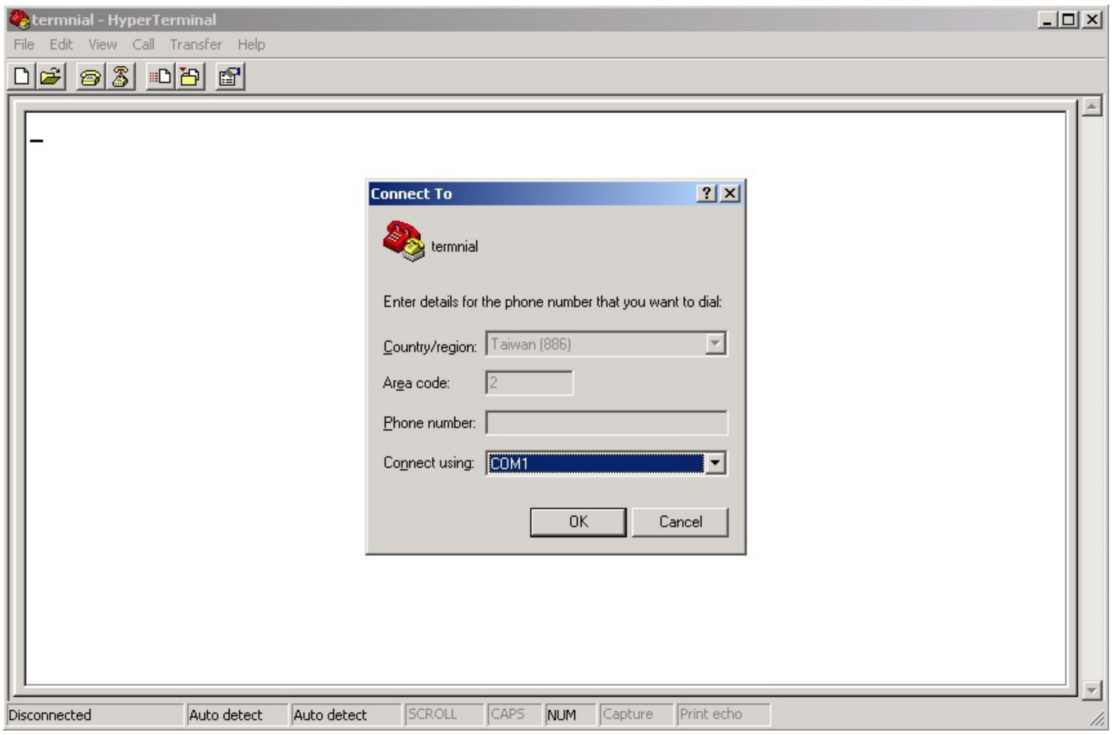
New Connection

Enter a name and choose an icon for the connection:

Name:

Icon:

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



termnial - HyperTerminal

Connect To

termnial

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

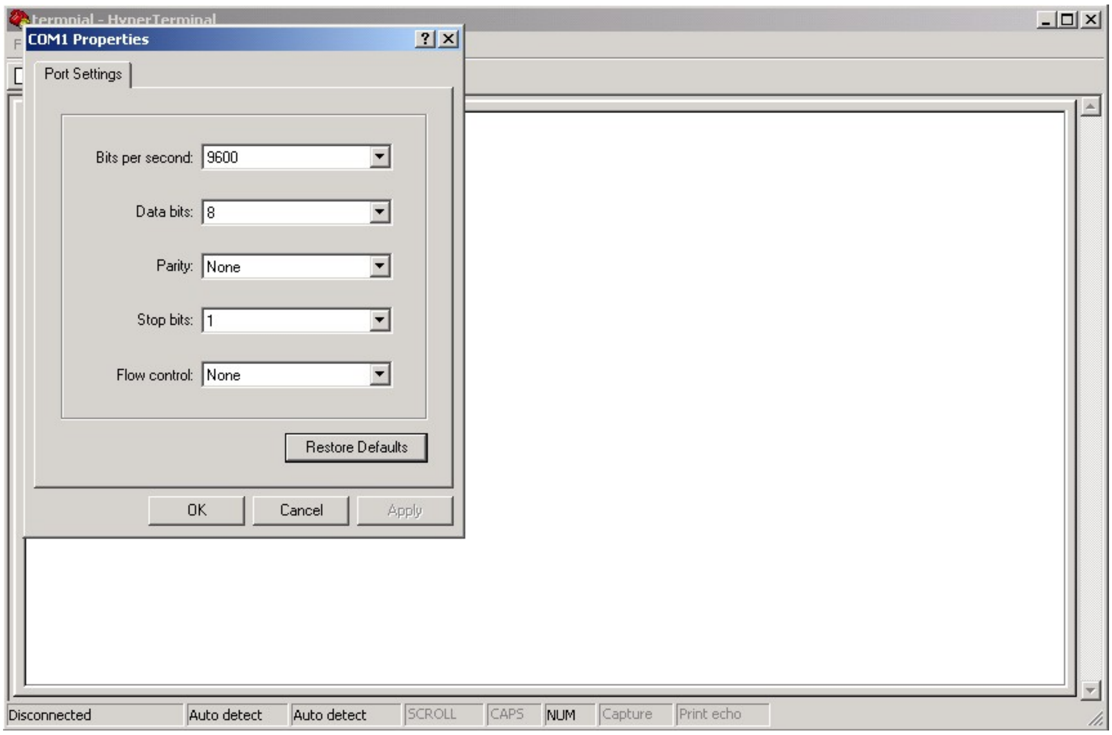
Country/region: Taiwan (886)

Area code: 2

Phone number:

Connect using: COM1

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



Bits per second: 9600

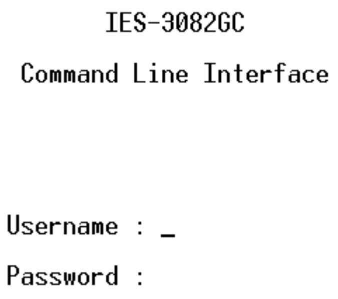
Data bits: 8

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 (same as the password for Web browsers), then press **Enter**.



```
      IES-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**

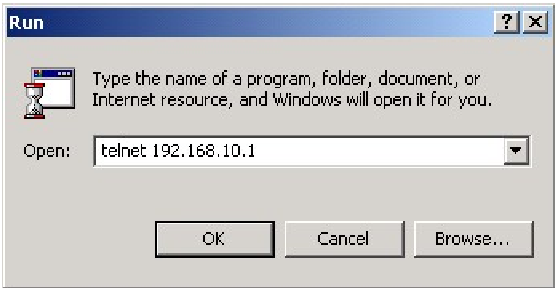
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

Follow the steps below to access the console via Telnet.

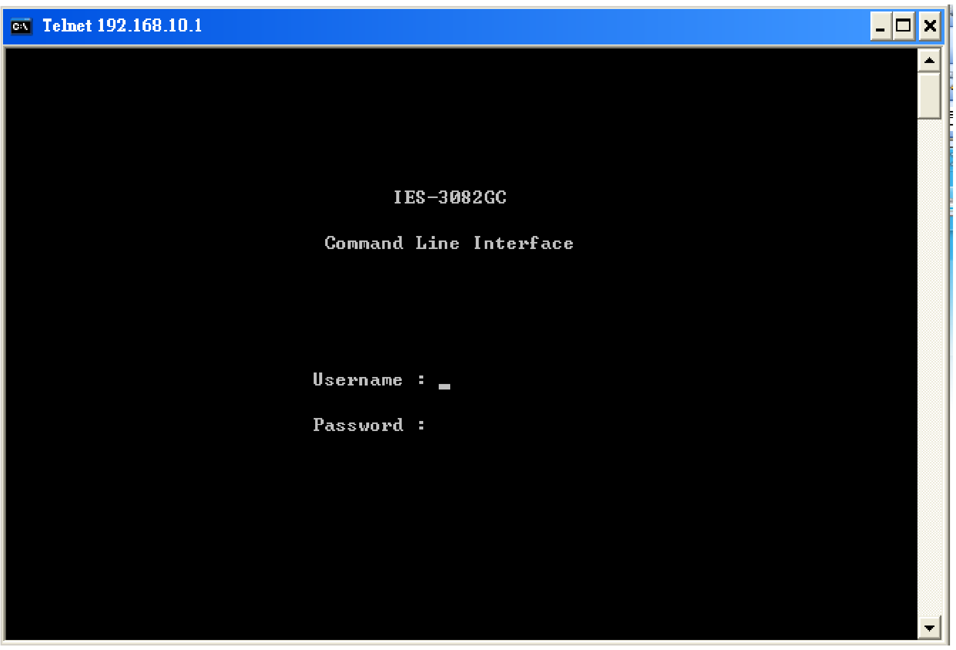
Step 1. Telnet to the IP address of the switch from the **Run** window by inputting commands (or from the MS-DOS prompt) as below.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: telnet 192.168.10.1

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



```
IES-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 Command Set List—System Command Set

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 server	switch#show dhcpserver ip-binding
no dhcpserver	**G**	Disable DHCP server function	switch(config)#no dhcpserver
security enable	**G**	Enable IP security function	switch(config)#security enable
security http	**G**	Enable IP security of HTTP server	switch(config)#security http

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

6.3 Command Set List—Port Command Set

Commands	Level	Description	Example
interface fastEthernet [Portid]	G	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex [full | half]	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
speed [10|100|1000|auto]	I	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
flowcontrol mode [Symmetric|Asymmetric]	I	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion.	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol mode Asymmetric
no flowcontrol	I	Disable flow control of interface	switch(config-if)#no flowcontrol
security enable	I	Enable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#security

			enable
no security	I	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
bandwidth type all	I	Set interface ingress limit frame type to “accept all frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to “accept broadcast, multicast, and flooded unicast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to “accept broadcast and multicast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast
bandwidth type broadcast-only	I	Set interface ingress limit frame type to “only accept broadcast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only
bandwidth in **[Value]**	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth in 100
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 Command Set List—Trunk Command Set

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**	G	Assign a trunk group with LACP active. [GroupID] :1to3	switch(config)#aggregator group 1 1-4 lacp workp 2 or

workp **[Workport]**		[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 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 Command Set List—VLAN Command Set

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**	**V**	Assign a access link for VLAN by port, if the port belong to a trunk group, this command can't be	switch(vlan)#vlan 802.1q port 3 access-link untag 33

[UntaggedVID]		applied.	
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] **access-link untag** [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)#vlan 8021q aggreator 3 access-link untag 33
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 Command Set List—Spanning Tree Command Set

Commands	Level	Description	Example
spanning-tree enable	G	Enable spanning tree	switch(config)#spanning-tree enable
spanning-tree priority [0to61440]	G	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
spanning-tree max-age [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)# spanning-tree max-age 15
spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
spanning-tree forward-time [seconds]	G	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)# spanning-tree forward-time 20
stp-path-cost [1to200000000]	I	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20

		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 Command Set List—QoS Command Set

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|**	G	Configure Port-based Priority	switch(config)#qos priority portbased 1 low

high]			
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 Command Set List—IGMP Command Set

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

6.9 Command Set List—MAC/Filter Table Command Set

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	G	Configure MAC address table(filter)	switch(config)#mac-address-table filter hwaddr

[MAC]			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 Command Set List—SNMP Command Set

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	**G**	Configure the community string right	switch(config)#snmp community-strings public

[Community-string] **right** [RO|RW]			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 Command Set List—Port Mirroring Command Set

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 Command Set List—802.1x Command Set

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 Command Set List—TFTP Command Set

Commands	Level	Description	Defaults Example
backup	G	Save configuration to TFTP and	switch(config)#backup

flash:backup_cfg		need to specify the IP of TFTP server and the file name of image.	flash:backup_cfg
restore flash:restore_cfg	G	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)#restore flash:restore_cfg
upgrade flash:upgrade_fw	G	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#upgrade lash:upgrade_fw

6.14 Command Set List—SYSLOG, SMTP, EVENT Command Set

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	G	Set cold start event type	switch(config)#event

device-cold-start [Systemlog|SMTP|Both]			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 Command Set List—SNTP Command Set

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

6.16 Command Set List—O-Ring Command Set

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-3082GC
Physical Ports	
10/100 Base-T(X) Ports in RJ45 Auto MDI/MDIX	**8**
Gigabit Combo Ports with 10/100/1000Base-T(X) and 100/1000Base-X SFP port	**2**
Technology	
Ethernet Standards	IEEE 802.3 for 10Base-T IEEE 802.3u for 100Base-TX and 100Base-FX IEEE 802.3z for 1000Base-X IEEE 802.3ab for 1000Base-T IEEE 802.3x for Flow control IEEE 802.3ad for LACP (Link Aggregation Control Protocol) IEEE 802.1D for STP (Spanning Tree Protocol) IEEE 802.1p for COS (Class of Service) IEEE 802.1Q for VLAN Tagging IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol) IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol) IEEE 802.1x for Authentication IEEE 802.1AB for LLDP (Link Layer Discovery Protocol)
MAC Table	8192 MAC addresses
Priority Queues	4
Processing	Store-and-Forward
Switch Properties	Switching latency: 7 us Switching bandwidth: 5.6Gbps Max. Number of Available VLANs: 4096 IGMP multicast groups: 1024 Port rate limiting: User Define
Security Features	Enable/disable ports, MAC based port security Port based network access control (802.1x) VLAN (802.1Q) to segregate and secure network traffic Supports Q-in-Q VLAN for performance & security to expand the VLAN space Radius centralized password management SNMP v1/v2c/v3 encrypted authentication and access security
Software Features	STP/RSTP/MSTP (IEEE 802.1D/w/s) Redundant Ring (O-Ring) with recovery time less than 10ms over 250 units TOS/Diffserv supported Quality of Service (802.1p) for real-time traffic VLAN (802.1Q) with VLAN tagging and GVRP supported IGMP Snooping for multicast filtering Port configuration, status, statistics, monitoring, security SNTP for synchronizing of clocks over network Support **PTP Client** (Precision Time Protocol) clock synchronization DHCP Server / Client support Port Trunk support MVR (Multicast VLAN Registration) support Modbus TCP
Network Redundancy	O-Ring Open-Ring O-Chain MRP STP/RSTP/MSTP
Warning / Monitoring System	Relay output for fault event alarming Syslog server / client to record and view events Include SMTP for event warning notification via email

	Event selection support
DDM Function	Voltage / Current / Temperature
RS-232 Serial Console Port	RS-232 in RJ45 connector with console cable. 9600bps, 8, N, 1
LED indicators	
Power	Green : Power LED x 3
O-Ring Indicator	Green : Indicate system operated in O-Ring mode
R.M. indicator	Green : Indicate system operated in O-Ring Master mode
Fault indicator	Amber : Indicate unexpected event occurred
10/100Base-T(X) RJ45 Port Indicator	Green for port Link/Act. Amber for Duplex/Collision
10/100/1000Base-T(X) RJ45 Port Indicator	Green for Link/Act. Amber for 100Mbps indicator
100/1000Base-X Fiber Port Indicator	Green for port Link/Act.
Fault contact	
Relay	Relay output to carry capacity of 1A at 24VDC
Power	
Redundant Input Power	Dual DC inputs. 12~48VDC on 6-pin screw type terminal block
Overload Current Protection	Present
Reverse polarity protection	Present
Physical Characteristic	
Enclosure	IP-30
Dimension (W x D x H)	74.3(W) x 109.2(D) x 153.6(H)mm (2.93 x 4.30 x 6.05 inches)
Environmental	
Storage Temperature	-40 to 85°C (-40 to 185°F)
Operating Temperature	-40 to 70°C (-40 to 158°F)
Operating Humidity	5% to 95% Non-condensing
Regulatory approvals	
EMI	FCC Part 15, CISPR (EN55022) class A, EN50155 (EN50121-3-2, EN55011, EN50121-4)
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11
Shock	IEC60068-2-27
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6
Safety	EN60950-1
Warranty	5 years