iS5 COMMUNICATIONS

SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS

Intelligent 8 Port Managed & Unmanaged Ethernet Switches

iES8(G) Series User's Manual

Version 2.28
May 2021

iS5 Communications Inc.

5895 Ambler Dr.

Mississauga, Ontario, L4W 5B7

Tel: 1 + 905 670 0004

Fax: 1 + 289 401 5201

Website: www.iS5Com.com

E-mail: support@iS5Com.com

www.iS5com.com

COPYRIGHT NOTICE

TRADEMARKS

iS5Com is a registered trademark of iS5. 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

iS5 warrants that all products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). iS5 will repair or replace products found to be defective within this warranty period including shipping costs. This warranty does not cover product modifications or repairs done by persons other than iS5-approved personnel, and this warranty does not apply to products that are misused, abused, improperly installed, or damaged by accident.

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. iS5 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. iS5 reserves the right to revise the contents of this publication without notice.

CONTACT INFORMATION

iS5 Communications Inc.

5895 Ambler Dr., Mississauga, Ontario, L4W 5B7

Tel:1 + 905-670-0004 // Fax:1 + 289-401-5206

Website: www.iS5Com.com

Technical Support E-mail: support@iS5Com.com

Sales Contact E-mail: sales@iS5Com.com

Table of Content

FCC Statement and Cautions

Federal Communications Commission Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment can generate, use, and radiate radio frequency energy. If not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will at his/her own expense, be required to correct the interference.

Caution: LASER

This product contains a laser system and is classified as a CLASS 1 LASER PRODUCT. Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.

Caution: Service

This product contains no user-serviceable parts. Attempted service by unauthorized personnel shall render all warranties null and void.

Changes or modifications not expressly approved by iS5 Communications Inc. could invalidate specifications, test results, and agency approvals, and void the user's authority to operate the equipment.

Should this device require service, please contact support@iS5Com.com.

Caution: Physical Access

This product should be installed in a restricted access location. Access should only be gained by qualified service personnel or users who have been instructed on the reasons for the restrictions applied at the location, and any precautions that have been taken. Access must only be via the use of a tool or lock and key, or other means of security, and is controlled by the authority responsible for the location.

Getting to Know Your Switch

1.1 About the iES8(G) Series Intelligent Managed Switch

The iES8(G) series switches are powerful, managed industrial grade switches with numerous features. These switches can operate under a wide temperature range, dusty environments, and in humid conditions. The switches can be managed either by using the WEB, TELNET, directly using the Console port on the switch, or any third-party SNMP software. The switch can also be managed by our own Network Management Suite called *"iManage"*. *iManage* has a friendly and powerful interface which can be easily used to configure multiple switches at the same time, and also monitor their status.

1.2 Software Features

- World's fastest Redundant Ethernet Ring (Recovery time < 30ms with up to 250 units)
- Supports Ring Linking, Dual Homing over iRing, and standard STP/RSTP
- Supports SNMPv1/v2c/v3 & RMON & Port base/802.1Q VLAN Network Management
- Event notification by Email, SNMP trap and Relay Output
- Web-based ,Telnet, Console, CLI configuration
- Enable/disable ports, MAC based port security
- Port based network access control (802.1x)
- 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)

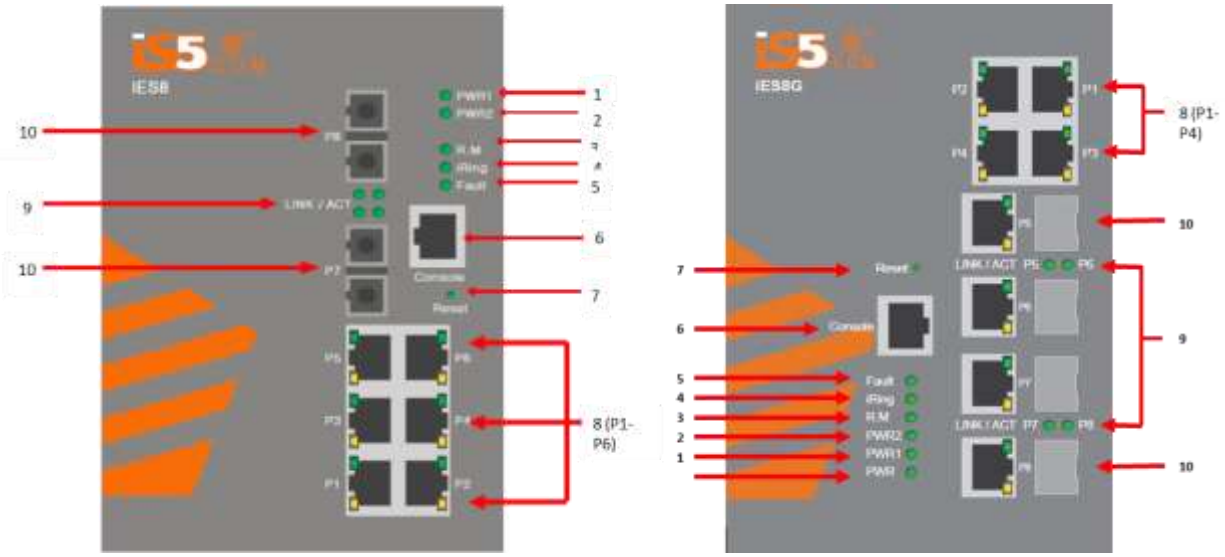
1.3 Hardware Features

- 6 x 10/100Base-T(X) Ethernet ports
- 2 x 10/100Base-T(X) Ethernet ports (Optional – iES8 version)
- 2 x 100Base-F(X) SC or ST Fiber ports (Optional – iES8 version)
- 2 x 1000Base-X SC or ST Fiber ports (Optional – iES8G version)
- Console Port
- Dual Input low-voltage (LV) DC (10-48VDC)
- Dual Input medium-voltage (MV) DC (36-75VDC)

- Single Input Hi-voltage (HV) AC/DC input (85-264VAC, 88-300VDC) with Single (10-48VDC) backup
- Wide Operating Temperature: -40 to 85°C
- Storage Temperature: -40 to 85°C
- Operating Humidity: 5% to 95%, non-condensing
- Chassis: IP-40 Galvanized Steel
- Dimensions(W x D x H) : 101.6 mm(W)x 128.3 mm(D)x 153.6 mm(H) (4 in x 5.05 in x 6.05 in)

Hardware Overview

2.1 Front Panel



iES8 Product description:

Port	Description
Ports 1-6 10/100 RJ45 fast Ethernet ports (8)	6 x 10/100Base-T(X) RJ45 fast Ethernet ports support auto-negotiation. Default Setting : Speed: auto Duplex: auto Flow control : disable
Ports 7 -8 (10)	2 x 10/100Base-T(X) RJ45 fast Ethernet ports (Optional, iES8 model) 2 x 100Base-F(X) SC or ST ports (Optional, iES8 model) 2 x 1000Base-X SC or ST ports (Optional, iES8G model)
Console (6)	Use a RS232 to RJ45 cable to manage switch.
Reset (7)	Push and hold the reset button for 2 to 3 seconds to reset the switch. Push and hold the reset button for 5 seconds to reset the switch into **Factory Default.**

Note: Ports 7 and 8 (Ref 10) Fiber option shown for reference only. Ports are also available as RJ45.

iES8G Product description:

Port	Description
Ports 1-4 10/100/1000 RJ45 fast Ethernet ports (8)	4 x 10/100/1000Base-T(X) RJ45 Ethernet ports support auto-negotiation. Default Setting : Speed: auto Duplex: auto Flow control : disable
Ports 4 -8 (10)	4 x 10/100/1000Base-T(X) RJ45 Ethernet ports (Optional, iES8G model) 4 x 100/1000Base-F(X) SFP ports (Optional, iES8G model) 4 x Combo Port 10/100/1000Base TX RJ45 and 4x 100/1000 (X) (Optional, iES8G model)
Console (6)	Use a RS232 to RJ45 cable to manage switch.
Reset (7)	Push and hold the reset button for 2 to 3 seconds to reset the switch. Push and hold the reset button for 5 seconds to reset the switch into **Factory Default.**

Front Panel LED's:

Item	Description	Color	Status	Function
1	PWR1	Green	On	Power supply 1 operational.
2	PWR2	Green	On	Power Supply 2 operational.
3	R.M	Green	On	Switch operating as iRIng Master.
4	iRing	Green	On	iRing enabled.
			Slowly blinking	iRing topology broken.
			Fast blinking	iRing working normally.
5	Fault	Amber	On	Fault relay. Power failure or Port down/fail.
Ports 1 to 6 - 10/100Base-T(X) Fast Ethernet ports				
8	LNK / ACT	Green	On	Port link up.
			Blinking	Data transmitted.
	Full Duplex	Amber	On	Port works under full duplex.
Ports 7 – 8 Optional 10/100Base-T(X) or 100Base-F(X) or 1000Base-X				
9	ACT	Green	On	Port link up.
			Blinking	Data transmitted.
	LNK	Amber	On	Port link up.

2.2 Rear

The image below shows the DIN bracket on the back of the switch. Circled in red are the mounting holes for the Panel bracket mounting option.

2.3 Bottom

The image below shows the 10 position terminal block and ground lug of the iES8(G) switch.

2.4 Side

The image below shows the side if the switch with the product label displaying switch information. Circled in red are the side mounting holes for the Panel bracket mounting option.

Hardware Installation

3.1 DIN Rail Mounting

Each switch has a DIN-Rail bracket on the rear panel that allows the switch to be mounted on a DIN Rail. To mount the switch on a DIN Rail follow the steps below.

1. Slant the top of the switch back and hook the top of the DIN bracket onto the top of the DIN rail.

2. Push the bottom of the switch towards the DIN Rail until in clicks in to place.

Note: To release the switch from the DIN Rail, pull the latch at the bottom of the switch down to release the DIN bracket from the DIN Rail. While pulling the latch down, pull the bottom of the switch away from the DIN Rail. The switch will now lift off of the DIN rail.

3.2 Panel Mounting Option

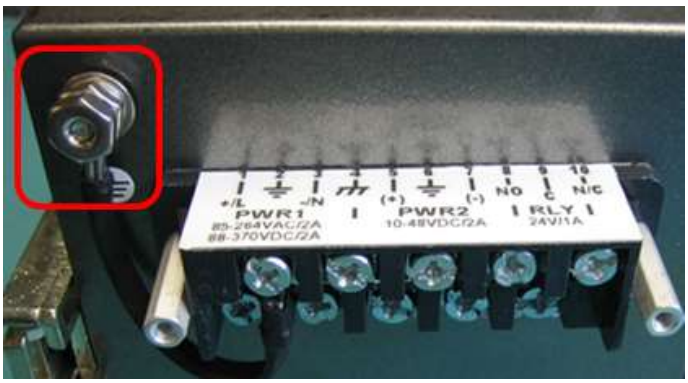
The switch can also has an option to be panel or wall mounted. The following steps show how to mount the switch on a panel or wall.

1. Install the Panel mounting hardware onto the switch. The user can choose rear mounting or side mounting. Note: To avoid damage to the unit please use the 4 screws provided to install the panel mount brackets onto the switch.

2. Use the holes in the brackets to secure the switch to a wall or panel.

3.3 Chassis Ground Connection

The iES8(G) chassis ground connection uses a #6-32 Screw. We recommend terminating the ground connection using a #6 ring lug, and a torque setting of 15 in.lbs (1.7Nm). The red outline indicates the location of the chassis ground.



3.4 Power Connections

The iES8(G) Series Ethernet switch supports 3 different dual redundant power supplies (PWR1 and PWR2):

1. LV: Dual Input 10-48VDC
2. MV: Dual Input 36-75VDC
3. HV: Single Input 85-264VAC or 88-370VDC with a Single 10-48VDC Backup.

The label on the terminal block will indicate the accepted voltage range for PWR1 and PWR2. Positions 2, 4 and 6 are all for ground connections (connected via a removable jumper) and can be used for any ground connection. The 3 tables below list the power connections for each type of input power.

The Phillips Screw Terminal Block has Phillips screws with compression plates, allowing either bare wire connections or crimped terminal lugs. The use of #6 size ring lugs is recommended to ensure secure and reliable connections under severe shock or vibration. The terminal block comes with a safety cover which must be removed before connecting any wires. This cover must be re-attached after wiring to ensure personnel safety.

1. LV: Dual Input 10-48VDC

Terminal Number	Description	Connection
1	PWR1 (+) : Positive	Connected to the positive of the 1st 10-48VDC power source.
2	PWR1 : Ground	Power supply 1 ground connection.
3	PWR1 (-) : Negative	Connected to the negative of the 1st 10-48VDC power source.
4	: Chassis Ground	Connected to the safety ground terminal for AC Units or the ground bus for DC inputs. Chassis Ground connects to both power supply surge grounds via a removable jumper.
5	PWR2 (+) : Positive	Connected to the positive terminal of the 2nd 10-48VDC power source.
6	PWR2 : Ground	Power supply 2 ground connection.
7	PWR2 (-) : Negative	Connected to the negative terminal of the 2nd 10-48VDC power source.
8	RLY NO	Failsafe relay, normally open contact.
9	RLY CM	Failsafe relay, common contact.
10	N/C	No connection

2. MV: Dual Input 36-75VDC

Terminal Number	Description	Connection
1	PWR1 (+): Positive	Connected to the positive of the 1st 36-75VDC power source.
2	PWR1 : Ground	Power supply 1 ground connection.
3	PWR1 (-) : Negative	Connected to the negative of the 1st 36-75VDC power source.
4	: Chassis Ground	Connected to the safety ground terminal for AC Units or the ground bus for DC inputs. Chassis ground connects to both power supply surge grounds via a removable jumper.
5	PWR2 (+) : Positive	Connected to the positive terminal of the 2nd 36-75VDC power source.
6	PWR2 : Ground	Power supply 2 ground connection.
7	PWR2 (-) : Negative	Connected to the negative terminal of the 2nd 36-75VDC power source.
8	RLY NO	Failsafe relay, normally open contact.
9	RLY CM	Failsafe relay, common contact.
10	N/C	No connection

3. HV: Single Input 85-264VAC or 88-370VDC with a Single 10-48VDC Backup

Terminal Number	Description	Connection
1	PWR1 (+/L) – Line or Positive	Connected to the line terminal of the 85-264VAC power source or the positive terminal of the 88-370VDC power source.
2	PWR1 – Ground	Power supply 1 ground connection.
3	PWR1 (-/N) – Neutral or Negative	Connected to the neutral terminal of the 85-264VAC power source or the negative terminal of the 88-370VDC power source.

4	– Chassis Ground	Connected to the safety ground terminal for AC units or the ground bus for DC inputs. Chassis ground connects to both power supply surge grounds via a removable jumper.
5	PWR2 (+) - Positive	Connected to the positive terminal of the 10-48VDC backup power source.
6	PWR2 – Ground	Power supply 2 ground connection.
7	PWR2 (-) – Negative	Connected to the negative terminal of the 10-48VDC backup power source.
8	RLY NO	Failsafe relay, normally open contact.
9	RLY CM	Failsafe relay, common contact.
10	N/C	No connection

- *100-240VAC rated equipment: A 250VAC appropriately rated circuit breaker must be installed.*
- *Equipment must be installed according to the applicable country wiring codes.*
- *When equipped with a HI voltage power supply and DC backup,*

- *88-300VDC rated equipment: A 300VDC appropriately rated circuit breaker must be installed.*
- *A circuit breaker is not required for DC power supply voltages of 10-48VDC.*
- *For Dual DC power supplies, separate circuit breakers must be installed and separately identified.*
- *Equipment must be installed according to the applicable country wiring*

3.5 Console Connection

To manage the switch via console port, connect the console cable (provided with the switch) from a PC serial port (DB9) to the Console port on the front of the switch (RJ45).

Cables

4.1 Ethernet Cables

The iES8(G) series switches have standard Ethernet ports. According to the link type, the switches use either CAT 3, 4, 5, 5e UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). See below 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.)	RJ45
100Base-T(X)	Cat.5 100-ohm UTP	UTP 100 m (328 ft.)	RJ45

4.1.1 10Base-T/100Base-T(X) Pin Assignments

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

10/100 Base-T RJ-45 Pin Assignments

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

The iES8(G) Series switches support auto MDI/MDI-X operation. You can use a straight-through cable to connect a PC to the switch. The table below shows the 10Base-T/100Base-T(X) MDI and MDI-X port pin outs.

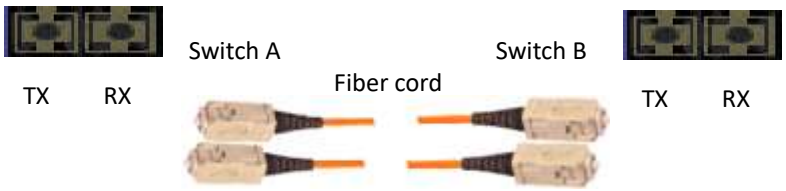
10/100 Base-T MDI/MDI-X pins assignment.

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

4.2 Fiber Optics

The iES8(G) Series Switch is available with optional fiber ports. The fiber optical ports are available in either Multimode or Singlemode, and with either SC or ST type connectors. The transceivers are also available for longer distances as required.

Note: T(X) port of Switch A should be connected to the R(X) port of Switch B.

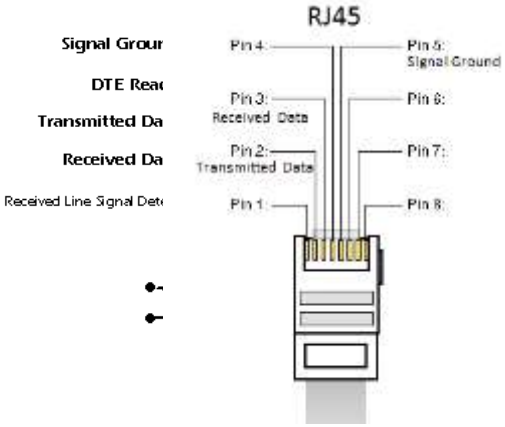


4.3 Console Cable

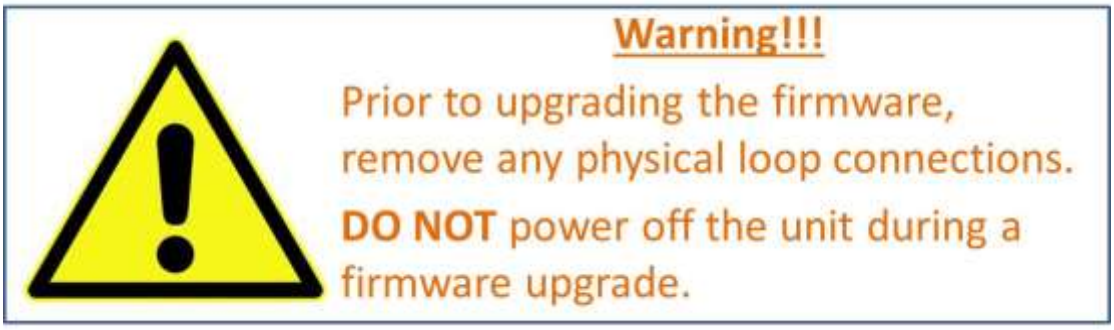
The iES8(G) Series switches can be managed via the console port on the front face using the RS-232 cable provided, and a local PC.

Console Cable pin assignments:

PC pin out (male) assignment	DB9 to RJ 45
Pin #2 RD	Pin #2 TD
Pin #3 TD	Pin #3 RD
Pin #5 GD	Pin #5 GD


RJ45
Signal Grour
DTE Reac
Transmitted Da
Received Da
Received Line Signal Det
Pin 4:
Pin 5:
Signal Ground
Pin 3:
Received Data
Pin 6:
Pin 2:
Transmitted Data
Pin 7:
Pin 1:
Pin 8:

WEB Management



5.1 Configuration by Web Browser

This section introduces the configuration by Web browser.

5.1.1 About Web-based Management

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

The Web-Based Management function supports Internet Explorer 5.0 or later. It is based on Java Applets with an aim at reducing network bandwidth consumption and enhances access speed in a viewing screen.

Note: By default, IE5.0 or later versions do not allow Java Applets to open sockets. The browser settings need to be explicitly modified in order to enable Java Applets to use the network ports.

Preparing for Web Management

The default value is as below:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

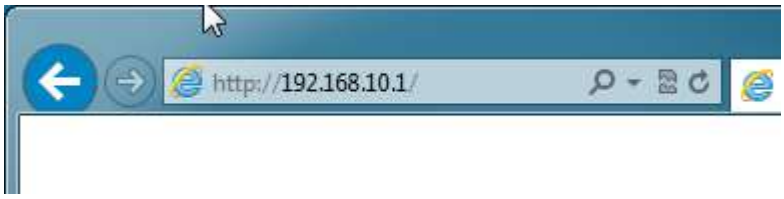
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

System Login

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



3. The login screen appears.

Login screen

4. Key in the username and password. The default username and password are "**admin**".
5. Press "**Enter**" or click the "**OK**" button. The main interface of the Web-based management appears.

Main interface

5.1.2 System Information

System Information interface

System Information

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

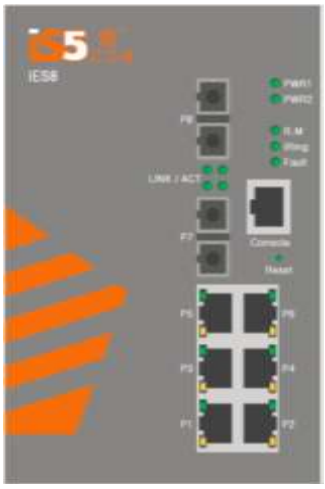
Enable Location Alert

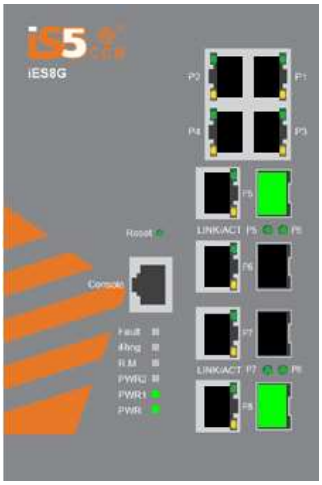
Click [Enable Location Alert] PWR1 and PWR2 LED's of the switch will start to flash.

Click [Disable Location Alert] and the LED's will stop flashing.

5.1.3 Front Panel

Clicking "Front Panel" will display the front panel of iES8(G) switch. Click "**Close**" to hide the image.





5.1.4 Basic setting

5.1.4.1 Switch Setting

Switch Setting

System Name	iES8F
System Description	Intelligent 8-port managed Ethernet switch with 6x10/100Base-T(X) and 2x100Bas
System Location	
System Contact	
System OID	1.3.6.1.4.1.41094.0.0.3
Firmware Version	v2.28
Kernel Version	v3.53
Device MAC	E8-E8-75-00-01-E5

[Apply] [Help]

Switch setting interface

The following table describes the labels for the Switch Setting screen.

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

5.1.4.2 Admin Password

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

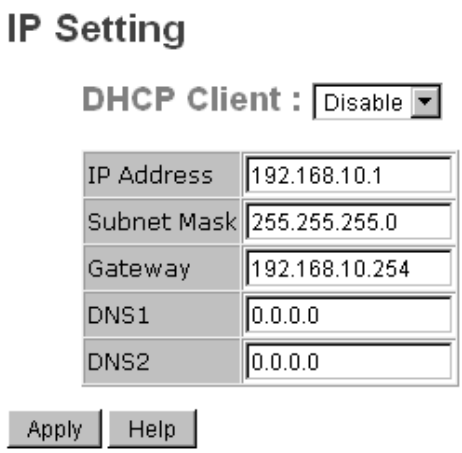
Admin Password interface

The following table describes the labels for the Admin Password screen.

Label	Description
User name	Key in the new username (The default is "**admin**").
New Password	Key in the new password (The default is "**admin**"). The maximum length for password is 10 characters.
Confirm password	Re-type the new password.
Apply	Click "**Apply**" to activate the configurations.

5.1.4.3 IP Setting

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



IP Configuration interface

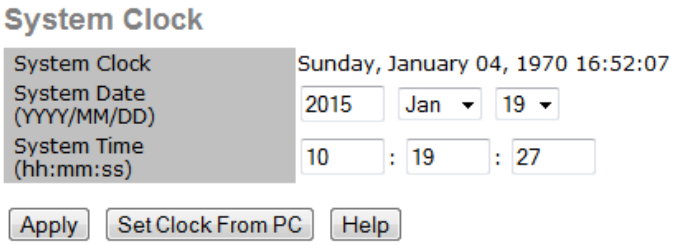
The following table describes the labels for the IP Setting screen.

Label	Description
DHCP Client	Enables or disables the DHCP client function. When the DHCP client function is enabled, an IP address from the network DHCP server will be assigned to the switch. The default IP address will be replaced by the IP address which the DHCP server. After clicking "**Apply**", a popup dialog shows up to inform you that the DHCP client is enabled. The current IP will be lost, and you should see the new IP address on the DHCP server.
IP Address	Assigns the IP address that the network is using. If the DHCP client function is enabled, you do not need to assign an IP address. The network DHCP server will assign the IP address for 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 the DHCP client function is enabled, you do not need to assign a subnet mask.
Gateway	Assigns the network gateway for the switch. The default gateway is 192.168.10.254.
DNS1	Assigns a primary DNS IP address.
DNS2	Assigns the secondary DNS IP address.
Apply	Click "**Apply**" to activate the configurations.

5.1.4.4 Time Setting

This page includes configurations of SNTP and system clock.

System Clock

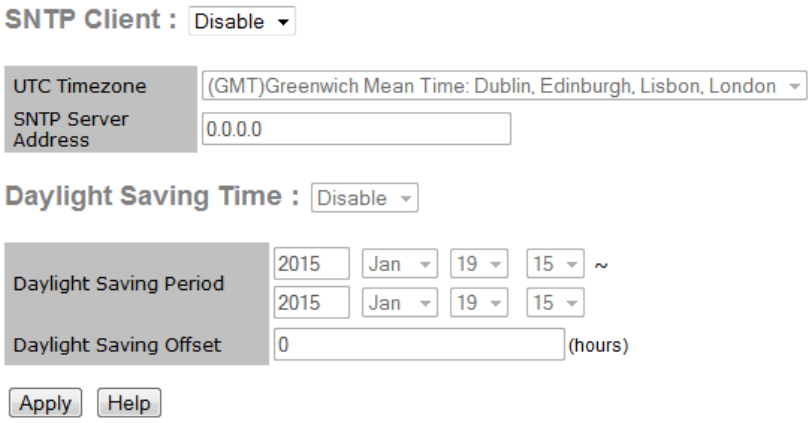


The following table describes the labels in this screen.

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

SNTP

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



SNTP Configuration interface

The following table describes the labels for the SNTP screen.

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

	time period.
Daylight Saving Period	Sets up the Daylight Saving beginning time and Daylight Saving ending time. Both times will be different each year.
Daylight Saving Offset	Sets up the offset time.
Apply	Click "**Apply**" to activate the configurations.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11 am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm

BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

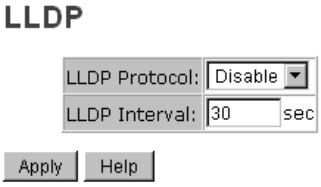
PTP Client

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

Label	Description
PTP Client	Enable / Disable PTP Client

5.1.4.5 LLDP

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



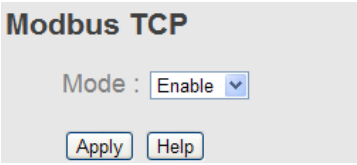
LLDP configuration interface

The following table describes the labels for the LLDP screen.

Label	Description
LLDP Protocol	"**Enable**" or "**Disable**" LLDP function.
LLDP Interval	The interval to resend LLDP (by default is 30 seconds).
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.4.6 Modbus TCP (iES8G Only)

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

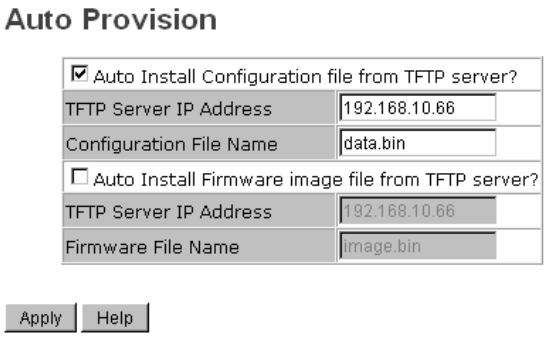


The following table describes the labels in this screen.

Label	Description
Mode	Enable or Disalble Modbus TCP function

5.1.4.7 Auto Provision

Auto Provision allows the system administrator to update the switch firmware automatically. The firmware and/or configuration files can be stored on the TFTP server. When the switch is rebooted, it will automatically be upgraded. Before updating, make sure the TFTP server is ready and the firmware image and the configuration files are on the TFTP server.



Auto Provision interface

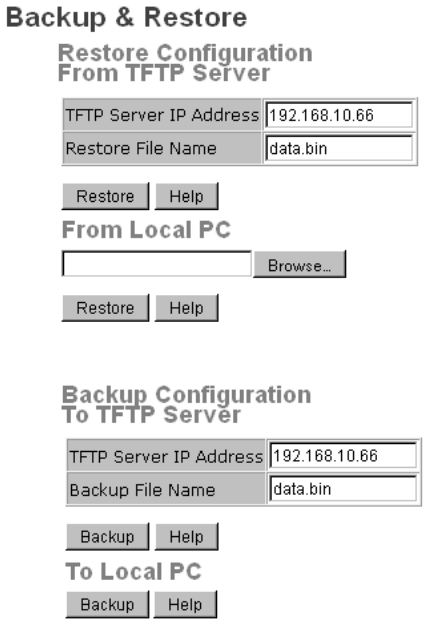
The following table describes the labels for the Auto Provision screen.

Label	Description
Auto Install Configuration file from	When selected this option is enabled.

TFTP server?	
Auto Install Firmware image file from TFTP server?	When selected this option is enabled.
TFTP Server IP Address	TFTP Server IP Address where firmware and configuration files are located.
File name	File name of the Configuration or Firmware file.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.4.8 Backup & Restore

The current configuration from the switch can either be saved to the TFTP server, or restored from the TFTP server on this page. The configuration file can also be saved to, and restored from a file on a local PC.



Backup & Restore interface

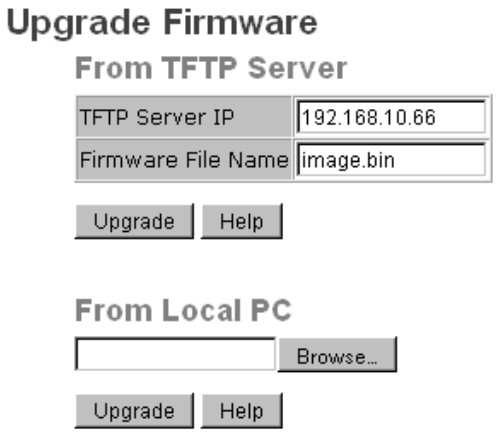
The following table describes the labels for the Backup & Restore screen.

Label	Description
TFTP Server IP Address	Enter in the TFTP server IP.
Restore File Name	Enter the file name.
Restore	Click "**restore**" to restore the configurations.
Restore File Name	Enter the file name.

Restore	Click "**restore**" to restore the configurations.
Backup	Click "**backup**" to back up the configurations.

5.1.4.9 Upgrade Firmware

Upgrade Firmware allows you to update the firmware of the switch via the TFTP or from your local PC. Before updating via the TFTP, make sure the TFTP server is ready and the firmware image is on the TFTP server. The firmware can also be updated from a file on a local PC.



Update Firmware interface

5.1.5 DHCP Server

5.1.5.1 DHCP Server – Setting

The system is provided with a DHCP server function. Enabling the DHCP server function, will allow the switch to act as a DHCP server.

DHCP Server Configuration interface

The following table describes the labels for the DHCP Server Setting screen.

Label	Description
DHCP Server	Enables or Disables the DHCP Server function. Enable – the switch will be the DHCP server on your local network.
Start IP Address	Sets the dynamic IP assign range. A low IP address is the beginning of the dynamic IP assigned range. For example: dynamic IP assigned range

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

5.1.5.2 DHCP Server – Client List

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

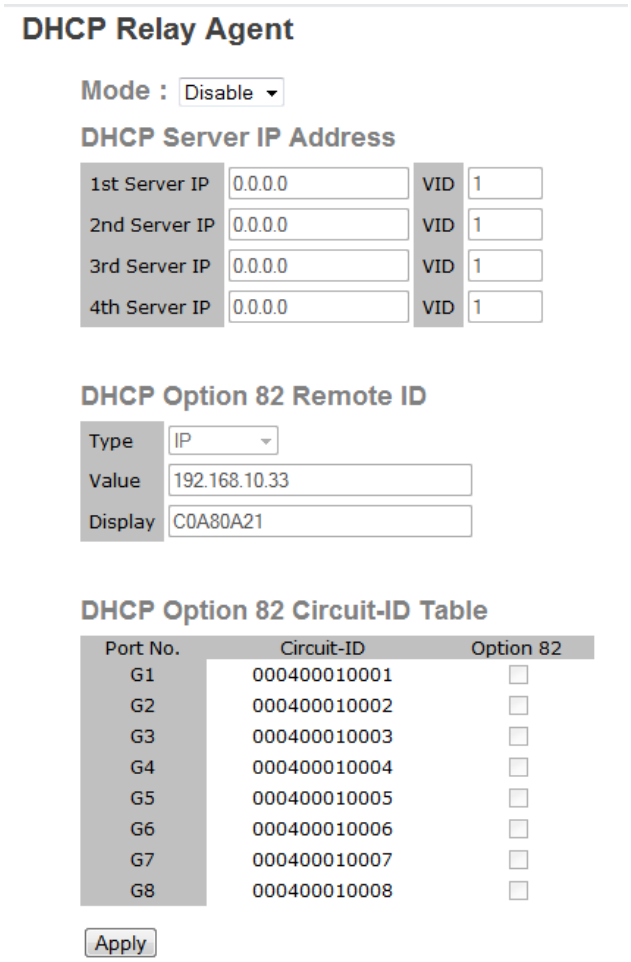
DHCP Server - Client List

IP Address	MAC Address	Type	Status	Lease

DHCP Server Client Entries interface

5.1.5.3 DHCP Server – DHCP Relay Agent (iES8G only)

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

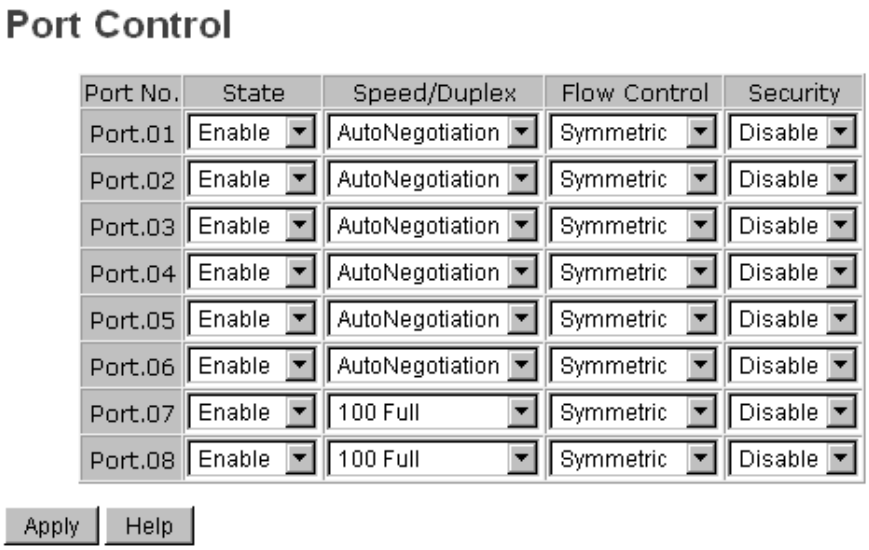


Label	Description
DHCP Relay	Enable/Disable DHCP Relay Agent.
DHCP Server IP Address and VID	Specify the IP address and VID of DHCP server. Keep "0.0.0.0" means server is inactive.
DHCP Option 82 Remote ID	"Option 82 Remote ID" provides a identifier for the remote server. There are 4 types supported: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

5.1.3 Port Setting

5.1.6.1 Port Control

With this function, the system administrator can set the state, speed/duplex, flow control, and security of the port.

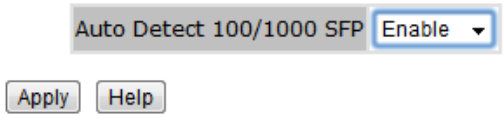


Port Control interface

The following table describes the labels for the Port Control screen.

Label	Description
Port No.	Port number for setting.
State	Enables/Disables Port Control.
Speed/Duplex	Set Auto-negotiation, 100 full, 100 half, 10 full or 10 half.
Flow Control	Supports symmetrical and asymmetrical mode to avoid packet loss when congestion occurs.
Security	Supports port security function. When enabled, the port will **STOP** learning the MAC address dynamically.
Apply	Click "**Apply**" to activate the configurations.

Auto Detect option (iES8G only)



The following table describes the labels in this screen.

Label	Description
Auto Detect 100/1000	Auto Detect SFP port SFP Module speed (100M / 1000M)

5.1.6.2 Port Status

The following information provides the current port status information.

Port Status

Port No.	Type	Link	State	Speed/Duplex	Flow Control
Port.01	100TX	Down	Enable	N/A	N/A
Port.02	100TX	Down	Enable	N/A	N/A
Port.03	100TX	Down	Enable	N/A	N/A
Port.04	100TX	Down	Enable	N/A	N/A
Port.05	100TX	UP	Enable	100 Full	Enable
Port.06	100TX	Down	Enable	N/A	N/A
Port.07	100FX	Down	Enable	N/A	N/A
Port.08	100FX	Down	Enable	N/A	N/A

Port Status interface

5.1.6.3 Rate Limit

This function allows the system administrator to limit the traffic of all ports, including broadcast, multicast and flooded Unicast. It can also set "Ingress" or "Egress" to limit traffic received or bandwidth transmitted.

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

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.

Apply Help

Rate Limit interface

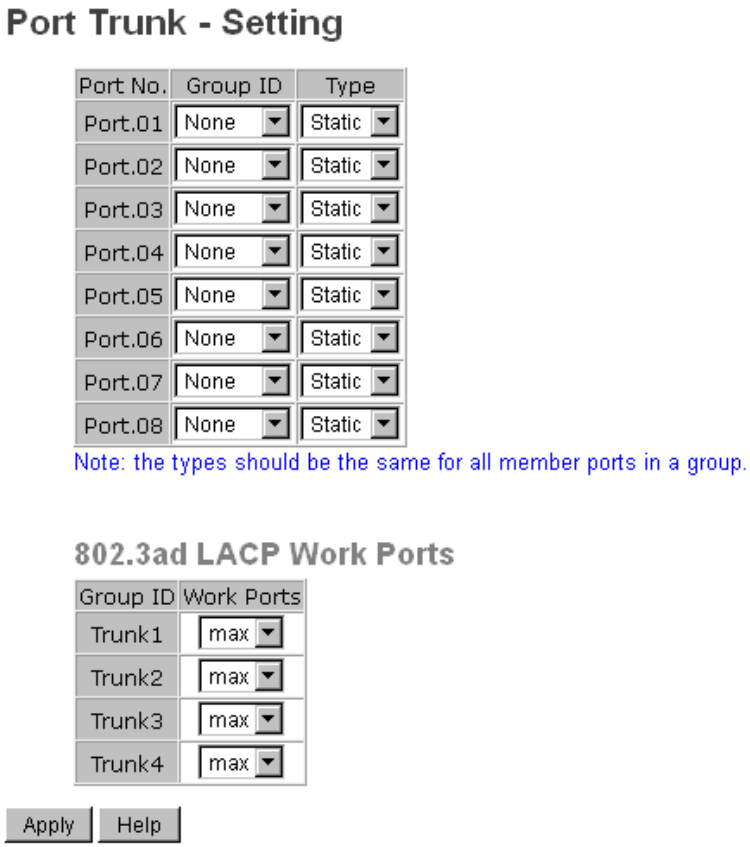
The following table describes the labels for the Rate Limit screen.

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

5.1.6.4 Port Trunk

Port Trunk – Setting

Static trunk or 802.3ad LACP can be selected to combine several physical links with a logical link to increase bandwidth.



Port Trunk - Setting interface

The following table describes the labels for the Port Trunk Setting screen.

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

Port Trunk – Status

You can check the configuration of port trunk.

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

Port Trunk - Status interface

5.1.6.5 Loop Guard (iES8G only)

This feature prevents the loop attack, when the port receives loop packet. This port will be automatically disabled to prevent the "loop attack" affecting other network devices.

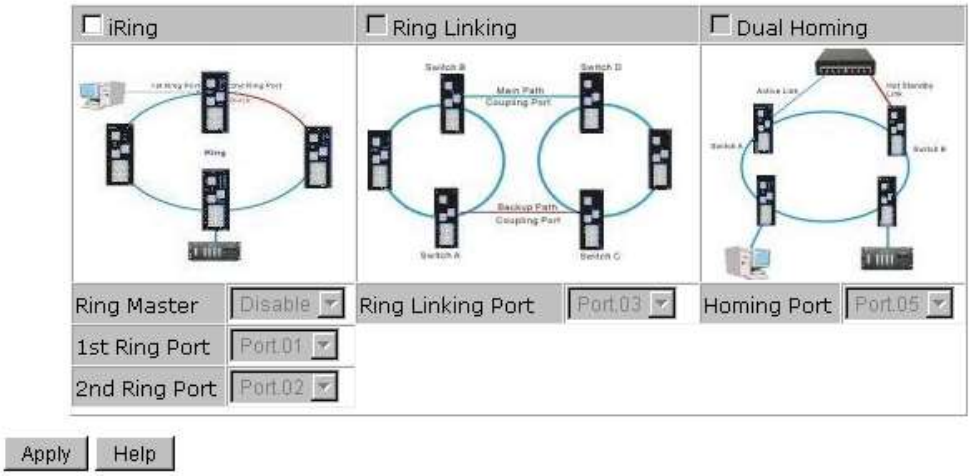
Label	Description
Active	Loop Guard Enable or Disable
Port Status	Port work status.

5.1.6 Redundancy

5.1.6.1 iRing

iRing is a powerful Redundant Ring technology. The recovery time of iRing is less than 30ms with over 250 units connected. It can reduce unexpected malfunctions caused by network topology changes. iRing technology supports three Ring topologies for network redundancy: iRing, Coupling Ring and Dual Homing.

iRing



iRing interface

The following table describes the labels for the iRing screen.

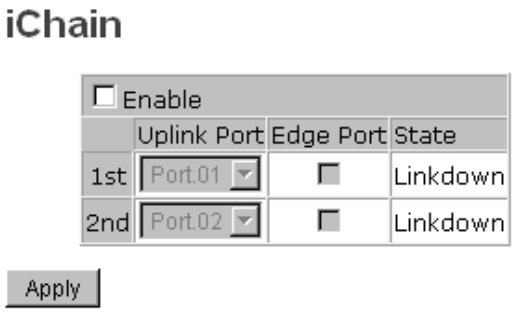
Label	Description
iRing	Enables iRing.
Ring Master	There should be only one Ring Master in a ring. However, if two or more

	switches have Ring Master enabled, the switch with the lowest MAC address will become the Ring Master and the others will become the Backup Masters.
1st Ring Port	The primary port when configured in iRing.
2nd Ring Port	The backup port when configured in iRing.
Ring Linking	Enables Ring Linking. Ring Linking can be used to divide a big ring into two smaller rings avoiding any change to the other switches if there is network topology change. It is a good application for connecting two rings.
Ring Linking Port	Set a port as the Ring Linking port to link to the Ring Linking port of the switch in the other ring. Ring Linking requires four switches to construct an active and a backup link. The linked four ports of the four switches will be operated in active/backup mode.
Dual Homing	Enables Dual Homing. By selecting Dual Homing mode, the ring will be connected to switches through two RSTP links (i.e., backbone Switch). The two links will act in active/backup mode, and connect each ring to the switches in RSTP mode.
Homing Port	Selects Homing Port
Apply	Click "**Apply**" to activate the configurations.

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

5.1.6.2 iChain

iChain can be enabled to provide network redundancy and maximize fault recovery speed by creating multiple redundant networks.

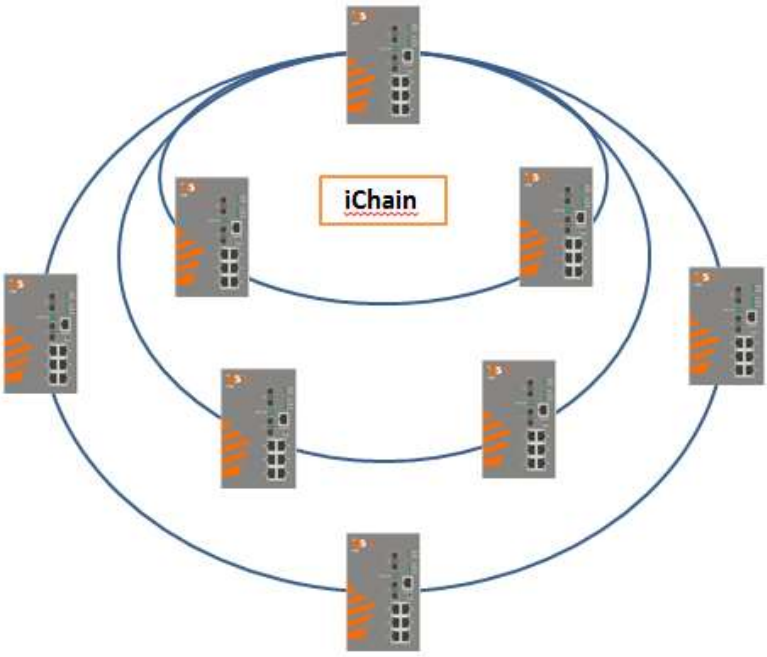


iChain Interface

The following table describes the labels for the iChain screen.

Label	Description
Enable	Enables the iChain function.
Uplink Port	Select the port (1 - 8) to be the Uplink Port.

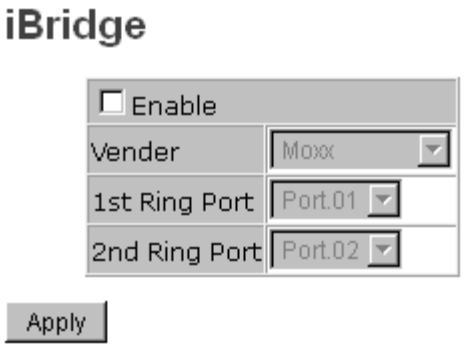
Edge Port	Defines the port as an Edge Port. Only one Edge Port of the Edge Switch needs to be defined. Other switches beside them just need to have iChain enabled.
State	Status is Forwarding or Linkdown.



Typical iChain Application

5.1.6.3 iBridge

iBridge technology can be enabled allowing the addition of iS5Com switches into a network constructed by another vendor's proprietary ring technology. This allows the interoperability between managed switches.

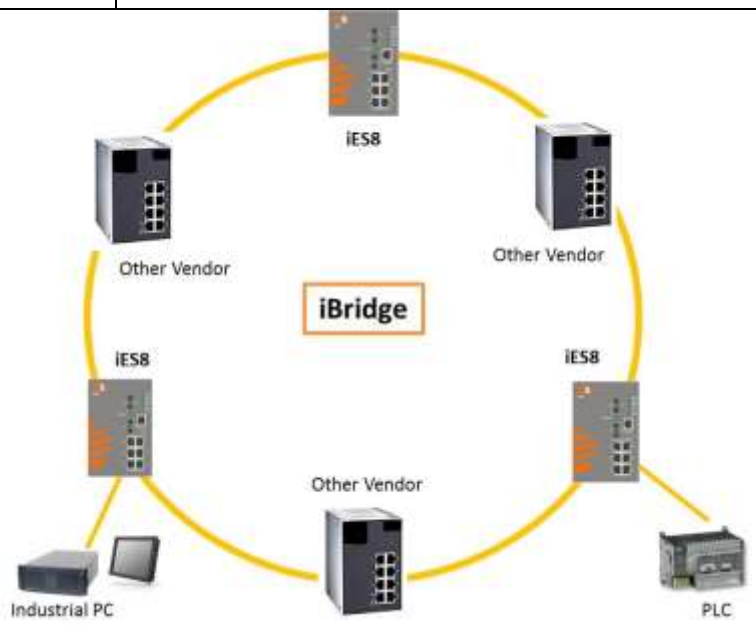


iBridge Interface

The following table describes the labels for the iBridge screen.

Label	Description

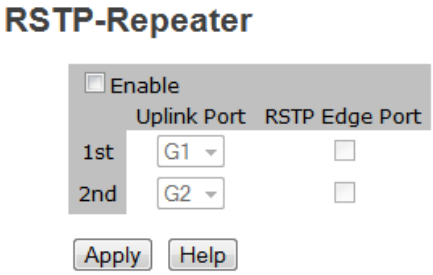
Enable	Enables the iBridge function
Vendor	Choose the vendors that you want to interoperate with.
1st Ring Port	Choose the port that will connect to the ring.
2nd Ring Port	Choose the port that will connect to the ring.



Typical iBridge Application

5.1.6.4 RSTP-Repeater (iES8G only)

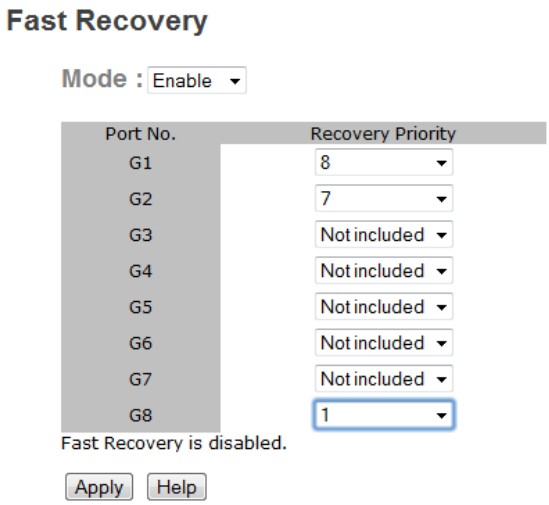
RSTP-Repeater is a simple function, this function can direct pass RSTP BPDU packet, like two RSTP devices connected through iES8G switch.



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

5.1.6.5 Fast Recovery

The Fast Recovery Mode can be set to connect multiple ports to one or more switches. The iES8G with its fast recovery mode will provide redundant links. Fast Recovery mode supports 5 priorities, only the first priority will be the act port, the other ports configured with other priority will be the backup ports.



Fast Recovery Mode interface

Label	Description
Active	Activate the fast recovery mode.
Port	Port can be configured as 5 priorities. Only the port with highest priority will be the active port. 1st Priority is the highest.
Apply	Click **"Apply"** to activate the configurations.

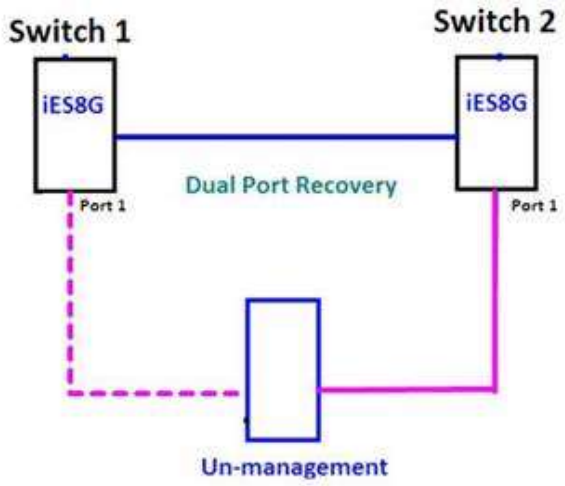
5.1.6.6 Dual Port Recovery

The Dual Port Recovery mechanism is the mechanism that allows execution of recovery protocol over the unmanaged devices/switches (ring of switches) that don't support other recovery protocols.

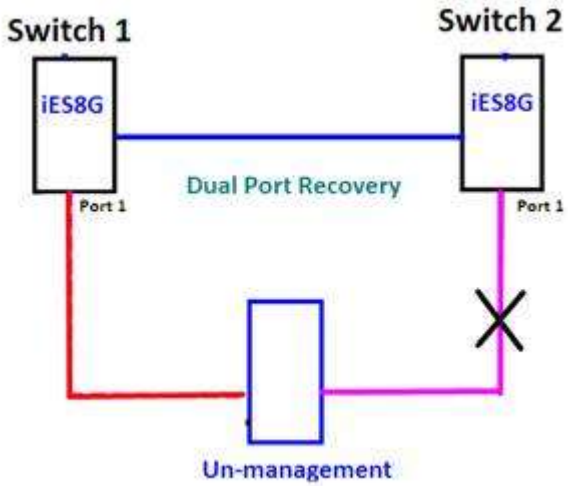
This protocols based on sending specific messages (BPDU format) from each port on both sides of unmanaged chain. The Dual Port Recovery feature can be executed with other redundancy protocols on same device.

Dual Port Recovery- Concept

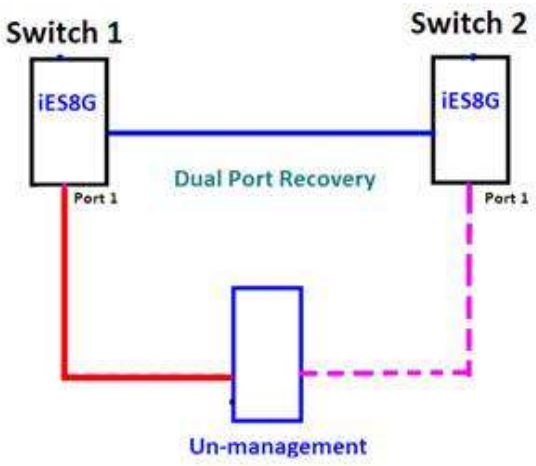
Dual Port Recovery allows connection to un-managed switch/ring of switches.



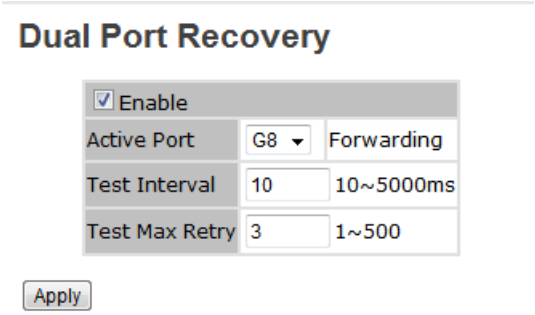
In Dual Port Recovery function if link of port in "Forwarding" state goes down, the "backup" port is changing its state to be forwarding, like in picture below. The disconnected port changes its status to "No Link"



When link of port 1 on switch 2 returns back to be link up, the switch 1 port 1 is in "forwarding" state and in this case the "No Link" port is changing its status to be "Blocking" port.



Dual Port Recovery-Configuration



Dual Port Recovery interface

Label	Description
Enable	Activate the Dual Port Recovery mode.
Active Port	Choosing the port which connects to the unmanaged switch/ring of switches. Note: User need to select one port to be Active Port on each of two devices of each side.
Test Interval	Setting Interval time for sending keep alive messages (10-5000ms default 10) Note: Test interval should be the same on both sides.
Test Max Retry	Set the maximum number of lost frames to start Dual Port Recovery mechanism (1-500 retries default 3) Note: Test Max Retry should be the same on both sides.
Apply	Click **"Apply"** to activate the configurations.

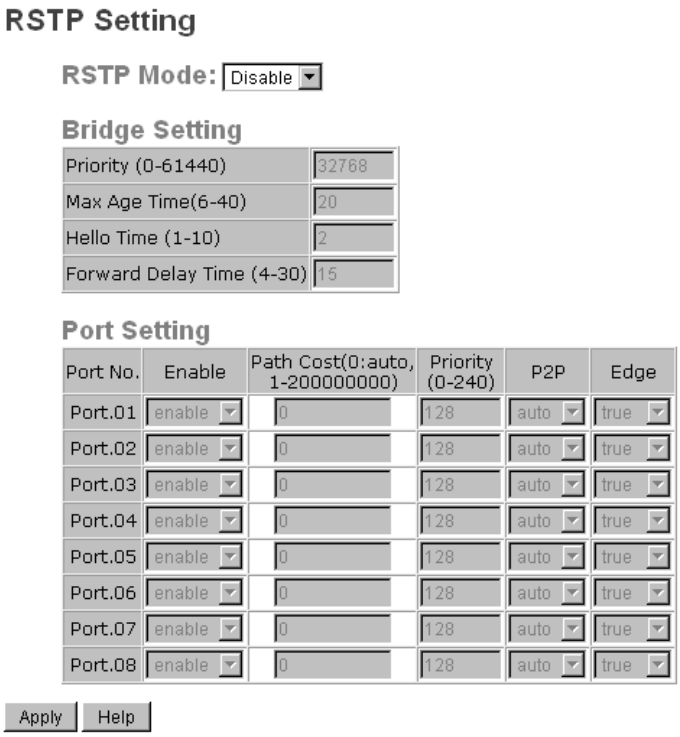
Recovery time is Test Max Retry x Test Interval + 10ms. Default Recovery time is 30ms<recovery time<40ms.

5.1.6.7 RSTP

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

RSTP Setting

The RSTP function can be enabled or disabled and parameters set for each port via the RSTP Setting interface.



RSTP Setting interface

The following table describes the labels for the RSTP Setting screen.

Label	Description
RSTP mode	The RSTP function must be enabled or disabled before configuring any of the related parameters.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value (highest priority) is selected as the root. If the value changes, the switch must be rebooted. The value must be a multiple of 4096 according to the protocol standard.
Max Age (6-40)	The number of seconds for a bridge to wait without receiving Spanning Tree Protocol configuration messages before reconfiguration. Enter a value between 6 and 40.
Hello Time (1-10)	The time that the Control Switch sends out the BPDU (Bridge Protocol Data Unit) packet to verify the current status of RSTP. Enter a value

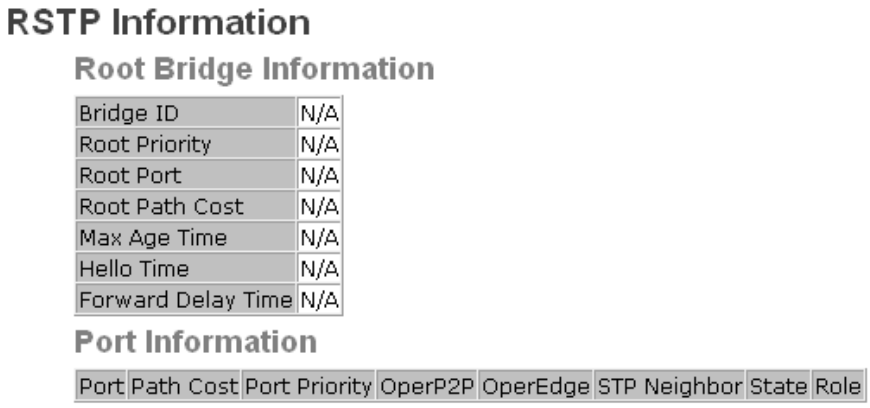
	between 1 and 10.
Forwarding Delay Time (4-30)	The number of seconds a port has to wait before changing from learning/listening state to forwarding state. Enter a value between 4 and 30.
Path Cost (1-200000000)	The Path Cost to the other bridge from the transmitting bridge at a specified port. Enter a number 1 to 200000000.
Priority (0-240)	Enter which port should be blocked by setting the priority on the LAN. Enter a number between 0 and 240. The value of priority must be a multiple of 16.
P2P	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to 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 is enabled. False means P2P is disabled.
Edge	Admin Edge is the port which is directly connected to end stations. It cannot create a bridging loop on the network. To configure the port as an edge port, set the port to "**True**".
Apply	Click "**Apply**" to activate the configurations.

NOTE: Follow this 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)

RSTP Information

Show RSTP algorithm result at this table.



RSTP Information interface

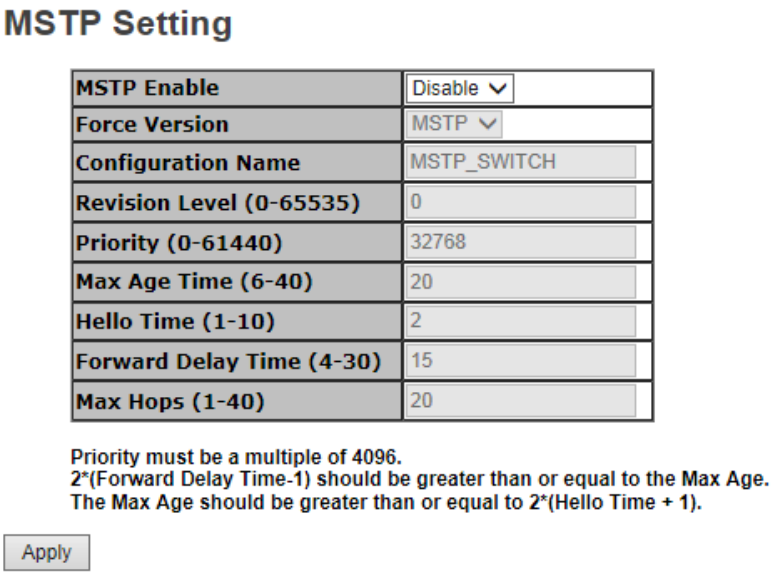
The following table describes the labels for the RSTP Information screen.

Label	Description
Root Priority	A value used to identify the root bridge. The bridge with the lowest value and with the highest priority is selected as the root.
Root Path Cost	The Path Cost to the other bridge from the transmitting bridge at a specified port.
Max Age Time	The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration.
Hello Time (1-10)	The time that the Control Switch sends out the BPDU (Bridge Protocol Data Unit) packet to verify the current status of RSTP. **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/listening states to the forwarding state.
Path Cost	The cost of the path to the other bridge from this transmitting bridge at the specified port. A number 1 through 200000000.
Port Priority	Which ports should be blocked by priority in LAN. A number 0 through 240. The value of priority must be the multiple of 16.
OperP2P	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). OperP2P shows the P2P status of the link to be manipulated administratively. True means P2P enabling. False means P2P disabling.
OperEdge	When True, OperEdge is enabled, the port is configured as an edge port and directly connected to an end station and cannot create a bridging loop. False means OperEdge disabled.
STP Neighbor	The port includes the STP mathematic calculation. True is not including STP mathematic calculation. False is including the STP mathematic calculation.
State	The State of each port is Disabled or Forwarding.
Role	The Role of each port is Disabled or Designated.

5.1.6.8 MSTP

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

MSTP Setting

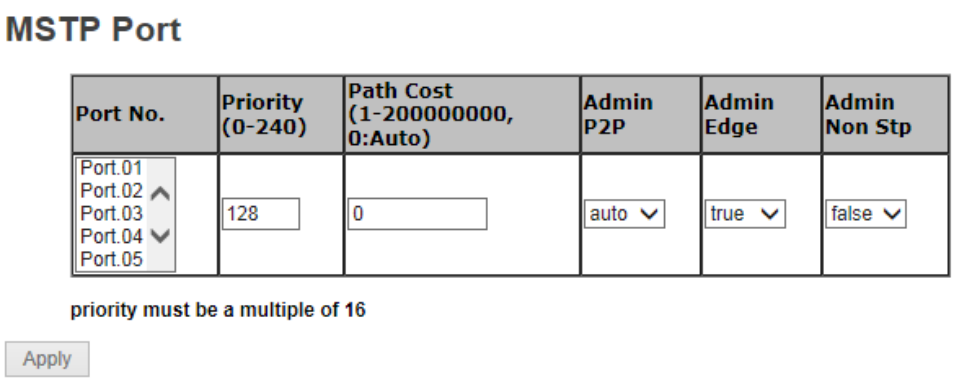


The following table describes the labels in this screen.

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

	Time, and Forward Delay Time that a controlled switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 and 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 and 30.
Max Hops (1-40)	This parameter is additional to those specified for RSTP. A single value applies to all Spanning Trees within an MST Region (the CIST and all MSTIs) for which the Bridge is the Regional Root.
Apply	Click "**Apply**" to activate the configurations.

MSTP Port

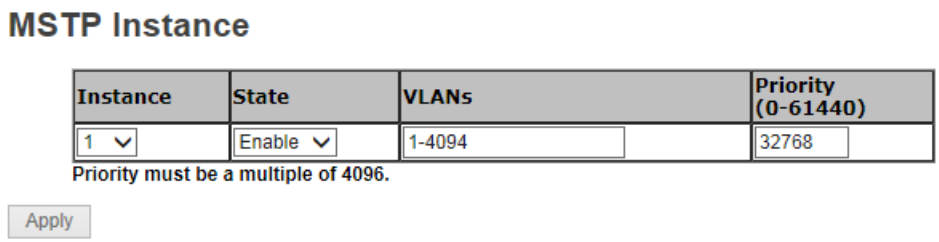


The following table describes the labels in this screen.

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

	P2P enabled. False means P2P disabled.
Admin Edge	Label
Admin Non STP	Label
Apply	Click "**Apply**" to activate the configurations.

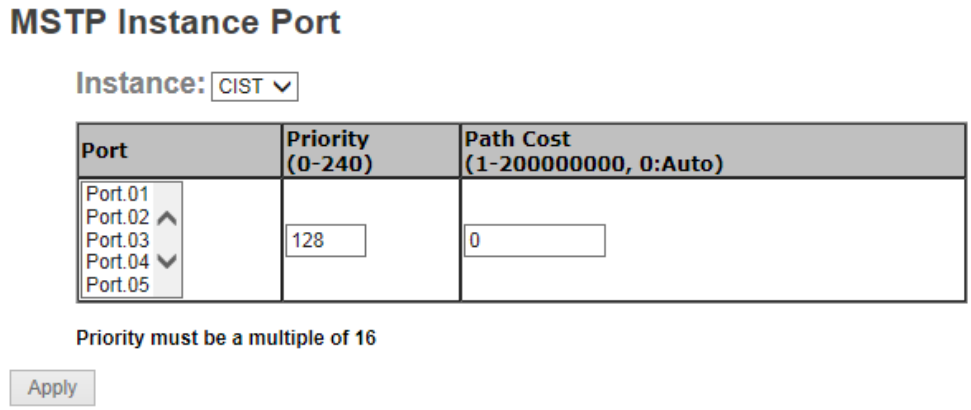
MSTP Instance



The following table describes the labels in this screen.

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

MSPT Instance Port



The following table describes the labels in this screen.

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

5.1.7 VLAN

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

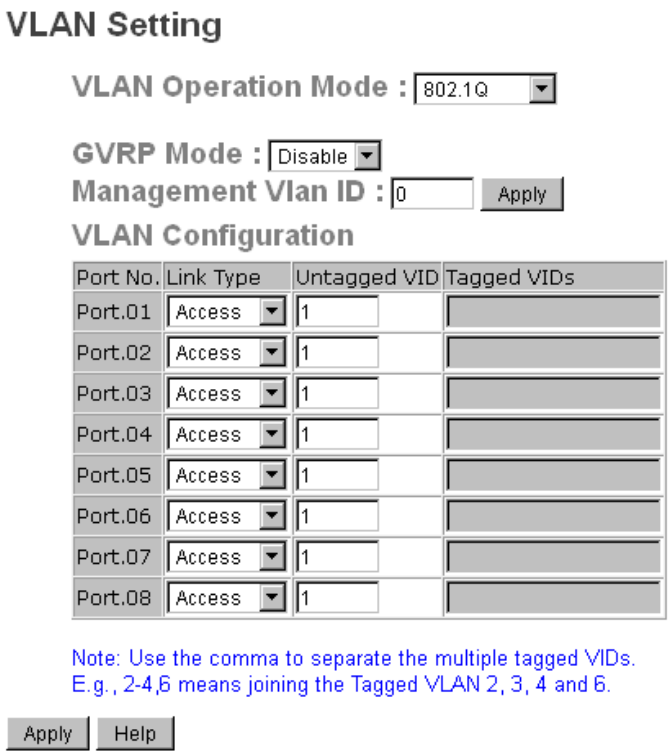
This managed switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration of VLAN operation mode is "**802.1Q**".

5.1.7.1 VLAN Setting

Tagged-based VLAN is an IEEE 802.1Q specification standard. It allows the creation of VLAN's across devices from different switch vendors. IEEE 802.1Q VLAN uses a technique which inserts a "tag" into the Ethernet frame. Tags contain a VLAN Identifier (VID) that indicates the VLAN number.

Tag-based VLAN's can be enabled or disabled using the GVRP protocol. There are 256 VLAN groups available. Default VLAN (VID is 1) is created when 802.1Q VLAN is enabled on all ports of the switch. 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; a GVRP request can be sent using the VID of a VLAN defined on the switch. The switch will automatically add that device to the existing VLAN.



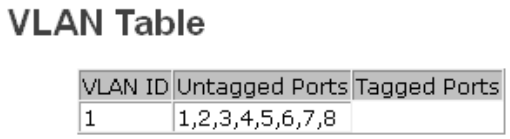
VLAN Configuration – 802.1Q interface

The following table describes the labels for the VLAN Setting screen.

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

5.1.7.2 VLAN Table

Traffic is forwarded to the member ports of the same VLAN group (Tagged Ports). VLAN ports started in the same group can be transmitted as normal packets without any restrictions. The current VLANs and Tagged Ports are shown here.



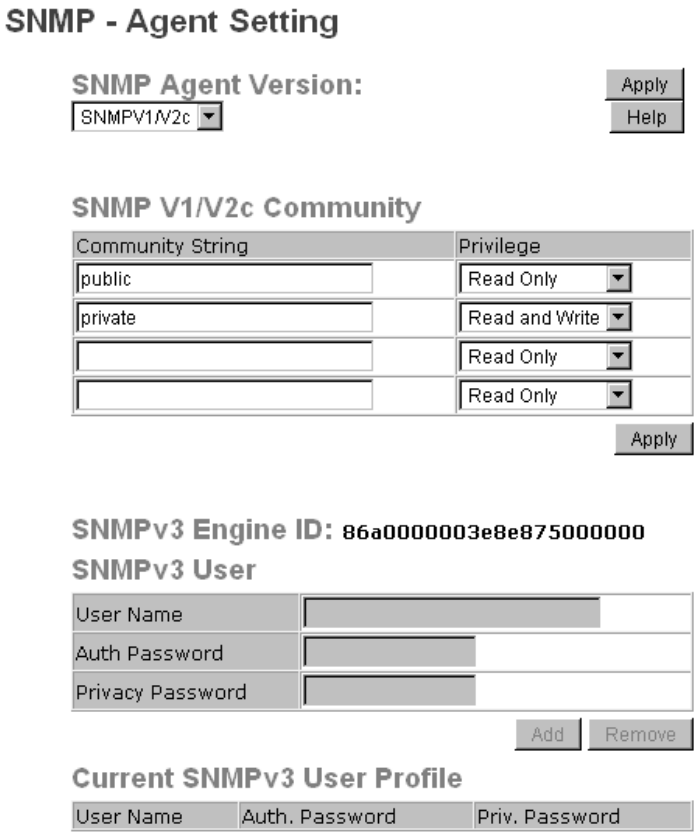
VLAN Table interface

5.1.8 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, resolve network problems, and plan for future network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

5.1.8.1 SNMP – Agent Setting

SNMP agent related information can be set using the Agent Setting Function.



SNMP Agent Setting interface

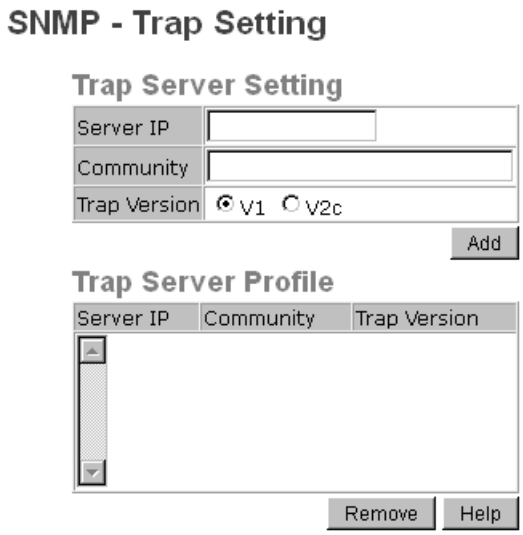
The following table describes the labels for the SNMP Agent Settings screen.

Label	Description
SNMP agent Version	Three SNMP versions are supported: SNMP V1/SNMP V2c, and SNMP V3. The SNMP V1/SNMP V2c agent uses a community string match for authentication, which means SNMP servers access objects with read-only or read/write permissions. The community default string is public/private. SNMP V3 requires an authentication level of MD5 or DES to encrypt data to enhance data security.
SNMP V1/V2c Community	SNMP Community should be set for SNMP V1/V2c. Four (4) sets of "Community String/Privilege" are supported. Each Community String has a maximum of 32 characters. Leave empty to remove the Community string.
SNMPv3User	If the SNMP V3 agent is selected, the SNMPv3 profiled should be set for authentication. A Username is required. The Auth. Password is encrypted using MD5 and the Privacy Password encrypted with DES. There are maximum 8 sets of SNMPv3 Users and a maximum 16 characters in the username and password. When the SNMP V3 agent is selected, you can: 1. Enter the SNMPv3 username only. 2. Enter the SNMPv3 username and Auth. Password. 3. Enter the SNMPv3 username, Auth. Password, and Privacy Password which can be different from the Auth. Password. To remove a current user profile: 1. Enter the SNMPv3 user name to remove. 2. Click "**Remove**" button
Current SNMPv3 User Profile	Shows all SNMPv3 user profiles.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.8.2 SNMP – Trap Setting

A trap manager is a management station that receives traps that are system alerts generated by the switch. If no trap manager is defined, no traps will be issued.

Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap managers, enter the SNMP community string and select the SNMP version.



SNMP Trap Setting interface

The following table describes the labels for SNMP Trap Setting.

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

5.1.8.3 SNMP – SNMPv3 Setting

SNMPv3 Setting

SNMPv3 Engine ID: **86a0000003e8e8750006ed**

Context Table

Context Name | Apply

User Profile

(none)

User ID
Authentication Password
Privacy Password

Add | Remove

Group Table

(none)

Security Name (User ID)
Group Name

Add | Remove

Access Table

(none)

Context Prefix
Group Name
Security Level: NoAuthNoPriv. AuthNoPriv. AuthPriv.
Context Match Rule: Exact Prefix
Read View Name
Write View Name
Notify View Name

Add | Remove

MIBView Table

(none)

View Name
SubOid-Tree
Type: Excluded Included

Add | Remove

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.

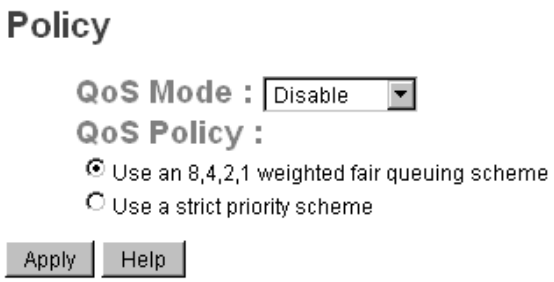
SNMPv3 Setting interface

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

5.1.6 Traffic Prioritization

Traffic Prioritization includes 3 modes: Port base, 802.1p/COS, and TOS/DSCP. With the traffic prioritization function, traffic can be classified into four classes for differential network application. The iES8(G) Series support 4 priority queues.

5.1.6.1 Policy

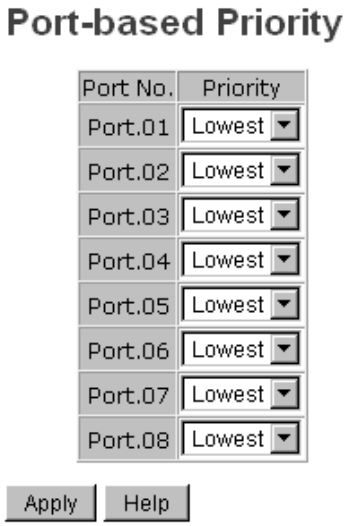


Policy Setting Interface

The following table describes the labels for Policy Traffic Prioritization.

Label	Description
QoS Mode	**Port-base:** Output priority is determined by the 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 follow the 8:4:2:1 ratio to transmit packets from the highest to lowest queue. For example: 8 high queue packets, 4 middle queue packets, 2 low queue packets, the lowest queue packets are transmitted in one turn. **Use the strict priority scheme:** the packets in the higher queue will always be transmitted first until a higher queue is empty.
Help	Show help file.
Apply	Click "**Apply**" to activate the configurations.

5.1.6.2 Port-based Priority

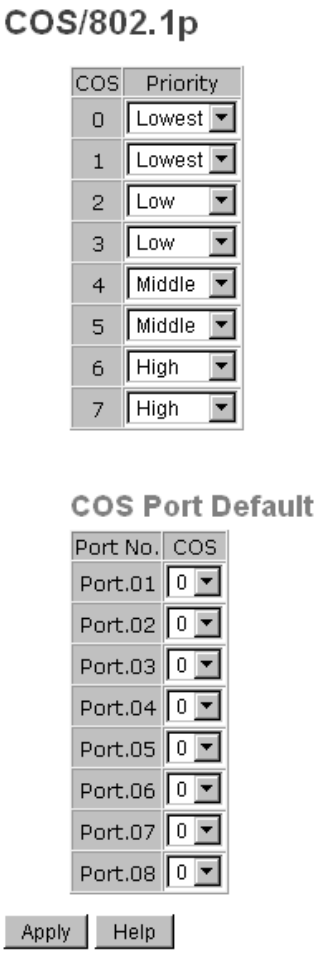


Port-based Priority interface

The following table describes the labels for the Port-based Priority screen.

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

5.1.6.3 COS/802.1p



COS/802.1p interface

The following table describes the labels for the Port-based Priority screen.

Label	Description
COS/802.1p	COS (Class Of Service) also known as 802.1p, describes the output priority of a packet as determined by the user priority field in the 802.1Q VLAN tag. The priority value supported is 0 to 7. The COS value map for 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 the ingress port.
Help	Show help file.
Apply	Click "**Apply**" to activate the configurations.

5.1.6.4 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

Apply Help

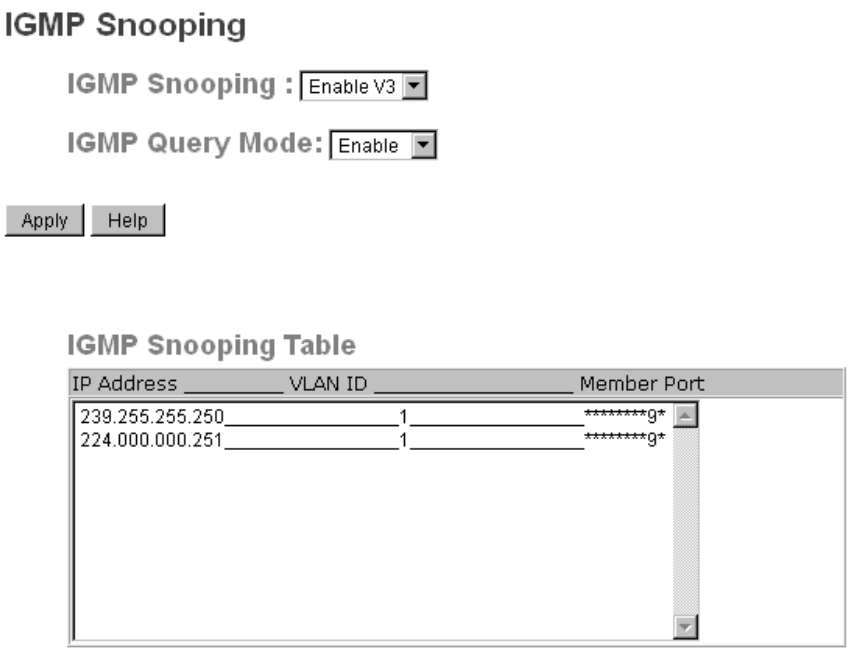
TOS/DSCP interface

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

5.1.7 Multicast

5.1.7.1 IGMP Snooping

The Internet Group Management Protocol (IGMP) is used by IP hosts to register the dynamic multicast group membership. IGMP has 3 versions: IGMP v1, v2 and v3. Please refer to RFC 1112, 2236 and 3376. IGMP snooping monitors the Internet Group Management Protocol (IGMP) traffic between hosts and multicast routers. This conserves bandwidth by allowing the switch to send multicast traffic to only those interfaces that are connected to hosts that want to receive the traffic, instead of flooding the traffic to all interfaces in the VLAN.



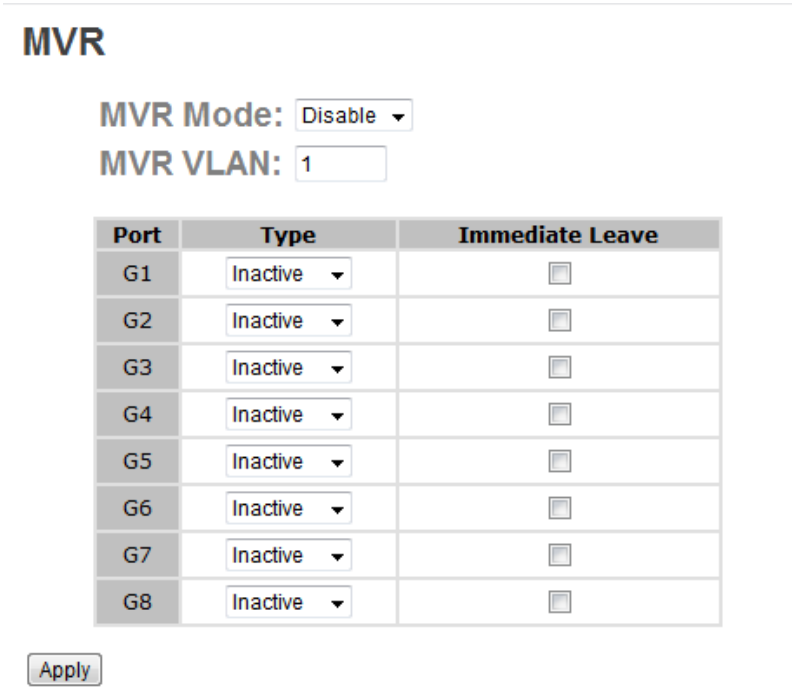
IGMP Snooping interface

The following table describes the labels for IGMP Snooping screen.

Label	Description
IGMP Snooping	Enable/Disable IGMP snooping. When enabling IGMP Snooping the version must be selected.
IGMP Query Mode	Defines if the switch will be in IGMP query mode or not. There should only be one switch in IGMP query mode for any IGMP application. The "Auto" mode means that the switch in IGMP query mode is the one with the lowest IP address.
IGMP Snooping Table	Shows the current IP multicast list.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.7.2 MVR

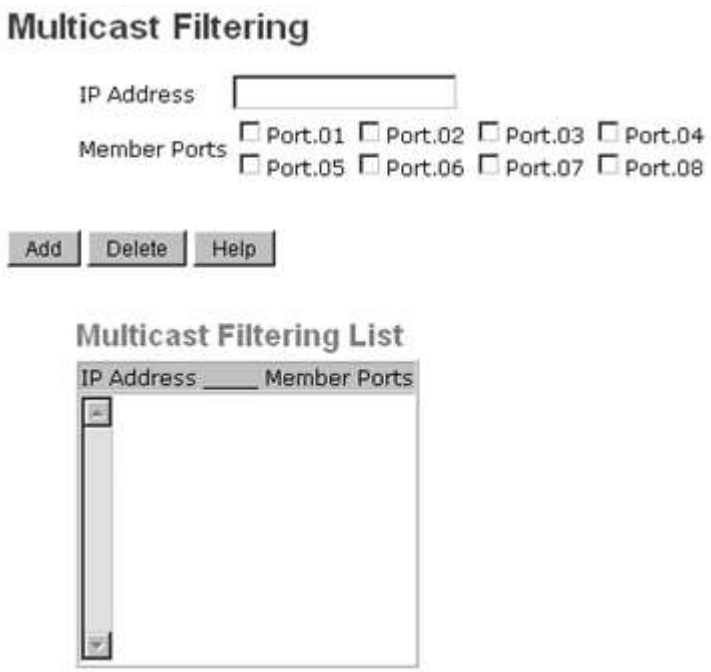
MVR Function can provide a different VLAN user to receive MVR Mode VLAN Multicast Packet.



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

5.1.7.3 Multicast Filter

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



Multicast Filtering interface

The following table describes the labels for Multicast Filtering screen.

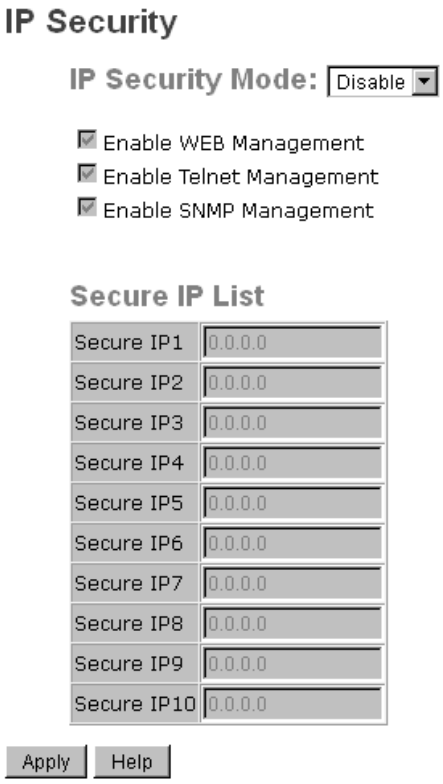
Label	Description
IP Address	Assigns a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255
Member Ports	Check the box beside the port number to include it as a member port in a specific multicast group IP address.
Add	Add a Multicast Filter to the list. Enter the IP Address, select the Member Ports, then click "Add".
Delete	Delete an entry from table
Help	Show help file.

5.1.8 Security

There are five (5) useful functions that can enhance the security of a switch: IP Security, Port Security, MAC Blacklist, MAC Address Aging, and the 802.1x protocol.

5.1.8.1 IP Security/Management Security

IP security can be enabled or disabled remotely via the WEB, Telnet or SNMP. Additionally, IP security can be restricted via remote management for specific IP addresses. Only these secure IP addresses can be managed by the switch remotely.



IP Security interface

The following table describes the labels for IP Security screen.

Label	Description
IP security MODE	Enables or Disables the IP security function.
Enable WEB Management	Check the box to enable WEB Management.
Enable Telnet Management	Check the box to enable Telnet Management.
Enable SNMP Management	Check the box to enable SNMP Management.
Secure IP List	Enter the IP addresses to be managed remotely.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.8.2 Port Security

Port security adds static MAC addresses to hardware forwarding databases. If port security is enabled on the **Port Control** page (found under Port Setting), only the frames with a MAC addresses in the list will be forwarded the rest will be discarded.

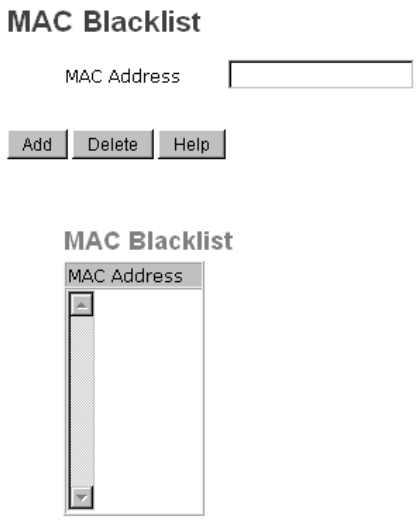
Port Security interface

The following table describes the labels for Port Security screen.

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

5.1.8.3 MAC Blacklist

The MAC Blacklist eliminates the forwarding traffic to specific MAC addresses in the list. Any frames forwarded to a MAC address in the list will be discarded. This will stop the device from receiving any such frame.



MAC Blacklist interface

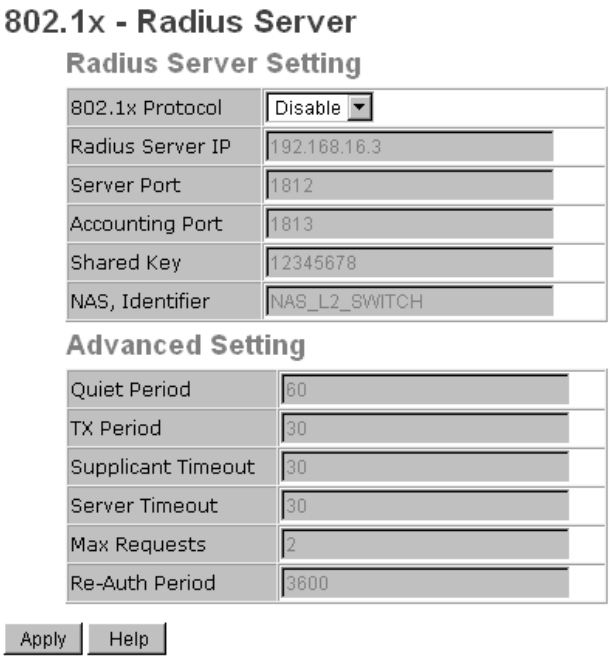
The following table describes the labels for MAC Blacklist screen.

Label	Description
MAC Address	Input the MAC Address to be added to the MAC Blacklist.
Add	Add an entry to the MAC Blacklist table.
Delete	Delete the entry.
Help	Show help file.

5.1.8.4 802.1x

802.1x - Radius Server

802.1x makes the use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide an authenticated and authorized device to attach to a LAN port. Please refer to IEEE 802.1x - Port Based Network Access Control.



802.1x Radius Server interface

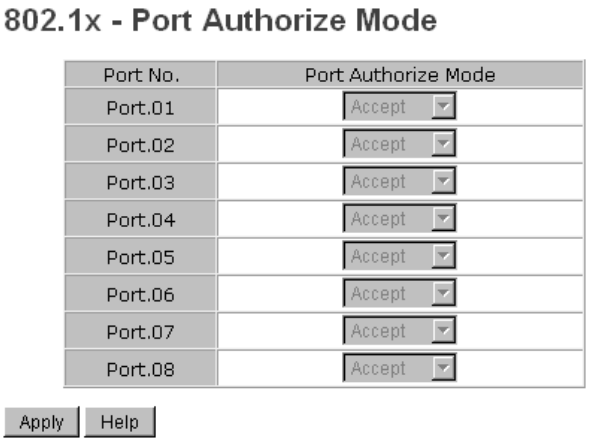
The following table describes the labels for 802.1x - Radius Server screen.

Label	Description
Radius Server Setting	
Radius Server IP	The IP address of the authentication server.
Server port	Set the UDP port number used by the authentication server to authenticate.
Accounting port	Set the UDP destination port for accounting requests to the specified Radius Server.
Shared Key	A shared key between the switch and the authentication server.
NAS, Identifier	A string used to identify the switch.
Advanced Setting	
Quiet Period	Set the time interval between authentication failure and the start of a new authentication attempt.
Tx Period	Set the time that the switch can wait for a response from an EAP request/identity frame client before resending the request.
Supplicant Timeout	Set the period of time the switch waits for a supplicant response to an EAP request.
Server Timeout	Set the period of time the switch waits for a Radius server response to an authentication request.
Max Requests	Set the maximum number of times to retry sending packets to the supplicant.

Re-Auth. Period	Set the period of time after which a client that is connected must be re-authenticated.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

802.1x Port Authorize Mode

Set the 802.1x authorized mode of each port.



802.1x Port Authorize interface

The following table describes the labels for the 802.1x- Port Authorize Mode screen.

Label	Description
Port Authorize Mode	**Reject:** force the port to be unauthorized. **Accept:** force the port to be authorized. **Authorize:** the state of the port which was determined by the outcome of the 802.1x authentication. **Disable:** the port will no longer participate in 802.1x.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

802.1x Port Authorize State

Show 802.1x port authorize 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

802.1x Port Authorize State interface

5.1.8.5 IP Guard (iES8G only)

IP Guard – Port Setting

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

IP Guard - Port Setting

Port No.	Mode
G1	Disabled
G2	Disabled
G3	Disabled
G4	Disabled
G5	Disabled
G6	Disabled
G7	Disabled
G8	Disabled

Apply Help

IP Guard – Port Setting State interface

The following table describes the labels in this screen.

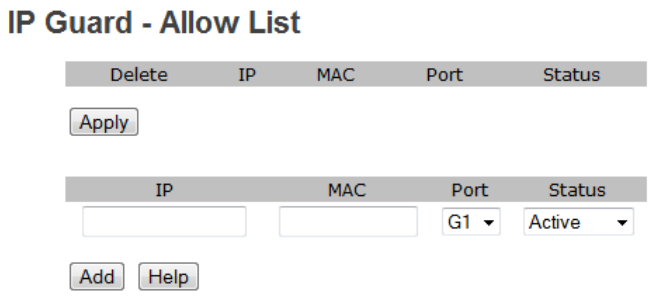
Label	Description
Mode	• Disable mode: function is totally disabled. • Monitor mode: function is disabled, but keeps monitor the IP traffic. • Security mode: function is enabled, the illegal IP traffic will be blocked.

Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

IP Guard – Allow List

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

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



IP Guard – Allow List State interface

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

IP Guard – Super-IP List

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

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

IP Guard – Super-IP List State interface

IP Guard – Monitor List

IP Guard Monitor List is an intelligent and easy use function to see IP security. It could protect the network from unknown IP (the IP not in allowed list) attack by adding the entry to allow list. The IP traffic from the edge device will be added to allow list.

The following table describes the labels in this screen.

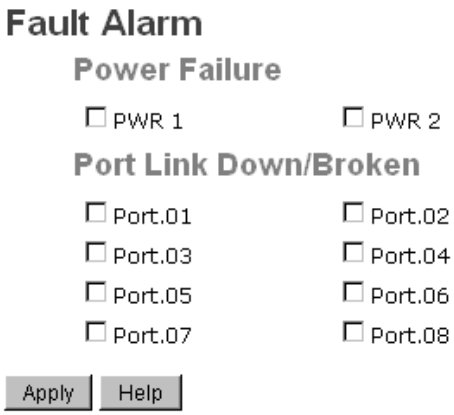
Label	Description
IP	IP address of entry.
MAC	MAC address of entry.
Port	Port number of entry.
Time	The logged time .
Add to Allow List	If you want to allow the IP traffic, please check this box and apply it.

5.1.6 Warning

The Warning function is very important for managing a switch. The switch can be managed using SYSLOG, E-MAIL, and Fault Relay. This can help to monitor the switch status on remote sites. When an event occurs, the warning message gets sent to an appointed server, E-MAIL, or relay fault on a switch panel.

5.1.6.1 Fault Alarm

When any selected fault event occurs, the Fault LED on the switch panel and the electric relay will turn on at the same time.



Fault Alarm interface

The following table describes the labels for the Fault Alarm screen.

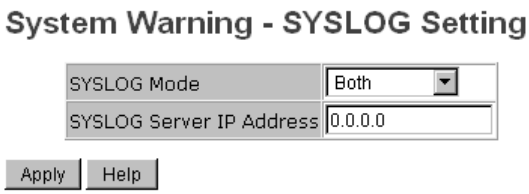
Label	Description
Power Failure	Check the box to monitor status of PWR 1 or PWR 2.
Port Link Down/Broken	Check the box to monitor status of port 1 to port 8.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.6.2 System Warning

System Warning supports two warning modes: 1. SYSLOG. 2. E-MAIL. The switch can be monitored through the selected system events.

System Warning – SYSLOG Setting

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



System Warning – SYSLOG Setting interface

The following table describes the labels for the SYSLOG Setting screen.

Label	Description
SYSLOG Mode	**Disable:** disable SYSLOG. **Client Only:** log to a local system. **Server Only:** log to a remote SYSLOG server. **Both:** log into both local and remote servers.
SYSLOG Server IP Address	The remote SYSLOG Server IP address.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

System Warning – SMTP Setting

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

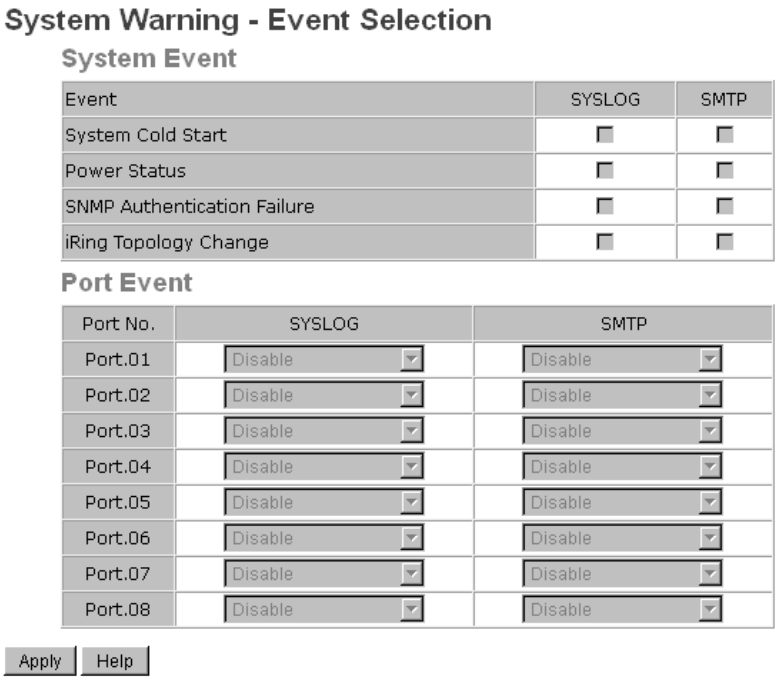
System Warning – SMTP Setting interface

The following table describes the labels for the SMTP Setting screen.

Label	Description
E-mail Alarm	Enables and Disables the transmission system warning events by e-mail.
SMTP Server Address	The SMTP server IP address (or domain name address).
Sender E-mail Address	The SMTP server IP address.
Mail Subject	The Subject of the e-mail.
Authentication	Select this option if the SMTP server needs authentication. • **Username:** the authentication username. • **Password:** the authentication password. • **Confirm Password:** re-enter password.
Recipient E-mail Address	The recipient's E-mail address. Supports up to 6 recipient emails.
Apply	Click "**Apply**" to activate the configurations.
Help	Show 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 system event warning method required. Please note that the check box cannot be checked while SYSLOG or SMTP is disabled.



System Warning – Event Selection interface

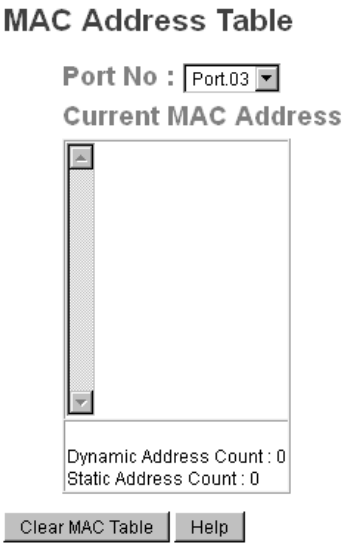
The following table describes the labels for the System Warning screen.

Label	Description
System Event	
System Cold Start	Alert when the system restarts.
Power Status	Alert when there is a power up or down.
SNMP Authentication Failure	Alert when there is a SNMP authentication failure.
iRing Topology Change	Alert when the iRing topology changes.
Port Event **SYSLOG / SMTP event**	**Disable** **Link Up** **Link Down** **Link Up & Link Down**
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.7 Monitor and Diagnostics

5.1.7.1 MAC Address Table

Please refer to IEEE 802.1 D Sections 7.9. The 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.



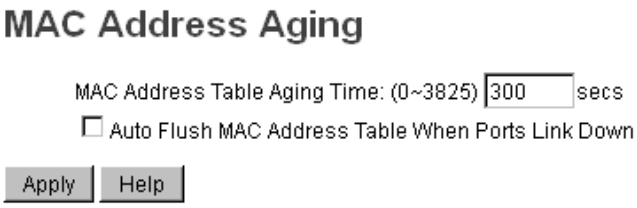
MAC Address Table interface

The following table describes the labels for the MAC Address Table screen.

Label	Description
Port No.	Shows all the MAC addresses mapped to a selected port in the table.
Clear MAC Table	Clears all MAC addresses in the table.
Help	Show help file.

5.1.7.2 MAC Address Aging

The MAC Address table aging time can be set between 0 and 3825 seconds. When the time expires, the unused MAC addresses will be cleared from the MAC table. The iES8(G) Series also supports "Auto Flush MAC Address Table When Ports Link Down".



MAC Address Aging interface

The following table describes the labels for the MAC Address Aging screen.

Label	Description
MAC Address Table Aging Time	Sets the aging time for the MAC table. The value must be a multiple of 15 and should be between 0 and 3825 seconds. The default setting is 300 seconds.
Auto Flush MAC Address Table When Ports Link Down	Enables and Disables the function.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.7.3 Port Statistics/Port Overview

Port statistics show several statistical counters for all ports. The counters can be reset to zero by pressing the "clear" button.

Port Statistics

Port	Type	Link	State	TX Good Packet	TX Bad Packet	RX Good Packet	RX Bad Packet	TX Abort Packet	Packet Collision
Port.01	100TX	Down	Enable	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0
Port.05	100TX	Up	Enable	3829	0	7470	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0
Port.07	100FX	Down	Enable	0	0	0	0	0	0
Port.08	100FX	Down	Enable	0	0	0	0	0	0

Clear Help

Port Statistics interface

The following table describes the labels for the Port Statistics screen.

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

5.1.7.4 Port Counters (iES8G only)

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

Port Counters

Port No. : G5

InGoodOctetsLo	InGoodOctetsHi	InBadOctets	OutFCSErr
510138294	7	0	0
InUnicasts	Deferred	InBroadcasts	InMulticasts
2595191	0	305648790	43260794
Octets64	Octets127	Octets255	Octets511
440396209	60895258	79558773	13497161
Octets1023	OctetsMax	OutOctetsLo	OutOctetsHi
45612	33594	3384366819	4
OutUnicasts	Excessive	OutMulticasts	OutBroadcasts
470161	0	31676439	210775533
Single	OutPause	InPause	Multiple
0	0	0	0
Undersize	Fragments	Oversize	Jabber
0	0	0	0
InMACRcvErr	InFCSErr	Collisions	Late
0	0	0	0

Clear

Port Counters interface

The following table describes the labels in this screen.

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

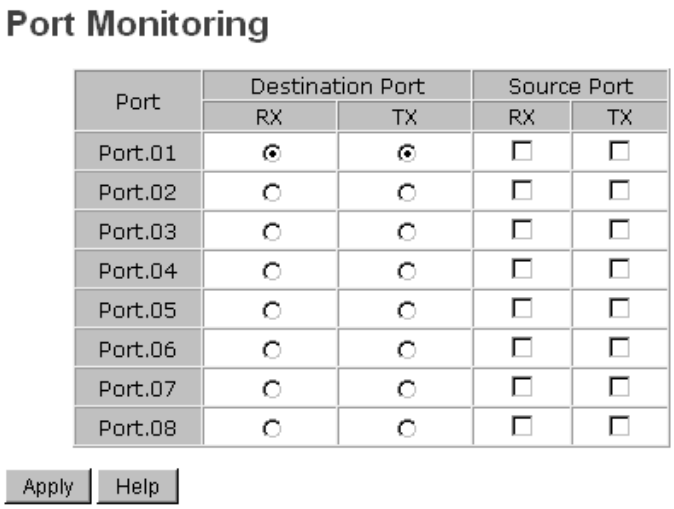
InMulticasts	The number of good frames received that have a Multicast destnation MAC address.
Octets64	Total frames received (and/or transmitted) with a length of exactly 64 octets, include those with errors.
Octets127	Total frames received (and/or transmitted) with a length of between 65 and 127 octets inclusive, including those with error.
Octets255	Total frames received (and/or transmitted) with a length of between 128 and 255 octets inclusive, including those with error.
Octets511	Total frames received (and/or transmitted) with a length of between 256 and 511 octets inclusive, including those with error.
Octets1023	Total frames received (and/or transmitted) with a length of between 512 and 1023 octets inclusive, including those with error.
OctetsMax	Total frames received (and/or transmitted) with a length of between 1024 and MaxSize octets inclusive, 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 counted 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.

5.1.7.5 Port Monitoring

The Port monitoring function supports TX (egress) only, RX (ingress) only, and both TX/RX. TX monitoring sends data that egressed out of the checked TX source port to a selected TX destination port. RX monitoring sends data that ingress in of the checked RX source ports out to a selected RX destination port. It also sends the frame to where it normally would have gone.

Note: Keep all source ports unchecked to disable port monitoring.



Port monitoring interface

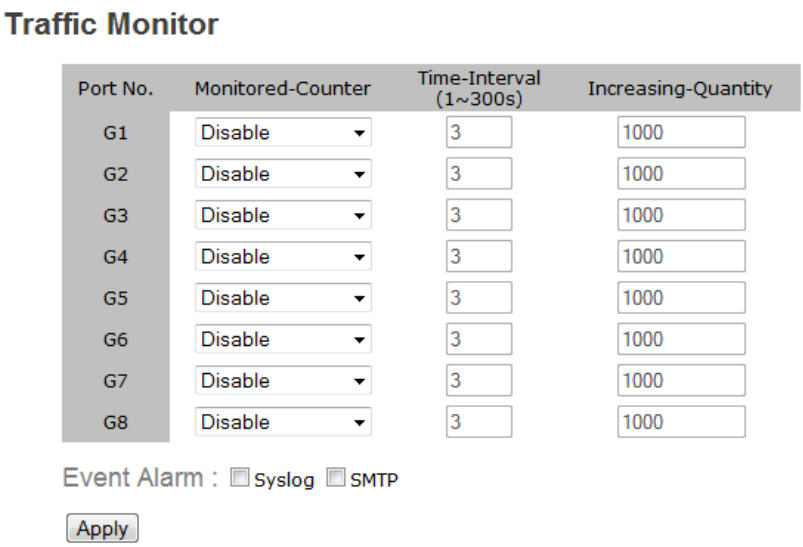
The following table describes the labels for the Port Monitoring screen.

Label	Description
Destination Port	The port that will receive a copied frame from a source port for monitoring purpose.

Source Port	The port that will be monitored. Check the TX or RX to be monitored.
TX	The frames that leave the switch port and proceed somewhere outside of the network.
RX	The frames that originate from outside the network and are received by the switch port within the network.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.7.6 Traffic Monitor (iES8G only)

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



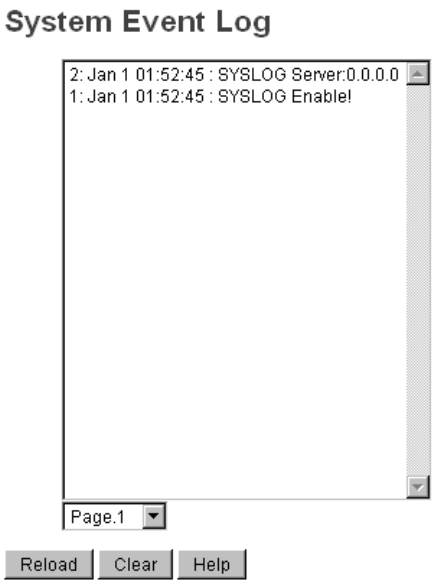
System event log interface

The following table describes the labels in this screen.

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

5.1.7.7 System Event Log

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



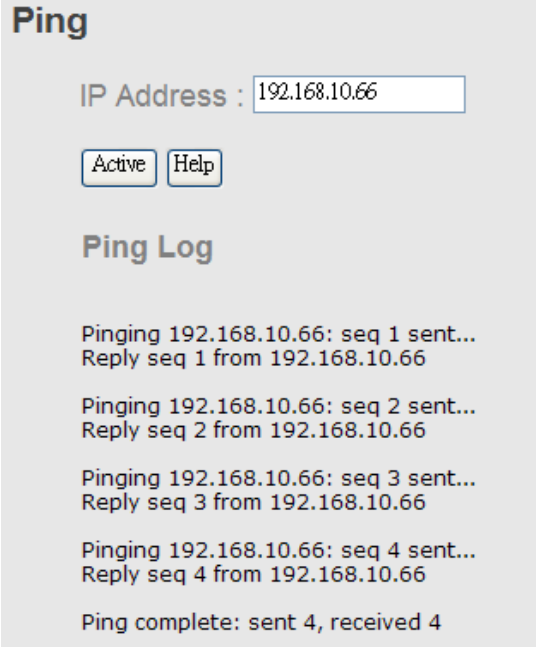
System event log interface

The following table describes the labels for the System Event Log screen.

Label	Description
Page	Selects the LOG page to view.
Reload	Gets the newest event logs and refreshes the page.
Clear	Clear the System Event Log.
Help	Show help file.

5.1.7.8 Ping

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



Ping interface

The following table describes the labels in this screen.

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

5.1.6 Save Configuration

If any configuration has been changed, "**Save Configuration**" should be clicked to save the current configuration data to the permanent flash memory. If not saved, the current configuration will be lost when the switch is powered off or there is a system reset.

System Configuration interface

The following table describes the labels for the Save Configuration screen.

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

5.1.7 Factory Default

Factory Default interface

To reset switch to the factory default configuration, click Reset. The default configuration will be applied after the next restart of the switch.

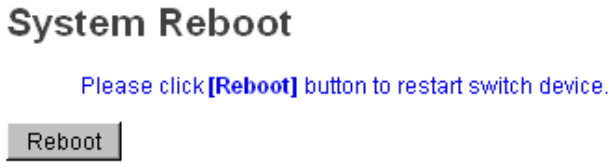
The following table describes the labels for the Factory Default screen.

Label	Description
Keep current IP address setting?	When selected the IP address will be retained when the switch is reset to the factory default.

Keep current username & password?	When selected the username & password will be retained when the switch is reset to the factory default
Reset	Resets configuration to the factory default
Help	Show help file.

5.1.8 System Reboot

The switch will be restarted when the "Reboot" button is pressed.



System Reboot interface

Command Line Interface Management

6.1 About CLI Management

Besides WEB-based management, iES8(G) Series also supports CLI management. The switch console port or Telnet can be used to configure the switch via the CLI.

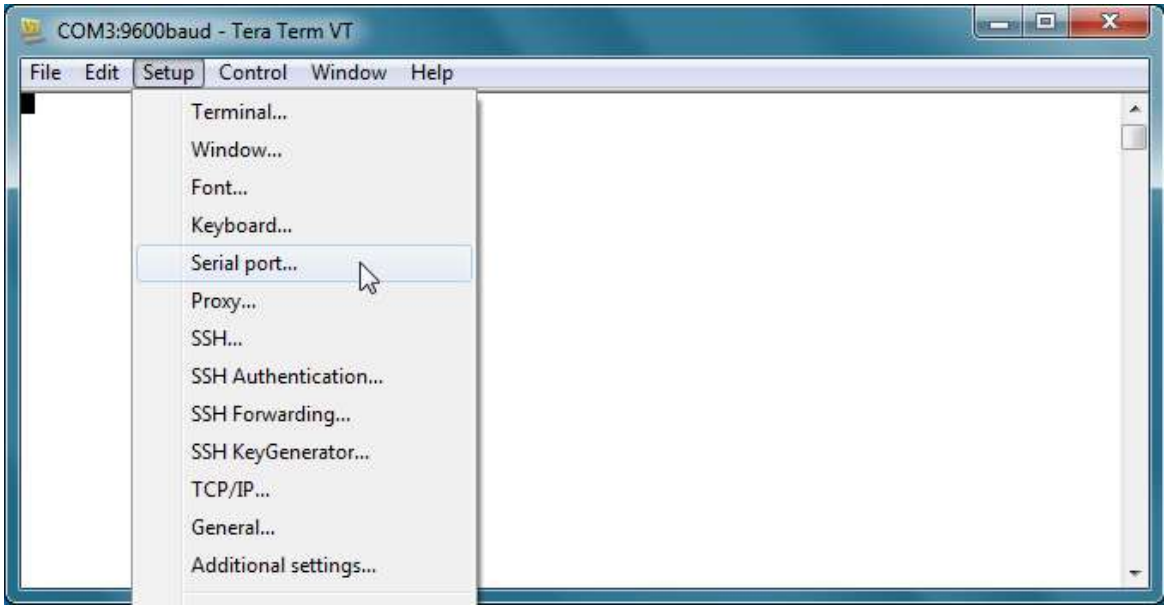
CLI Management by RS-232 Serial Console (9600, 8, none, 1, none)

Use an RJ45 to DB9-F cable to connect to the switch's console and to a local PC's COM port.

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

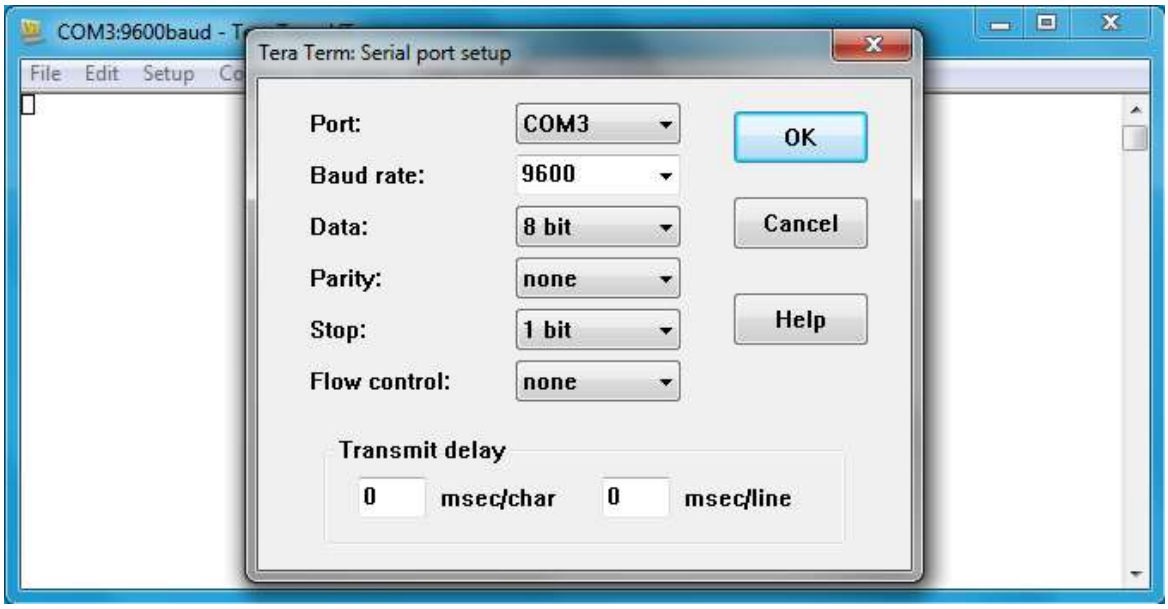
(1) Start Tara Term application.

(2) Under **Setup** select **Serial Port**.

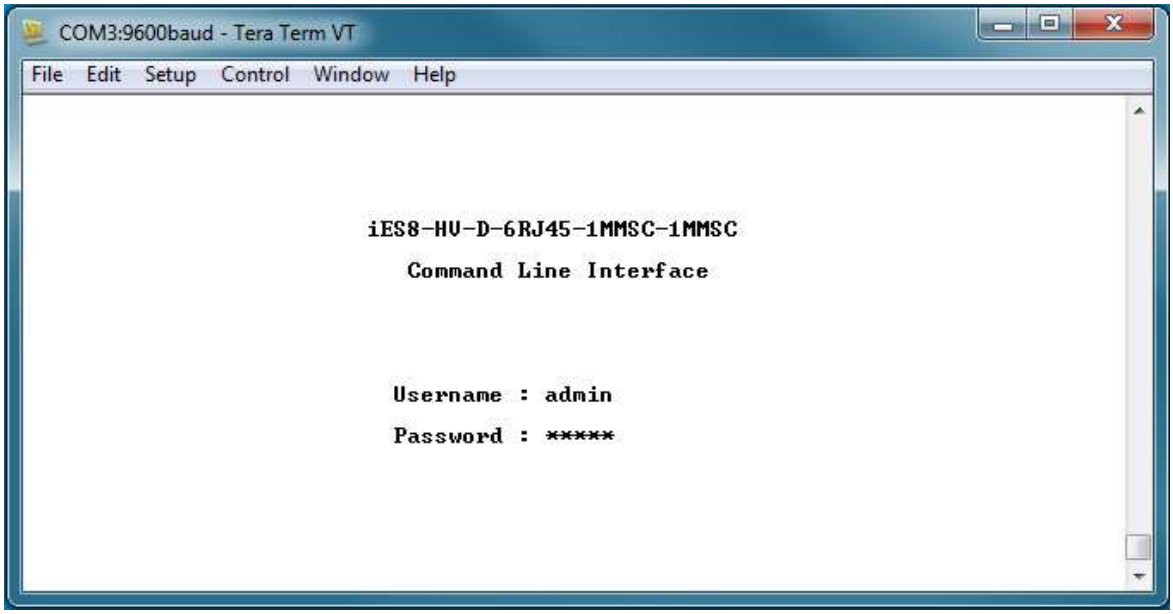


(3) Select the COM Port on your PC used to connect to the Console Port. Set the rest of the

properties to: 9600 for Baud rate, 8 for Data bits, None for Parity, 1 bit for Stop and none for Flow control, then press "OK".



(4) Press "**Enter**" on the keyboard for the Console login screen to appear. Use the keyboard to enter the Console Username and Password which is same as the Web Browser password (**admin** for both), then press "**Enter**".



CLI Management by Telnet

Users can use "**TELNET**" to configure the switches.

The default value is as below:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

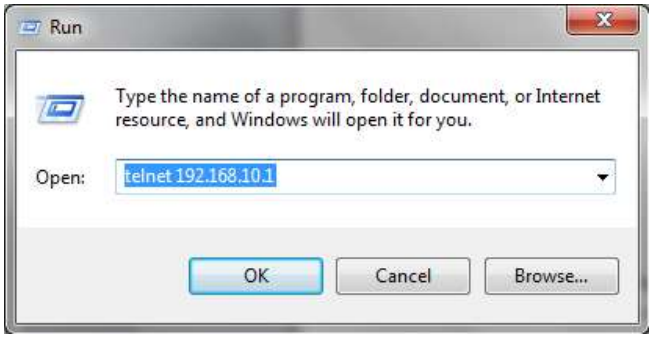
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

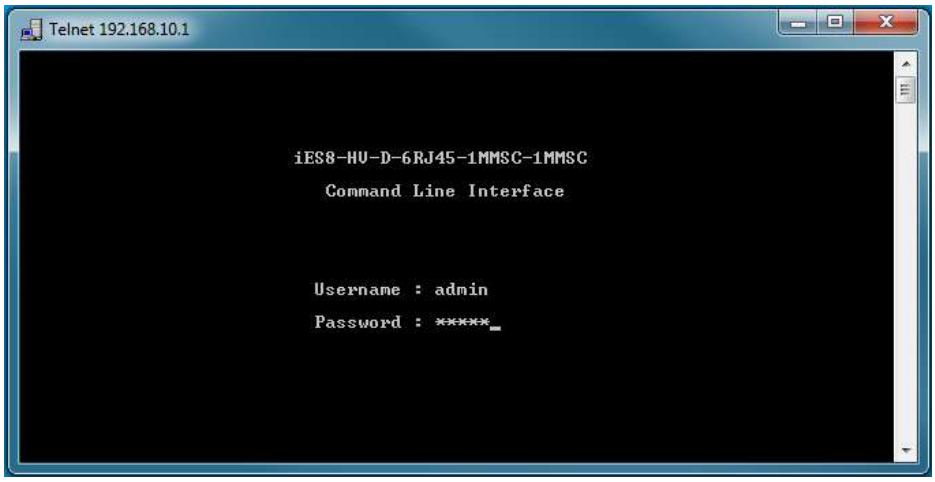
Follow the steps below to access the console via Telnet.

(1) Telnet to the IP address of the switch from the Windows "**Run"** command (or from



the MS-DOS prompt).

(2) The Console login screen appears. Use the keyboard to enter the Console Username and Password which is same as the Web Browser password (**admin** for both), then press "**Enter**"



Commands Level

Modes	Access Method	Prompt	Exit Method	About This Model
User EXEC	Begin a session with your switch.	switch>	Enter **logout** or **quit**.	The user command available at the level of user is the subset of those available at the privileged level. Use this mode to: • 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 exit privileged EXEC mode or **end.**	Use this mode to configure parameters for the switch and Ethernet ports.

Symbol of Command Level

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

6.2 Commands Set List — System Commands Set

iES8(G) Series Commands	Level	Description	Example
show config	**E**	Show switch configuration	switch>show config
show terminal	**P**	Show console information	Switch # show terminal
write memory	**P**	Save your configuration into permanent memory (flash rom)	Switch # write memory
system name [System Name]	**G**	Configure system name	switch(config)#system name xxx
system location [System Location]	**G**	Set switch system location string	switch(config)#system location xxx
system description [System Description]	**G**	Set switch system description string	switch(config)#system description xxx
system contact [System Contact]	**G**	Set switch system contact window string	switch(config)#system contact xxx
show system-info	**E**	Show system information	switch>show system-info
ip address [Ip-address] [Subnet-mask] [Gateway]	**G**	Configure the IP address of switch	switch(config)#ip address 192.168.1.1 255.255.255.0 192.168.1.254
ip dhcp	**G**	Enable DHCP client function of switch	switch(config)#ip dhcp
show ip	**P**	Show IP information of switch	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	switch(config)#reload

		restart	
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 clients
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 Commands Set List — Port Commands Set

iES8(G) Series Commands	Level	Description	Example
interface fastEthernet [Portid]	G	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex [full | half]	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
speed [10|100|1000|auto]	I	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a Gigabit 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	switch(config)#interface fastEthernet 2

		interface	switch(config-if)#security enable
no security	I	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
state [Enable | Disable]	I	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disabled form of this command to disable the port.	switch(config)#interface fastEthernet 2 switch(config-if)#state Disable
show interface configuration	I	show interface configuration status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface configuration
show interface status	I	show interface actual status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface status
show interface accounting	I	show interface statistic counter	switch(config)#interface fastEthernet 2 switch(config-if)#show interface accounting
no accounting	I	Clear interface accounting information	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting

6.4 Commands Set List — Trunk command set

iES8(G) Series Commands	Level	Description	Example
aggregator priority [1to65535]	G	Set port group system priority	switch(config)#aggregator priority 22
aggregator activityport [GroupID] [Port-list]	G	Set activity port	switch(config)#aggregator activityport 2 3-4
aggregator group [GroupID] [Port-list] **lacp** **workp** [Workport]	G	Assign a trunk group with LACP active. [GroupID] :1 to 3 [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	switch(config)#aggregator group 1 1-4 lacp workp 2 or switch(config)#aggregator group 2 1,4,3 lacp workp 3

		of work ports, this value could not be less than zero or be large than the amount of member ports.	
aggregator group [GroupID] [Port-list] **static**	G	Assign a static trunk group. [GroupID] :1 to 3 [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 static or switch(config)#aggregator group 2 1,3,4 static
show aggregator [GroupID]	P	Show the information of trunk group	switch#show aggregator 2
no aggregator lacp [GroupID]	G	Disable the LACP function of trunk group	switch(config)#no aggregator lacp 1
no aggregator group [GroupID]	G	Remove a trunk group	switch(config)#no aggregator group 2

6.5 Commands Set List—VLAN command set

iES8(G) series Commands	Level	Description	Example
vlan database	P	Enter VLAN configure mode	switch # vlan database
vlan **[8021q | portbased]**	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
Vlanmode [disable|portbase|802.1q|gvrp]	V	Assign Vlanmode	switch(vlan)#vlanmode gvrp
IEEE 802.1Q VLAN			
vlan 8021q port [PortNumber] **access-link untag** [UntaggedVID]	V	Assign an access link for VLAN by port; if the port belongs to a trunk group, this command can't be applied.	switch(vlan)#vlan 802.1q port 3 access-link untag 33
vlan 8021q port [PortNumber]	V	Assign a trunk link for VLAN by port; if the port	switch(vlan)#vlan 8021q port 3 trunk-link tag 2,3,6,99

trunk-link tag [TaggedVID List]		belongs to a trunk group, this command can't be applied.	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 belongs to a trunk group, this command can't be applied.	switch(vlan)# vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q port 3 hybrid-link untag 5 tag 6-8
vlan 8021q aggregator [TrunkID] **access-link untag** [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)#vlan 8021q aggregator 3 access-link untag 33
vlan 8021q 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 aggregator 3 trunk-link tag 3-20
vlan 8021q aggreator [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	V	Assign a hybrid link for VLAN by trunk group	switch(vlan)# vlan 8021q aggreator 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q aggreator 3 hybrid-link untag 5 tag 6-8
show vlan [VID] or **show vlan**	V	Show VLAN information	switch(vlan)#show vlan 23

6.6 Commands Set List — RSTP command set

iES8(G) series Commands	Level	Description	Example
RSTP enable	G	Enable RSTP	switch(config)#RSTP enable
RSTP priority [0to61440]	G	Configure RSTP priority parameter	switch(config)# RSTP priority 32768
RSTP max-age [seconds]	G	Use the RSTP max-age global configuration command to change the	switch(config)# RSTP max-age 15

		interval between messages the RSTP 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, the RSTP topology is recomputed.	
RSTP hello-time [seconds]	**G**	Use the RSTP hello-time global configuration command to specify the interval (1-10) between hello bridge protocol data units (BPDUs).	switch(config)# RSTP hello-time 3
RSTP forward-time [seconds]	**G**	Use the RSTP forward-time global configuration command to set the forwarding-time for the specified RSTP instances. The forwarding time (4-30) determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)# RSTP forward-time 20
RSTP max-age [seconds]	**G**	Configure RSTP max age parameter	switch(config)# RSTP max-age 25
RSTP path-cost [1to200000000]	**I**	Use the RSTP cost interface configuration command to set the path cost for RSTP calculations. In the event of a loop, RSTP considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#interface fastEthernet 2 switch(config-if)# rstp path-cost 2

RSTP port-priority [Port Priority]	I	Use the RSTP 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)# rstp port-priority 128
RSTP admin-p2p [Auto|True|False]	I	Admin P2P of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# rstp admin-p2p Auto
RSTP admin-edge [True|False]	I	Admin Edge of RSTP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# rstp admin-edge False
RSTP admin-non-stp [True|False]	I	Admin Non STP of RSTP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# rstp admin-non-stp True
Show RSTP	E	Display a summary of the RSTP states.	switch>show rstp
no RSTP	G	Disable RSTP.	switch(config)#no rstp

6.7 Commands Set List—QoS command set

iES8(G) Series Commands	Level	Description	Example
qos policy [weighted-fair|strict]	G	Select QOS policy scheduling	switch(config)#qos policy weighted-fair
qos prioritytype [port-based|cos-only|tos-only|cos-first|tos-first]	G	Setting of QOS priority type	switch(config)#qos prioritytype
qos priority portbased [Port] [lowest|low|middle|high]	G	Configure Port-based Priority	switch(config)#qos priority portbased 1 low
qos priority cos [Priority][lowest|low|middle|high]	G	Configure COS Priority	switch(config)#qos priority cos 22 middle
qos priority tos [Priority][lowest|low|middle|high]	G	Configure TOS Priority	switch(config)#qos priority tos 3 high
show qos	P	Display the information of QoS configuration	switch>show qos
no qos	G	Disable QoS function	switch(config)#no qos

6.8 Commands Set List — IGMP command set

iES8(G) Series Commands	Level	Description	Example
igmp enable	G	Enable IGMP snooping function	switch(config)#igmp enable
Igmp-query auto	G	Set IGMP query to auto mode	switch(config)#Igmp query auto
Igmp-query force	G	Set IGMP query to force mode	switch(config)#Igmp query force
show igmp configuration	P	Displays the details of an IGMP configuration.	switch#show igmp configuration
show igmp table	P	Displays the details of an IGMP snooping entries.	switch#show igmp table
no igmp	G	Disable IGMP snooping function	switch(config)#no igmp
no igmp query	G	Disable IGMP query	switch # no igmp query

6.9 Commands Set List — MAC/Filter Table command set

iES8(G) Series Commands	Level	Description	Example
mac-address-table static hwaddr [MAC]	I	Configure MAC address table of interface (static).	switch(config)#interface fastEthernet 2 switch(config-if)#mac-address-table static hwaddr 000012345678
mac-address-table filter hwaddr [MAC]	G	Configure MAC address table(filter)	switch(config)#mac-address-table filter hwaddr 000012348678
show mac-address-table	P	Show all MAC address table	switch#show mac-address-table
show mac-address-table static	P	Show static MAC address table	switch#show mac-address-table static
show mac-address-table filter	P	Show filter MAC address table.	switch#show mac-address-table filter
no mac-address-table static hwaddr [MAC]	I	Remove an entry of MAC address table of interface (static)	switch(config)#interface fastEthernet 2 switch(config-if)#no mac-address-table static hwaddr 000012345678
no mac-address-table filter hwaddr [MAC]	G	Remove an entry of MAC address table (filter)	switch(config)#no mac-address-table filter hwaddr 000012348678
no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#no mac-address-table

6.10 Commands Set List — SNMP command set

iES8(G) Series Commands	Level	Description	Example
snmp agent-mode [v1v2c | v3]	G	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2c
Snmp trap server [IP address] **community** [Community-string] **trap-version** [v1|v2c]	G	Configure SNMP trap server host information and community string	switch(config)# snmp trap server 192.168.10.50 community public trap-version v1
snmp community-strings [Community-string] **right** [RO|RW]	G	Configure the community string right	switch(config)#snmp community-strings public right RO or switch(config)#snmp community-strings public right RW
snmp snmpv3-user [User Name] **password** [Authentication Password] [Privacy Password]	G	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#snmp snmpv3-user test01 password AuthPW PrivPW
show snmp	P	Show SNMP configuration	switch#show snmp
show snmp trap	P	Show specified trap server information	switch#show snmp trap
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 trap server [Host-address]	G	Remove the SNMP server host.	switch(config)#no snmp trap server 192.168.10.50

6.11 Commands Set List — Port Mirroring command set

iES8(G) Series Commands	Level	Description	Example
monitor destination [RX|TX|Both]	I	Set destination port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)# monitor destination RX
monitor source [RX|TX|Both]	I	Set source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)# monitor source both
show monitor	P	Show port monitor information	switch#show monitor
show monitor	I	Show port monitor information	switch(config)#interface fastEthernet 2 switch(config-if)#show monitor
no monitor	I	Disable source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#no monitor

6.12 Commands Set List — 802.1x command set

iES8(G) Series Commands	Level	Description	Example
8021x enable	G	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiusip [IP address]	G	Use the 802.1x system radius IP global configuration command to change the radious server IP.	switch(config)# 8021x system radiusip 192.168.1.1
8021x system serverport [port ID]	G	Use the 802.1x system server port global configuration command to change the 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 sharedkey [ID]	G	Use the 802.1x system share key global configuration command	switch(config)# 8021x system sharedkey 123456

		to change the shared key value.	
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 supptimeout [sec.]	G	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# 8021x misc supptimeout 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	switch(config)#interface fastethernet 3 switch(config-if)#8021x portstate accept

		of the selected port.	
show 8021x	**E**	Display a summary of the 802.1x properties and also the port sates.	switch>show 8021x
no 8021x	**G**	Disable 802.1x function	switch(config)#no 8021x

6.13 Commands Set List — TFTP command set

iES8(G) Series Commands	Level	Description	Defaults Example
TFTP [IP address] **backup** [File name]	**G**	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)# tftp 192.168.10.66 backup file.cfg
TFTP [IP address] **restore** [File name]	**G**	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)# tftp 192.168.10.66 restore file.cfg
TFTP [IP address] **upgrade** [File name]	**G**	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)# tftp 192.168.10.66 upgrade firmware.bin

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

iES8(G) Series Commands	Level	Description	Example
syslog ip [IP address]	**G**	Set System log server IP address.	switch(config)# syslog ip 192.168.1.100
syslog mode [client|server|both]	**G**	Specified the log mode	switch(config)# syslog mode both
show syslog	**P**	Show system log client & server information	switch#show syslog
no syslog	**G**	Disable systemlog function	switch(config)#no syslog
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 auth.	switch(config)#smtp authentication
smtp account [account]	**G**	Configure authentication account	switch(config)#smtp account User
smtp password [password]	**G**	Configure authentication password	switch(config)#smtp password
smtp rcptemail [Index] [Email address]	**G**	Configure Rcpt e-mail Address	switch(config)#smtp rcptemail 1 Alert@test.com
show smtp	**P**	Show the information of SMTP	switch#show smtp
no smtp	**G**	Disable SMTP function	switch(config)#no smtp
event device-restart [Systemlog|SMTP|Both]	**G**	Set restart event type	switch(config)#event device-restart both
event authentication-failure [Systemlog|SMTP|Both]	**G**	Set Authentication failure event type	switch(config)#event authentication-failure both
event iRing-topology-change [Systemlog|SMTP|Both]	**G**	Set ring topology changed event type	switch(config)#event ring-topology-change both
event syslog [Link-UP|Link-Down|Both]	**I**	Set port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#event syslog 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-restart [Systemlog|SMTP|Both]	**G**	Disable cold start event type	switch(config)#no event device-restart
no event authentication-failure [Systemlog|SMTP|Both]	**G**	Disable Authentication failure event typ	switch(config)#no event authentication-failure
no event iRing-topology-change [Systemlog|SMTP|Both]	**G**	Disable iRing topology changed event type	switch(config)#no event ring-topology-change
no event syslog	**I**	Disable port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#no event syslog
no event smtp	**I**	Disable port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#no event smtp
show syslog	**P**	Show system log client & server information	switch#show syslog

6.15 Commands Set List — SNTP command set

iES8(G) Series Commands	Level	Description	Example
sntp enable	G	Enable SNTP function	switch(config)#sntp enable
sntp daylight	G	Enable daylight saving time, if SNTP function 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 Commands Set List — iRing command set

iES8(G) Series Commands	Level	Description	Example
iRing enable	G	Enable iRing	switch(config)# iring enable
iRing master	G	Enable iRing master	switch(config)# iring master
iRing ring-linking	G	Enable iRing linking	switch(config)# iring ring-linking
iRing dual-homing	G	Enable dual homing	switch(config)# iring dual-homing
iRing port [1st Ring Port] [2nd Ring Port]	G	Configure 1st/2nd Ring Port	switch(config)# iring port 7 8
iRing ring-linking-port [Coupling Port]	G	Configure iRing linking Port	switch(config)#iring ring-linking-port 1
iRing homing-port [Dual Homing Port]	G	Configure Dual Homing Port	switch(config)# iring homing-port 3
show iRing	P	Show the information of iRing	switch#show iring
no iRing	G	Disable iRing	switch(config)#no iring
no iRing master	G	Disable iRing master	switch(config)# no iring master
no iRing ring-linking	G	Disable iRing linking	switch(config)# no iring ring-linking
no iRing dual-homing	G	Disable dual homing	switch(config)# no iring dual-homing

Technical Specifications

Model Number iES8	
Technology	
Ethernet Standards	802.3 - 10Base-T, 802.3u - 100Base-TX, 100Base-FX, 802.3z - 1000Base-LX/SX 802.3ad - Link Aggregation Control Protocol 802.3x - Flow Control 802.1D - Spanning Tree Protocol 802.1p - Class of Service, 802.1Q - VLAN Tagging 802.1w - Rapid Spanning Tree Protocol, 802.1X - Authentication 802.1ad - VLAN QinQ 802.1AB - LLDP
MAC addresses	8192
Priority Queues	4
Flow Control	IEEE 802.3x Flow Control and Back-pressure
Processing	Store-and-Forward
Interface	
RJ45 Ports	10/100Base-T(X), Auto MDI/MDI-X (iES8 model)
Fiber Ports	100 Base-FX (SC/ST Connector) (iES8 model) Multi-Mode: 0 to 2 km, 1310 nm (50/125 µm or 62.5/125 µm) Single-Mode: 0 to 30km, 1310 nm (9/125 µm) 1000 Base-X (SC/ST Connector) (iES8G model) Multi-Mode: 0 to 550m, 850 nm (50/125 µm or 62.5/125 µm) Single-Mode: 0 to 10km, 1310 nm (9/125 µm)
LED Indicators	Per Unit : Power x 3(Green) RJ45 Ports: Per Port : Link/Activity(Green/Blinking Green), Full duplex(Amber) Giga/Fiber Ports: Per Port : Activity(Green), Link (Amber)
Power Requirements	
Power Input Voltage (10 Pin Terminal Block)	Dual Input low-voltage (LV) DC (10-48VDC) Dual Input medium-voltage (MV) DC (36-75VDC) Single Input Hi-voltage (HV) AC/DC input (85-264VAC, 88-300VDC) with Singl (10-48VDC) backup

Reverse Polarity Protection	Present at power supply input
Power Consumption	9 Watts Max
Environmental	
Operating Temperature	-40 to 85 °C
Storage Temperature	-40 to 85 °C
Operating Humidity	5% to 95%, non-condensing
Mechanical	
Dimensions(W x D x H)	101.6 mm(W)x 128.3 mm(D)x 153.6 mm(H); 4 in (W)x 5.05 in (D)x 6.05 in (H)
Casing	IP-40 protection
Regulatory Approvals	
Regulatory Approvals	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11
Shock	IEC 60068-2-27
Free Fall	IEC 60068-2-32
Vibration	IEC 60068-2-6
Warranty	5 years

Model Number iES8G	
Physical Ports	
10/100/1000 Base-T(X) Ports in RJ45 Auto MDI/MDIX	4
Gigabit Combo Port with 10/100/1000Base-T(X) or 100/1000Base-X SFP Port	4- Base-T(X) or 4- Base (X) SFP
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: 16Gbps 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 (iRing) with recovery time less than 30ms over 250 units TOS/Diffserv supported Quality of Service (802.1p) for real-time traffic VLAN (802.1Q) with VLAN tagging and GVRP supported IGMP Snooping for multicast filtering Port configuration, status, statistics, monitoring, security SNTP for synchronizing of clocks over network Support PTP Client (Precision Time Protocol) clock synchronization DHCP Server / Client support Port Trunk support MVR (Multicast VLAN Registration) support
Network Redundancy	iRing, MSTP
Warning / Monitoring System	Relay output for fault event alarming Syslog server / client to record and view events Include SMTP for event warning notification via email Event selection support
RS-232 Serial Console Port	RS-232 in RJ45 connector with console cable. 9600bps, 8, N, 1
LED Indicators	
Power Indicator	Green : Power LED x 3
R.M. Indicator	Green : Indicate system operated in iRing Master mode
Ring Indicator	Green : Indicate system operated in iRing mode
Fault Indicator	Amber : Indicate unexpected event occurred
10/100/1000Base-T(X) RJ45 port indicator	Green for port Link/Act. Amber for 100Mbps indicator
100/1000Base-X SFP Port Indicator	Green for port Link/Act.
Fault contact	
Relay	Relay output to carry capacity of 1A at 24VDC
Power	
Redundant Input Power	Dual DC inputs 10 to 48VDC, Dual DC Inputs 36-72VDC, or Single input universal supply 88-370VDC or 85-264VAC with a single 10-48VDC Backup.
Power Consumption (Typ.)	10 Watt
Overload Current Protection	Present
Reverse Polarity Protection	Internal
Physical Characteristic	
Enclosure	IP-40 Galvanized Steel
Dimension (W x D x H)	74.3(W)x109.2(D)x153.6(H) mm (2.93 x 4.3 x 6.05 inch)

Weight	1kg
Environmental	
Storage Temperature	-40 to 85oC (-40 to 185oF)
Operating Temperature	-40 to 85oC (-40 to 185oF)
Operating Humidity	5% to 95% Non-condensing
Regulatory approvals	
EMI	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11
Shock	IEC60068-2-27
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6
Safety	EN60950-1
Warranty	
Warranty	5 Years

Appendix A: iES8 (G) Modbus Information

*Device ID/PLC is 1

*04 Read Input Register (3x) should be used.

*The returned values are in hex format

Address	Description
16	VendorName
48	ProductName
81	Version
85	MacAddress
256	SysName
512	SysDescription
768	SysLocation
1024	SysContact
4096	PortStatus: Port :1~VTSS_PORTS Value :0x0000 Link down 0x0001 Link up 0x0002 Disable 0xffff NoPort
4352	PortSpeed: Port :1~VTSS_PORTS Value :0x0000 10M-Half 0x0001 10M-Full 0x0002 100M-Half 0x0003 100M-Full 0x0004 1G-Half 0x0005 1G-Full 0xffff NoPort
4608	PortFlowCtrl : Port :1~VTSS_PORTS Value :0x0000 Off 0x0001 On 0xffff NoPort