SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS

Intelligent 10 Port Managed Ethernet Switch

iES10G(F) Series User's Manual

Version 2.30-4
Mar 2023

iS5 Communications Inc.
5895 Ambler Dr.
Mississauga, Ontario, L4W 587
Tel: + 905- 670- 0004
Website: www.iS5Com.com
E-mail: info@is5com.com

www.iS5com.com

All Rights Reserved

Disclaimer Of Liability

We have checked the contents of this manual against the hardware and software described. However, deviations from the description cannot be completely ruled out.

iS5 Communications shall not be liable for any errors or omissions contained herein or for consequential damages in connection with the furnishing, performance, or use of this material.

The information given in this document is reviewed regularly and any necessary corrections will be included in subsequent editions. We appreciate any suggested improvements. We reserve the right to make technical improvements without notice.

Registered Trademarks

iS5Com™, is a trademark of iS5 Communications Inc. Other designations in this manual might be trademarks whose use by third parties for their own purposes would infringe the rights of the owner.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

The registered trademark Linux® is used pursuant to a sublicense from LMI, the exclusive licensee of Linus Torvalds, owner of the mark on a world-wide basis.

Third Party Copyrights

If any. All Rights Reserved.

Warranty

Five (5) years from date of purchase, return to factory. For warranty details, visit www.iS5Com.com or contact your customer service representative.

Table of Contents

CAUTION: LASER 6

CAUTION: SERVICE 6

CAUTION: PHYSICAL ACCESS 6

INTRODUCTION 7

1.1 About the iES10G(F) Series Intelligent Managed Ethernet Switch 7

1.2 Software Features 7

1.3 Hardware Features 7

Hardware Installation 8

2.1 Installing the Switch on a DIN-Rail 8

2.1.1 Mounting the iES10G(F) on a DIN-Rail 8

2.2 Wall Mount Installation 9

2.2.1 Mounting the iES10G(F) on a Wall or Panel 9

Hardware Overview 10

3.1 Front Panel 10

3.2 Front Panel LED's 11

3.3 Bottom View Panel 12

3.4 Rear Panel 13

3.5 Side Panel 14

Cables 15

4.1 Ethernet Cables 15

4.1.1 100BASE-TX/10BASE-T Pin Assignements 15

4.2 SFP 16

4.3 Console Cable 17

WEB Management 18

5.1 Configuration by Web Browser 18

5.1.1 About Web-based Management 18

5.1.2 System Information 20

5.1.3 Front Panel 21

5.1.4 Basic setting 21

5.1.4.1 Switch Setting 21

5.1.4.2 Admin Password 22

5.1.4.3 IP Setting 23
5.1.4.4 SNTP (Time) 24
5.1.4.5 LLDP 26
5.1.4.6 Modbus TCP 26
5.1.4.7 Auto Provision 27
5.1.4.8 Backup & Restore 27
5.1.4.9 Upgrade Firmware 28
5.1.5 DHCP Server 29
5.1.5.1 DHCP Server – Setting 29
5.1.5.2 DHCP Server – Client List 31
5.1.5.3 DHCP Server – Port and IP bindings 31
5.1.6 Port Setting 31
5.1.6.1 Port Control 31
5.1.6.2 Port Status 33
5.1.6.3 Rate Limit 33
5.1.6.4 Port Trunk 34
5.1.7 Redundancy 36
5.1.7.1 iRing 36
5.1.7.2 iChain 37
5.1.7.3 iBridge 38
5.1.7.4 RSTP-Repeater 39
5.1.7.5 Fast Recovery 39
5.1.7.6 Dual Port Recovery 40
5.1.7.7 RSTP 43
5.1.7.8 MSTP 46
5.1.7.9 MRP 49
5.1.8 VLAN 50
5.1.8.1 VLAN Setting 50
5.1.8.2 VLAN Setting – Port Based 52
5.1.9 SNMP 53
5.1.9.1 SNMP – Agent Setting 53
5.1.9.2 SNMP – Trap Setting 55
5.1.10 Traffic Prioritization 56
5.1.11 Multicast 60
5.1.11.1 IGMP Snooping 60
5.1.11.2 Multicast Filter 61
5.1.12 Security 62
5.1.12.1 IP Security 62

5.1.12.2 Port Security 63
5.1.12.3 MAC Blacklist 63
5.1.12.4 802.1x 64
5.1.13 Warning 67
5.1.13.1 Fault Alarm 67
5.1.13.2 System Alarm 68
5.1.14 Monitor and Diagnostics 71
5.1.14.1 MAC Address Table 71
5.1.14.2 MAC Address Aging 71
5.1.14.3 Port Statistics 72
5.1.14.4 Port Monitoring 73
5.1.14.5 System Event Log 74
5.1.15 Save Configuration 75
5.1.16 Factory Default 75
5.1.17 System Reboot 76

Command Line Interface Management (CLI) 77

6.1 About CLI Management 77
6.2 Commands Set List—System Commands Set 82
6.3 Commands Set List—Port Commands Set 84
6.4 Commands Set List—Trunk command set 86
6.5 Commands Set List—VLAN command set 87
6.6 Commands Set List—Spanning Tree command set 88
6.7 Commands Set List—QoS command set 90
6.8 Commands Set List—IGMP command set 90
6.9 Commands Set List—MAC/Filter Table command set 91
6.10 Commands Set List—SNMP command set 91
6.11 Commands Set List—Port Mirroring command set 92
6.12 Commands Set List—802.1x command set 93
6.13 Commands Set List—TFTP command set 95
6.14 Commands Set List—SYSLOG, SMTP, EVENT command set 95
6.15 Commands Set List—SNTP command set 96
6.16 Commands Set List—iRing command set 97

Technical Specifications 99

APPENDIX A: IES10G(F) MODBUS INFORMATION 102

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.

INTRODUCTION

1.1 About the iES10G(F) Series Intelligent Managed Ethernet Switch

The iES10G(F) is an industrial grade managed Ethernet switch with numerous features. The iES10G(F) is capable of operating under a wide temperature range, dusty environments, and in humid conditions. The switch 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 used to easily configure multiple switches at the same time, and also monitor their status.

1.2 Software Features

- World's fastest Rapid Redundant Ethernet Ring (Recovery time < 30ms with up to 250 units)
- Supports Ring Linking, Dual Homing over iRing, and standard STP/RSTP/MSTP
- 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

- 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°C to +85°C
- Storage Temperature: -40°C to 85°C
- Operating Humidity: 5% to 95%, non-condensing
- Chassis: IP-40 Galvanized Steel
- 7 x 10/100Base-T(X) Ethernet ports

- 1 x 10/100/1000Base-T(X) Ethernet ports
- Up to 3 x 100/1000Base-(X) SFP ports (Optional)
- Console Port
- iES10G Dimensions(W x D x H) : IES10G - 101.6 mm(W)x 109.2 mm(D)x 153.8 mm(H) (4x4.3 x 6.05 inch)
- iES10GF Dimensions (W x D x H): iES10GF – 101.8(W)x163.2(D)x153.6(H) mm (4 x 6.43 x 6.05 inch)
- Complies with: iEC 61850 -3; IEC 61800-3 (variable speed drive systems); IEC 61000-6-2 (generic industrial) (iES10GF only)

Hardware Installation

2.1 Installing the Switch on a DIN-Rail

Each switch has a DIN-Rail bracket on the rear panel. The DIN-Rail bracket helps secure the switch on to the DIN-Rail.

2.1.1 Mounting the iES10G(F) on a DIN-Rail

Step 1: Slant the switch and hook the top 2 catches of the metal bracket onto the top of the DIN-Rail.

Step 2: Push the bottom of the switch toward the DIN-Rail until the bracket snaps in place.

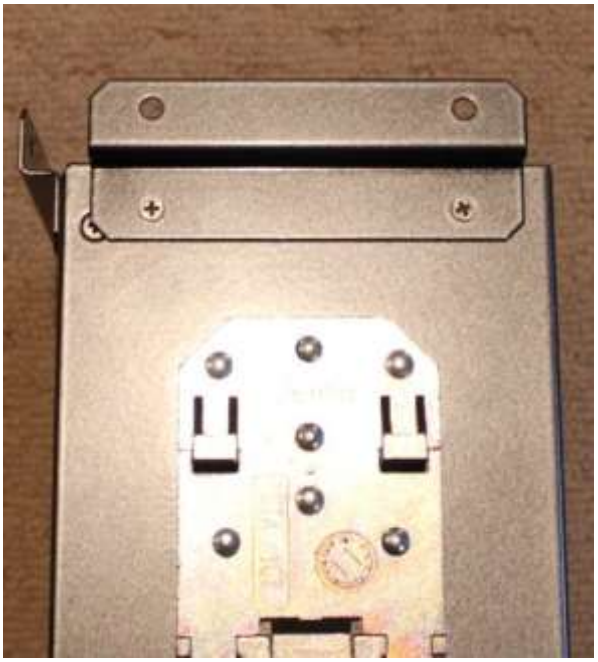
2.2 Wall Mount Installation

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

2.2.1 Mounting the iES10G(F) on a Wall or Panel

Option 1: Fix mounting brackets to the side of switch using the 4 screws included in the package.

Option 2: Fix mounting brackets to back of switch using 4 screws included in the package.



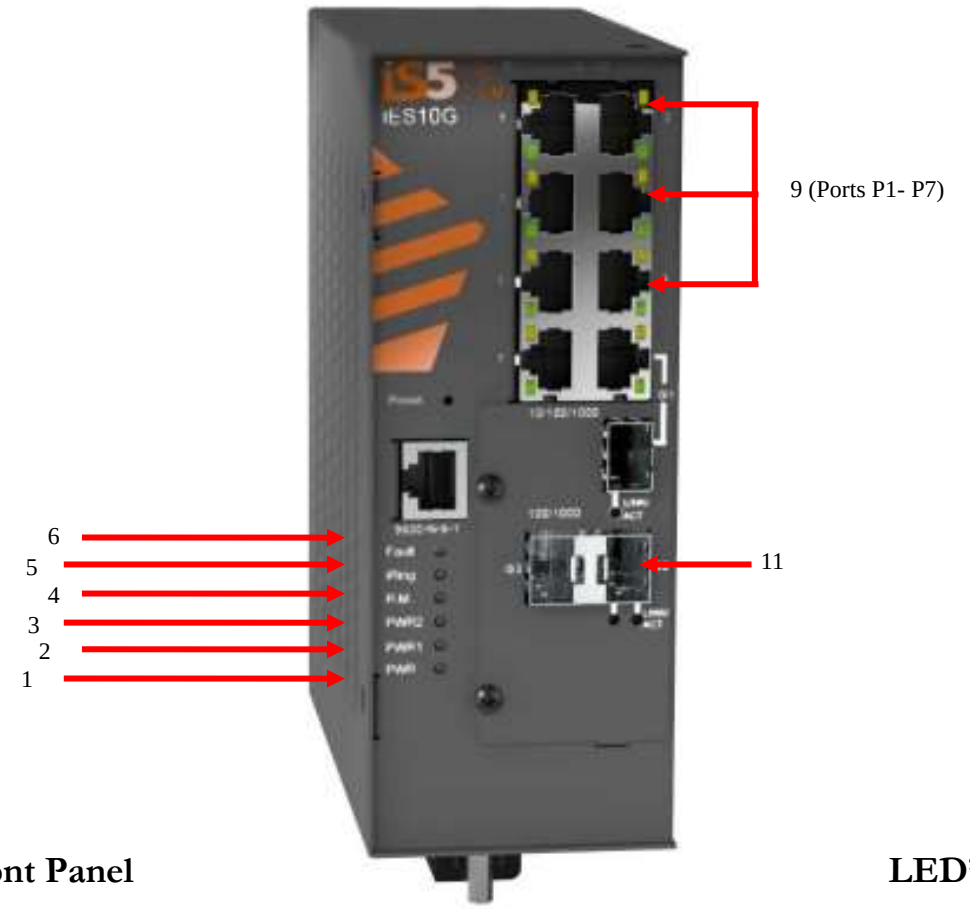
Note: To avoid damage to the unit please use the screws provided to mount the panel mount brackets to the unit.

Hardware Overview

3.1 Front Panel

Product description:

Port	Description
10/100 RJ45 fast Ethernet ports (9)	7 x 10/100Base-T(X) RJ45 fast Ethernet ports support auto-negotiation. Default Setting : Speed: auto Duplex: auto Flow control : disable
Gigabit RJ45 port (10)	2 x 10/100/1000Base-T(X) ports (Optional)
Fiber port (not shown)	3x 100/1000Base-(X) SFP ports (Optional)
Console (7)	Use a RS232 to RJ45 cable assembly to manage switch.
Reset (8)	Push and hold the reset button for 2-3 seconds to reset the switch. Push and hold the reset button for 5 seconds to reset the switch into **Factory Default.**



3.2 Front Panel LED's

Item	Description	Color	Status	Function
1	PWR	Green	On	DC power ready
2	PWR 1	Green	On	DC power module 1 activated.
3	PWR 2	Green	On	DC power module 2 activated.
4	R.M	Green	On	iRing Master.
5	iRing	Green	On	iRing enabled.
			Slow blinking	iRing topology has problem
			Fast blinking	iRing work normally.
6	Fault	Amber	On	Fault relay. Power failure or Port down/fail.
9	10/100Base-TX Fast Ethernet ports			
	LNK / ACT	Green	On	Port link up.
			Blinking	Data transmission.
	Full Duplex	Amber	On	Port working at full duplex.
11	Gigabit Ethernet ports (combo ports)			
	LNK/ACT	Green	On	Port link up.
			Blinking	Data transmission.

	Speed	Amber	On	Port operating at 100Mbps
Not Shown	Gigabit SFP ports (combo ports)			
	LNK / ACT	Green	On	Port link up.
			Blinking	Data transmission.

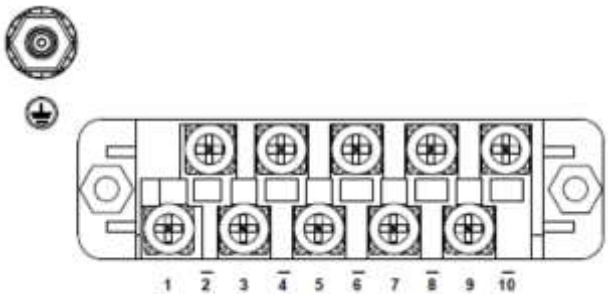
3.3 Bottom View Panel

The Phillips Screw Terminal Block, located on the bottom of the unit, 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.

The iES10G(F) series supports dual redundant power supplies (PWR1 and PWR2). There are 3 options:

1. LV: Dual Input 10-48VDC
2. MV: Dual Input 36-72VDC
3. HV: Single Input 120-370VDC or 85-264VAC with a Single 10-48VDC backup.

There are also connections for the Failsafe Relay. The Failsafe Relay is rated 1A @ 24VDC. Connections to the Terminal block are listed in the table below.



Terminal Number	Description	Connection
1	PWR1 (L) – Live	Connect to the (Live) of DC power supply 1 or (Live) terminal of an AC power source.
2	PWR1 (G) – Ground	DC Power supply 1 ground connection or AC power round connection.
3	PWR1 (N) – Neutral	Connect to the Neutral of the DC power supply 1 or (Neutral) terminal of an AC power source.
4	G – Chassis Ground	Connected to the ground bus for DC inputs or Safety Ground terminal for AC Units. Chassis

		Ground connects to both power supply surge grounds via a removable jumper.
5	PWR2 (L) – Live	Connect to the (Live) terminal of Power supply 2 or backup DC power source.
6	PWR2 (G) – Ground	Power supply 2 or backup DC power source ground connection.
7	PWR2 (N) – Neutral	Connect to the (Neutral) terminal of Power supply 2 the second or backup DC power source.
8	RLY NO	Failsafe Relay, (Normally Open) contact.
9	RLY CM	Failsafe Relay (Common) contact.
10	RLY NC	Failsafe Relay (Normally Closed) contact.

Chassis Ground Connection

The iES10G(F) chassis ground connection, located next to the terminal block, 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).

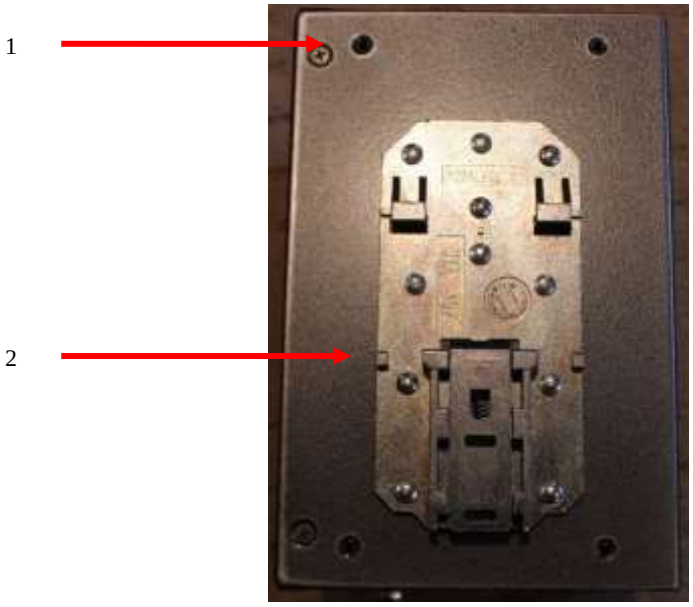
- *100-240VAC rated equipment: A 250VAC appropriately rated circuit breaker must be installed.*
- *Equipment must be installed according to the applicable country wiring codes.*
- *When equipped with a HI voltage power supply and DC backup, independent sources can be used to power the product for greater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

- *120-370VDC rated equipment: A 370VDC 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 codes.*

3.4 Rear Panel

The components on the rear of the iES10G(F) are shown below:

1. Screw holes (4) for wall mount kit.
2. DIN-Rail mount



3.5 Side Panel

The components on the side of the iES10G(F) are shown below:

1. Screw holes (4) for wall mount kit.

Cables

4.1 Ethernet Cables

The iES10G(F) switch uses standard Ethernet ports, hence enabling use of CAT 3, 4, 5, 5e UTP cables to connect to any network device i.e. PC's, server's, switch's, router's, and hub's. Please refer to the following table for cable specifications.

Cable Types and Specifications:

Cable	Type	Max. Length	Connector
10BASE-T	Cat.3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ45
100BASE-TX	Cat.5 100-ohm UTP	UTP 100 m (328 ft)	RJ45
1000BASE-TX	Cat.5/Cat.5e 100-ohm UTP	UTP 100 m (328ft)	RJ45

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

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

RJ45 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 iES10G(F) switch supports auto MDI/MDI-X operation. Use a straight-through cable to connect a PC to the switch. The following table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

MDI/MDI-X pins assignment:

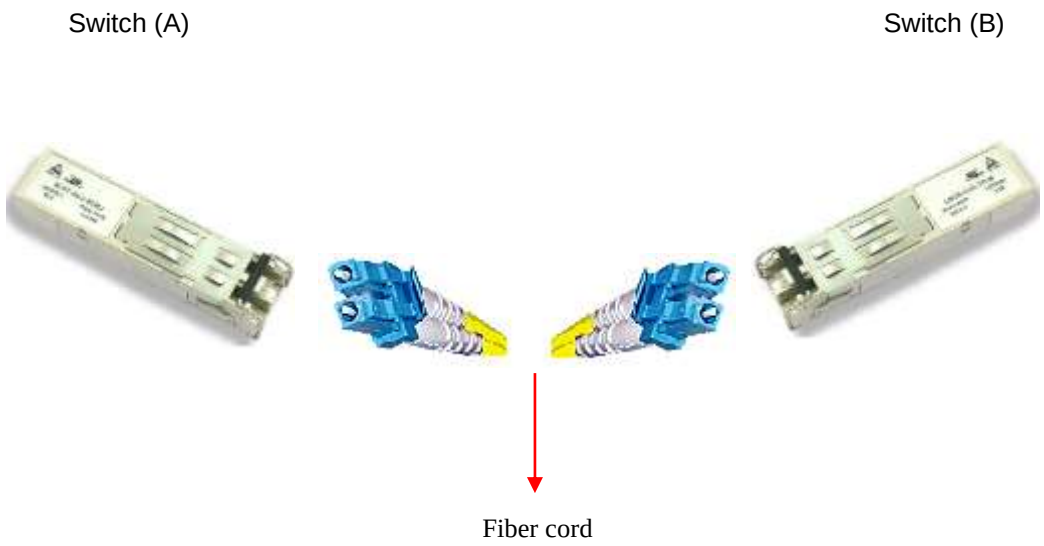
Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

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

4.2 SFP

The iES10G(F) has optional fiber optical ports with SFP connectors. The fiber optical ports are Multimode LC connectors (0 to 550m, 850 nm with 50/125 µm, and 62.5/125 µm fiber), or Singlemode LC connectors.

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

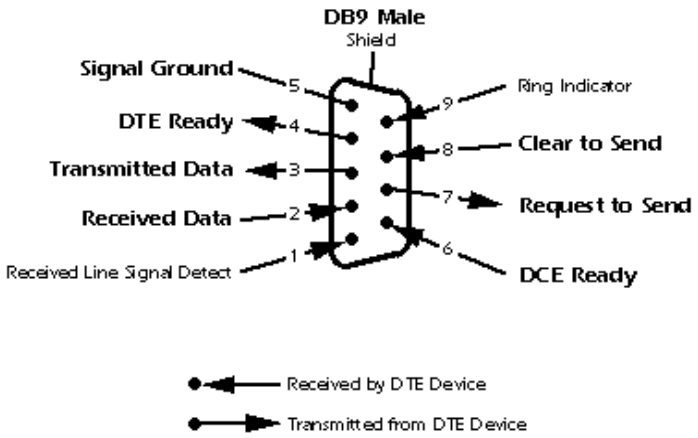


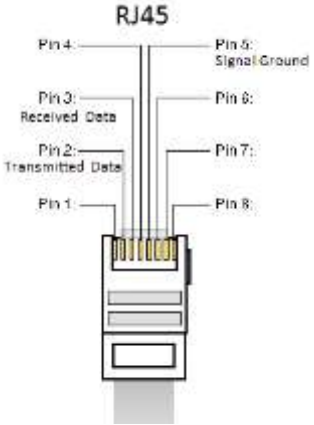
4.3 Console Cable

The iES10G(F) switch can be managed via the console port using the RS232 / DB-9 to RJ-45 cable provided. Connect to the PC via the RS-232/DB9 connector and the RJ45 connector to the console port of the switch.

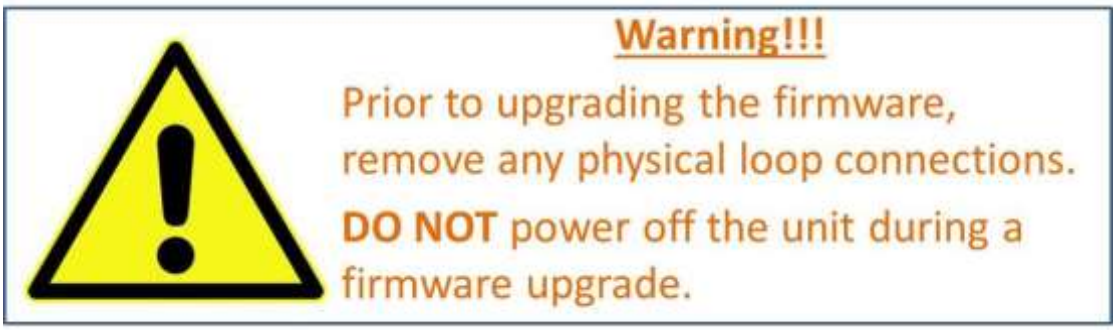
Console Cable pin assignments:

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





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 website resides in the flash memory of the CPU board. It contains advanced management features that allows management of the switch from anywhere on the network through a standard web browser such as Microsoft Internet Explorer.

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

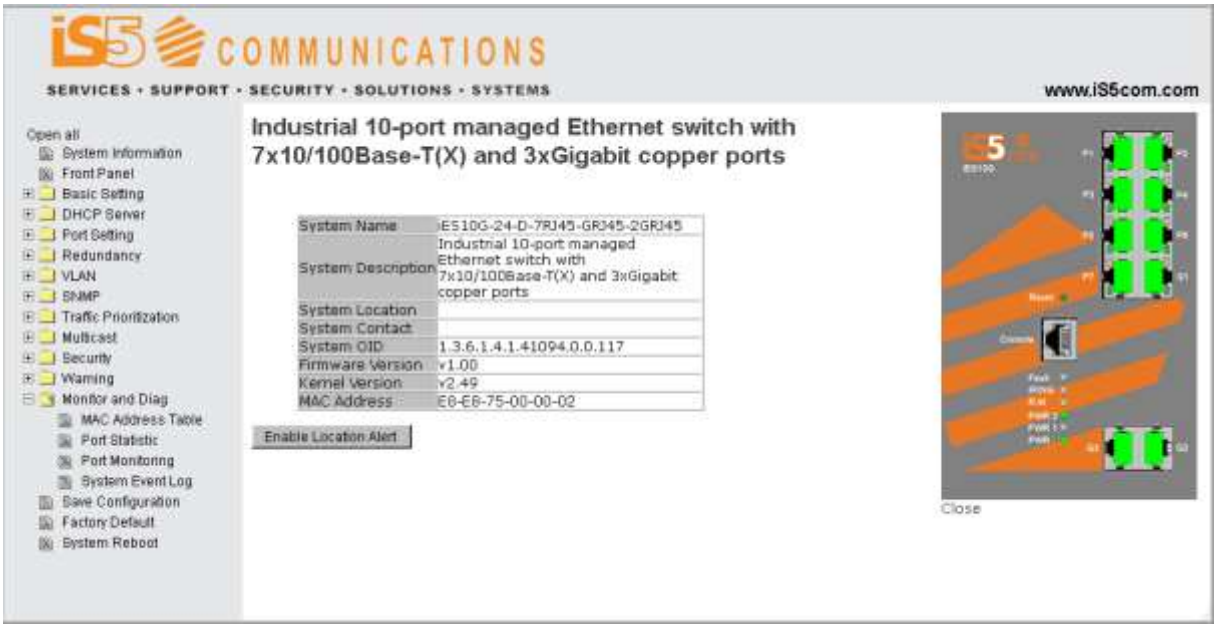
System Login

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

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

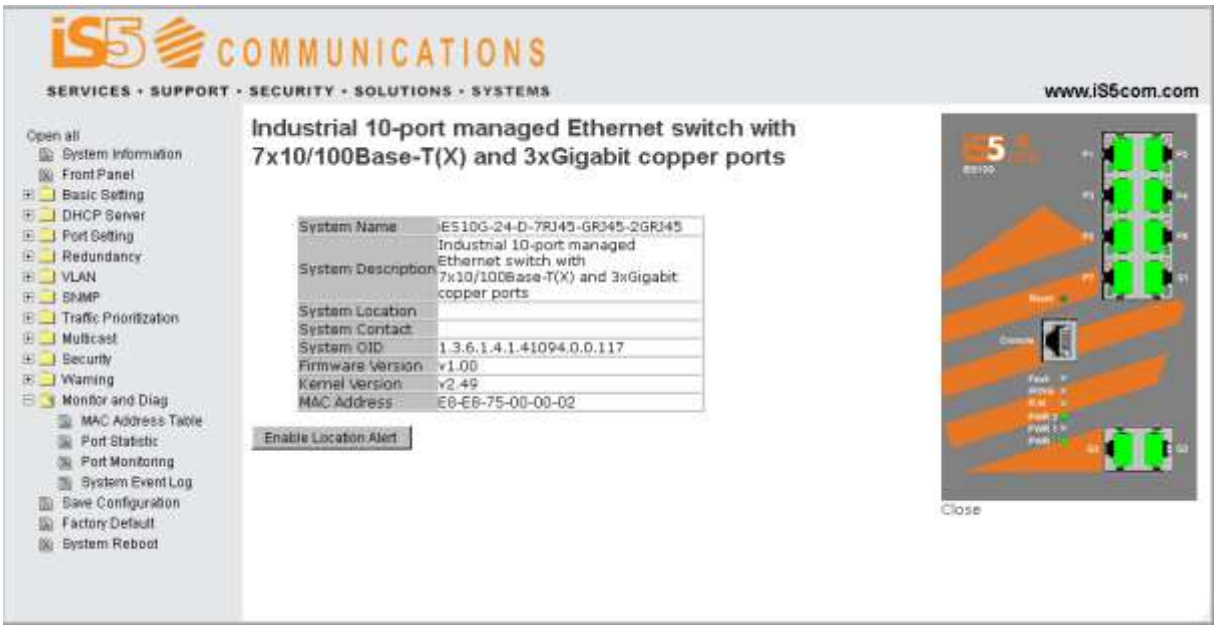
Login screen

Main Interface



Main interface

5.1.2 System Information



System Information interface

System Information

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

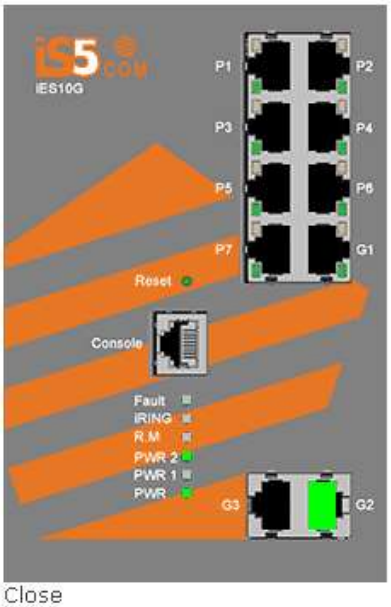
Enable Location Alert

Click Enable Location Alert, PWR1 and PWR2 LED's of the switch will start to flash together;

Click Disable Location Alert, the LED's stop flashing.

5.1.3 Front Panel

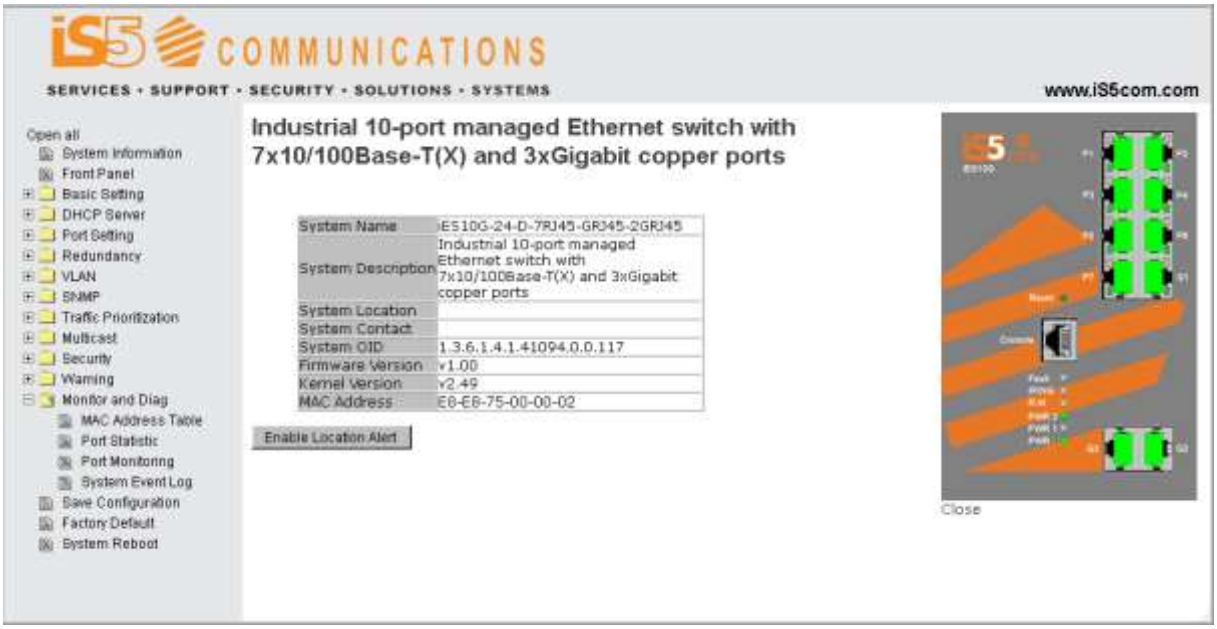
Displays the front panel of the iES10G(F). Click "**Close**" to hide the image.



Close

5.1.4 Basic setting

5.1.4.1 Switch Setting



Switch setting interface

The following table describes the Switch setting interface page.

Label	Description
System Name	Assign a name to the switch. The maximum length is 64 bytes
System Description	Displays the description of the switch.
System Location	Assign the switch a physical location. The maximum length is 64 bytes

System Contact	Enter the name of contact person or organization
System OID	Displays the switch's OID information
Firmware Version	Displays the switch's firmware version
Kernel Version	Displays the kernel software version
MAC Address	Displays the unique hardware address assigned by manufacturer (default)

5.1.4.2 Admin Password

Change the web management login username and password for management security. The maximum length of the admin password is 10 characters.

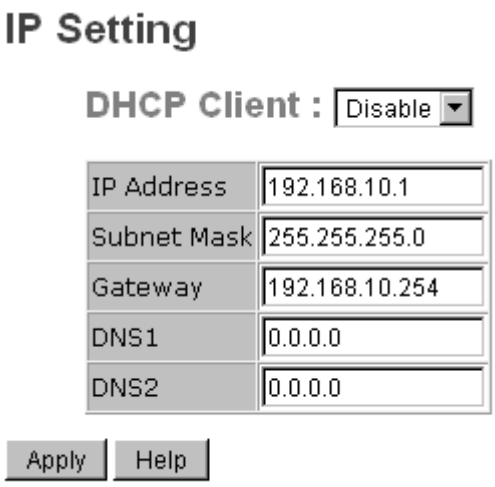
Admin Password interface

The following table describes the Admin Password interface page.

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

5.1.4.3 IP Setting

Configuring the IP Settings and DHCP client function through IP configuration interface.



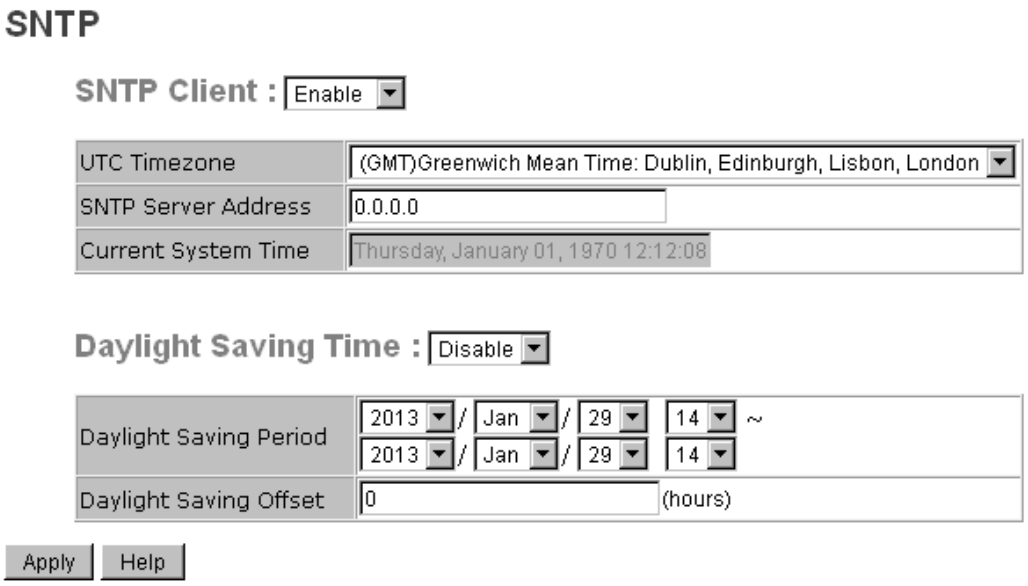
IP Configuration interface

The following table describes the labels in IP configuration interface page.

Label	Description
DHCP Client	To enable or disable the DHCP client function. When DHCP client function is enabled, the switch assigns the IP address from the network DHCP server. The default IP address is replaced by the IP address assigned by the DHCP server. After clicking the "**Apply**" button, a popup dialog shows up to inform when the DHCP client is enabled.
IP Address	Assign the IP address that the network is using. If DHCP client function is enabled, there is no 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 address is 192.168.10.1.
Subnet Mask	Assign the subnet mask of the IP address. If the DHCP client function is enabled, there is no need to assign a subnet mask.
Gateway	Assign the network gateway for the switch. The default gateway is 192.168.10.254.
DNS1	Assign the primary DNS IP address
DNS2	Assign the secondary DNS IP address
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.4.4 SNTP (Time)

The SNTP (Simple Network Time Protocol) settings allow synchronization of the switch clocks to the Internet.



SNTP Configuration interface

The following table describes the SNTP Configuration interface page.

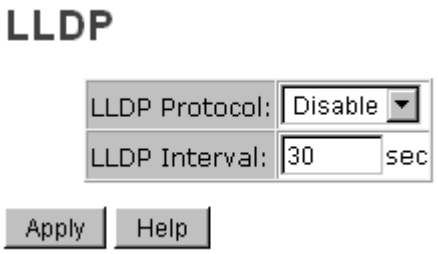
Label	Description
SNTP Client	Enables or disables the SNTP function to get the time from the SNTP server.
Daylight Saving Time	Enables or disables daylight saving time function. When daylight saving time is enabled, the daylight saving time period needs to be configured.
UTC Time zone	Set the switch location time zone. The following table lists the different time zones for reference.
SNTP Sever Address	Set the SNTP server IP address.
Current System Time	Display the switch current time.
Daylight Saving Period	Set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different each year.
Daylight Saving Offset	Set up the offset time.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

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

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 LLDP configuration interface page.

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

5.1.4.6 Modbus TCP

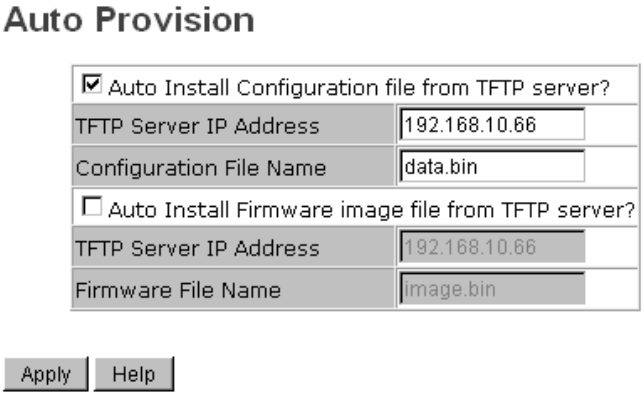
This page shows Modbus TCP support of the switch. (For more information regarding Modbus, please visit http://www.modbus.org/)

Label	Description
Mode	Shows the existing status of the Modbus TCP function
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values.

Note: For Modbus commands please see Appendix A.

5.1.4.7 Auto Provision

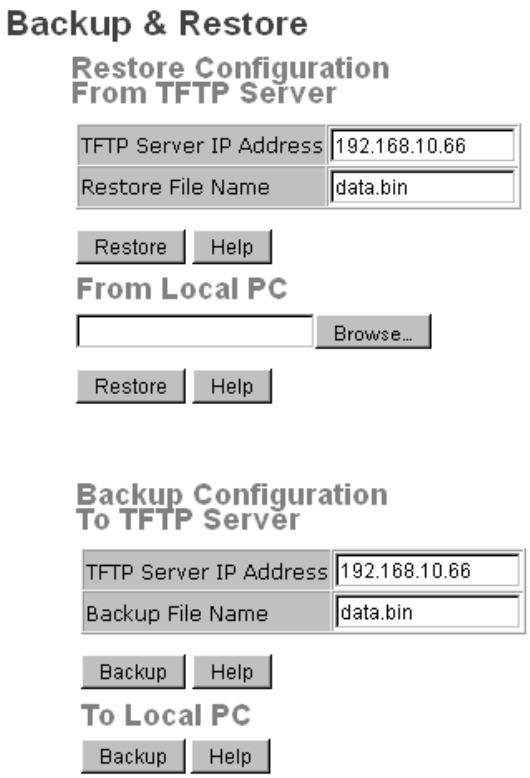
Auto Provision allows the system administrator to update the switch firmware automatically. Firmware and/or the configuration file can be stored on the TFTP server. When the switch is rebooted, the switch will upgrade automatically. Before updating, make sure the TFTP server is ready and the firmware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



Auto Provision interface

5.1.4.8 Backup & Restore

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



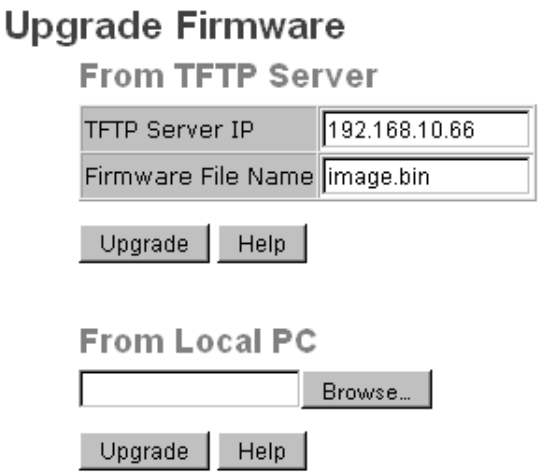
Backup & Restore interface

The following table describes the Backup & Restore interface page.

Label	Description
TFTP Server IP Address	Enter the TFTP server IP address.
Restore File Name	Enter the file name.
Restore	Click "**restore**" to restore the configurations.
Backup File Name	Enter the file name.
Backup	Click "**backup**" to backup the configurations.
Help	Show help file.

5.1.4.9 Upgrade Firmware

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



Update Firmware Interface

5.1.5 DHCP Server

5.1.5.1 DHCP Server – Setting

The Switch had 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 DHCP Server Configuration interface page.

Label	Description
DHCP Server	Enable or Disable the DHCP Server function. Enable – the switch will act as the DHCP server on your local network.
Start IP Address	The dynamic IP assign range. The lowest IP address is the starting of the dynamic IP assigned range. For example: dynamic IP assigned range

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

5.1.5.2 DHCP Server – Client List

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

DHCP Server - Client List

IP Address	MAC Address	Type	Status	Lease

DHCP Server Client Entries interface

5.1.5.3 DHCP Server – Port and IP bindings

You can assign the specific IP address in the assigned dynamic IP range to a specific port. While the device is connecting to the port, it will ask for dynamic IP to be assigned. The system automatically assigns the IP address which was assigned prior to the connected device.

DHCP Server - Port and IP Binding

Port No.	IP Address
Port.01	0.0.0.0
Port.02	0.0.0.0
Port.03	0.0.0.0
Port.04	0.0.0.0
Port.05	0.0.0.0
Port.06	0.0.0.0
Port.07	0.0.0.0
G1	0.0.0.0
G2	0.0.0.0
G3	0.0.0.0

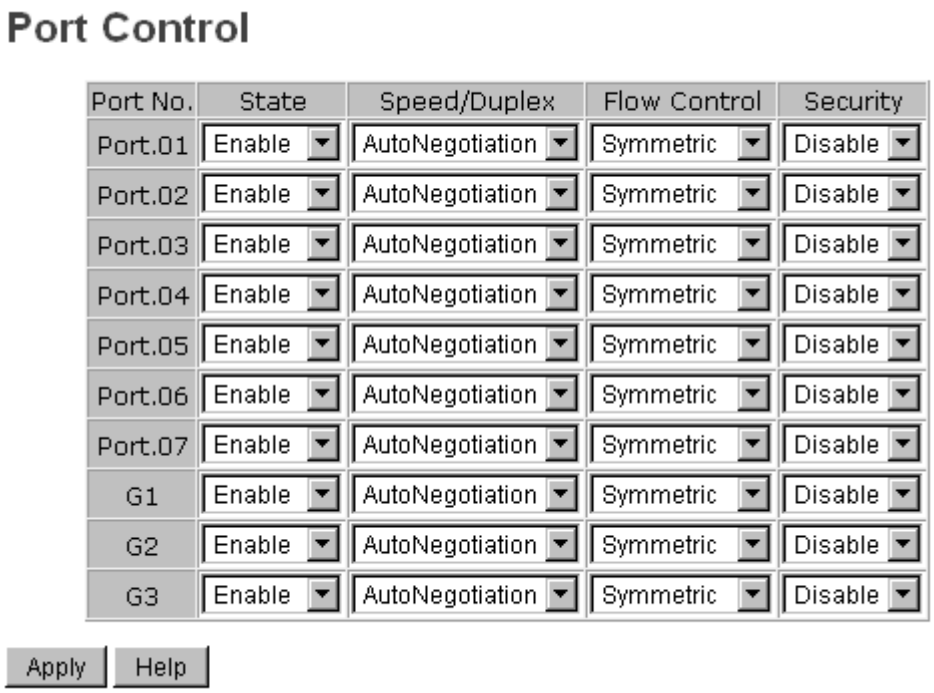
Apply Help

DHCP Server Port and IP Binding interface

5.1.6 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 Port Control interface page.

Label	Description
Port No.	Port number for setting.
Speed/Duplex	You can 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.
Help	Show help file.

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	Down	Enable	N/A	N/A
Port.06	100TX	Down	Enable	N/A	N/A
Port.07	100TX	Down	Enable	N/A	N/A
G1	1000TX	Down	Enable	N/A	N/A
G2	1000TX	UP	Enable	1000 Full	Enable
G3	1000TX	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 on all ports, including broadcast, multicast and flooded Unicast. It can also set “Ingress” or “Egress” to limit traffic received or 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
G1	All	0 kbps	0 kbps
G2	All	0 kbps	0 kbps
G3	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

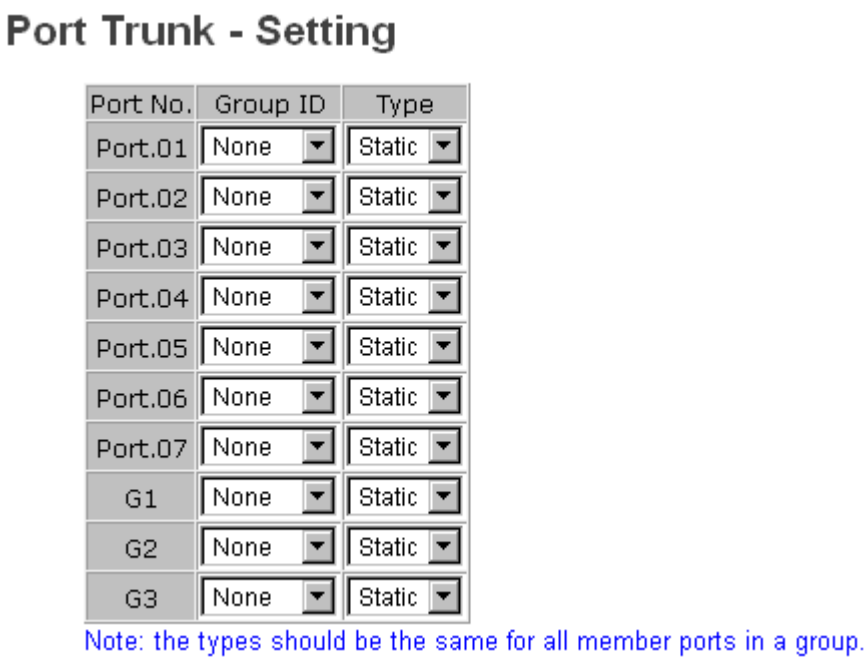
The following table describes the Rate Limit interface page.

Label	Description
Ingress Limit Frame Type	Can be set to: "**All**", "**Broadcast only**", "**Broadcast/Multicast**" or "**Broadcast/Multicast/Flooded Unicast**" mode.
Ingress	The switch port received traffic.
Egress	The switch port transmitted traffic.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.6.4 Port Trunk

Port Trunk – Setting

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



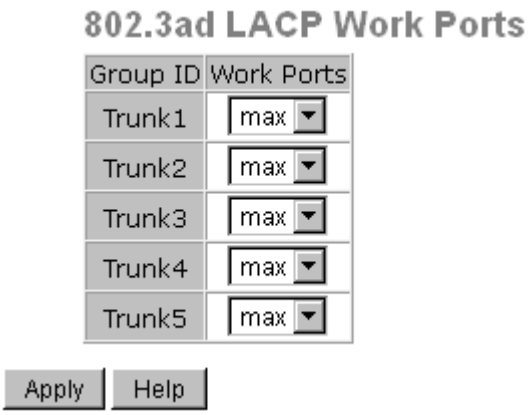
Port Trunk - Setting interface

The following table describes the Port Trunk Setting interface page.

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.
Help	Show help file.

Port Trunk – LACP

LACP is part of the IEEE standard 802.3ad that allows you to bundle several physical ports to form a single logical channel. When you change the number of active bundled ports on a port channel, traffic patterns will reflect the rebalanced state of the port channel.

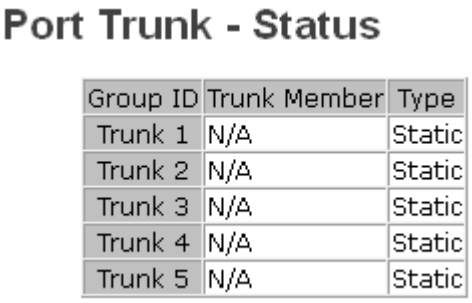


The following table describes the Port Trunk LACP interface page.

Label	Description
Work Ports	Work ports counted (max:4 ports)
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

Port Trunk – Status

You can check the configuration of a port trunk.

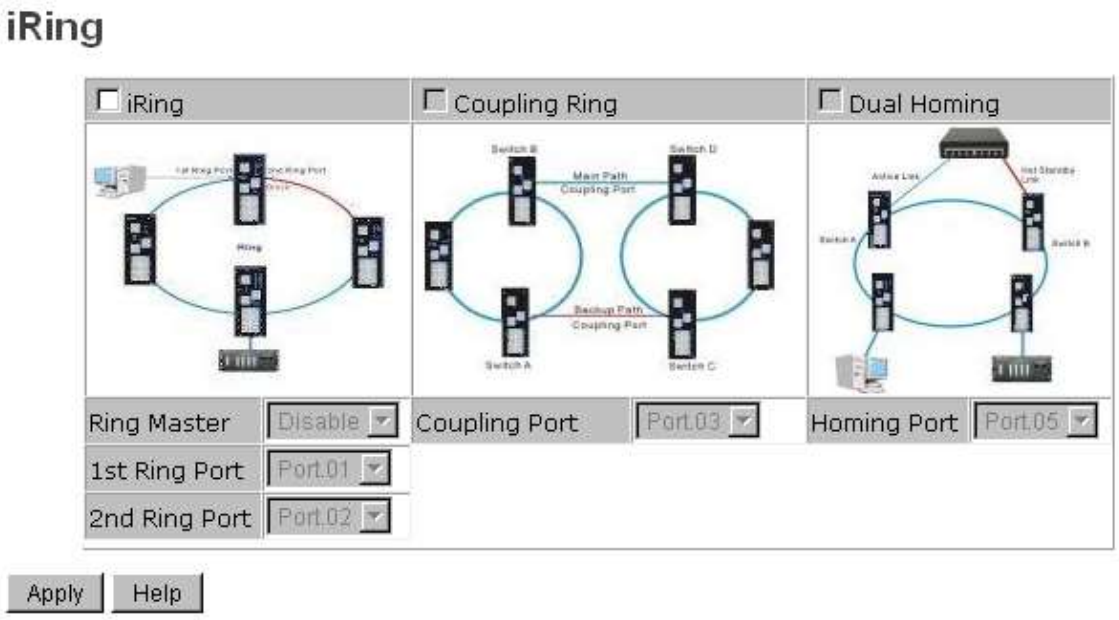


Port Trunk - Status interface

5.1.7 Redundancy

5.1.7.1 iRing

iRing is one of the most powerful rapid redundant ring technologies in the world. The recovery time of iRing is < 30ms with up to 250 units. It can reduce any unexpected malfunction caused by a network topology change. iRing technology supports a three Ring topology for network redundancy: iRing, Ring Linking and Dual Homing.



iRing interface

The following table describes the iRing interface page.

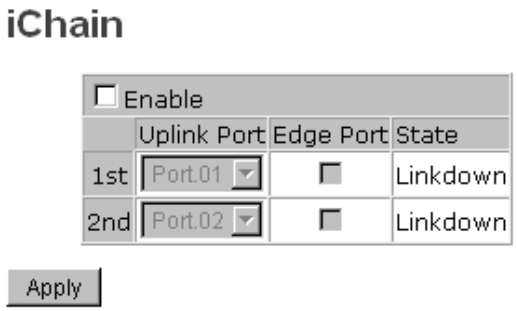
Label	Description
iRing	To enable iRing.
Ring Master	There should only be one Ring Master in a ring. However, if there are two or more switches which have Ring Master set to enable; the switch with the lowest MAC address will be the actual Ring Master and the others will become Backup Masters.
1st Ring Port	The primary port; when this switch is configured in iRing.
2nd Ring Port	The backup port; when this switch is configured in iRing.
Coupling Ring	Enables Coupling Ring. Coupling Ring can be used to divide a big ring into two smaller Rings to avoid affecting all switches when a network topology change has been made. It is a good application when connecting two Rings.
Coupling Port	Set a port as the coupling port to link to the Coupling Port of the switch in another ring. Coupling Ring needs four switches to construct an

	active and a backup link. The coupled four ports of four switches will be operated in active/backup mode.
Dual Homing	To enable Dual Homing. Select Dual Homing mode, Ring will be connected to normal switches through two RSTP links (i.e., backbone Switch). The two links will act in active/backup mode, and connect each Ring to the normal switches in RSTP mode.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

Note: It is not recommended to set one switch as a Ring Master and a Coupling Ring at the same time. This will burden the system.

5.1.7.2 iChain

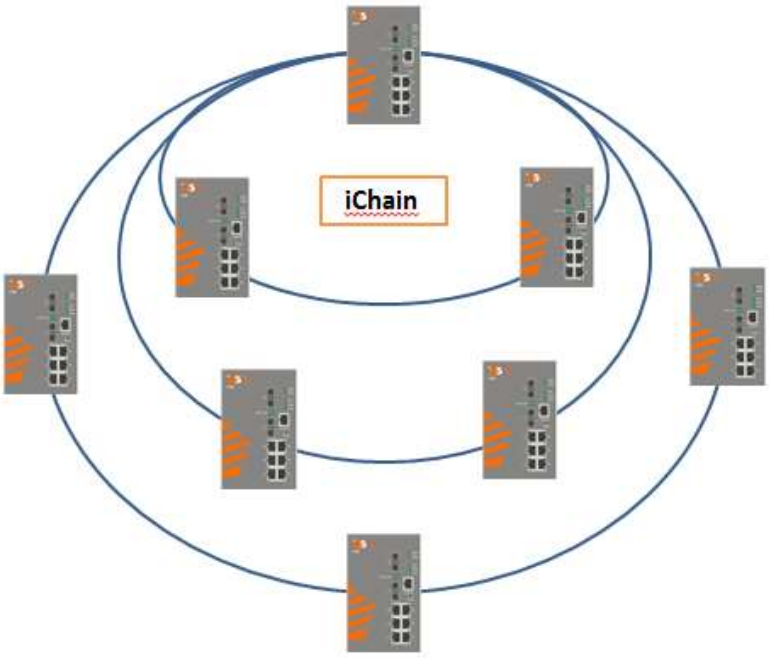
iChain can be enabled to provide network redundancy and maximize fault recovery speed by creating multiple redundant networks.



iChain Interface

The following table describes the labels for the iChain screen.

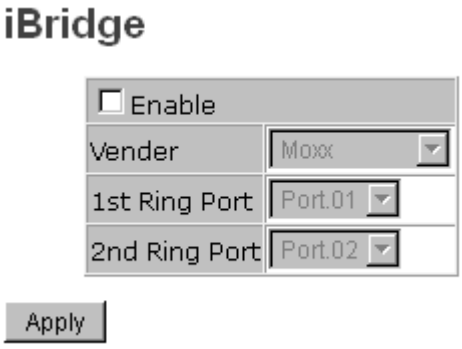
Label	Description
Enable	Enables the iChain function.
Uplink Port	Select the port (1 - 8) to be the Uplink Port.
Edge Port	Defines the port as an Edge Port. Only one Edge Port of the Edge Switch needs to be defined. Other switches beside them just need to have iChain enabled.
State	Status is Forwarding or Linkdown.



Typical iChain Application

5.1.7.3 iBridge

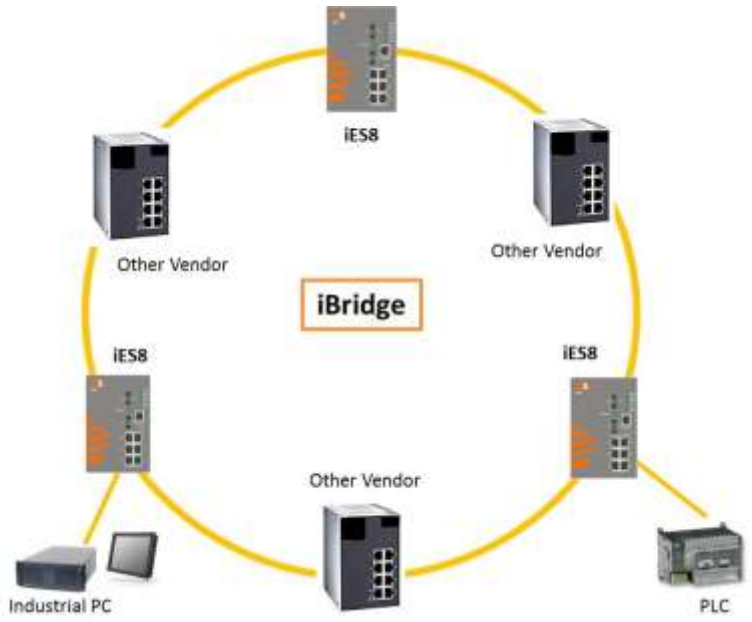
iBridge technology can be enabled allowing the addition of iS5Com switches into a network constructed by another vendor's proprietary ring technology. This allows the interoperability between managed switches.



iBridge Interface

The following table describes the labels for the iBridge screen.

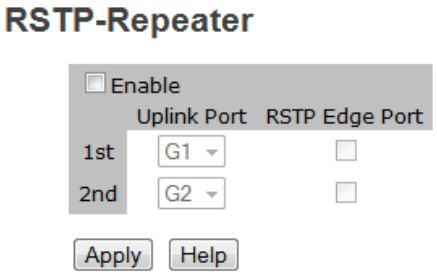
Label	Description
Enable	Enables the iBridge function
Vendor	Choose the vendors that you want to interoperate with.
1st Ring Port	Choose the port that will connect to the ring.
2nd Ring Port	Choose the port that will connect to the ring.



Typical iBridge Application

5.1.7.4 RSTP-Repeater

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

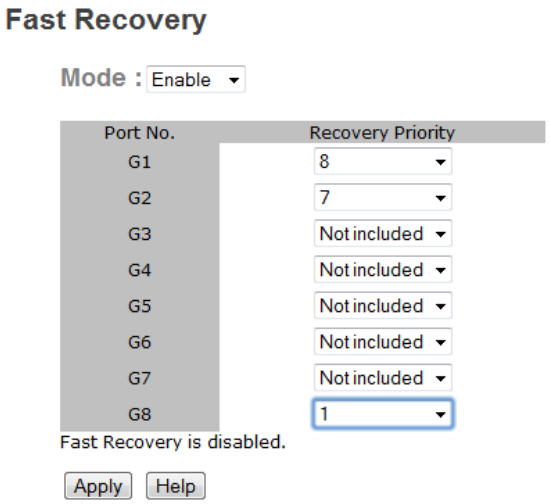


Label	Description
Enable	Check this box to enable RSTP-Repeater.
1stRing Port	Choosing the port which connect to the RSTP
2ndRing Port	Choosing the port which connect to the RSTP
Edge Port	Only the edge device (connected to RSTP device) needs to specify edge port. The user must specify the edge port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

5.1.7.5 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.

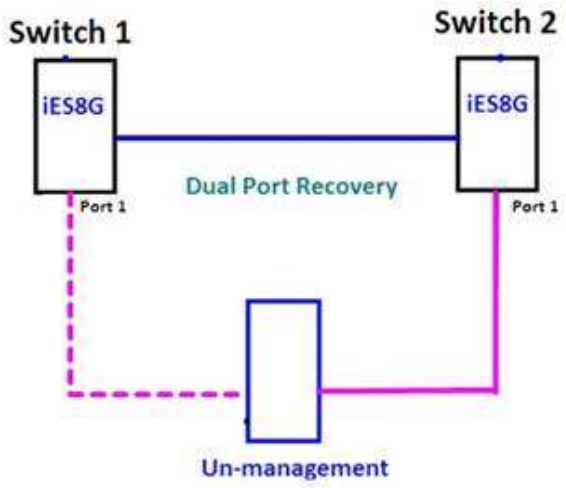
5.1.7.6 Dual Port Recovery

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.

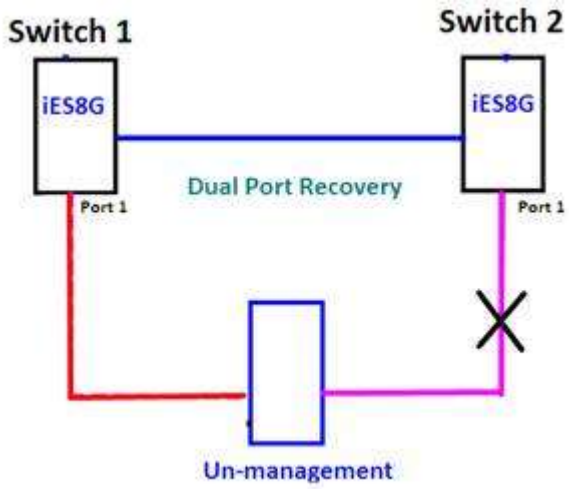
This protocols based on sending specific messages (BPDU format) from each port on both sides of unmanaged chain. The Dual Port Recovery feature can be executed with other redundancy protocols on same device.

Dual Port Recovery- Concept

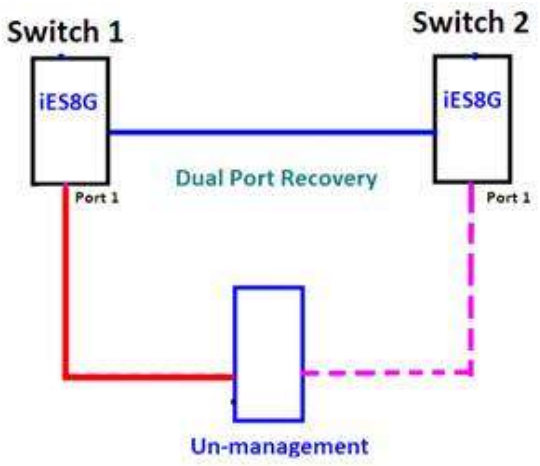
Dual Port Recovery allows connection to un-managed switch/ring of switches.



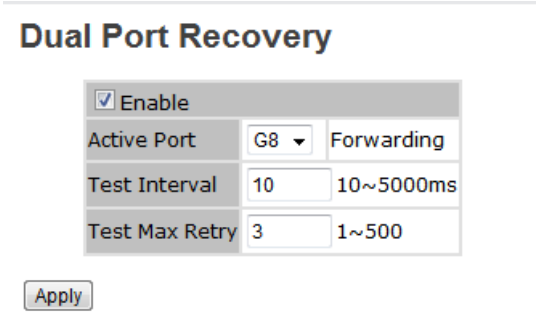
In Dual Port Recovery function if link of port in “Forwarding” state goes down, the “backup” port is changing its state to be forwarding, like in picture below. The disconnected port changes its status to “No Link”



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.

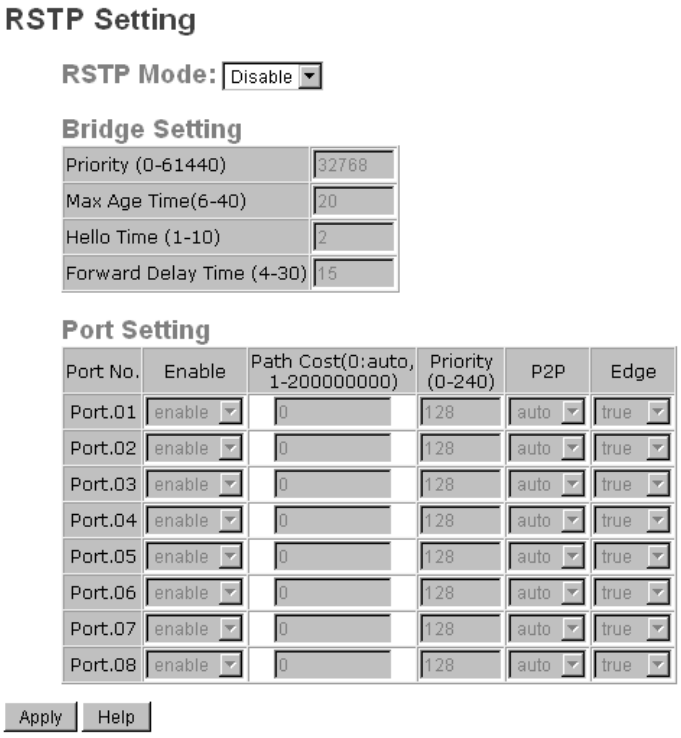
Recovery time is Test Max Retry x Test Interval + 10ms. Default Recovery time is 30ms<recovery time<40ms.

5.1.7.7 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

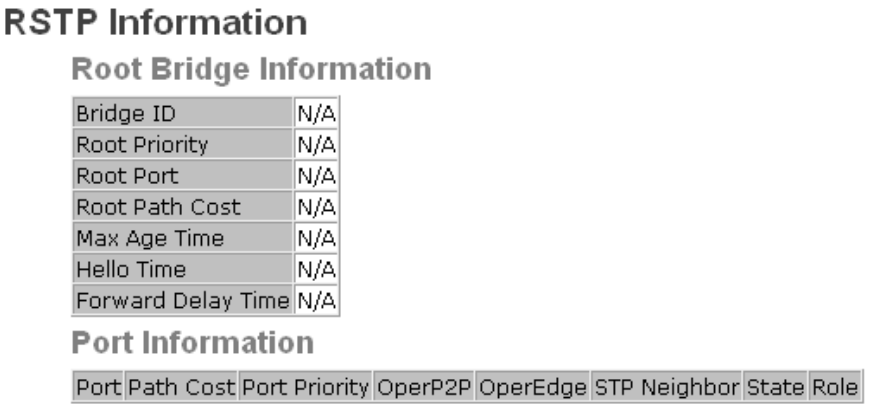
Label	Description
	Data Unit) packet to verify the current status of RSTP. Enter a value between 1 and 10.
Forwarding Delay Time (4-30)	The number of seconds a port has to wait before changing from learning/listening state to forwarding state. Enter a value between 4 and 30.
Path Cost (1-200000000)	The 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

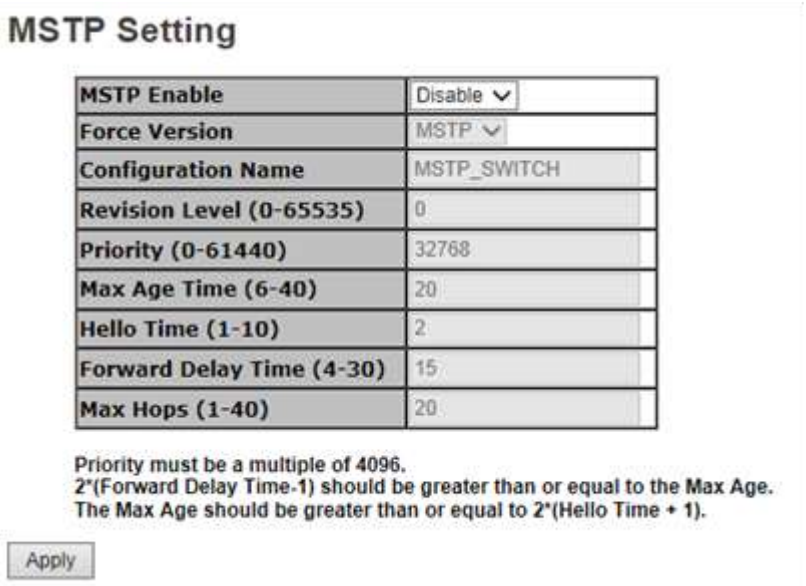
The following table describes the labels for the RSTP Information screen.

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.

5.1.7.8 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

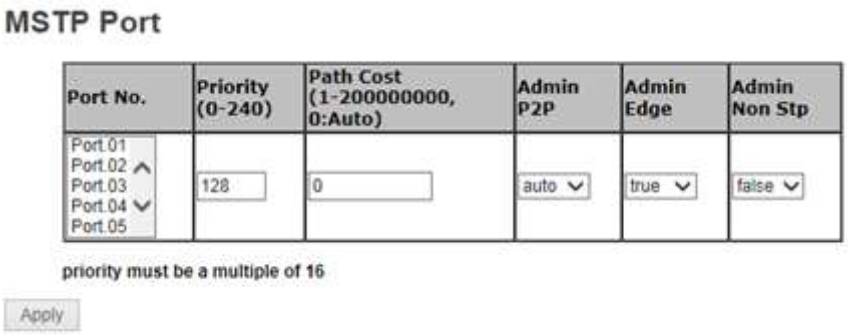


The following table describes the labels in this screen.

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

Label	Description
	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

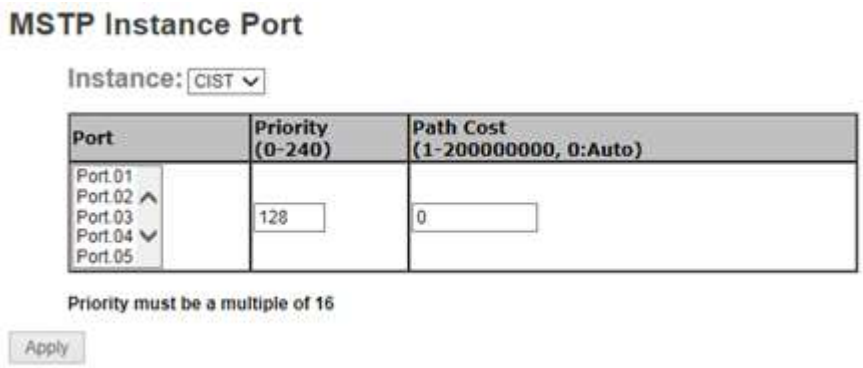


The following table describes the labels in this screen.

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.

Label	Description
Admin Edge	Label
Admin Non STP	Label
Apply	Click "**Apply**" to activate the configurations.

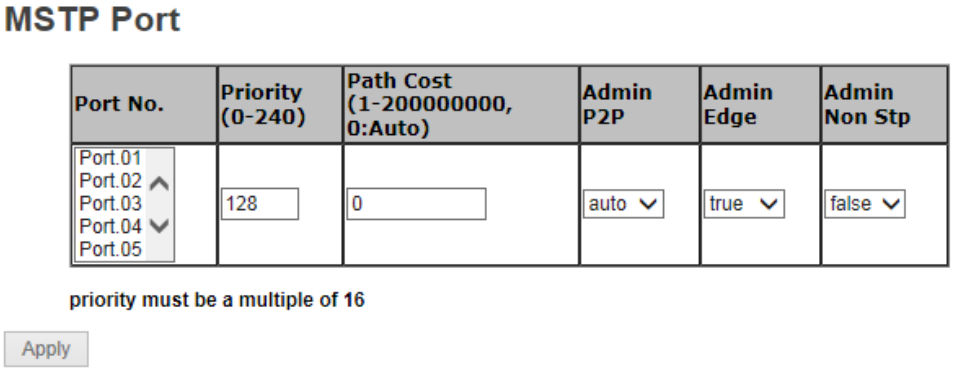
MSTP Instance



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

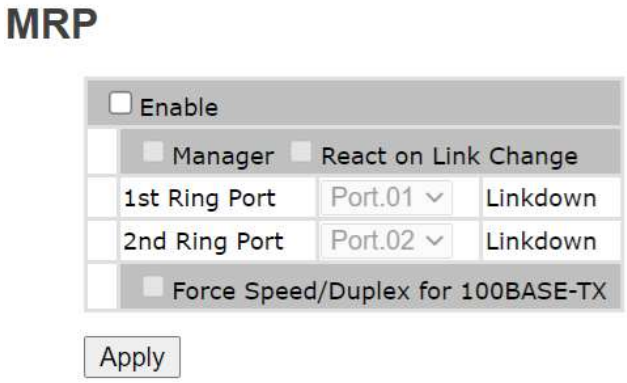


The following table describes the labels in this screen.

Label	Description

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.

5.1.7.9 MRP



Label	Description
Enable	Enables the MRP function.
Manager	Every MRP topology needs a MRP manager, and can only have one manager. If two or more switches are set to be Managers at the same time, the MRP topology will fail.
React on Link Change (Advanced mode)	Faster mode. Enabling this function will ensure MRP topology a more rapid converge. This function only can be set by the MRP manager switch.
1st Ring Port	Chooses the port that connects to the MRP ring.
2nd Ring Port	Chooses the port that connects to the MRP ring.
Force Speed / Duplex for 100 Base-TX	Add a checkmark to activate Force Speed / Duplex for 100 Base-TX.

5.1.8 VLAN

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, and allows the network traffic to be isolated. Only the members of the same VLAN will receive the 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.

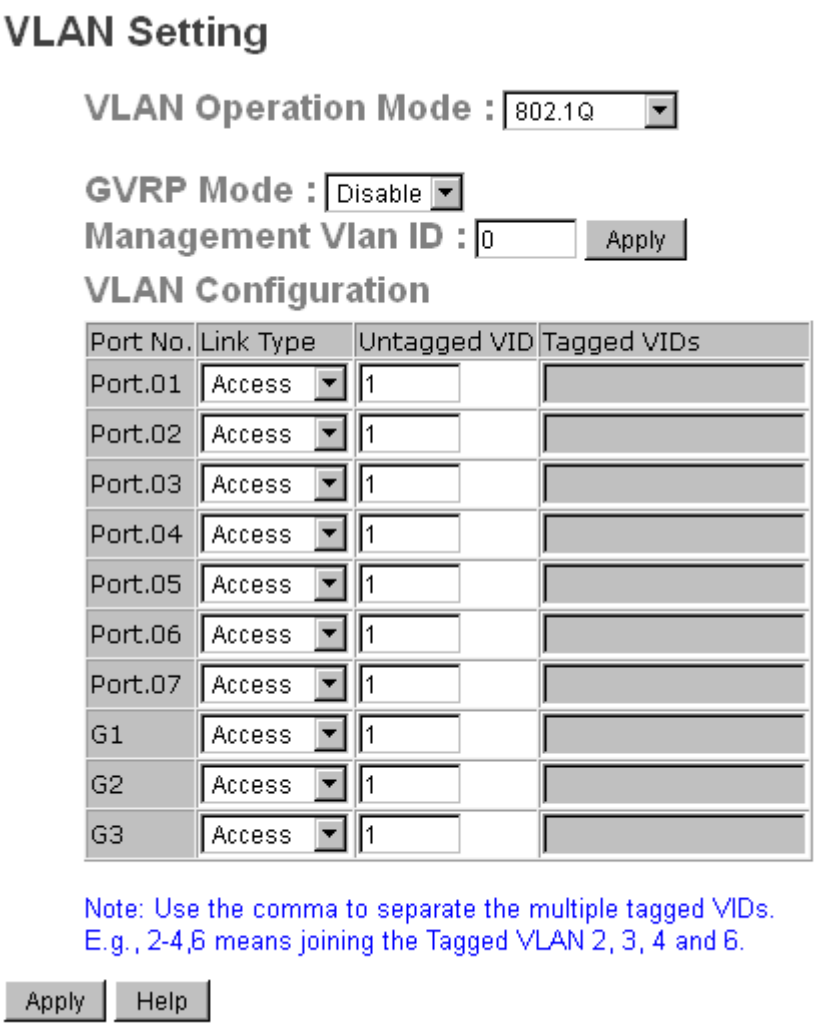
The iES10G(F) switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration for VLAN operation mode is "**802.1Q**".

5.1.8.1 VLAN Setting

Tagged-based VLAN is an IEEE 802.1Q specification standard. It allows the creation of VLAN's across devices from different switch venders. IEEE 802.1Q VLAN uses a technique to insert a "tag" into the Ethernet frames. This tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

Tag-based VLAN's can be created the GVRP protocol can either be enabled or disabled. There are 256 VLAN groups available. Enabling 802.1Q VLAN, and all ports on the switch belong to the default VLAN, VID is 1. The default VLAN cannot be deleted.

GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled; a GVRP request can be sent by 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

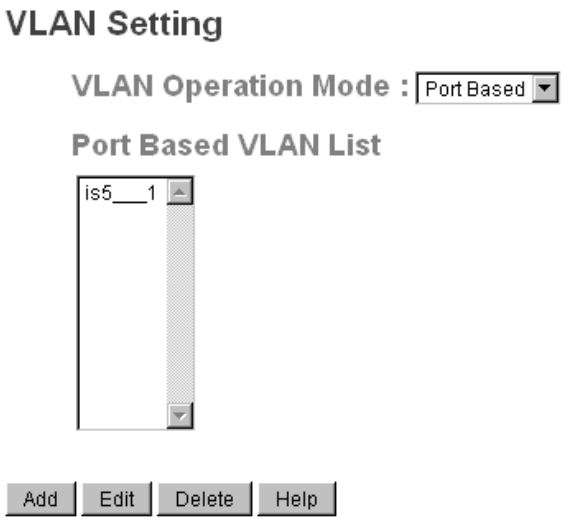
The following table describes the VLAN Configuration – 802.1Q interface page.

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 secure VLAN to manage the switch. Only the devices in the management VLAN can access the switch.
Link type	There are 3 link types: **Access Link:** single switch only, allows the grouping of ports by setting the same VID. **Trunk Link:** extended application of **Access Link**, allows the grouping of 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 the insertion of one

	more VLAN tag in an original VLAN frame.
Untagged VID	Set the port default VLAN ID for untagged devices that connect to the port. The range is 1 to 4094.
Tagged VIDs	Set the tagged VIDs to carry different VLAN frames to other switches.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.8.2 VLAN Setting – Port Based

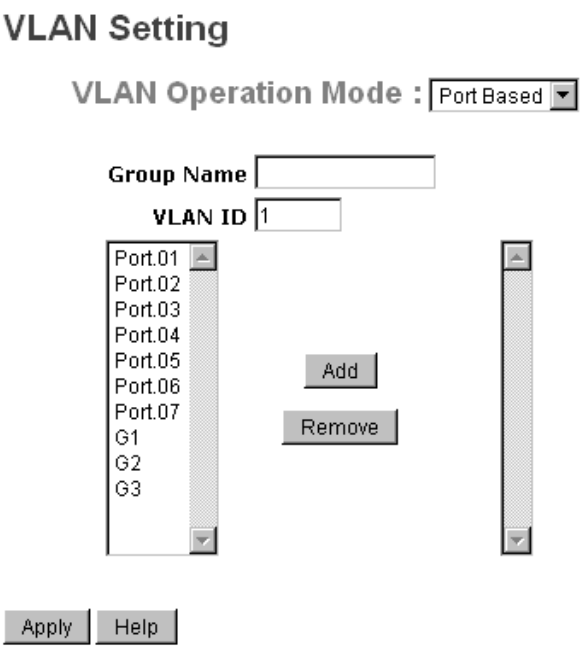
Traffic is forwarded to the member ports of the same VLAN group. VLAN port based startup, set in the same group of the port, can be a normal transmission packet without restricting the types of packets.



VLAN Configuration – Port Base interface-1

The following table describes the VLAN Configuration – Port Base interface-1 page.

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



VLAN Configuration – Port Base interface-2

The following table describes the VLAN Configuration Port Base interface-2 page.

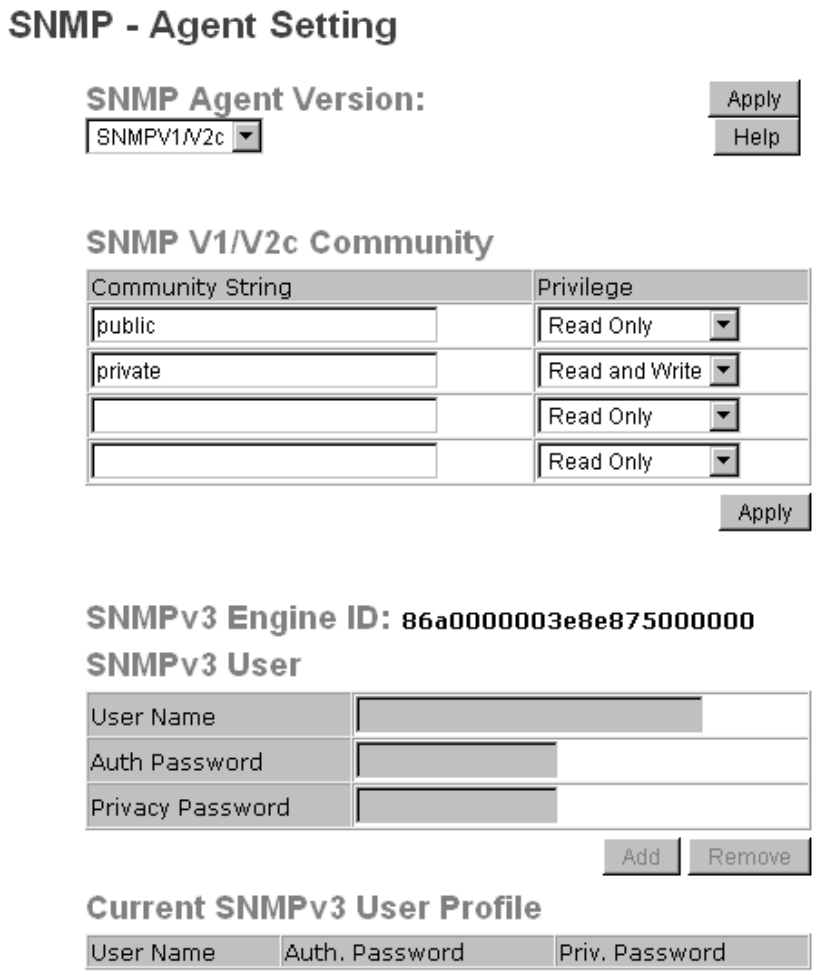
Label	Description
Group Name	VLAN name.
VLAN ID	Specify the VLAN ID.
Add	Select which port to join the VLAN group.
Remove	Remove port of the VLAN group.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.9 SNMP

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

5.1.9.1 SNMP – Agent Setting

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



SNMP Agent Setting interface

The following table describes the SNMP Agent Setting interface page.

Label	Description
SNMP agent Version	Three SNMP versions are supported such as SNMP V1/SNMP V2c, and SNMP V3. SNMP V1/SNMP V2c agent use a community string match for authentication, which means SNMP server's access objects with read-only or read/write permissions with the community default string public/private. SNMP V3 requires an authentication level of MD5 or DES to encrypt data to enhance data security.
SNMP V1/V2c Community	SNMP Community should be set for SNMP V1/V2c. Four sets of "Community String/Privilege" are supported. Each Community String is a maximum of 32 characters. Keep empty to remove this Community string.
SNMPv3User	If SNMP V3 agent is selected, the SNMPv3 profiled should be set for authentication. The Username is necessary. The Auth. Password is

	encrypted by MD5 and the Privacy Password which is encrypted by DES. There are maximum 8 sets of SNMPv3 User's and maximum 16 characters in username, and password. When SNMP V3 agent is selected, it is possible to: 1. Input SNMPv3 username only. 2. Input SNMPv3 username and Auth Password. 3. Input SNMPv3 username, Auth Password and Privacy Password, which can be different with Auth Password. To remove a current user profile: 1. Input SNMPv3 user name to be removed. 2. Click "**Remove**" button
Current SNMPv3 User Profile	Show all SNMPv3 user profiles.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.9.2 SNMP – Trap Setting

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

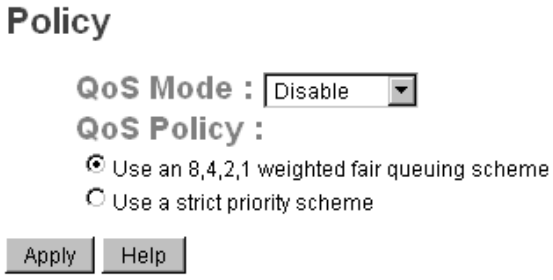
SNMP Trap Setting interface

The following table describes the SNMP Trap Setting interface page.

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.

5.1.10 Traffic Prioritization

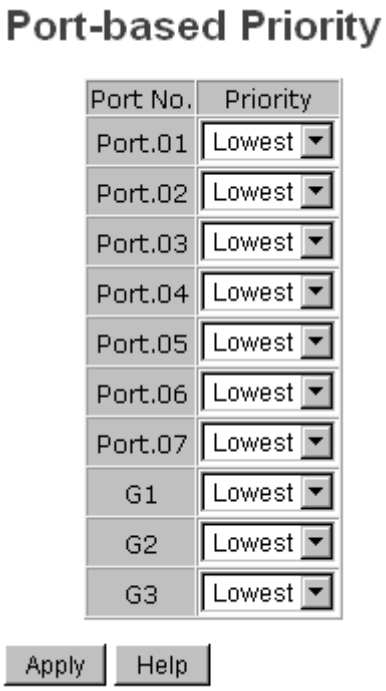
Traffic Prioritization includes 3 modes: port base, 802.1p/COS, and TOS/DSCP. With the traffic prioritization function, traffic can be classified into four classes for differential network applications. The iES10G(F) supports 4 priority queues.



Policy Setting interface

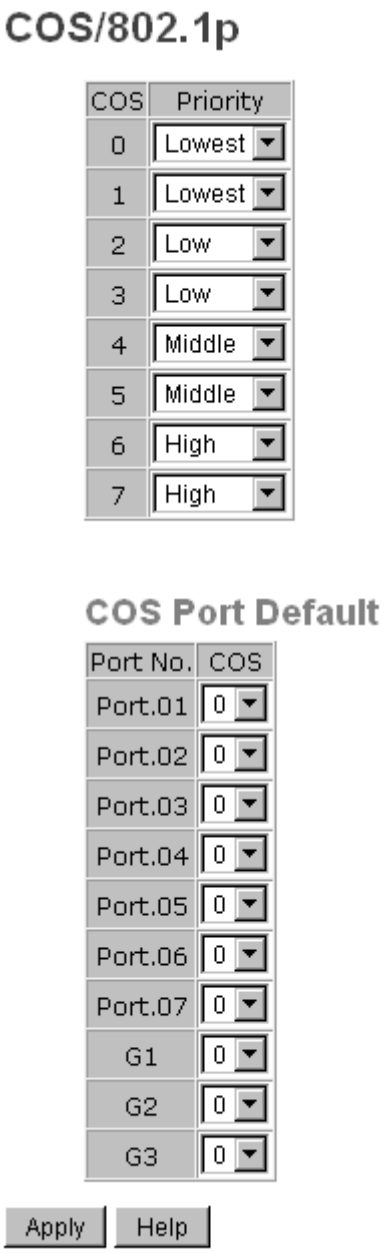
The following table describes the Traffic Prioritization Policy interface page.

Label	Description
QoS Mode	■ **Port-base:** the output priority is determined by ingress port. ■ **COS only:** the output priority is determined by COS only. ■ **TOS only:** the output priority is determined by TOS only. ■ **COS first:** the output priority is determined first by COS and then by TOS. ■ **TOS first:** the output priority is determined first by TOS and then by COS.
QoS policy	■ **Using the 8,4,2,1 weight fair queue scheme:** the output queues will follow 8:4:2:1 ratio to transmit packets from the highest to lowest queue. For example: 8 high queue packets, 4 middle queue packets, 2 low queue packets, and the one lowest queue packet are transmitted in one turn. ■ **Use the strict priority scheme:** the packets in higher queue will always be transmitted first until a higher queue is empty.
Help	Show help file.
Apply	Click "**Apply**" to activate the configurations.



Port-based Priority interface

Label	Description
Port base 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.



COS/802.1p interface

Label	Description
COS/802.1p	COS (Class Of Service) is well known as 802.1p. It describes that the output priority of a packet is determined by the user priority field in 802.1Q VLAN tag. The priority value is supported 0-7. COS value map to 4 priority queues: High, Middle, Low, and Lowest.
COS Port Default	When an ingress packet does not have a 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.

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

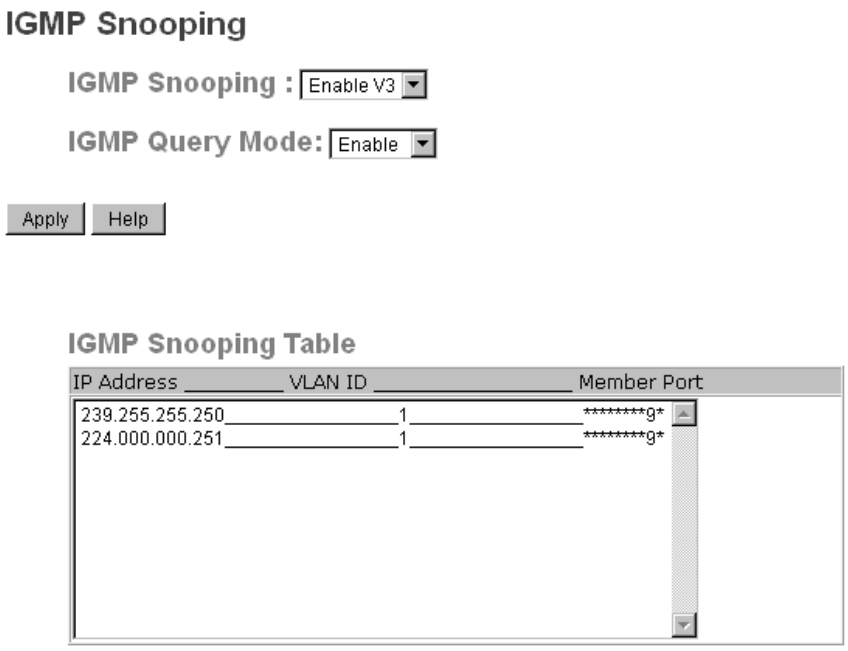
TOS/DSCP interface

Label	Description
TOS/DSCP	TOS (Type of Service) is a field in the 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 maps to 4 priority queues: High, Middle, Low, and Lowest.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.11 Multicast

5.1.11.1 IGMP Snooping

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



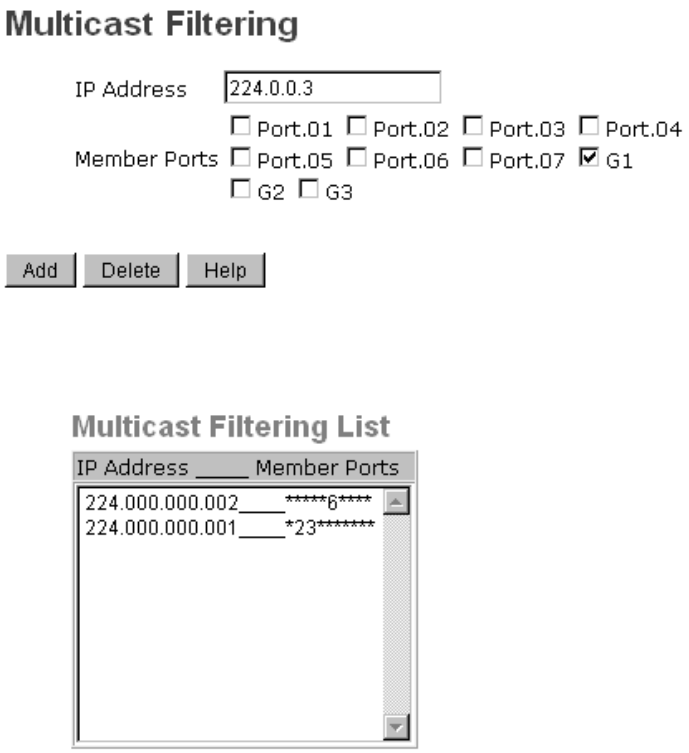
IGMP Snooping interface

The following table describes the IGMP Snooping interface page.

Label	Description
IGMP Snooping	Enable (V2 or V3) or Disable IGMP snooping.
IGMP Query Mode	Switch will receive IGMP queries or not. There should only be one switch receiving IGMP queries in an IGMP application. The "Auto" mode means that the switch receiving the IGMP query is the one with lower IP address.
IGMP Snooping Table	Show current IP multicast list
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.11.2 Multicast Filter

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



Multicast Filtering interface

The following table describes the Multicast Filtering interface page.

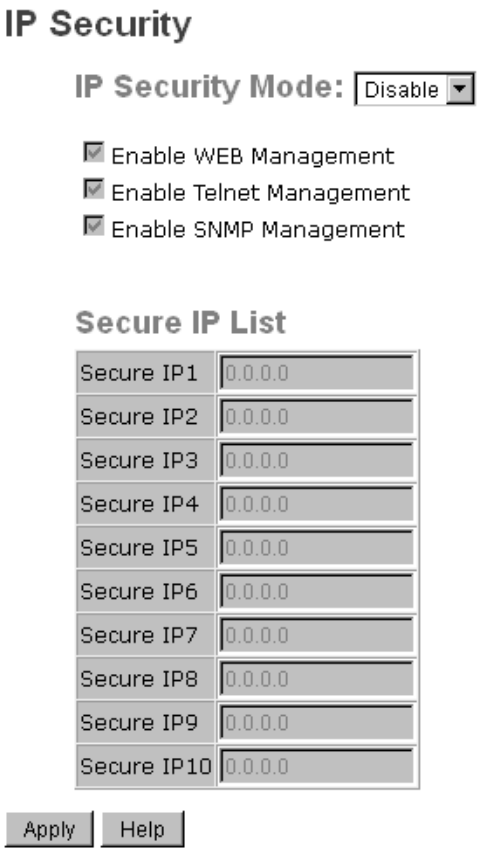
Label	Description
IP Address	Assign a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255.
Member Ports	Tick the check box beside the port number to include them as the member ports in the specific multicast group IP address.
Add	Show current IP multicast list.
Delete	Delete an entry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

5.1.12 Security

There are 5 useful functions that can enhance the security of a switch: IP Security, Port Security, MAC Blacklist, and MAC address Aging 802.1 x protocols.

5.1.12.1 IP Security

IP security can be enabled or disabled via remote management from the WEB, Telnet or SNMP. Additionally, IP security can be restricted via remote management to some specific IP addresses. Only these secure IP addresses can manage this switch remotely.



IP Security interface

The following table describes the IP Security interface page.

Label	Description
IP security MODE	Enable/Disable the IP security function.
Enable WEB Management	Check the blank to enable WEB Management.
Enable Telnet Management	Check the blank to enable Telnet Management.
Enable SNMP Management	Check the blank to enable SNMP Management.

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

5.1.12.2 Port Security

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

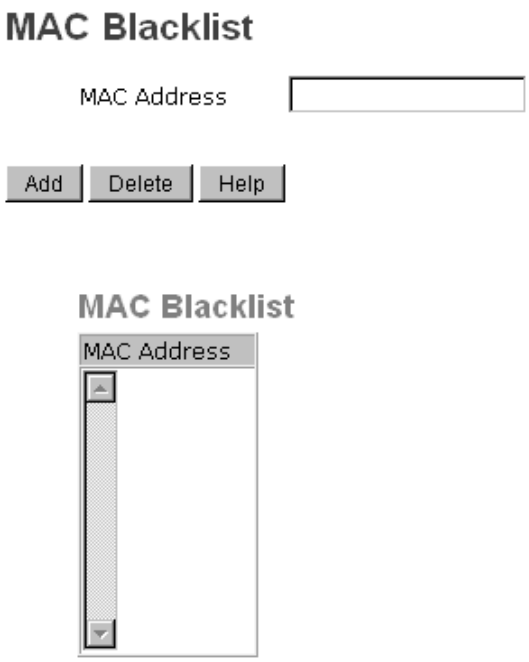
Port Security interface

The following table describes the Port Security interface page.

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

5.1.12.3 MAC Blacklist

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



MAC Blacklist interface

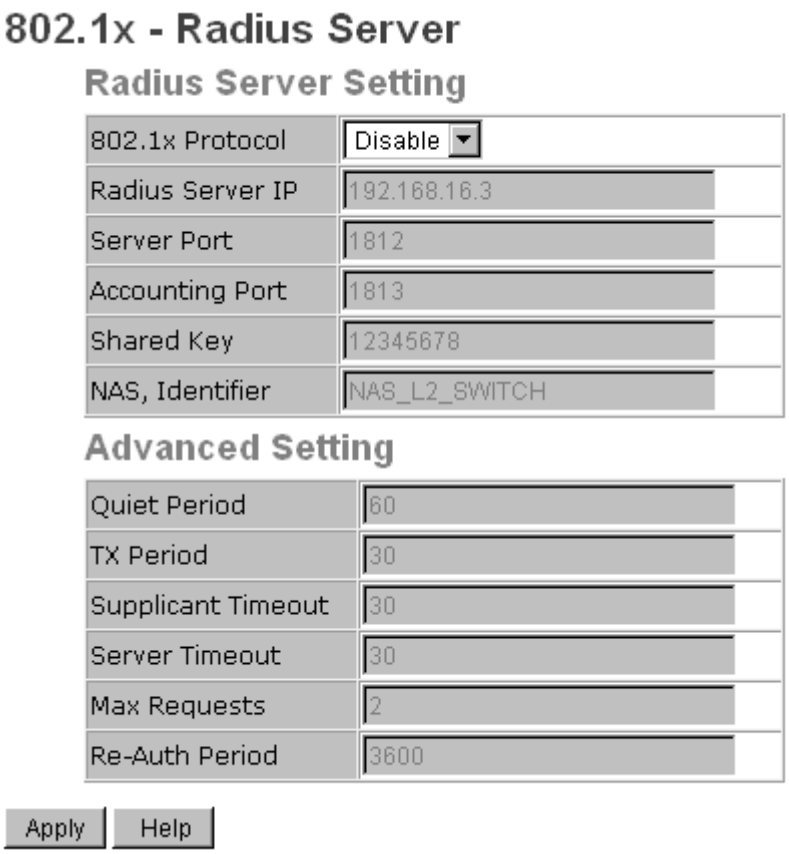
The following table describes the MAC Blacklist interface page.

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

5.1.12.4 802.1x

802.1x - Radius Server

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



802.1x Radius Server interface

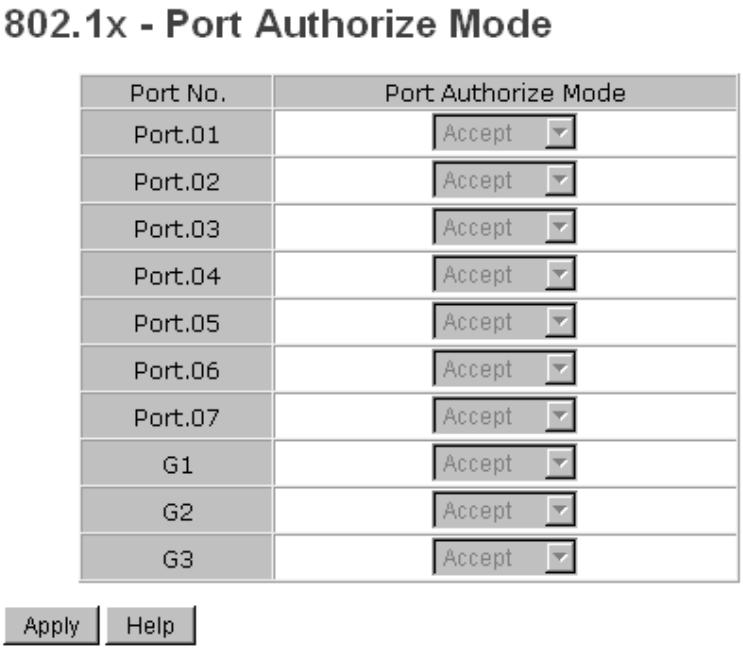
The following table describes the 802.1x Radius Server interface page.

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 key shared between this switch and authentication server.
NAS, Identifier	A string used to identify this switch.
Advanced Setting	
Quiet Period	Set the time interval between authentication failure and the start of a new authentication attempt.
Tx Period	Set the time that the switch can wait for response to an EAP request/identity frame from the client before resending the request.
Supplicant Timeout	Set the period of time the switch waits for a supplicant response to an EAP request.

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

802.1x - Port Authorized Mode

Set the 802.1x authorized mode of each port.



802.1x Port Authorize interface

The following table describes the 802.1x Port Authorize interface page.

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

802.1x - Port Authorized State

Show 802.1x port authorized state.

802.1x - Port Authorize State

Port No.	Port Authorize State
Port.01	Accept
Port.02	Accept
Port.03	Accept
Port.04	Accept
Port.05	Accept
Port.06	Accept
Port.07	Accept
G1	Accept
G2	Accept
G3	Accept

802.1x Port Authorize State interface

5.1.13 Warning

The Warning function is very important for managing the switch. It can be managed by SYSLOG, E-MAIL, and Fault Relay. It also helps monitor the switch status on remote sites. When events occur, a warning message will be send to the appointed server, E-MAIL, or relay fault on a switch panel.

5.1.13.1 Fault Alarm

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

Fault Alarm

Power Failure

☐ PWR 1 ☐ PWR 2

Port Link Down/Broken

☐ Port.01 ☐ Port.02
☐ Port.03 ☐ Port.04
☐ Port.05 ☐ Port.06
☐ Port.07 ☐ G1
☐ G2 ☐ G3

Apply Help

Fault Alarm interface

The following table describes the Fault Alarm interface page.

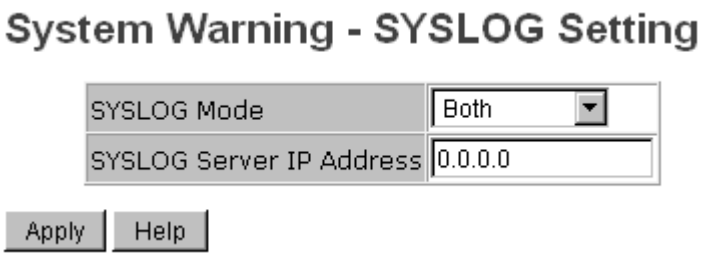
Label	Description
Power Failure	Check the box of PWR 1 or PWR 2 to monitor.
Port Link Down/Broken	Check the box of port 1 to port 10 to monitor.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.13.2 System Alarm

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

System Warning – SYSLOG Setting

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



System Warning – SYSLOG Setting interface

The following table describes the SYSLOG Setting interface page.

Label	Description
SYSLOG Mode	■ **Disable:** disable SYSLOG. ■ **Client Only:** log to local system. ■ **Server Only:** log to a remote SYSLOG server. ■ **Both:** log to both, local and remote server.
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 transmission across the Internet. Please refer to RFC 821 - Simple Mail Transfer Protocol.

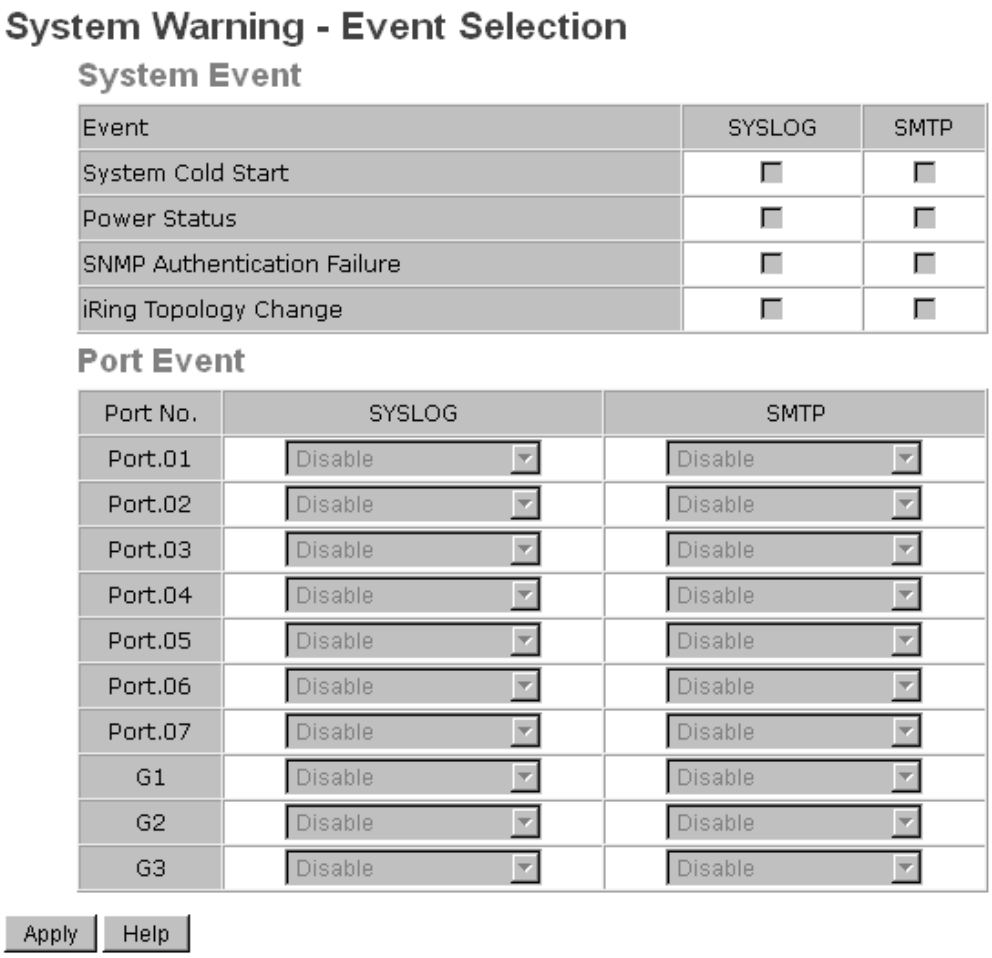
System Warning – SMTP Setting interface

The following table describes the System Warning – SMTP Setting interface page.

Label	Description
E-mail Alarm	Enable/Disable transmission system warning events by e-mail.
SMTP Server Address	The SMTP server IP address.
Sender E-mail Address	Email address that the mail will be sent from.
Mail Subject	The Subject of the mail.
Authentication	■ **Username:** the authentication username. ■ **Password:** the authentication password. ■ **Confirm Password:** re-enter password.
Recipient E-mail Address	The recipient's E-mail address. It supports up to 6 recipients.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

System Warning – Event Selection

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



System Warning – Event Selection interface

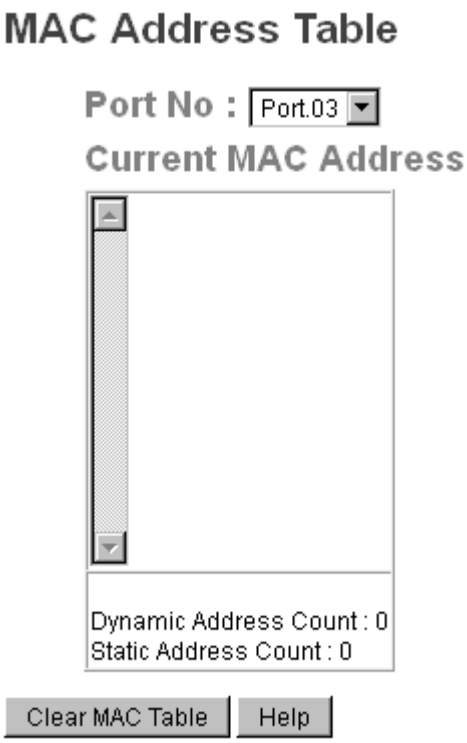
The following table describes the System Warning – Event Selection interface page.

Label	Description
System Event	
System Cold Start	Alert when system restarts.
Power Status	Alert when power is up or down.
SNMP Authentication Failure	Alert when SNMP authentication fails.
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.

5.1.14 Monitor and Diagnostics

5.1.14.1 MAC Address Table

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



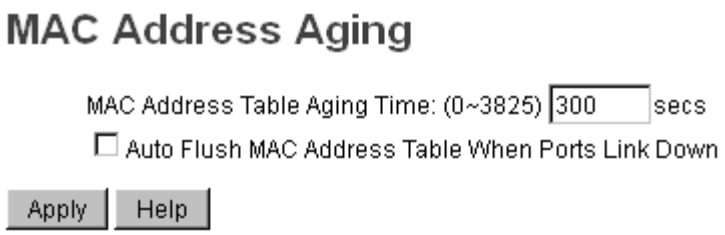
MAC Address Table interface

The following table describes the MAC Address Table interface page.

Label	Description
Port No.:	Show all MAC addresses mapping to a selected port.
Clear MAC Table	Clear all MAC addresses in a table.
Help	Show help file.

5.1.14.2 MAC Address Aging

The MAC Address aging time can be set between 0 and 3825 seconds. When the time expires, the unused MAC address will be cleared from MAC table. The iES10G(F) also supports “Auto Flush MAC Address Table When Ports Link Down”.



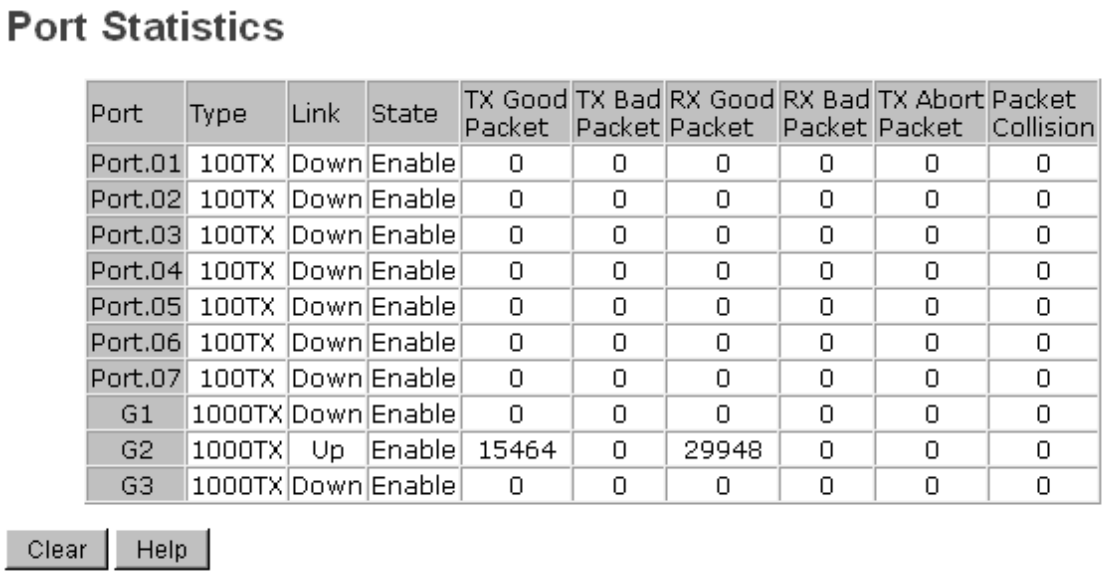
MAC Address Aging interface

The following table describes the MAC Address Aging interface page.

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

5.1.14.3 Port Statistics

Port statistics show several statistics counters for all ports



Port Statistics

Port	Type	Link	State	TX Good Packet	TX Bad Packet	RX Good Packet	RX Bad Packet	TX Abort Packet	Packet Collision
Port.01	100TX	Down	Enable	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0
Port.07	100TX	Down	Enable	0	0	0	0	0	0
G1	1000TX	Down	Enable	0	0	0	0	0	0
G2	1000TX	Up	Enable	15464	0	29948	0	0	0
G3	1000TX	Down	Enable	0	0	0	0	0	0

Clear Help

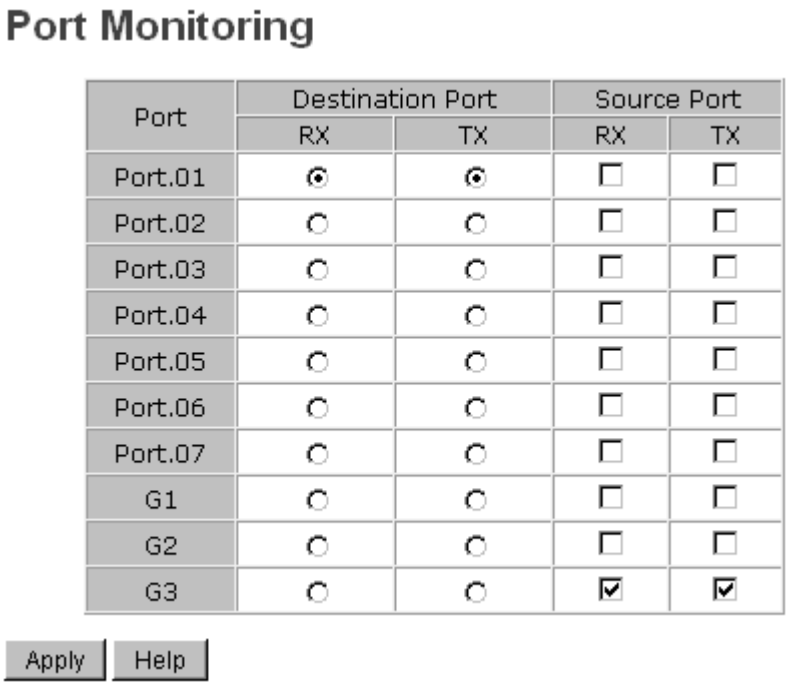
Port Statistics interface

The following table describes the Port Statistics interface page.

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

5.1.14.4 Port Monitoring

The Port Monitoring function supports TX (egress) only, RX (ingress) only, and both TX/RX monitoring. TX monitoring sends any data that egresses out of the Source Port to another port for monitoring. Check TX Source Ports to a selected TX destination port. RX monitoring sends any data that ingress in to the Source Port to another port for monitoring. Check RX Source Ports out to a selected RX destination port. It also sends the frame where it normally would have gone. Note: keep all source ports unchecked to disable Port Monitoring.



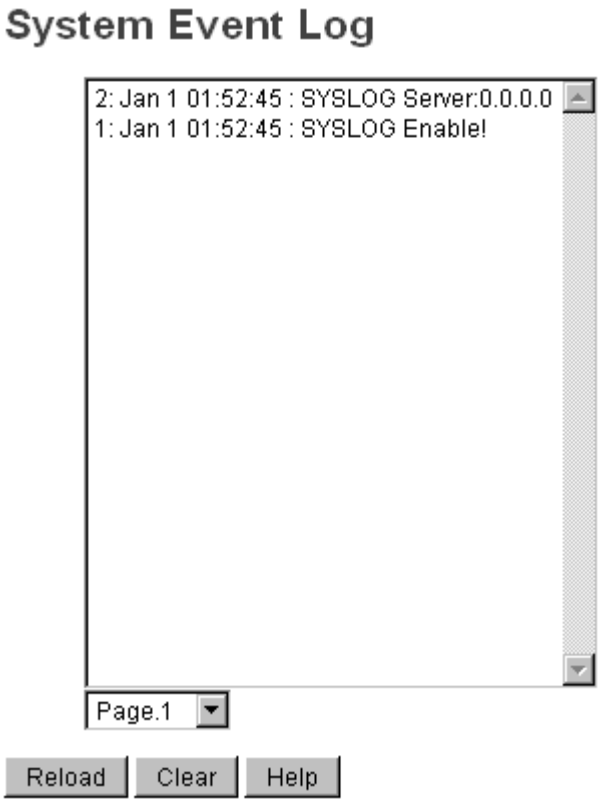
Port monitoring interface

The following table describes the Port Monitoring interface page.

Label	Description
Destination Port	The port will receive a copied frame from the source port for monitoring purpose.
Source Port	The port will be monitored. Check the TX or RX to be monitored.
TX	The frames leave the switch port and proceed somewhere outside of the network.
RX	The frames originate from outside the network and are received by the switch port within the network.
Apply	Click "**Apply**" to activate the configurations.
Clear	Clear all marked blank.(disable the function)
Help	Show help file.

5.1.14.5 System Event Log

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



System Event Log interface

The following table describes the System Event Log interface page.

Label	Description
Page	Select LOG page.
Reload	Gets the newest event logs and refreshes the page.
Clear	Clear log.
Help	Show help file.

5.1.15 Save Configuration

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

System Configuration interface

The following table describes the System Configuration interface page.

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

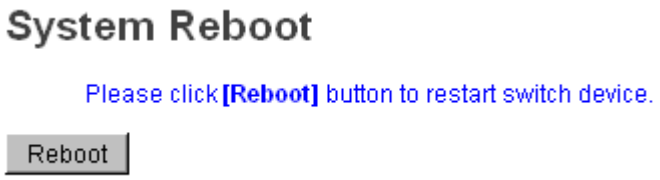
5.1.16 Factory Default

Factory Default interface

Reset switch to default configuration. Click Reset to reset all configurations to the default value.

Select "**Keep current IP address setting**" and "**Keep current username & password**" to keep current IP address, username, and password.

5.1.17 System Reboot



System Reboot interface

Command Line Interface Management (CLI)

6.1 About CLI Management

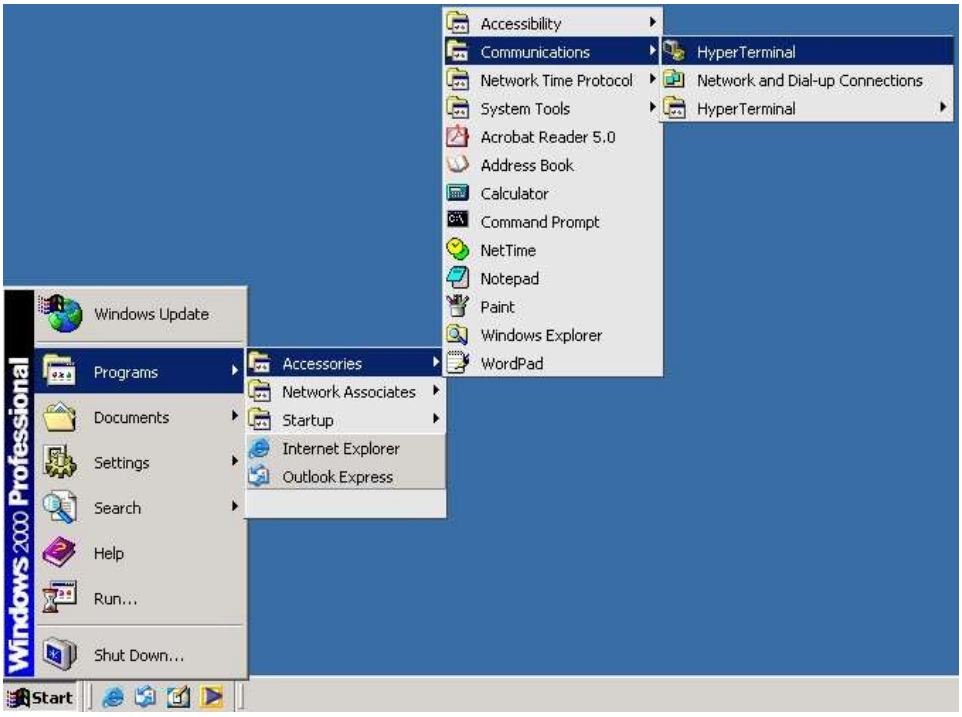
Besides WEB-based management, the iES10G(F) also supports CLI management. The console port or telnet can be used to configure the switch by the CLI.

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

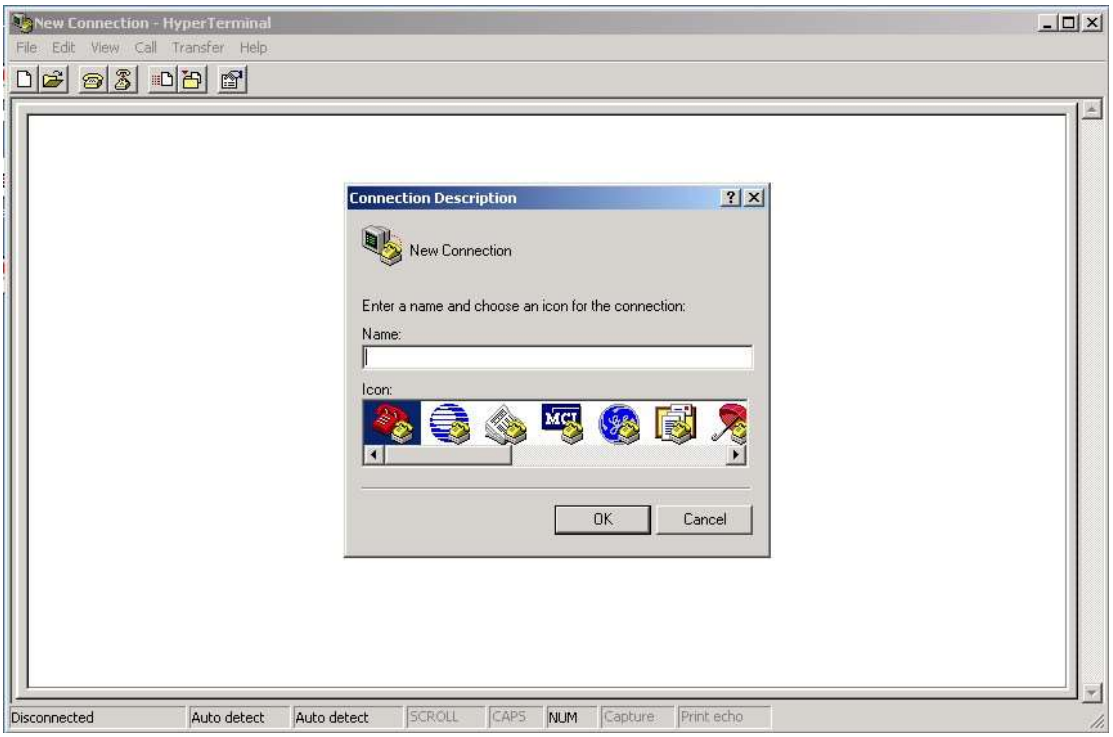
Use the RJ45 to DB9-F cable provided to connect the Switches RS-232 Console port to a PC's COM port.

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

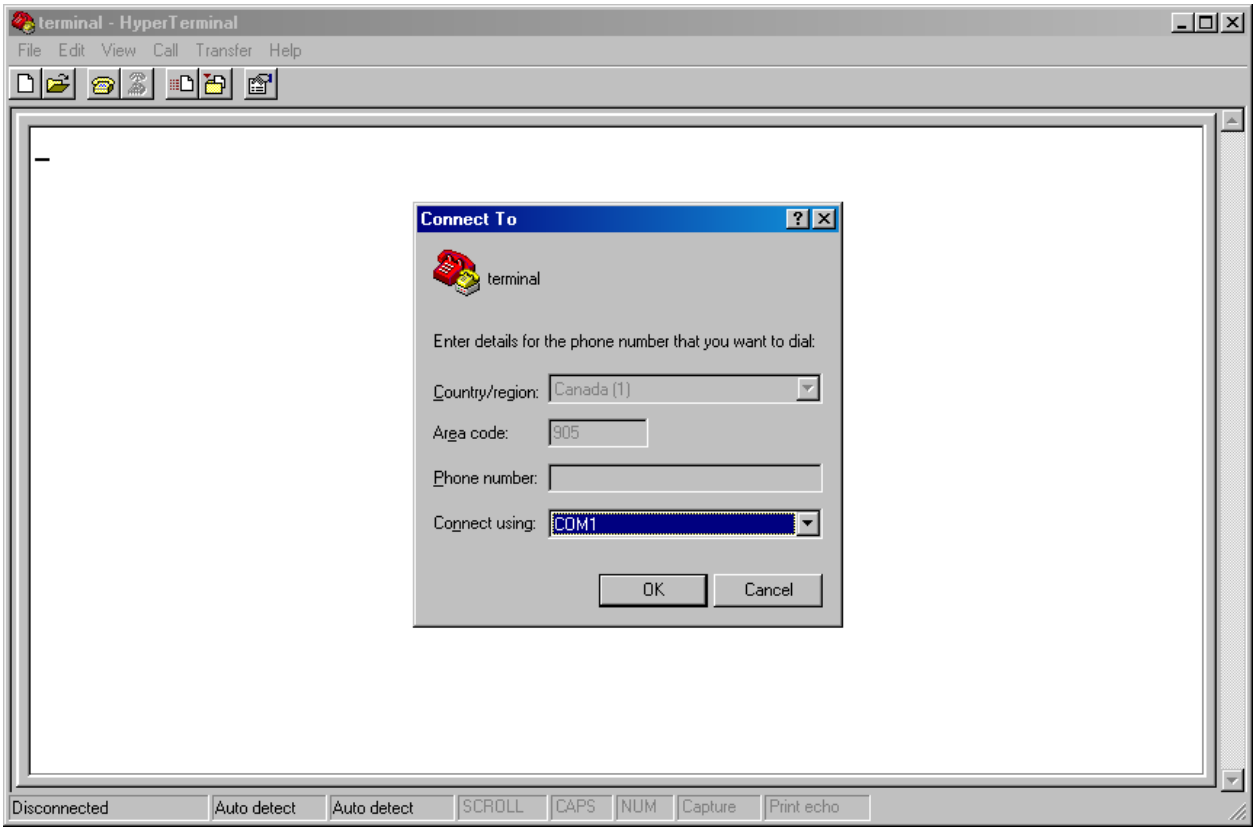
Step 1) From the Windows desktop, click on Start -> Programs -> Accessories -> Communications -> Hyper Terminal.



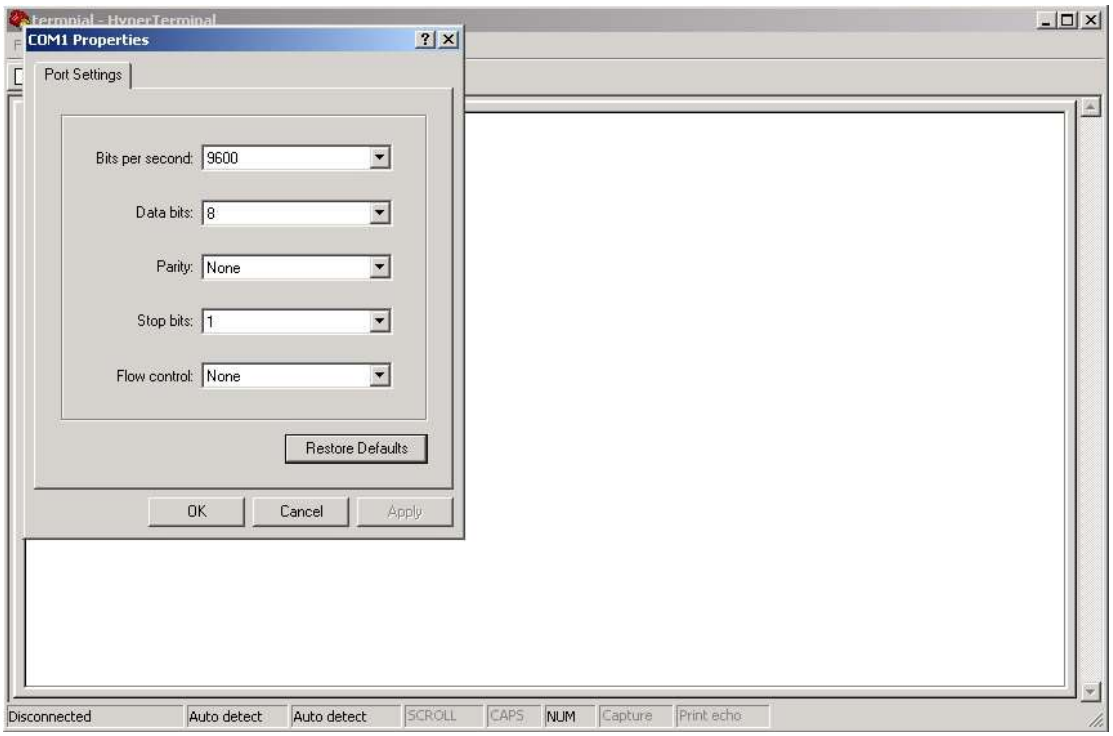
Step 2) Enter a name for the new connection.



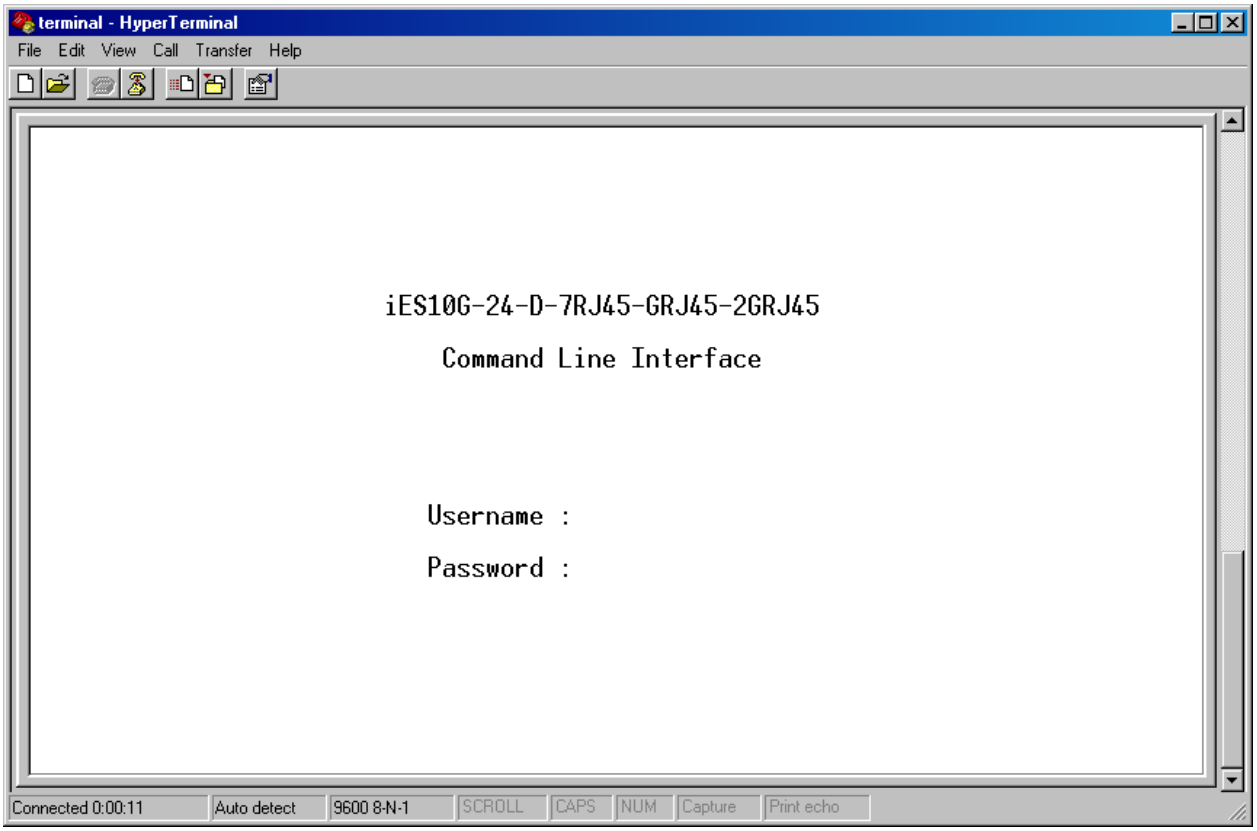
Step 3) Select appropriate COM port number



Step 4) Set the COM port properties to the following: 9600 Bits per second, 8 Data bits, No Parity, 1 Stop bit and no Flow control.



Step 5) The Console login screen will appear. Enter the Username and Password (same as the password for the Web Browser), then press "**Enter**".



CLI Management by Telnet

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

The default values are as below:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

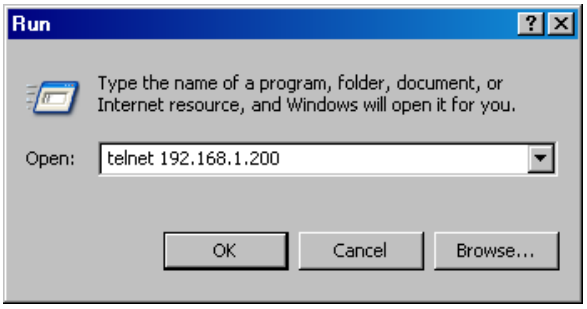
Default Gateway: **192.168.10.254**

User Name: **admin**

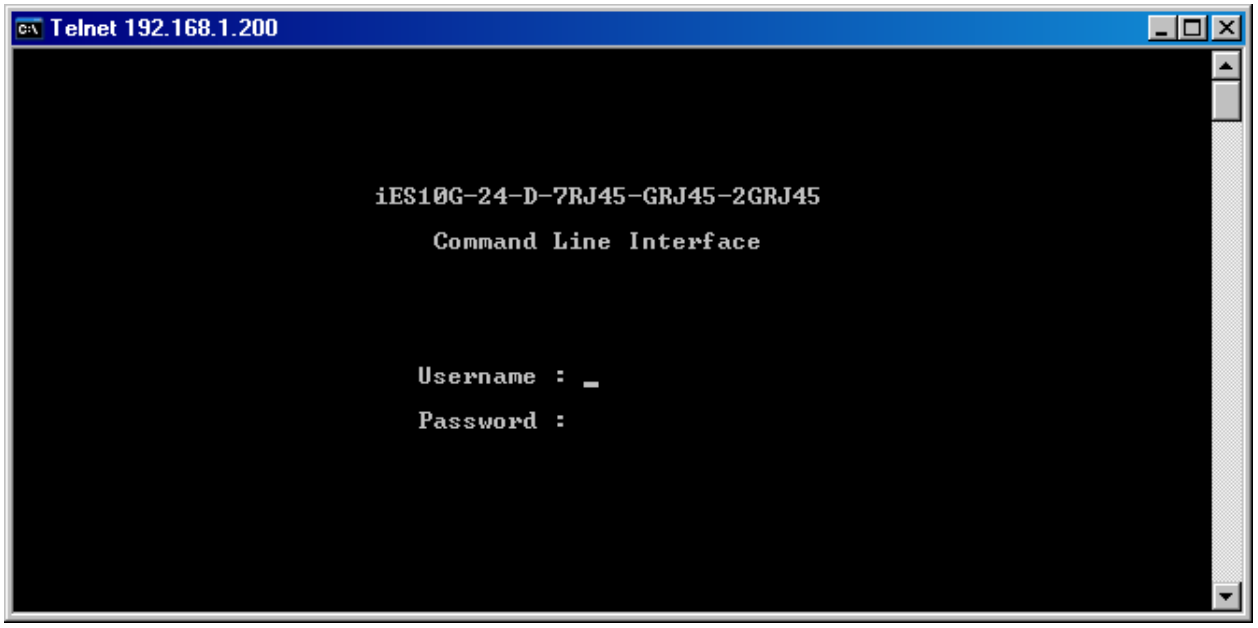
Password: **admin**

Follow the steps below to access the console via Telnet.

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



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



Commands Level

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

Symbols for 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

iES10G(F) Commands	Level	Description	Example
show config	E	Show switch configuration	switch>show config
show terminal	P	Show console information	switch#show terminal
write memory	P	Save your configuration into permanent memory (flash rom)	switch#write memory
system name [System Name]	G	Configure system name	switch(config)#system name xxx
system location [System Location]	G	Set switch system location string	switch(config)#system location xxx
system description [System Description]	G	Set switch system description string	switch(config)#system description xxx
system contact [System Contact]	G	Set switch system contact window string	switch(config)#system contact xxx
show system-info	E	Show system information	switch>show system-info
ip address [Ip-address] [Subnet-mask] [Gateway]	G	Configure the IP address of switch	switch(config)#ip address 192.168.1.1 255.255.255.0 192.168.1.254
ip dhcp	G	Enable DHCP client function of switch	switch(config)#ip dhcp
show ip	P	Show IP information of switch	switch#show ip
no ip dhcp	G	Disable DHCP client function of switch	switch(config)#no ip dhcp
reload	G	Halt and perform a cold restart	switch(config)#reload
default	G	Restore to default	Switch(config)#default
admin username [Username]	G	Changes a login username. (maximum 10 characters)	switch(config)#admin username xxxxxx
admin password [Password]	G	Specifies a password (maximum 10 characters)	switch(config)#admin password xxxxxx
show admin	P	Show administrator information	switch#show admin
dhcpserver enable	G	Enable DHCP Server	switch(config)#dhcpserver enable

dhcpserver lowip [Low IP]	G	Configure low IP address for IP pool	switch(config)# dhcpserver lowip 192.168.1.1
dhcpserver highip [High IP]	G	Configure high IP address for IP pool	switch(config)# dhcpserver highip 192.168.1.50
dhcpserver subnetmask [Subnet mask]	G	Configure subnet mask for DHCP clients	switch(config)#dhcpserver subnetmask 255.255.255.0
dhcpserver gateway [Gateway]	G	Configure gateway for DHCP clients	switch(config)#dhcpserver gateway 192.168.1.254
dhcpserver dnsip [DNS IP]	G	Configure DNS IP for DHCP clients	switch(config)# dhcpserver dnsip 192.168.1.1
dhcpserver leasetime [Hours]	G	Configure lease time (in hour)	switch(config)#dhcpserver leasetime 1
dhcpserver ipbinding [IP address]	I	Set static IP for DHCP clients by port	switch(config)#interface fastEthernet 2 switch(config-if)#dhcpserver ipbinding 192.168.1.1
show dhcpserver configuration	P	Show configuration of DHCP server	switch#show dhcpserver configuration
show dhcpserver clients	P	Show client entries of DHCP server	switch#show dhcpserver clinets
show dhcpserver ip-binding	P	Show IP-Binding information of DHCP server	switch#show dhcpserver ip-binding
no dhcpserver	G	Disable DHCP server function	switch(config)#no dhcpserver
security enable	G	Enable IP security function	switch(config)#security enable
security http	G	Enable IP security of HTTP server	switch(config)#security http
security telnet	G	Enable IP security of telnet server	switch(config)#security telnet
security ip [Index(1..10)] [IP Address]	G	Set the IP security list	switch(config)#security ip 1 192.168.1.55
show security	P	Show the information of IP security	switch#show security
no security	G	Disable IP security function	switch(config)#no security
no security http	G	Disable IP security of HTTP server	switch(config)#no security http

no security telnet	**G**	Disable IP security of telnet server	switch(config)#no security telnet

6.3 Commands Set List—Port Commands Set

iES10G(F) Commands	Level	Description	Example
interface fastEthernet [Portid]	**G**	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex [full | half]	**I**	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
speed [10|100|1000|auto]	**I**	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a Giga port.	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
flowcontrol mode [Symmetric|Asymmetric]	**I**	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion.	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol mode Asymmetric
no flowcontrol	**I**	Disable flow control of interface	switch(config-if)#no flowcontrol
security enable	**I**	Enable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#security enable
no security	**I**	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
bandwidth type all	**I**	Set interface ingress limit frame type to "accept all frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
bandwidth type broadcast-multicast-flooded-unicast	**I**	Set interface ingress limit frame type to "accept broadcast, multicast, and flooded unicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast

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

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

6.4 Commands Set List—Trunk command set

iES10G(F) Commands	Level	Description	Example
aggregator priority [1to65535]	G	Set port group system priority	switch(config)#aggregator priority 22
aggregator activityport [Port Numbers]	G	Set activity port	switch(config)#aggregator activityport 2
aggregator group [GroupID] [Port-list] **lacp** **workp** [Workport]	G	Assign a trunk group with LACP active. [GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	switch(config)#aggregator group 1 1-4 lacp workp 2 or switch(config)#aggregator group 2 1,4,3 lacp workp 3
aggregator group [GroupID] [Port-list] **nolacp**	G	Assign a static trunk group. [GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#aggregator group 1 2-4 nolacp or switch(config)#aggreator group 1 3,1,2 nolacp
show aggregator	P	Show the information of trunk group	switch#show aggregator
no aggregator lacp [GroupID]	G	Disable the LACP function of trunk group	switch(config)#no aggreator lacp 1
no aggregator group [GroupID]	G	Remove a trunk group	switch(config)#no aggreator group 2

6.5 Commands Set List—VLAN command set

iES10G(F) Commands	Level	Description	Example
vlan database	P	Enter VLAN configure mode	switch#vlan database
vlan **[8021q | gvrp]**	V	To set switch VLAN mode.	switch(vlan)# vlanmode 802.1q or switch(vlan)# vlanmode gvrp
no vlan [VID]	V	Disable vlan group(by VID)	switch(vlan)#no vlan 2
no gvrp	V	Disable GVRP	switch(vlan)#no gvrp
IEEE 802.1Q VLAN			
vlan 8021q port [PortNumber] **access-link untag** [UntaggedVID]	V	Assign 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] **trunk-link tag** [TaggedVID List]	V	Assign a trunk 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 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q port 3 trunk-link tag 3-20
vlan 8021q port [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	V	Assign a hybrid link for VLAN by port; if the port 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 aggreator [TrunkID] **access-link untag** [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)#vlan 8021q aggreator 3 access-link untag 33
vlan 8021q aggreator [TrunkID] **trunk-link tag** [TaggedVID List]	V	Assign a trunk link for VLAN by trunk group	switch(vlan)#vlan 8021q aggreator 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q aggreator 3 trunk-link tag 3-20
vlan 8021q aggreator	V	Assign a hybrid link for	switch(vlan)# vlan 8021q aggreator 3

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

6.6 Commands Set List—Spanning Tree command set

iES10G(F) Commands	Level	Description	Example
spanning-tree enable	**G**	Enable spanning tree	switch(config)#spanning-tree enable
spanning-tree priority [0to61440]	**G**	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
spanning-tree max-age [seconds]	**G**	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)# spanning-tree max-age 15
spanning-tree hello-time [seconds]	**G**	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
spanning-tree forward-time	**G**	Use the spanning-tree	switch(config)# spanning-tree forward-time

[seconds]		forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	20
stp-path-cost [1to200000000]	I	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20
stp-path-priority **[Port Priority]**	I	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-path-priority 127
stp-admin-p2p [Auto|True|False]	I	Admin P2P of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-p2p Auto
stp-admin-edge [True|False]	I	Admin Edge of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-edge True
stp-admin-non-stp [True|False]	I	Admin NonSTP of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-non-stp False
Show spanning-tree	E	Display a summary of the spanning-tree states.	switch>show spanning-tree

no spanning-tree	**G**	Disable spanning-tree.	switch(config)#no spanning-tree

6.7 Commands Set List—QoS command set

iES10G(F) 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

iES10G(F) Commands	Level	Description	Example
igmp enable	**G**	Enable IGMP snooping function	switch(config)#igmp enable
Igmp-query auto	**G**	Set IGMP query to auto mode	switch(config)#Igmp-query auto
Igmp-query force	**G**	Set IGMP query to force mode	switch(config)#Igmp-query force
show igmp configuration	**P**	Displays the details of an IGMP configuration.	switch#show igmp configuration
show igmp multi	**P**	Displays the details of an IGMP snooping entries.	switch#show igmp multi

no igmp	**G**	Disable IGMP snooping function	switch(config)#no igmp
no igmp-query	**G**	Disable IGMP query	switch#no igmp-query

6.9 Commands Set List—MAC/Filter Table command set

iES10G(F) 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

iES10G(F) Commands	Level	Description	Example
snmp agent-mode [v1v2c | v3]	**G**	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2c
snmp-server host [IP address]	**G**	Configure SNMP server host information and	switch(config)#snmp-server host 192.168.10.50 community public

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

6.11 Commands Set List—Port Mirroring command set

iES10G(F) Commands	Level	Description	Example
monitor rx	G	Set RX destination port of monitor function	switch(config)#monitor rx
monitor tx	G	Set TX destination port of monitor function	switch(config)#monitor tx
show monitor	P	Show port monitor information	switch#show monitor

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

6.12 Commands Set List—802.1x command set

iES10G(F) Commands	Level	Description	Example
8021x enable	G	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiousip [IP address]	G	Use the 802.1x system radius IP global configuration command to change the radius server IP.	switch(config)# 8021x system radiusip 192.168.1.1
8021x system serverport [port ID]	G	Use the 802.1x system server port global configuration command to change the radius server port	switch(config)# 8021x system serverport 1815
8021x system accountport [port ID]	G	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# 8021x system accountport 1816
8021x system sharekey [ID]	G	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# 8021x system sharekey 123456
8021x system nasid [words]	G	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# 8021x system nasid test1

8021x misc quietperiod [sec.]	G	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# 8021x misc quietperiod 10
8021x misc txperiod [sec.]	G	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# 8021x misc txperiod 5
8021x misc supportimeout [sec.]	G	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# 8021x misc supportimeout 20
8021x misc servertimeout [sec.]	G	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#8021x misc servertimeout 20
8021x misc maxrequest [number]	G	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# 8021x misc maxrequest 3
8021x misc reauthperiod [sec.]	G	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# 8021x misc reauthperiod 3000
8021x portstate [disable | reject | accept | authorize]	I	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch(config)#interface fastethernet 3 switch(config-if)#8021x portstate accept
show 8021x	P	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

iES10G(F) Commands	Level	Description	Defaults Example
backup flash:backup_cfg	G	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#backup flash:backup_cfg
restore flash:restore_cfg	G	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)#restore flash:restore_cfg
upgrade flash:upgrade_fw	G	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#upgrade lash:upgrade_fw

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

iES10G(F) Commands	Level	Description	Example
systemlog ip [IP address]	G	Set System log server IP address.	switch(config)# systemlog ip 192.168.1.100
systemlog mode [client|server|both]	G	Specified the log mode	switch(config)# systemlog mode both
show systemlog	E	Display system log.	Switch>show systemlog
show systemlog	P	Show system log client & server information	switch#show systemlog
no systemlog	G	Disable systemlog function	switch(config)#no systemlog
smtp enable	G	Enable SMTP function	switch(config)#smtp enable
smtp serverip [IP address]	G	Configure SMTP server IP	switch(config)#smtp serverip 192.168.1.5
smtp authentication	G	Enable SMTP authentication	switch(config)#smtp authentication
smtp account [account]	G	Configure authentication account	switch(config)#smtp account User

smtp password [password]	G	Configure authentication password	switch(config)#smtp password
smtp rcptemail [Index] [Email address]	G	Configure Rcpt e-mail Address	switch(config)#smtp rcptemail 1 Alert@test.com
show smtp	P	Show the information of SMTP	switch#show smtp
no smtp	G	Disable SMTP function	switch(config)#no smtp
event device-cold-start [Systemlog|SMTP|Both]	G	Set cold start event type	switch(config)#event device-cold-start both
event 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 s ring topology changed event type	switch(config)#event ring-topology-change both
event systemlog [Link-UP|Link-Down|Both]	I	Set port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#event systemlog both
event smtp [Link-UP|Link-Down|Both]	I	Set port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#event smtp both
show event	P	Show event selection	switch#show event
no event device-cold-start	G	Disable cold start event type	switch(config)#no event device-cold-start
no event authentication-failure	G	Disable Authentication failure event type	switch(config)#no event authentication-failure
no event iRing-topology-change	G	Disable iRing topology changed event type	switch(config)#no event ring-topology-change
no event systemlog	I	Disable port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#no event systemlog
no event smpt	I	Disable port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#no event smtp
show systemlog	P	Show system log client & server information	switch#show systemlog

6.15 Commands Set List—SNTP command set

iES10G(F) 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	switch(config)#sntp daylight

		inactive, this command can't be applied.	
sntp daylight-period [Start time] [End time]	G	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# sntp daylight-period 20060101-01:01 20060202-01-01
sntp daylight-offset [Minute]	G	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight-offset 3
sntp ip [IP]	G	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp ip 192.169.1.1
sntp timezone [Timezone]	G	Set timezone index, use "show sntp timezone" 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

iES10G(F) Commands	Level	Description	Example
Ring enable	G	Enable iRing	switch(config)# ring enable
Ring master	G	Enable ring master	switch(config)# ring master
Ring couplering	G	Enable couple ring	switch(config)# ring couplering
Ring dualhoming	G	Enable dual homing	switch(config)# ring dualhoming

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

Technical Specifications

Model Number iES10G/iES10GF	
Physical Ports	
10/100 Base-TX Ports (RJ45) Auto MDI/MDIX	7
Gigabit combo Ports with 10/100/1000Base-TX and 100/1000Base-X SFP Ports	3- Base T(X) or 3- Base (X) SFP
Technology	
Ethernet Standards	802.3 - 10Base-T, 802.3u - 100Base-TX, 100Base-FX, 802.3z - 1000Base-X 802.3ab - 1000Base-TX, 802.3ad - Link Aggregation Control Protocol 802.3x - Flow Control 802.1D - Spanning Tree Protocol 802.1p - Class of Service, 802.1Q - VLAN Tagging 802.1w - Rapid Spanning Tree Protocol, 802.1X - Authentication 802.1ad - VLAN QinQ 802.1AB – LLDP
MAC addresses	8192
Priority Queues	4
Flow Control	IEEE 802.3x Flow Control and Back-pressure
Processing	Store-and-Forward
Switch Properties	Switching latency: 7 us Switching bandwidth: 7.4Gbps Max. Number of Available VLANs: 4096 IGMP multicast groups: 1024 Port rate limiting: User Defined
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 20ms up to 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 Supports PTP Client (Precision Time Protocol) clock synchronization DHCP Server / Client support Port Trunk support MVR (Multicast VLAN Registration) support
Network Redundancy	iRing, iBridge, STP, RSTP, MSTP
Warning / Monitoring System	Relay output for fault event alarming Syslog server / client to record and view events 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
Fault Contact	
Relay	Relay output capacity: 1A at 24VDC
Power	
Power Input Voltage	Dual DC inputs 10 to 48VDC, Dual DC Inputs 36-72VDC, or Dual Input Universal Supplies 120-370VDC or 85-264VAC
Power Consumption (Typ.)	iES10G - 12 Watts Max iES10GF - 20 Watts Max.
Overload Current Protection	Present
Reverse Polarity Protection	Internal
Physical Characteristic	
Enclosure	IP-40 Galvanized Steel Housing
Dimension (W x D x H)	IES10G - 101.6 mm(W)x 109.2 mm(D)x 153.8 mm(H) (4x4.3 x 6.05 inch) iES10GF – 101.8(W)x163.2(D)x153.6(H) mm (4 x 6.43 x 6.05 inch)
Weight (g)	iES10G – 1.1 kg

	iES10GF - 1.2 kg
Environmental	
Operating Temperature	-40oC to 85oC (-40oF to 185oF)
Storage Temperature	40oC to 85oC (-40oF to 185oF) NO FANS
Operating Humidity	5% to 95% Non-condensing
Regulatory Approvals	
Regulatory Approvals	FCC Part 15, CISPER (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS) EN61000-4-8, EN61000-4-11
Shock	IEC 60068-2-27
Free Fall	IEC 60068-2-32
Vibration	IEC 60068-2-6
Safety	EN60950-1
Warranty	
Warranty	5 years

Appendix A: iES10G(F) Modbus Information

Address	Description
16	VendorName
48	ProductName
81	Version
85	MacAddress
90	FaultAlarm: 0x0000 – No Fault Alarm 0x0001 – Fault Alarm
256	SysName
512	SysDescription
768	SysLocation
1024	SysContact
4096 -4105	PortStatus: Port :1~VTSS_PORTS Value :0x0000 Link down 0x0001 Link up 0x0002 Disable 0xffff NoPort
4352-4361	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
4608-4617	PortFlowCtrl : Port :1~VTSS_PORTS Value :0x0000 Off 0x0001 On 0xffff NoPort