

## Intelligent 10 Port Managed Ethernet Switch

### iES10G(F) Series User's Manual



**Version 2.30**  
**Jan 2022**

**iS5 Communications Inc.**  
5895 Ambler Dr. ,  
Mississauga, Ontario, L4W 5B7  
Tel: + 905- 670- 0004  
Fax: + 289- 401- 5206  
Website: [www.iS5Com.com](http://www.iS5Com.com)  
E-mail: [support@iS5Com.com](mailto:support@iS5Com.com)



## All Rights Reserved

Dissemination or reproduction of this document, or evaluation and communication of its contents, is not authorized except where expressly permitted. Violations are liable for damages. All rights are reserved, particularly for the purposes of patent application or trademark registration.

This document contains proprietary information, which is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced or translated to another language without the prior written consent of iS5 Communications Inc.

## 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](http://www.iS5Com.com) or contact your customer service representative.

# Table of Contents

<b><i>CAUTION: LASER</i></b> .....	<b>6</b>
<b><i>CAUTION: SERVICE</i></b> .....	<b>6</b>
<b><i>CAUTION: PHYSICAL ACCESS</i></b> .....	<b>6</b>
<b>INTRODUCTION</b> .....	<b>7</b>
1.1 About the iES10G(F) Series Intelligent Managed Ethernet Switch.....	7
1.2 Software Features .....	7
1.3 Hardware Features.....	7
<b>Hardware Installation</b> .....	<b>8</b>
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
<b>Hardware Overview</b> .....	<b>10</b>
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
<b>Cables</b> .....	<b>15</b>
4.1 Ethernet Cables.....	15
4.1.1 100BASE-TX/10BASE-T Pin Assignments .....	15
4.2 SFP .....	16
4.3 Console Cable .....	17
<b>WEB Management</b> .....	<b>18</b>
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
<b>Command Line Interface Management (CLI) .....</b>		<b>77</b>
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
<b>Technical Specifications.....</b>		<b>99</b>
<b>APPENDIX A: IES10G(F) MODBUS INFORMATION .....</b>		<b>102</b>

## 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](mailto: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

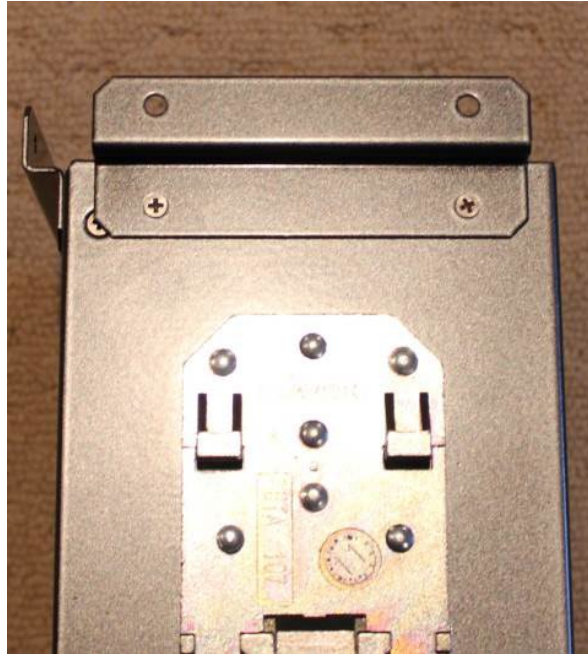
The switch can also be panel or wall mounted. The following steps show how to mount the switch on a panel or wall.

### 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.



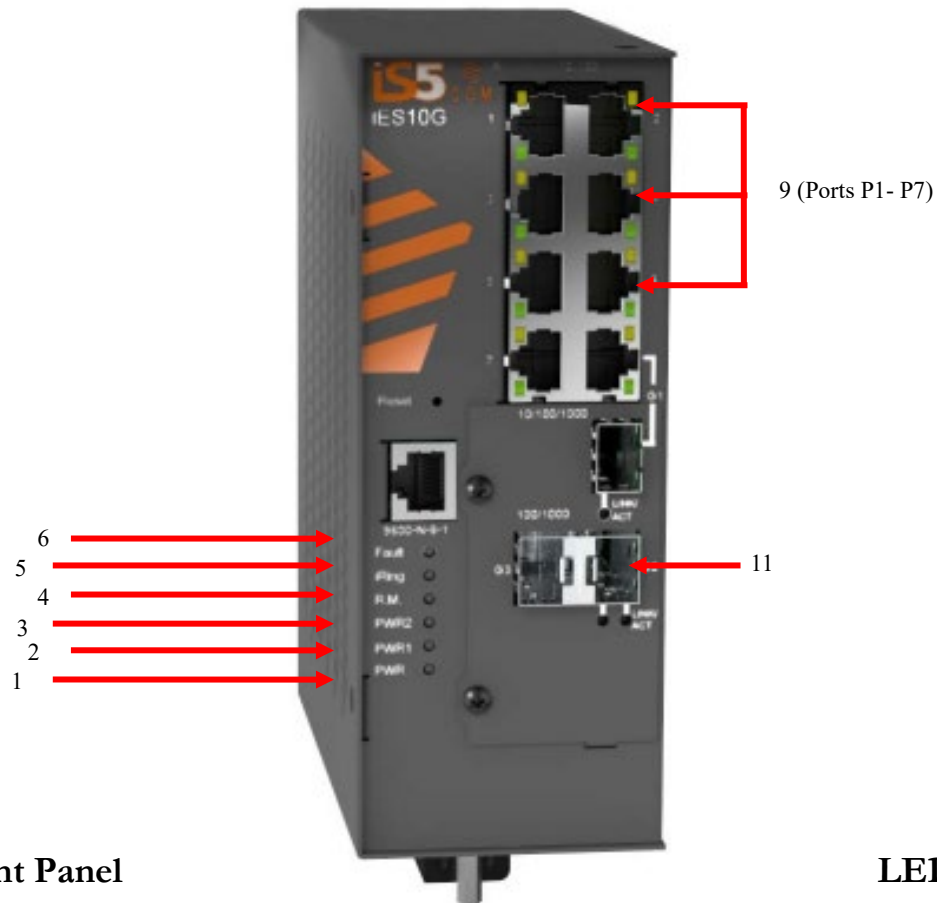
Note: To avoid damage to the unit please use the screws provided to mount the panel mount brackets to the unit.

## Hardware Overview

### 3.1 Front Panel

Product description:

Port	Description
<b>10/100 RJ45 fast Ethernet ports (9)</b>	7 x 10/100Base-T(X) RJ45 fast Ethernet ports support auto-negotiation. Default Setting : Speed: auto Duplex: auto Flow control : disable
<b>Gigabit RJ45 port (10)</b>	2 x 10/100/1000Base-T(X) ports (Optional)
<b>Fiber port (not shown)</b>	3x 100/1000Base-(X) SFP ports (Optional)
<b>Console (7)</b>	Use a RS232 to RJ45 cable assembly to manage switch.
<b>Reset (8)</b>	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 <b>Factory Default</b> .



### 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.

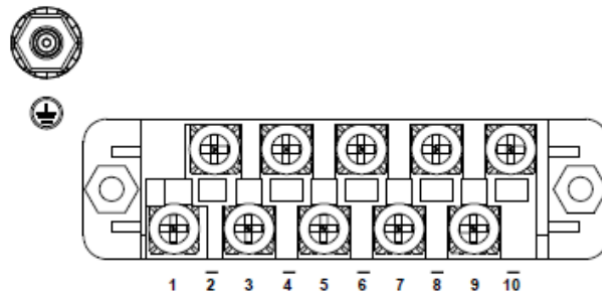
### 3.3 Bottom View Panel

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.

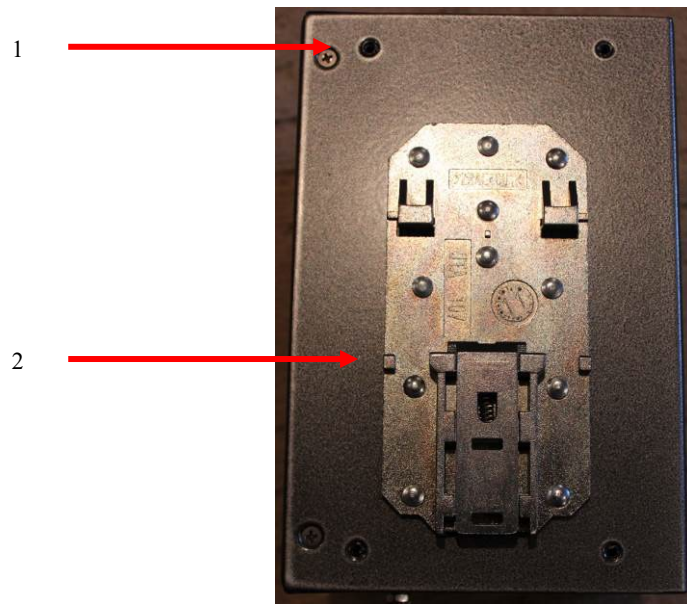


- ⚡ 120-370VDC rated equipment: A 370VDC appropriately rated circuit breaker must be installed.
- ⚡ A circuit breaker is not required for DC power supply voltages of 10-48VDC.
- ⚡ For Dual DC power supplies, separate circuit breakers must be installed and separately identified.
- ⚡ Equipment must be installed according to the applicable country wiring codes.

## 3.4 Rear Panel

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

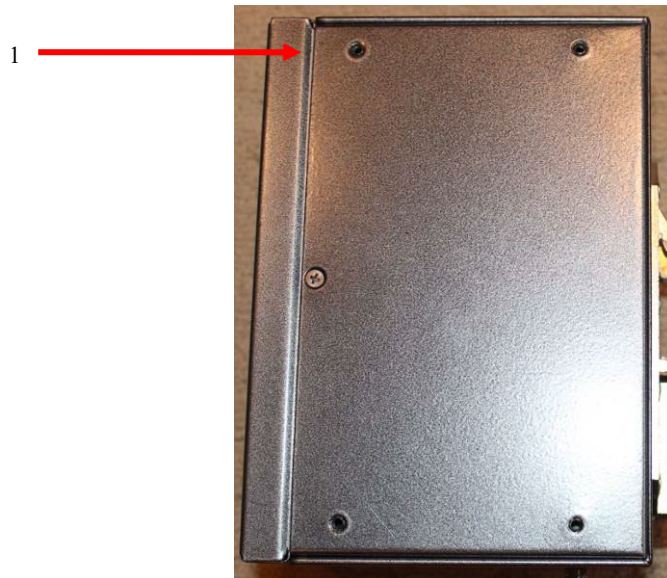
1. Screw holes (4) for wall mount kit.
2. DIN-Rail mount



### 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 Assignments

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

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:

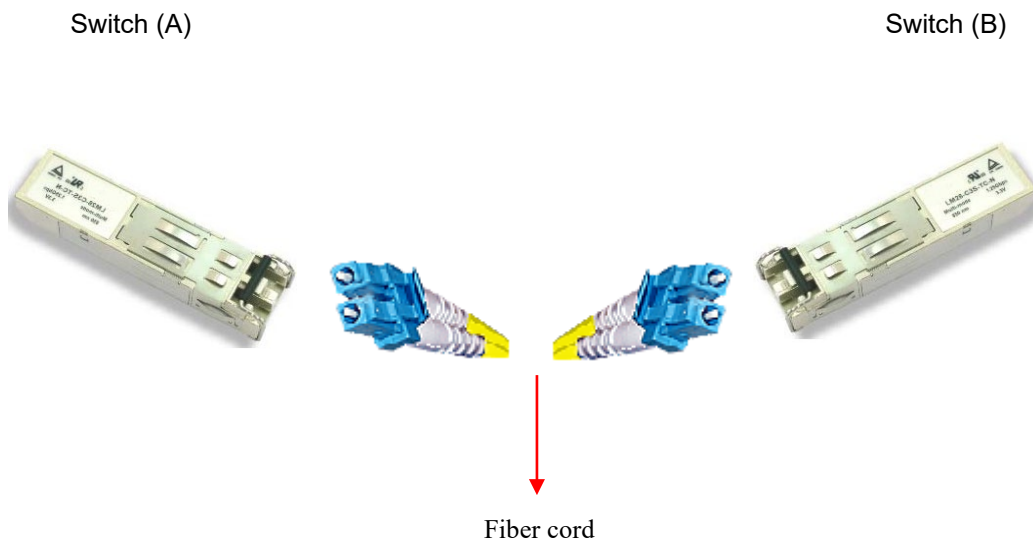
Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

**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  $\mu$ m, and 62.5/125  $\mu$ m fiber), or Singlemode LC connectors.

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



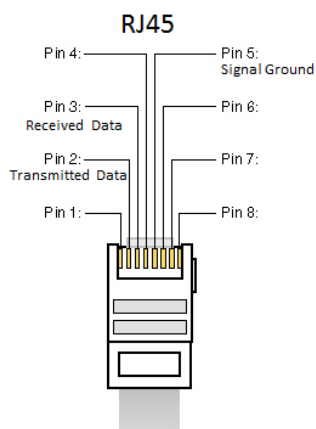
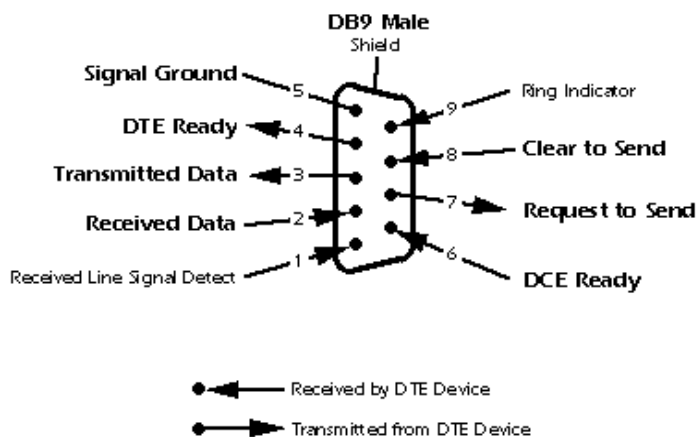


### 4.3 Console Cable


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



**Warning!!!**

Prior to upgrading the firmware,  
remove any physical loop connections.  
**DO NOT** power off the unit during a  
firmware upgrade.

## 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**

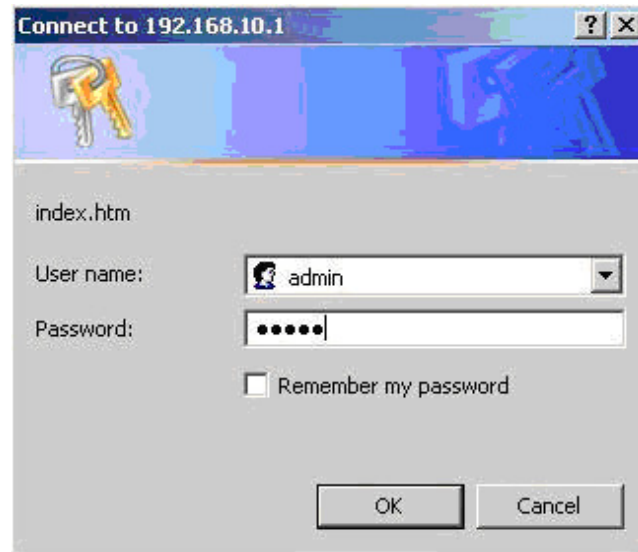
Password: **admin**

### System Login

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

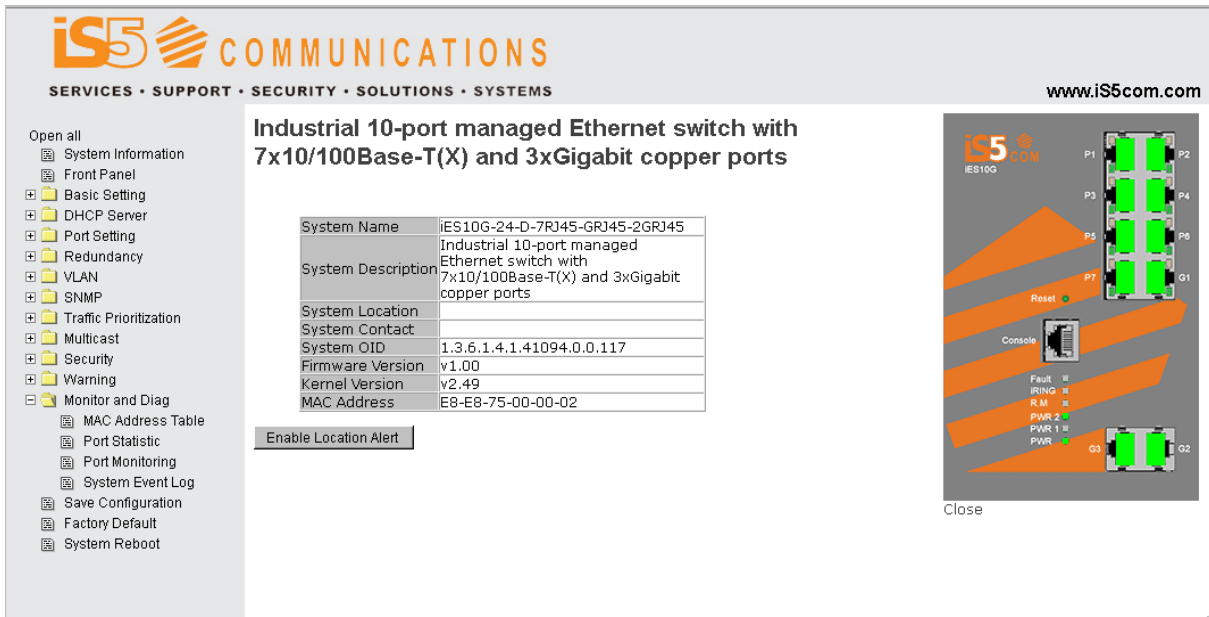


3. The login screen appears.
4. Key in the default username and password.
5. Click “Enter” or “OK”. The main interface of the Web-based management appears.



Login screen

## Main Interface



Main interface

## 5.1.2 System Information

**iS5 COMMUNICATIONS**  
SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS

www.iS5com.com

Open all  
☐ System Information  
☐ Front Panel  
☐ Basic Setting  
☐ DHCP Server  
☐ Port Setting  
☐ Redundancy  
☐ VLAN  
☐ SNMP  
☐ Traffic Prioritization  
☐ Multicast  
☐ Security  
☐ Warning  
☐ Monitor and Diag  
     ☐ MAC Address Table  
     ☐ Port Statistic  
     ☐ Port Monitoring  
     ☐ System Event Log  
☐ Save Configuration  
☐ Factory Default  
☐ System Reboot

### Industrial 10-port managed Ethernet switch with 7x10/100Base-T(X) and 3xGigabit copper ports

System Name	iES10G-24-D-7RJ45-GRJ45-2GRJ45
System Description	Industrial 10-port managed Ethernet switch with 7x10/100Base-T(X) and 3xGigabit copper ports
System Location	
System Contact	
System OID	1.3.6.1.4.1.41094.0.0.117
Firmware Version	v1.00
Kernel Version	v2.49
MAC Address	E8-E8-75-00-00-02

Close

System Information interface

### System Information

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

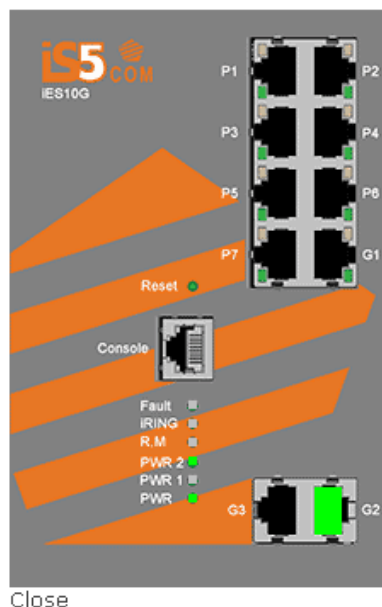
#### Enable Location Alert

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

Click , 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

**iS5 COMMUNICATIONS**  
SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS

www.iS5com.com

Open all

- System Information
- Front Panel
- Basic Setting
- DHCP Server
- Port Setting
- Redundancy
- VLAN
- SNMP
- Traffic Prioritization
- Multicast
- Security
- Warning
- Monitor and Diag
  - MAC Address Table
  - Port Statistic
  - Port Monitoring
  - System Event Log
- Save Configuration
- Factory Default
- System Reboot

**Industrial 10-port managed Ethernet switch with 7x10/100Base-T(X) and 3xGigabit copper ports**

System Name	iES10G-24-D-7RJ45-GRJ45-2GRJ45
System Description	Industrial 10-port managed Ethernet switch with 7x10/100Base-T(X) and 3xGigabit copper ports
System Location	
System Contact	
System OID	1.3.6.1.4.1.41094.0.0.117
Firmware Version	v1.00
Kernel Version	v2.49
MAC Address	E8-E8-75-00-00-02

Close

Switch setting interface

The following table describes the Switch setting interface page.

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

<b>System Contact</b>	Enter the name of contact person or organization
<b>System OID</b>	Displays the switch's OID information
<b>Firmware Version</b>	Displays the switch's firmware version
<b>Kernel Version</b>	Displays the kernel software version
<b>MAC Address</b>	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

User Name	<input type="text" value="admin"/>
New Password	<input type="password" value="•••••"/>
Confirm Password	<input type="password" value="•••••"/>

Admin Password interface

The following table describes the Admin Password interface page.

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

### 5.1.4.3 IP Setting

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

**IP Setting**

**DHCP Client :** Disable ▼

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

Apply
Help

IP Configuration interface

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

Label	Description
<b>DHCP Client</b>	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 “ <b>Apply</b> ” button, a popup dialog shows up to inform when the DHCP client is enabled.
<b>IP Address</b>	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.
<b>Subnet Mask</b>	Assign the subnet mask of the IP address. If the DHCP client function is enabled, there is no need to assign a subnet mask.
<b>Gateway</b>	Assign the network gateway for the switch. The default gateway is 192.168.10.254.
<b>DNS1</b>	Assign the primary DNS IP address
<b>DNS2</b>	Assign the secondary DNS IP address
<b>Apply</b>	Click “ <b>Apply</b> ” to activate the configurations.
<b>Help</b>	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

**SNTP Client :**

UTC Timezone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
SNTP Server Address	0.0.0.0
Current System Time	Thursday, January 01, 1970 12:12:08

**Daylight Saving Time :**

Daylight Saving Period	2013 / Jan / 29 14 ~ 2013 / Jan / 29 14
Daylight Saving Offset	0 (hours)

SNTP Configuration interface

The following table describes the SNTP Configuration interface page.

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

LLDP configuration interface

The following table describes the LLDP configuration interface page.

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

#### 5.1.4.6 Modbus TCP

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

## MODBUS Configuration

**Mode** Enabled ▼  
Save Reset

Label	Description
<b>Mode</b>	Shows the existing status of the Modbus TCP function
<b>Save</b>	Click to save changes
<b>Reset</b>	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

☒ Auto Install Configuration file from TFTP server?  
 TFTP Server IP Address 192.168.10.66  
 Configuration File Name data.bin  
☐ Auto Install Firmware image file from TFTP server?  
 TFTP Server IP Address 192.168.10.66  
 Firmware File Name image.bin

Apply Help

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

### Restore Configuration From TFTP Server

TFTP Server IP Address	192.168.10.66
Restore File Name	data.bin

### From Local PC

<input type="text"/>	<input type="button" value="Browse..."/>
----------------------	--

### Backup Configuration To TFTP Server

TFTP Server IP Address	192.168.10.66
Backup File Name	data.bin

### To Local PC

Backup & Restore interface

The following table describes the Backup & Restore interface page.

Label	Description
<b>TFTP Server IP Address</b>	Enter the TFTP server IP address.
<b>Restore File Name</b>	Enter the file name.
<b>Restore</b>	Click “ <b>restore</b> ” to restore the configurations.
<b>Backup File Name</b>	Enter the file name.
<b>Backup</b>	Click “ <b>backup</b> ” to backup the configurations.
<b>Help</b>	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.

## Upgrade Firmware

### From TFTP Server

TFTP Server IP	192.168.10.66
Firmware File Name	image.bin

### From Local PC

<input type="text"/>	<input type="button" value="Browse..."/>
----------------------	--

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 - Setting

DHCP Server :

Start IP Address	192.168.10.2
End IP Address	192.168.10.200
Subnet Mask	255.255.255.0
Gateway	192.168.10.254
DNS	0.0.0.0
Lease Time (Hour)	168

DHCP Server Configuration interface

The following table describes the DHCP Server Configuration interface page.

Label	Description
<b>DHCP Server</b>	Enable or Disable the DHCP Server function. Enable – the switch will act as the DHCP server on your local network.
<b>Start IP Address</b>	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.
<b>End IP Address</b>	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.
<b>Subnet Mask</b>	The dynamic IP assigned range subnet mask.
<b>Gateway</b>	The gateway in the network.
<b>DNS</b>	Domain Name Server IP Address in the network.
<b>Lease Time (Hour)</b>	It is the period that the system will reset the assigned dynamic IP address to ensure the IP address is in use.
<b>Apply</b>	Click “ <b>Apply</b> ” to activate the configurations.
<b>Help</b>	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

Port No.	State	Speed/Duplex	Flow Control	Security
Port.01	Enable ▾	AutoNegotiation ▾	Symmetric ▾	Disable ▾
Port.02	Enable ▾	AutoNegotiation ▾	Symmetric ▾	Disable ▾
Port.03	Enable ▾	AutoNegotiation ▾	Symmetric ▾	Disable ▾
Port.04	Enable ▾	AutoNegotiation ▾	Symmetric ▾	Disable ▾
Port.05	Enable ▾	AutoNegotiation ▾	Symmetric ▾	Disable ▾
Port.06	Enable ▾	AutoNegotiation ▾	Symmetric ▾	Disable ▾
Port.07	Enable ▾	AutoNegotiation ▾	Symmetric ▾	Disable ▾
G1	Enable ▾	AutoNegotiation ▾	Symmetric ▾	Disable ▾
G2	Enable ▾	AutoNegotiation ▾	Symmetric ▾	Disable ▾
G3	Enable ▾	AutoNegotiation ▾	Symmetric ▾	Disable ▾



Port Control interface

The following table describes the Port Control interface page.

Label	Description
<b>Port No.</b>	Port number for setting.
<b>Speed/Duplex</b>	You can set Auto-negotiation, 100 full, 100 half, 10 full or 10 half
<b>Flow Control</b>	Supports symmetrical and asymmetrical mode to avoid packet loss when congestion occurs.
<b>Security</b>	Supports port security function. When enabled, the port will <b>STOP</b> learning the MAC address dynamically.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.
<b>Help</b>	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
<b>Ingress Limit Frame Type</b>	Can be set to: “All”, “Broadcast only”, “Broadcast/Multicast” or “Broadcast/Multicast/Flooded Unicast” mode.
<b>Ingress</b>	The switch port received traffic.
<b>Egress</b>	The switch port transmitted traffic.
<b>Apply</b>	Click “Apply” to activate the configurations.
<b>Help</b>	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

Port No.	Group ID	Type
Port.01	None	Static
Port.02	None	Static
Port.03	None	Static
Port.04	None	Static
Port.05	None	Static
Port.06	None	Static
Port.07	None	Static
G1	None	Static
G2	None	Static
G3	None	Static

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

Port Trunk - Setting interface

The following table describes the Port Trunk Setting interface page.

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

### 802.3ad LACP Work Ports

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

Apply Help

The following table describes the Port Trunk LACP interface page.

Label	Description
<b>Work Ports</b>	Work ports counted (max:4 ports)
<b>Apply</b>	Click “ <b>Apply</b> ” to activate the configurations.
<b>Help</b>	Show help file.

## Port Trunk – Status

You can check the configuration of a port trunk.

### Port Trunk - Status

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

Port Trunk - Status interface

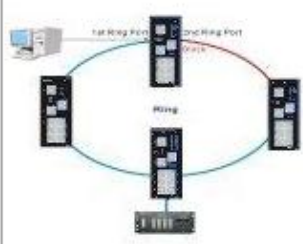
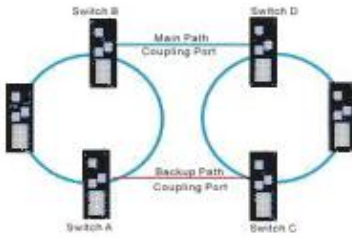
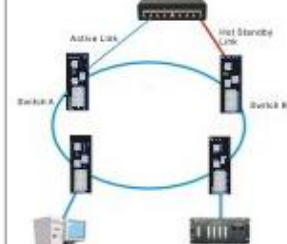
## 5.1.7 Redundancy

### 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

<input type="checkbox"/> iRing	<input type="checkbox"/> Coupling Ring	<input type="checkbox"/> Dual Homing
		
Ring Master: <input type="text" value="Disable"/>	Coupling Port: <input type="text" value="Port.03"/>	Homing Port: <input type="text" value="Port.05"/>
1st Ring Port: <input type="text" value="Port.01"/>		
2nd Ring Port: <input type="text" value="Port.02"/>		
<input type="button" value="Apply"/> <input type="button" value="Help"/>		

iRing interface

The following table describes the iRing interface page.

Label	Description
<b>iRing</b>	To enable iRing.
<b>Ring Master</b>	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.
<b>1<sup>st</sup> Ring Port</b>	The primary port; when this switch is configured in iRing.
<b>2<sup>nd</sup> Ring Port</b>	The backup port; when this switch is configured in iRing.
<b>Coupling Ring</b>	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.
<b>Coupling Port</b>	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.
<b>Dual Homing</b>	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.
<b>Apply</b>	Click “ <b>Apply</b> ” to activate the configurations.
<b>Help</b>	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

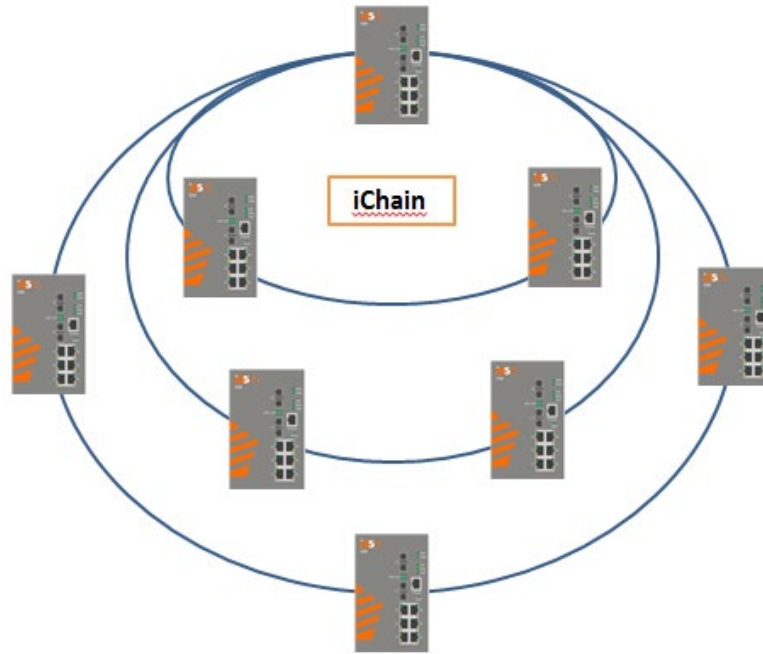
<input type="checkbox"/> Enable		
Uplink Port	Edge Port	State
1st Port.01	<input type="checkbox"/>	Linkdown
2nd Port.02	<input type="checkbox"/>	Linkdown

Apply

iChain Interface

The following table describes the labels for the iChain screen.

Label	Description
<b>Enable</b>	Enables the iChain function.
<b>Uplink Port</b>	Select the port (1 - 8) to be the Uplink Port.
<b>Edge Port</b>	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.
<b>State</b>	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

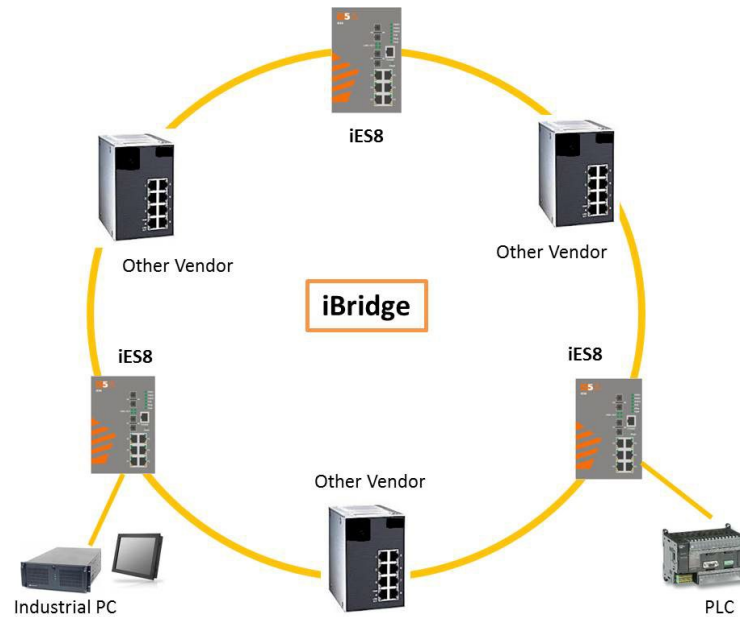
<input type="checkbox"/> Enable	
Vendor	Moxa
1st Ring Port	Port.01
2nd Ring Port	Port.02

Apply

iBridge Interface

The following table describes the labels for the iBridge screen.

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

#### RSTP-Repeater

☐ Enable

	Uplink Port	RSTP Edge Port
1st	G1	<input type="checkbox"/>
2nd	G2	<input type="checkbox"/>

Label	Description
<b>Enable</b>	Check this box to enable RSTP-Repeater.
<b>1stRing Port</b>	Choosing the port which connect to the RSTP
<b>2ndRing Port</b>	Choosing the port which connect to the RSTP
<b>Edge Port</b>	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 : Enable ▾

Port No.	Recovery Priority
G1	8 ▾
G2	7 ▾
G3	Not included ▾
G4	Not included ▾
G5	Not included ▾
G6	Not included ▾
G7	Not included ▾
G8	1 ▾

Fast Recovery is disabled.

Apply Help

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

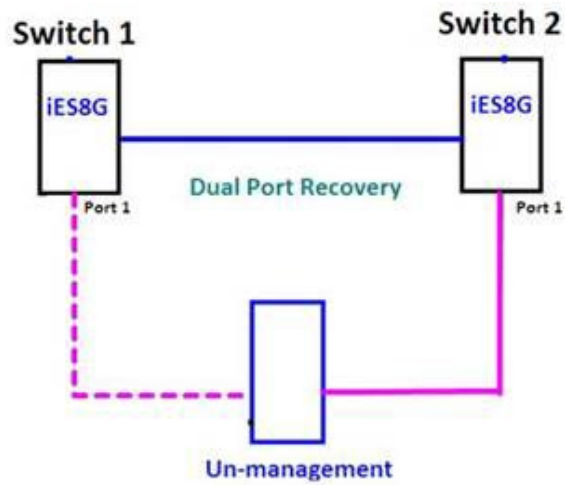
The Dual Port Recovery mechanism is the mechanism that allows execution of recovery protocol over the unmanaged devices/switches (ring of switches) that don't support other recovery protocols.

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.

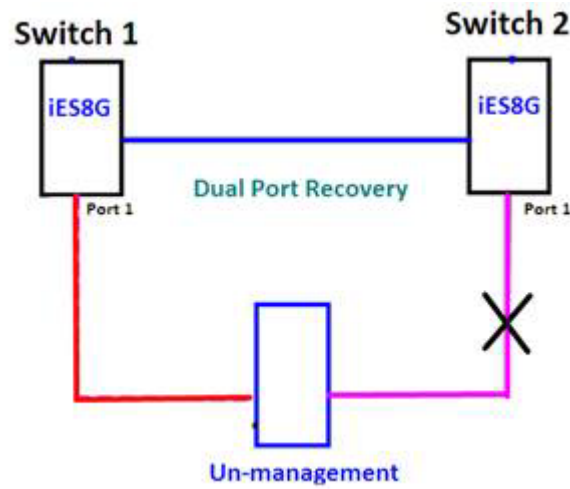
#### Dual Port Recovery- Concept

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

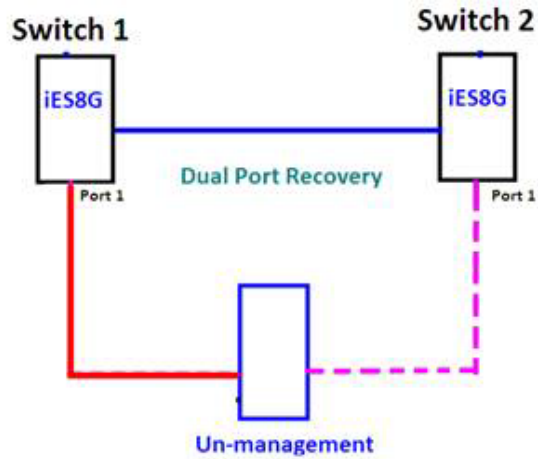




In Dual Port Recovery function if link of port in "Forwarding" state goes down, the "backup" port is changing its state to be forwarding, like in picture below. The disconnected port changes its status to "No Link"



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

<input checked="" type="checkbox"/> Enable		
Active Port	G8 ▼	Forwarding
Test Interval	10	10~5000ms
Test Max Retry	3	1~500
<input type="button" value="Apply"/>		

Dual Port Recovery interface

Label	Description
<b>Enable</b>	Activate the Dual Port Recovery mode.
<b>Active Port</b>	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.
<b>Test Interval</b>	Setting Interval time for sending keep alive messages (10-5000ms default 10) Note: Test interval should be the same on both sides.
<b>Test Max Retry</b>	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.
<b>Apply</b>	Click <b>"Apply"</b> 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

**RSTP Mode:**

##### Bridge Setting

Priority (0-61440)	<input type="text" value="32768"/>
Max Age Time(6-40)	<input type="text" value="20"/>
Hello Time (1-10)	<input type="text" value="2"/>
Forward Delay Time (4-30)	<input type="text" value="15"/>

##### Port Setting

Port No.	Enable	Path Cost(0:auto, 1-200000000)	Priority (0-240)	P2P	Edge
Port.01	<input type="button" value="enable"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="button" value="auto"/>	<input type="button" value="true"/>
Port.02	<input type="button" value="enable"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="button" value="auto"/>	<input type="button" value="true"/>
Port.03	<input type="button" value="enable"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="button" value="auto"/>	<input type="button" value="true"/>
Port.04	<input type="button" value="enable"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="button" value="auto"/>	<input type="button" value="true"/>
Port.05	<input type="button" value="enable"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="button" value="auto"/>	<input type="button" value="true"/>
Port.06	<input type="button" value="enable"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="button" value="auto"/>	<input type="button" value="true"/>
Port.07	<input type="button" value="enable"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="button" value="auto"/>	<input type="button" value="true"/>
Port.08	<input type="button" value="enable"/>	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="button" value="auto"/>	<input type="button" value="true"/>

RSTP Setting interface

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

Label	Description
<b>RSTP mode</b>	The RSTP function must be enabled or disabled before configuring any of the related parameters.
<b>Priority (0-61440)</b>	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.
<b>Max Age (6-40)</b>	The number of seconds for a bridge to wait without receiving Spanning Tree Protocol configuration messages before reconfiguration. Enter a value between 6 and 40.
<b>Hello Time (1-10)</b>	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.
<b>Forwarding Delay Time (4-30)</b>	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.
<b>Path Cost (1-200000000)</b>	The Path Cost to the other bridge from the transmitting bridge at a specified port. Enter a number 1 to 200000000.
<b>Priority (0-240)</b>	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.
<b>P2P</b>	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to 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.
<b>Edge</b>	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 <b>"True"</b> .
<b>Apply</b>	Click <b>"Apply"</b> to activate the configurations.

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

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

## RSTP Information

Show RSTP algorithm result at this table.

### RSTP Information

#### Root Bridge Information

Bridge ID	N/A
Root Priority	N/A
Root Port	N/A
Root Path Cost	N/A
Max Age Time	N/A
Hello Time	N/A
Forward Delay Time	N/A

#### Port Information

Port	Path Cost	Port Priority	OperP2P	OperEdge	STP Neighbor	State	Role
------	-----------	---------------	---------	----------	--------------	-------	------

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. <b><math>2 \times (\text{Forward Delay Time value} - 1) \geq \text{Max Age value} \geq 2 \times (\text{Hello Time value} + 1)</math></b>
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

### MSTP Setting

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

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

The following table describes the labels in this screen.

Label	Description
<b>MSTP Enable</b>	You must enable or disable MSTP function before configuring the related parameters.
<b>Force Version</b>	The Force Version parameter can be used to force a VLAN Bridge that supports RSTP to operate in an STP-compatible manner.
<b>Configuration Name</b>	The same MST Region must have the same MST configuration name.
<b>Revision Level (0-65535)</b>	The same MST Region must have the same revision level.
<b>Priority (0-61440)</b>	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, You must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.
<b>Max Age Time(6-40)</b>	The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 and 40.
<b>Hello Time (1-10)</b>	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. <b><math>2 \times (\text{Forward Delay Time value} - 1) \geq \text{Max Age value} \geq 2 \times (\text{Hello Time value} + 1)</math></b>
<b>Forwarding Delay Time (4-30)</b>	The number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 and 30.
<b>Max Hops (1-40)</b>	This parameter is additional to those specified for RSTP. A single value applies to all Spanning Trees within an MST Region (the CIST and all MSTIs) for which the Bridge is the Regional Root.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.

## MSTP Port

### MSTP Port

Port No.	Priority (0-240)	Path Cost (1-2000000000, 0:Auto)	Admin P2P	Admin Edge	Admin Non Stp
Port.01 Port.02 Port.03 Port.04 Port.05	128	0	auto	true	false

priority must be a multiple of 16

Apply

The following table describes the labels in this screen.

Label	Description
<b>Port No.</b>	Select the port that you want to configure.
<b>Priority (0-240)</b>	Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16
<b>Path Cost (1-2000000000)</b>	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 2000000000.
<b>Admin P2P</b>	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. It is served by a point-to-point LAN segment), or it can be connected to two or more bridges (i.e. It is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True means P2P enabled. False means P2P disabled.

Label	Description
Admin Edge	Label
Admin Non STP	Label
Apply	Click “Apply” to activate the configurations.

## MSTP Instance

### MSTP Instance Port

Instance: CIST ▼

Port	Priority (0-240)	Path Cost (1-2000000000, 0:Auto)
Port.01		
Port.02 ^		
Port.03	128	0
Port.04 v		
Port.05		

Priority must be a multiple of 16

Apply

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

### MSTP Port

Port No.	Priority (0-240)	Path Cost (1-2000000000, 0:Auto)	Admin P2P	Admin Edge	Admin Non Stp
Port.01					
Port.02 ^					
Port.03	128	0	auto ▼	true ▼	false ▼
Port.04 v					
Port.05					

priority must be a multiple of 16

Apply

The following table describes the labels in this screen.

Label	Description
-------	-------------



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

### 5.1.7.9 MRP

#### MRP

☐ Enable

☐ Manager
 ☐ React on Link Change

1st Ring Port
 Port.01 ▾
 Linkdown

2nd Ring Port
 Port.02 ▾
 Linkdown

☐ Force Speed/Duplex for 100BASE-TX

Apply

Label	Description
<b>Enable</b>	Enables the MRP function.
<b>Manager</b>	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.
<b>React on Link Change (Advanced mode)</b>	Faster mode. Enabling this function will ensure MRP topology a more rapid converge. This function only can be set by the MRP manager switch.
<b>1st Ring Port</b>	Chooses the port that connects to the MRP ring.
<b>2nd Ring Port</b>	Chooses the port that connects to the MRP ring.
<b>Force Speed / Duplex for 100 Base-TX</b>	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 vendors. 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 Setting

VLAN Operation Mode : 802.1Q

GVRP Mode : Disable

Management Vlan ID : 0

### VLAN Configuration

Port No.	Link Type	Untagged VID	Tagged VIDs
Port.01	Access	1	
Port.02	Access	1	
Port.03	Access	1	
Port.04	Access	1	
Port.05	Access	1	
Port.06	Access	1	
Port.07	Access	1	
G1	Access	1	
G2	Access	1	
G3	Access	1	

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



#### VLAN Configuration – 802.1Q interface

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

Label	Description
<b>VLAN Operation Mode</b>	Configure VLAN Operation Mode: disable, Port Base, 802.1Q.
<b>GVRP Mode</b>	Enable/Disable GVRP function.
<b>Management VLAN ID</b>	Management VLAN provides the network administrator a secure VLAN to manage the switch. Only the devices in the management VLAN can access the switch.
<b>Link type</b>	<p>There are 3 link types:</p> <p><b>Access Link:</b> single switch only, allows the grouping of ports by setting the same VID.</p> <p><b>Trunk Link:</b> extended application of <b>Access Link</b>, allows the grouping of ports by setting the same VID with 2 or more switches.</p> <p><b>Hybrid Link:</b> Both <b>Access Link</b> and <b>Trunk Link</b> are available.</p> <p><b>Hybrid (QinQ) Link:</b> enable QinQ mode, allows the insertion of one</p>

	more VLAN tag in an original VLAN frame.
<b>Untagged VID</b>	Set the port default VLAN ID for untagged devices that connect to the port. The range is 1 to 4094.
<b>Tagged VIDs</b>	Set the tagged VIDs to carry different VLAN frames to other switches.
<b>Apply</b>	Click <b>“Apply”</b> to activate the configurations.
<b>Help</b>	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 Setting

VLAN Operation Mode : Port Based ▼

#### Port Based VLAN List

is5\_\_1 ▲

▼

Add Edit Delete Help

#### VLAN Configuration – Port Base interface-1

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

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

## VLAN Setting

VLAN Operation Mode : Port Based ▼

Group Name

VLAN ID

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

Add  
Remove

VLAN Configuration – Port Base interface-2

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

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

### 5.1.9 SNMP

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, 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

**SNMP Agent Version:**

SNMPV1/V2c ▼

Apply

Help

### SNMP V1/V2c Community

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

Apply

**SNMPv3 Engine ID: 86a0000003e8e875000000**

### SNMPv3 User

User Name	
Auth Password	
Privacy Password	
<div> Add Remove </div>	

### Current SNMPv3 User Profile

User Name	Auth. Password	Priv. Password
-----------	----------------	----------------

SNMP Agent Setting interface

The following table describes the SNMP Agent Setting interface page.

Label	Description
<b>SNMP agent Version</b>	Three SNMP versions are supported such as SNMP V1/SNMP V2c, and SNMP V3. SNMP V1/SNMP V2c agent use a community string match for authentication, 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.
<b>SNMP V1/V2c Community</b>	SNMP Community should be set for SNMP V1/V2c. Four sets of "Community String/Privilege" are supported. Each Community String is a maximum of 32 characters. Keep empty to remove this Community string.
<b>SNMPv3User</b>	If SNMP V3 agent is selected, the SNMPv3 profiled should be set for authentication. The Username is necessary. The Auth. Password is

	<p>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.</p> <p>When SNMP V3 agent is selected, it is possible to:</p> <ol style="list-style-type: none"> <li>1. Input SNMPv3 username only.</li> <li>2. Input SNMPv3 username and Auth Password.</li> <li>3. Input SNMPv3 username, Auth Password and Privacy Password, which can be different with Auth Password.</li> </ol> <p>To remove a current user profile:</p> <ol style="list-style-type: none"> <li>1. Input SNMPv3 user name to be removed.</li> <li>2. Click "<b>Remove</b>" button</li> </ol>
<b>Current SNMPv3 User Profile</b>	Show all SNMPv3 user profiles.
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.
<b>Help</b>	Show help file.

### 5.1.9.2 SNMP – Trap Setting

A trap manager is a management station that receives traps 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

### Trap Server Setting

Server IP	<input type="text"/>
Community	<input type="text"/>
Trap Version	<input checked="" type="radio"/> V1 <input type="radio"/> V2c
<b>Add</b>	

### Trap Server Profile

Server IP	Community	Trap Version
<div style="border: 1px solid gray; width: 100%; height: 100%;"></div>		
<b>Remove</b>		<b>Help</b>

SNMP Trap Setting interface

The following table describes the SNMP Trap Setting interface page.

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

### 5.1.10 Traffic Prioritization

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

### Policy

**QoS Mode :**

**QoS Policy :**

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

☐ Use a strict priority scheme

**Apply** **Help**

Policy Setting interface



The following table describes the Traffic Prioritization Policy interface page.

Label	Description
<b>QoS Mode</b>	<ul style="list-style-type: none"> <li>■ <b>Port-base:</b> the output priority is determined by ingress port.</li> <li>■ <b>COS only:</b> the output priority is determined by COS only.</li> <li>■ <b>TOS only:</b> the output priority is determined by TOS only.</li> <li>■ <b>COS first:</b> the output priority is determined first by COS and then by TOS.</li> <li>■ <b>TOS first:</b> the output priority is determined first by TOS and then by COS.</li> </ul>
<b>QoS policy</b>	<ul style="list-style-type: none"> <li>■ <b>Using the 8,4,2,1 weight fair queue scheme:</b> the output queues will follow 8:4:2:1 ratio to transmit packets from the highest to lowest queue. For example: 8 high queue packets, 4 middle queue packets, 2 low queue packets, and the one lowest queue packet are transmitted in one turn.</li> <li>■ <b>Use the strict priority scheme:</b> the packets in higher queue will always be transmitted first until a higher queue is empty.</li> </ul>
<b>Help</b>	Show help file.
<b>Apply</b>	Click “ <b>Apply</b> ” to activate the configurations.

## Port-based Priority

Port No.	Priority
Port.01	Lowest ▼
Port.02	Lowest ▼
Port.03	Lowest ▼
Port.04	Lowest ▼
Port.05	Lowest ▼
Port.06	Lowest ▼
Port.07	Lowest ▼
G1	Lowest ▼
G2	Lowest ▼
G3	Lowest ▼

Apply Help

Port-based Priority interface

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

## COS/802.1p

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

## COS Port Default

Port No.	COS
Port.01	0
Port.02	0
Port.03	0
Port.04	0
Port.05	0
Port.06	0
Port.07	0
G1	0
G2	0
G3	0

COS/802.1p interface

Label	Description
<b>COS/802.1p</b>	COS (Class Of Service) is well known as 802.1p. It describes that the output priority of a packet is determined by 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.
<b>COS Port Default</b>	When an ingress packet does not have a VLAN tag, a default priority value is considered and determined by the ingress port.
<b>Help</b>	Show help file.
<b>Apply</b>	Click “ <b>Apply</b> ” to activate the configurations.

## TOS/DSCP

DSCP	0	1	2	3	4	5	6	7
Priority	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
DSCP	8	9	10	11	12	13	14	15
Priority	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
DSCP	16	17	18	19	20	21	22	23
Priority	Low ▾	Low ▾	Low ▾	Low ▾	Low ▾	Low ▾	Low ▾	Low ▾
DSCP	24	25	26	27	28	29	30	31
Priority	Low ▾	Low ▾	Low ▾	Low ▾	Low ▾	Low ▾	Low ▾	Low ▾
DSCP	32	33	34	35	36	37	38	39
Priority	Middle ▾	Middle ▾	Middle ▾	Middle ▾	Middle ▾	Middle ▾	Middle ▾	Middle ▾
DSCP	40	41	42	43	44	45	46	47
Priority	Middle ▾	Middle ▾	Middle ▾	Middle ▾	Middle ▾	Middle ▾	Middle ▾	Middle ▾
DSCP	48	49	50	51	52	53	54	55
Priority	High ▾	High ▾	High ▾	High ▾	High ▾	High ▾	High ▾	High ▾
DSCP	56	57	58	59	60	61	62	63
Priority	High ▾	High ▾	High ▾	High ▾	High ▾	High ▾	High ▾	High ▾



TOS/DSCP interface

Label	Description
<b>TOS/DSCP</b>	TOS (Type of Service) is a field in 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.
<b>Apply</b>	Click “ <b>Apply</b> ” to activate the configurations.
<b>Help</b>	Show help file.

## 5.1.11 Multicast

### 5.1.11.1 IGMP Snooping

Internet Group Management Protocol (IGMP) is used by IP hosts to register their dynamic multicast group membership. IGMP has 3 versions, IGMP v1, v2 and v3. Please refer to RFC 1112, 2236 and 3376. IGMP snooping 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

IGMP Snooping :

IGMP Query Mode:

#### IGMP Snooping Table

IP Address	VLAN ID	Member Port
239.255.255.250	1	*****G*
224.000.000.251	1	*****G*

IGMP Snooping interface

The following table describes the IGMP Snooping interface page.

Label	Description
<b>IGMP Snooping</b>	Enable (V2 or V3) or Disable IGMP snooping.
<b>IGMP Query Mode</b>	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.
<b>IGMP Snooping Table</b>	Show current IP multicast list
<b>Apply</b>	Click " <b>Apply</b> " to activate the configurations.
<b>Help</b>	Show help file.

### 5.1.11.2 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

IP Address

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

#### Multicast Filtering List

IP Address	Member Ports
224.000.000.002	*****6****
224.000.000.001	*23*****

Multicast Filtering interface

The following table describes the Multicast Filtering interface page.

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

## 5.1.12 Security

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

IP Security Mode: Disable ▾

- ☒ Enable WEB Management
- ☒ Enable Telnet Management
- ☒ Enable SNMP Management

#### Secure IP List

Secure IP1	0.0.0.0
Secure IP2	0.0.0.0
Secure IP3	0.0.0.0
Secure IP4	0.0.0.0
Secure IP5	0.0.0.0
Secure IP6	0.0.0.0
Secure IP7	0.0.0.0
Secure IP8	0.0.0.0
Secure IP9	0.0.0.0
Secure IP10	0.0.0.0

Apply Help

IP Security interface

The following table describes the IP Security interface page.

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

<b>Apply</b>	Click “ <b>Apply</b> ” to activate the configurations.
<b>Help</b>	Show help file.

### 5.1.12.2 Port Security

Port security 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

MAC Address

Port No.

Port.03

Add

Delete

Help

## Port Security List

MAC Address	Port

### Port Security interface

The following table describes the Port Security interface page.

Label	Description
<b>MAC Address</b>	Input MAC Address of a specific port.
<b>Port No.</b>	Select switch port.
<b>Add</b>	Add MAC and port information to the Port Security List.
<b>Delete</b>	Delete the entry.
<b>Help</b>	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

MAC Address

\_\_\_\_\_

Add

Delete

Help



MAC Address

## MAC Blacklist interface

The following table describes the MAC Blacklist interface page.

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

#### 5.1.12.4 802.1x

## 802.1x - Radius Server

802.1x makes the use of the physical access characteristics of IEEE802 LAN 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

### Radius Server Setting

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

### Advanced Setting

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



802.1x Radius Server interface

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

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

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

## 802.1x - Port Authorized Mode

Set the 802.1x authorized mode of each port.

### 802.1x - Port Authorize Mode

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

Apply Help

802.1x Port Authorize interface

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

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

## 802.1x - Port Authorized State

Show 802.1x port authorized state.

### 802.1x - Port Authorize State

Port No.	Port Authorize State
Port.01	Accept
Port.02	Accept
Port.03	Accept
Port.04	Accept
Port.05	Accept
Port.06	Accept
Port.07	Accept
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
<b>Power Failure</b>	Check the box of PWR 1 or PWR 2 to monitor.
<b>Port Link Down/Broken</b>	Check the box of port 1 to port 10 to monitor.
<b>Apply</b>	Click “ <b>Apply</b> ” to activate the configurations.
<b>Help</b>	Show help file.

### 5.1.13.2 System Alarm

System alarm 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

System Warning – SYSLOG Setting interface

The following table describes the SYSLOG Setting interface page.

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

#### System Warning – SMTP Setting

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

## System Warning - SMTP Setting

E-mail Alert :

SMTP Server Address	<input type="text" value="0.0.0.0"/>
Sender E-mail Address	<input type="text" value="administrator"/>
Mail Subject	<input type="text" value="Automated Email Alert"/>
<input type="checkbox"/> Authentication	
Recipient E-mail Address 1	<input type="text"/>
Recipient E-mail Address 2	<input type="text"/>
Recipient E-mail Address 3	<input type="text"/>
Recipient E-mail Address 4	<input type="text"/>
Recipient E-mail Address 5	<input type="text"/>
Recipient E-mail Address 6	<input type="text"/>

System Warning – SMTP Setting interface

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

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

### System Warning – Event Selection

SYSLOG and SMTP are the two warning methods that 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

### System Event

Event	SYSLOG	SMTP
System Cold Start	<input type="checkbox"/>	<input type="checkbox"/>
Power Status	<input type="checkbox"/>	<input type="checkbox"/>
SNMP Authentication Failure	<input type="checkbox"/>	<input type="checkbox"/>
iRing Topology Change	<input type="checkbox"/>	<input type="checkbox"/>

### Port Event

Port No.	SYSLOG	SMTP
Port.01	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>
Port.02	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>
Port.03	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>
Port.04	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>
Port.05	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>
Port.06	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>
Port.07	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>
G1	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>
G2	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>
G3	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>



System Warning – Event Selection interface

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

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

## 5.1.14 Monitor and 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

**Port No :**

**Current MAC Address**

Dynamic Address Count : 0  
Static Address Count : 0

MAC Address Table interface

The following table describes the MAC Address Table interface page.

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

MAC Address Table Aging Time: (0~3825)  secs

☐ Auto Flush MAC Address Table When Ports Link Down

Apply

Help

MAC Address Aging interface

The following table describes the MAC Address Aging interface page.

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

### 5.1.14.3 Port Statistics

Port statistics show several statistics counters for all ports

## Port Statistics

Port	Type	Link	State	TX Good Packet	TX Bad Packet	RX Good Packet	RX Bad Packet	TX Abort Packet	Packet Collision
Port.01	100TX	Down	Enable	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0
Port.03	100TX	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
<b>Type</b>	Shows port speed and media type.
<b>Link</b>	Shows port link status.
<b>State</b>	Shows port enabled or disabled.
<b>TX GOOD Packet</b>	The number of good packets sent by this port.
<b>TX Bad Packet</b>	The number of bad packets sent by this port.
<b>RX GOOD Packet</b>	The number of good packets received by this port.
<b>RX Bad Packet</b>	The number of bad packets received by this port.
<b>TX Abort Packet</b>	The number of packets aborted by this port.
<b>Packet Collision</b>	The number of times a collision detected by this port.
<b>Clear</b>	Clear all counters.
<b>Help</b>	Show help file.

#### 5.1.14.4 Port Monitoring

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

Port	Destination Port		Source Port	
	RX	TX	RX	TX
Port.01	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.02	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.03	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.04	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.05	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.06	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.07	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
G1	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
G2	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
G3	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Port monitoring interface

The following table describes the Port Monitoring interface page.

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

#### 5.1.14.5 System Event Log

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

### System Event Log

The screenshot displays the 'System Event Log' interface. It features a scrollable text area containing two log entries: '2: Jan 1 01:52:45 : SYSLOG Server:0.0.0.0' and '1: Jan 1 01:52:45 : SYSLOG Enable!'. Below the scroll area is a 'Page.1' dropdown menu. At the bottom of the interface are three buttons: 'Reload', 'Clear', and 'Help'.

System Event Log interface

The following table describes the System Event Log interface page.

Label	Description
<b>Page</b>	Select LOG page.
<b>Reload</b>	Gets the newest event logs and refreshes the page.
<b>Clear</b>	Clear log.
<b>Help</b>	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.

#### Save Configuration



System Configuration interface

The following table describes the System Configuration interface page.

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


### 5.1.16 Factory Default

#### Factory Default

- ☒ Keep current IP address setting?
- ☒ Keep current username & password?



Factory Default interface

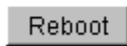
Reset switch to default configuration. Click  to reset all configurations to the default value.

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

Please click **[Reboot]** button to restart switch device.



System Reboot interface

# Command Line Interface Management (CLI)

## 6.1 About CLI Management

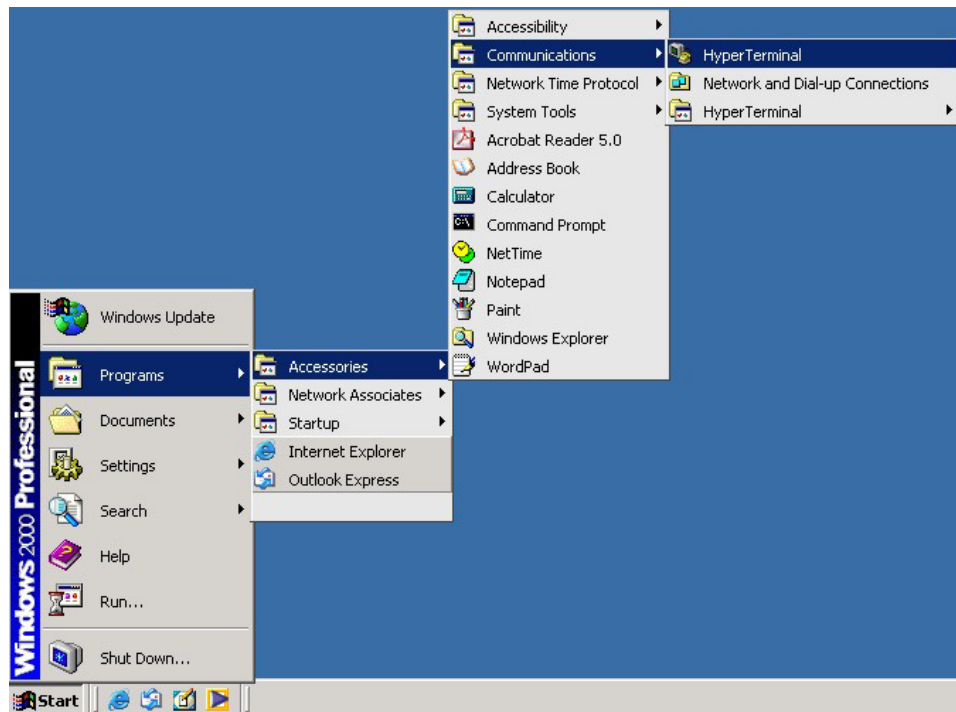
Besides WEB-based management, the iES10G(F) also supports CLI management. The console port or telnet can be used to configure the switch by the CLI.

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

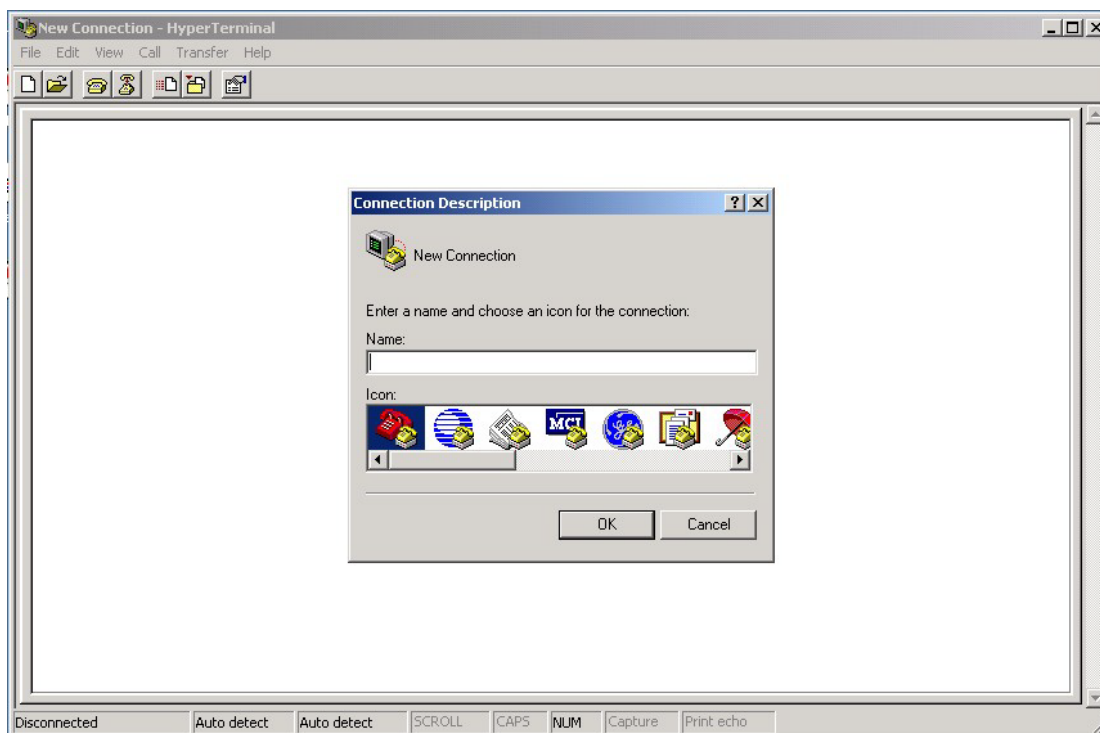
Use the RJ45 to DB9-F cable provided to connect the Switches RS-232 Console port to a PC's COM port.

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

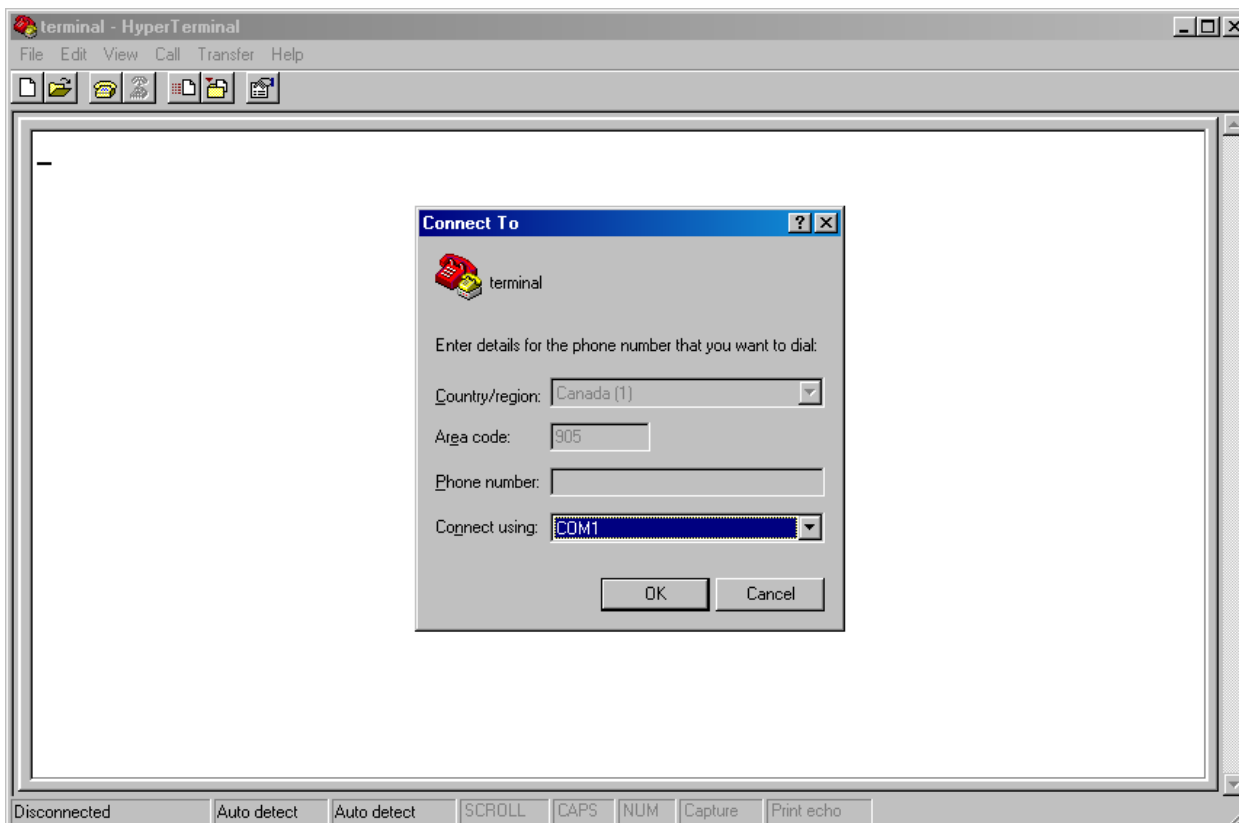
Step 1) From the Windows desktop, click on Start -> Programs -> Accessories -> Communications -> Hyper Terminal.



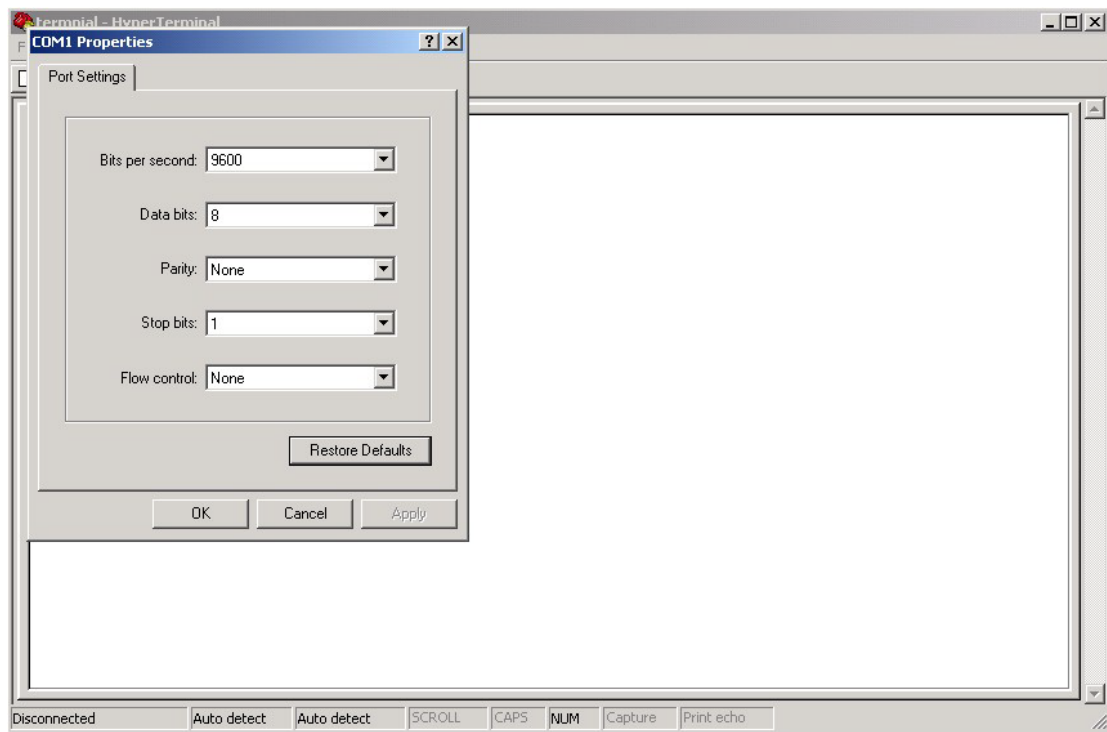
Step 2) Enter a name for the new connection.



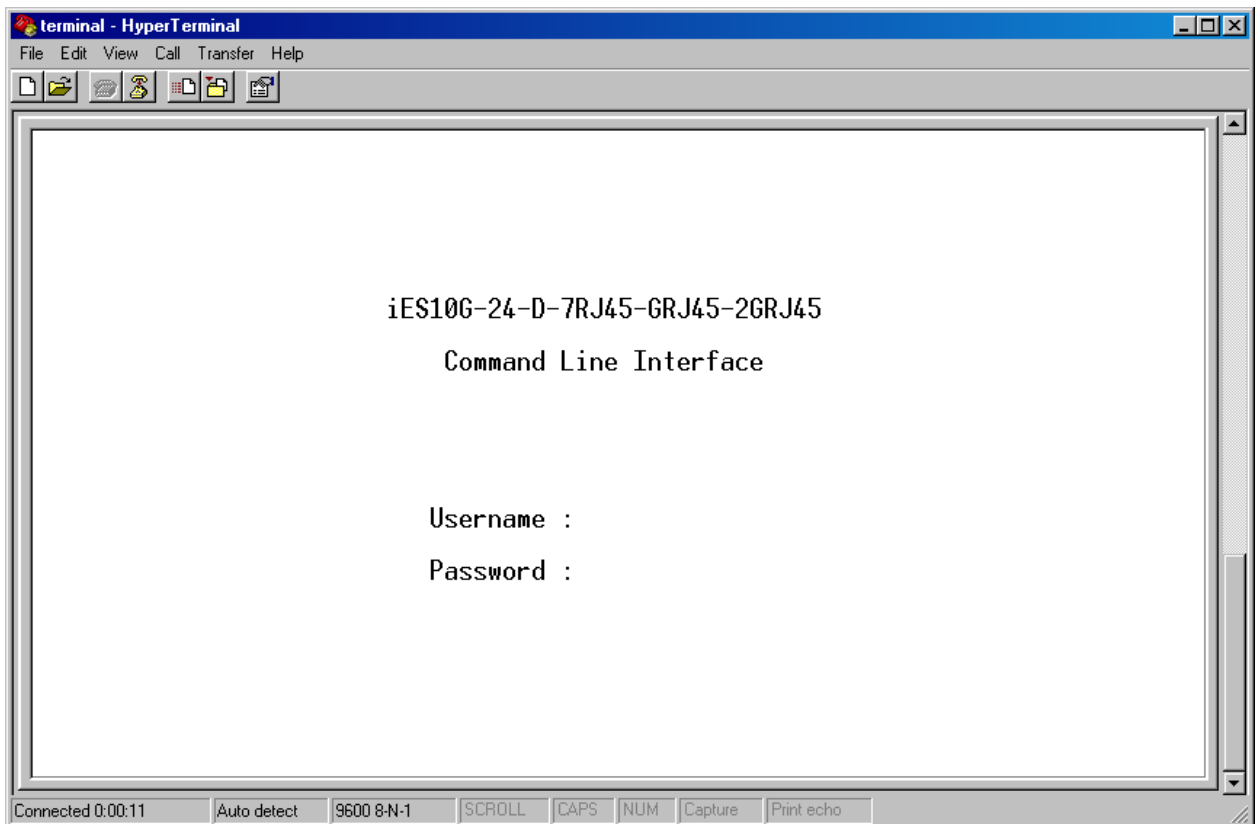
Step 3) Select appropriate COM port number



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**

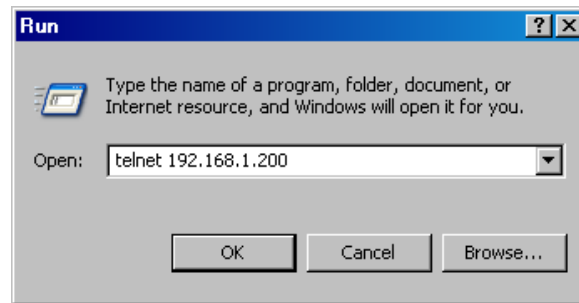
Default Gateway: **192.168.10.254**

User Name: **admin**

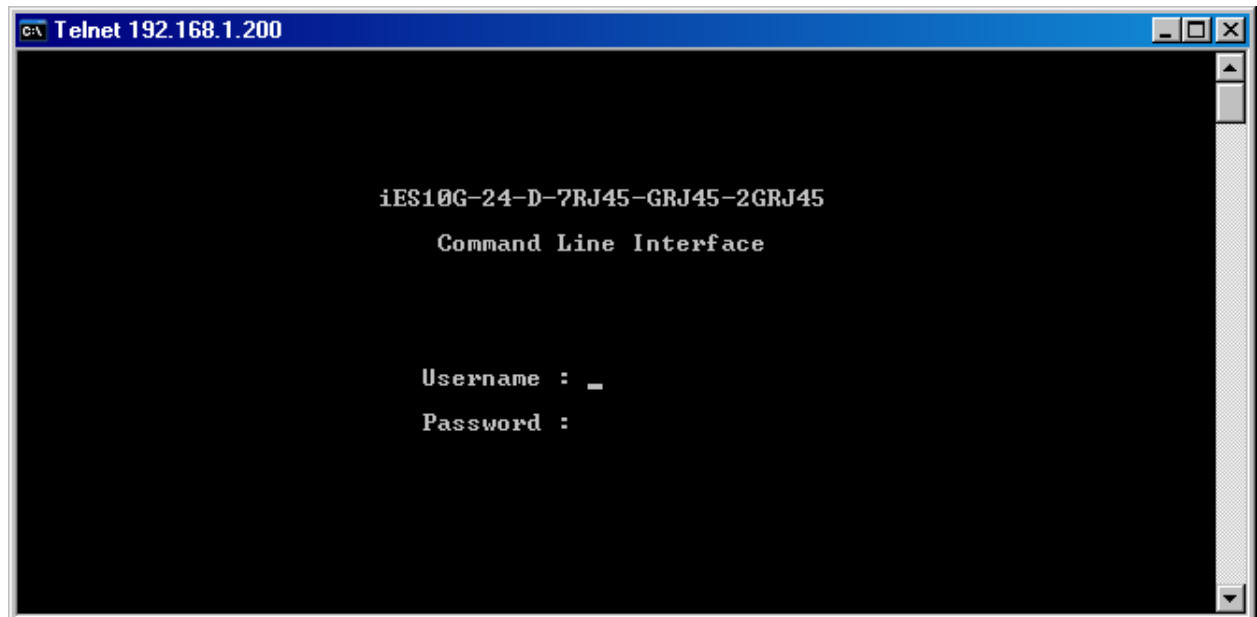
Password: **admin**

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 <b>logout</b> or <b>quit</b> .	The user command available at the level of user is the subset of those available at the privileged level. Use this mode to: <ul style="list-style-type: none"> <li>• Enter menu mode.</li> <li>• Display system information.</li> </ul>
Privileged EXEC	Enter the <b>enable</b> command while in user EXEC mode.	switch#	Enter <b>disable</b> to exit.	The privileged command is in advance mode. Privileged this mode to: <ul style="list-style-type: none"> <li>• Display advance function status</li> <li>• save configures</li> </ul>
Global configuration	Enter the <b>configure</b> command while in privileged EXEC mode.	switch(con fig)#	To exit to privileged EXEC mode, enter <b>exit</b> or <b>end</b>	Use this mode to configure parameters that apply to the Switch as a whole.
VLAN database	Enter the <b>vlan database</b> command while in privileged EXEC mode.	switch(vlan)#	To exit to user EXEC mode, enter <b>exit</b> .	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the <b>interface</b> command (with a specific interface)while in global configuration mode	switch(con fig-if)#	To exit to global configuration mode, enter <b>exit</b> . To exist privileged EXEC mode or <b>end</b> .	Use this mode to configure parameters for the switch and Ethernet ports.

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

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

<b>no security telnet</b>	<b>G</b>	Disable IP security of telnet server	switch(config)#no security telnet
---------------------------	----------	--------------------------------------	-----------------------------------

### 6.3 Commands Set List—Port Commands Set

iES10G(F) Commands	Level	Description	Example
<b>interface fastEthernet</b> [Portid]	<b>G</b>	Choose the port for modification.	switch(config)#interface fastEthernet 2
<b>duplex</b> [full   half]	<b>I</b>	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
<b>speed</b> [10 100 1000 auto]	<b>I</b>	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
<b>flowcontrol mode</b> [Symmetric Asymmetric]	<b>I</b>	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion.	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol mode Asymmetric
<b>no flowcontrol</b>	<b>I</b>	Disable flow control of interface	switch(config-if)#no flowcontrol
<b>security enable</b>	<b>I</b>	Enable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#security enable
<b>no security</b>	<b>I</b>	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
<b>bandwidth type all</b>	<b>I</b>	Set interface ingress limit frame type to "accept all frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
<b>bandwidth type broadcast-multicast-flooded-unicast</b>	<b>I</b>	Set interface ingress limit frame type to "accept broadcast, multicast, and flooded unicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast

<b>bandwidth type</b> <b>broadcast-multicast</b>	I	Set interface ingress limit frame type to “accept broadcast and multicast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast
<b>bandwidth type</b> <b>broadcast-only</b>	I	Set interface ingress limit frame type to “only accept broadcast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only
<b>bandwidth in</b> [Value]	I	Set interface input bandwidth. Rate Range is from 100 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
<b>bandwidth out</b> [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
<b>show bandwidth</b>	I	Show interfaces bandwidth control	switch(config)#interface fastEthernet 2 switch(config-if)#show bandwidth
<b>state</b> [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
<b>show interface configuration</b>	I	show interface configuration status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface configuration
<b>show interface status</b>	I	show interface actual status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface status
<b>show interface accounting</b>	I	show interface statistic counter	switch(config)#interface fastEthernet 2 switch(config-if)#show interface accounting

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

#### 6.4 Commands Set List—Trunk command set

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

## 6.5 Commands Set List—VLAN command set

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

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

## 6.6 Commands Set List—Spanning Tree command set

iES10G(F) Commands	Level	Description	Example
<b>spanning-tree enable</b>	<b>G</b>	Enable spanning tree	switch(config)#spanning-tree enable
<b>spanning-tree priority</b> [0to61440]	<b>G</b>	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
<b>spanning-tree max-age</b> [seconds]	<b>G</b>	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)# spanning-tree max-age 15
<b>spanning-tree hello-time</b> [seconds]	<b>G</b>	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
<b>spanning-tree forward-time</b>	<b>G</b>	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
<b>stp-path-cost</b> [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
<b>stp-path-priority</b> [Port Priority]	I	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-path-priority 127
<b>stp-admin-p2p</b> [Auto   True   False]	I	Admin P2P of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-p2p Auto
<b>stp-admin-edge</b> [True   False]	I	Admin Edge of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-edge True
<b>stp-admin-non-stp</b> [True   False]	I	Admin NonSTP of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-non-stp False
<b>Show spanning-tree</b>	E	Display a summary of the spanning-tree states.	switch>show spanning-tree

<b>no spanning-tree</b>	<b>G</b>	Disable spanning-tree.	switch(config)#no spanning-tree
-------------------------	----------	------------------------	---------------------------------

## 6.7 Commands Set List—QoS command set

iES10G(F) Commands	Level	Description	Example
<b>qos policy</b> [weighted-fair   strict]	<b>G</b>	Select QoS policy scheduling	switch(config)#qos policy weighted-fair
<b>qos prioritytype</b> [port-based   cos-only   tos-only   cos-first   tos-first]	<b>G</b>	Setting of QoS priority type	switch(config)#qos prioritytype
<b>qos priority portbased</b> [Port] [lowest   low   middle   high]	<b>G</b>	Configure Port-based Priority	switch(config)#qos priority portbased 1 low
<b>qos priority cos</b> [Priority][lowest   low   middle   high]	<b>G</b>	Configure COS Priority	switch(config)#qos priority cos 22 middle
<b>qos priority tos</b> [Priority][lowest   low   middle   high]	<b>G</b>	Configure TOS Priority	switch(config)#qos priority tos 3 high
<b>show qos</b>	<b>P</b>	Display the information of QoS configuration	switch#show qos
<b>no qos</b>	<b>G</b>	Disable QoS function	switch(config)#no qos

## 6.8 Commands Set List—IGMP command set

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

<b>no igmp</b>	<b>G</b>	Disable IGMP snooping function	switch(config)#no igmp
<b>no igmp-query</b>	<b>G</b>	Disable IGMP query	switch#no igmp-query

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

iES10G(F) Commands	Level	Description	Example
<b>mac-address-table static</b> <b>hwaddr</b> [MAC]	<b>I</b>	Configure MAC address table of interface (static).	switch(config)#interface fastEthernet 2 switch(config-if)#mac-address-table static hwaddr 000012345678
<b>mac-address-table filter</b> <b>hwaddr</b> [MAC]	<b>G</b>	Configure MAC address table(filter)	switch(config)#mac-address-table filter hwaddr 000012348678
<b>show mac-address-table</b>	<b>P</b>	Show all MAC address table	switch#show mac-address-table
<b>show mac-address-table static</b>	<b>P</b>	Show static MAC address table	switch#show mac-address-table static
<b>show mac-address-table filter</b>	<b>P</b>	Show filter MAC address table.	switch#show mac-address-table filter
<b>no mac-address-table static</b> <b>hwaddr</b> [MAC]	<b>I</b>	Remove an entry of MAC address table of interface (static)	switch(config)#interface fastEthernet 2 switch(config-if)#no mac-address-table static hwaddr 000012345678
<b>no mac-address-table filter</b> <b>hwaddr</b> [MAC]	<b>G</b>	Remove an entry of MAC address table (filter)	switch(config)#no mac-address-table filter hwaddr 000012348678
<b>no mac-address-table</b>	<b>G</b>	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
<b>snmp agent-mode</b> [v1v2c   v3]	<b>G</b>	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2c
<b>snmp-server host</b> [IP address]	<b>G</b>	Configure SNMP server host information and	switch(config)#snmp-server host 192.168.10.50 community public

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

## 6.11 Commands Set List—Port Mirroring command set

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

<b>monitor</b> [RX TX Both]	I	Configure source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#monitor RX
<b>show monitor</b>	I	Show port monitor information	switch(config)#interface fastEthernet 2 switch(config-if)#show monitor
<b>no monitor</b>	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
<b>8021x enable</b>	G	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
<b>8021x system radiusip</b> [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
<b>8021x system serverport</b> [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
<b>8021x system accountport</b> [port ID]	G	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# 8021x system accountport 1816
<b>8021x system sharekey</b> [ID]	G	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# 8021x system sharekey 123456
<b>8021x system nasid</b> [words]	G	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# 8021x system nasid test1

<b>8021x misc quietperiod</b> [sec.]	<b>G</b>	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# 8021x misc quietperiod 10
<b>8021x misc txperiod</b> [sec.]	<b>G</b>	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# 8021x misc txperiod 5
<b>8021x misc supportimeout</b> [sec.]	<b>G</b>	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# 8021x misc supportimeout 20
<b>8021x misc servertimeout</b> [sec.]	<b>G</b>	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#8021x misc servertimeout 20
<b>8021x misc maxrequest</b> [number]	<b>G</b>	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# 8021x misc maxrequest 3
<b>8021x misc reauthperiod</b> [sec.]	<b>G</b>	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# 8021x misc reauthperiod 3000
<b>8021x portstate</b> [disable   reject   accept   authorize]	<b>I</b>	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch(config)#interface fastethernet 3 switch(config-if)#8021x portstate accept
<b>show 8021x</b>	<b>P</b>	Display a summary of the 802.1x properties and also the port sates.	switch#show 8021x
<b>no 8021x</b>	<b>G</b>	Disable 802.1x function	switch(config)#no 8021x

### 6.13 Commands Set List—TFTP command set

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

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

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

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

## 6.15 Commands Set List—SNTP command set

iES10G(F) Commands	Level	Description	Example
<b>sntp enable</b>	<b>G</b>	Enable SNTP function	switch(config)#sntp enable
<b>sntp daylight</b>	<b>G</b>	Enable daylight saving time, if SNTP function is	switch(config)#sntp daylight



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

## 6.16 Commands Set List—iRing command set

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

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

# Technical Specifications

<b>Model Number iES10G/iES10GF</b>	
<b>Physical Ports</b>	
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
<b>Technology</b>	
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

	<p>Supports Q-in-Q VLAN for performance &amp; security to expand the VLAN space</p> <p>Radius centralized password management</p> <p>SNMP v1/v2c/v3 encrypted authentication and access security</p>
Software Features	<p>STP/RSTP/MSTP (IEEE 802.1D/w/s)</p> <p>Redundant Ring (iRing) with recovery time less than 20ms up to 250 units</p> <p>TOS/Diffserv supported</p> <p>Quality of Service (802.1p) for real-time traffic</p> <p>VLAN (802.1Q) with VLAN tagging and GVRP supported</p> <p>IGMP Snooping for multicast filtering</p> <p>Port configuration, status, statistics, monitoring, security</p> <p>SNTP for synchronizing of clocks over network</p> <p>Supports PTP Client (Precision Time Protocol) clock synchronization</p> <p>DHCP Server / Client support</p> <p>Port Trunk support</p> <p>MVR (Multicast VLAN Registration) support</p>
Network Redundancy	iRing, iBridge, STP, RSTP, MSTP
Warning / Monitoring System	<p>Relay output for fault event alarming</p> <p>Syslog server / client to record and view events</p> <p>SMTP for event warning notification via email</p> <p>Event selection support</p>
RS-232 Serial Console Port	RS-232 in RJ45 connector with console cable. 9600bps, 8, N, 1
<b>Fault Contact</b>	
Relay	Relay output capacity: 1A at 24VDC
<b>Power</b>	
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.)	<p>iES10G - 12 Watts Max</p> <p>iES10GF - 20 Watts Max.</p>
Overload Current Protection	Present
Reverse Polarity Protection	Internal
<b>Physical Characteristic</b>	
Enclosure	IP-40 Galvanized Steel Housing
Dimension (W x D x H)	<p>iES10G - 101.6 mm(W)x 109.2 mm(D)x 153.8 mm(H) (4x4.3 x 6.05 inch)</p> <p>iES10GF – 101.8(W)x163.2(D)x153.6(H) mm (4 x 6.43 x 6.05 inch)</p>
Weight (g)	iES10G – 1.1 kg

	iES10GF - 1.2 kg
<b>Environmental</b>	
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
<b>Regulatory Approvals</b>	
Regulatory Approvals	FCC Part 15, CISPER (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS) EN61000-4-8, EN61000-4-11
Shock	IEC 60068-2-27
Free Fall	IEC 60068-2-32
Vibration	IEC 60068-2-6
Safety	EN60950-1
<b>Warranty</b>	
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