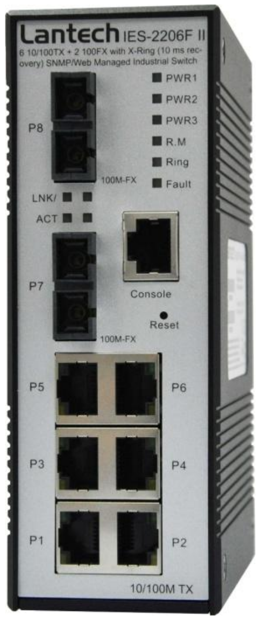
Lantech

IES-2206F-II

6 10/100TX + 2 100FX

Industrial Management Switch

User's Manual



Version 1.1

September, 2009.

Table of Content

1

Getting to Know Your Switch

1.1 About the IES-2206F-II Industrial Switch

The IES-2206F-II are powerful managed industrial switches which have many features. These switches can work under wide temperature, dusty environment and humid condition. They can be managed by WEB, TELNET, Console or other third-party SNMP software as well. Besides, these switches can be managed by a Windows utility that we called Lantech-VIEW.

Lantech-VIEW is powerful network management software. With its friendly and powerful interface, you can easily configure multiple switches at the same time, and monitor switches' status. **(The free version of Lantech – View can monitor up to 10 switches)**

1.2 Software Features

- World's fastest Redundant Ethernet Ring (Recovery time < 10ms over 250 units connection)
- Supports Coupling Ring, Dual Homing, RSTP over X-Ring
- Supports SNMPv1/v2/v3 & RMON & Port base/802.1Q VLAN Network Management
- Event notification by Email, SNMP trap and Relay Output
- Web-based ,Telnet, Console, CLI configuration
- Enable/disable ports, MAC based port security
- Port based network access control (802.1x)
- 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

- Redundant three DC power inputs (two on terminal block & one on power jack)
- Operating Temperature: -20 to 60^{o}C (Wide temperature model: -40 to 75 ^{o}C)
- Storage Temperature: -20 to 85 ^{o}C
- Operating Humidity: 5% to 95%, non-condensing
- Casing: IP-30
- 10/100Base-T(X) Ethernet port
- 100Base-FX Fiber port
- Console Port
- Dimensions(W x D x H) : 52 mm(W)x 106 mm(D)x 144 mm(H)

2

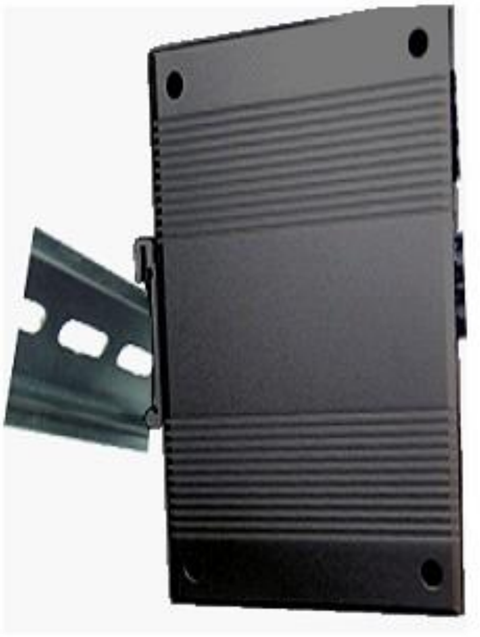
Hardware Installation

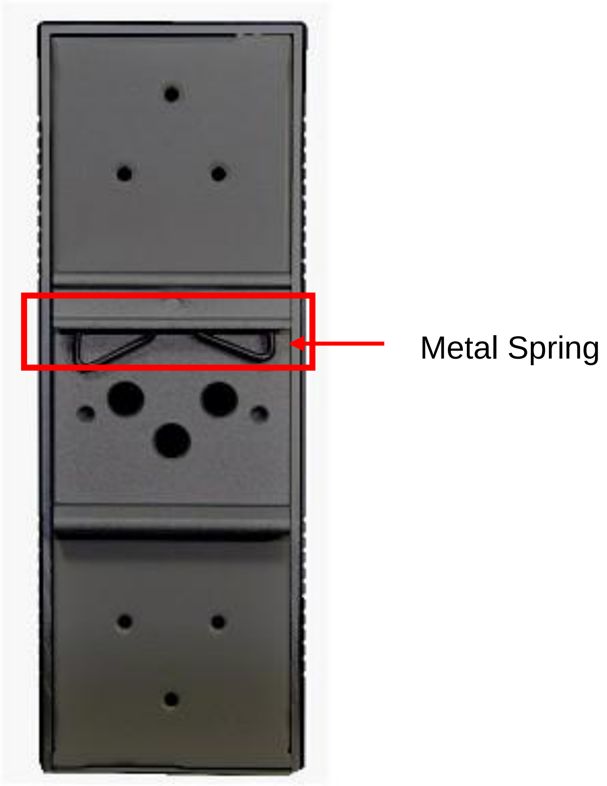
2.1 Installation Switch on DIN-Rail

Each switch has a Din-Rail kit on rear panel. The Din-Rail kit helps switch to fix on the Din-Rail. It is easy to install the switch on the Din-Rail:

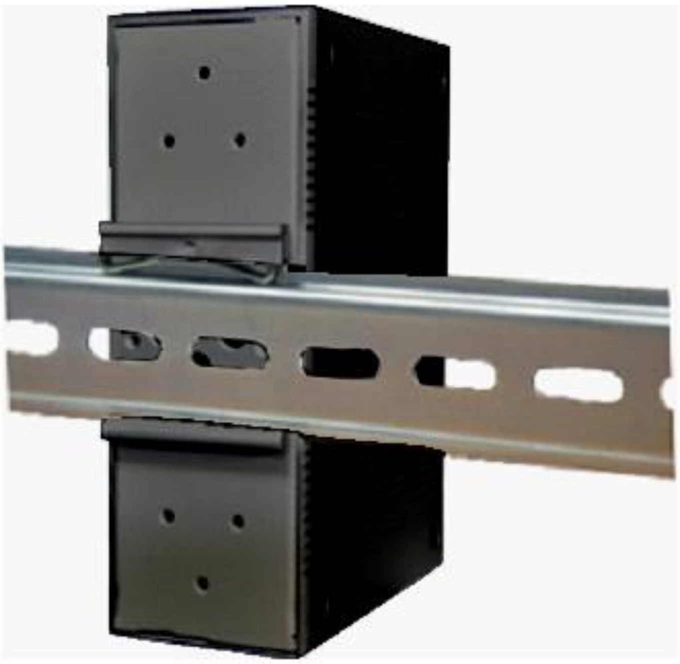
2.1.1 Mount IES-2206F-II on DIN-Rail

Step 1: Slant the switch and mount the metal spring to Din-Rail.





Step 2: Push the switch toward the Din-Rail until you heard a “click” sound.

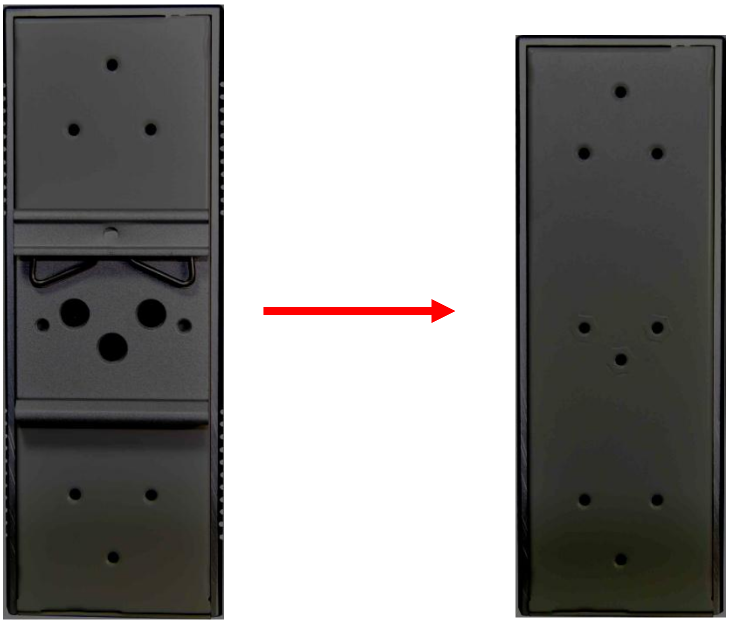


2.2 Wall Mounting Installation

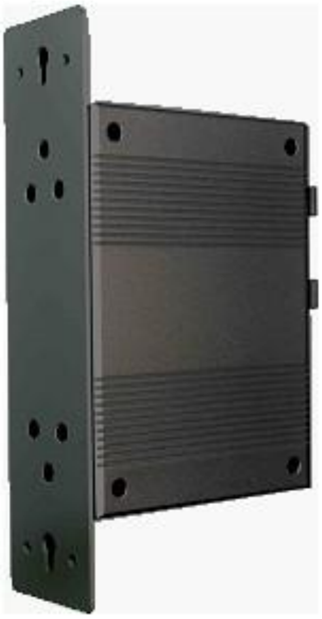
Each switch has another installation method for users to fix the switch. A wall mount panel can be found in the package. The following steps show how to mount the switch on the wall:

2.2.1 Mount IES-2206F-II on wall

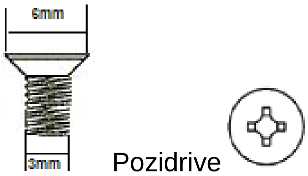
Step 1: Remove Din-Rail kit.



Step 2: Use 6 screws that can be found in the package to combine the wall mount panel. Just like the picture shows below:



The screws specification shows in the following two pictures. In order to prevent switches from any damage, the screws should not larger than the size that used in IES-2206F-II switches.



Step 3: Mount the combined switch on the wall.

3

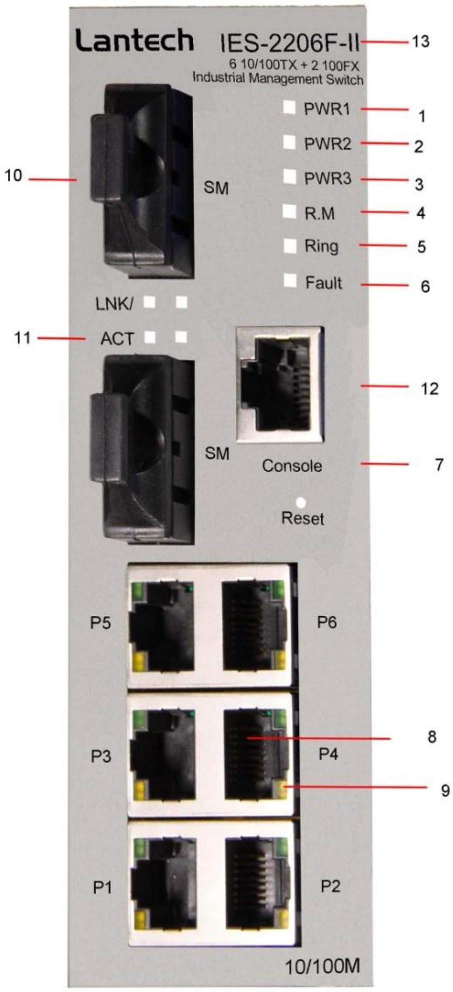
Hardware Overview

3.1 Front Panel

The following table describes the labels that stick on the IES-2206F-II.

Port	Description
10/100 RJ-45 fast Ethernet ports	6 10/100Base-T(X) RJ-45 fast Ethernet ports support auto-negotiation. Default Setting : Speed: auto Duplex: auto Flow control : disable
Fiber port	100BaseFX for IES-2206F II Series
Console	Use RS-232 with RJ-45 connecter to manage switch.
Reset	Push reset bottom 2 to 3 seconds to reset the switch. Push reset bottom 5 second to reset the switch into **Factory Default.**

IES-2206F-II



1. LED for PWR1. When the PWR1 links, the green led will be light on.
2. LED for PWR2. When the PWR2 links, the green led will be light on.
3. LED for PWR3. When the PWR3 links, the green led will be light on.
4. LED for R.M (Ring master). When the LED light on, it means that the switch is the ring master of X-Ring.
5. LED for Ring. When the led light on, it means the X-Ring is activated.
6. LED for Fault Relay. When the fault occurs, the amber LED will be light on.
7. Reset bottom. Push the bottom 3 seconds for reset; 5 seconds for factory default.
8. 10/100Base-T(X) Ethernet ports..
9. LED for Ethernet ports status.
10. 100BaseFX fiber port.
11. LED for fiber port.
12. Console port (RJ-45).
13. Model name

3.2 Front Panel LEDs

LED	Color	Status	Description
PW1	Green	On	DC power module 1 activated.
PW2	Green	On	DC power module 2 activated.
PW3	Green	On	Power jack activated.
R.M	Green	On	X-Ring Master.
Ring	Green	On	X-Ring enabled.
		Slowly blinking	X-Ring has only One link. (lack of one link to build the ring.)
		Fast blinking	X-Ring work normally.
Fault	Amber	On	Fault relay. Power failure or Port down/fail.
10/100Base-T(X) Fast Ethernet ports			
LNK	Green	On	Port link up.
ACT	Green	Blinking	Data transmitted.
Full Duplex	Amber	On	Port works under full duplex.
Fiber ports			
ACT	Green	Blinking	Data transmitted.
LNK	Amber	On	Port link up.

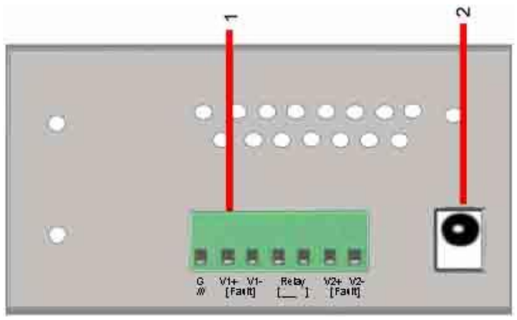
3.3 Bottom Panel

The bottom panel components of IES-2206F-II are showed as below:

1. Terminal block includes: PWR1, PWR2 (12-48V DC) and Relay output (1A@24VDC).
2. Power jack for PWR3 (12-45VDC).

PWR1, PWR2 (12-48V DC) and Relay output (1A@24VDC).

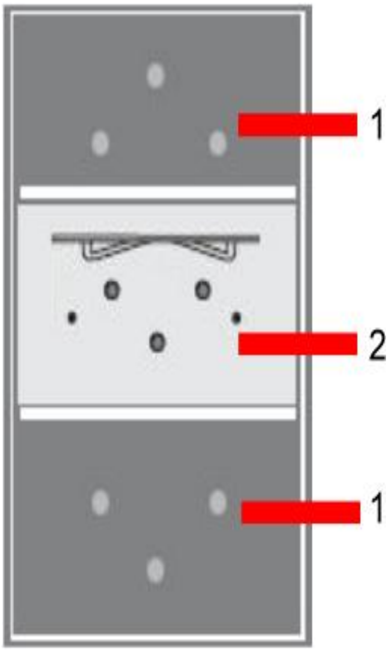
Power jack for PWR3 (12-45VDC)



3.4 Rear Panel

The rear panel components of IES-2206F-II are showed as below:

1. Screw holes for wall mount kit.
2. Din-Rail kit



4

Cables

4.1 Ethernet Cables

The IES-2206F-II switches have standard Ethernet ports. According to the link type, the switches use CAT 3, 4, 5,5e UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

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

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

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

RJ-45 Pin Assignments

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

The IES-2206F-II switches support auto MDI/MDI-X operation. You can use a straight-through cable to connect PC to switch. The following table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

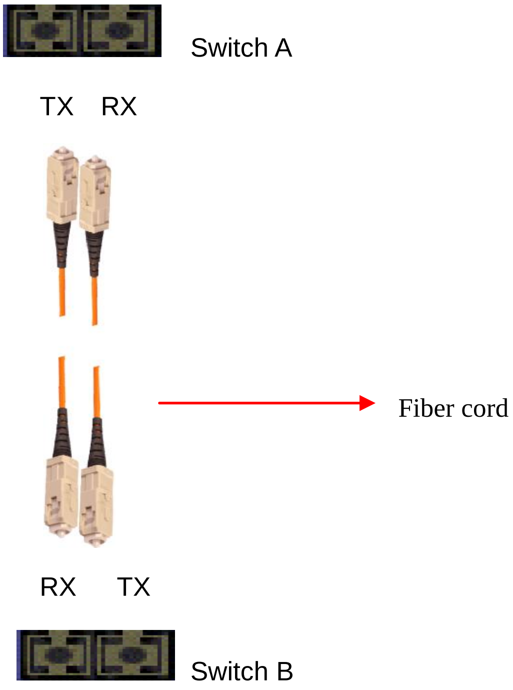
MDI/MDI-X pins assignment

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 Fibers

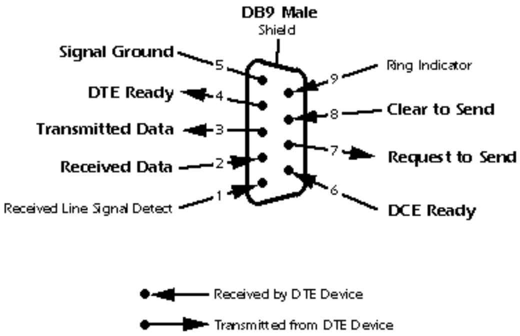
The fiber optical ports are in multi-mode (0 to 2 km, 1310 nm (50/125 µm, 62.5/125 µm) and single-mode with SC connector. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.

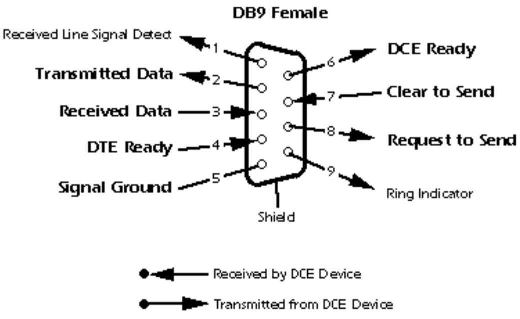


4.3 Console Cable

IES-2206F II Series switches can be management by console port. The DB-9 to RJ-45 cable can be found in the package. You can connect them to PC via a RS-232 cable with DB-9 female connector and the other end (RJ-45 connector) connects to console port of switch.

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





5

WEB Management

5.1 Configuration by Web Browser

This section introduces the configuration by Web browser.

5.1.1 About Web-based Management

Inside the CPU board of the switch, an embedded HTML web site resides in flash memory. It contains advanced management features and allows you to manage the switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 5.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

Note: By default, IE5.0 or later version does not allow Java Applets to open sockets. You need to explicitly modify the browser setting in order to enable Java Applets to use network ports.

Preparing for Web Management

The default value is as below:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

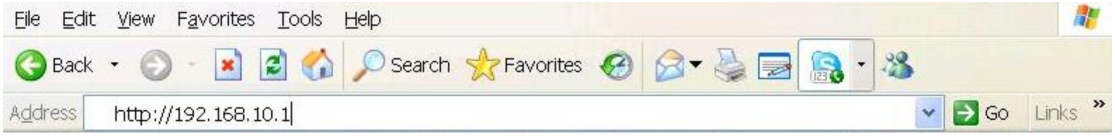
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

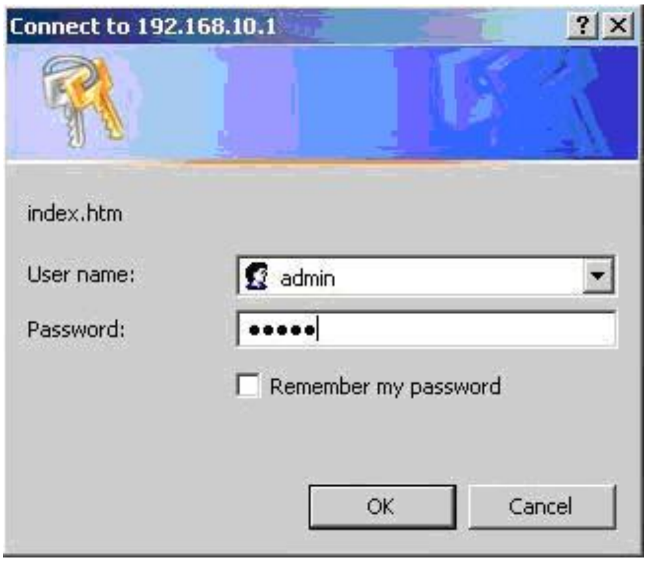
System Login

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



http://192.168.10.1

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



Connect to 192.168.10.1

index.htm

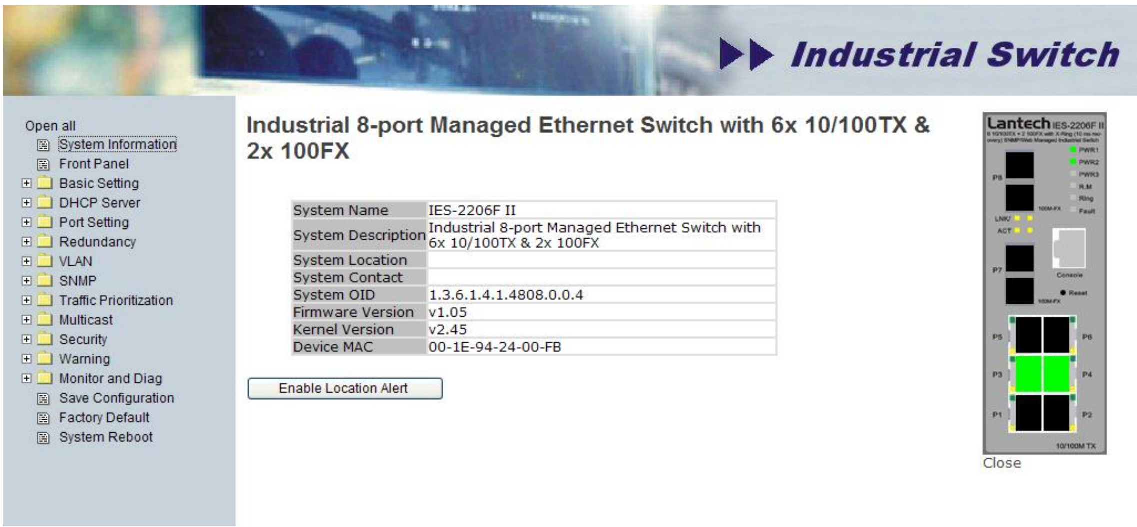
User name: admin

Password: ●●●●●

☐ Remember my password

Login screen

Main Interface



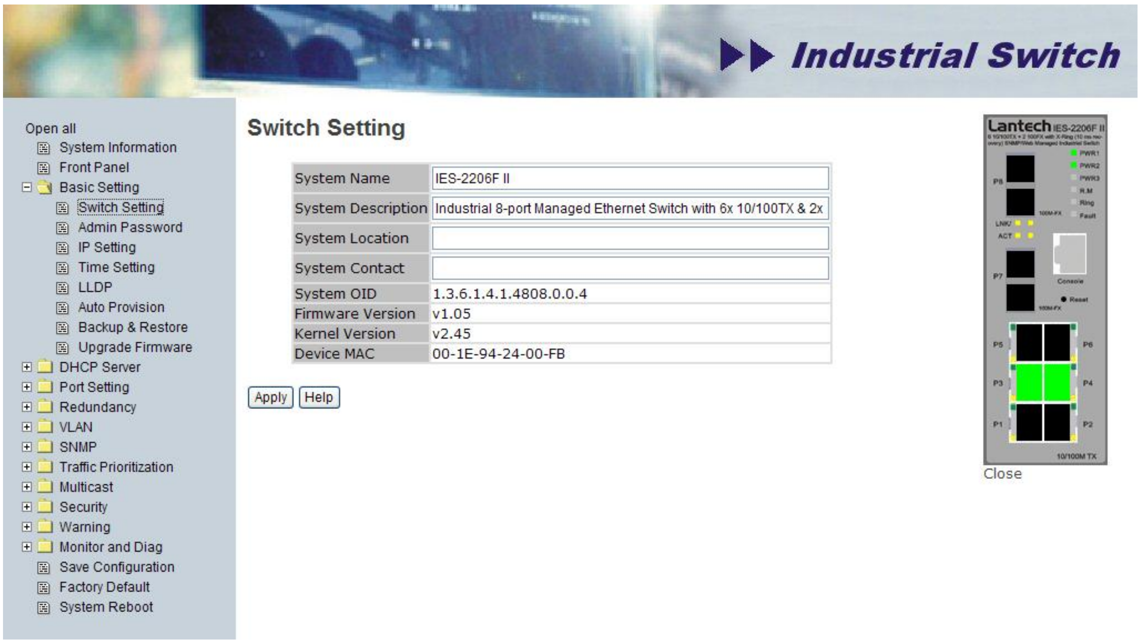
Industrial 8-port Managed Ethernet Switch with 6x 10/100TX & 2x 100FX

System Name	IES-2206F II
System Description	Industrial 8-port Managed Ethernet Switch with 6x 10/100TX & 2x 100FX
System Location	
System Contact	
System OID	1.3.6.1.4.1.4808.0.0.4
Firmware Version	v1.05
Kernel Version	v2.45
Device MAC	00-1E-94-24-00-FB

Main interface

5.1.2 Basic Setting

5.1.2.1 Switch setting



Switch Setting

System Name	IES-2206F II
System Description	Industrial 8-port Managed Ethernet Switch with 6x 10/100TX & 2x
System Location	
System Contact	
System OID	1.3.6.1.4.1.4808.0.0.4
Firmware Version	v1.05
Kernel Version	v2.45
Device MAC	00-1E-94-24-00-FB

Apply Help

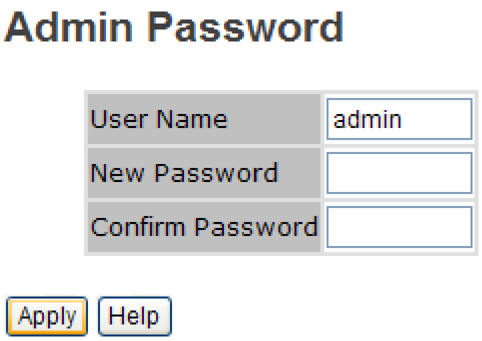
Switch setting interface

The following table describes the labels in this screen.

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

5.1.2.2 Admin Password

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



Admin Password

User Name	admin
New Password	
Confirm Password	

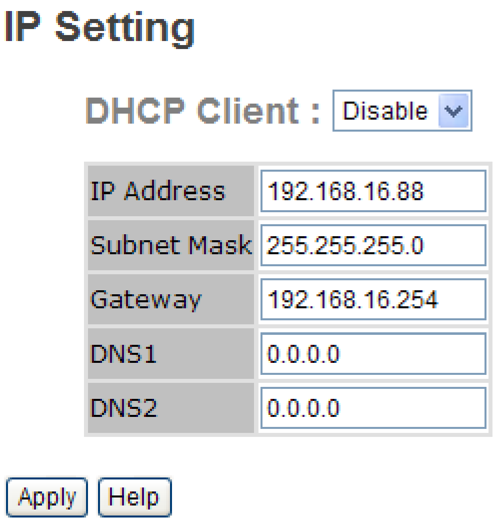
Admin Password interface

The following table describes the labels in this screen.

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

5.1.2.3 IP configuration

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



IP Setting

DHCP Client : Disable

IP Address	192.168.16.88
Subnet Mask	255.255.255.0
Gateway	192.168.16.254
DNS1	0.0.0.0
DNS2	0.0.0.0

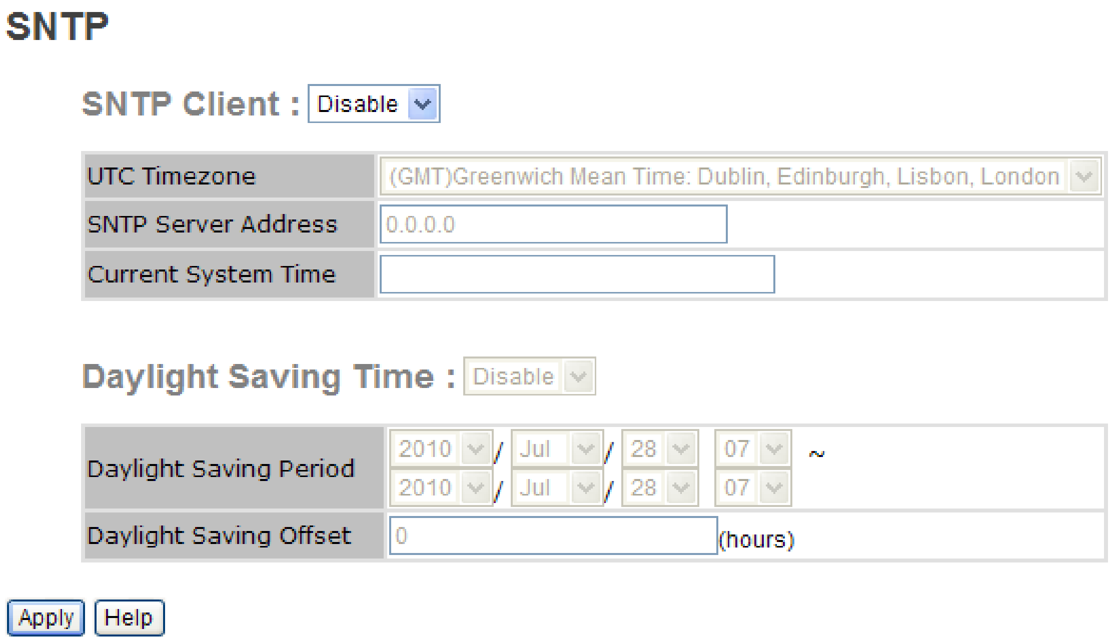
IP Configuration interface

The following table describes the labels in this screen.

Label	Description
DHCP Client	To enable or disable the DHCP client function. When DHCP client function is enabling, the switch will be assigned the IP address from the network DHCP server. The default IP address will be replaced by the IP address which the DHCP server has assigned. After clicking "**Apply**" button, a popup dialog show up up to inform the you when the DHCP client is enabling. The current IP will lose and you should find a new IP on the DHCP server.
IP Address	Assign the IP address that the network is using. If DHCP client function is enabling, you do not need to assign the IP address. The network DHCP server will assign the IP address for the switch and it will be display in this column. The default IP is 192.168.10.1
Subnet Mask	Assign the subnet mask of the IP address. If DHCP client function is enabling, you do not need to assign the subnet mask
Gateway	Assign the network gateway for the switch. The default gateway is 192.168.10.254
DNS1	Assign the primary DNS IP address
DNS2	Assign the secondary DNS IP address
Apply	Click "**Apply**" to set the configurations.

5.1.2.4 SNTP Configuration

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



SNTP

SNTP Client : Disable

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

Daylight Saving Time : Disable

Daylight Saving Period	2010 / Jul / 28 07 ~ 2010 / Jul / 28 07
Daylight Saving Offset	0 (hours)

SNTP Configuration interface

The following table describes the labels in this screen.

Label	Description
SNTP Client	Enable or disable SNTP function to get the time from the SNTP server.
Daylight Saving Time	Enable or disable daylight saving time function. When daylight saving time is enabling, you need to configure the daylight saving time period.
UTC Time zone	Set the switch location time zone. The following table lists the different location time zone for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11 am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard	-7 hours	5 am

PDT - Pacific Daylight		
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

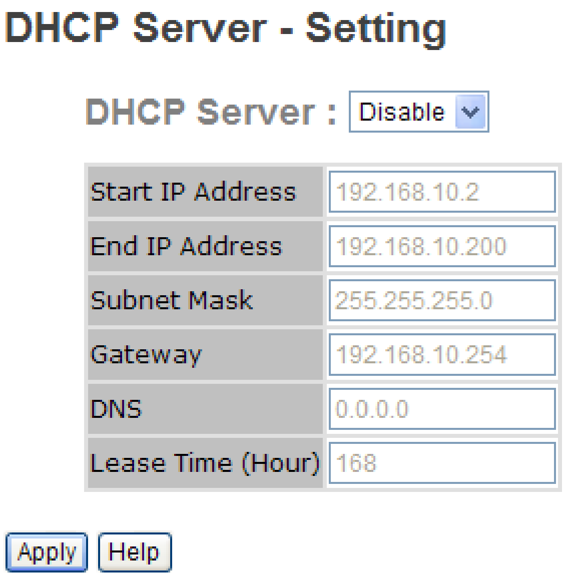
Label	Description
SNTP Sever IP Address	Set the SNTP server IP address.

Daylight Saving Period	Set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different each year.
Daylight Saving Offset	Set up the offset time.
Switch Timer	Display the switch current time.
Apply	Click "**Apply**" to set the configurations.

5.1.2.5 DHCP Server

DHCP Server – Setting

The system provides with DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.



DHCP Server - Setting

DHCP Server : Disable

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

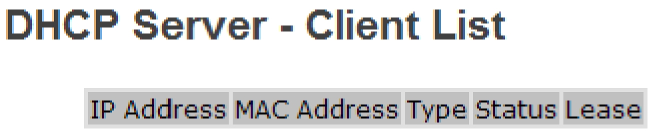
DHCP Server Setting interface

The following table describes the labels in this screen.

Label	Description
DHCP Server	Enable or Disable the DHCP Server function. Enable – the switch will be the DHCP server on your local network
Start IP Address	The dynamic IP assign range. Low IP address is the beginning of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 to 192.168.1.200. 192.168.1.100 will be the Start IP address.
End IP Address	The dynamic IP assign range. High IP address is the end of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 to 192.168.1.200. 192.168.1.200 will be the End IP address
Subnet Mask	The dynamic IP assign range subnet mask
Gateway	The gateway in your network.
DNS	Domain Name Server IP Address in your network.
Lease Time (Hour)	It is the period that system will reset the assigned dynamic IP to ensure the IP address is in used.
Apply	Click "**Apply**" to set the configurations.

DHCP Server – Client List

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



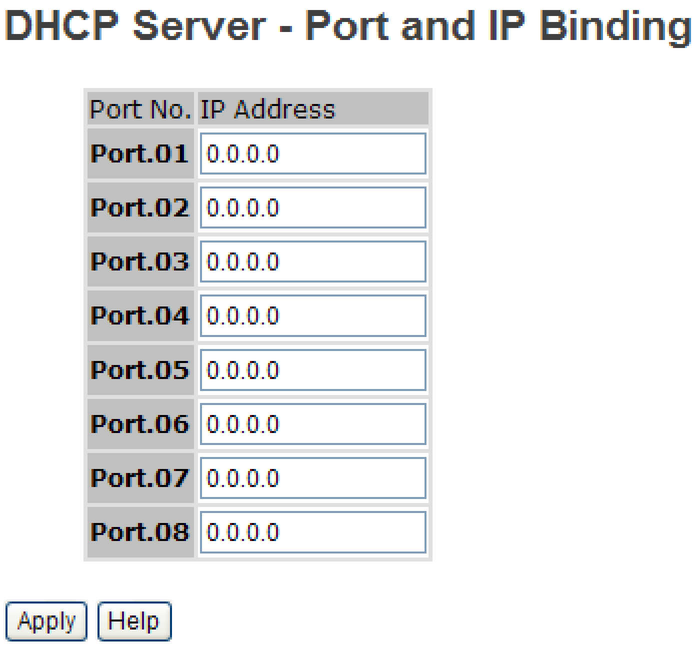
DHCP Server - Client List

IP Address	MAC Address	Type	Status	Lease

DHCP Server Client List interface

DHCP Server – Port and IP bindings

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



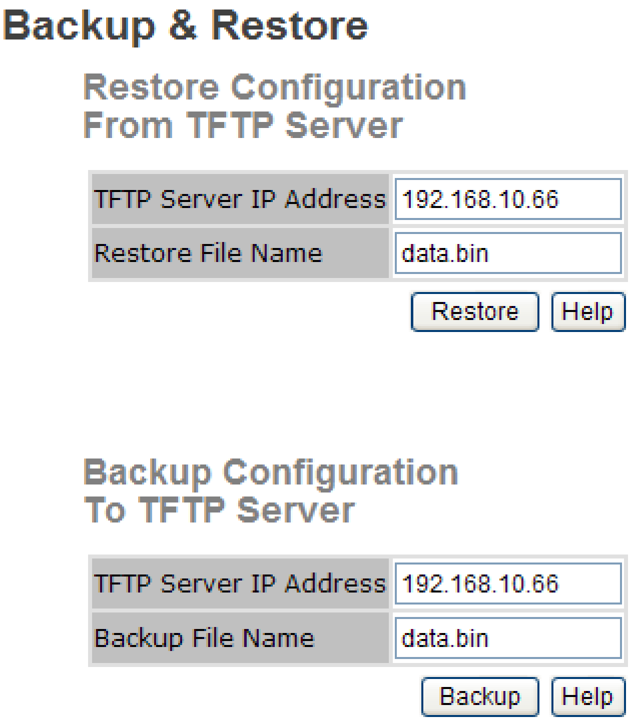
DHCP Server - Port and IP Binding

Port 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
Port.08	0.0.0.0

DHCP Server Port and IP Binding interface

5.1.2.6 Backup & Restore

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



Backup & Restore

Restore Configuration From TFTP Server

TFTP Server IP Address	192.168.10.66
Restore File Name	data.bin

Backup Configuration To TFTP Server

TFTP Server IP Address	192.168.10.66
Backup File Name	data.bin

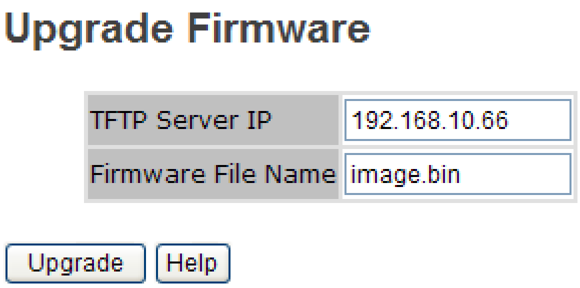
Backup & Restore interface

The following table describes the labels in this screen.

Label	Description
TFTP Server IP Address	Fill in the TFTP server IP
Restore File Name	Fill the file name.
Restore	Click “**restore**” to restore the configurations.
Restore File Name	Fill the file name.
Restore	Click “**restore**” to restore the configurations.
Backup	Click “**backup**” to backup the configurations.

5.1.2.7 Upgrade Firmware

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



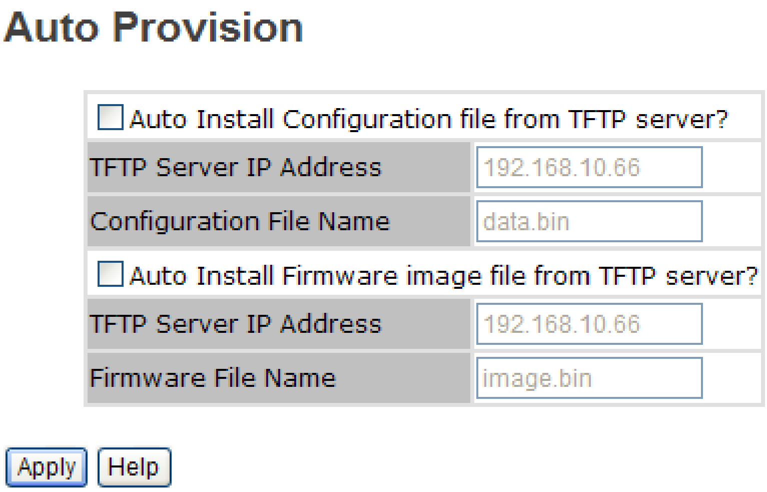
Upgrade Firmware

TFTP Server IP	192.168.10.66
Firmware File Name	image.bin

Upgrade Firmware interface

5.1.2.8 Auto Provision

Auto Provision allows you to update the switch firmware automatically. You can put firmware or configuration file on TFTP server. When you reboot the switch, it will upgrade automatically. Before updating, make sure you have your TFTP server ready and the firmware image and configuration file is on the TFTP server.

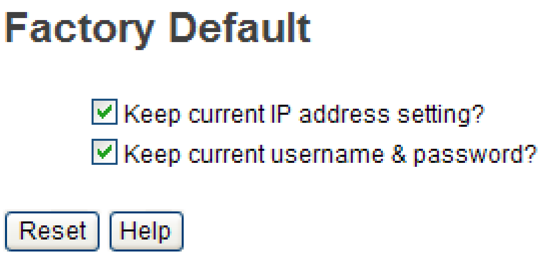


Auto Provision

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

Auto Provision interface

5.1.2.9 Factory Default



Factory Default

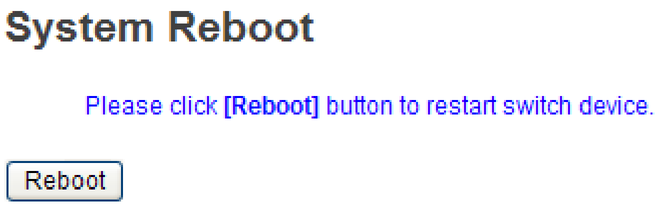
☑ Keep current IP address setting?

☑ Keep current username & password?

Factory Default interface

Reset switch to default configuration. Click Reset to reset all configurations to the default value. You can select “**Keep current IP address setting**” and “**Keep current username & password**” to prevent IP and username and password form default.

5.1.2.10 System Reboot



System Reboot

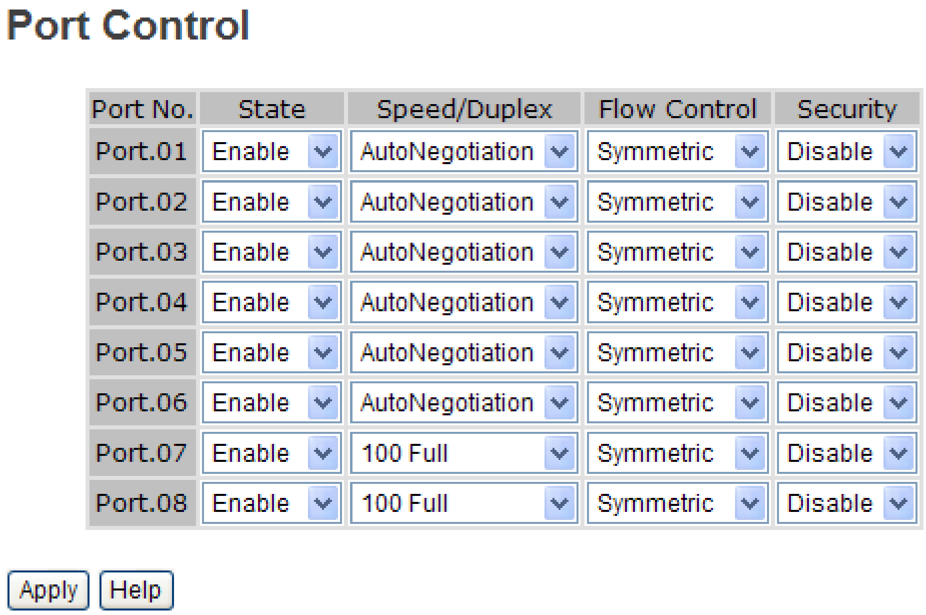
Please click **[Reboot]** button to restart switch device.

System Reboot interface

5.1.3 Port Configuration

5.1.3.1 Port Control

By this function, you can set the state, speed/duplex, flow control, and security of the port.



Port Control

Port No.	State	Speed/Duplex	Flow Control	Security
Port.01	Enable	AutoNegotiation	Symmetric	Disable
Port.02	Enable	AutoNegotiation	Symmetric	Disable
Port.03	Enable	AutoNegotiation	Symmetric	Disable
Port.04	Enable	AutoNegotiation	Symmetric	Disable
Port.05	Enable	AutoNegotiation	Symmetric	Disable
Port.06	Enable	AutoNegotiation	Symmetric	Disable
Port.07	Enable	100 Full	Symmetric	Disable
Port.08	Enable	100 Full	Symmetric	Disable

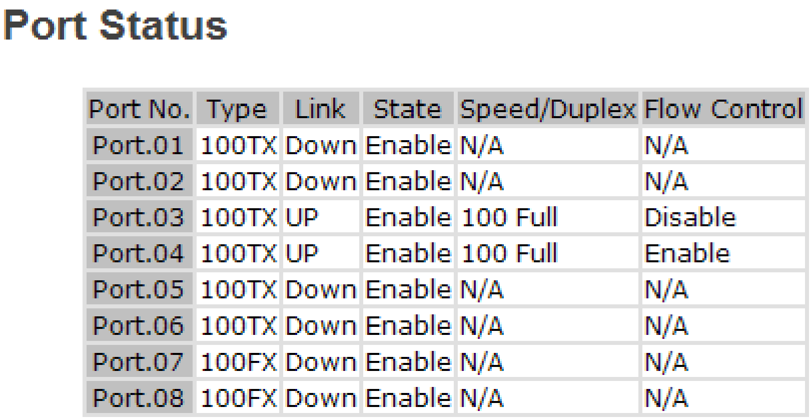
Port Control interface

The following table describes the labels in this screen.

Label	Description
Port NO.	Port number for setting.
Speed/Duplex	You can set Autonigotiation,100 full ,100 half,10 full,10 half mode.
Flow Control	Support symmetric and asymmetric mode to avoid packet loss when congestion occurred.
Security	Support port security function. When enable the function, the port will STOP learning MAC address dynamically.
Apply	Click "**Apply**" to set the configurations.

5.1.3.2 Port Status

The following information provides the current port status information



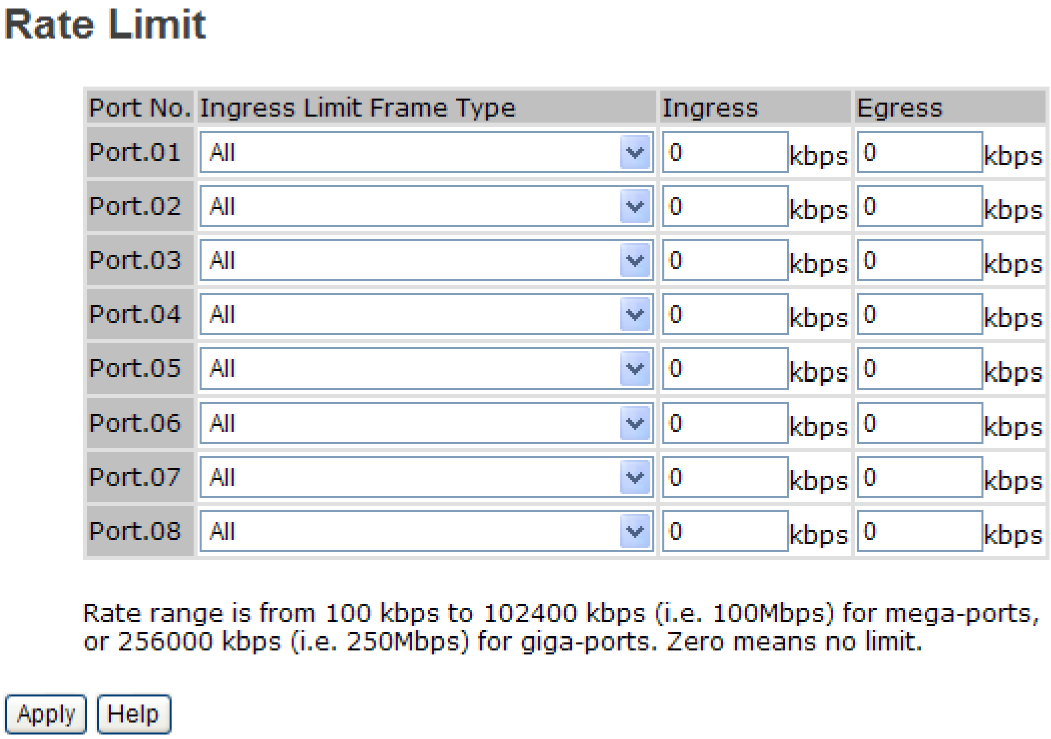
Port Status

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

Port Status interface

5.1.3.3 Rate Limit

By this function, You can limit traffic of all ports, including broadcast, multicast and flooded unicast. You can also set "Ingress" or "Egress" to limit traffic received or transmitted bandwidth.



Rate Limit

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

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

Rate Limit interface

The following table describes the labels in this screen.

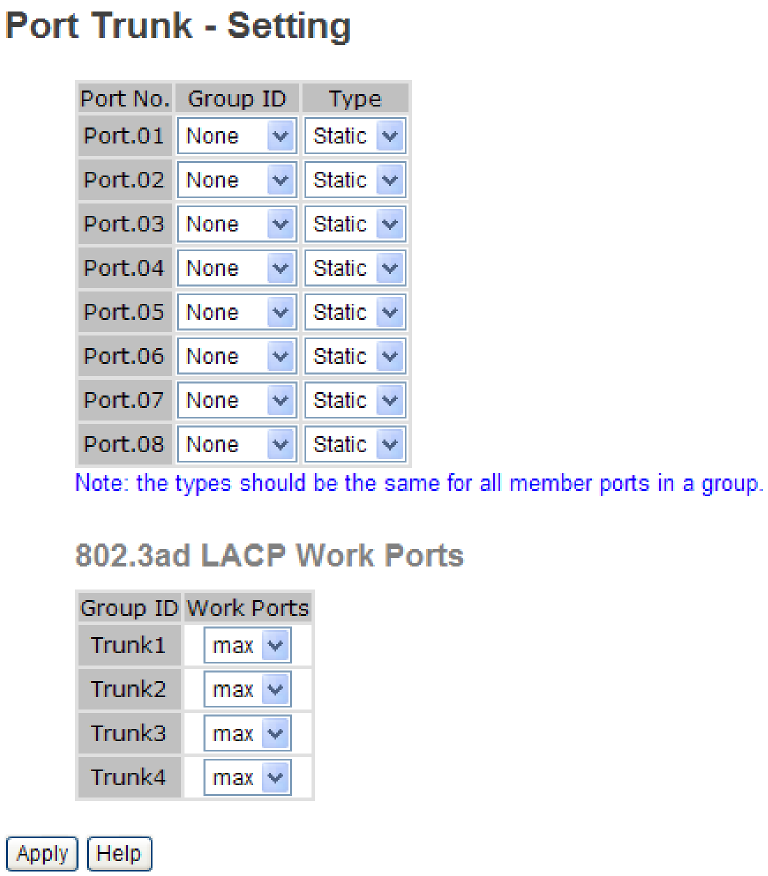
Label	Description
Ingress Limit Frame Type	You can set "all", "Broadcast only", "Broadcast/Multicast"

	or ”Broadcast/Multicast/Flooded Unicast” mode.
Ingress	The switch port received traffic.
Egress	The switch port transmitted traffic.
Apply	Click “**Apply**” to set the configurations.

5.1.3.4 Port Trunk

Port Trunk – Setting

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



Port Trunk - Setting

Port No.	Group ID	Type
Port.01	None	Static
Port.02	None	Static
Port.03	None	Static
Port.04	None	Static
Port.05	None	Static
Port.06	None	Static
Port.07	None	Static
Port.08	None	Static

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

802.3ad LACP Work Ports

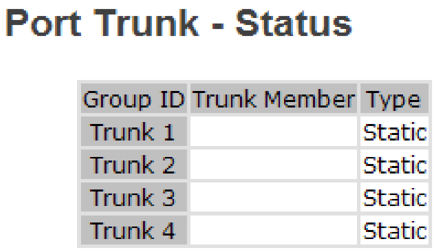
Group ID	Work Ports
Trunk1	max
Trunk2	max
Trunk3	max
Trunk4	max

Port Trunk - Setting interface

The following table describes the labels in this screen.

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

Port Trunk – Status



Port Trunk - Status

Group ID	Trunk Member	Type
Trunk 1		Static
Trunk 2		Static
Trunk 3		Static
Trunk 4		Static

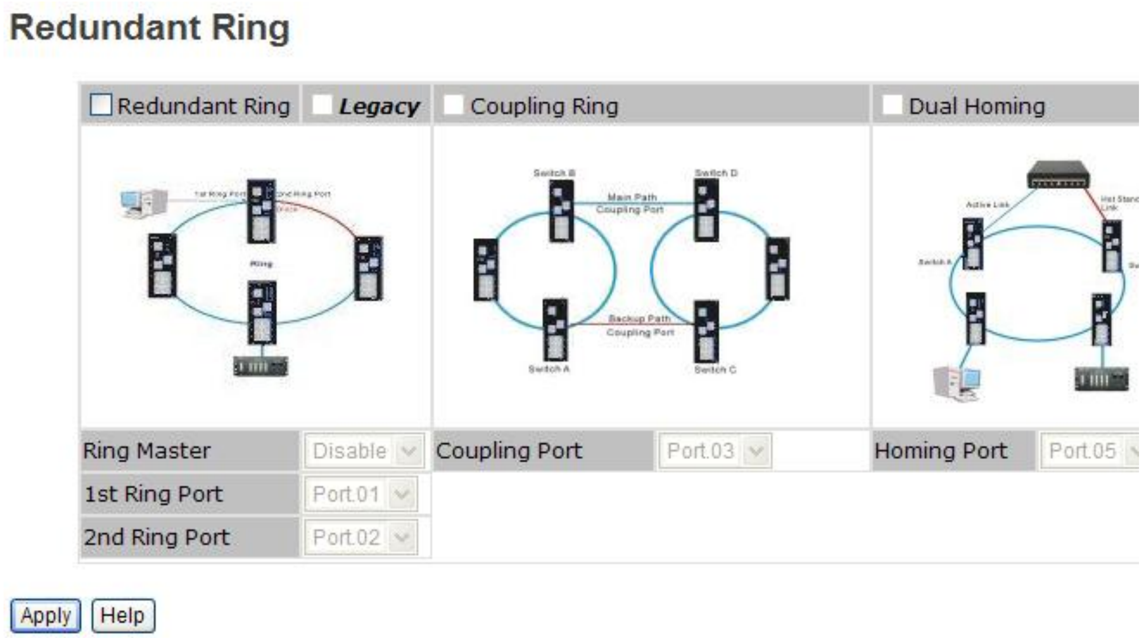
Port Trunk - Status interface

5.1.4 Redundancy

5.1.4.1 Pro-Ring

Pro-Ring is the most powerful Ring in the world. Pro-Ring Supports 3 Ring topology: X-Ring, Coupling Ring and Dual Homing. The recovery time of X-Ring is less than 10 ms. It can reduce unexpected damage caused by network topology change.

NOTE: IES-2206F-II is supporting X-Ring 10ms recovery. When IES-2206F-II is set as Master connecting with IES-2206F, the X-Ring will automatically backward compatible to 300ms. Should you need IES-2206F to be set as Master, please click on “Legacy mode” for X-Ring 300ms.



Redundant Ring

□ Redundant Ring □ Legacy □ Coupling Ring □ Dual Homing

Ring Master: Disable
1st Ring Port: Port.01
2nd Ring Port: Port.02
Coupling Port: Port.03
Homing Port: Port.05

Pro-Ring interface

The following table describes the labels in this screen.

Label	Description
X-Ring	Mark to enable Ring.
Ring Master	There should be one and only one Ring Master in a ring. However if there are two or more switches which set Ring Master to enable, the switch with the lowest MAC address will be the actual Ring Master and others will be Backup Masters.
1st Ring Port	The primary port, when this switch is Ring Master.
2nd Ring Port	The backup port, when this switch is Ring Master.
Coupling Ring	Mark to enable Coupling Ring. Coupling Ring can be used to divide a big ring into two smaller rings to avoid effecting all

	switches when network topology change. It is a good application for connecting two Rings.
Coupling Port	Link to Coupling Port of the switch in another ring. Coupling Ring need four switch to build an active and a backup link. Set a port as coupling port. The coupled four ports of four switches will be run at active/backup mode.
Control Port	Link to Control Port of the switch in the same ring. Control Port used to transmit control signals.
Dual Homing	Mark to enable Dual Homing. By selecting Dual Homing mode, X-Ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work as active/backup mode, and connect each X-Ring to the normal switches in RSTP mode.
Apply	Click "**Apply**" to set the configurations.

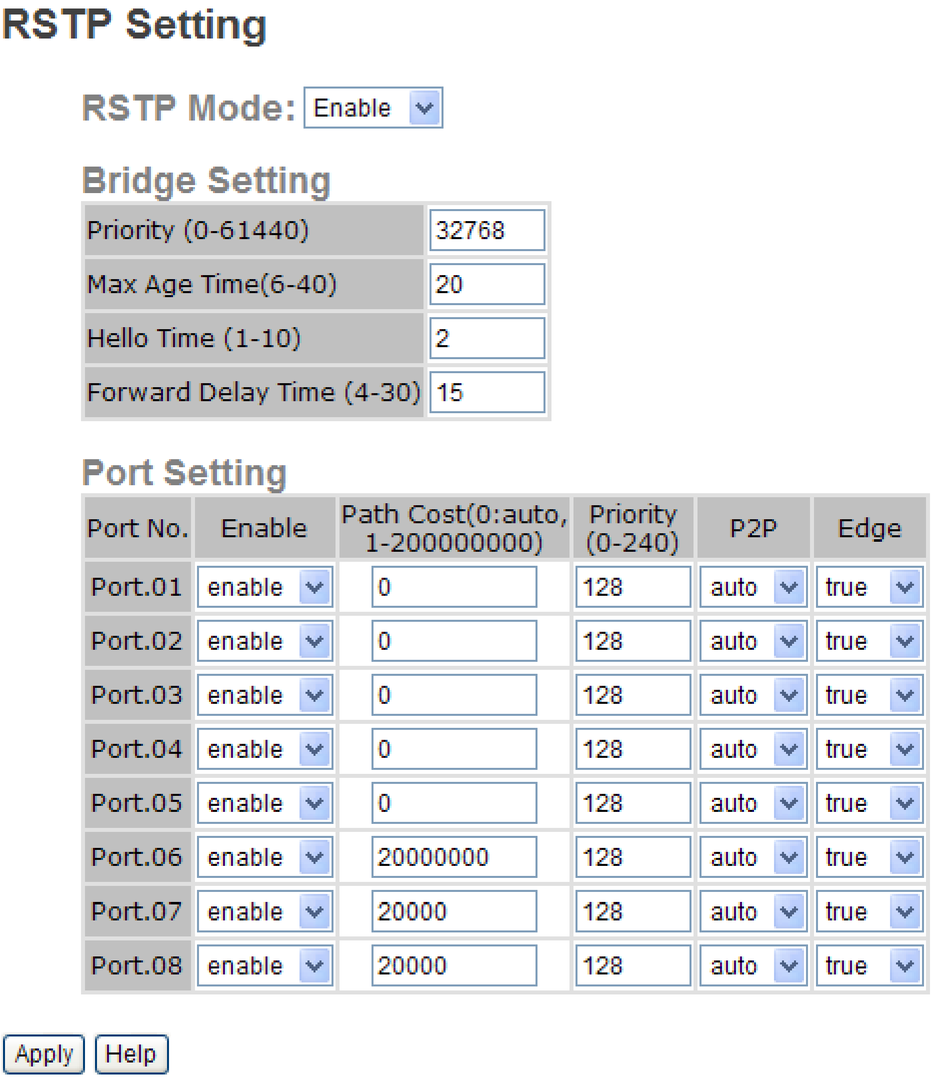
Note: We don't suggest you to set one switch as a Ring Master and a Coupling Ring at the same time due to heavy load.

5.1.4.2 RSTP

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

RSTP setting

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



RSTP Setting

RSTP Mode: Enable

Bridge Setting

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

Port Setting

Port No.	Enable	Path Cost(0:auto, 1-200000000)	Priority (0-240)	P2P	Edge
Port.01	enable	0	128	auto	true
Port.02	enable	0	128	auto	true
Port.03	enable	0	128	auto	true
Port.04	enable	0	128	auto	true
Port.05	enable	0	128	auto	true
Port.06	enable	20000000	128	auto	true
Port.07	enable	20000	128	auto	true
Port.08	enable	20000	128	auto	true

RSTP Setting interface

The following table describes the labels in this screen.

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

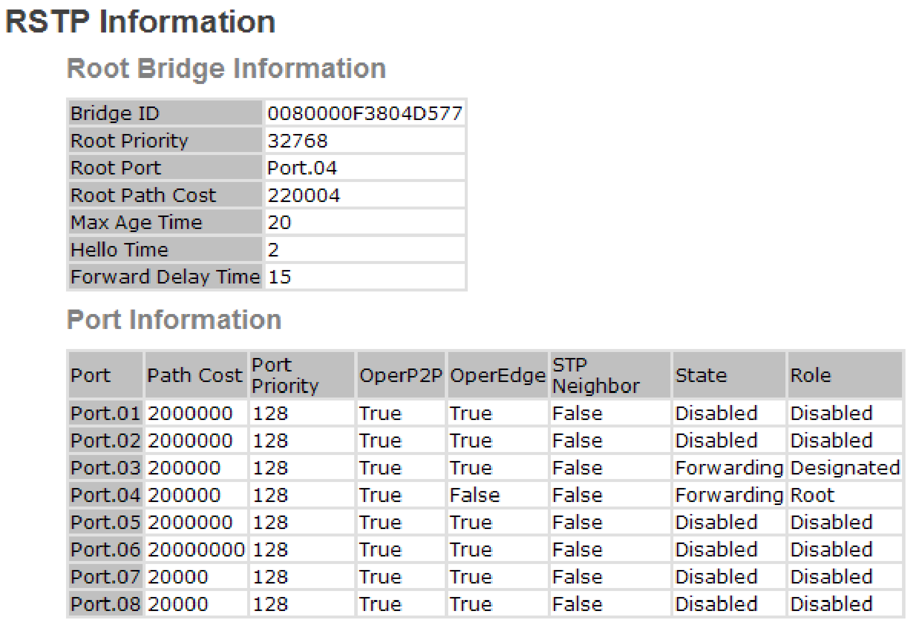
	4096 according to the protocol standard rule.
Max Age (6-40)	The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
Hello Time (1-10)	The time that controls switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.
Forwarding Delay Time (4-30)	The number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.
Path Cost (1-200000000)	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
Priority (0-240)	Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16
Admin P2P	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. It is served by a point-to-point LAN segment), or it can be connected to two or more bridges (i.e. It is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True means P2P enabling. False means P2P disabling.
Admin Edge	The port directly connected to end stations, and it cannot create bridging loop in the network. To configure the port as an edge port, set the port to "**True**".
Admin Non STP	The port includes the STP mathematic calculation. **True** is not including STP mathematic calculation. **False** is including the STP mathematic calculation.
Apply	Click "**Apply**" to set the configurations.

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

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

RSTP Information

Show RSTP algorithm result at this table.



RSTP Information

Root Bridge Information

Bridge ID	0080000F3804D577
Root Priority	32768
Root Port	Port.04
Root Path Cost	220004
Max Age Time	20
Hello Time	2
Forward Delay Time	15

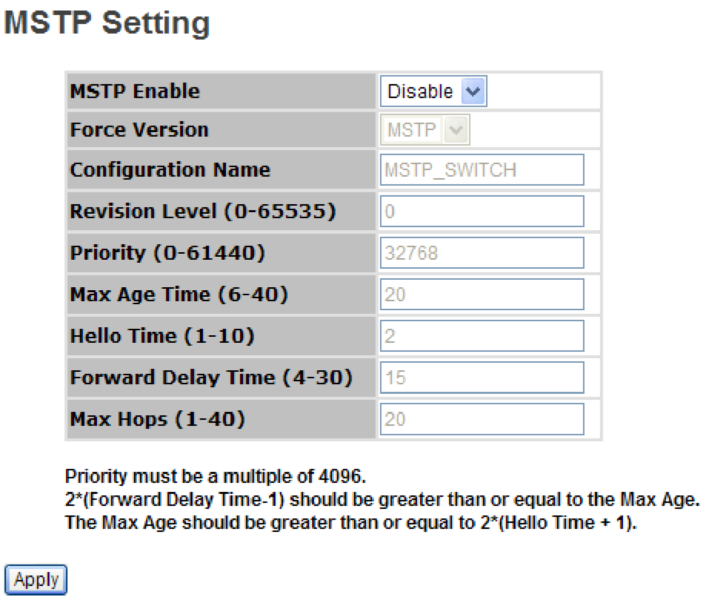
Port Information

Port	Path Cost	Port Priority	OperP2P	OperEdge	STP Neighbor	State	Role
Port.01	2000000	128	True	True	False	Disabled	Disabled
Port.02	2000000	128	True	True	False	Disabled	Disabled
Port.03	200000	128	True	True	False	Forwarding	Designated
Port.04	200000	128	True	False	False	Forwarding	Root
Port.05	2000000	128	True	True	False	Disabled	Disabled
Port.06	20000000	128	True	True	False	Disabled	Disabled
Port.07	20000	128	True	True	False	Disabled	Disabled
Port.08	20000	128	True	True	False	Disabled	Disabled

RSTP Information interface

5.1.4.3 MSTP (optional feature)

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



MSTP Setting

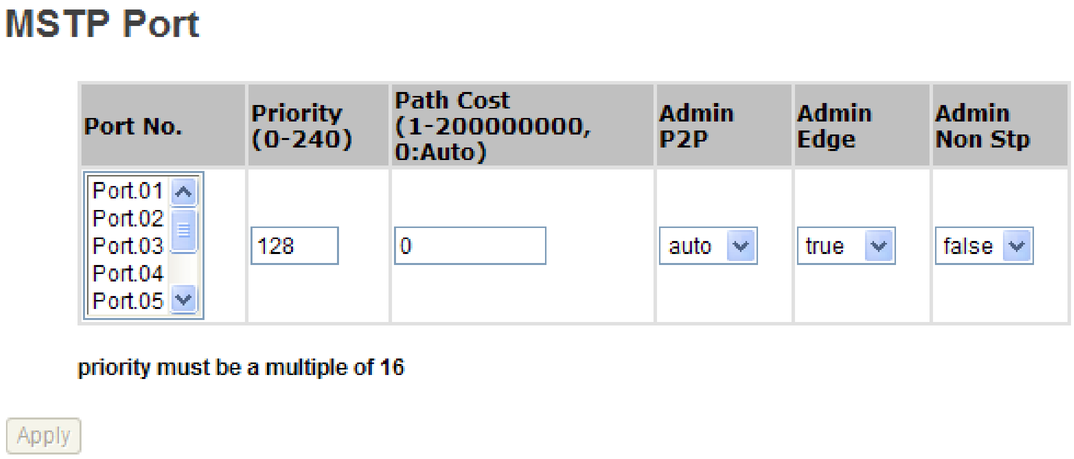
MSTP Enable	Disable
Force Version	MSTP
Configuration Name	MSTP_SWITCH
Revision Level (0-65535)	0
Priority (0-61440)	32768
Max Age Time (6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15
Max Hops (1-40)	20

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

MSTP (optional feature) Setting interface

The following table describes the labels in this screen.

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



MSTP Port

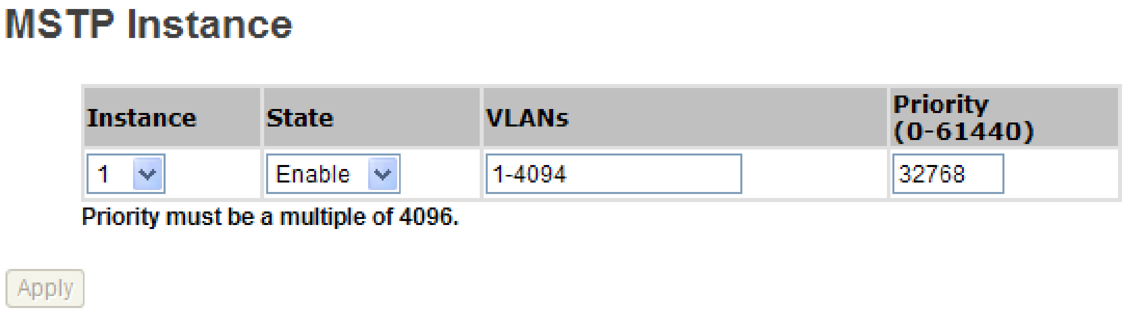
Port No.	Priority (0-240)	Path Cost (1-200000000, 0:Auto)	Admin P2P	Admin Edge	Admin Non Stp
Port.01 Port.02 Port.03 Port.04 Port.05	128	0	auto	true	false

priority must be a multiple of 16

MSTP (optional feature) Port interface

The following table describes the labels in this screen.

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



MSTP Instance

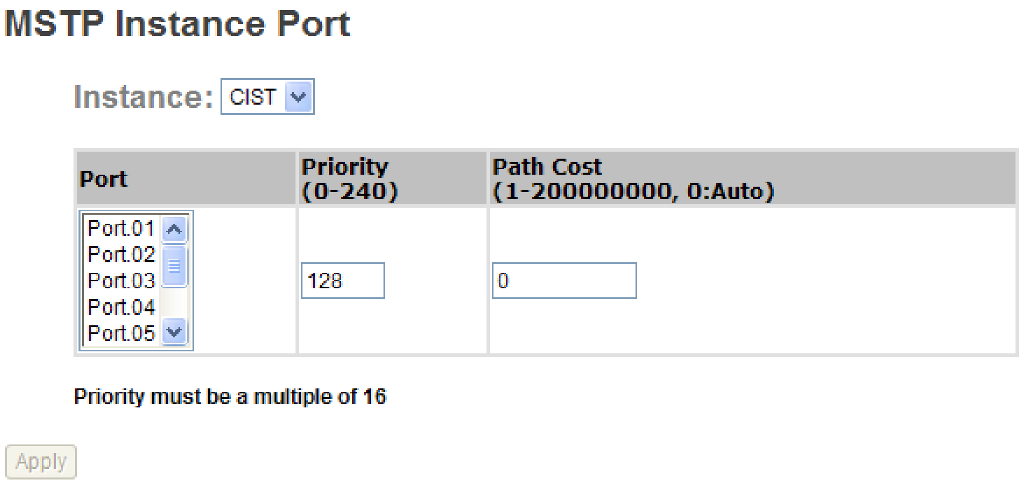
Instance	State	VLANs	Priority (0-61440)
1	Enable	1-4094	32768

Priority must be a multiple of 4096.

MSTP (optional feature) Instance interface

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.



MSTP Instance Port

Instance: CIST

Port	Priority (0-240)	Path Cost (1-200000000, 0:Auto)
Port.01 Port.02 Port.03 Port.04 Port.05	128	0

Priority must be a multiple of 16

MSTP (optional feature) Instance Port interface

The following table describes the labels in this screen.

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

5.1.5 VLAN

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which allows you to isolate network traffic. Only the members of the VLAN will receive traffic from the same members of VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

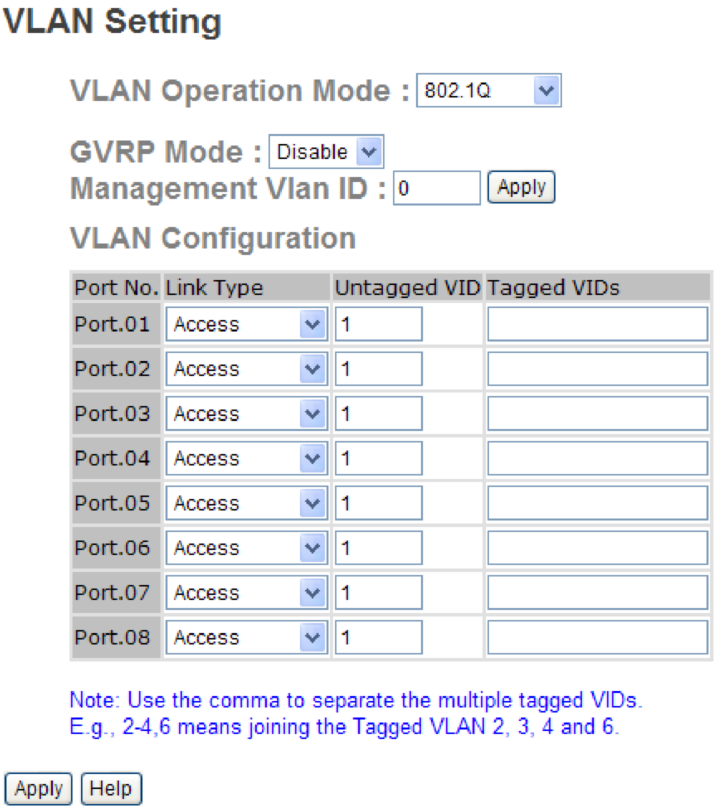
The switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration of VLAN operation mode is at "**802.1Q**".

5.1.5.1 VLAN Configuration – 802.1Q

Tagged-based VLAN is an IEEE 802.1Q specification standard, and t is possible to create a VLAN across devices from different switch venders. IEEE 802.1Q VLAN uses a technique to insert a "tag" into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

You can create Tag-based VLAN, and enable or disable GVRP protocol. There are 256 VLAN groups to provide configure. Enable 802.1Q VLAN, the all ports on the switch belong to default VLAN, VID is 1. The default VLAN cannot be deleted.

GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request by using the VID of a VLAN defined on the switch; the switch will automatically add that device to the existing VLAN.



VLAN Setting

VLAN Operation Mode : 802.1Q

GVRP Mode : Disable

Management Vlan ID : 0

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	
Port.08	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.

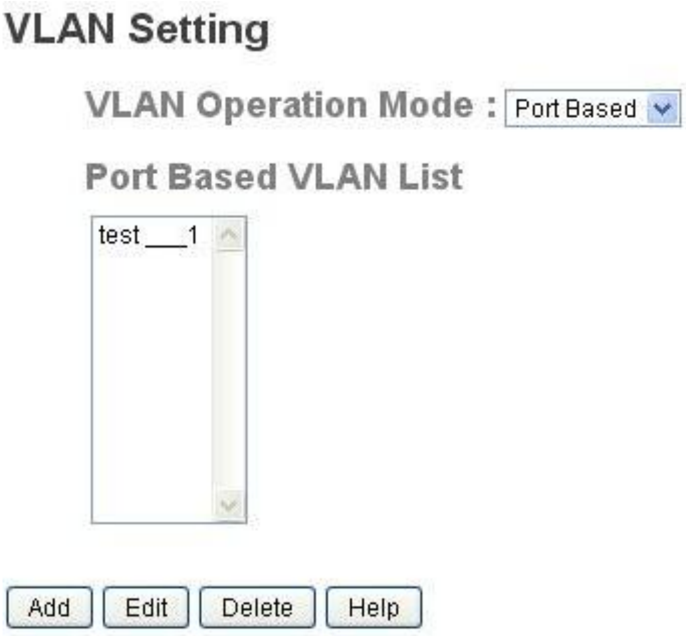
VLAN Setting – 802.1Q interface

The following table describes the labels in this screen.

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

5.1.5.2 VLAN Configuration – Port Based

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



VLAN Setting

VLAN Operation Mode : Port Based

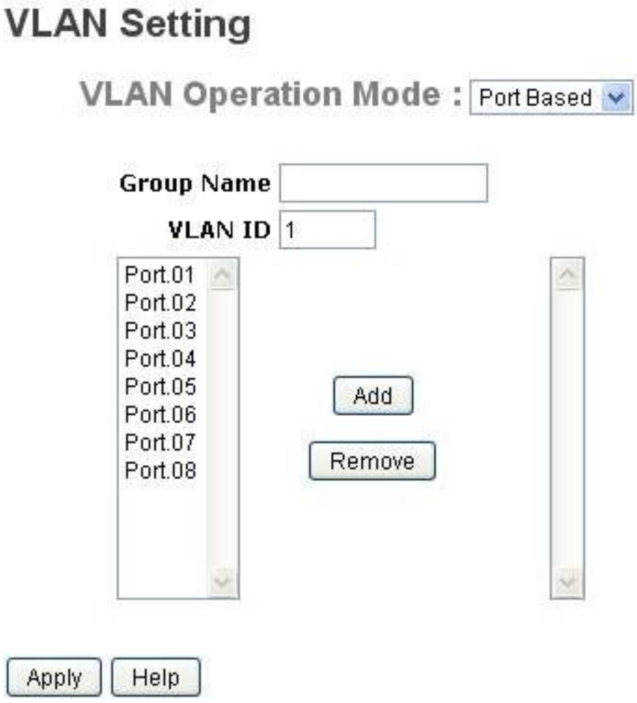
Port Based VLAN List

test___1

VLAN Setting – Port Base interface-1

The following table describes the labels in this screen.

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



VLAN Setting – Port Base interface-2

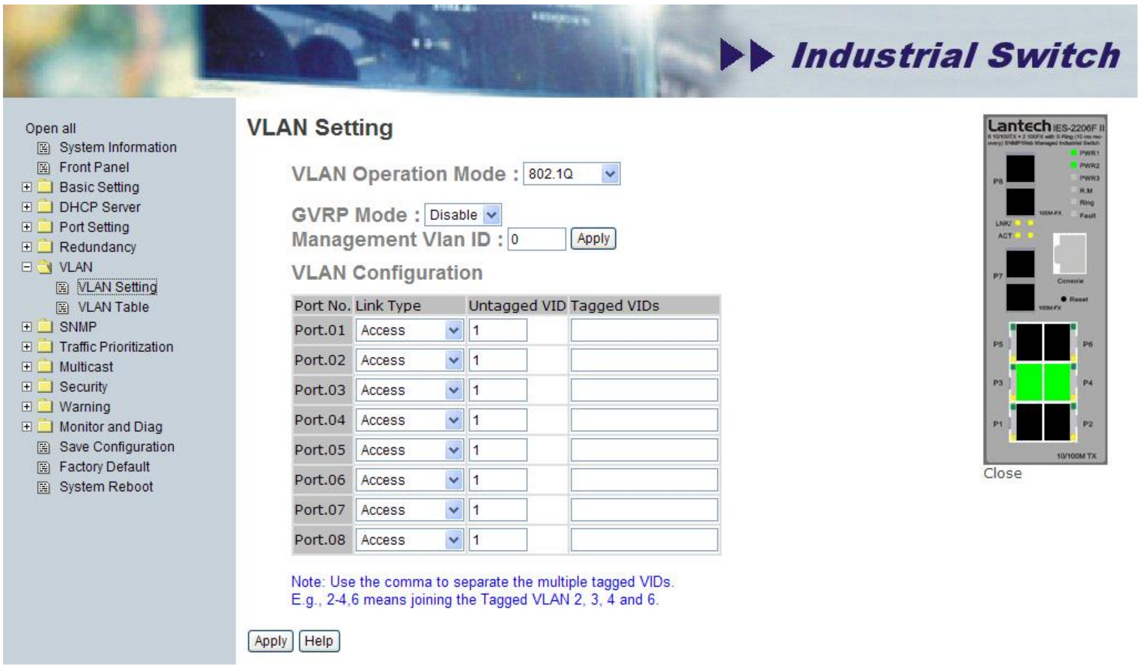
The following table describes the labels in this screen.

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

5.1.5.3 QinQ (Double Tag VLAN) configuration

Double Tag VLAN is another mechanism employed in a Metro LAN in which it can save IP v4 address by residing groups of sub-VLANs (customer port) in a VLAN(Host) and utilizing the default gateway IP address of Double Tag VLAN sharing the same IP subnet mask. Double Tag VLAN in L2 provides enhances security between customer (each home), by dis-communication between the sub-VLANs, even they are located in the same LAN and have the same IP subnet mask. Better yet, the configuration is simple than assigning each VLAN as per port based VLAN to customer (each home).

Please select Hybrid VLAN in Port VLAN to enable QinQ (Double Tag VLAN) function.



VLAN Setting

VLAN Operation Mode : 802.1Q

GVRP Mode : Disable

Management Vlan ID : 0 Apply

VLAN Configuration

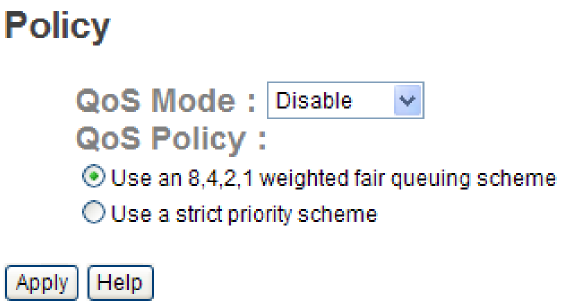
Port No.	Link Type	Untagged VID	Tagged VIDs
Port.01	Access	1	
Port.02	Access	1	
Port.03	Access	1	
Port.04	Access	1	
Port.05	Access	1	
Port.06	Access	1	
Port.07	Access	1	
Port.08	Access	1	

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.

Apply Help

5.1.6 Traffic Prioritization

Traffic Prioritization includes 3 modes: port base, 802.1p/COS, and TOS/DSCP. By traffic prioritization function, you can classify the traffic into four classes for differential network application. IES-2206F-II support 4 priority queues.



Policy

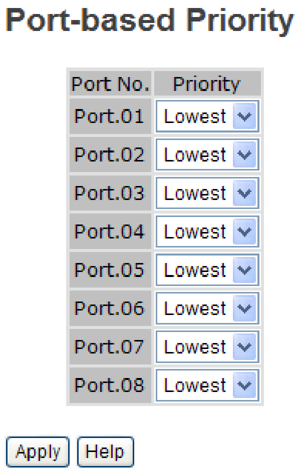
QoS Mode : Disable

QoS Policy :

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

○ Use a strict priority scheme

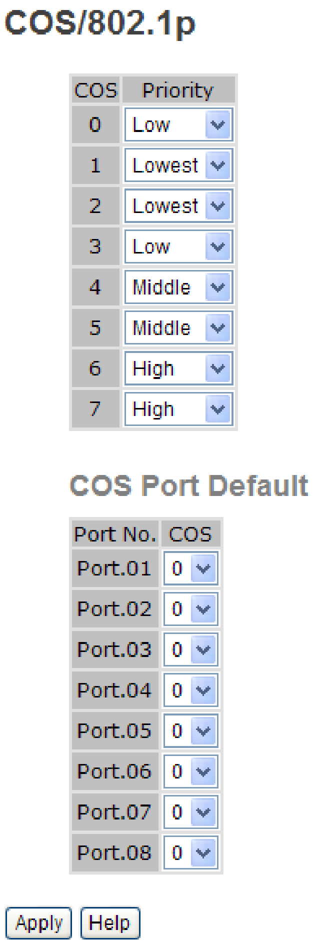
Policy interface



Port-based Priority

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

Port-based Priority interface



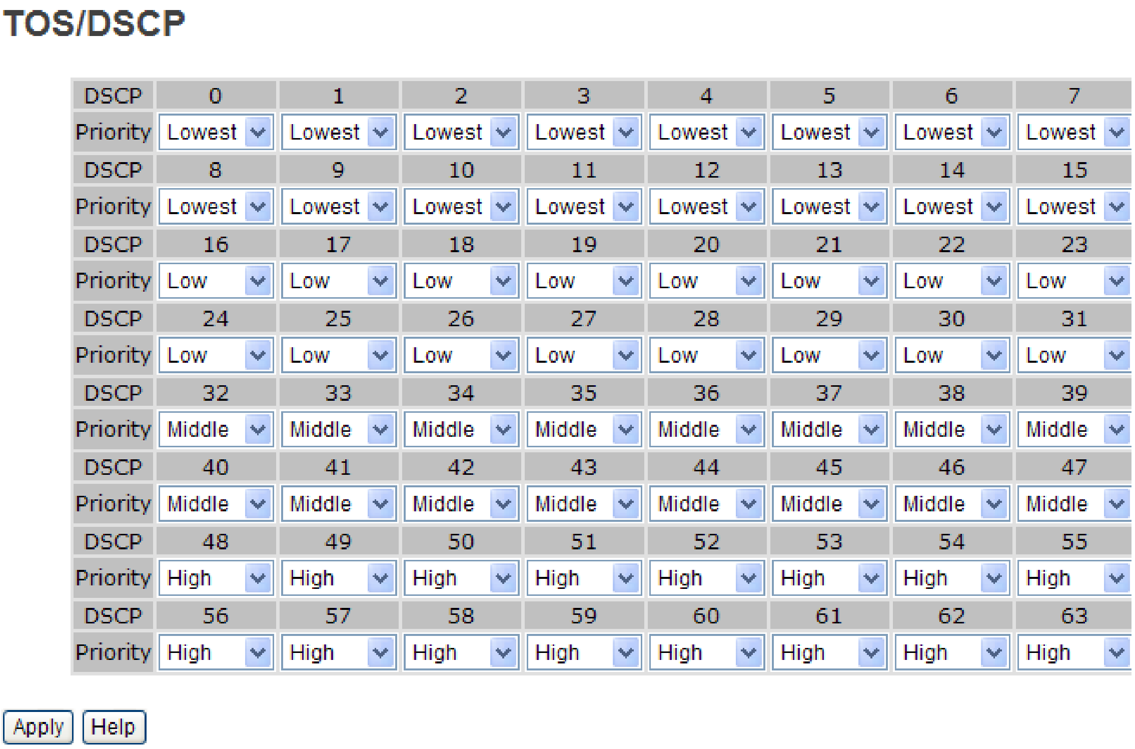
COS/802.1p

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

COS Port Default

Port No.	COS
Port.01	0
Port.02	0
Port.03	0
Port.04	0
Port.05	0
Port.06	0
Port.07	0
Port.08	0

COS/ 802.1p interface



TOS/DSCP

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

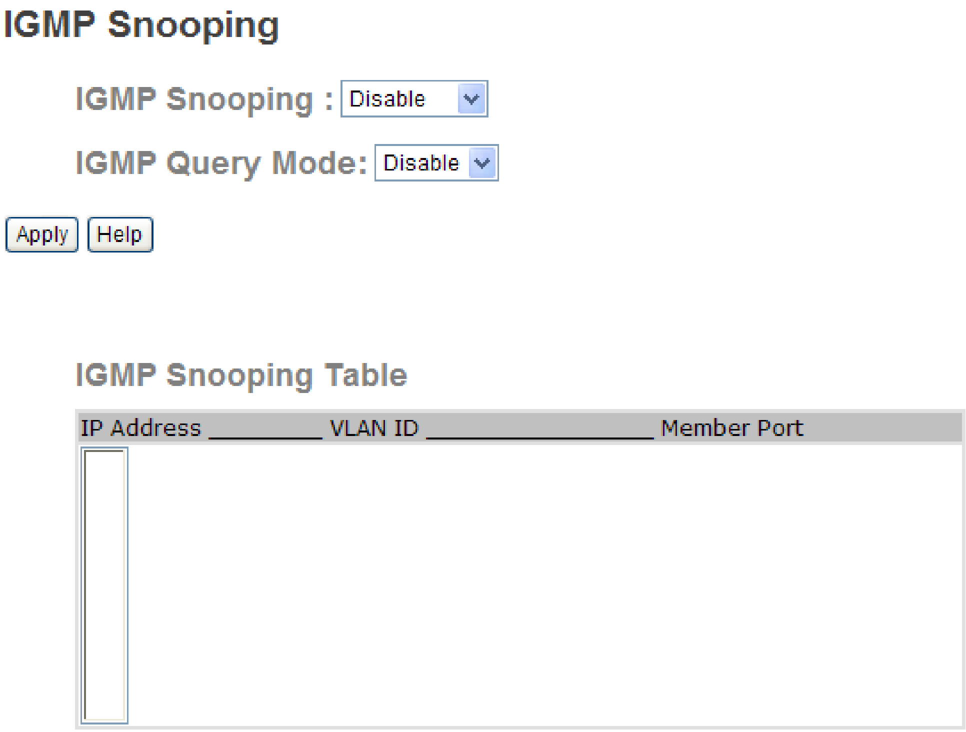
TOS/ DSCP interface

The following table describes the labels in this screen.

Label	Description
QOS policy	■ **Using the 8,4,2,1 weight fair queue scheme:** the output queues will follow 8:4:2:1 ratio to transmit packets from the highest to lowest queue. For example: 8 high queue packets, 4 middle queue packets, 2 low queue packets, and the one lowest queue packets are transmitted in one turn. ■ **Use the strict priority scheme:** always the packets in higher queue will be transmitted first until higher queue is empty.
Priority Type	■ **Port-base:** the output priority is determined by ingress port. ■ **COS only:** the output priority is determined by COS only. ■ **TOS only:** the output priority is determined by TOS only. ■ **COS first:** the output priority is determined by COS and TOS, but COS first. ■ **TOS first:** the output priority is determined by COS and TOS, but TOS first.
Port base Priority	Assign Port with a priority queue. 4 priority queues can be assigned: High, Middle, Low, and Lowest.
COS/802.1p	COS (Class Of Service) is well known as 802.1p. It describes that the output priority of a packet is determined by user priority field in 802.1Q VLAN tag. The priority value is supported 0to7.COS value map to 4 priority queues: High, Middle, Low, and Lowest.
COS Port Default	When an ingress packet has not VLAN tag, a default priority value is considered and determined by ingress port.
TOS/DSCP	TOS (Type of Service) is a field in IP header of a packet. This TOS field is also used by Differentiated Services and is called the Differentiated Services Code Point (DSCP). The output priority of a packet can be determined by this field and the priority value is supported 0to63. DSCP value map to 4 priority queues: High, Middle, Low, and Lowest.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.1.7 IGMP Snooping

Internet Group Management Protocol (IGMP) is used by IP hosts to register their dynamic multicast group membership. IGMP has 3 versions, IGMP v1, v2 and v3. Please refer to RFC 1112, 2236 and 3376. IGMP Snooping improves the performance of networks that carry multicast traffic. It provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic and reduces the amount of traffic on the Ethernet LAN.



IGMP Snooping

IGMP Snooping : Disable

IGMP Query Mode: Disable

IGMP Snooping Table

IP Address	VLAN ID	Member Port

IGMP Snooping interface

The following table describes the labels in this screen.

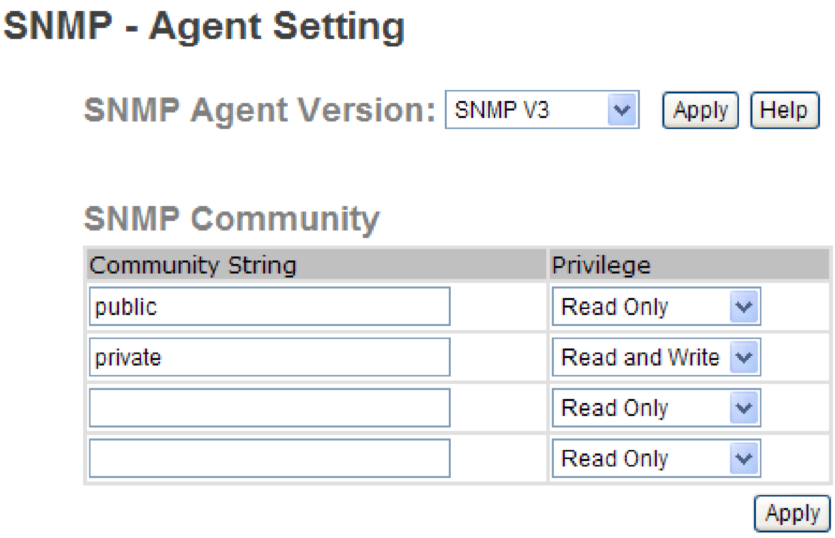
Label	Description
IGMP Snooping	Enable/Disable IGMP snooping.
IGMP Query Mode	Switch will be IGMP querier or not. There should exist one and only one IGMP querier in an IGMP application. The "Auto" mode means that the querier is the one with lower IP address.
IGMP Snooping Table	Show current IP multicast list
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.1.8 SNMP Configuration

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

5.1.8.1 SNMP –Agent Setting

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



SNMP - Agent Setting

SNMP Agent Version: SNMP V3

SNMP Community

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

SNMP Agent Setting interface

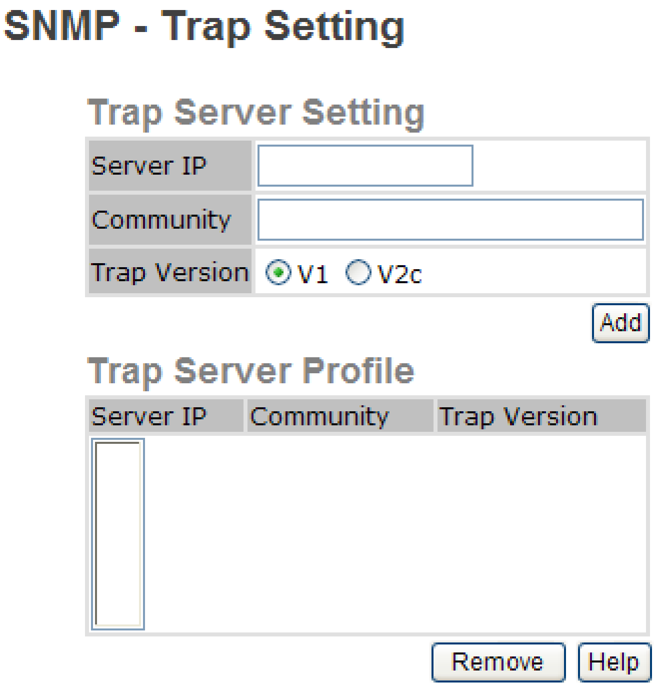
The following table describes the labels in this screen.

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

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

5.1.8.2 SNMP –Trap Setting

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will issue. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager and enter SNMP community strings and selects the SNMP version.


SNMP - Trap Setting

Trap Server Setting

Server IP	
Community	
Trap Version	● V1 ○ V2c

Trap Server Profile

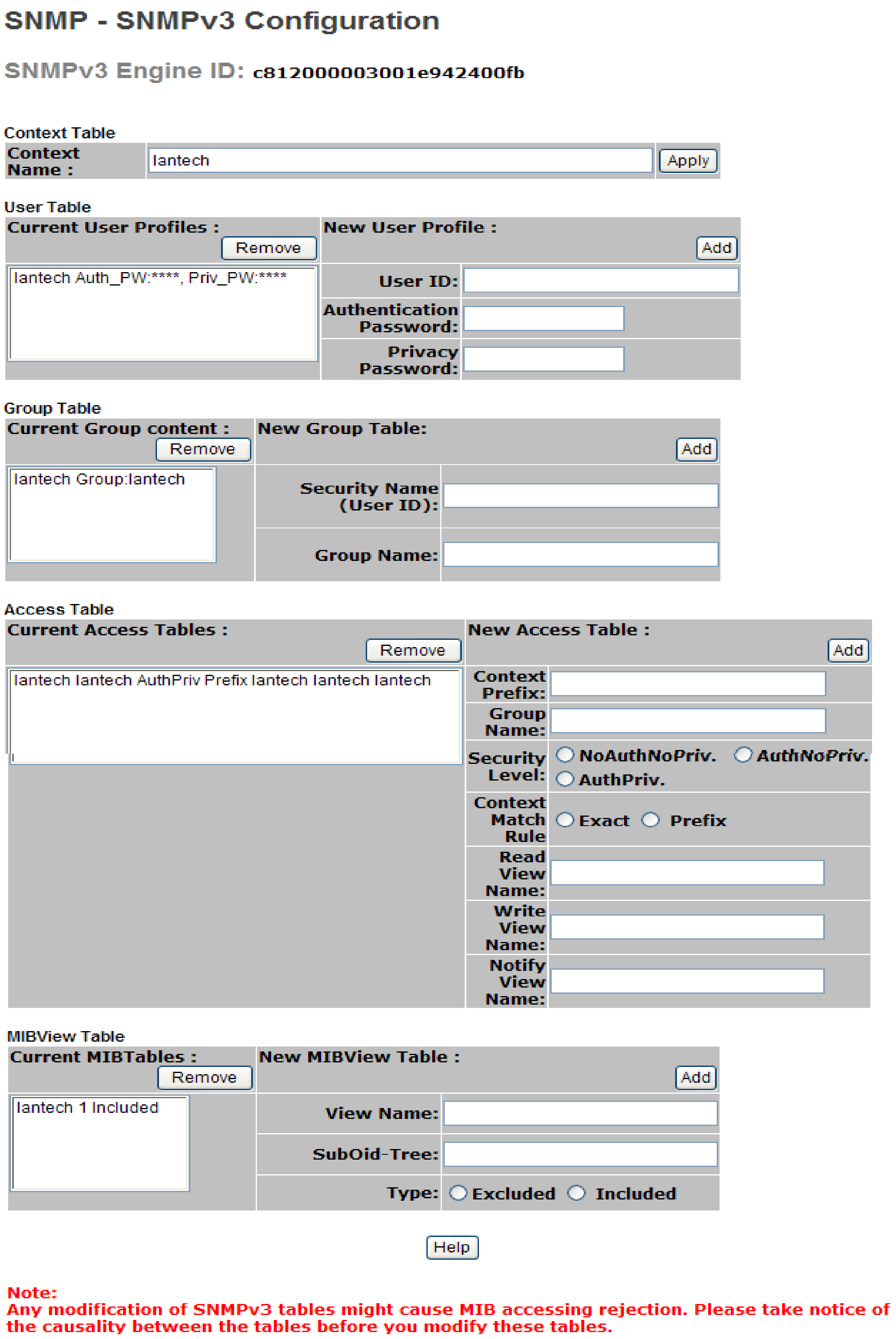
Server IP	Community	Trap Version

SNMP Trap Setting interface

The following table describes the labels in this screen.

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

5.1.8.3 SNMP –SNMP v3 Configuration



SNMP - SNMPv3 Configuration

SNMPv3 Engine ID: c812000003001e942400fb

Context Table

Context Name :	Iantech	Apply

User Table

Current User Profiles : Remove

Iantech Auth_PW:****, Priv_PW:****

New User Profile : Add

User ID:

Authentication Password:

Privacy Password:

Group Table

Current Group content : Remove

Iantech Group:Iantech

New Group Table: Add

Security Name (User ID):

Group Name:

Access Table

Current Access Tables : Remove

Iantech Iantech AuthPriv Prefix Iantech Iantech Iantech

New Access Table : Add

Context Prefix:

Group Name:

Security Level: ○ NoAuthNoPriv. ○ AuthNoPriv. ○ AuthPriv.

Context Match Rule: ○ Exact ○ Prefix

Read View Name:

Write View Name:

Notify View Name:

MIBView Table

Current MIBTables : Remove

Iantech 1 Included

New MIBView Table : Add

View Name:

SubOid-Tree:

Type: ○ Excluded ○ Included

Help

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

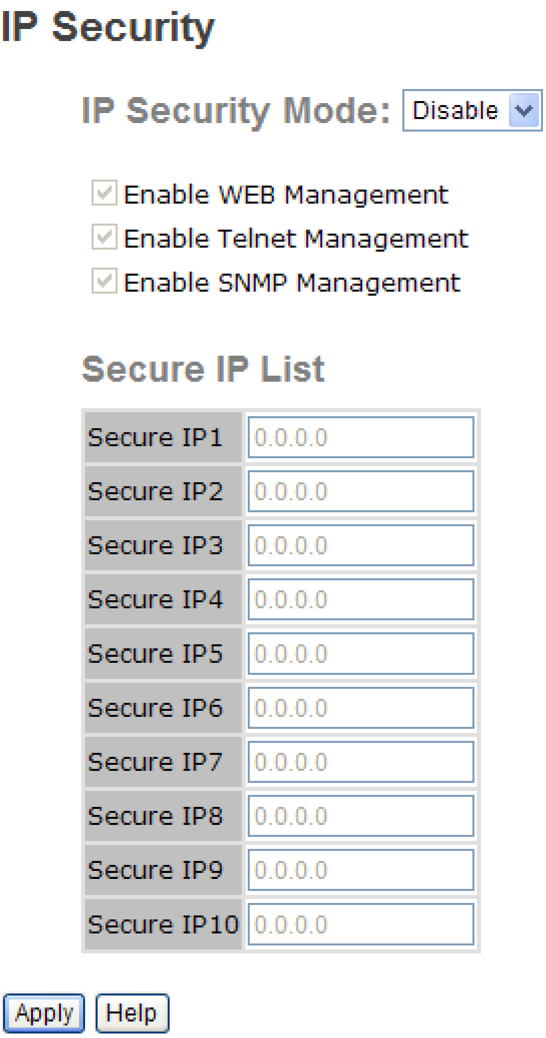
SNMP v3 Configuration interface

5.1.9 Security

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

5.1.9.1 IP Security

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



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

IP Security interface

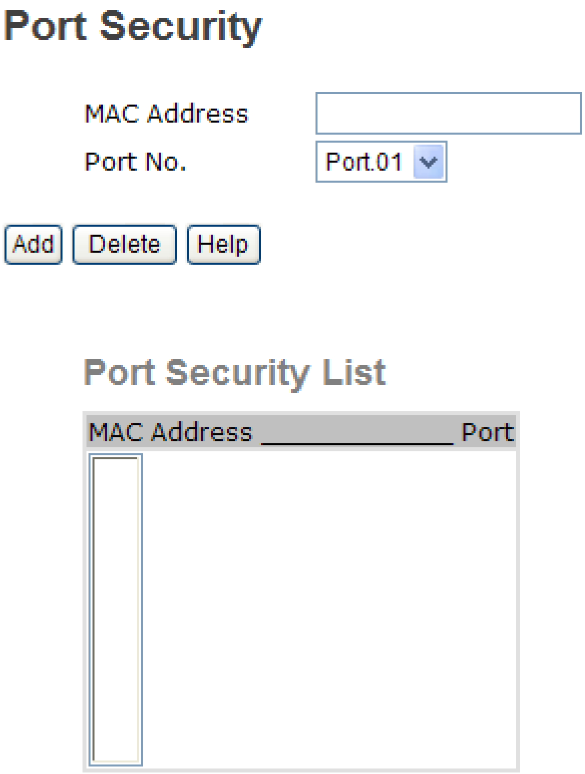
The following table describes the labels in this screen.

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

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

5.1.9.2 Port Security

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



Port Security

MAC Address

Port No. Port.01

Port Security List

MAC Address	Port

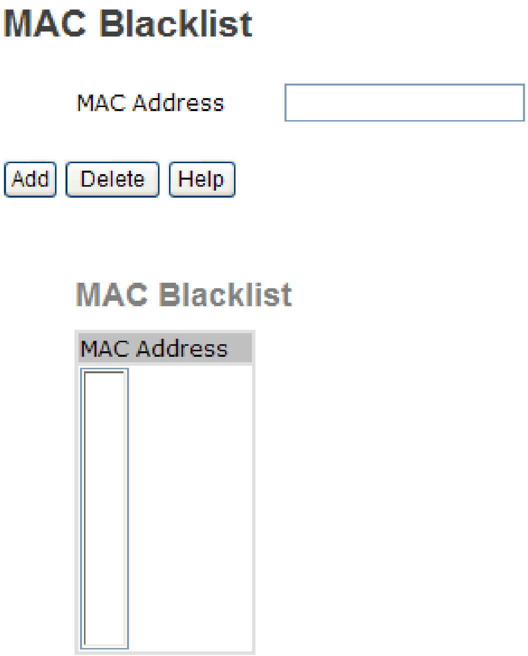
Port Security interface

The following table describes the labels in this screen.

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

5.1.9.3 MAC Blacklist

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



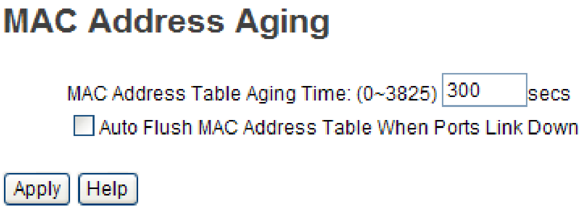
MAC Blacklist interface

The following table describes the labels in this screen.

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

5.1.9.4 MAC Address Aging

You can set MAC Address aging timer, as time expired, the unused MAC will be cleared from MAC table. IES-2206F-II also support Auto Flush MAC Address Table When ports Link Down.



MAC Address Table Aging Time: (0~3825) 300 secs

□ Auto Flush MAC Address Table When Ports Link Down

MAC Address Aging interface

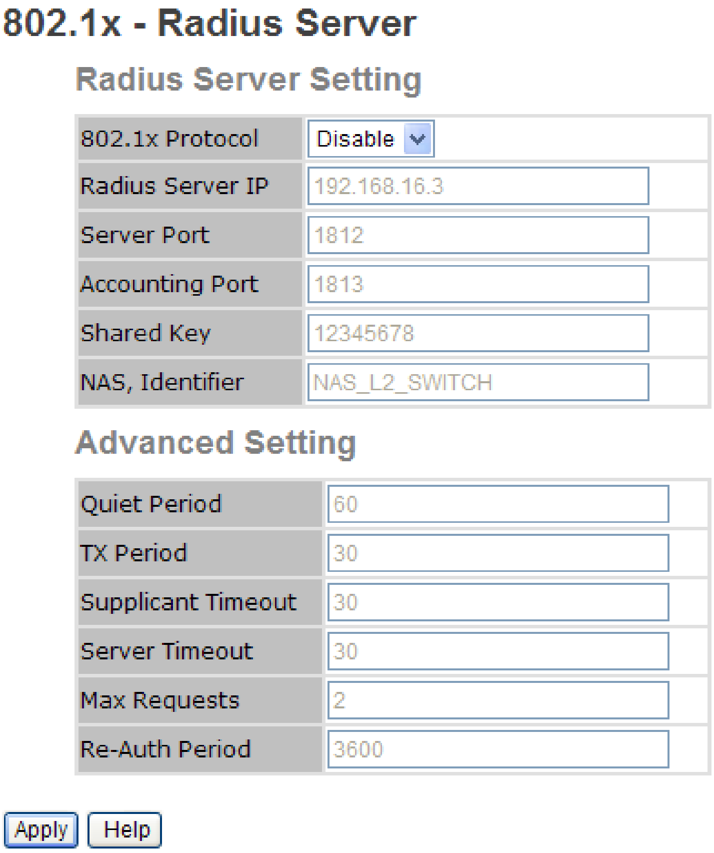
The following table describes the labels in this screen.

Label	Description
MAC Address Table Aging Time: (0to3825)	Set the timer.
Auto Flush MAC Address Table When ports Link Down.	Mark the blank to enable the function,
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.1.9.5 802.1x

802.1x - Radius Server

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



802.1x - Radius Server

Radius Server Setting

802.1x Protocol	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

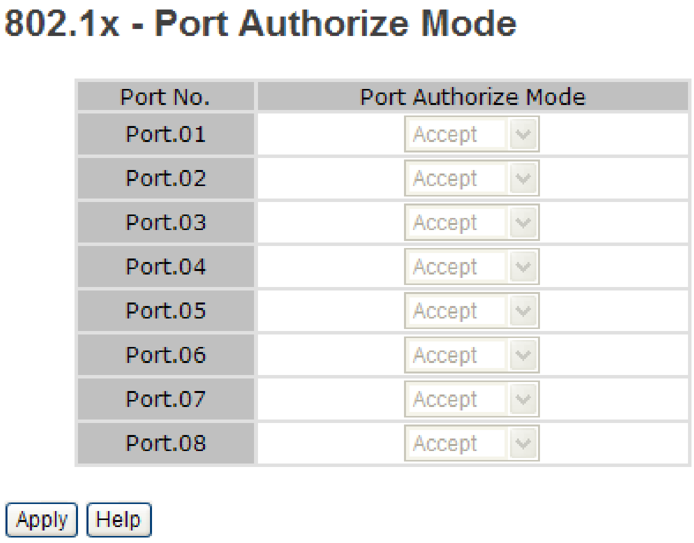
The following table describes the labels in this screen.

Label	Description
Radius Server Setting	

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

802.1x-Port Authorized Mode

Set the 802.1x authorized mode of each port.



802.1x - Port Authorize 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
Port.08	Accept

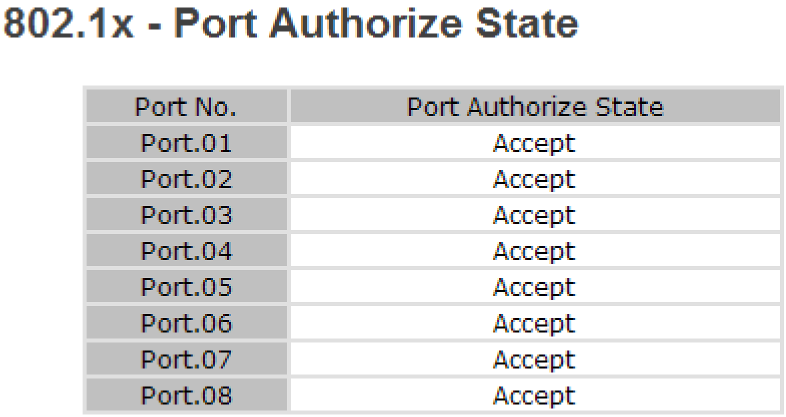
802.1x Port Authorize interface

The following table describes the labels in this screen.

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

802.1x-Port Authorized Mode

Show 802.1x port authorized state.



802.1x - Port Authorize State

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

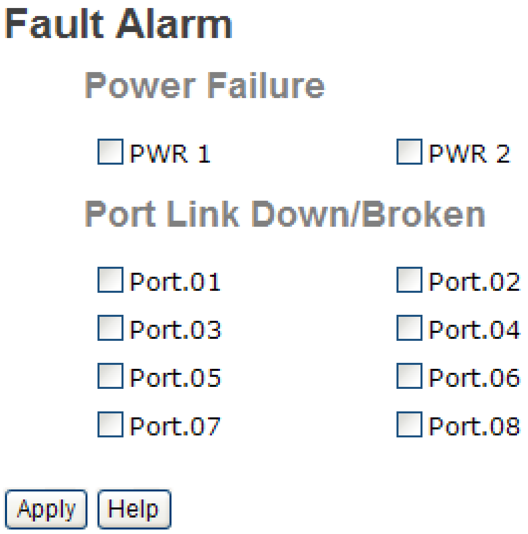
802.1x Port Authorize State interface

5.1.10 Warning

Warning function is very important for managing switch. You can manage switch by SYSLOG, E-MAIL, and Fault Relay. It helps you to monitor the switch status on remote site. When events occurred, the warning message will send to your appointed server, E-MAIL, or relay fault to switch panel.

5.1.10.1 Fault Alarm

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



Fault Alarm

Power Failure

□ PWR 1　□ PWR 2

Port Link Down/Broken

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

Fault Alarm interface

The following table describes the labels in this screen.

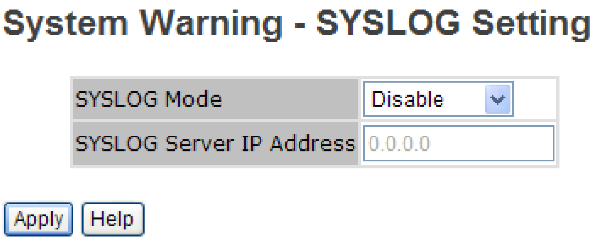
Label	Description
Power Failure	Mark the blank of PWR 1 or PWR 2 to monitor.
Port Link Down/Broken	Mark the blank of port 1 to port 8 to monitor.
Apply	Click “**Apply**” to set the configurations.
Help	Show help file.

5.1.10.2 System Alarm

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

SYSLOG Mode	Disable
SYSLOG Server IP Address	0.0.0.0

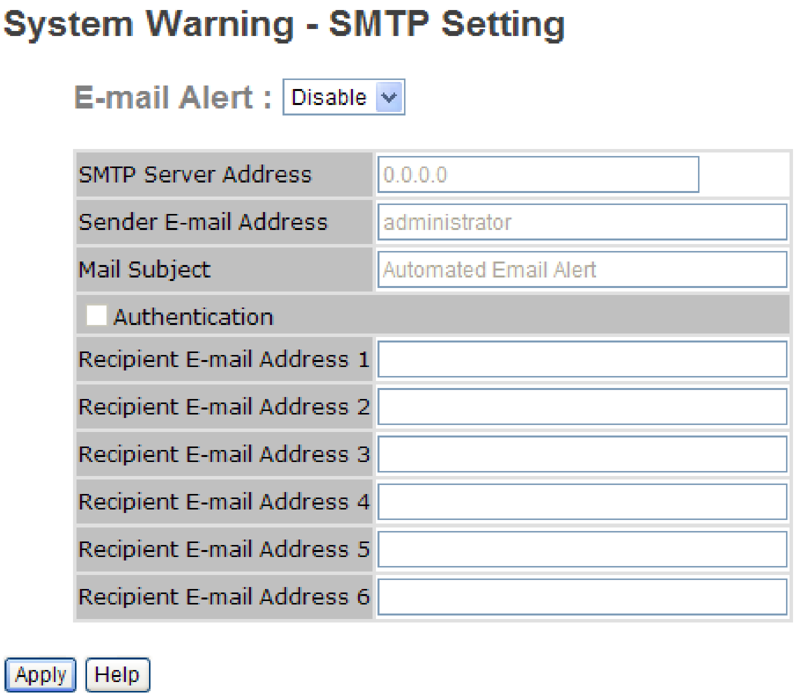
System Warning – SYSLOG Setting interface

The following table describes the labels in this screen.

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

System Warning – SMTP Setting.

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



System Warning - SMTP Setting

E-mail Alert : Disable

SMTP Server Address	0.0.0.0
Sender E-mail Address	administrator
Mail Subject	Automated Email Alert
□ Authentication	
Recipient E-mail Address 1	
Recipient E-mail Address 2	
Recipient E-mail Address 3	
Recipient E-mail Address 4	
Recipient E-mail Address 5	
Recipient E-mail Address 6	

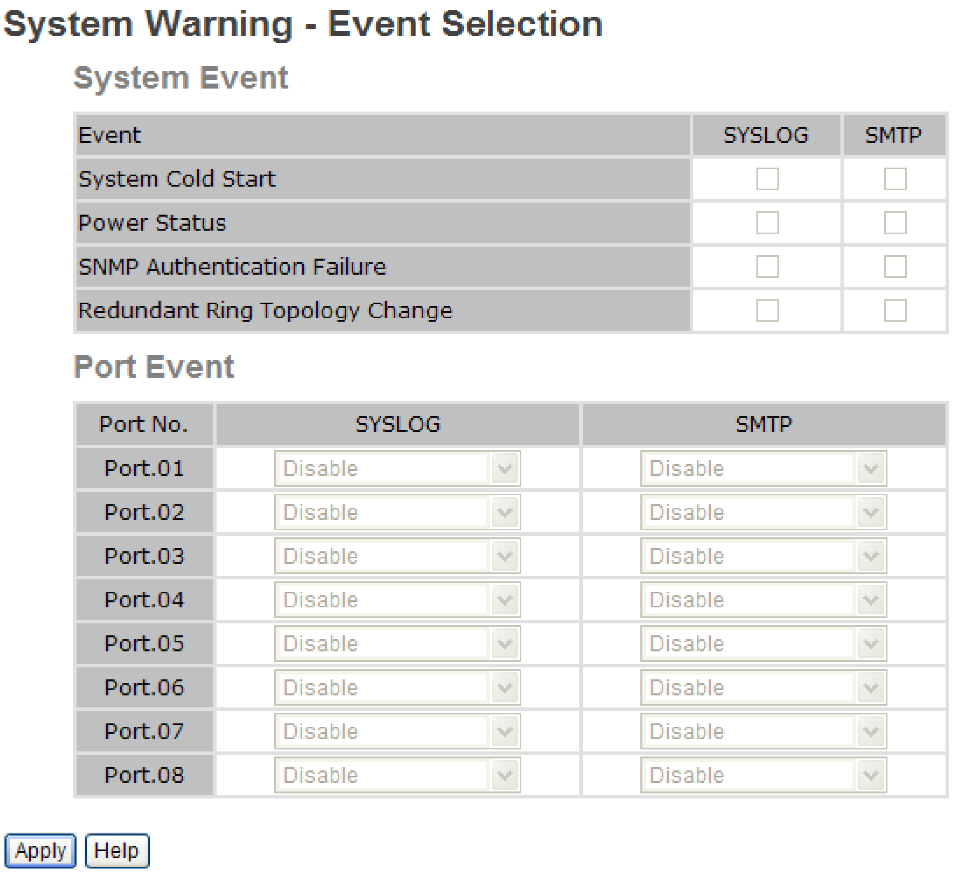
System Warning – SMTP Setting interface

The following table describes the labels in this screen.

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

System Warning – Event Selection

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



System Warning - Event Selection

System Event

Event	SYSLOG	SMTP
System Cold Start	□	□
Power Status	□	□
SNMP Authentication Failure	□	□
Redundant Ring Topology Change	□	□

Port Event

Port No.	SYSLOG	SMTP
Port.01	Disable	Disable
Port.02	Disable	Disable
Port.03	Disable	Disable
Port.04	Disable	Disable
Port.05	Disable	Disable
Port.06	Disable	Disable
Port.07	Disable	Disable
Port.08	Disable	Disable

System Warning – Event Selection interface

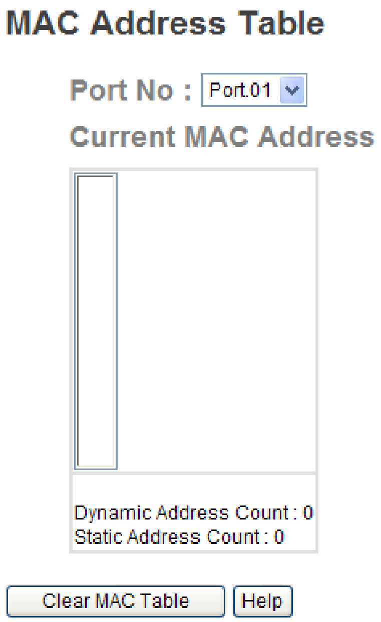
The following table describes the labels in this screen.

Label	Description
System Event	
System Cold Start	Alert when system restart
Power Status	Alert when a power up or down
SNMP Authentication Failure	Alert when SNMP authentication failure.
X-Ring Topology Change	Alert when X-Ring topology changes.
Port Event	■ **Disable** ■ **Link Up** ■ **Link Down** ■ **Link Up & Link Down**
Apply	Click “**Apply**” to set the configurations.
Help	Show help file.

5.1.11 Monitor and Diag

5.1.11.1 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 : Port.01

Current MAC Address

Dynamic Address Count : 0
Static Address Count : 0

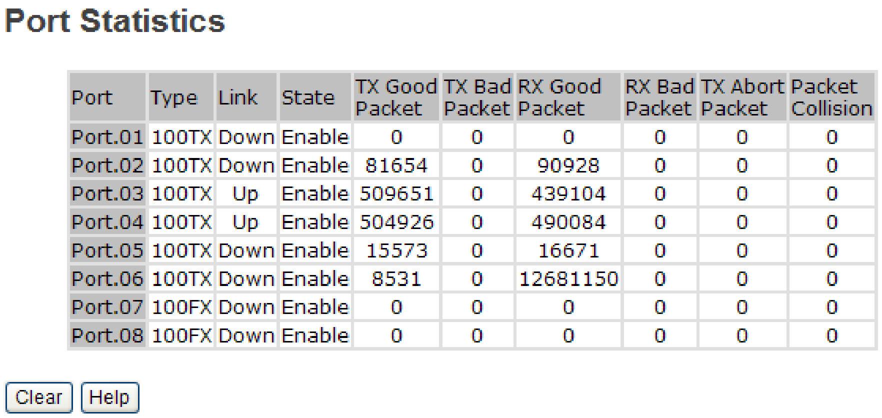
MAC Address Table interface

The following table describes the labels in this screen.

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

5.1.11.2 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	81654	0	90928	0	0	0
Port.03	100TX	Up	Enable	509651	0	439104	0	0	0
Port.04	100TX	Up	Enable	504926	0	490084	0	0	0
Port.05	100TX	Down	Enable	15573	0	16671	0	0	0
Port.06	100TX	Down	Enable	8531	0	12681150	0	0	0
Port.07	100FX	Down	Enable	0	0	0	0	0	0
Port.08	100FX	Down	Enable	0	0	0	0	0	0

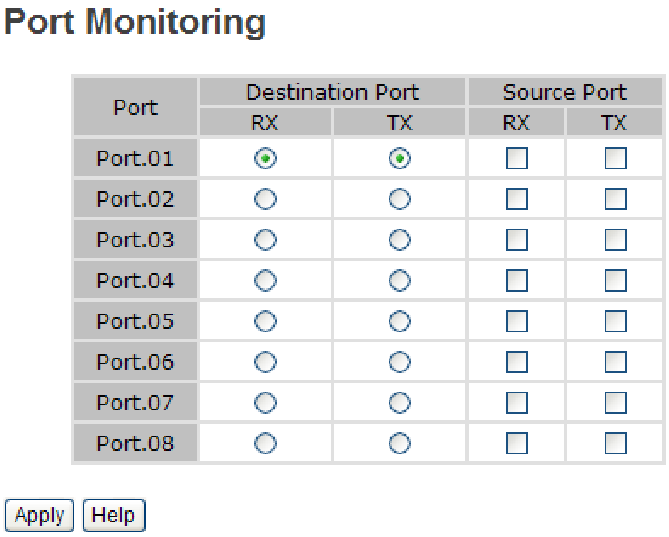
Port Statistics interface

The following table describes the labels in this screen.

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

5.1.11.3 Port Monitoring

Port monitoring supports TX (egress) only, RX (ingress) only, and TX/RX monitoring. TX monitoring sends any data that egress out checked TX source ports to a selected TX destination port as well. RX monitoring sends any data that ingress in checked RX source ports out to a selected RX destination port as well as sending the frame where it normally would have gone. Note that keep all source ports unchecked in order to disable port monitoring.



Port Monitoring

Port	Destination Port		Source Port	
	RX	TX	RX	TX
Port.01	●	●	□	□
Port.02	○	○	□	□
Port.03	○	○	□	□
Port.04	○	○	□	□
Port.05	○	○	□	□
Port.06	○	○	□	□
Port.07	○	○	□	□
Port.08	○	○	□	□

Port monitoring interface

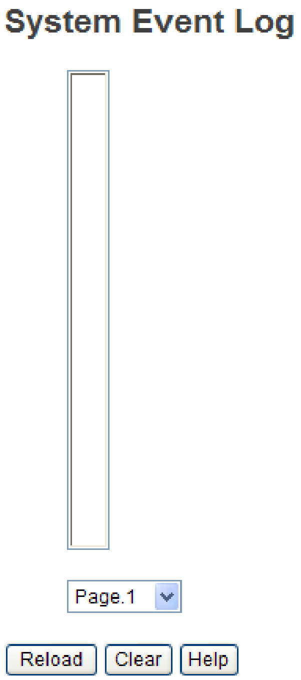
The following table describes the labels in this screen.

Label	Description
Destination Port	The port will receive a copied frame from source port for

	monitoring purpose.
Source Port	The port will be monitored. Mark the blank of TX or RX to be monitored.
TX	The frames come into switch port.
RX	The frames receive by switch port.
Apply	Click “**Apply**” to set the configurations.
Clear	Clear all marked blank.(disable the function)
Help	Show help file.

5.1.11.4 System Event Log

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



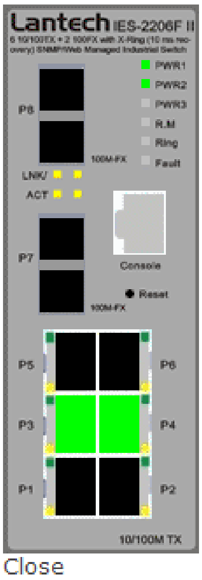
System event log interface

The following table describes the labels in this screen.

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

5.1.12 Front Panel

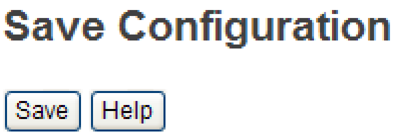
Show IES-2206F-II panel. Click "**Close**" to close panel on web.



Front Panel interface

5.1.13 Save Configuration

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



System Configuration interface

The following table describes the labels in this screen.

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

6

Command Line Interface Management

Configuration by Command Line Interface (CLI).

6.1 About CLI Management

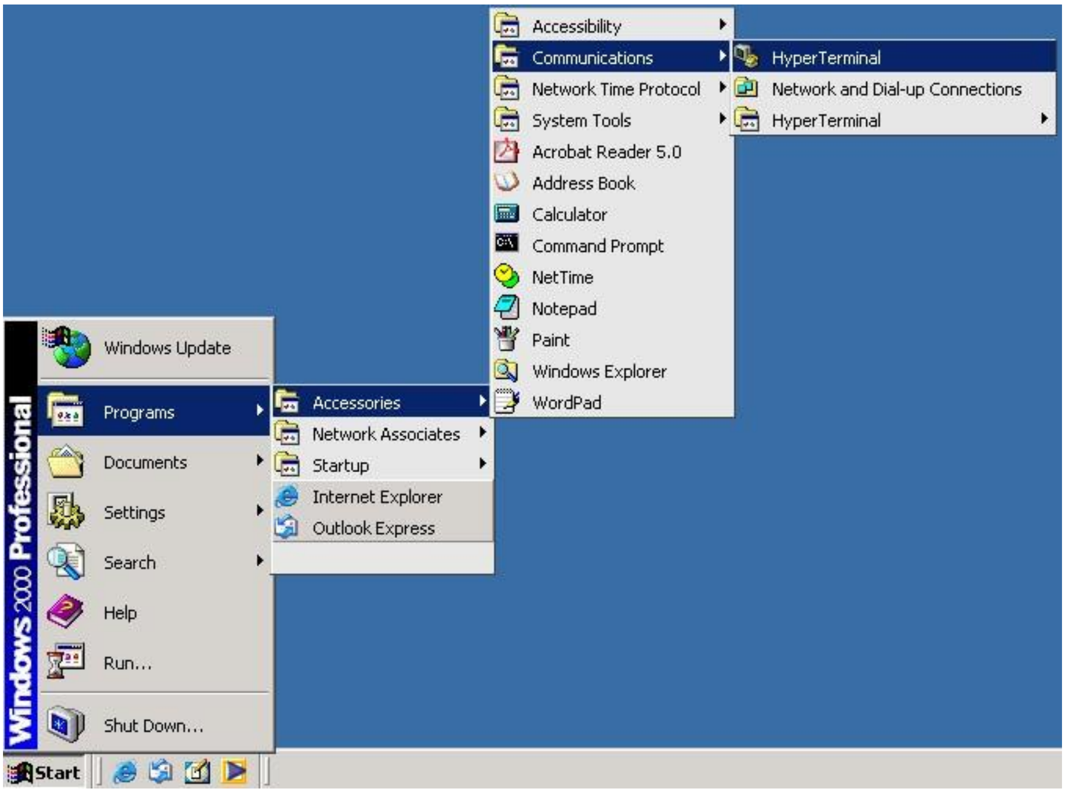
Besides WEB-base management, IES-2206F-II also support CLI management. You can use console or telnet to management switch by CLI.

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

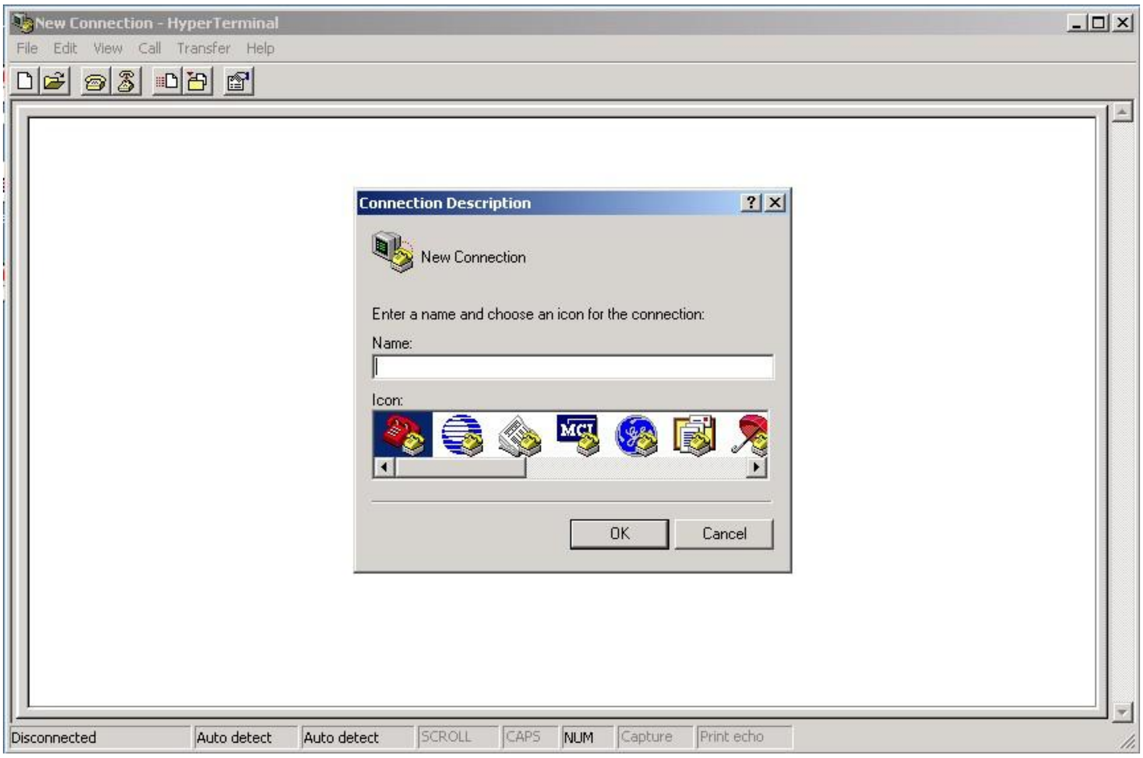
Before Configuring by RS-232 serial console, use an RJ45 to DB9-F cable to connect the Switches' RS-232 Console port to your PC's COM port.

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

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



(2)Input a name for new connection



New Connection - HyperTerminal

Connection Description

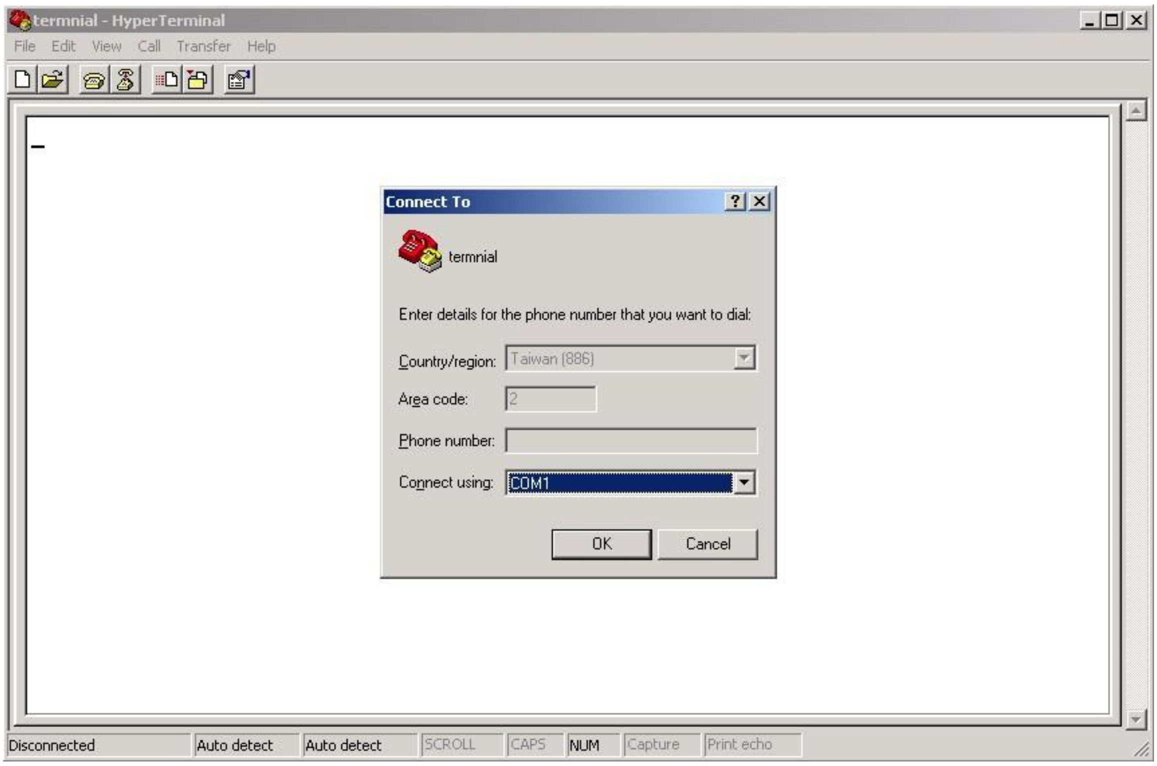
New Connection

Enter a name and choose an icon for the connection:

Name:

Icon:

(3)Select to use COM port number



termnial - HyperTerminal

Connect To

termnial

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

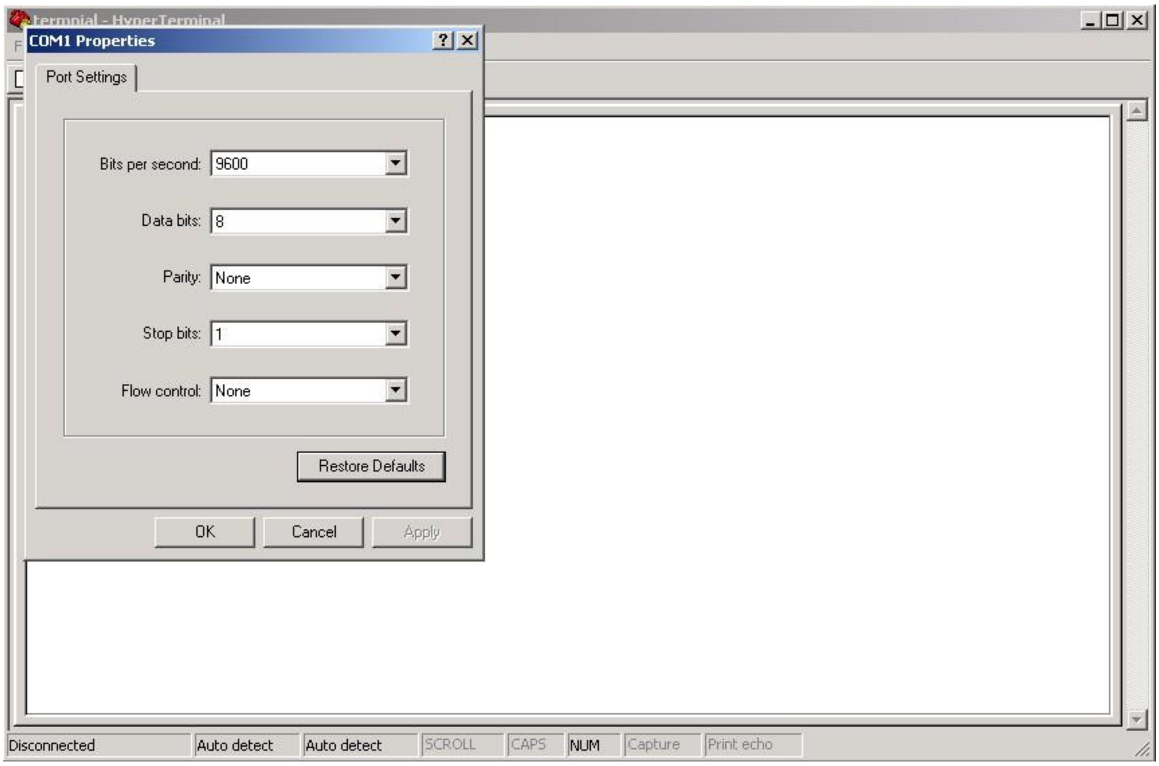
Country/region: Taiwan (886)

Area code: 2

Phone number:

Connect using: COM1

(4) The COM port properties setting, 9600 for Bits per second, 8 for Data bits, None for Parity, 1 for Stop bits and none for Flow control.



COM1 Properties

Bits per second: 9600

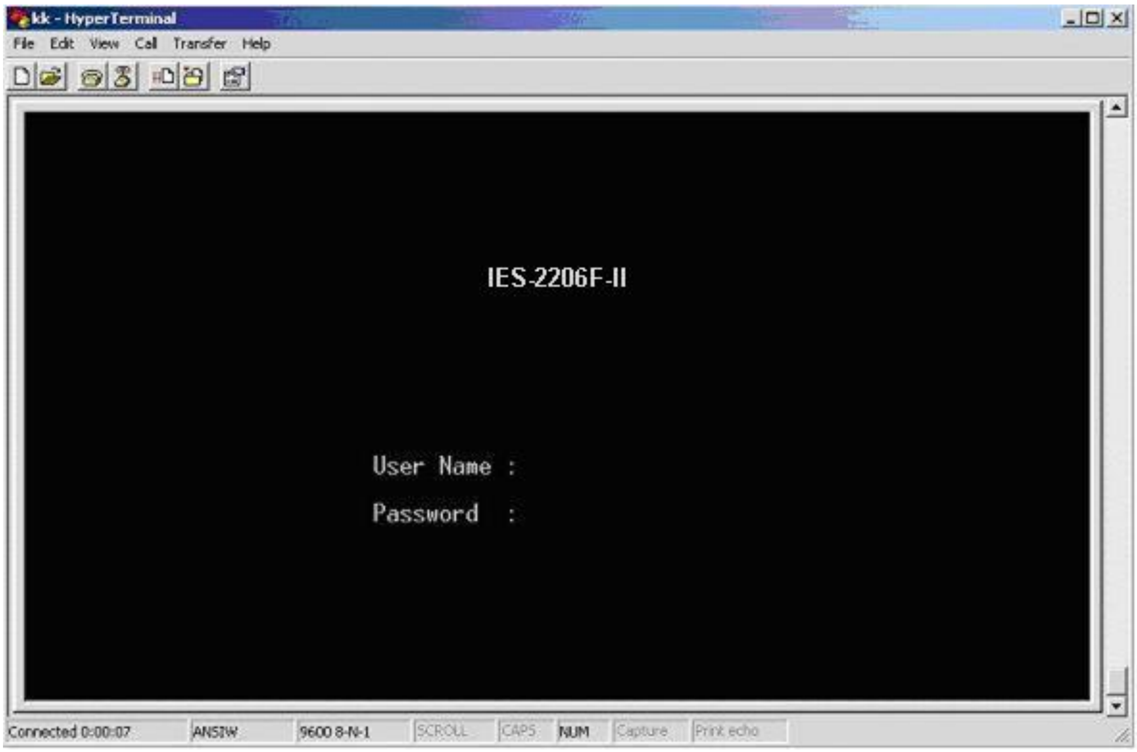
Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

(5) The Console login screen will appear. Use the keyboard enter the Console Username and Password that is same as the Web Browser password), and then press “**Enter**”.



```
IES-2206F-II

User Name :
Password  :
```

CLI Management by Telnet.

Users can use telnet to configure the switches.

The default value is as below:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

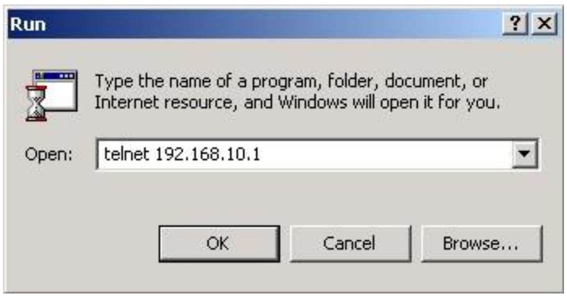
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

Follow the steps below to access the console via Telnet.

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

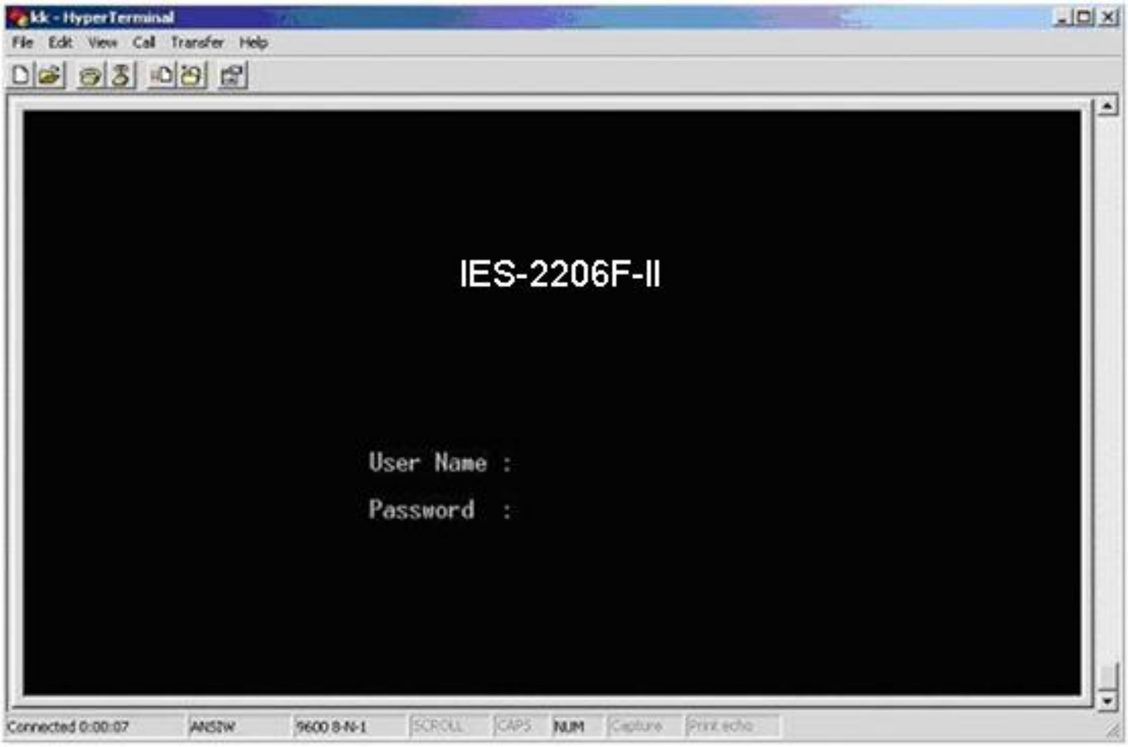


Run

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

Open: telnet 192.168.10.1

(2) The Console login screen will appear. Use the keyboard enter the Console Username and Password that is same as the Web Browser password), and then press "**Enter**"



kk - HyperTerminal

```
IES-2206F-II

User Name :
Password  :
```

Connected 0:00:07 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Commands Level

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

Symbol of Command Level.

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

6.2 Commands Set List—System Commands Set

IES-2206F-II Commands	Level	Description	Example
show config	**E**	Show switch configuration	switch>show config
show terminal	**P**	Show console information	switch#show terminal
menu	**E**	Enter MENU mode	switch>menu
write memory	**P**	Save your configuration into permanent memory (flash rom)	switch#write memory
system name **[System Name]**	**G**	Configure system name	switch(config)#system name xxx
system location **[System Location]**	**G**	Set switch system location string	switch(config)#system location xxx
system description **[System Description]**	**G**	Set switch system description string	switch(config)#system description xxx
system contact **[System Contact]**	**G**	Set switch system contact window string	switch(config)#system contact xxx
show system-info	**E**	Show system information	switch>show system-info
ip address **[Ip-address]** **[Subnet-mask] [Gateway]**	**G**	Configure the IP address of switch	switch(config)#ip address 192.168.1.1 255.255.255.0 192.168.1.254
ip dhcp	**G**	Enable DHCP client function of switch	switch(config)#ip dhcp
show ip	**P**	Show IP information of switch	switch#show ip

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

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

6.3 Commands Set List—Port Commands Set

IES-2206F-II Commands	Level	Description	Example
interface fastEthernet **[Portid]**	**G**	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex **[full | half]**	**I**	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
speed **[10|100|1000|auto]**	**I**	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can’t be set to 1000 if the port isn’t a giga port..	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
flowcontrol mode **[Symmetric|Asymmetric]**	**I**	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion.	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol mode Asymmetric

no flowcontrol	I	Disable flow control of interface	switch(config-if)#no flowcontrol
security enable	I	Enable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#security enable
no security	I	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
bandwidth type all	I	Set interface ingress limit frame type to "accept all frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to "accept broadcast, multicast, and flooded unicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to "accept broadcast and multicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast
bandwidth type broadcast-only	I	Set interface ingress limit frame type to "only accept broadcast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only
bandwidth in **[Value]**	I	Set interface input	switch(config)#interface fastEthernet 2

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

		form of this command to disable the port.	
show interface configuration	I	show interface configuration status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface configuration
show interface status	I	show interface actual status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface status
show interface accounting	I	show interface statistic counter	switch(config)#interface fastEthernet 2 switch(config-if)#show interface accounting
no accounting	I	Clear interface accounting information	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting

6.4 Commands Set List—Trunk command set

IES-2206F-II Commands	Level	Description	Example
aggregator priority [1to65535]	G	Set port group system priority	switch(config)#aggregator priority 22
aggregator activityport [Port Numbers]	G	Set activity port	switch(config)#aggregator activityport 2
aggregator group [GroupID] [Port-list] **lacp** **workp** [Workport]	G	Assign a trunk group with LACP active. [GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	switch(config)#aggregator group 1 1-4 lacp workp 2 or switch(config)#aggregator group 2 1,4,3 lacp workp 3
aggregator group [GroupID] [Port-list] **nolacp**	G	Assign a static trunk group. [GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#aggregator group 1 2-4 nolacp or switch(config)#aggreator group 1 3,1,2 nolacp
show aggregator	P	Show the information of trunk group	switch#show aggregator
no aggregator lacp [GroupID]	G	Disable the LACP function of trunk group	switch(config)#no aggreator lacp 1
no aggregator group [GroupID]	G	Remove a trunk group	switch(config)#no aggreator group 2

6.5 Commands Set List—VLAN command set

IES-2206F-II Commands	Level	Description	Example
vlan database	**P**	Enter VLAN configure mode	switch#vlan database
vlan **[8021q | gvrp]**	**V**	To set switch VLAN mode.	switch(vlan)# vlanmode 8021q or switch(vlan)# vlanmode gvrp
no vlan **[VID]**	**V**	Disable vlan group(by VID)	switch(vlan)#no vlan 2
no gvrp	**V**	Disable GVRP	switch(vlan)#no gvrp
IEEE 802.1Q VLAN			
vlan 8021q port **[PortNumber]** **access-link untag** **[UntaggedVID]**	**V**	Assign a access link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 8021q port 3 access-link untag 33
vlan 8021q port **[PortNumber]** **trunk-link tag** **[TaggedVID List]**	**V**	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 8021q port 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q port 3 trunk-link tag 3-20
vlan 8021q port **[PortNumber]** **hybrid-link untag** **[UntaggedVID]** **tag** **[TaggedVID List]**	**V**	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)# vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q port 3 hybrid-link untag 5 tag 6-8
vlan 8021q aggreator **[TrunkID]** **access-link untag** **[UntaggedVID]**	**V**	Assign a access link for VLAN by trunk group	switch(vlan)#vlan 8021q aggreator 3 access-link untag 33
vlan 8021q aggreator **[TrunkID]** **trunk-link tag** **[TaggedVID List]**	**V**	Assign a trunk link for VLAN by trunk group	switch(vlan)#vlan 8021q aggreator 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q aggreator 3 trunk-link tag 3-20
vlan 8021q aggreator **[PortNumber]**	**V**	Assign a hybrid link for VLAN by trunk group	switch(vlan)# vlan 8021q aggreator 3 hybrid-link untag 4 tag 3,6,8

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

6.6 Commands Set List—Spanning Tree command set

IES-2206F-II Commands	Level	Description	Example
spanning-tree enable	**G**	Enable spanning tree	switch(config)#spanning-tree enable
spanning-tree priority [0to61440]	**G**	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
spanning-tree max-age [seconds]	**G**	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)# spanning-tree max-age 15
spanning-tree hello-time [seconds]	**G**	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
spanning-tree forward-time [seconds]	**G**	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified	switch(config)# spanning-tree forward-time 20

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

		interface.	switch(config-if)# stp-admin-edge True
stp-admin-non-stp **[True|False]**	**I**	Admin NonSTP of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-non-stp False
Show spanning-tree	**E**	Display a summary of the spanning-tree states.	switch>show spanning-tree
no spanning-tree	**G**	Disable spanning-tree.	switch(config)#no spanning-tree

6.7 Commands Set List—QoS command set

IES-2206F-II Commands	Level	Description	Example
qos policy **[weighted-fair|strict]**	G	Select QOS policy scheduling	switch(config)#qos policy weighted-fair
qos prioritytype **[port-based|cos-only|tos-only|cos-first|tos-first]**	G	Setting of QOS priority type	switch(config)#qos prioritytype
qos priority portbased **[Port] [lowest|low|middle|high]**	G	Configure Port-based Priority	switch(config)#qos priority portbased 1 low
qos priority cos **[Priority][lowest|low|middle|high]**	G	Configure COS Priority	switch(config)#qos priority cos 22 middle
qos priority tos **[Priority][lowest|low|middle|high]**	G	Configure TOS Priority	switch(config)#qos priority tos 3 high
show qos	P	Display the information of QoS configuration	switch>show qos
no qos	G	Disable QoS function	switch(config)#no qos

6.8 Commands Set List—IGMP command set

IES-2206F-II Commands	Level	Description	Example
igmp enable	G	Enable IGMP snooping function	switch(config)#igmp enable
Igmp-query auto	G	Set IGMP query to auto mode	switch(config)#Igmp-query auto
Igmp-query force	G	Set IGMP query to force mode	switch(config)#Igmp-query force
show igmp configuration	P	Displays the details of an IGMP configuration.	switch#show igmp configuration
show igmp multi	P	Displays the details of an IGMP snooping entries.	switch#show igmp multi
no igmp	G	Disable IGMP snooping function	switch(config)#no igmp
no igmp-query	G	Disable IGMP query	switch#no igmp-query

6.9 Commands Set List—MAC/Filter Table command set

IES-2206F-II Commands	Level	Description	Example
mac-address-table static hwaddr **[MAC]**	I	Configure MAC address table of interface (static).	switch(config)#interface fastEthernet 2 switch(config-if)#mac-address-table static hwaddr 000012345678
mac-address-table filter hwaddr **[MAC]**	G	Configure MAC address table(filter)	switch(config)#mac-address-table filter hwaddr 000012348678
show mac-address-table	P	Show all MAC address table	switch#show mac-address-table
show mac-address-table static	P	Show static MAC address table	switch#show mac-address-table static
show mac-address-table filter	P	Show filter MAC address table.	switch#show mac-address-table filter
no mac-address-table static hwaddr **[MAC]**	I	Remove an entry of MAC address table of interface (static)	switch(config)#interface fastEthernet 2 switch(config-if)#no mac-address-table static hwaddr 000012345678
no mac-address-table filter hwaddr **[MAC]**	G	Remove an entry of MAC address table (filter)	switch(config)#no mac-address-table filter hwaddr 000012348678
no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#no mac-address-table

6.10 Commands Set List—SNMP command set

IES-2206F-II Commands	Level	Description	Example
snmp agent-mode [v1v2c | v3]	G	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2c
snmp-server host [IP address] **community** [Community-string] **trap-version** [v1|v2c]	G	Configure SNMP server host information and community string	switch(config)#snmp-server host 192.168.10.50 community public trap-version v1 (remove) Switch(config)# no snmp-server host 192.168.10.50
snmp community-strings [Community-string] **right** [RO|RW]	G	Configure the community string right	switch(config)#snmp community-strings public right RO or switch(config)#snmp community-strings public right RW
snmp snmpv3-user [User Name] **password** [Authentication Password] [Privacy Password]	G	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#snmp snmpv3-user test01 password AuthPW PrivPW
show snmp	P	Show SNMP configuration	switch#show snmp
show snmp-server	P	Show specified trap server information	switch#show snmp-server
no snmp community-strings [Community]	G	Remove the specified community.	switch(config)#no snmp community-strings public
no snmp snmpv3-user [User Name] **password** [Authentication Password] [Privacy Password]	G	Remove specified user of SNMPv3 agent. Privacy password could be empty.	switch(config)# no snmp snmpv3-user test01 password AuthPW PrivPW
no snmp-server host [Host-address]	G	Remove the SNMP server host.	switch(config)#no snmp-server 192.168.10.50

6.11 Commands Set List—Port Mirroring command set

IES-2206F-II Commands	Level	Description	Example
monitor rx	**G**	Set RX destination port of monitor function	switch(config)#monitor rx
monitor tx	**G**	Set TX destination port of monitor function	switch(config)#monitor tx
show monitor	**P**	Show port monitor information	switch#show monitor
monitor [RX|TX|Both]	**I**	Configure source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#monitor RX
show monitor	**I**	Show port monitor information	switch(config)#interface fastEthernet 2 switch(config-if)#show monitor
no monitor	**I**	Disable source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#no monitor

6.12 Commands Set List—802.1x command set

IES-2206F-II Commands	Level	Description	Example
8021x enable	G	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiousip **[IP address]**	G	Use the 802.1x system radious IP global configuration command to change the radious server IP.	switch(config)# 8021x system radiousip 192.168.1.1
8021x system serverport **[port ID]**	G	Use the 802.1x system server port global configuration command to change the radious server port	switch(config)# 8021x system serverport 1815
8021x system accountport **[port ID]**	G	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# 8021x system accountport 1816
8021x system sharekey **[ID]**	G	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# 8021x system sharekey 123456
8021x system nasid **[words]**	G	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# 8021x system nasid test1
8021x misc quietperiod **[sec.]**	G	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# 8021x misc quietperiod 10
8021x misc txperiod **[sec.]**	G	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# 8021x misc txperiod 5

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

6.13 Commands Set List—TFTP command set

IES-2206F-II Commands	Level	Description	Defaults Example
backup flash:backup_cfg	**G**	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#backup flash:backup_cfg
restore flash:restore_cfg	**G**	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)#restore flash:restore_cfg
upgrade flash:upgrade_fw	**G**	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#upgrade lash:upgrade_fw

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

IES-2206F-II Commands	Level	Description	Example
systemlog ip **[IP address]**	G	Set System log server IP address.	switch(config)# systemlog ip 192.168.1.100
systemlog mode **[client|server|both]**	G	Specified the log mode	switch(config)# systemlog mode both
show systemlog	E	Display system log.	Switch>show systemlog
show systemlog	P	Show system log client & server information	switch#show systemlog
no systemlog	G	Disable systemlog functon	switch(config)#no systemlog
smtp enable	G	Enable SMTP function	switch(config)#smtp enable
smtp serverip **[IP address]**	G	Configure SMTP server IP	switch(config)#smtp serverip 192.168.1.5
smtp authentication	G	Enable SMTP authentication	switch(config)#smtp authentication
smtp account **[account]**	G	Configure authentication account	switch(config)#smtp account User
smtp password **[password]**	G	Configure authentication password	switch(config)#smtp password
smtp rcptemail **[Index] [Email address]**	G	Configure Rcpt e-mail Address	switch(config)#smtp rcptemail 1 Alert@test.com
show smtp	P	Show the information of SMTP	switch#show smtp
no smtp	G	Disable SMTP function	switch(config)#no smtp
event device-cold-start **[Systemlog|SMTP|Both]**	G	Set cold start event type	switch(config)#event device-cold-start both
event authentication-failure **[Systemlog|SMTP|Both]**	G	Set Authentication failure event type	switch(config)#event authentication-failure both
event X-Ring-topology-change **[Systemlog|SMTP|Both]**	G	Set s ring topology changed event type	switch(config)#event X-Ring-topology-change both
event systemlog	I	Set port event for	switch(config)#interface fastethernet

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

6.15 Commands Set List—SNTP command set

IES-2206F-II Commands	Level	Description	Example
sntp enable	G	Enable SNTP function	switch(config)#sntp enable
sntp daylight	G	Enable daylight saving time, if SNTP function is inactive, this command can’t be applied.	switch(config)#sntp daylight
sntp daylight-period **[Start time] [End time]**	G	Set period of daylight saving time, if SNTP function is inactive, this command can’t be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# sntp daylight-period 20060101-01:01 20060202-01-01
sntp daylight-offset **[Minute]**	G	Set offset of daylight saving time, if SNTP function is inactive, this command can’t be applied.	switch(config)#sntp daylight-offset 3
sntp ip **[IP]**	G	Set SNTP server IP, if SNTP function is inactive, this command can’t be applied.	switch(config)#sntp ip 192.169.1.1
sntp timezone **[Timezone]**	G	Set timezone index, use “show sntp timzezone” command to get more information of index number	switch(config)#sntp timezone 22
show sntp	P	Show SNTP information	switch#show sntp
show sntp timezone	P	Show index number of time zone list	switch#show sntp timezone
no sntp	G	Disable SNTP function	switch(config)#no sntp
no sntp daylight	G	Disable daylight saving time	switch(config)#no sntp daylight

6.16 Commands Set List—Pro-Ring command set

IES-2206F-II Commands	Level	Description	Example
Ring enable	**G**	Enable X-Ring	switch(config)# X-Ring enable
Ring master	**G**	Enable ring master	switch(config)# X-Ring master
Ring couplering	**G**	Enable couple ring	switch(config)# X-Ring couplering
Ring dualhoming	**G**	Enable dual homing	switch(config)# X-Ring dualhoming
Ring ringport **[1st Ring Port] [2nd Ring Port]**	**G**	Configure 1st/2nd Ring Port	switch(config)# X-Ring ringport 7 8
Ring couplingport **[Coupling Port]**	**G**	Configure Coupling Port	switch(config)# X-Ring couplingport 1
Ring controlport **[Control Port]**	**G**	Configure Control Port	switch(config)# X-Ring controlport 2
Ring homingport **[Dual Homing Port]**	**G**	Configure Dual Homing Port	switch(config)# X-Ring homingport 3
show Ring	**P**	Show the information of X-Ring	switch#show X-Ring
no Ring	**G**	Disable X-Ring	switch(config)#no X-Ring
no Ring master	**G**	Disable ring master	switch(config)# no X-Ring master
no Ring couplering	**G**	Disable couple ring	switch(config)# no X-Ring couplering
no Ring dualhoming	**G**	Disable dual homing	switch(config)# no X-Ring dualhoming

7

Technical Specifications

Technology	
Ethernet Standards	802.3-10BaseT, 802.3u-100BaseTX, 100BaseFX, 802.3x- 802.3z-1000BaseLX, 802.3ab-1000BaseTX, 802.3ad-, 802.1d-MAC Bridges, 802.1d-, 802.1p-Class of Service, 802.1q-, 802.1w-Rapid Spanning Tree Protocol, 802.1x-Port Based Network Access Control, 802.1s – MSTP (optional feature)
MAC addresses	8192
Priority Queues	4
Flow Control	IEEE 802.3x Flow Control and Back-pressure
Processing	Store-and-Forward
Interface	
RJ45 Ports	6 x 10/100Base-T(X), Auto MDI/MDI-X
Fiber Ports	2 x 100 Base-FX(SC Connector) Multi-Mode: Up to 2 km, 1310 nm (50/125 µm to 62.5/125 µm) Single-Mode: Up to 30 km, 1310 nm (9/125µm)
LED Indicators	Per Unit : Power x 3(Green) RJ45 Ports: Per Port : Link/Activity(Green/Blinking Green), Full duplex(Amber) Fiber Ports: Per Port : Activity(Green),Link (Amber)
Power Requirements	
Power Input Voltage	PWR1/2: 12 to 48VDC in 7-pin Terminal Block PWR3: 12 to 45VDC in Power Jack
Reverse Polarity	Present

Protection	
Power Consumption	10 Watts Max
Environmental	
Operating Temperature	-20 to 60 ^{o}C (Wide temperature model -40 to 75^{o}C)
Storage Temperature	-20 to 85 ^{o}C
Operating Humidity	5% to 95%, non-condensing
Mechanical	
Dimensions(W x D x H)	52 mm(W)x 106 mm(D)x 144 mm(H)
Casing	IP-30 protection
Regulatory Approvals	
Regulatory Approvals	CE class A RoHS
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), Level 3, EN61000-4-6 (CS), Level 3
Shock	IEC60068-2-27
Free Fall	IEC 60068-2-32
Vibration	IEC 60068-2-6