Case Communications

IFE-8T2GB-MXE

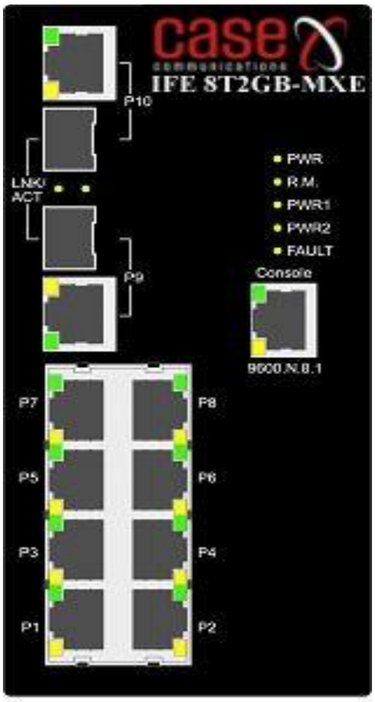
Ethernet Switch

8 10/100TX + 2 10/100/1000T/Mini-GBIC

Combo with X-Ring

L2 Managed Industrial Switch

User Manual



Notice

The contents of this manual are based on the following software kernel version, hardware version, and firmware version. If the switch functionality differs from the manual description, please contact your local Case Communications' reseller for more information.

Manual Date	Feb 2011 V1.6
Firmware Version	V1.02K293
Kernel Version	V1.40
Hardware Version	----------

FCC Warning

The Case Communications IFE-8T2GB-MXE has been tested and found to comply with standards for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

The Case Communications IFE-8T2GB-MXE Industrial Switch is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Content

APPENDIX A

APPENDIX B

Introduction

The Case Communications IFE-8T2GB-MXE is a Layer 2 Managed Industrial Switch which has been designed to meet the highest levels of reliability as demanded by industrial applications. The IFE-8T2GB-MXE can be easily managed through the Web GUI or via a Command Line Interface (CLI). The fibre optic ports can extend the distance over which the switches can operate increasing network flexibility and performance. The IFE-8T2GB-MXE supports X-Ring technology which provides network re-routing of under 10ms in the event of a link or switch failing.

Features

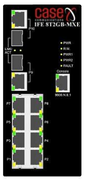
- System Interface/Performance
  - RJ-45 port support Auto MDI/MDI-X Function
  - SFP (mini-GBIC) supports 100/1000 Dual Mode
  - Store-and-Forward Switching Architecture
  - Back-plane (Switching Fabric): 5.6Gbps
  - 1Mbits Packet Buffer
  - 8K MAC Address Table
- Power Supply
  - Wide-range Redundant Power Design
  - Power Polarity Reverse Protect
  - Overload Current Protection
- VLAN
  - Port Based VLAN
  - Support 802.1 Q Tag VLAN
  - GVRP
  - Double Tag VLAN (Q in Q)
  - Private VLAN
- Port Trunk with LACP
- QoS (Quality of Service)
  - Support IEEE 802.1p Class of Service,
  - Per port provides 4 priority queues
  - Port Base, Tag Base and Type of Service Priority

- Port Mirror: Monitor traffic in switched networks.
  - TX Packet only
  - RX Packet only
  - Both of TX and RX Packet
- Security
  - Port Security: MAC address entries/filter
  - IP Security: IP address security management to prevent unauthorized intruder.
  - Login Security: IEEE802.1X/RADIUS
- IGMP with Query mode for Multi Media Application
- Case/Installation
  - IP-30 Protection
  - DIN Rail and Wall Mount Design
- Spanning Tree
  - Support IEEE802.1d Spanning Tree
  - Support IEEE802.1w Rapid Spanning Tree
- X-ring
  - X-ring, Dual Homing, and Couple Ring Topology
  - Provide redundant backup feature and the recovery time below 300ms
- Supports IEEE 802.1ab LLDP**
- Bandwidth Control
  - Ingress Packet Filter and Egress Rate Limit
  - Broadcast/Multicast Packet Filter Control
- System Event Log
  - System Log Server/Client
  - SMTP e-mail Alert
  - Relay Alarm Output System Events
- SNMP Trap
  - Device cold start
  - Power status
  - Authentication failure
  - X-ring topology changed
  - Port Link up/Link down
- TFTP Firmware Update and System Configuration Restore and Backup

Package Contents

On receiving your IFE-8T2GB-MXE Ethernet switch please check the contents against the checklist below.

- IFE-8T2GB-MXE Switch
- User manual - either in Paper or CD Format
- RS-232/RJ-45 cable
- Block connector
- 2 wall mount plates and 6 screws
- One DIN-Rail (attached on the switch)

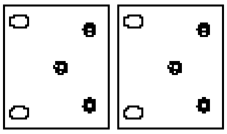


IFE-8T2GB-MXE

User Manual

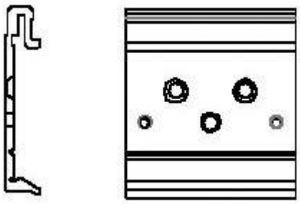
RS-232/RJ-45 connector cable

block connector



Wall Mount Plate

Screws



DIN-Rail

Compare the contents of the industrial switch with the standard checklist above. If any item is damaged or missing, please contact your local Case Communications dealer for service.

Hardware Description

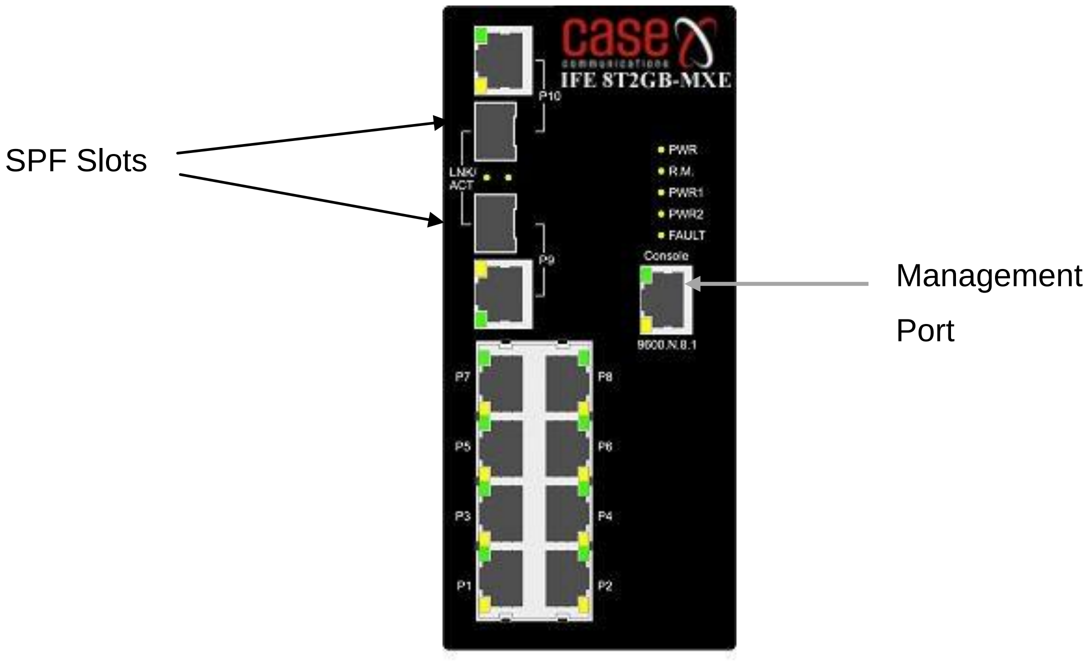
This paragraph, describes the IFE-8T2GB-MXE hardware spec, ports, cabling information, and wiring installation.

Physical Dimension

IFE-8T2GB-MXE Switch dimensions are (W x D x H) is **72mm x 105mm x 152mm**

Front Panel

The Front Panel of the IFE-8T2GB-MXE is shown below



Front Panel of the IFE-8T2GB-MXE

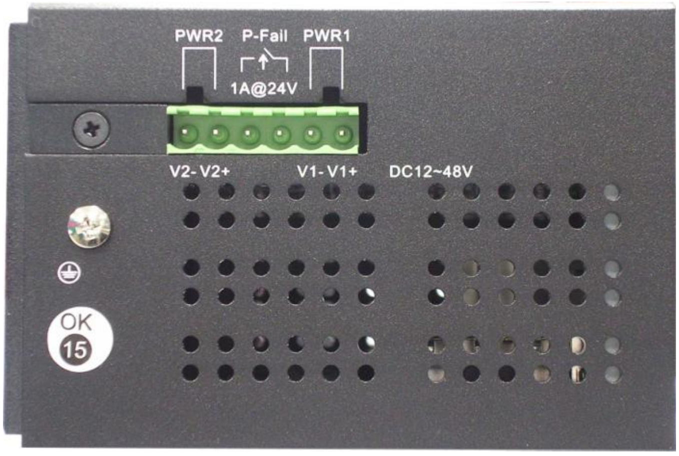
Top View

The top panel of the IFE-8T2GB-MXE has one terminal block connector for the two DC power inputs.

Pwr

V1- Negative

V+ Positive



Voltage

12Volt - 48 Vdc

Top Panel of the IFE-8T2GB-MXE

LED Indicators

The diagnostic LEDs are located on the front panel of the IFE-8T2GB-MX. They provide real-time information on the system and optional status. The following table provides a description of the LED status and their meaning.

LED	Status	Meaning
PWR	Green	The switch unit is power on
	Off	The switch unit is no power input
PWR1	Green	Power on
	Off	No power inputs
PWR2	Green	Power on
	Off	No power inputs

Fault	Red	Power failure or UTP port failure or Fibre port failure
	Off	No Power failure or UTP port failure or Fibre port failure occurs
R.M.	Green	The industrial switch is the master of the X-Ring group
	Off	The industrial switch is not a ring master in the X-Ring group
LNK/ACT (for P9, P10 SFP)	Green	SFP port is linking
	Blinks	Networking is active
	Off	No device attached
P9, P10 (RJ-45)	Green (Upper LED)	Network device detected
	Blinking (Upper LED)	Networking is active
	Off (Upper LED)	No device detected
	Green (Lower LED)	The port is operating at speed of 1000M
	Off (lower LED)	The port is disconnected or not operating at speed of 1000M
P1 ~ P8	Green (Upper LED)	Network device detected
	Blinking (Upper LED)	Networking is active
	Off (Upper LED)	No device attached

	Yellow (Lower LED)	The port is operating in full-duplex mode
	Blinking (Lower LED)	Collision of Packets occurs
	Off (Lower LED)	The port is in half-duplex mode or no device attached

Ports

- **RJ-45 ports**

The 10/100Mbps UTP/STP ports will auto-sense 10Base-T or 100Base-TX connections. Auto MDI/MDIX means that the switch can connect to another switch or workstation without needing to change cables to a straight through or crossover cable. The figures below show the wiring for both straight and crossover cables.

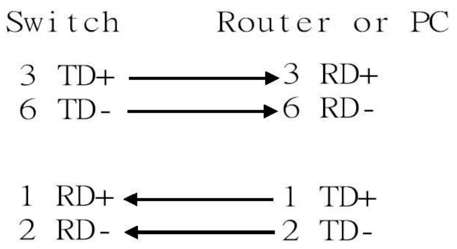
- **RJ-45 Pin Assignments**

Pin Number	Assignment
1	Tx+
2	Tx-
3	Rx+
6	Rx-

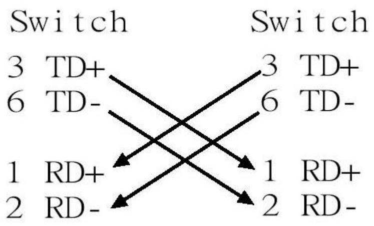
[NOTE] '+' and '–' signs represent the polarity of the wires that make up each wire pair.

All ports on the IFE-8T2GB-MXE support automatic MDI/MDI-X operation, users can use straight-through cables (See figure below) for all network connections to PCs or servers, or to other switches or hubs. With straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3 and 6 at the other end of the cable. The table below shows the 10BASE-T/100BASE-TX MDI and MDI-X port pin outs.

Pin MDI-X	Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)



Straight Through Cable Schematic



Cross Over Cable Schematic

- **2 Gigabit Copper/SFP (mini-GBIC) combo port:**

The IFE-8T2GB-MXEhas two auto-detect Gigabit ports—UTP / Fibre combo ports. The Gigabit Copper (10/100/1000T) ports should use Category 5e (or above) UTP/STP cables. The SFP slots are fitted with appropriate SFP's to connect the switch to single or multi-mode fiber, with the data rate (100Mbps or 1Gbps being derived from the SFP). Select an appropriate mini-GBIC module to plug into the slots. Make sure the module is aligned correctly and then slide the module into the SFP slot until a click is heard.

Both multi-mode and single-mode fibre can be supported using the appropriate SFP's. With fibre optic cable, transmission speeds up to 1000 Mbps and transmission media distances of up to 120 km, can be achieved depending on the mini-GBIC module.

The small form-factor pluggable (SFP) is a compact optical transceiver used in optical communications for both telecommunication and data communications applications.

To connect the transceiver and LC cable, please follow the steps shown below:

First, insert the transceiver into the SFP module. Notice that the triangle mark is the bottom of the module.

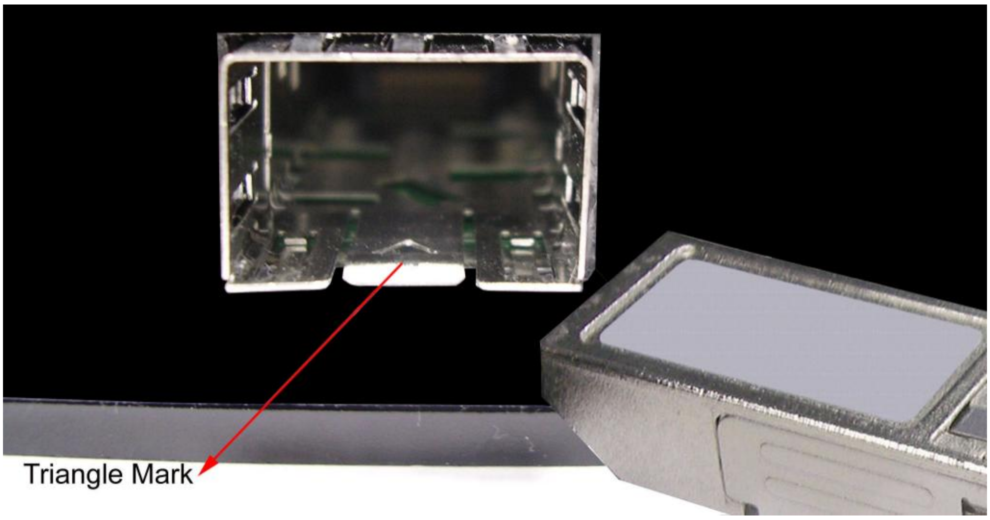


Figure 2.8: Transceiver to the SFP module

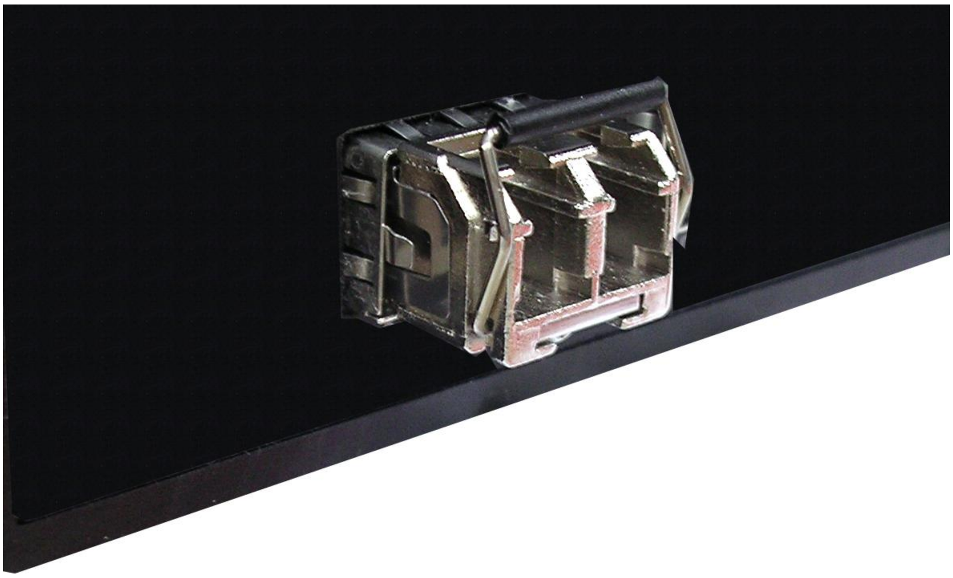


Figure 2.9: Transceiver Inserted

Second, insert the fibre cable of LC connector into the transceiver.

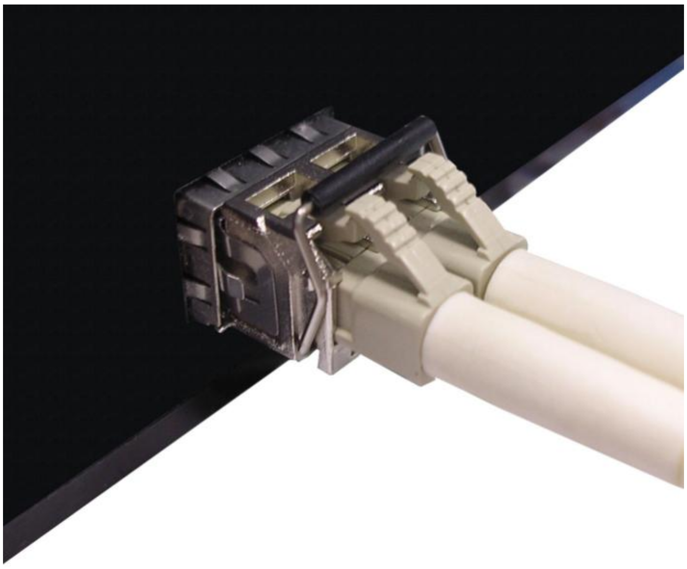


Figure 2.10: LC connector to the transceiver

To remove the LC connector from the transceiver, please follow the steps shown below:

First, press the upper side of the LC connector to release from the transceiver and pull it out.

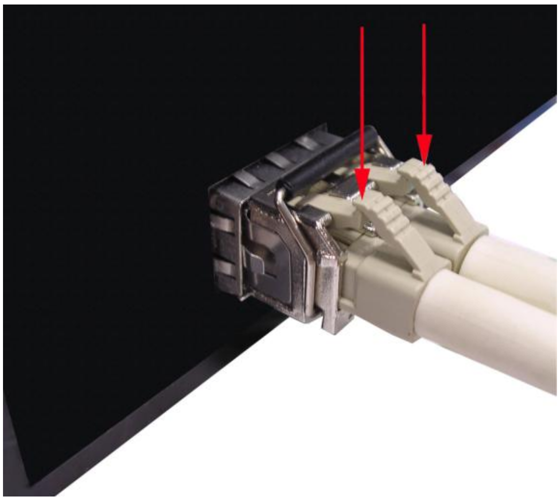


Figure 2.11: Remove LC connector

Second, push down the metal loop and pull the transceiver out by the plastic handle.

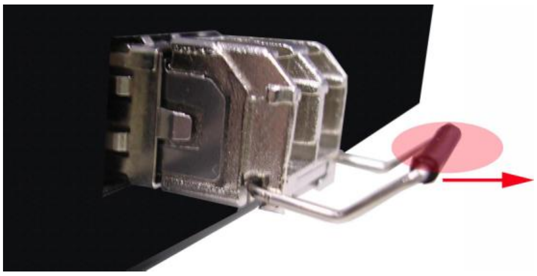


Figure 2.12: Pull out from the transceiver

Cabling

- **100TX –** Use a four twisted-pair cable, Category 5e or above cabling for RJ-45 port connection. The cable between the converter and the link partner (switch, hub, workstation, etc.) must be less than 100 meters (328 ft.) long.

- **single-mode** connectors must use 9/125 µm single-mode fibre cable. Users can connect two devices in the distance up to **30 Kilometers**.

- **multi-mode** connector must use 50 or 62.5/125 µm multi-mode fibre cable. Users can connect two devices up to **2Km** distances.

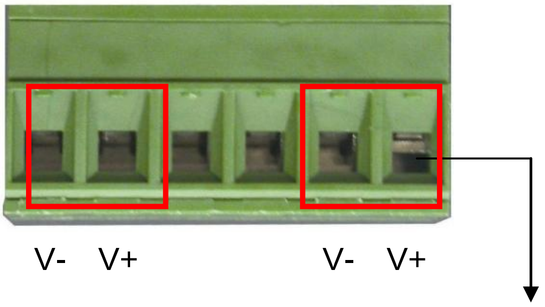
Notes on fibre distances.

The distance an SFP can drive a fibre cable is dependent on several factors and these must be taken into account when determining the distance the SFP's in the switches need to drive . The list below provides some of the factors to be taken into consideration.

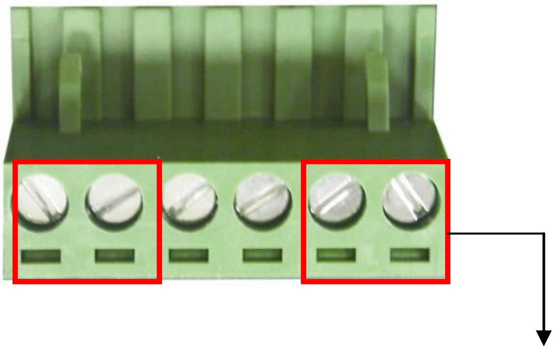
1. The quality of the Fibre cable
2. The number of splices in the cable – (every splice adds loss)
3. The age of the cable
4. Ambient temperature
5. The number of patch panels in the circuit
6. The number of times each patch lead has been removed and replaced (They can attract dirt which in turn increases cable loss)
7. The quality of the SFP – even the same models from the same manufacturer can vary. (Typically an SFP may transmit at +5db to -3db and receive levels maybe down to 25db)
8. Age of the SFP's.

Wiring the Power Inputs

Please follow the below steps to insert the power wire.



1. Insert the positive and negative wires into the V+ and V- contacts on the terminal block connector.



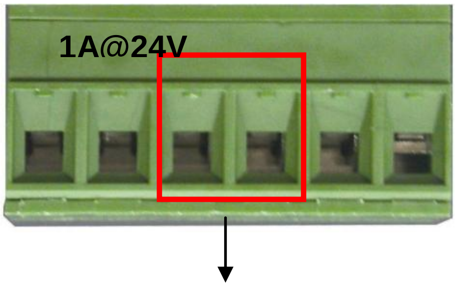
2. To tighten the wire-clamp screws for preventing the DC wires to loose.

[NOTE] The wire range of terminal block is from 12~ 24 AWG.

Wiring the Fault Alarm Contact

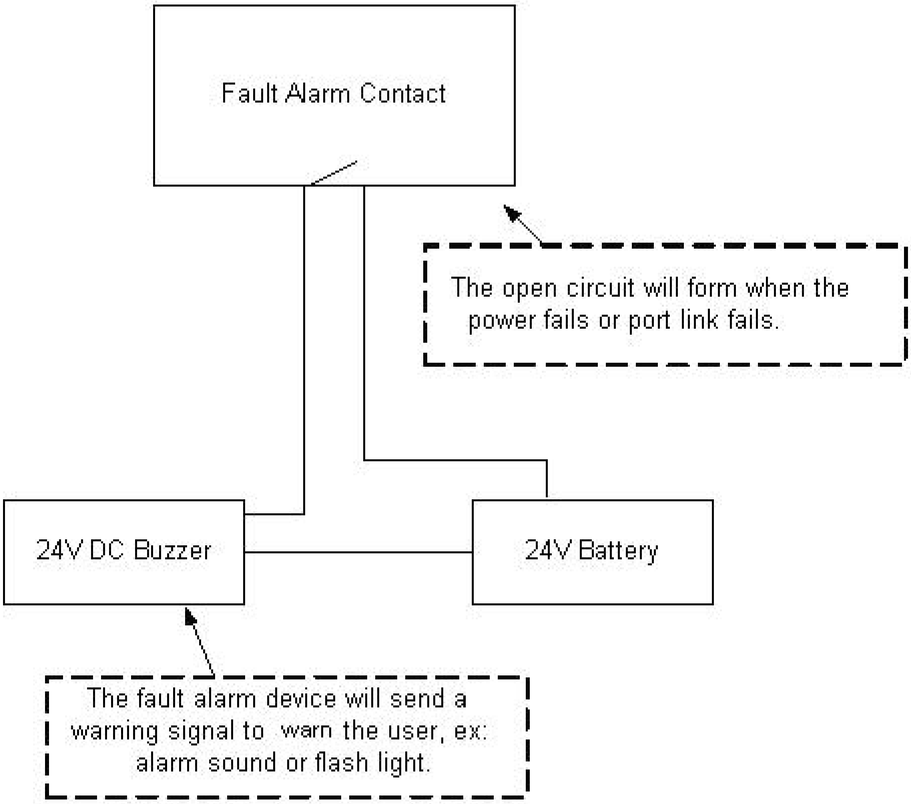
The external alarm contact is in the middle of a terminal block connector on top of the switch as the picture below shows. Connecting a cable to a remote alarm wiring block will allow events to bring up an external alarm, indicating power failure or port / link failure, by making the circuit an open circuit.

An application example for the fault alarm contact is shown below:



Insert the wires into the fault alarm contact

[NOTE] The wire range of terminal block is from 12~ 24 AWG.



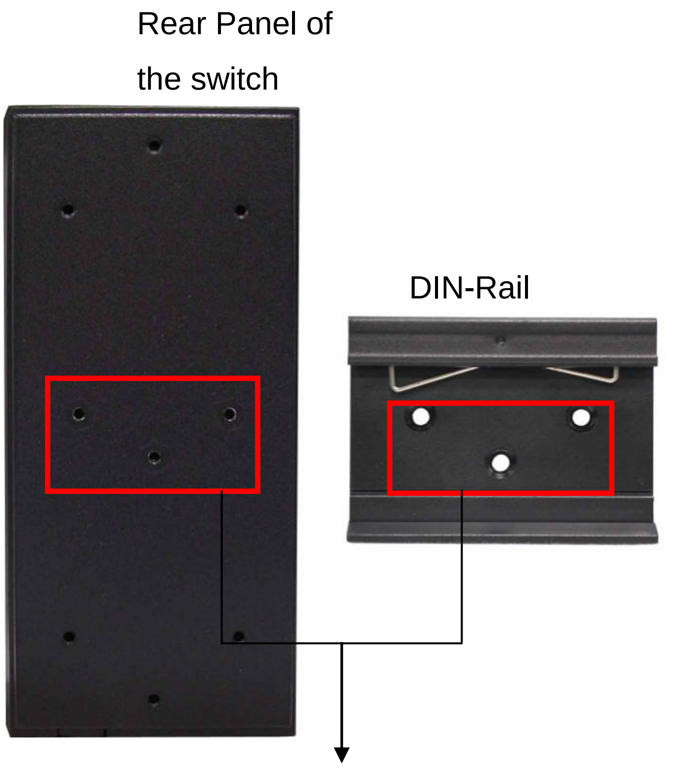
The open circuit will form when the power fails or port link fails.

The fault alarm device will send a warning signal to warn the user, ex: alarm sound or flash light.

Mounting Installation

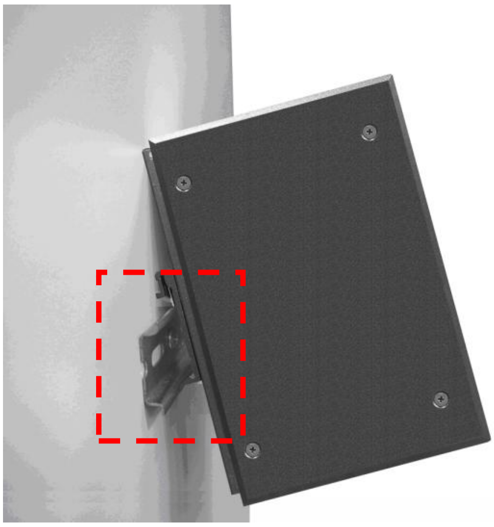
DIN-Rail Mounting

The DIN-Rail is usually screwed onto the IFE-8T2GB-MXE in the factory. If the DIN-Rail is not screwed onto the industrial switch, please see the following instructions on how to screw the DIN-Rail onto the switch. Follow the below steps to hang the industrial switch.

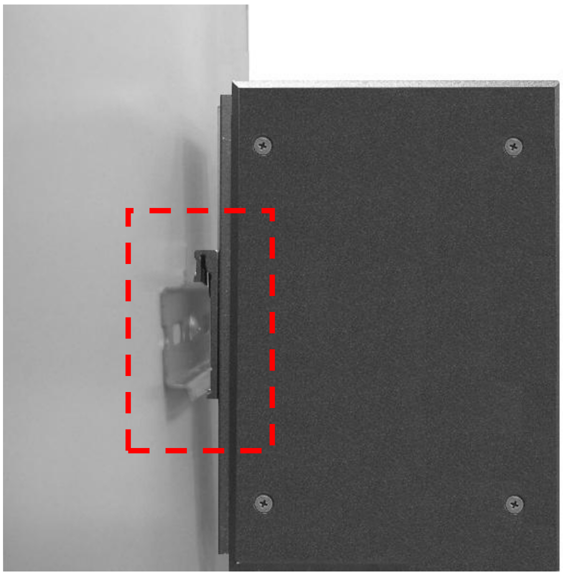


1. Use the screws to screw the DIN-Rail on the industrial switch
2. To remove the DIN-Rail, reverse the step 1.

1. First, insert the top of DIN-Rail into the track.



2. Then, lightly push the DIN-Rail into the track.

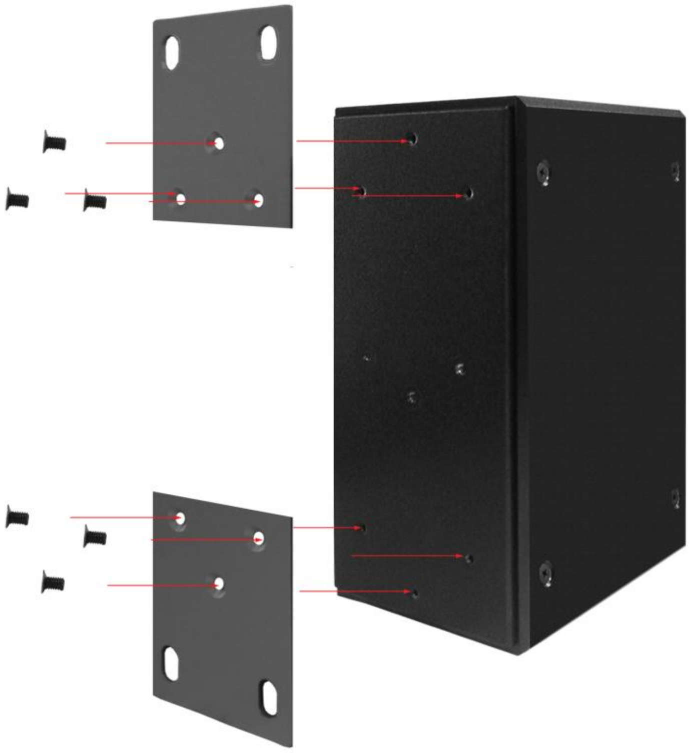


3. Check if the DIN-Rail is tightened on the track or not.
4. To remove the industrial switch from the track, reverse steps above.

Wall Mount Plate Mounting

Follow the steps below to mount the IFE-8T2GB-MXE with wall mount plate.

1. Remove the DIN-Rail from the industrial switch; loose the screws to remove the DIN-Rail.
2. Place the wall mount plate on the rear panel of the industrial switch.
3. Use the screws to screw the wall mount plate on the industrial switch.
4. Use the hook holes at the corners of the wall mount plate to hang the industrial switch on the wall.
5. To remove the wall mount plate, reverse the steps above.



Screwing the wall mount plate on the Industrial media converter

Hardware Installation

This paragraph describes how to install the IFE-8T2GB-MXE

Installation Steps

1. Unpack the IFE-8T2GB-MXE Industrial Switch.

2. Check if the DIN-Rail is screwed onto the switch. If the DIN-Rail is not screwed on and it is required please refer to the **DIN-Rail Mounting** section for installation. If the wall mounting is to be used for the IFE-8T2GB-MXE Industrial switch, then please refer to **Wall Mount Plate Mounting** section for wall mount plate installation.

3. To hang the IFE-8T2GB-MXE Industrial switch onto the DIN-Rail track or wall, please refer to the **Mounting Installation** section.

4. Power on the IFE-8T2GB-MXE Industrial switch. Please refer to the **Wiring the Power Inputs** section to determine how to wire the power. The power LED on the Industrial switch will light up. Please refer to the **LED Indicators** section for indication of LED lights.

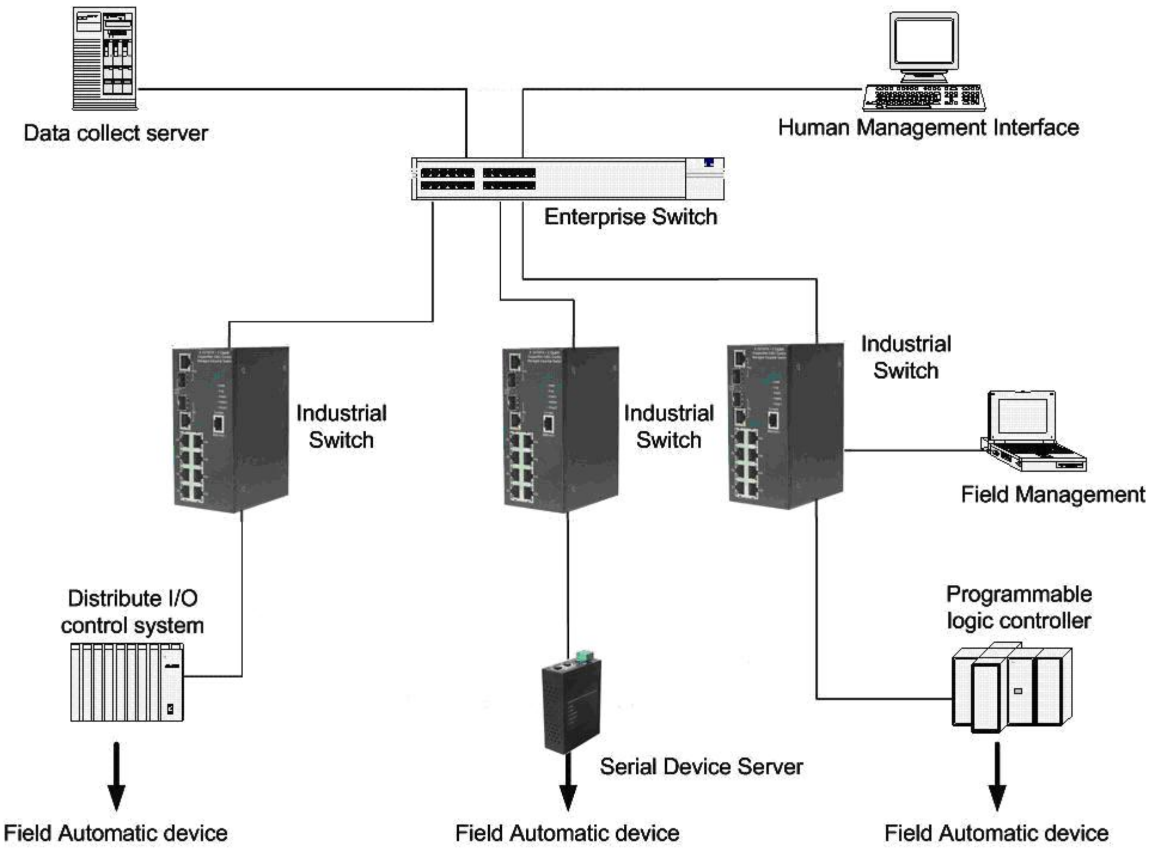
5. Prepare the twisted-pair, straight through Category 5e cable for Ethernet connection.

6. Insert one side of RJ-45 cable (category 5e) into the IFE-8T2GB-MXE switch Ethernet port (RJ-45 port) and another side of RJ-45 cable (category 5e) to the network device's Ethernet port (RJ-45 port), e.g. Switch PC or Server. The UTP port (RJ-45) LED on the Industrial switch will light up when the cable is connected with the network device. Please refer to the **LED Indicators** section for LED light indication.

7. When all connections are made and the LED's show 'normal', the installation is complete.

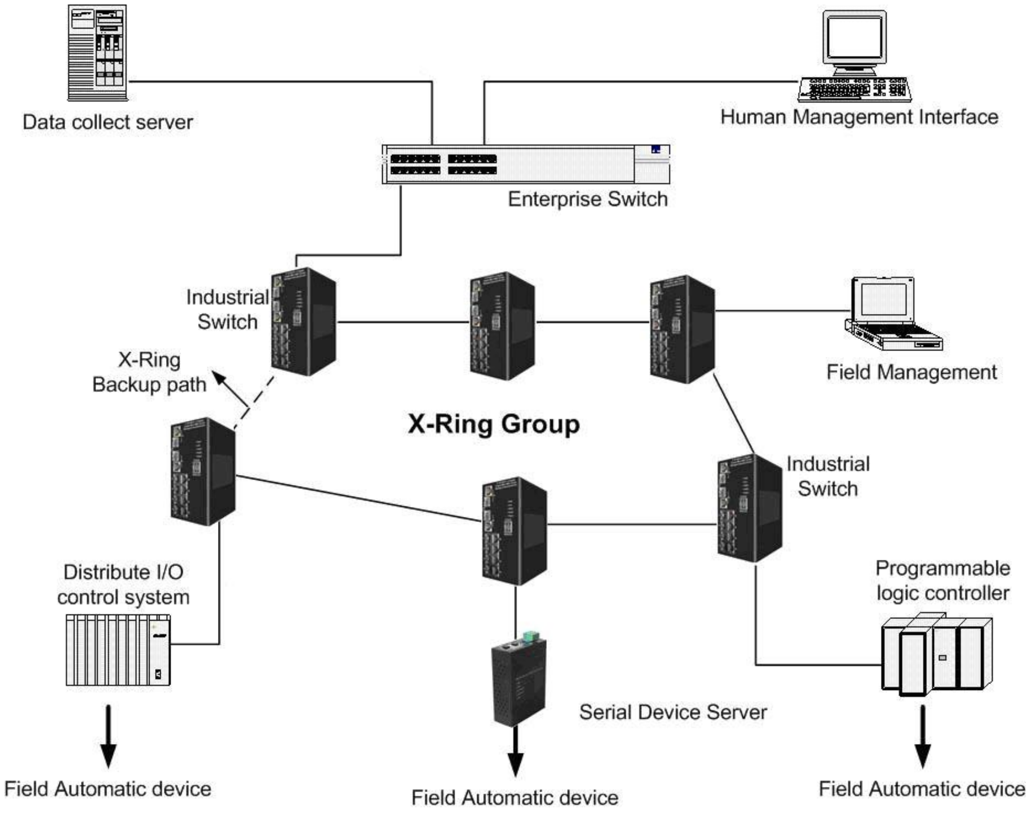
Network Application

This chapter provides some sample applications to provide some examples of how the IFE-8T2GB-MXE is used. The diagram below provides a sample application.



X-Ring Application

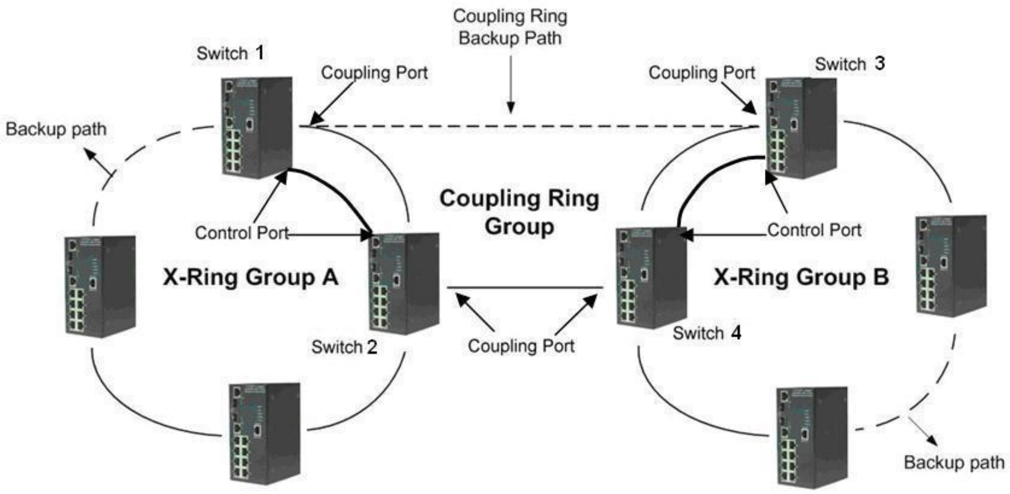
The IFE-8T2GB-MXE switch supports the X-Ring protocol that can help the network system to recover from network connection failures within 10ms or less, and make the network system more reliable. The X-Ring algorithm is similar to Spanning Tree Protocol (STP) and Rapid STP (RSTP) algorithm but its recovery time is very much quicker than STP/RSTP. The figure below is a sample of X-Ring application.



Coupling Ring Application

It is possible to attach two X-rings using dual coupling links as shown below. The coupling ring function provides each X-Ring with a level of redundancy for back up.

It provides high levels of reliability between the two rings and removes any single point of failure. The following figure is a sample of coupling ring application.



Dual Homing Application

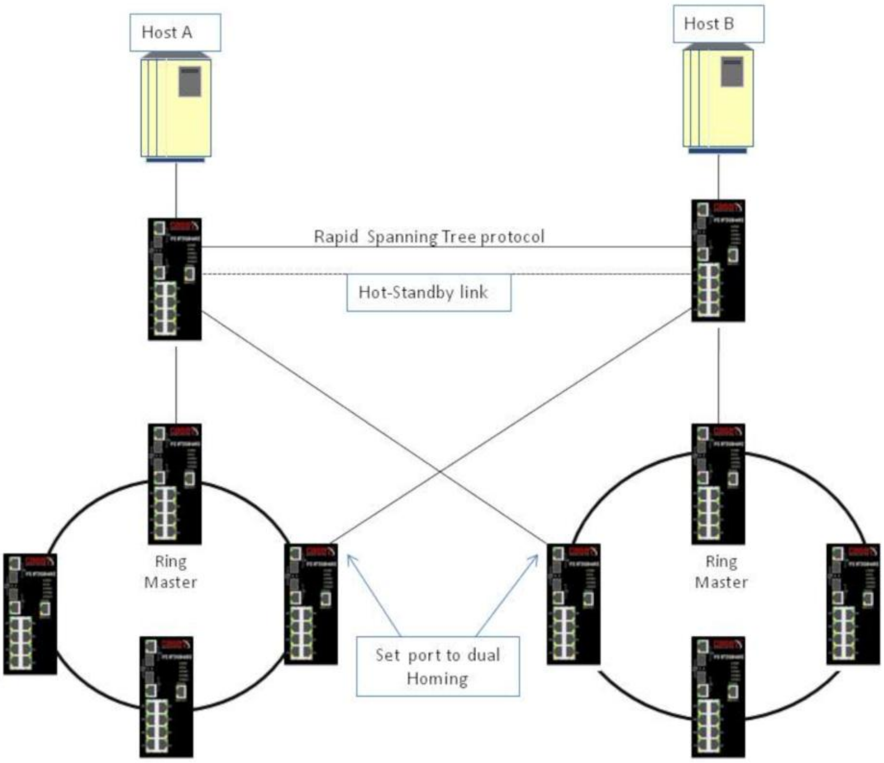
Dual Homing allows rings to connect to two different head end switches in such a way to allow no single point of failure. The diagram below shows two X-ring networks each dual homed to two ‘Head End ‘Switches.

Dual Homing prevents any single point of failure from creating a loss of connection between X-Ring groups and the head end switches. Assign one port per ring to be the Dual Homing port and one standard port for the path out. **Note** The Dual Homing function only works when the X-Ring function is active, and each X-Ring group while having two paths out only has ‘one’ port assigned as the ‘Dual homing Port’

[NOTE] In Dual Homing application architecture, the ‘Head end’ switches need to enable the Rapid Spanning Tree protocol.

[NOTE] In this configuration do not enable more than 1 ring Master per X-ring

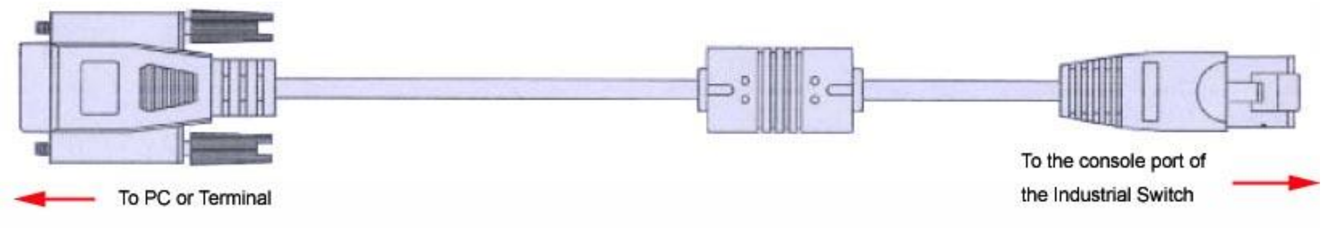
[NOTE] Only 2 ports set to ‘Dual Homing’ per ring, these cannot be on the Ring Master

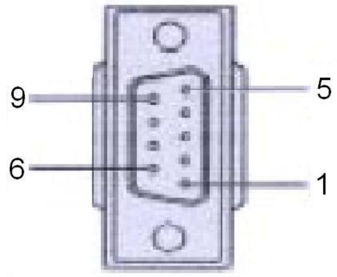


Console Management

Connecting to the Console Port

The cable supplied with the IFE-8T2GB-MXE has an RS-232 connector at one end and an RJ-45 connector at the other. Attach the RS-232 connector to PC or terminal and the other end with the RJ-45 connector to the console port of switch. The connected terminal or PC must support a terminal emulation program such as Hyper-Term or similar.





DB 9-pin Female

Pin Assignment

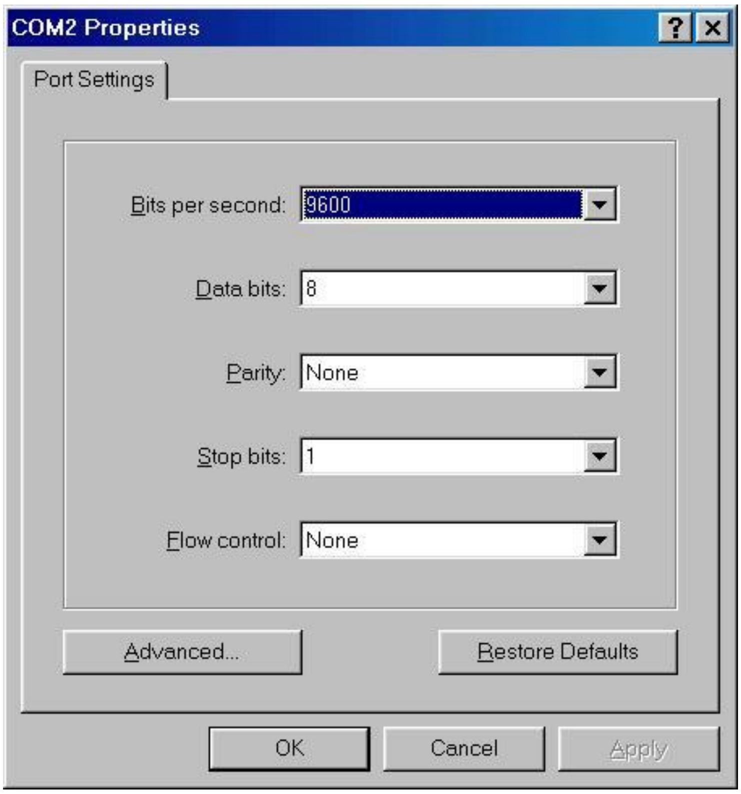
DB9 Connector	RJ-45 Connector
NC	1 Orange/White
2	2 Orange
3	3 Green/White
NC	4 Blue
5	5 Blue/White
NC	6 Green
NC	7 Brown/White
NC	8 Brown

Login in the Console Interface

When the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program such as **Hyper Terminal** and configure the **communication parameters** to match the following default characteristics of the console port:

Baud Rate: 9600 bps
Data Bits: 8
Parity: none
Stop Bit: 1
Flow control: None

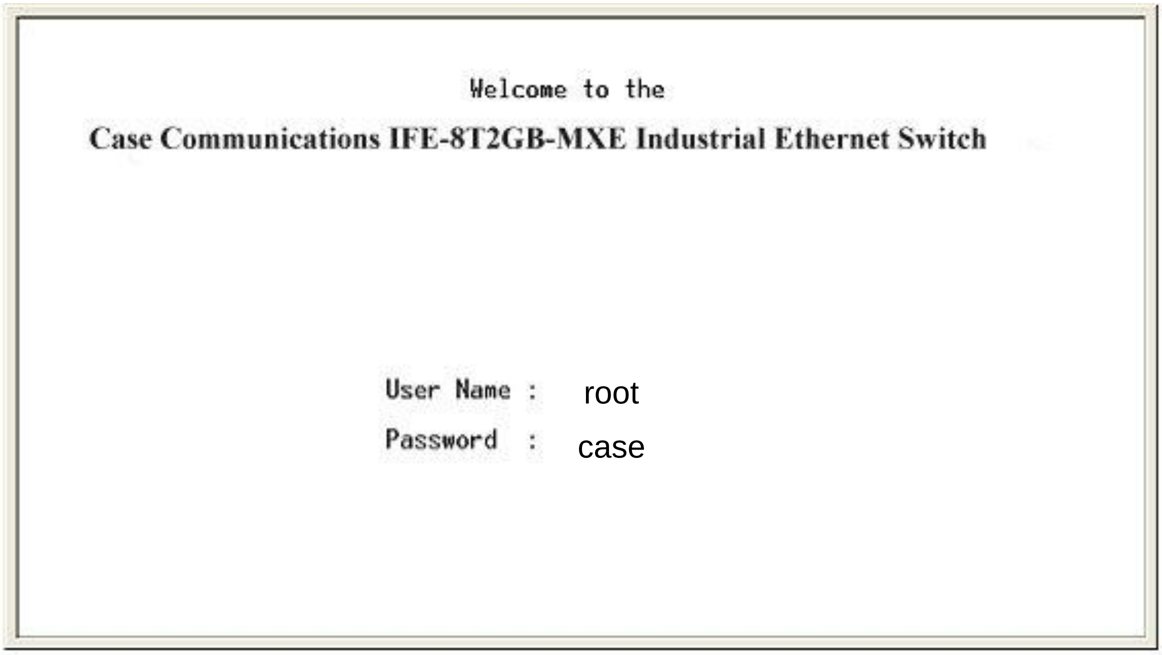
Default Logon details
Logon – root
Password - case



Bits per second: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None

The settings of communication parameters

After finishing the parameter settings, click '**OK**'. When the blank screen is displayed press the Enter key to bring out the login prompt. Key in the '**root**' (default value) for the User name and 'Case' for the Password (use the **Enter** key to switch), then press the Enter key and the Main Menu from the console management appears. Please see below figure for login screen.



Welcome to the

Case Communications IFE-8T2GB-MXE Industrial Ethernet Switch

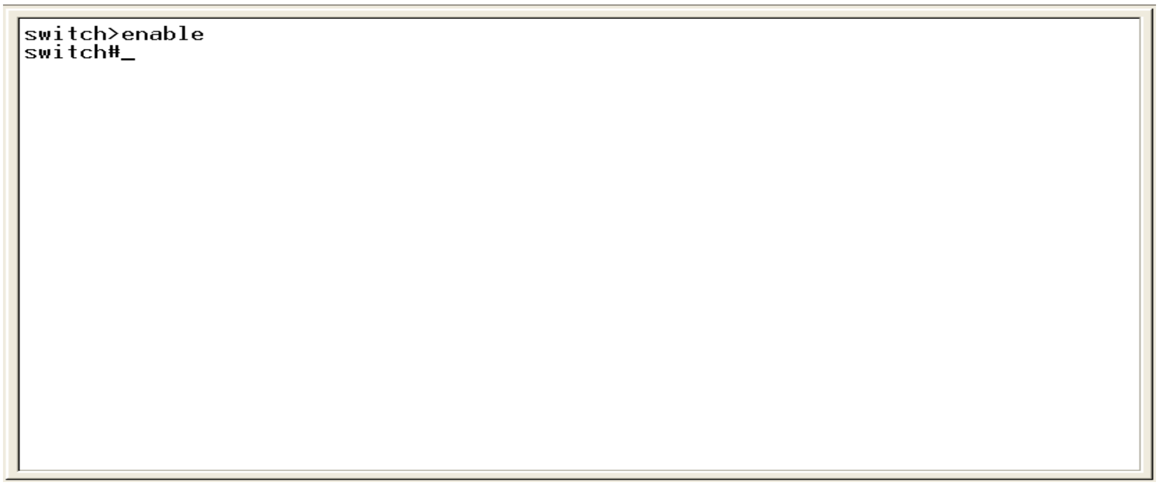
User Name : root

Password : case

Console login interface

CLI Management

The system supports the standard CLI console management. After you login to the system, you will see a command prompt. To enter the CLI management interface, type in the command 'enable'



```
switch>enable
switch#_
```

CLI command interface

The following table lists the CLI commands and description.

Commands Level

Modes	Access Method	Prompt	Exit Method	About This Mode1
User EXEC	‘enable’ Begin a session with your switch.	switch>	Enter logout or quit.	The user commands available at the user level are a subset of those available at the privileged level. Use this mode to • Perform basic tests. •Displays system information.
Privileged EXEC	‘configure’ Enter the enable command while in user EXEC mode.	switch#	Enter disable to exit.	The privileged command is advance mode Privileged this mode to •Displays 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 of fast Ethernet command (with a specific interface) while in global configuration mode	switch (config-if)#	To exit to global configuration mode, enter exit. To exist to privileged EXEC mode, or end.	Use this mode to configure parameters for the switch and Ethernet ports.

Note

Example to set the IP address of the switch using the CLI

^=space,

CR=carriage return

Input	**Response**
	Switch
(en) ‘enable – cr (enter exec mode)	switch#
(co) ‘configure’ – cr (enter command mode)	switch(config)#
Set IP address subnet mask Gateway address	
ip^add^192.168.1.200^255.255.255.0^ 192.168.1.10 OK	
ex – cr (to exit to exec mode)	
wr^mem cr (to save to memory)	

Commands Set List - System Commands Set

Commands	Level	Description	Example
show config	**E**	Show switch configuration	switch>**show config**
show terminal	**P**	Show console information	switch#**show terminal**
write memory	**P**	Save user 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 192.168.16.1 255.255.255.0 192.168.16.254**
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 disable	G	Disable DHCP Server	switch(config)#**no dhcpserver**
dhcpserver lowip [Low IP]	G	Configure low IP address for IP pool	switch(config)#**dhcpserver lowip 192.168.1.100**
dhcpserver highip [High IP]	G	Configure high IP address for IP pool	switch(config)#**dhcpserver highip 192.168.1.200**
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)#**dhcpserver ipbinding 192.168.1.1**
show dhcpserver configuration	P	Show configuration of DHCP server	switch#**show dhcpserver configuration**
show dhcpserver clients	P	Show client entries of DHCP server	switch#**show dhcpserver clients**
show dhcpserver ip-binding	P	Show IP-Binding information of DHCP server	switch#**show dhcpserver ip-binding**
no dhcpserver	G	Disable DHCP server function	switch(config)#**no dhcpserver**
security enable	G	Enable IP security function	switch(config)#**security enable**
security http	G	Enable IP security of HTTP server	switch(config)#**security http**
security telnet	G	Enable IP security of telnet server	switch(config)#**security telnet**
security ip [Index(1..10)] [IP Address]	G	Set the IP security list	switch(config)#**security ip 1 192.168.1.55**

show security	**P**	Show the information of IP security	switch#**show security**
no security	**G**	Disable IP security function	switch(config)#**no security**
no security http	**G**	Disable IP security of HTTP server	switch(config)#**no security http**
no security telnet	**G**	Disable IP security of telnet server	switch(config)#**no security telnet**

Port Commands Set

Commands	Level	Description	Example
interface fastEthernet **[Portid]**	**G**	Choose the port for modification.	switch(config)#**interface fastEthernet 2**
duplex **[full | half]**	**I**	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#**interface fastEthernet 2** switch(config-if)#**duplex full**
speed **[10|100|1000|auto]**	**I**	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	switch(config)#**interface fastEthernet 2** switch(config-if)#**speed 100**
no flowcontrol	**I**	Disable flow control of interface	switch(config-if)#**no flowcontrol**
security enable	**I**	Enable security of interface	switch(config)#**interface fastEthernet 2** switch(config-if)#**security enable**
no security	**I**	Disable security of interface	switch(config)#**interface fastEthernet 2** switch(config-if)#**no security**
bandwidth type all	**I**	Set interface ingress limit frame type to 'accept all frame'	switch(config)#**interface fastEthernet 2**

			switch(config-if)#**bandwidth type all**
bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to 'accept broadcast, multicast, and flooded unicast frame'	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-multicast-flooded-unicast**
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to 'accept broadcast and multicast frame'	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-multicast**
bandwidth type broadcast-only	I	Set interface ingress limit frame type to 'only accept broadcast frame'	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-only**
bandwidth in **[Value]**	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth in 100**
bandwidth out **[Value]**		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** (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** (config-if)#**show interface status**
show interface accounting	I	show interface statistic counter	switch(config)#**interface fastEthernet 2** (config-if)#**show interface accounting**
no accounting	I	Clear interface accounting information	switch(config)#**interface fastEthernet 2** switch(config-if)#**no accounting**

Trunk Commands Set

Commands	Level	Description	Example
aggregator priority **[1~65535]**	G	Set port group system priority	switch(config)#**aggregator priority 22**
aggregator activityport **[Group ID]** **[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] :1~4 [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	switch(config)#**aggregator group 1 1-4 lacp workp 2** or switch(config)#**aggregator group 2 1,4,3 lacp workp 3**

		large than the amount of member ports.	
aggregator group [GroupID] [Port-list] nolacp	G	Assign a static trunk group. [GroupID] :1~4 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#**aggregator group 1 2-4 nolacp** or switch(config)#**aggregator group 1 3,1,2 nolacp**
show aggregator	P	Show the information of trunk group	switch#**show aggregator 1** or switch#**show aggregator 2** or switch#**show aggregator 3**
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**

Notes

After making configuration changes do not forget to save the changes to memory

Ex^ (carriage return) to return to User level

Wr^mem (carriage return) to save

VLAN Commands Set

Commands	Level	Description	Example
vlan database	**P**	Enter VLAN configure mode	switch#**vlan database**
Vlanmode [portbase| 802.1q | gvrp]	**V**	To set switch VLAN mode.	switch(vlan)#**vlanmode portbase** or switch(vlan)#**vlanmode 802.1q** or switch(vlan)#**vlanmode gvrp**
no vlan	**V**	No VLAN	Switch(vlan)#**no vlan**
Ported based VLAN configuration			
vlan port-based **grpname** **[Group Name]** **grpid** **[GroupID]** **port** **[PortNumbers]**	**V**	Add new port based VALN	switch(vlan)#**vlan port-based grpname test grpid 2 port 2-4** or switch(vlan)#**vlan port-based grpname test grpid 2 port 2,3,4**
show vlan [GroupID] or **show vlan**	**V**	Show VLAN information	switch(vlan)#**show vlan 23**
no vlan group [GroupID]	**V**	Delete port base group ID	switch(vlan)#**no vlan group 2**
		IEEE 802.1Q VLAN	
vlan 8021q name **[GroupName]** **vid** **[VID]**	**V**	Change the name of VLAN group, if the group didn't exist, this command can't be applied.	switch(vlan)#**vlan 8021q name test vid 22**
vlan 8021q port **[PortNumber]** **access-link untag** **[UntaggedVID]**	**V**	Assign a access link for VLAN by port, if the port belongs to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 access-link untag 33**
vlan 8021q port **[PortNumber]** **trunk-link tag**	**V**	Assign a trunk link for VLAN by port, if the	switch(vlan)#**vlan 8021q port 3 trunk-link tag 2,3,6,99**

[TaggedVID List]		port belongs to a trunk group, this command can't be applied.	or switch(vlan)#**vlan 8021q port 3 trunk-link tag 3-20**
vlan 8021q port [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	**V**	Assign a hybrid link for VLAN by port, if the port belongs to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q port 3 hybrid-link untag 5 tag 6-8**
vlan 8021q trunk [PortNumber] **access-link untag** [UntaggedVID]	**V**	Assign a access link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 access-link untag 33**
vlan 8021q trunk [PortNumber] **trunk-link tag** [TaggedVID List]	**V**	Assign a trunk link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 trunk-link tag 2,3,6,99** or switch(vlan)#**vlan 8021q trunk 3 trunk-link tag 3-20**
vlan 8021q trunk [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	**V**	Assign a hybrid link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q trunk 3 hybrid-link untag 5 tag 6-8**
show vlan [GroupID] or **show vlan**	**V**	Show VLAN information	switch(vlan)#**show vlan 23**
no vlan group [GroupID]	V	Delete port base group ID	switch(vlan)#**no vlan group 2**

Spanning Tree Commands Set

Commands	Level	Description	Example
spanning-tree enable	G	Enable spanning tree	switch(config)#**spanning-tree enable**
spanning-tree priority [0~61440]	G	Configure spanning tree priority parameter	switch(config)#**spanning-tree priority 32767**
spanning-tree max-age [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)#**spanning-tree max-age 15**
spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#**spanning-tree hello-time 3**
spanning-tree forward-time [seconds]	G	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)#**spanning-tree forward-time 20**
stp-path-cost [1~200000000]	I	Use the spanning-tree cost interface configuration command to set the path cost	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-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.	**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 128**
stp-admin-p2p **[Auto|True|False]**	**I**	Admin P2P of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-p2p Auto**
stp-admin-edge **[True|False]**	**I**	Admin Edge of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-edge True**
stp-admin-non-stp **[True|False]**	**I**	Admin NonSTP of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-non-stp False**
show spanning-tree	**E**	Displays a summary of the spanning-tree states.	switch>**show spanning-tree**
no spanning-tree	**G**	Disable spanning-tree.	switch(config)#**no spanning-tree**

QOS Commands Set

Commands	Lev	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 0 middle**
qos priority tos [Priority][lowest|low|middle|high]	G	Configure TOS Priority	switch(config)#**qos priority tos 3 high**
show qos	P	Displays the information of QoS configuration	Switch#**show qos**
no qos	G	Disable QoS function	switch(config)#**no qos**

IGMP Commands Set

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

Mac / Filter Table Commands Set

Commands	Level	Description	Example
mac-address-table static hwaddr **[MAC]**	**I**	Configure MAC address table of interface (static).	switch(config)#**interface fastEthernet 2** switch(config-if)#**mac-address-table static hwaddr 000012345678**
mac-address-table filter hwaddr **[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**

SNMP Commands Set

Commands	Level	Description	Example
snmp system-name [System Name]	G	Set SNMP agent system name	switch(config)#**snmp system-name l2switch**
snmp system-location [System Location]	G	Set SNMP agent system location	switch(config)#**snmp system-location lab**
snmp system-contact [System Contact]	G	Set SNMP agent system contact	switch(config)#**snmp system-contact where**
snmp agent-mode [v1v2c|v3|v1v2cv3]	G	Select the agent mode of SNMP	switch(config)#**snmp agent-mode v1v2cv3**
snmp community-strings [Community] **right** [RO/RW]	G	Add SNMP community string.	switch(config)#**snmp community-strings public right rw**
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 192.168.1.50 community public trap-version v1** **(remove)** Switch(config)# **no snmp-server host 192.168.1.50**
snmpv3 context-name [Context Name]	G	Configure the context name	switch(config)#**snmpv3 context-name Test**
snmpv3 user [User Name] **group** [Group Name] **password** [Authentication Password] [Privacy Password]	G	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#**snmpv3 user test01 group G1 password AuthPW PrivPW**
snmpv3 access context-name [Context Name]	G	Configure the access table of SNMPV3 agent	switch(config)#**snmpv3 access context-name Test group G1**

group [Group Name] security-level [NoAuthNoPriv|AuthNoPriv|AuthPriv] match-rule [Exact|Prifix] views [Read View Name] [Write View Name] [Notify View Name]			**security-level AuthPriv match-rule Exact views V1 V1 V1**
snmpv3 mibview view [View Name] type [Excluded|Included] sub-oid [OID]	**G**	Configure the mibview table of SNMPV3 agent	switch(config)#**snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**
show snmp	**P**	Show SNMP configuration	switch#**show snmp**
no snmp community-strings [Community]	**G**	Remove the specified community.	switch(config)#**no snmp community-strings public**
no snmp-server host [Host-address]	**G**	Remove the SNMP server host.	switch(config)#**no snmp-server 192.168.1.50**
no snmpv3 user [User Name]	**G**	Remove specified user of SNMPv3 agent.	switch(config)#**no snmpv3 user Test**
no snmpv3 access context-name [Context Name] group [Group Name] security-level [NoAuthNoPriv|AuthNoPriv|AuthPriv] match-rule [Exact|Prifix] views [Read View Name] [Write View Name]	**G**	Remove specified access table of SNMPv3 agent.	switch(config)#**no snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1**

[Notify View Name]			
no snmpv3 mibview view [View Name] **type** [Excluded|Included] **sub-oid** [OID]	**G**	Remove specified mibview table of SNMPV3 agent.	switch(config)#**no snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**

Port Mirroring Commands Set

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

802.1x Commands Set

Commands	Level	Description	Example
8021x enable	**G**	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# **8021x enable**

8021x system radiusip [IP address]	G	Use the 802.1x system radius IP global configuration command to change the radius server IP.	switch(config)# **8021x system radiusip 192.168.1.1**
8021x system serverport [port ID]	G	Use the 802.1x system server port global configuration command to change the radius server port	switch(config)# **8021x system serverport 1815**
8021x system accountport [port ID]	G	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# **8021x system accountport 1816**
8021x system sharekey [ID]	G	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# **8021x system sharekey 123456**
8021x system nasid [words]	G	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# **8021x system nasid test1**
8021x misc quietperiod [sec.]	G	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# **8021x misc quietperiod 10**
8021x misc txperiod [sec.]	G	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# **8021x misc txperiod 5**
8021x misc supportimeout [sec.]	G	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# **8021x misc supportimeout 20**
8021x misc servertimeout [sec.]	G	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#**8021x misc servertimeout 20**
8021x misc maxrequest [number]	G	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# **8021x misc maxrequest 3**
8021x misc	G	Use the 802.1x misc reauth	switch(config)# **8021x misc**

reauthperiod **[sec.]**		period global configuration command to set the reauth period.	**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**	Displays 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**

TFTP Commands Set

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**

SystemLog, SMTP and Event Commands Set

Commands	Level	Description	Example
systemlog ip **[IP address]**	G	Set System log server IP address.	switch(config)# **systemlog ip 192.168.1.100**
systemlog mode **[client|server|both]**	G	Specified the log mode	switch(config)# **systemlog mode both**
show systemlog	E	Displays 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 X-ring topology changed event type	switch(config)#**event X-ring-topology-change both**
event systemlog **[Link-UP|Link-Down|Both]**	I	Set port event for system log	switch(config)#**interface fastethernet 3**

			switch(config-if)#**event systemlog both**
event smtp [Link-UP|Link-Down|Both]	**I**	Set port event for SMTP	switch(config)#**interface fastethernet 3** switch(config-if)#**event smtp both**
show event	**P**	Show event selection	switch#**show event**
no event device-cold-start	**G**	Disable cold start event type	switch(config)#**no event device-cold-start**
no event authentication-failure	**G**	Disable Authentication failure event typ	switch(config)#**no event authentication-failure**
no event 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**

SNTP Commands Set

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

X-ring Commands Set

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

Web-Based Management

This section introduces the web man machine interface within the Case Communications IFE-8T2GB-MXE Rugged switch.

About Web-based Management

The IFE-8T2GB-MXE has an embedded HTML web server residing in flash memory within the switch. The web manager offers advanced management features and allows users to manage the switch from anywhere in the network through a standard browser such as Microsoft Internet Explorer. The switch may also be managed via a Case Communications 'CaseView' SNMP based Network Management System

The Web-Based Management supports Internet Explorer 6.0 or later version. Java Applets are used to reduce network bandwidth, to improve the response time and make the configuration easier.

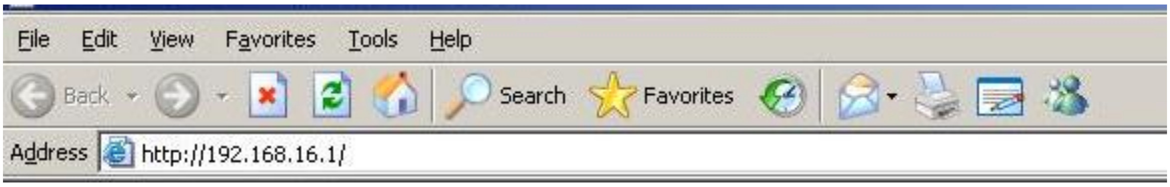
Preparing for Web Management

Before using the web management, install the IFE-8T2GB-MXE industrial switch into the network and make sure that any of the PCs on the network can connect to the industrial switch through the web browser. The industrial switch default IP Address, subnet mask, username and password are shown below:

- IP Address: **192.168.16.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.16.254**
  (NB the Gateway out of the local network for management)
- User Name: **root**
- Password: **case**

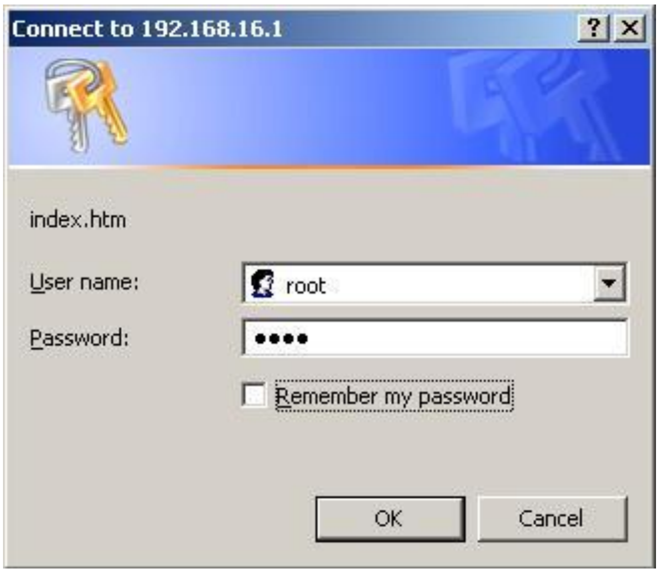
System Login

1. Launch Internet Explorer on your PC
2. Key in ‘http:// ‘+’ the IP address of the switch’, and then Press ‘**Enter**’.



http://192.168.16.1/

3. The login screen will appear right after
4. Key in the user name and password. The default user name is **‘root’** and password is **’case’**
5. Press ‘**Enter**’ or ‘**OK**’, and then the home screen of the Web-based management appears as below:



Connect to 192.168.16.1

index.htm

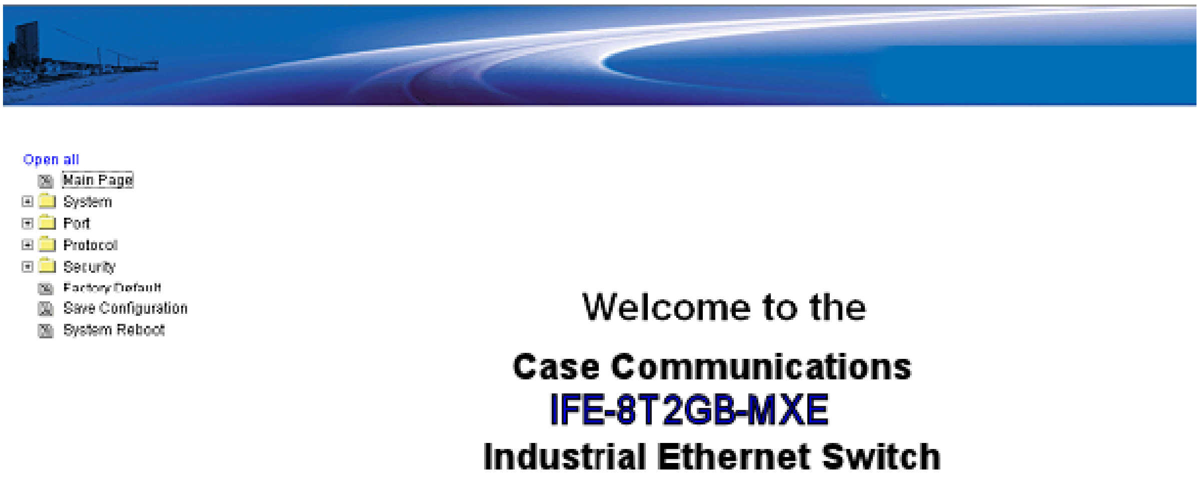
User name: root

Password: ●●●●

□ Remember my password

IFE-8T2GB-MXE Login screen

Main interface



Welcome to the

Case Communications
IFE-8T2GB-MXE
Industrial Ethernet Switch

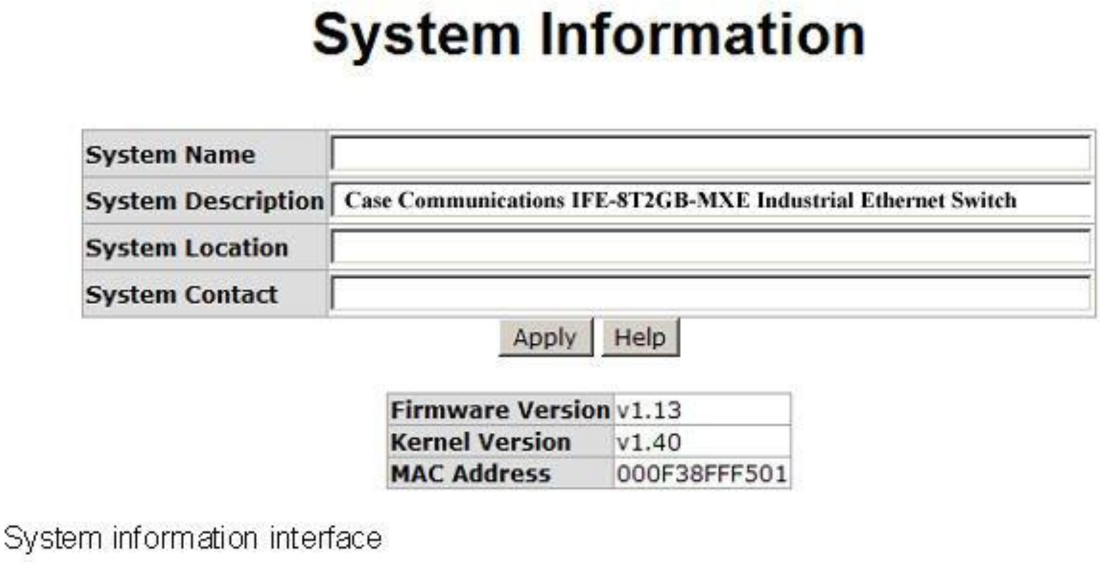
IFE-8T2GB-MXE Main Web interface

IFE-8T2GB-MXE Main Web interface

System Information

Assigning the system name, location and view the system information

- **System Name:** Assign the name of switch. The maximum length is 64 bytes
- **System Description:** Displays the description of switch. Read only cannot be modified
- **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:** Displays the switch's firmware version
- **Kernel Version:** Displays the kernel software version
- **MAC Address:** Displays the unique hardware address assigned by manufacturer (default)



System Information

System Name	
System Description	Case Communications IFE-8T2GB-MXE Industrial Ethernet Switch
System Location	
System Contact	

Firmware Version	v1.13
Kernel Version	v1.40
MAC Address	000F38FFF501

System information interface

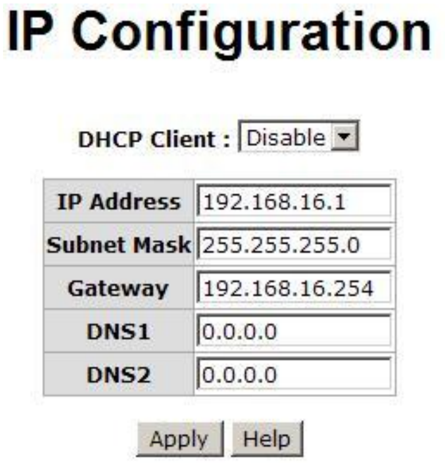
IFE-8T2GB-MXE System information interface

IP Configuration

Users can configure the IP Settings and DHCP client function

- **DHCP Client:** To enable or disable the DHCP client function. If the DHCP client function is enabled, the industrial switch will be assigned an IP address from the DHCP server on the network. The default IP address will be replace by the DHCP server assigned IP address. If the manager selects the 'Apply' button, a popup dialog box is shown. This informs the user that when the DHCP client is enabled, the current IP will be provided by the DHCP Server

- **IP Address:** Assigns the IP address that the network is using. If the DHCP client function is enabled, users don’t need to assign the IP address. And, the network DHCP server will assign the IP address to the switch and display the address in this column. The default IP is 192.168.16.1.
- **Subnet Mask:** Assigns the subnet mask. If the DHCP client function is enabled then users do not need to assign a subnet mask.
- **Gateway:** Assigns the network gateway for the industrial switch. The default gateway is 192.168.16.254. (This is the Gateway address for the switch management to find a way out of the local network)
- **DNS1:** Assign the primary DNS IP address.
- **DNS2:** Assign the secondary DNS IP address.
- And then, click Apply



IP Configuration

DHCP Client : Disable

IP Address	192.168.16.1
Subnet Mask	255.255.255.0
Gateway	192.168.16.254
DNS1	0.0.0.0
DNS2	0.0.0.0

IP configuration interface

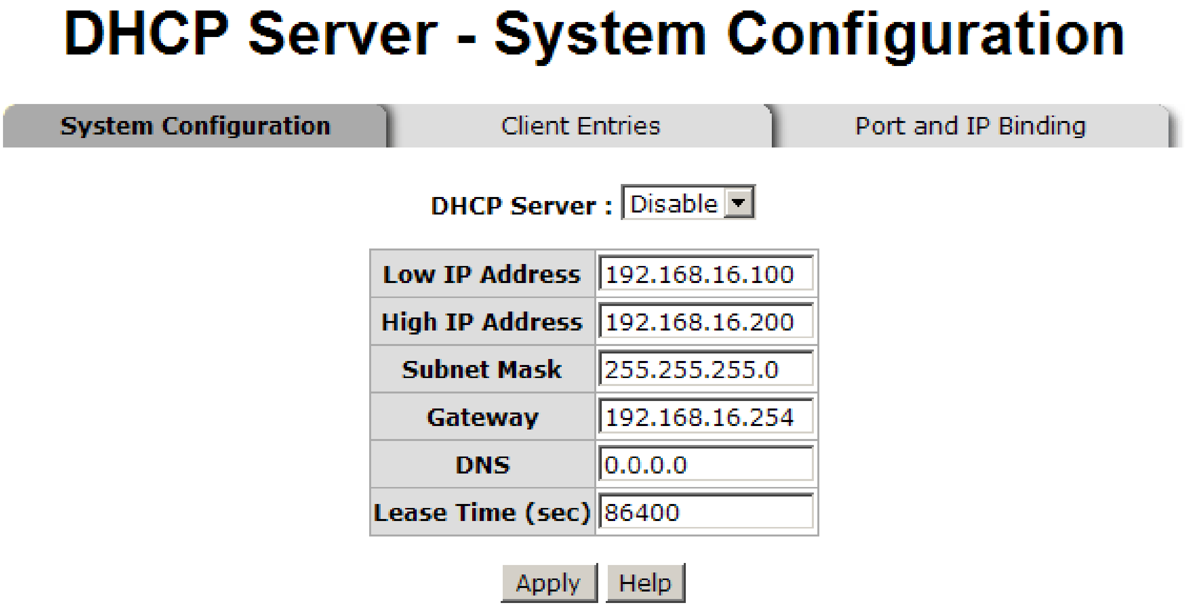
DHCP Server – System configuration

The system acts as a DHCP server. By setting this to ‘Enable’ the switch will act as a DHCP server .

- **DHCP Server:** Enable or Disable the DHCP Server function. If set to enable – the switch will be the DHCP server on your local network.
- **Low IP Address:** the dynamic IP assign range. Low IP address sets the start of the dynamic IP assigns range. For example: the dynamic IP assign range is from 192.168.1.100 ~ 192.168.1.200.

  192.168.1.100 will be the Low IP address.

- **High IP Address:** the dynamic IP assign range. High IP address selects the higher end of the dynamic IP range. For example: dynamic IP assign range is from 192.168.1.100 ~ 192.168.1.200. 192.168.1.200 will be the High 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 (sec):** Is the time that the switch will reset the dynamic IP address to ensure the address has not been occupied for a long time.
- And then, click Apply



DHCP Server - System Configuration

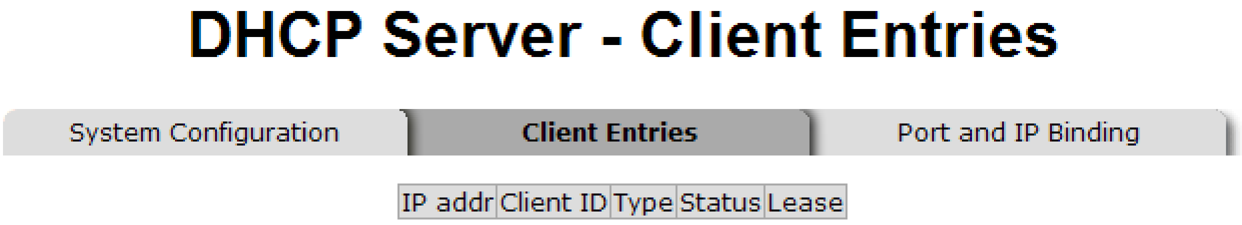
DHCP Server : Disable

Low IP Address	192.168.16.100
High IP Address	192.168.16.200
Subnet Mask	255.255.255.0
Gateway	192.168.16.254
DNS	0.0.0.0
Lease Time (sec)	86400

DHCP Server Configuration interface

DHCP Client – System Configuration

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



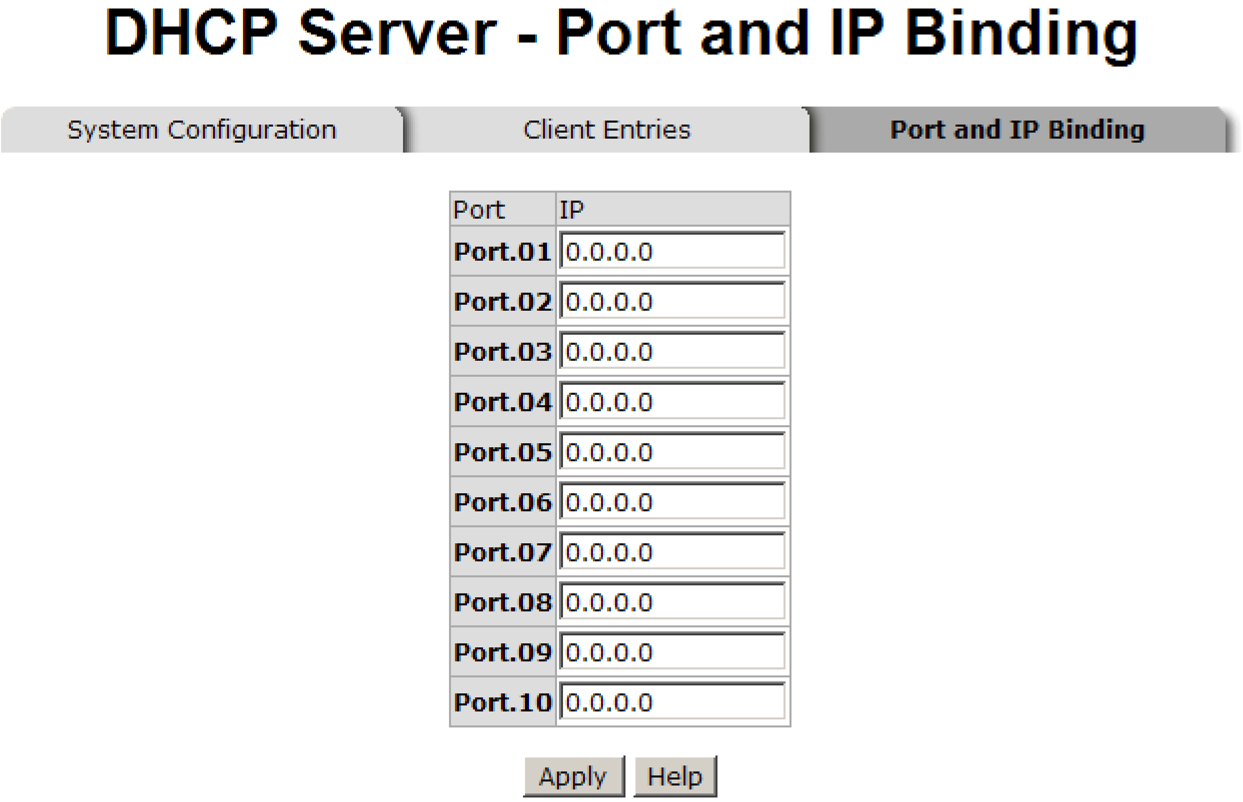
DHCP Server - Client Entries

IP addr	Client ID	Type	Status	Lease

DHCP Client Entries interface

DHCP Server - Port and IP Bindings

You can assign a specific IP address that is within the dynamic IP assigned range for the specific port. When a device connects to the port and asks for a dynamic IP address, the IFE-8T2GB-MXE will assign an IP address that has been pre-assigned to the device that has connected.



DHCP Server - Port and IP Binding

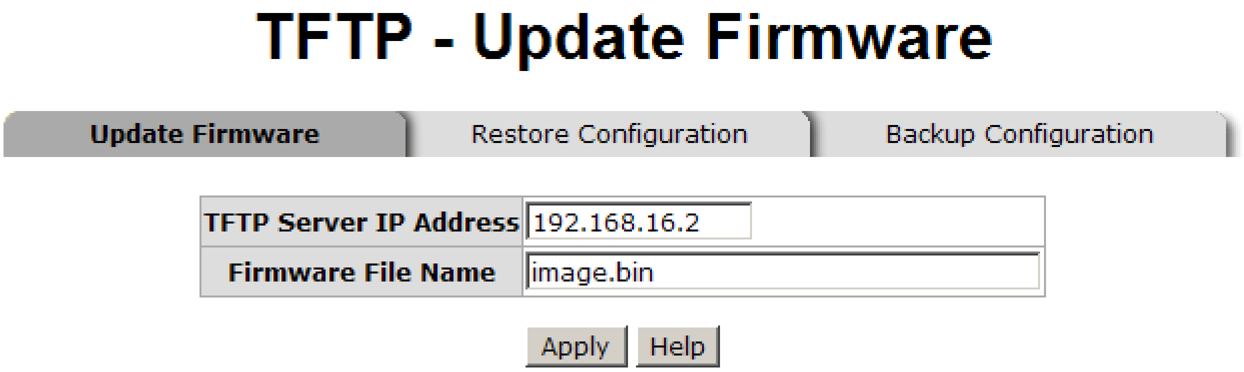
Port	IP
Port.01	0.0.0.0
Port.02	0.0.0.0
Port.03	0.0.0.0
Port.04	0.0.0.0
Port.05	0.0.0.0
Port.06	0.0.0.0
Port.07	0.0.0.0
Port.08	0.0.0.0
Port.09	0.0.0.0
Port.10	0.0.0.0

Port and IP Bindings interface

TFTP - Update Firmware

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

1. **TFTP Server IP Address:** fill in your TFTP server IP.
2. **Firmware File Name:** the name of firmware image.
3. Click Apply.



TFTP - Update Firmware

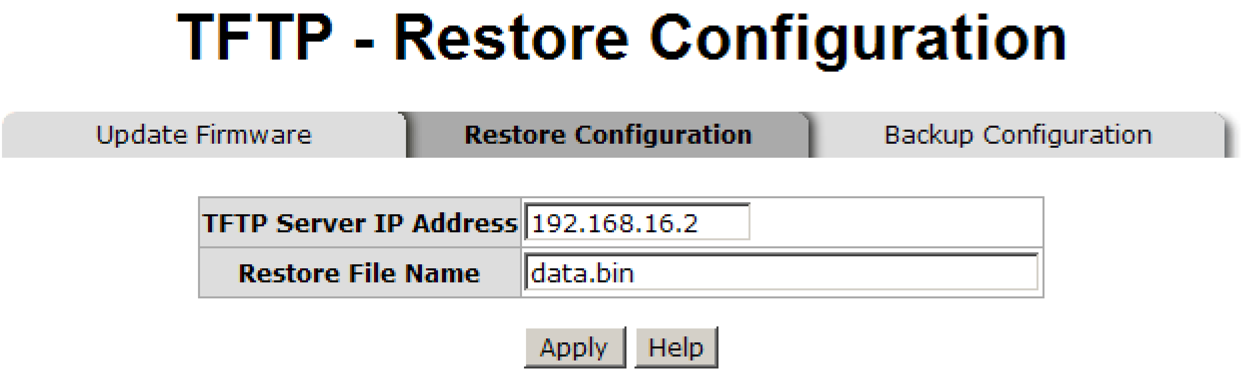
TFTP Server IP Address	192.168.16.2
Firmware File Name	image.bin

Update Firmware interface

TFTP – Restore Configuration

You can restore the EEPROM value from an external TFTP server. Before you do this you must put the image file onto a TFTP server, the switch can then download the flash image from that TFTP Server.

1. **TFTP Server IP Address:** fill in the TFTP server IP.
2. **Restore File Name:** fill in the correct restore file name.
3. Click Apply.



TFTP - Restore Configuration

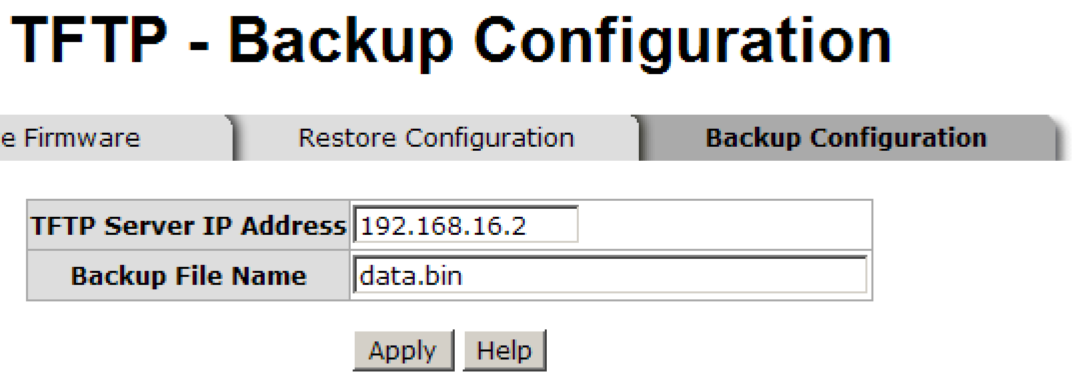
TFTP Server IP Address	192.168.16.2
Restore File Name	data.bin

Restore Configuration interface

TFTP - Backup Configuration

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

1. **TFTP Server IP Address:** fill in the TFTP server IP
2. **Backup File Name:** fill the file name
3. Click Apply.



TFTP Server IP Address	192.168.16.2
Backup File Name	data.bin

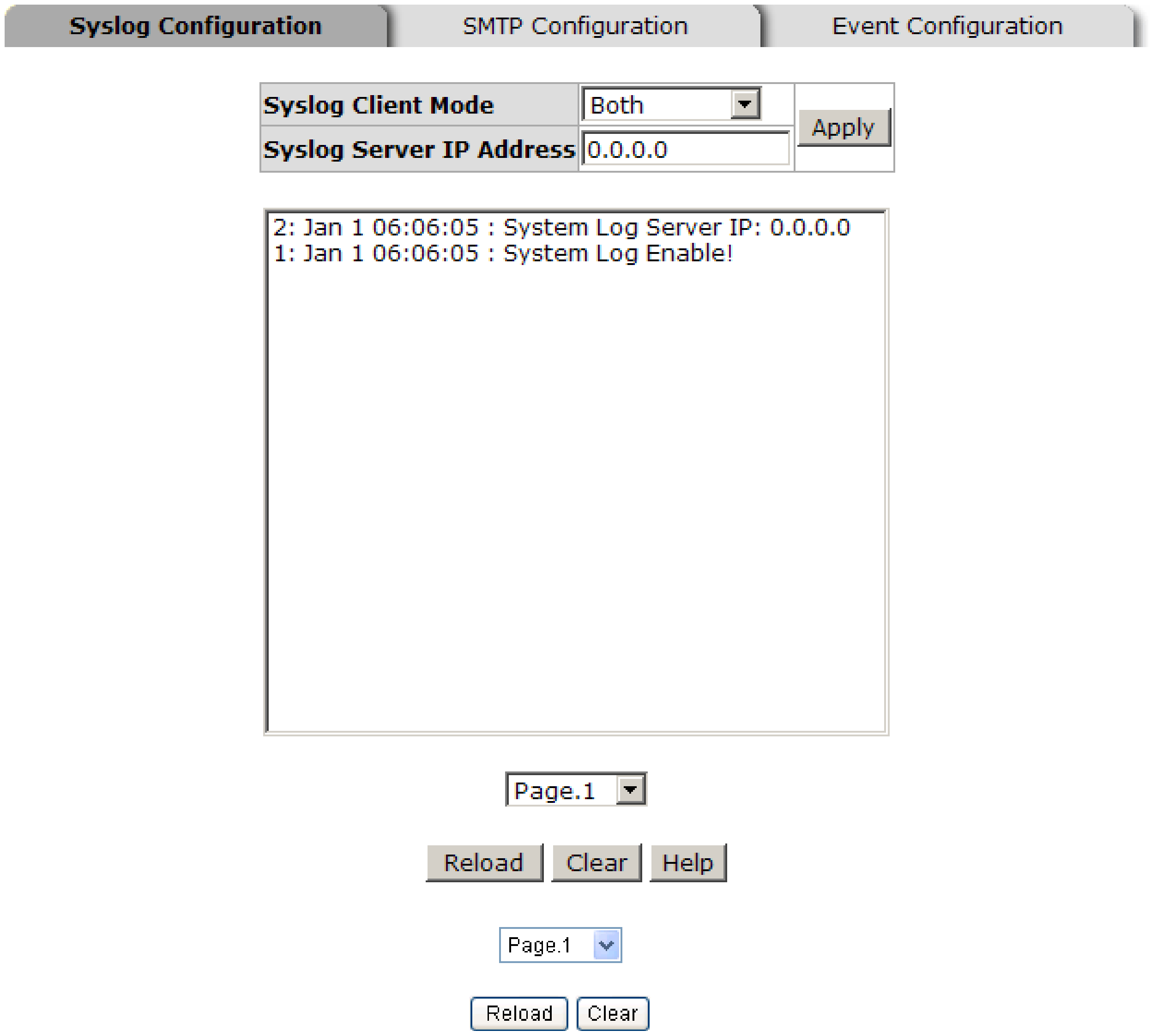
Backup Configuration interface

System Event Log – Syslog Configuration

Configuring the system event mode that needs to be collected and system log server IP.

1. **Syslog Client Mode:** select the system log mode – client only, server only, or both S/C.
2. **System Log Server IP Address:** assigned the system log server IP.
3. Click Reload to refresh the events log.
4. Click Clear to clear all current events log.
5. After configuring, Click Apply.

System Event Log - Syslog Configuration



Syslog Client Mode: Both
Syslog Server IP Address: 0.0.0.0

```
2: Jan 1 06:06:05 : System Log Server IP: 0.0.0.0
1: Jan 1 06:06:05 : System Log Enable!
```

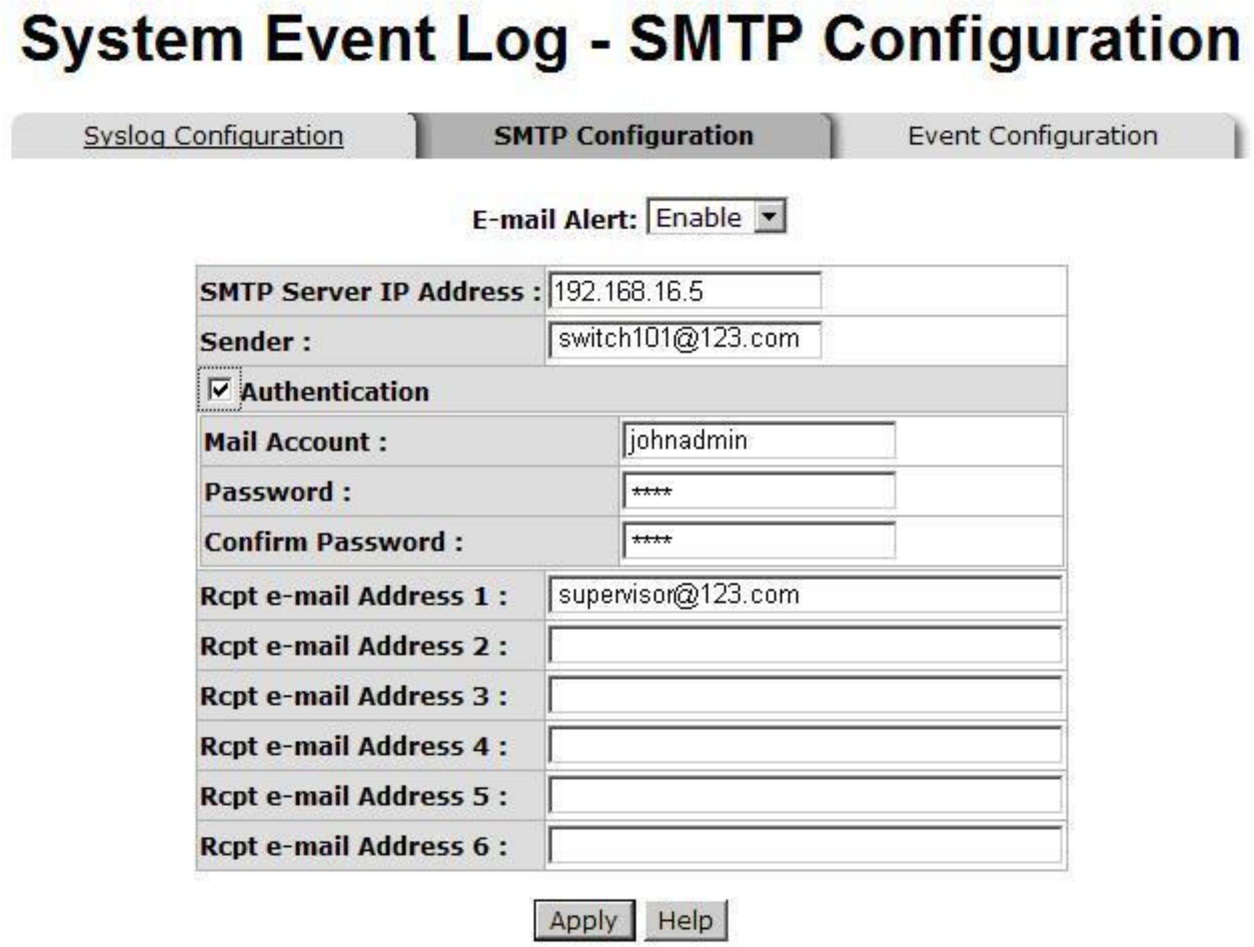
Syslog Configuration interface

System Event Log - SMTP Configuration

You can set up the mail server IP, mail account, account password, and forwarded email account for receiving the event alert.

1. **Email Alert:** enable or disable the email alert function.
2. **SMTP Server IP:** set up the mail server IP address (when the **Email Alert** is enabled, this function will become available).
3. **Sender:** key in a complete email address, e.g. switch101@123.com to identify where the event log comes from (This is the e-mail address you give to your switch).

4. **Authentication:** mark the check box to enable and configure the email account and password for authentication (when the **Email Alert** is enabled, this function will then be available).
5. **Mail Account:** set up the email account, e.g. johnadmin, to receive the alert. It must be an existing email account on the mail server, which you had set up in the **SMTP Server IP Address** column.
6. **Password:** The email account password.
7. **Confirm Password:** reconfirm the password.
8. **Rcpt e-mail Address 1 ~ 6:** you can assign up to 6 e-mail accounts also to receive the alert.
9. Click Apply .



System Event Log - SMTP Configuration

Syslog Configuration | SMTP Configuration | Event Configuration

E-mail Alert: Enable

SMTP Server IP Address :	192.168.16.5
Sender :	switch101@123.com
☑ Authentication	
Mail Account :	johnadmin
Password :	****
Confirm Password :	****
Rcpt e-mail Address 1 :	supervisor@123.com
Rcpt e-mail Address 2 :	
Rcpt e-mail Address 3 :	
Rcpt e-mail Address 4 :	
Rcpt e-mail Address 5 :	
Rcpt e-mail Address 6 :	

SMTP Configuration interface

System Event Log - Event Configuration

You can select the system log events and SMTP events. When selected events occur, the system will send out the log information. Also, per port log and SMTP events can be selected. After configure, Click Apply.

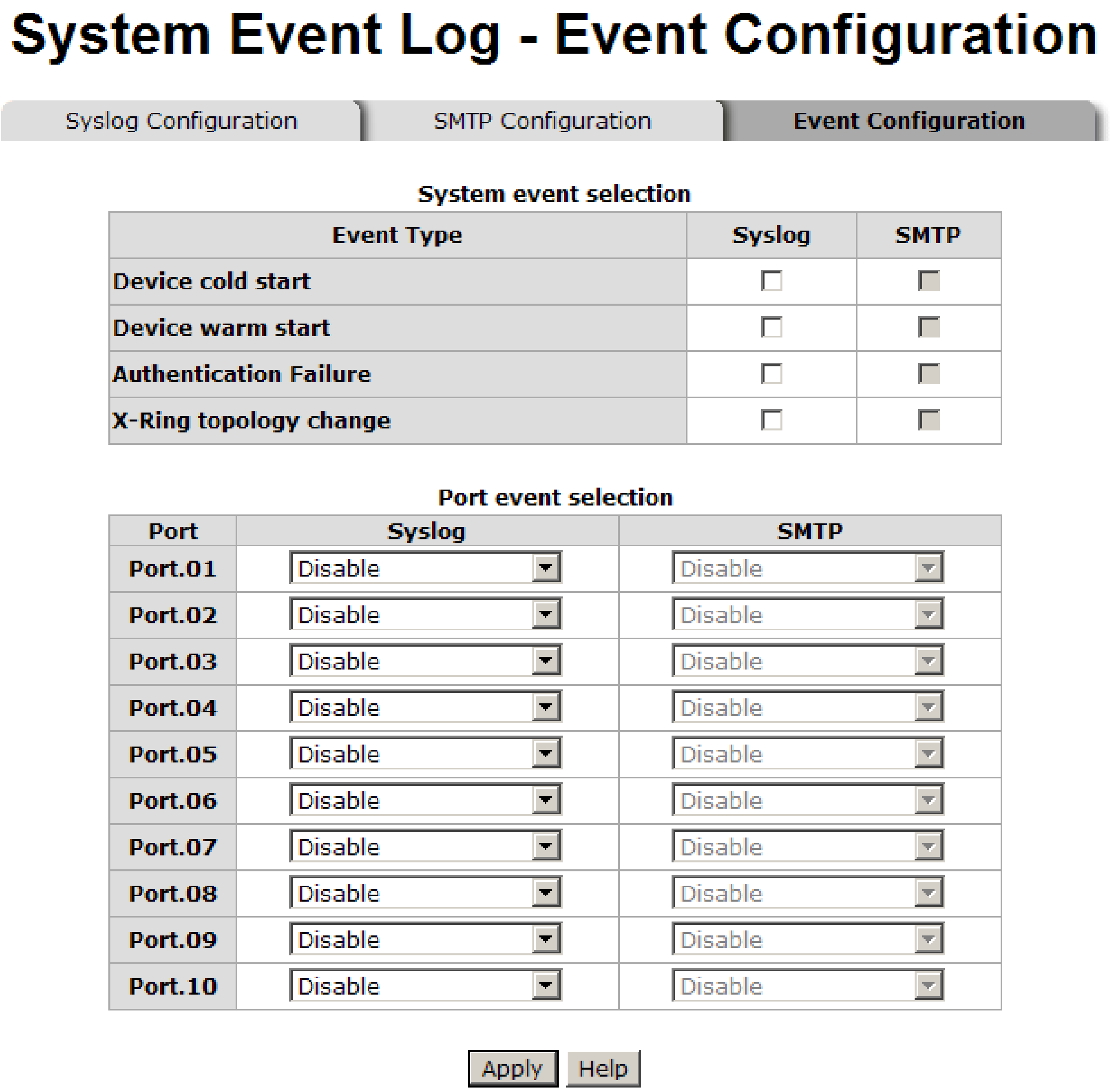
- **System event selection:** 4 selections – Device cold start, Device warm start, SNMP Authentication Failure, and X-ring topology change. Mark the checkbox to select the event. When selected events occur, the system will issue the logs.

  - **Device cold start:** when the device executes a cold start action, the system will issue a log event.

  - **Device warm start:** when the device executes **a** warm start, the system will issue a log event.

  - **Authentication Failure:** when the SNMP authentication fails, the system will issue a log event.

  - **X-ring topology change:** when the X-ring topology has changed, the system will issue a log event.



System Event Log - Event Configuration

System event selection

Event Type	Syslog	SMTP
Device cold start	☐	☐
Device warm start	☐	☐
Authentication Failure	☐	☐
X-Ring topology change	☐	☐

Port event selection

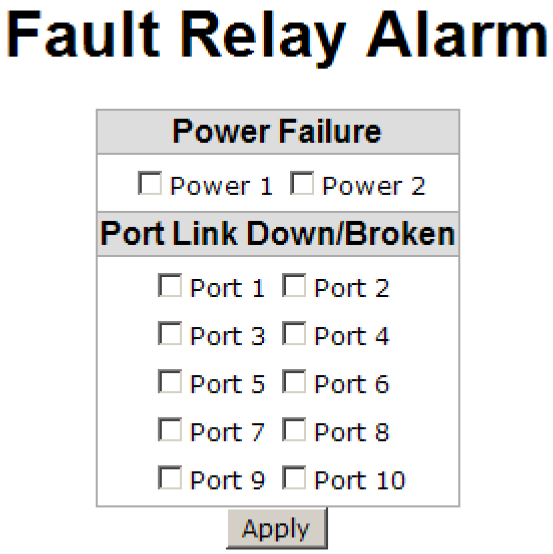
Port	Syslog	SMTP
Port.01	Disable	Disable
Port.02	Disable	Disable
Port.03	Disable	Disable
Port.04	Disable	Disable
Port.05	Disable	Disable
Port.06	Disable	Disable
Port.07	Disable	Disable
Port.08	Disable	Disable
Port.09	Disable	Disable
Port.10	Disable	Disable

Event Configuration interface

- **Port event selection:** select the per port events and per port SMTP events. There are 3 selections – Link UP, Link Down, and Link UP & Link Down. Disable means no event is selected.
    - **Link UP:** the system will issue a log message when port connection is up only.
    - **Link Down:** the system will issue a log message when port connection is down only.
    - **Link UP & Link Down:** the system will issue a log message when port connection is up and down.

Fault Relay Alarm

- **Power Failure:** Select the required option box to enable the function of lighting up the FAULT LED on the panel when power fails.
- **Port Link Down/Broken:** Mark the check box to enable the function of lighting up the **FAULT** LED on the panel when Ports' states are link down or broken.



Fault Relay Alarm

Power Failure

□ Power 1 □ Power 2

Port Link Down/Broken

□ Port 1 □ Port 2

□ Port 3 □ Port 4

□ Port 5 □ Port 6

□ Port 7 □ Port 8

□ Port 9 □ Port 10

Fault Relay Alarm interface

SNTP Configuration

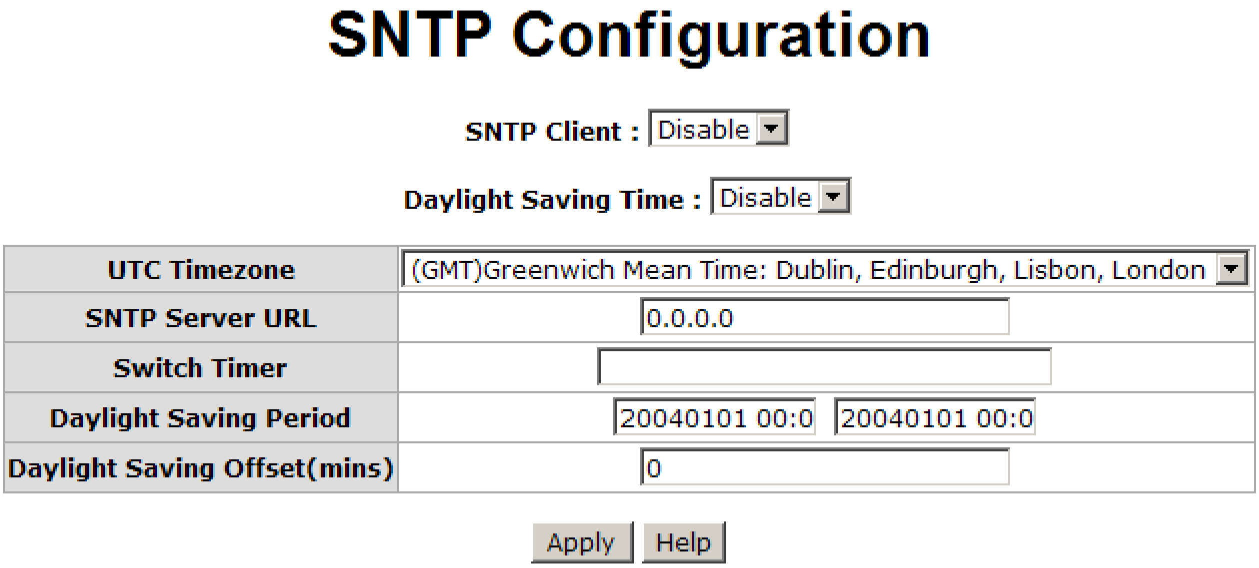
You can configure the SNTP (Simple Network Time Protocol) settings. The SNTP allows you to synchronize the IFE-8T2GB-MXE switch clocks with the Internet.

1. **SNTP Client:** enable or disable SNTP function to get the time from the SNTP server.
2. **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.
3. **UTC Timezone:** 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	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm

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

4. **SNTP Sever URL:** set the SNTP server IP address.
5. **Daylight Saving Period:** set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different in every year.
6. **Daylight Saving Offset (mins):** set up the offset time.
7. **Switch Timer:** Displays the switch current time.
8. Click Apply.



SNTP Configuration

SNTP Client : Disable ▾

Daylight Saving Time : Disable ▾

UTC Timezone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▾
SNTP Server URL	0.0.0.0
Switch Timer	
Daylight Saving Period	20040101 00:0 20040101 00:0
Daylight Saving Offset(mins)	0

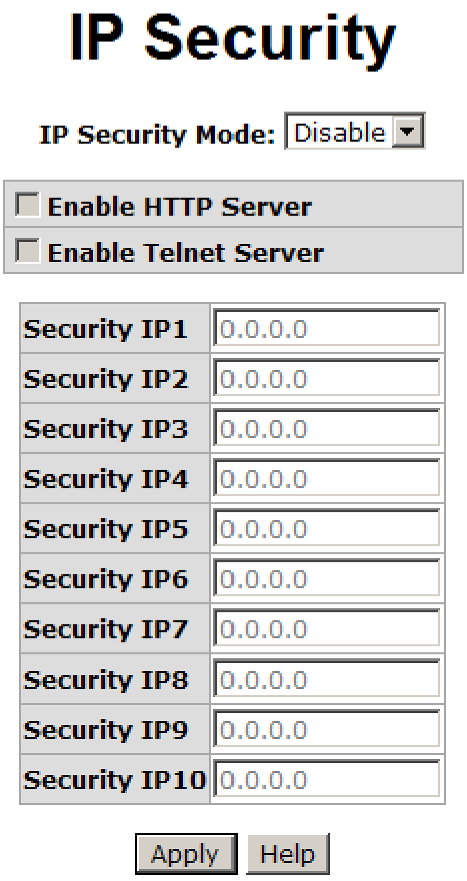
SNTP Configuration interface

IP Security

The IP security function allows users to assign 10 specific IP addresses that have permission to access the switch through the web browser for switch management.

- **IP Security Mode:** when this option is in **Enable** mode, the **Enable HTTP Server** and **Enable Telnet Server** check boxes will then be available.
- **Enable HTTP Server:** when this check box is checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access via HTTP service.
- **Enable Telnet Server:** when checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access via telnet service.
- **Security IP 1 ~ 10:** Assign up to 10 specific IP address. Only these 10 IP address can access and manage the switch through the Web browser
- And then, click Apply button to apply the configuration

[NOTE] Remember to execute the 'Save Configuration' action, otherwise the new configuration will lose when switch power off.



IP Security

IP Security Mode: Disable ▾

☐ Enable HTTP Server

☐ Enable Telnet Server

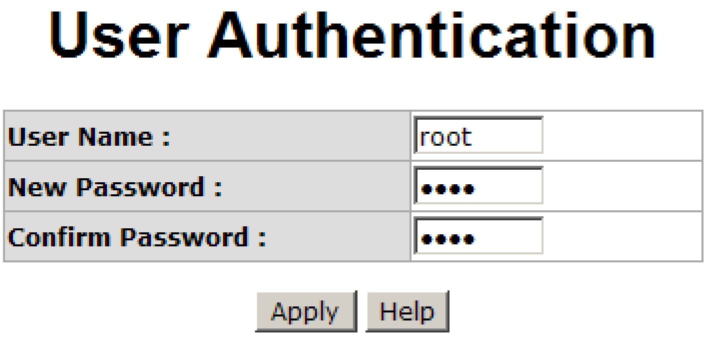
Security IP1	0.0.0.0
Security IP2	0.0.0.0
Security IP3	0.0.0.0
Security IP4	0.0.0.0
Security IP5	0.0.0.0
Security IP6	0.0.0.0
Security IP7	0.0.0.0
Security IP8	0.0.0.0
Security IP9	0.0.0.0
Security IP10	0.0.0.0

IP Security interface

User Authentication

Change web management login user name and password for the management security issue

1. **User name:** Key in the new user name(The default is 'root')
2. **Password:** Key in the new password(The default is 'root')
3. **Confirm password:** Re-type the new password
4. And then, click Apply



User Authentication

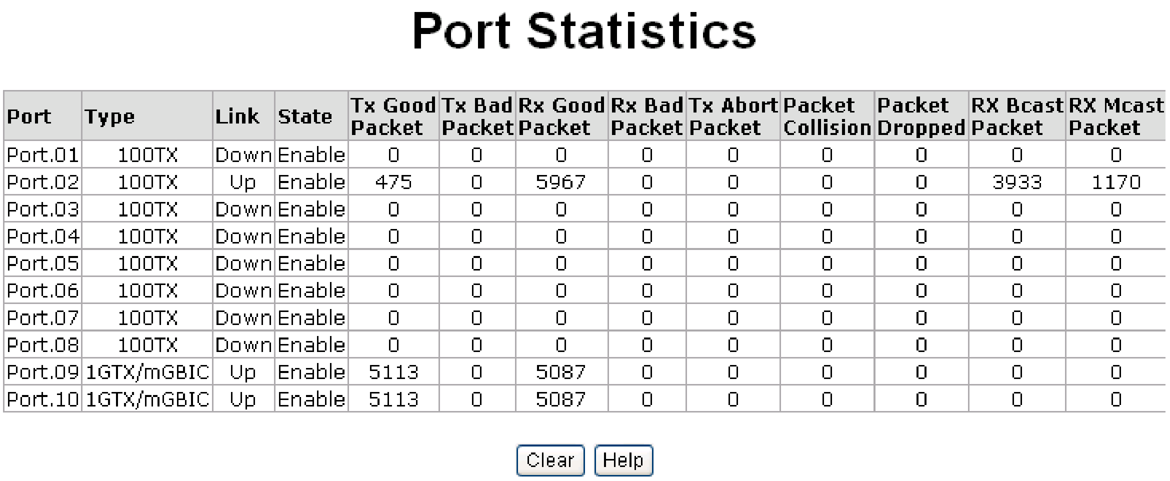
User Name :	root
New Password :	••••
Confirm Password :	••••

User Authentication interface

Port Statistics

The following information provides the current port statistic information.

- **Port:** The port number.
- **Type:** Displays the current speed of connection to the port.
- **Link:** The status of linking—'**Up**' or '**Down**'.
- **State:** Is set by Port Control. When the state is disabled, the port will not transmit or receive any packets.
- **Tx Good Packet:** The number of good packets transmitted via this port.
- **Tx Bad Packet:** The number of bad packets transmitted (including undersize [less than 64 octets], oversize, CRC Align errors, fragments and jabbers packets) via this port.
- **Rx Good Packet:** The number of good packets received via this port.
- **Rx Bad Packet:** The number of good packets received (including undersize [less than 64 octets], oversize, CRC error, fragments and jabbers) via this port.
- **Tx Abort Packet:** The number of aborted packet while transmitting.
- **Packet Collision:** The number of collision packets.
- **Packet Dropped:** The number of dropped packets.
- **Rx Bcast Packet:** The number of broadcast packets.
- **Rx Mcast Packet:** The number of multicast packets.
- Click Clear button to clean all counts.



Port Statistics

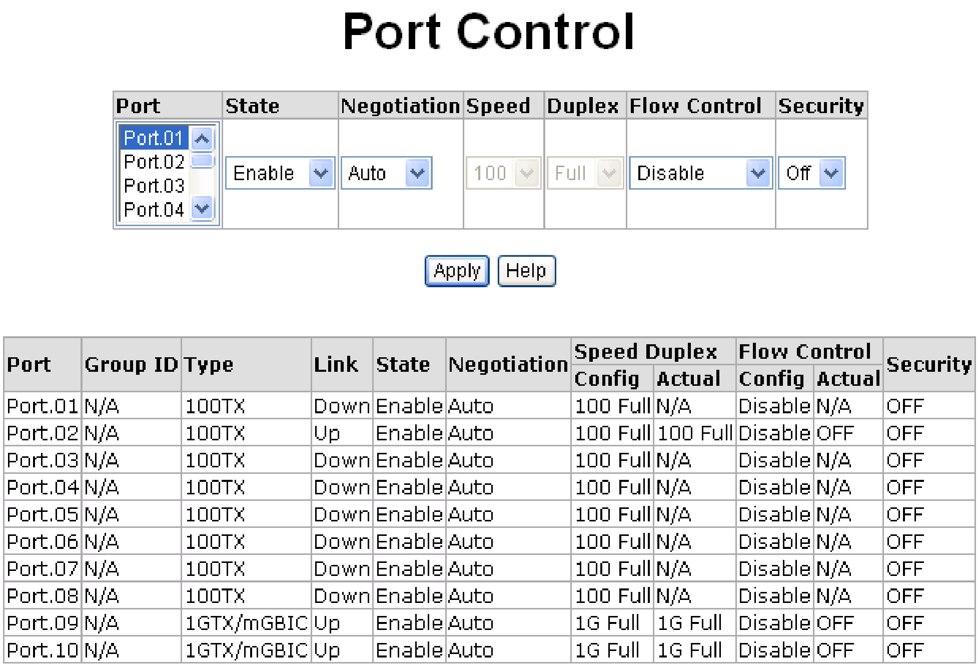
Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision	Packet Dropped	RX Bcast Packet	RX Mcast Packet
Port.01	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.02	100TX	Up	Enable	475	0	5967	0	0	0	0	3933	1170
Port.03	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.07	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.08	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.09	1GTX/mGBIC	Up	Enable	5113	0	5087	0	0	0	0	0	0
Port.10	1GTX/mGBIC	Up	Enable	5113	0	5087	0	0	0	0	0	0

Port Statistics interface

Port Control

In Port control, you can view the port status of every port according to the configuration setting and the negotiation results.

1. **Port:** select the port that you want to configure.
2. **State:** Current port status. The port can be set to disable or enable mode. If the port setting is disable then will not receive or transmit any packet.
3. **Negotiation:** set auto negotiation status of port.
4. **Speed:** set the port link speed.(If using SFP's the data rate is derived from the SFP)
5. **Duplex:** set full-duplex or half-duplex mode of the port.
6. **Flow Control:** set flow control function is **Symmetric** or **Asymmetric** in Full Duplex mode. The default value is **Symmetric**.
7. **Security:** When its state is '**On**', means this port accepts only one MAC address.
8. Click Apply .



Port Control

Port	State	Negotiation	Speed	Duplex	Flow Control	Security
Port.01 Port.02 Port.03 Port.04	Enable	Auto	100	Full	Disable	Off

Port	Group ID	Type	Link	State	Negotiation	Speed Duplex		Flow Control		Security
						Config	Actual	Config	Actual	
Port.01	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.02	N/A	100TX	Up	Enable	Auto	100 Full	100 Full	Disable	OFF	OFF
Port.03	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.04	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.05	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.06	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.07	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.08	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.09	N/A	1GTX/mGBIC	Up	Enable	Auto	1G Full	1G Full	Disable	OFF	OFF
Port.10	N/A	1GTX/mGBIC	Up	Enable	Auto	1G Full	1G Full	Disable	OFF	OFF

Port Control interface

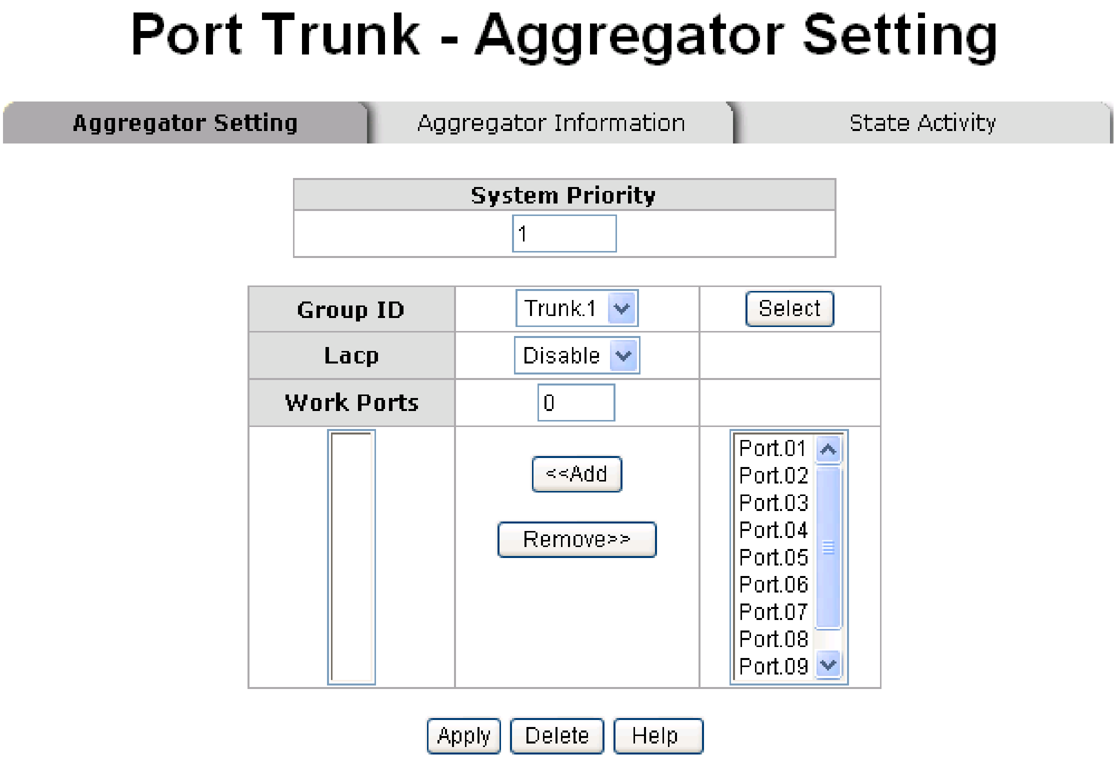
Port Trunking (LACP)

The Link Aggregation Protocol (LACP) provides a standard means for bonding multiple links together to achieve higher data rates.

Link aggregation lets you group up to 4 consecutive ports into two dedicated connections. **LACP operation requires full-duplex mode,** for more detail information please refer to IEEE 802.3ad.

Aggregator setting

1. **System Priority:** a value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
2. **Group ID:** There are three trunk groups to provide configure. Choose the '**Group ID**' and click Select.
3. **LACP:** If enabled, the group is an LACP static trunk group. If disabled, the group is local static trunk group. All ports support LACP dynamic trunk groups. If connecting to a device that also supports LACP, then the LACP dynamic trunk group will be automatically created.
4. **Work ports:** allows a maximum of four ports that can be aggregated at the same time. With LACP static trunk group, the additional ports are standby ports and can be aggregated if working ports fail. If they are on the local static trunk group, the number of ports must be the same as the group member ports.
5. Select the ports to join the trunk group. A max four ports can be aggregated at the same time. Click Add button to add the port. To remove unwanted ports, select the port and click Remove button.
6. If LACP is enabled, you can configure LACP Active / Passive status in each of the ports on State Activity page.
7. Click Apply.
8. Use Delete button to delete Trunk Group. Select the Group ID and click Delete button.
9. LACP Port trunking can be used in at the same time as 'X-ring'



Port Trunk - Aggregator Setting

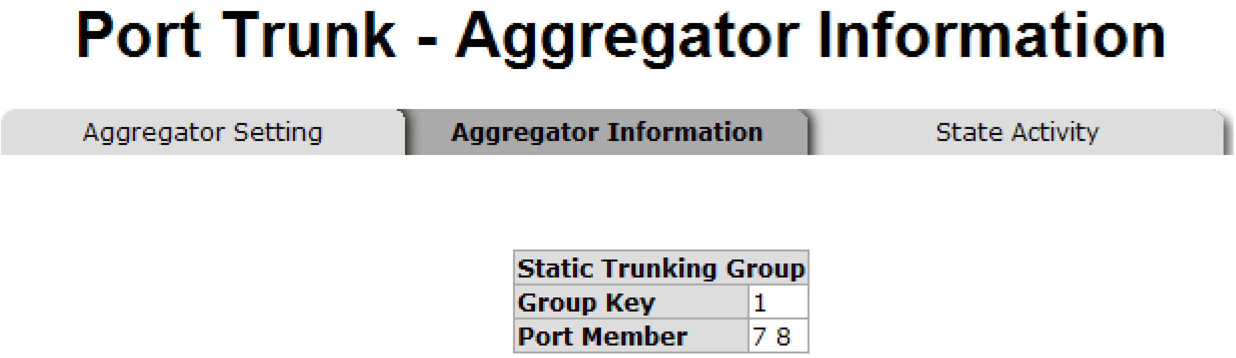
System Priority
1

Group ID	Trunk.1	Select
Lacp	Disable	
Work Ports	0	
	<<Add Remove>>	Port.01 Port.02 Port.03 Port.04 Port.05 Port.06 Port.07 Port.08 Port.09

Port Trunk—Aggregator Setting interface

Aggregator Information

When you have setup the aggregator setting with LACP disabled, you will see the local static trunk group information here.



Port Trunk - Aggregator Information

Static Trunking Group	
Group Key	1
Port Member	7 8

Port Trunk – Aggregator Information interface

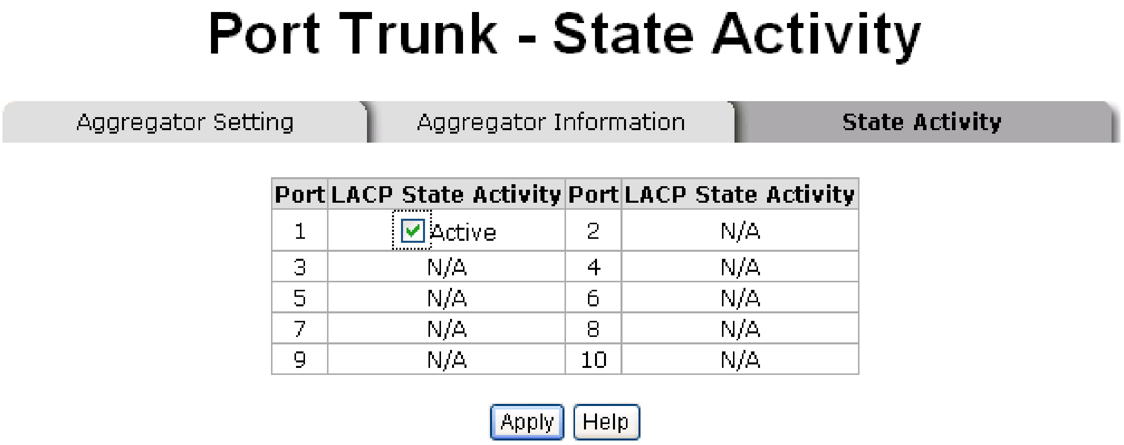
State Activity

When you have setup the LACP aggregator, you can configure the port state activity. You can mark or un-mark each port. When you mark the port and click the Apply button the port state activity will change to **Active**. The opposite state is **Passive**.

- **Active:** The port automatically sends LACP protocol packets.
- **Passive:** The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

[NOTE]

1. A link having either two active LACP ports or one active port can perform dynamic LACP trunk.
2. A link has two passive LACP ports will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.
3. If you set active LACP’s after you have selected the trunk ports, the active status will be created automatically.



Port Trunk - State Activity

Port	LACP State Activity	Port	LACP State Activity
1	☑ Active	2	N/A
3	N/A	4	N/A
5	N/A	6	N/A
7	N/A	8	N/A
9	N/A	10	N/A

Port Trunk – State Activity interface

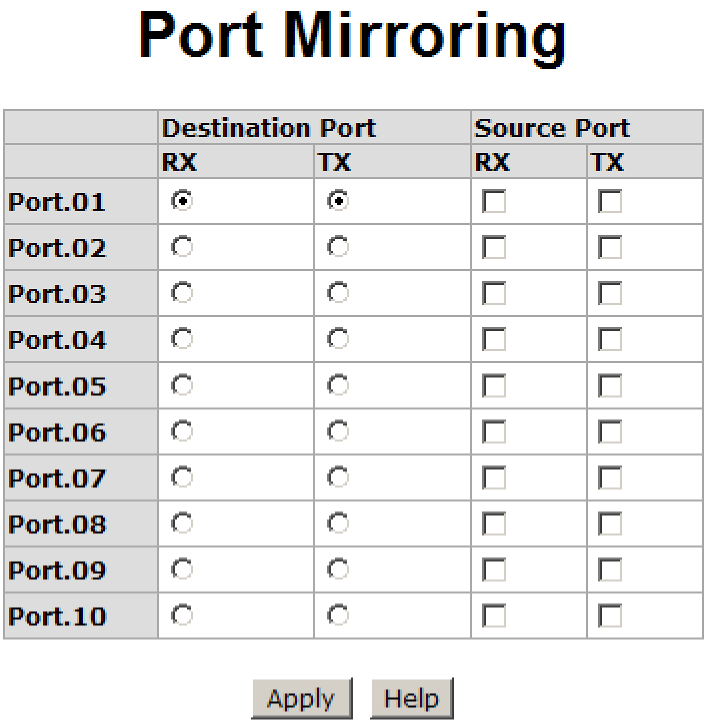
Port Mirroring

Port mirroring is a method for monitor traffic in switched networks. Traffic through ports can be monitored by one specific port. That means the traffic that goes in or out of monitored (source) port will be duplicated into the mirrored (destination) ports.

- **Destination Port:** Only one port can be selected to be the destination (mirror) port for monitoring both RX and TX traffic from the source port. Alternatively it’s possible to use two ports for monitoring. One for RX traffic only and the other for TX traffic only. Users can connect mirrored ports to LAN network analysers

- **Source Port:** The ports that the user wants to monitor. All monitored port traffic will be copied to the mirror (destination) port. Users can select multiple source ports by checking the **RX** or **TX** check boxes to be monitored.

- And then, click Apply button.



Port Mirroring

	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.09	○	○	□	□
Port.10	○	○	□	□

Port Trunk – Port Mirroring interface

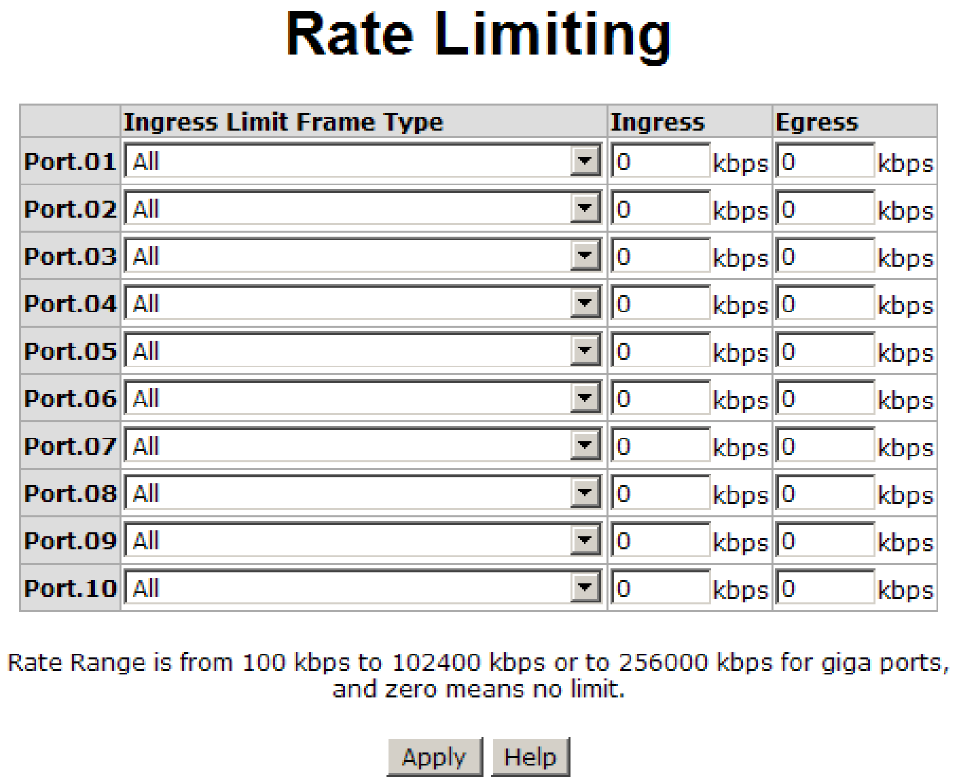
Rate Limiting

You can set up every port's bandwidth rate and frame limitation type.

- **Ingress Limit Frame type:** select the frame type that you want to filter

  There are four possible frame types you can filter.

1. **All, Broadcast / Multicast / Flooded Unicast,**
2. **Broadcast / Multicast** and **Broadcast only**.
3. **Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast** and
4. **Bbroadcast only** types are only for ingress frames. The egress rate only supports **All** type.



Rate Limiting

	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
Port.09	All	0 kbps	0 kbps
Port.10	All	0 kbps	0 kbps

Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.

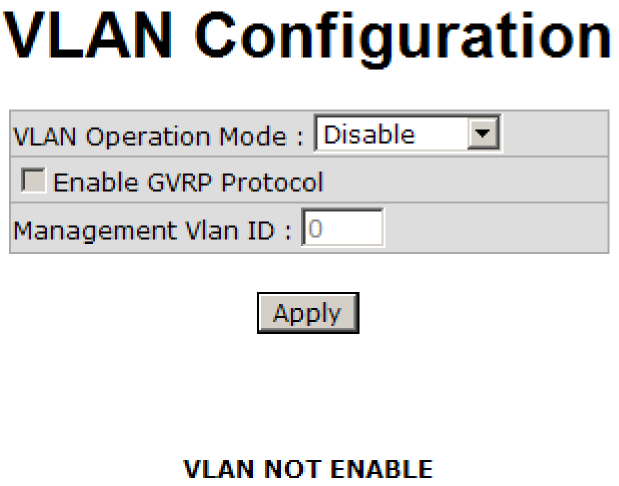
Rate Limiting interface

- All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set it's effective egress rate is 1Mbps, ingress rate is 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate
  - ➢ **Ingress:** Enter the port effective ingress rate(The default value is '0')
  - ➢ **Egress:** Enter the port effective egress rate(The default value is '0')
- And then, click Apply to apply the settings

VLAN configuration

A Virtual LAN (VLAN) is a logical network grouping that limits a broadcast domain, which allows you to isolate network traffic, so 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 to 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 Case Communicaitons IFE-8T2GB-MXE industrial switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration of VLAN operation mode is **Disable**.



VLAN Configuration

VLAN Operation Mode : Disable

□ Enable GVRP Protocol

Management Vlan ID : 0

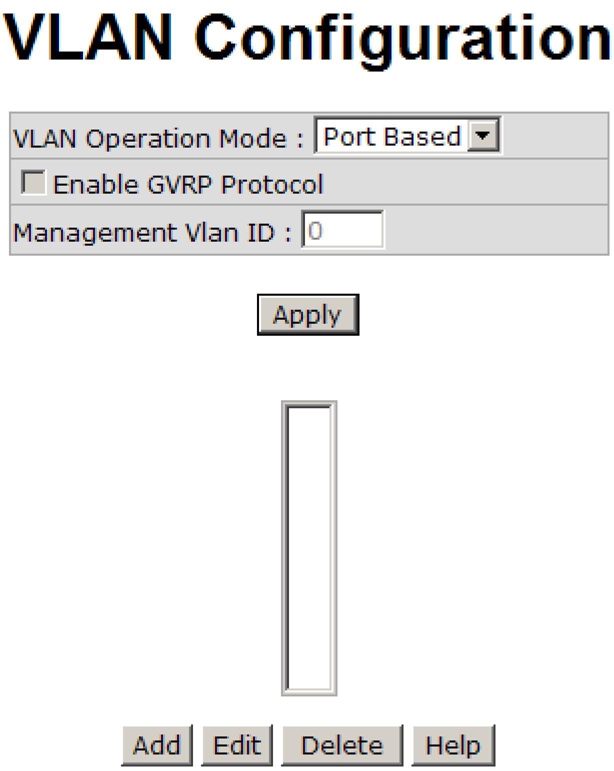
VLAN NOT ENABLE

VLAN Configuration interface

VLAN configuration - Port-based VLAN

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

In order for an end station to send packets to different VLAN groups, it has to be either capable of tagging packets it sends with VLAN tags or be attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.



VLAN Configuration

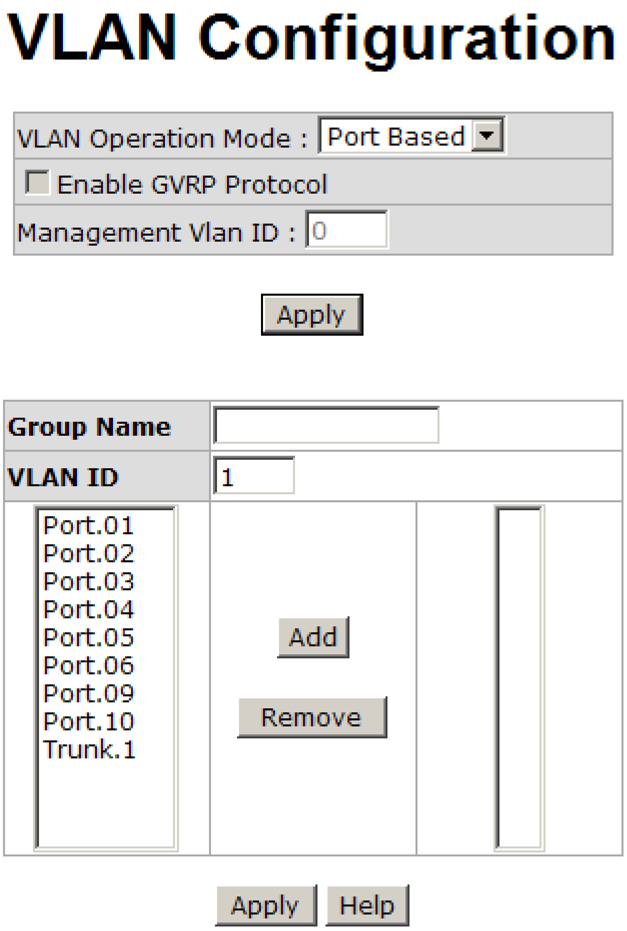
VLAN Operation Mode : Port Based

□ Enable GVRP Protocol

Management Vlan ID : 0

VLAN – Port Based interface

- Click Add to add a new VLAN group(The maximum VLAN group is up to 64 VLAN groups)
- Entering the VLAN name, group ID and grouping the members of VLAN group
- And then, click Apply



VLAN Configuration

VLAN Operation Mode : Port Based

□ Enable GVRP Protocol

Management Vlan ID : 0

Group Name:

VLAN ID: 1

Port.01
Port.02
Port.03
Port.04
Port.05
Port.06
Port.09
Port.10
Trunk.1

VLAN—Port Based Add interface

- You will see the VLAN displays.
- Use Delete button to delete unwanted VLAN.
- Use Edit button to modify existing VLAN group.

[NOTE] Remember to execute the 'Save Configuration' otherwise the new configuration will be lost when the switch is powered off.

802.1Q VLAN

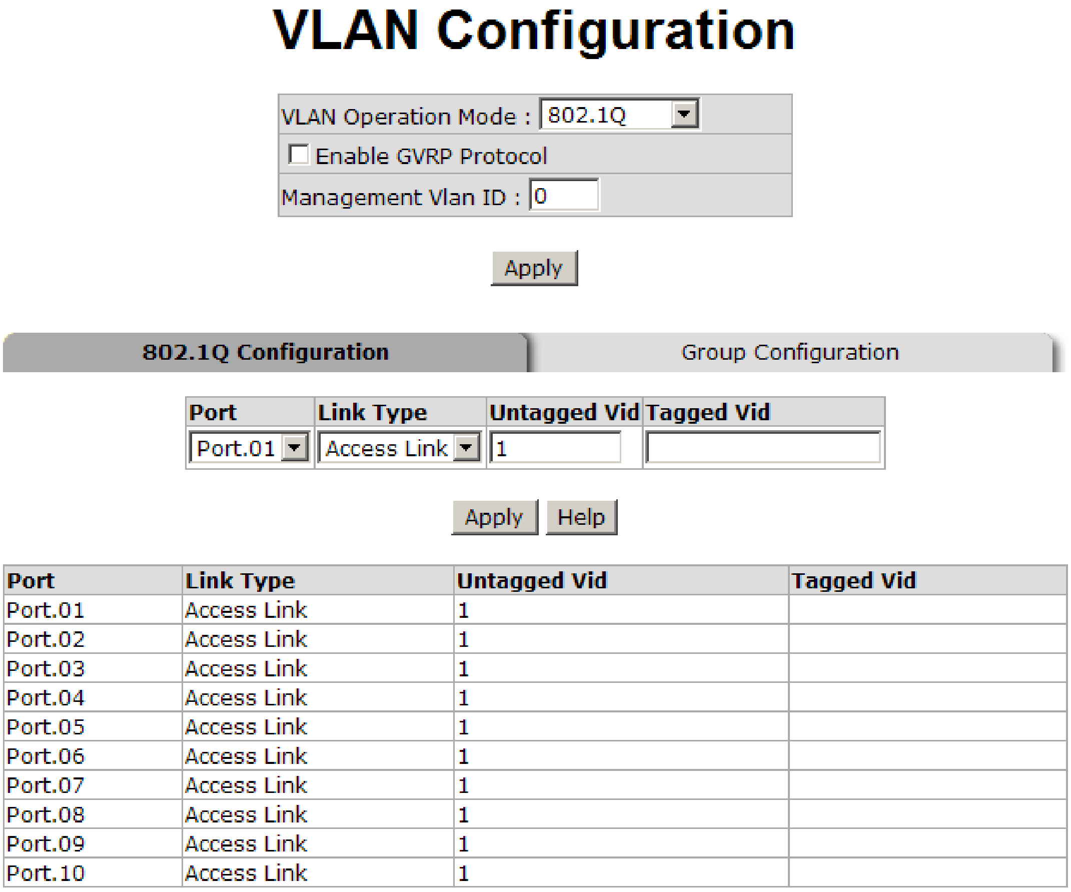
This refers to Tagged-based VLAN’s conforming to the IEEE 802.1Q specification.

As IEEE 802.1Q is a standard it is possible to create a VLAN across different switch venders. IEEE 802.1Q VLAN uses a technique to insert a ‘tag’ into the Ethernet frames. This Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

You can create Tag-based VLAN, and enable or disable GVRP protocol. It’s possible to configure a possible maximum of 256 VLAN groups. If we enable an 802.1Q VLAN, then all ports on the switch belong to the default VLAN, VID is 1.

The default VLAN can’t 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 using the VID of a VLAN defined on the switch; the switch will automatically add that device to the existing VLAN.



VLAN Configuration

VLAN Operation Mode : 802.1Q

☐ Enable GVRP Protocol

Management Vlan ID : 0

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	
Port.02	Access Link	1	
Port.03	Access Link	1	
Port.04	Access Link	1	
Port.05	Access Link	1	
Port.06	Access Link	1	
Port.07	Access Link	1	
Port.08	Access Link	1	
Port.09	Access Link	1	
Port.10	Access Link	1	

802.1q VLAN interface

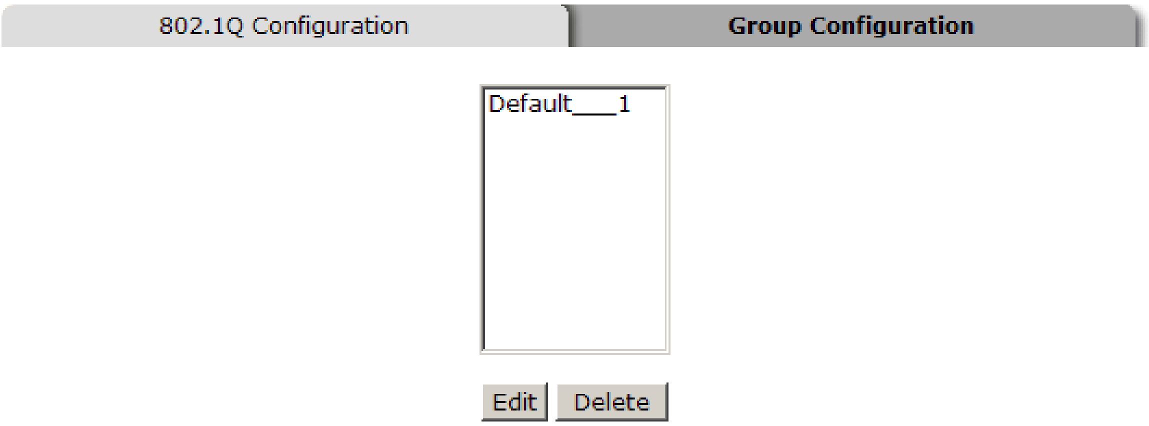
802.1Q Configuration

1. **Enable GVRP Protocol:** select the box to enable GVRP protocol.
2. Select the port that you want to configure.
3. **Link Type**: there are 3 types of link type.
   - **Access Link:** single switch only, allows a user to group ports by setting the same VID.
   - **Trunk Link:** extended application of **Access Link**, allows users to group ports by setting the same VID with 2 or more switches.
   - **Hybrid Link:** Both **Access Link** and **Trunk Link** are available.
4. **Untagged VID:** assign the untagged frame VID.
5. **Tagged VID:** assign the tagged frame VID.
6. Click Apply
7. You can see each port setting in the below table on the screen.

Group Configuration

Edit the existing VLAN Group.

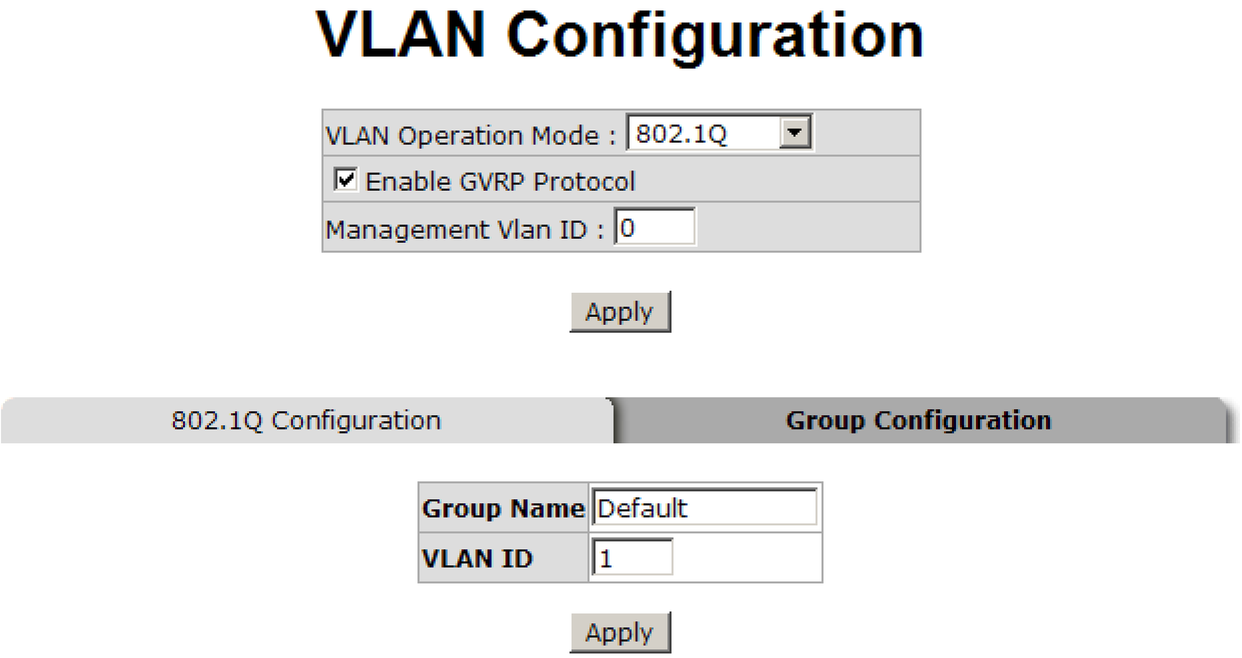
1. Select the VLAN group in the table list.
2. Click Apply



Default___1

Group Configuration interface

3. You can Change the VLAN group name and VLAN ID.
4. Click Apply.



VLAN Configuration

VLAN Operation Mode :	802.1Q
☑ Enable GVRP Protocol	
Management Vlan ID :	0

Group Name	Default
VLAN ID	1

Group Configuration interface

Rapid Spanning Tree

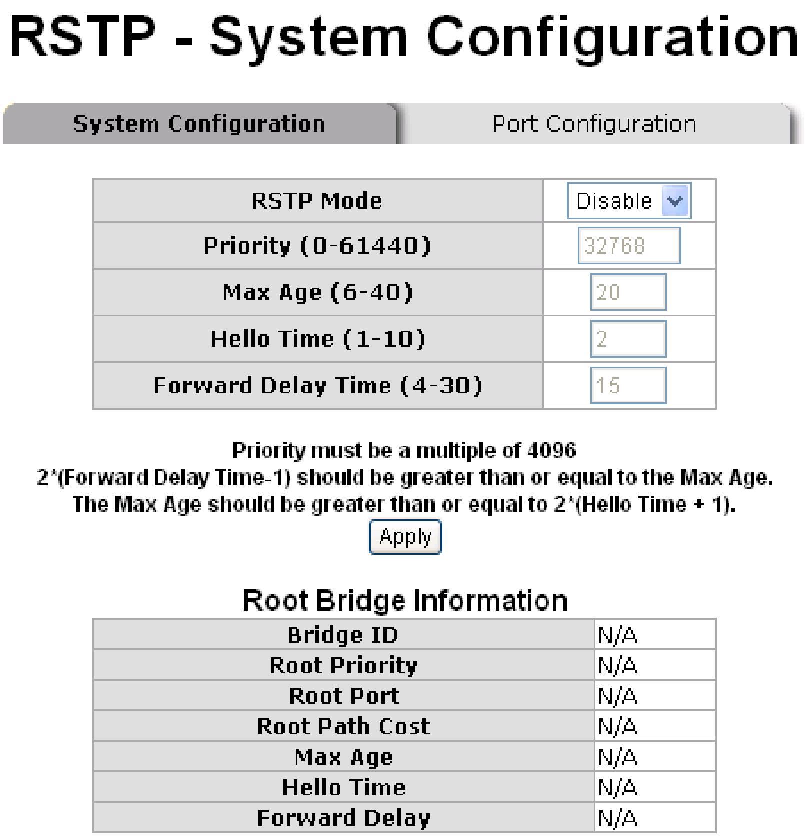
The Rapid Spanning Tree Protocol (RSTP) has evolved from the Spanning Tree Protocol and provides faster re-routing after a link failure. The system also supports STP and the system will auto detect any devices that are connected and running the STP or RSTP protocol.

RSTP - System Configuration

- Users can view spanning tree information relating to the Root Bridge
- Users can modify RSTP state. After modification, click Apply button
    - **RSTP mode:** users must enable or disable the RSTP function before configuring RSTP 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, users must reboot the switch. In accordance with RSTP rules the priority value must be in multiples of 4096.For example 4096, (x2) 8192, (x3) 12,288, (x4) 20,480, (x5) 24,576, (x6) 28672 etc**.**
    - **Max Age (6-40):** the number of seconds a bridge waits without receiving the Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40
    - **Hello Time (1-10):** the time that controls the switch sending out the BPDU packet to check RSTP current status. Enter a value between 1 through 10
    - **Forward 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

[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 - System Configuration

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

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

Root Bridge Information

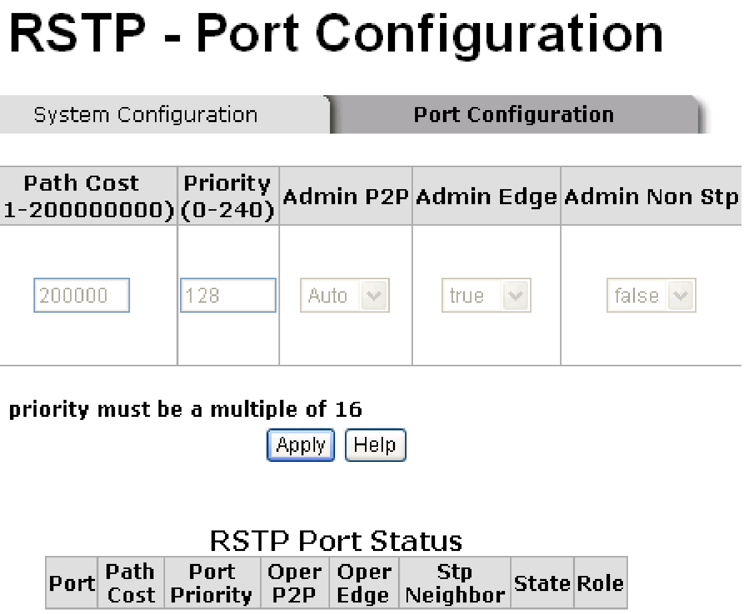
Bridge ID	N/A
Root Priority	N/A
Root Port	N/A
Root Path Cost	N/A
Max Age	N/A
Hello Time	N/A
Forward Delay	N/A

RSTP System Configuration interface

RSTP - Port Configuration

You can configure path cost and priority for every port.

1. Select the port in Port column.
1. **Path Cost:** The cost of the path to the remote bridge from this bridge at the specified port. Enter a number 1 through 200,000,000. (**NB** Path cost is more important than priority level) Typical settings 1Gbps=20,000, 100Mbps, 200,000, 10Mbps=2,000,000)
2. **Priority:** Enter a number 0 through 240. The value of priority must be the multiple of 16. (The lower the number the higher the priority, so to block ports of equal weighting set a higher priority number on the port to be blocked).
3. **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 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 is enables P2P while, false disables P2P. **(NB Switch to Switch=P2P=true)**
4. **Edge:** The port directly connected to end stations cannot create a bridging loop in the network. To configure the port as an edge port, set the port to '**True**' status.
5. **Non Stp:** The port includes the STP mathematic calculation. **True** is not including STP mathematic calculation. **False** is including the STP mathematic calculation.
6. Click Apply.



RSTP - Port Configuration

Port	Path Cost (1-200000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non Stp
	200000	128	Auto	true	false

priority must be a multiple of 16

RSTP Port Status

Port	Path Cost	Port Priority	Oper P2P	Oper Edge	Stp Neighbor	State	Role

RSTP Port Configuration interface

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 such as CaseView learn of problems by receiving traps or change notices from network devices that are SNMP enabled.

System Configuration

- **Community Strings**

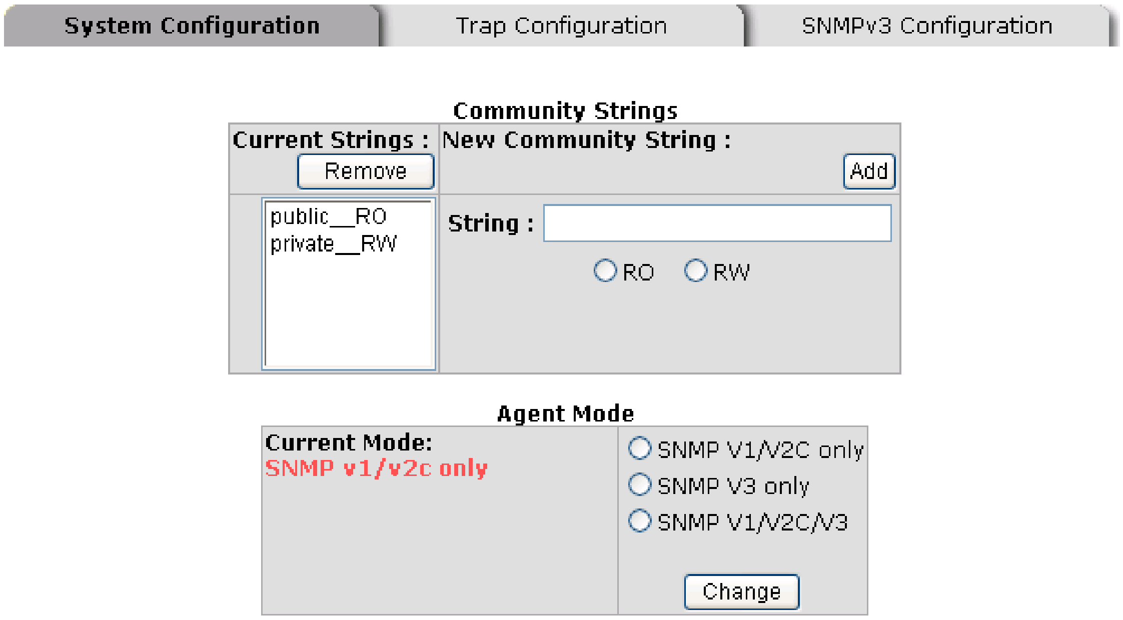
You can define new community strings and set and remove unwanted community strings.

1. **String:** fill the name of string.
2. **RO:** Read only. Enables requests accompanied by this string to display MIB-object information.
3. **RW:** Read write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.

1. Click Add.
2. To remove the community string, select the community string that you have defined and click Remove. You cannot edit the name of the default community string set.

- **Agent Mode:** Select the SNMP version that you want to use. And then click Change to switch to the selected SNMP version mode.

SNMP - System Configuration



System Configuration | Trap Configuration | SNMPv3 Configuration

Community Strings

Current Strings : [Remove]

public__RO
private__RW

New Community String : [Add]

String :

○ RO ○ RW

Agent Mode

Current Mode:
SNMP v1/v2c only

○ SNMP V1/V2C only
○ SNMP V3 only
○ SNMP V1/V2C/V3

[Change]

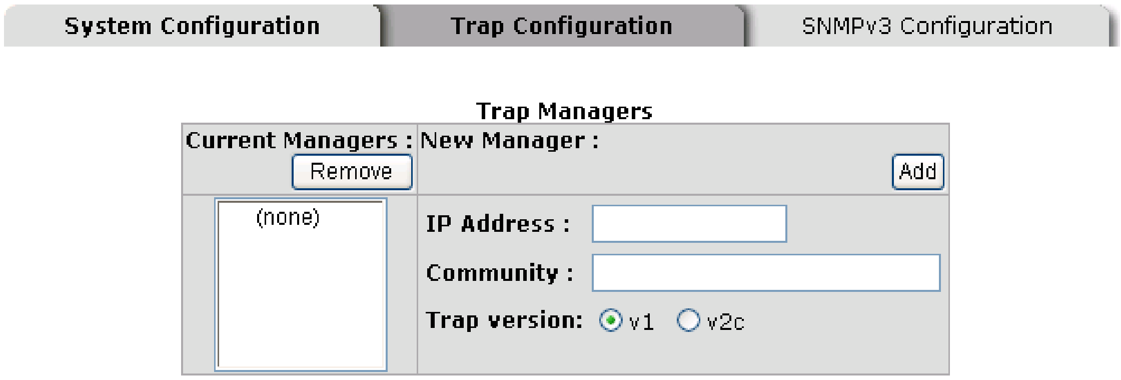
SNMP System Configuration interface

Trap Configuration

A trap manager (such as the CaseView Network Management System) is a management station that receives the traps, and system alerts generated by the switch. If no trap manager is defined, no traps will be issued. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager and enter SNMP community strings and selects the SNMP version.

1. **IP Address:** Enter the IP address of trap manager.
2. **Community:** Enter the community string.
3. **Trap Version:** Select the SNMP trap version type – v1 or v2c.
4. Click Add.
5. To remove the community string, select the community string that you have defined and click Remove. You cannot edit the name of the default community string set.

SNMP - Trap Configuration



System Configuration | Trap Configuration | SNMPv3 Configuration

Trap Managers

Current Managers : Remove

New Manager : Add

(none)

IP Address :

Community :

Trap version: ● v1 ○ v2c

Trap Managers interface

SNMPV3 Configuration

Configure the SNMP V3 function.

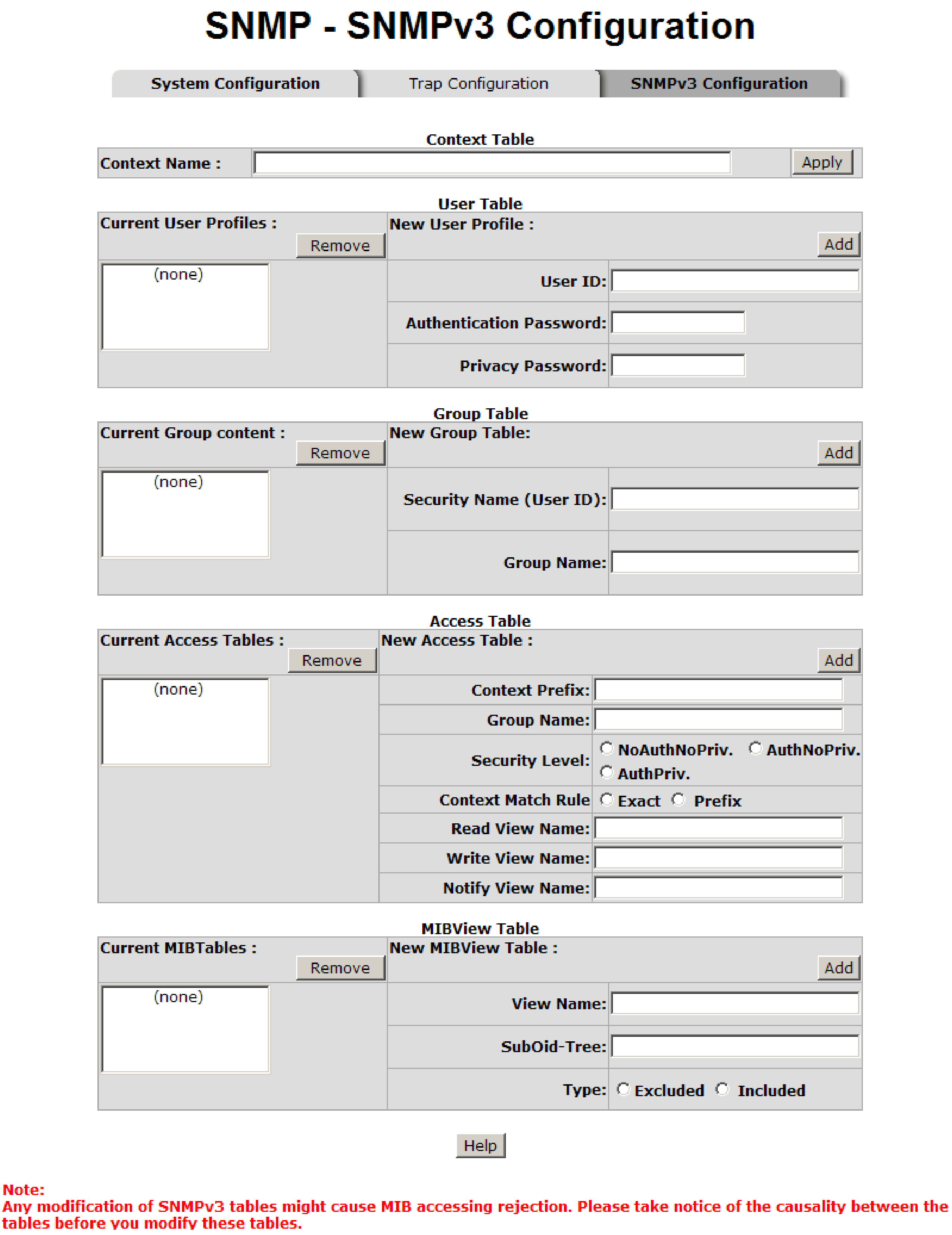
Context Table

Configure SNMP v3 context table. Assign the context name of context table. Click Add to add context name. Click Remove to remove unwanted context name.

User Profile

Configure SNMP v3 user table..

- **User ID:** set up the user name.
- **Authentication Password:** set up the authentication password.
- **Privacy Password:** set up the private password.
- Click Add to add context name.
- Click Remove to remove unwanted context name.



SNMP - SNMPv3 Configuration

Context Table

Context Name : [ ] Apply

User Table

Current User Profiles : Remove

(none)

New User Profile : Add

User ID:	
Authentication Password:	
Privacy Password:	

Group Table

Current Group content : Remove

(none)

New Group Table: Add

Security Name (User ID):	
Group Name:	

Access Table

Current Access Tables : Remove

(none)

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

(none)

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

Group Table

Configure SNMP v3 group table.

- **Security Name (User ID):** Assign the user name that you have set up in the user table.
- **Group Name:** Set up the group name.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

Access Table

Configure SNMP v3 access table.

- **Context Prefix:** Set up the context name.
- **Group Name:** Set up the group.
- **Security Level:** Set up the access level.
- **Context Match Rule:** Select the context match rule.
- **Read View Name:** Set up the read view.
- **Write View Name:** Set up the write view.
- **Notify View Name:** Set up the notify view.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

MIBview Table

Configure MIB view table.

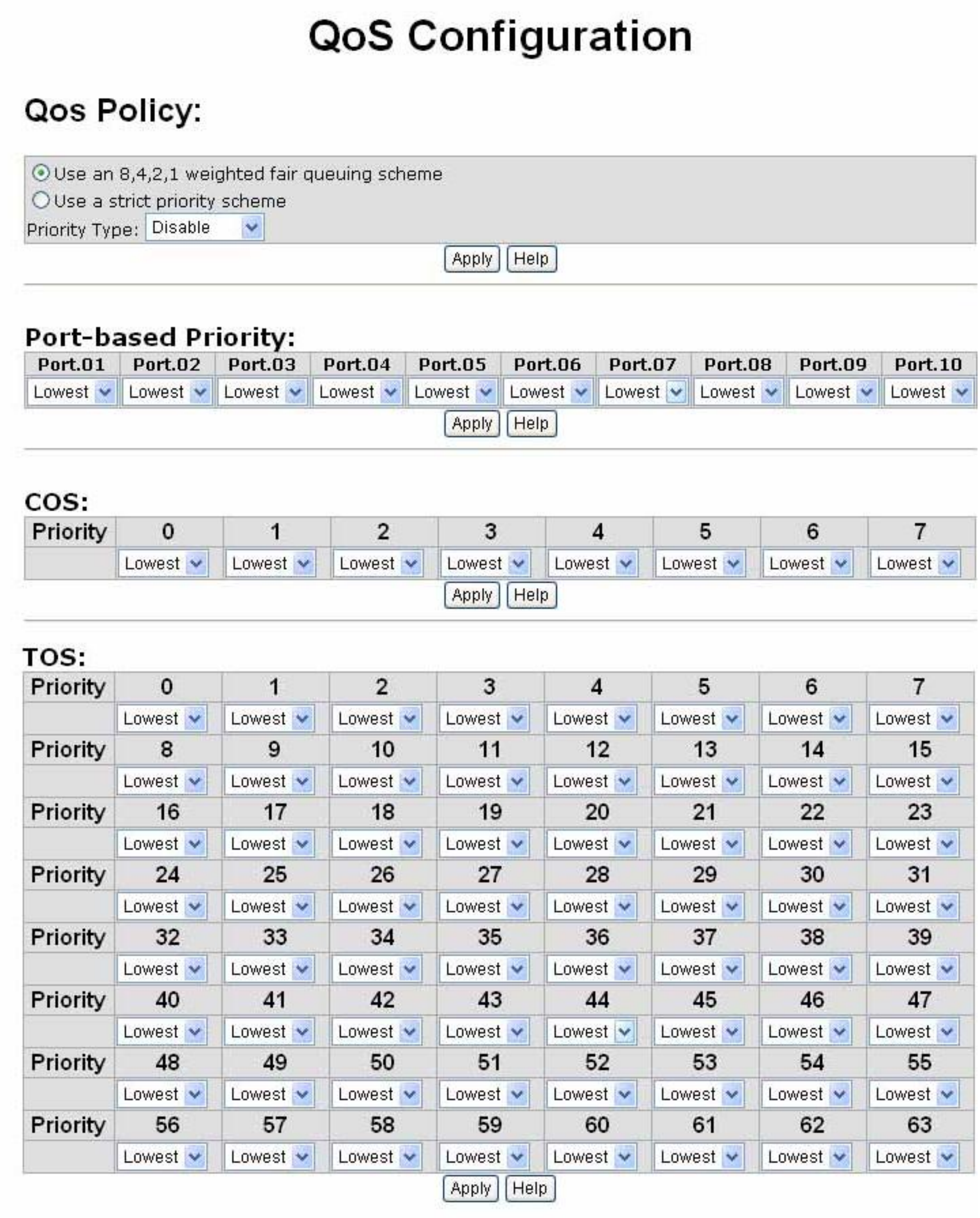
- **ViewName:** Set up the name.
- **Sub-Oid Tree:** Fill the Sub OID.
- **Type:** Select the type – exclude or included.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

QoS Configuration

You can configure the switch (Quality of Service) Qos policy and priority setting, on a per port priority setting, using COS and TOS.

QoS Policy and Priority Type

- **Qos Policy:** select the Qos policy rule.
  - **Using the 8,4,2,1 weight fair queue scheme:** The switch will follow the 8:4:2:1 rule to process priority queues from High to lowest queue. For example, the system will process, 1 frame of the lowest queue, 2 frames of the low queue, 4 frames of the middle queue, and 8 frames of the high queue. These will be processed at the same time in accordance with the 8,4,2,1 policy rule.
  - **Use the strict priority scheme:** The Highest queue will be processed first, except where the higher queue is empty.
- **Priority Type:** there are 5 priority type selections available. If set to disabled it means no priority type is selected.
- **Port-base:** the port priority will follow the **Port-base** that you have assigned – High, middle, low, or lowest.
  - **COS only:** the port priority will only follow the **COS priority** that you have assigned.
  - **TOS only:** the port priority will only follow the **TOS priority** that you have assigned.
  - **COS first:** the port priority will follow the COS priority first, and then other priority rule.
  - **TOS first:** the port priority will follow the TOS priority first, and the other priority rule.
- Click Apply.



QoS Configuration

Qos Policy:

● Use an 8,4,2,1 weighted fair queuing scheme
○ Use a strict priority scheme
Priority Type: Disable

Apply Help

Port-based Priority:

Port.01	Port.02	Port.03	Port.04	Port.05	Port.06	Port.07	Port.08	Port.09	Port.10
Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

Apply Help

COS:

Priority	0	1	2	3	4	5	6	7
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

Apply Help

TOS:

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

Apply Help

QoS Configuration interface

Port Base Priority

Configure per port priority level.

- **Port:** each port has 4 priority levels – High, Middle, Low, and Lowest.
- Click Apply.

COS Configuration

Set up the COS priority level.

- **COS priority:** Set up the COS priority level 0~7 –High, Middle, Low, Lowest.
- Click Apply.

TOS Configuration

Set up the TOS priority.

- **TOS priority:** the system provides 0~63 TOS priority levels. Each level has 4 types of priority – high, middle, low, and lowest.

  The default value is ‘Lowest’ priority for each level.

  When an IP packet is received, the system will check the TOS level value in that IP packet.

  For example, if a user has set TOS level 25 to be high, and port 1 is following the TOS priority policy only, when a packet is received on port 1, the system will check the TOS value of the received packet. If the TOS value of the received packet is 25 (priority = high), then the packet will have highest priority.
- Click Apply.

IGMP Configuration

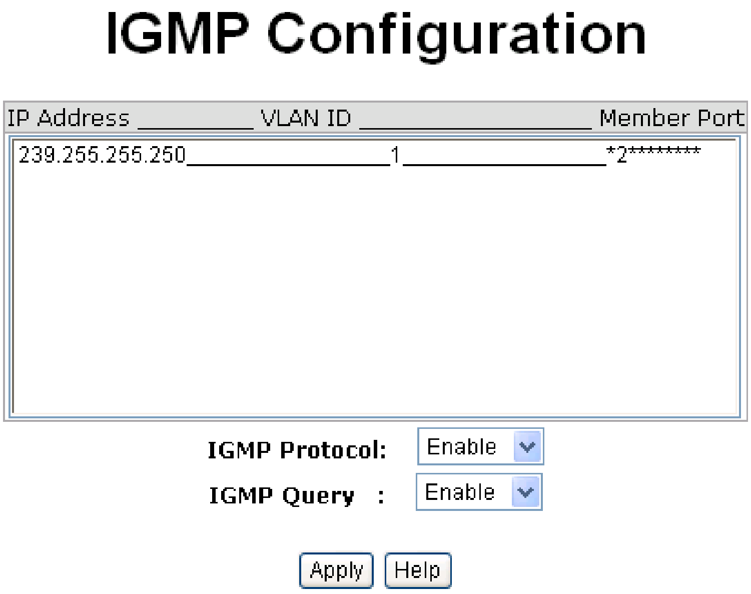
The Internet Group Management Protocol (IGMP) is an internal protocol within the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP has three fundamental types of message as follows:

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

The IFE-8T2GB-MXE switch supports IP multicasting, and you can enable the IGMP protocol on the web management's switch setting under the 'advanced page'. This displays the IGMP snooping information.

IP multicast addresses range are from 224.0.0.0 through to 239.255.255.255.

- **IGMP Protocol:** Enable or disable the IGMP protocol.
- **IGMP Query:** Select the IGMP query function as Enable or Auto to set the switch as a querier for IGMP version 2 multicast network.
- Click Apply.



IGMP Configuration

IP Address	VLAN ID	Member Port
239.255.255.250	1	*2*********

IGMP Protocol: Enable

IGMP Query : Enable

IGMP Configuration interface

X-Ring

X-Ring provides a faster redundant recovery than the Spanning Tree Protocol or Rapid Spanning Tree Protocol. The action is similar to STP or RSTP, but the algorithms are not the same.

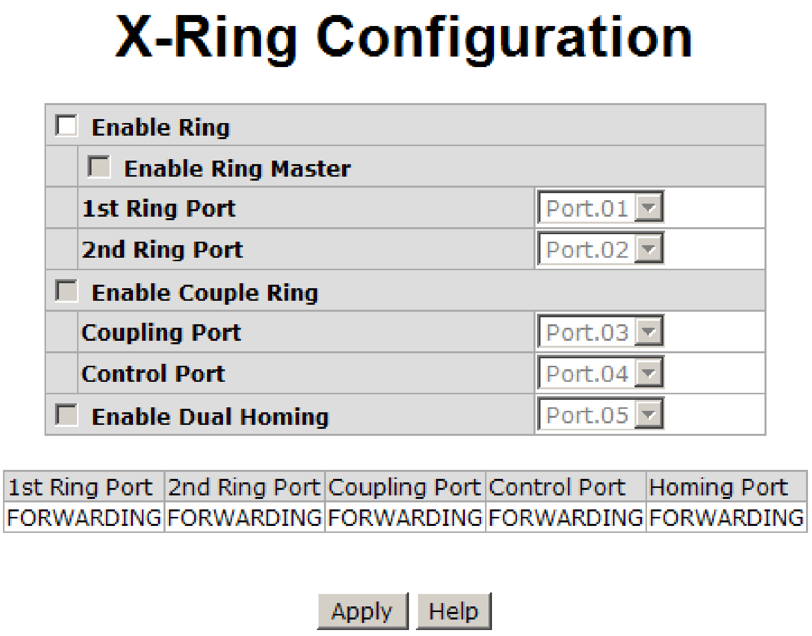
In the X-Ring topology, every switch should be set to use X-Ring and assign two member ports for the ring. Only one switch in the X-Ring group should be set as a Ring master switch and that switch detects a loop and closes one of its ports, leaving the second port open. The closed port is then called the backup port, and the active port is called the 'working port. Other switches in the X-Ring group are called working switches and their two member ports are called working ports. By looking at the management interface of the switch the network manager can view both X-ring ports, and see forwarding on the Ring switches and will notice on the Ring master switch one port is set to forwarding and the other is listed as 'Blocked'
When a network failure occurs, the backup port will automatically become a working port to recover the failure, and the Ring Master will show the previously blocked port as now forwarding.

Each and every switch can be a Ring Master or Slave switch. The network manager sets up which switch is Ring Master from the switches management interface.
The Ring Master can negotiate and place commands to other switches in the X-Ring group. If there are 2 or more switches set to Ring Master, then software will automatically select the switch with lowest MAC address number as the Ring Master. Users can identify which switch has become the Ring Master from the R.M. LED panel of the LED panel on the switch. **NB.** It is advisable to use just one Ring Master especially if running dual homing.

The system also supports the coupling ring protocol to allow managers to connect 2 or more X-Ring groups for redundant backup and dual homing to prevent connection loss between X-Ring groups and the higher level / core switches.

- **Enable X-Ring:** To enable the X-Ring function. Marking the check box to enable the X-Ring function.

- **Enable Ring Master:** Mark the check box for enabling this machine to be a ring master.
- **1st & 2nd Ring Ports:** Pull down the selection menu to assign two ports as member ports. **1st Ring Port** is the working port and **2nd Ring Port** is the backup port to be used if the **1st Ring Port** fails, when the system will automatically set the **2nd Ring Port** to be the working port.
- **Enable Coupling Ring:** To enable the coupling ring function. Select the check box to enable the coupling ring function.
- **Coupling port:** Assign the member port.
- **Control port:** Set the switch as the master switch in the coupling ring.
- **Enable Dual Homing:** Set up one of the ports on the switch to be the Dual Homing port. In an X-Ring group, the maximum number Dual Homing ports is one, although two ports per ring go the head end switches. Dual Homing only works when the X-Ring is enabled.
- And then, click Apply to apply the configuration.



X-Ring Configuration

□ Enable Ring	
□ Enable Ring Master	
1st Ring Port	Port.01
2nd Ring Port	Port.02
□ Enable Couple Ring	
Coupling Port	Port.03
Control Port	Port.04
□ Enable Dual Homing	Port.05

1st Ring Port	2nd Ring Port	Coupling Port	Control Port	Homing Port
FORWARDING	FORWARDING	FORWARDING	FORWARDING	FORWARDING

X-ring Interface

[NOTE]

1. You cannot run X-Ring and RSTP at the same time.
2. Remember to 'Save' the configuration changes otherwise they will be lost if the switches are powered off.

Security

This section, configures the 802.1x and MAC address table.

802.1X / Radius Configuration

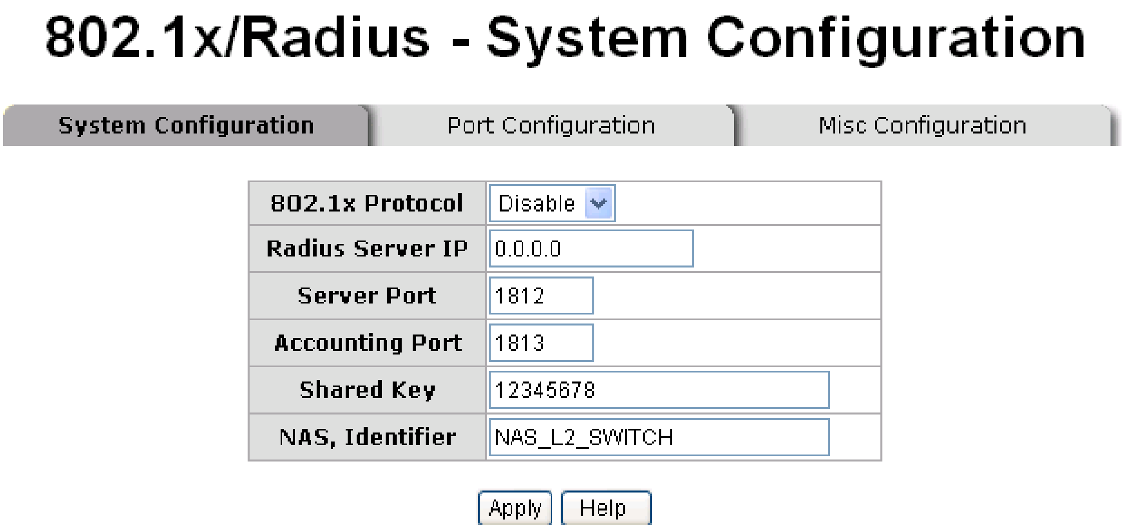
802.1x is an IEEE authentication specification that allows a client to connect to a wireless access point or wired switch but prevents the client from gaining access to the Internet until authorised to do so, by entering, a user name and password that are verified by a separate server.

System Configuration

After enabling the IEEE 802.1X, you can configure the parameters for 801.1X

.

1. **IEEE 802.1x Protocol:** .enable or disables 802.1x protocol.
2. **Radius Server IP:** set the Radius Server IP address.
3. **Server Port:** set the UDP destination port for authentication requests to the specified Radius Server.
4. **Accounting Port:** set the UDP destination port for accounting requests to the specified Radius Server.
5. **Shared Key:** set an encryption key for using during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
6. **NAS, Identifier:** set the identifier for the radius client.
7. Click Apply .



802.1x/Radius - System Configuration

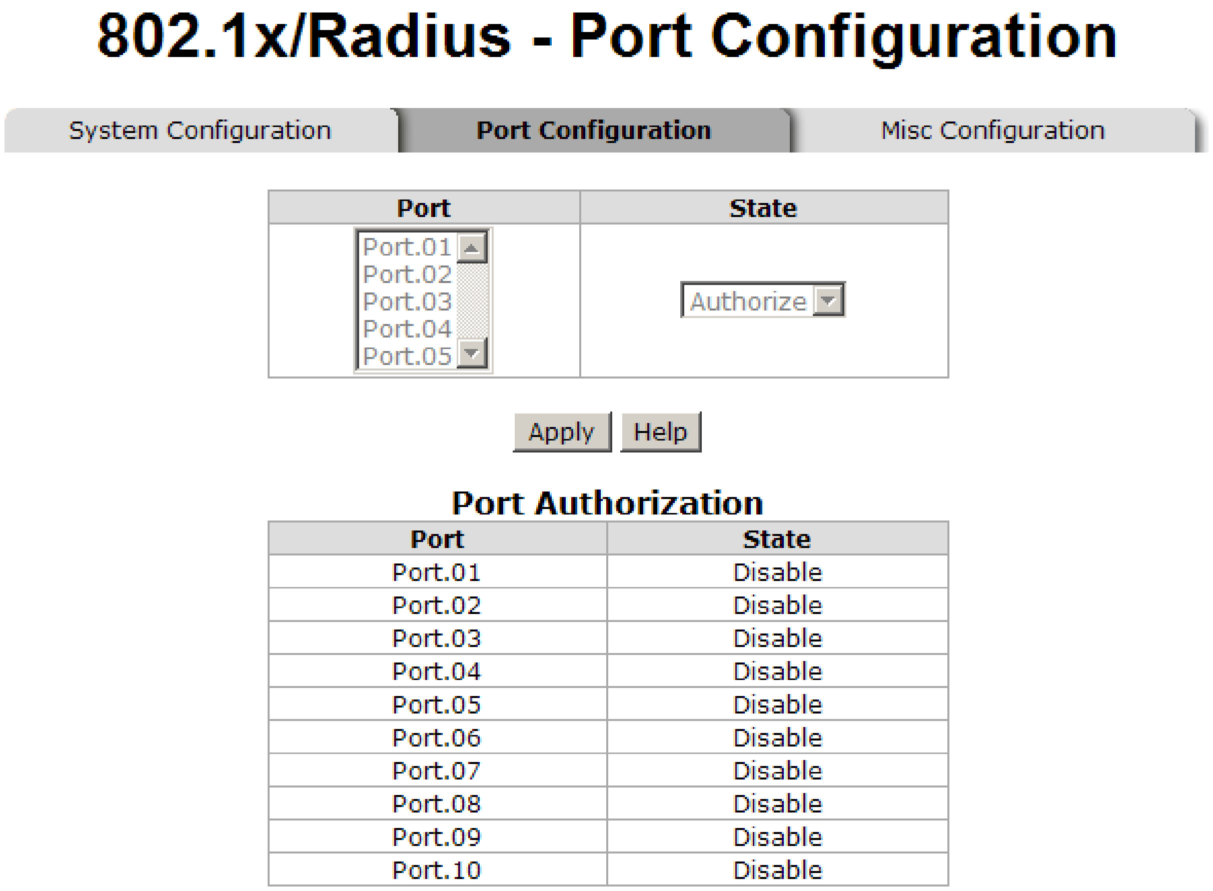
802.1x Protocol	Disable
Radius Server IP	0.0.0.0
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

802.1x System Configuration interface

802.1x Per Port Configuration

You can configure 802.1x authentication state for each port. The State provides Disable, Accept, Reject and Authorize. Use '**Space**' key change the state value.

- **Reject:** the specified port is required to be held in the unauthorized state.
- **Accept:** the specified port is required to be held in the Authorized state.
- **Authorized:** the specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
- **Disable:** The specified port is required to be held in the Authorized state
- Click Apply.



802.1x/Radius - Port Configuration

Port	State
Port.01 Port.02 Port.03 Port.04 Port.05	Authorize

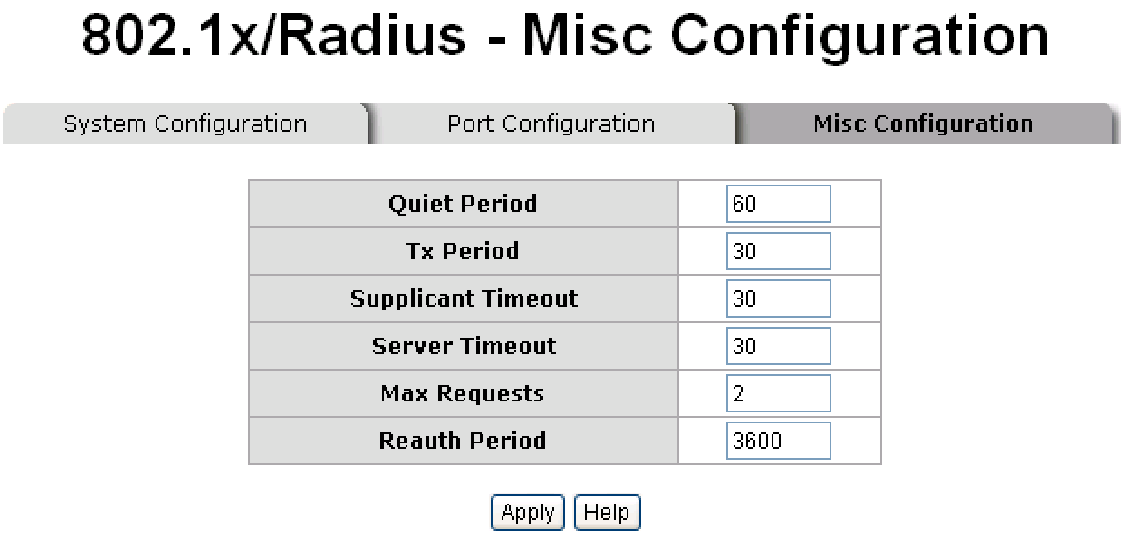
Port Authorization

Port	State
Port.01	Disable
Port.02	Disable
Port.03	Disable
Port.04	Disable
Port.05	Disable
Port.06	Disable
Port.07	Disable
Port.08	Disable
Port.09	Disable
Port.10	Disable

802.1x Per Port Setting interface

Misc Configuration

1. **Quiet Period:** set the period during which the port doesn't try to acquire a supplicant.
2. **TX Period:** set the period the port waits for retransmitting the next EAPOL PDU during an authentication session.
3. **Supplicant Timeout:** set the period of time the switch waits for a supplicant response to an EAP request.
4. **Server Timeout:** set the period of time the switch waits for a server response to an authentication request.
5. **Max Requests:** set the number of authentication that must time-out before authentication fails and the authentication session ends.
6. **Reauth period:** set the period of time after which clients connected must be re-authenticated.
7. Click Apply.



802.1x/Radius - Misc Configuration

Quiet Period	60
Tx Period	30
Supplicant Timeout	30
Server Timeout	30
Max Requests	2
Reauth Period	3600

802.1x Misc Configuration interface

MAC Address Table

Use the MAC address table to ensure port security.

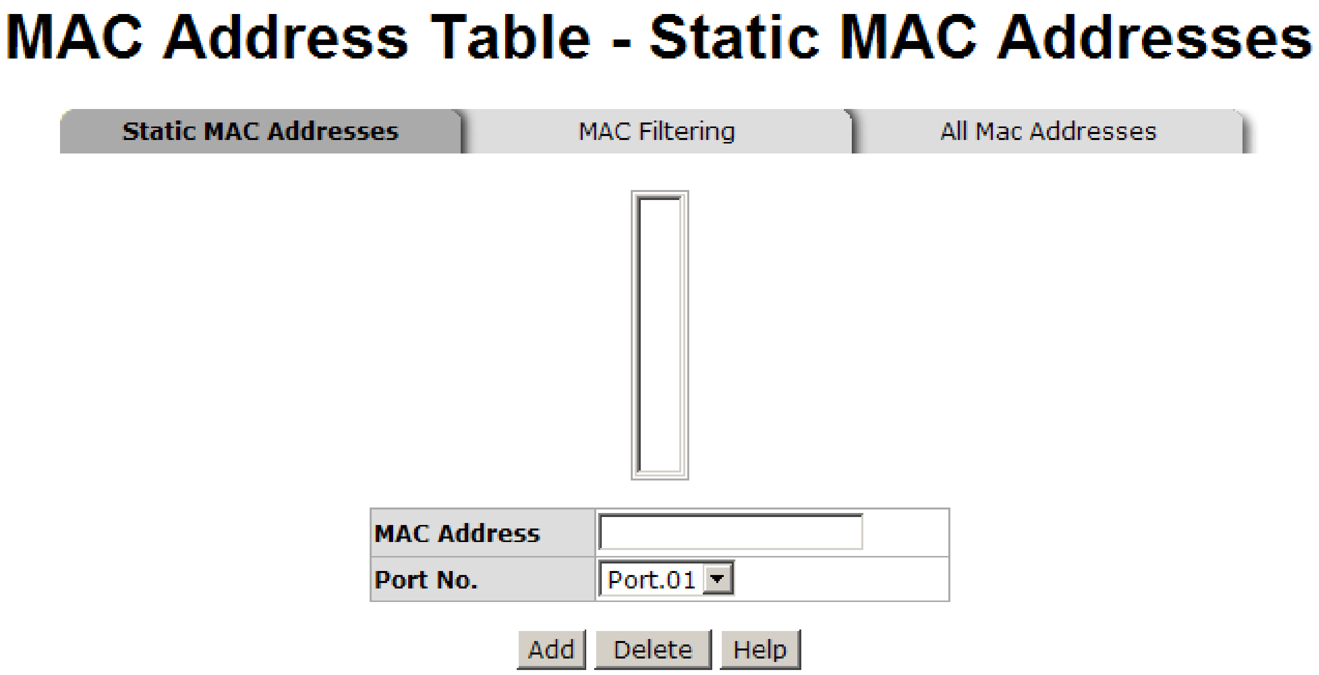
Static MAC Address

You can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off the device is active on the network again. You can add / modify / delete a static MAC address.

- **Add the Static MAC Address**

You can add static MAC address in switch MAC table.

1. **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
2. **Port No.:** pull down the selection menu to select the port number.
3. Click Add.
4. If you want to delete the MAC address from filtering table, select the MAC address and click Delete.



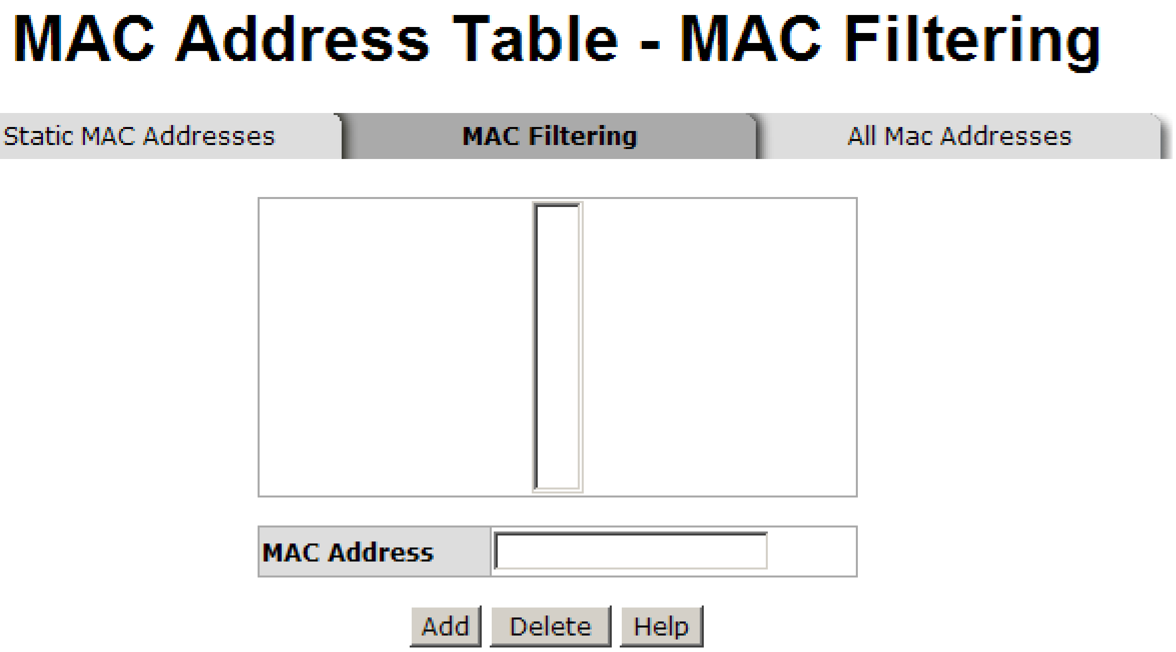
MAC Address Table - Static MAC Addresses

MAC Address	
Port No.	Port.01

Static MAC Addresses interface

MAC Filtering

By filtering MAC address, the switch can easily filter pre-configure MAC address and reduce the un-safety. You can add and delete filtering MAC address.



MAC Address Table - MAC Filtering

MAC Address	

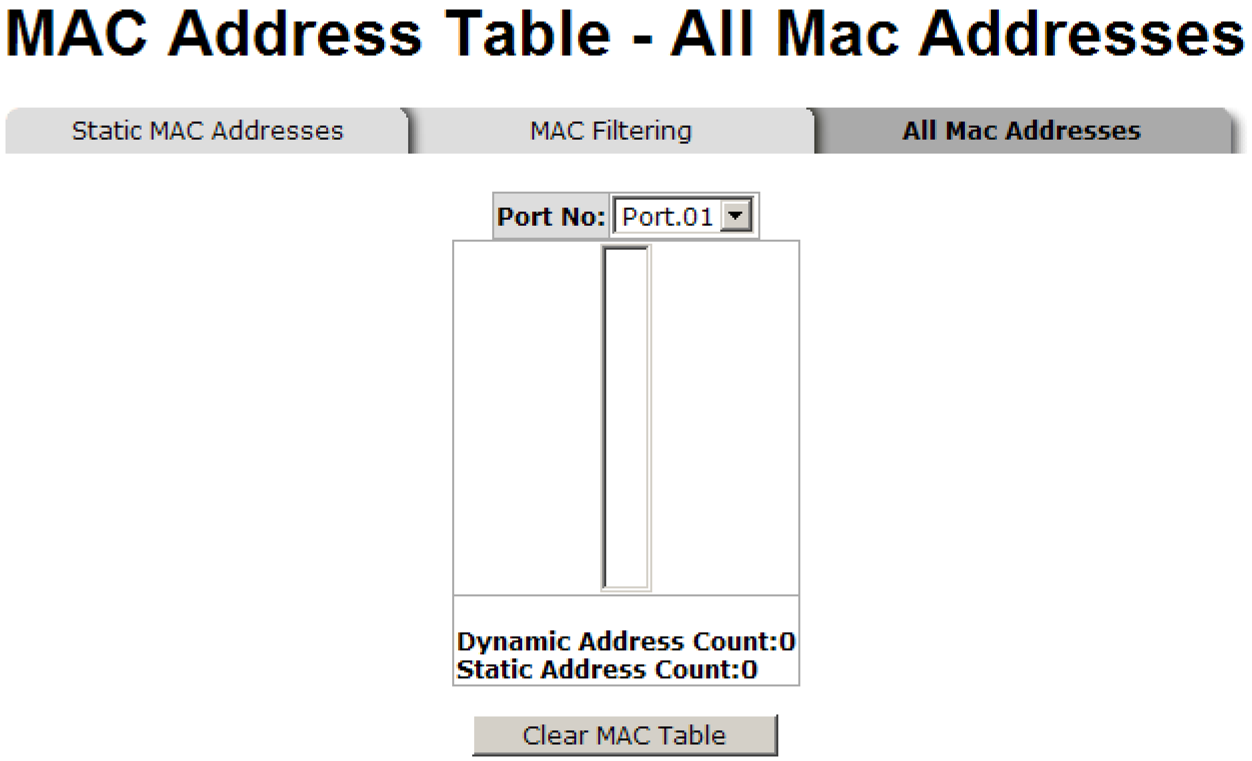
MAC Filtering interface

1. **MAC Address:** Enter the MAC address that you want to filter.
2. Click Add.
3. If you want to delete the MAC address from filtering table, select the MAC address and click Delete.

All MAC Addresses

You can view the port that connected device's MAC address and related devices' MAC address.

1. Select the port.
2. The selected port of static MAC address information will be displayed here.
3. Click Clear MAC Table to clear the current port static MAC address information on screen.



MAC Address Table - All Mac Addresses

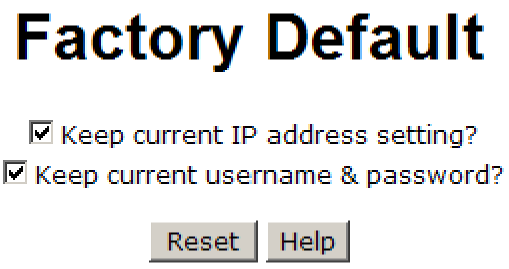
Port No: Port.01

Dynamic Address Count:0
Static Address Count:0

All MAC Address interface

Factory Default

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



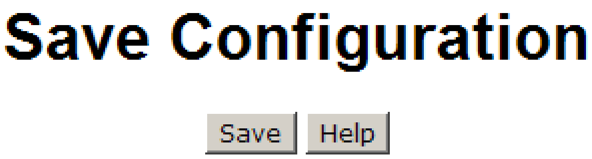
Factory Default

☑ Keep current IP address setting?
☑ Keep current username & password?

Factory Default interface

Save Configuration

Save all configuration changes that you have made to the system. To ensure the all configuration will be saved. Click Save to save the all configuration to the flash memory.

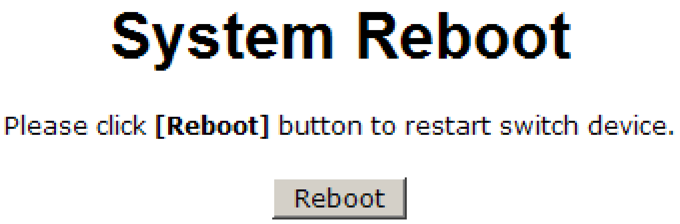


Save Configuration

Save Configuration interface

System Reboot

Reboot the switch in software reset. Click Reboot to reboot the system.



System Reboot

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

System Reboot interface

Trouble shooting

- Verify that you have the right power cord/adapter (DC 12-48V), please don’t use the power adapter with a DC output higher than 48V, or the switch will be damaged.

- Select the proper UTP cable to build the network. Please check that you’re using the right cable. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable with RJ-45 connections. 100Ω Category 5e or above cable for 100/1000Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

- **Diagnosing LED Indicators:** the Switch can be monitored through the panel indicators, which can identify common problems the user may encounter and find it easier to identify problems.

- If the power indicator does not light when the power cord is plugged in, you may have a problem with power cord. Check for a loose power connections, power losses or surges at power outlet. If you still cannot resolve the problem, contact your local Case Communications reseller for assistance.

- If the IFE-8T2GB-MXE switch LED indicators are normal and the cables are correctly connected but the your unable to send or receive data, please check your system’s Ethernet devices’ configuration status. Check that the attached devices don’t require the Ethernet ports set to a fixed data rate or flow control negotiation.

Technical Specification

The IFE-8T2GB-MXE is an 8 x 10/100TX + 2 10/100/1000T/Mini-GBIC Combo with X-Ring L2 Managed Industrial Switch. The table below shows the technical specification for the switch.

Standard	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX Ethernet IEEE 802.3ab 1000Base-T IEEE 802.3z Gigabit fiber IEEE 802.3x Flow Control and Back-pressure IEEE 802.3ad Port trunk with LACP IEEE 802.1d spanning tree / IEEE802.1w rapid spanning tree IEEE 802.1p class of service IEEE 802.1Q VLAN Tag IEEE 802.1x User Authentication (Radius) IEEE 802.1ab LLDP**
Protocol	CSMA/CD
Management	SNMP v1, v2c and v3 management Web interface management Telnet interface management Command Line Interface (CLI) management
SNMP MIB	RFC 1215 Trap RFC 1213 MIBII RFC 1157 SNMP MIB RFC 1493 Bridge MIB RFC 2674 VLAN MIB RFC 1643

	RFC 1757 RSTP MIB Private MIB LLDP MIB
SNMP Trap	Up to 3 Trap stations Cold start Port link Up / Port link down Authentication Failure Private Trap for power status Port Alarm configuration Fault alarm X-Ring topology change
Technology	Store and forward switching architecture
Transfer Rate	14,880 pps for Ethernet port 148,800 pps for Fast Ethernet port 1,488,000 pps for Gigabit Fiber Ethernet port
MAC address	8K MAC address table
Packet Buffer	1Mbits
LED	**8 10/100TX:** Link/Activity (Green), Full duplex/Collision (Yellow) **Giga Copper:** Link/Activity (Green), Speed (Green) **SFP:** Link/Activity (Green) **Per unit:** Power (Green), Power 1 (Green), Power 2 (Green), Fault (Red), Master (Green)
Network Cable	10Base-T: 2-pair UTP/STP Cat. 3, 4, 5 cable EIA/TIA-568 100-ohm (100m) 100Base-TX: 2-pair UTP/STP Cat. 5/5e cable EIA/TIA-568 100-ohm (100m) 1000Base-T: 2-pair UTP/STP Cat. 5e or above cable EIA/TIA-568 100-ohm (100m)

Optical cable	■ **LC (Multi-mode):** 50/125 or 62.5/125 μm ■ **LC (Single mode):** 9/125 μm ■ **Available distance:** 2km (Multi-mode)/30km (single-mode) ■ **Wavelength:** 1310nm (multi-mode/single mode)
Back-plane	5.6Gbps
Packet throughput ability	8.3Mpps at 64bytes
Power Supply	12 ~48 VDC Redundant power with polarity reverse protection and removable terminal block.
Power consumption	9.5 Watts
X-Ring/X-Ring plus	Support X-Ring, Dual Homing, and Couple Ring Provides redundant backup feature and the recovery time below 300ms **X-Ring plus can be below 1 ms
VLAN	Port based VLAN IEEE802.1Q Tag VLAN (256 entries)/VLAN ID (up to 4k in number which can be assigned from 1 to 4096) GVRP (256 groups) Double Tag VLAN (Q in Q)* Private VLAN**
Port Trunk with LACP	LACP Port Trunk: 4 Trunk groups/Maximum 4 trunk members
LLDP**	Supports LLDP that allows the switch to advertise its identity and capabilities

Quality of service	The quality of service determined by port, Tag and IPv4 Type of Service, IPv4/IPv6 Different Service
Class of service	Supports IEEE 802.1p class of service, per port provides 4 priority queues
Spanning tree	IEEE802.1d spanning tree IEEE802.1w rapid spanning tree.
IGMP	Supports IGMP snooping v1, v2 and v3 Up to 256 multicast groups and IGMP query
SMTP	Supports SMTP Server and 6 e-mail accounts for receiving event alert
SNTP	Supports SNTP to synchronize system clock in Internet
IP Security	Supports 10 IP addresses of permission to access the switch management and to prevent unauthorized intruder
Login Security	Supports IEEE-802.1X Authentication/RADIUS
Port Security	Supports 100 entries of MAC address for static MAC and another 100 for MAC filter
Port mirror	TX packet only RX packet only, Both of TX and RX packet
Firmware update	TFTP firmware update TFTP backup and restore
Relay Alarm	Provides one relay output for port breakdown, power fail Alarm Relay current carry ability: 1A @ DC24V

Bandwidth control	Supports ingress packet filter and egress packet limit The egress rate control supports all of packet type and the limit rates are 100K ~ 250Mbps Ingress filter packet type combination rules are Broadcast/Multicast/Unknown Unicast packet, Broadcast/Multicast, Broadcast packet only and all of packets The packet filter rate can be set from 100k to 250Mbps
Flow Control	Supports Flow Control for Full-duplex and Back Pressure for Half-duplex
System Log	Supports System log record and remote system log server
DHCP	Provides DHCP Client/DHCP Server function
DNS	Provides DNS client feature Supports Primary and Secondary DNS Server
Install	DIN rail kit and wall mount ear
Operation Temp.	-40℃ to +75℃
Operation Humidity	5% to 95% (Non-condensing)
Storage Temperature	-40℃ to 85℃
Case Dimension	IP-30, 72 mm (W) x 105 mm (D) x 152mm (H)

EMI	FCC Class A CE EN61000-4-2 CE EN61000-4-3 CE EN61000-4-4 CE EN61000-4-5 CE EN61000-4-6 CE EN61000-4-8 CE EN61000-4-11 CE EN61000-4-12
Safety	UL cUL CE/EN60950-1
Stability testing	IEC60068-2-32 (Free fall) IEC60068-2-27 (Shock) IEC60068-2-6 (Vibration)

* Future Release

** Optional

APPENDIX A

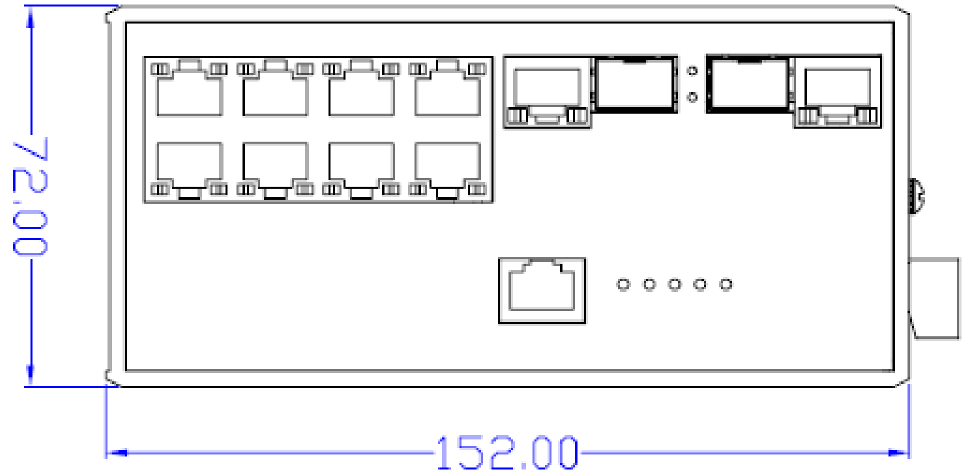
HEAT AND POWER CONSUMPTION

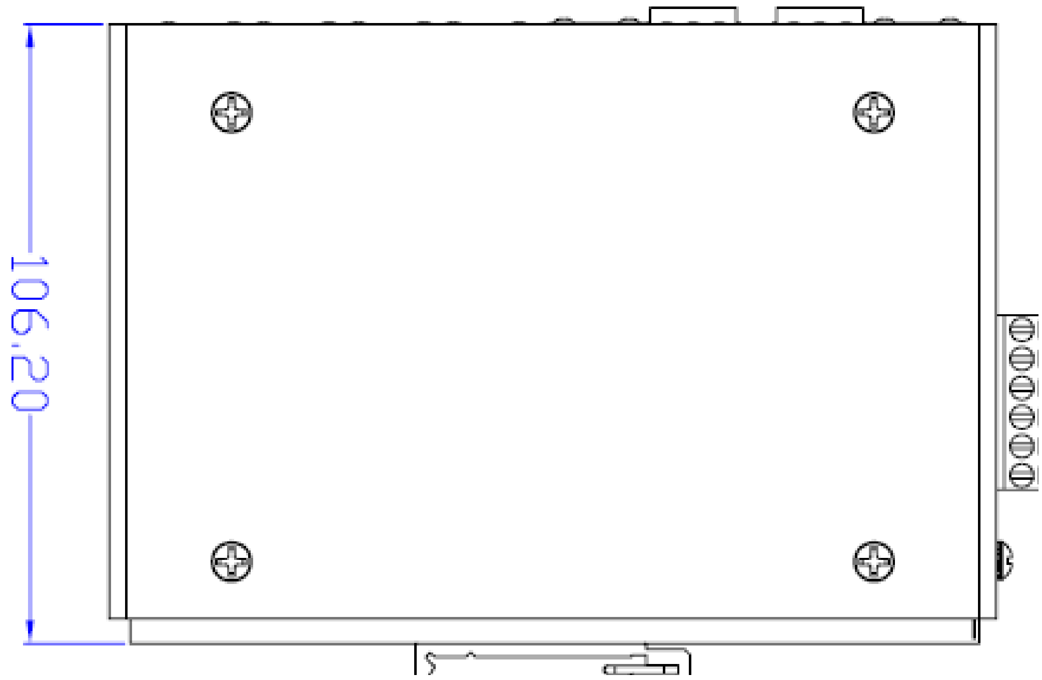
Power consumption and heat

Power Consumption Test	Power spec: DC input 12~48V, Redundant power with polarity reverse protection					
	DC Input		DC 12V	DC 24V	DC 36V	DC 48V
	Unloaded	A	0.341	0.184	0.128	0.098
		W	4.092	4.416	4.608	4.704
	Full Load	A	0.792	0.367	0.253	0.168
		W	9.504	8.808	9.108	8.064

APPENDIX B

PHYSICAL CHARACTERISTICS





Installation

DIN Rail and Wall Mounting

Housing – IP30