Case Communications

IGE 4T4GB-MX

Industrial Ethernet Switch

User Manual

V3.0 October 2012

FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. 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:

- Reorient 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

This 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

Overview

Introduction

The Case Communications IGE 4T4GB-MX is an Industrial Ethernet Switch with redundant network protocol called X-Ring+ which provides resilient ring technology re-routing from a network failure in under 10 ms, and supports up to 250 switches in each ring.

The IGE-4T4GB-MX comes equipped with 4 Mini GBIC sockets which can be used for Short Form Pluggable Modules known as SFP's, typically these will be Gigabit fibre optic drivers.

Heavy Duty

Designed with metal housing, the IGE-4T4GB-MX complies with IP30 standards.

Dual Power Inputs

The IGE-4T4GB-MX is equipped with dual DC power inputs which provide additional resilience. With both the power inputs supplied, if either one fails the other one will be activated to keeps the system operating continually. If one of the power inputs fails, the P-Fail LED indicator lights up and send an alarm through the relay output for notification purposes.

Flexible Mounting

The IGE-4T4GB-MX can be mounted on the wall or a standard DIN rail.

Wide Operating Temperature

The IGE-4T4GB-MX operating temperature is between -40 and +75^{o}C allowing it operate in some of the harshest conditions.

Easy Troubleshooting

LED indicators on the front of the IGE-4T4GB-MX make troubleshooting quick and easy. Users can identify status of the switch by observing the LED indicators with the definition table.

Features

- 16Gbps back-plane (switching fabric)
- 4 x 100/1000Base-FX dual mode SFP
- DMI – Dynamic Management Interface, monitoring the fibre interface.
- Wide-range redundant power
- IPv4 and IPv6
- X-Ring+ path redundant supported
- TFTP firmware update and system configuration restoration/backup

Technical Specifications

Communications

Standards	IEEE 802.3, 802.3u, 802.3x, 802.3ad, 802.3ab, 802.3z IEEE 802.1ab, 802.1d, 802.1p, 802.1Q, 802.1w, 802.1x
LAN	10/100/1000BaseT, 100/1000BaseFX
Transmission Speed	Up to 1000 Mbps
Packet Buffer	1Mbits
MAC Address Table	8K-entry

Interface

Ethernet	4 x RJ-45 (10/100/1000T) 4 x SFP/mini-GBIC (100/1000FX)
Console	1 x RJ-45 (RS-232)
Power & Relay Alarm	1 x 6-plug terminal block
LED Indicators	System: Power1, Power2, P-Fail, R-Master 10/100/1000BaseT: Link/Active, Speed SFP: Link/Activity

Management

Configuration	Web browser, serial console, SNMP v1/v2c/v3, Telnet, TFTP, IPv6, SNTP
SNMP MIB	RFC 1215 Trap, RFC1213 MIBII, RFC 1157 SNMP MIB, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC1643 , RFC 1757, RSTP MIB, LLDP MIB, Private MIB
VLAN	IEEE 802.1Q tagged, GVRP
Redundancy	802.1w/d RSTP/STP X-Ring+ (Recovery time < 10ms)
Security	SSL, DHCP Server with Port-IP binding, IP access security, user authentication, IP access security, user authentication, 802.1X port access control
Traffic Control	Port trunking with LACP, rate limit and storm control, IGMP Snooping/Query for multicast group, multicast filtering, IEEE 802.3x flow control, IEEE 802.1p QoS
Diagnostics	Port mirroring, real-time traffic statistics, MAC address table, system event log, E-mail alert, SNMP trap, RMON, LLDP, DMI for SFP

Power

Power Consumption	11.2 watts @V_{DC} (max.)
Power Input	12 ~ 48 V_{DC}; 18 ~ 30 V_{AC}

Mechanism

Dimensions (WxHxD)	59.6 x 152 x 105 mm
Enclosure	IP30 protection, aluminum shell
Installation	Wall/DIN-rail mounting

Environment

Operating Temperature	-40 ~ 75°C (-40 ~ 167°F)
Operating Humidity	5% ~ 95% (non-condensing)
Storage Temperature	-40 ~ 85°C (-40 ~ 185°F)
Storage Humidity	5% ~ 95% (non-condensing)

Certifications

Safety	UL508 (suitable for use in Class I, Division 2, Groups A, B, C, and D locations)
EMC	CE, FCC Class A CE EN61000-6-2 CE EN61000-6-4 CE EN61000-4-2 (ESD) CE EN61000-4-3 (RS) CE EN61000-4-4 (EFT) CE EN61000-4-5 (Surge) CE EN61000-4-6 (CS) CE EN61000-4-8 (Magnetic Field) CE EN61000-4-11 (Voltage Dip)
Free Fall	IEC60068-2-32
Shock	IEC60068-2-27
Vibration	IEC60068-2-6

Packing List

- 1 x Managed IGE-4T4GB-MXIndustrial Ethernet Switch
- 1 x RJ-45 to D-sub 9 female console cable
- 1 x User Manual (CD-ROM)
- 1 x Wall-mount kit

Check the contents of the IGE-4T4GB-MX carton with the standard checklist above. If any item is damaged or missing, please contact your local Case Communications reseller for service.

Alternately please e. mail Case Communications at support@casecomms.com

Or enquire via the Case Communications web site www.casecomms.com

Safety Precaution

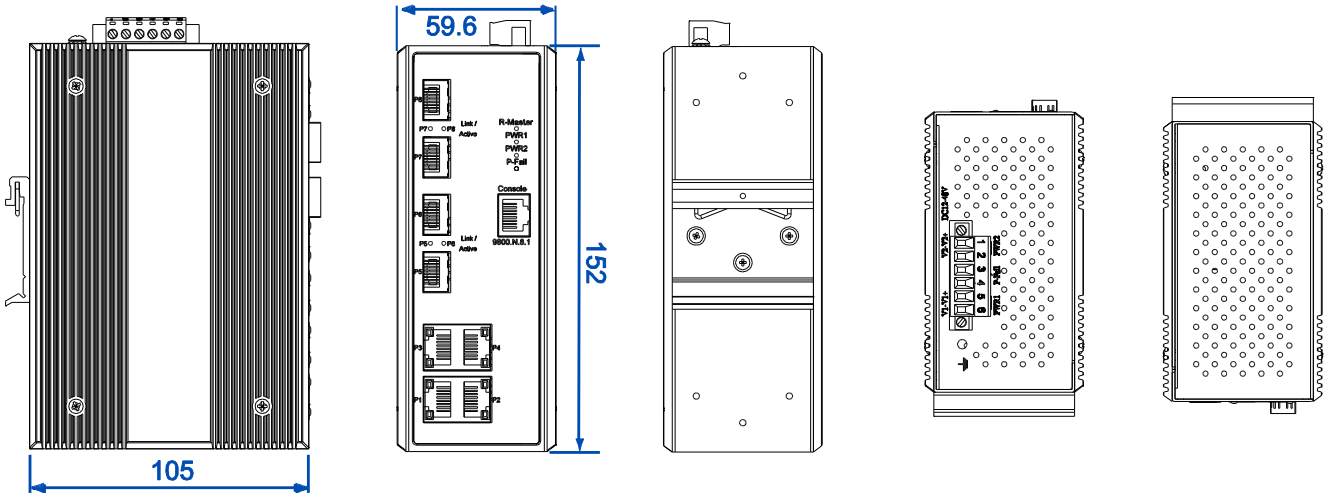
Attention *If DC voltage is supplied by an external circuit, please use a protection device on the power supply input.*
Please ground the switch using the earthing point on the switch.

Hardware Description

This section details the Case Communications IGE 4T4GB-MX Industrial Ethernet hardware specification, port, cabling and wiring information.

Physical Dimensions

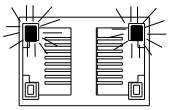
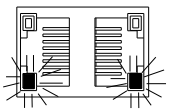
The figure below illustrates the dimensions 59.6mm x 152mm x 105mm (W x H x D) for the Managed IGE-4T4GB-MX.



Mechanical Dimensions

LED Indicators

LED indicators located on the front panel display the power status and network status of the IGE-4T4GB-MX Ethernet switch. Please refer to the following table for further details.

LED	Color	Description	
R-Master	Green	On	The switch is the master device of the X-ring group
		Off	Non-master device
PWR1	Green	On	Power input 1 is active
		Off	Power input 1 is inactive
PWR2	Green	On	Power input 2 is active
		Off	Power input 2 is inactive
P-Fail (depends on the **Fault Relay Alarm** configuration)	Red	On	Power or Ethernet port linking failure occurs
		Off	No failure occurs
P1 ~ P4 (10/100/1000T)	Green 	On	Connected to network
		Blinks	Data is transmitting or receiving
		Off	Not connected to network
	Green 	On	1000M
		Off	Disconnected or 10/100M
P5 ~ P8 (100/1000 SFP)	Green	On	Connected to network
		Blinks	Data is transmitting or receiving
		Off	Not connected to network

Definition of LED indicators

Installation

RJ-45 Cabling

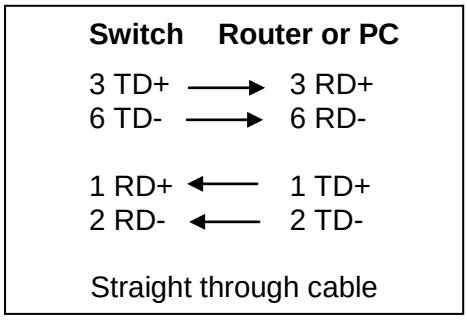
Use a four twisted-pair, Category 5e or higher spec cable for RJ-45 port connection. The cable between the switch and the link partner (switch, hub, workstation, etc.) must be less than 100 meters (328 ft.) long. The RJ-45 copper ports will auto-sense for 10Base-T, 100Base-TX, or 1000Base-T connections. Auto MDI/MDIX means that the switch can connect to another switch or workstation without changing straight through or crossover cabling.

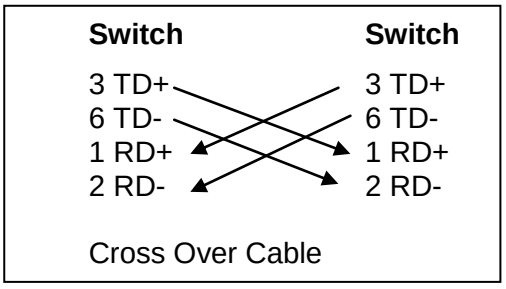
■ 10/100Base-TX Pinouts

Pin Number	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-)

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

■ 10/100Base-TX Cable Schematic





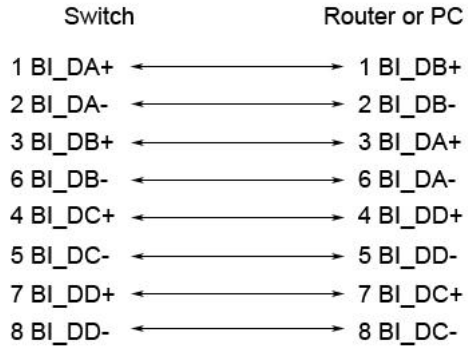
■ 10/100/1000Base-T Pinouts

The table below describes the gigabit Ethernet RJ-45 pin outs.

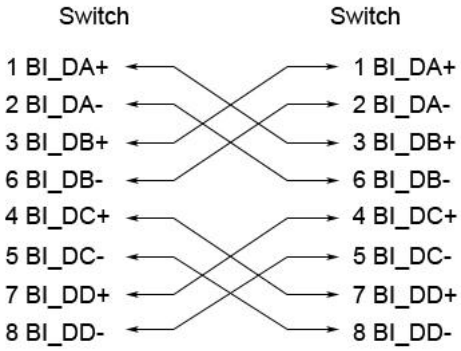
Pin	Signal name	Description
1	BI_DA+	Bi-directional pair A+
2	BI_DA-	Bi-directional pair A-
3	BI_DB+	Bi-directional pair B+
4	BI_DC+	Bi-directional pair C+
5	BI_DC-	Bi-directional pair C-
6	BI_DB-	Bi-directional pair B-
7	BI_DD+	Bi-directional pair D+
8	BI_DD-	Bi-directional pair D-

■ 10/100/1000Base-T Cable Schematic

The following two figures illustrate the 10/100/1000Base-T cable schematic.



Straight Through Cable Schematic



Crossover Cable Schematic

SFP Cabling

SFP Connection

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

First, insert the transceiver into the SFP slot. Notice that the triangle mark indicates the bottom of the slot.

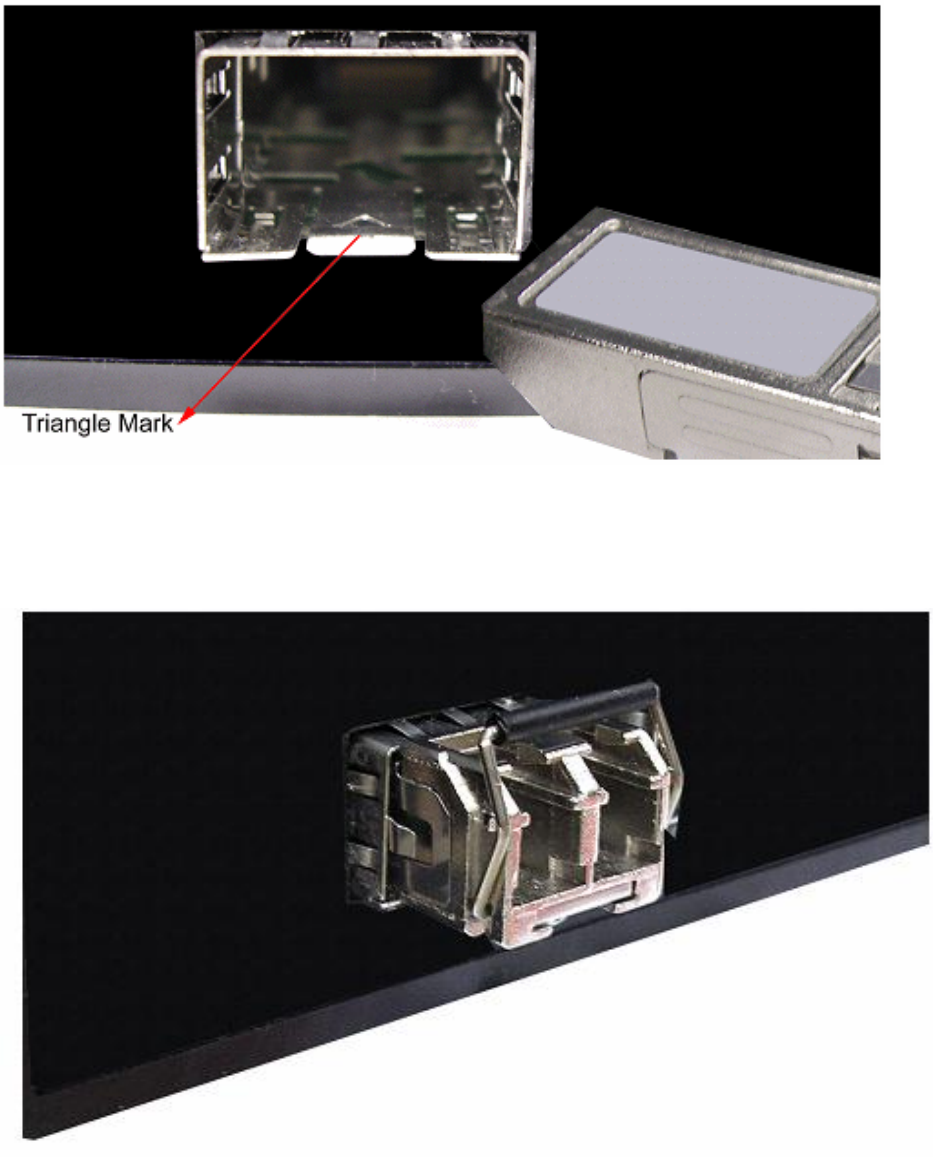
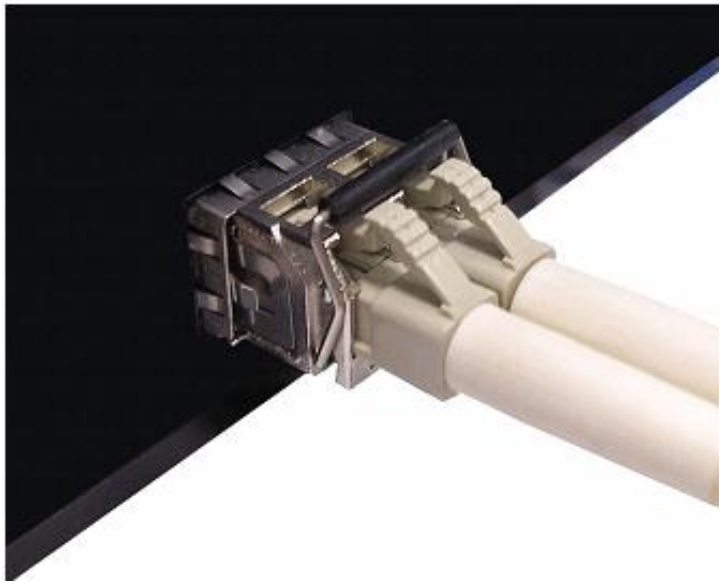


Figure - Insert transceiver into the SFP slot

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

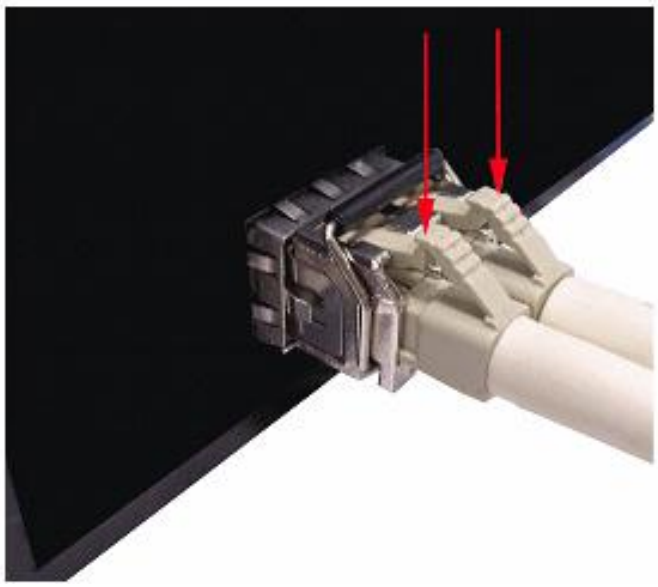


LC cable connector to the transceiver

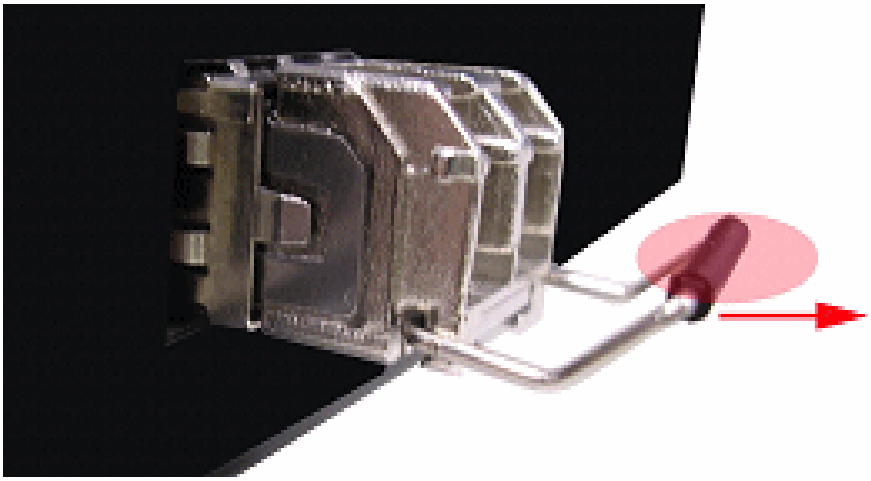
SFP Disconnection

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

First, press down the latches and pull the LC cable out of the SFP



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



Pull the transceiver out of the slot

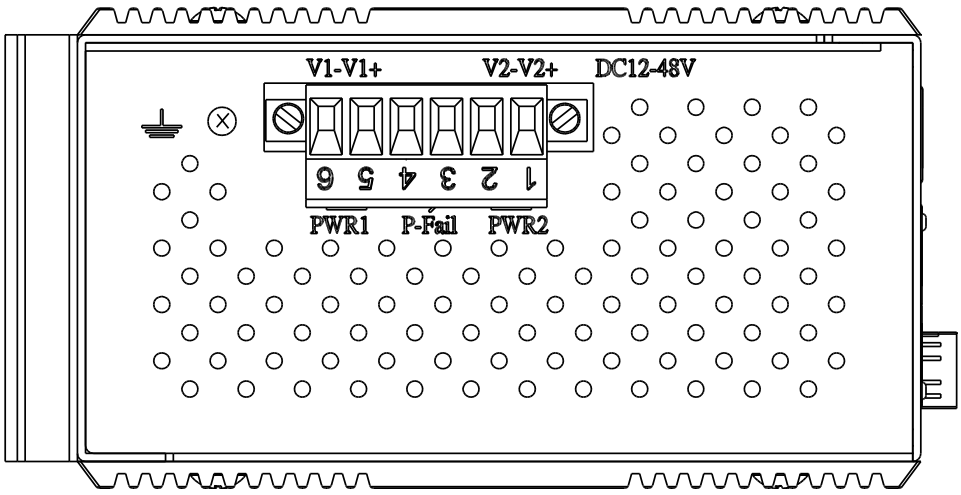
Grounding the IGE-4T4GB-MX

Follow the instructions below to connect the IGE 4T4GB MX to ground.

ATTENTION

When installing the IGE-4T4GB-MX, the ground connection must always be made first and disconnected last.

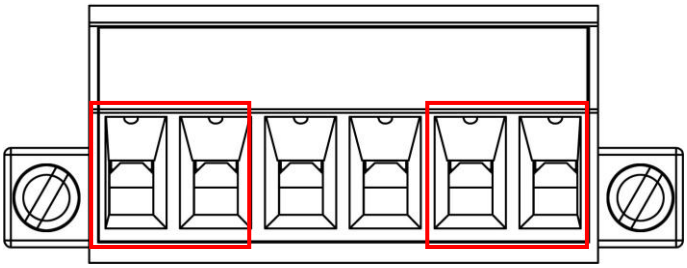
1. On the top of the IGE 4T4GB MX, locate and remove the dome screw which has a ground symbol beside it.
2. Attach the ground wire to the screw hole with the dome screw.



Wiring the Power Inputs

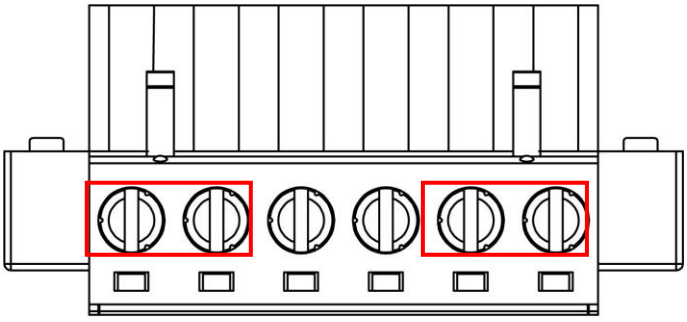
Please follow the steps below to wire power lines from the terminal block to the compliant external DC power source.

1. Before wiring, make sure the power source is disconnected.
2. Using the wire-stripping tool, strip a short piece of insulation from the output wires of the DC power source.
3. Identify the positive and negative feed positions for the terminal block connection. See the symbols printed on the panel indicating the polarities and DC input power range in voltage.



Plugs for Power 1 & Power 2

4. Insert the exposed wires into the terminal block plugs. Only wires with insulation should extend from the terminal block plugs. Note that the polarities between the wires and the terminal block plugs must be positive to positive and negative to negative.
5. Use a slotted screwdriver to tighten the captive screws.



Captive Screws for Fixing Wires

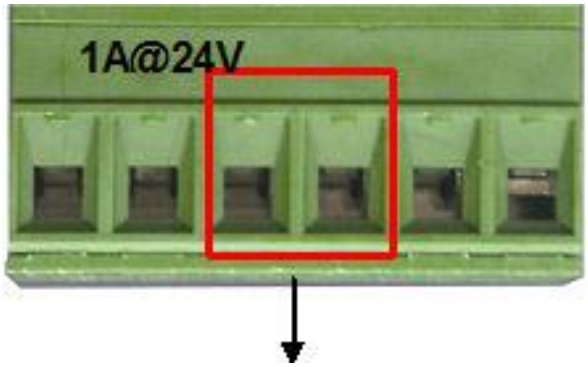
ATTENTION

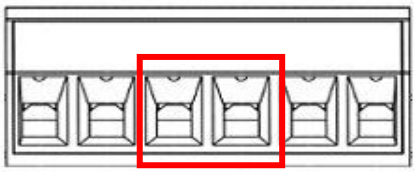
- *Use Copper Conductors Only, **60/75℃**, tightening to **5 lb-in***
- *The wire gauge for the terminal block should be in the range between **12~ 24 AWG**.*

Wiring the P-Fail Alarm Contacts

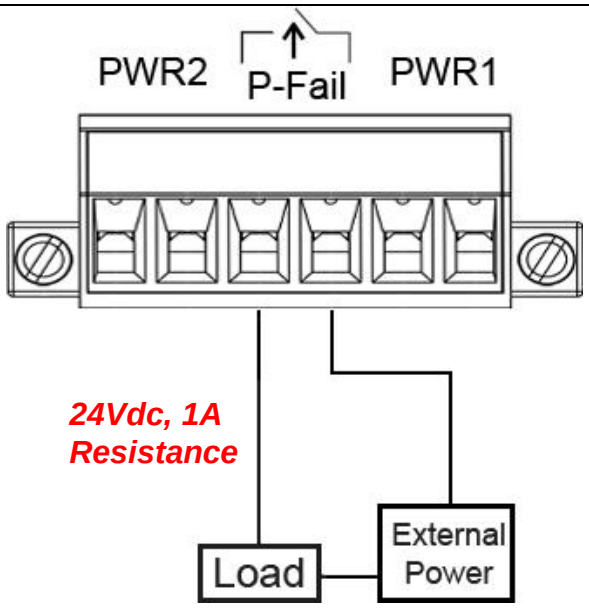
The “P-Fail” alarm relay is provided to signal critical error conditions that may occur on the switch. The contacts are energized upon powering up of the switch and remain energized until a critical error occurs including power failure and Ethernet port disconnection. The wiring diagram below shows the relay status under normal conditions forming a closed circuit. In the event of a critical failure the connection is broken.

Note. Normal conditions relay closed, fault condition relay opens.





Terminal Block Plugs for Fault Alarm Contacts



Fault Alarm Wiring Example

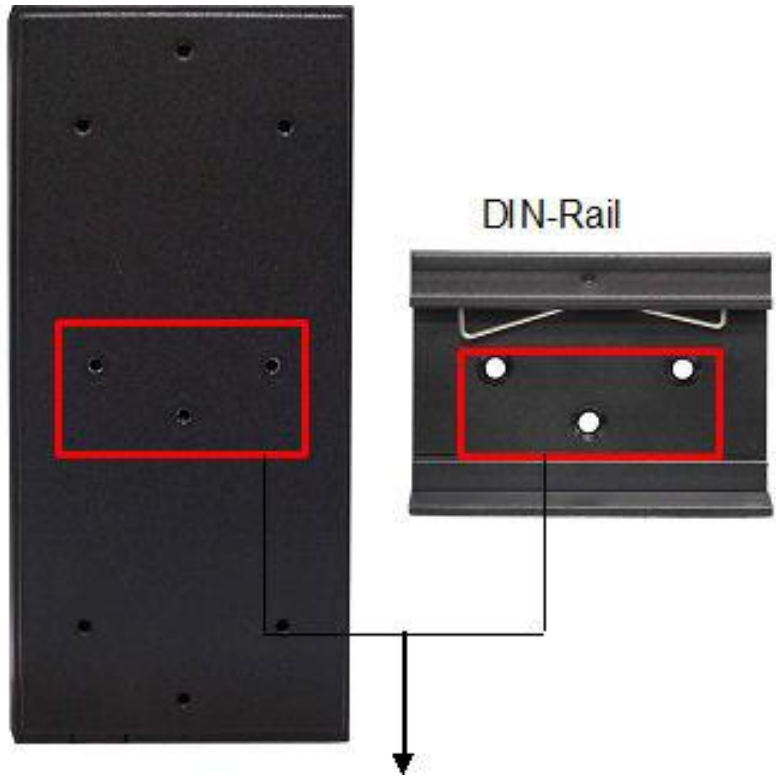
DIN-Rail Mounting

Assembling the DIN-Rail Clip

The DIN-rail clip should already be fitted on the IGE-4T4GB-MX when delivered from the factory. If this is not fitted, please refer to the following steps to secure the DIN-rail clip on the switch.

1. Use the screws included to secure the DIN-rail clip on the IGE-4T4GB-MX.
2. To remove the DIN-rail clip, reverse step 1.

Rear Side of the Switch



1. Use the screws to screw the DIN-Rail on the industrial switch

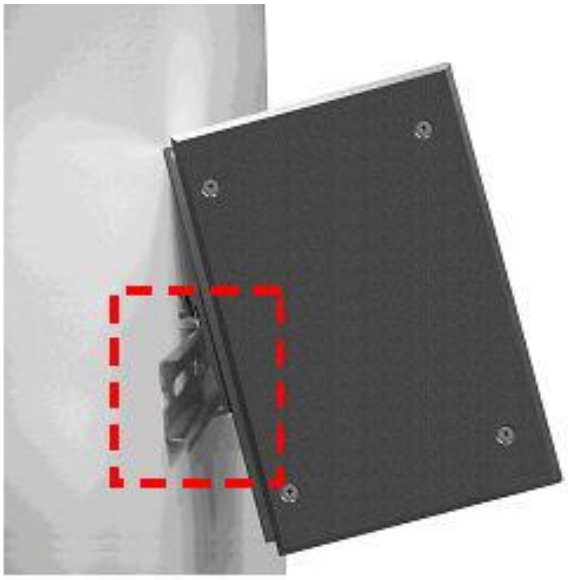
2. To remove the DIN-Rail, reverse the step 1.

.

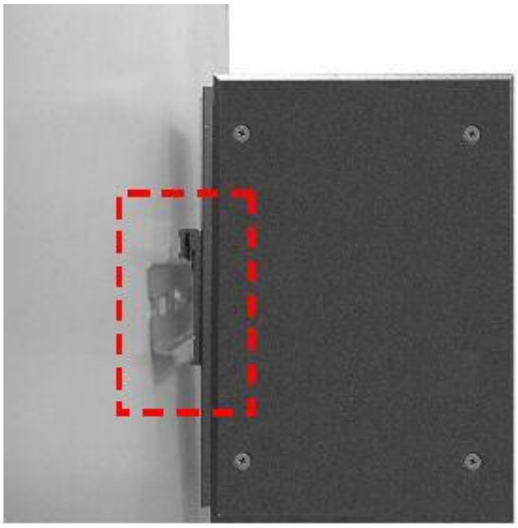
Hanging the IGE-4T4GB-MX

Follow the steps below to install the IGE-4T4GB-MX on a DIN rail.

1. First, position the rear side of the switch directly in front of the DIN rail. Make sure the top of the clip hooks over the top of the DIN rail.



2. Push the unit downward.



3. Check the DIN-Rail clip is tightly fixed on the DIN rail.

4. To remove the IGE-4T4GB-MX from the track, reverse the steps above.

Wall Mounting

To hang the Ethernet switch on the wall, please follow the steps below.

1. Remove the DIN-rail clip.
2. Prepare the two wall-mount plates and six screws included.
3. Align the screw holes between the wall-mount plates and the unit as the figure illustrated.
4. Secure the plates to the unit with the accompanying screws.

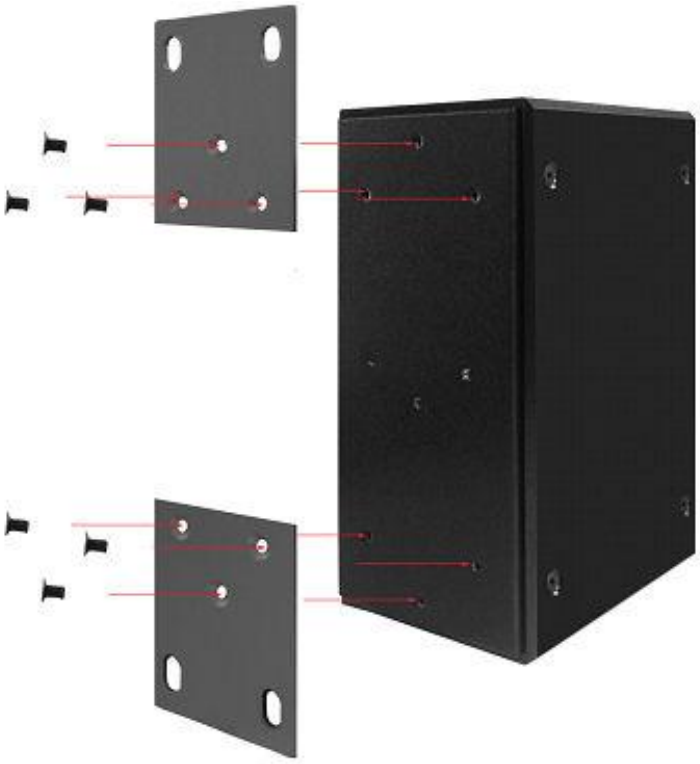


Diagram – Wall Mounting the IGE-4T4GB-MX

Installation Steps

1. Unpack the IGE-4T4GB-MX.
2. To install the IGE-4T4GB-MX on a wall, please refer to the **Wall Mounting** section.
3. Ground the IGE-4T4GB-MX.
4. To power on the IGE-4T4GB-MX, please refer to the **Wiring the Power Inputs** section for further information on how to wire the power. And then the power LED on the IGE-4T4GB-MX will light up. Please refer to the **LED Indicators** section for indication of LED lights.
5. Prepare the appropriate cables for Ethernet connection.
6. The Ethernet port LED on the IGE-4T4GB-MX 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 set and LED lights all show in normal, the installation is complete.

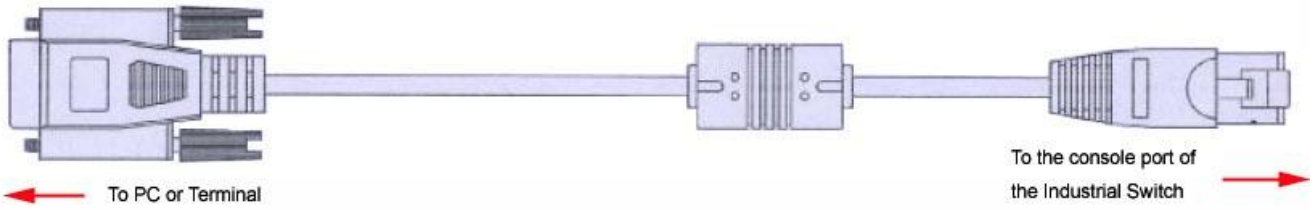
Note ***This equipment is intended for use in a Pollution Degree 2 industrial environment.***

Configuration

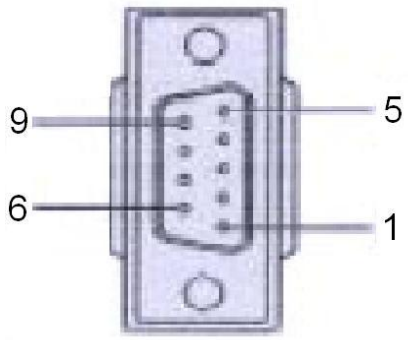
The IGE-4T4GB-MX can be configured via RS-232 Console, or a web browser.

RS-232 Console

Attach the supplied configuration cable. One end has a 9 way D-Type connector which connects to you PC serial port and the other end is RJ-45, which connects to the IGE-4T4GB-MX. Your PC or terminal must support a terminal emulation program such as Terra Term or Hyper-Term.



Pin Assignments



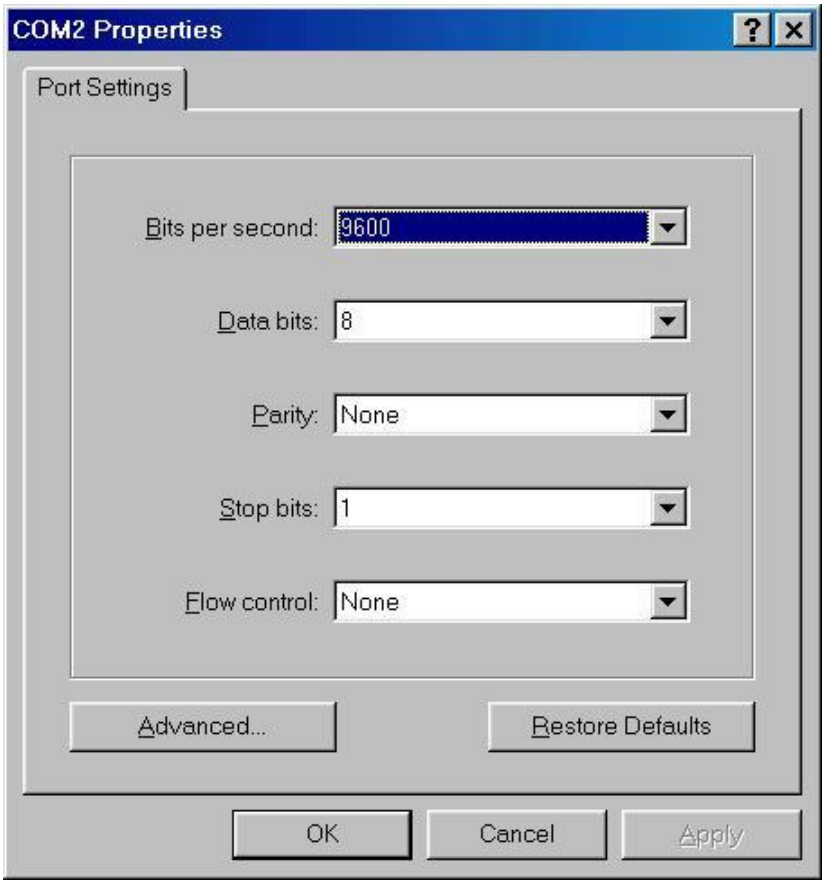
DB 9-pin Female

D-sub 9 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

After the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program like **Hyper Terminal** and configure its **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

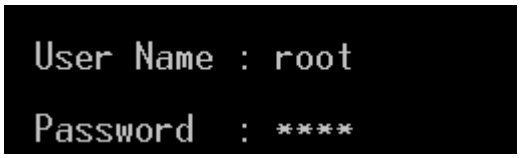


The settings of communication parameters

Having finished the parameter settings, click '**OK**'. When the blank screen shows up, press **Enter** to have the login prompt appear.

- Key in '**root**' (default value) for the User Name
- Key in '**case'** (default value) for the Password (press **Enter** to switch between);

Then press **Enter** to display the Main Menu.. Please see the figure below.



Console login interface

The system supports a CLI command console management. After you log in on to the system, you will see a command prompt. To enter CLI management interface, type in "**enable**" command.

CLI command interface

For further details of the CLI commands, please refer to ***Appendix A Command Sets***.

Web-Based Management

This IGE-4T4GB-MX provides an easy way to configure the switch via a web browser. You can follow the steps below to access the equipment.

Note *Your host PC should be in the same VLAN setting with the IGE-4T4GB-MX, or the management will not be configured.*

Connect the IGE-4T4GB-MX to the Ethernet port on your host PC to allow configuration via Ethernet and a browser. You can use either a straight-through or cross over Ethernet cable. Before using the web management, connect the switch to the network and make sure that any one of the PCs on the network can connect to the switch through their web browser. The default IP Address, subnet mask and username and password of the IGE-4T4GB-MX are as below.

- IP Address: **192.168.16.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.16.254**
- User Name: **root**
- Password: **case**

[NOTE] Don't set "0" for the first segment of the subnet mask and default gateway (000.xxx.xxx.xxx).
Refresh the web screen if the web interface is not displayed after changing the setting.

1. Launch your browser (e.g. Internet Explorer, Firefox etc.) on your PC.
2. Type the IP address of the switch in the URL field, and then Press "**Enter**".

3. With the login dialog box showing up, type the user name and password in the respective fields. The default user name is **'root'** and password is **'case'**

4. Press **Enter** or click the **OK** button, and then the home screen of the Web-based management system appears. You can change user name/password in the ***User Authentication*** section.

In the event that the default IP Address has been changed, it maybe necessary to logon via the Console port and set the IP address the commands for this are;

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)

SSL

The Case Communications IGE-4T4GB-MX also provides an option for you to connect with your browser via HTTP over SSL, (called HTTPS). The SSL (Secure Socket Layer) protocol allows users to make a secured session between the browser (client) and the Ethernet switch (server). You can then type the prefix "***https://***" followed by the IP address of the Ethernet switch in the URL of the browser. Beside the URL a padlock icon shows up indicating that client is successfully connecting to server via HTTPS.

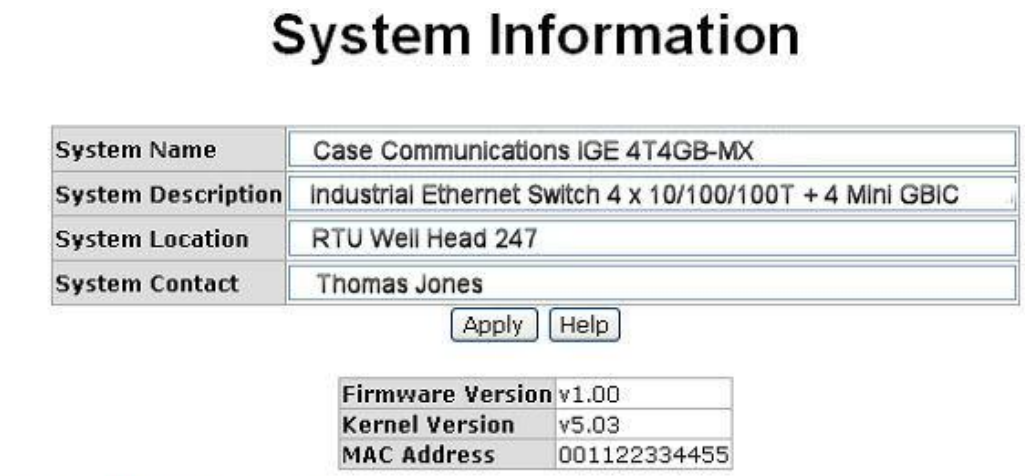
On the main menu page, you can find the tree menu structure of the IGE-4T4GB-MX.

To expand the folder option and display more configuration options the click the "+" symbol on the left of the screen to open the hyperlink. Click any one of the hyperlinks to open its function page.

System Information

This page allows you to view the system information, assign the system name and location to make this IGE-4T4GB-MX switch more easily identified on your network.

- **System Name:** Assign a name for this switch. The maximum length is 64 bytes.
- **System Description:** A read-only field displaying the description for the switch.
- **System Location:** Assign the switch physical location. The maximum length is 64 bytes.
- **System Contact:** Enter the name of contact person or department.
- **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).
- Click Apply to have the configuration take effect.



System Information interface

System Information interface

IP Configuration

Due to the shortage of IPv4 IP Addresses, the IGE-4T4GB-MX is designed to be configured by PC's running either IPv4 or IPv6.

IPv4

The IPv4 tab allows users to configure the switch to receive an IP address from DHCP server or manually fill in **IP Address**, **Subnet Mask**, **Gateway**, IP addresses of the primary and the secondary DNS servers.

- **DHCP Client**: Enable or disable the DHCP client function. When the **DHCP Client** function is enabled, the IGE-4T4GB-MX will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address on DHCP server. After users click Apply, a popup dialog shows up. It is to inform the user that when the DHCP client is enabled, the current IP will lose and the user should find the new IP on the DHCP server

- **IP Address:** Assign the IP address for the industrial switch. With the **DHCP Client** function enabled, the switch is configured as a DHCP client and users doesn't need to assign the IP address that is assigned by the DHCP server. The default IP is 192.168.16.1 or the user has to assign an IP address manually when DHCP Client is disabled.

- **Subnet Mask:** Assign the subnet mask to the IP address. If the **DHCP Client** function is disabled, the user has to assign the subnet mask manually.

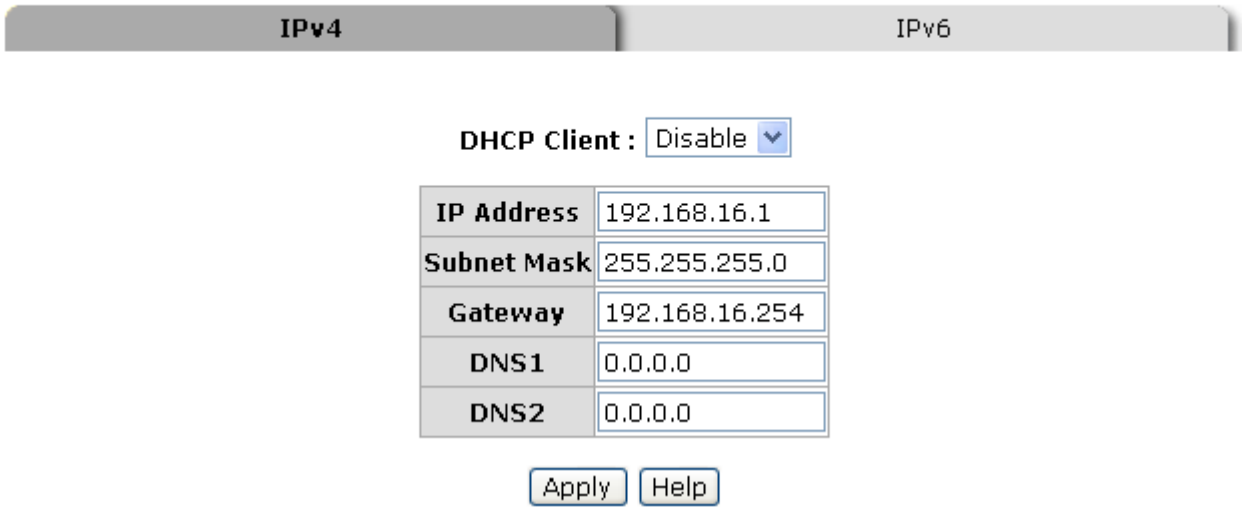
- **Gateway:** Assign the network gateway for the switch. If the **DHCP Client** function is disabled, the user has to assign the gateway manually. The default gateway is 192.168.16.254.

- **DNS1:** The abbreviation of Domain Name Server—an Internet service that translates domain names into IP addresses. The domain name is in alphabetic order, which is easy to be remembered. The Internet is based on IP address. Therefore, every time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.net.com might translate to 192.168.16.1.

- **DNS2:** The backup for DNS1. When DNS1 cannot function, DNS2 will then replace DNS1

- When finished, click Apply to have the configuration take effect.

IP Configuration



IP configuration—IPv4

IPv6

The IPv6 tab mainly features two fields displaying the Ethernet switch's **Global Unicast Address** and **Link-Local Address**.

Global Unicast Address: A display-only field. When this Ethernet switch is connected to a network segment where one or more routers connected, the Ethernet switch will be assigned an address known as Global Unicast Address by the router(s). Being assigned the Global Unicast Address, the Ethernet switch can then have access to different network segments.

Link-Local Address: A display-only field. Link-Local Address is for use during auto-configuration and when no routers are present. Being assigned the Link-Local Address, the Ethernet switch can have access to any hosts on the same local segment.

Neighbour Cache

IPv4	IPv6
Global Unicast Address	3FFE:501:FFFF:100:20f:3FFF:FE60:3321
Link-Local Address	FE80:20F:38FF:FE80:2221

IPv6 Address	Link Layer (MAC) Address State	
3FFE:501:FFFF:100:550F:F689:EOEC:5722	00-25-64-9D-1B-E6	Reachable
FE80::201:8OFF:FE63:D688	00.01.80.63.D6.B8	Stale

IP configuration—IPv6

DHCP Server

DHCP is Dynamic Host Configuration Protocol which is a protocol for assigning dynamic IP addresses to devices on a network.

With dynamic addressing, a device does not have a fixed IP address but can have a different IP address every time it connects to the network.

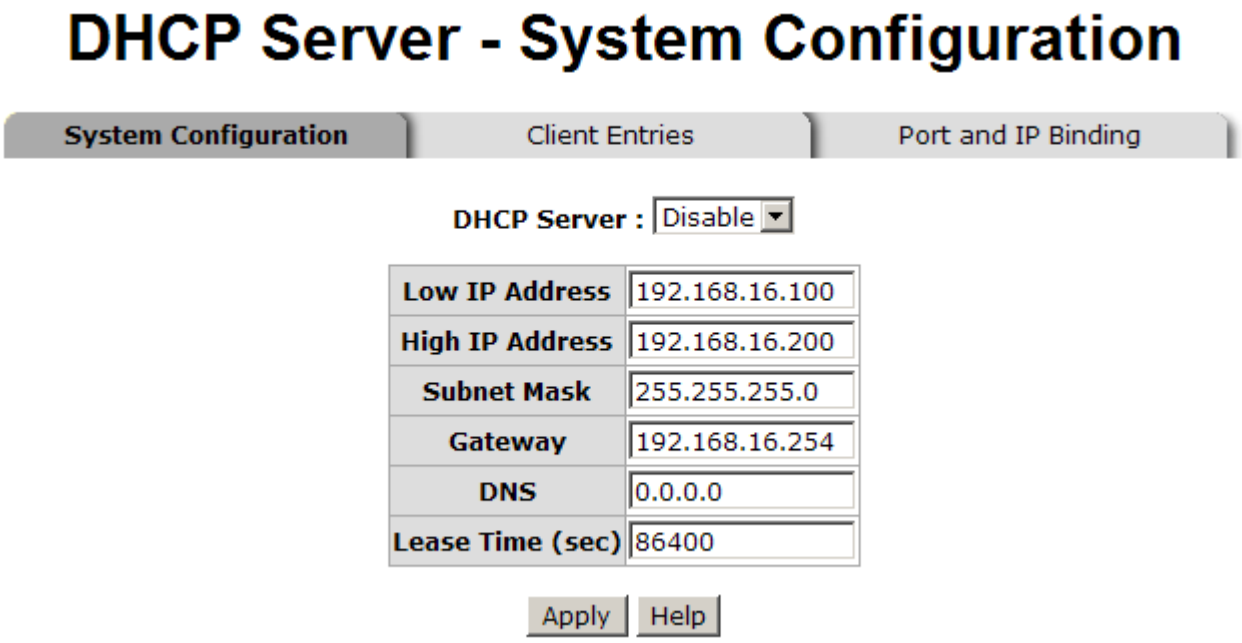
In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task.
This means that a new computer can be easily added to a network without the hassle of manually assigning it a unique IP address.

With the DHCP option enabled, the IGE-4T4GB-MX can be configured as a DHCP server and provide devices on its network to obtain their IP address from the switch.

System Configuration

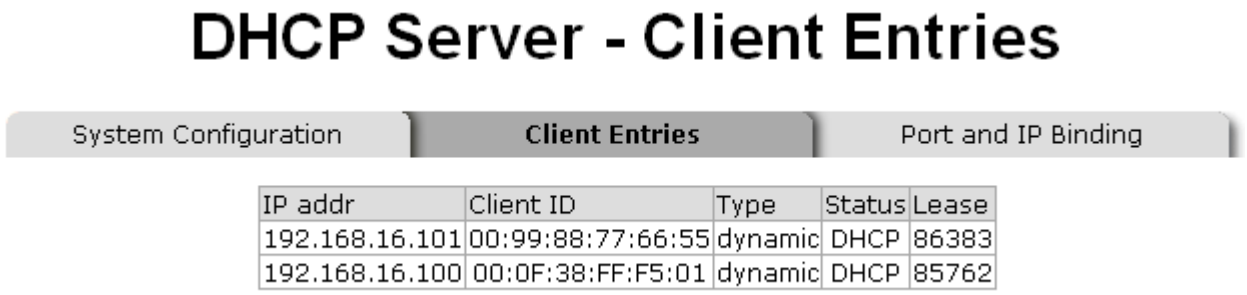
- **DHCP Server:** This pull-down menu allows you to configure the switch to be the DHCP server on your local network.
- **Low IP Address:** Type in an IP address as the first of a range of the dynamic IP address. As the figure shown below, 192.168.16.100 is the first IP address in the range.
- **High IP Address:** Type in an IP address which will be the highest address in the range of dynamic IP addresses. As the figure below, shows 192.168.16.200 is the highest IP address in the range.
- **Subnet Mask:** Type in the subnet mask of the IP configuration.
- **Gateway:** Type in the IP address of the gateway in your network.
- **DNS:** Type in the IP address of Domain Name Server in your network.
- **Lease Time (sec):** The length of time the dynamic IP addresses is assigned to the client's device.
- Click Apply to have the configuration take effect.



DHCP Server—System Configuration interface

Client Entries

When the **DHCP Server** function is enabled, the system will collect the DHCP client information including the assigned IP address, the MAC address of the client device, the IP assigning type, states and lease time. This menu option displays these parameters.



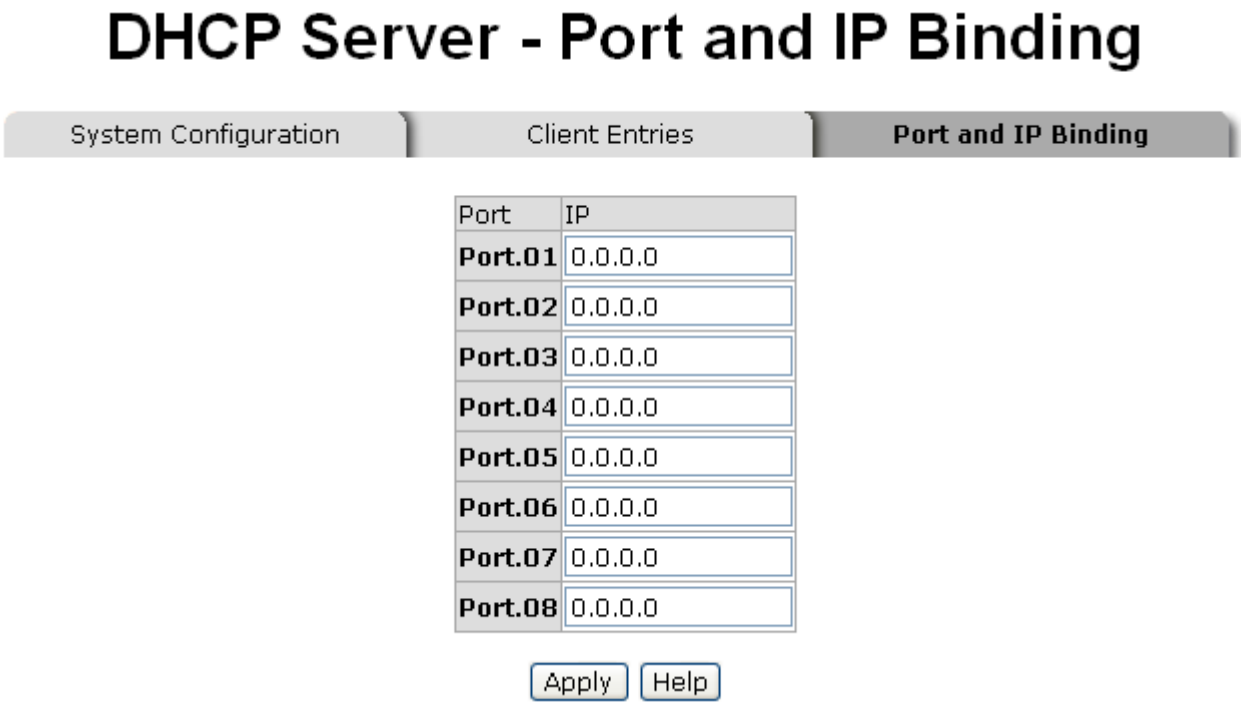
DHCP Client Entries interface

Port and IP Bindings

The figure below shows, that the IGE 4T4GB-MX switch will assign an IP address to its connected clients according to the Port-IP binding table.

The network manager may also configure each port with one particular IP address. When a device connects to its port on the IGE-4T4GB-MX then the switch assigns the device an IP Address that is displayed in the table.

IP assigning, the system will assign the IP address bound with the port to the device.



Port and IP Bindings interface

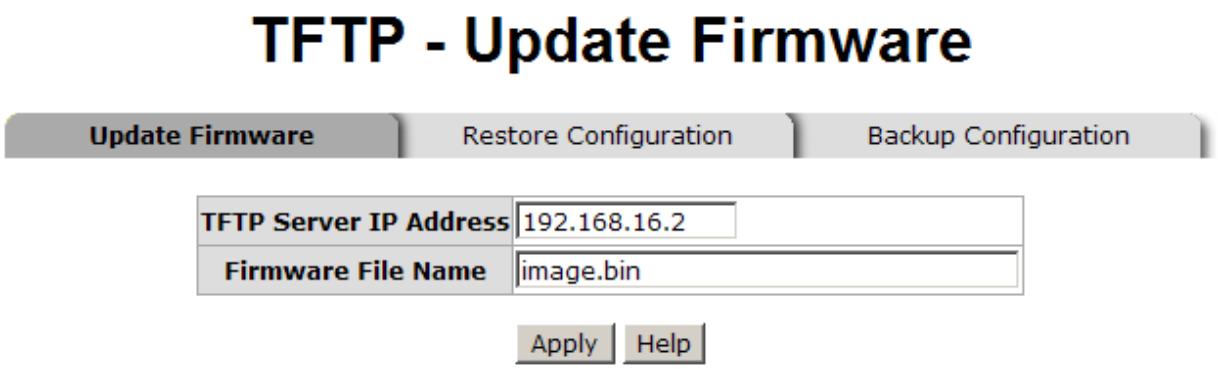
TFTP

TFTP (Trivial File Transfer Protocol) allows a network manager to update the IGE-4T4GB-MX firmware from a TFTP Server on the network.

Before updating your switches firmware ensure the TFTP server is ready and the firmware image is located on the TFTP Server.

Update Firmware

- **TFTP Server IP Address:** Type in the IP address of the networks TFTP server.
- **Firmware File Name:** Type in the name of the firmware image file to be updated.
- When finished, click Apply to start updating.

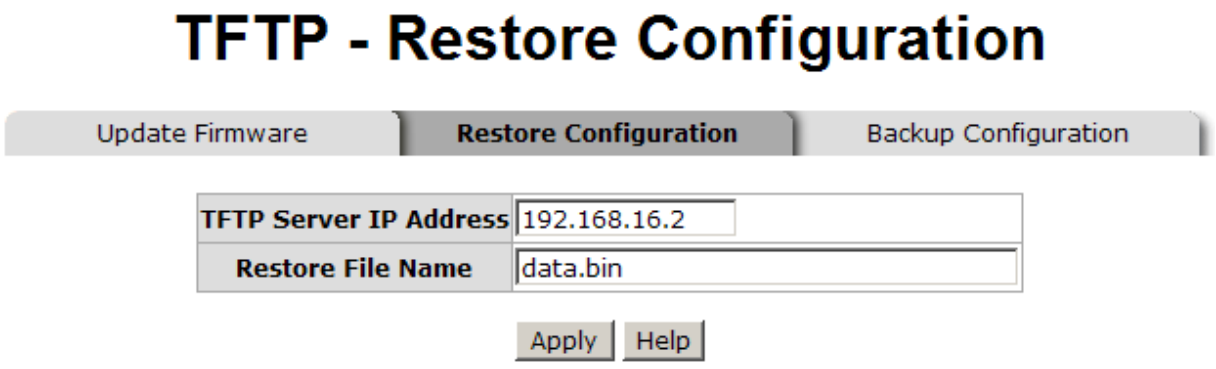


Updating the firmware interface

Restore Configuration

You can restore a previous backup configuration from the TFTP server to recover the settings. Before doing that, you must locate the image file on the TFTP server first for the switch to download back the flash image.

- **TFTP Server IP Address:** Type in the IP address of the TFTP server.
- **Restore File Name:** Type in the correct file name for restoring.
- When finished, click Apply to start configuration restoration.



Restoring the configuration interface

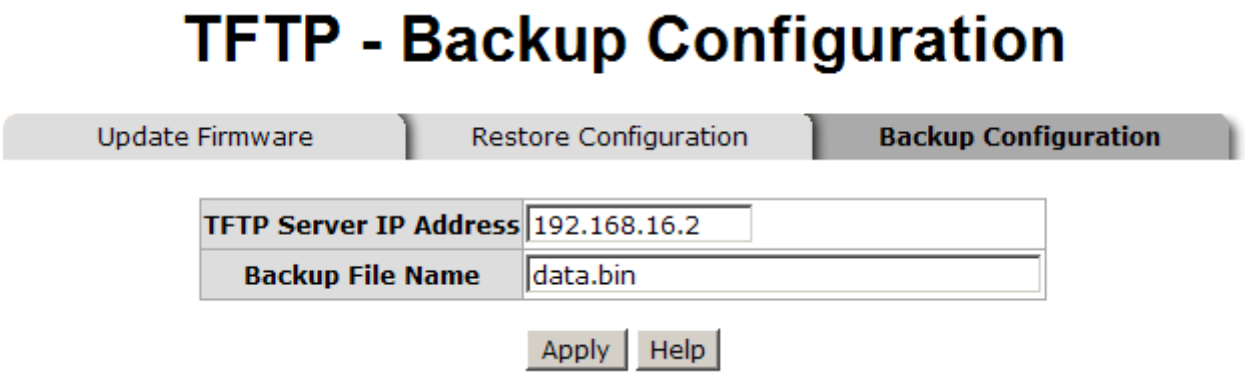
Backup Configuration

You can back up the current configuration from flash ROM (on the switch) to a TFTP server to allow the network manager to recover the configuration later. Therefore an engineer can install a switch in the field, configure its IP address and name and then download the rest of the configuration from the TFTP server.

Note for security reasons the following details will not be restored into the switch.

- IP Address
- Site description
- User Logon details

- **TFTP Server IP Address:** Type in the IP address of the TFTP server.
- **Backup File Name:** Type in the file name.
- When finished, click Apply to start backing up.



Backup Configuration interface

System Event Log

This page allows the user to decide whether to send the system event log, to a remote system log server or management system, and select the mode which the system event log will be sent to, these will be

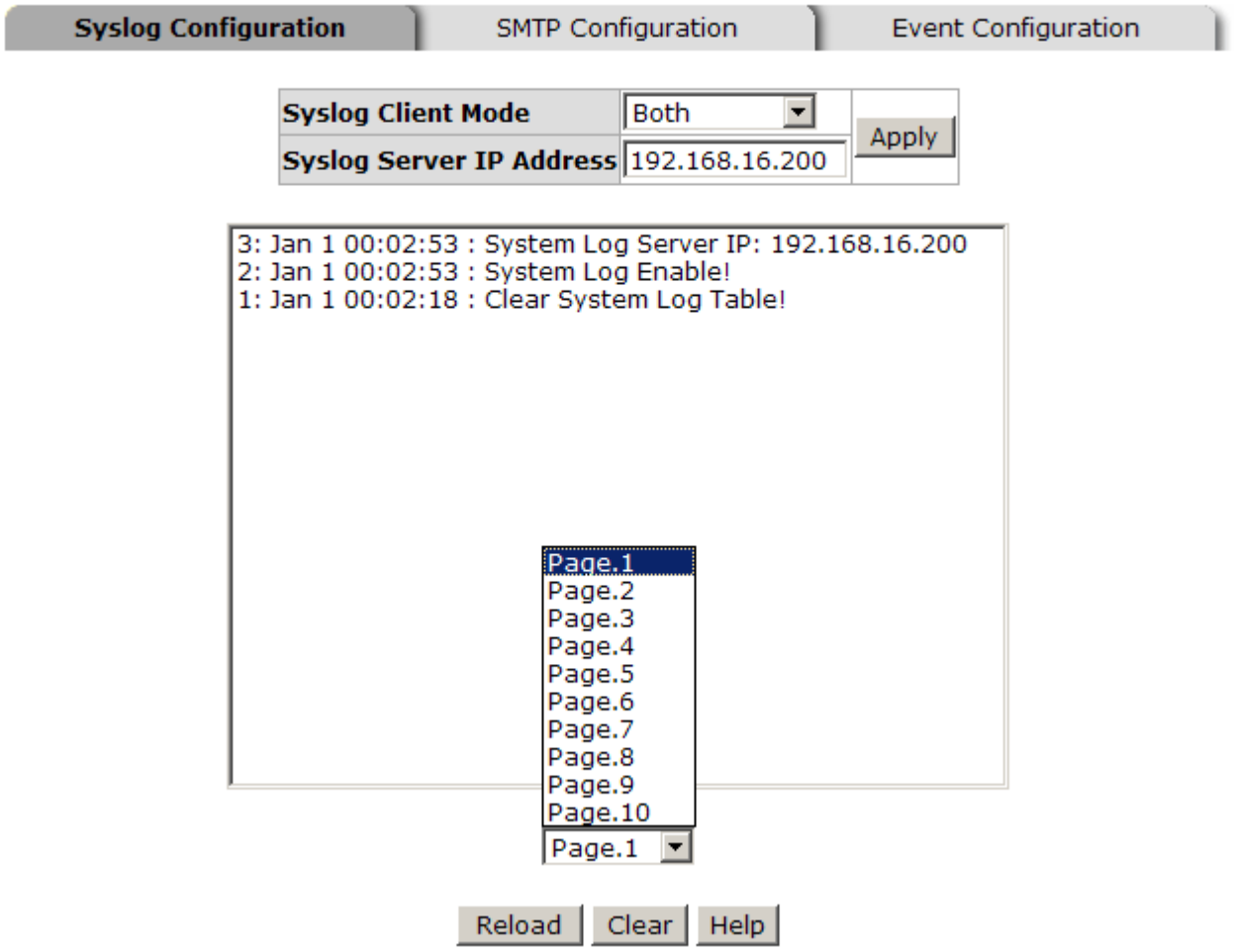
- Client only
- Server only,
- Both client and server.

What kind of event log will be issued to the client/server depends on the selection on the **Event Configuration** tab.

System Event Log—Syslog Configuration

- **Syslog Client Mode:** Select the system log mode—**Client Only**, **Server Only**, or **Both**. ‘Client Only’ means the system event log will only be sent to internal system log within the switch. ‘Server Only’ means the system log will only be sent to a remote system log server with a fixed IP address. If the parameter is set to ‘Both’, the system event log will be sent to the remote server and the internal system log.
- **Syslog Server IP Address:** When the ‘Syslog Mode’ item is set as Server Only/Both, the user is required to assign the system log server IP address where the log will be sent.
- Click Reload to refresh the event log displaying area.
- Click Clear to clear the page.
- Make sure the selected mode and IP address, if needed, is correct and click Apply to have the setting take effect.

System Event Log - Syslog Configuration



Syslog Configuration interface

System Event Log—SMTP Configuration

Simple Mail Transfer Protocol (SMTP) is a standard for email transmissions across the network. You can configure an SMTP server IP address, sender mail account, password, and the recipient email account to which the e-mail alert will send. Besides, this page provides the authentication mechanism including authentication steps through which the client effectively logs in to the SMTP server during the process of sending e-mail alert.

- **Email Alert:** With this function enabled, the user is allowed to configure the settings for sending an e-mail alert to the SMTP server when the events occur.
- **SMTP Server IP Address:** Assign your mail server IP address (this field will only be available when **Email Alert** is enabled).
- **Sender:** Type in an alias e-mail address for the switch for e.g. switch101@123.com, to identify where the e-mail alert comes from.
- **Authentication:** Tick the checkbox to enable the mail account, password and confirm password fields show up. Configure the email account and password for authentication procedures when this switch logs in to your SMTP server.
- **Mail Account:** Set up the email account, e.g. johnadmin, to receive the email alert. It must be an existing email account on the mail server.
- **Password:** Type in the password for the email account.
- **Confirm Password:** Reconfirm the password.
- **Rcpt e-mail Address 1 ~ 6:** You can also specify up to 6 e-mail accounts to receive the email alert.
- Click Apply to have the configuration take effect.

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 :	

Apply Help

SMTP Configuration interface

System Event Log—Event Configuration

The option fields and pull-down menus are not available unless the **Syslog Client Mode** on the Syslog Configuration tab and the **E-mail Alert** on the SMTP Configuration tab are enabled first.

This tab mainly controls whether an event notification is to be sent to the **Syslog**/**SMTP** server. The part of **System Event Selection** controls the event notification including Device Cold Start and Authentication Failure. With the **Syslog**/**SMTP** checkbox ticked, the event log/email alert will be sent to the system log server / SMTP server respectively. As for the part of **Port Event Selection**, port events (link up, link down, and both) can be sent to the system log server/SMTP server by setting the trigger condition for each port respectively.

- **System event selection:** There are two event types—*Device Cold Start* and *Authentication Failure*.
  - **Device Cold Start:** Select the Syslog/SMTP checkboxes respectively to have the system issue the event log/email alert to the system log / SMTP server when the device executes a cold start.
  - **Authentication Failure:** In the event an SNMP authentication fails, the system will issue the event log/email alert to the system log / SMTP server respectively.

- **Port event selection:** Each drop-down menu has four options—**Disable**, **Link UP**, **Link Down**, and **Link UP & Link Down**. Disable means no event will be sent to the system log/SMTP server.
  - **Link UP:** The system will issue a log message only when a ‘link-up’ event on this port occurs.
  - **Link Down:** The system will issue a log message only when a ‘link-down’ event on this port occurs.
  - **Link UP & Link Down:** The system will issue a log message when a port connection has suffered a link-up and link-down, event.

System Event Log - Event Configuration

Syslog Configuration | SMTP Configuration | **Event Configuration**

System event selection

Event Type	Syslog	SMTP
Device cold start	☑	☐
Authentication Failure	☐	☑

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

Disable
Link Up
Link Down
Link Up & Link Down

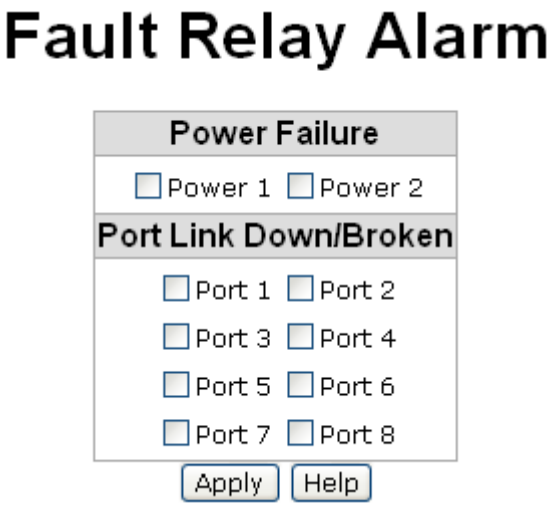
Apply Help

Event Configuration interface

Fault Relay Alarm

The Fault Relay Alarm function supports an external alarm indication when a Power Failure or Port Link Down/Broken are detected, in which instance the relay contacts are opened. Under normal power on conditions the relay ports are closed.
Selected the option to enable the relay alarm function. Please refer to the segment of '**Wiring the Fault Alarm Contacts**' for the external warning device installation.

- **Power Failure:** With this option selected the relay device inside the IGE-4T4GB-MXchanges its state (i.e. relay opens) and the **FAULT** LED indicator is on if a power failure occurs. (note unless you connect both DC Inputs don't select both PSU alarms, otherwise you will have a permanent alarm)
- **Port Link Down/Broken:** With this option selected the relay device inside the IGE-4T4GB-MXchanges its state (relay opens) and the **FAULT** LED indicator is on if the corresponding port's states become link down or broken.



Fault Relay Alarm interface

SNTP Configuration

SNTP (Simple Network Time Protocol) is a simplified version of NTP which is an Internet protocol used to synchronize the clocks of computers and network devices with an external time reference. Instead of each device in the network incrementing its own clock, this option allows all the devices to operate from a single central clock.

Therefore, the switch provides configuration options to access a national time server and time-synchronization its subnet and the local clock in each participating subnet peer.

Daylight Saving Time (DST) is the convention of advancing clocks so that afternoons have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

- **SNTP Client:** Enable/disable the SNTP function to get the time from the SNTP server.
- **Daylight Saving Time:** This function is used to enable/disable *Daylight Saving Period* and *Daylight Saving Offset* fields.
- **UTC Timezone:** Set the location time zone for the switch. The following table lists different location time zones for your reference.

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

MST - Mountain Standard 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

- **SNTP Sever URL:** Specify the SNTP server IP address. You can assign a local network time server IP address or an internet time server IP address.

- **Switch Timer:** When the switch has successfully connected to the SNTP server whose IP address was configured in the field of **SNTP Server URL**, the current server time is displayed in this field.

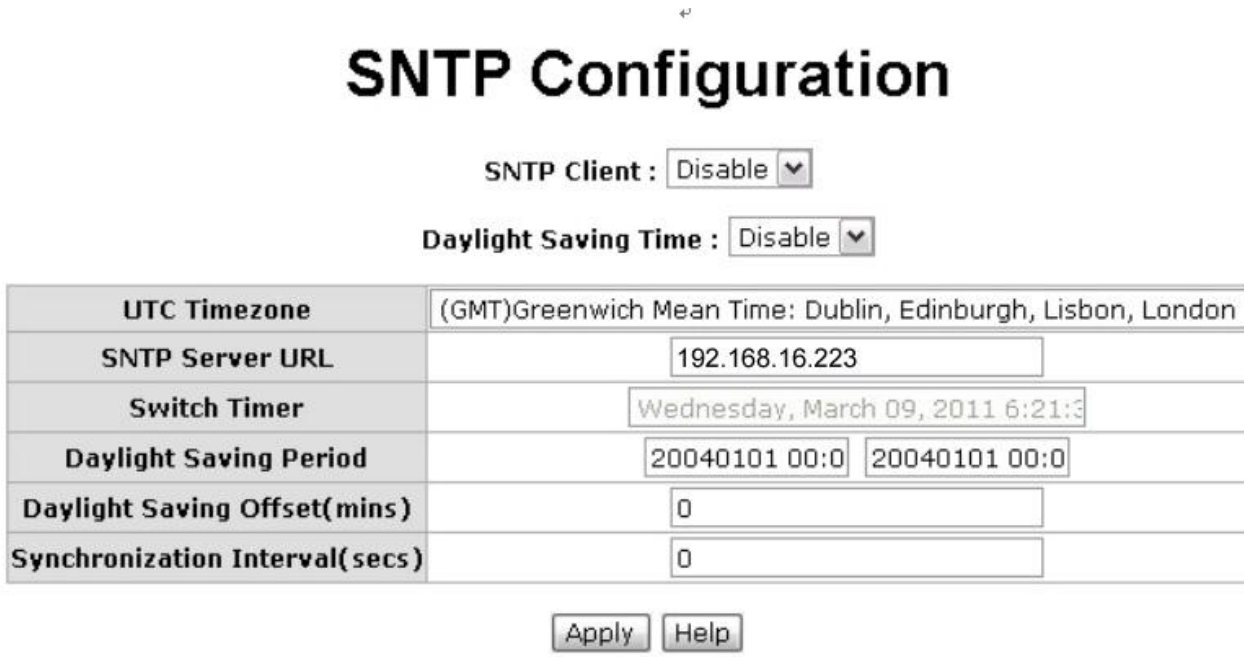
- **Daylight Saving Period:** Set up the start and end date/time of the daylight saving period. Please key in the value in the format of 'YYYYMMDD' and 'HH:MM' (leave a space between 'YYYYMMDD' and 'HH:MM').
  - **YYYYMMDD:** an eight-digit year/month/day specification.
  - **HH:MM:** a five-digit (including a colon mark) hour/minute specification.

  For example, enter '20070701 02:00' and '20071104 02:00' in the two fields respectively to represent that DST begins at 2:00 a.m. on March 11, 2007 and ends at 2:00 a.m. on November 4, 2007.

- **Daylight Saving Offset (mins):** For non-US and European countries, specify the amount of time for day light savings. Please key in the valid figure in the range of minute between 0 and 720, which means you can set the offset up to 12 hours.

- **Synchronization Interval (secs):** The Synchronization Interval is used for sending synchronizing packets periodically. Users can assign the time ranging from 64 to 1024 seconds. The "0" value displaying by default means that you disable the auto-synchronized feature in the SNTP client mode. You can enable the feature by filling the interval range from 64~1024 seconds.

- Click Apply to have the configuration take effect.



SNTP Configuration interface

IP Security

The IP security function allows a network manager to assign up to 10 specific IP addresses that have permission to manage the switch through the http Browser and Telnet services. By configuring these IP addresses its possible to only allow the listed / authorized personnel to manage this switch.

- **IP Security Mode:** With this item selected in the **Enable** mode, the **Enable HTTP Server**, **Enable Telnet Server** options showing the ten security IP fields will then be visible, if this option is not selected, those options will be greyed out.

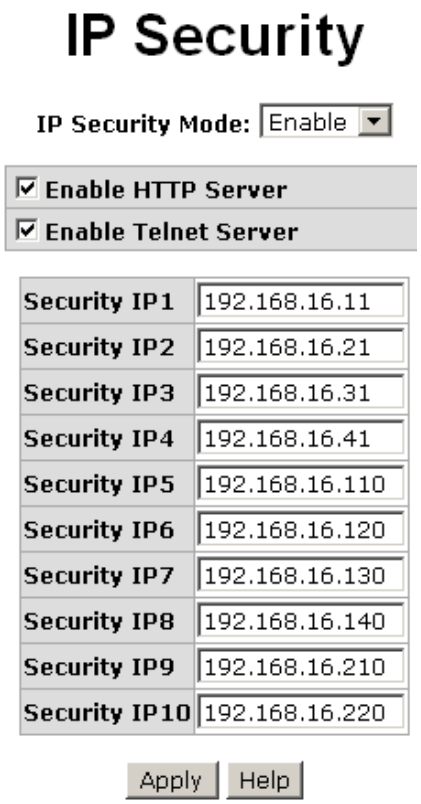
- **Enable HTTP Server:** With this option selected, Ethernet devices whose IP addresses match any one of the ten IP addresses in the Security IP table will be given permission to access this switch via an HTTP / browser.

- **Enable Telnet Server:** With this option selected, Ethernet devices whose IP addresses match any one of the ten IP addresses in the Security IP table will be given permission to access this switch via a telnet (CLI) service.

- **Security IP 1 ~ 10:** The system allows the user to assign up to 10 specific IP addresses for access security. Only when the **IP Security Mode** is enabled can these 10 IP addresses access and manage the switch through the HTTP/Telnet services.

- After configuring the options click Apply to allow the configuration take effect.

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



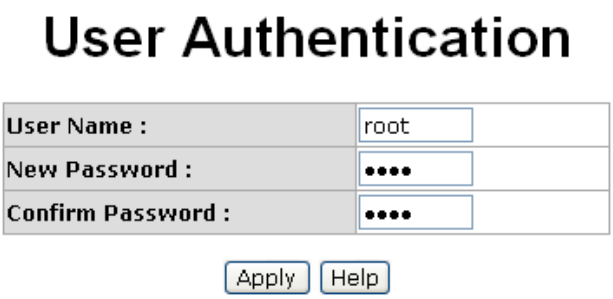
IP Security interface

User Authentication

This option allows the network manager to change the login user name and password of the switch.

Admin User

- **User Name:** The user account is ***root*** by default. Type in the User Name field with a new name as you wish.
- **New Password:** The password to the user account is ***case*** by default. Type in the New Password field with a new password of your choice.
- **Confirm password:** Type in the new password again for confirmation.
- When finished, click Apply to have the configuration take effect.



User Authentication interface

Port Statistics

The following page provides current statistics information which displays real-time packet transfer states for each port. A network manager may use this information to plan and implement network changes or expansion, or check and find the problem when the collision or heavy traffic occurs.

- **Port:** Port number indexed.
- **Type:** Displays the network media type of the port.
- **Link:** The states of linking—'**Up**' or '**Down**'.
- **State:** Displays port states set by the Port Control interface. When the state is disabled, the port will not transmit or receive any packet.
- **Tx Good Packet:** The number of **good** transmitted packets via this port.
- **Tx Bad Packet:** The number of **bad** packets transmitted (including undersize [less than 64 bytes], oversize, CRC Alignment 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 **bad** packets received via this port (including undersize [less than 64 bytes], oversize, CRC error, fragments and jabbers) via this port.
- **Tx Abort Packet:** The number of aborted transmit packets via this port.
- **Packet Collision:** The number of packet collisions via this port.
- **Packet Dropped:** The number of dropped packets via this port.
- **Rx Bcast Packet:** The number of broadcast packets via this port.
- **Rx Mcast Packet:** The number of multicast packets via this port.
- Click the 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	1000TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.02	1000TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.03	1000TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.04	1000TX	Up	Enable	448	0	728	0	0	0	0	4	2
Port.05	mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.06	mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.07	mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.08	mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0

Clear Help

Port Statistics interface

Port Control

In Port Control you can configure each of the ports within the switch.

- **Port:** Scroll up/down the scroll bar and select the port number to choose a particular port to be configured.
- **State:** Enable/disable the port. If the port state is set to 'Disable', the port will be disabled and not be able to receive or transmit any packets.
- **Negotiation:** Options include Auto and Force.

  Auto - With this parameter set to *Auto*, the speed and duplex fields display in grey, which means the port are negotiated automatically.

  Force - When you set the port to *Force*, you have to set the speed and duplex mode manually by selecting the pull-down menus of the Speed and Duplex fields.
- **Speed:** This option is only available when the Negotiation field is set to Force. When the Negotiation field is set to Auto, this field becomes a read-only field displaying in grey.
- **Duplex:** This option is only available when the Negotiation field is set on Force. If the Negotiation field is set to Auto, this field becomes a read-only field and is shown as greyed out.
- **Flow Control:** Whether the receiving node sends feedback to the sending node is determined by this option. With this item enabled, if the input data rate of the receiving device exceeds, the receiving device will send a PAUSE frame which halts the transmission of the sender for a specified period of time. With this item disabled, the receiving device will drop the packets it is unable to process.
- **Security:** When the Security selection is set as '**On**', any access from the device which connects to this port will be blocked unless the MAC address of the device is included in the static MAC address table.
- Click Apply to have the configuration take effect.

Port Control

Port	State	Negotiation	Speed	Duplex	Flow Control	Security
Port.01 Port.02 Port.03 Port.04	Enable	Auto	1000	Full	Enable	Off

Apply Help

Port	Group ID	Type	Link	State	Negotiation	Speed Duplex		Flow Control		Security
						Config	Actual	Config	Actual	
Port.01	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.02	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.03	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.04	N/A	1000TX	Up	Enable	Auto	1G Full	100 Full	Enable	ON	OFF
Port.05	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.06	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.07	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.08	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF

Port Control interface

Port Trunk

Port trunking is where several ports are grouped to expand the network data rate above any single pros data rate. For example by trunking 3 x 100Mbps ports we get a 300Mbps Trunk.

Link Aggregation Control Protocol (LACP), is a protocol running at layer 2, which provides a standard means (in accordance with IEEE 802.3ad) of bundling several physical ports together to form a single logical channel. All the ports within the logical channel or so-called logical aggregator work at the same connection speed .

LACP operation requires full-duplex mode.

Aggregator Setting

Please read the instructions below to configure an LACP or non-LACP trunk group.

- **System Priority:** A value which is used to identify the controlling switch of an LACP link system. The switch with the lower value has the higher system priority and is selected as the controlling end. The controlling end controls the port priorities, of the LACP link system.

- **Group ID:** There are four trunk groups to be selected. Assign a group ID to the particular trunk group.

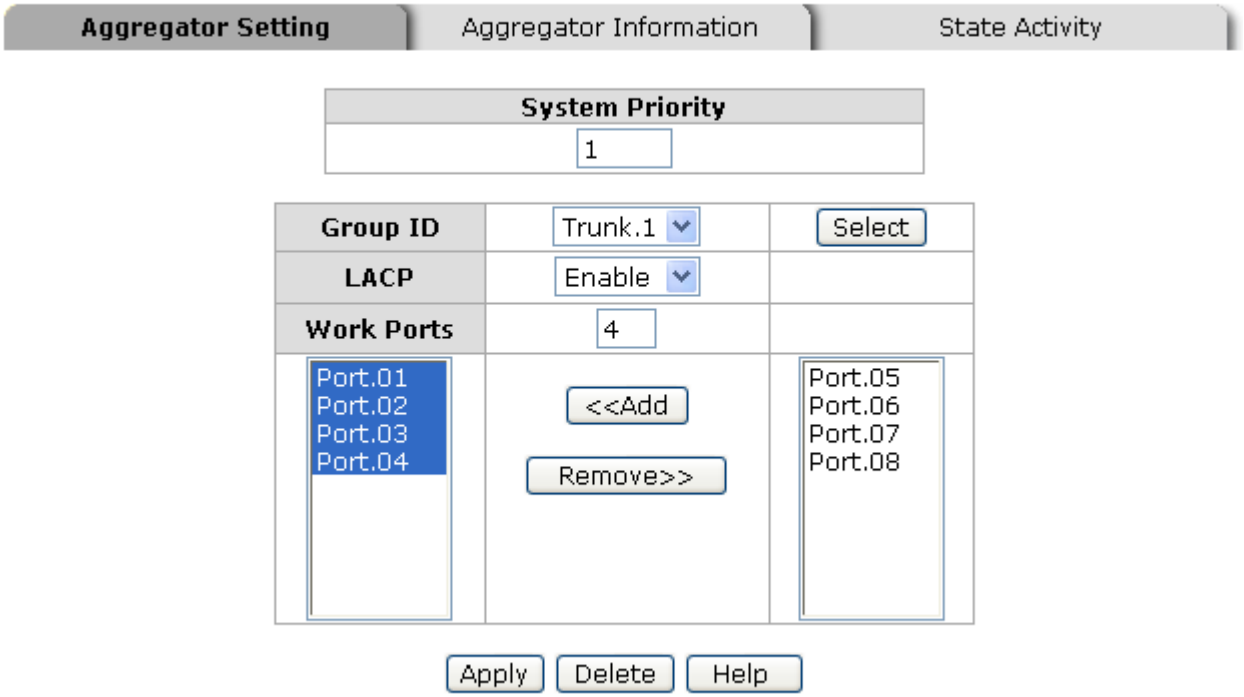
- **LACP:** Click the pull-down menu to enable/disable LACP for the trunk group. With LACP enabled, a port which joins an **LACP trunk group** to negotiate and agree with its member ports first. A trunk group, including member ports split between two switches, has to enable the LACP function on each of the two switches.

  If disabled, the trunk group is a **static trunk group**. The advantage of having the LACP disabled is that a port joins the trunk group without any handshaking with its member ports; but member ports won't know that they should be aggregated together to form a logical trunk group.

- **Work Ports:** This field allows the user to type in the total number of active ports in the LACP group, (a maximum of 4 ports). Using an **LACP trunk group** for example you can assign four ports to be members of the trunk group whose *Work Ports* field is set to two, with a further two ports assigned as standby/redundant ports that can join the working group if any of the working ports fail.

  With Static trunk groups (non-LACP), the number of working ports must equal the total number of group member ports.
- The system allows a maximum of four ports to be aggregated into a trunk group. Having configured the parameters above, highlight the ports in the right box to join the trunk group. Click the 'Add' button and the ports highlighted in the right box will be moved to the left box. To remove unwanted ports, select the ports in the left box and click the 'Remove' button.
- When LACP is enabled, you can configure LACP Active/Passive states for each member port on the **State Activity** tab.
- When you have completed your configuration, click Apply to allow the configuration take effect.
- To remove a trunk group, select the Group ID by clicking the pull-down menu labeled as 'Group ID' and click then click the Delete button.

Port Trunk - Aggregator Setting



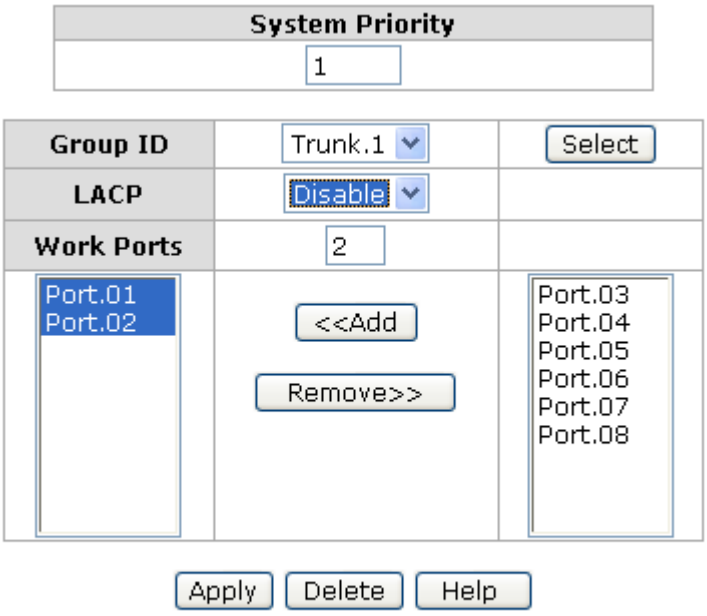
Notice: The trunk function do not support GVRP and X-Ring.

Port Trunk—Aggregator Setting interface (four ports are added to the left field with LACP enabled)

Aggregator Information

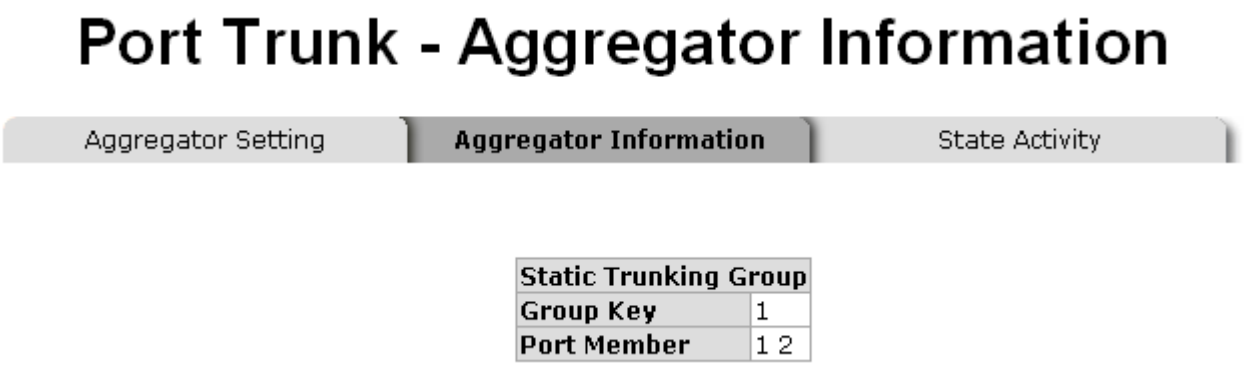
- **LACP Disabled**

Having configured the aggregator setting with LACP disabled, you can check the static trunk group information on the **Aggregator Information** tab.



Notice: The trunk function do not support GVRP and X-Ring.

Assigning 2 ports to a trunk group with LACP disabled



Static Trunking Group Information tab

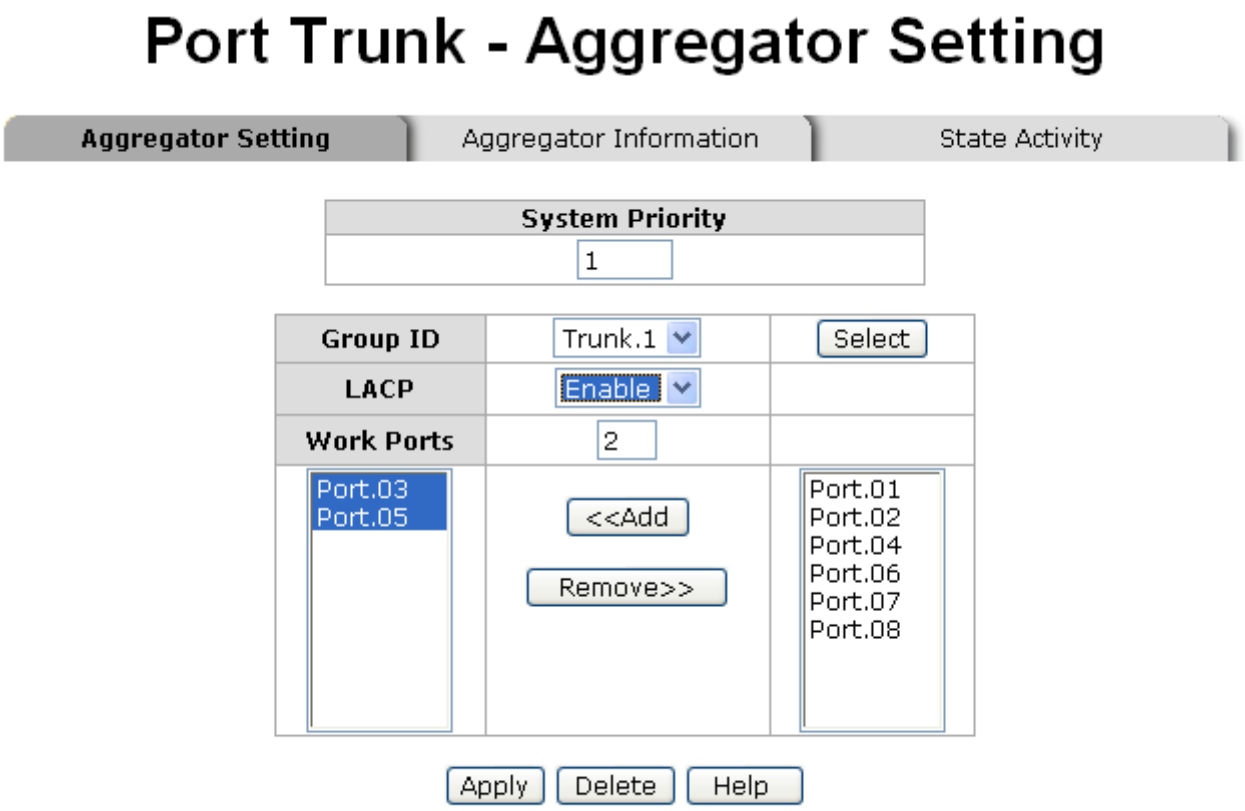
- **Group Key:** This is a read-only field that displays the trunk group ID.
- **Port Member:** This is a read-only field that displays the members of the static trunk group.

- **LACP Enabled**

Having configured the aggregator setting with LACP enabled, you can select the trunking group information between two switches on the **Aggregator Information** tab.

■ Configuration for Switch 1

1. Set **System Priority** of the trunk group. The field displays with '1' by default.
2. Select a trunk group ID by clicking the pull-down menu.
3. Enable LACP.
4. Include the member ports by highlighting the ports in the right list box and then click the **Add** button. Note the number in the *Work Ports* field changes automatically depending on how many ports you have selected.



Switch 1 configuration interface

Port Trunk - Aggregator Information

Aggregator Setting | **Aggregator Information** | State Activity

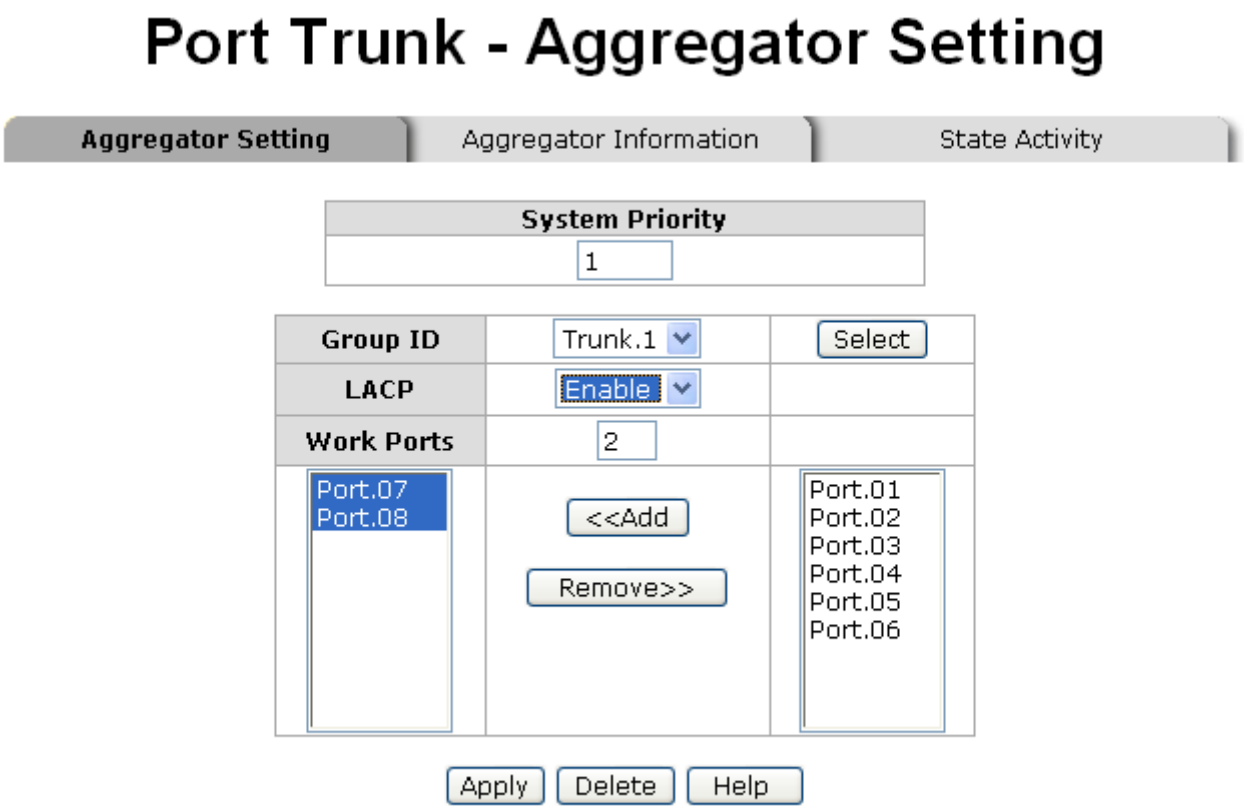
Group1						
Actor				**Partner**		
Priority	1			1		
MAC	001F3820820E			000F38FFF501		
PortNo	**Key**	**Priority**	**Active**	**PortNo**	**Key**	**Priority**
3	513	1	selected	8	513	1
5	513	1	selected	7	513	1

Static Trunking Group	
Group Key	2
Port Member	Port.01 Port.02

Aggregation Information of Switch 1

5. Click on the **Aggregator Information** tab to select the trunked group information as the illustration shown above after the two switches configured.

- **Configuration for Switch 2**



Switch 2 configuration interface

1. Set **System Priority** of the trunk group. The field displays with '1' by default.
2. Select a trunk group ID by clicking the pull-down menu.
3. Enable LACP.
4. Include the member ports by highlighting the ports in the right list box and then click the **Add** button. Note the number in the *Work Ports* field changes automatically depending on how many ports you have selected.

Port Trunk - Aggregator Information

Aggregator Setting | **Aggregator Information** | State Activity

Group1						
Actor				**Partner**		
Priority	1			1		
MAC	000F38FFF501			001F3820820E		
PortNo	**Key**	**Priority**	**Active**	**PortNo**	**Key**	**Priority**
7	513	1	selected	5	513	1
8	513	1	selected	3	513	1

Aggregation Information of Switch 2

5. Click on the **Aggregator Information** tab to check the trunked group information as the illustration shown above after the two switches configured.

Within the IEEE specification the **Link Aggregation Control Protocol** (**LACP**) provides a method of controling the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).

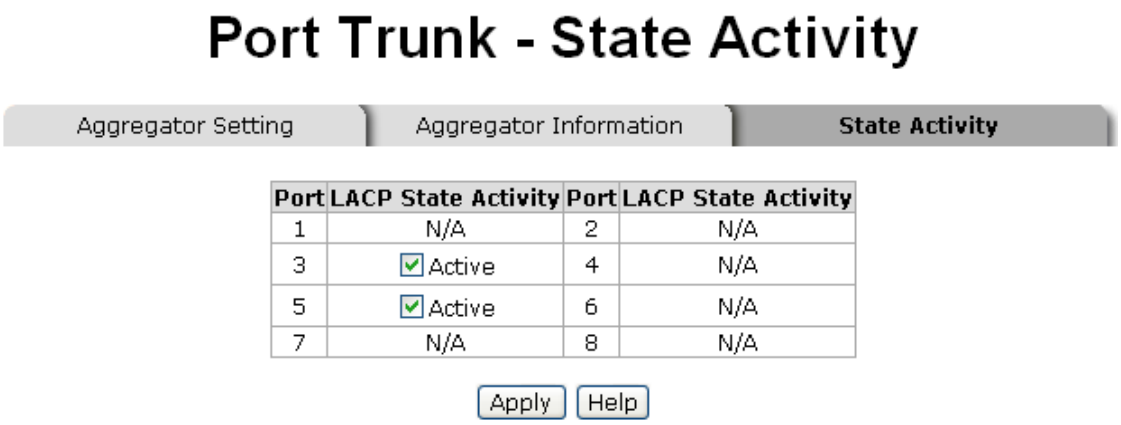
LACP works by sending frames (LACPDUs) down all links that have the protocol enabled. If it finds a device on the other end of the link that also has LACP enabled, it will also independently send frames along the same links enabling the two units to detect multiple links between themselves and then combine them into a single logical link. LACP can be configured in one of two modes: active or passive. In active mode the IGE 4T4GB-MX will always send frames down the configured links. In passive mode however, the switch acts as "speak when spoken to", mode and therefore can be used as a way of controlling accidental loops (as long as the other device is in active mode)

State Activity

Having configured the LACP aggregator on the **Aggregator Setting** tab, you may want to change the state activity for the members of the LACP trunk group. You can tick/untick the checkbox beside the state label. If you remove the tick in the box for the corresponding port and click the Apply button, the port state will change to **Passive**.

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

[NOTE] **A link** having two passive LACP nodes will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.

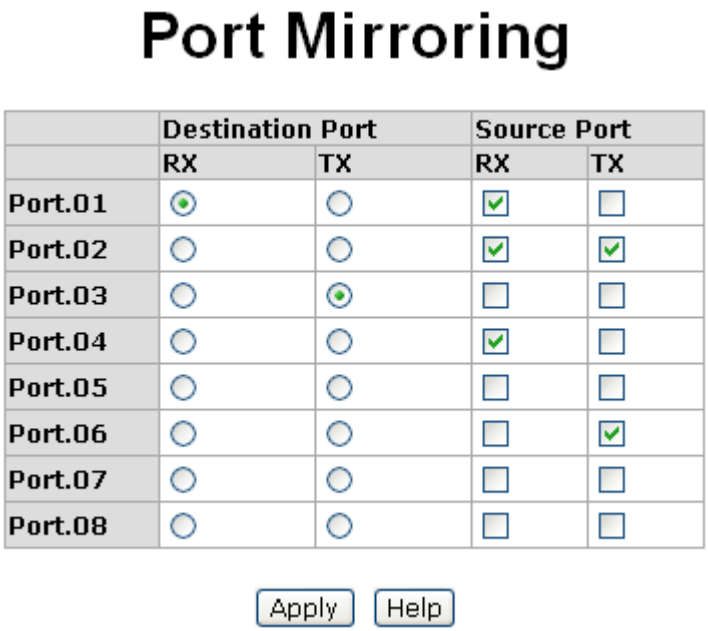


State Activity of Switch 1

State Activity of Switch 2

Port Mirroring

Port Mirroring is a method for monitoring network traffic on switched networks. Traffic through one port ports can be monitored by another port, which means traffic going in or out the monitored (source) ports will be duplicated into the mirroring (destination) port.



Port Mirroring interface

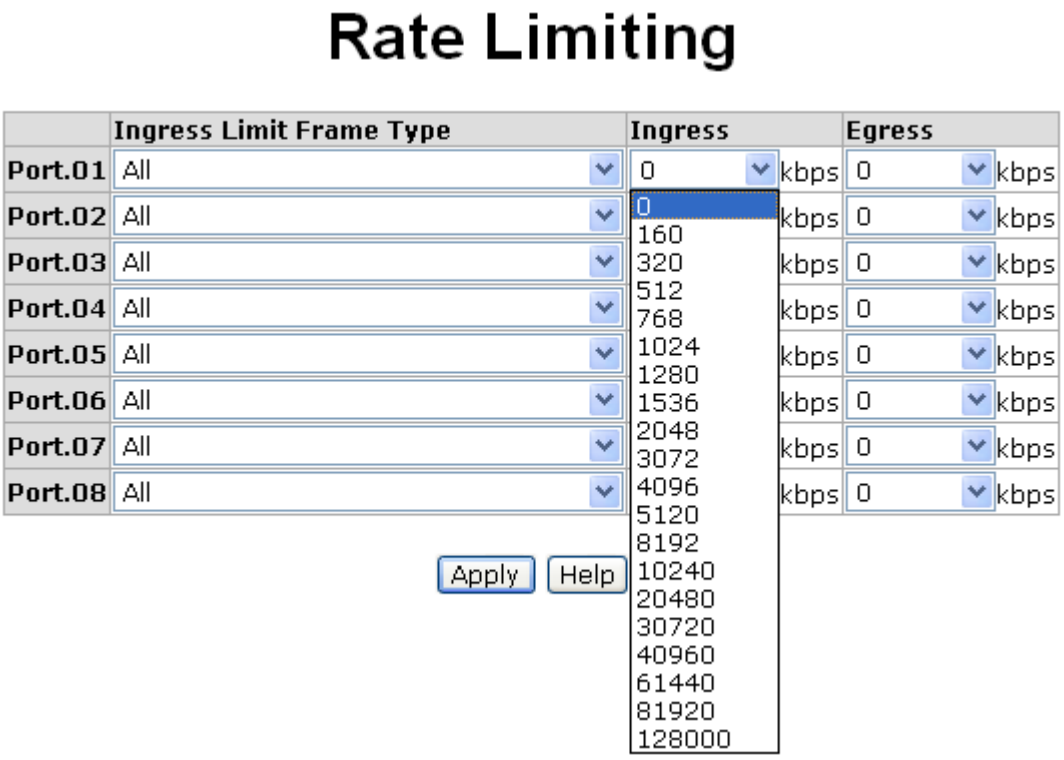
- **Destination Port:** Select one port to be the destination (mirroring) port for monitoring both RX and TX traffic coming from the source port. Or, select two ports for monitoring RX traffic and TX traffic respectively. Users can forward the traffic captured by the mirroring port to the packet analyzer like a Wire shark or Netxray for further analyses.
- **Source Port:** Select the option to monitor the corresponding port. All monitored port traffic will be copied to the mirroring (destination) port. Users can select multiple source ports by ticking the **RX** or **TX** checkboxes.
- After the options have been configured, click the Apply button.

Rate Limiting

You can respectively configure the ingress data rate and ingress / egress data rate for each port.

- **Ingress Limit Frame Type:** Select the limit type for ingress frames. Four options are available as follows:
  - **All**
  - **Broadcast/Multicast/Flooded Unicast**
  - **Broadcast/Multicast**
  - **Broadcast only**

  The egress rate will limit all types of frame.



Rate Limiting interface

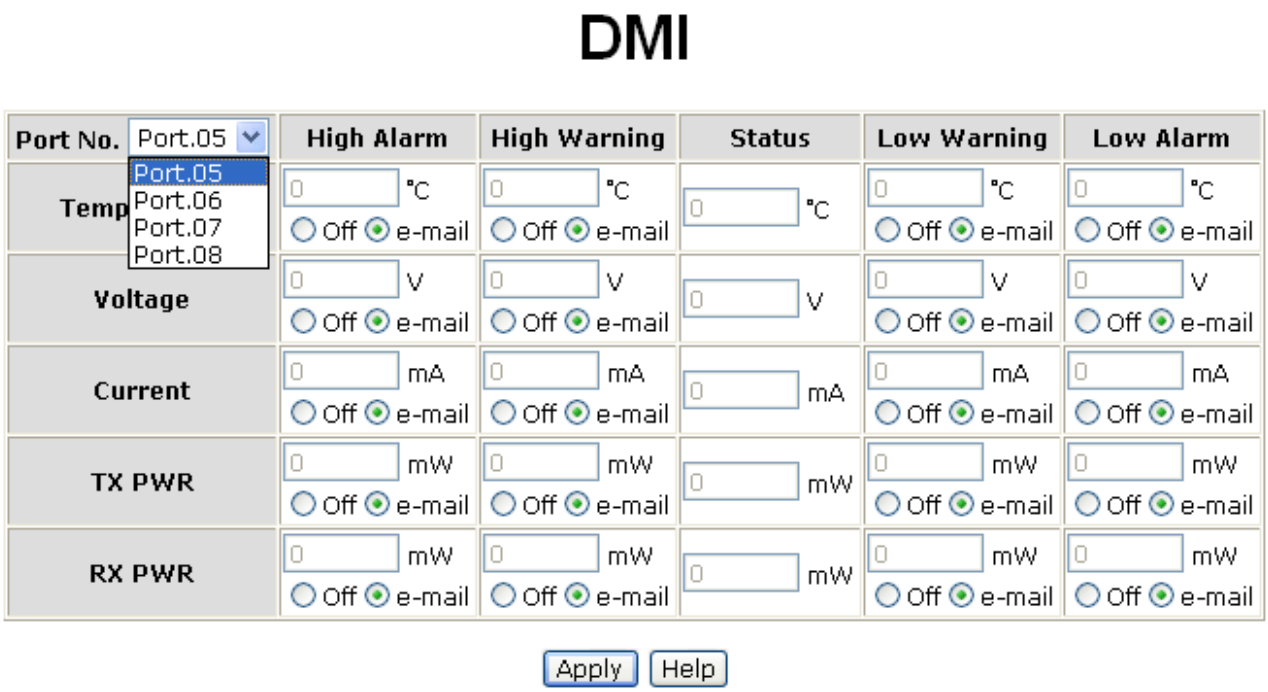
- Click the Ingress/Egress pull-down menus to select the bandwidth limit.
- When finished, click Apply to have the configuration take effect.

DMI

The DMI (Diagnostic Monitoring Interface) has been developed for monitoring the SFP (MINI GBIC) ports in particular the following parameters

1. Temperature,
2. Voltage,
3. Current,
4. Transmitting power
5. Receiving power

If the real time values, of the respective ports reach the threshold of the connected transceiver, the system will shut down the device or send an e-mail to the network manager or network engineer. The recipients can be specified via the SMTP configuration. Please refer to the ***System Event Log—SMTP Configuration*** section.



DMI interface

- **Port No.:** Click the pull-down menu to select a particular SFP port to display its information and define reaction options.

- **Temperature:** This field shows the values measured in degrees Celsius. Click the radio button labeled as '***Off***' to shut down the device if the temperature threshold of the port is reached. or the other one labeled as '***e-mail***' to send an e-mail to notify the network manager.

- **Voltage:** This field shows the values measured in voltage. Click the radio button labeled as '***Off***' to shut down the device or the other one labeled as '***e-mail***' to send e-mail if the port voltage reaches the threshold.

- **Current:** This field shows the values measured in milli amperes. Click the radio button labeled as '***Off***' to shut down the device or the other one labeled as '***e-mail***' to send e-mail the network manager if the port current reaches the current threshold.

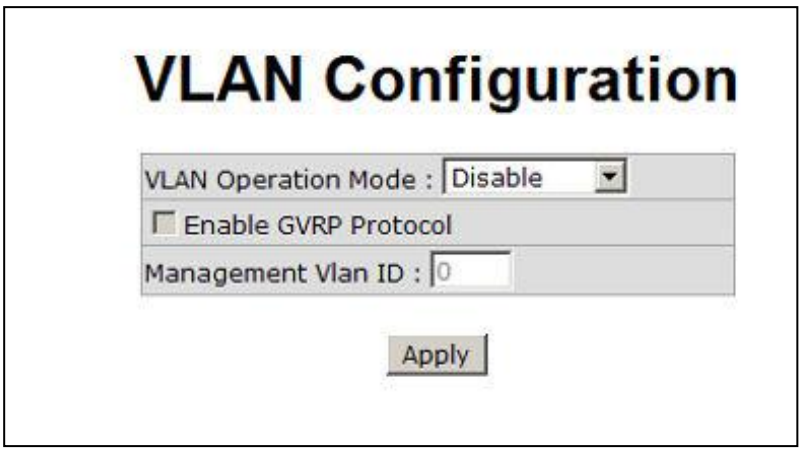
- **TX PWR:** This field shows the values measured in milli watts. Click the radio button labeled as '***Off***' to shut down the device or the other one labeled as '***e-mail***' to send e-mail for notifications when the port transmitting power reaches the transmit power threshold.

- **RX PWR:** The fields shows the values measured in milli watts. Click the radio button labeled as '***Off***' to shut down the device or the other one labeled as '***e-mail***' to send e-mail if the port receiving power reaches the receive power threshold.

VLAN Configuration

A Virtual LAN (VLAN) is a logical network that limits the broadcast domain, allowing a network manager to isolate network traffic. Therefore only the members of the same VLAN will receive traffic from the other members of the same VLAN.
Creating a VLAN provides a separate logical network amongst the member's, even though the devices are physically connected to the same physical Layer 2 network.

The IGE 4T4GB-MX supports both **Port-based** and **802.1Q** (tagged-based) VLAN. Please read the following instructions to configure the appropriate type of VLAN for your need.



VLAN Configuration interface

Port-based VLAN

A port-based VLAN usually consists of its members—ports, which means the VLAN is created by grouping a number of selected ports.

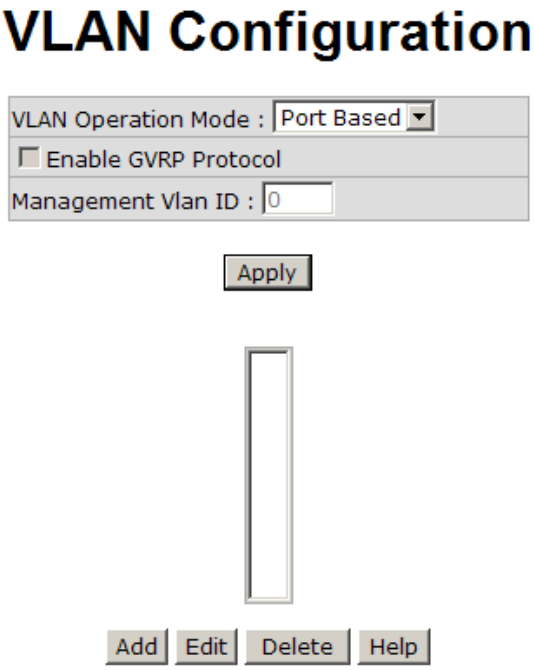
A port based VLAN is the easiest to configure and can be undertaken by simply selecting ports and allocating VLAN numbers to them.

Data can flow freely between members of the same VLAN.

Note all unselected ports are treated as belonging to another single VLAN that is, technically, a single broadcast domain.

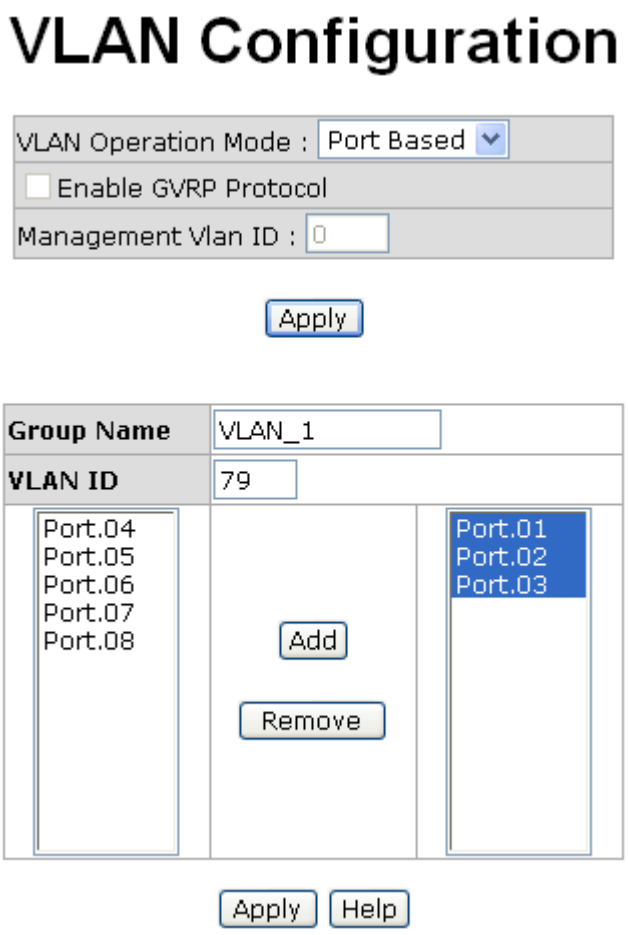
If a port-based VLAN is enabled, then VLAN-tagging will be ignored. A port-based VLAN allows the user to create separate VLANs to limit unnecessary packets flooding; the network.

Its possible to allow a port to belong to a number of different VLANS, allowing the device connected to that port to talk to multiple other VLANS, that are configured on that port.



VLAN – Port Based interface

- Select the pull-down menu and select **Port Based** and then click the Apply button to set the VLAN operation mode to **Port Based**.
- With the VLAN operation mode selected, click Add to create a new VLAN group.



Add a Port Based VLAN

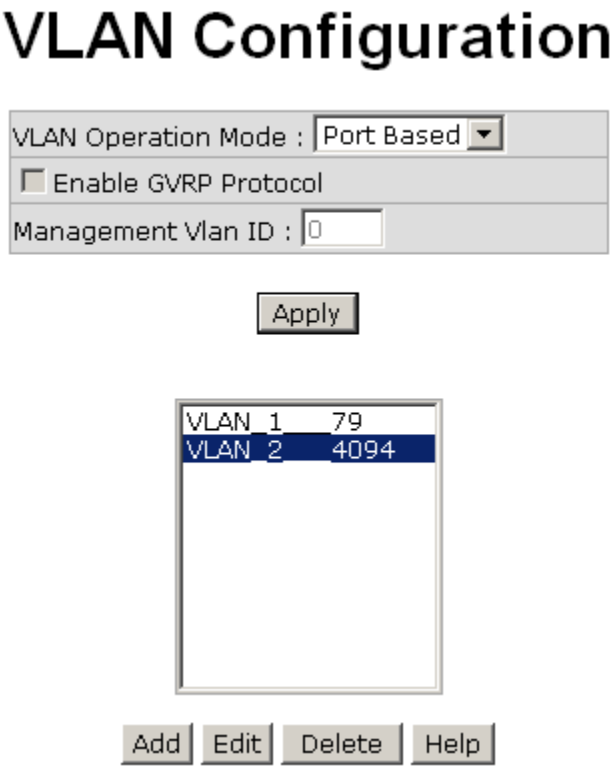
- Group Name – Enter a group name for your VLAN, and also a VLAN ID. In our example we can see we have VLAN_1 with a VLAN_ID of 79

- Select ports from the left side box to be member's of that VLAN group and ID, as can be seen above VLAN 1 has ports 1,2 and 3 as member's.

- To remove ports from the VLAN group, select the port in the right hand box and click 'remove'.

- When finished, click 'Apply' enable the VLAN configuration to take effect.

- The VLAN list is then displayed.



Edit/Delete Port Based VLAN

- With the VLAN list box displayed, select VLAN(s) and click the Delete button to get delete the VLAN(s).

- Highlight a VLAN and click the Edit button to change group name, VLAN ID, or to add/remove the members of the existing VLAN group.

[NOTE] Remember to select “Save Configuration”, otherwise the new configuration will be lost when the switch is powered off.

802.1Q VLAN (Tagged VLAN)

Introduction

802.1Q does not actually encapsulate the original frame. Instead, for Ethernet frames, it adds a 32-bit field between the source MAC address and the EtherType /Length fields of the original frame, extending the minimum and maximum frame sizes from 64 and 1,518 bytes (octets) to 64 and 1,522 bytes (42 octet minimum applies when 802.1Q is present. Two bytes are used for the tag protocol identifier (TPID), the other two bytes for tag control information (TCI). The TCI field is further divided into PCP, CFI, and VID

When the IGE 4T4GB-MXis set for 802.1Q VLAN operation all ports on the switch belong to the default VLAN of VID 1. This means they logically are regarded as members of the same broadcast domain.
The valid VLAN ID range is from 1 to 4094. The number of VLAN groups is up to 256 including the default VLAN 9VLAN_1) which cannot be deleted.

GVRP (GARP VLAN Registration Protocol) is a protocol that controls VLANs within a larger network. GVRP conforms to the IEEE 802.1Q specification, which as mentioned above defines a method of tagging frames with VLAN configuration data and extends the frame to 1522 byte.

This allows network devices to dynamically exchange VLAN configuration information with other devices. For example, with GVRP enabled, the switches are able to automatically exchange the information of their VLAN database. Therefore, the user does not need to manually configure the link type. Packets belonging to the same VLAN can communicate across switches.

Each member port of an 802.1Q VLAN is either an;
Access Link (VLAN-tagged)
or a
Trunk Link (not VLAN-tagged).

All frames entering an IGE-4T4GB-MX switch Access Port carry no VLAN identification. Conversely, all frames on a Trunk Link are VLAN-tagged.

Hybrid

There is also a third VLAN mode— called Hybrid.

A Hybrid Link can carry both VLAN-tagged frames and untagged frames.

A single port is should belong to a particular VLAN group, except if it is on a Trunk/Hybrid Link. This is because the port can attach a VLAN tag to any packets passing through that port. The technique of 802.1Q tagging inserts a 4-byte tag, including of the VLAN ID of the destination port—PVID, in the frame.

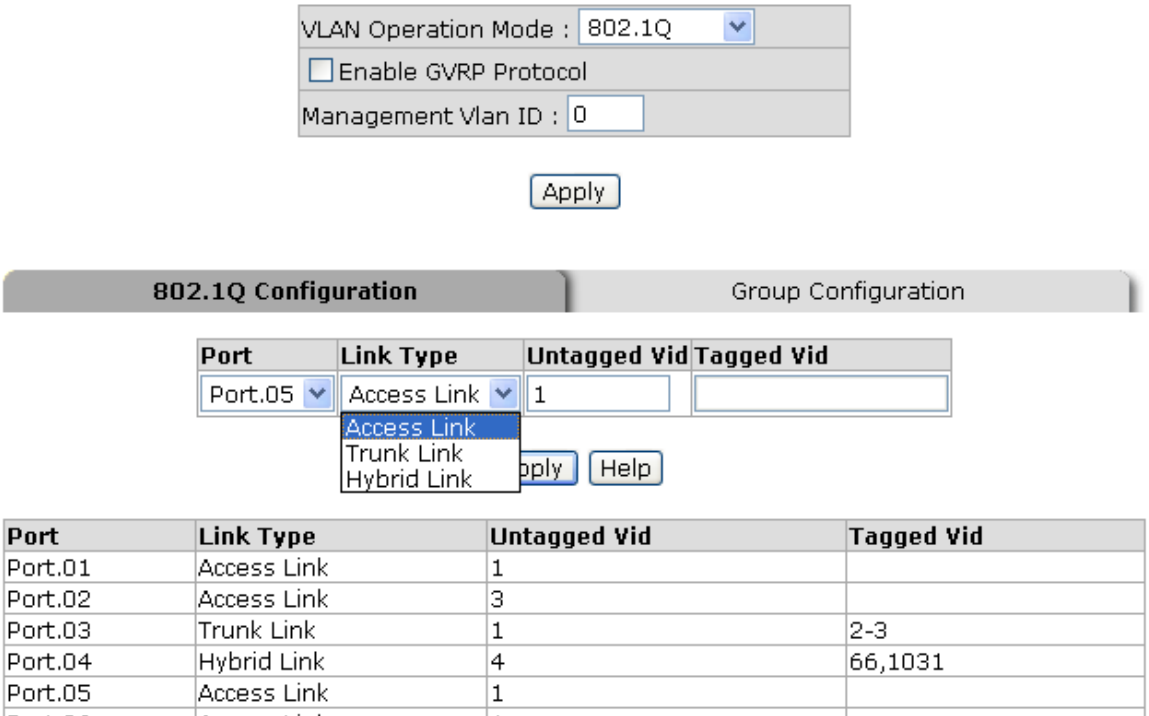
With a combination of Access / Trunk / Hybrid Links, communications across switches is possible whether the VLAN packets are tagged or untagged.

802.1Q Configuration

To configure an 802.1Q VLAN please follow the following steps.

- Click the pull-down menu to select **802.1Q** and click Apply to configure the VLAN Operation Mode for 802.1Q operation.
- **Enable GVRP Protocol:** Select this option to enable the GVRP protocol. This option is available only when VLAN Operation Mode is set on **802.1Q**.
- **Management VLAN ID:** Only the VLAN members, whose Untagged VID (PVID) equals to the value specified in this field, have permission to access the switch. The default value is ‘0’ that means this limit is not enabled (all members in different VLANs can access this switch). To only allow members of a specific VLAN manage the switch use that VLAN ID in this field.
- After you have configured the three parameters, select the Apply button right beneath this area to finish creating an 802.1Q VLAN.

VLAN Configuration



Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	
Port.02	Access Link	3	
Port.03	Trunk Link	1	2-3
Port.04	Hybrid Link	4	66,1031
Port.05	Access Link	1	
Port.06	Access Link	1	
Port.07	Access Link	1	
Port.08	Access Link	1	

802.1Q VLAN interface

- On the 802.1Q Configuration tab, select the *Port* pull-down menu to select a port you want to configure within the VLAN.
- **Link Type**: Three options are available. Select the pull-down menu to select the link type.

  Access Link:

  This option allows any packet entering the switch to be given a tagged VLAN-ID Any device connecting to an Access Port (untagged port) has an untagged Frame VID (also called PVID).

  After the untagged frame gets into the access port, the IGE-4T4GB-MX inserts a four-byte tag in the frame. The contents of the last 12-bit of the tag is the untagged VID. When this frame is sent out of the network via any of the of VLAN_ID Access ports the switch will remove the tag from the frame to put it back to its original state.

  Those ports of the same untagged VID are regarded as the same VLAN group members.

[NOTE] *Because the access port doesn't understand a tagged frame, the Tagged VID field is not available.*

- **Trunk Link:** A segment which provides a path for one or more VLAN-aware devices. A Trunk Port connecting to the trunk link has knowledge of tagged frames, which are used for communications across VLANs.
  The VID frames which will be forwarded across the trunks will depend on the values entered into the Tagged VID field. Please insert a comma between two VIDs.

[NOTE]

1. *A trunk port doesn't insert tags into an untagged frame, and therefore the untagged VID field is not available.*
2. *It's not necessary to type '1' in the tagged VID field. The trunk port will forward the frames of VLAN 1.*
3. *The trunk port must be connected to a trunk / hybrid port of the other switch. Both the tagged VID of the two ports have to be the same.*

- **Hybrid Link:** A segment which consists of Access and Trunk links. The hybrid port has both the features of the Access and Trunk ports. A Hybrid port has a PVID belonging to a particular VLAN, and also forwards the specified tagged-frames for the purpose of VLAN communications between switches.

[NOTE]

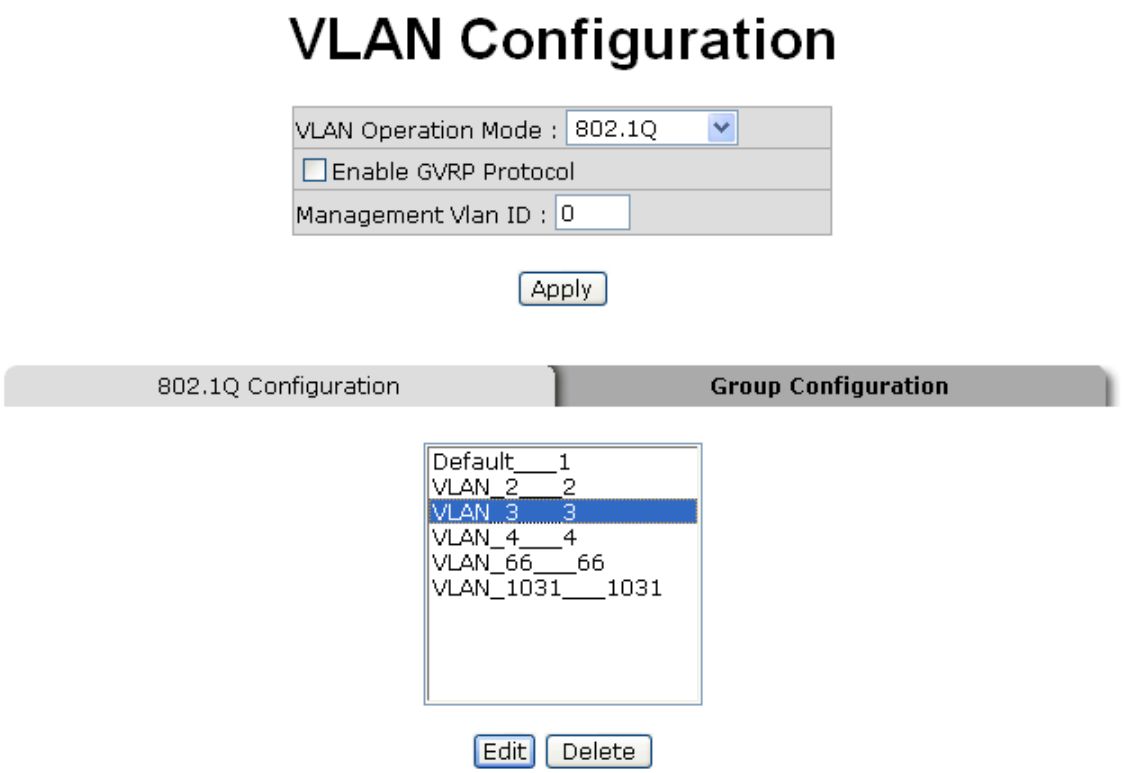
1. *It's not necessary to type '1' in the tagged VID field. The hybrid port will forward the frames of VLAN 1.*
2. *The trunk port has to be connected to a trunk/hybrid port of the other switch. Both the tagged VID of the two ports have to be the same.*

- **Untagged Vid:** This field is available when the *Link Type* pull-down menu is set to *Access Link* or *Hybrid Link*. Assign a number in the range between 1 and 4094.
- **Tagged Vid:** This field is available when the *Link Type* pull-down menu is set on *Trunk Link* or *Hybrid Link*. Assign a number in the range between 1 and 4094.
- Click the Apply button on the tab to have the port configuration take effect.
- And then you can see the link type, untagged VID, and tagged VID information of each port shown in the table on the screen.

Group Configuration

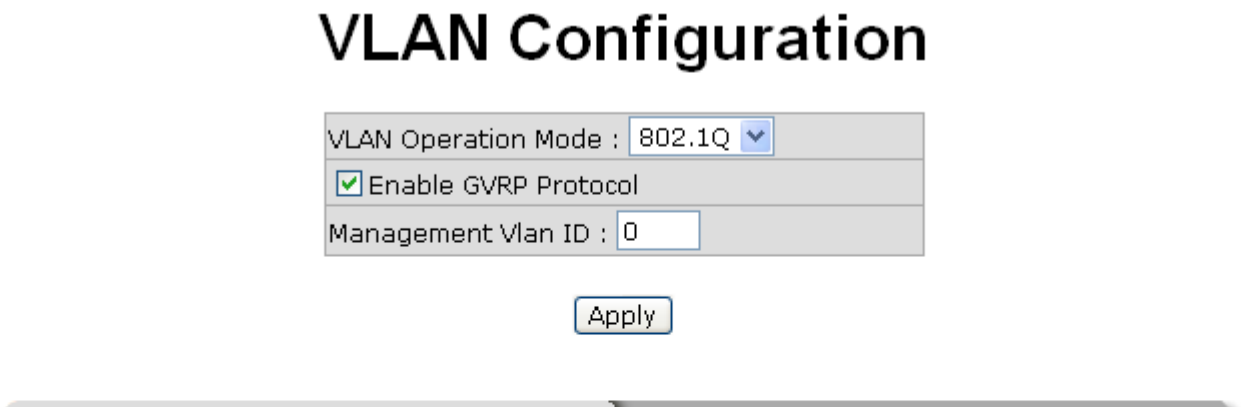
Edit the existing VLAN Groups.

- Select the 'Group Configuration' tab.
- Select a VLAN group in the list box and click the Edit button.



Group Configuration interface

- After clicking the Edit button, you can change group name and VLAN ID of the selected VLAN group.



Group Configuration interface

- When you have finished, click Apply to have the modification take effect.

Rapid Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol providing faster re-routing after a link failure or topology change. The IGE-4T4GB-MX also supports Spanning Tree Protocol (STP) and will auto-detect the connected device running STP or RSTP.

RSTP System Configuration

This tab allows users to configure parameters for RSTP and displays the spanning tree information of the root bridge.

- **RSTP mode:** Select the pull-down menu to enable the RSTP function.
- **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):** Enter the time in seconds between 6 and 40 which the switch waits to attempt to save its configuration.
- **Hello Time (1-10):** Enter the time in seconds between 1 and 10 that controls the switch to send out the BPDU packet to check current states of RSTP.
- **Forward Delay Time (4-30):** Enter the time in seconds between 4 and 30 that a port spends changing from its learning and listening state to the forwarding state.
- When finished, click the Apply button to have the configuration take effect.

[NOTE]	Follow the rule below to configure *Max Age*, *Hello Time*, and *Forward Delay Time* parameters. **2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)**

Root Bridge Information

The column fields give the current bridge information for the switch.

- **Bridge ID:** This field displays the bridge ID by showing the MAC address of this switch.

- **Root Priority:** This field displays the numerical value indicating bridge priority of the IGE-4T4GB-MXE-C switch. Usually the switch with the lowest numerical value in the network is set as the root bridge.

- **Root Port:** This field indicates which port is connecting to the root bridge. When the switch is set as the root bridge, the word ‘Root’ shows here.

- **Root Path Cost:** This field displays the path cost between the switch’s root port and the designated port of the root bridge. Path cost is a value to each port typically based on rules described as part of 802.1d. For the root bridge this is zero. For all other bridges, it is the sum of the port path costs on the least cost path to the root bridge.

- **Max Age:** Displays the configured aging time of the switch.

- **Hello Time:** Displays the configured Hello Time.

- **Forward Delay:** Displays the configured forward delay time.

RSTP - System Configuration

System Configuration | Port Configuration

RSTP Mode	Enable
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).

Apply Help

Root Bridge Information

Bridge ID	0080000F3800055E
Root Priority	32768
Root Port	Root
Root Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15

RSTP System Configuration interface

Port Configuration

This tab offers the interface for RSTP port configuration where you can assign parameters to each port. The rapid spanning tree protocol will have the port with the higher priority in forwarding state and block other ports to make certain that there is no loop in the LAN.

- Scroll the list box to select a port for configuration.
- **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)
- **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).
- **Admin P2P:** The rapid state transitions possible within RSTP are dependent upon whether the port concerned can only be connected to exactly another 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 states of the link to be manipulated administratively. **True** means the port is regarded as a point-to-point link. **False** means the port is regarded as a shared link. Auto means the link type is determined by the auto-negotiation between the two peers. **(NB Switch to Switch=P2P=true)**
- **Admin Edge:** The port directly connected to an end station is known as an edge port that won't create bridging loop in the network. To configure the port as an edge port, set the port to "**True**" state.
- **Admin Non Stp:** Configure whether the port includes the STP mathematic calculation. **True** means not to include the STP mathematic calculation. **False** means the STP mathematic calculation is included.
- After configuring the port, click 'Apply' to have the configure take effect.

RSTP - Port Configuration

System Configuration | **Port Configuration**

Port	Path Cost (1-200000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non STP
Port.01 Port.02 Port.03 Port.04 Port.05	20000(	128	Auto	True	false

priority must be a multiple of 16

Apply Help

RSTP Port Status

Port	Path Cost	Port Priority	Oper P2P	Oper Edge	STP Neighbor	State	Role
Port.01	20000	128	True	True	False	Disabled	Disabled
Port.02	20000	128	True	True	False	Disabled	Disabled
Port.03	20000	128	True	True	False	Disabled	Disabled
Port.04	20000	128	True	True	False	Forwarding	Designated
Port.05	20000	128	True	True	False	Disabled	Disabled
Port.06	20000	128	True	True	False	Disabled	Disabled
Port.07	20000	128	True	True	False	Disabled	Disabled
Port.08	20000	128	True	True	False	Disabled	Disabled

RSTP Port Configuration interface

SNMP Configuration

Simple Network Management Protocol (SNMP) is a protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enabled network, usually containing an SNMP Network Management System such as 'CaseView'. An SNMP system can receive traps from the IGE-4T4GB-MX which in turn register in the NMC's database and change the colour of the icons on the NMC map display.
In addition an SNMP system usually polls the devices in the network, and those devices respond to the poll, with any failure to reply also resulting in a network alarm on the NMC.

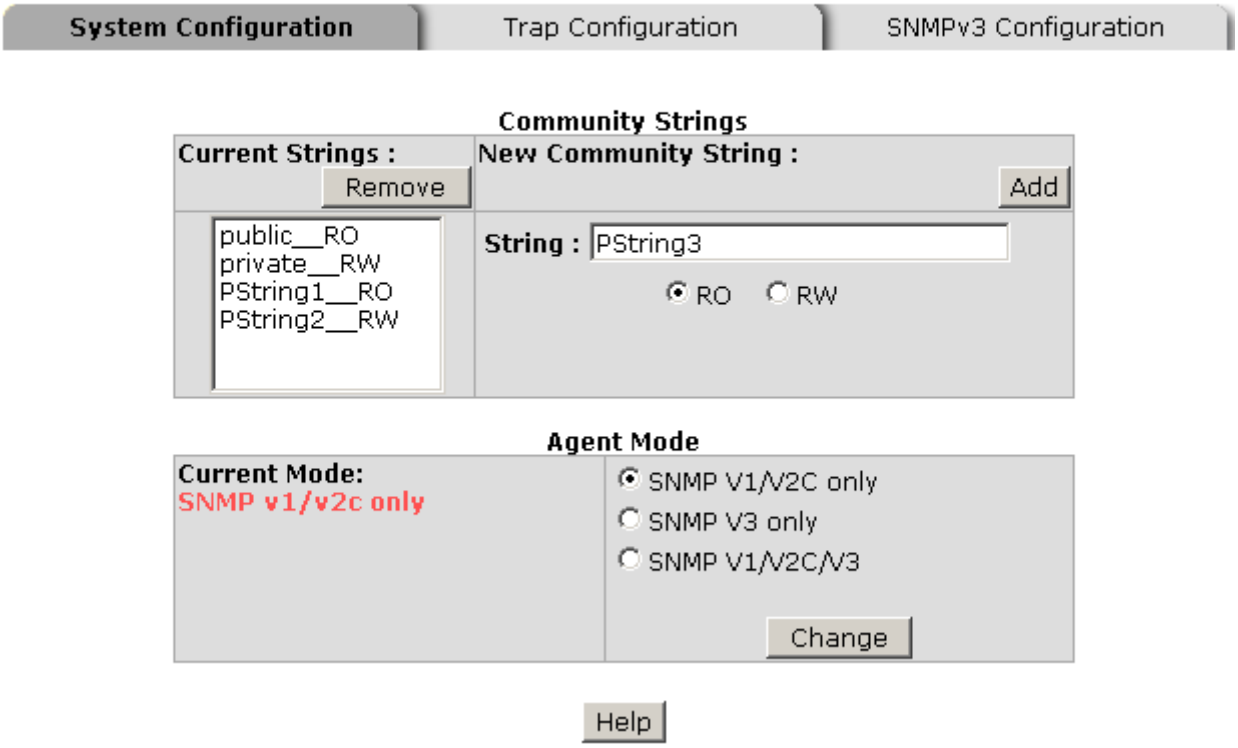
System Configuration

This tab allows users to define new community strings and remove the unwanted community strings for authentication purposes. When adding a new community string, the network manager should also specify the type of access permission and the agent mode.

- **String:** Enter the community string in the field as a password for authentication.
- **RO:** Read only. With this option selected, the community string is given the read-only permission for the MIB objects.
- **RW:** Read/write. With this option selected, the community string is given read/write permission for the MIB objects.
- Click Add to finish adding a new community string.
- To remove a specific community string, select the community string shown in the list box and click Remove. The default strings in the IGE-4T4GB-MXare Public_RO and Private_RW. It's possible to remove these if the IGE-4T4GB-MX is reset back to its default, these strings will re-appear.

- **Agent Mode:** Select one of the option to select the SNMP version that the community string will use. And then select 'Change' to ensure the selected SNMP version mode is changed.

SNMP - System Configuration

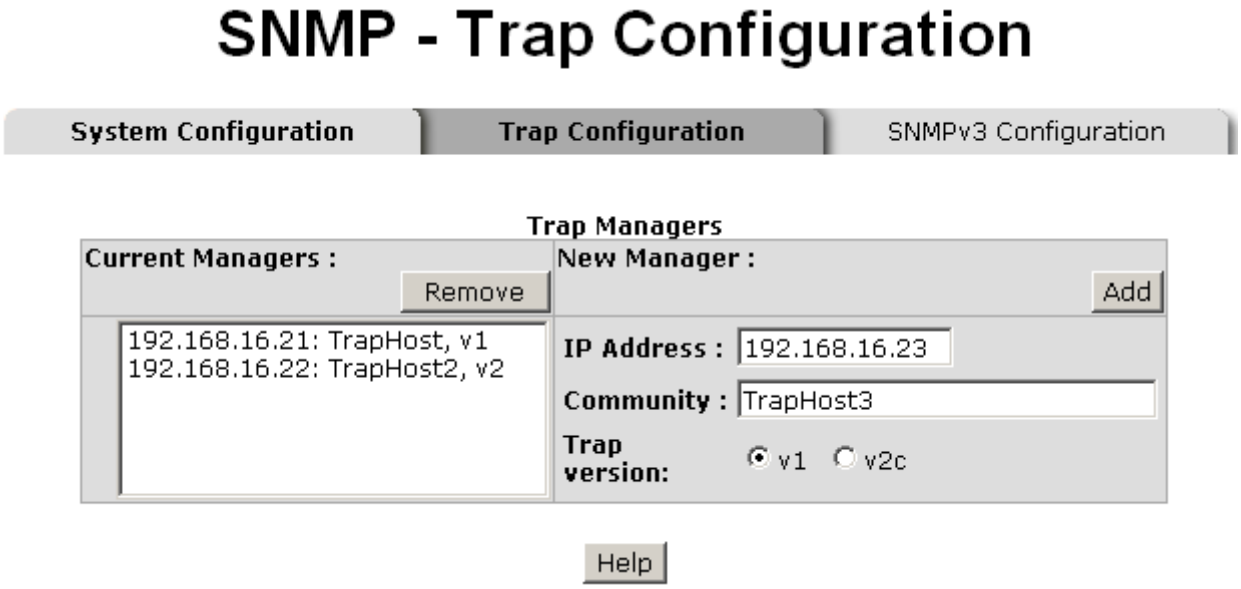


SNMP System Configuration interface

Trap Configuration

A trap manager is a management station (such as an network management system such as ‘CaseView’ that receives trap messages generated by the IGE-4T4GB-MX.
If no trap manager is defined, no traps will be issued. To define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version.

- **IP Address:** Enter the IP address of the network management system or trap manager.
- **Community:** Enter the community string for the trap station.
- **Trap Version:** Select the SNMP trap version—v1 or v2c.
- When finished, click Add.
- To remove a specific manager station, select the entries listed in the Current Managers field and click Remove.



Trap Managers interface

SNMPV3 Configuration

The SNMPv3 protocol uses different terminology than the SNMPv1 and SNMPv2c. In the SNMPv1 and SNMPv2c protocols, the terms agent and manager are used. An agent is the software within an SNMP device such as the IGE-4T4GB-MXwhile a manager is an SNMP host such as CaseView. In the SNMPv3 protocol, agents and managers are called entities. In any SNMPv3 communication, there is an authoritative entity and a non-authoritative entity. The authoritative entity checks the authenticity of the non-authoritative entity. And, the non-authoritative entity checks the authenticity of the authoritative entity.

This tab allows a network manager to configure the SNMPv3 settings for an SNMPv3 management system.

►Context Table

Contexts were really designed to allow talking through an agent to a remote device. Configure the SNMPv3 context table. Assign the context name in the field.

Click Apply to add the context name or to change it..

►User Table

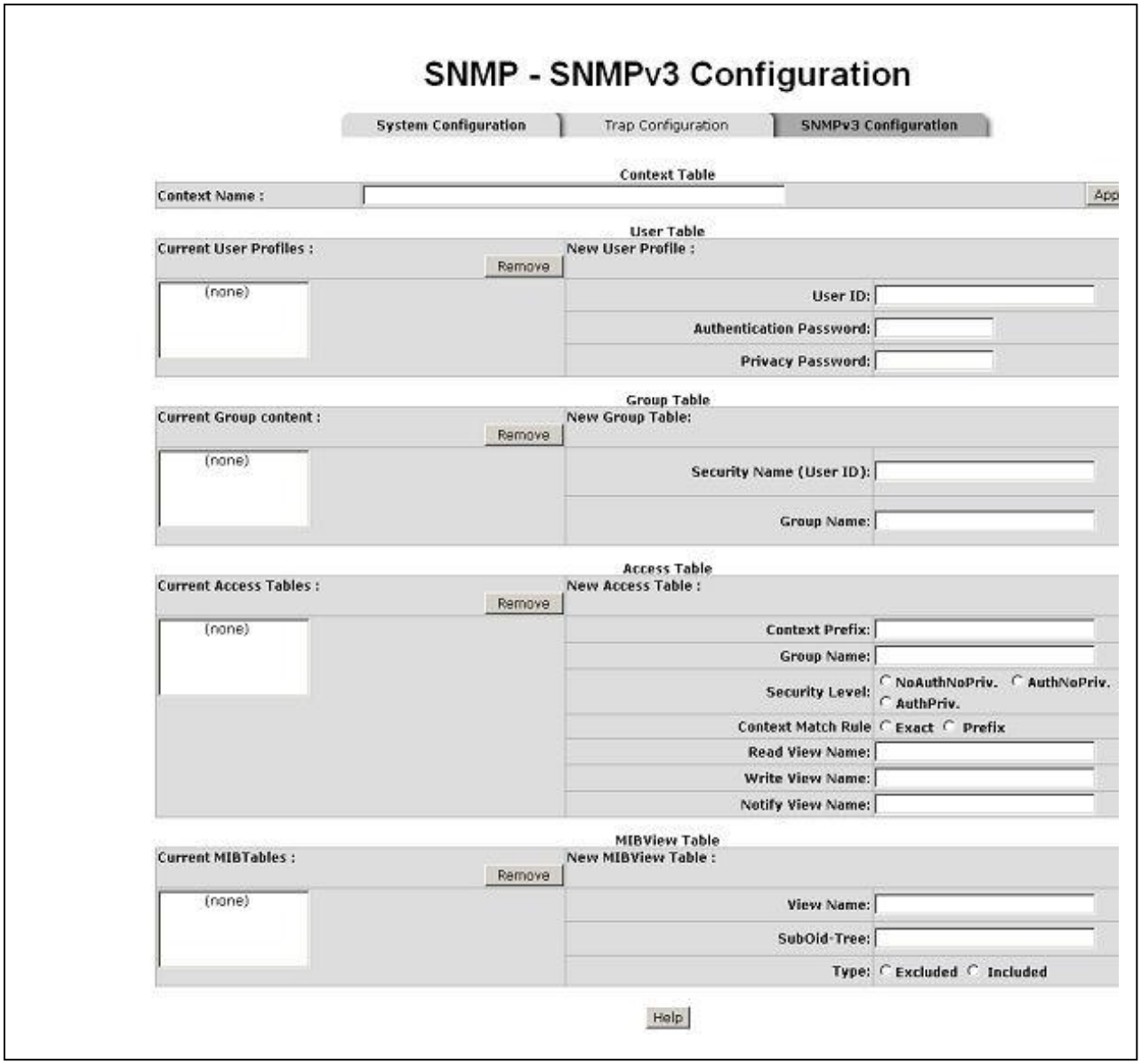
Configure the SNMPv3 user table.

- **User ID:** Type the user name in the field.
- **Authentication Password:** Assign the authentication password to the user ID.
- **Privacy Password:** Assign the private password to the user ID.
- Click the Add button to create a new user profile.
- To remove a user profile, select an entry in the Current User Profiles list box and click the Remove button to remove the unwanted user profile.

►Group Table

Configure the SNMPv3 group table.

- **Security Name (User ID):** Specify the user name that you have set up in the user table.
- **Group Name:** Type the group name in the field.
- Click the Add button to create a new group name
- To remove a group name, select an entry in the Current Group Content list box and click the Remove button to remove the unwanted group.



SNMPv3 configuration interface

NB. Modifying the SNMPv3 tables might cause the MIB to be rejected. Please check that these options are in line with your NMS system before making changes.

►Access Table

Configure the SNMPv3 access table.

- **Context Prefix:** In this filed type in the prefix letters of the context name that is assigned in the context table.

- **Group Name:** Type in the group name that is assigned in the group table.

- **Security Level:** Select the option to determine which security level is assigned to the group. The options include:
  NoAuthNoPriv: Communications are made without authentication or encryption.
  AuthNoPriv: Communications are made with authentication but without encryption.
  AuthPriv: Communications are made with authentication and encryption.

- **Context Match Rule:** Select the radio button to determine the context matching rule. You can configure it as a complete matching or prefix matching condition.

- **Read View Name:** Assign permission of reading to a user ID typed that exists in the User Table.

- **Write View Name:** Assign permission of writing to a user ID typed that exists in the User Table.

- **Notify View Name:** Assign permission of notifying to a user ID typed that exists in the User Table.

- Click Add to create a new access entry

- Select an entry in the Current Access Tables list box and click Remove to delete the unwanted access entry.

►MIBview Table

Configure the SNMPv3 MIB view table.

- **ViewName:** Type in a new view name in the field.
- **Sub-Oid Tree:** Type in the Sub OID that allows the NMS to view objects of the particular object.
  MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing object identifiers (OID).
- **Type:** Select the radio button to determine the view type – exclude or included.
- Click Add to create a new entry.
- Click Remove to delete the unwanted entry.

QoS Configuration

In general, traffic on networks is treated as the same priority and delivered equally. With QoS enabled, users can classify frames or packets into different priority types to ensure specific traffic is delivered on best-effort. The incoming frames or packets can be sent to different priority queues for different priorities according to the configured polices.

►QoS Policy

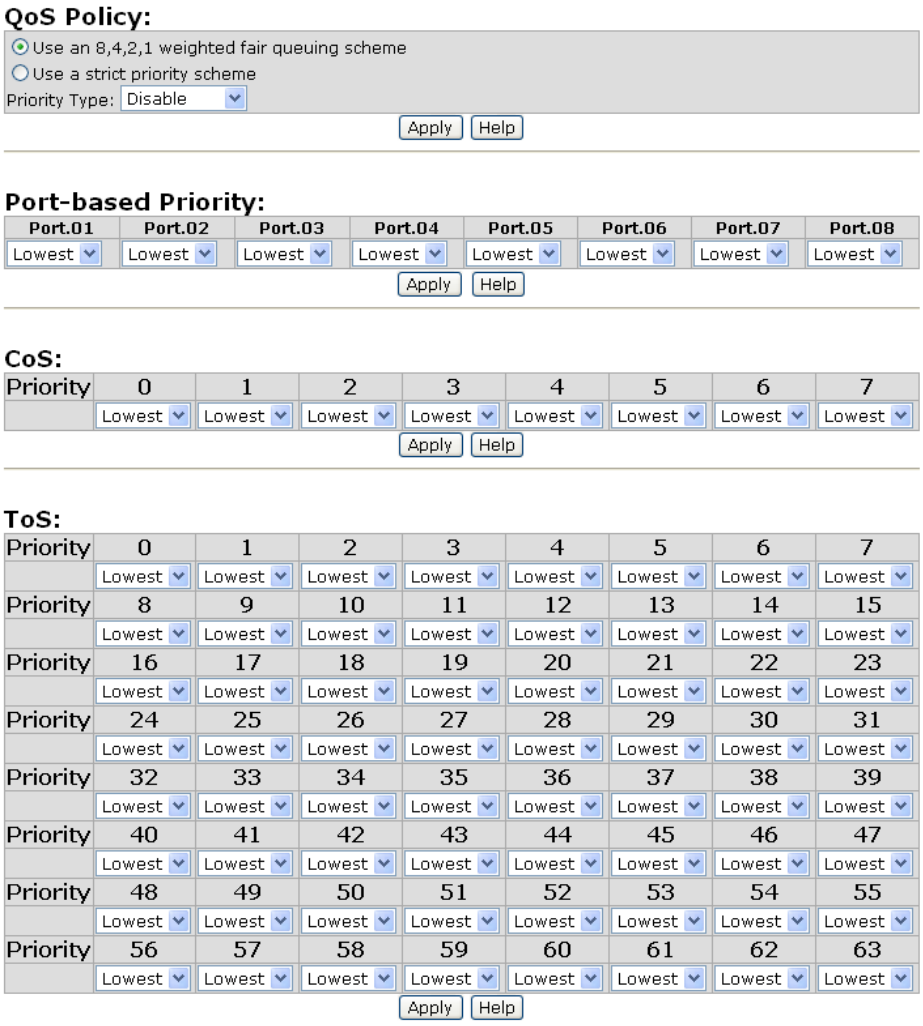
Select one of the two options to determine the QoS policy—

- An 8-4-2-1 weighted fair queuing scheme or a strict priority scheme. The 8-4-2-1 weighed fair queuing scheme designed with four queues to which allocate traffic in the rate of 8:4:2:1.
- A strict priority scheme, traffic will be identified according to the determined priority.

- **Qos Policy:** Select the QoS policy rule.
  - **Use an 8,4,2,1 weighted fair queuing scheme:** The switch will follow the ratio of 8:4:2:1 to process priority queues these are High, Middle, Low and Lowest. For example, while the system processing, 1 frame in the lowest queue, 2 frames in the low queue, 4 frames in the middle queue, and 8 frames in the high queue will be processed at the same time in accordance with the 8,4,2,1 policy rule.
  - **Use a strict priority scheme:** With this option selected, you have to click the pull-down menu labeled ‘Priority Type’.
  - **Priority Type:** There are five options;
    1. Port-based,
    2. TOS only.
    3. COS only,
    4. TOS first,
    5. COS first

These options are selected to enable or ‘Disable’. Disable means QoS function is not activated.

- Click Apply to have the configuration take effect.



QoS Configuration interface

►Port-based Priority

Configure a priority level for each port. Any packet received from a single port is sent to the 'Lowest' queue by default. This option allows users to change the priority level for each port respectively.

- **Port x:** Four priority levels, High, Middle, Low, and Lowest, are available.
- Click the Apply button to have the configuration take effect.

►COS Configuration

Configure this option to allocate an identified packet to different queues according to the packet's 3-bit 802.1p priority classification field that is embedded in the 4-byte 802.1q VLAN tag field. Before configuring this field, users have to select the option to **Use a strict priority scheme** and set the **Priority Type** to *COS only* or *COS first*.

- **Priority:** The 3-bit 802.1p priority values range from 0 to 7. Click the pull-down menu to specify the corresponding queue for the identified COS value (priority) to which the identified frame will be sent.

- Click the Apply button to have the configuration take effect.

►TOS Configuration

Configure this item to allocate the identified packet to different queues according to the packet's 6-bit DSCP (Differentiated Service Code Point) value inside the 1-byte ToS (Type of Service) field. The 6-bit DSCP value defines up to 64 priority values. Therefore, you can assign one of the four queues to each priority respectively.

- **Priority:** Click the pull-down menu to specify the corresponding queue for the identified TOS (DSCP) value to which the identified packet will be sent.

- Click the Apply button to have the configuration take effect.

X-Ring+

X-Ring provides a faster redundant recovery than the Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same. To configure an X-Ring group, the X-Ring option has to be enabled on each IGE 4T4GB-MX switch whose ports are connect to the ring network.

The two switches forming the last segment of a multi-device X-Ring group will automatically be designated as master switches. The link between the two master switches is called the backup path. Known as backup ports, the two ports on the backup path will be blocked. Also, network manager can identify which IGE-4T4GB-MX switch is the ring master by checking the LED indicator on the panel of the switch.

Other switches in the X-Ring group are normal working (forwarding) switches and both their two member ports are working (forwarding) ports. In the event of a network failure, the backup ports of the master switches (ring masters) will automatically become working (forwarding) ports to recover the network from the failure.

- **X-Ring+ Operation Mode:** Click the pull-down menu to configure the operation mode for X-Ring+ or disable the X-Ring+ function.

►X-Ring+ Mode

- **Ring ID:** Specify a number ranging from 0 to 99 for identifying a given ring group.
- **1st Ring Port:** One of the two IGE-4T4GB-MX ports connecting to the ring. Click the pull-down menu to select a port as the first ring port.
- **2nd Ring Port:** The other member port of IGE-4T4GB-MXE connecting to the ring. Select the pull-down menu to select a port as the second ring port.
- When finished, click the Apply button to ensure the configuration takes effect.

X-Ring+ Interface

►Legacy_Ring Mode

Setting the X-Ring+ Operation Mode to Legacy-Ring mode means the switch is configured as a backward compatible device, talking to switches running the original X-Ring technology. In this mode the IGE-4T4GB-MX cannot be a 'Ring Master' in the legacy X-Ring network.

- **1st Ring Port:** Select the pull-down menu to select a port as the first ring port.
- **2nd Ring Port:** Select the pull-down menu to select a port as the second ring port.
- Having configured X-Ring, click the Apply button to ensure the configuration takes effect.

Legacy-Ring Interface

[NOTE]

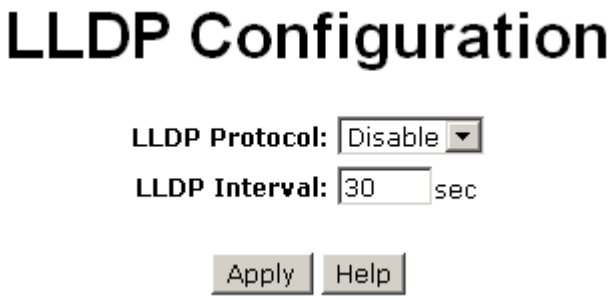
1. When the X-Ring+ function is enabled, the network manager must disable the RSTP function. The X-Ring+ and RSTP functions cannot work simultaneously on a switch.
2. Remember to execute the “Save Configuration”, otherwise the new configuration will be lost when the switch is powered off.

LLDP Configuration

The Link Layer Discovery Protocol (LLDP) is a one way protocol, specified in the IEEE 802.1AB standard which allows stations attached to the same IEEE 802 LAN to advertise their information to neighbors and store the information received from adjacent stations.

Receivers on the same physical LAN will store the information distributed via LLDP in a standard Management Information Base (MIB) where the information can be accessed by a Network Management System (NMS) using a protocol like the Simple Network Management Protocol (SNMP).
LLDP runs on all 802 media. The protocol runs over the data-link layer only, allowing two systems running different network layer protocols to learn about each other.

- **LLDP Protocol**: Select the pull-down menu to disable or enable the LLDP function.
- **LLDP Interval**: Type the value in seconds as the interval for the switch to advertise its information to other nodes.
- Click Apply to have the configuration take effect.



LLDP Interface

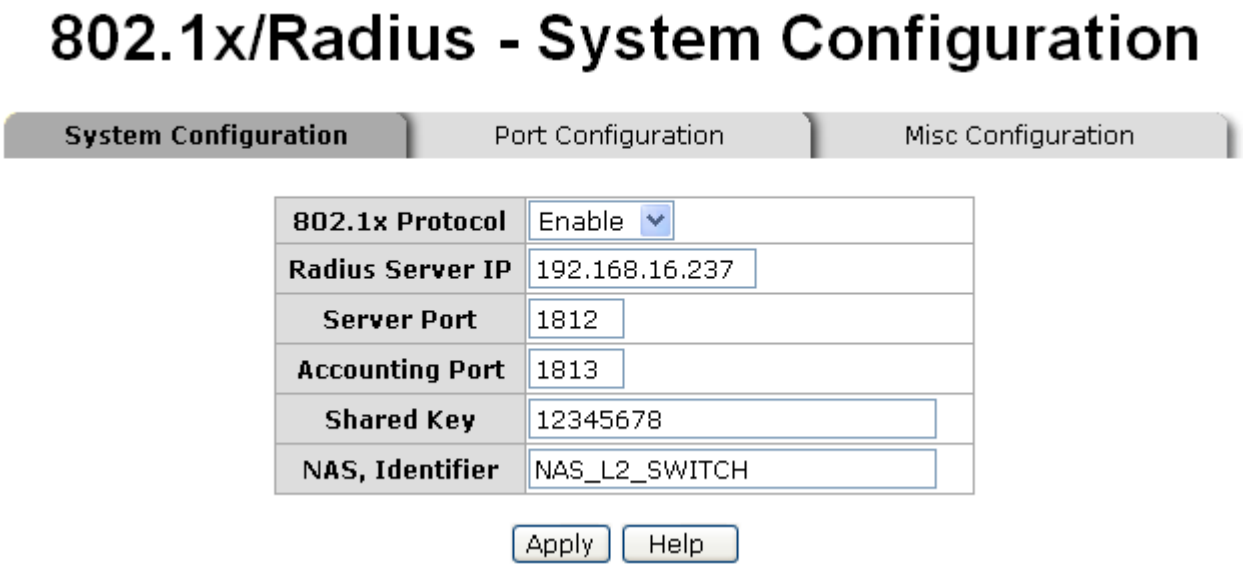
802.1X/Radius

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 or network until it provides authority, such as 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 of this function.

- **IEEE 802.1x Protocol:** Select the pull-down menu to enable or disable the 802.1x protocol on the switch.
- **Radius Server IP:** Assign the RADIUS Server IP address.
- **Server Port:** Set the UDP destination port for authentication requests to the specified RADIUS Server.
- **Accounting Port:** Set the UDP destination port for accounting requests to the specified RADIUS Server.
- **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.
- **NAS, Identifier:** Set the identifier for the RADIUS client.
- Select the Apply button to have the configuration take effect.

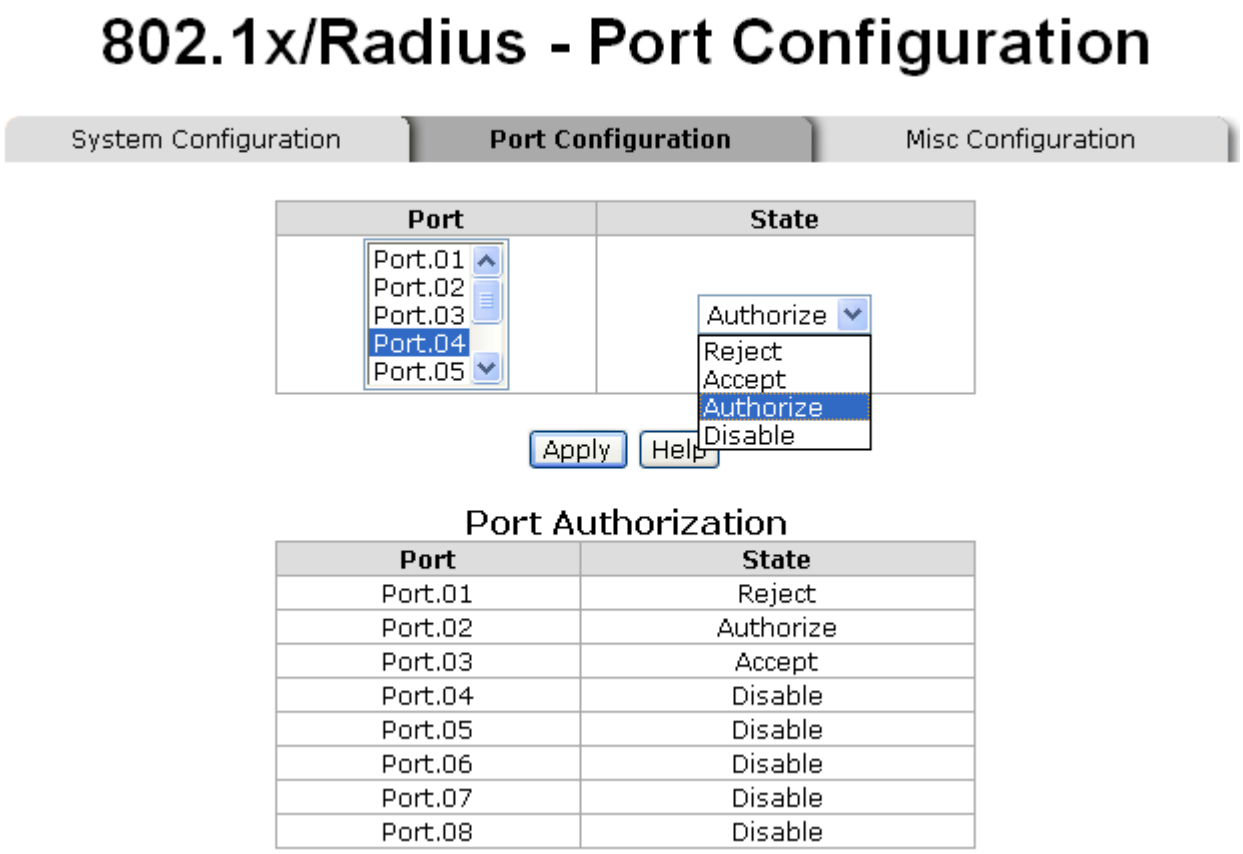


802.1x System Configuration interface

Port Configuration

You can configure the 802.1x authentication state for each port. The following states can be set, Disable, Accept, Reject, and Authorize.

- **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.
- **Authorize:** 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:** When disabled, the specified port works without complying with 802.1x protocol.
- Click Apply to have the configuration take effect.



802.1x Per Port Setting interface

Misc Configuration

802.1X uses three terms that are important to know.

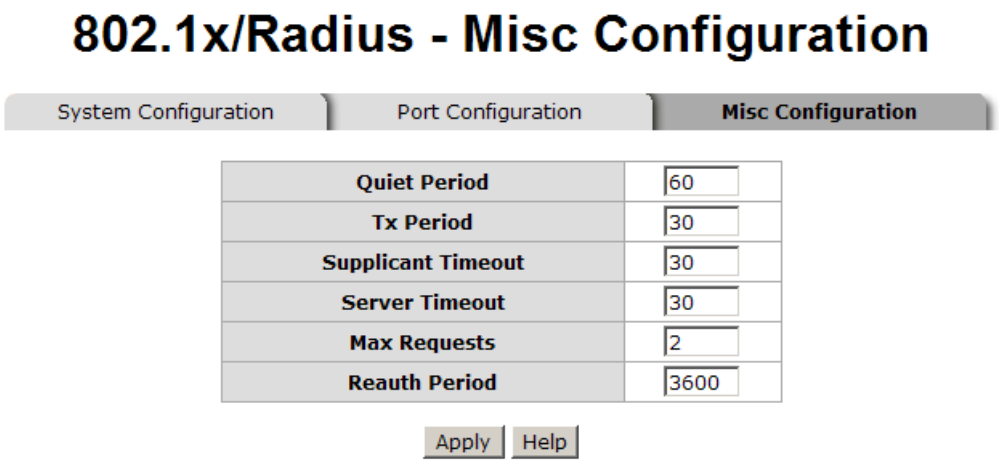
The user or client that wants to be authenticated is called a supplicant.

The actual server doing the authentication, typically a RADIUS server, is called the authentication server.

And the device in between, such as a wireless access point, is called the authenticator.

One of the key points of 802.1X is that the authenticator can be simple and dumb - all of the brains have to be in the supplicant and the authentication server. This makes 802.1X ideal for wireless access points, which are typically small and have little memory and processing power.

- **Quiet Period:** Set the period which the port doesn't try to acquire a supplicant.
- **TX Period:** Set the period the port waits for retransmitting the next EAPOL PDU during an authentication session.
- **Supplicant Timeout:** Set the period of time the switch waits for a supplicant response to an EAP request.
- **Server Timeout:** Set the period of time the switch waits for a server response to an authentication request.
- **Max Requests:** Set the number of authentication that must time-out before authentication fails and the authentication session ends.
- **Reauth Period:** Set the period of time the connected clients authenticated to be authenticated again.
- Click Apply to have the configuration take effect.



802.1x Misc Configuration interface

MAC Address Table

This menu option allows users to determine whether the incoming traffic passes through the particular ports or is blocked in accordance with the MAC address filtering table.

Static MAC Address

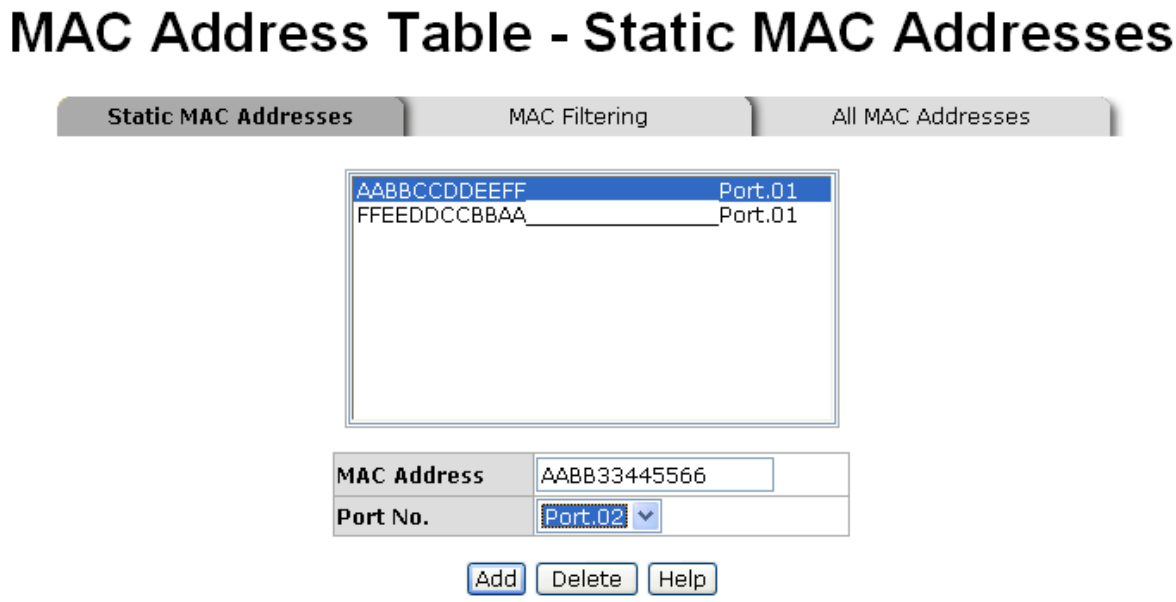
This list is a list of MAC addresses which are allowed to pass through the port.

You can add a static MAC address that 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 a powered-off device is active on the network again. Via this interface, you can add, modify and delete entries of static MAC address.

Add the Static MAC Address

You can add static MAC addresses up to 256 entries in the switch MAC table here.

- **MAC Address:** Enter entries of MAC address on the port that should permanently forward traffic, regardless of the device network activity.
- **Port No.:** Select the pull-down menu to select the port number.
- Click the Add button to finish adding the entry.
- If you want to delete the entry from the table, select the MAC address entry listed in the list and click the Delete button.



Static MAC Addresses interface

MAC Filtering

This table lists MAC addresses that are to be blocked by the IGE-4T4GB-MX switch port.

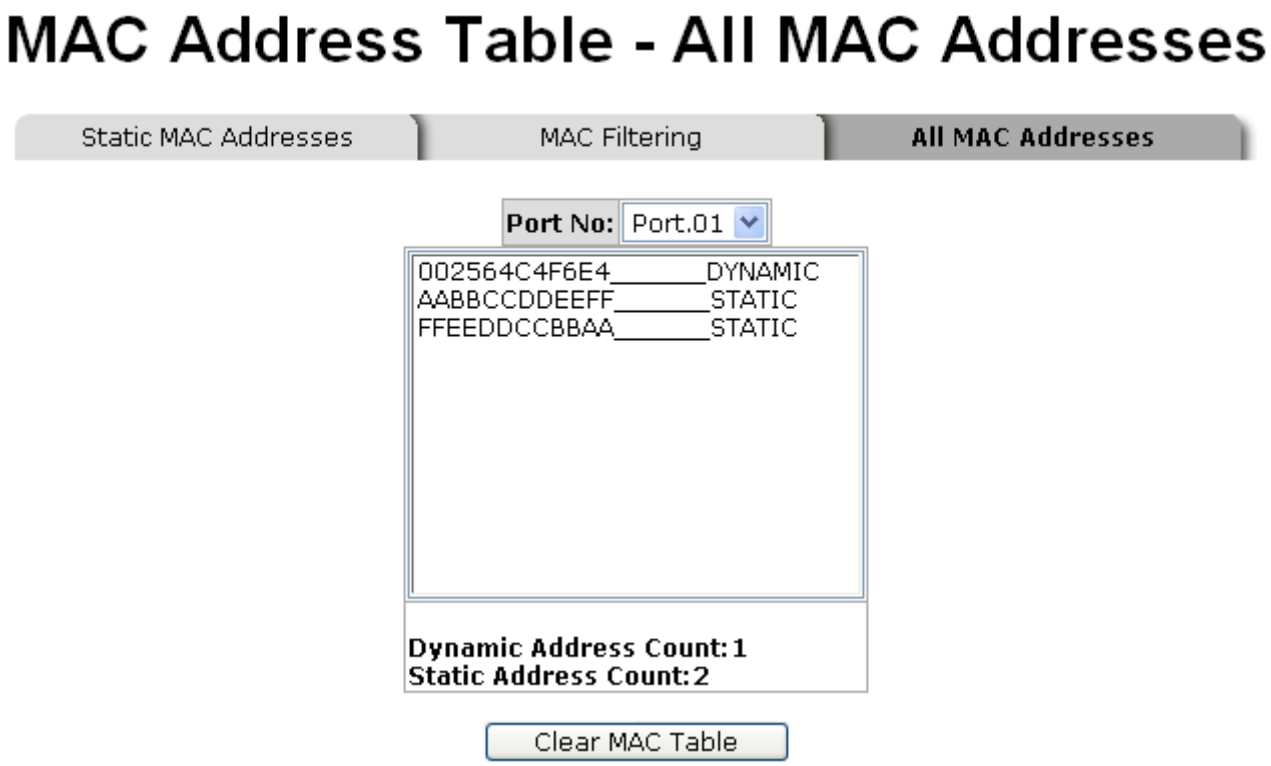
MAC Filtering interface

- **MAC Address:** Enter the MAC address up to 256 entries.
- Click the Add button.
- If you want to delete the MAC address from the table, select the MAC address entry and click the Delete button.

All MAC Addresses

This tab displays dynamic and static MAC addresses on each port.

- **Port No:** Select the pull-down menu to select a particular port to show its MAC address information.
- Select the Clear MAC Table button to clear the listed entries of the current MAC address information.



All MAC Address interface

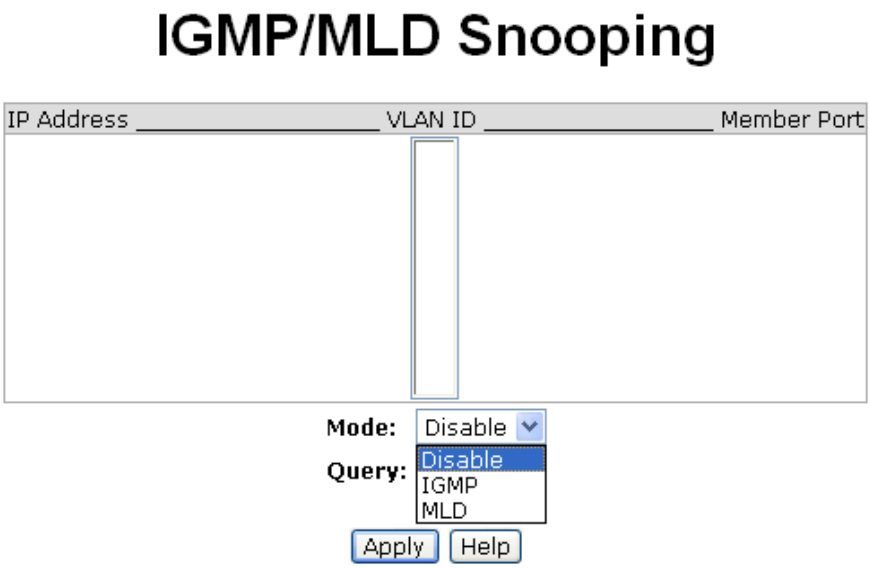
IGMP/MLD Snooping

IGMP is the protocol used by IPv4 systems to report their IP multicast group memberships to neighbouring multicast routers.

IGMP is used on IPv4 networks. To handle multicast management on IPv6 networks, Multicast Listener Discovery (MLD) is used in a similar way by IPv6 systems.

With the switch supporting IP multicast, you can enable IGMP/MLD protocol via this interface. Destination IP multicast addresses range from 224.0.0.0 to 239.255.255.255.

- **Mode:** Select the pull-down menu to specify the snooping mode, IGMP or MLD.
- **Query:** Select the pull-down menu to select the IGMP query functions including enable, disable and auto.
- Select ‘ Apply’ to enable the configuration take effect.



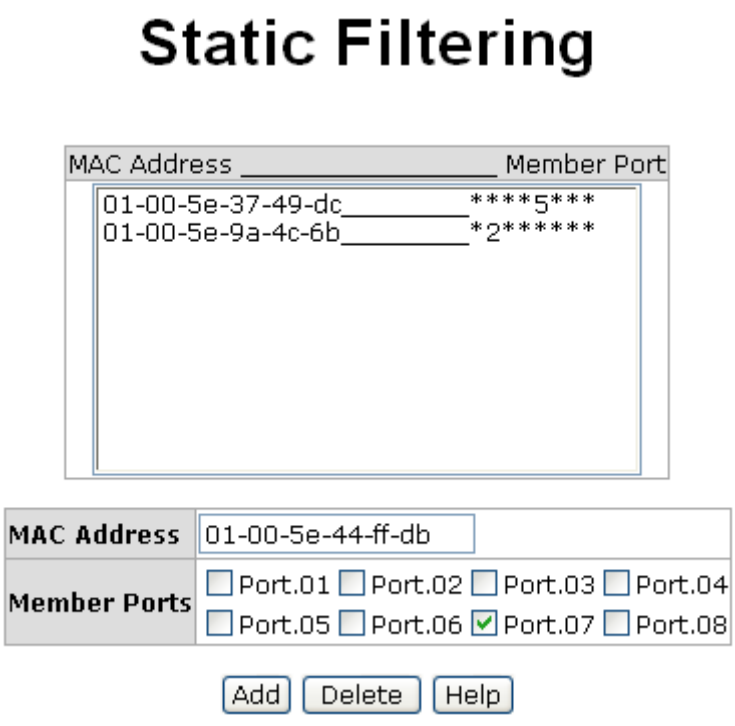
IGMP/MLD Snooping interface

Static Filtering

Multicasts are similar to broadcasts, they are sent to all end stations on a LAN or VLAN. Static filtering is the function for a network manager to configure a list of multicast groups by specifying the multicast MAC address and member ports for each entry.

A multicast MAC address is expressed in the format with a 24-bit prefix: ***01-00-5E*** (Hexadecimal). For example, a multicast MAC address like 01-00-5E-xx-xx-xx would be used for the multicast group from which end stations can receive multicast traffic via the connected ports which have been included in the specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to the registered end stations.

- **MAC Address**: Assign a multicast group MAC address in the format of 01-00-5E-xx-xx-xx.
- **Member Ports**: Select the option beside the port number to include them as the member ports in the specific multicast group MAC address.
- Select ‘Add’ to append a static filter of multicast group, or select the filter listed in the field and click Delete to remove it.



Static Filtering interface

Factory Default

Select the Reset button to reset the IGE-4T4GB-MX switch back to factory defaults. Before resetting the switch, you can tick the checkboxes to keep the current IP address and user name / password, this is useful if making changes remotely over the network.

Factory Default interface

Save Configuration

Save all changes you have made in the system. To ensure the configurations you have made will be implemented the next time you power on the switch, remember to click the Save button to save all configurations into the flash memory.

Save Configuration interface

System Reboot

Reboot the switch under software control. Click the Reboot button to restart the system.

System Reboot interface

Appendix A—Command Sets

Command Level

User EXEC	**E**	VLAN database	**V**
Privileged EXEC	**P**	Interface configuration	**I**
Global configuration	**G**		

Modes	Access Method	Prompt	Exit Method	About This Model
User EXEC	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	Enter the enable command while in user EXEC mode.	switch#	Enter **disable** to exit.	The privileged commands are the advanced mode. Use this mode to • Display advance function states • Save configurations
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 to be applied to your switch.
VLAN database	Enter the vlan database command while in privileged EXEC mode.	switch (vlan)#	To return to User EXEC mode, enter **exit**.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the interface command with a specific interface while in global configuration mode	switch (config-if)#	To return to the previous mode, enter **exit** or **end**.	Use this mode to configure parameters for the switch and Ethernet ports.

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 192.168.1.1 255.255.255.0 192.168.1.254**
ip dhcp	G	Enable DHCP client function of switch	switch(config)#**ip dhcp**
show ip	P	Show IP information of switch	switch#**show ip**
no ip dhcp	G	Disable DHCP client function of switch	switch(config)#**no ip dhcp**
reload	G	Halt and perform a cold restart	switch(config)#**reload** Do you want reboot the device now? **yes**
default	G	Restore to default	switch(config)#**default** Keep current IP address setting? **yes** Keep current user ID/password? **yes** Default setting restored. Do you want to reboot the system now? **yes**
admin username [Username]	G	Configure the administrator's login username. (maximum 10 words)	switch(config)#**admin username root**
admin password [Password]	G	Configure the password for the administrator account (maximum 10 words)	switch(config)#**admin password case**

show admin	**P**	Show administrator information	switch#**show admin**
dhcpserver enable	**G**	Enable DHCP Server	switch(config)#**dhcpserver enable**
dhcpserver lowip [Low IP]	**G**	Configure low IP address for IP pool	switch(config)#**dhcpserver lowip 192.168.1.100**
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 [sec.]	**G**	Configure lease time in seconds	switch(config)#**dhcpserver leasetime 1**
dhcpserver ipbinding [IP address]	**I**	Set static IP for DHCP clients by port	switch(config)#**interface fastEthernet 2** switch(config-if)#**dhcpserver ipbinding 192.168.1.1**
show dhcpserver configuration	**P**	Show configuration of DHCP server	switch#**show dhcpserver configuration**
show dhcpserver clients	**P**	Show client entries of DHCP server	switch#**show dhcpserver clients**
show dhcpserver ip-binding	**P**	Show IP-Binding information of DHCP server	switch#**show dhcpserver ip-binding**
no dhcpserver	**G**	Disable DHCP server function	switch(config)#**no dhcpserver**
security enable	**G**	Enable IP security function	switch(config)#**security enable**
security http	**G**	Enable IP security of HTTP server	switch(config)#**security http**
security telnet	**G**	Enable IP security of telnet server	switch(config)#**security telnet**
security ip [Index(1..10)] [IP Address]	**G**	Set the IP security list	switch(config)#**security ip 1 192.168.1.55**
show security	**P**	Show the information of IP security	switch#**show security**
no security	**G**	Disable IP security function	switch(config)#**no security**
no security http	**G**	Disable IP security of HTTP server	switch(config)#**no security http**
no security telnet	**G**	Disable IP security of telnet server	switch(config)#**no security telnet**

Port Commands Set

Commands	Level	Description	Example
interface fastEthernet [Portid]	G	Choose the port for modification.	switch(config)#**interface fastEthernet 2**
state [enable|disable]	I	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#**interface fastEthernet 2** config-if)#**state disable**
duplex [full | half]	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#**interface fastEthernet 2** switch(config-if)#**duplex full**
speed [10|100|1000|auto]	I	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet. The speed can't be set to 1000 if the port isn't a giga port.	switch(config)#**interface fastEthernet 2** switch(config-if)#**speed 100**
flowcontrol [enable|disable]	I	Configure flow control	switch(config-if)# **flowcontrol enable**
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	I	Set interface ingress limit frame	switch(config)#**interface**

broadcast-only		type to “only accept broadcast frame”	**fastEthernet 2** switch(config-if)#**bandwidth type broadcast-only**
bandwidth in [0/160/320/512/768/1024/1280/1536/2048/3072/4096/5120/8192/10240/20480/30720/40960/61440/81920/128000]	**I**	Set interface input bandwidth. Zero means no limit.	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth in 160**
bandwidth out [0/160/320/512/768/1024/1280/1536/2048/3072/4096/5120/8192/10240/20480/30720/40960/61440/81920/128000]		Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports. Zero means no limit.	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth out 160**
show bandwidth	**I**	Show interfaces bandwidth control	switch(config)#**interface fastEthernet 2** switch(config-if)#**show bandwidth**
alias [name]		Set port alias name	switch(config)#**interface fastEthernet 2** switch(config-if)#**alias 1111**
show interface configuration	**I**	show interface configuration status	switch(config)#**interface fastEthernet 2** switch(config-if)#**show interface configuration**
show interface status	**I**	show interface actual status	switch(config)#**interface fastEthernet 2** switch (config-if)#**show interface status**
show interface accounting	**I**	show interface statistic counter	switch(config)#**interface fastEthernet 2** switch (config-if)#**show interface accounting**
no accounting	**I**	Clear interface accounting information	switch(config)#**interface fastEthernet 2** switch(config-if)#**no accounting**

Trunk Commands Set

Commands	Level	Description	Example
aggregator priority [1~65535]	G	Set port group system priority	switch(config)#**aggregator priority 22**
aggregator group [GroupID] [Port-list] **lacp** **workp** [Workport]	G	Assign a trunk group with LACP active. [GroupID]: 1~3 [Port-list]: Member port list. This parameter could be a port range (ex.1-4) or a port list separate by a comma (ex.2, 3, 6). [Workport]: The amount of work ports. This value could not be less than zero or greater than the amount of member ports.	switch(config)#**aggregator group 1 1-4 lacp workp 2** or switch(config)#**aggregator group 2 1,4,3 lacp workp 3**
aggregator activityport [Group ID] [Port Numbers]	G	Set activity port	switch(config)#**aggregator activityport 1 2**
aggregator group [GroupID] [Port-list] **nolacp**	G	Assign a static trunk group. [GroupID] :1~3 [Port-list]: Member port list. This parameter could be a port range (ex.1-4) or a port list separate by a comma (ex.2, 3, 6).	switch(config)#**aggregator group 1 2-4 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 aggregator lacp 1**
no aggregator group [GroupID]	G	Remove a trunk group	switch(config)#**no aggregator group 1**

DMI Commands Set

Commands	Level	Description	Example
show dmi	I	Display DMI status for Mini-GBIC ports	switch(config)#**interface fastEthernet 7** switch(config-if)#**show dmi**
dmi temperature [HighAlarm | HighWarning | LowWarning | LowAlarm] [E-mail | ShutDown]	I	Set reactions for port temperature monitoring	switch(config)#**interface fastEthernet 7** switch(config-if)#**dmi temperature highalarm shutdown**
dmi voltage [HighAlarm | HighWarning | LowWarning | LowAlarm] [E-mail | ShutDown]	I	Set reactions for port voltage monitoring	switch(config)#**interface fastEthernet 7** switch(config-if)#**dmi voltage highwarning e-mail**
dmi current [HighAlarm | HighWarning | LowWarning | LowAlarm] [E-mail | ShutDown]	I	Set reactions for port current monitoring	switch(config)#**interface fastEthernet 7** switch(config-if)#**dmi current highalarm shutdown**
dmi txpwr [HighAlarm | HighWarning | LowWarning | LowAlarm] [E-mail | ShutDown]	I	Set reactions for port transmitting power monitoring	switch(config)#**interface fastEthernet 7** switch(config-if)#**dmi txpwr highwarning e-mail**
dmi rxpwr [HighAlarm | HighWarning | LowWarning | LowAlarm] [E-mail | ShutDown]	I	Set reactions for port receiving power monitoring	switch(config)#**interface fastEthernet 7** switch(config-if)#**dmi rxpwr highalarm shutdown**

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 VLAN	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 2**
no vlan group [GroupID]	**V**	Delete port base group ID	switch(vlan)#**no vlan group 2**
IEEE 802.1Q VLAN			
vlan 8021q mnt-vid [VID]	**V**	Configure management VID (0 means disabled)	switch(vlan)#**vlan 8021q mnt-vid 22** Is Management VLAN ID equal to Management Port VLAN ID?**yes**
vlan 8021q name [GroupName] **vid** [VID]	**V**	Change the name of VLAN group. If the group doesn'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 an 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 22**
vlan 8021q port [PortNumber] **trunk-link tag** [TaggedVID List]	**V**	Assign a trunk link for VLAN by port. If the port belongs to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 trunk-link tag 2,3,6,99** or switch(vlan)#**vlan 8021q port 3 trunk-link tag 3-20**

vlan 8021q port [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	**V**	Assign a hybrid link for VLAN by port. If the port belongs to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q port 3 hybrid-link untag 5 tag 6-8**
vlan 8021q trunk [PortNumber] **access-link untag** [UntaggedVID]	**V**	Assign an 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 2**
no vlan group [GroupID]	**V**	Delete the 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 parameters	switch(config)#**spanning-tree priority 4096**
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 for Spanning Tree Protocol (STP) calculations. In the event of looping, the spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-cost 20**
stp-path-priority [0-240]	**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 16**
stp-admin-p2p [Auto|True|False]	**I**	Configure 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**	Configure 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**	Configure Admin NonSTP of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-non-stp False**
show spanning-tree	**E**	Display a summary of the spanning-tree states.	switch>**show spanning-tree**
no spanning-tree	**G**	Disable spanning-tree.	switch(config)#**no spanning-tree**

QOS Commands Set

Commands	Level	Description	Example
qos policy [weighted-fair|strict]	G	Select QOS policy scheduling	switch(config)#**qos policy weighted-fair**
qos prioritytype [port-based|cos-only|tos-only|cos-first|tos-first]	G	Setting of QOS priority type	switch(config)#**qos prioritytype port-base**
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	Display 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 enable	G	Set IGMP query to force mode	switch(config)#**igmp query enable**
igmp unregister [flooding/blocking]	G	Configure IGMP unregister stream	switch(config)#**igmp unregister flooding**
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(config)#**no igmp query**

MLD Commands Set

Commands	Level	Description	Example
mld enable	G	Enable MLD function	switch(config)#**mld enable**
mld query auto	G	Configure MLD query mode	switch(config)# **mld query auto**
mld query enable	G	Set MLD query to force mode	switch(config)# **mld query enable**
mld unregister [flooding/blocking]	G	Configure MLD unregister stream	switch(config)#**igmp unregister flooding**
show mld configuration	P	Show MLD configuration	switch#**show mld configuration**
show mld multi	P	Show MLD multicast table	switch#**show mld multi**
no mld	G	Disable MLD snooping function	switch(config)#**no mld**
no mld query	G	Disable MLD query function	switch#**no mld query**

Multicast Static Filtering Table Commands Set

Commands	Level	Description	Example
multicast-filtering [IP-Addr]	I	Add entries for the multicast filtering.	switch(config)#**interface fastEthernet 2** switch(config-if)# **multicast-filtering 01-00-5e-00-00-01** or switch(config-if)# **multicast-filtering 33-33-00-00-00-01**
no multicast-filtering [IP-Addr]	I	Remove entries for the multicast filtering.	switch(config)#**interface fastEthernet 2** switch(config-if)#**no multicast-filtering 01-00-5e-00-00-01** or switch(config-if)# **no multicast-filtering 33-33-00-00-00-01**

MAC / Filter Table Commands Set

Commands	Level	Description	Example
mac-address-table static hwaddr [MAC]	I	Configure the MAC address table (static).	switch(config)#**interface fastEthernet 2** switch(config-if)#**mac-address-table static hwaddr 000012345678**
mac-address-table filter hwaddr [MAC]	G	Configure the MAC address table (filter)	switch(config)#**mac-address-table filter hwaddr 000012348678**
show mac-address-table	P	Show the table with all MAC addresses	switch#**show mac-address-table**
show mac-address-table static	P	Show the table with static MAC addresses	switch#**show mac-address-table static**
show mac-address-table filter	P	Show entries of the filter MAC address table.	switch#**show mac-address-table filter**
no mac-address-table static hwaddr [MAC]	I	Remove an entry from the MAC address table (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 from the MAC address table (filter)	switch(config)#**no mac-address-table filter hwaddr 000012348678**
no mac-address-table	G	Remove dynamic entries from the 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**
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 can be empty.	switch(config)#**snmpv3 user test01 group G1 password AuthPW PrivPW**
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] [Notify View Name]	G	Configure the access table of the SNMPV3 agent	switch(config)#**snmpv3 access context-name Test group G1 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 the 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 host 192.168.1.50**
no snmpv3 user [User Name]	**G**	Remove the specified user of the SNMPv3 agent.	switch(config)#**no snmpv3 user test01**
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] [Notify View Name]	**G**	Remove the specified access table of the SNMPv3 agent.	switch(config)#**no snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1**
no snmpv3 mibview view [View Name] **Type** [Excluded|Included] **sub-oid** [OID]	**G**	Remove the 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|TX|Both]	**I**	Configure the source port of monitor function	switch(config)#**interface fastEthernet 2** switch(config-if)#**monitor RX**
monitor rx [Port ID]	**G**	Set RX destination port of monitor function	switch(config)#**monitor rx 3**
monitor tx [Port ID]	**G**	Set TX destination port of monitor function	switch(config)#**monitor tx 4**
show monitor	**P**	Show port monitor information	switch#**show monitor**
show monitor	**I**	Show port monitor information	switch(config)#**interface fastEthernet 2** switch(config-if)#**show monitor**
no monitor	**I**	Disable source port of monitor function	switch(config)#**interface fastEthernet 2** switch(config-if)#**no monitor**

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 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 global configuration command to change the radius server port	switch(config)# **8021x system serverport 1815**
8021x system accountport [port ID]	G	Use the global configuration command to change the accounting port	switch(config)# **8021x system accountport 1816**
8021x system sharedkey [ID]	G	Use the global configuration command to change the shared key value.	switch(config)# **8021x system sharedkey 123456**
8021x system nasid [words]	G	Use the global configuration command to change the NAS ID	switch(config)# **8021x system nasid test1**
8021x misc quietperiod [sec.]	G	Use the global configuration command to specify the quiet period of the switch in seconds	switch(config)# **8021x misc quietperiod 10**
8021x misc txperiod [sec.]	G	Use the global configuration command to set the TX period in seconds.	switch(config)# **8021x misc txperiod 5**
8021x misc supptimeout [sec.]	G	Use the global configuration command to set the supplicant timeout in seconds.	switch(config)# **8021x misc supptimeout 20**
8021x misc servertimeout [sec.]	G	Use the global configuration command to set the server timeout in seconds.	switch(config)#**8021x misc servertimeout 20**
8021x misc maxrequest [number]	G	Use the global configuration command to set the maximum requests.	switch(config)# **8021x misc maxrequest 3**
8021x misc reauthperiod [sec.]	G	Use the global configuration command to set the reauthorized period in seconds.	switch(config)# **8021x misc reauthperiod 3000**
8021x portstate [disable | reject | accept | authorize]	I	Use the configuration command to set the state of the selected port.	switch(config)#**interface fastethernet 3** switch(config-if)#**8021x portstate accept**

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

TFTP Commands Set

Commands	Level	Description	Defaults Example
backup flash:backup_cfg	**G**	Save configuration to the TFTP server. IP address of the TFTP server and the file name of the image are required.	switch(config)#**backup flash:backup_cfg**
restore flash:restore_cfg	**G**	Get configuration from the TFTP server. IP address of the TFTP server and the file name of the image are required.	switch(config)#**restore flash:restore_cfg**
upgrade flash:upgrade_fw	**G**	Upgrade firmware via TFTP. IP address of the TFTP server and the file name of the image are required.	switch(config)#**upgrade flash:upgrade_fw**

SystemLog, SMTP and Event Commands Set

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

[IP address]		IP	**192.168.1.5**
smtp sender	**G**	Send the sender identification when an event occurs	switch(config)#**smtp sender test01**
smtp authentication	**G**	Enable SMTP authentication	switch(config)#**smtp authentication**
smtp account [account]	**G**	Configure authentication account	switch(config)#**smtp account John**
smtp password password: [password] **confirm password:** [password]	**G**	Configure authentication password	switch(config)#**smtp password** password: **1234** confirm password: **1234**
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 the event type of Authentication failure	switch(config)#**event authentication-failure 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 [Systemlog|SMTP|Both]	**G**	Disable cold start event type	switch(config)#**no event device-cold-start both**
no event authentication-failure [Systemlog|SMTP|Both]	**G**	Disable the event type of Authentication failure	switch(config)#**no event authentication-failure both**
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**

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 the 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 the SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# **sntp daylight-period 20110101-01:01 20110202-01:01**
sntp daylight-offset [Minute]	G	Set offset of daylight saving time. If SNTP is inactive, this command can't be applied.	switch(config)#**sntp daylight-offset 3**
sntp ip [IP]	G	Set the SNTP server IP. If SNTP is inactive, this command can't be applied.	switch(config)#**sntp ip 192.168.1.1**
sntp timezone [Timezone]	G	Set timezone index. Use the "show sntp timzezone" command to get more information of index number	switch(config)#**sntp timezone 22**
sntp sync-interval [Secs]	G	Set synchronization interval in seconds	switch(config)# **sntp sync-interval 1024**
show sntp	P	Show SNTP information	switch#**show sntp**
show sntp timezone	P	Show index number of the time zone list	switch#**show sntp timezone**
no sntp	G	Disable SNTP	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+ mode [X-Ring+|Legacy-Ring]	G	Set X-ring+ in X-ring+ mode	switch(config)#**xring+ mode x-ring+**
xring+ create [Ring ID] **port** [1st Ring Port] **port** [2nd Ring Port] **name** [name string]	G	Create X-Ring+ Ring entry	switch(config)#**xring+ create 1 port 1 port 2 name test1**
xring+ create [Ring ID] **port** [1st Ring Port] **ring** [2nd Ring ID] **name** [name string]	G	Create X-Ring+ Coupling entry	switch(config)#**xring+ create 2 port 3 ring 1 name test2**
xring+ delete [Ring ID]	G	Delete X-Ring+ entry	switch(config)#**xring+ delete 1**
xring+ show	G	Show X-Ring+ configuration	switch(config)#**xring+ show**
Xring+ legacyringport [1st Ring Port] [2nd Ring ID]	G	Configure Legacy-Ring $1^{st}/2^{nd}$ Ring port	switch(config)# **xring+ legacyringport 1 2**
show xring+	P	Show X-Ring+ configuration	switch#**show xring+**

Fault Relay Alarm Commands Set

Commands	Level	Description	Example
faultrelay power [number] [enable/disable]	G	Enable/Disable Power Relay Alarm function	switch(config)#**faultrelay power 1 enable**
faultrelay [enable/disable]	I	Enable/Disable Port Fault Relay Alarm function	switch(config)#**interface fastEthernet 1** switch(config-if)#**faultrelay enable**
show faultrelay	P	Show Fault Relay Alarm setting	switch#**show faultrelay**

LLDP Commands Set

Commands	Level	Description	Example
lldp enable	**G**	Enable LLDP function	switch(config)# **lldp enable**
lldp interval [TIME sec]	**G**	Configure LLDP interval in seconds	switch(config)#**lldp interval 1800**
show lldp	**P**	Show LLDP information	switch#**show lldp**
no lldp	**G**	Disable LLDP	switch(config)#**no lldp**

IPv6 Commands Set

Commands	Level	Description	Example
show ipv6	**P**	Show ipv6 and ND cache information	switch#**show ipv6**
ping6 [ipv6 address]	**G**	Start ICMPv6 ping	switch(config)#**ping6 ff02::1**
show ndclear	**G**	Clear neighbor discovery cache	switch#**show ndclear**

Troubleshooting

- Verify that you are using the right power cord/adapter. Don't use a power adapter with a DC output higher than the rated voltage of the switch (48vdc). Or it will burn this switch down.

- Select the proper network cable to build your network.

- **Diagnosing LED Indicators:** The Ethernet switch can be easily monitored through the LED indicators on the front panel, which describes common problems you may encounter and where you can find possible solutions, to assist in identifying problems.

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

- **System not working but LEDS okay -** If the LED indicators are normal while the cables are correctly connected but the system is still not working, please check your system's Ethernet devices' configuration or status, for example port configuration settings (negotiation, flow control) and the attached devices IP Addresses.

- **Ethernet Loops** – in the event of an Ethernet loop occurring, immediately remove one of the switch ring cables to manually break the loop. Then check each and every switch on the ring to ensure they are set for 'X-Ring' operation, if using dual homing or ring coupling, check the configuration for the head end switches, SRTP configuration and ring coupling