



TRENDNET[®]



User's Guide

TEG-S2620is

H/W: V1

Federal Communication Commission Interference Statement

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

European Union Notice:

Radio products with the CE marking comply with the R&TTE Directive (1999/5/EC), the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms:

- EN 60950 Product Safety
- EN 300 328 Technical requirement for radio equipment
- EN 301 489-1/-17 General EMC requirements for radio equipment

Trademark recognition

All product names used in this manual are the properties of their respective owners and are acknowledged.

1. INTRODUCTION	1
Features.....	2
Package Contents.....	2
Ethernet Switching Technology	3
2. HARDWARE DESCRIPTION	5
Physical Dimension.....	5
Front Panel	5
LED Indicators	6
Rear Panel.....	7
Desktop Installation.....	7
Rack-mounted Installation	8
3. NETWORK APPLICATION	11
4. CONSOLE MANAGEMENT	14
Login in the Console Interface	14
Main Menu	15
Function Description	17
Status and Counters	17
Port Status	17
Port Counters	18
System Information	19
Switch Static Configuration	21
Administration Configuration	21
Port Configuration	25
Trunk Configuration	26
Port Mirroring Configuration	27
VLAN Configuration	29
Priority Configuration	35
MAC Address Configuration	36
Misc Configuration	39
Protocol Related Configuration	42

STP	42
SNMP	45
LACP	50
IGMP/GVRP	54
802.1x Configuration	55
System Reset Configuration	59
Factory Default	59
System Reboot	60
TFTP Configuration	60
X-modem Upgrade	64
5. WEB-BASED MANAGEMENT	66
About Web-based Management	66
Preparing for Web Management	66
Online Help	67
System Login	67
Port status.....	67
View the Port Information	69
Port Statistics	69
Administrator.....	70
IP Address	71
Switch Setting	72
Basic Switch Settings	72
Advanced Setting	73
Misc Config	74
Console Port Information	78
Port Controls	78
Trunking	80
Aggregator setting	80
Aggregator Information	81
State Activity	82
Forwarding and Filtering	84
IGMP Snooping	84

Static MAC Address	85
MAC filtering	86
VLAN configuration	87
Port-based VLAN	88
802.1Q VLAN	90
Spanning Tree	94
System Configuration	95
Per Port Configuration	95
Port Mirroring	96
SNMP Management	97
Security Manager	99
802.1X	100
System Configuration	100
Per port Configuration	101
Misc Configuration	102
TFTP Update Firmware	102
Configuration Backup.....	103
TFTP Restore Configuration	103
TFTP Backup Configuration	104
Factory Default	104
System Reboot	105
Panel List.....	105
IP Stacking.....	106
6. TROUBLESHOOTING	109
7. TECHNICAL SPECIFICATION	111
APPENDIX	113
Console Port Pin Assignments	113
Cables.....	114
100BASE-TX/10BASE-T Pin Assignments	114
LIMITED WARRANTY	116

1. Introduction

Welcome to the World of Network Switching. In the modern business society, communication and information sharing are fundamental to our life. And computer networks have proven to be one of the fastest ways of communication.

TEG-S2620is is a multi-port Switch that can be used to build high-performance switched workgroup networks. This switch is a store-and-forward device that offers low latency for high-speed networking. The Switch is targeted at workgroup, department or backbone computing environment.



Figure 1-1. TEG-S2620is

TEG-S2620is features a “store-and-forward” switching scheme. This allows the switch to auto-learn and store source address in an 8K-entry MAC address table.

MDI (Medium Dependent Interface) Port is also called an "uplink port". The MDI port does not cross the transmit and receive lines, which is done by the regular ports (MDI-X ports) that connect to end stations. In general, **MDI** means connecting to another Hub or Switch while **MDIX** means connecting to a workstation or PC. Therefore, **Auto MDI/MDIX** means that you can connect to another Switch or workstation without changing non-crossover or crossover cabling.

TEG-S2620is has 24 auto-sensing 10/100Base-TX RJ-45 ports and 2 auto detect Gigabit ports for higher connection speed.

Features

- Confirms to IEEE802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit fiber
- 24 10/100 TX plus 2 Gigabit copper/Mini GBIC slot stackable intelligent switch
- High back-plane bandwidth 8.8Gbps
- 8K-entry MAC address table
- Management via single IP address
- IGMP support for Multi Media application
- Port mirror supported
- Support Port bandwidth control
- Supports GVRP function
- DHCP client supported
- Support Port Based VLAN /802 .1Q VLAN
- IEEE802.3x Flow control
 - Flow control for full duplex
 - Backpressure for half duplex
- Support IEEE802.3ad Port trunk with LACP
- Broadcast storm filter supported
- Support IEEE 802.1p class of service
- Support Port security
- IEEE 802.1d Spanning tree protocol supported
- Auto detect Gigabit copper and MINI GBIC
- Support IEEE 802.1x user authentication

Package Contents

Unpack the contents of the TEG-S2620is and verify them against the checklist below.

- TEG-S2620is

- Power Cord
- Four Rubber Feet
- RS-232 cable
- Rack-mounted Kit
- User Guide (CD-ROM)

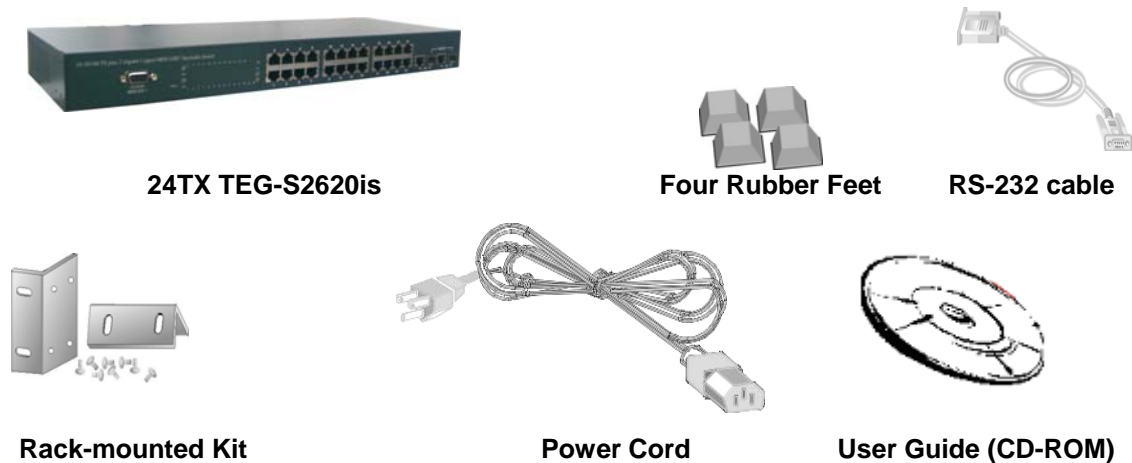


Figure 1-2. Package Contents

Compare the contents of your TEG-S2620is package with the standard checklist above. If any item is missing or damaged, please contact your local dealer for service.

Ethernet Switching Technology

Ethernet Switching Technology dramatically boosted the total bandwidth of a network, eliminated congestion problems inherent with CSMA/CD (Carrier Sense multiple access with Collision Detection) protocol, and greatly reduced unnecessary transmissions.

This revolutionized networking. First, by allowing two-way, simultaneous transmissions over the same port (Full-duplex), which essentially doubled the bandwidth. Second, by reducing the collision domain to a single switch-port, which eliminated the need for carrier sensing. Third, by using the store-and-forward technology's approach of inspecting each packet to intercept

corrupt or redundant data, switching eliminated unnecessary transmission that slow the network. By employing address learning, which replaced the inefficient receiving port.

Auto-negotiation regulates the speed and duplex of each port, based on the capability of both devices. Flow-control allows transmission from a 100Mbps node to a 10Mbps node without loss of data. Auto-negotiation and flow-control may require disablement for some networking operations involves legacy equipment. Disabling the auto-negotiation is accomplished by fixing the speed or duplex of a port.

Ethernet Switching Technology supplied higher performance at costs lower than other solutions. Wider bandwidth, no congestion, and the reduction in traffic is why switching is replacing expensive routers and inefficient hubs as the ultimate networking solution. Switching brought a whole new way of thinking to networking.

2. Hardware Description

This Section mainly describes the hardware of the TEG-S2620is, and gives a physical and functional overview of this Module Switch.

Physical Dimension

TEG-S2620is's physical dimensions is **440mm x 161mm x 44mm (L x W x H)**.

Front Panel

The Front Panel of the TEG-S2620is consists of 24x 10/100Base-TX RJ-45 ports (Auto MDI/MDIX) and 2 auto detect Giga port which could be Copper Gigabit port or Mini Gigabit Fiber module (optional). The LED Indicators are also located on the front panel of the Switch.

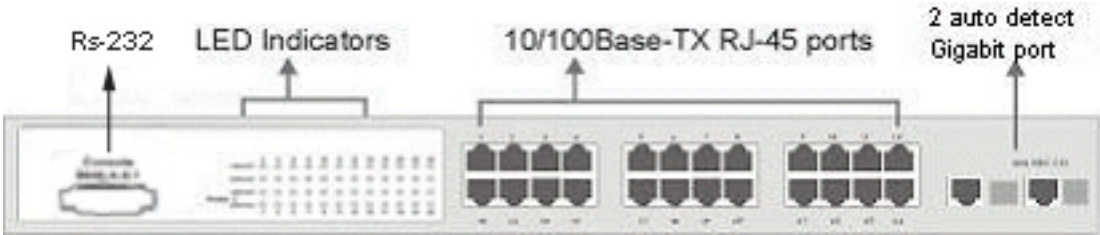


Figure 2-1. The Front panel of TEG-S2620is

RJ-45 Ports (Auto MDI/MDIX): 24x 10/100 N-way auto-sensing for 10Base-T or 100Base-TX connections.

[In general, **MDI** means connecting to another Hub or Switch while **MDIX** means connecting to a workstation or PC. Therefore, **Auto MDI/MDIX** means that you can connect to another Switch or workstation without changing non-crossover or crossover cabling.]

2 Gigabit ports: 2 auto-detect Gigabit ports—UTP or fiber. Gigabit fiber is the mini GBIC module that is optional.

[Note] When you are using the Gigabit copper port or Mini GBIC port, only one of them will work, ex: when Gigabit copper port is connecting, then Mini GBIC is disabling.

LED Indicators

The LED Indicators gives real-time information of systematic operation status. The following table provides descriptions of LED status and their meaning.

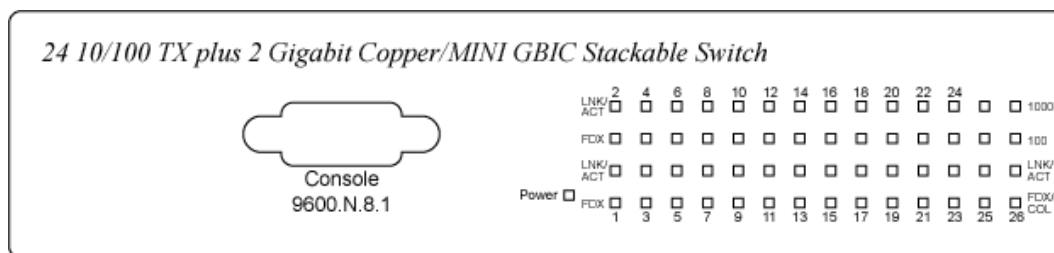


Figure 2-2. LED indicators

LED	Status	Description
Power	Green	Power On
	Off	Power is not connected
LNK/ACT	Green	The port is connecting with the device.
	Blink	The port is receiving or transmitting data.
	Off	No device attached.
FDX	Orange	The port is operating in Full-duplex mode.
	Off	In half-duplex mode

1000(Gigabit port) #25, #26 port	Green	In 1000Mbps connection speed
100(Gigabit port) #25, #26 port	Orange	In 100Mbps connection speed
LNK/ACT (Gigabit port) #25, #26 port	Green	The port is connecting with the device.
	Blink	The port is receiving or transmitting data.
	Off	No device attached
FDX/COL (Gigabit port) #25, #26 port	Orange	The port is operating in Full-duplex mode
	Blink	Collision of Packets occurs in the port
	Off	In half-duplex mode

Table 2-1. The Description of LED Indicators

Rear Panel

The 3-pronged power plug is located at the rear Panel of the TEG-S2620is as shown in Figure 2-3. The Switch will work with AC in the range 100-240V AC, 50-60Hz.



Figure 2-3. The Rear Panel of TEG-S2620is

Desktop Installation

Set the Switch on a sufficiently large flat space with a power outlet nearby. The surface where you put your Switch should be clean, smooth, level and sturdy. Make sure there is enough clearance around the Switch to allow attachment of

cables, power cord and allow air circulation.

Attaching Rubber Feet

- A. Make sure mounting surface on the bottom of the Switch is grease and dust free.
- B. Remove adhesive backing from your Rubber Feet.
- C. Apply the Rubber Feet to each corner on the bottom of the Switch. These footpads can prevent the Switch from shock/vibration.

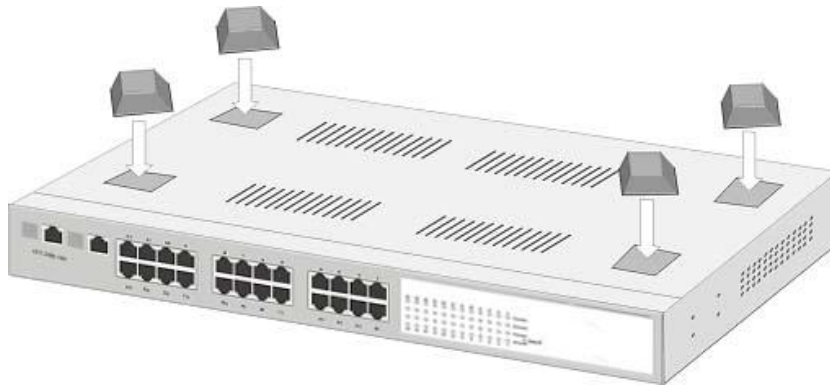


Figure 2-4. Attaching Rubber Feet to each corner on the bottom of the Switch

Rack-mounted Installation

The TEG-S2620is come with a rack-mounted kit and can be mounted in an EIA standard size, 19-inch Rack. The Switch can be placed in a wiring closet with other equipment.

Perform the following steps to rack mount the switch:

- A. Position one bracket to align with the holes on one side of the switch and secure it with the smaller bracket screws. Then attach the remaining bracket to the other side of the Switch.



Figure 2-4. Attach mounting brackets with screws

- B. After attached mounting brackets, position the TEG-S2620is in the rack by lining up the holes in the brackets with the appropriate holes on the rack. Secure the Switch to the rack with a screwdriver and the rack-mounting screws.

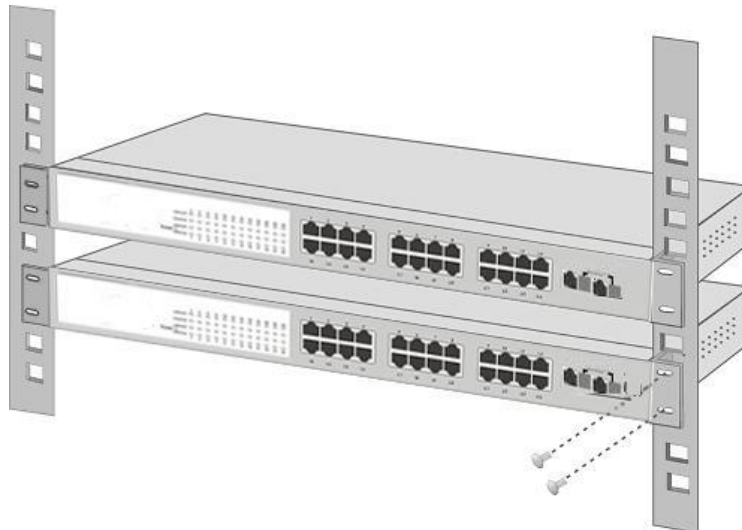


Figure 2-5. Mount the Switch in 19" Rack

Note: For proper ventilation, allow about at least 4 inches (10 cm) of clearance on the front and 3.4 inches (8 cm) on the back of the Switch. This is especially important for enclosed rack installation.

Power On

Connect the power cord to the power socket on the rear panel of the Switch. The other side of power cord connects to the power outlet. The internal power supply

of the Switch works with voltage range of AC in the 100-240VAC, frequency 50~60Hz. Check the power indicator on the front panel to see if power is properly supplied.

3. Network Application

This section provides you a few samples of network topology in which the Switch is used. In general, the TEG-S2620is is designed as a segment switch. That is, with its large address table (8k MAC address) and high performance, it is ideal for interconnecting networking segments.

PC, workstations, and servers can communicate each other by directly connecting with TEG-S2620is. The switch automatically learns nodes address, which are subsequently used to filter and forward all traffic based on the destination address.

By using Uplink port, the Switch can connect with another switch or hub to interconnect other small-switched workgroups to form a larger switched network. Meanwhile, you can also use fiber ports to connect switches. The distance between two switches via fiber cable can be up to 550 m (multi-mode fiber) or 10 kilometer (single-mode fiber).

Small Workgroup

The TEG-S2620is can be used as a standalone switch to which personal computers, server, printer server, are directly connect to form small workgroup.

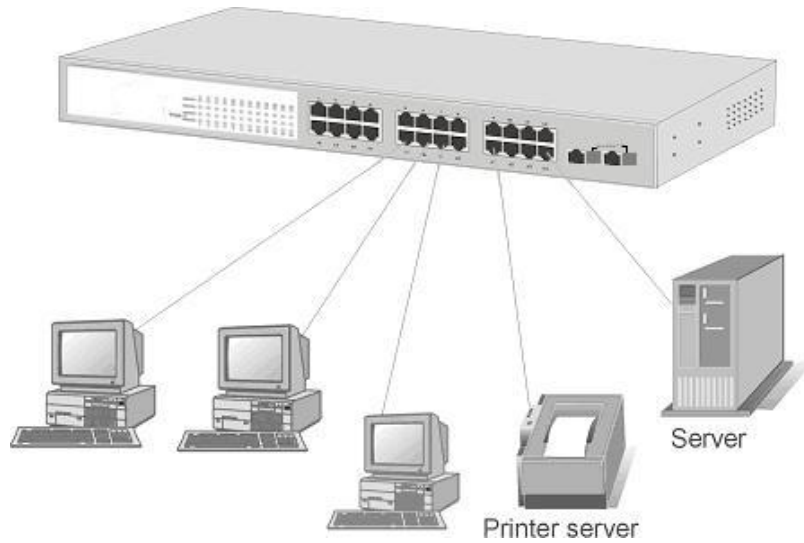


Figure 3-1. Small Workgroup Application

Segment Bridge

For enterprise networks where large data broadcasts are constantly processed, this switch is an ideal solution for department users to connect to the corporate backbone.

In the illustration below, two Ethernet switches with PCs, print server, and local server attached, are both connect to the Switch. All the devices in this network can communicate with each other through the Switch. Connecting servers to the Switch allow other users to access the data on server.

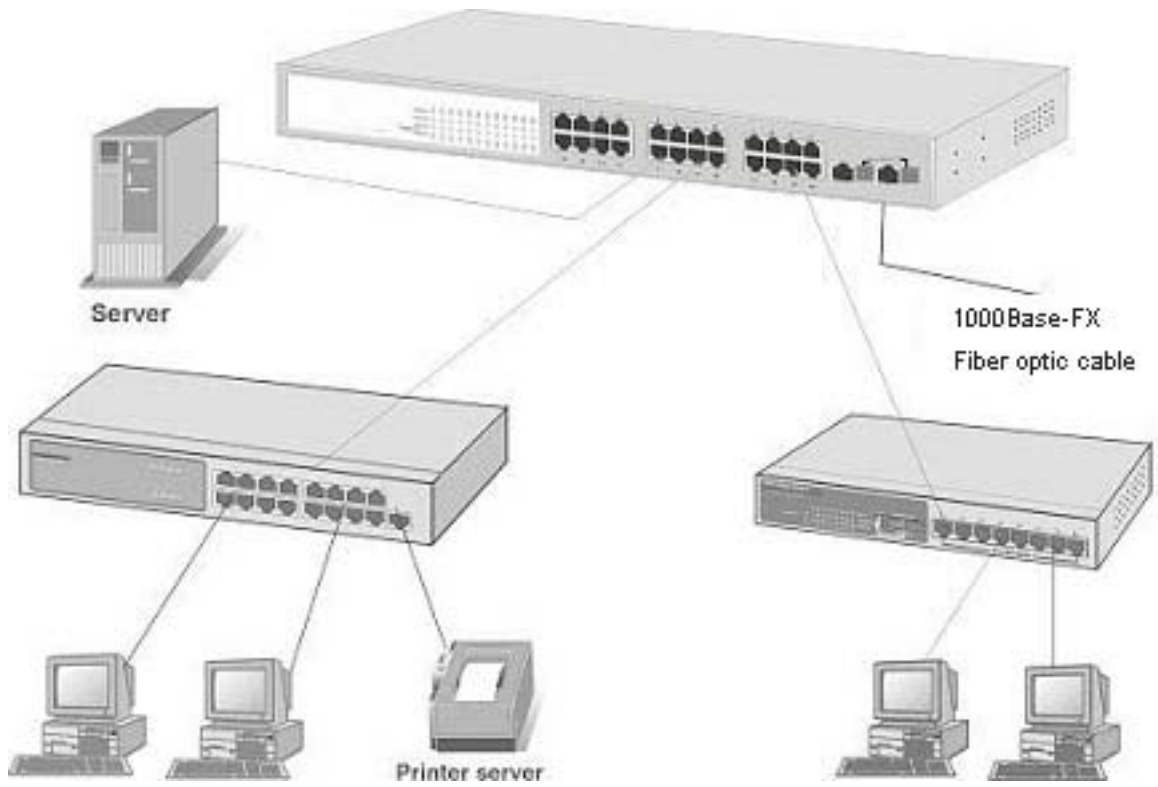


Figure 3-2 Department Bridge Applications

4. Console Management

Login in the Console Interface

When the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program or **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

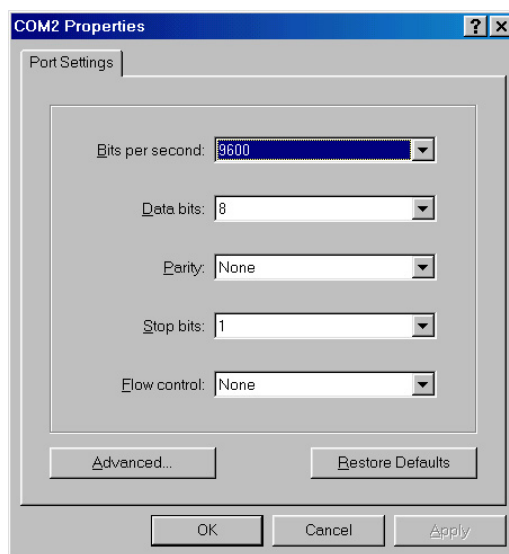
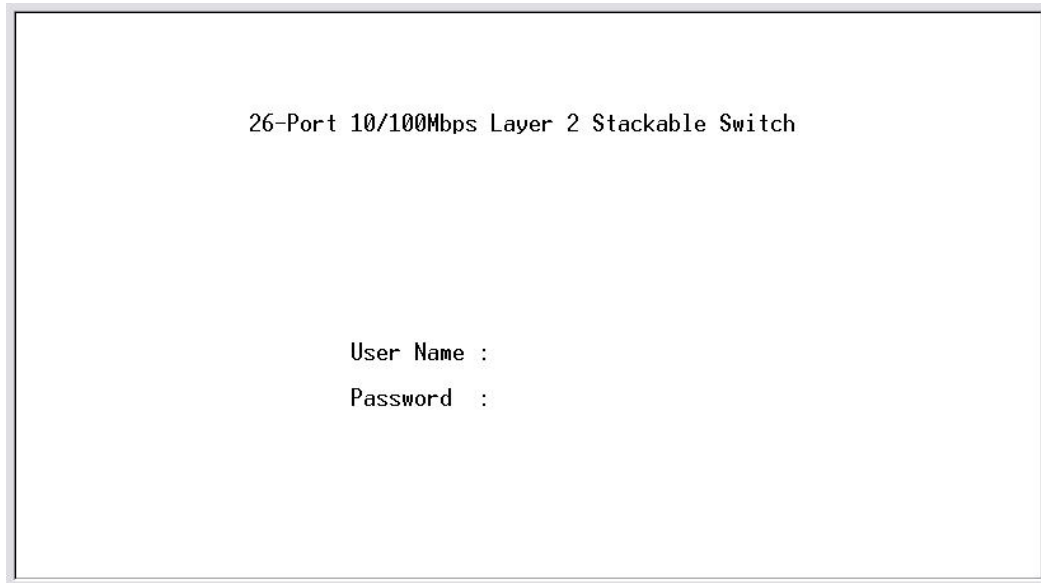


Figure 4-1. The settings of communication parameters

After finished the parameter settings, click “**OK**”. When the blank screen shows up, press Enter key to bring out the login prompt. Key in the “**admin**”(default value) for the both User name and Password (use **Enter** key to switch), then press Enter key and the Main Menu of console management appears. Please see below figure for login screen.



Console login screen

Main Menu

There are five selections as follow.

- **Status and Counters:** Show the status of the switch.
- **Switch Configuration:** Configure the switch.
- **Protocol Related Configuration:** Configure the protocol function.
- **System Reset Configuration:** Restart the system or reset switch to default configuration.
- **Logout:** Exit the menu line program.

```

Main Menu
=====

Status and Counters
Switch Configuration
Protocol Related Configuration
System Reset Configuration
Logout

Show the status of the switch.
[Enter] Select Item
[Tab/BKSPC] Move Item
```

Main menu line interface

■ **Control Key description:**

The control keys provided in all menus:

Tab: Move the vernier to next item.

Backspace: Move the vernier to previous item.

Enter: Select item.

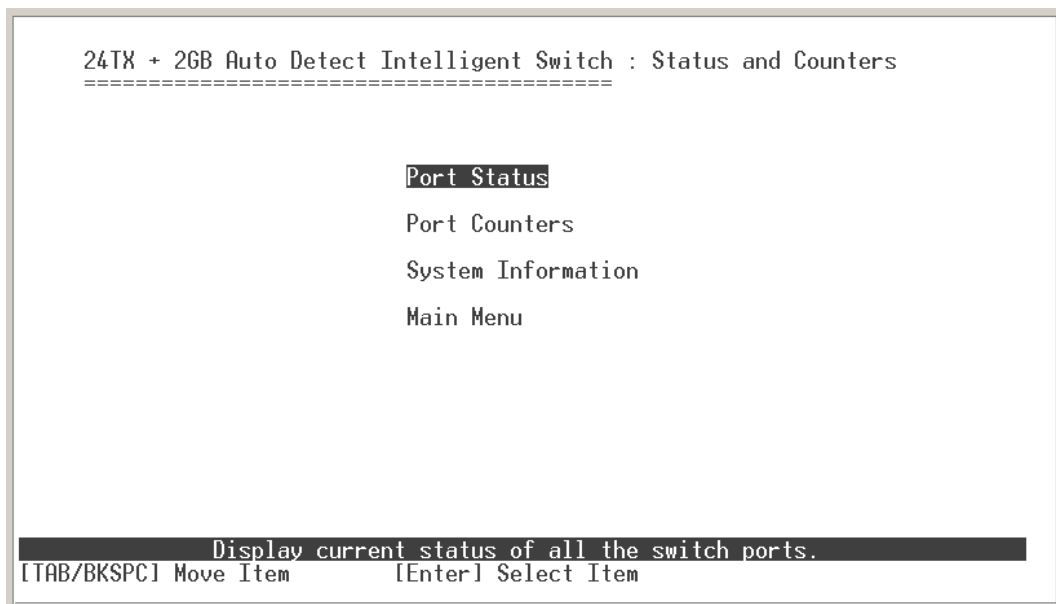
Space: Toggle selected item to next configure or change the value.

Esc: Exit the current action mode.

Function Description

Status and Counters

In Status and Counters, you can view Port status, counters, and configure system parameter. You can press the “**Tab**” or “**Backspace**” to choose the item, and press “**Enter**” key to select the item.



Status and Counters main configuration interface

Port Status

It displays status of the port. Select the <**Previous Page**> action to display previous page. And, select the <**Next page**> action to display next page.

- **Type:** Display port connection speed type.
- **Link:** Display port link status. When the port is connecting with the device and work normally, the link status is “**UP**”. Opposite is “**Down**”.
- **State:** The port current status. “**Enable**” – it means this port working status is normal. “**Disable**” – it means this port is not function event the device is connected.

- **Negotiation:** display the auto negotiation status.
- **Speed Duplex:** display port speed and duplex mode.
- **FC:** display the flow control status is “enable” or “disable”.
- **BP:** display backpressure status.
- **Bandwidth In/Out:** display bandwidth In/out control status.
- **Priority:** display the port priority status.
- **Security:** display the port security status.

```

24TX + 2GB Auto Detect Intelligent Switch : Port Status
=====

```

Port	Type	Link	State	Negotiation	Speed	Duplex	FC	BP	Band	Width	Security
									In	Out	Priority
Port.01	100TX	Down	Enable	Auto	100	Full	ON	OFF	OFF	OFF	Disable OFF
Port.02	100TX	Down	Enable	Auto	100	Full	ON	OFF	OFF	OFF	Disable OFF
Port.03	100TX	Down	Enable	Auto	100	Full	ON	OFF	OFF	OFF	Disable OFF
Port.04	100TX	Down	Enable	Auto	100	Full	ON	OFF	OFF	OFF	Disable OFF
Port.05	100TX	Down	Enable	Auto	100	Full	ON	OFF	OFF	OFF	Disable OFF
Port.06	100TX	Down	Enable	Auto	100	Full	ON	OFF	OFF	OFF	Disable OFF
Port.07	100TX	Down	Enable	Auto	100	Full	ON	OFF	OFF	OFF	Disable OFF
Port.08	100TX	Down	Enable	Auto	100	Full	ON	OFF	OFF	OFF	Disable OFF

```

Actions->  <Previous Page>  <Next Page>  <Quit>
Select the action menu.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu

```

Port status interface

Port Counters

It displays the current port counter information. Select the **<Refresh>** action to get newest port counter information. Select **<Clear>** action to set the port counter information back to 0.

24TX + 2GB Auto Detect Intelligent Switch : Port Counters							
Port	Type	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision
Port.01	100TX	0	0	0	0	0	0
Port.02	100TX	0	0	0	0	0	0
Port.03	100TX	0	0	0	0	0	0
Port.04	100TX	0	0	0	0	0	0
Port.05	100TX	0	0	0	0	0	0
Port.06	100TX	0	0	0	0	0	0
Port.07	100TX	0	0	0	0	0	0
Port.08	100TX	0	0	0	0	0	0

Actions->	<Refresh>	<Clear>	<Previous Page>	<Next Page>	<Quit>
Configure the action menu.					
[TAB/BKSPC]	Move Item	[Enter]	Select Item	[Esc]	Previous Menu

Port counter information interface

System Information

It displays the system parameter.

1. **System Name:** the name of device.
2. **System Location:** where the device is located.
3. **System Description:** the name of device type.
4. **Firmware Version:** the switch's firmware version.
5. **Hardware Version:** the switch's Hardware version.
6. **Kernel Version:** the system kernel software version.
7. **MAC Address:** The unique hardware address assigned by manufacturer.
8. **Module Information:** display the Module type that you have installed in switch.

24TX + 2GB Auto Detect Intelligent Switch : System Information
=====

System Name :
System Location :
System Description : 24 TX Port + 2 Giga Auto Detect Intelligent Switch

Firmware Version : v1.01
Kernel Version : v3.00
Hardware Version : A7.00
MAC Address : 00001C050453

Module	Type	Description
Port 25	Auto	1000TX Copper/1000FX MiniGBIC
Port 26	Auto	1000TX Copper/1000FX MiniGBIC

Actions-> <Quit>
Display the switch system information.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

System Information interface

Switch Static Configuration

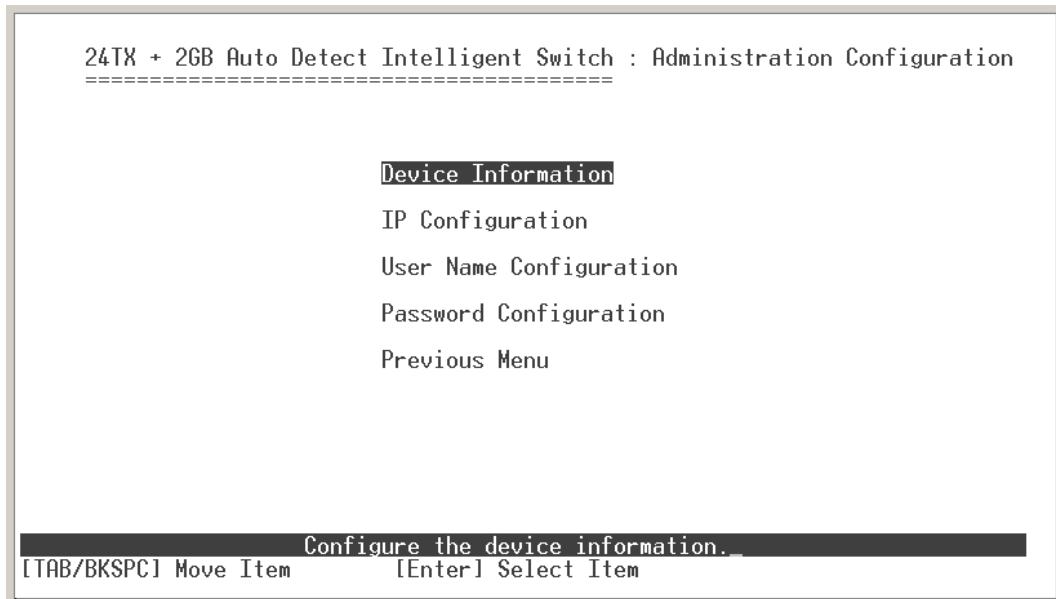
In Switch Static Configuration, it has 8 main functions – Administration, Port, Trunk, Port Mirroring, VLAN, Priority, MAC Address, and Misc Configuration. Under each function, there are more sub-functions. We will describe in following paragraph.

```
24TX + 2GB Auto Detect Intelligent Switch : Switch Configuration
=====
Administration Configuration
Port Configuration
Trunk Configuration
Port Mirroring Configuration
VLAN Configuration
Priority Configuration
MAC Address Configuration
Misc Configuration
Main Menu
-----
Configure the system, IP, and password.
[TAB/BKSPC] Move Item      [Enter] Select Item
```

Switch Configuration interface

Administration Configuration

In Administration Configuration, you can configuration system parameter, IP, login username and password.



Administration Configuration main interface

Device Information

You can configure the device information.

1. Select **<Edit>** action to configure.
2. **Name:** assign the name for the switch.
3. **Description:** a short description for the switch.
4. **Location:** the switch location, ex: Taipei.
5. **Contact:** the contact person or information.
6. Select **<Save>** action to save the configuration.

```
24TX + 2GB Auto Detect Intelligent Switch : Device Information
=====

Name      :
Description : 24 TX Port + 2 Giga Auto Detect Intelligent Switch
Location  :
Contact   :

Actions->  <Edit>  <Save>  <Quit>
Select the action menu.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu
```

Device Information interface

IP Configuration

You can configure the IP for this switch. The system has the default IP address.

You can re-configure or use the default value.

1. Select the **<Edit>**
2. **DHCP:** disable or enable the DHCP client function.
3. **IP Address:** assign the switch IP address. The default IP is 192.168.0.1.
4. **Subnet Mask:** assign the switch IP subnet mask.
5. **Gateway:** assign the switch gateway. The default value is 192.168.0.254.
6. Select **<Save>** action to save the configuration.

[Note] Always restart the switch after finished the setup.

```
Intelligent Switch : IP Configuration
=====

DHCP Client : Disable
IP Address   : 192.168.0.1
Subnet Mask  : 255.255.255.0
Gateway      : 192.168.0.254

Actions->  <Edit>  <Save>  <Quit>
Select the action menu.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu
```

IP Configuration interface

User Name Configuration

You can change the console and web management login user name.

1. Select the **<Edit>**
2. Enter the new user name
3. Select the **<Save>**

```
Intelligent Switch : User Name Configuration
=====

User Name : admin

Actions->  <Edit>  <Save>  <Quit>
Select the action menu.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu
```

User Name Configuration interface

Password Configuration

You can change the console and web management login password.

1. Select the **<Edit>**
2. **Old Password:** enter the old password.
3. **New Password:** enter the new password.
4. **Enter Again:** reenter the new password for confirmation.
5. Select the **<Save>**

```
24TX + 2GB Auto Detect Intelligent Switch : Password Configuration
=====

Old Password :
New Password :
Enter Again  :

Actions->  <Edit>  <Save>  <Quit>
Select the action menu.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu
```

Password Configuration interface

Port Configuration

You can set up every port status.

1. Select **<Edit>**
2. Use “**Tab**” key to move between items.
3. **State:** Current port status. The port can be set to disable or enable mode. If the port setting is disable then will not receive or transmit any packet.
4. **Negotiation:** set auto negotiation status of port.

5. **Speed/Duplex:** set the port link speed and duplex mode.
6. **FC:** enable or disable **Flow control** function (Flow control for full duplex link mode).
7. **BP:** enable or disable **Back Pressure** function (Backpressure for half duplex mode).
8. **Bandwidth In/Out:** per port packet transmission rate control. Per level is 100Kbps. It supports individual control method of TX and RX.
9. **Priority:** set port to high or low priority.
10. **Security:** enable or disable port security function.
11. Select the **<Save>**.

```

24TX + 2GB Auto Detect Intelligent Switch : Port Configuration
=====

```

Port	Type	Negotiation State	Speed Duplex	FC	BP	Band Width In	Out	Priority	Security
Port.01	100TX	Enable Auto	100 Full	ON	OFF	0	0	Disable	OFF
Port.02	100TX	Enable Auto	100 Full	ON	OFF	0	0	Disable	OFF
Port.03	100TX	Enable Auto	100 Full	ON	OFF	0	0	Disable	OFF
Port.04	100TX	Enable Auto	100 Full	ON	OFF	0	0	Disable	OFF
Port.05	100TX	Enable Auto	100 Full	ON	OFF	0	0	Disable	OFF
Port.06	100TX	Enable Auto	100 Full	ON	OFF	0	0	Disable	OFF
Port.07	100TX	Enable Auto	100 Full	ON	OFF	0	0	Disable	OFF
Port.08	100TX	Enable Auto	100 Full	ON	OFF	0	0	Disable	OFF

```

Actions->  <Edit>  <Save>  <Previous Page>  <Next Page>  <Quit>
Select the Action menu.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu

```

Port Configuration interface

Trunk Configuration

You can configure port trunk group.

1. Select **<Edit>**
2. Using “**Tab**” key move to the port that want to be added into trunk group.
3. Using “**Space**” key to mark the port.
4. Using **Tab** key move to “**Trunk #**” (ex. Trunk 1, Trunk 2...) to change the Trunk

value to “Static”.

5. Save the configuration by selecting <Save>.

```
24TX + 2GB Auto Detect Intelligent Switch : Trunk Configuration
=====
 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
T1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
T2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
T3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
T4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
T5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
T6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
T7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Trunk 1: Disable
Trunk 2: Disable
Trunk 3: Disable
Trunk 4: Disable
Trunk 5: Disable
Trunk 6: Disable
Trunk 7: Disable

Actions->  <Edit>  <Save>  <Quit>
Select the action menu.
[Tab/BKSPC] Move Item          [Enter] Select Item          [Esc] Previous Menu
```

Trunk Configuration interface

Port Mirroring Configuration

The port mirroring is a method for monitor traffic of switched networks. The specific port can monitor traffic through the mirror ports. The monitored ports in or out traffic will be duplicated into monitoring port.

1. Select the <Edit>
2. **Mirroring State:** select the port-mirroring mode. The default value is “Disable”. To start port mirroring, you must select one of port mirroring mode.
 - **RX:** RX packet only
 - **TX:** TX packet only
 - **Both:** RX and TX packet

```

24TX + 2GB Auto Detect Intelligent Switch : Port Mirroring
=====

Mirroring State : Disable

Actions->  <Edit>  <Save>  <Quit>
Select the action menu.
[TAB/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu

```

Port Mirroring interface

3. **Analysis port:** Set the destination port of mirroring packet. All of the packets of mirroring port will be duplicated and sent to Analysis port.
4. Use “**Space**” key to mark the mirroring port.
5. Select the **<Save>**.

```

24TX + 2GB Auto Detect Intelligent Switch : Port Mirroring
=====

Mirroring State : Both
Analysis Port : Port.01

Port State      Port State      Port State      Port State
-----
Port.01 -      Port.09 -      Port.17 -      Port.25 -
Port.02 -      Port.10 -      Port.18 -      Port.26 -
Port.03 -      Port.11 -      Port.19 -
Port.04 -      Port.12 -      Port.20 -
Port.05 -      Port.13 -      Port.21 -
Port.06 -      Port.14 -      Port.22 -
Port.07 -      Port.15 -      Port.23 -
Port.08 -      Port.16 -      Port.24 -

Actions->  <Edit>  <Save>  <Quit>
Select the action menu.
[TAB/BKSPC] Move Item      [Space] Toggle      [Esc] Previous Menu

```

Port Mirroring interface

VLAN Configuration

You can configure VLAN in VLAN Configuration. There are four functions in VLAN Configuration mode: VLAN Configuration, Create a VLAN Group, Edit/Delete VLAN Group and Group Sorted Node. Follow the below description to configure VLAN.

```
24TX + 2GB Auto Detect Intelligent Switch : VLAN Configuration
=====
VLAN Configure
Create VLAN Group
Edit/Delete VLAN Group
Group Sorted Mode
Previous Menu

Configure VLAN mode and ingress, egress rule.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu
```

VLAN Configuration Main interface

VLAN Configure

Before starting to configure VLAN, you must select the VLAN mode in VLAN Configure function. Otherwise, user cannot create any new VLAN.

1. Select the **<Edit>**.
2. Select the VLAN mode by using “**Space**” key. There are two VLAN modes: PortBase mode and 802.1Q mode.
 - **802.1Q VLAN mode:** configuration VLAN ID, Ingress Filter, and Acceptable Frame Type.
 - ✧ **VLAN ID (Port VID: 1~255):** Type the PVID.
 - ✧ **Ingress Filter:** It matches that Ingress Filtering Rule 1 on web. Only

forward packets with VID matching this port's configured VID. Press "Space" key to choose forward or drop the frame that VID not matching this port's configured VID.

- ✧ **Acceptable Frame type:** It matches that Ingress Filtering Rule 2 on web. Drop untagged frame. Press "Space" key to select drop or forward the untagged frame.

3. Select <Save> to save the configuration.

```

24TX + 2GB Auto Detect Intelligent Switch : VLAN Configure
=====
VLAN Mode : 802.1Q
VLAN ID Range : 1~255

Port      VLAN ID      Ingress Filter      Acceptable
Frame Type
-----
Port.01   1            Enable              All
Port.02   1            Enable              All
Port.03   1            Enable              All
Port.04   1            Enable              All
Port.05   1            Enable              All
Port.06   1            Enable              All
Port.07   1            Enable              All
Port.08   1            Enable              All

Actions->  <Edit>  <Save>  <Previous Page>  <Next Page>  <Quit>
Select the Action menu.
[TAB/BKSPC] Move Item      [Space] Toggle      [Esc] Previous Menu

```

VLAN Configure interface

Create VLAN Group

■ Create Port-Based VLAN

1. Select <Edit>.
2. **VLAN Name:** Type a name for the new VLAN, ex: VLAN01.
3. **Group ID:** Type the VLAN group ID. The group ID rang is from 1 to 4094.
4. **Member:** Press "Space" key to change the member value. There are two types to selected:
 - a. **Member:** the port is a member port.
 - b. **NO:** it means that the port is NOT a member port.
5. Press "ESC" key to go back action menu line.

6. Select **<Save>** to save the configuration.

NOTE: If you had configured the trunk groups, you can see it (ex: Trunk 1, Trunk 2...) in the port list. You also can configure the trunk group as the VLAN member.

```

24TX + 2GB Auto Detect Intelligent Switch : Create VLAN Group
=====

VLAN Name :                               Group ID :

Port      Member
-----
Port.01   No
Port.02   No
Port.03   No
Port.04   No
Port.05   No
Port.06   No
Port.07   No
Port.08   No

Actions->  <Edit>  <Save>  <Previous Page>  <Next Page>  <Quit>
Select the Action menu.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu

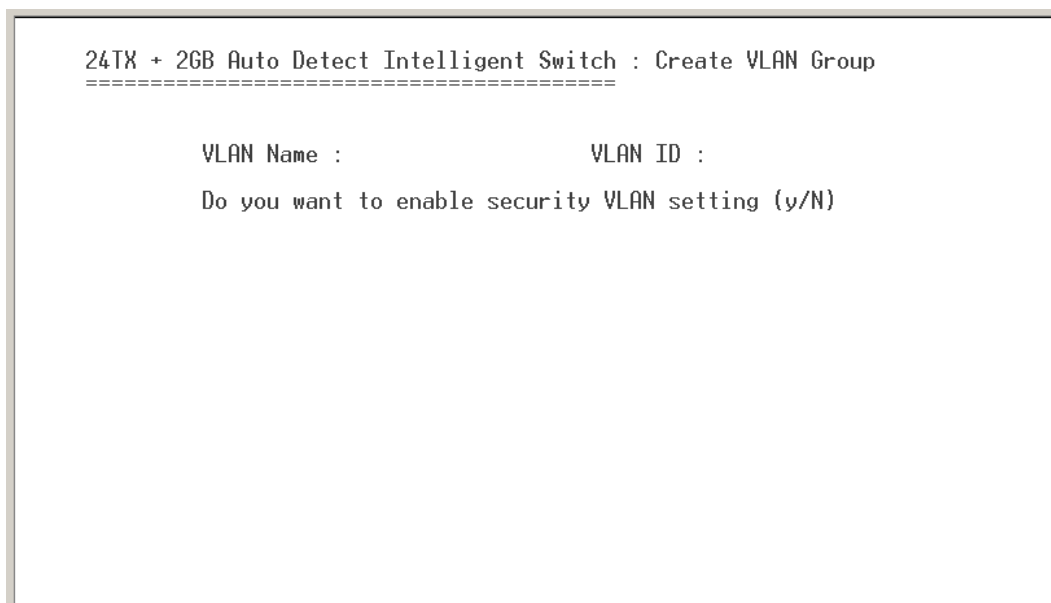
```

Create VLAN Group: PortBase interface

■ **Create 802.1Q VLAN**

1. **Enable security VLAN setting:** select to enable or disable security VLAN group. When you select to enable security VLAN group, only the members in this VLAN group can access to the switch. The steps of setting security VLAN refer to the following step 2~ 8. After you have configured the security VLAN group, you can continue to create other VLAN groups. When you don't select to configure security VLAN group, then just create VLAN group refer to following step 2 ~ 8.

Note: There is only one security VLAN group.



Create VLAN group: 802.1Q interface

2. Select **<Edit>**.
3. **VLAN Name:** Type a name for the new VLAN, ex: VLAN01.
4. **VLAN ID:** Type a VID (between 1~4094). The default is 1. There are 256 VLAN groups to provided configure.
5. **Protocol VLAN:** Press “**Space**” key to choose protocols type.
6. **Member:** Press “**Space**” key to change the member value.
 - **Untagged:** this port is the member port of this VLAN group and outgoing frames are NO VLAN-Tagged frames.
 - **Tagged:** this port is the member port of this VLAN group and outgoing frames are VLAN-Tagged frames.
 - **NO:** it means that the port is NOT member of this VLAN group.
7. Press “**ESC**” key to go back action menu line.
8. Select **<Save>** to save the configuration.

```

24TX + 2GB Auto Detect Intelligent Switch : Create VLAN Group
=====

VLAN Name :                VLAN ID :

Protocol VLAN : None

Port      Member
-----
Port.04   No
Port.05   No
Port.06   No
Port.07   No
Port.08   No
Port.09   No
Port.10   No
Port.11   No

Actions->  <Edit>  <Save>  <Previous Page>  <Next Page>  <Quit>
Select the Action menu.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu

```

Create VLAN Group: 802.1Q interface

Edit / Delete VLAN Group

User can edit or delete a VLAN group.

1. Select **<Edit>** or **<Delete>** action.
2. Select the VLAN group that you want to edit or delete, then press enter.
3. In **<Edit>** action, user can modify the member port and remove member ports from this VLAN group.
4. After edit or delete the VLAN, select **<Save>** action to save all configures value.

NOTE:

1. The VLAN Name and VLAN ID cannot modify.
2. In 802.1Q VLAN mode, the default VLAN can't be deleting.
3. In Port Base VLAN mode, there is no default VLAN.

```

Name          VLAN ID      Name          VLAN ID
-----
DEFAULT      1
VLAN1        2

Actions->  <Edit>  <Delete>  <Previous Page>  <Next Page>  <Quit>
Edit/Delete a VLAN Group.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu

```

Edit/Delete a VLAN Group interface

Group Sorted Mode

You can select VLAN groups sorted mode: (1) **Name** (2) **VLAN ID**.

In the Edit/Delete a VLAN group page will display the result.

1. Select **<Edit>**
2. Use **"Space"** key to select the sort mode.
3. Select **<Save>**

```

24TX + 2GB Auto Detect Intelligent Switch : Group Sorted Mode
=====

VLAN Group Sorted by : Name

Actions->  <Edit>  <Save>  <Quit>
Select the action menu.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu

```

Group Sorted Mode interface

Priority Configuration

You can configure port priority level. There are 0~7-priority level can map to high or low queue.

1. Select **<Edit>**.
2. Set the Level 0~7 priority, use “**Space**” key to change the value..
3. Press “**Space**” key to select the priority level mapping to high or low queue.
4. **QoS Mode:** select the mode to process incoming packets.
 - **First Come first service:** the switch will process the packet that is coming first.
 - **All High Before low:** the packet priority is high will be process before the packet priority is low.
 - **Weight Round Ration 2:1:** the switch will process 2 high priority packet first, the process 1 low priority packet.
 - **Weight Round Ration 3:1:** the switch will process 3 high priority packet first, the process 1 low priority packet.
 - **Weight Round Ration 4:1:** the switch will process 4 high priority packet first, the process 1 low priority packet.
 - **Weight Round Ration 5:1:** the switch will process 5 high priority packet first, the process 1 low priority packet.
 - **Weight Round Ration 6:1:** the switch will process 6 high priority packet first, the process 1 low priority packet.
 - **Weight Round Ration 7:1:** the switch will process 7 high priority packet first, the process 1 low priority packet.
5. Press “**ESC**” goes back action menu line.
6. Select **<Save>** to save all configure value.

```

24TX + 2GB Auto Detect Intelligent Switch : Priority Configuration
=====

Level 0 : Low
Level 1 : Low
Level 2 : Low
Level 3 : Low
Level 4 : High
Level 5 : High
Level 6 : High
Level 7 : High

QoS Mode : All High Before Low

Actions->  <Edit>  <Save>  <Quit>
Select the action menu.
[TAB/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu

```

Priority Configuration interface

MAC Address Configuration

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

```

24TX + 2GB Auto Detect Intelligent Switch : MAC Address Configuration
=====

Static MAC Address
Filtering MAC Address
Previous Menu

Configure the MAC address.
[TAB/BKSPC] Move Item      [Enter] Select Item

```

MAC Address Configuration interface

Static MAC Address

■ Add the Static MAC Address

You can add static MAC address in switch MAC table.

1. Select **<Add>** → **<Edit>** key to add the static MAC address.
2. **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
3. **Port No.:** press “**Space**” key to select the port number.
4. **VLAN ID:** enter the Mac address’ s VLAD ID, if the Mac address belongs to any VLAN group.
5. Press “**ESC**” to go back action menu line.
6. Select **<Save>** to save all configure value.

```
24TX + 2GB Auto Detect Intelligent Switch : Add Static MAC Address
-----

MAC Address :
Port No.    :
VLAN ID    :

Actions->  <Edit>  <Save>  <Quit>
Select the action menu.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu
```

Add Static MAC Address interface

■ Edit static MAC address

1. Select **<Edit>**.
2. Choose the MAC address that you want to modify and then press “**Enter**”.
3. Press **<Edit>** key to modify.
4. Press “**ESC**” to go back action menu line.

5. Select **<Save>** to save all configure value.

■ Delete static MAC address

1. Select **<Delete>** key.
2. Choose the MAC address that you want to delete and then press **“Enter”**.
3. When pressing **“Enter”** will complete deletion.

Filtering MAC Address

You can add, delete, and edit filtering MAC address.

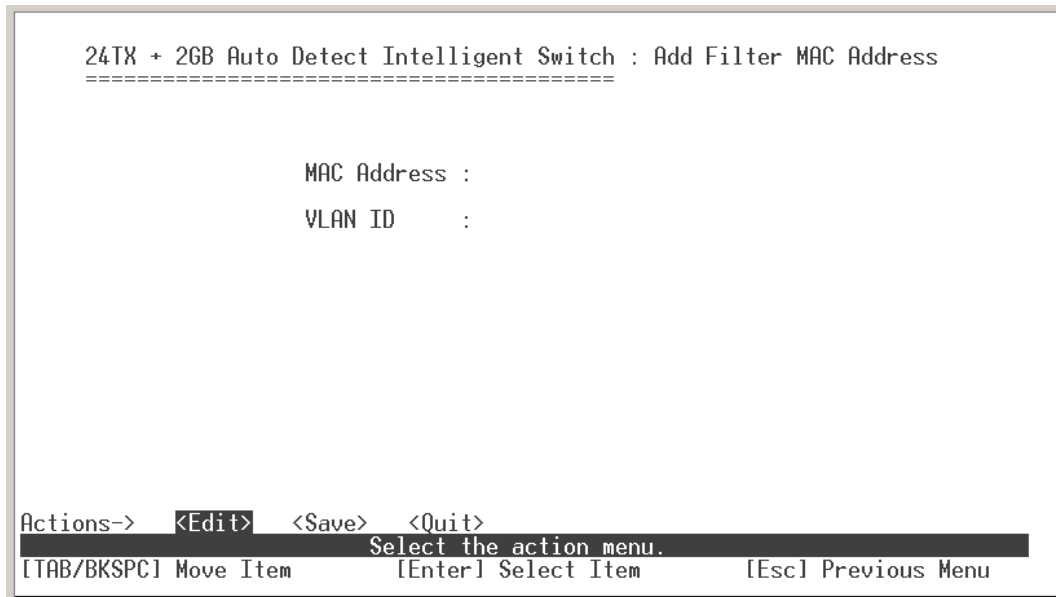
```
24TX + 2GB Auto Detect Intelligent Switch : Filtering MAC Address
=====
MAC Address      VLAN ID          MAC Address      VLAN ID
-----
[TAB/BKSPC] Move Item          [Enter] Select Item          [Esc] Previous Menu

Actions->  <Add>  <Edit>  <Delete>  <Previous Page>  <Next Page>  <Quit>
Add/Edit/Delete a Mac.
```

Filtering MAC Address interface

■ Add the Filtering MAC Address

1. Select **<Add>** → **<Edit>** key to add the static MAC address.
2. **MAC Address:** Enter the MAC address that you want to filter.
3. Press **“ESC”** to go back action menu line.
4. Select **<Save>** to save all configure value.



Add Filtering MAC Address interface

■ Edit Filtering MAC address

1. Select **<Edit>** key to modify a static Filtering address.
2. Choose the MAC address that you want to modify and then press **“Enter”**.
3. Select **<Edit>** key to modify.
4. Press **“ESC”** to go back action menu line
5. Select **<Save>** to save all configure value.

■ Delete Filtering MAC address

1. Select **<Delete>** to delete a Filtering MAC address.
2. Choose the MAC address that you want to delete and then press **“Enter”**.
3. After delete Filtering MAC address, you have to select **<Save>** to complete the deleting operation.

Misc Configuration

You can configure the switch parameters and stacking function. The stacking function provides you can centralize the control of the switch in the network. For

the manager personal, he/she can save the time and easily on switches controlling.

- **MAC Address Ageing Time:** MAC address table refresh time setting. Type the number of seconds that an inactive MAC address remains in the switch's address table. The valid range is 0, 300~765 seconds. Default is 300 seconds.
- **Broadcast Storm Filter mode:** configure the broadcast storm filter mode. The valid threshold values are 5%, 10%, 15%, 20%, 25%, and N/A. The port will be block cause of broadcast packet is over the percentage of traffic.
- **Max Bridge Transmit Delay Bound:** Limit the packets queuing time in switch. If enable, the packets queued exceed will be drop. Press **Space** key to set the time. This valid value are 1sec, 2sec, 4sec and off. Default is off.
- **Low Queue Delay Bound:** Limit the low priority packets queuing time in switch. If enable, the low priority packet stays in switch exceed Low Queue Max Delay Time, it will be sent. Press **Space** key to enable or disable this function.
- **Low Queue Max Delay Time:** To set the time that low priority packets queuing in switch. Default Max Delay Time is 255ms. The valid range is 1~255 ms.
NOTE: Make sure of "Max bridge transit delay bound control" is enabled before enable Low Queue Delay Bound, because Low Queue Delay Bound must be work under "Max bridge transit delay bound control" is enabled situation.
- **Collisions Retry Forever:** Disable – In half duplex, if happens collision, the switch will retry 48 times and then drop frame. Enable – In half duplex, if happens collision, the switch will retry forever
- **Hash Algorithm:** This Hash Algorithm is for hardware maintaining on the MAC table calculation. Provide CRC or Direct Map.
- **IFG compensation:** Disable or Enable.
- **IP Stacking Group ID (0...65535):** assign the stacking group ID. The switches must assign the same stacking group ID to be stacked as a group.
- **IP Stacking Mode:** enabling/disabling the stacking function. There are three stacking modes. Any port on the switch can be used to stack. To configure

the switch in stacking group, please use the Web GUI configuration interface.

- **Disable:** The stacking function is not working.
- **Master:** There must have a leader switch to control all other switches in stacking group. You can only assign one switch to be the master switch in one stacking group. When the stacking group is set up, the master switch will control all switches in the stacking group.
- **Slave:** besides the master switch, rest of the switches are called slave switch in stacking group. When the stacking group is set up, you can only configure the slave switches through the master switch.

Note:

1. Before configuring the stacking function, make sure all stack switches are in the same network.
2. Configure stacking function; you must configure the master switch first.
3. After you have configured the stacking function, use Cat. 5 cable to connect every switch in the stacking group.
4. To remove the switch from stacking group, you must remove the slave switch first. When all slave switches are removed, you can remove the master switch from stacking group.

```
24TX + 2GB Stackable Intelligent Switch : Misc Configuration
=====
MAC Address Ageing Time (0, 300..765) : 300
Broadcast Storm Filter Mode           : 5%
Max Bridge Transmit Delay Bound       : OFF
Low Queue Delay Bound                  : Disable
Low Queue Max Delay Time (1..255)     : 255
Collisions Retry Forever               : Enable
Hash Algorithm                        : CRC Hash
IFG Compensation                       : Enable
IP Stacking Group ID (0..65535)       : 0
IP Stacking Mode                      : Disable

Actions->  <Edit>  <Save>  <Quit>
           Select the action menu.
[TAB/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu
```

Misc Configuration interface

Protocol Related Configuration

You can configure Spanning Tree Protocol, SNMP, LACP, IGMP/GVRP, and 802.1x in Protocol Relate Configuration section.

```
24TX + 2GB Auto Detect Intelligent Switch : Protocol Related Configuration
=====
          STP Configuration
          SNMP Configuration
          LACP Configuration
          IGMP/GVRP Configuration
          802.1x Configuration
          Previous Menu

          Configure the Spanning Tree Protocol.
[TAB/BKSPC] Move Item      [Enter] Select Item
```

Protocol Relate Configuration interface

STP

Spanning tree is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

```

24TX + 2GB Auto Detect Intelligent Switch : STP Configuration
=====

      STP Setup

      System Configuration
      Per Port Setting
      Previous Menu

      Enable or disable Spanning Tree function.
[Tab/BKSPC] Move Item      [Enter] Select Item

```

STP Configuration interface

STP Setup

You must enable Spanning Tree function before configure STP function.

1. Select **<Edit>**.
2. Use “**Space**” key to select the option.
3. Select **<Save>**.

```

24TX + 2GB Auto Detect Intelligent Switch : STP Setup
=====

      STP : Disable

      Actions->  <Edit>  <Save>  <Quit>
                  Select the action menu.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu

```

STP Setup interface

System Configuration

You can configure the STP system parameter after enable the STP function. You can view spanning tree information about the Root Bridge on the left.

1. Select **<Edit>**.
2. **Priority:** assign path priority number.
3. **Max Age:** the maximum path age.
4. **Hello Time:** the time that controls switch sends out the BPDU packet to check STP current status.
5. **Forward Delay Time:** forward delay time.
6. Select **<Save>**.

```
24TX + 2GB Auto Detect Intelligent Switch : STP System Configuration
=====

Root Bridge Information          Configure Spanning Tree Parameters
-----
Priority       : 32768           Priority (0-65535)       : 32768
Mac Address   : 001122334455    Max Age (6-40)         : 20
Root Path Cost : 0              Hello Time (1-10)      : 2
Root Port     : Root            Forward Delay Time (4-30) : 15
Max Age       : 20
Hello Time    : 2
Forward Delay : 15

Actions->  <Edit>  <Save>  <Quit>
          Select the action menu.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu
```

STP System Configuration interface

Per Port Setting

1. Select **<Edit>**.
2. **Path Cost:** specifies the path cost of the port that switch uses to determine which port are the forwarding ports.
3. **Priority:** This is mean port priority; you can make it more or less likely to become the root port.

4. Press “**ESC**” goes back action menu line.
5. Select **<Save>** to save all configure value.
6. On the action menu line you can press **<Next Page>** to configure port9 ~ port26, press **<Previous Page>** return to previous page.

```

24TX + 2GB Auto Detect Intelligent Switch : STP Per Port Setting
=====
Port          State          Path Cost      Priority
-----
Port.04      Forwarding      10             128
Port.05      Forwarding      10             128
Port.06      Forwarding      10             128
Port.07      Forwarding      10             128
Port.08      Forwarding      10             128
Port.09      Forwarding      10             128
Port.10      Forwarding      10             128
Port.11      Forwarding      10             128

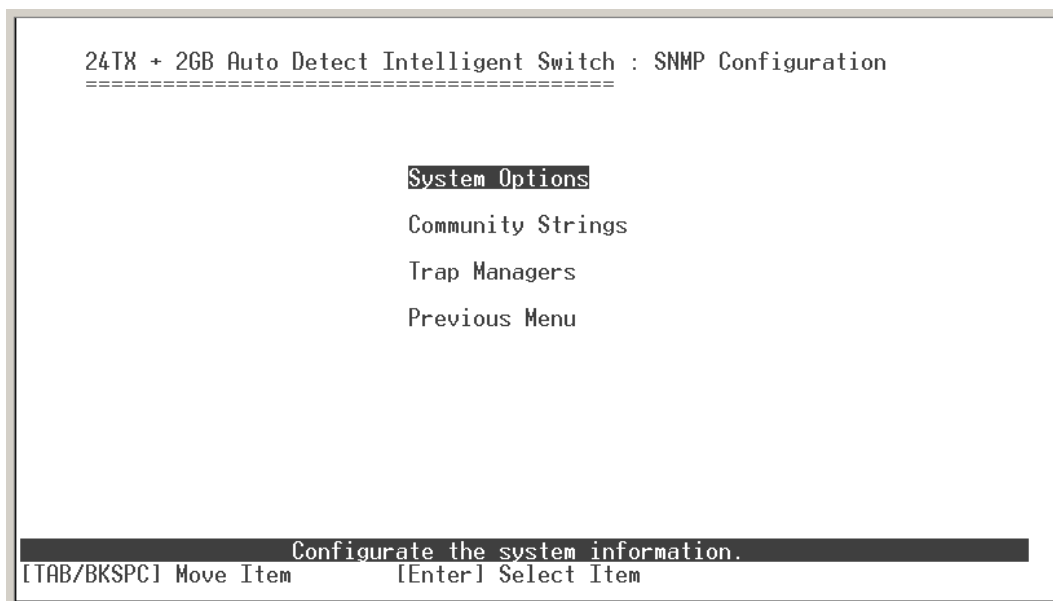
Actions->  <Edit>  <Save>  <Previous Page>  <Next Page>  <Quit>
Select the Action menu.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu

```

Per Port Setting interface

SNMP

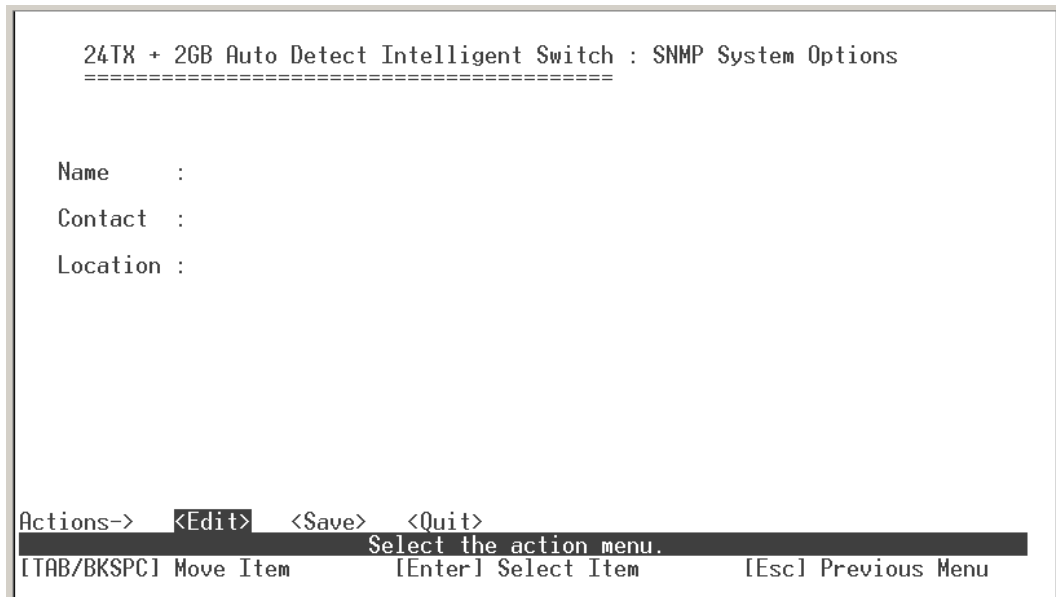
To define management stations as trap managers and to enter SNMP community strings. You can also define a name, location, and contact person for the switch.



SNMP Configuration interface

SNMP System Options

1. Press **<Edit>**.
2. **System Name:** assign a name for the switch.
3. **System Contact:** Type the name of contact person or organization.
4. **System Location:** Type the location of the switch.
5. Press “**ESC**” goes back action menu line.
6. Press **<Save>** to save configure value.



SNMP System Options interface

Community Strings

■ Add Community Strings

1. Select **<Add>**.
2. Select **<Edit>**.
3. **Community Name:** type the name of community strings.
4. **Write Access:** enable the rights is read only or read/write.
 - **Read only:** Read only, enables requests accompanied by this string to display MIB-object information.
 - **Read/Write:** Read write, enables requests accompanied by this string to display MIB-object information and to set MIB objects.

```

24TX + 2GB Auto Detect Intelligent Switch : Add SNMP Community
=====

Community Name :
Write Access   : Read Only

Actions->  <Edit>  <Save>  <Quit>
Select the action menu.
[TAB/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu

```

Add Community Strings interface

■ **Edit Community Name**

1. Select **<Edit>** .
2. Choose the item that you want to modify and then press **“Enter”**.
3. **Community Name:** type the new name.
4. **Write Access:** Press **“Space”** key to change the right.
5. Select **<Save>**.

```

24TX + 2GB Auto Detect Intelligent Switch : Edit SNMP Community
=====

Community Name : public
Write Access   : Read Only

Actions->  <Edit>  <Save>  <Quit>
Select the action menu.
[TAB/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu

```

Edit Community Strings interface

■ Delete Community Name

1. Select <Delete>.
2. Choose the community name that you want to delete and then press “Enter”.

Trap Managers

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will issue. Create a trap manager by entering the IP address of the station and a community string.

```
24TX + 2GB Auto Detect Intelligent Switch : SNMP Trap Managers
=====
IP          Community Name
-----

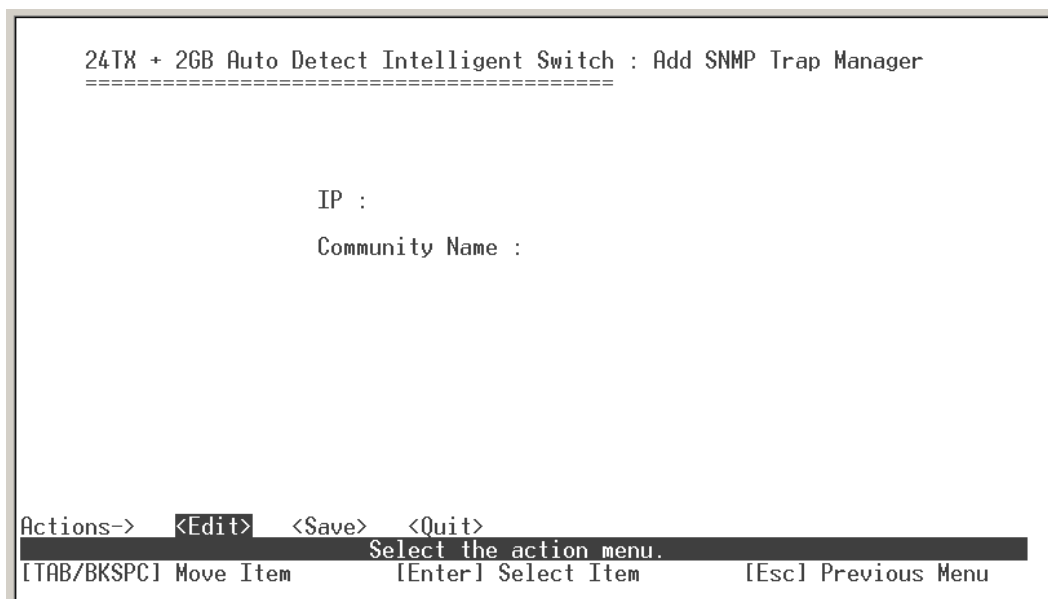
```

```
Actions->  <Add>  <Edit>  <Delete>  <Quit>
Add/Edit/Delete trap managers.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu
```

Trap Managers interface

■ Add the trap manager

1. Select <Add> → <Edit> to add the trap manager.
2. **IP:** enter the IP address of trap manager.
3. **Community Name:** enter the community string.
4. Press “ESC” go back to actions menu line
5. Select <Save> to save all configure.



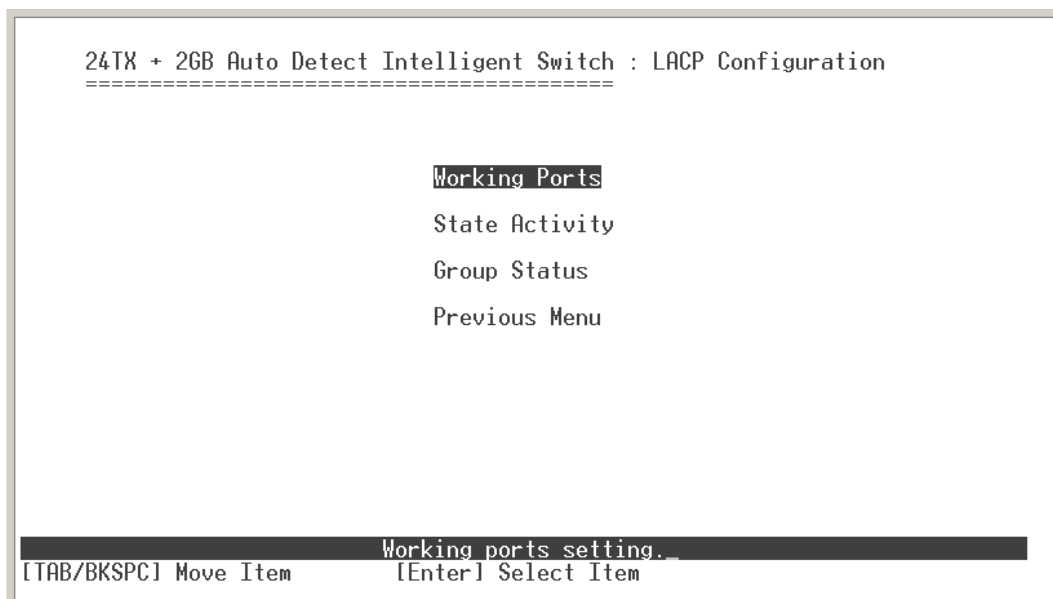
Add Trap Manager interface

■ Delete Trap Manager

1. Select **<Delete>**
2. Choose the trap manager that you want to delete and then press **“Enter”**.

LACP

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode**, more detail information refers to IEEE 802.3ad.



LACP Configuration interface

Working Ports Setting

1. Select **<Edit>**
 2. **Group:** Display the trunk group ID.
 3. **LACP:** Press “**Space**” key to enable or disable LACP (Link Aggregation Control Protocol) support. When LACP enable, the group is LACP static trunk group. When LACP disable, the group is local static trunk group.
 4. **Working Port Num:** The max number of ports can be aggregated at the same time. If LACP static trunk group, the exceed ports is standby and able to aggregate if work ports fail. If it is local static trunk group, the number must be the same as group ports.
 5. Select **<Save>**
- NOTE:** Before set LACP support, you have to set trunk group on the Trunk Configuration.

```

24TX + 2GB Auto Detect Intelligent Switch : LACP Working Ports
=====

      Group      Work Ports
      -----

Actions->  <Edit>  <Save>  <Quit>
           Select the action menu.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu

```

LACP Working Ports configuration interface

LACP State Activity

1. Select **<Edit>**
2. Use “**Space**” key to select the Port State Activity.
 - **Active:** The port automatically sends LACP protocol packets.
 - **Passive:** The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.
3. Select **<Save>**.


```

24TX + 2GB Auto Detect Intelligent Switch : LACP State Activity
=====

Port          State Activity          Port          State Activity
-----

Actions->  <Edit>  <Save>  <Quit>
Select the action menu.
[TAB/BKSPC] Move Item          [Enter] Select Item          [Esc] Previous Menu

```

LACP State Activity configuration interface

Group Status

When you are setting trunk group, you can see the relation information in here.

```

24TX + 2GB Auto Detect Intelligent Switch : LACP Group Status
=====

                Static Trunking Group

Group Key   : 1
Port Member : 1 2 3

Actions->  <Previous Page>  <Next Page>  <Quit>
Select the action menu.
[TAB/BKSPC] Move Item          [Enter] Select Item          [Esc] Previous Menu

```

LACP Group State interface

IGMP/GVRP

You can enable or disable the IGMP/GVRP (GARP VLAN Registration Protocol).

1. Select **<Edit>**
2. Use **"Space"** key to change the value
3. Select **<Save>**

```
24TX + 2GB Auto Detect Intelligent Switch : IGMP/GVRP Configuration
=====

IGMP      : Disable
Query Mode : Disable
GVRP      : Disable

Actions->  <Edit>  <Save>  <Quit>
Select the action menu.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu
```

IGMP/GVRP Configuration interface

802.1x Configuration

```
24TX + 2GB Auto Detect Intelligent Switch : 802.1x Configuration
=====

      802.1x Setup

      System Configuration
      Per Port Setting
      Misc Configuration
      Previous Menu

      Enable or disable 802.1x Protocol function.
[TAB/BKSPC] Move Item      [Enter] Select Item
```

802.1x Configuration interface

802.1x Setup

1. Select **<Edit>**
2. Use “**Space**” key to Enable or Disable the 802.1x.
3. Select **<Save>**

```
24TX + 2GB Auto Detect Intelligent Switch : 802.1x Setup
=====

802.1x : Disable

Actions->  <Edit>  <Save>  <Quit>
           Select the action menu.
[TAB/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu
```

802.1x Setup interface

System Configuration

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

1. Select **<Edit>**.
2. **Radius Server IP:** set the Radius Server IP address.
3. **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.
4. **NAS, Identifier:** set the identifier for the radius client.
5. **Server Port:** set the UDP destination port for authentication requests to the specified Radius Server.
6. **Accounting Port:** set the UDP destination port for accounting requests to the specified Radius Server.
7. Select **<Save>**.

```

24TX + 2GB Auto Detect Intelligent Switch : 802.1x System Configuration
=====

Radius Server IP : 192.168.16.3
Shared Key       : 12345678
NAS, Identifier  : NAS_L2_SWITCH
Server Port      : 1812
Accounting Port  : 1813

Actions->  <Edit>  <Save>  <Quit>
Select the action menu.
[TAB/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu

```

802.1x System Configuration interface

Per Port Configuration

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

```

24TX + 2GB Auto Detect Intelligent Switch : 802.1x Per Port Setting
=====

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

Actions->  <Edit>  <Save>  <Previous Page>  <Next Page>  <Quit>
Select the Action menu.
[TAB/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu

```

802.1x Per Port Setting interface

Misc Configuration

1. Select **<Edit>**
2. **Quiet Period:** set the period during which the port doesn't try to acquire a supplicant.
3. **TX Period:** set the period the port wait for retransmit next EAPOL PDU during an authentication session.
4. **Supplicant Timeout:** set the period of time the switch waits for a supplicant response to an EAP request.
5. **Server Timeout:** set the period of time the switch waits for a server response to an authentication request.
6. **Reauthorize Maximum:** set the number of authentication that must time-out before authentication fails and the authentication session ends.
7. **Reauthorize period:** set the period of time after which clients connected must be re-authenticated.
8. Select **<Save>**

```
24TX + 2GB Auto Detect Intelligent Switch : 802.1x Misc Configuration
=====

Quiet Period (0..65535, Default=60)      : 60
Tx Period (0..65535, Default=30)         : 30
Supplicant Timeout (1..300, Default=30)   : 30
Server Timeout (1..300, Default=30)       : 30
Reauthorize Maximum (1..10, Default=2)    : 2
Reauth Period (1..9999999, Default=3600) : 3600

Actions->  <Edit>  <Save>  <Quit>
           Select the action menu.
[TAB/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu
```

802.1x Misc Configuration interface

System Reset Configuration

You can reset the system back to default value, reboot the system and update the system firmware.

```
24TX + 2GB Auto Detect Intelligent Switch : System Reset Configuration
=====

Factory Default
System Reboot
TFTP Configuration
Previous Menu

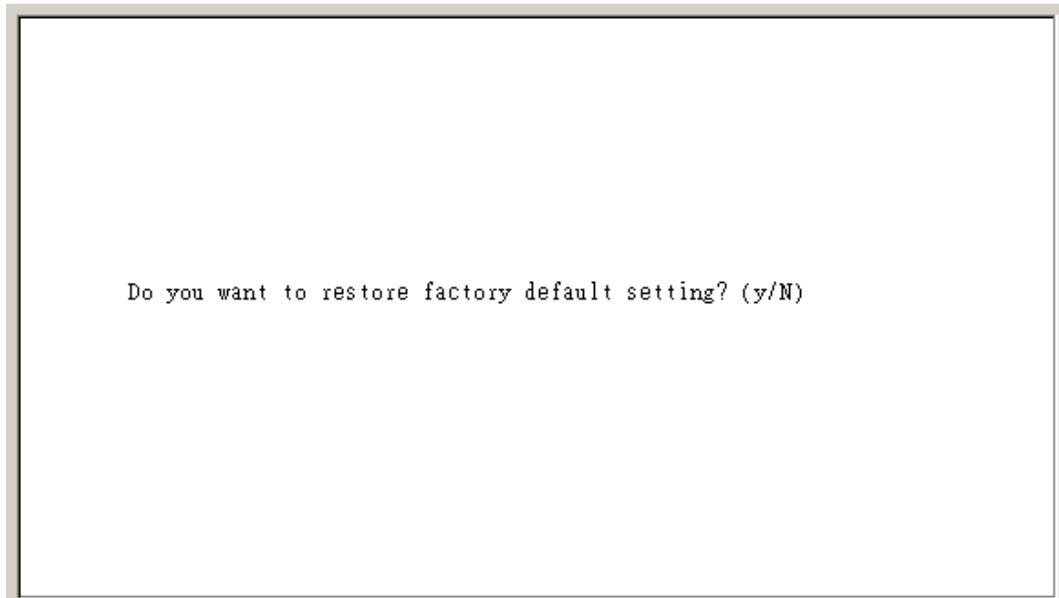
Restore to factory default setting.
[TAB/BKSPC] Move Item      [Enter] Select Item
```

System Reset Configuration interface

Factory Default

Reset switch to default configuration.

Press “Y”, switch will load default setting. After finished load default setting, switch will reboot automatically.



Factory Default interface

System Reboot

Reboot the switch in software reset.

TFTP Configuration

It provides user to update firmware or restore EEPROM value or upload current EEPROM value.



TFTP Update Firmware interface

Update Firmware

It provides the TFTP updating firmware.

1. Start the TFTP server, and copy new firmware version image file to the TFTP server.
2. Select **<Edit>**.
3. **TFTP Server IP:** type the IP of TFTP server.
4. **Firmware File Name:** type the image file name.
5. Press "**ESC**" to back to action line.
6. Select **<Save>**, the system will start to download the image file.
7. When save successfully, the image file download finished, too.
8. Restart switch.

```
24TX + 2GB Auto Detect Intelligent Switch : TFTP Update Firmware
=====

TFTP Server IP      : 192.168.16.2
Firmware File Name : image.bin

Actions->  <Edit>  <Save>  <Quit>
           Select the action menu.
[TAB/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu
```

Update Firmware interface

TFTP Restore Configuration

You can restore EEPROM value, which saved in TFTP server, from TFTP server.

1. Start the TFTP server.
2. Select **<Edit>**.
3. **TFTP Server IP:** type the IP of TFTP server.
4. **Restore File Name:** type the image file name.
5. Press "**ESC**" back to action menu line.
6. Select **<Save>**, it will start to download the image file.
7. When save successfully, the image file download finished too.
8. Restart switch.

```
24TX + 2GB Auto Detect Intelligent Switch : TFTP Restore Configuration
=====

TFTP Server IP      : 192.168.16.2
Restore File Name   : data.dat

Actions->  <Edit>  <Save>  <Quit>
           Select the action menu.
[TAB/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu
```

TFTP Restore Configuration interface

TFTP Backup Configuration

You can save current EEPROM value to TFTP server as backup. The backup file can be restore from TFTP server when you need.

1. Start the TFTP server.
2. Select **<Edit>**.
3. **TFTP Server IP:** type the IP of TFTP server.
4. **Backup File Name:** type the image file name.
5. Press “**ESC**” back to action line.
6. Select **<Save>** key, it will start to upload the image file.
7. When save successfully, the image file upload finished too.
8. Restart switch.

```
24TX + 2GB Auto Detect Intelligent Switch : TFTP Backup Configuration
=====

TFTP Server IP   : 192.168.16.2
Backup File Name : data.dat

Actions->  <Edit>  <Save>  <Quit>
Select the action menu.
[TAB/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu
```

TFTP Backup Configuration interface

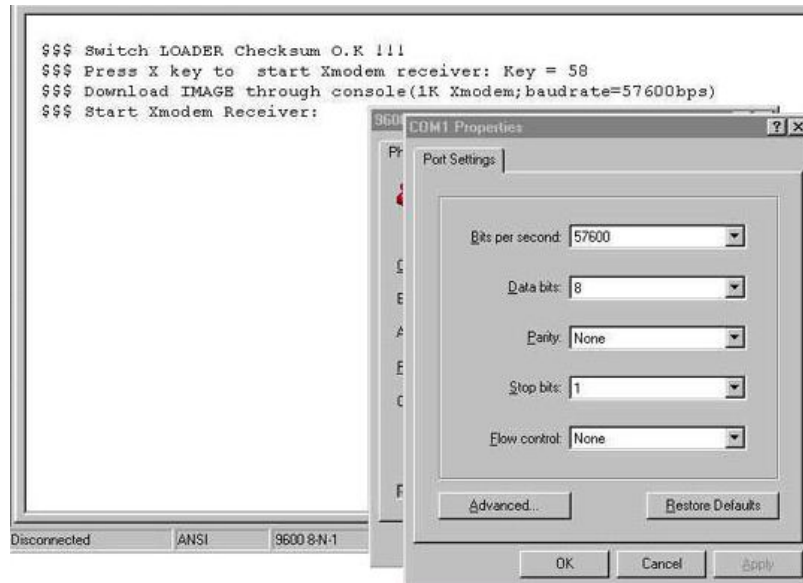
X-modem Upgrade

Before using X-modem upgrade, disconnect terminal and modify baud rate to 57600bps, then connect again.

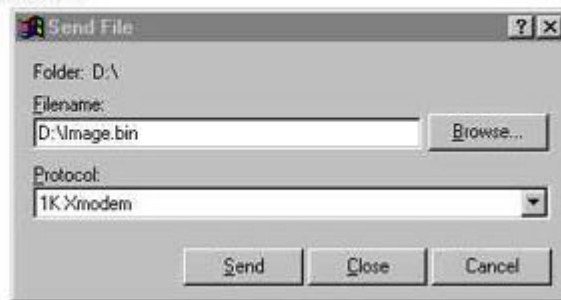
1. Press "X" key to start upgrading from X-modem.
2. You will see the following screen displays.

```
$$$ Switch LOADER Checksum O.K !!!
$$$ Press X key to start Xmodem receiver:
$$$ Download IMAGE through console(1K Xmodem;baudrate=57600bps)
$$$ Start Xmodem Receiver:
```

3. Select "send file" under **Transfer** menu from menu bar.
4. Select "**browse**" button to select the path.
5. Select "**1K X-modem**" of protocol and click "**Send**" button.



```
$$$ Switch LOADER Checksum O.K !!!  
$$$ Press X key to start Xmodem receiver: Key = 58  
$$$ Download IMAGE through console(1K Xmodem;baudrate=57600bps)  
$$$ Start Xmodem Receiver:
```



6. After successfully upgraded the new firmware, please modify baud rate to 9600bps.

5. Web-Based Management

This section introduces the configuration and functions of the Web-Based management.

About Web-based Management

Inside the CPU board of the switch exists an embedded HTML web site residing in flash memory. It offers advanced management features and allow users to manage the switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

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

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

Preparing for Web Management

Before to use web management, you can use console to login the Switch checking the default IP of the Switch. Please refer to **Console Management** Chapter for console login. If you need change IP address in first time, you can use console mode to modify it. The default value is as below:

IP Address: **192.168.0.1**


Subnet Mask: **255.255.255.0**

Default Gateway: **192.168.0.254**

User Name: **admin**

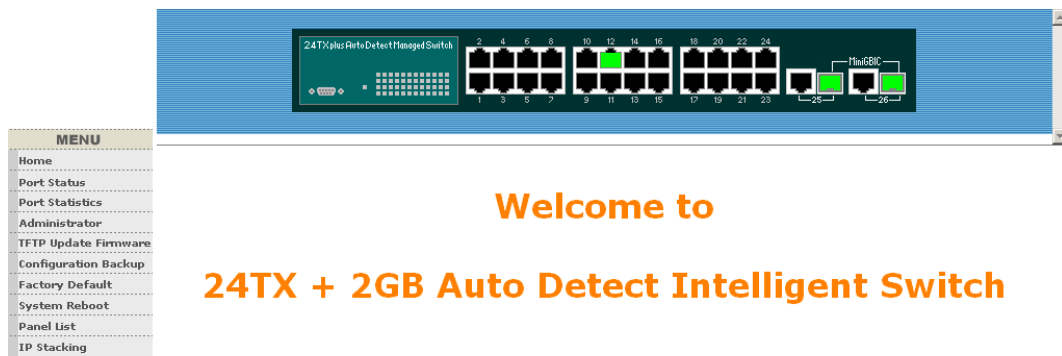
Password: **admin**

Online Help

You can click  button when you have any configuration question during the configuring.

System Login

1. Launch the Internet Explorer.
2. Type http:// and the IP address of the switch. Press “Enter”.
3. The login screen appears.
4. Key in the user name and password. The default user name and password is “admin”.
5. Click “Enter” or “OK”, then the home screen of the Web-based management appears.



Copyright (c) 2004 NETSTAR Technology Corporation, all rights reserved.

TEG-S2620is

Port status

In Port status, you can view every port status that depended on user setting and

the negotiation result.

1. **Link:** “Down” is “No Link”. “UP” is “Link”.
2. **State:** display port statuses “disable” or “enable”. “Unlink” will be treated as “off”.
3. **Auto Negotiation:** display the auto negotiation mode: auto/force/Nway-force. “Config” means the value that user configured. “Actual” means the current value of the port.
4. **Speed Duplex:** display port connection speed. “Config” means the value that user configured. “Actual” means the current value of the port.
5. **Flow Control:** display the flow control status is “enable” or “disable” in full duplex mode. “Config” means the value that user configured. “Actual” means the current value of the port.
6. **Back Pressure:** Display the Back Pressure status setting. “Config” means the value that user configured. “Actual” means the current value of the port.
7. **Bandwidth:** display the port incoming and outgoing bandwidth.
8. **Priority:** display the port static priority status is “High” or “Low” or “Disable”.
9. **Port Security:** display the port security is “enable” or “disable”.

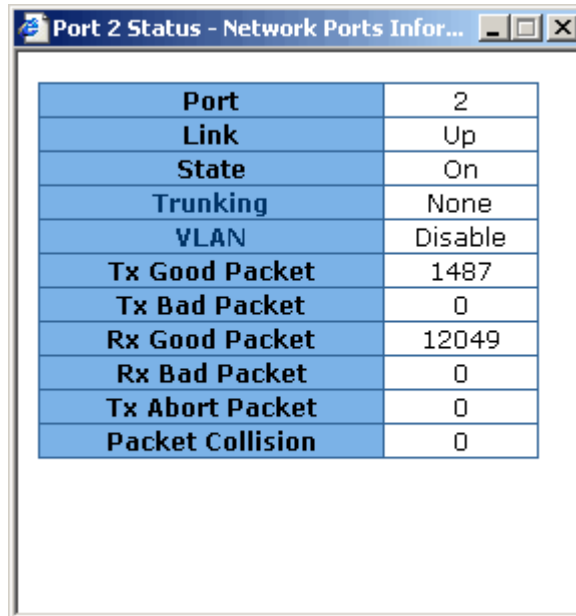
Port Status

Port	Type	Link	State	Negotiation		Speed Duplex		Flow Control		Back Pressure		Band Width		Priority	Security
				Config	Actual	Config	Actual	Config	Actual	Config	Actual	In	Out		
Port.01	100TX	Down	Enable	Auto	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.02	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.03	100TX	Down	Enable	Auto	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.04	100TX	Down	Enable	Auto	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.05	100TX	Down	Enable	Auto	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.06	100TX	Down	Enable	Auto	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.07	100TX	Down	Enable	Auto	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.08	100TX	Down	Enable	Auto	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.09	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.10	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.11	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.12	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.13	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.14	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.15	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.16	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.17	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.18	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.19	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.20	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.21	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.22	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.23	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.24	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.25	Auto	Down	Enable	Auto	N/A	1G Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.26	Auto	Up	Enable	Force	Auto	1G Full	1G Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF

Port Status interface

View the Port Information

You can direct click the port on the Switch figure on the top of web page. Then, you will see the port information.



Port	2
Link	Up
State	On
Trunking	None
VLAN	Disable
Tx Good Packet	1487
Tx Bad Packet	0
Rx Good Packet	12049
Rx Bad Packet	0
Tx Abort Packet	0
Packet Collision	0

Port information interface

Port Statistics

The following information provides a view of the current port statistic information.

Click 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
Port.01	100TX	Down	Enable	0	0	0	0	0	0
Port.02	100TX	Up	Enable	1856	0	13674	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0
Port.07	100TX	Down	Enable	0	0	0	0	0	0
Port.08	100TX	Down	Enable	0	0	0	0	0	0
Port.09	100TX	Up	Enable	11834	0	0	0	0	0
Port.10	100TX	Up	Enable	11834	0	0	0	0	0
Port.11	100TX	Up	Enable	11834	0	0	0	0	0
Port.12	100TX	Up	Enable	11834	0	0	0	0	0
Port.13	100TX	Up	Enable	11834	0	0	0	0	0
Port.14	100TX	Up	Enable	11834	0	0	0	0	0
Port.15	100TX	Up	Enable	11834	0	0	0	0	0
Port.16	100TX	Up	Enable	11834	0	0	0	0	0
Port.17	100TX	Up	Enable	11834	0	0	0	0	0
Port.18	100TX	Up	Enable	11834	0	0	0	0	0
Port.19	100TX	Up	Enable	11834	0	0	0	0	0
Port.20	100TX	Up	Enable	11834	0	0	0	0	0
Port.21	100TX	Up	Enable	11834	0	0	0	0	0

Clear

Port Statistics

Administrator

In Administrator function, it provides the following functions:

IP Configuration, Switch Settings, Console Port Information, Port Controls, Trunking, Forwarding and Filtering, VLAN Configuration, Spanning Tree, Port Mirroring, SNMP Management, Security Manager, and 802.1x Configuration.



Administrator interface

IP Address

User can configure the IP Settings and DHCP client function, than clicks button. After reset the IP address, you must reboot the switch.

- **DHCP:** disable or enable the DHCP client function.
- **IP Address:** assign the switch IP address. The default IP is 192.168.0.1.
- **Subnet Mask:** assign the switch IP subnet mask.
- **Gateway:** assign the switch gateway. The default value is 192.168.0.254.

IP Configuration

DHCP Client :

IP Address	<input type="text" value="192.168.0.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.0.254"/>

IP configuration interface

Switch Setting

In Switch setting, it has three parts of setting – Basic, Advance, and Misc Config. We will describe the configure detail in following.

Basic Switch Settings

In Basic Switch Setting, it displays the switch basic information.

- **System Name:** the name of switch.
- **System Location:** the switch physical location.
- **System Description:** the description of switch.
- **Firmware Version:** the switch's firmware version.
- **Kernel Version:** the kernel software version.
- **Hardware version:** the switch hardware version.
- **MAC Address:** the unique hardware address assigned by manufacturer (default)
- **Module:** the module information, if the switch doesn't install the module, then this column will not display any information.

Switch Settings

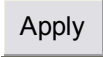
Basic Advanced Misc Config

System Name	
System Location	
System Description	24 TX Port + 2 Giga Auto Detect Intelligent Switch
Firmware Version	v1.00
Kernel Version	v3.00
Hardware Version	A7.00
MAC Address	001122334455

Module	Type	Description
Port 25	Auto	1000TX Copper/1000FX MiniGBIC
Port 26	Auto	1000TX Copper/1000FX MiniGBIC

Switch basic setting interface

Advanced Setting

In Advanced setting, it has two sections – MAC Table Address Entry and Priority Queue Service. After the configuration, click  button to complete the configuration.

■ **Enable MAC address Aging Out:** to enable the MAC address age out function. When it is disabling, the following configure item will not function.

- ✧ **Age-out Time:** fill in the number of seconds that an inactive MAC address remains in the switch's address table. The valid range is 300~765 seconds. Default is 300 seconds.
- ✧ **Max Bridge Transmit Delay Bound Control:** limit the packets queuing time in switch. If enable, the packets queued exceed will be drop. This valid value are 1sec, 2 sec, 4 sec and off.
- ✧ **Enable Low Queue Delay Bound:** limit the low priority packets queuing time in switch. If the low priority packet stays in switch exceed Max Delay Time, it will be sent. The valid range is 1~255 ms.

NOTE: Make sure of “Max bridge transit delay bound control” is enabled before enable Delay Bound, because Enable Delay Bound must be work under “Max bridge transit delay bound control is enabled” situation.

- ✧ **Broadcast Storm Filter:** configure broadcast storm control. Enable it and set the upper threshold for individual ports. The threshold is the percentage of the port's total bandwidth used by broadcast traffic. When broadcast traffic for a port rises above the threshold you set, broadcast storm control becomes active. The valid threshold value are 5%, 10%, 15%, 20%, 25% and off.

Switch Settings

Basic | **Advanced** | Misc Config

Enable MAC Address Aging Out
Age-Out Time : seconds (300..765, must multiple of 3)

Max Bridge Transmit Delay Bound :

Enable Low Queue Delay Bound ----- Max Delay Time : (1..255, 2ms/unit)

Broadcast Storm Filter Mode :

Priority Queue Service

802.1p Priority

First Come First Service

All High Before Low

Weight Round Ratio

Qos Policy (Checked for High Priority) :

Level0 Level1 Level2 Level3 Level4 Level5 Level6 Level7

Switch Advanced setting interface

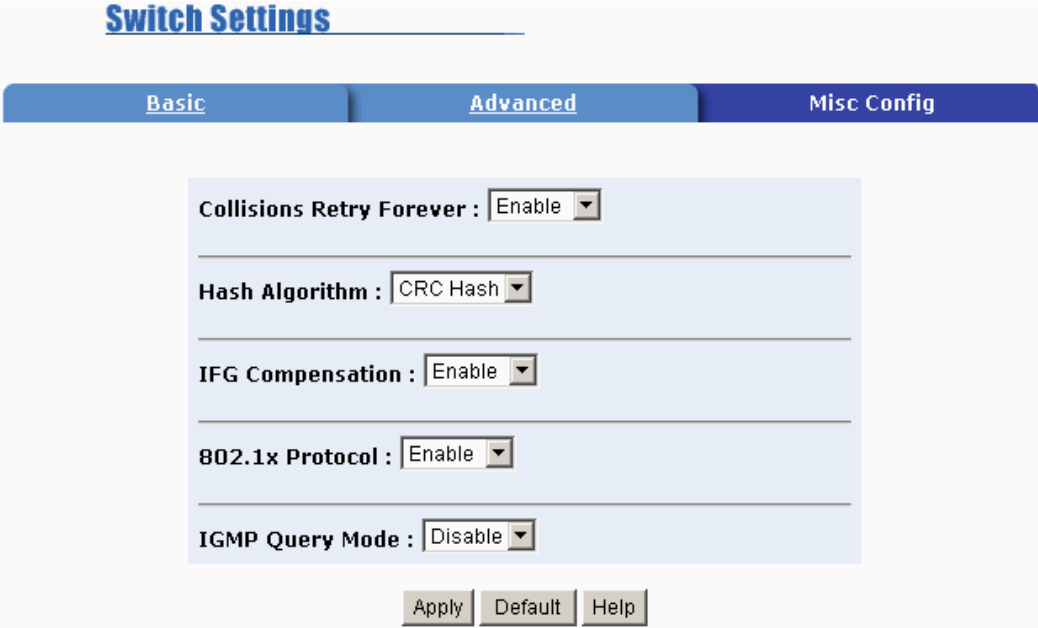
- **Priority Queue Service settings:** select the priority queue service type.
 - ✧ **First Come First Service:** the sequence of packets sent is depend on arrive order.
 - ✧ **All High before Low:** the high priority packets sent before low priority packets.
 - ✧ **Weighted Round Ratio:** select the preference given to packets in the switch's high-priority queue. These options represent the number of high priority packets sent before one low priority packet is sent. For example, 5 High: 1 Low means that the switch sends 5 high priority packets before sending 1 low priority packet.
- **Qos Policy: High Priority Levels:** 0~7 priority level can map to high or low queue.

Misc Config

- **Collisions Retry Forever:** disable is in half duplex. If happen collision will

retry 48 times and then drop frame. Enable is in half duplex. If happen collision will retry forever.

- **Hash Algorithm:** CRC Hash or Direct Map for MAC address learning algorithm
- **IFG Compensation:** Internal Packet Gap time compensation configure. Select to “Enable” or “Disable”.
- **802.1x Protocol:** enable or disable 802.1x protocol.
- **IGMP Query Mode:** recognizes different queries from clients or servers to decide which Query will be the first priority. The modes are:
 - a. **Auto Mode:** chooses the switch that has the smallest IP address to be set for the IGMP Query mode.
 - b. **Enable Mode:** enables the switch to be the IGMP Querier.
 - c. **Disable Mode:** disables all other switches from being the IGMP Querier.



Switch Settings

Basic **Advanced** Misc Config

Collisions Retry Forever : Enable

Hash Algorithm : CRC Hash

IFG Compensation : Enable

802.1x Protocol : Enable

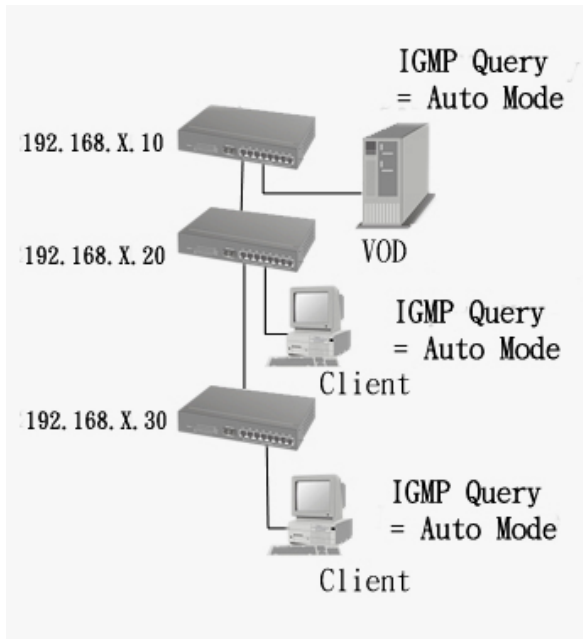
IGMP Query Mode : Disable

Apply Default Help

Switch Misc Config setting interface

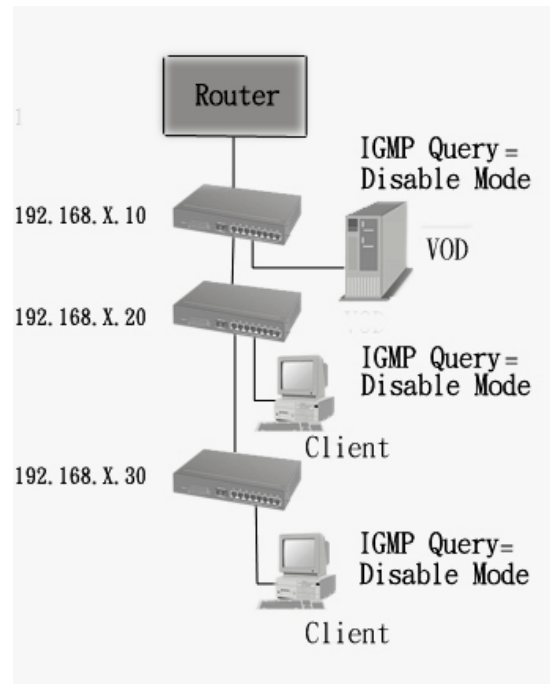
■ IGMP Theory of Operation

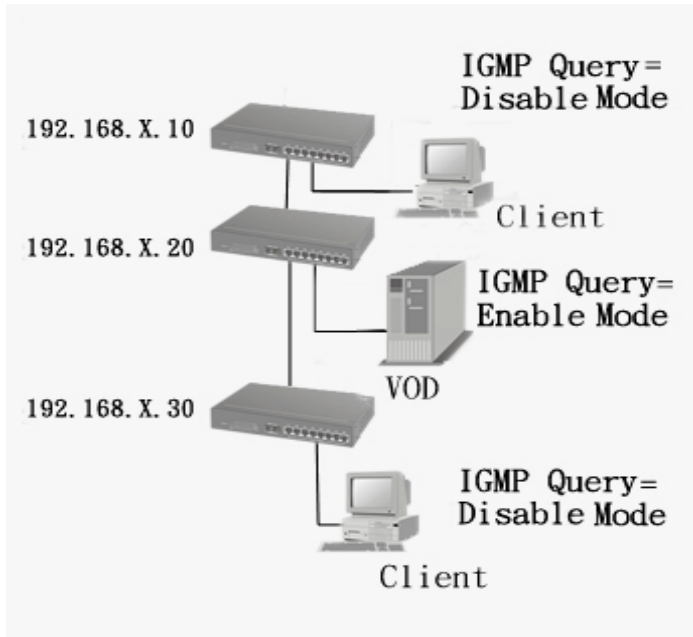
The following three topologies detail how IGMP Query works and to be configured within a network:



1. Auto mode needs to be enabled when the router's IP address is smaller than other switches in the subnet.

2. IGMP needs to be enabled when the router's IP address is not smaller than other switches in the subnet. This Router supports IGMP protocol, but IGMP has to be enabled, and the Router has to be the Querier.





3. The following topology must be set when the IP address of the switch is not the smallest in the subnet. The network will cause a multi-cast storm from the IGMP client report if it is in Auto mode. All switches must be in disable mode when the VOD server is configured for IGMP Querier.

Note: It is suggested that the VOD server switch have the smallest IP address.

Console Port Information

Console is a standard UART interface to communicate with Serial Port. User can use windows HyperTerminal program to link the switch. Please refer to **Console Management** → **Console login** for detail steps.

Console port information shows as follow:

Bits per seconds: 9600

Data bits: 8

Parity: none

Stop Bits: 1

Flow control: none

Console Port Information

Baud Rate (bps)	9600
Parity Check	none
Data Bits (bit)	8
Stop Bits (bit)	1
Flow Control	none

Console Port Information interface

Port Controls

You can change the port status.

1. Select the port by scroll the list in **Port** column.
2. **State:** User can disable or enable this port control.
3. **Negotiation:** User can set auto negotiation mode is Auto, Nway (specify the speed/duplex on this port and enable auto-negotiation), Force of the port.
4. **Speed:** set the speed of each port.
5. **Duplex:** set full-duplex or half-duplex mode of the port.
6. **Flows control:** set flow control function is **ON** or **OFF** in Full Duplex mode.
7. **Back Pressure:** set Back Pressure is **ON** or **OFF** in Half Duplex mode.
8. **Band Width:** The port1 ~ port 24, supports port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set it's effective

egress rate is 1Mbps, ingress rate is 500Kbps. The switch will perform flow control or Back Pressure to confine the ingress rate to meet the specified rate.

- **In:** fill in the port effective ingress rate. The valid range is 0 ~ 999. The unit is 100K. 0: disable rate control. 1 ~ 999: valid rate value.
- **Out:** fill in the port effective egress rate. The valid range is 0~999. The unit is 100K. 0: disable rate control. 1 ~ 999: valid rate value.

9. **Priority:** this static priority based on port, if you set the port is high priority, income frame from this port always high priority frame.
10. **Security:** when the port is in security mode, the port will be “locked” without permission of address learning. Only the incoming packets with SMAC already existing in the address table can be forwarded normally. User can disable the port from learning any new MAC addresses, and then use the static MAC addresses screen to define a list of MAC addresses that can use the secure port.
11. Click Apply button to apply all configuration.
12. When you select the port, you can see port current configure shows in below column.

Port Controls

Port	State	Negotiation	Speed	Duplex	Flow Control	Back Pressure	Band Width		Priority	Security
							In	Out		
Port.01										
Port.02	Enable	Auto	100	Full	ON	OFF	0	0	Disable	<input type="checkbox"/>
Port.03										
Port.04										

Apply

Port	Type	Link	State	Negotiation		Speed Duplex		Flow Control		Back Pressure		Band Width		Priority	Security
				Config	Actual	Config	Actual	Config	Actual	Config	Actual	In	Out		
Port.02	100TX	Up	Enable	Auto	Auto	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF

Port Control interface

Trunking

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode**, more detail information refers to IEEE 802.3ad.

Aggregator setting

1. **System Priority:** a value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
2. **Group ID:** There are seven trunk groups to provided configure. Choose the "Group ID" and click .
3. **LACP:** If enable, the group is LACP static trunk group. If disable, the group is local static trunk group. All ports support LACP dynamic trunking group. If connecting to the device that also supports LACP, the LACP dynamic trunking group will be created automatically.
4. **Work ports:** allow max four ports can be aggregated at the same time. If LACP static trunk group, the exceed ports are standby and able to aggregate if work ports fail. If it is local static trunk group, the number must be as same as the group member ports.
5. Select the ports to join the trunk group. Allow max four ports can be aggregated at the same time. Click button to add the port. To remove unwanted ports, select the port and click button.
6. If LACP enable, you can configure LACP Active/Passive status in each ports

on State Activity page.

7. Click **Apply**.
8. Use **Delete** button to delete Trunk Group. Select the Group ID and click **Delete** button.

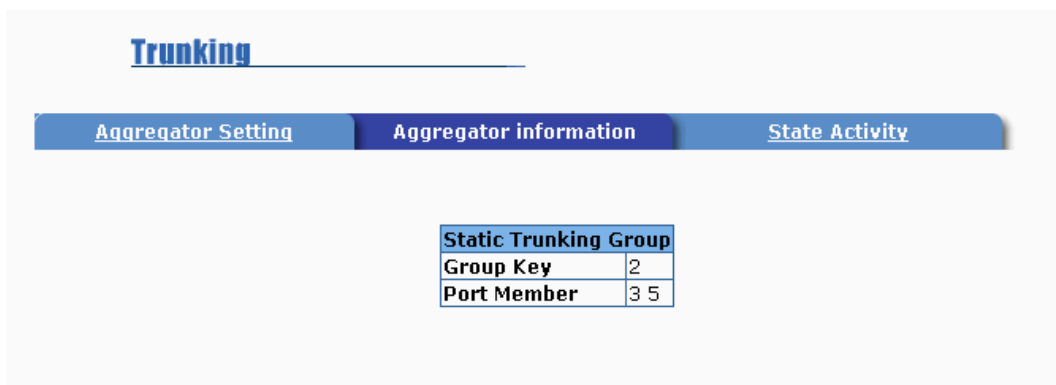
System Priority			
1			
Group ID	Trunk.1	Select	
Lacp	Disable		
Work Ports	0		
	<<Add		Port.01
	Remove>>		Port.02
			Port.03
			Port.04
			Port.05
			Port.06
			Port.07
			Port.08
			Port.09

Apply Delete Help

Trunking—Aggregator Setting interface

Aggregator Information

When you had setup the LACP aggregator, you will see relation information in here.



Trunking – Aggregator Information interface

State Activity

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

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

Note:

1. A link having either two active LACP ports or one active port can perform dynamic LACP trunking.
2. A link has two passive LACP ports will not perform dynamic LACP trunking because both ports are waiting for and LACP protocol packet from the opposite device.
3. If you are active LACP's actor, when you are select trunking port, the active status will be created automatically.

Trunking

Aggregator Setting

Aggregator information

State Activity

Port	LACP State Activity	Port	LACP State Activity
1	<input checked="" type="checkbox"/> Active	2	<input checked="" type="checkbox"/> Active
3	N/A	4	N/A
5	N/A	6	N/A
7	N/A	8	N/A
9	N/A	10	N/A
11	N/A	12	N/A
13	N/A	14	N/A
15	N/A	16	N/A
17	N/A	18	N/A
19	N/A	20	N/A
21	N/A	22	N/A
23	N/A	24	N/A
25	N/A	26	N/A

Apply Help

Trunking – State Activity interface

Forwarding and Filtering

IGMP Snooping

The switch support IP multicast, you can enable IGMP protocol on web management's switch setting advanced page, then display the IGMP snooping information in this page, you can view difference multicast group VID and member port in here, IP multicast addresses range from 224.0.0.0 through 239.255.255.255.

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

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

When you enable the IGMP Snooping, you will see the relate information show as following figure.

Forwarding and Filtering

IGMP Snooping Static MAC Addresses MAC Filtering

IP Address	VLAN ID	Member Port
224.000.000.002	0	*2*****
224.000.000.009	0	*2*****
224.000.001.024	0	*2*****
235.080.068.083	0	*2*****
239.255.255.250	0	*2*****

IGMP Protocol:

IGMP Snooping interface

Static MAC Address

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

1. In **MAC Address** column, enter the MAC address to and from which the port should permanently forward traffic, regardless of the device network activity.
2. In the **Port Number** box, select a port number.
3. **VLAN ID:** If tag-based (IEEE 802.1Q) VLANs are set up on the switch, static addresses are associated with individual VLANs. Type the VID (tag-based VLANs) to associate with the MAC address.
4. Click button.
5. Use button to delete unwanted MAC address.

Forwarding and Filtering

[IGMP Snooping](#) **Static MAC Addresses** [MAC Filtering](#)

MAC Address _____ Port _____ VLAN ID

MAC Address

Port No.

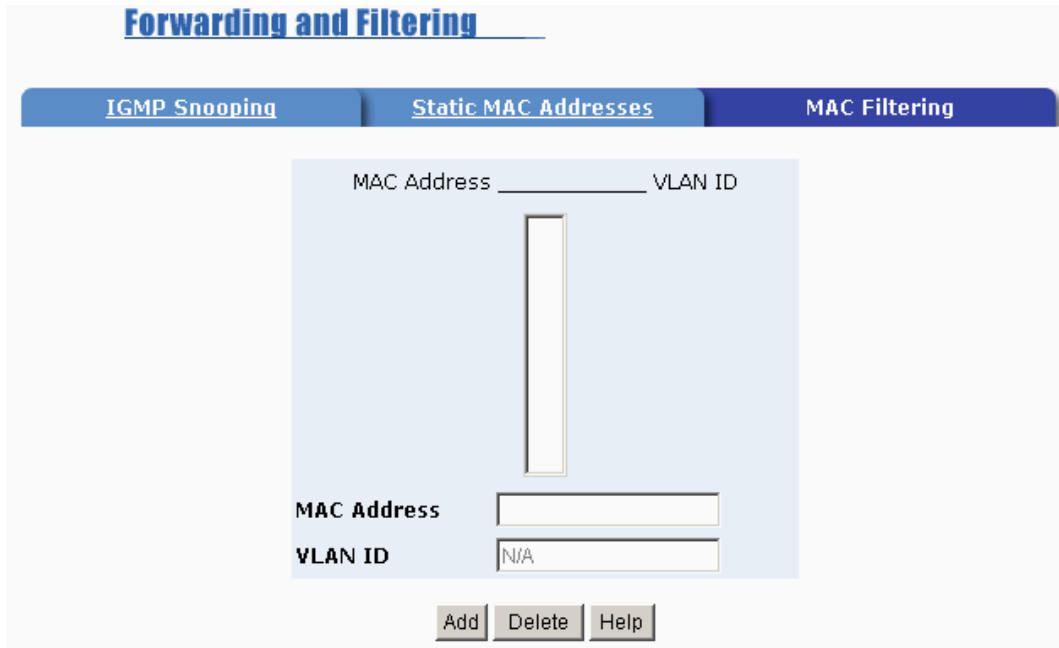
VLAN ID

Static MAC Address interface

MAC filtering

MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination addresses.

1. In **MAC Address** box, enter the MAC address that wants to filter.
2. **VLAN ID:** If tag-based (802.1Q) VLAN are set up on the switch, in the VLAN ID box, type the VID to associate with the MAC address.
3. Click button.
4. Use button to delete unwanted MAC address.



MAC Filtering interface

VLAN configuration

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

The switch supports port-based, 802.1Q (tagged-based) and protocol-base VLAN in web management page. In the default configuration, VLAN support is “disable”.

VLAN Configuration

VLAN Operation Mode :

Enable GVRP Protocol

VLAN NOT ENABLE

VLAN Configuration interface

Port-based VLAN

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

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

VLAN Configuration

VLAN Operation Mode :

Enable GVRP Protocol

VLAN – PortBase interface

1. Click to create a new VLAN group.
2. Enter the Group name, VLAN ID and select the members of VLAN group.
3. Click .

VLAN Configuration

VLAN Operation Mode :

Enable GVRP Protocol

Group Name

VLAN ID

Port.01 ▲

Port.02

Port.03

Port.04

Port.05

Port.06

Port.07

Port.08

Port.09

Port.10

Port.11

Port.12 ▼

VLAN—PortBase Add interface

4. You will see the VLAN displays.
5. If the groups' list is over one page, you can click [Next Page](#) to view other VLAN groups.
6. Use [Delete](#) button to delete unwanted VLAN.
7. Use [Edit](#) button to modify existing VLAN group.

802.1Q VLAN

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

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

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

802.1q VLAN interface

■ **Basic**

1. Click **Add** button.
2. **Enable GVRP Protocol:** check the check box to enable GVRP protocol.
3. **Group Name:** assign a name for the new VLAN.
4. **VLAN ID:** fill in a VLAN ID (between 2-4094). The default is 1.
5. **Protocol VLAN:** choose the protocol type. Default is NONE.
6. From the Available ports box, select ports to add to the switch and click **Add** button. If the trunk groups exist, you can see it in here (ex: TRK1, TRK2...), and you can configure it is the member of the VLAN or not.

VLAN Configuration

VLAN Operation Mode : 802.1Q
 Enable GVRP Protocol

Basic | **Port VID**

Group Name :

VLAN ID : 1

Protocol VLAN : NONE

Port.01
Port.02
Port.03
Port.04
Port.05
Port.06
Port.07
Port.08
Port.09
Port.10
Port.11
Port.12

Add
Remove

Next Help

802.1q VLAN –Add interface

7. Click **Next**. Then you will see the page as follow.

VLAN Configuration

VLAN Operation Mode : 802.1Q
 Enable GVRP Protocol

VLAN Name	VLAN02			
VLAN ID	2			
UnTag Member				
Port.08	Untag	Port.09	Untag	
Port.10	Untag			

Apply

8. To set the outgoing frames are VLAN-Tagged frames or untagged. Then click

.

- Tag: outgoing frames with VLAN-Tagged.
- Untag: outgoing frames without VLAN-Tagged.

■ **Port VID:** Configure port VID settings

1. **Port VLAN ID:** enter the port VLAN ID.

2. **Ingress Filtering:** Ingress filtering lets frames belonging to a specific VLAN to be forwarded if the port belongs to that VLAN.

- **Enable:** Forward only packets with VID matching this port's configured VID.

- **Disable:** Disable Ingress filter function

3. **Acceptable Frame type:**

- **Tag Only:** Only packet with match VLAN ID can be permission to go through the port.

- **ALL:** Acceptable all Packet

4. **VLAN ID Range:** select a range of VLAN ID. There are 16 VLAN ID range. The ports are assigned to the same VLAN ID will be in the same VLAN group.

5. Click .

6. To reset back to default value, click button.

Basic		Port VLAN ID		
Port	Port VLAN ID	Ingress Filter	Acceptable Frame Type	VLAN ID Range
Port.01 Port.02 Port.03 Port.04	1	Enable	All	256~511

Apply Default Help

Port	VLAN ID	Ingress Filter	Acceptable Frame Type
Port.02	1	Enable	All

802.1q VLAN – Port VLAN ID interface

Spanning Tree

The Spanning-Tree Protocol (STP) is a standardized method (IEEE 802.1d) for avoiding loops in switched networks. When STP enabled, to ensure that only one path at a time is active between any two nodes on the network. We are recommended that you enable STP on all switches ensures a single active path on the network.

Spanning Tree

System Configuration		Per Port Configuration	
STP State	<input type="checkbox"/>		
Priority (0-65535)	32768		
Max Age (6-40)	20		
Hello Time (1-10)	2		
Forward Delay Time (4-30)	15		


Apply

Root Bridge Information

Priority	32768
Mac Address	001122334455
Root Path Cost	0
Root Port	Root
Max Age	20
Hello Time	2
Forward Delay	15


Spanning Tree – System Configuration interface

System Configuration

1. You can view spanning tree information about the Root Bridge.
2. You can view spanning tree status about the switch.
3. You can modify STP state. After modification, click  button.
 - **Priority:** assign path priority number.
 - **Max Age:** the maximum path age
 - **Hello Time:** the time that controls switch sends out the BPDU packet to check STP current status.
 - **Forward Delay Time:** forward delay time.

Per Port Configuration

You can configure path cost and priority of every port.

1. Select the port in Port column.
2. Assign the **Path Cost**. The value range is from 1 to 65535.
3. Assign the **port priority value**. The value range is from 0 to 255. The lowest value has higher priority.
4. Click  button.

Spanning Tree

System Configuration
Per Port Configuration

Port	Path Cost (1-65535)	Priority (0-255)
<div style="border: 1px solid #ccc; padding: 2px;"> Port.01 ▲ Port.02 Port.03 Port.04 Port.05 ▼ </div>	<input style="width: 50px; height: 20px;" type="text" value="10"/>	<input style="width: 50px; height: 20px;" type="text" value="128"/>

STP Port Status

Port	Path Cost	Priority	State
Port.01	10	0	Forwarding
Port.02	10	0	Forwarding
Port.03	10	0	Forwarding
Port.04	10	0	Forwarding
Port.05	10	0	Forwarding
Port.06	10	0	Forwarding
Port.07	10	0	Forwarding
Port.08	10	0	Forwarding
Port.09	10	0	Forwarding
Port.10	10	0	Forwarding
Port.11	10	0	Forwarding
Port.12	10	0	Forwarding
Port.13	10	0	Forwarding
Port.14	10	0	Forwarding
Port.15	10	0	Forwarding
Port.16	10	0	Forwarding
Port.17	10	0	Forwarding
Port.18	10	0	Forwarding
Port.19	10	0	Forwarding
Port.20	10	0	Forwarding
Port.21	10	0	Forwarding
Port.22	10	0	Forwarding
Port.23	10	0	Forwarding
Port.24	10	0	Forwarding
Port.25	4	0	Forwarding
Port.26	4	0	Forwarding

SPT – Per Port Configuration interface

Port Mirroring

The Port mirroring is a method for monitor traffic in switched networks. Traffic through ports can be monitored by one specific port. That is, traffic goes in or out monitored ports will be duplicated into mirror port.

1. **Port Mirroring State:** set mirror mode: Disable, RX, TX, and Both.
2. **Analysis Port:** It's mean mirror port can be used to see all monitor port traffic. You can connect mirror port to LAN analyzer or Netxray.
3. **Monitor Port:** the ports you want to monitor. All monitor port traffic will be copied to mirror port. You can select max 25 monitor ports in the switch. User

can choose which port to monitor in only one mirror mode.

Note: If you want to disable the function, you must select monitor port to none.

Port Mirroring

Port Mirroring State : <input type="button" value="Disable"/>	
Analysis Port : <input type="button" value="None"/>	
Monitor Port	State
Port.01	<input type="checkbox"/>
Port.02	<input type="checkbox"/>
Port.03	<input type="checkbox"/>
Port.04	<input type="checkbox"/>
Port.05	<input type="checkbox"/>
Port.06	<input type="checkbox"/>
Port.07	<input type="checkbox"/>
Port.08	<input type="checkbox"/>
Port.09	<input type="checkbox"/>
Port.10	<input type="checkbox"/>
Port.11	<input type="checkbox"/>
Port.12	<input type="checkbox"/>
Port.13	<input type="checkbox"/>
Port.14	<input type="checkbox"/>
Port.15	<input type="checkbox"/>
Port.16	<input type="checkbox"/>
Port.17	<input type="checkbox"/>
Port.18	<input type="checkbox"/>
Port.19	<input type="checkbox"/>
Port.20	<input type="checkbox"/>
Port.21	<input type="checkbox"/>
Port.22	<input type="checkbox"/>
Port.23	<input type="checkbox"/>
Port.24	<input type="checkbox"/>
Port.25	<input type="checkbox"/>
Port.26	<input type="checkbox"/>

Port Mirroring interface

SNMP Management

The SNMP is a Protocol that governs the transfer of information between management and agent. The switch supports SNMP V1.

You can define management stations as trap managers and to enter SNMP

community strings. You also can define a name, location, and contact person for the switch. Fill in the system options data, and then click Apply to update the changes.

■ System Options

1. **Name:** enter a name for the switch.
2. **Location:** enter the switch physical location.
3. **Contact:** enter the name of contact person or organization.

SNMP Management

The screenshot displays the SNMP Management interface with three main sections:

- System Options:** Contains three text input fields for 'Name', 'Location', and 'Contact'. Below these fields are 'Apply' and 'Help' buttons.
- Community Strings:** Features a list of 'Current Strings' (public__RO, private__RW) with 'Add' and 'Remove' buttons. To the right, there is a 'New Community String' section with a 'String' input field and radio buttons for 'RO' (selected) and 'RW'.
- Trap Managers:** Features a list of 'Current Managers' (none) with 'Add' and 'Remove' buttons. To the right, there is a 'New Manager' section with 'IP Address' and 'Community' input fields.

SNMP Management interface

■ Community strings

Serve as a password between trap manager and switch.

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

MIB-object information and to set MIB objects.

4. Click .

■ Trap Manager

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will issue. Create a trap manager by entering the IP address of the station and a community string.

1. **IP Address:** fill in the trap device IP.
2. **Community Strings:** the trap device community strings.
3. Click .

Security Manager

You can change web management login user name and password.

1. **User name:** type the new user name. The default is “**admin**”
2. **Password:** type the new password. The default is “**admin**”
Confirm password: retype the new password.
3. Click .

Security Manager

User Name :	<input type="text" value="admin"/>
New Password :	<input type="password" value="....."/>
Confirm Password :	<input type="password" value="....."/>
	<input type="button" value="Apply"/>

Security Manager interface

802.1X

When enabling the IEEE 802.1X function, you can configure the parameters of this function.

System Configuration

1. **Radius Server IP:** set the Radius Server IP address.
2. **Server Port:** set the UDP destination port for authentication requests to the specified Radius Server.
3. **Accounting Port:** set the UDP destination port for accounting requests to the specified Radius Server.
4. **Shared Key:** set an encryption key for use during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
5. **NAS, Identifier:** set the identifier for the radius client.
6. Click .

802.1x Configuration		
System Configuration	Per Port Configuration	Misc Configuration
Radius Server IP	<input type="text" value="192.168.16.3"/>	
Server Port	<input type="text" value="1812"/>	
Accounting Port	<input type="text" value="1813"/>	
Shared Key	<input type="text" value="12345678"/>	
NAS, Identifier	<input type="text" value="NAS_L2_SWITCH"/>	

802.1x Configuration – System Configuration interface

Per port Configuration

1. Select the port in Port column.
2. Select the state of port. There are four states:
 - **Reject:** the specified port is required to be held in the Unauthorized state.
 - **Accept:** the specified port is required to be held in the Authorized state.
 - **Authorized:** the specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
 - **Disable:** The specified port is required to be held in the Authorized state.
3. Click .
4. You can see the every port Authorization information list in table.

802.1x Configuration

System Configuration **Per Port Configuration** Misc Configuration

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

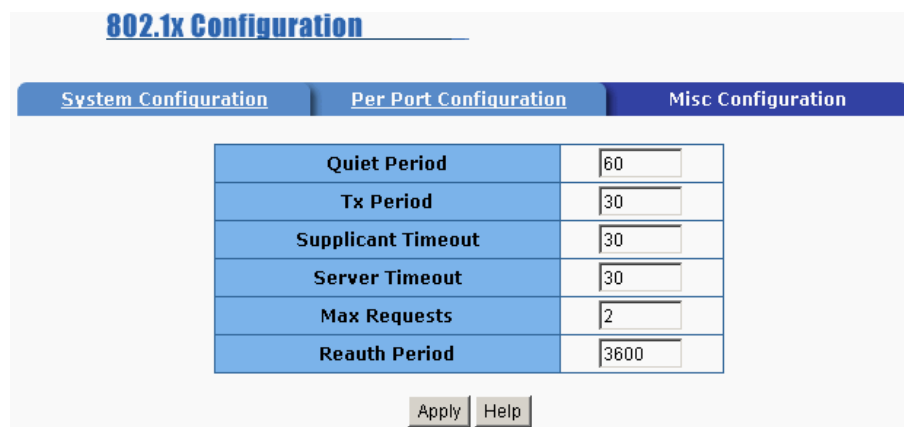
Port Authorization

Port	State
Port.01	Disable
Port.02	Disable
Port.03	Disable
Port.04	Disable
Port.05	Disable
Port.06	Disable
Port.07	Disable
Port.08	Disable
Port.09	Disable
Port.10	Disable
Port.11	Disable
Port.12	Disable
Port.13	Disable
Port.14	Disable
Port.15	Disable
Port.16	Disable
Port.17	Disable
Port.18	Disable
Port.19	Disable
Port.20	Disable
Port.21	Disable
Port.22	Disable
Port.23	Disable
Port.24	Disable
Port.25	Disable
Port.26	Disable

802.1x Configuration – Per Port Configuration

Misc Configuration

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



802.1x Configuration

System Configuration | Per Port Configuration | Misc Configuration

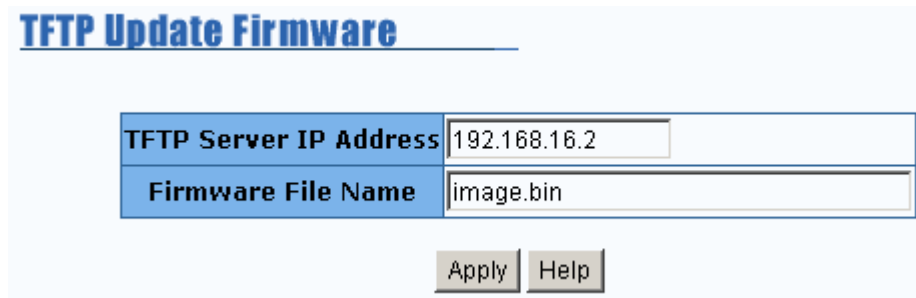
Quiet Period	60
Tx Period	30
Supplicant Timeout	30
Server Timeout	30
Max Requests	2
Reauth Period	3600

802.1x Configuration – Misc Configuration interface

TFTP Update Firmware

It provides the functions to allow a user to update the switch firmware. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server.

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



TFTP Update Firmware

TFTP Server IP Address	192.168.16.2
Firmware File Name	image.bin

TFTP Update Firmware interface

Configuration Backup

In Configuration Backup, you can restore the backup configuration into the switch. Also, you can backup the configuration to TFTP server.

TFTP Restore Configuration

You can restore EEPROM value from TFTP server, but you must put back image in TFTP server, switch will download back flash image.

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

Configuration Backup

TFTP Restore Configuration TFTP Backup Configuration

TFTP Server IP Address: 192.168.16.2

Restore File Name: data.dat

Apply Help

TFTP Restore Configuration interface

TFTP Backup Configuration

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

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

Configuration Backup

TFTP Restore Configuration TFTP Backup Configuration

TFTP Server IP Address: 192.168.16.2

Backup File Name: data.dat

Apply Help

TFTP Backup Configuration interface

Factory Default

Reset Switch to default configuration, default value to as following configuration:

- **Default IP address:** 192.168.0.1

- **Default Gateway:** 192.168.0.254
- **Subnet mask:** 255.255.255.0
- The other setting value is back to disable or none.

Click button to reset switch to default setting.

Factory Default

Please click **[Default]** button to restore factory default setting.

Factory Default interface

System Reboot

Reboot the Switch in software reset. Click button to reboot the switch.

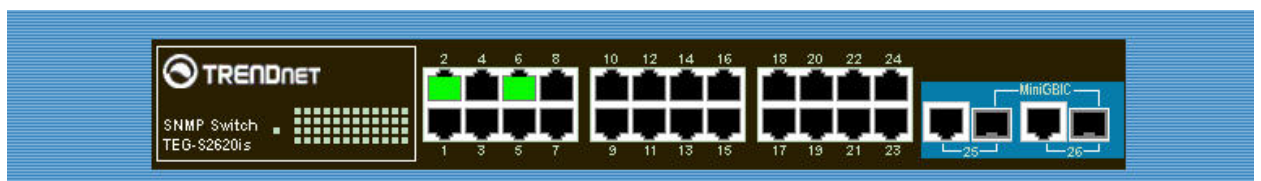
System Reboot

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

System Reboot interface

Panel List

Display the switch panel GUI. When the switch is in stacking status, it display the slaves panel GUI. When the switch is stand-alone status, it display itself panel GUI. You can click the port on the panel GUI to check port current information.



Panel list interface

IP Stacking

This function allows switch to stack up to 8 stackable switches as a unit group. When configuring the stacking function, beware the following points.

- Any port on the switch can be used to stack.
- Before configuring the stacking function, make sure all stack switches are in the same network.
- When configure stacking function, must configure the master switch first.
- After stacking group has set up, all slave switches are configured through master switch. You still can direct access to slave switch, but all functions are read and view only.
- To remove the switch from stacking group, you must remove the slave switch first. When all slave switches are removed, and then you can remove the master switch from stacking group. If you remove the master switch before slave switch, go to slave switches one by one and use console configuration to re-configure the switch configuration or you re-configure one of the slave switched as the master by console interface.

1. Click "**IP Stacking**" in the menu bar.
2. **Group ID (0...65535)**: Assign a group ID for stacking group. The switches in the same stacking group have same group ID.
3. **Stacking Mode**: select the stacking mode from drag down list.
 - **Disable**: it means the switch doesn't belong to any stacking group or stacking function is disable.
 - **Master**: it means the switch is the leader (master) in the stacking group. The master switch can control all the slave switches in stacking group.
 - **Slave**: it means the switch is a slave switch of the stacking group. To configure the slave switch that you must access by the master switch.

IP Stacking

IP = 192.168.16.1 [Disabled]

Group ID (0..65535)	<input type="text"/>
Stacking Mode	Disable ▾
System Information	<input type="text"/>

Apply

IP Stacking interface

- Click **Apply** button to apply the configuration. When the master switch has configured, you will see the following screen.

IP Stacking

IP = 192.168.16.1 [Master]

Group ID (0..65535)	65535
Stacking Mode	Master ▾
System Information	Switch01_master

Apply

IP Stacking master switch configure finished interface

- After you have configured the stacking function, use Cat. 5 cable to connect

each switch in the stacking group. And wait for few minutes for the master switch to communicate and collect the data from the slave switches.

6. Connect to the master switch through the Web. You will see the following screen display.
7. Click any function in the menu bar of the master switch to configure the switch in the stacking group. You will see the IP of stacking group list that display the IP and the switch name.

IP Stacking

IP = 192.168.16.1 [Master]
IP = 192.168.16.2 [Slave]

Group ID (0..65535)	<input type="text" value="65535"/>
Stacking Mode	Master
System Information	Switch01_master

IP Stacking Finished configuring interface

8. If you want to configure one of switch in stacking group, click the hyper link on the top of screen and login to the switch that you want to configure. You will see the screen of the switch that you have selected.

Port Statistics

Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision
Port.01	100TX	Down	Enable	0	0	0	0	0	0
Port.02	100TX	Up	Enable	966	0	206	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0
Port.07	100TX	Down	Enable	0	0	0	0	0	0
Port.08	100TX	Down	Enable	0	0	0	0	0	0
Port.09	100TX	Down	Enable	0	0	0	0	0	0
Port.10	100TX	Down	Enable	0	0	0	0	0	0
Port.11	100TX	Down	Enable	0	0	0	0	0	0
Port.12	100TX	Down	Enable	0	0	0	0	0	0
Port.13	100TX	Down	Enable	0	0	0	0	0	0
Port.14	100TX	Down	Enable	0	0	0	0	0	0
Port.15	100TX	Down	Enable	0	0	0	0	0	0

Stacking group configuration interface

6. Troubleshooting

This section is intended to help you solve the most common problems on the TEG-S2620is.

Incorrect connections

The switch port can auto detect straight or crossover cable when you link switch with other Ethernet device. For the RJ-45 connector should use correct UTP or STP cable, 10/100Mbps port use 2 pairs twisted cable and Gigabit 1000T port use 4 pairs twisted cable. If the RJ-45 connector is not correct pin on right position then the link will fail. For fiber connection, please notice that fiber cable mode and fiber module should be match.

■ Faulty or loose cables

Look for loose or obviously faulty connections. If they appear to be OK, make sure the connections are snug. IF that does not correct the problem, try a different cable.

■ Non-standard cables

Non-standard and miss-wired cables may cause numerous network collisions and other network problem, and can seriously impair network performance. A category 5-cable tester is a recommended tool for every 100Base-T network installation.

■ Improper Network Topologies

It is important to make sure that you have a valid network topology. Common topology faults include excessive cable length and too many repeaters (hubs) between end nodes. In addition, you should make sure that your network topology

contains no data path loops. Between any two ends nodes, there should be only one active cabling path at any time. Data path loops will cause broadcast storms that will severely impact your network performance.

Diagnosing LED Indicators

The Switch can be easily monitored through panel indicators to assist in identifying problems, which describes common problems you may encounter and where you can find possible solutions.

If the power indicator does turn on when the power cord is plugged in, you may have a problem with power outlet, or power cord. However, if the Switch powers off after running for a while check for loose power connections, power losses or surges at power outlet. If you still cannot resolve the problem, contact your local dealer for assistance.

■ Cabling

RJ-45 ports: use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections: 100Ω Category 3, 4 or 5 cable for 10Mbps connections or 100Ω Category 5 cable for 100Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet). Gigabit port should use Cat-5, Cat-5e, or Cat-6 cable for 1000Mbps connections. The length does not exceed 100 meters.

7. Technical Specification

This section provides the specifications of TEG-S2620is, and the following table lists these specifications.

Standard	<p>IEEE802.3 10BASE-T IEEE802.3u 100BASE-TX/100BASE-FX IEEE802.3z Gigabit SX/LX IEEE802.3ab Gigabit 1000T IEEE802.3x Flow Control and Back pressure IEEE802.3ad Port trunk with LACP IEEE802.1d Spanning tree protocol IEEE802.1p Class of service IEEE802.1Q VLAN Tagging</p>
LED Indicators	<p>System power 10/100Base-TX: Link/Activity, Full Duplex/Collision 1000Base-T: 100, 1000, Link/Activity, Full Duplex/Collision</p>
Connector	<p>10/100TX: RJ-45 Gigabit 1000T module: RJ-45 Mini GBIC slot: supports 3.3 VDC MINI GBIC transceiver</p>
Switch architecture	<p>Store and forward switch architecture</p>
Back-plane	<p>8.8Gbps</p>

MAC address	8K Mac with Auto Learning
Memory	3Mbits
Power Consumption	34Watts(Maximum)
Dimensions	440mm x 161mm x 44mm (L x W x H)
EMI & Safety	FCC Class A, CE, UL, cUL, CE/EN60590

Appendix

Console Port Pin Assignments

The DB-9 serial port on the Switch is used to connect to the switch for out-of-band console configuration. The console menu-driven configuration program can be accessed from a terminal or a PC running a terminal emulation program. The pin assignments used to connect to the serial port are provided in the following tables.

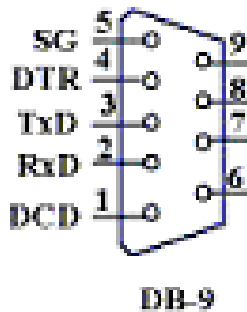


Figure A-1. DB-9 Console Port Pin Numbers

■ DB-9 Port Pin Assignments

EIA Circuit	CCITT Signal	Description	Switch's DB9 DTE Pin #	PC DB9 DTE Pin #
BB	104	RxD (Received Data)	2	2
BA	103	TxD (Transmitted Data)	3	3
AB	102	SGND (Signal Ground)	5	5

■ **Console Port to 9-Pin DTE Port on PC**

Switch's 9-Pin Serial Port	CCITT Signal PC's 9-Pin	DTE Port
2 RXD	<-----RXD ----->	3 TxD
3 TXD	-----TXD ----->	2 RxD
5 SGND	-----SGND -----	5 SGND

Cables

The RJ-45 ports on the switch support automatic MDI/MDI-X operation, so you can use standard straight-through twisted-pair cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

■ **Cable Types and Specifications**

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	100 m (328 ft)	RJ-45
100BASE-FX	50/125 or 62.5/125 micron core multimode fiber (MMF)	2 km (1.24 miles)	SC or ST

Cable specification table

100BASE-TX/10BASE-T Pin Assignments

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

■ **RJ-45 Pin Assignments**

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

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

All ports on this switch support automatic MDI/MDI-X operation, you can use straight-through cables for all network connections to PCs or servers, or to other switches or hubs. In straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3 and 6 at the other end of the cable. The table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

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

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service, for the following lengths of time from the date of purchase.

TEG-S2620is	5 years
--------------------	----------------

If a product does not operate as warranted above during the applicable warranty period, TRENDnet shall, at its option and expense, repair the defective product or deliver to customer an equivalent product to replace the defective item. All products that are replaced will become the property of TRENDnet. Replacement products may be new or reconditioned.

TRENDnet shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to TRENDnet pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product through any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting TRENDnet office within the applicable warranty period for a Return Material Authorization (RMA) number, accompanied by a copy of the dated proof of the purchase. Products returned to TRENDnet must be pre-authorized by TRENDnet with RMA number marked on the outside of the package, and sent prepaid, insured and packaged appropriately for safe shipment.

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR

ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.
Note: AC/DC Power Adapter, Cooling Fan, Cables and Power Supply carry 1-Year Warranty

Some TRENDnet products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL").

Go to <http://www.trendnet.com/gpl> or <http://www.trendnet.com> Download section and look for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please go to <http://www.gnu.org/licenses/gpl.txt> or <http://www.gnu.org/licenses/lgpl.txt> for specific terms of each license.



TRENDNET®

Product Warranty Registration

Please take a moment to register your product online.
Go to TRENDnet's website at <http://www.trendnet.com/register>

TRENDNET®

20675 Manhattan Place
Torrance, CA 90501
USA