



GSW-2493
4-slot modularized L2 SNMP Switch

User Manual

Contents

1. INTRODUCTION	1
Features	1
Software Features	2
Package Contents	4
Ethernet Switching Technology	4
2. HARDWARE DESCRIPTION	6
Physical Dimension	6
Front Panel	6
LED Indicators	6
Rear Panel.....	7
Desktop Installation	7
Attaching Rubber Feet.....	8
Rack-mounted Installation	8
Power On.....	8
3. NETWORK APPLICATION	9
Stacking Workgroup	9
Connecting to the Switch	10
4. CONSOLE MANAGEMENT	11
Login in the Console Interface	11
Main Menu.....	12
Function Description	14
Status and Counters.....	14
Switch Static Configuration.....	18
Protocol Related Configuration.....	39
System Reset Configuration.....	54
X-modem Upgrade	58
5. WEB-BASED MANAGEMENT	60
About Web-based Management	60
Preparing for Web Management.....	60
Online Help.....	61
System Login	61
Port status	62
View the Port Information	63
Port Statistics.....	64
Administrator	65
IP Configuration.....	65
Switch Setting.....	66
Console Port Information.....	72
Port Controls.....	72
Trunking	73
Forwarding and Filtering.....	77
VLAN configuration.....	80

Spanning Tree	88
Port Mirroring.....	90
SNMP Management	91
Security Manager	93
802.1X	94
TFTP Update Firmware	96
Configuration Backup	97
TFTP Restore Configuration.....	97
TFTP Backup Configuration	98
Factory Default	98
System Reboot	99
Panel List.....	99
IP Stacking	100
6. TROUBLESHOOTING	104
Incorrect connections.....	104
Faulty or loose cables	104
Non-standard cables	104
Improper Network Topologies	104
Diagnosing LED Indicators	105
Cabling	105
7. TECHNICAL SPECIFICATION	106

1. Introduction

LevelOne GSW-2493, 4-slot intelligent chassis switch, is a modular 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.

The GSW-2493 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 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.

The GSW-2493 has 4-module slot. User can accord their needs to purchase the modules. This can give elasticity on network application.

Features

- Confirms to IEEE802.3u 10BASE-T, 802.3u 100BASE-TX/FX, 802.3ab 1000BASE-T, 802.3z Gigabit fiber
- 4 slots for 8 ports 10/100TX, 8 port 100FX and Gigabit uplink module
- IEEE802.3x Flow control
 - Flow control for full duplex
 - Backpressure for half duplex
- High back-plane bandwidth 8.8Gbps
- Support IEEE802.3ad Port trunk with LACP
- Broadcast storm filter supported

- Stack management via one IP address, easy management by Web GUI
- IGMP support for Multi Media application
- Support IEEE 802.1p class of service
- Port security supported
- Port bandwidth control supported
- Support IEEE 802.1d Spanning tree protocol
- Supports GVRP function
- PortBase VLAN/802.1Q VLAN supported
- IEEE 802.1X user authentication
- Support DHCP client
- Web/ SNMP / Telnet / CLI management
- Option Module for slot:
 - MDU-2493TX 8 ports 10/100TX module
 - MDU-2493SXSC 8 ports 100FX module
 - MDU-0140 2-port 1000T copper module
 - MDU-0142 2-port miniGBIC module

Software Features

Management	Telnet management, web management, Terminal console management (RS-232)
Software Upgrade	TFTP and Console firmware upgradeable
RFC Standard	RFC 1157 SNMP, RFC 1213 MIB II, RFC 1643 Ethernet like, RFC 1493 Bridge MIB, RFC 1757 RMON 1, RFC 1215 Trap, RFC 2674 VLAN MIB, private MIB
SNMP Trap	Cold start, link down, link up, authorization fail, fan fail trap. Trap station up to 3
Port Trunk	Support IEEE802.3ad with LACP function and provide 7-trunk group of 4 member ports within 26 ports
Spanning Tree	IEEE802.1d spanning Tree
VLAN	Port based VLAN IEEE802.1Q Tag VLAN

	IEEE802.1v Protocol VLAN (IP, IPX,..) Static VLAN groups up to 256, Dynamic VLAN group up to 2048, VLAN ID from 0 to 4094
QOS Policy	Supports 8 priority levels ID for two priority queue
Class of Service	Per port 2 queues, High/ low queue. Service rule: first come first service; all High before Low, WRR for High or low weight
Port Based Priority	Support 3 settings: "Disable, Low and High priority". When set to "Disable", the income packet will follow QoS policy; Otherwise, the packet will follow port priority setting to "High/Low" queue
IGMP	It supports IGMP V1 and V2 snooping. IGMP Snooping for Multi-Media application, IGMP group supports 256 groups
Port Security	MAC address filter for ingress and egress packet Static MAC address lock for source address
Port Mirror	Global system supports 3 mirroring types: "RX, TX and Both packet". The maximum of port mirror entries is up to 25
Bandwidth Control	Per port support Bandwidth control. Per level 100K
Stacking	The switch provide Stack Grouping feature and through master switch interface can manage and stack up to 8 units.
802.1x	Support IEEE802.1x User-Authentication and can report to RADIUS server. <ul style="list-style-type: none"> ■ Reject ■ Accept ■ Authorize ■ Disable
DHCP	DHCP Client
Packet filter	Broadcast storm

Package Contents

Unpack the contents of the GSW-2493 and verify them against the checklist below.

- GSW-2493
- Power Cord
- Four Rubber Feet
- RS-232 cable
- Rack-mounted kit
- User Guide



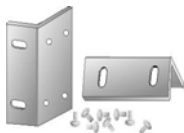
GSW-2493



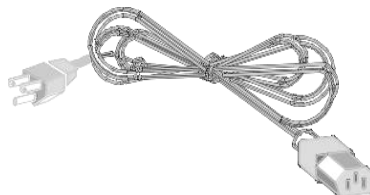
Four Rubber Feet



RS-232 Cable



Rack-mounted Kit



Power Cord



User Manual

Figure 1-2. Package Contents

Compare the contents of your GSW-2493 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 GSW-2493, and gives a physical and functional overview of the switch.

Physical Dimension

The GSW-2493 physical dimension is **440mm(W) x 280mm(D) x 44mm(H)**.

Front Panel

The Front Panel of the GSW-2493 consists of 3 module slots. One module slot is located in rear-panel of the switch.

LED Indicators

The LED Indicators gives real-time information of systematic operation status. The LED indicators are located in every module. The LED indicators will be different for different module. The following table provides descriptions of LED status and their meaning.

LED	Status	Description
Power	Green	Power On
	Off	Power is not connected

LNK/ACT	Green	The port is connecting with the device.
	Blinks	The port is receiving or transmitting data.
	Off	No device attached.
FDX/COL	Orange	The port is operating in Full-duplex mode.
	Blinks	Collision of Packets occurs in the port.
	Off	In half-duplex mode

Table 2-1. The Description of LED Indicators

Rear Panel

One module slot, 3-pronged power plug, 2 fans, power switching, and one console port is located at the rear Panel of the GSW-2493 as shown in Figure 2-1. The Switch will work with AC power in the range of 100-240V AC, 50-60Hz.



Figure 2-1. The Rear Panel of the GSW-2493

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.

Rack-mounted Installation

The GSW-2493 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.
- B. After attached both mounting brackets, position the switch 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.

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

GSW-2493 is designed as a segment switch. That is, with its large address table (8000 MAC address) and high performance, it is ideal for interconnecting networking segments.

PC, workstations, and servers can communicate each other by directly connecting with GSW-2493. The switch automatically learns nodes address, which are subsequently used to filter and forward all traffic based on the destination address.

By using Gigabit, Gigabit Fiber, or Ethernet Fiber 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 Ethernet or Gigabit fiber ports to connect switches.

Stacking Workgroup

With stackable technology can unites up to eight individual stackable switches into a single logical unit, using cables and with stacking software supported. The stack behaves as a single switching unit that is managed by a master switch elected from one of the member switches. The master switch automatically creates and updates all the switching tables. A working stack can accept new members or delete old ones without service interruption

Each switch in the stack has the capability to behave as a master or subordinate in the hierarchy. The master switch is elected and serves as the control center for the stack. The subordinates act as forwarding processors. Each switch is assigned to a one workgroup ID. Up to eight separate switches can be joined together as a workgroup. The stack can have switches added and removed without affecting stack performance.

There are no special tools, extra software, or expensive equipment needed to form a Stacking workgroup. It provides single image management for entire Stack (fewer

devices to manage); management applications represent the Stack as a single device, and simple point and click management. Stackable technology allows you to increase the resiliency and the versatility of your network edge to accommodate evolution for speed and converged applications. Following figures are example of stacking workgroup application.

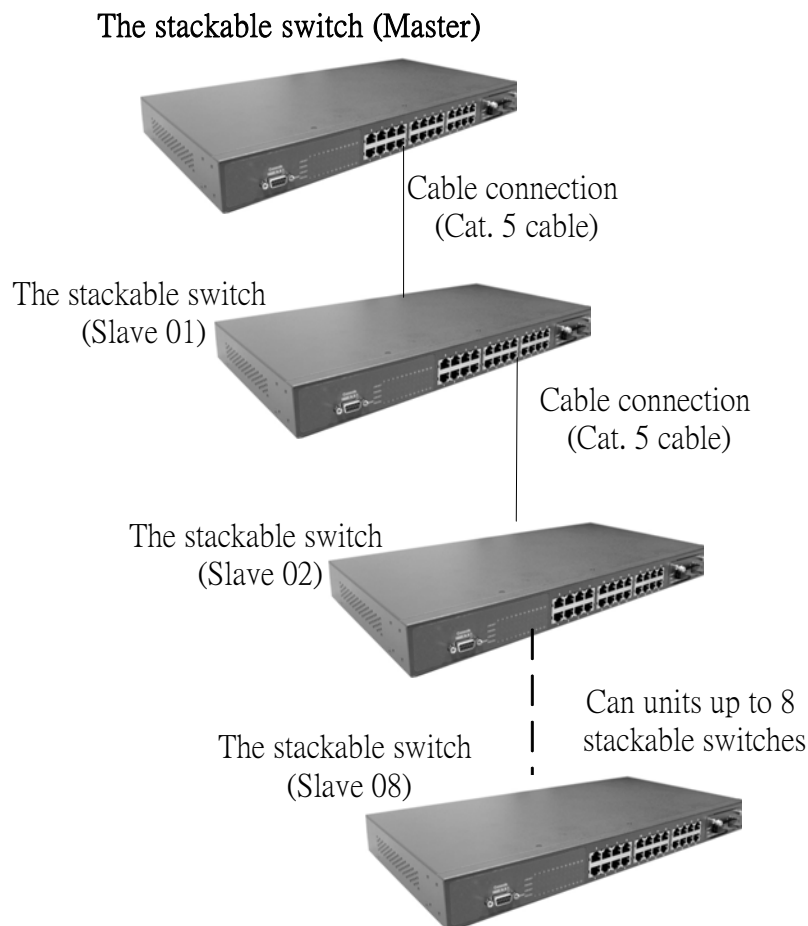


Figure 3-2. A stacking workgroup application

Connecting to the Switch

The Console port is a female DB-9 connector that enables a connection to a PC or terminal for monitoring and configuring the Switch. Use the supplied RS-232 cable with a male DB-9 connector to connect a terminal or PC to the Console port.

The Console configuration (out of band) allows you to set Switch for remote terminal as if the console terminal were directly connected to it.

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**
- Control flow: None**

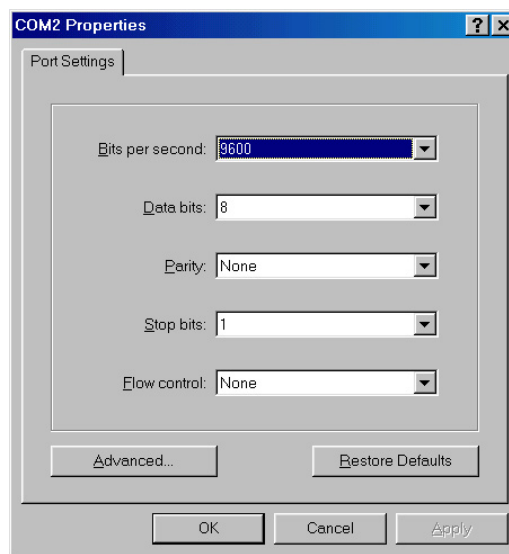
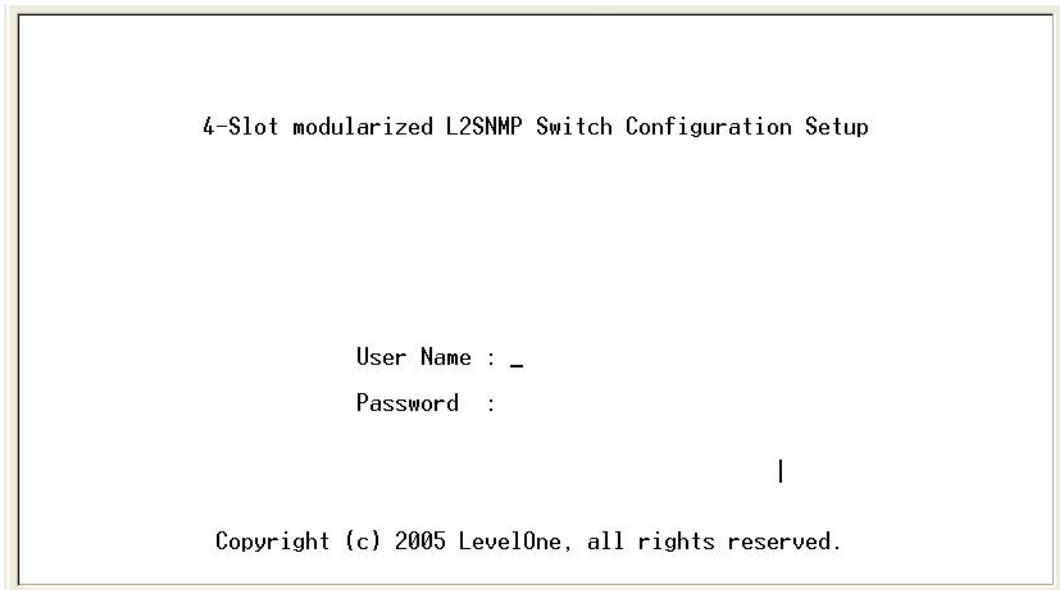


Figure 4-1. The settings of communication parameters

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 “**root**”(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 Static 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.
[TAB/BKSPC] Move Item      [Enter] Select 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: to 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 item, and press “**Enter**” key to select item.

```
4-Slot Chassis Managed Switch : Status and Counters
=====
                                Port Status
                                Port Counters
                                System Information
                                Main Menu

Display current status of all the switch ports.
[Tab/BKSPC] Move Item          [Enter] Select Item
```

Status and Counters interface

Port Status

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

- **Port:** display the number of port. The first integer is the module slot number. The second integer is the port number in the module. For example: Port 1-1, it means the first port on the first module slot.
- **Type:** display port connection speed.
- **Link:** display port statuses link status. When the port is connecting with the device and work normally, the link status is “**UP**”. Opposite is “**Down**”.
- **Speed Duplex:** display port duplex mode.
- **State:** The port current status.

- **Negotiation:** display the auto negotiation status.
- **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.

```

4-Slot Chassis Managed Switch : Port Status
=====

```

Port	Type	Link	State	Negotiation	Speed	Duplex	FC	BP	Band	Width	Security
									In	Out	Priority
Port.1-1	100FX	Down	Enable	Force	100	Full	ON	OFF	OFF	OFF	Disable OFF
Port.1-2	100FX	Down	Enable	Force	100	Full	ON	OFF	OFF	OFF	Disable OFF
Port.1-3	100FX	Down	Enable	Force	100	Full	ON	OFF	OFF	OFF	Disable OFF
Port.1-4	100FX	Down	Enable	Force	100	Full	ON	OFF	OFF	OFF	Disable OFF
Port.1-5	100FX	Down	Enable	Force	100	Full	ON	OFF	OFF	OFF	Disable OFF
Port.1-6	100FX	Down	Enable	Force	100	Full	ON	OFF	OFF	OFF	Disable OFF
Port.1-7	100FX	Down	Enable	Force	100	Full	ON	OFF	OFF	OFF	Disable OFF
Port.1-8	100FX	Down	Enable	Force	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. **<Clear>** to set all counter value to zero.

```

4-Slot Chassis Managed Switch : Port Counters
=====

```

Port	Type	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision
Port.1-1	100FX	0	0	0	0	0	0
Port.1-2	100FX	0	0	0	0	0	0
Port.1-3	100FX	0	0	0	0	0	0
Port.1-4	100FX	0	0	0	0	0	0
Port.1-5	100FX	0	0	0	0	0	0
Port.1-6	100FX	0	0	0	0	0	0
Port.1-7	100FX	0	0	0	0	0	0
Port.1-8	100FX	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. **Kernel Version:** the system kernel software version.
6. **Hardware Version:** the switch's Hardware version.
7. **MAC Address:** The unique hardware address assigned by manufacturer.
8. **Fan State:** the fan operates status.
9. **Module Information:** display the Module type that user has installed in switch.

```
4-Slot Chassis Managed Switch : System Information
=====
System Name      :
System Location  :
System Description : 4-Slot Chassis Managed Switch
Firmware Version : v1.00
Kernel Version   : v3.00
Hardware Version : A7.00
MAC Address      : 00001C005678
Fan state        : Working Working

Module   Type      Description
-----
Module 1 100FX      100BASE-FX Multi Mode
Module 2 100TX      100BASE-TX
Module 3 100FX      100BASE-FX Single Mode
Port.4-1 N/A         N/A
Port.4-2 N/A         N/A

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.

```
4-Slot Chassis Managed 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.

```
4-Slot Chassis Managed Switch : Administration Configuration
=====

Device Information
IP Configuration
User Name Configuration
Password Configuration
Previous Menu

Configure the device information.
[Tab/BKSPC] Move Item      [Enter] Select Item
```

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.

```
4-Slot Chassis Managed Switch : Device Information
=====

Name      :
Description : 4-Slot Chassis Managed 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 Client:** disable or enable the DHCP client function.
3. **IP Address:** assign the switch IP address. The default IP is 192.168.16.1.
4. **Subnet Mask:** assign the switch IP subnet mask.
5. **Gateway:** assign the switch gateway. The default value is 192.168.16.254.
6. Select **<Save>** action to save the configuration.

Note: Always restart the switch after change the IP address.


```
4-Slot Chassis Managed Switch : IP Configuration
=====

DHCP Client : Disable
IP Address  : 192.168.16.1
Subnet Mask : 255.255.255.0
Gateway    : 192.168.16.254

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>**

```
4-Slot Chassis Managed Switch : User Name Configuration
=====

User Name : root

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>**

```
4-Slot Chassis Managed 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>**.

```

4-Slot Chassis Managed Switch : Port Configuration
=====

```

Port	Type	Negotiation State	Speed Duplex	FC	BP	Band In	Width Out	Security Priority
Port.1-1	100FX	Enable	Force 100 Full	ON	OFF	0	0	Disable OFF
Port.1-2	100FX	Enable	Force 100 Full	ON	OFF	0	0	Disable OFF
Port.1-3	100FX	Enable	Force 100 Full	ON	OFF	0	0	Disable OFF
Port.1-4	100FX	Enable	Force 100 Full	ON	OFF	0	0	Disable OFF
Port.1-5	100FX	Enable	Force 100 Full	ON	OFF	0	0	Disable OFF
Port.1-6	100FX	Enable	Force 100 Full	ON	OFF	0	0	Disable OFF
Port.1-7	100FX	Enable	Force 100 Full	ON	OFF	0	0	Disable OFF
Port.1-8	100FX	Enable	Force 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 as trunk group.
3. Using **"Space"** key to mark the port.
4. Using **Tab** key move to **Trunk#** (ex. Trunk1, Trunk2...) to change the Trunk# value to **Static**.
5. Save the configuration by selecting **<Save>**.

```

4-Slot Chassis Managed Switch : Trunk Configuration
=====
          MOD 1          |          MOD 2          |          MOD 3          |          MOD4
01 02 03 04 05 06 07 08 | 01 02 03 04 05 06 07 08 | 01 02 03 04 05 06 07 08 | 01 02
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

```

4-Slot Chassis Managed 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. **Port State:** use “**Space**” key to mark the port that wanted to be mirrored.
5. Select the **<Save>**.

```

4-Slot Chassis Managed Switch : Port Mirroring
=====

Mirroring State : Both
Analysis Port : Port.1-5

Port State      Port State      Port State      Port State
-----
Port.1-5 -      Port.2-5 -      Port.3-5 -
Port.1-6 -      Port.2-6 -      Port.3-6 -
Port.1-7 -      Port.2-7 -      Port.3-7 -
Port.1-8 -      Port.2-8 -      Port.3-8 -
Port.2-1 -      Port.3-1 -      Trunk.1 -
Port.2-2 -      Port.3-2 -
Port.2-3 -      Port.3-3 -
Port.2-4 -      Port.3-4 -

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.

```
4-Slot Chassis Managed 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 Range:** Type the PVID. The ID range is from 1~255.
 - **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.

```

4-Slot Chassis Managed Switch : VLAN Configure
=====
VLAN Mode : 802.1Q
VLAN ID Range : 1~255

Port      VLAN ID  Ingress Filter  Acceptable
-----
Port.1-5  1        Enable          All
Port.1-6  1        Enable          All
Port.1-7  1        Enable          All
Port.1-8  1        Enable          All
Port.2-1  1        Enable          All
Port.2-2  1        Enable          All
Port.2-3  1        Enable          All
Port.2-4  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 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: Trunk1, Trunk2...) in the port list. You also can configure the trunk group as the VLAN member.

```

4-Slot Chassis Managed Switch : Create VLAN Group
=====

VLAN Name :                Group ID :

Port      Member
-----
Port.1-5  No
Port.1-6  No
Port.1-7  No
Port.1-8  No
Port.2-1  No
Port.2-2  No
Port.2-3  No
Port.2-4  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.

```

4-Slot Chassis Managed Switch : Create VLAN Group
=====

VLAN Name:                VLAN ID :

Do you want to enable security VLAN setting (y/N)

```

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.

```

4-Slot Chassis Managed Switch : Create VLAN Group
=====

VLAN Name :                VLAN ID :
Protocol VLAN : None
Port          Member
-----
Port.1-5     No
Port.1-6     No
Port.1-7     No
Port.1-8     No
Port.2-1     No
Port.2-2     No
Port.2-3     No
Port.2-4     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 some 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		
vlan02	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 (802.1Q VLAN group)

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>**

```
4-Slot Chassis Managed 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. Press “**Space**” key to select the priority level mapping to high or low queue.
3. **Qos Mode:** select the mode to process incoming packets.
 - **First comes 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.
4. Press “**ESC**” goes back action menu line.
5. Select **<Save>** to save all configure value.

```

4-Slot Chassis Managed 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.

```

4-Slot Chassis Managed 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.

```
4-Slot Chassis Managed 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.

```
4-Slot Chassis Managed Switch : Filtering MAC Address
=====
MAC Address      VLAN ID          MAC Address      VLAN ID
-----

```

```
Actions->  <Add>  <Edit>  <Delete>  <Previous Page>  <Next Page>  <Quit>
Add/Edit/Delete a Mac.
[Tab/BKSPC] Move Item      [Enter] Select Item      [Esc] Previous Menu  _
```

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. **VLAN ID:** enter the Mac address' s VLAD ID, if the Mac address belongs to any VLAN group.
4. Press **"ESC"** to go back action menu line.
5. Select **<Save>** to save all configure value.

```

4-Slot Chassis Managed Switch : Add Filter MAC Address
=====

MAC Address :
VLAN ID    :

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

```

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 maintain on 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 assigned 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.

- **IP Stacking System Information:** Shows the current IP stacking status.

```
DDC GSW-2493 : 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
IP Stacking System Information         :
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.

```
4-Slot Chassis Managed 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.

```
4-Slot Chassis Managed 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>**.

```
4-Slot Chassis Managed 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>**.

```

4-Slot Chassis Managed Switch : STP System Configuration
=====

Root Bridge Information          Configure Spanning Tree Parameters
-----
Priority       : 32768           Priority (0-65535)       : 32768
Mac Address   : 00001C005678   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

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.

```

4-Slot Chassis Managed Switch : STP Per Port Setting
=====

Port          State          Path Cost      Priority
-----
Port.1-5      Forwarding     10             128
Port.1-6      Forwarding     10             128
Port.1-7      Forwarding     10             128
Port.1-8      Forwarding     10             128
Port.2-1      Forwarding     10             128
Port.2-2      Forwarding     10             128
Port.2-3      Forwarding     10             128
Port.2-4      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.

```

4-Slot Chassis Managed Switch : SNMP Configuration
=====

System Options
Community Strings
Trap Managers
Previous Menu

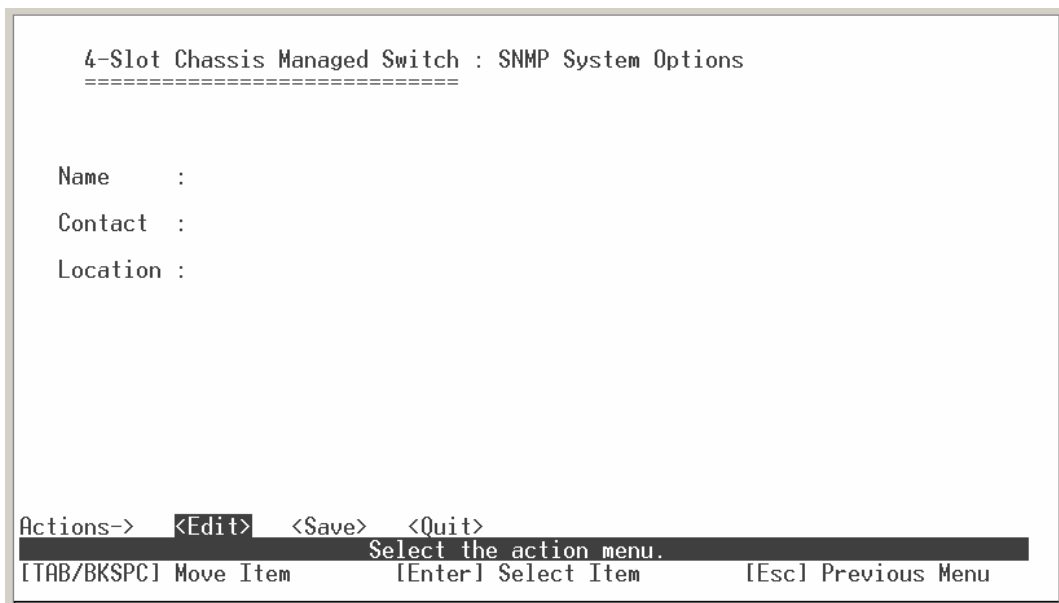
Configure the system information.
[Tab/BKSPC] Move Item      [Enter] Select Item

```

SNMP Configuration interface

SNMP System Options

1. Press **<Edit>**.
2. **Name:** assign a name for the switch.
3. **Contact:** Type the name of contact person or organization.
4. **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.

```
4-Slot Chassis Managed 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>**.

```
4-Slot Chassis Managed 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**”.
3. When pressing “**Enter**” will complete deletion.

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.

```
4-Slot Chassis Managed 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.

```
4-Slot Chassis Managed Switch : Add SNMP Trap Manager
=====

IP :
Community Name :

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

Add Trap Manager interface

■ Delete Trap Manager

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

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. You can configure and view all the LACP status.

```
4-Slot Chassis Managed Switch : LACP Configuration
=====
Working Ports
State Activity
Group Status
Previous Menu

Working ports setting.
[Tab/BKSPC] Move Item      [Enter] Select Item
```

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.

```

4-Slot Chassis Managed 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>**.

```

4-Slot Chassis Managed 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 setting trunk group, you can see the relation information in here.

```
4-Slot Chassis Managed Switch : LACP Group Status
=====

                Static Trunking Group

Group Key   : 1
Port Member : 1-1 1-2 1-3 1-4

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>**

```

4-Slot Chassis Managed 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

```

4-Slot Chassis Managed 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>**

```
4-Slot Chassis Managed 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>**

```

4-Slot Chassis Managed 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.

```

4-Slot Chassis Managed Switch : 802.1x Per Port Setting
=====

Port          State
-----
Port.1-5      Disable
Port.1-6      Disable
Port.1-7      Disable
Port.1-8      Disable
Port.2-1      Disable
Port.2-2      Disable
Port.2-3      Disable
Port.2-4      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 wait for a supplicant response to an EAP request.
5. **Server Timeout:** set the period of time the switch wait 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. **Reauth Period:** set the period of time after which clients connected must be re-authenticated.
8. Select **<Save>**

```
4-Slot Chassis Managed 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..999999, 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

```
4-Slot Chassis Managed 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.

```
Do you want to restore factory default setting? (y/N)
|
```

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.

```
4-Slot Chassis Managed Switch : TFTP Configuration
-----

Update Firmware
Restore Configuration
Backup Configuration
Previous Menu

Update system firmware from TFTP server.
[Tab/BKSPC] Move Item      [Enter] Select Item
```

TFTP Update Firmware interface

Update Firmware

It provides user uses TFTP to update firmware.

1. Start the TFTP server, and copy firmware update version image file to 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**” goes back to action 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.

```
4-Slot Chassis Managed 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.

```
4-Slot Chassis Managed 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.

```
4-Slot Chassis Managed 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

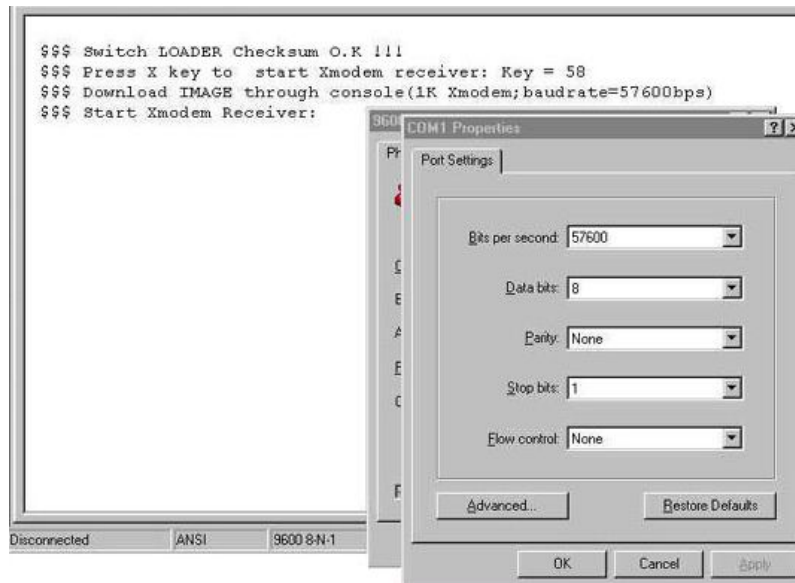
X-modem Upgrade

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

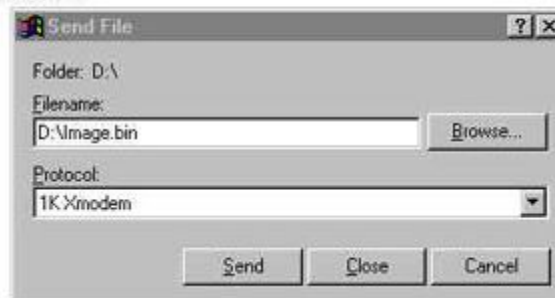
1. Press "X" key to start upgrading from X-modem.
2. You will see the following screen displays.

```
$$$ Switch LOADER Checksum O.K !!!
$$$ 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.

If your OS is Windows XP with Service Pack 2, please disable the windows firewall before connecting to UI.

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: **192.168.16.1**


Subnet Mask: **255.255.255.0**

Default Gateway: **192.168.16.254**

User Name: **root**

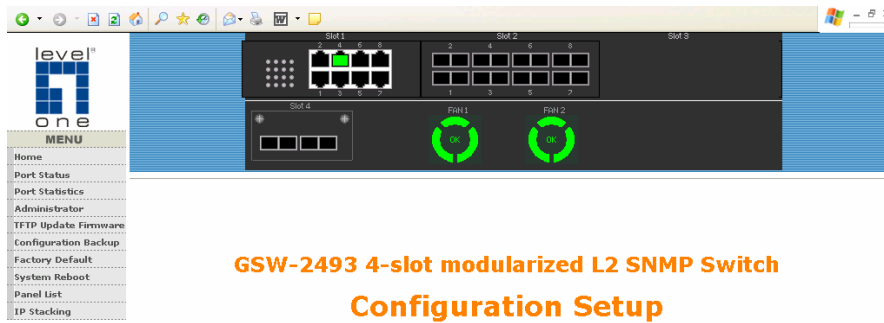
Password: **root**

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 "**root**".
5. Click "**Enter**" or "**OK**", then the home screen of the Web-based management appears.
6. The Panel GUI will show the module GUI, the copper module and fiber module GUI display will be different. In the following figure, the slot 1 is copper module and slot 2 is fiber module.



Copyright (c) 2005 LevelOne, all rights reserved.

GSW-2493

Port status

In Port status, you can view every port status that depended on user setting and the negotiation result.

1. **Port:** display the number of port. The first integer is the module slot number. The second integer is the port number in the module. For example: Port 1-1, it means the first port on the first module slot.
2. **Type:** display port connection speed.
3. **Link:** “Down” is “No Link”. “UP” is “Link”.
4. **State:** display port statuses “disable” or “enable”. “Unlink” will be treated as “off”.
5. **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.
6. **Speed Duplex:** display port connection speed. “Config” means the value that user configured. “Actual” means the current value of the port.
7. **Flow Control:** Full: display the flow control status is “enable” or “disable” in full mode. “Config” means the value that user configured. “Actual” means the current value of the port.

8. **Back Pressure:** Display the Back Pressure status setting. “Config” means the value that user configured. “Actual” means the current value of the port.
9. **Bandwidth In/ Out:** display the port incoming and outgoing bandwidth.
10. **Priority:** display the port static priority status is “High” or “Low” or “Disable”.
11. **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.1-1	100FX	Down	Enable	Force	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.1-2	100FX	Up	Enable	Force	Force	100 Full	100 Full	ON	ON	ON	OFF	OFF	OFF	Disable	OFF
Port.1-3	100FX	Down	Enable	Force	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.1-4	100FX	Down	Enable	Force	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.1-5	100FX	Down	Enable	Force	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.1-6	100FX	Down	Enable	Force	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.1-7	100FX	Down	Enable	Force	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.1-8	100FX	Down	Enable	Force	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.2-1	100TX	Down	Enable	Auto	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.2-2	100TX	Down	Enable	Auto	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.2-3	100TX	Down	Enable	Auto	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.2-4	100TX	Down	Enable	Auto	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.2-5	100TX	Down	Enable	Auto	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.2-6	100TX	Down	Enable	Auto	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.2-7	100TX	Down	Enable	Auto	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.2-8	100TX	Down	Enable	Auto	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.3-1	100FX	Down	Enable	Force	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.3-2	100FX	Down	Enable	Force	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.3-3	100FX	Down	Enable	Force	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.3-4	100FX	Down	Enable	Force	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.3-5	100FX	Down	Enable	Force	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.3-6	100FX	Down	Enable	Force	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.3-7	100FX	Down	Enable	Force	N/A	100 Full	N/A	ON	N/A	ON	N/A	OFF	OFF	Disable	OFF
Port.3-8	100FX	Down	Enable	Force	N/A	100 Full	N/A	ON	N/A	ON	N/A	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	1-2
Link	Up
State	On
Trunking	None
VLAN	Disable
Tx Good Packet	1479
Tx Bad Packet	0
Rx Good Packet	1346
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.1-1	100TX	Down	Enable	0	0	0	0	0	0
Port.1-2	100TX	Down	Enable	0	0	0	0	0	0
Port.1-3	100TX	Down	Enable	0	0	0	0	0	0
Port.1-4	100TX	Up	Enable	5350	0	6113	0	0	0
Port.1-5	100TX	Down	Enable	0	0	0	0	0	0
Port.1-6	100TX	Down	Enable	0	0	0	0	0	0
Port.1-7	100TX	Down	Enable	0	0	0	0	0	0
Port.1-8	100TX	Down	Enable	0	0	0	0	0	0
Port.2-1	100FX	Down	Enable	0	0	0	0	0	0
Port.2-2	100FX	Down	Enable	0	0	0	0	0	0
Port.2-3	100FX	Down	Enable	0	0	0	0	0	0
Port.2-4	100FX	Down	Enable	0	0	0	0	0	0
Port.2-5	100FX	Down	Enable	0	0	0	0	0	0
Port.2-6	100FX	Down	Enable	0	0	0	0	0	0
Port.2-7	100FX	Down	Enable	0	0	0	0	0	0
Port.2-8	100FX	Down	Enable	0	0	0	0	0	0
Port.4-1	mGBIC	Down	Enable	0	0	0	0	0	0
Port.4-2	mGBIC	Down	Enable	0	0	0	0	0	0

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 Configuration

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

IP Configuration

DHCP Client :

IP Address	<input type="text" value="192.168.16.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.16.254"/>

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)
- **Fan 1:** display fan current status.
- **Fan 2:** display fan current status.
- **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	4-Slot Chassis Managed Switch
Firmware Version	v1.00
Kernel Version	v3.00
Hardware Version	A7.00
MAC Address	00001C005678
Fan 1	Working
Fan 2	Working

Module	Type	Description
Module 1	100FX	100BASE-FX Multi Mode
Module 2	100TX	100BASE-TX
Module 3	100FX	100BASE-FX Single Mode
Port.4-1	100FX	N/A
Port.4-2	100FX	N/A

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 Apply 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) :

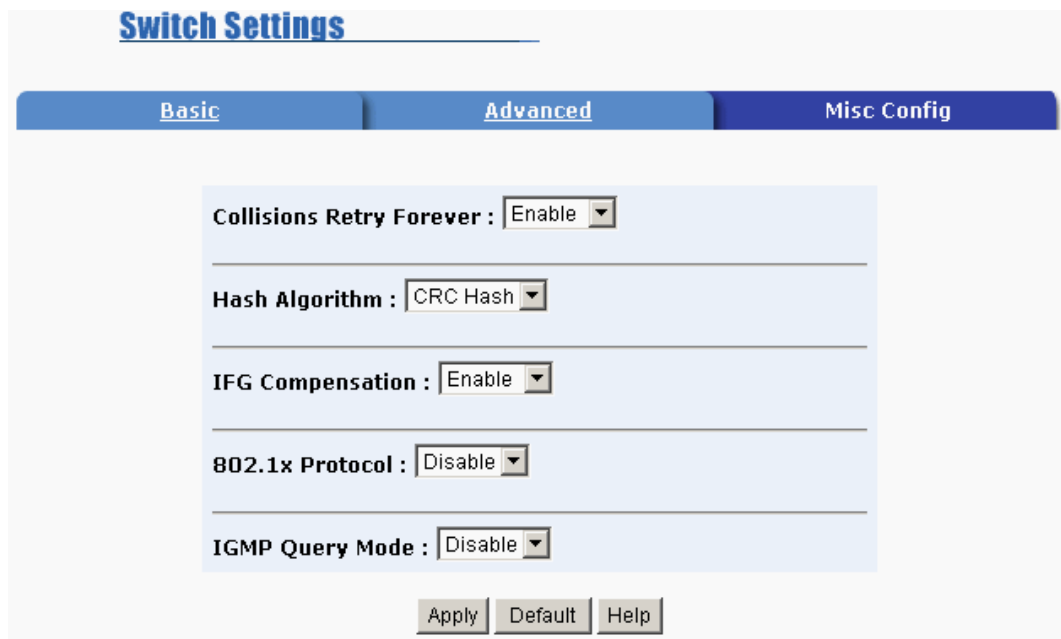
Level0 Level1 Level2 Level3 Level4 Level5 Level6 Level7

Switch Advanced setting interface

- **802.1p Priority:** 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: 2 Low means that the switch sends 5 high priority packets before sending 2 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.



The screenshot displays the 'Switch Settings' interface with the 'Misc Config' tab selected. The configuration options are as follows:

Setting	Value
Collisions Retry Forever	Enable
Hash Algorithm	CRC Hash
IFG Compensation	Enable
802.1x Protocol	Disable
IGMP Query Mode	Disable

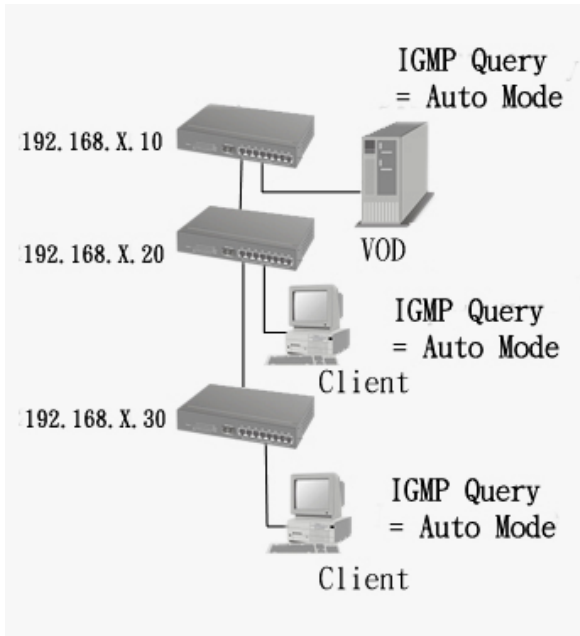
Buttons: Apply, Default, Help

Switch Misc Config setting interface

■ IGMP Theory of Operation

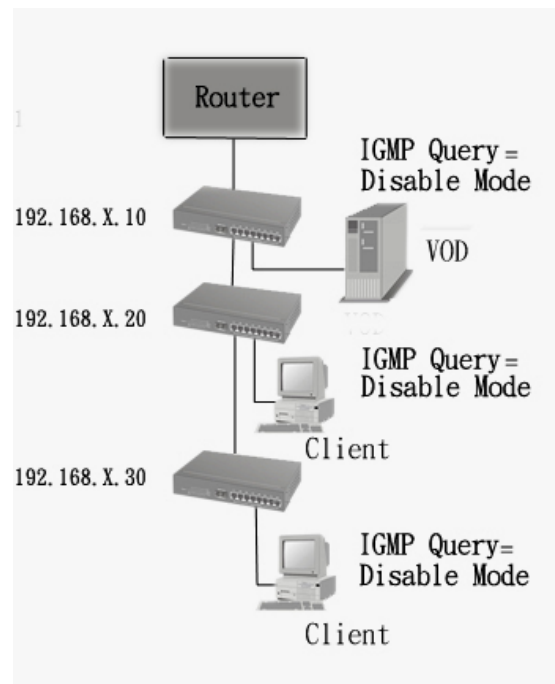
The following three topologies detail how IGMP Query works and to be configured

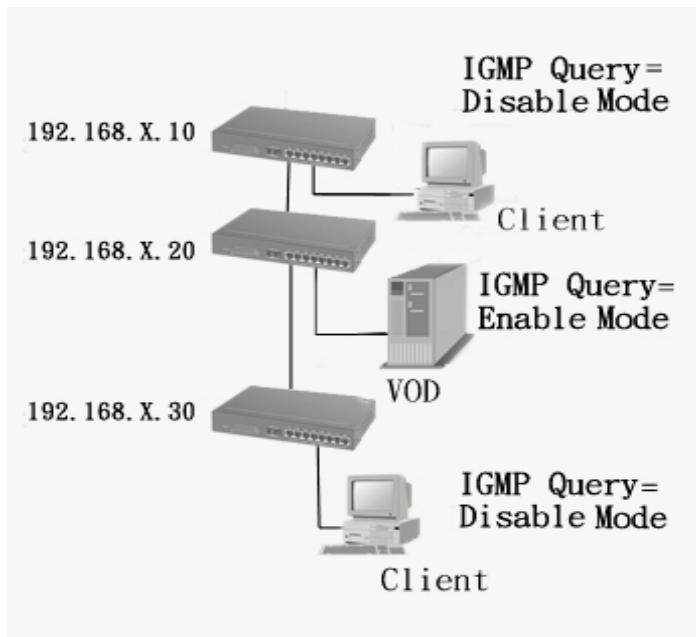
within a network:



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.

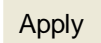
1. Select the port by scroll the list in **Port** column.
2. **State:** User can disable or enable this port control.
3. **Negotiation:** User can set auto negotiation mode is Auto, Nway (specify the speed/duplex on this port and enable auto-negotiation), Force of the port.
4. **Speed:** set the speed 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 ~ 1000. The unit is 100K. 0: disable rate control. 1 ~ 1000: valid rate value.
- **Out:** fill in the port effective egress rate. The valid range is 0~1000. The unit is 100K. 0: disable rate control. 1 ~ 1000: 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  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.1-1	Enable	Auto	100	Full	ON	OFF	0	0	Disable	<input type="checkbox"/>
Port.1-2										
Port.1-3										
Port.1-4										



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.1-1	100FX	Down	Enable	Force	N/A	100	Full	N/A	ON	N/A	ON	N/A	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 - 6. If LACP enable, you can configure LACP Active/Passive status in each ports on State Activity page.
- 7. Click - 8. Use

Trunking

Aggregator Setting **Aggregator information** State Activity

System Priority

1

Group ID	Trunk.1	Select
Lacp	Disable	
Work Ports	0	
	<<Add Remove>>	Port.1-1 Port.1-2 Port.1-3 Port.1-4 Port.1-5 Port.1-6 Port.1-7 Port.1-8 Port.2-1

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 Setting **Aggregator information** State Activity

Group2						
Actor			Partner			
Priority	1		1			
MAC	000f38fff1b2		00001c05944a			
PortNo	Key	Priority	Active	PortNo	Key	Priority
PORT3-1	514	1	selected	PORT3-7	513	1
PORT3-2	514	1	selected	PORT3-8	513	1

Trunking – Aggregator Information interface

Aggregator Information 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 **Apply** 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.

The screenshot shows the 'Trunking' configuration page with the 'State Activity' tab selected. It displays a table with two columns for 'Port' and 'LACP State Activity'. The first two columns are for ports 1-1 through 1-8, and the next two are for ports 2-1 through 2-8, 3-1 through 3-8, and 4-1 through 4-2. Ports 1-1, 1-2, and 1-3 are marked as 'Active' with a checked checkbox, while all other ports are marked as 'N/A'. There are 'Apply' and 'Help' buttons at the bottom of the interface.

Port	LACP State Activity	Port	LACP State Activity
1-1	<input checked="" type="checkbox"/> Active	1-2	<input checked="" type="checkbox"/> Active
1-3	<input checked="" type="checkbox"/> Active	1-4	N/A
1-5	N/A	1-6	N/A
1-7	N/A	1-8	N/A
2-1	N/A	2-2	N/A
2-3	N/A	2-4	N/A
2-5	N/A	2-6	N/A
2-7	N/A	2-8	N/A
3-1	N/A	3-2	N/A
3-3	N/A	3-4	N/A
3-5	N/A	3-6	N/A
3-7	N/A	3-8	N/A
4-1	N/A	4-2	N/A

Trunking – State Activity interface

Forwarding and Filtering

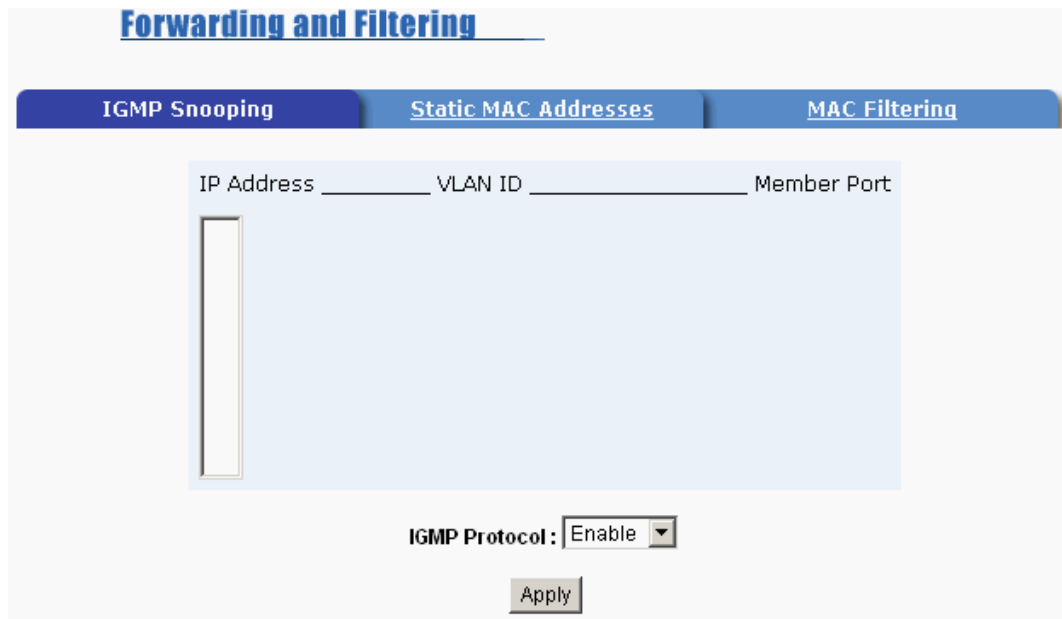
IGMP Snooping

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.



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 No.** column, 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 **Add** button.
5. Use **Delete** 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.

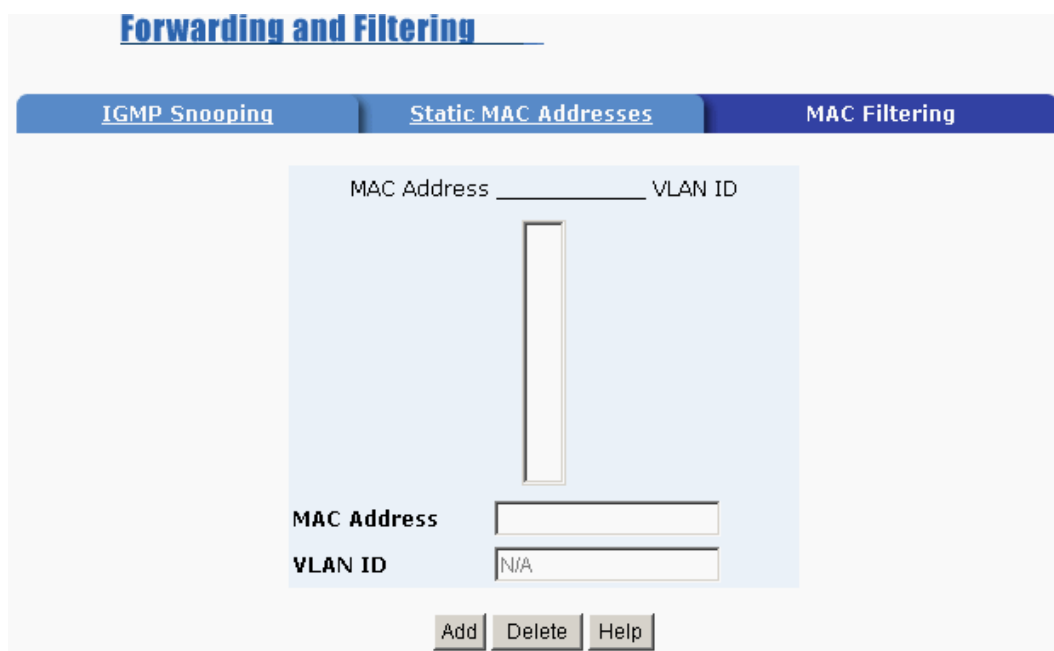
VLAN ID

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 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.

If an end station sends packets to different VLANs, it 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 VLAN name, group ID and select the members of VLAN group.
3. Click .

VLAN Configuration

VLAN Operation Mode :

Enable GVRP Protocol

Group Name

VLAN ID

Port.1-1
Port.1-2
Port.1-3
Port.2-2
Port.2-3
Port.2-4
Port.2-5
Port.2-6
Port.2-7
Port.2-8
Port.3-1
Port.3-2

Add>>

<<Remove

Apply Help

Add PortBase VLAN interface

- You will see the VLAN displays.

VLAN Configuration

VLAN Operation Mode :

Enable GVRP Protocol

v01__1

Add Edit Delete Previous Page Next Page Help

PortBase VLAN group list interface

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.

VLAN Configuration

VLAN Operation Mode : 802.1Q

Enable GVRP Protocol

Basic | **Port VLAN ID**

DEFAULT__1

Add Edit Delete Previous Page Next Page Help

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.1-1
 Port.1-2
 Port.1-3
 Port.2-2
 Port.2-3
 Port.2-4
 Port.2-5
 Port.2-6
 Port.2-7
 Port.2-8
 Port.3-1
 Port.3-2

Add>>

<<Remove

Next Help

Add 802.1q VLAN interface -1

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

VLAN Configuration

VLAN Operation Mode : 802.1Q

Enable GVRP Protocol

VLAN Name	v002		
VLAN ID	2		
UnTag Member			
Port.1-1	Untag	Port.1-2	Untag
Port.1-3	Untag		

Apply



Add 802.1q VLAN interface -1

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

Apply .

- 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.

VLAN Configuration

VLAN Operation Mode : 802.1Q

Enable GVRP Protocol

Basic

Port VLAN ID

Port	Port VLAN ID	Ingress Filter	Acceptable Frame Type	VLAN ID Range
Port.1-1	1	Enable	All	256~511
Port.1-2				
Port.1-3				
Port.2-2				

Apply Default Help

Port	VLAN ID	Ingress Filter	Acceptable Frame Type
Port.1-1	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)	<input type="text" value="32768"/>
Max Age (6-40)	<input type="text" value="20"/>
Hello Time (1-10)	<input type="text" value="2"/>
Forward Delay Time (4-30)	<input type="text" value="15"/>

Root Bridge Information

Priority	32768
Mac Address	00001C005678
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.

- Assign the port priority value. The value range is from 0 to 255. The lowest value has higher priority.
- Click **Apply** button.

Spanning Tree

System Configuration		Per Port Configuration
Port	Path Cost (1-65535)	Priority (0-255)
Port.1-1 ▲ Port.1-2 ▲ Port.1-3 ▲ Port.1-4 ▲ Port.1-5 ▼	10	128
<input type="button" value="Apply"/> <input type="button" value="Help"/>		

STP Port Status

Port	Path Cost	Priority	State
Port.1-1	10	0	Forwarding
Port.1-2	10	0	Forwarding
Port.1-3	10	0	Forwarding
Port.1-4	10	0	Forwarding
Port.1-5	10	0	Forwarding
Port.1-6	10	0	Forwarding
Port.1-7	10	0	Forwarding
Port.1-8	10	0	Forwarding
Port.2-1	10	0	Forwarding
Port.2-2	10	0	Forwarding
Port.2-3	10	0	Forwarding
Port.2-4	10	0	Forwarding
Port.2-5	10	0	Forwarding
Port.2-6	10	0	Forwarding
Port.2-7	10	0	Forwarding
Port.2-8	10	0	Forwarding
Port.3-1	10	0	Forwarding
Port.3-2	10	0	Forwarding
Port.3-3	10	0	Forwarding
Port.3-4	10	0	Forwarding
Port.3-5	10	0	Forwarding
Port.3-6	10	0	Forwarding
Port.3-7	10	0	Forwarding
Port.3-8	10	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.

- 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 want 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.1-1	<input type="checkbox"/>
Port.1-2	<input type="checkbox"/>
Port.1-3	<input type="checkbox"/>
Port.1-4	<input type="checkbox"/>
Port.1-5	<input type="checkbox"/>
Port.1-6	<input type="checkbox"/>
Port.1-7	<input type="checkbox"/>
Port.1-8	<input type="checkbox"/>
Port.2-1	<input type="checkbox"/>
Port.2-2	<input type="checkbox"/>
Port.2-3	<input type="checkbox"/>
Port.2-4	<input type="checkbox"/>
Port.2-5	<input type="checkbox"/>
Port.2-6	<input type="checkbox"/>
Port.2-7	<input type="checkbox"/>
Port.2-8	<input type="checkbox"/>
Port.3-1	<input type="checkbox"/>
Port.3-2	<input type="checkbox"/>
Port.3-3	<input type="checkbox"/>
Port.3-4	<input type="checkbox"/>
Port.3-5	<input type="checkbox"/>
Port.3-6	<input type="checkbox"/>
Port.3-7	<input type="checkbox"/>
Port.3-8	<input type="checkbox"/>

Prot 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 image displays the SNMP Management interface, which is divided into three main sections:

- System Options:** This section contains three text input fields labeled "Name:", "Location:", and "Contact:". Below these fields are two buttons: "Apply" and "Help".
- Community Strings:** This section is split into two parts. On the left, under "Current Strings:", there is a list box containing "public__RO" and "private__RW", with "Add" and "Remove" buttons next to it. On the right, under "New Community String:", there is a "String:" text input field and two radio buttons labeled "RO" (which is selected) and "RW".
- Trap Managers:** This section is also split into two parts. On the left, under "Current Managers:", there is a list box containing "(none)", with "Add" and "Remove" buttons next to it. On the right, under "New Manager:", there are two text input fields: "IP Address:" and "Community:".

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.

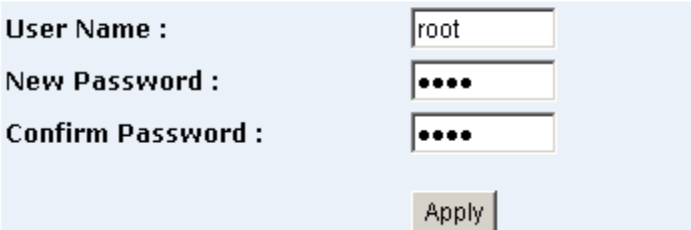
1. **IP Address:** fill in the trap device IP.
2. **Community Strings:** the trap device community strings.
3. Click .

Security Manager

You can change web management login user name and password.

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

Security Manager



The screenshot shows a light blue rectangular form with three input fields and one button. The first field is labeled 'User Name :' and contains the text 'root'. The second field is labeled 'New Password :' and contains five black dots. The third field is labeled 'Confirm Password :' and also contains five black dots. Below these fields is a button labeled '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



Port	State
<div style="border: 1px solid gray; padding: 2px;"> Port.1-1 ▲ Port.1-2 ▲ Port.1-3 ▲ Port.1-4 ▲ Port.1-5 ▼ </div>	<input type="button" value="Authorize"/> ▼

Port Authorization

Port	State
Port.1-1	Disable
Port.1-2	Disable
Port.1-3	Disable
Port.1-4	Disable
Port.1-5	Disable
Port.1-6	Disable
Port.1-7	Disable
Port.1-8	Disable
Port.2-1	Disable
Port.2-2	Disable
Port.2-3	Disable
Port.2-4	Disable
Port.2-5	Disable
Port.2-6	Disable
Port.2-7	Disable
Port.2-8	Disable
Port.3-1	Disable
Port.3-2	Disable
Port.3-3	Disable
Port.3-4	Disable
Port.3-5	Disable
Port.3-6	Disable
Port.3-7	Disable
Port.3-8	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 .

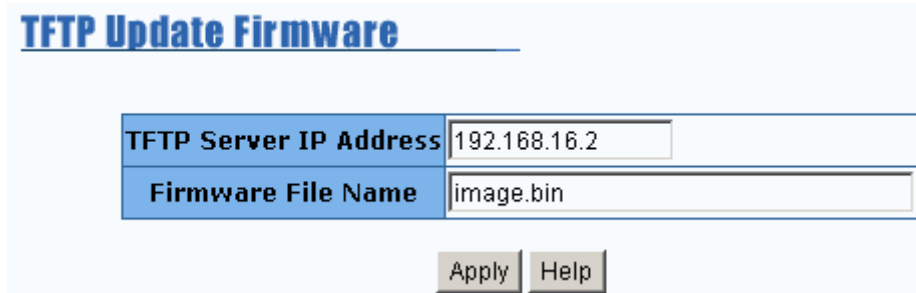
802.1x Configuration		
System Configuration	Per Port Configuration	Misc Configuration
Quiet Period	<input type="text" value="60"/>	
Tx Period	<input type="text" value="30"/>	
Supplicant Timeout	<input type="text" value="30"/>	
Server Timeout	<input type="text" value="30"/>	
Max Requests	<input type="text" value="2"/>	
Reauth Period	<input type="text" value="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:** 192.168.16.1
- **Default Gateway:** 192.168.16.254

- **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.

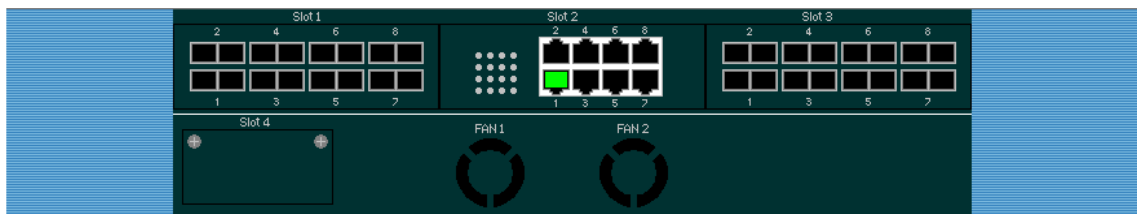
System Reboot

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 disabling.
 - **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.

192.168.16.1 [Switch01_master]

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.

[192.168.16.1 \[Switch01_master \]](#)
[192.168.16.2 \[Switch02 \]](#)

192.168.16.1 [Switch01_master]

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.

[192.168.16.1 \[Switch01_master\]](#)
[192.168.16.2 \[Switch02\]](#)

192.168.16.1 [Switch01_master]

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

Clear

Stacking group configuration interface

6. Troubleshooting

This section is intended to help you solve the most common problems on the GSW-2493.

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: 100 Ω Category 3, 4 or 5 cable for 10Mbps connections or 100 Ω 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 or cat-5e cable for 1000Mbps connections. The length does not exceed 100 meters.

7. Technical Specification

This section provides the specifications of the GSW-2493, 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>
Switch architecture	Store and forward switch architecture.
Back plane	8.8Gbps
LED Indicators	<p>System Power 8 10/100TX module: Link/Activity (Green), Full duplex (Green) 8 100Base-FX module: Link (Green), Activity (Green Blinking) Gigabit Fiber: Link/ Activity Gigabit Copper: Link/Activity, Full duplex, 1000Mbps, 100Mbps</p>
Connector	<p>8-port 10/100TX module: RJ-45 8-port 100FX(Multi /Single Mode) module: SC 2-port Gigabit SX/LX module: SC 2-port Gigabit 1000T module: RJ-45</p>
Expansion module	<p>8 port 10/100TX module with RJ-45 connector (MDU-2493TX) 8 port 100Mbps multi mode fiber module with SC connector (MDU-2493SXSC) 2 Gigabit copper module with RJ-45 connector (MDU-0140) 2 Gigabit miniGBIC module (MDU-0142)</p>

MAC address	8K MAC address table with Auto learning function
Memory	3Mbits for packet buffer
CPU	ARM-7 32 bits RISC processor
Flash ROM	512Kbytes x 1
System memory	8Mbytes
Power Consumption	60Watts(Maximum)
Dimensions	440mm(W) x 280mm(D) x 44mm(H)
Power Supply	100~240VAC, 50 /60Hz, 0.8A (maximum)
Ventilation	2 x DC cooling fan with auto detect function
Operating temperature	-10°C ~60°C, 10%~95%RH
Storage temperature	-40°C ~70°C, 95% RH
EMI	FCC Class A, CE
Safety	UL, cUL, CE/EN60950

