



MIL-SM2401MAF

24-Port 10/100 BASE-TX POE

Two combo ports

10/100/1000BASE-T/1000Base-X SFP

Advanced Managed Switch

User Guide

Rev.1.01
Nov-2009

FCC Warning

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

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

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Contents

FCC Warning	i
CE Mark Warning	i
INTRODUCTION	1
Features	1
Software Features	2
Package Contents	6
HARDWARE DESCRIPTION	7
Physical Dimension	7
Front Panel	7
LED Indicators	8
Rear Panel	10
Desktop Installation	10
Attaching Rubber Pads	10
Rack-mounted Installation	11
Power On	11
NETWORK APPLICATION	12
Small Workgroup	12
Segment workgroup	13
DC Power Input	14
CONSOLE MANAGEMENT	15
Connecting to the Switch	15
Login in the Console Interface	15
CLI Management	16
Commands Level	16
Commands Set List	18
System Commands Set	18
Port Commands Set	21
Trunk Commands Set	25

VLAN Commands Set26

Spanning Tree Commands Set.....31

QOS Commands Set35

IGMP Commands Set37

Mac / Filter Table Commands Set.....38

SNMP Commands Set40

Port Mirroring Commands Set.....41

802.1x Commands Set.....42

TFTP Commands Set45

UPS Commands Set.....46

PoE Commands Set.....47

System log Commands Set.....48

SNTP Commands Set.....49

WEB-BASED MANAGEMENT.....50

About Web-based Management50

Preparing for Web Management.....50

System Login50

Port status51

 View the Port Information53

Port Statistics.....53

Administrator54

 IP Address55

 Switch Setting.....55

 Basic55

 Advanced56

 Misc Configuration.....58

Console Port Information.....59

Port Controls.....60

Trunking61

 Aggregator setting61

 Aggregator Information.....63

- Aggregator State Activity64
- Forwarding and Filtering65
 - IGMP Snooping65
 - Static MAC Address66
- VLAN configuration.....68
 - Port-based VLAN68
 - 802.1Q VLAN71
- Spanning Tree76
 - System Configuration77
 - Per Port Configuration78
- Port Mirroring80
- SNMP Management82
- Security Manager83
- SNTP Configuration.....84
- 802.1X Configuration.....85
 - System Configuration85
 - Per port Configuration86
 - Misc Configuration.....87
- System Log.....87
- Save Configuration89
- TFTP Update Firmware89
- Configuration Backup90
 - TFTP Restore Configuration.....90
 - TFTP Backup Configuration91
- Factory Default91
- System Reboot92
- Power Status92
- PoE Status.....93
- TROUBLESHOOTING96**
- Incorrect connections.....96
 - Faulty or loose cables96
 - Non-standard cables96

Improper Network Topologies97

Diagnosing LED Indicators97

Diagnosing PoE problems97

TECHNICAL SPECIFICATION100

APPENDIX103

Console Port Pin Assignments 103

Cables 104

100BASE-TX/10BASE-T Pin Assignments..... 104

2 Gigabit Copper/SFP (mini-GBIC) combo port: 105

Introduction

The 24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch is a multi-port Switch that can be used to build high-performance switched workgroup networks. This switch is a store-and-forward device that offers low latency for high-speed networking and allows the switch to auto-learn and store source address in an 8K-entry MAC address table. The switch is targeted at workgroup, department or backbone computing environment.

The 24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch has 24x auto-sensing 10/100Base-TX RJ-45 ports and all ports support PoE injector function. The switch has 2 auto-detected Giga port for higher connection speed. Also, the switch provides one extra 48V_{DC} power input for the power supply input connection.

Features

- 24 10/100 plus 2 Mini-GBIC /Gigabit Copper combo switch with 24 PoE injectors and build in 200W AC power
- Confirms to IEEE802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit Fiber, 802.3af Power over Ethernet
- Provides extra DC 48V input with redundant function and management power status through RS-232 port
- High Back-Plane bandwidth 8.8Gbps
- Supports IEEE802.1w Rapid Spanning Tree
- Supports IGMP Snooping and IGMP Query mode for Multi-media application
- Port Mirror and Bandwidth Control supported
- Supports GVRP function
- End point insert mode remote power feeding
- Supports IEEE802.3x Flow Control
 - Flow Control with full duplex

- Back Pressure with half duplex
- Supports Port Based VLAN /802 .1Q Tag VLAN
- Supports IEEE802.3ad Port Trunk with LACP
- Supports Spanning Tree protocol IEEE 802.1d
- Supports IEEE 802.1p Class of Service
- Supports IEEE 802.1x User Authentication
- Supports Broadcast Storm Filter
- Supports DHCP Client
- Supports SNTP
- Supports System Event Log
- Management by Web/SNMP/Telnet/Console

Software Features

Management	SNMP management Telnet management Web management RS-232 terminal console for command line interface management
SNMP MIB	RFC 1157 SNMP RFC 1213 MIB II RFC 1643 Ethernet like RFC 1493 Bridge MIB RFC 2674 VLAN MIB private MIB RFC 1628 UPS MIB RFC3621 Power Ethernet MIB

<p>Type of Trap</p>	<p>Cold start Link down Link up, Authorization fail Trap stations up to 3 Private trap for power supply device</p>
<p>RFC Standard</p>	<p>RFC 2030 SNMP RFC 2821 SMTP (option) RFC 1492 TACACS+ (option) RFC 1215 Trap RFC 1757 RMON 1</p>
<p>Software Upgrade</p>	<p>TFTP Console</p>
<p>Port Trunk</p>	<p>Support IEEE802.3ad with LACP function Up to 7 trunk groups and group members up to 4 The trunk port within 24-port 10/100TX and extension module</p>
<p>Spanning Tree</p>	<p>IEEE802.1d Spanning Tree IEEE802.1w Rapid Spanning Tree</p>
<p>VLAN</p>	<p>Port based VLAN IEEE802.1Q Tag VLAN VLAN groups up to 256 The VLAN ID can be assigned from 1 to 4094</p>
<p>Class of Service</p>	<p>Per system supports high and low queues The priority service rule: first come first service, all High before Low, WRR for High or low weight</p>

Port Based Priority	<p>Supports 3 settings: Disable, Low or High priority</p> <p>When set to “Disable”, the income packet will follow QOS policy; Otherwise, the packet will follow port priority setting to “High/Low” queue</p>
IGMP	<p>IGMP snooping for multimedia application and supports 256 groups</p>
Port Security	<p>Ingress and egress MAC address filter and static source MAC address lock</p>
Port Mirror	<p>Global system supports 3 mirroring types: RX, TX and Both packet</p> <p>The maximum of port mirror entries is up to 25</p>
Bandwidth Control	<p>Per port supports bandwidth control</p> <p>Per level 100Kbps</p>
802.1x Authentication	<p>IEEE802.1x User-Authentication and can report to RADIUS server</p> <ul style="list-style-type: none"> ■ Reject ■ Accept ■ Authorize ■ Disable
DHCP	<p>DHCP client</p>
Packet filter	<p>Broadcast storm filter</p>

<p>Fault status detect</p>	<p>Null: no PD presents Overload: current support over 475mA @ DC 48V and over 50 milliseconds DR fail: PD discovery resistor is not in the limited range</p>
<p>Parametric information</p>	<p>Displays current PD parameters:</p> <ul style="list-style-type: none"> ■ Discover-resistor detected value ■ Current ■ Voltage ■ Power consumption ■ Classification current ■ Determined class
<p>Port configuration control</p>	<p>Port Disable/Enable PD detect control (enable/disable) Classification detect control (enable/disable) DC disconnect detect control</p>
<p>Mode status</p>	<p>System detects status:</p> <ul style="list-style-type: none"> ■ I-sample ■ V-sample ■ R-detect
<p>SNTP</p>	<p>RFC 2030 Simple Network Time Protocol</p>
<p>SMTP</p>	<p>RFC2821 Simple Mail Transfer protocol (option)</p>
<p>System Log</p>	<p>System Log record up to 1000 entries</p>

Power monitor	Power supply monitoring function for AC power, DC power Additional DC power supply can be installed with PoE switch, and PoE-UPWM
Power testing	Supports power supply testing (CLI)

Package Contents

Unpack the contents of the 24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch and verifies them against the checklist below:

- 24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch x 1
- Power Cord x 1
- Rubber Pad x 1
- Rack-mounted kit x 1
- RS-232 cable x 1
- User Manual x 1

Compare the contents of the 24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch package with the standard checklist above. If any item is missing or damaged, please contact the local dealer for exchanging.

Hardware Description

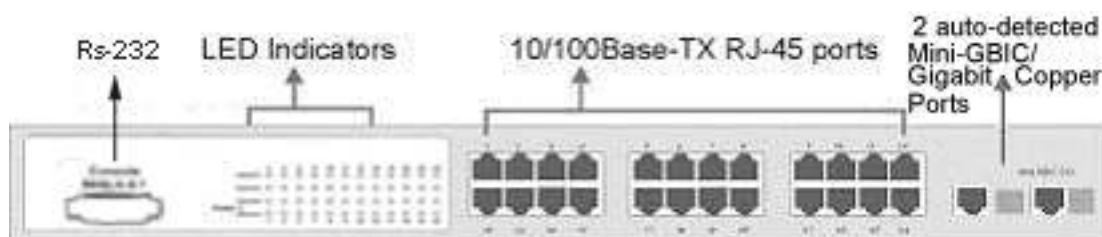
This chapter mainly describes the hardware of the 24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch and gives a physical and functional overview on the certain switch.

Physical Dimension

The physical dimension of 24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch is **440mm x 280mm x 44mm (W x D x H)**

Front Panel

The front panel of the 24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch consists of 24x 10/100Base-TX RJ-45 ports (Auto MDI/MDIX), 2 auto-detected Gigabit Copper/Mini-GBIC ports, and one console port. The LED Indicators are also located on the front panel of the Switch.



Front panel of the 24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch

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

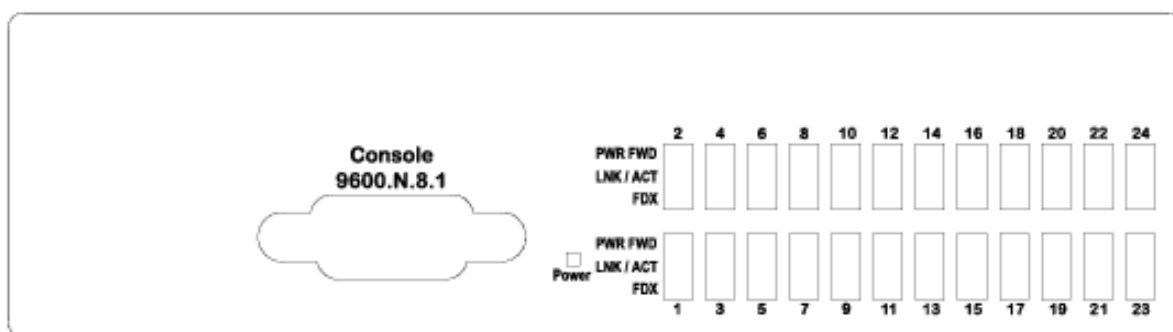
In general, **MDI** means connecting to another Hub or Switch while **MDIX** means connecting to a workstation or PC. Therefore, **Auto MDI/MDIX** would allow connecting to another Switch or workstation without changing non-crossover or

crossover cabling.

- **2 Giga port:** Traditional RJ-45 ports can be used for uplinking wide-band paths in short distance (< 100 m), or the appropriate replaceable mini-GBIC ports can be used for the application of wideband uplinking and long distance transmissions to fit the field request flexibly.

LED Indicators

The LED indicators display a real-time indication of systematic operation status. There are three LED-Indicators (Link/Activity, Full duplex, power forwarding) for each UTP port and one power LED for the system unit. The following table provides descriptions of the LED statuses and meaning.



LED indicators

LED	Status	Description
Power	Green	Power On
	OFF	Power is not connected
LNK/ACT	Green	The port is connecting with the device.

	BLINK	The port is receiving or transmitting data.
	OFF	No device attached.
FDX	Orange	The port is operating in Full-duplex mode.
	OFF	In Half-duplex mode
Power Forwarding	Green	The PoE Injector function is on and power is forwarding the attached PD device
	OFF	The PoE injector function disables
LNK/ACT (25 & 26 port /Giga port)	Green	The port is connecting with the device and operating at speed of 1000Mbps
	Orange	The port is connecting with the device and operating at speed of 100Mbps
	BLINK	The port is receiving or transmitting data.
	OFF	No device attached
FDX/COL (25 & 26 port /Giga port)	Orange	The port is operating in Full-duplex mode

	BLINK	Collision of Packets occurs in the port
	OFF	In Half-duplex mode

Rear Panel

The two fans, two console ports, and the 3-pronged power plugs are located at the rear panel of 24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch shown as below. The switch also provides one DC 48V input for the extra power connection and one DC 48V internal power supply for the power redundant. The two-console ports are for connecting with UPS device to manage UPS device or connect with the power supply device for managing it.



The rear panel of the 24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch

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 Pads

1. Make sure mounting surface on the bottom of the switch is grease and dust free.

2. Remove adhesive backing from the Rubber Pads.
3. Apply the Rubber Pads to each corner on the bottom of the switch. These footpads can prevent the switch from shock/vibration.

Rack-mounted Installation

The switch 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:

1. 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.
2. After attaching both mounting brackets, position the 24 10/100TX plus 2 Mini-GBIC/Copper managed PoE 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 AC voltage range of 100-240V and Frequency of 50~60Hz. Check the power indicator on the front panel to see if power is properly supplied.

Network Application

This section provides a few samples of network topology in which the switch is used. In general, the 24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch with its large address table (8K MAC address) and high performance are ideal for interconnecting networking segments.

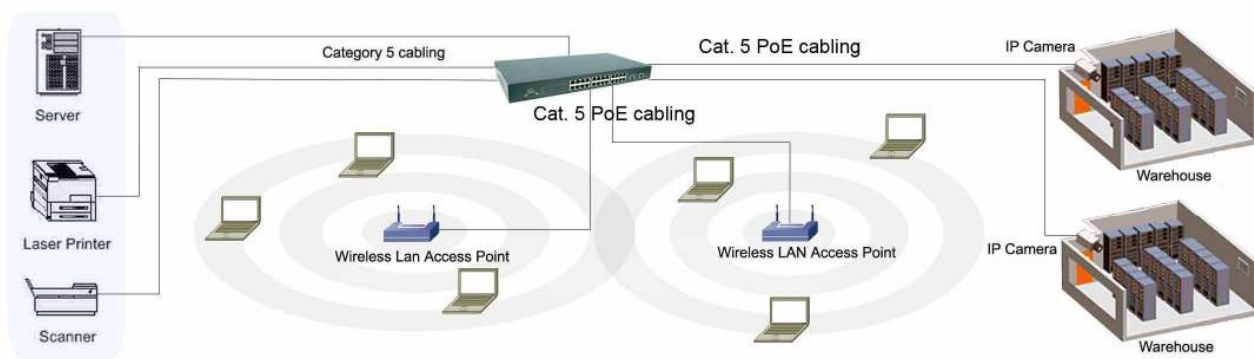
PC, workstations, and servers can communicate each other by directly connecting with 24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch. The switch automatically learns node addresses, which are subsequently used to filter and forward all traffic based on the destination address.

24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch provides PoE injector function on every Ethernet port which can provide the power to the PD device, such as AP or switch. It can solve the problem of the PD device position limitation of power supply.

Using Uplink port, the Switch can connect with another switch or hub to interconnect other small-switched workgroups to form a larger switched network. Meanwhile, you can also use fiber ports to connect switches.

Small Workgroup

24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch can be used as a standalone switch to which personal computers, server, printer server, are directly connected to form a small workgroup.

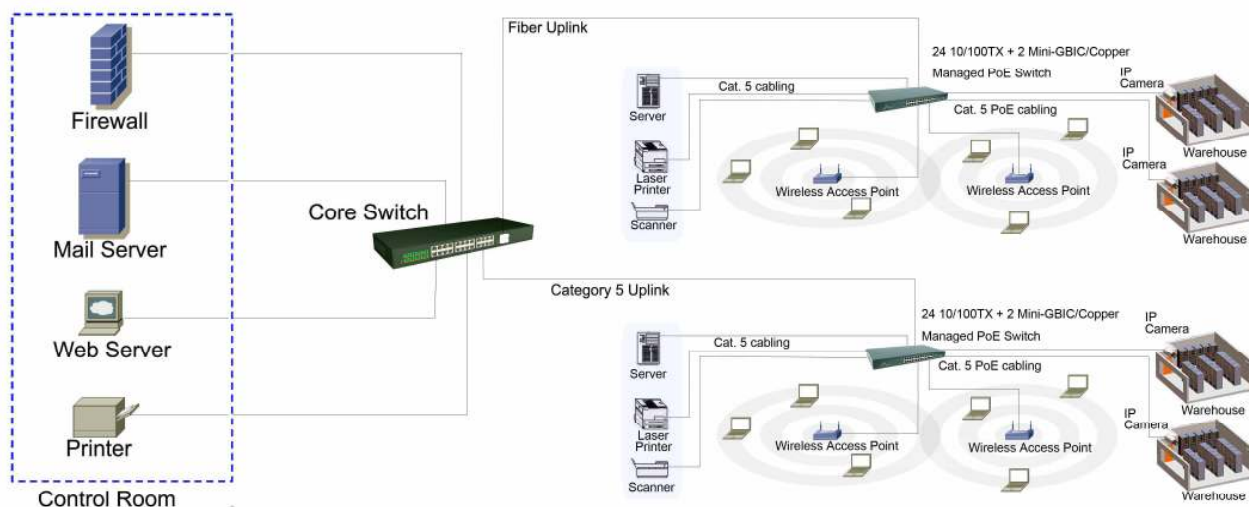


Small Workgroup Application

Segment workgroup

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

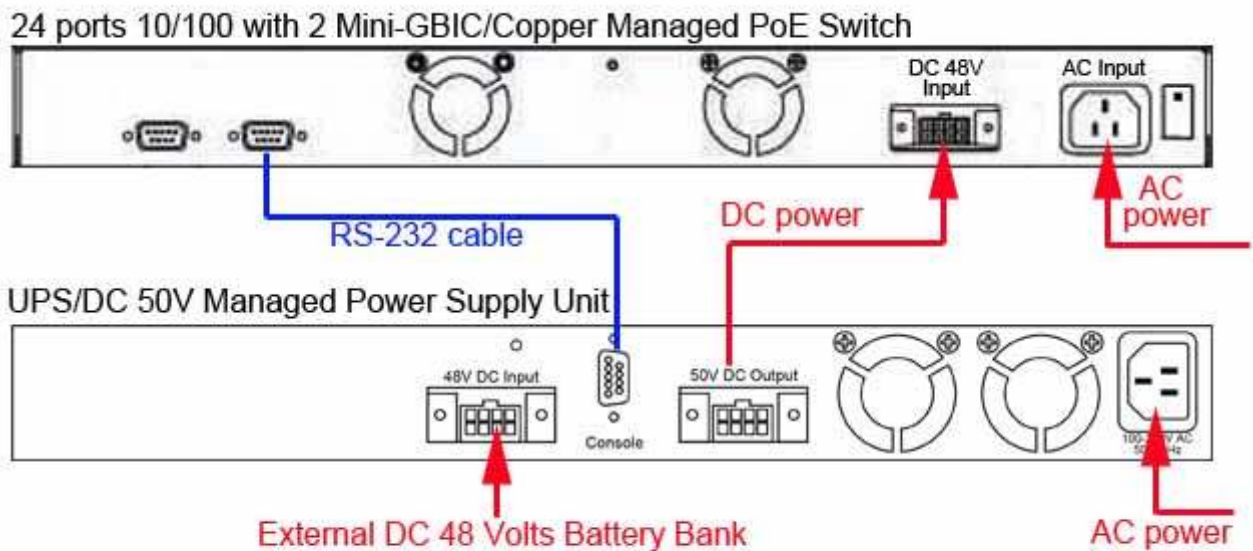
In the illustration below, two managed PoE switches with PCs, print server, local server, wireless AP (IEEE 802.3af compliant), and IP camera (IEEE 802.3af compliant) attached are both connect to the core switch. All the devices in this network can communicate with each other through the core switch.



Segment workgroup Application

DC Power Input

The 24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch has a DC 48V power input for the extra power supply connection. The DC 48V power input can be used as a power backup when the AC power is down or no AC power supply in the installation. The AC power and the DC 48V power can be connected at the same time, but the switch will use the DC 48V as the master power input and the AC power as the secondary or backup power input. The following figures are example of the application. In the figure, the DC 48V power input connects with the power supply device and through the RS-232 connection to manage the power supply device.



Console Management

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 users to set switch for remote terminal as if the console terminal were directly connected to it.

Login in the Console Interface

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

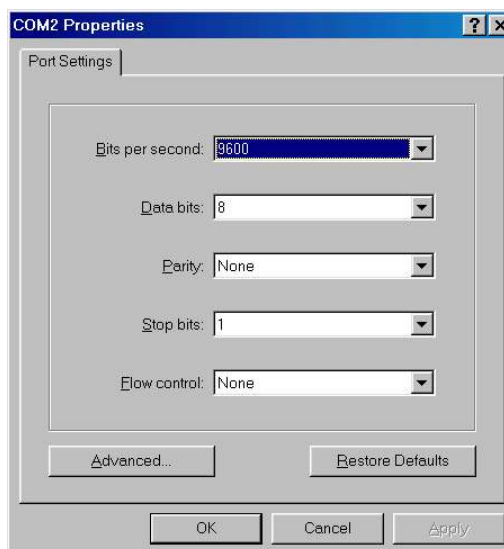
Baud Rate: 9600 bps

Data Bits: 8

Parity: none

Stop Bit: 1

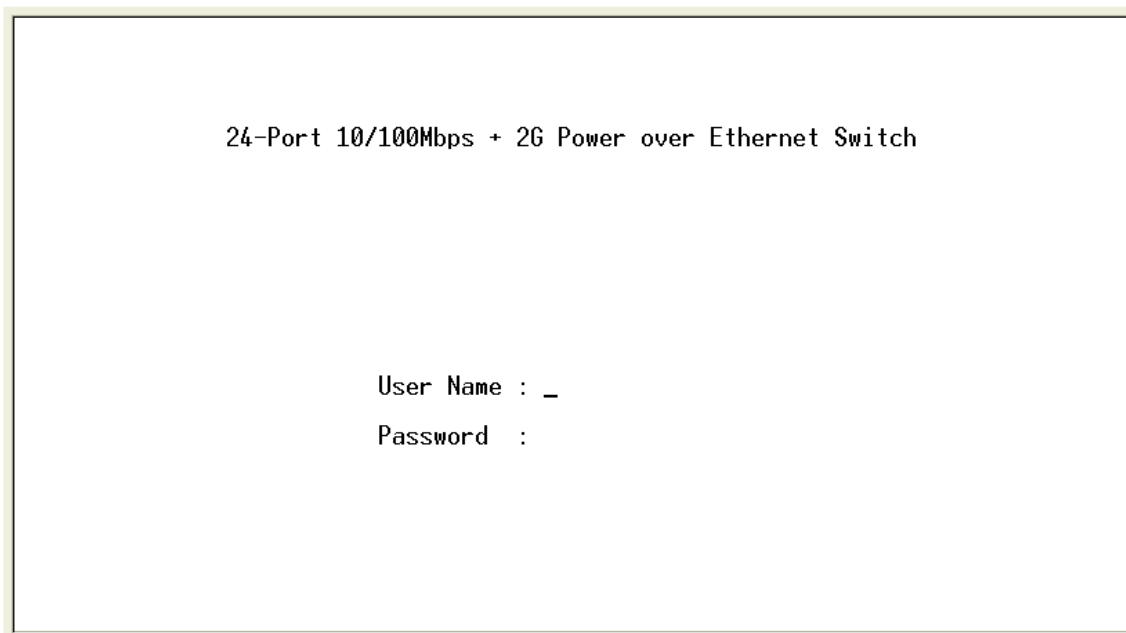
Flow control: None



The settings of communication parameters

After finishing 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 right after as below. The figure shown below is a login screen:



Console login screen

CLI Management

The system supports console management—CLI command. After logging in to the system, a command prompt shows up. To enter CLI management interface, enter “**enable**” command. The following tables list the CLI commands and description.

Commands Level

Modes	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your switch.	switch>	Enter logout or quit.	The user commands available at the user level are a subset of those available at the privileged level.

				Use this mode to <ul style="list-style-type: none"> • Perform basic tests. • Display system information.
Privileged EXEC	Enter the enable command while in user EXEC mode.	switch#	Enter disable to exit.	The privileged command is advance mode Privileged this mode to <ul style="list-style-type: none"> • Display advance function status • Save configures
Global Configuration	Enter the configure command while in privileged EXEC mode.	switch (config)#	To exit to privileged EXEC mode, enter exit or end	Use this mode to configure parameters that apply to your switch as a whole.
VLAN database	Enter the vlan database command while in privileged EXEC mode.	switch (vlan)#	To exit to user EXEC mode, enter exit.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the interface command (with a specific interface) while in global configuration mode	switch (config-if)#	To exit to global configuration mode, enter exit. To exist to privileged EXEC mode, or end.	Use this mode to configure parameters for the switch and Ethernet ports.

UPS	Enter the ups command while in privileged EXEC mode.	switch(ups)#	To exit to privileged EXEC mode, enter exit	Use this mode to UPS parameters for the switch.
PoE	Enter the PoE command while in privileged EXEC mode.	switch(PoE)#	To exit to privileged EXEC mode, enter exit	Use this mode to PoE parameters for the switch.

Commands Set List

■ System Commands Set

Commands	Command Level	Description	Defaults	Example
system name [word]	Global configuration mode	Set switch system name string		Switch (config)# system name xxx
system location [word]	Global configuration mode	Set switch system location string		Switch (config)# system location xxx
system description [word]	Global configuration mode	Set switch system description string		Switch (config)# system description xxx
system contact [word]	Global configuration mode	Set switch system contact window string		Switch (config)# system contact xxx

<p>ip address [IP-address] [subnet-mask]] [gateway]</p>	<p>Global configuration mode</p>	<p>Use the ip address interface configuration command to set an IP address for a switch. Use the no form of this command to remove an IP address or to disable IP processing.</p>	<p>Switch (config)# ip address 192.168.1.1 255.255.255.0 192.168.1.254</p>
<p>write [memory] terminal]</p>	<p>Privileged EXEC</p>	<p>The “write memory” is save configuration and the “write terminal” is show all configuration.</p>	<p>Switch# write memeory Update NVRAM to Flash Complete Switch# write terminal</p>
<p>reload</p>	<p>Global configuration mode</p>	<p>Halt and perform a cold restart</p>	<p>Switch (config)# reload</p>
<p>default</p>	<p>Global configuration mode</p>	<p>Restore to default</p>	<p>Switch (config)# default</p>
<p>username [word]</p>	<p>Global configuration mode</p>	<p>Changes a login username. (maximum 10 words)</p>	<p>Switch (config)# username xxxxxx</p>
<p>password [word]</p>	<p>Global configuration mode</p>	<p>Specifies a password (maximum 10 words)</p>	<p>Switch (config)# password xxxxxx</p>

<p>show accounting</p>	<p>Privileged EXEC</p>	<p>Show username & password</p>	<p>Switch# show accounting Username: root Password: root</p>
<p>show system-info</p>	<p>User EXEC</p>	<p>Show system information</p>	<p>Switch> show system-info Name: switch1 location: lab Description: layer2 switch Contact: somewhere Serial NO: 1.00</p>
<p>show ip</p>	<p>Privileged EXEC</p>	<p>Show IP information</p>	<p>Switch# show ip address ip: 192.168.1.1 Address subnet: 255.255.255.0 Address gateway: 192.168.1.254</p>
<p>show version</p>	<p>User EXEC</p>	<p>Use the show version user EXEC command to display version information for the hardware and firmware.</p>	<p>Switch> show version Firmware version: 1.0 Hardware version: 3.0 Kernel version: 1.10</p>

■ **Port Commands Set**

Commands	Command Level	Description	Defaults	Example
interface [FastEthernet /module Ethernet] [slot id] [id]	Interface configuration mode	Use the fast Ethernet interface configuration command		Switch (config)# interface fastEthernet 0/1
		Use the module Ethernet interface configuration command		Switch (config)# interface moduleEthernet 1/1
duplex [full half] auto]	Interface configuration mode	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	Auto	Switch (config)# interface fastEthernet 0/1 Switch (config-if)# duplex full
		Use the duplex configuration command to specify the duplex mode of operation for module Ethernet.	Auto	Switch (config)# interface moduleEthernet 1/1 Switch (config-if)# duplex full
speed [10 100 auto]	Interface configuration mode	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet.	Auto	Switch (config)# interface fastEthernet 0/1 Switch (config-if)# speed 10

<p>speed [10 100 1000 auto]</p>	<p>Interface configuration mode</p>	<p>Use the speed configuration command to specify the speed mode of operation for module Ethernet.</p> <ul style="list-style-type: none"> ■ The 100Base-FX module only supported for speed 100 ■ The 1000Base-FX module only supported for speed 1000 & auto 		<p>Switch (config)# interface fastEthernet 1/2 Switch (config-if)# speed 1000</p>
<p>flowcontrol on or no flowcontrol</p>	<p>Interface configuration mode</p>	<p>Use the flow control configuration command on Ethernet ports to control traffic rates during congestion.</p> <p>Use the no form of this command to disable security on the port.</p>	<p>On</p>	<p>Switch (config)# interface fastEthernet 0/1 Switch (config-if)# flowcontrol on</p>
<p>security on or no security</p>	<p>Interface configuration mode</p>	<p>Use the security configuration command on Ethernet ports.</p> <p>Use the no form of this command to disable security on the port.</p>	<p>Disable</p>	<p>Switch (config)# interface fastEthernet 0/1 Switch (config-if)# security on</p>

<p>priority on [high low] or no priority</p>	<p>Interface configuration mode</p>	<p>Use the priority configuration command on Ethernet ports. Use the no form of this command to disable security on the port.</p>	<p>Disable</p>	<p>Switch (config)# interface fastEthernet 0/1 Switch (config-if)# priority on high</p>
<p>Bandwidth [in out] [value]</p>	<p>Interface configuration mode</p>	<p>Set bandwidth in or out rate. The value range is (0~999), and zero of the value is disable (The module can't be setting)</p>	<p>Disable</p>	<p>Switch (config)# interface fastEthernet 0/1 Switch (config-if)# bandwidth in 50</p>
<p>State [Enable Disable]</p>	<p>Interface configuration mode</p>	<p>Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.</p>	<p>Enable</p>	<p>Switch (config)# interface fastEthernet 0/1 Switch (config-if)# state disable</p>

<p>show interface configuration</p>	<p>Interface configuration mode</p>	<p>show interface configuration status</p>		<p>Switch (config)# interface fastEthernet 0/1 Switch (config-if)# show interface configuration</p>
<p>show interface status</p>	<p>Interface configuration mode</p>	<p>show interface actual status</p>		<p>Switch (config)# interface fastEthernet 0/1 Switch (config-if)# show interface status</p>
<p>show interface accounting</p>	<p>Interface configuration mode</p>	<p>show interface statistic counter</p>		<p>Switch (config)# interface fastEthernet 0/1 Switch (config-if)# show interface accounting</p>
<p>show bandwidth</p>	<p>Interface configuration mode</p>	<p>Display the bandwidth of the values</p>		<p>Switch (config)# interface fastEthernet 0/1 Switch (config-if)# show bandwidth</p>

interface [FastEthernet /module Ethernet] [slot id] [id]	Interface configuration mode	Use the fast Ethernet interface configuration command	Switch (config)# interface fastEthernet 0/1
---	------------------------------	---	---

■ **Trunk Commands Set**

Commands	Command Level	Description	Defaults	Example
show group [group-ID]	Privileged EXEC mode	Display trunk group information. If there is no group-number in put, display all trunk groups.		Switch # show group 1 Group Trunk.1: Ports: 02 03 04 Priority: 0001 Lacp: Enable Work ports: 0
port group [group-ID] [port-list] lacp [on off] workp [work ports] no port group [group-ID] lacp [on off] workp [work ports]	Global configuration mode	Add trunking group. Use the no form of this command to delete trunking group.	Disable	LACP: Switch (config)# port group 1 1-4 lacp on workp 2 Trunk without LACP: Switch (config)# port group 1 1-4 lacp off workp 4
port group [group-ID] activityport [port ID]	Global configuration mode	Set trunking group port active		Switch (config)# port group 3 activityport 2-4 Trunk.1 Lacp:

				Enable Check OK! NEW: 2 4 Update finished!!
--	--	--	--	--

■ VLAN Commands Set

Commands	Command Level	Description	Defaults	Example
Vlan database	Privileged EXEC mode	To enter the VLAN configuration interface		Switch# vlan database Switch(vlan)#
vlanmode [disable] portbase 802.1q gvrp]	VLAN database mode	To set switch VLAN mode .Use the no form of this command to restore to default.	Disable	Switch (vlan)# vlanmode 802.1q
Port Base VLAN				
vlan [Group Name] grp-id [Group ID] port [Port ID]	VLAN database mode	Add new Port Base VLAN		Switch (vlan)# vlan v2 grp-id 2 port 1-4
no vlan [Group Name] [Group ID]	VLAN database mode	Delete port base VLAN group		Switch (vlan)# no vlan v2 2
show vlan [Group Name] [Group ID] or show vlan	VLAN database mode	Show VLAN of Group Name or Group ID information		Switch (vlan)# Show vlan v2 2

vlan [Group name] add [port ID]	VLAN database mode	Set the port of some port group		Switch (vlan)# vlan v2 add 5
vlan [Group name] delete [port ID]	VLAN database mode	Remove the port from it's port group.		Switch (vlan)# vlan v2 delete 5
802.1Q 802.1Q with GVRP VLAN mode				
vlan [Group name] vlanid [group ID] port [port ID] tag [port ID]	VLAN database mode	Add new 802.1Q VLAN [group name]: VLAN name [group ID]: 2 ~ 4094 [port ID]: port members 1~9		Switch(vlan)# vlan v2 vlanid 2 port 1-4 tag 2-4
vlan [group name] add [port ID] [tagged untagged]	VLAN database mode	Set the port of some port group tagged or untagged		Switch(vlan)# vlan v2 add 5-8 tagged or vlan v2 add 5-8 untagged
vlan [group name] delete [port ID]	VLAN database mode	Remove the port from its port group.		Switch(vlan)# vlan v2 delete 5
no vlan [Group name] or [group ID]	VLAN database mode	Delete 802.1Q VLAN group		Switch (vlan)# no vlan v2 Switch (vlan)# no vlan v2 2

<p>vlan protocol [group name] [protocol value] vlanid [group ID] port [port ID] tag [port ID]</p>	<p>VLAN database mode</p>	<p>Add protocol vlan [group name]: vlan group name</p> <p>IP-ip ARP-arp Appletalk-app Appletalk_AARP-app_arp Novell_IPX-ipx Banyan_vines-banyan_c4 Banyan_vines-banyan_c5 Banyan_vines-banyan_ad Decent_mop_01-decent_01 Decent_mop_02-decent_02 Decent_dpr-decent_dpr Decent_LAT-decent_lat Decent_LAVC-decent_lavc IBM SNA-ibm X.75 internet-x75 X.25 Layer3-x25</p> <p>[VLAN ID]: 2 ~ 4094 [port ID]: port ID 1~10</p>	<p>Switch(vlan)# vlan protocol v3 ip vlanid 2 port 5-8 tag 6,8</p> <p>Switch(vlan)# vlan protocol v3 arp vlanid 2 port 5-8 tag 6,8</p> <p>Switch(vlan)# vlan protocol v3 banyan vlanid 2 port 5-8 tag 6,8</p>
--	---------------------------	---	--

<p>vlanidrange [VLAN ID range]</p>	<p>VLAN database mode</p>	<p>Set VLAN ID range [1~255] range 0 [256~511] range 1 [512~767] range 2 [768~1023] range 3 [1024~1279] range 4 [1280~1535] range 5 [1536~1791] range 6 [1792~2047] range 7 [2048~2303] range 8 [2304~2559] range 9 [2560~2815] range 10 [2816~3071] range 11 [3072~3327] range 12 [3328~3583] range 13 [3584~3839] range 14 [3840~4094] range 15</p>		<p>Switch (vlan)# vlanidrange 2</p> <p>OLD: 0 NEW: 2</p>
<p>VLAN protocol [Group name] add [port ID] [tagged </p>	<p>VLAN database mode</p>	<p>Set the port of some port group tagged or untagged</p>		<p>Switch (vlan)# vlan protocol v2 add 5 tagged</p>

untagged]				
VLAN protocol [Group name] delete [port ID]	VLAN database mode	Remove the port from its port group.		Switch (vlan)# vlan protocol v2 delete 5
show vlan [Group name] [Group ID] or show vlan	VLAN database mode	Show VLAN of Group Name or VLAN ID information vlanid: 1 ~ 4094		Switch (vlan)# show vlan v2 2
show vlan protocol	VLAN database mode	show protocol vlan Protocol ip ipx netbios		Switch (vlan)# show vlan protocol
port [port ID] pvid [port VID] ingressfilter1 [on off] ingressfilter2 [on off]	VLAN database mode	Set Port PVID and Ingress Filter Rules1 & Ingress Filter Rules2		Switch (vlan)# port 2 pvid 2 ingressfilter1 off ingressfilter2 on
show port [port ID]	VLAN database mode	show Port PVID and Ingress Filter Rules1 & Ingress Filter Rules2		Switch (vlan)# show port 2 Port ID: 2 Port Vid: 2 Ingress 1 Filter: Disable Ingress 2 Filter: Enable

■ **Spanning Tree Commands Set**

Commands	Command Level	Description	Defaults	Example
<p>show spanning-tree</p>	<p>User EXEC mode</p>	<p>Display a summary of the spanning-tree states.</p>		<p>Switch> show spanning-tree System: Priority: 32768 Max Age: 20 Hello Time: 2 Forward Delay: 15 Priority: 32768 Mac Address: 004063800030 Root_Path_Cost: 0 Root Port: we are root Max Age: 20 Hello Time: 2 Forward Delay: 15</p>
<p>spanning-tree [on / off] or no spanning-tree</p>	<p>Global configuration mode</p>	<p>Use the spanning-tree global configuration command to enable Spanning Tree Protocol (STP). Use the no form of the command to restore to default</p>	<p>Disable</p>	<p>Switch (config)# spanning-tree on or Switch (config)# no spanning-tree</p>

<p>spanning-tree priority [number]</p>	<p>Global configuration mode</p>	<p>Use the spanning-tree max-age global configuration command to change the priority.</p> <p>Use the no form of this command to return to the default interval.</p>	<p>32768</p>	<p>Switch (config)# spanning-tree priority 32767</p>
<p>spanning-tree max-age [seconds]</p>	<p>Global configuration mode</p>	<p>Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputes the Spanning Tree Protocol (STP) topology. Use the</p>	<p>20 sec</p>	<p>Switch (config)# spanning-tree max-age 15</p>

		no form of this command to return to the default interval.		
spanning-tree hello-time [seconds]	Global configuration mode	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs). Use the no form of this command to return to the default interval.	2 sec.	Switch (config)# spanning-tree hello-time 3
stp-path-cost [number]	Interface configuration mode	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the	10 Mbps – 100 100 Mbps – 10	Switch (config)# interface fastEthernet 0/2 Switch (config-if)# stp-path-cost 20

		<p>forwarding state.</p> <p>Use the no form of this command to return to the default value.</p>		
<p>spanning-tree forward-time [seconds]</p>	<p>Global configuration mode</p>	<p>Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding. Use the no form of this command to return to the default value.</p>	<p>15 sec.</p>	<p>Switch (config)# spanning-tree forward-time 20</p>
<p>stp-path-priority [number]</p>	<p>Interface configuration mode</p>	<p>Use the spanning-tree port-priority interface configuration command to configure a port</p>	<p>128</p>	<p>Switch (config)# interface fastEthernet 0/2 Switch (config-if)# stp-path-priority 127</p>

		priority that is used when two switches tie for position as the root switch. Use the no form of this command to return to the default value.		
--	--	--	--	--

■ QOS Commands Set

Commands	Command Level	Description	Defaults	Example
qos storm-control [5 10 15 20 25] off (%) or no storm-control	Global configuration mode	Enable/Disable broadcast storm control. Use the no form of this command to restore to default.	OFF	Switch (config)# qos storm-control 5
qos low-priority-delay-bound [on off] [sec.] or no qos low-priority-delay-bound	Global configuration mode	Enable/Disable low priority delay board. Use the no form of this command to restore to default.	OFF	Switch (config)# qos low-priority-delay-bound on 1
qos level [priority]	Global configuration mode	[Priority] 0~7	0~3 LOW 4~7 HI	Switch (config)# qos level 2,3
no qos level [priority]	Global configuration mode	[Priority] 0~7	0~3 LOW 4~7 HI	Switch (config)# no qos level 0-7

<p>qos queuepolicy [Policy] hi [number] low [number]</p>	<p>Global configuration mode</p>	<p>[Policy]:fcfs: first in and first out wrr: weight round robin ahbl: all high before low. [Priority] Hi:1~7 Low:1</p>	<p>WRR Hi 2 Low 1</p>	<p>WRR: Switch (config)# qos queuepolicy wrr hi 7 low 1 First Come First Served: Switch (config)# qos queuepolicy fcfs All High before Low: Switch (config)# qos queuepolicy ahbl</p>
<p>qos bridge-delay-bound [sec.] no qos bridge-delay-bound</p>	<p>Global configuration mode</p>	<p>Set qos bridge delay bound Use the no form of this command to restore to default.</p>	<p>OFF</p>	<p>Switch (config)# qos bridge-delay-bound 1</p>
<p>show qos storm-control</p>	<p>Global configuration mode</p>	<p>Show broadcast storm control.</p>		<p>Switch (config)# show qos storm-control QOS storm control mode: ENABLE</p>
<p>show qos policy</p>	<p>Global configuration mode</p>	<p>Show qos policy</p>		<p>Switch (config)# show qos policy Qos Mode: WRR</p>

show qos low-priority-delay-bound	Global configuration mode	Show low priority delay board.	Switch (config)# show qos low-priority-delay-bound Qos low priority delay bound: 1
show qos bridge-delay-bound	Global configuration mode	Show bridge delay bound	Switch (config)# show qos bridge-delay-bound bridge-delay-bound 5

■ IGMP Commands Set

Commands	Command Level	Description	Defaults	Example
igmp [on off]	Global configuration mode	Enable /Disable IGMP snooping function	Off	Switch (config)# igmp on
igmp-query [auto enable disable]	Global configuration mode	Modify IGMP query mode	Disable	Switch (config)# igmp-query enable
show ip igmp profile	Privileged EXEC mode	Displays the details of an IGMP profile entry.		Switch# show ip igmp profile IP VID Port 224.1.1.1 10 1,2,6

■ **Mac / Filter Table Commands Set**

Commands	Command Level	Description	Defaults	Example
<p>mac-address-table aging-time [on off]</p> <p>mac-address-table aging-time [sec.]</p> <p>or no mac-address-table aging-time</p>	<p>Global configuration mode</p>	<p>Use the mac-address-table aging-time global configuration command to set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.</p> <p>Use the no form of this command to use the default aging-time interval. The aging time applies to all VLANs.</p>	<p>300 secs</p>	<p>Switch (config)# mac-address-table aging-time on</p> <p>Switch (config)# mac-address-table aging-time 333</p> <p>(Disable)</p> <p>Switch (config)# mac-address-table aging-time off</p> <p>Or</p> <p>Switch(config)# no mac-address-table aging-time</p>
<p>mac-address-table table [static filter] hwaddr [MAC address] vlanid [VLAN-ID]</p>	<p>Interface configuration mode</p>	<p>Use the mac-address-table static to add static filter addresses to the MAC address table. Use the no form of this command to remove static entries from the MAC address table.</p>	<p>N/A</p>	<p>Switch (config)# interface fastEthernet 0/2</p> <p>Switch (config-if)# mac-address-table static hwaddr 004063112233 vlanid 10</p>

<p>no mac-address-table [static filter] hwaddr [MAC address] vlanid [VLAN-ID]</p>	<p>Interface configuration mode</p>	<p>Use the no mac-address-table privileged EXEC command to delete entries from the MAC address table.</p>	<p>Switch (config)# interface fastEthernet 0/2 Switch (config-if)# no mac-address-table static hwaddr 004063112233 vlanid 10</p>
<p>show mac-address-table [static filter]</p>	<p>Privileged EXEC mode</p>	<p>Use the show mac-address-table user EXEC command to display the MAC address table.</p>	<p>Switch # show mac-address-table static</p>
<p>show mac-address-table aging-time</p>	<p>Privileged EXEC mode</p>	<p>Use the show mac-address-table user EXEC command to display the MAC address table.</p>	<p>Switch# show mac-address-table aging-time MAC Address aging-time: 300</p>

■ **SNMP Commands Set**

Commands	Command Level	Description	Defaults	Example
snmp system-name [word]	Global configuration mode	Set SNMP agent system name	N/A	Switch (config)# snmp system-name l2switch
snmp system-location [word]	Global configuration mode	Set SNMP agent system location	N/A	Switch (config)# snmp system-location lab
snmp system-contact [word]	Global configuration mode	Set SNMP agent system contact	N/A	Switch (config)# snmp system-contact where
snmp community-strings [word] right [RO RW] Or no snmp community-strings [word]	Global configuration mode	Add SNMP community string. Use the no form of this command to remove the specified community.	PUBLIC RO	Switch (config)# snmp community-strings public right RW Switch(config)# no snmp community-strings public right rw
snmp-server host [IP-address] community [word] No snmp-server	Global configuration mode	Configure SNMP server host information and community string	N/A	Switch(config)# snmp-server host 192.168.1.50 community public Switch(config)# no

host [IP address] community [word]				<i>snmp-server host 192.168.1.50 community public</i>
snmp system-name [word]	Global configuration mode	Set SNMP agent system name	N/A	Switch (config)# <i>snmp system-name I2switch</i>

■ **Port Mirroring Commands Set**

Commands	Command Level	Description	Defaults	Example
port monitor [RX TX both] [port ID] Or no port monitor	Interface configuration mode	Use the port monitor interface configuration command to enable Switch Port Analyzer (SPAN) port monitoring on a port. Use the no form of this command to return the port to its default value.	N/A	Switch (config)# <i>Interface fastEthernet 0/8</i> Switch (config-if)# <i>port monitor both 3</i>
show port monitor	Privileged EXEC mode	Use the show port monitor privileged EXEC command to display the ports for which Switched Port Analyzer (SPAN)		Switch # <i>show port monitor</i> State: Enable AnalysisPortId: 8 Port 01 TxRx: Monitor Port 02 TxRx: Port 03 TxRx:

		port monitoring is enabled.		Port 04 TxRx: Port 05 TxRx: Port 06 TxRx: Port 07 TxRx: Port 08 TxRx: Analysis Port 09 TxRx: Port 10 TxRx: OK.
--	--	-----------------------------	--	---

■ **802.1x Commands Set**

Commands	Command Level	Description	Defaults	Example
show 8021x	User EXEC mode	Display a summary of the 802.1x properties and also the port sates.	N/A	Switch> show 8021x
8021x [on off] or No 8021x	Global configuration mode	Use the 802.1x global configuration command to enable 802.1x protocols. Use the no form of the command to restore to default	Disable	Switch (config)# 8021x on
8021x system radiusip [IP address] Or no 8021x system radiusip	Global configuration mode	Use the 802.1x system radius IP global configuration command to change the radius server IP. Use the no form of this command to return to the default interval.	192.16 8.16.3	Switch (config)# 8021x system radiusip 192.168.1.1 (Default) Switch(config)# no 8021x system radiusip

<p>8021x system sharekey [number] Or no 8021x system sharekey</p>	<p>Global configuration mode</p>	<p>Use the 802.1x system sharekey global configuration command to change the shared key value.</p> <p>Use the no form of this command to return to the default interval.</p>	<p>123456 78</p>	<p>Switch (config)# 8021x system sharekey 123456</p> <p>(Default)</p> <p>Switch (config)# no 8021x system sharekey</p>
<p>8021x system serverport [Port Number]</p>	<p>Global configuration mode</p>	<p>set radius server port</p>	<p>1812</p>	<p>Switch (config)# 8021x system serverport 1815</p>
<p>8021x system accountport [Port Number]</p>	<p>Global configuration mode</p>	<p>set accounting port</p>	<p>1813</p>	<p>Switch (config)# 8021x system accountport 1816</p>
<p>8021x system nasid [word]</p>	<p>Global configuration mode</p>	<p>set NAS ID</p>	<p>NAS_L 2_ SWITC H</p>	<p>Switch (config)# 8021x system nasid test1</p>
<p>8021x misc quietperiod [sec.] Or no 8021x misc quietperiod</p>	<p>Global configuration mode</p>	<p>Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.</p> <p>Use the no form of this command to return to the default interval.</p>	<p>60 sec.</p>	<p>Switch (config)# 8021x misc quietperiod 10</p> <p>(Default)</p> <p>Switch(config)# no 8021x misc quietperiod</p>

<p>8021x misc txperiod [sec.] Or no 8021x txperiod</p>	<p>Global configuration mode</p>	<p>Use the 802.1x misc TX period global configuration command to set the TX period. Use the no form of this command to return to the default value.</p>	<p>30 sec.</p>	<p>Switch (config)# 8021x misc txperiod 5 (Default) Switch(config)# no 8021x misc txperiod</p>
<p>8021x misc supptimeout [sec.]</p>	<p>Global configuration mode</p>	<p>Set the period of time the switch wait for a supplicant response to an EAP request.</p>	<p>30 sec.</p>	<p>Switch (config)# 8021x misc supptimeout 30</p>
<p>8021x misc servertimeout [sec.]</p>	<p>Global configuration mode</p>	<p>Set the period of time the switch waits for a server response to an authentication request.</p>	<p>30 sec.</p>	<p>Switch (config)# 8021x misc servertimeout 50</p>
<p>8021x misc maxrequest [Number]</p>	<p>Global configuration mode</p>	<p>Set the number of authentication that must time-out before authentication fails and the authentication session ends.</p>	<p>2</p>	<p>Switch (config)# 8021x misc maxrequest 2</p>
<p>8021x misc reauthperiod [sec.]</p>	<p>Global configuration mode</p>	<p>Set the period of time after which clients connected must be re-authenticated.</p>	<p>3600</p>	<p>Switch(config)# 8021x misc reauthperiod 20</p>
<p>8021x prostate [reject accept authorize disable]</p>	<p>Interface configuration mode</p>	<p>Use the 802.1x port state interface configuration command to set the state of the selected port.</p>	<p>N/A</p>	<p>Switch (config)# interface fastethernet 0/3 Switch (config-if)# 8021x portstate</p>

		<ul style="list-style-type: none"> ■ 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. 		accept
--	--	---	--	---------------

■ **TFTP Commands Set**

Commands	Command Level	Description	Defaults	Example
copy flash:config.txt tftp [TFTP IP address] [filename]	Global configuration mode	Backup configure file command		Switch (config)# copy flash:config.txt tftp Server

				IP:192.168.1.1 Image Filename:backup.dat
tftp:config.text flash [TFTP IP address] [file name]	Global configuration mode	Restore configure file command		Switch(config)# Tftp:config.text flash Server IP:192.168.1.1 Image Filename:restore. dat
tftp:firmware flash [TFTP IP address] [file name]	Global configuration mode	Update firmware command		Switch (config)# Tftp:firmware flash Server IP:192.168.1.1 Image Filename:image.bi n

■ **UPS Commands Set**

Commands	Command Level	Description	Defaults	Example
status	UPS mode	Display a summary of the UPS status.		Switch (ups)# status Input Output Voltage.....

Info	UPS mode	Show UPS information	Switch (ups)# info Company Name :xxx Model :xxx Version :xxx
Test 10	UPS mode	UPS will perform the self-test for 10 seconds.	Switch (ups)# test10 test OK

■ **PoE Commands Set**

Commands	Command Level	Description	Defaults	Example
status	PoE mode	Show PoE information		Switch(PoE)# status
setpm [on off]	PoE mode	Enabling or disabling the power management.		Switch(PoE)# setpm on Set Power Management Enable
setlimit [value]	PoE mode	Enabling or disabling total power output limit. When is enabling, the total power output limit will follow the value that set in power limit max.		Switch(PoE)# setlimit 100

portebi [enable disable] [ports]	PoE mode	Enabling or disabling the port PoE injected function.		Switch(PoE)# portebi disable 1-3
portcls [enable disable] [ports]	PoE mode	Enabling or disabling per port power limit by classification.		Switch(PoE)# portcls enable 1-3
portmng [enable disable] [ports]	PoE mode	Enabling or disabling per port power limit by management.		Switch(PoE)# portmng enable 2-5
portleg [enable disable] [ports]	PoE mode	Enabling or disabling per port legacy detection.		Switch(PoE)# portleg enable 3-6
portpri [critical high low] [ports]	PoE mode	Set port priority for the power supply management.		Switch(PoE)# portpri critical 2
portplm [value] [ports]	PoE mode	Set per port power limit Max.		Switch(PoE)# portplm 12200 5-7

■ **System log Commands Set**

Commands	Command Level	Description	Defaults	Example
show systemlog	User EXEC	Display system log.		Switch> show systemlog

show systemlog	Privileged EXEC	Show system log client & server information		switch# show systemlog Syslog Client: Enable Syslog Server Ip: 192.168.16.2
systemlog ip [IP address]	Global configuration mode	Set System log server IP address.		Switch(config)# systemlog ip 192.168.1.100
systemlog [enable disable]	Global configuration mode	Enable or disable system log mode		Switch(config)# systemlog enable

■ **SNTP Commands Set**

Commands	Command Level	Description	Defaults	Example
sntp [enable disable]	Global configuration mode	Enable/Disable SNTP.	Disable	Switch(config)# sntp enable Switch(config)# sntp disable
sntp ip [IP address]	Global configuration mode	Set SNTP server IP address.		switch# sntp ip 192.168.16.123
sntp timezone [value]	Global configuration mode	Set time zone.		Switch(config)# sntp timezone 8

Web-Based Management

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

About Web-based Management

On the CPU board of the switch there is an embedded HTML web site residing in flash memory, which 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 6.0. And, it is applied with Java Applets for reducing network bandwidth consumption, enhance access speed and present an easy viewing screen.

Preparing for Web Management

Before starting web management, user can use console to log in the switch for checking the default IP of the switch. Please refer to **Console Management** Chapter for console login. If user needs change IP address in first time, please use console mode to modify it. The default value is shown as below:

IP Address: **192.168.1.77**

Subnet Mask: **255.255.255.0**

Default Gateway: **192.168.1.254**

User Name: **root**

Password: **root**

System Login

1. Launch the Internet Explorer on the PC

- Key in “http:// +” the IP address of the switch”, and then Press “**Enter**”.



Uniform Resource Locator

- The login screen appears right after.



Login screen

- Key in the user name and password. The default user name and password are the same as ‘**root**’
- Press **Enter** or click **OK** button, and then the home screen of the Web-based management shows up.

Port status

View every port status that depended on user setting and the negotiation result.

- **Port:** Displays the port number.
- **Type:** Displays the media type of the port.
- **Link:** Down is “No Link”. UP is for “Link”.
- **State:** Displays port status. Unlink will be regarded as “OFF”.

- **Negotiation:** Displays the Auto Negotiation mode. Config column means that its value was configured by the user. Actual means the current value of the port.
- **Speed Duplex:** Displays port connection speed. Config column means that its value was configured by the user. Actual means the current value of the port.
- **Flow Control:** Displays the Flow Control status in full mode. Config column means that its value was configured by the user. Actual means the current value of the port.
- **Back Pressure:** Displays the Back Pressure status. Config column means that its value was configured by the user. Actual means the current value of the port.
- **Bandwidth:** Displays the in and out bandwidth of each port.
- **Priority:** Displays the port static priority status.
- **Security:** Displays the port security status.

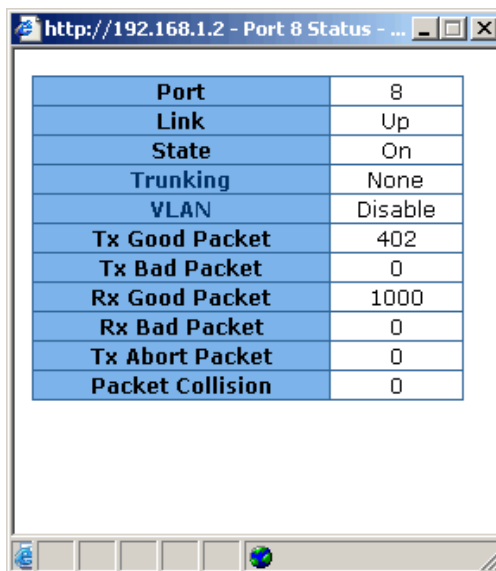
Port Status

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

Port Status interface

View the Port Information

Click the port on the switch panel figure on the web page and a port information window will show up as below:



Port	8
Link	Up
State	On
Trunking	None
VLAN	Disable
Tx Good Packet	402
Tx Bad Packet	0
Rx Good Packet	1000
Rx Bad Packet	0
Tx Abort Packet	0
Packet Collision	0

Port information interface

Port Statistics

Display the current port statistic information

- Scroll down for more ports statistics
- Click button to clean all counts

Port Statistics

Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision
Port.01	100TX	Down	Enable	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	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	Up	Enable	1535	0	11318	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
Port.16	100TX	Down	Enable	0	0	0	0	0	0
Port.17	100TX	Down	Enable	0	0	0	0	0	0
Port.18	100TX	Down	Enable	0	0	0	0	0	0
Port.19	100TX	Down	Enable	0	0	0	0	0	0
Port.20	100TX	Down	Enable	0	0	0	0	0	0
Port.21	100TX	Down	Enable	0	0	0	0	0	0
Port.22	100TX	Down	Enable	0	0	0	0	0	0
Port.23	100TX	Down	Enable	0	0	0	0	0	0
Port.24	100TX	Down	Enable	0	0	0	0	0	0
Port.25	Auto	Up	Enable	9833	0	0	0	0	0
Port.26	Auto	Up	Enable	9833	0	0	0	0	0

Port Statistics interface

Administrator

Administrator function 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, 802.1x Configuration, and System Log.**

IP Address

Configure the IP address and DHCP client function.

- **DHCP Client:** Enable or disable the DHCP client function. When DHCP client function is enabled, the switch will be assigned an IP address from the network DHCP server. Moreover, the default IP address will be replaced by the assigned IP address on DHCP server. After the user clicks **Apply** button, a popup window shows up. It is to inform the user that when the DHCP client is enabled, the current IP will lose and the user should find the new IP on the DHCP server.
- **IP Address:** Assign the switch IP address. The default IP is 192.168.1.77
- **Subnet Mask:** Assign the switch IP subnet mask
- **Gateway:** Assign the switch gateway. The default value is 192.168.1.254
- And then, click button
- Reboot the switch

IP Configuration

DHCP Client :

IP Address	192.168.1.77
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

IP configuration interface

Switch Setting

Basic

Displays the switch basic information

- **System Name:** Displays the name of the switch.
- **System Location:** Displays the switch physical location.

- **System Description:** Displays the description of the switch.
- **Firmware Version:** Displays the Firmware version of the switch.
- **Kernel Version:** Displays the Kernel Software version.
- **Hardware version:** Displays the Hardware version of the switch.
- **MAC Address:** Displays the unique hardware address assigned by manufacturer (default).
- **Module:** The module information. If the modules are not installed in the switch, this column will not be displayed.

Switch Settings



System Name	
System Location	
System Description	24-Port 10/100Mbps + 2G PoE Switch
Firmware Version	v1.02
Kernel Version	v17.06
Hardware Version	A7.00
MAC Address	001E24F21B16

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

Switch basic setting interface

Advanced

- **Enable MAC Address Aging Out:** Tick the check box to enable MAC address aging out function.
- **Age-out Time:** Key in the number of seconds that an inactive dynamic MAC address remains in the switch's address table. The valid range is from 300 ~ 765 seconds. The default value is 300 seconds.
- **Max Bridge Transmit Delay Bound:** Limit the packets queuing time in the switch. If the delay bound is set, the packets exceeding the queue time will be dropped. The valid values are 1sec, 2 sec, 4 sec, and off.

- **Enable Low Queue Delay Bound:** Limit the low priority packets queuing time in the switch. If the low priority packet stays in switch exceeding Max Delay Time, it will be sent. The valid range is from 1 ~ 255 ms.

[NOTE] Delay Bound must work under “Max bridge transit delay bound” function being in active status

- **Broadcast Storm Filter Mode:** To configure broadcast storm control, enable it and set the upper broadcast storm threshold. The threshold is the percentage of the total packet buffer used by broadcast traffic. When broadcast traffic for a port rises above the threshold you set, broadcast storm control becomes active. The valid threshold values are 5%, 10%, 15%, 20%, 25% and off.
- Click button to complete the configuration.

Switch Settings

Basic
Advanced
Misc Config

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

Max Bridge Transmit Delay Bound :

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

Broadcast Storm Filter Mode :

Priority Queue Service

802.1p Priority

First Come First Service

All High Before Low

Weight Round Ratio

Qos Policy (Checked for High Priority) :

Level0
 Level1
 Level2
 Level3
 Level4
 Level5
 Level6
 Level7

Switch Advanced setting interface

- ⊙ **Priority Queue Service settings:** Select the priority queue service type.

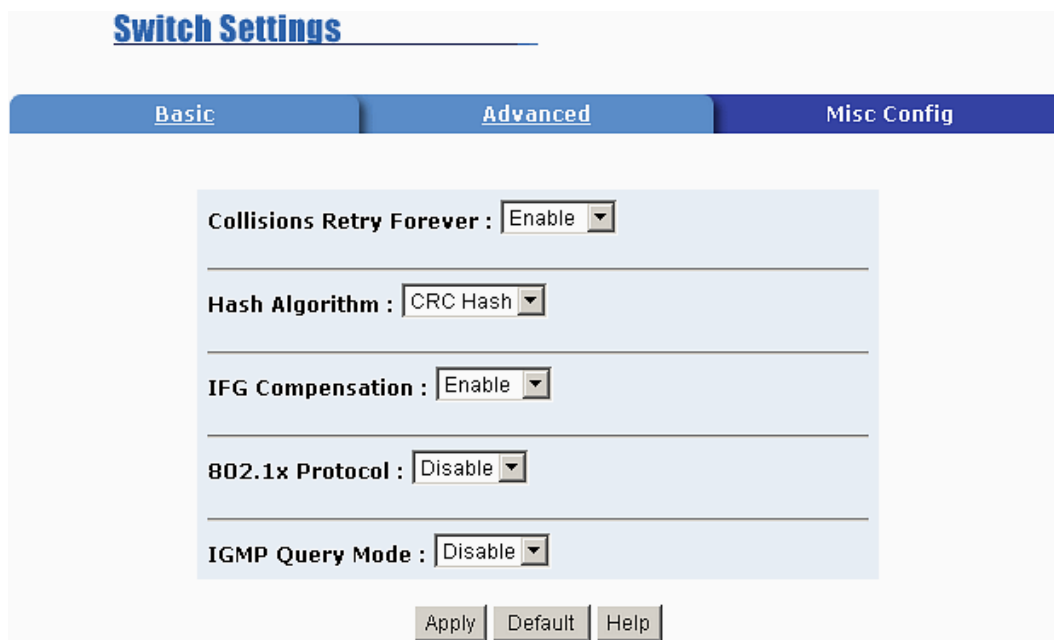
801.1p Priority

- **First Come First Service:** The sequence of packets sent depend on arriving 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 being sent. For example, 5 High: 1 Low means that the switch sends 5 high priority packets before sending 1 low priority packet.

Qos Policy (Checked for High Priority): 0 ~ 7 priority level can map onto high or low queue.

Misc Configuration

- **Collisions Retry Forever:**
 - **Disable (in half duplex):** When collisions occur, the system will retry 48 times and then drop frame.
 - **Enable (in half duplex):** When collisions occur, the system will retry forever.
- **Hash Algorithm:** CRC Hash or Direct Map for MAC address learning algorithm.
- **IFG Compensation:** Enable or disable Inter Frame Gap time compensation.
- **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:** Choose the switch that has the lowest IP address to be set as the IGMP Query mode.
 - b. **Enable Mode:** Enables the switch to be the IGMP Querier.
 - c. **Disable Mode:** Disables the query function of the switch.



Switch Misc Config setting interface

Console Port Information

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

Console port information displays 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

Change the port status

- Select the port by scroll the list in **Port** column
- **State:** Current port status. The port can be set to disable or enable mode. If the port state is set as 'Disable', it will not receive or transmit any packet.
- **Negotiation:** Auto and Force. Being set as Auto, the speed and duplex mode are negotiated automatically. When you set it as Force, you have to assign the speed and duplex mode manually.
- **Speed:** It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read only.
- **Duplex:** It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read only.
- **Flow Control:** Set flow control function as Enable or Disable. When enabled, once the device exceed the input data rate of another device as a result the receiving device will send a PAUSE frame which halts the transmission of the sender for a specified period of time. When disabled, the receiving device will drop the packet if too much to process.
- **Back Pressure:** Set Back Pressure as **ON** or **OFF** in Half Duplex mode.
- **Band Width:** All ports support port ingress and egress rate control. For example, assume the wire speed of port 1 is 100Mbps; users can set its effective egress rate as 2Mbps, ingress rate as 1Mbps. The switch will perform Flow Control or Back Pressure to confine the ingress rate to meet the specified rate.
 - **In:** Key in the port effective ingress rate. The valid range is from 0 ~ 999. 0 means rate control is disabled.
 - **Out:** Key in the port effective egress rate. The valid range is from 0 ~ 999. 0 means rate control is disabled.
- **Priority:** The static priority is based on port. If the port is set as high priority, income frames from the port always are high priority frame.
- **Security:** When the port is in security mode, the port will be "locked" without permission of address learning. Only the incoming packets with static MAC 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 function to define a list of MAC addresses that can access to secure port.

- Click **Apply** button to apply all configuration.
- The port current configuration also will be displayed when the port is selected.

Port Controls

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

Apply

Port	Type	Link	State	Negotiation		Speed Duplex		Flow Control		Back Pressure		Band Width		Priority	Security	
				Config	Actual	Config	Actual	Config	Actual	Config	Actual	In	Out			
Port.01	100TX	Down	Enable	Auto	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 4 ports into one dedicated connections. 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

- **System Priority:** A value which is used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.

- **Group ID:** There are four trunk groups to be selected. Choose the "**Group ID**" and click button.
- **LACP:** When enabled, the trunk group is using LACP. A port which joins an LACP trunk group has to make an agreement with its member ports first. When disabled, the trunk group is a static trunk group. The advantage of having the LACP disabled is that a port joins the trunk group without any handshaking with its member ports. But member ports won't know that they should be aggregated together to form a logic trunk group.
- **Work ports:** This column field allows the user to type in the total number of active port up to four. With LACP trunk group, you create a trunk group by connecting two or more switches (e.g. you assign four ports to be the members of the trunk group whose work ports column field is set as two). The exceed ports are standby (the **Aggregator Information** tab will show standby status on the exceed ports) and can be aggregated if work ports fail. If it is a static trunk group, the number of work ports must equal the total number of group member ports.
- Select the ports to join the trunk group. The system allows four ports maximum to be aggregated in a trunk group. Click button to add the port which is focused to the left field. To remove unwanted ports, select the port and click button.
- When LACP enabled, you can configure LACP Active/Passive status for each port on State Activity page.
- Click button.
- Use button to delete Trunk Group. Select the Group ID and click button.

Trunking

Aggregator Setting Aggregator information State Activity

System Priority

1

Group ID	Trunk.1	Select
Lacp	Disable	
Work Ports	3	
Port.01 Port.02 Port.03	<<Add Remove>>	Port.07 Port.08 Port.09 Port.10 Port.11 Port.12 Port.13 Port.14 Port.15

Apply Delete Help

Trunking—Aggregator Setting interface

Aggregator Information

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

- **Group Key:** Displays the trunk group ID.
- **Port Member:** Displays the members of this static trunk group.

Trunking

Aggregator Setting Aggregator information State Activity

Static Trunking Group	
Group Key	2
Port Member	1-4 1-5 1-6

Trunking—Aggregator Information interface

Aggregator State Activity

Having set up the LACP aggregator on the tab of Aggregator Setting, you can configure the state activity for the members of the LACP trunk group. You can tick or cancel the checkbox beside the state display. When you remove the tick mark to the port and click button, the port state activity will change to **Passive**.

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

[NOTE] 1. **A link** having either two active LACP nodes or one active node can perform dynamic LACP trunk.

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

The screenshot shows the 'Trunking' configuration page with the 'State Activity' tab selected. It displays a table with 26 rows, each representing a port. The columns are 'Port' and 'LACP State Activity'. Ports 4 and 6 are marked as 'Active' with a checked checkbox, while all other ports are marked as 'N/A'.

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

At the bottom of the interface, there are two buttons: and .

Trunking – State Activity interface

Forwarding and Filtering

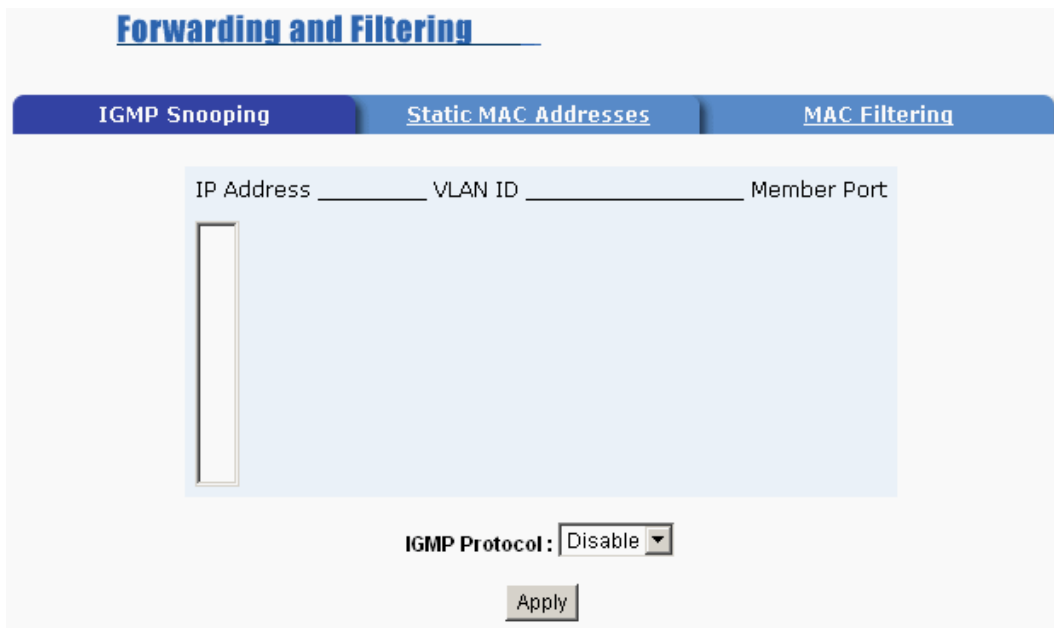
IGMP Snooping

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, report packets, and manage IP multicast traffic through the switch. IGMP have three fundamental types of message shown as follows:

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

The switch supports IP multicast. You can enable IGMP protocol via setting the IGMP Configuration page to see the IGMP snooping information. IP multicast addresses are in the range of 224.0.0.0 through 239.255.255.255.

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

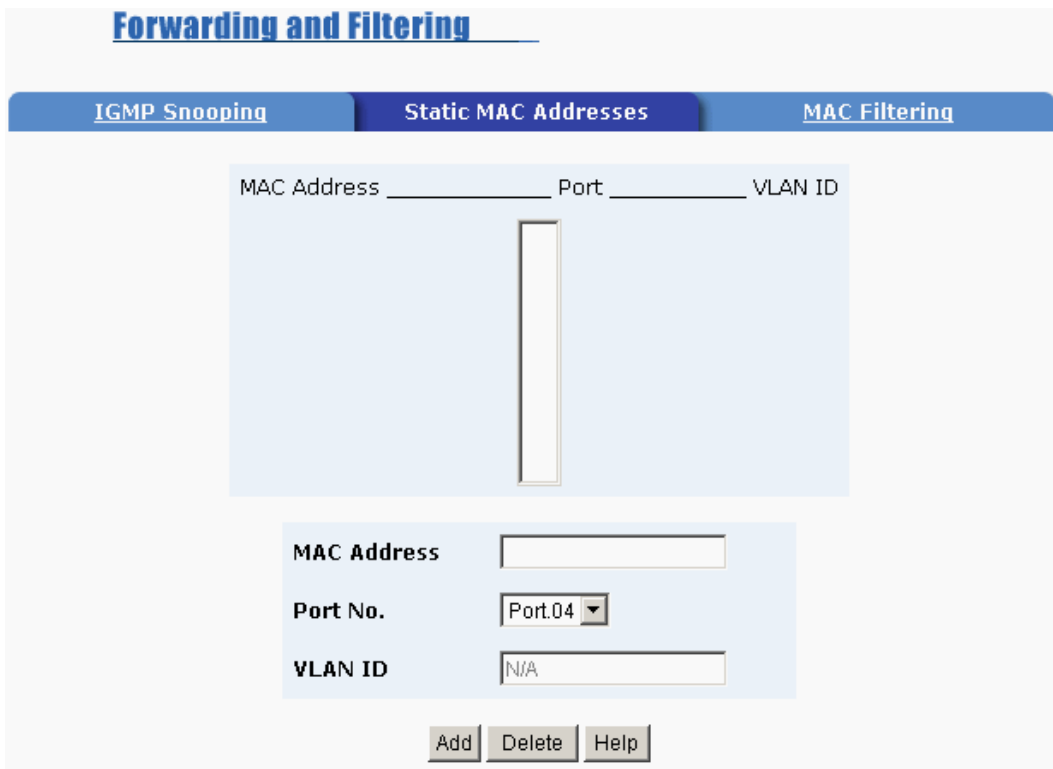


IGMP Snooping interface

Static MAC Address

When the user adds a static MAC address which will remain 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.

- **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
- **Port Number:** Select a port number.
- **VLAN ID:** If tag-based (802.1Q) VLAN are set up on the switch, key in the VID in the VLAN ID box to associate with the MAC address.
- And then, click **Add** button.
- To delete MAC address, press **Delete** button

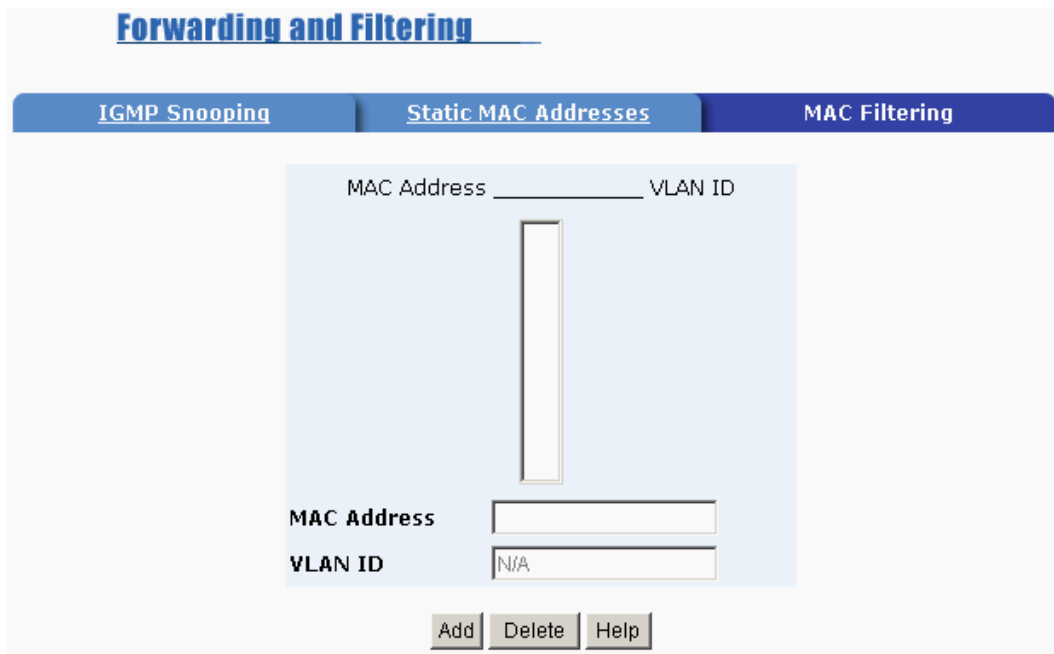


Static MAC Address interface

MAC filtering

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

- **MAC Address:** Enter the MAC address that you want to filter.
- **VLAN ID:** If tag-based (802.1Q) VLAN are set up on the switch, key in the VID in the VLAN ID field to associate with the MAC address.
- And then, click **Add** button
- To delete MAC address, press **Delete** button



MAC Filtering interface

VLAN configuration

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

The switch supports **Port-based** and **802.1Q** (tagged-based) VLAN. The default configuration of VLAN operation mode is “**Disable**”.

[NOTE] To reboot the switch when the VLAN mode is changed

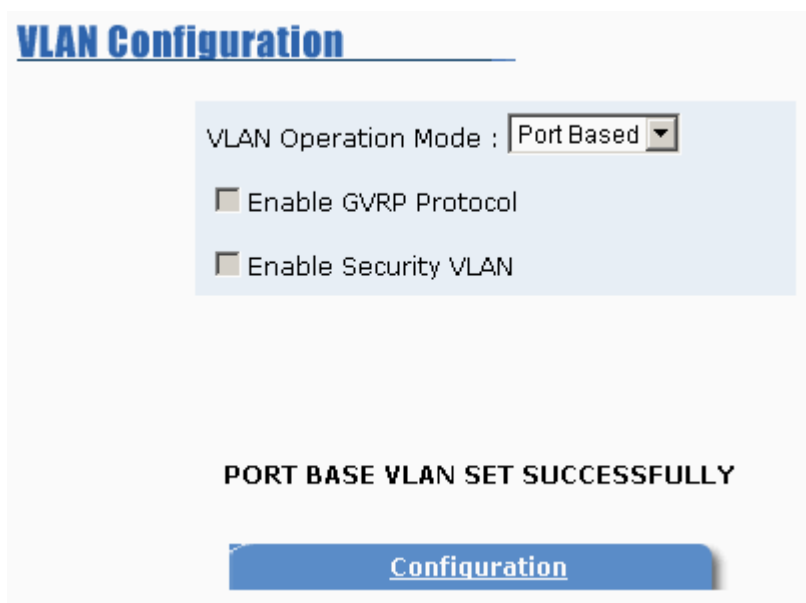
Port-based VLAN

Packets can go among only members of the same VLAN group. Note all unselected

ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

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

- Click the hyperlink “**Configuration**” to enter the VLAN configuration interface



VLAN – PortBase interface

- And then, click [Add](#) to create a new VLAN group

VLAN Configuration

VLAN Operation Mode :

Enable GVRP Protocol

Enable Security VLAN

VLAN—PortBase Add interface

- Key in the VLAN name, VLAN ID and select the members for the VLAN group.
- And then, click

VLAN Configuration

VLAN Operation Mode : Port Based

Enable GVRP Protocol

Enable Security VLAN

Group Name

VLAN ID

Port.01
Port.02
Port.03
Port.07
Port.08
Port.09
Port.10
Port.11
Port.12
Port.13
Port.14
Port.15

Add>>

<<Remove

Apply Help

- The VLAN groups will be displayed in table
- To view the VLAN groups in next page, press **Next Page** to the next page
- To delete VLAN groups, press **Delete** button
- To modify VLAN groups, click **Edit** button

[Note] If the trunk groups have been configured, the trunk groups will list in the port list (For example: Trunk1, Trunk2...). The trunk group also can be configured as the VLAN member.

802.1Q VLAN

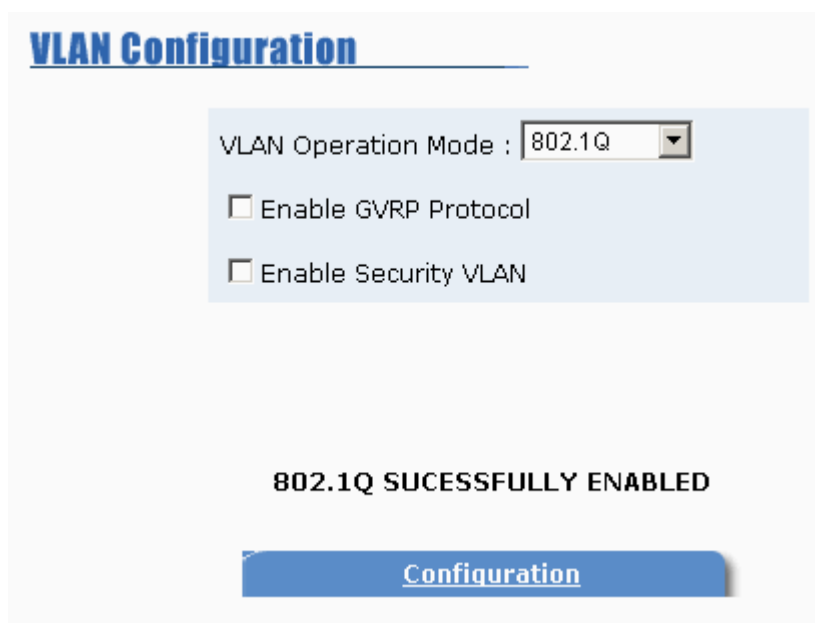
Tagged-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different switch vendors. IEEE 802.1Q VLAN uses a technique to insert a “tag” into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

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

GVRP (GARP VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices.

GVRP is based on GARP (Generic Attribute Registration Protocol), a protocol that defines procedures by which end stations and switches in a local area network (LAN) can register and de-register attributes, such as identifiers or addresses, with each other.

Every end station and switch thus has a current record of all the other end stations and switches that can be reached.



802.1q VLAN interface

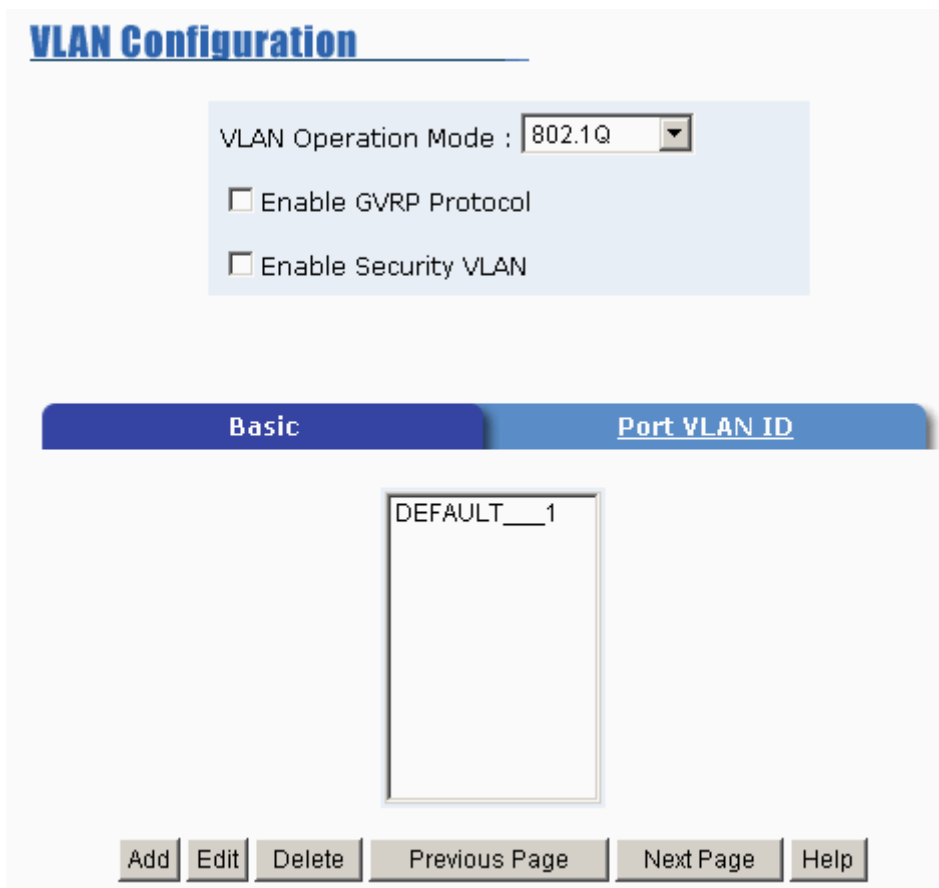
- Click the hyperlink **“Configuration”** to enter the VLAN configuration interface.
- **Enable GVRP Protocol:** Ticked the check box to enable GVRP protocol.
- **Enable security VLAN setting:** Tick the check box to enable security VLAN group. When you select to enable security VLAN group, only the members in this

VLAN group can access the switch. The steps of setting security VLAN refer to the following below steps in **Basic** section. After the security VLAN group has been configured, you can add other VLAN groups.

[Note] Only one security VLAN group is allowed.

⊙ **Basic**

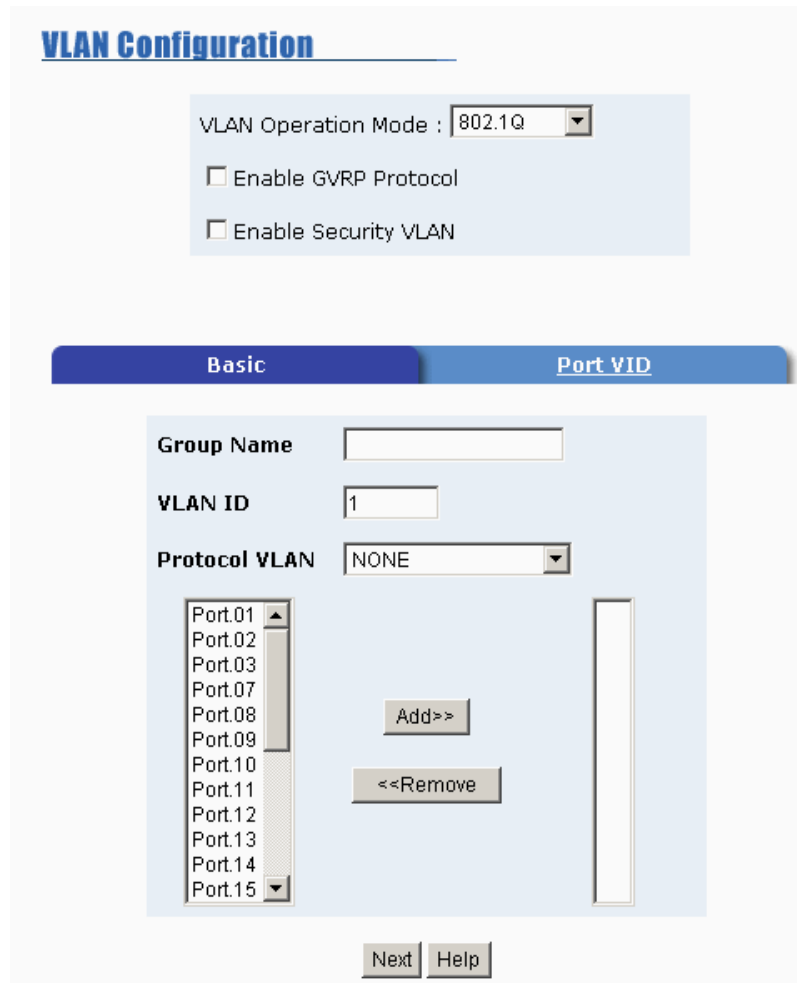
- Click **Add** button.
- **Group Name:** Assign a name for the new VLAN.
- **VLAN ID:** Key in a VLAN ID (1-4094). The default is 1.
- **Protocol VLAN:** Choose the protocol type. Default is NONE.



802.1q VLAN –Add interface

- Group the ports, and then click **Add** button. If the trunk groups have been

configured, the trunk groups will list in the port list (For example: Trunk1, Trunk2...). The trunk group also can be configured as the VLAN member.



- And then, click **Next** will see the page as below:

VLAN Configuration

VLAN Operation Mode : 802.1Q

Enable GVRP Protocol

Enable Security VLAN

VLAN Name	Vlan001		
VLAN ID	2		
UnTag Member			
Port.01	Untag	Port.02	Untag
Port.03	Untag		

Apply

- Set the outgoing frames as VLAN-Tagged frames or untagged.
 - **Tag:** The outgoing frames involve VLAN tag.
 - **Untag:** The outgoing frames don't involve VLAN tag.
- And then, click Apply button.

⊙ **Port VID:** Configure port VID.

- **VLAN ID:** Set the port VLAN ID that will be assigned to untagged traffic on a given port. This feature is useful for accommodating devices that you want them to join in the VLAN which doesn't support tagging. Each port of the switch allows the user to set one VLAN ID (the range is from 1 ~ 255 and the default VLAN ID is 1). The VLAN ID must be as same as the VLAN ID of the VLAN group that the port belongs to, or the untagged traffic will be dropped.
- **Ingress Filtering:** Ingress filtering lets frames belonging to a specific VLAN to be forwarded if the port belongs to that VLAN.
 - **Enable:** Forward only when the packets with VID match the configured VID of this port.
 - **Disable:** Disable Ingress filter function.
- **Acceptable Frame type:**

- **ALL:** Acceptable all Packet.
- **Tag Only:** Only packets with matched VLAN ID have the permission to go through the port.
- And then, click Apply button.

VLAN Configuration

VLAN Operation Mode : 802.1Q
 Enable GVRP Protocol
 Enable Security VLAN

Basic
Port VLAN ID

Port	Port VLAN ID	Ingress Filter	Acceptable Frame Type	VLAN ID Range
<div style="border: 1px solid #ccc; padding: 2px;"> Port.01 Port.02 Port.03 Port.04 </div>	1	Enable	All	1~255

Apply
Default
Help

Port	VLAN ID	Ingress Filter	Acceptable Frame Type
Port.01	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. It's recommended to enable STP on all switches to ensure only one active path on the network.

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change.

The system also supports STP and the system will auto-detect the connected device that is running STP or RSTP protocol.

System Configuration

- User can choose the RSTP mode and view Root Bridge information.
- Modifying STP state:
 - **RSTP Mode:** Set RSTP mode as 802.1d or 802.1w.
 - **Priority (0-61440):** The switch with the lowest value has the highest priority and is selected as the root. If the value is changed, the user must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.
 - **Max Age (6-40):** The number of seconds a switch waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
 - **Hello Time (1-10):** The time that controls the switch to send out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.
 - **Forward Delay Time (4-30):** The number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.
- And then, click  button.

Spanning Tree

System Configuration **Per Port Configuration**

RSTP Mode	Disabled
Priority (0-61440)	<div style="border: 1px solid black; padding: 2px;"> Disabled 802.1d 802.1w </div>
Max Age (6-40)	
Hello Time (1-10)	2
Forward Delay Time (4-30)	15

Priority must be a multiple of 4096
 $2 \times (\text{Forward Delay Time} - 1)$ should be greater than or equal to Max Age
 Max Age should be greater than or equal to $2 \times (\text{Hello Time} + 1)$

Apply

Root Bridge Information

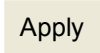
Bridge ID	0000000000000000
Root Port	Root
Root Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15

Spanning Tree – System Configuration interface

Per Port Configuration

Configure path cost and priority of every port

- Select the port in **Port** column.
- **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200,000,000.
- **Priority:** Decide which port should be blocked by priority in LAN. Enter a number 0 through 240 (the port of the highest value will be blocked). The value of priority must be the multiple of 16.
- **Admin P2P:** Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True is P2P enabling. False is P2P disabling.

- **Admin Edge:** The port directly connected to end stations won't create bridging loop in the network. To configure the port as an edge port, set the port to "**True**" status.
- **Admin Non Stp:** The port includes the STP mathematic calculation. **True** is not including STP mathematic calculation. **False** is including the STP mathematic calculation.
- And then, click  button.

Spanning Tree

System Configuration
Per Port Configuration

Port	Path Cost (1-200000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non Stp
<div style="border: 1px solid black; padding: 2px;"> Port.01 ▲ Port.02 ▾ Port.03 Port.04 Port.05 ▼ </div>	<input type="text" value="10"/>	<input type="text" value="128"/>	Auto ▼	True ▼	False ▼

priority must be a multiple of 16

RSTP Port Status

Port	Path Cost	Port Priority	Admin P2P	Admin Edge	Stp Neighbor	State	Role
Port.01	20000	128	True	True	False	Disabled	Disabled
Port.02	20000	128	True	True	False	Disabled	Disabled
Port.03	20000	128	True	True	False	Disabled	Disabled
Port.04	20000	128	True	True	False	Disabled	Disabled
Port.05	20000	128	True	True	False	Disabled	Disabled
Port.06	20000	128	True	True	False	Disabled	Disabled
Port.07	20000	128	True	True	False	Disabled	Disabled
Port.08	20000	128	True	True	False	Disabled	Disabled
Port.09	20000	128	True	True	False	Disabled	Disabled
Port.10	20000	128	True	True	False	Disabled	Disabled
Port.11	20000	128	True	True	False	Disabled	Disabled
Port.12	20000	128	True	True	False	Disabled	Disabled
Port.13	20000	128	True	True	True	Forwarding	Designated
Port.14	20000	128	True	True	False	Disabled	Disabled
Port.15	20000	128	True	True	False	Disabled	Disabled
Port.16	20000	128	True	True	False	Disabled	Disabled
Port.17	20000	128	True	True	False	Disabled	Disabled
Port.18	20000	128	True	True	False	Disabled	Disabled
Port.19	20000	128	True	True	False	Disabled	Disabled
Port.20	20000	128	True	True	False	Disabled	Disabled
Port.21	20000	128	True	True	False	Disabled	Disabled
Port.22	20000	128	True	True	False	Disabled	Disabled
Port.23	20000	128	True	True	False	Disabled	Disabled
Port.24	20000	128	True	True	False	Disabled	Disabled
Port.25	20000	128	True	True	False	Disabled	Disabled
Port.26	20000	128	True	True	False	Disabled	Disabled

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 which means traffic goes in or out monitored (source) ports will be duplicated into mirroring (analysis) port.

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

Apply Default Help

Prot Mirroring interface

- **Port Mirroring State:** Set mirroring mode—Disable, RX, TX, and Both.
- **Analysis Port:** Select one port to be the analysis port which can be used to see all monitored port traffic. User can connect mirror port to LAN analyzer or Netxray.
- **Monitor Port:** Tick the check box to monitor port traffic which will be copied to mirror (analysis) port (The maximum monitored ports are 25).

[NOTE] If you want to disable the function, you must select analysis port to none.

SNMP Management

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

Define management stations as trap managers and to enter SNMP community strings.

- ⊙ **System Options:** Assign the name, location, contact information of the switch.
- **Name:** Key in a name for the switch.
- **Location:** Key in the switch physical location.
- **Contact:** Key in the name of contact person or organization.


SNMP Management

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

- System Options:** A form with three input fields labeled "Name:", "Location:", and "Contact:". Below the fields are "Apply" and "Help" buttons.
- Community Strings:** A section with a list of "Current Strings" containing "public__RO" and "private__RW". There are "Add" and "Remove" buttons. To the right, the "New Community String:" section has a "String:" input field and radio buttons for "RO" (selected) and "RW".
- Trap Managers:** A section with a list of "Current Managers" containing "(none)". There are "Add" and "Remove" buttons. To the right, the "New Manager:" section has "IP Address:" and "Community:" input fields.


SNMP Management interface

- ⊙ **Community strings:** Serve as password.

- **Strings:** Key in the name of string.
- **RO:** Enable requests accompanied by this string to display MIB-object information (Read only).
- **RW:** Enable requests accompanied by this string to display MIB-object information and to set MIB objects (Read/Write).
- And then, click  button.


⊙ **Trap Manager**

A trap manager is a management station that receives traps. The management station then generates alerts based on the received traps. If no trap manager is defined, no traps are issued. Create a trap manager by entering the IP address of the station and a community string.

- **IP Address:** Key in IP address of the trap manager.
- **Community Strings:** Key in the community strings
- And then, click  button.

Security Manager

Change management login user name and password

- **User name:** Key in the new user name (the default is root).
- **New Password:** Key in the new password (the default is root).
- **Confirm password:** Enter the new password again.
- And then, click  button.

Security Manager

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

Security Manager interface

SNTP Configuration

Configure the SNTP (Simple Network Time Protocol) setting which SNTP allows the switch to synchronize switch clocks in the Internet. Use this page to Enable/Disable SNTP client; set SNTP server IP address, and UTC (Coordinated Universal Time) timezone.

- **SNTP Client:** Enable or disable SNTP function to get the time from the SNTP server.
- **UTC Timezone:** Enter between -12 and +13 in the UTC Timezone field. For example, 8.5 means UTC +8.5 hours.
- **Server IP:** Assign the SNTP server IP address.
- **Switch Timer:** Displays the current time of the switch.

SNTP Configuration

SNTP Client : ▼

UTC Timezone	<input type="text" value="0"/>
SNTP Server IP	<input type="text" value="192.168.16.2"/>
Switch Timer	<input type="text"/>

SNTP Configuration Interface

802.1X Configuration

When the IEEE 802.1X protocol is enabled, user can configure the parameters of 802.1X. To enable the IEEE 802.1X protocol, go to **Administrator** → **Switch Setting** → **Misc Config**

System Configuration

- **Radius Server IP:** Set the Radius Server IP address.
- **Server Port:** Set the UDP destination port for authentication requests to the specified Radius Server.
- **Accounting Port:** Set the UDP destination port for accounting requests to the specified Radius Server.
- **Shared Key:** Set an encryption key for use during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
- **NAS, Identifier:** Set the identifier for the radius client.
- And then, click button.

802.1x Configuration	
System Configuration	
Per Port Configuration	
Misc Configuration	
Radius Server IP	192.168.16.3
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

802.1x Configuration—System Configuration interface

Per port Configuration

- Select the port in **Port** column
- Select the state of port:
 - **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:** When disabled, the specified port works without complying with 802.1x protocol.
- And then, click Apply button.

802.1x Configuration

System Configuration
Per Port Configuration
Misc Configuration

Port	State
<div style="border: 1px solid black; padding: 2px;"> Port.01 ▲ Port.02 ▲ Port.03 ▲ Port.04 ▲ Port.05 ▼ </div>	<div style="border: 1px solid black; padding: 2px; display: inline-block;"> Authorize ▼ </div>

Apply
Help

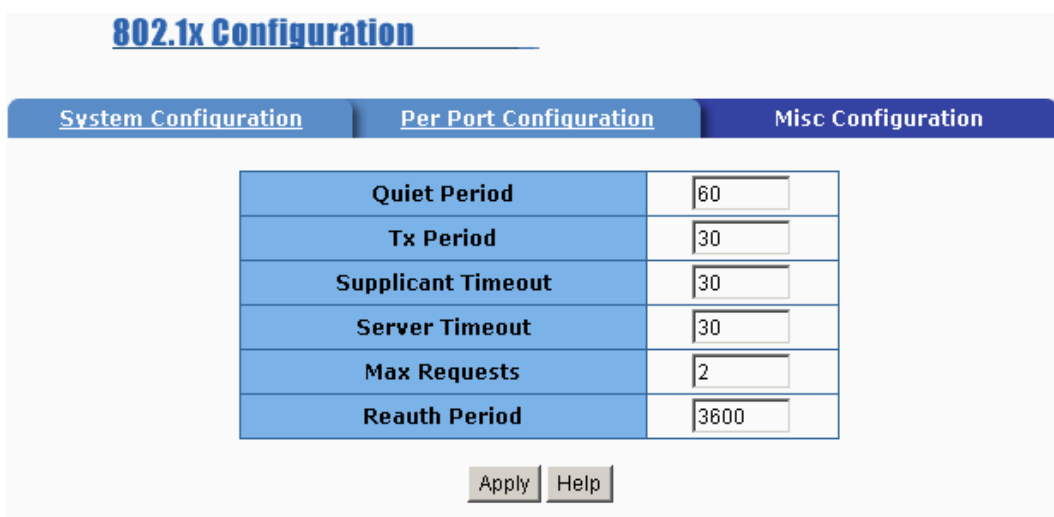
Port Authorization

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

802.1x Configuration—Per Port Configuration

Misc Configuration

- **Quiet Period:** Set the period which the port doesn't try to acquire a supplicant.
- **TX Period:** Set the period the port waits for retransmit next EAPOL PDU during an authentication session.
- **Supplicant Timeout:** Set the period of time the switch waits for a supplicant response to an EAP request.
- **Server Timeout:** Set the period of time the switch waits for a server response to an authentication request.
- **Max Requests:** Set the number of authentication that must time-out before authentication fails and the authentication session ends.
- **Reauth period:** Set the period of time which clients connected must be re-authenticated.
- And then, click



802.1x Configuration – Misc Configuration interface

System Log

Configure the system event mode to collect system log.

- **System Log Client Mode:** Select the system log mode—Client Only, Server Only, or Both.
- **System Log Server IP Address:** Assign the system log server IP.
- When Syslog Client Mode is set as Client Only, the system event log will only be reserved in the switch’s RAM until next reboot. When Syslog Client Mode is set as Server Only, the system log will only be sent to the syslog server and you have to type the IP address in the Sysylog Server IP Address column. If the Syslog Client Mode is set as Both, the system log will be reserved in the switch’s RAM and sent to server.
- Click **Reload** to refresh the events log.
- Click **Clear** to clear all current events log.
- After configuring, Click **Apply**.

System Log

System Log Client Mode	Disable ▾	Apply
System Log Server IP Address	192.168.16.2	

```
1: Jan 1 00:00:05 : Clear System Log Table!  
2: Jan 1 00:00:07 : Port.02 ---LINKUP---  
3: Jan 1 00:20:27 : Set Spanning Tree Protocol Enable!  
4: Jan 1 01:00:06 : Set Collision Retry Forever : Enable  
5: Jan 1 01:00:06 : Set Hash Algorithm : CRC Hash  
6: Jan 1 01:00:06 : Set IFG Compensation : Enable  
7: Jan 1 01:00:06 : Set 802.1x Protocol : Enable  
8: Jan 1 01:00:06 : Set IGMP Query Mode : Enable  
9: Jan 1 01:00:20 : Set IGMP Protocol: Enable!
```

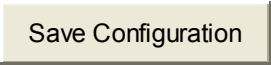
Page.1 ▾

Reload **Clear**

System Log Interface

Save Configuration

Save the configuration to the flash memory when the configurations have been changed. If users want to keep their configuration after rebooting the switch, they must save the configuration. Otherwise, the new configuration will be lost when the switch restart or power off.

- Click the  button to save the configuration to the flash memory.


Save Configuration



Save Configuration Interface

TFTP Update Firmware

Use this page (TFTP—Trivial File Transfer Protocol) to configure to update the switch's flash image bank.

- Place the updated image file on the TFTP server.
- **TFTP Server IP Address:** Key in TFTP server IP address.
- **Firmware File Name:** The name of firmware image.
- And then, click  button; the switch will download the new image file from TFTP server.

TFTP Update Firmware

TFTP Server IP Address	<input type="text" value="192.168.16.2"/>
Firmware File Name	<input type="text" value="image.bin"/>

TFTP Update Firmware interface

Configuration Backup

Restore the backup configuration from TFTP server to the switch. Also, user can backup the configuration to TFTP server.

TFTP Restore Configuration

Restore the stored configuration file from TFTP server.

- Place the stored configuration file on the TFTP server.
- **TFTP Server IP Address:** Key in the TFTP server IP address.
- **Restore File Name:** Key in the correct restore file image name.
- And then, click button.

Configuration Backup

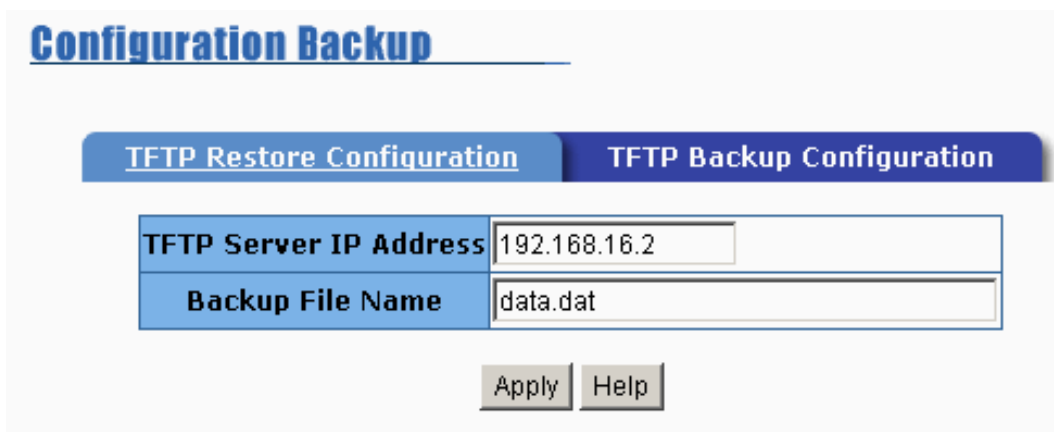
TFTP Restore Configuration	TFTP Backup Configuration
TFTP Server IP Address	<input type="text" value="192.168.16.2"/>
Restore File Name	<input type="text" value="data.dat"/>

TFTP Restore Configuration interface

TFTP Backup Configuration

Save current flash ROM value from the switch to TFTP server.

- **TFTP Server IP Address:** Key in the TFTP server IP address.
- **Backup File Name:** Key in the file image name.
- And then, click **Apply** button.



TFTP Backup Configuration interface

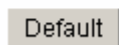
Factory Default

Reset Switch to default configuration.

- **Default IP address:** 192.168.1.77
- **Default Gateway:** 192.168.1.254
- **Subnet mask:** 255.255.255.0
- Click **Default** 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 **Reboot** button to reboot the switch.

System Reboot

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

Reboot

System Reboot interface

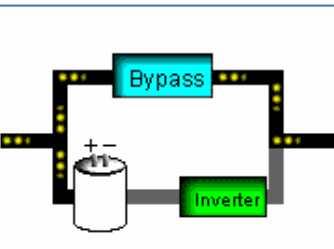
Power Status

View the connected UPS information and set command to UPS.

Power Status



com 1 Refresh

	Input Voltage	Ouput Voltage	Frequency
Now	0.0 Volt.	0.0 Volt.	0.0 Hz
Min	0 Volt.	0 Volt.	0 Hz
Max	0.0 Volt.	0.0 Volt.	0.0 Hz
	Battery Capacity	UPS Overload	Temperature
Now	0 %	0 %	0.0 C
Min	0 %	0 %	0 C
Max	0 %	0 %	0.0 C

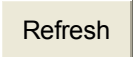


RatVoltage 0.0 Vac RatBtyVoltage 0.0 Vdc RatCurrent 0 A RatFrequency 0.0 Hz

Model Version

 UPS Disconnect	 UPS Input	 Potential Status	 Beeper Status
 UPS State	 UPS Bypass	 UPS Test	 UPS Shutdown

Power Status Interface

- **UPS information:** The information will be available when the UPS is connected to the switch and the connection is normal and UPS is powered on.
- Click  button to refresh.
 - **Input Voltage:** Displays the current value, minimum, and maximum value of UPS input voltage.
 - **Output Voltage:** Displays the current value, minimum, and maximum value of UPS output voltage.
 - **Frequency:** Display the frequency value of UPS.
 - **Battery Capacity:** Displays the battery capacity of UPS.
 - **UPS Overload:** Displays the overload capacity of UPS.
 - **Temperature:** Displays the current temperature of UPS.
 - **RatVoltage:** Displays Range of the UPS voltage.
 - **RatBtyVoltage:** Displays Range of the UPS battery voltage.
 - **RatCurrent:** Displays Range of the UPS current.
 - **RatFrequency:** Displays Range of the UPS frequency.
 - **Model:** Model name of the UPS.
 - **Version:** UPS internal software version.



The figure represents the UPS status, when the status has been detected; the figure color will change from yellow to red and the status description will change, too.

PoE Status

View PoE port information and set configuration to each port.

- Select the port and set configuration.
- And then, click **Apply** button.
- Press the **Refresh** button to refresh.

POE Status

Power Limit Management	Enable	Total Power Limit (W)	369
Firmware	2.1	Total Power (W)	0.0

Port	Enable	Bypass Detection	Power Limit By Classification	Power Limit By Management	Detect Legacy Signature	Priority	Power Limit Max (mW) (<15400)	Fault Status	Mode Status	Discovery R (ohms)	Port Current (mA)	Port Voltage (V)	Port Power (mW)	Class Current (mA)	Determined Class
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low	15400	null	Port off	0	0	47.8	0	0.0	0:15.4W
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low	15400	null	Port off	131068	0	48.0	0	0.3	0:15.4W
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low	15400	null	Port off	131068	0	47.9	0	0.3	0:15.4W
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low	15400	null	R Detect	131068	0	2.2	0	0.0	0:15.4W
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low	15400	null	R Detect	131068	0	2.1	0	0.0	0:15.4W
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low	15400	null	R Detect	131068	0	2.1	0	0.0	0:15.4W
7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low	15400	null	R Detect	131068	0	2.1	0	0.0	0:15.4W
8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low	15400	null	R Detect	131068	0	2.0	0	0.0	0:15.4W

port 1-8

port 1-8

port 9-16

port 17-24

PoE Status Interface

- **Power Limit Management:** Enable/disable the PoE power management function.
 - **Firmware:** Displays the system firmware version.
 - **Total Power Limit:** Set limit value of the total provided power to the PDs.
 - **Total Power (W):** Displays the total power of all the port that provided to PDs.
- **Port:** Select the port you want to configure.
- **Enable:** Enable or disable the port status.
 - **Bypass Detection:** Generally, this check box should not be ticked. Once this check box is ticked, the port will provide power without detecting whether the connected device is a PD or not.
 - **Power Limit by Classification:** Tick this check box to enable/disable

power classification function.

- **Power Limit by Management:** Tick this check box to enable/disable the port power limit management for PoE power management.
- **Detect Legacy Signature:** By default, the PoE switch only provides power to the connected PD which follows the IEEE 802.3af standard. Having ticked this check box, the legacy detection is to identify the PD (not in compliance with the IEEE 802.3af standard) their unique electrical signatures in order for the PoE switch can provide the power to the PD.
- **Priority:** Set port priority for the PoE power management. 1 = C (critical), 2 = H (High), 3 = L (Low).
- **Power Limit Max (mW) (<15400):** Set the power limit value. The maximum value must less 15400mW.
- **Fault Status:** The PD error status message.
 - **Null:** It means no PD is connected or the connected PD status is normal.
 - **Overload:** It means the current is over the PD current classification limited (475mA @ 48V DC) over 50ms.
- **Mode Status:** The PD current operation mode status.
 - **V sample or I sample:** It means Current sample or Voltage sample. When PD is detected and current is supplied, the PoE switch will keep detecting and sampling some current or voltage to ensure whether the PD is still active on the port. It is an IEEE 802.3af operating procedure.
 - **R detect:** When the port doesn't connect with any PD, the PoE switch will poll each port and detects the resistor.
- **Discovery R (ohms):** Displays the resistance value.
- **Port Current (mA):** Displays the current value.
- **Port Voltage (V):** Displays the voltage value.
- **Port Power (W):** Displays the watt value.
- **Class Current (mA):** Displays current class. When the Bypass classification is enabled, the class value will not show in here.
- **Determined Class:** Displays power class. When the Bypass classification is enabled, the class value will not show in here.

Troubleshooting

This section is intended to help solve the most common problems on the 24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch.

Incorrect connections

The switch port can automatically detect straight or crossover cable when the user links the switch with other Ethernet device. For the RJ-45 connector should use correct UTP or STP cable, 10/100Mbps ports use 2 pairs twisted cable. If the RJ-45 connector is not correctly pinned on right position, 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.

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

■ Improper Network Topologies

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

Diagnosing LED Indicators

To assist in identifying problems, the switch can be easily monitored through panel indicators, which describe common problems the user may encounter and where the user can find possible solutions.

If the power indicator does turn on when the power cord is plugged in, the user 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 the problem still cannot be solved, please contact the local dealer for assistance.

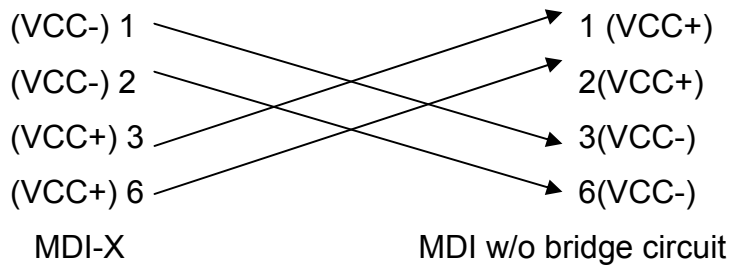
Diagnosing PoE problems

■ No Power Forward

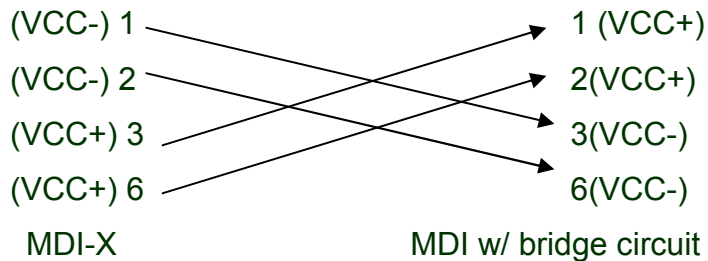
- Make sure the connected PD device complies with IEEE 802.3af standard. The PoE switch only supports the IEEE 802.3af compliant PD.
- The PoE switch uses the signal power pair to forward power, the data and the power traverse the pin. Please check the documentation for your PD device to make sure the power pair it uses. The following table is the signal power pair RJ-45 port pin out:

Pin	Signal / Name
1	RX+ / VCC -
2	RX- / VCC -
3	TX+ / VCC +
4	NC
5	NC
6	TX- / VCC +
7	NC
8	NC

- When the PD device pin out is in MDI mode without bridge circuit function, please use the crossover cable for power and data transmission. Please refer to the above table for the pin out transform.



- When the PD device is in MDI mode with bridge circuit function, the straight forward and crossover cable both workable for power and data transmit. Please refer to the above table for the pin out antithesis.



OR



Technical Specification

This section provides the specifications of the 24 10/100TX plus 2 Mini-GBIC/Copper managed PoE switch.

Standard	<p>IEEE802.3 10BASE-T</p> <p>IEEE802.3u 100BASE-TX</p> <p>IEEE802.3z Gigabit Fiber</p> <p>IEEE802.3ab Gigabit 1000BASE-T</p> <p>IEEE802.3x Flow Control and Back pressure</p> <p>IEEE802.3ad Port trunk with LACP</p> <p>IEEE802.1d Spanning tree protocol</p> <p>IEEE802.1w Rapid spanning tree protocol</p> <p>IEEE802.1p Class of service</p> <p>IEEE802.1Q VLAN Tagging</p> <p>IEEE 802.1x user authentication</p> <p>IEEE802.3af Power over Ethernet</p>
LED Indicators	<p>System Power</p> <p>10/100TX RJ-45 Port: Link/Active (Green), Full-duplex (Orange)</p> <p>Mini-GBIC/ Copper: Link/Activity (Green: 1000Mbps/ Orange: 10/100Mbps), Full duplex/collision (Orange)</p>
Connector	<p>10/100TX: 24 x RJ-45</p> <p>Gigabit Copper: 2 x RJ-45</p> <p>2 Mini-GBIC for Mini-GBIC transceiver</p>

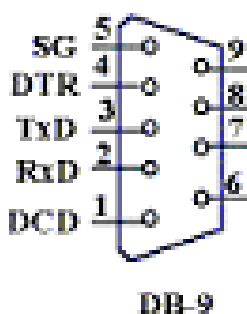
RS-232 connector	One RS-232 DB-9 female connector for switch management 2 RS-232 DB-9 male connectors on rear side for DC power supply and UPS management
Switch architecture	Store and forward switch architecture.
Back-plane	Up to 8.8Gbps
MAC address	8K MAC address table with Auto learning function
Memory	3Mbits for packet buffer
Flash ROM	512Kbytes x 2
System memory	8Mbytes x 1
Dimensions	440mm(W) x 280mm(D) x 44mm(H)
Operating environment	0°C ~ 40°C, 10% ~ 95% RH
Storage Temp.	-40°C ~ 70°C (-40°F ~ 158°F), 95% RH
Remote power feeding	End-point insert type and compatible with IEEE802.3af Per port feeding power: 15.4Watts (maximum)
Power	Embedded AC power supply: AC 100 ~ 240V, 50/60Hz, 200W Extra power input: DC48V
Power consumption	20W (maximum without PD)

Ventilation	2 DC Fans with detection
EMI	FCC Class A, CE
Safety	UL, cUL, CE/EN60950

Appendix

Console Port Pin Assignments

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



DB-9 Console Port Pin Numbers

■ DB-9 Port Pin Assignments

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

■ Console Port to 9-Pin DTE Port on PC

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

Cables

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

■ Cable Types and Specifications

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP/STP 100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm	UTP/STP 100 m (328 ft)	RJ-45
1000BASE-T	Cat. 5e, 6 100-ohm	UTP/STP 100 m (328 ft)	RJ-45

Cable specification table

100BASE-TX/10BASE-T Pin Assignments

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

■ RJ-45 Pin Assignments

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

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

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

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

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

The PoE switch has the auto-detected Giga port—Gigabit Mini-GBIC/Copper combo ports. The Gigabit Copper (10/100/1000T) ports should use Category 5e or above UTP/STP cable for the connection up to 1000Mbps. The small form-factor pluggable (SFP) is a compact optical transceiver used in optical communications for both telecommunication and data communications. They are for connecting to the network segment with single or multi-mode fiber. You can choose the appropriate SFP module to plug into the slots. Then use proper multi-mode or single-mode fiber according to the used SFP module. With fiber optic, it transmits at speed up to 1000 Mbps and you can prevent noise interference from the system; the transmission distance depending on the mini-GBIC module is up to 110 km.