



INSTALLATION AND OPERATION MANUAL

CWGE24MODMS

MODULAR 24 PORT MANAGED SWITCH

V2.02 – October 2010

The ComNet™ CWGE24MODMS Managed Ethernet Switch Chassis provides transmission of twenty-four (24) Ethernet Ports with the use of three eight port expansion modules. This Ethernet switch is easily configurable by selecting, sold separately, eight port modules that allow for all copper, optical with four copper and four SFP modules, or all optical with SFP modules making the CWGE24MODMS switch available for use with either conventional CAT-5e copper or optical transmission media. The 24 electrical ports support the 10/100/1000 Mbps Ethernet IEEE 802.3 protocol, and auto-negotiating and auto-MDI/MDIX features are provided for simplicity and ease of installation. These network managed layer 2 switches are optically (1000 BASE-FX) and electrically compatible with any IEEE 802.3 compliant Ethernet devices. Plug-and-play design ensures ease of installation, and no electrical or optical adjustments are ever required. The CWGE24MODMS incorporates LED indicators for monitoring the operating status of the managed switch and network. The CWGE24MODMS and its corresponding modules are designed for installation in benign (0° – +45° C) operating environments.

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 and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

CE Mark Warning

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

Content

Chapter 1 Introduction	1
1.1 Hardware Features.....	2
1.2 Software Feature.....	3
1.3 Package Contents.....	5
Chapter 2 Hardware Description	6
2.1 Physical Dimension.....	6
2.2 Rear Panel.....	7
Chapter 3 Hardware Installation	8
3.1 Desktop Installation	8
3.2 Rack-mounted Installation	9
3.3 Power On	9
Chapter 4 Module Hardware Description.....	10
4.1 Package Contents.....	10
4.2 Module Features	11
4.3 Module Hardware Description	12
4.3.1 Module LED Indicators.....	12
4.3.2 Port Description.....	14
4.4 Installing Module in CWGE24MODMS Switch Chassis.....	14
4.5 Module Troubleshooting	15
Chapter 5 Network Application	16
5.1 Desktop Application.....	17
5.2 Segment Application.....	17
Chapter 6 Console Management	18
6.1 Connecting to the Console Port	18
6.2 Login in the Console Interface	18
6.3 CLI Management.....	19
Chapter 7 Web-Based Management.....	20
7.1 About Web-based Management.....	20
7.2 Preparing for Web Management.....	20
7.3 System Login	21
7.4 System	22

7.4.1 System Information.....	22
7.4.2 Switch Information.....	23
7.4.2.1 Main Board	23
7.4.2.2 Management Software	23
7.4.3 IP Configuration	24
7.4.4 DHCP Configuration	25
7.4.5 Firmware Update	27
7.4.5.1 TFTP Download Firmware	27
7.4.5.2 TFTP Backup Configuration	27
7.4.5.3 TFTP Restore Configuration	28
7.4.6 System Event Log.....	29
7.4.6.1 LOG Configuration.....	29
7.4.6.2 Logging Events Level	31
7.4.6.3 Logging RAM Table	32
7.4.6.4 Logging Flash Table	32
7.4.7 Security Manager.....	33
7.5 Port	34
7.5.1 Port Statistics	34
7.5.2 Port Information	35
7.5.3 Port Control	35
7.5.4 Port Trunk	37
7.5.4.1 Trunk Configuration.....	37
7.5.4.2 Trunk Information	38
7.5.4.3 Port Activity	39
7.5.5 Port Mirror.....	39
7.5.6 Rate Limiting.....	41
7.6 Protocol.....	42
7.6.1 VLAN	42
7.6.1.1 VLAN Mode Configuration.....	42
7.6.1.2 Port VLAN Id Configuration	43

7.6.1.3 VLAN Entry	44
7.6.2 Rapid Spanning Tree	45
7.6.2.1 STP System Configuration	45
7.6.2.2 STP Port Configuration.....	47
7.6.3 SNMP.....	48
7.6.4 QoS.....	51
7.6.4.1 QoS Configuration	51
7.6.4.2 Port-bace Configuration	51
7.6.4.3 COS Configuration	52
7.6.4.4 DSCP Configuration	53
7.6.5 SNTP.....	54
7.6.6 IGMP	56
7.6.6.1 IGMP Configuration	56
7.6.6.2 IGMP Static Configuration.....	57
7.6.7 LLDP	58
7.6.7.1 LLDP Configuration	58
7.6.7.2 LLDP Neighbor Table	59
7.7 Security	60
7.7.1 802.1x/ RADIUS	60
7.7.1.1Misc Configuration	60
7.7.1.2Port Configuration	61
7.7.1.3Radius Client Configuration.....	62
7.7.2 Port Security	63
7.7.2.1 Static MAC Address Table	63
7.7.2.2 Filter MAC Address Table.....	64
7.7.2.3 MAC Address Table Aging	66
7.7.2.4 Dynamic MAC Address Table	66
7.7.3 IP Security.....	67
7.7.4 ACL	68
7.8 Factory Default.....	69

7.9 Save Configuration	69
7.10 System Reboot	70
Troubleshooting.....	71
Appendix A- Command Sets	73
Commands Set List	73
System Commands Set	74
Port Commands Set	76
Mac / Filter Table Commands Set	79
Port Mirroring Commands Set	81
TFTP Commands Set.....	81
QOS Commands Set	82
Spanning Tree Commands Set.....	83
VLAN Commands Set	85
System log Commands Set	88
SNTP Commands Set.....	91
IGMP Commands Set	92
TRUNK Commands Set	93
SNMP Commands Set.....	95
DHCP Server Commands Set.....	96
Security IP Commands Set.....	96
802.1X Commands Set.....	97
LLDP Commands Set	98
ACL Commands Set	99

Chapter 1 Introduction

The CWGE24MODMS Managed Switch is a modular switch that can be used to build high-performance switched workgroup networks. This switch is a store-and-forward device that offers low latency for high-speed networking. The switch is targeted to workgroup, department or backbone computing environments.

The CWGE24MODMS Managed Switch features a store-and-forward switching scheme. This allows the switch to auto-learn and store source addresses in a 16K-entry MAC address table.

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

The CWGE24MODMS Managed Switch has three module slots which provide flexibility on network application. Users can purchase the modules in accordance with their needs.

1.1 Hardware Features

Standards	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3z Gigabit fiber IEEE 802.3ab 1000Base-T IEEE 802.3x Flow control and Back pressure IEEE 802.3ad Port trunk with LACP IEEE 802.1d Spanning tree protocol IEEE 802.1w Rapid spanning tree IEEE 802.1p Class of service IEEE 802.1q VLAN Tagging IEEE 802.1x User authentication IEEE 802.1ab LLDP
LED Indicators	System Power 10/100/1000TX module: Link/Activity, 1000/100/10Mbps speed 8 Port Gigabit Fiber module: Link/Activity 8 Port SFP: Link/Activity 4 Port Gigabit copper + 4 Port SFP module: RJ45 (Link/Activity, 1000/100/10Mbps speed), SFP (Link/Activity)
Connector	RS232 console: Female DB-9 Gigabit copper module: 8 x RJ45 SFP module: 8 x SFP socket Gigabit Fiber module: 8 x SC for Gigabit SX or LX 4 Gigabit Copper & 4 SFP module: 4 x RJ45 + 4 x 3.3v SFP Socket
Switch architecture	Store and forward switch architecture with Back-plane up to 48Gbps.
Packet buffer	6Mbits
Dimensions	440mm(W) x 280mm(D) x 44mm(H)
MAC Address	16K
Storage Temp.	-40°~70°C, 5%~95%RH
Operational Temp.	0°~45°C, 5%~95%RH
Power Supply	AC 100~240V 50/60Hz, Redundant Power: DC 12~48V
Power Consumption	35 Watts
Ventilation	2 fan at the rear
EMI	Compliance with FCC Class A, CE
Safety	Compliance with UL, cUL, CE/EN60950-1

1.2 Software Feature

Management	SNMP v1/v2c, Telnet, RMON1, CLI and Web management.
MIB	RFC 2863 Interface Group MIB, RFC 1213 MIBII, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC 1643 Ethernet Like MIB, RFC 1215 Trap MIB, RFC 1757 RMON MIB, Private MIB
SNMP Trap	Cold start/Warm start trap, Link down/Link up trap, Authentication fail trap,
Firmware Upgrade	TFTP
Configuration upload and download	System quick installation and backup by TFTP
Port Trunk	Support IEEE802.3ad with LACP function. Up to 7 trunk groups with failover feature and the member up to 8 ports.
Spanning Tree	IEEE802.1w Rapid spanning tree (Compatible with STP)
VLAN	Port based VLAN, up to 24 groups IEEE802.1Q Tag VLAN Static VLAN groups up to 256 entries and dynamic VLAN groups up to 2048, the VLAN ID can be assigned from 1 to 4094. GVRP*
Class of Service	Per port 8 priority queues and support strict and WRR priority rule. Weight round ratio (WRR):1:2:3:4:5:6:7:8 Weight round ratio (WRR):1:1:2:2:3:3:4:4 Weight round ratio (WRR):1:1:2:2:4:4:8:8
Quality of service	Port based, Tag based, IPv4 Type of service, IPv4 Different service.
IGMP	IGMP v1, v2 Supports 256 multicast groups and IGMP query
Port Security	Support 128 entries of MAC address for static MAC and another 128 for MAC filter

Port Mirror	Supports 3 mirroring types: “RX”, “TX” and “Both” packet.
Bandwidth Control	Per port support ingress rate limiting and egress rate shaping control.
Access security	IP Management Security: Support IP addresses security to prevent unauthorized intruder.
802.1x Authentication	Support IEEE802.1x User-Authentication and can report to RADIUS server. <ul style="list-style-type: none"> ● Reject ● Accept ● Authorize ● Disable
Access Control List	The system provides control list on Source IP & Destination IP.
DHCP	DHCP Client and DHCP Server
DNS	Provide DNS client feature and support Primary and Secondary DNS server.
System log	1000 records (Maximum) Provide remote storage ability and also can view the log by Web/Telnet/SNMP interface.
SNTP	Support RFC 2030 SNTP client.
SMTP	System supports 5 mail accounts and 2 Mail servers for Primary and Secondary. The SMTP will auto send event message to supervisor whom is pre-defined in the SMTP system through the pre-defined mail server.
Packet filter	Broadcast storm control
LLDP	Support IEEE 802.1ab Link Layer Discovery Protocol

*Future release

1.3 Package Contents

Unpack the contents of the CWGE24MODMS Managed Switch and verify them against the checklist below:

- CWGE24MODMS Managed Switch Chassis
- Four Rubber Feet
- Power Cord
- Rack-mounted kit
- RS232 Cable
- User Guide

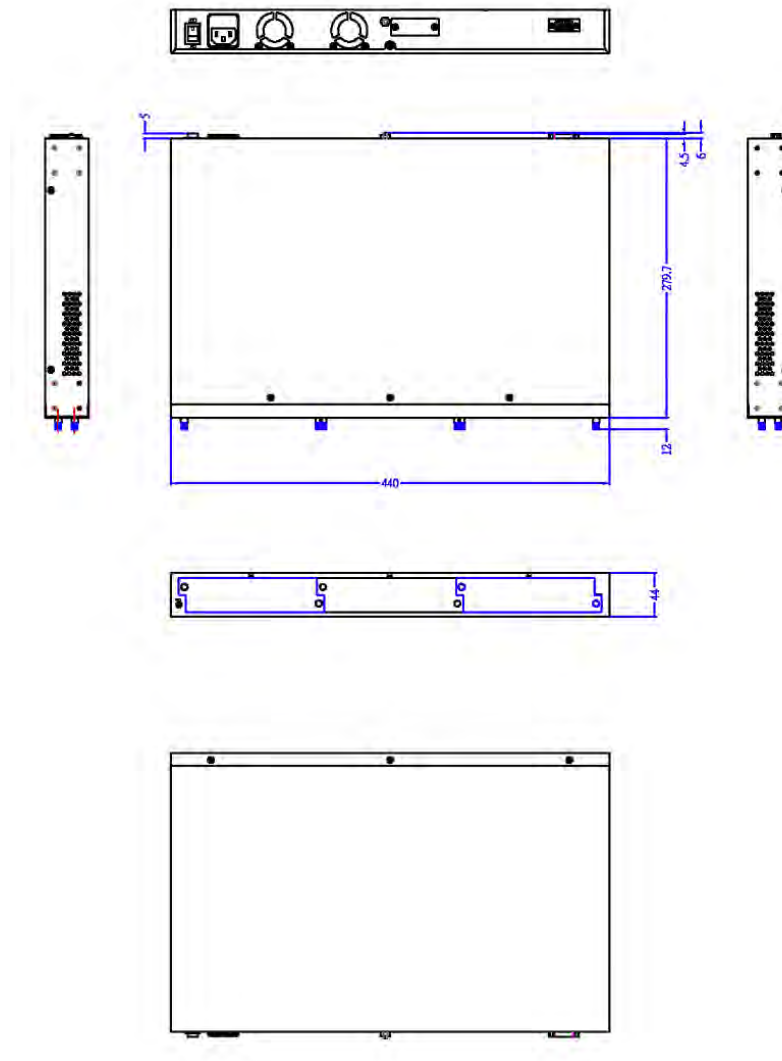
Compare the contents of your CWGE24MODMS Managed Switch package with the standard checklist above. If any item is missing or damaged, please contact your local dealer.

Chapter 2 Hardware Description

This section describes the hardware of the CWGE24MODMS Managed Switch.

2.1 Physical Dimension

The physical dimensions of the CWGE24MODMS Managed Switch are 440mm(W) x 280mm(D) x 44mm(H)



2.2 Rear Panel

The 3-pronged power plug is located at the Rear Panel of the CWGE24MODMS Managed Switch as shown in figure below. The switches will work with AC in the range 100-240V AC, 50-60Hz. The DC redundant power jack is optional.



Rear Panel of the CWGE24MODMS Managed Switch

Chapter 3 Hardware Installation

3.1 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 air circulation.

Attaching Rubber Feet

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

3.2 Rack-mounted Installation

The switch comes 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, provided there is proper ventilation.

Perform the following steps to rack mount the switch:

- A. Position one bracket to align with the holes on one side of the switch and secure it with the smaller bracket screws. Then attach the remaining bracket to the other side of the switch.
- B. After attaching both mounting brackets, position the switch in the rack by lining up the holes in the brackets with the appropriate holes on the rack. Secure the switch to the rack with a screwdriver and the rack-mounting screws.

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

3.3 Power On

Connect the power cord to the power socket at the rear panel of the switch. The other end of the power cord connects to the power outlet. The internal power can work with AC in the voltage range of 100-240VAC/ frequency 50~60Hz or 12-48VDC (optional). The AC and DC input can be used for redundant power supply. When one fails, the other is able to continue providing power to the switch. Check the power LED indicator on the front panel to see if power is properly supplied.

Chapter 4 Module Hardware Description

4.1 Package Contents

Unpack the contents of the **module package** and verify them against the checklist below:

- Module (your selection of the following):

CWGE24MODMS/8TX

CWGE24MODMS/8FXSCM1

CWGE24MODMS/8FXSCS1

CWGE24MODMS/8FXSFP

CWGE24MODMS/8TX4SFP4

- User Guide

If any item is damaged or missing, please contact your local dealer or provider.

4.2 Module Features

- Gigabit copper: complies with IEEE802.3 10Base-T, IEEE 802.3u 100Base-TX, IEEE802.3ab 1000Base-T
- Gigabit fiber: complies with IEEE802.3z Gigabit fiber (SX or LX)
- Connector: Gigabit copper (RJ45), Gigabit SX (SC, Multimode Fiber), Gigabit LX (SC, Single Mode Fiber)
- LED: Gigabit Fiber (Link/Activity), Gigabit Copper (Link/Activity, 100/1000)
- Connect Distance:
 - Gigabit Copper: 100 meters
 - Gigabit SX: 500 meters/ Multimode Fiber 50/125um or 62.5/125um
 - Gigabit LX: 10 km / Single Mode Fiber 8 /125um or 9/125 um

4.3 Module Hardware Description

4.3.1 Module LED Indicators

The LED Indicators gives real-time information of systematic operation status. The LED indicators are located on each module. The LED indicators will be different depending on which module is installed in the CWGE24MODMS Chassis. The following tables provide descriptions of the LED status and their meaning for each module:

CWGE24MODMS/8TX Module

LED	Status	Meaning
100/1000	Green	Link on 1000Mbps speed mode
	Amber	Link on 100Mbps speed mode
	Off	Link on 10Mbps speed mode / No device attached
LK/ACT	Green	Ethernet Link connected
	Blink	The port is receiving or transmitting data.
	Off	No device attached / Link is disconnected

CWGE24MODMS/8FXSC(M,S)1 Module

LED	Status	Meaning
LK/ACT	Green	Link is connected
	Blink	The port is receiving or transmitting data.
	Off	No device attached / Link is disconnected

CWGE24MODMS/8TX4SFP4 Module

LED	Status	Meaning
Gigabit Copper		
1000/100	Green	Link on 1000Mbps mode
	Amber	Link on 100Mbps speed mode
	Off	Link on 10Mbps speed mode / No device attached
LK/ACT	Green	Ethernet Link is connected
	Blink	The port is receiving or transmitting data.
	Off	No device attached / Link is disconnected
SFP		
LK/ACT	Green	Link is connected
	Blink	The port is receiving or transmitting data.
	Off	No device attached / Link is disconnected

CWGE24MODMS/8FXSFP Module

LED	Status	Meaning
LNK/ACT	Green	Link connected
	Blink	The port is receiving or transmitting data.
	Off	No device attached / Link is disconnected

4.3.2 Port Description

- **UTP:** The UTP port will auto-sense connections, it can auto detect crossover or straight cable when plugged into a connector. The Gigabit connection requires use of Cat-6 or Cat5e 4 pairs twisted cable with correct pin alignment. If using cat-5 cable, only 100Mbps link speed is supported. The available link distance is up to 100 meters.
- **SC:** supports Gigabit SX or Gigabit LX for different link distance. (Please see Fiber Transceiver label on the Module)
- **SX:** uses Multimode fiber cable (62.5/125um ~ 50/125um), distance < 500 meters.
- **LX:** uses Single mode fiber cable (8/125um ~ 9/125um), distance < 10 km.
- **SFP:** Hot swappable, allowing you to install different fiber transceiver while the switch is running. The slot only supports 3.3 VDC; therefore, **please confirm the transceiver's power voltage is same as module.**

4.4 Installing Module in CWGE24MODMS Switch Chassis

- A. Remove the module slot cover from the chassis switch.
- B. Install the module by inserting it into the guides and sliding it in until it stops. Press it firmly.
- C. Gently push the thumbscrews in and turn clockwise to tighten. Do not over tighten the thumbscrews.

4.5 Module Troubleshooting

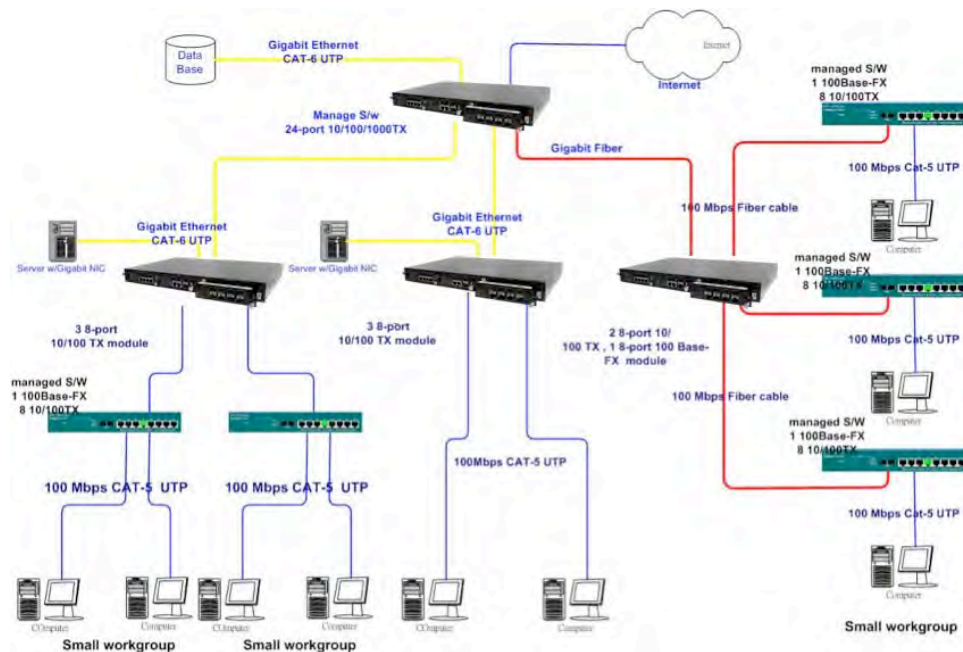
- Select the proper UTP cable for 1000Base-T (Gigabit 1000T) module.
- Select the proper Fiber cable to construct your network. The Fiber TX and RX port should be connect to partner's right fiber port. Example: TX connects to partner's Fiber RX connector and RX should to partner's TX connector.

Chapter 5 Network Application

This section provides you a few samples of network topology in which the switch can be used. In general, the CWGE24MODMS Managed Switch is designed as a segment switch. That is, with its large address table (16K MAC address) and high performance, it is ideal for interconnecting networking segments.

PC, workstations, and servers can communicate with each other by directly connecting with CWGE24MODMS Managed Switch. The switch automatically learns node addresses, which are subsequently used to filter and forward all traffic based on the destination address.

By using Gigabit or Gigabit Fiber, the switch can connect with another switch or hub to interconnect other small-switched workgroups to form a larger switched network. Meanwhile, you can also use Ethernet or Gigabit fiber ports to connect switches. The following figure is an example of the CWGE24MODMS Managed Switch application topology.



The example of application topology

5.1 Desktop Application

The CWGE24MODMS Managed Switch is an ideal solution for small workgroups. The switch can be used as a standalone switch to which personal computers, server, printer server are directly connected to form a small workgroup.

5.2 Segment Application

For enterprise networks where large data broadcast are constantly processed this switch is suitable for a department user to connect to the corporate backbone.

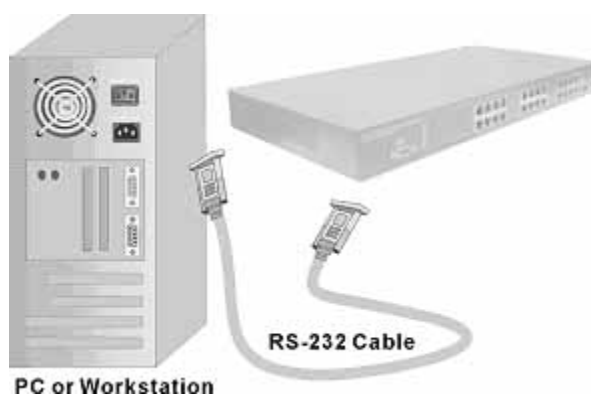
You can use the CWGE24MODMS Managed Switch to connect PCs, workstations, and servers to each other. All the devices in this network can communicate with each other by connecting directly to the switch. Connecting servers to the backbone switch allow other users to access the server's data.

The switch automatically learns node addresses, which are subsequently used to filter and forward all traffic based on the destination address. You can use any of the RJ45 ports of the CWGE24MODMS Managed Switch to connect with another switch or hub to interconnect each of your small-switched workgroups to form a larger switched network.

Chapter 6 Console Management

6.1 Connecting to the Console Port

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 RS232 cable with a male DB-9 connector to connect a terminal or PC to the Console port.



Connecting the switch to a terminal via RS-232 cable

6.2 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:

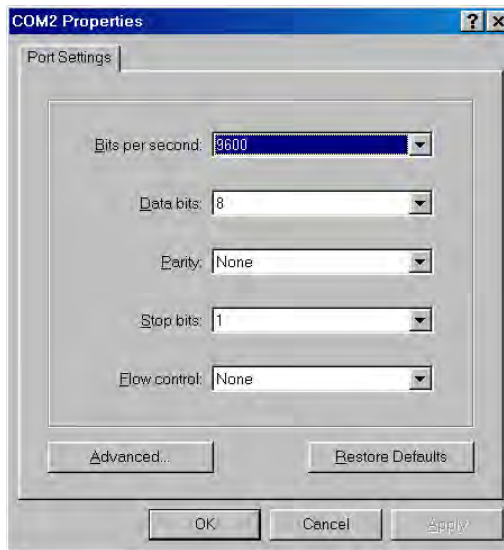
Baud Rate: 9600 bps

Data Bits: 8

Parity: none

Stop Bit: 1

Flow control: None

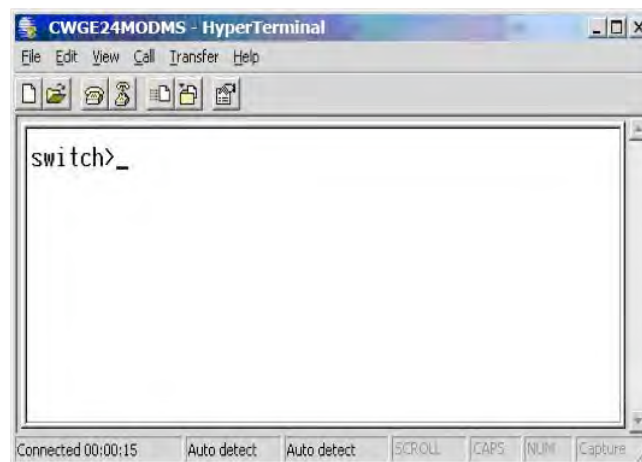


The settings of communication parameters

After finishing the parameter settings, click “**OK**”. When the blank screen shows up, press **Enter** key to get into command line mode. Please see below figure for login screen.

6.3 CLI Management

The system supports console management (CLI command). After you login to the system, you will see a command prompt. To enter CLI management interface, enter “**enable**” or “**e**” command.



CLI command interface

Chapter 7 Web-Based Management

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

7.1 About Web-based Management

On 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 5.0 or later. And, it is applied for Java Applets for reducing network bandwidth consumption, enhance access speed and present an easy viewing screen.

[NOTE] By default, IE5.0 or later version does not allow Java Applets to activate sockets. The user has to explicitly modify the browser setting to enable Java Applets to operate network ports.

7.2 Preparing for Web Management

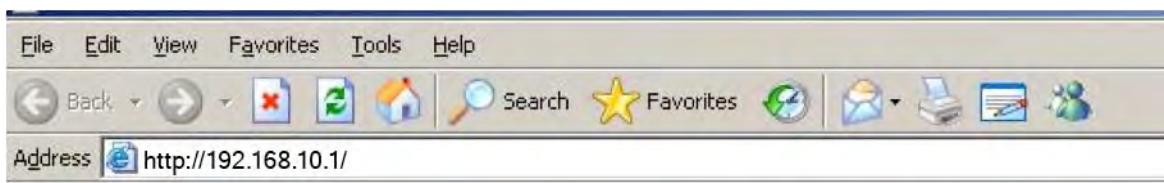
Before using web management, install the industrial switch on the network and make sure that any one of PC on the network can connect with the industrial switch through the web browser. The switch default value of IP, subnet mask, username and password is as below:

- IP Address: **192.168.10.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.10.254**

- User Name: **admin**
- Password: **admin**

7.3 System Login

1. Launch a browser, such as Microsoft Internet Explorer, via the PC
2. Key in “http:// +” the IP address of the switch”, and then Press “**Enter**”.



3. The login screen will appear right after
4. Key in the user name and password. The default user name and password are the same as “**admin**”
5. Press “**Enter**” or “**OK**”, and then the home screen of the Web-based management appears as below:



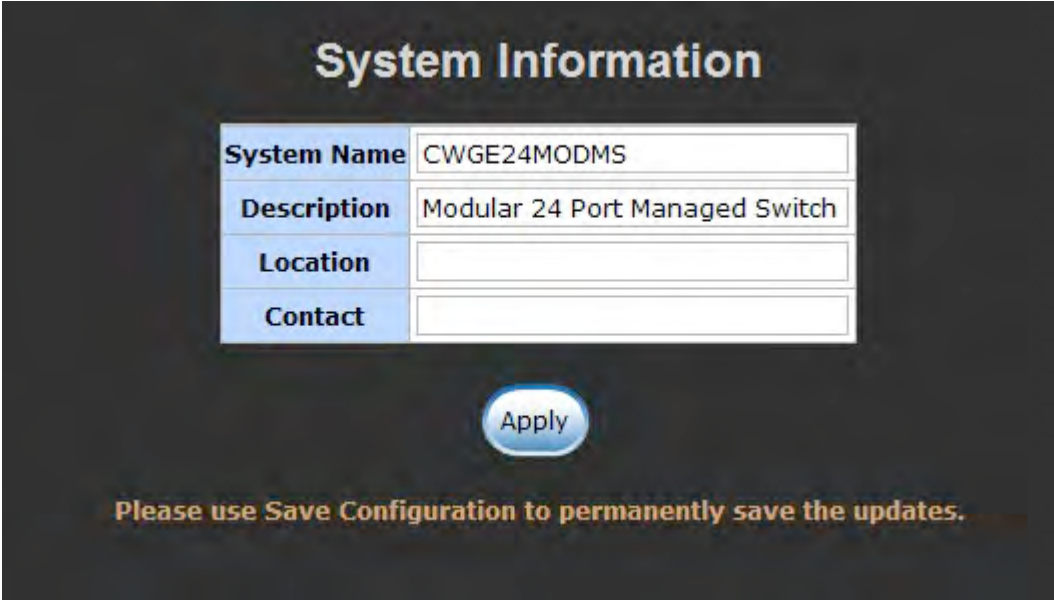
Login screen

7.4 System

7.4.1 System Information

Assigning the system name, location and view the system information

- **System Name:** Assign the name of switch. The maximum length is 31 bytes
- **Description:** Display the description of switch. The maximum length is 31 bytes
- **Location:** Assign the switch physical location. The maximum length is 31 bytes
- **Contact:** Enter the name of contact person or organization
- **Object ID:** The most common OIDs seen "in the wild" usually belong to the private enterprise numbers allocated by IANA under the 1.3.6.1.4.1 (iso.org.dod.internet.private.enterprise) arc. In computer networking, an **OID**, in the context of the Simple Network Management Protocol (SNMP), consists of the object identifier for an object in a Management Information Base (MIB).



The image shows a web-based configuration interface titled "System Information". It features a table with four rows: "System Name", "Description", "Location", and "Contact". Each row has a corresponding text input field. The "System Name" field contains the text "CWGE24MODMS", and the "Description" field contains "Modular 24 Port Managed Switch". Below the table is a blue "Apply" button. At the bottom of the interface, there is a message: "Please use Save Configuration to permanently save the updates."

System Name	Description	Location	Contact
CWGE24MODMS	Modular 24 Port Managed Switch		

Apply

Please use Save Configuration to permanently save the updates.

System information interface

7.4.2 Switch Information

7.4.2.1 Main Board

- **Hardware Version:** display the hardware version
- **Fan 1 Status:** display the status of Fan 1
- **Fan 2 Status:** display the status of Fan 2

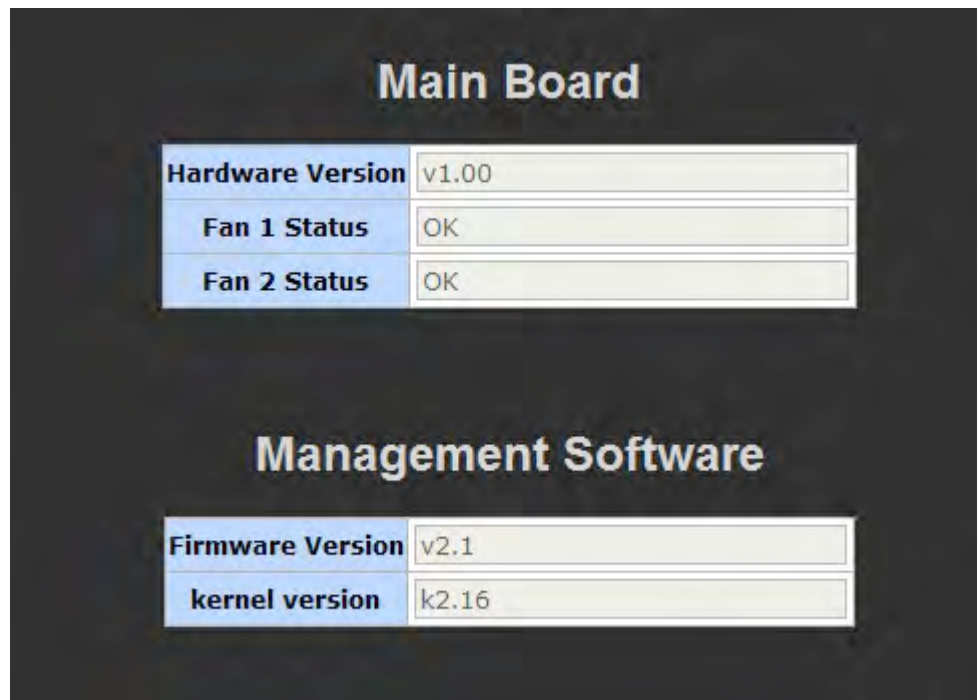
7.4.2.2 Management Software

Firmware Version: display the firmware version

Configure Data version: display the configure data version

Command Line Version: display the command line version

Web UI Version: display the Web UI version



The screenshot displays a web interface for switch information. It is divided into two main sections: 'Main Board' and 'Management Software'. The 'Main Board' section contains three rows: 'Hardware Version' with value 'v1.00', 'Fan 1 Status' with value 'OK', and 'Fan 2 Status' with value 'OK'. The 'Management Software' section contains two rows: 'Firmware Version' with value 'v2.1' and 'kernel version' with value 'k2.16'. Each row has a label on the left and a value in a text box on the right.

Main Board	
Hardware Version	v1.00
Fan 1 Status	OK
Fan 2 Status	OK

Management Software	
Firmware Version	v2.1
kernel version	k2.16

Switch information interface


7.4.3 IP Configuration

User can configure the IP Settings.

- **IP Address Mode:**

Static: IP address of this switch will be assigned by user.

DHCP: IP address of this switch will be assigned by the network DHCP server.

- **IP Address:** Assign the IP address that the network is using. If **IP Address Mode** function is set in DHCP mode, user needn't assign the IP address manually. The network DHCP server will assign the IP address that is going to be displayed in this column for the switch. The default IP is 192.168.10.1
- **Subnet Mask:** Assign the subnet mask of the IP address. If **IP Address Mode** function is in DHCP mode, user need not assign the subnet mask manually.
- **Gateway IP Address:** Assign the network gateway for the switch. The default gateway is 192.168.10.254
- **DNS1:** Assign the IP address of DNS server1 that the network is using.
- **DNS2:** Assign the IP address of DNS server2 that the network is using.
- **MAC Address:** Display the unique hardware address assigned by manufacturer (default)
- And then, click 

IP Configuration

IP Address Mode	STATIC ▾
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.254
DNS1	0.0.0.0
DNS2	0.0.0.0
MAC Address	00223b03097c

Apply
Help

Please use Save Configuration to permanently save the updates.


IP configuration interface

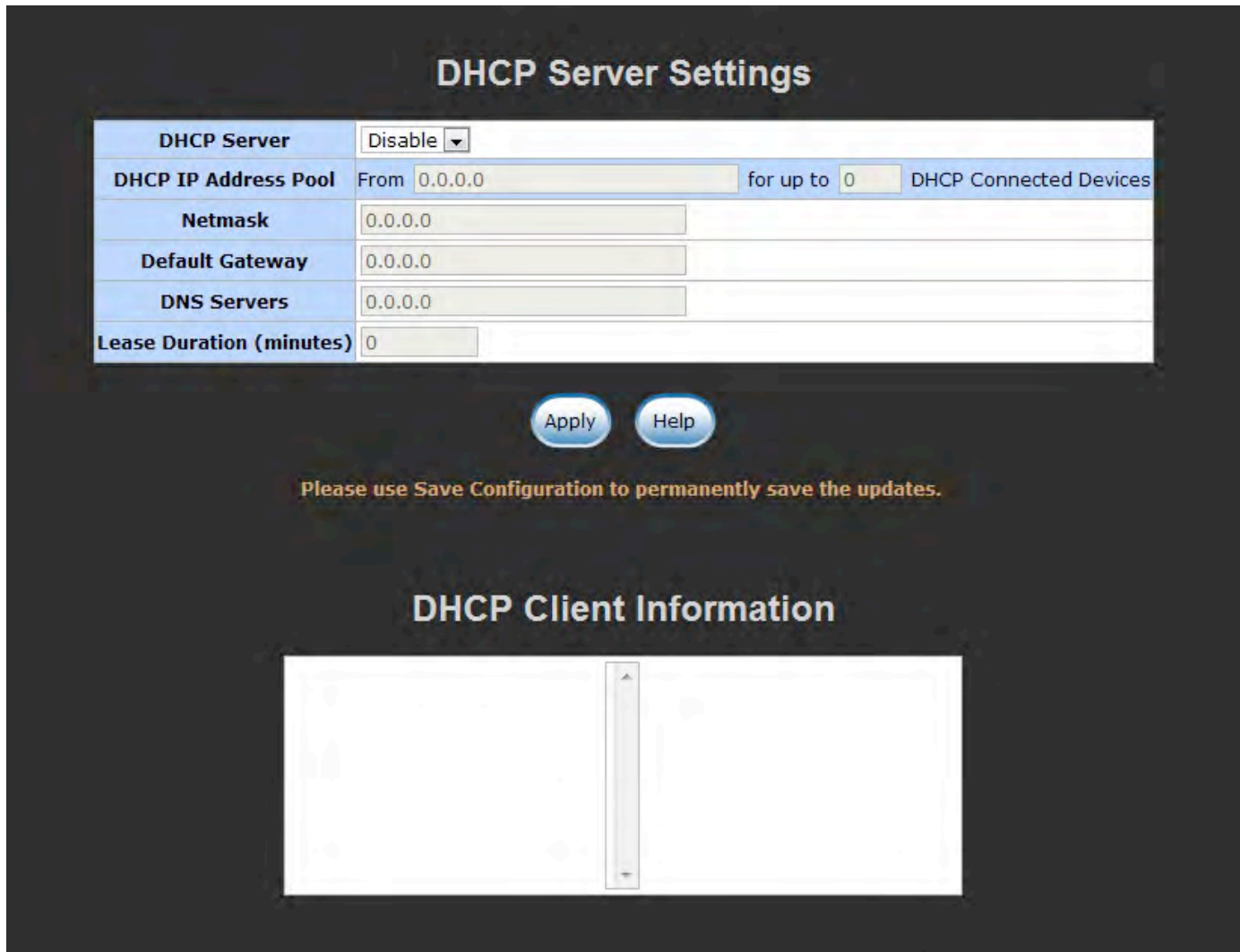
7.4.4 DHCP Configuration

The system provides the DHCP server function. By enabling the DHCP server function, the switch system will be a DHCP server.

■ DHCP Server Settings

1. **DHCP Server:** Enable or disable the DHCP Server function. Enable – the switch will be a DHCP server on your local network.
2. **DHCP IP Address Pool:** User has to set a range of IP addresses for the DHCP server assigning an IP address to the DHCP client by giving the starting IP address and how many IP addresses within this address pool. For instance, user can set 192.168.1.100 to be the beginning IP address and 50 (can't be greater than 253) to be the maximum number. The range of the address pool should be from 192.168.1.100 to 192.168.1.49.
3. **Netmask:** the dynamic IP assign range subnet mask.
4. **Default Gateway:** the gateway in your network.

5. **DNS Servers:** Domain Name Server IP Address in your network.
6. **Lease Duration (hours):** Assign the lease duration time in hours
7. And then, click 



The image shows a network configuration interface with two main sections. The top section, titled "DHCP Server Settings", contains a table with the following fields: "DHCP Server" (a dropdown menu set to "Disable"), "DHCP IP Address Pool" (a range from "0.0.0.0" to "0" for up to "0" DHCP Connected Devices), "Netmask" (0.0.0.0), "Default Gateway" (0.0.0.0), "DNS Servers" (0.0.0.0), and "Lease Duration (minutes)" (0). Below this table are "Apply" and "Help" buttons. A message below the buttons reads: "Please use Save Configuration to permanently save the updates." The bottom section, titled "DHCP Client Information", contains a large, empty rectangular box with a vertical scrollbar on the right side.

DHCP Server Settings	
DHCP Server	Disable ▼
DHCP IP Address Pool	From 0.0.0.0 for up to 0 DHCP Connected Devices
Netmask	0.0.0.0
Default Gateway	0.0.0.0
DNS Servers	0.0.0.0
Lease Duration (minutes)	0

Apply Help

Please use Save Configuration to permanently save the updates.

DHCP Client Information

DHCP Server Configuration interface


■ DHCP Client Information

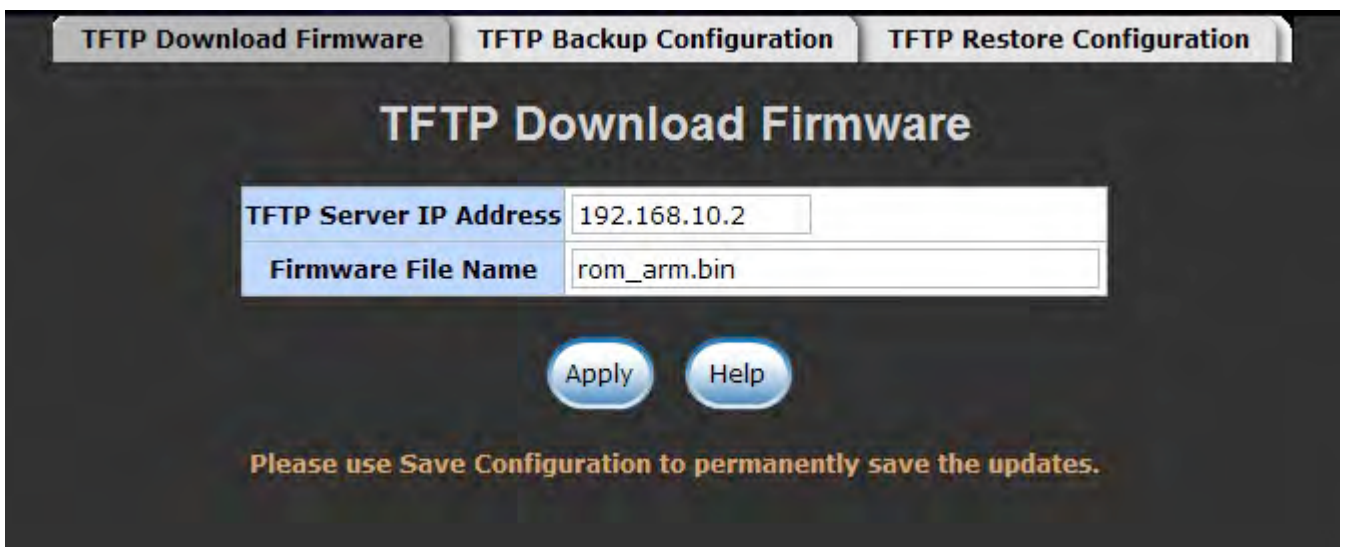
Display the DHCP Client information that has gotten an IP address from the DHCP server.

7.4.5 Firmware Update

7.4.5.1 TFTP Download Firmware

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


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



TFTP-Update Firmware interface

7.4.5.2 TFTP Backup Configuration


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

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

TFTP-Configuration Backup interface

7.4.5.3 TFTP Restore Configuration

User can restore EEPROM value from TFTP server, but user must put back the backup file in TFTP server, switch will download it back.

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

TFTP-Configuration Restore interface

7.4.6 System Event Log

7.4.6.1 LOG Configuration

You can mark the check box of Local Logging, Remote Logging, and SMTP Logging to enable the functions of LOG Configuration.

- **Local Logging:** Mark this check box for enabling to set Flash Level and RAM Level. Set Flash Level to send event log to flash ROM or RAM by assigning the level.
 - **Flash Level:** Set the level range of 0 to 7.
 - **RAM Level:** Set the level range of 0 to 7.
- **Remote Logging:** Mark this check box for enabling to set Facility Level, Trap Level, Log Server IP 1, and Log Server IP 2.
 - **Facility Level:** Set the level range of 16 to 23.
 - **Trap Level:** Set the level range of 0 to 7.
 - **Log Server IP 1:** Assign a remote log server IP address.
 - **Log Server IP 2:** Assign a remote log server IP address.

Log Configuration

Logging Events Level

Logging Ram Table

Logging Flash Table

Log Configuration

☒ Local Logging

Flash Level:

Level 3

 RAM Level:

Level 7

☐ Remote Logging

Facility Level:

23

 Trap Level:

Level 7

Log Server IP 1:

Log Server IP 2:

☐ SMTP Logging

Trap Level:

Level 7

Mail Server:

From Address:

☐ Authentication

To Address 1:

To Address 2:

To Address 3:

To Address 4:

To Address 5:

Mail Server:

From Address:

☐ Authentication

To Address 1:

To Address 2:

To Address 3:

To Address 4:

To Address 5:

Apply


Help

Please use Save Configuration to permanently save the updates.

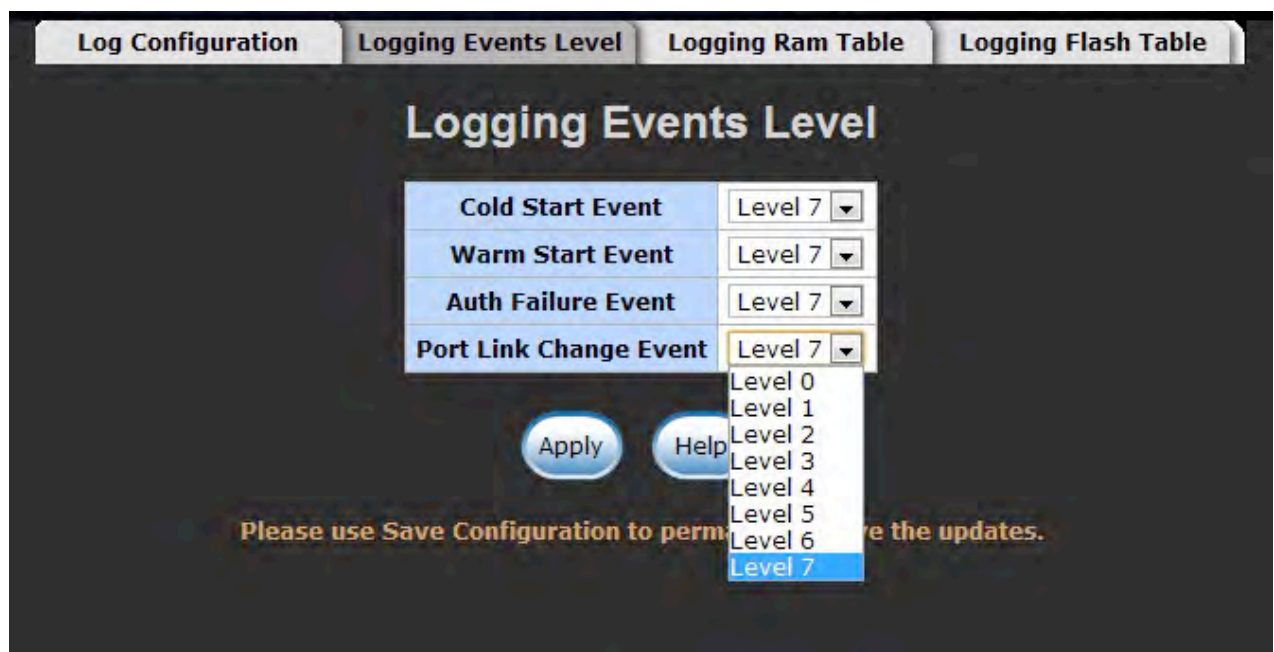
LOG Configuration interface

7.4.6.2 Logging Events Level

User can select the system log events and SMTP events. When selected events occur, the system will send out the log information. The range of Logging Event Level is from level 0 to level 7. When the level value is the same as the one among Local Logging, Remote Logging, and SMTP Logging, the system will issue a log record to location where user has designated.

After configuring, click .

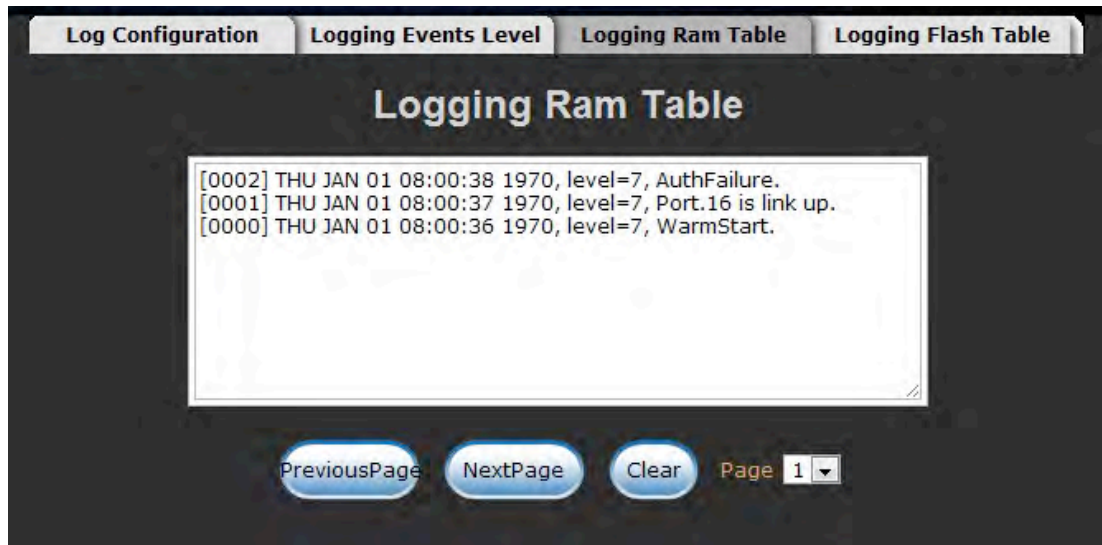
- **Logging Event Level:** 4 events – Cold Start Event, Warm Start Event, Auth Failure Event, and Port Link Change Event. Pull down the right side item menu to select the event level. When selected events occur, the system will issue the logs.
 - **Cold Start Event:** when the device executes cold start action, the system will issue a log event.
 - **Warm Start Event:** when the device executes warm start, the system will issue a log event.
 - **Auth Failure Event:** You get this trap if a network management system (NMS) polls the device with the wrong community string.
 - **Port Link Change Event:** when the port link has changed, the system will issue a log event.



Logging Events Level interface

7.4.6.3 Logging RAM Table

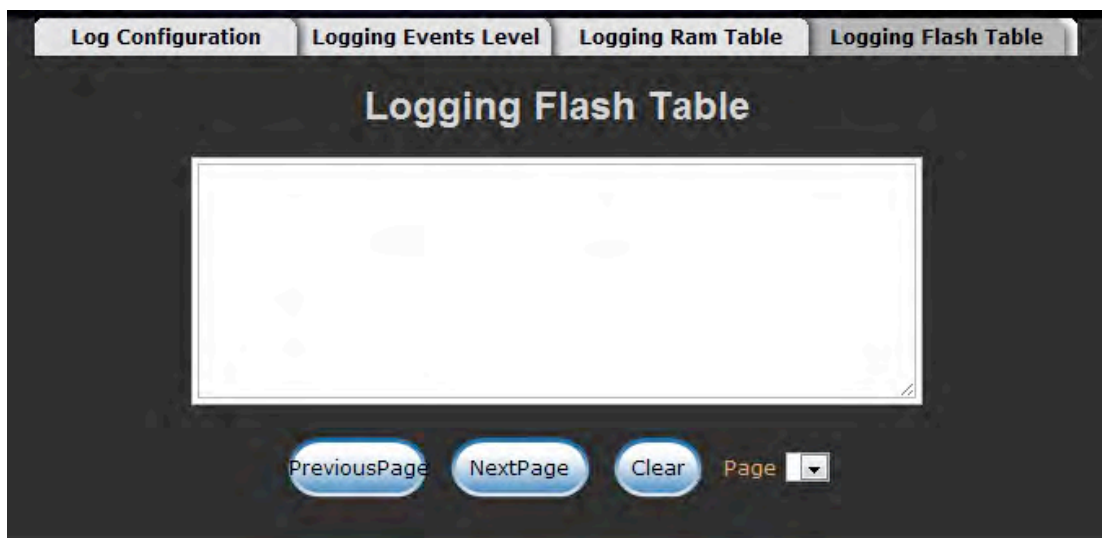
Logging RAM Table displays the logs that have been sent to RAM.



Logging RAM Table interface.

7.4.6.4 Logging Flash Table


Logging Flash Table displays the logs that have been sent to Flash ROM.

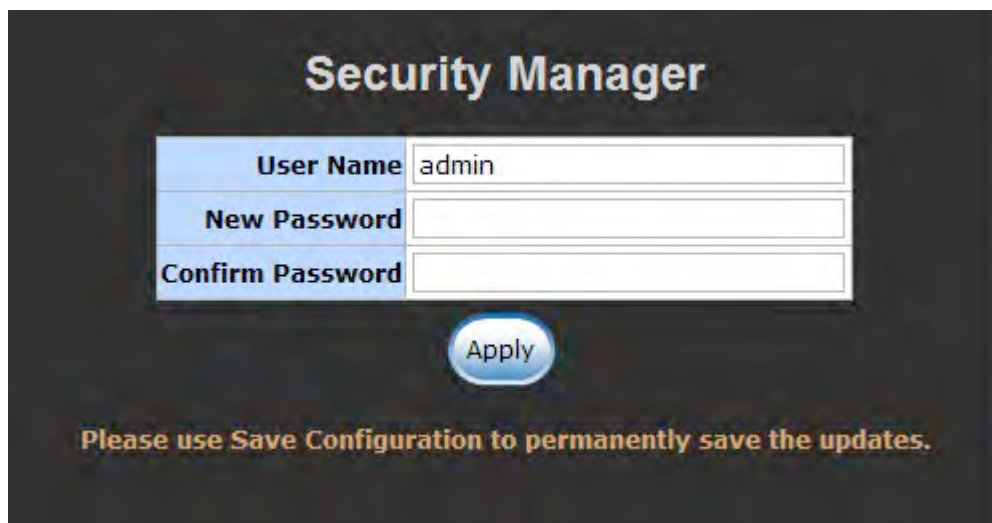


Logging ROM Table interface

7.4.7 Security Manager

Change login user name and password for the management security issue

- **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:** Re-type the new password
- And then, click 



The screenshot shows the 'Security Manager' interface. It has a dark background with the title 'Security Manager' in a large, bold, yellow font at the top. Below the title is a form with three rows. The first row is labeled 'User Name' in a blue box, with a text input field containing 'admin'. The second row is labeled 'New Password' in a blue box, with an empty text input field. The third row is labeled 'Confirm Password' in a blue box, with an empty text input field. Below the form is a blue, oval-shaped button with the word 'Apply' in white. At the bottom of the interface, there is a line of text in yellow: 'Please use Save Configuration to permanently save the updates.'

Security Manager Interface

7.5 Port

7.5.1 Port Statistics

Display the port statistic information.

Interface Statistic

Interface		Port.16 ▾	
goodOctetsRcv	720918	badOctetsRcv	0
macTransmitErr	0	goodPktsRcv	3990
badPktsRcv	0	brdcPktsRcv	3720
mcPktsRcv	2122	pkts64Octets	1125
pkts65to127Octets	1518	pkts128to255Octets	1000
pkts256to511Octets	966	pkts512to1023Octets	165
pkts1024tomaxOctets	555	goodOctetsSent	969444
goodPktsSent	1339	excessiveCollisions	0
mcPktsSent	0	brdcPktsSent	0
unrecogMacCntrRcv	0	fcSent	0
goodFcRcv	0	dropEvents	0
undersizePkts	0	fragmentsPkts	0
oversizePkts	0	jabberPkts	0
macRcvError	0	badCrc	0
collisions	0	lateCollisions	0
badFcRcv	0		0

ClearHelp

Port Statistic interface

7.5.2 Port Information

The following information provides the current port statistic information


Port Information												
Port	Type	Link	State	Auto Negotiation		Speed		Duplex		Flow Control		Jumbo
				Config	Actual	Config	Actual	Config	Actual	Config	Actual	
Port.01	MINI_GBIC	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.02	MINI_GBIC	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.03	MINI_GBIC	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.04	MINI_GBIC	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.05	MINI_GBIC	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.06	MINI_GBIC	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.07	MINI_GBIC	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.08	MINI_GBIC	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.09	GIGA_COPPER	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.10	GIGA_COPPER	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.11	GIGA_COPPER	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.12	GIGA_COPPER	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.13	GIGA_COPPER	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.14	GIGA_COPPER	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.15	GIGA_COPPER	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.16	GIGA_COPPER	Up	Enable	Enable	Enable	1000	100	full	full	Enable	Enable	1522
Port.17	GIGA_COPPER	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.18	GIGA_COPPER	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.19	GIGA_COPPER	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.20	GIGA_COPPER	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.21	MINI_GBIC	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.22	MINI_GBIC	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.23	MINI_GBIC	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522
Port.24	MINI_GBIC	Down	Enable	Enable	N/A	1000	N/A	full	N/A	Enable	N/A	1522

Port Information interface

7.5.3 Port Control



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

1. **Port:** select the port that user wants to configure.
2. **State:** Current port status. The port can be set to disable or enable mode. If the port setting is disabled, it will not receive or transmit any packet.

3. **Auto Negotiation:** enable or disable auto negotiation
4. **Speed:** when Auto Negotiation is disabled, user can select the port link speed.
5. **Duplex:** set full-duplex or half-duplex mode of the port.
6. **Flow Control:** set flow control function is Enable or Disable. The default value is Enabled.
7. **Jumbo:** Assign the Jumbo frame size. The maximum is 10K bytes.
8. Click .

Port Configuration

Port	State	Auto Negotiation	Speed	Duplex	Flow Control	Jumbo
Port.13 ▲						
Port.14 ☰	Enable ▼	Enable ▼	1G ▼	Full ▼	Disable ▼	1522
Port.15 ▼						
Port.16 ▼						

Please use Save Configuration to permanently save the updates.

Port Information




Port	Type	Link	State	Auto Negotiation		Speed		Duplex		Flow Control		Jumbo
				Config	Actual	Config	Actual	Config	Actual	Config	Actual	
Port.16	GIGA_COPPER	Up	Enable	Enable	Enable	1000	100	full	full	Enable	Enable	1522

Port Configuration interface

7.5.4 Port Trunk

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to eight ports into two dedicated connections. This feature can expand bandwidth between 2 (or more) devices. LACP operation requires full-duplex mode, more detail information refers to IEEE 802.3ad.

7.5.4.1 Trunk Configuration

1. **Group ID:** list the Trunk group ID.
2. **Type:** Static and LACP for selecting
3. Select the port number from the right column list and then click  button to add the port into a trunk group
4. Click  button to remove the port from a trunk group
5. To delete Trunk Group, select the Group ID and click the  button.

The interface shows the 'Trunking Group Configuration' window. At the top are three tabs: 'Trunk Configuration' (selected), 'Trunk Information', and 'Port Activity'. The main title is 'Trunking Group Configuration'. Below it, there are two dropdown menus: 'Group Id' set to 'Trunk.01' and 'Type' set to 'Static'. A list of ports (Port.01 to Port.12) is on the right. Below the 'Type' dropdown are buttons '<<Add' and 'Remove>>'. At the bottom are 'Apply', 'Delete', and 'Help' buttons. A message at the bottom says: 'Please use Save Configuration to permanently save the updates.'

Trunk Configuration interface

7.5.4.2 Trunk Information

After setting up the trunk group, user will see the related information as below.

The interface shows the 'Static Trunking Group Information' window. At the top are three tabs: 'Trunk Configuration', 'Trunk Information' (selected), and 'Port Activity'. The main title is 'Static Trunking Group Information'. Below it is a table with two columns: 'Group Id' and 'Port Member'.

Group Id	Port Member
1	Port.23,Port.24

Trunk Information interface

7.5.4.3 Port Activity

User will see the related information of LACP Port Activity State as below.

Port	Activity State
Port.01	Passive
Port.02	Passive
Port.03	Passive
Port.04	Passive

Apply Help

Please use Save Configuration to permanently save the updates.

Port	State
Port.01	Active
Port.02	Active
Port.03	Active
Port.04	Active

Port Activity interface

7.5.5 Port Mirror

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


Port Mirror Configuration

Port Mirroring State	Enable ▼
Analysis Port	Port.01 ▼
Monitor Port (Max. 8 ports)	State
Port.01	None ▼
Port.02	Both ▼
Port.03	None ▼
Port.04	None ▼
Port.05	None ▼
Port.06	None ▼
Port.07	None ▼
Port.08	None ▼
Port.09	None ▼
Port.10	None ▼
Port.11	None ▼
Port.12	None ▼
Port.13	None ▼
Port.14	None ▼
Port.15	None ▼
Port.16	None ▼
Port.17	None ▼
Port.18	None ▼
Port.19	None ▼
Port.20	None ▼
Port.21	None ▼
Port.22	None ▼
Trunk.01	None ▼

Apply
Help

Please use Save Configuration to permanently save the updates.

Port Mirror Configuration interface

1. **Port Mirroring State:** enable or disable the port mirror function
2. **Analysis Port:** Select a port for analyzing all monitor port traffic. User can connect mirror port to LAN analyzer or Netxray.
3. **Monitor Port:** The ports which user wants to monitor. All monitored port traffic will be copied to analysis port. (Up to 8 ports)
4. **State:** User can choose the monitored port packet in RX, TX or Both state by pulling down the pull-down menu.
5. Click  .

7.5.6 Rate Limiting

User can set up the bandwidth rate and packet limitation type of each port.

■ Input

- **State:** There are 4 check boxes of Bc, Mc, UnkUc, KnownUc for selecting.
- **Rate (1~1526)(Rate*655Kbps):** Type in the input rate limit in number between 1~1526.

■ Output

- **State:** Enable or disable the output rate limit.
- **Rate (Rate*312Kbps):** Type in the output rate limit (multiple of 312).

Rate Limit Configuration

Port	Input		Output	
	State	Rate(1~1526)(Rate*655Kbps)	State	Rate(1~3130)(Rate*312Kbps)
Port.01	<input type="checkbox"/> Bc <input type="checkbox"/> Mc <input type="checkbox"/> UnkUc <input type="checkbox"/> KnownUc	<input type="text"/>	Disable ▾	<input type="text"/>
Port.02				
Port.03				
Port.04				

Apply Help

Please use Save Configuration to permanently save the updates.

Port	Input		Output	
	State	Rate(1~1526)(Rate*655Kbps)	State	Rate(1~3130)(Rate*312Kbps)

Port Configuration interface

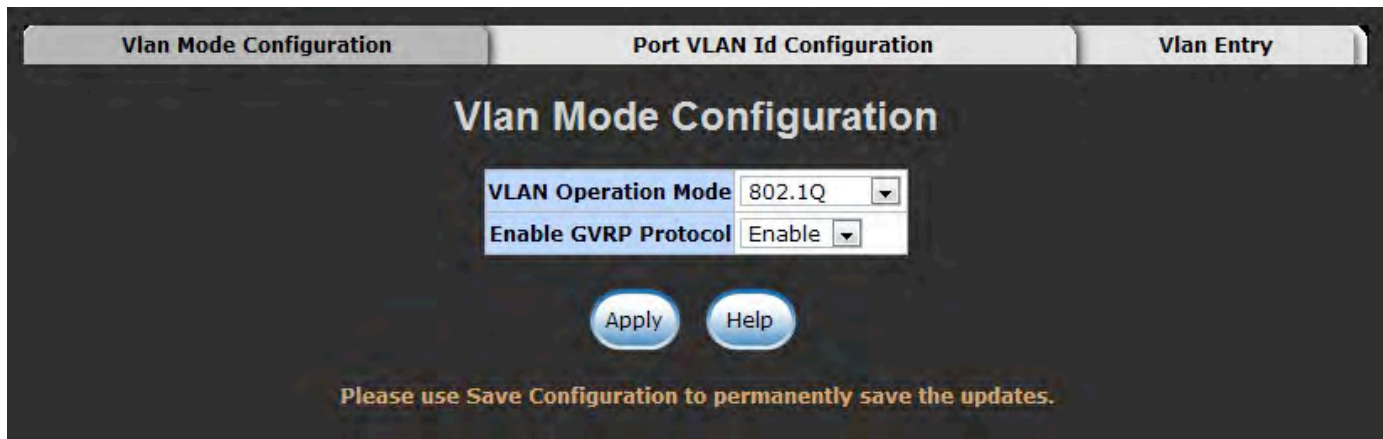
7.6 Protocol

7.6.1 VLAN

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 VLAN will receive traffic from the same members of 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.


7.6.1.1 VLAN Mode Configuration

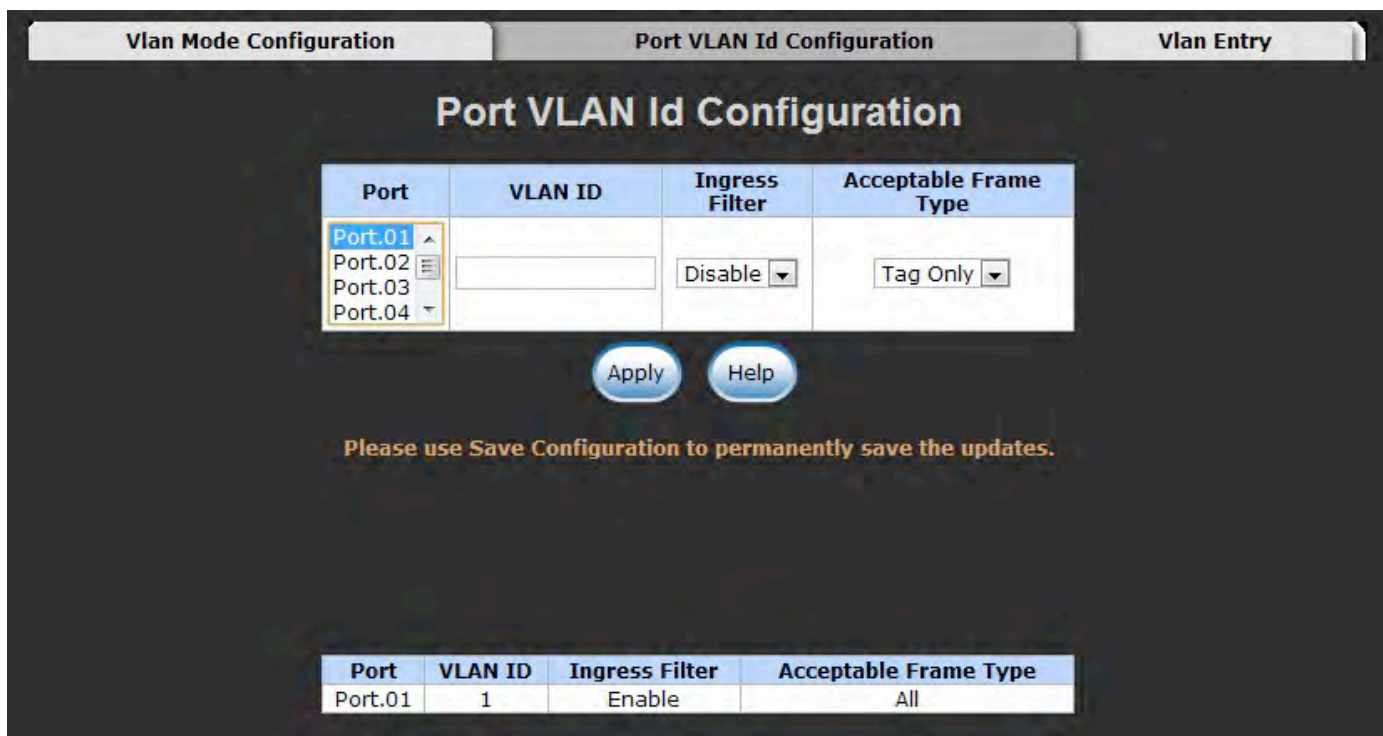
The switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration of VLAN operation mode is “**802.1Q**”.



VLAN Mode Configuration interface

7.6.1.2 Port VLAN Id Configuration

1. **Port:** Select the port number in the table list.
2. **VLAN ID:** Key in the VLAN ID.
3. **Ingress Filter:** Enable or Disable the ingress filter.
4. **Acceptable Frame Type:** Choose **Tag only** or **All type**.
5. Click 



The screenshot shows the 'Port VLAN Id Configuration' interface. At the top, there are three tabs: 'Vlan Mode Configuration', 'Port VLAN Id Configuration' (which is active), and 'Vlan Entry'. The main title 'Port VLAN Id Configuration' is centered. Below it is a configuration table with four columns: 'Port', 'VLAN ID', 'Ingress Filter', and 'Acceptable Frame Type'. The 'Port' column has a list box with 'Port.01' selected. The 'VLAN ID' column has an empty text input field. The 'Ingress Filter' column has a dropdown menu set to 'Disable'. The 'Acceptable Frame Type' column has a dropdown menu set to 'Tag Only'. Below the table are 'Apply' and 'Help' buttons. A message states: 'Please use Save Configuration to permanently save the updates.' At the bottom, there is a summary table showing the current configuration for Port.01.

Port	VLAN ID	Ingress Filter	Acceptable Frame Type
Port.01		Disable	Tag Only
Port.02			
Port.03			
Port.04			

Apply Help

Please use Save Configuration to permanently save the updates.

Port	VLAN ID	Ingress Filter	Acceptable Frame Type
Port.01	1	Enable	All

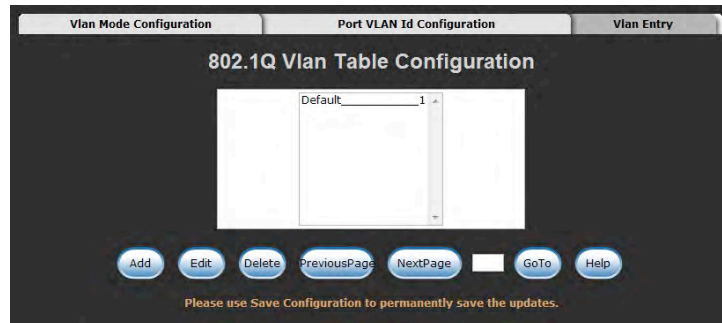
Port VLAN Id Configuration interface

7.6.1.3 VLAN Entry

Edit the existing VLAN Group.

1. Select the VLAN group in the table list.

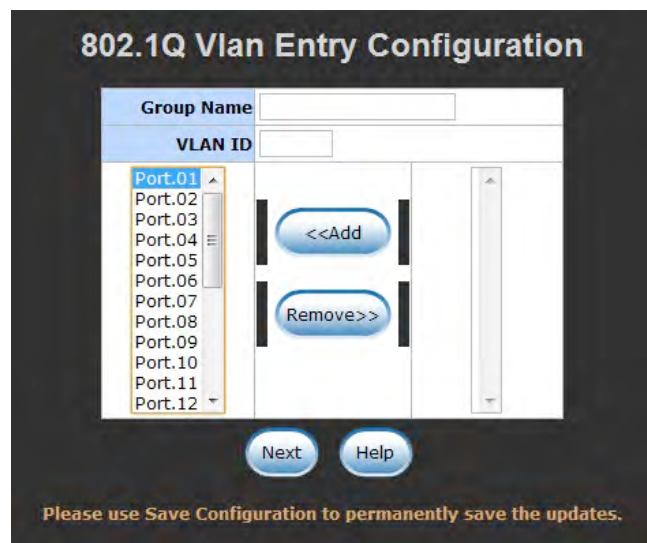
2. Click .



VLAN Table Configuration interface

3. User can add/ remove the ports from a VLAN group.

4. Click .



VLAN Table Configuration - Edit interface

5. Mark the check box to tag the ports of a VLAN group.

6. Click .

802.1Q Vlan Entry Tag Configuration

Group Name	Default	
VLAN ID	1	
Port.01	<input type="checkbox"/> Tagged	Port.02 <input type="checkbox"/> Tagged
Port.03	<input type="checkbox"/> Tagged	Port.04 <input type="checkbox"/> Tagged
Port.05	<input type="checkbox"/> Tagged	Port.06 <input type="checkbox"/> Tagged
Port.07	<input type="checkbox"/> Tagged	Port.08 <input type="checkbox"/> Tagged
Port.09	<input type="checkbox"/> Tagged	Port.10 <input type="checkbox"/> Tagged
Port.11	<input type="checkbox"/> Tagged	Port.12 <input type="checkbox"/> Tagged
Port.13	<input type="checkbox"/> Tagged	Port.14 <input type="checkbox"/> Tagged
Port.15	<input type="checkbox"/> Tagged	Port.16 <input type="checkbox"/> Tagged
Port.17	<input type="checkbox"/> Tagged	Port.18 <input type="checkbox"/> Tagged
Port.19	<input type="checkbox"/> Tagged	Port.20 <input type="checkbox"/> Tagged
Port.21	<input type="checkbox"/> Tagged	Port.22 <input type="checkbox"/> Tagged
Port.23	<input type="checkbox"/> Tagged	Port.24 <input type="checkbox"/> Tagged


Please use Save Configuration to permanently save the updates.

VLAN Table Configuration - Edit interface

7.6.2 Rapid Spanning Tree

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.

7.6.2.1 STP System Configuration

- User can view spanning tree information about the Root Bridge
- User can modify RSTP state. After modification, click  .
 - **Mode:** user must enable or disable RSTP function before configure the related parameters
 - **Priority (0-61440):** a value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root.
 - **Max Age (6-40):** the number of seconds a bridge 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 switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10
- **Forward Delay Time (4-30):** the number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30

[NOTE] Follow the rule to configure the MAX Age, Hello Time, and Forward Delay Time.

$2 \times (\text{Forward Delay Time value} - 1) \geq \text{Max Age value} \geq 2 \times (\text{Hello Time value} + 1)$

The screenshot displays the RSTP System Configuration interface. At the top, there are two tabs: "STP System Configuration" (active) and "STP Port Configuration". Below the tabs, the "STP System Configuration" section contains a table with the following fields and values:

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


Below the table are two buttons: "Apply" and "Help". A message states: "Please use Save Configuration to permanently save the updates." Below this is the "Root Bridge Information" section, which contains another table with the following fields and values:

Root Priority	32768
Root MAC Address	00-22-3B-03-09-7C
Max Age	20
Hello Time	2
Forward Delay	15
Root Port	root
Root Path Cost	0

RSTP System Configuration interface

7.6.2.2 STP Port Configuration

User can configure path cost and priority of every port.

1. Select the port in Port column.
1. **Priority:** Decide which port should be blocked by priority in LAN. Enter a number 0 through 240.
2. **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
3. **AdmP2P:** 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. Enable is P2P enabled; disable is P2P disabled; and auto means auto-sense.
4. **AdmEdge:** The port directly connected to end stations that cannot create bridging loop in the network. To configure the port as an edge port, set the port to “**Enable**” status.
5. **AdmStp:** The port includes the STP mathematic calculation. **Enable** is including STP mathematic calculation. **Disable** is not including the STP mathematic calculation.
6. Click  .

STP System Configuration
STP Port Configuration

STP Port Configuration

Port	Priority (0~240)	Path Cost (1~200000000)	AdmP2P	AdmEdge	AdmStp
Port.01					
Port.02	0	1	Auto	Disable	Enable
Port.03					
Port.04					

Apply
Help

Please use Save Configuration to permanently save the updates.

Port	State	Priority	Path Cost	AdmP2P	AdmEdge	AdmStp	Role
Port.01	Discarding	0	1	Enable	Disable	Enable	Disabled

RSTP Port Configuration interface

7.6.3 SNMP

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

■ SNMP Information

Enter the system name, contact and location information.

- **Name:** Assign a name for the switch.
- **Location:** Type the location of the switch.
- **Contact:** Type the name of contact person or organization.


■ SNMP Community String

User can define new community string set and remove unwanted community string.

- **RO:** Read only. Enable requests accompanied by this string to display MIB-object information.
- **RW:** Read write. Enable requests accompanied by this string to display MIB-object information and to set MIB objects.

■ SNMP Trap managers

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will issue. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager and enter SNMP community strings and selects the SNMP version.

- **IP Address:** enter the IP address of trap manager.
- **Community:** enter the community string.
- Click  .

SNMP Information

Name	<input type="text"/>
Location	<input type="text"/>
Contact	<input type="text"/>

Please use Save Configuration to permanently save the updates.

SNMP Community Strings

Current Strings	New Community String	
<div>public__RO private__RW</div>	<input type="button" value="Add"/>	<input type="text"/>
<input type="button" value="Remove"/>	<input checked="" type="checkbox"/> RO <input type="checkbox"/> RW	

SNMP Trap Managers


Current Managers	New Manager	
<div></div>	<input type="button" value="Add"/>	IP Address <input type="text"/>
<input type="button" value="Remove"/>	Community <input type="text"/>	
	Trap version <input checked="" type="radio"/> v1 <input type="radio"/> v2	

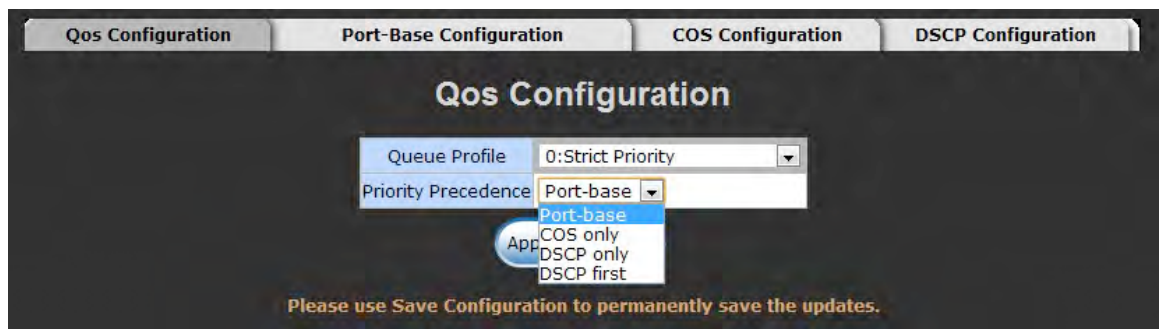
SNMP Configuration interface

7.6.4 QoS

User can configure QoS policy and priority setting, per port priority setting, COS and DSCP setting.


7.6.4.1 QoS Configuration

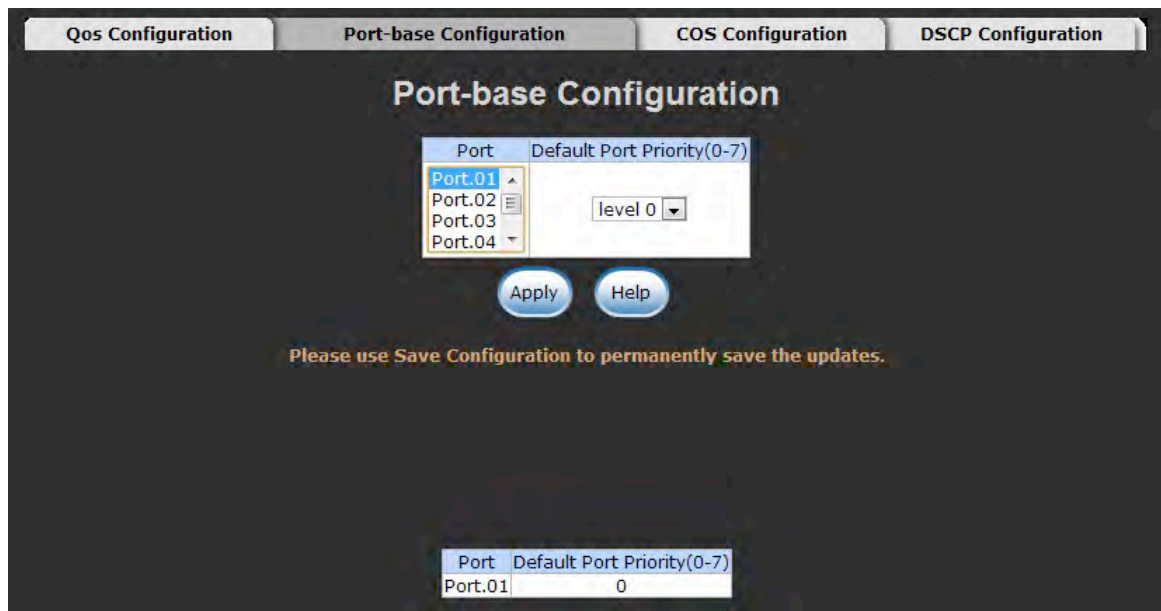
- **Queue Profile:** Select the queue profile from the column list.
- **Priority Precedence:** There are 4 priority precedence selections available.
- Click  .



QoS Configuration interface

7.6.4.2 Port-base Configuration

- **Port:** Select the number port from the column list.
- **Default Port Priority (0-7):** Assign the priority level.
- Click  .



The screenshot shows the 'Port-base Configuration' window. At the top, there are four tabs: 'Qos Configuration', 'Port-base Configuration' (which is active), 'COS Configuration', and 'DSCP Configuration'. The main title is 'Port-base Configuration'. Below it, there is a table with two columns: 'Port' and 'Default Port Priority(0-7)'. The 'Port' column has a list box containing 'Port.01', 'Port.02', 'Port.03', and 'Port.04', with 'Port.01' selected. The 'Default Port Priority(0-7)' column has a dropdown menu showing 'level 0'. Below the table are two buttons: 'Apply' and 'Help'. A message at the bottom says 'Please use Save Configuration to permanently save the updates.' At the very bottom, there is a small table with two columns: 'Port' and 'Default Port Priority(0-7)', with 'Port.01' and '0' listed.


Port	Default Port Priority(0-7)
Port.01	level 0

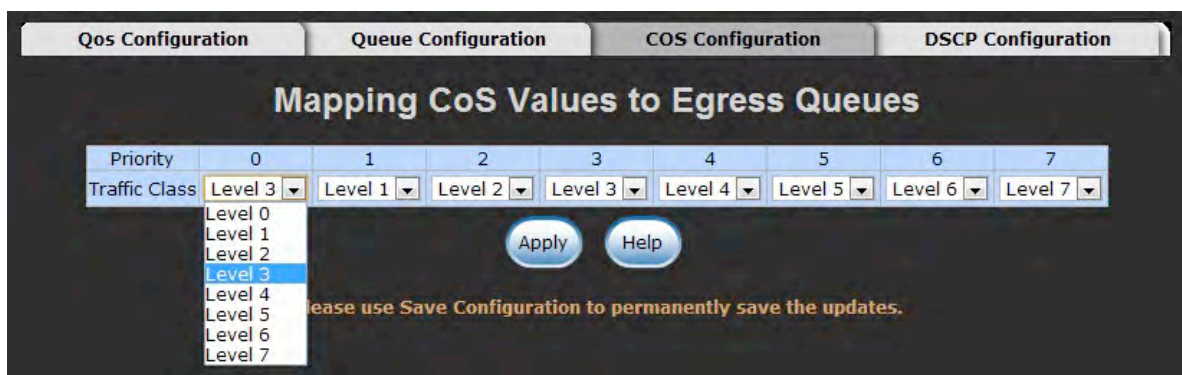
Port	Default Port Priority(0-7)
Port.01	0

Port-base Configuration interface

7.6.4.3 COS Configuration

Set up the COS priority level.

- **COS priority:** Set up the COS priority level 0~7, 7 is the highest priority.
- Click  .



The screenshot shows the 'COS Configuration' window. At the top, there are four tabs: 'Qos Configuration', 'Queue Configuration', 'COS Configuration' (which is active), and 'DSCP Configuration'. The main title is 'Mapping CoS Values to Egress Queues'. Below it, there is a table with two rows: 'Priority' and 'Traffic Class'. The 'Priority' row has columns for values 0 through 7. The 'Traffic Class' row has dropdown menus for each priority level, showing 'Level 3' for 0, 'Level 1' for 1, 'Level 2' for 2, 'Level 3' for 3, 'Level 4' for 4, 'Level 5' for 5, 'Level 6' for 6, and 'Level 7' for 7. A dropdown menu for 'Level 3' is open, showing a list of levels from 0 to 7, with 'Level 3' highlighted. Below the table are two buttons: 'Apply' and 'Help'. A message at the bottom says 'Please use Save Configuration to permanently save the updates.'

Priority	0	1	2	3	4	5	6	7
Traffic Class	Level 3	Level 1	Level 2	Level 3	Level 4	Level 5	Level 6	Level 7

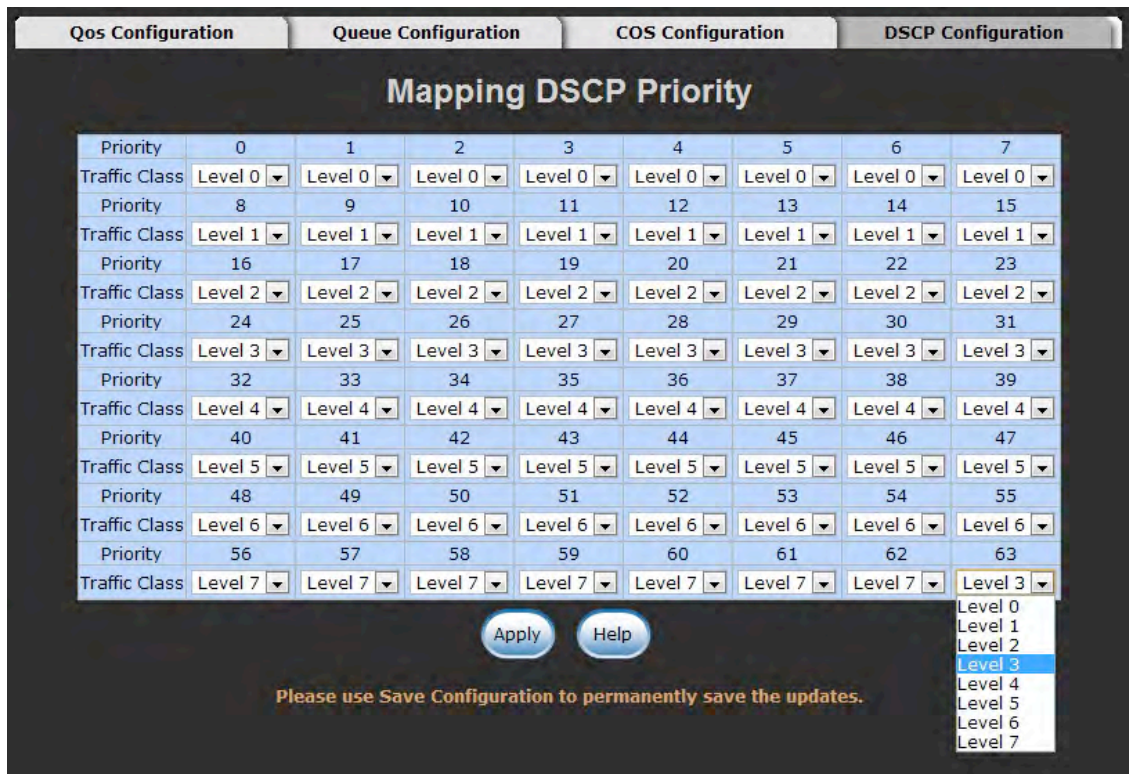
COS Configuration interface

7.6.4.4 DSCP Configuration

Set up the DSCP priority.

■ **Mapping DSCP priority:** The system provides 0~63 DSCP priority level. Each level has 8 types of priority – 0~7, 7 is the highest priority. When the IP packet is received, the system will check the DSCP level value in the IP packet that has been received. For example: user set the DSCP level 25 as high. When the packet received, the system will check the DSCP value of the received IP packet. If the DSCP value of received IP packet is 25(priority = high), and then the packet priority will have highest priority.

■ Click  .



The interface shows a tabbed menu at the top with 'Qos Configuration', 'Queue Configuration', 'COS Configuration', and 'DSCP Configuration'. The 'DSCP Configuration' tab is active, displaying a 'Mapping DSCP Priority' table. The table has 8 columns representing traffic classes (0-7) and 8 rows representing DSCP priority ranges (0-7). Each cell contains a dropdown menu for mapping a specific DSCP priority to a traffic class. Below the table are 'Apply' and 'Help' buttons. A message at the bottom states: 'Please use Save Configuration to permanently save the updates.' A dropdown menu is open on the right side of the table, showing the available traffic class levels from Level 0 to Level 7, with Level 3 currently selected.

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

DSCP Configuration interface

7.6.5 SNTP

User can configure the SNTP (Simple Network Time Protocol) settings. The SNTP allows user to synchronize switch clocks in the Internet.

1. **SNTP Server Link Status:** Display the link status of SNTP server.
2. **Switch Current Time:** Display the current time of the switch.
3. **SNTP Client:** Enable or disable SNTP function. When it is enabled, user can assign the domain name or IP address of SNTP server for getting the time from SNTP server.
4. **UTC Timezone:** Set the switch location time zone. The following table lists the different location time zone for your reference:

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am

CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

5. SNTP Period: The SNTP period is used for sending synchronizing packets periodically.

6. SNTP Sever IP Address: Assign the SNTP server IP address.

7. Click  .

SNTP Configuration

SNTP Server Link Status	DOWN
Switch Current Time	THU JAN 01 09:16:44 1970
SNTP Client	Enable <input type="button" value="v"/>
UTC Timezone	(GMT-06:00) Mexico, Central Time (USA & Canada) <input type="button" value="v"/>
SNTP Period	16
SNTP Server IP Address	192.168.10.2

Please use Save Configuration to permanently save the updates.

SNTP Configuration interface

7.6.6 IGMP

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

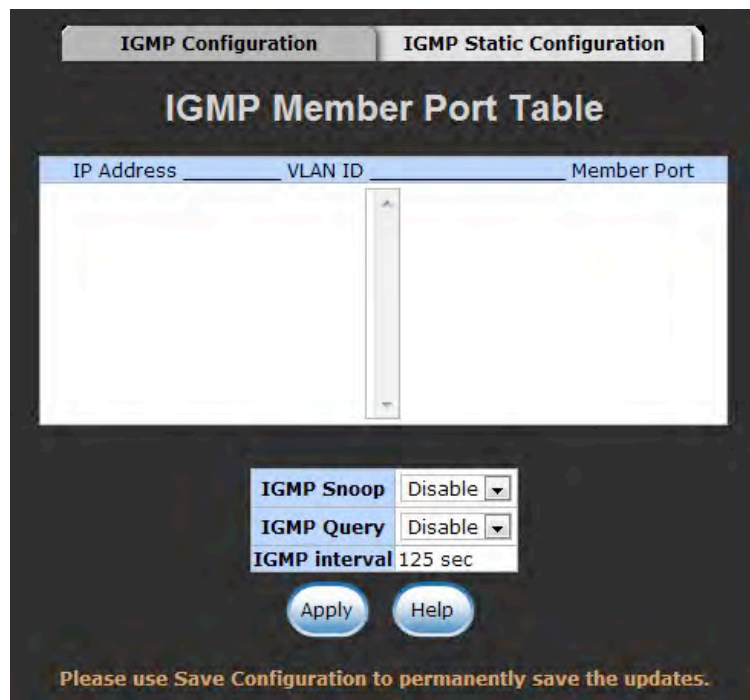
Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Join Group	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.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

7.6.6.1 IGMP Configuration

The switch support IP multicast, user can enable IGMP protocol on web management's switch setting advanced page, then display the IGMP snooping information. IP multicast addresses range from 224.0.0.0 through 239.255.255.255.

- **IGMP Snoop:** Enable or disable the IGMP snoop.
- **IGMP Query:** The IGMP query function has 3 modes - Enable, Disable or Auto - for selection. The IGMP query information will be displayed in IGMP status section.
- **IGMP interval:** The interval of General Query being sent. (Read Only)

- Click  .



The screenshot shows the 'IGMP Configuration' tab of a network device's web interface. At the top, there are two tabs: 'IGMP Configuration' (selected) and 'IGMP Static Configuration'. Below the tabs is the title 'IGMP Member Port Table'. Under this title is a table with three columns: 'IP Address', 'VLAN ID', and 'Member Port'. The table is currently empty. Below the table, there are three configuration options: 'IGMP Snoop' set to 'Disable', 'IGMP Query' set to 'Disable', and 'IGMP interval' set to '125 sec'. At the bottom of the configuration section are two buttons: 'Apply' and 'Help'. A red message at the very bottom states: 'Please use Save Configuration to permanently save the updates.'

IGMP Configuration interface

7.6.6.2 IGMP Static Configuration

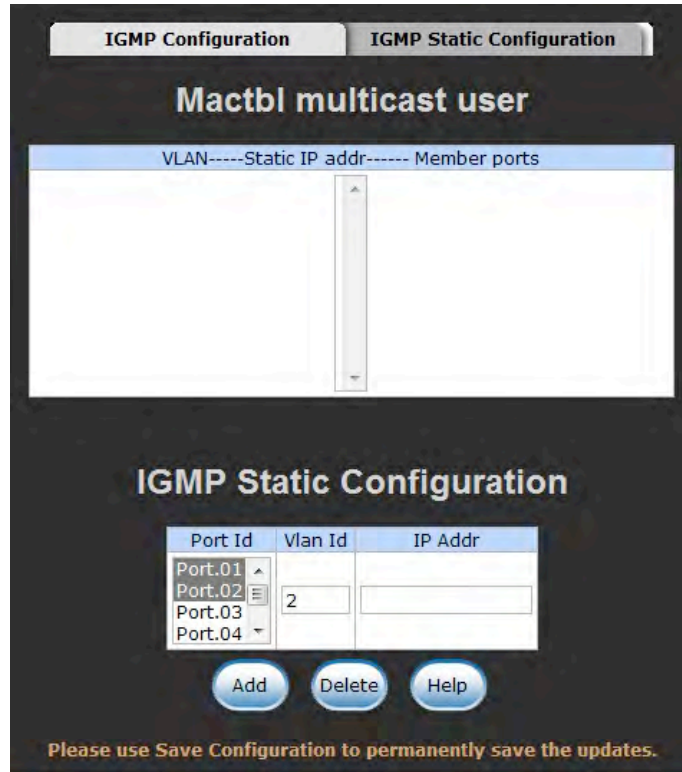
Multicasts are similar to broadcasts, they are sent to all end stations on a LAN or VLAN. Multicast filtering is the system by which end stations only receive multicast traffic if they register to join specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the end stations that are connected to registered ports.

This function action when **IGMP Configuration** disable.

- **Port ID:** Select the port number in the specific multicast group IP address.
- **VLAN ID:** Input the value of VLAN ID.
- **IP Address:** Assign a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255.

- Click  .

If you want to delete an entry from table, select the entry and click "Delete".



The screenshot shows the 'IGMP Static Configuration' interface. At the top, there are two tabs: 'IGMP Configuration' and 'IGMP Static Configuration'. Below the tabs is a title 'Mactbl multicast user'. Underneath is a table with columns 'VLAN-----', 'Static IP addr-----', and 'Member ports'. The table is currently empty. Below the table is a section titled 'IGMP Static Configuration' containing a table with three columns: 'Port Id', 'Vlan Id', and 'IP Addr'. The 'Port Id' column has a list box with options 'Port.01', 'Port.02', 'Port.03', and 'Port.04'. The 'Vlan Id' column has a text box containing the number '2'. The 'IP Addr' column has an empty text box. Below this table are three buttons: 'Add', 'Delete', and 'Help'. At the bottom of the interface, there is a message: 'Please use Save Configuration to permanently save the updates.'

IGMP Static Configuration interface

7.6.7 LLDP

The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station's point of attachment to the IEEE 802 LAN required by those management entity or entities.

7.6.7.1 LLDP Configuration

- Mode Configuration: Enable or disable the LLDP function.
- Port Configuration: Enable or disable the LLDP state of the number port.

LLDP Configuration

LLDP Neighbour Table

Mode Configuration

Enable

Apply

Please use Save Configuration to permanently save the updates.

Port Configuration

Port	State
Port.01	
Port.02	Disable
Port.03	
Port.04	

Apply

Disable

RX and TX

TX Only

RX Only

Please use Save Configuration to permanently save the updates.

Port	State
Port.02	Disable

LLDP Configuration interface

7.6.7.2 LLDP Neighbor Table

User will see all information of port by LLDP enable.

LLDP Configuration

LLDP Neighbour Table

LLDP Neighbour Table

Port	Chassis Id	Remote Port ID	System Name	Port description
------	------------	----------------	-------------	------------------


LLDP Neighbor Table interface

7.7 Security

7.7.1 802.1x/ RADIUS

802.1x is an IEEE authentication specification that allows a client to connect to a wireless access point or wired switch but prevents the client from gaining access to the port until it provides authority, like a user name and password that are verified by a separate server.

7.7.1.1 Misc Configuration

1. **Mode:** Enable or disable 802.1 x protocols.
2. **Quiet Period:** Set the period during which the port doesn't try to acquire a supplicant.
3. **TX Period:** Set the period the port waits for retransmit next EAPOL PDU during an authentication session.
4. **Supplicant Timeout:** Set the period of time the switch waits for a supplicant response to an EAP request.
5. **Server Timeout:** Set the period of time the switch waits for a server response to an authentication request.
6. **ReAuthMax:** Set the number of authentication that must time-out before authentication fails and the authentication session ends.
7. **Reauth period:** set the period of time after which clients connected must be re-authenticated.
8. Click  .

Misc Configuration

Port Configuration

Radius Configuration

802.1X Configuration

Mode

Disable

Apply

Please use Save Configuration to permanently save the updates.

802.1X Misc Configuration

Quiet Period	60
Tx Period	30
Supplicant Timeout	30
Server Timeout	30
ReAuthMax	2
Reauth Period	3600

Apply

Help

Please use Save Configuration to permanently save the updates.

MISC Configuration interface

7.7.1.2 Port Configuration

Misc Configuration

Port Configuration

Radius Configuration

802.1X Port Configuration

Port	State
Port.01	Disable
Port.02	
Port.03	
Port.04	

Apply


Help

Please use Save Configuration to permanently save the updates.

Port	State
Port.01	Disable


Port Configuration interface

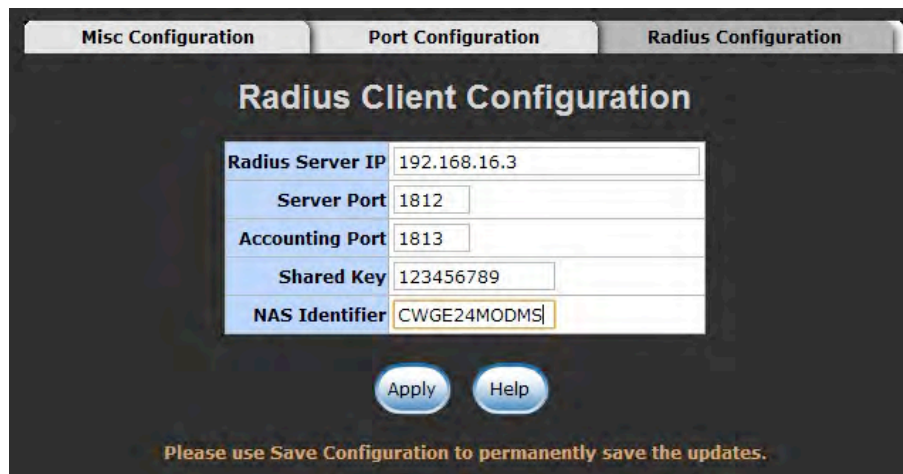
You can configure 802.1x authentication state for each port. The State provides Disable, Authorize, Accept and Reject.

- **Disable:** This function is disabled.
- **Authorize:** The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the supplicant and the authenticator.
- **Accept:** The specified port will allow the client accessing in any case.
- **Reject:** The specified port rejects the client accessing regardless of whether the authentication passed or not.
- Click  .

7.7.1.3 Radius Client Configuration

After having enabled the IEEE 802.1X function, user can configure the parameters of this function.

1. **Radius Server IP:** Set the Radius Server IP address.
2. **Server Port:** Set the UDP destination port for authentication requests to the specified Radius Server.
3. **Accounting Port:** Set the UDP destination port for accounting requests to the specified Radius Server.
4. **Shared Key:** Set an encryption key for using during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
5. **NAS Identifier:** A string used to identify this switch.
6. Click  .



Radius Client Configuration	
Radius Server IP	192.168.16.3
Server Port	1812
Accounting Port	1813
Shared Key	123456789
NAS Identifier	CWGE24MODMS

Apply Help

Please use Save Configuration to permanently save the updates.

Radius Client Configuration interface

7.7.2 Port Security

Use the MAC address table to ensure the port security.

7.7.2.1 Static MAC Address Table

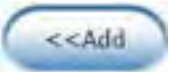

User can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. User can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

Packets with the specified destination address received in the specified VLAN are forwarded to the specified interface.

Static MAC Addresses interface

Add the Static MAC Address

User can add static MAC address in switch MAC table.

1. **MAC Address Port VLAN ID:** list the MAC Address Port. VLAN ID
2. **MAC Address:** Specify the destination MAC address to add to the address table.
3. **Port.No:** pull down the selection menu to select the port number.
4. **Vid:** enter the Vid of the MAC address (between 1 and 4094).
5. Click .
6. If user wants to delete the MAC address from filtering table, select the MAC address and click .

7.7.2.2 Filter MAC Address Table

MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination addresses. For example, if your network is congested because of high utilization from one MAC address, you can filter all traffic transmitted to that MAC address, restoring network flow while you troubleshoot the problem.

Static Mac Address Table Filter Mac Address Table Mac Address Table Aging Dynamic Mac Address Table

Filter Mac Address Table

MAC Address	VLAN ID
-------------	---------



MAC Address:

Vid:

Add Delete Help

Please use Save Configuration to permanently save the updates.

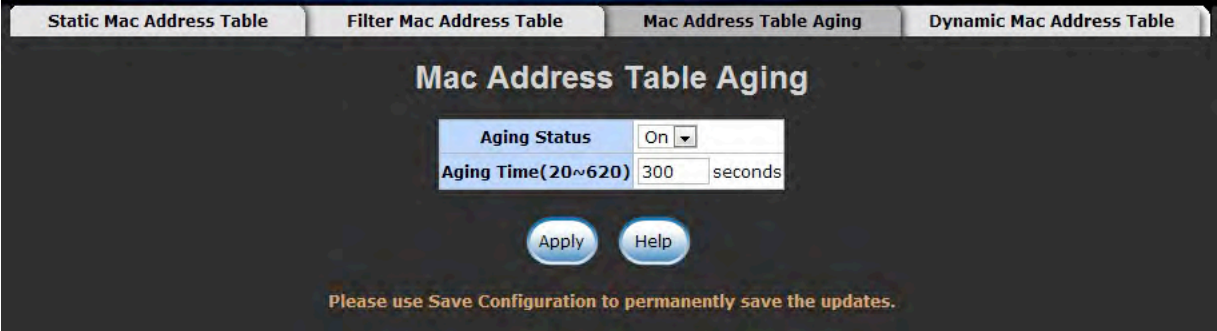
MAC Filtering interface

1. **MAC Address:** Enter the MAC address that user wants to filter.
2. **Vid:** enter the Vid of the MAC address (between 1 and 4094).
3. Click  .
4. If user wants to delete the MAC address from filtering table, select the MAC address and click  .

7.7.2.3 MAC Address Table Aging

Aging Status: Pull-down menu to enable MAC address table aging function.

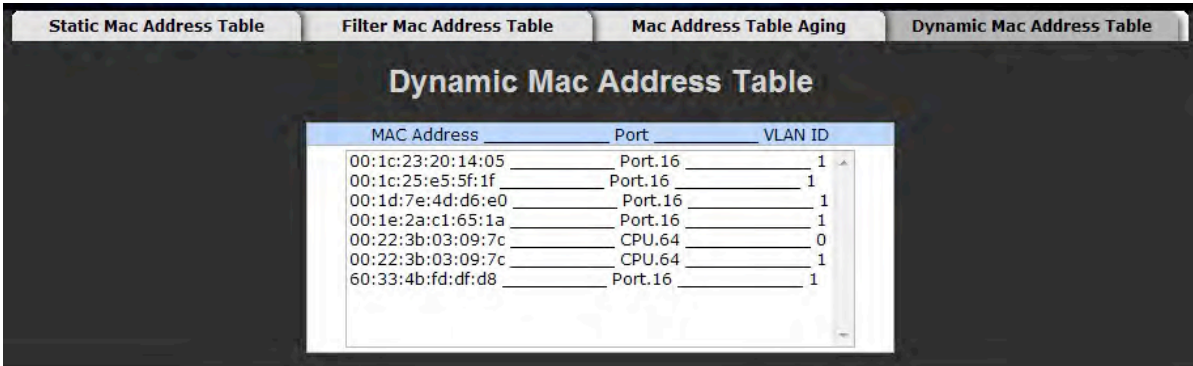
Aging Time (20~620): Assign the aging time in second.



The interface shows the 'Mac Address Table Aging' configuration page. It has a top navigation bar with four tabs: 'Static Mac Address Table', 'Filter Mac Address Table', 'Mac Address Table Aging' (selected), and 'Dynamic Mac Address Table'. The main title is 'Mac Address Table Aging'. Below the title, there are two configuration fields: 'Aging Status' with a pull-down menu set to 'On', and 'Aging Time(20~620)' with a text box containing '300' and the unit 'seconds'. There are two buttons, 'Apply' and 'Help', below the fields. At the bottom, a message states: 'Please use Save Configuration to permanently save the updates.'

Address Aging interface

7.7.2.4 Dynamic MAC Address Table



The interface shows the 'Dynamic Mac Address Table' configuration page. It has a top navigation bar with four tabs: 'Static Mac Address Table', 'Filter Mac Address Table', 'Mac Address Table Aging', and 'Dynamic Mac Address Table' (selected). The main title is 'Dynamic Mac Address Table'. Below the title, there is a table with three columns: 'MAC Address', 'Port', and 'VLAN ID'. The table contains the following data:

MAC Address	Port	VLAN ID
00:1c:23:20:14:05	Port.16	1
00:1c:25:e5:5f:1f	Port.16	1
00:1d:7e:4d:d6:e0	Port.16	1
00:1e:2a:c1:65:1a	Port.16	1
00:22:3b:03:09:7c	CPU.64	0
00:22:3b:03:09:7c	CPU.64	1
60:33:4b:fd:df:d8	Port.16	1

Dynamic Mac Address Table interface

7.7.3 IP Security

User can assign up to 10 security IP addresses for accessing the switch via HTTP, TELNET or both, any other IPs which are not included will be restricted.





The image shows the 'Security IP Manager' web interface. At the top, the title 'Security IP Manager' is displayed. Below it, there is a 'Mode' dropdown menu currently set to 'On'. The main area contains a table with 10 rows, each representing a security IP address. Each row has a blue-numbered cell (1-10), an input field for the IP address, two checkboxes for 'HTTP' and 'TELNET', and a 'Clear' button. At the bottom of the interface, there are 'Apply' and 'Help' buttons. A warning message at the very bottom states: 'Please use Save Configuration to permanently save the updates.'

Mode	On ▼			
1.	<input type="text"/>	<input type="checkbox"/> HTTP	<input type="checkbox"/> TELNET	<input type="button" value="Clear"/>
2.	<input type="text"/>	<input type="checkbox"/> HTTP	<input type="checkbox"/> TELNET	<input type="button" value="Clear"/>
3.	<input type="text"/>	<input type="checkbox"/> HTTP	<input type="checkbox"/> TELNET	<input type="button" value="Clear"/>
4.	<input type="text"/>	<input type="checkbox"/> HTTP	<input type="checkbox"/> TELNET	<input type="button" value="Clear"/>
5.	<input type="text"/>	<input type="checkbox"/> HTTP	<input type="checkbox"/> TELNET	<input type="button" value="Clear"/>
6.	<input type="text"/>	<input type="checkbox"/> HTTP	<input type="checkbox"/> TELNET	<input type="button" value="Clear"/>
7.	<input type="text"/>	<input type="checkbox"/> HTTP	<input type="checkbox"/> TELNET	<input type="button" value="Clear"/>
8.	<input type="text"/>	<input type="checkbox"/> HTTP	<input type="checkbox"/> TELNET	<input type="button" value="Clear"/>
9.	<input type="text"/>	<input type="checkbox"/> HTTP	<input type="checkbox"/> TELNET	<input type="button" value="Clear"/>
10.	<input type="text"/>	<input type="checkbox"/> HTTP	<input type="checkbox"/> TELNET	<input type="button" value="Clear"/>

Please use Save Configuration to permanently save the updates.

IP Security interface

1. **Mode:** When mode is set at **ON**, user can assign up to 10 Security IP addresses.
2. **HTTP:** mark the check box to enable the access via HTTP for the assigned IP
3. **TELNET:** mark the check box to enable the access via TELNET for the assigned IP.
4. Click  button to clear IP address and all the check box.
5. And then, click 

7.7.4 ACL

An ACL is a sequential list of permit or deny conditions that apply to IP addresses. This switch tests ingress or egress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match for a list of all permit rules, the packet is dropped; and if no rules matches for a list of all deny rules, the packet is accepted.

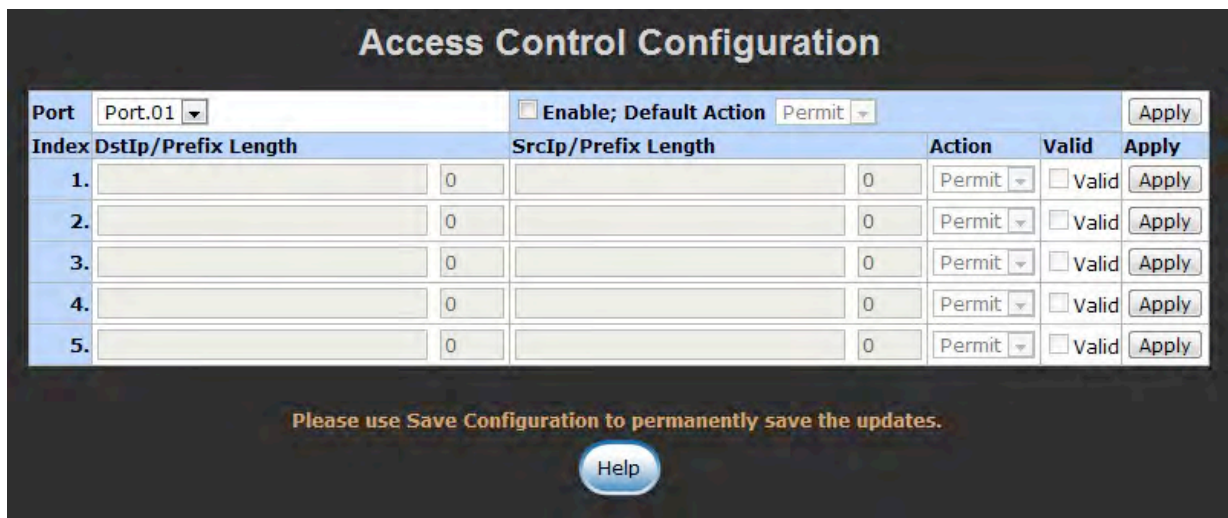
The following restrictions apply to ACLs:

- The ACL only support single port and not support trunk group.
- The maximum number of ACLs is also 5 for each port.

Command Attributes

- **Enable:** An ACL can be enabled per port.
- **Default Action:** The action if no rules matched.
- **Action:** An ACL can be permit or deny rule.
- **IP Address and Prefix Length:** Include destination and source IP address.

Ex: source 192.168.10.1/24 means all frames that source IP address is 192.168.10.x matched.



The screenshot shows the 'Access Control Configuration' interface. At the top, there's a title bar. Below it, a 'Port' dropdown is set to 'Port.01'. To its right, there's a checkbox for 'Enable' and a 'Default Action' dropdown set to 'Permit'. An 'Apply' button is to the right of these. Below this is a table with 5 rows. The table has columns: 'Index', 'DstIp/Prefix Length', 'SrcIp/Prefix Length', 'Action', 'Valid', and 'Apply'. Each row has input fields for the IP and prefix length, a dropdown for the action (all set to 'Permit'), a checkbox for 'Valid' (all unchecked), and an 'Apply' button. At the bottom of the interface, there's a message: 'Please use Save Configuration to permanently save the updates.' and a 'Help' button.



Index	DstIp/Prefix Length	SrcIp/Prefix Length	Action	Valid	Apply
1.	<input type="text"/> 0	<input type="text"/> 0	Permit	<input type="checkbox"/> Valid	Apply
2.	<input type="text"/> 0	<input type="text"/> 0	Permit	<input type="checkbox"/> Valid	Apply
3.	<input type="text"/> 0	<input type="text"/> 0	Permit	<input type="checkbox"/> Valid	Apply
4.	<input type="text"/> 0	<input type="text"/> 0	Permit	<input type="checkbox"/> Valid	Apply
5.	<input type="text"/> 0	<input type="text"/> 0	Permit	<input type="checkbox"/> Valid	Apply

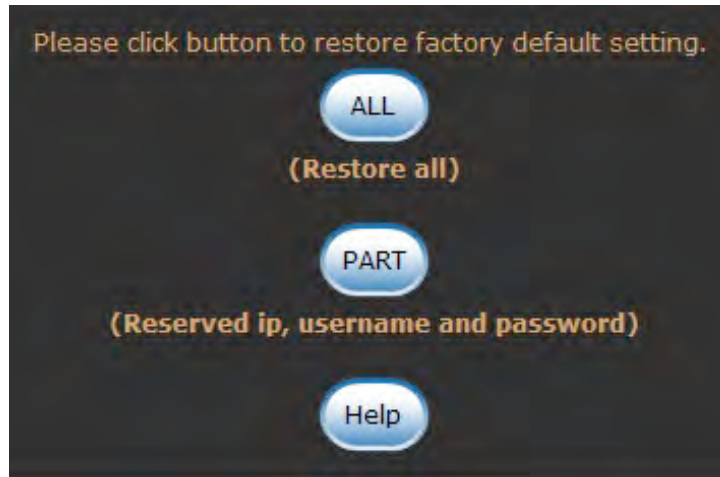
Please use Save Configuration to permanently save the updates.

Help

Access Control Configuration Interface


7.8 Factory Default

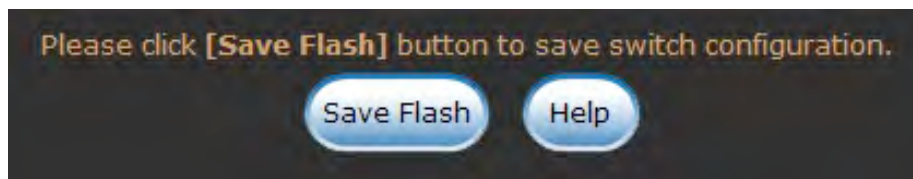
Reset switch to default configuration. Click  to reset all configurations to the default value or  to reset all configuration except reserved IP, user name and password.



Factory Default interface


7.9 Save Configuration

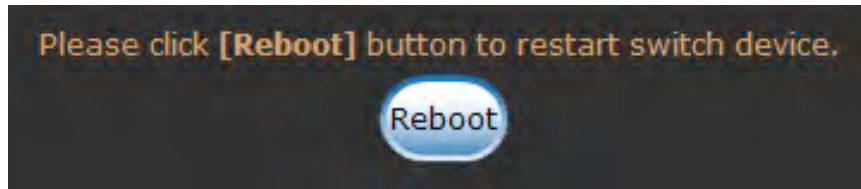
Save all configurations that user has made in the system. To ensure the all configuration will be saved. Click  to save the all configuration to the flash memory.



Save Configuration interface

7.10 System Reboot

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



System Reboot interface

Troubleshooting

This section is intended to help you solve the most common problems that may occur on the CWGE24MODMS Managed Switch.

■ Incorrect connections

The switch port can automatically detect straight or crossover cable when linked with another Ethernet device. For the RJ45 connection, use correct UTP or STP cables. The 10/100/1000Mbps port uses 2-pairs twisted cable and the Gigabit 1000T port uses 4 pairs twisted cable. If the RJ45 connector is not correctly pinned then the link will fail. For the fiber connection, please note that the fiber cable mode and fiber module should 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.

RJ45 ports: Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ45 connections: 100Ω Category 3, 4 or 5 cable for 10Mbps connections, 100Ω Category 5 cable for 100Mbps connections or Category-5e / Category-6 for above 1000Mbps connections. The length of any twisted-pair connection should not exceed 100 meters (328 feet). The Gigabit port uses Cat-5 or cat-5e cable for 1000Mbps connections. The length should not exceed 100 meters.

■ **Improper Network Topologies**

It is important to make sure that you have a valid network topology. Common topology faults include excessive cable length and too many repeaters (hubs) between end nodes. In addition, you should make sure that your network topology contains no data path loops. Between any two ends nodes, there should be only one active cabling path at any time. Data path loops will cause broadcast storms that will severely impact your network performance.

■ **Diagnosing LED Indicators**

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

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

Appendix A- Command Sets

Commands Set List

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

System Commands Set

Netstar Commands	Command Level	Description	Defaults	Example
system name [system name]	Global configuration mode	Set switch system name string		switch(config)# system name xxx
system location [system Location]	Global configuration mode	Set switch system location string		switch(config)# system location xxx
system description [description]	Global configuration mode	Set switch system description string		switch(config)# system description xxx
system contact [contact]	Global configuration mode	Set switch system contact window string		switch(config)# system contact xxx
ip address [ip-address] [subnet-mask] [gateway]	Global configuration mode	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.		switch(config)# ip address 192.168.1.1 255.255.255.0 192.168.1.254
write memory	Privileged EXEC	Save user configuration into permanent memory(flash rom)		switch# write memory

reload	Global configuration mode	Halt and perform a cold restart		switch(config)# reload
default	Global configuration mode	Restore to default no : restore all to default. yes : reserved ip, username and password.		switch(config)# default
admin username [Username]	Global configuration mode	Changes a login username. (maximum 32 words)		switch(config)# admin username xxxxxx
admin password [Username]	Global configuration mode	Specifies a password (maximum 32 words)		switch(config)# admin password xxxxxx
console-timeout [time(sec)]	Global configuration mode	Set console timeout. The range of timeout is 30 sec ~ 600 sec.	180 sec	switch(config)# console-timeout 30
show system-info	Privileged EXEC	Show system information		switch# show system-info
show ip	Privileged EXEC	Show ip information of switch		switch# show ip
show admin	Privileged EXEC	Show username & password		switch# show admin
show version	Privileged EXEC	Use the show version user EXEC command to display version information for the hardware and firmware.		switch# show version
show terminal	Privileged EXEC	Use the show terminal command to display console information for the switch		switch# show terminal
show fan-status	Privileged EXEC	Use the show fan-status command to display fan status		switch(config)# show fan-status

Port Commands Set

Netstar Commands	Command Level	Description	Default	Example
interface gigaethernet [port ID]	Interface configuration mode	Use the Ethernet interface configuration command		switch(config)# interface gigaethernet 1
		Use the module Ethernet interface configuration command		switch(config)# interface gigaethernet 1
duplex [full half]	Interface configuration mode	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	Auto	switch(config)# interface gigaethernet 1 switch(config-if)# duplex full or switch(config-if)# duplex half
speed [10 100 1000 auto]	Interface configuration mode	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet.		switch(config)# interface gigaethernet 1 switch(config-if)# speed 1000 or switch(config-if)# speed 100 or switch(config-if)# speed 10 or switch(config-if)# speed auto
flowcontrol [enable disable]	Interface configuration mode	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion. Use the no form of this command to disable security on the port. Configure flow control Disable flow control of interface	Off	switch(config)# interface gigaethernet 1 switch(config-if)# flowcontrol enable or switch(config-if)# flowcontrol disable

jumbo [size]	Interface configuration mode	Set jumbo frame size. Use the no form of this command to default value. [Jumbo size must be even and between 1522~10240]	1522	switch(config)# interface gigaethernet 1 switch(config-if)# jumbo 1524 or switch(config-if)# jumbo 10240
rate-limit input-mode {bc mc unkuc kno wnuc} or no rate-limit input-mode {bc mc unkuc kno wnuc}	Interface configuration mode	Set rate-limit input mode. You can enable rate-limit for specific packets such as broadcast, multicast, unknown unicast and known unicast. Use the no form of this command to disable for that packets	Disable	switch(config)# interface gigaethernet 1 switch(config-if)# rate-limit input-mode bc or switch(config-if)# no rate-limit input-mode bc or switch(config-if)# rate-limit input-mode mc or switch(config-if)# no rate-limit input-mode mc
rate-limit input-rate [value]	Interface configuration mode	Set rate-limit input rate value. Input rate limit must be between 1~1526	Disable	switch(config)# interface gigaethernet 1 switch(config-if)# rate-limit input-rate 1000
rate-limit output-mode or no rate-limit output-mode	Interface configuration mode	Set rate-limit output mode. You can enable output rate-limit. Use the no form of this command to disable output rate limit.	Disable	switch(config)# interface gigaethernet 1 switch (config-if)# rate-limit output-mode switch (config-if)# no rate-limit output-mode

rate-limit output-rate [value]	Interface configuration mode	Set rate-limit output rate value. Range is 1~3130 for 312Kbps unit on the port. Output rate limit must be between 1~3130	Disable	switch (config)# interface gigaethernet 1 switch (config-if)# rate-limit output-rate 1000
shutdown or no shutdown	Interface configuration mode	Use the shutdown Interface configuration command to disable the port. Use the no shutdown form of this command to enable the port.	Enable	switch (config)# interface gigaethernet 1 switch(config-if)# shutdown switch(config-if)# no shutdown
show interfaces status [gigaethernet port -channel vlan] [if-num]	Privileged EXEC	Show interface configuration status and configuration.		switch # show interfaces status gigaethernet 1 or switch # show interfaces status port- channel 1 or switch # show interfaces status vlan 1
show interfaces counters [gigaethernet port -channel] [if-num]	Privileged EXEC	Show interface statistic counter.		switch # show interfaces counters gigaethernet 1 or switch # show interfaces counters port-channel 1

Mac / Filter Table Commands Set

Netstar Commands	Command Level	Description	Default	Example
mac-address-table aging-time [sec.] or no mac-address-table aging-time	Global configuration mode	<p>Use the mactbl 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>Range: 0-300 seconds; 0 to disable aging)</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>time must be 20~620 and in steps of 20 seconds</p>	300 secs	(Enable) switch(config)# mac-address-table aging-time 150 (Disable) switch(config)# mac-address-table aging-time 0 (Default) switch(config)# no mac-address-table aging-time
mac-address-table static hwaddr [MAC] vlan [VLAN-ID] or no mac-address-table static hwaddr [MAC] vlan [VLAN-ID]	Interface configuration mode	<p>Configure MAC address table of interface (static)</p> <p>Remove an entry of MAC address table of interface (static)</p>		config)# interface gigaethernet 1 switch(config-if)# mac-address-table static hwaddr 000012345678 vlan 1 or config)# interface gigaethernet 1 switch(config-if)# no mac-address-table static hwaddr 000012345678 vlan 1

mac-address-table filter hwaddr [MAC] vlan [VLAN-ID] or no mac-address-table filter hwaddr [MAC] vlan [VLAN-ID]	Global configuration mode	Configure MAC address table(filter) Remove an entry of MAC address table (filter)		switch(config)# mac-address-table filter hwaddr 000012348678 vlan 1 or switch(config)# no mac-address-table filter hwaddr 000012348678 vlan 1
show mac-address-table [static filter all] or show mac-address-table static or show mac-address-table filter or show mac-address-table all	Privileged EXEC mode	Show static MAC address table Show filter MAC address table. Show all MAC address table		switch# show mac-address-table static or switch# show mac-address-table filter or switch# show mac-address-table all
show mac-address-table aging-time	Privileged EXEC mode	Show current aging time setup		switch# show mac-address-table aging-time

Port Mirroring Commands Set

Netstar Commands	Command Level	Description	Default	Example
monitor [port number] [rx tx both] or no monitor [port number all]	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.		switch(config)#interface gigaethernet 1 switch(config-if)#monitor 3 both or switch(config-if)#no monitor 3 or (Disable) switch(config-if)# no monitor all
show monitor	Privileged EXEC	Show port monitor information		switch#show monitor

TFTP Commands Set

Netstar Commands	Command Level	Description	Default	Example
backup flash:backup_cfg	Global configuration mode	Save configuration to TFTP server and need to specify the IP of TFTP server and the file name of image.		switch(config)# backup flash:backup_cfg
restore flash:restore_cfg	Global configuration mode	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.		switch(config)# restore flash:restore_cfg TFTP server ip address [192.168.10.2]: Restore file name [restore.dat]: *config success.*
upgrade flash:upgrade_fw	Global configuration mode	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.		switch(config)# upgrade lash:upgrade_fw

QOS Commands Set

Netstar Commands	Command Level	Description	Default	Example
show qos	Privileged EXEC	Show QoS settings		switch# show qos
qos priority cos [Cos] [Qid] or no qos priority cos	Global configuration mode	Configure COS Priority	Qid = Traffic Class	switch(config)# qos priority cos 0 2 or (Default) switch(config)# no qos priority cos
qos priority dscp [dscp] [Qid] or no qos priority dscp	Global configuration mode	Set DSCP Map		switch(config)# qos priority dscp 61 5 or (Default) switch(config)# no qos priority dscp
qos priority profile [profile]	Global configuration mode	Set Qos Port Profile [0~3]	0	switch(config)# qos priority profile 3
qos priority portbased [Qid] or no qos priority portbased	Interface configuration mode	Set Qos Port Priority [0~7]	0	switch(config)# interface gigaethernet 1 switch(config-if)# qos priority portbased 3 or (Default) switch(config-if)# no qos priority portbased

qos priority precedence [port-base cos-only dscp-only dscp-first] or no qos priority precedence	Global configuration mode	Set Priority Precedence	Port-base	switch(config)# qos priority precedence port-base or switch(config)# qos priority precedence cos-only or switch(config)# qos priority precedence dscp-only or switch(config)# qos priority precedence dscp-first or (Default) switch(config)# no qos priority precedence
---	----------------------------------	-------------------------	-----------	--

Spanning Tree Commands Set

Netstar Commands	Command Level	Description	Default	Example
show spanning-tree	Privileged EXEC	Display a summary of the spanning-tree states.		switch# show spanning-tree
spanning-tree enable or no spanning-tree	Global configuration mode	Enable/disable spanning tree	Disable	switch(config)# spanning-tree enable or switch(config)# no spanning-tree
spanning-tree priority [0~61440]	Global configuration mode	Use the spanning-tree priority global configuration command to change the priority. Priority must be a multiple of 4096	32768	switch(config)# spanning-tree priority 4096

spanning-tree max-age [6~40seconds]	Global configuration mode	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	20 sec	switch(config)# spanning-tree max-age 15
spanning-tree hello-time [1~10seconds]	Global configuration mode	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	2 sec.	switch(config)# spanning-tree hello-time 3
spanning-tree forward-time [4~30seconds]	Global configuration mode	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.	15 sec.	switch(config)# spanning-tree forward-time 20
stp-port priority [port priority] pathcost [path cost]	Interface configuration mode	Use the stp-port interface configuration command to configure a port priority and path cost that is used when two switches tie for position as the root switch.	128	switch(config)# interface gig Ethernet 1 switch(config-if)# stp-port priority 16 pathcost 200000

stp-admin-p2p [disable enable auto]	Interface configuration mode	Use the stp-admp2p interface configuration command to configure a port AdmP2P variable.	Enable	switch (config)# interface gigaethernet 1 switch(config-if)# stp-admin-p2p auto or switch(config-if)# stp-admin-p2p enable or switch(config-if)# stp-admin-p2p disable
stp-admin-edge [disable enable]	Interface configuration mode	Use the stp-admedge interface configuration command to configure a port AdmEdge variable.	Enable	switch (config)# interface gigaethernet 1 switch(config-if)# stp-admin-edge enable or switch(config-if)# stp-admin-edge disable
stp-admin- stp [disable enable]	Interface configuration mode	Use the stp-admstp interface configuration command to configure a port controlled by stp protocol.	Enable	switch (config)# interface gigaethernet 1 switch(config-if)# stp-admin stp enable

VLAN Commands Set

Netstar Commands	Command Level	Description	Default	Example
vlan database	Privileged EXEC	Enter VLAN configure mode		switch# vlan database switch(vlan)#
vlanmode [portbase 802.1q gvrp]	VLAN database mode	To set switch VLAN mode.	8021q	switch(vlan)# vlanmode portbase or switch(vlan)# vlanmode 802.1q or switch(vlan)# vlanmode gvrp
show vlan or	VLAN database	Show VLAN information		switch(vlan)# show vlan

show vlan [GroupName] VLAN ID]	mode			or switch(vlan)# show vlan 2
Port Base VLAN mode				
no vlan group [VLAN ID]	VLAN database mode	Delete port base group ID		switch(vlan)# no vlan group 2
vlan port-based grpname [Group Name] grp id [VLAN ID] port [PortNumbers]	VLAN database mode	Add new port based VALN		switch(vlan)# vlan port-based grpname test grp id 2 port 2-4 or switch(vlan)# vlan port-based grpname test grp id 2 port 2,3,4
802.1Q 802.1Q with GVRP VLAN mode*				
vlan 8021q name [GroupName] vid [VLAN ID] media gigaethernet state active or no vlan 8021q [VLAN ID]	VLAN database mode	Change the name of VLAN group, if the group didn't exist, this command can't be applied. or Delete port base group ID		switch(vlan)# vlan 8021q name RD vid 2 media gigaethernet state active or switch(vlan)# no vlan 8021q 2

switchport allowed vlan 8021q add [VLAN ID] [tagged untagged] or switchport allowed vlan 8021q remove [VLAN ID] or no switchport allowed vlan8021q	Interface configuration mode	Add port to the VLAN Remove port to the VLAN Remove port from all VLAN except default VLAN		switch(config)# interface gigaethernet 1 switch(config-if)# switchport allowed vlan 8021q add 2 tagged or switch(config-if)# switchport allowed vlan 8021q remove 2 or switch(config-if)# no switchport allowed vlan 8021q
switchport native vlan [PVID] or no switchport native vlan	Interface configuration mode	Set Port PVID	1	switch(config)# interface gigaethernet 1 switch(config-if)# switchport native vlan 2 or switch(config-if)# no switchport native vlan
switchport acceptable-frame- types [all tagged] or no switchport acceptable-frame- types	Interface configuration mode	Set accept frame type	all	switch(config)# interface gigaethernet 1 switch(config-if)# switchport acceptable-frame-types all or switch(config-if)# no switchport acceptable-frame-types

switchport ingress-filtering or no switchport ingress-filtering	Interface configuration mode	Set ingress filter	disable	switch(config)# interface gigaethernet 1 switch(config-if)# switchport ingress-filtering or switch(config-if)# no switchport ingress-filtering
show vlan [id name] [VLAN ID Name]	Privileged EXEC	Show VLAN of Group Name or VLAN ID information vlanid: 1 ~ 4094		switch# show vlan id
show interfaces switchport [gigaethernet port -channel] [port]	Privileged EXEC	show Port PVID and ingress filter & accept frame type		switch# show interfaces switchport gigaethernet 1

*Future Release

System log Commands Set

Netstar Commands	Command Level	Description	Default	Example
show logging [flash ram sendmail trap map]	Privileged EXEC	Show system log information		switch# show logging flash
logging-mode {local remote smtp } or no logging-mode {local remote smtp }	Global configuration mode	Enable logging mode for local, remote and smtp		Switch(config)# logging-mode local Switch(config)# no logging-mode local Switch(config)# logging-mode remote

logging-local history [flash ram] [level] or no logging-local history [flash ram]	Global configuration mode	Set system log level	Flash:3(level 3-0) RAM:7(level 7-0)	Switch(config)# logging-local history flash 3
logging-events [coldstart warmstart authfailure portlinkchange] [level] or no logging-events [coldstart warmstart authfailure portlinkchange]	Global configuration mode	Set the level of each logging events.	Level 7	Switch(config)# logging-events coldstart 3 Switch(config)# no logging-events coldstart
Logging-host [server] or no logging-host [server]	Global configuration mode	Add or delete the remote server address		Switch(config)# logging-host 192.168.10.5 Switch(config)# no logging-host 192.168.10.5
logging facility [value] or no logging facility	Global configuration mode	Set system log facility	23	Switch(config)# logging facility 19 Switch(config)# no logging facility

logging trap [value] or no logging trap	Global configuration mode	Set system log trap	7	Switch(config)# logging trap 4 Switch(config)# no logging trap 4
clear logging-local [flash ram]	Global configuration mode	Clear system log buffer		Switch(config)# clear logging-local flash
logging sendmail {host-0 host-1} [server] or no logging sendmail {host-0 host-1}	Global configuration mode	Set the SMTP server address		Switch(config)# logging sendmail host-0 192.168.10.5 Switch(config)# no logging sendmail host-0 192.168.10.5
logging sendmail level [value] or no logging sendmail level	Global configuration mode	Set system log SMTP level	7	Switch(config)# logging sendmail level 4 Switch(config)# no logging sendmail level 4
logging sendmail {src-0 src-1} [email addr] or no logging sendmail {src-0 src-1}	Global configuration mode	Set system log SMTP source-email address		Switch(config)# logging sendmail src-0 bill@this-company.com Switch(config)# no logging sendmail src-0 bill@this-company.com

logging sendmail {dst-0 dst-1} [email addr] or no logging sendmail {dst-0 dst-1} [email addr]	Global configuration mode	Add or delete system log SMTP destination-email address		Switch(config)# logging sendmail dst-0 bill@this-company.com Switch(config)# no logging sendmail dst-0 bill@this-company.com
logging sendmail service or no logging sendmail service	Global configuration mode	Enable or disable system log SMTP	Disable	Switch(config)# logging sendmail service Switch(config)# No logging sendmail service

SNTP Commands Set

Netstar Commands	Command Level	Description	Default	Example
calendar set [hour] [min] [sec] [day] [mon] [year]	Global configuration mode	Set system time		switch(config)# calendar set 15 03 30 29 4 2006
sntp timezone hours [hours] minute [min] [after-UTC before-UTC]	Global configuration mode	Set timezone index, use “show sntp timezone” command to get more information of index number		switch(config)# sntp timezone hours 9 minute 0 after-UTC
show sntp timezone	Privileged EXEC	Show index number of time zone list		switch# show sntp timezone
no sntp timezone	Global configuration mode	Set system time zone to default	(GMT+08:00)	switch(config)# no sntp timezone
show sntp	Privileged EXEC	Show system time configuration.		switch# show sntp

sntp server [ipaddr]	Global configuration mode	Set SNTP server IP address.		switch(config)# sntp server 192.168.10.5
no sntp server	Global configuration mode	Set SNTP server IP address to default.	NULL	switch(config)# no sntp server
sntp enable	Global configuration mode	Enable SNTP Client.		switch(config)# sntp enable
no sntp	Global configuration mode	Disable SNTP Client.		switch(config)# no sntp
sntp poll [sec]	Global configuration mode	Set SNTP client polling interval seconds.	16	switch(config)# sntp poll 60
no sntp poll	Global configuration mode	Set SNTP client polling interval seconds to default.		switch(config)# no sntp poll

IGMP Commands Set

Netstar Commands	Command Level	Description	Default	Example
igmp enable	Global configuration mode	Enable IP IGMP Snooping service.	disable	switch(config)# igmp enable
no igmp	Global configuration mode	Disable IP IGMP Snooping service to default disable.		switch(config)# no igmp
igmp-query {enable disable auto}	Global configuration mode	Set IP IGMP query mode.	disable	switch(config)# igmp-query auto

igmp vlan [vid] static [ipaddr] [gigaethernet port -channel] [port]	Global configuration mode	Adds a static multicast group and its member port.		switch(config)# igmp vlan 1 static 224.0.0.251 gigaethernet 1
no igmp vlan [vid] static [ipaddr] [gigaethernet port -channel] [port]	Global configuration mode	Remove a static multicast group and its member port.		switch(config)# no igmp vlan 1 static 224.0.0.251 gigaethernet 1
show igmp configuration	Privileged EXEC	Displays the details of an IGMP configuration		switch# show igmp configuration
show mactbl multicast vlan [vid]	Privileged EXEC	Shows known multicast addresses for specific VLAN Id.		switch#show mactbl multicast vlan 1
show mactbl multicast [user igmp-snooping]	Privileged EXEC	Shows known multicast addresses only the user-configured multicast entries or only entries learned through IGMP snooping.		switch#show mactbl multicast user

TRUNK Commands Set

Netstar Commands	Command Level	Description		Example
interface port-channel [group id]	Global configuration mode	Configures a trunk and enters interface configuration mode for the trunk. If the trunk group isn't exist, you should create it by add a member port		switch(config)# interface port-channel 1
no interface port-channel [group id]	Global configuration mode	Delete the trucking group.		switch(config)# no interface port-channel 1

trunk mode [lacp static] or no trunk mode	Interface configuration mode	Configure the mode of the trunk group.	static	switch(config)# interface port-channel 1 switch(config-if)# trunk mode static or switch(config-if)# no trunk mode
channel-group [group id]	Interface configuration mode	Adds a port to a trunk. If the trunk group doesn't exist, it will create the group.		switch(config)# interface gigaethernet 1 switch(config-if)# channel-group 1
no channel-group	Interface configuration mode	Remove a port from a trunk.		switch(config)# interface gigaethernet 1 switch(config-if)# no channel-group 1
show interfaces status port-channel [group id]	Privileged EXEC	Shows trunk information		switch# show interfaces status port-channel 1
show port activity	Privileged EXEC	Show lacp port activity information	active	switch# show port activity
port {active passive}	Interface configuration mode	Set port active passive		switch(config)# interface gigaethernet 1 switch(config-if)# port passive

SNMP Commands Set

Netstar Commands	Command Level	Description	Default	Example
snmp name [station name]	Global configuration mode	Configure station name.		switch(config)# snmp name station1
snmp location [station location]	Global configuration mode	Configure station location.		switch(config)# snmp location Taiwan
snmp contact [station contact]	Global configuration mode	Configure station contact.		switch(config)# snmp contact support@netstar.com
snmp community-string s [Community] right [RO/RW]	Global configuration mode	Add SNMP community string.	public, private	switch(config)# snmp community-strings public right rw
no snmp community-string s [Community]	Global configuration mode	Remove the specified community.		switch(config)# no snmp community-strings public
snmp-server host [IP address] community [Community-string]	Global configuration mode	Configure SNMP trap manager information and community string		switch(config)# snmp-server host 192.168.1.50 community public
no snmp-server host [Host-address]	Global configuration mode	Remove the SNMP server host.		switch(config)# no snmp-server host 192.168.1.50
show snmp	Privileged EXEC	Show snmp configuration		switch# show snmp

DHCP Server Commands Set

Netstar Commands	Command Level	Description		Example
dhcpserver [ip start] [ip number]	Global configuration mode	Enable dhcp server and add lease entry.		switch(config)# dhcpserver 192.168.1.5 5 Netmask [255.255.255.0]: 255.255.255.0 Gateway [192.168.10.254]: 192.168.10.254 DNS [192.168.10.254]: 192.168.10.254 Lease Duration [24](hours) 24
no dhcpserver	Global configuration mode	Disable dhcp server.		switch(config)# no dhcpserver
show dhcpserver	Privileged EXEC	Show configuration of dhcp server and client status.		switch# show dhcpserver

Security IP Commands Set

Netstar Commands	Command Level	Description	Default	Example
security [entry id] ip [ip address] http [on/off] telnet [on/off]	Global configuration mode	Enable and add security ip. Entry id: 1 - 10		switch(config)# security 1 ip 192.168.10.5 http on telnet on
no security	Global configuration mode	Disable IP security function		switch(config)# no security
show security	Privileged EXEC	Show the information of IP security		switch# show security

802.1X Commands Set

Netstar Commands	Command Level	Description		Example
8021x enable	Global configuration mode	Use the 802.1x global configuration command to enable 802.1x protocols.	Disable	switch(config)# 8021x enable
8021x misc quietperiod [sec.]	Global configuration mode	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	60	switch(config)# 8021x misc quietperiod 10
8021x misc txperiod [sec.]	Global configuration mode	Use the 802.1x misc TX period global configuration command to set the TX period.	30	switch(config)# 8021x misc txperiod 5
8021x misc supportimeout [sec.]	Global configuration mode	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	30	switch(config)# 8021x misc supportimeout 20
8021x misc servertimeout [sec.]	Global configuration mode	Use the 802.1x misc server timeout global configuration command to set the server timeout.	30	switch(config)# 8021x misc servertimeout 20
8021x misc maxrequest [number]	Global configuration mode	Use the 802.1x misc max request global configuration command to set the MAX requests.	2	switch(config)# 8021x misc maxrequest 3
8021x misc reauthperiod [sec.]	Global configuration mode	Use the 802.1x misc reauth period global configuration command to set the reauth period.	3600	switch(config)# 8021x misc reauthperiod 3000
8021x portstate [disable reject accept authorize]	Interface configuration mode	Use the 802.1x port state interface configuration command to set the state of the selected port.	Disable	switch(config)# interface gigaethernet 1 switch(config-if)# 8021x portstate accept

show 8021x	Privileged EXEC	Displays a summary of the 802.1x properties and also the port status.		switch# show 8021x
8021x system radiusip [IP address]	Global configuration mode	Use the 802.1x system radius IP global configuration command to change the radius server IP.		switch(config)# 8021x system radiusip 192.168.1.1
8021x system serverport [port ID]	Global configuration mode	Use the 802.1x system server port global configuration command to change the radius server port		switch(config)# 8021x system serverport 1815
8021x system accountport [port ID]	Global configuration mode	Use the 802.1x system account port global configuration command to change the accounting port		switch(config)# 8021x system accountport 816
8021x system sharekey [ID]	Global configuration mode	Use the 802.1x system share key global configuration command to change the shared key value.		switch(config)# 8021x system sharekey 123456

LLDP Commands Set

Netstar Commands	Command Level	Description	Default	Example
lldp [enable] or no lldp	Global configuration mode	Enable or disable LLDP protocol.	Disable	switch(config)# lldp enable or switch(config)# no lldp
show lldp status	Privileged EXEC	Show LLDP status.		switch# show lldp status
show lldp remote	Privileged EXEC	Show LLDP remote table.		switch# show lldp remote

lldp-port [disable rx tx both]	Interface configuration mode	Use those commands to set lldp port tx and rx mode.	Disable	switch(config)# interface gigaethernet 1 switch(config-if)# lldp-port disable or switch(config-if)# lldp-port rx
--	---	--	---------	--

ACL Commands Set

Netstar Commands	Command Level	Description	Defaults	Example
acl-port [deny permit] or no acl-port	Interface configuration mode	Use the acl-port interface configuration command to enable Access Control on a port. The default action can be Deny or Permit. Use the no form of this command to return the port to its default value (disable).	Disable	switch(config)# interface gigaethernet 1 switch(config-if)# acl-port deny or switch(config-if)# no acl-port
acl-rule [index] dst [dstIp/prefix] src [srcIp/prefix] {deny permit} or no acl-rule [index]	Interface configuration mode	Use those commands to add or delete the acl rules of the port. [index] range= 0~4	N/A	switch(config)# interface gigaethernet 1 switch(config-if)# acl-rule 0 dst 192.168.10.1/32 src 192.168.10.2/32 permit or switch(config-if)# no acl-rule 0
show acl [gigaethernet port -channel]][port]	Privileged EXEC	Show acl configuration of the port.	N/A	switch# show acl gigaethernet 1

ComNet Customer Service

Customer Care is ComNet Technology's global service center, where our professional staff are ready to answer your questions at any time. Email address of ComNet Global Service Center: customercare@ComNet.net



World Headquarters

3 Corporate Drive
Danbury, CT 06810 USA
T 203 796-5300
F 203 796-5303
888 678-9427 Tech Support
info@ComNet.net

ComNet Europe Ltd

8 Turnberry Park Road
Gildersome, Morley
Leeds, LS27 7LE, UK
T +44 (0)113 307 6400
F +44 (0)113 253 7462
info-europe@ComNet.net

© 2010 Communication Networks. All rights reserved.

The COMNET logo is a registered trademark of Communication Networks Corporation.
Additional Company and product names may be trademarks or registered trademarks of the individual companies and are respectfully acknowledged and do not imply endorsement.