comnet
Communication Networks

INSTALLATION AND OPERATION MANUAL

CNGE5MS

ENVIRONMENTALLY HARDENED MANAGED ETHERNET SWITCH WITH (3) 10/100/1000BASE-TX & (2) 10/100/1000BASE-TX/FX COMBO PORTS

v1.4 February 21, 2013

The ComNet™ CNGE5MS is a hardened, industrial five port all gigabit managed Ethernet switch. It has three 10/100/1000Base-TX and two Gigabit combo ports that utilize ComNet Small Form Factor (SFP) pluggable modules for the selection of fiber and connector type and distance. The IEEE 802.3 compliant unit is a redundant switch offering multiple Ethernet redundancy protocols, C-Ring, ComRing, C-RSTP and MSTP/RSTP/STP. This redundancy feature protects your applications from network interruptions or temporary malfunctions by redirecting transmission within the network. The CNGE5MS offers centralized and convenient management through a windows-based utility called eConsole. Redundant DC power inputs provide non-stop operation in case of power supply disruption. The backup power input will take over immediately when the primary DC power input fails. The unit provides relay outputs that can be set up to indicate events and notify in case of potential problems.

Contents

Regulatory Compliance Statement

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

Warranty

ComNet warrants that all ComNet products are free from defects in material and workmanship for a specified warranty period from the invoice date for the life of the installation. ComNet will repair or replace products found by ComNet to be defective within this warranty period, with shipment expenses apportioned by ComNet and the distributor. This warranty does not cover product modifications or repairs done by persons other than ComNet-approved personnel, and this warranty does not apply to ComNet products that are misused, abused, improperly installed, or damaged by accidents.

Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

Disclaimer

Information in this publication is intended to be accurate. ComNet shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ComNet reserves the right to revise the contents of this publication without notice.

Safety Indications

» The equipment can only be accessed by trained ComNet service personnel.

» This equipment should be installed in secured location.

Overview

Introduction

The CNGE5MS is a powerful, managed, hardened Ethernet switch that contains many features. The switch will work under a wide variety of temperature, dirty and humid conditions. It can be managed through WEB, TELNET, Consol or other third-party SNMP software. The CNGE5MS also can be managed by a utility called eConsole.

eConsole is network management software that is very effective. With easy to use and intuitive interface, you can easily configure multiple switches at the same time, and monitor the status of those switches.

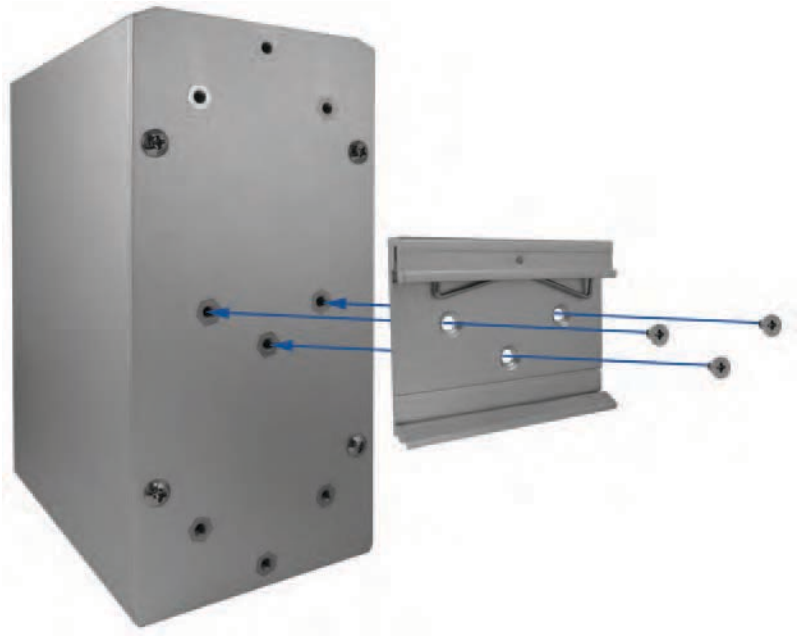
Software Features

» Fast Redundant Ethernet Ring : C-Ring Technology (Recovery time < 20ms over 250 units connection)
» Supports Ring Coupling, Dual Homing over C-Ring
» Supports SNMPv1/v2c/v3 & RMON & Port base/802.1Q VLAN Network Management
» Event notification by Email, SNMP trap and Relay Output
» Web-based ,Telnet, Console, CLI configuration
» Enable/disable ports, MAC based port security
» Port based network access control (802.1x)
» VLAN (802.1q) to segregate and secure network traffic
» Radius centralized password management
» SNMPv3 encrypted authentication and access security
» RSTP (802.1w)
» Quality of Service (802.1p) for real-time traffic
» VLAN (802.1q) with double tagging and GVRP supported
» IGMP v2/v3 (support IGMP Snooping) for multicast filtering
» Port configuration, status, statistics, mirroring, security
» Remote Monitoring (RMON)

Hardware Features

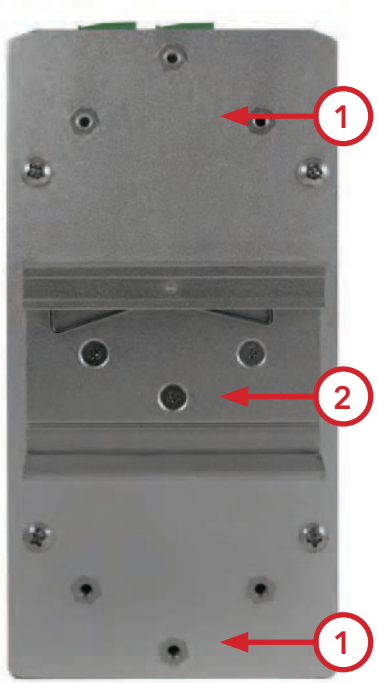
» 3 × Redundant DC power inputs
» Operating Temperature: -40 – 75°C
» Storage Temperature: -40 – 85°C
» Operating Humidity: 5% – 95%, non-condensing
» Casing: IP-30
» 3 × 10/100/1000Base-T(X) Gigabit Ethernet port
» 2 × 100/1000Base-X SFP & 10/100/1000Base-TX Combo ports
» Console Port
» Dimensions (W × D × H): 54.1 × 106.1 × 145.4mm
(2.13 × 4.18 × 5.72in)

Installing Switch on DIN-Rail



The rear panel components of CNGE5MS shown below:

1. Screw holes for wall mount kit.
2. Din-Rail kit

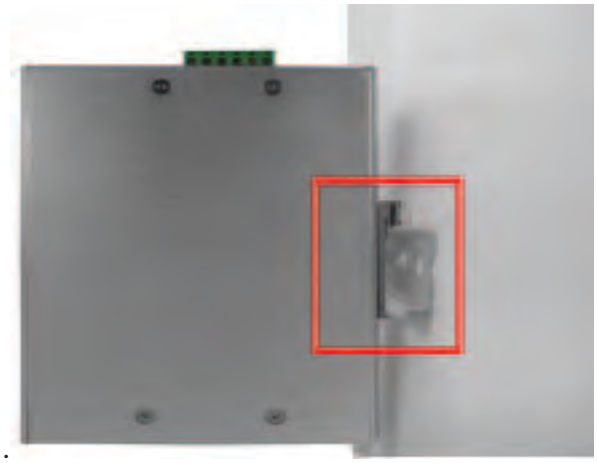


Each switch has a DIN-Rail kit on the rear panel. The DIN-Rail kit affixes the switch to the DIN-Rail. It is easy to install the switch on the Din-Rail:

Mount Series on DIN-Rail

Step 1: Tilt the switch and mount the metal spring to DIN-Rail.

Step 2: Push the switch toward the DIN-Rail until you hear the spring snap into place



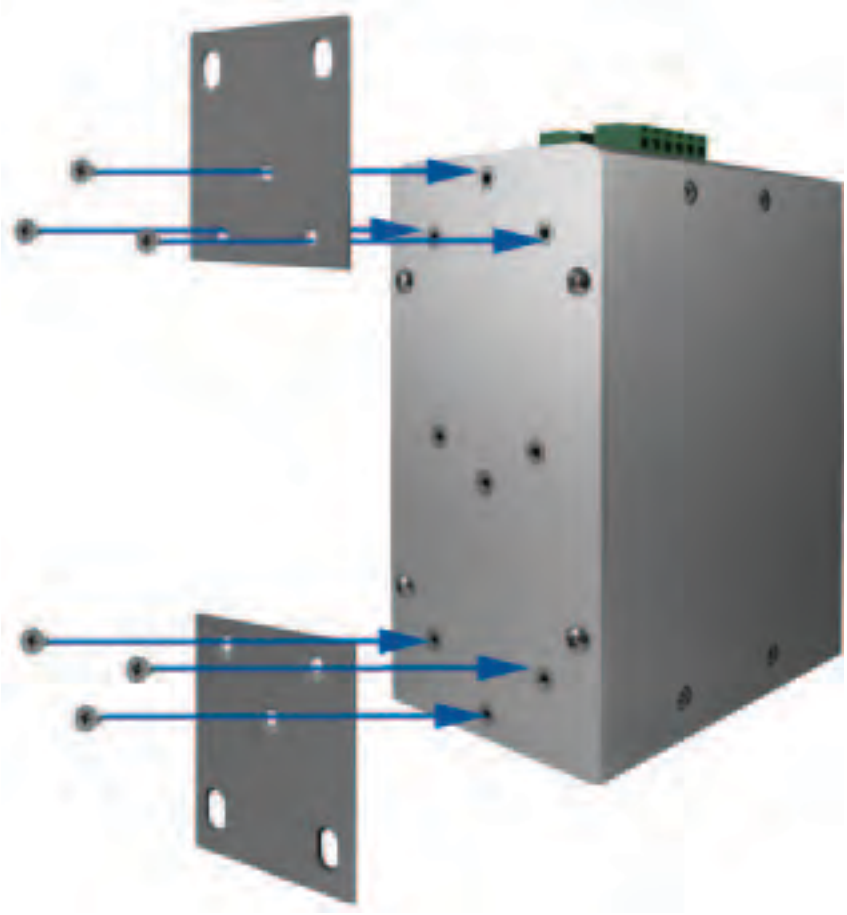
Wall Mounting Installation

Each switch has another installation method for users to install the switch. A wall mount kit can be found in the package. The following steps show how to mount the switch on the wall:

Mounting the CNGE5MS on a Wall

Step 1: Remove DIN-Rail kit if it is attached to the switch.

Step 2: Use the 6 included screws to attach the wall mount panel as shown in the diagram below.



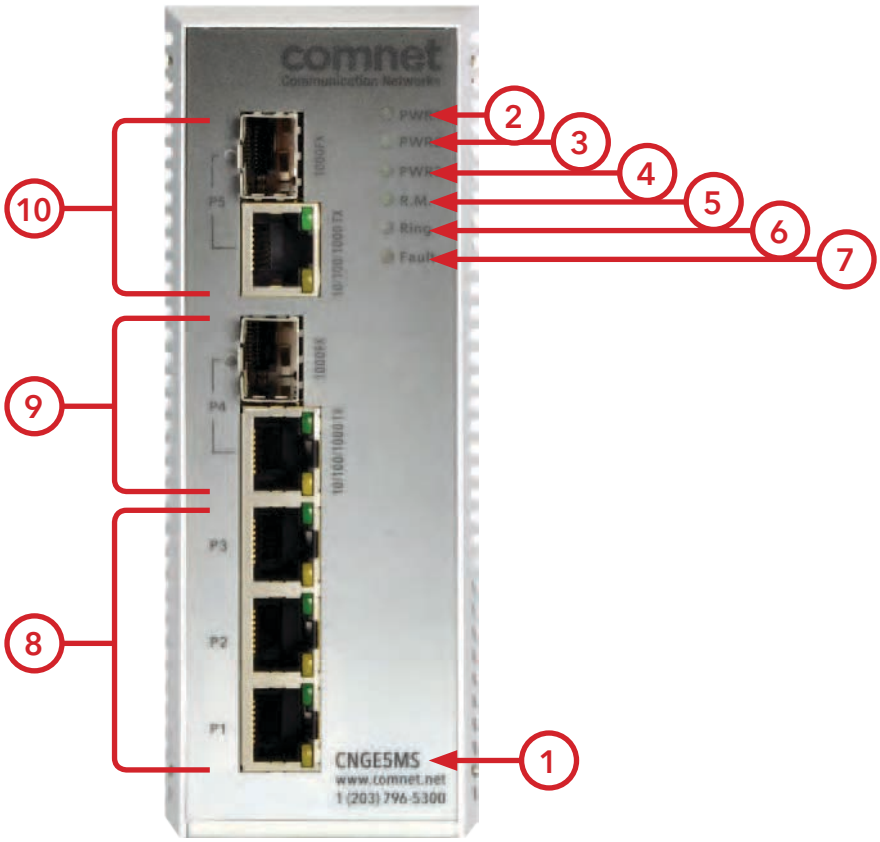
In order to prevent switches from being damaged, use only the screws included with the mounting kit for the CNGE5MS switch.

Hardware Overview

Front Panel

The following table describes the LEDs and ports that are on the front of the CNGE5MS.

Port	Description
10/100/1000Base-T(X) RJ-45 fast Ethernet ports	3 × 10/100/1000Base-T(X) RJ-45 fast Ethernet ports support auto-negotiation. Default Settings: Speed: auto Duplex: auto Flow control: disable
Combination Port	2 × 100/1000Base-X SFP and 2x10/100/1000Base-T(X) ports
Console	Use RS-232 with RJ-45 connecter to manage switch.



CNGE5MS Front Panel

1. Model name
2. LED for PWR1. When the PWR1 UP, the green LED will be light on
3. LED for PWR2. When the PWR2 UP, the green LED will be light on.
4. LED for PWR3. When the PWR3 UP, the green LED will be light on.
5. LED for R.M (Ring Master). When the LED light is on, it means that the switch is the ring master of Ring.
6. LED for Ring. When the LED light on, it means the C-Ring is activated.
7. LED for Fault. When the light on, it means Power failure or Port down/fail.
8. 10/100/1000 Base-T(X) Ethernet ports (RJ-45)
9. 100/1000Base-X SFP port (combo port)
10. 10/100/1000 Base-T(X) Ethernet port (combo port)

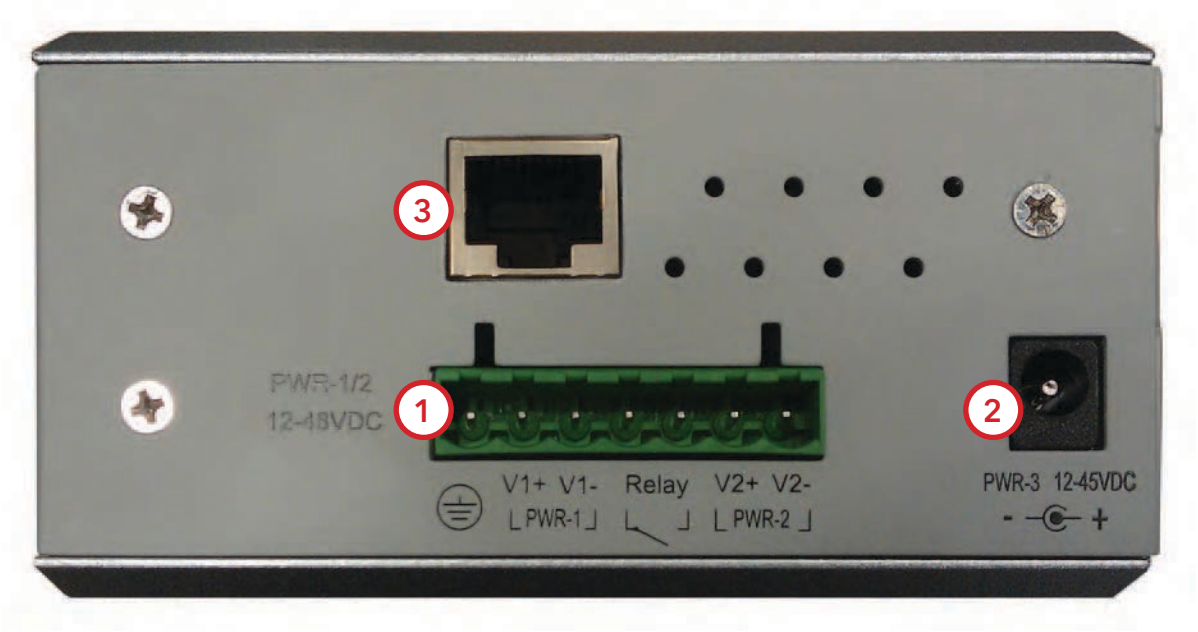
Front Panel LEDs

LED indicators

LED	Color	Status	Description
PWR1	Green	On	DC power module 1 activated
PWR2	Green	On	DC power module 2 activated
PWR3	Green	On	DC Power module 3 activated
R.M	Green	On	Ring Master.
Ring	Green	On	Ring enabled.
		Slowly blinking	Ring has only One link. (lack of one link to build the ring.)
Fault	Amber	On	Fault relay. Power failure or Port down/ fail.
10/100/1000Base-T(X) Ethernet ports			
LNK/ACT	Green	On	Port link up.
		Blinking	Data transmitted.
100Mbps indicator	Amber	On	Port speed is 100Mbps
SFP			
LNK/ACT	Green	On	Port link up.
		Blinking	Data transmitted.

Bottom Panel

The bottom panel of CNGE5MS is displayed as below:



CNGE5MS Rear Panel

1. Terminal block includes: PWR1, PWR2 (12-48V DC) and Relay output (1A@24VDC).
2. Power jack for PWR3 (12-45VDC).
3. Console port (RJ-45).

Cables

Ethernet Cables

The CNGE5MS switches have standard Ethernet ports. According to the link type, the switches use CAT 3, 4, 5, & 5e UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

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

10/100/1000BASE-T(X) Pin Assignments

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

10/100 Base-T RJ-45 Pin Assignments

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

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

1000 Base-T RJ-45 Pin Assignments

Pin Number	Assignment
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-

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

The CNGE5MS switches support auto MDI/MDI-X operation. You can use a straight-through cable to connect PC to switch. The following table below shows the 10/100BASE-T(X) MDI and MDI-X port pin-outs:

10/100 Base-T MDI/MDI-X pin assignments

Pin Number	MDI port	MDI-X port
1	TD+ (transmit)	RD+ (receive)
2	TD- (transmit)	RD- (receive)
3	RD+ (receive)	TD+ (transmit)
4	Not used	Not used
5	Not used	Not used
6	RD- (receive)	TD- (transmit)
7	Not used	Not used
8	Not used	Not used

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

1000 Base-T MDI/MDI-X pin assignments

Pin Number	MDI port	MDI-X port
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

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

SFP

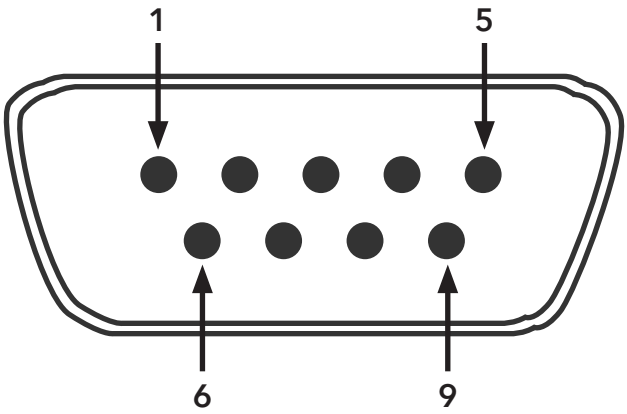
The Switch has fiber optic ports that utilize SFP connectors. ComNet offers a wide selection of SFP modules that offer different fiber type, connector type and distances. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.

Switch A *Fiber Cord* *Switch B*

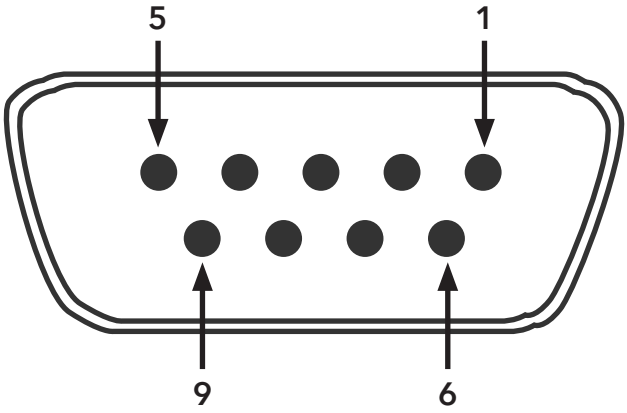
Console Cable

Each CNGE5MS switch can be managed by its console port. You can connect them to PC via an RJ-45 cable with DB-9 female connector.

PC pin out (male) assignment	RS-232 with DB9 female connector	DB9 to RJ 45
Pin #2 RD	Pin #2 TD	Pin #2
Pin #3 TD	Pin #3 RD	Pin #3
Pin #5 GD	Pin #5 GD	Pin #5



DB-9 Male



DB-9 Female

Pin	Male Connector	Female Connector
1	Received Line Signal Detect (Received by DTE Device)	Received Line Signal Detect (Transmitted from DCE Device)
2	Received Data (Received by DTE Device)	Transmitted Data (Transmitted from DCE Device)
3	Transmitted Data (Transmitted from DTE Device)	Received Data (Received by DCE Device)
4	DTE Ready (Transmitted from DTE Device)	DTE Ready (Received by DCE Device)
5	Signal Ground	Signal Ground
6	DCE Ready (Received by DTE Device)	DCE Ready (Transmitted from DCE Device)
7	Request to Send (Transmitted from DTE Device)	Clear to Send (Received by DCE Device)
8	Clear to Send (Received by DTE Device)	Request to Send (Transmitted from DCE Device)
9	Ring Indicator (Received by DTE Device)	Ring Indicator (Transmitted from DCE Device)

WEB Management

Attention: While installing and upgrading firmware, please remove physical loop connection first. DO NOT power off equipment while the firmware is upgrading!

Configuration by Web Browser

This section provides instruction on configuration through the Web browser.

About Web-based Management

An embedded HTML web site resides in the flash memory on the CPU board. It contains advanced management features and allows you to manage the switch from anywhere on the network through a standard web browser such as Microsoft Internet Explorer.

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

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

Preparing for Web Management

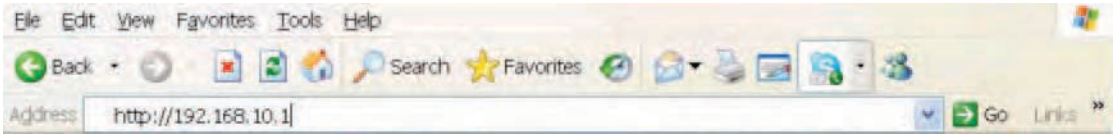
The default value is as below:

IP Address: 192.168.10.1
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.10.254
User Name: admin
Password: admin

System Login

1. Launch your Web Browser.

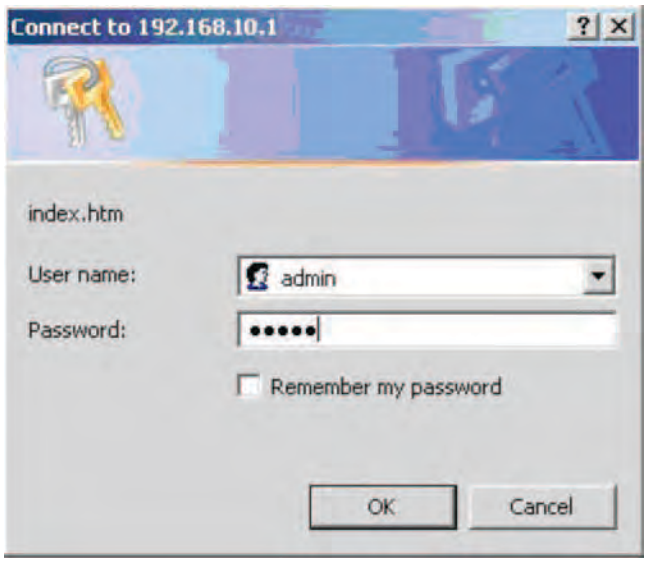
2. Type http:// and the IP address of the switch. Press **Enter**.



3. The login screen appears.

4. Enter username and password. The default username and password is **admin**.

5. Select **Enter** or **OK** button, then the main interface of the Web-based management appears.



Login screen

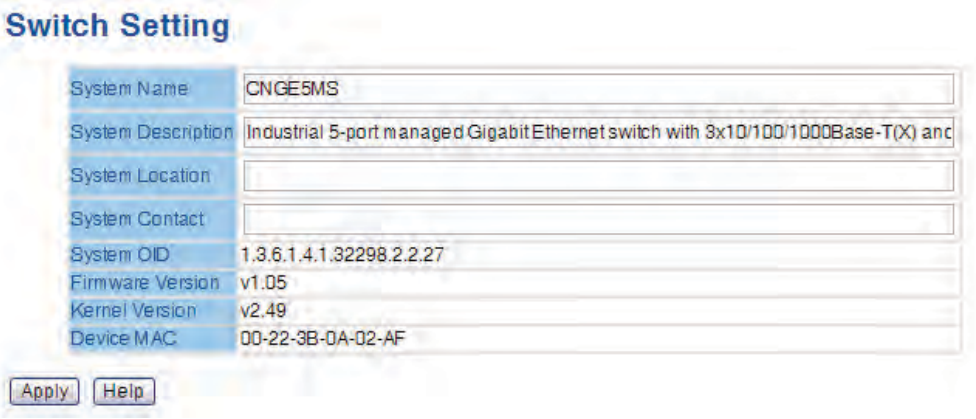
Main Interface

Main interface

Basic Setting

System Information

The switch system information is provided here.

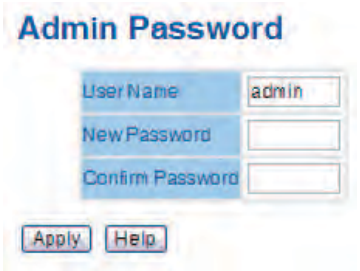


System Information interface

Label	Description
System Name	Assign the name of switch. The maximum length is 64 bytes
System Description	Display the description of switch.
System Location	Assign the switch physical location. The maximum length is 64 bytes
System Contact	Enter the name of contact person or organization
Firmware Version	Display the switch's firmware version
Kernel Version	Display the kernel software version
MAC Address	Display the unique hardware address assigned by manufacturer (default)

Admin & Password

This page allows you to configure the system password that is required to access the web pages or log in from CLI.



Label	Description
User name	Key in the new username (The default is **admin**)
New Password	Key in the new password (The default is **admin**)
Confirm password	Re-type the new password.
Apply	Select **Apply** to set the configurations.

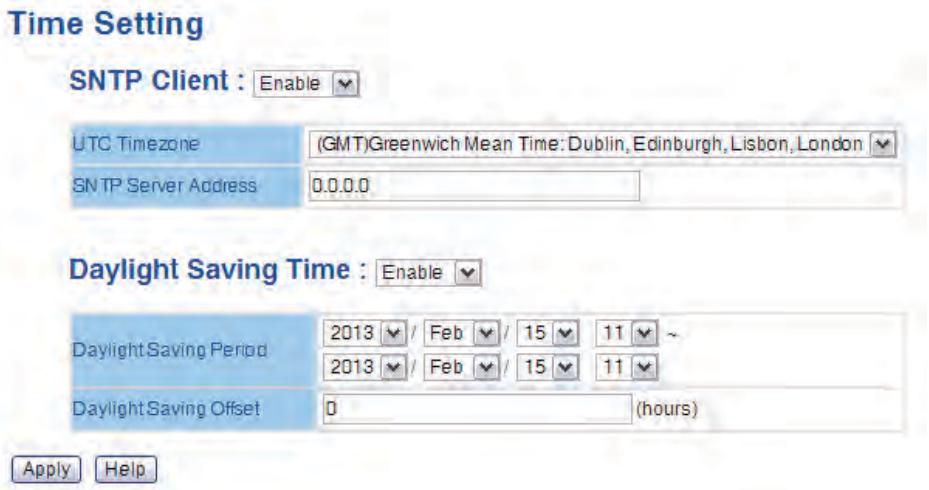
IP Setting

Configure the switch-managed IP information on this page.

Label	Description
DHCP Client	To enable or disable the DHCP client function. When DHCP client function is enabled, the switch will be assigned the IP address from the network DHCP server. The default IP address will be replaced by the IP address which the DHCP server has assigned. After selecting the **Apply** button, a popup dialog will appear to inform you that the DHCP client is enabled. The current IP will be lost and you should find a new IP address on the DHCP server.
IP Address	Assign the IP address that the network is using. If DHCP client function is enabled, you do not need to assign the IP address. The network DHCP server will assign the IP address for the switch and it will be displayed in this column. The default IP is 192.168.10.1
Subnet Mask	Assign the subnet mask of the IP address. If DHCP client function is enabled, you do not need to assign the subnet mask
Gateway	Assign the network gateway for the switch. The default gateway is 192.168.10.254
DNS1	Assign the primary DNS IP address
DNS2	Assign the secondary DNS IP address
Apply	Select **Apply** to set the configurations.

SNTP

The SNTP (Simple Network Time Protocol) settings allow you to synchronize switch clocks with the Internet.



SNTP Configuration interface

The following table describes the labels in this screen.

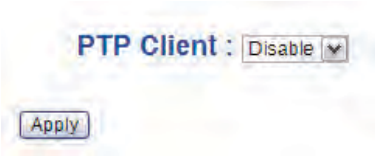
Label	Description
SNTP Client	Enable or disable SNTP function to get the time from the SNTP server.
UTC Time zone	Set the switch location time zone.
SNTP Server IP Address	Set the SNTP server IP address.
Daylight Saving Time	Enable or disable daylight saving time function. When daylight saving time is enabled, you need to configure the daylight saving time period.
Daylight Saving Period	Set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different each year.
Daylight Saving Offset	Set up the offset time.
Apply	Select **Apply** to set the configurations.

The following table lists the different location time zones for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11 am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

PTP Client

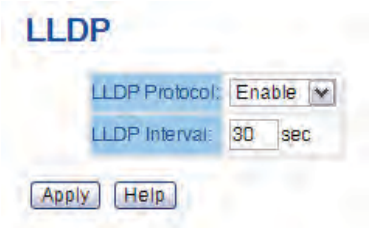
The Precision Time Protocol (PTP) is a time-transfer protocol defined in the IEEE 1588-2002 standard that allows precise synchronization of networks (e.g., Ethernet). Accuracy within the nanosecond range can be achieved with this protocol when using hardware generated timestamps.



Label	Description
PTP Client	Enable / Disable PTP Client

LLDP

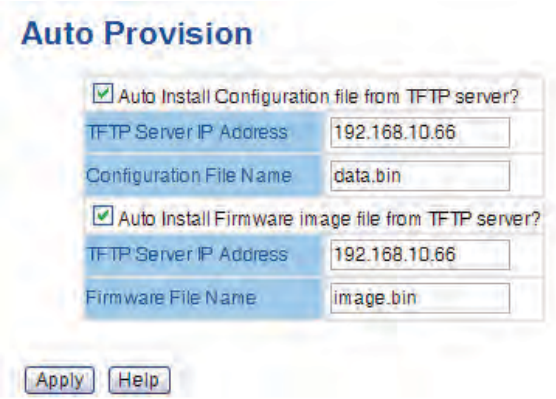
LLDP (Link Layer Discovery Protocol) function allows the switch to advertise its information to other nodes on the network and store the information it discovers.



LLDP configuration interface

Auto Provision

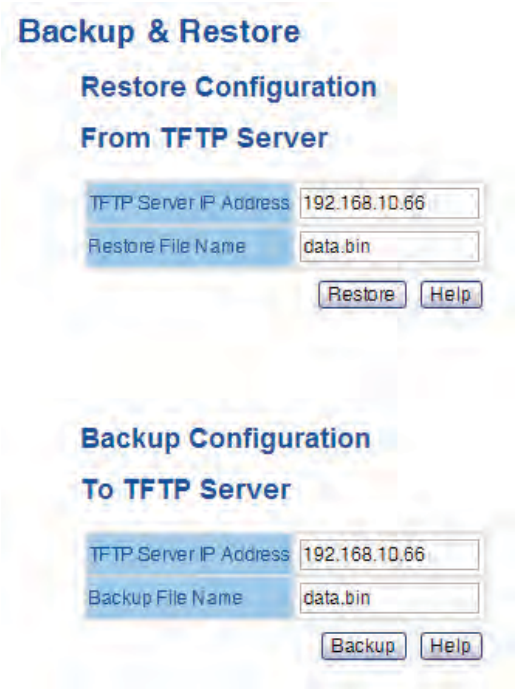
Auto Provision allows you to update the switch firmware automatically. You can put firmware or configuration files on the TFTP server. When you reboot the switch, it will upgrade automatically. Before updating, make sure you have your TFTP server ready and the firmware image and configuration file is on the TFTP server.



Auto Provision interface

Backup & Restore

You can save current configuration from the switch to a TFTP server, or restore the configuration from TFTP server in this page.



Backup & Restore interface

The following table describes the labels in this screen.

Label	Description
TFTP Server IP Address	Fill in the TFTP server IP
Restore File Name	Fill in the file name
Restore	Restore the configurations
Restore File Name	Fill the file name
Restore	Restore the configurations
Backup	Backup the configurations

Upgrade Firmware

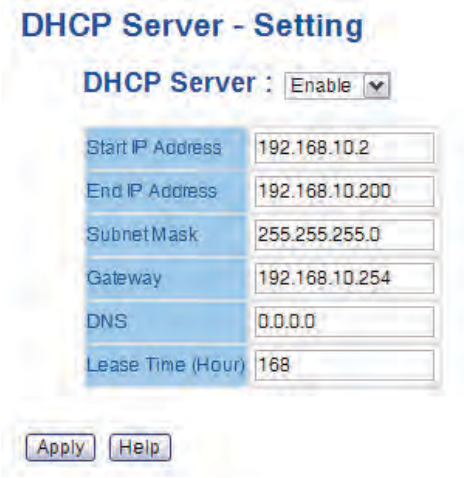
Upgrade Firmware allows you to update the firmware of the switch. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server.

Update Firmware interface

DHCP Server

Setting

The system provides DHCP server function. Enable the DHCP server function to use the switch as a DHCP server.



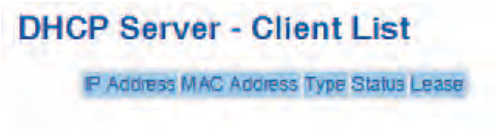
DHCP Server Configuration interface

The following table describes the labels in this screen.

Label	Description
DHCP Server	Enable or Disable the DHCP Server function. When enabled, the switch will be the DHCP server on your local network
Start IP Address	The dynamic IP assigned range. A low IP address is the beginning of the assigned dynamic IP range. For example: a dynamic IP assign range is from 192.168.1.100 to 192.168.1.200. 192.168.1.100 will be the starting IP address.
End IP Address	The dynamic IP assigned range. High IP address is the end of the assigned dynamic IP range. For example: dynamic IP assign range is from 192.168.1.100 to 192.168.1.200. 192.168.1.200 will be the End IP address
Subnet Mask	The dynamic IP assignment range subnet mask
Gateway	The gateway in your network.
DNS	Domain Name Server IP Address in your network.
Lease Time (Hour)	The period of time, in hours, after which the system will reset the assigned dynamic IP to ensure the IP address is unused.
Apply	Select **Apply** to set the configurations.

DHCP Server – Client Entries

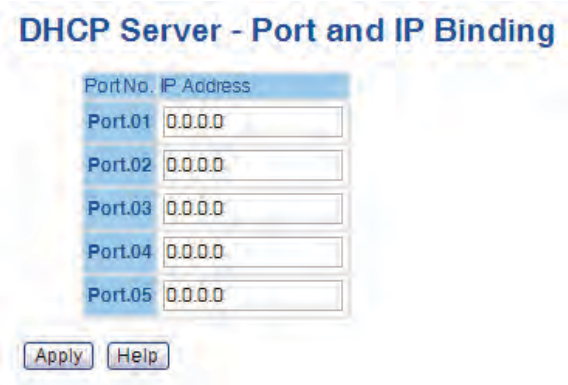
When the DHCP server function is activated, the system will collect the DHCP client information and display in here.



DHCP Server Client Entries interface

DHCP Server – Port and IP bindings

You can assign the specific IP address that is in the assigned dynamic IP range to the specific port. When the device is connecting to the port and asks for dynamic IP assignment, the system will assign the IP address that has been assigned before in the connected device.

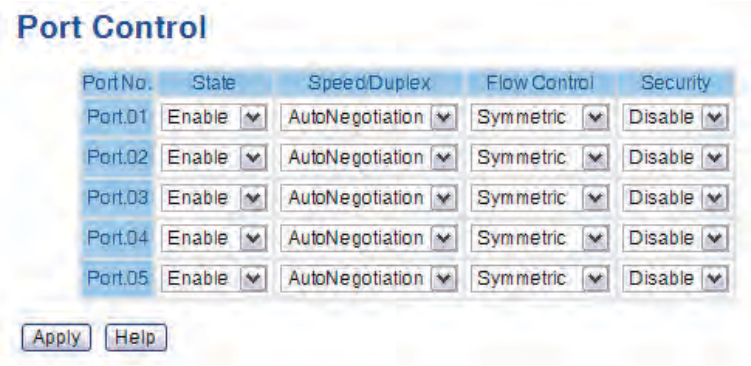


DHCP Server Port and IP Binding interface

Port Configuration

Port Control

Here you can set the state, speed/duplex, flow control, and security of the port.



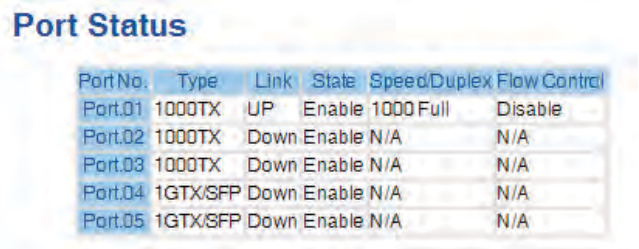
Port Control interface

The following table describes the labels in this screen.

Label	Description
Port NO.	Port number for setting.
Speed/Duplex	You can set Auto negotiation, 1000 full, 1000 half, 100 full, 100 half, 10 full, 10 half mode.
Flow Control	Support symmetric and asymmetric mode to avoid packet loss when congestion occurred.
Security	Support port security function. When the function is enabled, the port will stop learning MAC address dynamically.
Apply	Select **Apply** to set the configurations.

Port Status

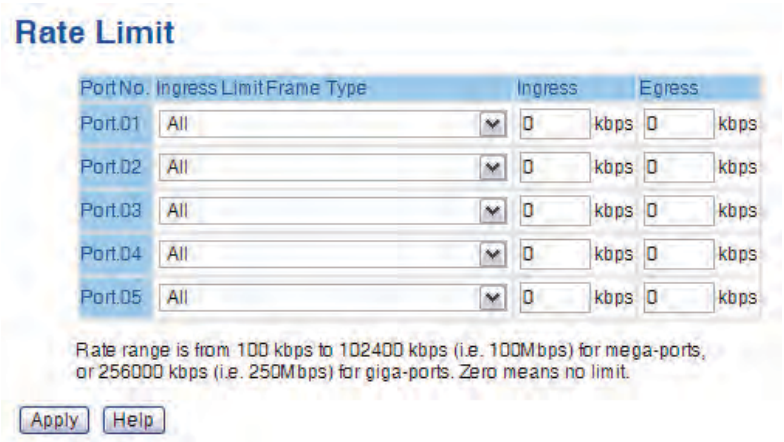
The following information provides the current port status information



Port Status interface

Rate Limit

With this function, you can limit traffic of all ports, including broadcast, multicast and flooded unicast. You can also set "Ingress" or "Egress" to limit traffic received or transmitted bandwidth.



Rate Limit interface

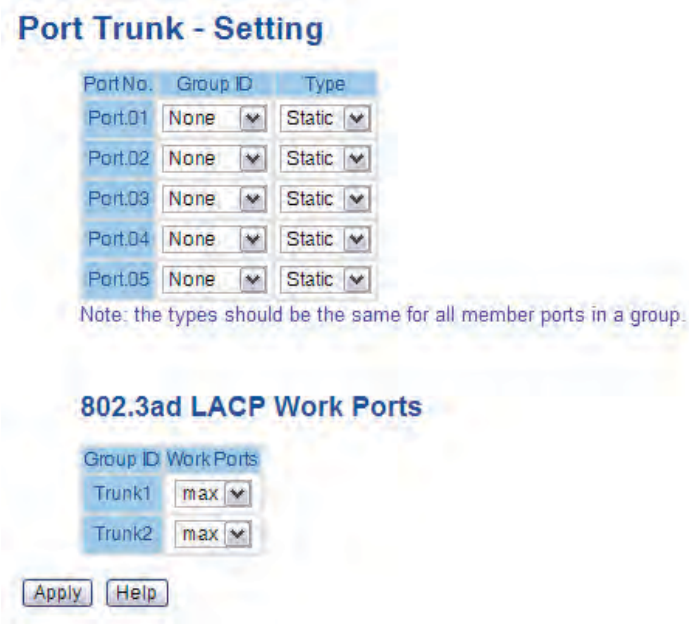
The following table describes the labels in this screen.

Label	Description
Ingress Limit Frame Type	You can set **all**, **Broadcast only**, **Broadcast/Multicast** or **Broadcast/Multicast/Flooded Unicast** mode.
Ingress	The switch port received traffic.
Egress	The switch port transmitted traffic.
Apply	Select **Apply** to set the configurations.

Port Trunk

Port Trunk – Setting

You can select a static trunk or 802.3ad LACP to combine several physical links with a logical link to increase the bandwidth.



Port Trunk - Setting interface

The following table describes the labels in this screen.

Label	Description
Group ID	Select port to join a trunk group.
Type	Support static trunk and 802.3ad LACP
Apply	Select **Apply** to set the configurations.

Port Trunk – Status

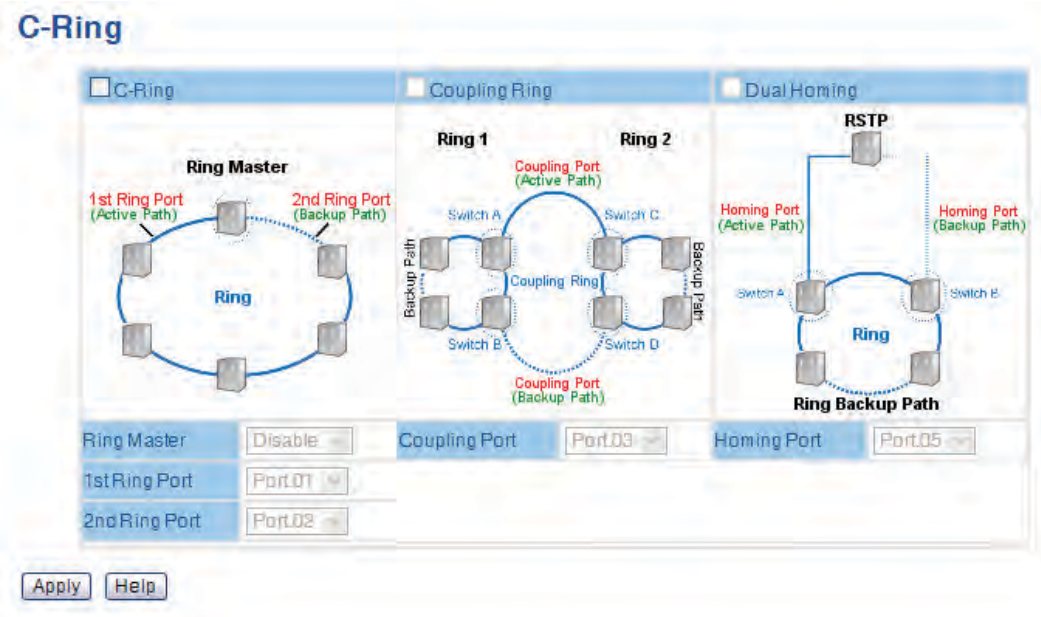
Port Trunk - Status interface

Redundancy

C-Ring

C-Ring technology is a powerful redundant Ring system. The recovery time of the Ring is less than 20 milliseconds. It can reduce unexpected damage caused by a network topology change.

C-Ring Supports 3 Ring topologies: C-Ring, Coupling Ring and Dual Homing.



Ring interface

The following table describes the labels in this screen.

Label	Description
C-Ring	Mark to enable C-Ring.
Ring Master	There should be one and only one Ring Master in a C-Ring. However if there are two or more switches which set Ring Master to enable, the switch with the lowest MAC address will be the actual Ring Master and others will be Backup Masters.
1st Ring Port	Choosing the primary port which connect to the ring
2nd Ring Port	Choosing the backup port which connect to the ring
Coupling Ring	Mark to enable Coupling Ring. Coupling Ring can be used to divide a big ring into two smaller rings to avoid effecting all switches when network topology change. It is a good application for connecting two Rings.
Coupling Port	Link to Coupling Port of the switch in another ring. Coupling Ring need four switches to build an active and a backup link. Set a port as coupling port. The coupled four ports of four switches will be run at active/backup mode.
Dual Homing	Mark to enable Dual Homing. By selecting Dual Homing mode, Ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work as active/backup mode, and connect each Ring to the normal switches in RSTP mode.
Apply	Select **Apply** to set the configurations.

Note: We don't recommend that you set one switch as a Ring Master and a Coupling Ring at the same time due to heavy load.

Legacy Ring

Legacy ring provides support for the switch to be used in an existing ring of ComNet X-Ring enabled switches.

X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same. In the X-Ring topology, every switch should be enabled with X-Ring or Legacy Ring function and two ports should be assigned as the member ports in the ring. Only one switch in the X-Ring group would be set as the master switch that one of its two member ports would be blocked, called backup port, and another port is called working port. Other switches in the X-Ring group are called working switches and their two member ports are called working ports. When the failure of network connection occurs, the backup port of the master switch (Ring Master) will automatically become a working port to recover from the failure.

The switch supports the function and interface for setting the switch as the ring master or not. The ring master can negotiate and place command to other switches in the X-Ring group. If there are 2 or more switches in master mode, the software will select the switch with lowest MAC address number as the ring master. The X-Ring master ring mode can be enabled by setting the Legacy Ring configuration interface. Also, the user can identify whether the switch is the ring master by checking the R.M. LED indicator on the front panel of the switch.

Label	Description
Legacy Ring	To enable the Legacy Ring (X-Ring) function, tick the checkbox beside the Legacy Ring label. If this checkbox is not ticked, all the ring functions are unavailable.
Ring Master	Select Enable for this switch to be the ring master or Disable for this switch to be a working switch.
1st Ring Port	The primary port, when this switch is Ring Master. Select a port to assign from the pull down selection menu.
2nd Ring Port	The backup port, used when this switch is Ring Master and the primary port fails. Select a port to assign from the pull down selection menu.
Save	Select to save changes.
Refresh	Select to refresh the page immediately.

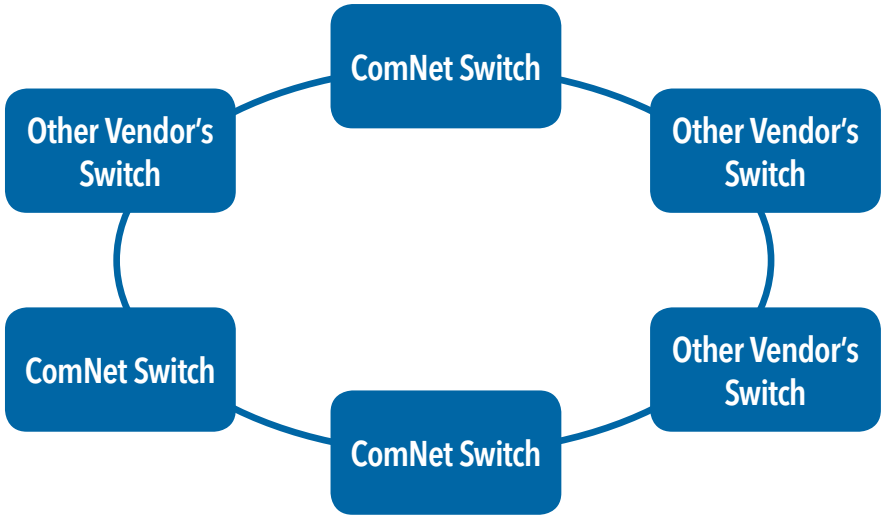
COM-Ring

You can add ComNet switches into a network constructed by another ring technology and enable COM-Ring to cooperate with another vendor's managed switch.

ComRing interface

Label	Description
Enable	Enable the COM-Ring function
Vendor	Select the vendor whose ring you want to join
1st Ring Port	Select the port that connects to the ring
2nd Ring Port	Select the port that connects to the ring

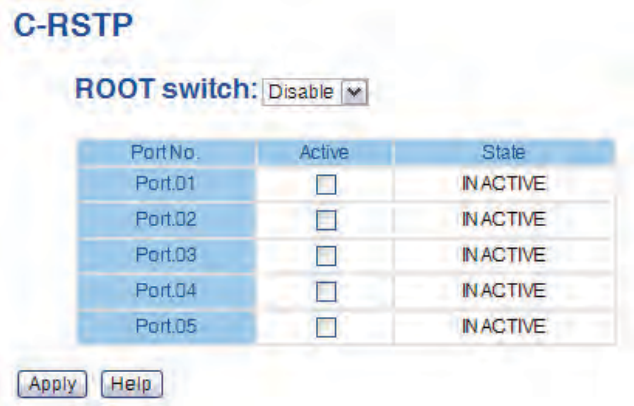
The application of COM-Ring is shown as below.



COM-Ring connection

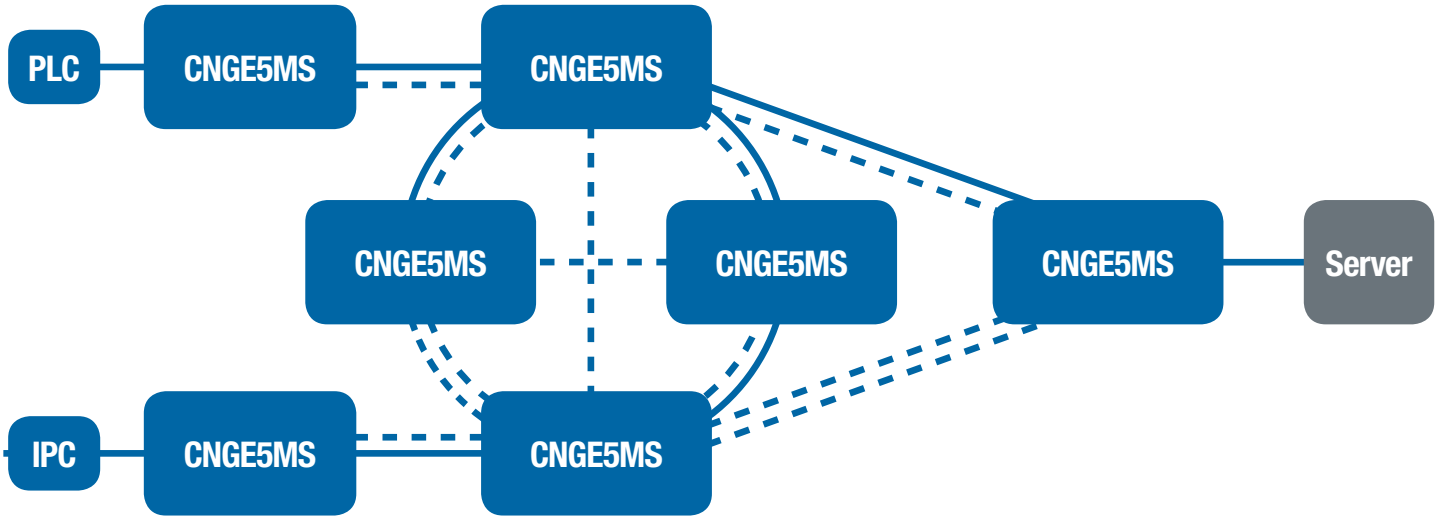
C-RSTP

C-RSTP is different from standard STP/RSTP, the recovery time of C-RSTP is less than 20 milliseconds and it supports more connected nodes in a ring topology.



C-RSTP interface

The application of C-RSTP is shown as below.



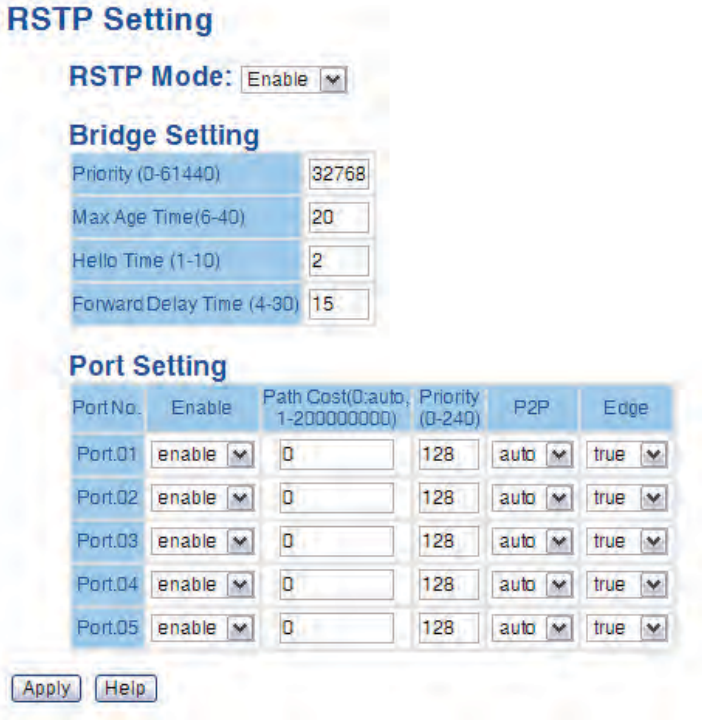
C-RSTP connection

RSTP

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol. It provides 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.

RSTP setting

You can enable/disable RSTP function, and set parameters for each port.



RSTP Setting interface

The following table describes the labels in this screen.

Label	Description
RSTP mode	You must enable or disable RSTP function before configuring 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. If the value changes, you must reboot the switch. The value must be multiple of 4096 according to the protocol standard rule.
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.
Forwarding 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.
Path Cost (1-200000000)	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
Priority (0-240)	Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16
Admin P2P	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. It is served by a point-to-point LAN segment), or it can be connected to two or more bridges (i.e. It is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True means P2P enabling. False means P2P disabling.
Admin Edge	The port directly connected to end stations, and it cannot create bridging loop in the network. To configure the port as an edge port, set the port to **True**.
Admin Non STP	The port includes the STP mathematical calculation. True is not including STP mathematical calculation. False is including the STP mathematical calculation.
Apply	Select **Apply** to set the configurations.

NOTE: Follow the rule to configure the MAX Age, Hello Time, and Forward Delay Time.
2 × (Forward Delay Time value –1) ≥ Max Age value ≥ 2 × (Hello Time value +1)

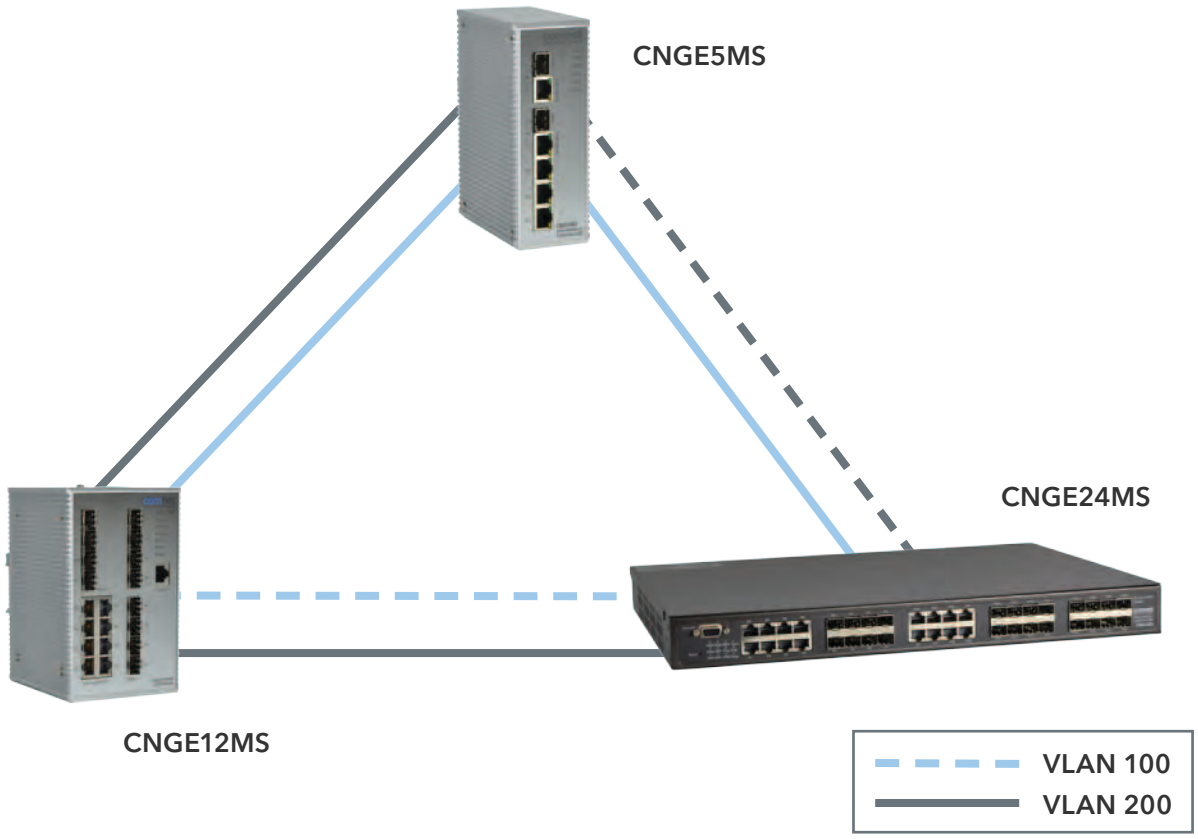
RSTP Information

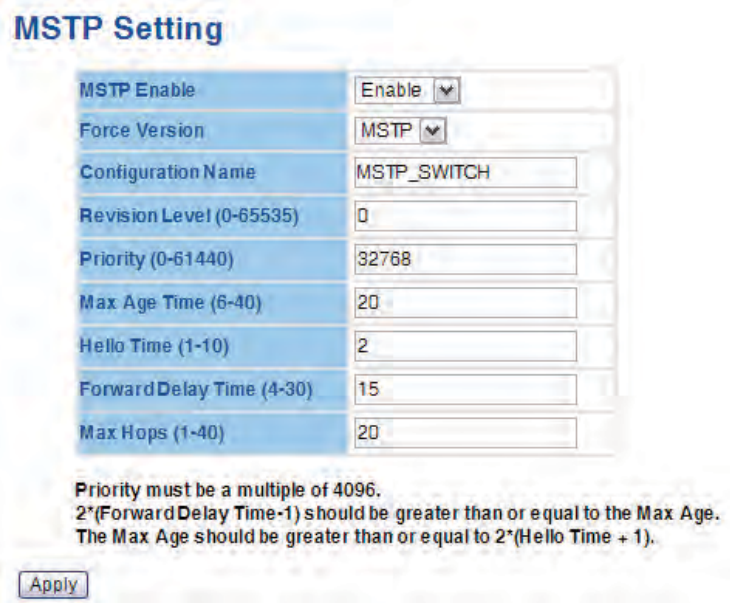
RSTP algorithm results are displayed in this table.

RSTP Information interface

MSTP

Multiple Spanning Tree Protocol (MSTP) is a standard protocol base on IEEE 802.1s. The function is that several VLANs can be mapping to a reduced number of spanning tree instances because most networks do not need more than a few logical topologies. It supports load balancing schemes and the CPU is sparer than PVST (Cisco proprietary technology).





MSTP Setting Interface

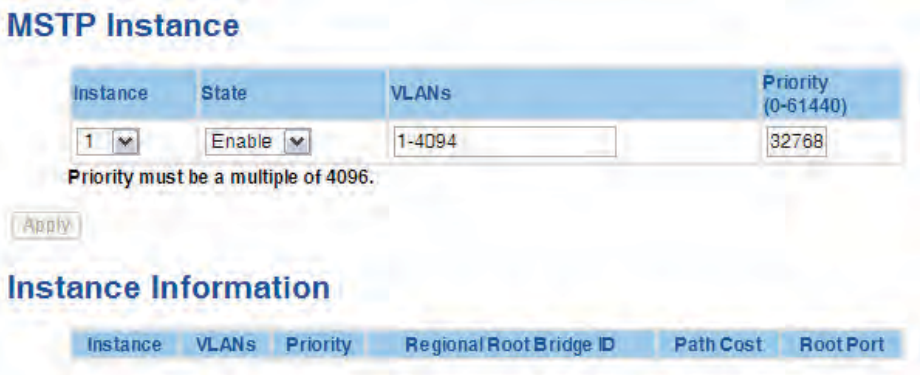
The following table describes the labels on this screen.

Label	Description
MSTP Enable	You must enable or disable MSTP function before configuring the related parameters.
Force Version	The Force Version parameter can be used to force a VLAN Bridge that supports RSTP to operate in an STP-compatible manner.
Configuration Name	The same MST Region must have the same MST configuration name.
Revision Level (0-65535)	The same MST Region must have the same revision level.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, You must reboot the switch. The value must be multiple of 4096 according to the protocol standard rule.
Max Age Time (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)	Follow the rule below to configure the MAX Age, Hello Time, and Forward Delay Time that the managed switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10. 2 × (Forward Delay Time value –1) ≥ Max Age value ≥ 2 × (Hello Time value +1)
Forwarding 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.

Max Hops (1-40)	This parameter is additional to those specified for RSTP. A single value applies to all Spanning Trees within an MST Region (the CIST and all MSTIs) for which the Bridge is the Regional Root.
Apply	Select **Apply** to activate the configurations.

MSTP Port interface

Label	Description
Port No.	Select the port that you want to configure.
Priority (0-240)	Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16
Path Cost (1-200000000)	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
Admin P2P	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. It is served by a point-to-point LAN segment), or it can be connected to two or more bridges (i.e. It is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True means P2P enabling. False means P2P disabling.
Admin Edge	The port directly connected to end stations, and it cannot create bridging loop in the network. To configure the port as an edge port, set the port to **True**.
Admin Non STP	The port includes the STP mathematical calculation. True is not including STP mathematical calculation. False is including the STP mathematical calculation.
Apply	Select **Apply** to activate the configurations.



MSTP Instance interface

Label	Description
Instance	Set the instance from 1 to 15
State	Enable or disable the instance
VLANs	Set which VLAN will belong which instance
Proprietary (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, You must reboot the switch. The value must be multiple of 4096 according to the protocol standard rule.
Apply	Select **Apply** to activate the configurations.

MSTP Instance Port interface

Label	Description
Instance	Set the instance's information except CIST
Port	Selecting the port that you want to configure.
Priority (0-240)	Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16
Path Cost (1-200000000)	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
Apply	Select **Apply** to activate the configurations.

VLAN

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which allows you to isolate network traffic. 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.

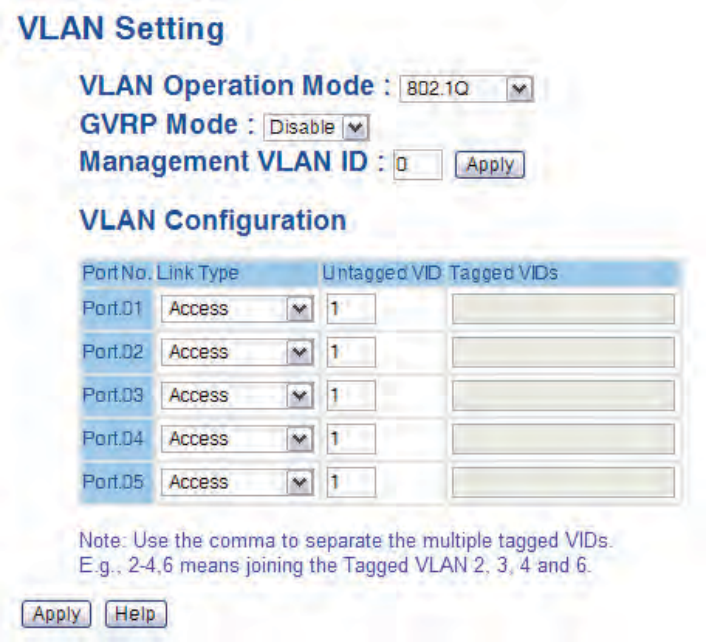
The switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration of VLAN operation mode is at **802.1Q**.

VLAN Configuration – 802.1Q

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

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

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



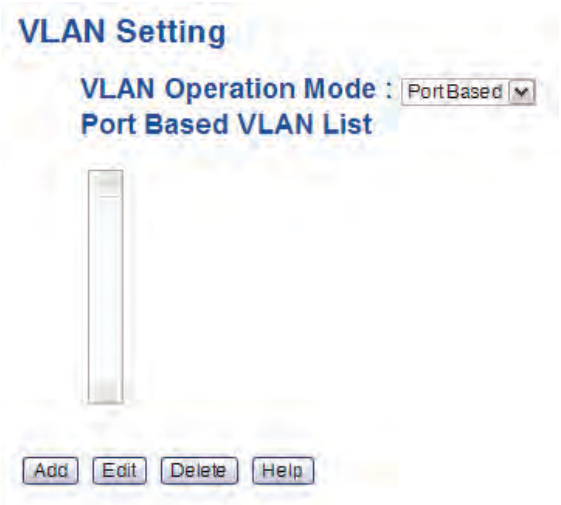
VLAN Configuration – 802.1Q interface

The following table describes the labels in this screen.

Label	Description
VLAN Operation Mode	Configure VLAN Operation Mode: disable, Port Base, 802.1Q
GVRP Mode	Enable/Disable GVRP function.
Management VLAN ID	Management VLAN can provide network administrator a secure VLAN to management Switch. Only the devices in the management VLAN can access the switch.
Link type	There are 3 types of link type: Access Link: single switch only, allows you to group ports by setting the same VID. Trunk Link: extended application of Access Link, allows you to group ports by setting the same VID with 2 or more switches. Hybrid Link: Both Access Link and Trunk Link are available.
Untagged VID	Set the port default VLAN ID for untagged devices that connect to the port. The range is 1 to 4094.
Tagged VIDs	Set the tagged VIDs to carry different VLAN frames to other switch.
Apply	Select **Apply** to activate the configurations.

VLAN Configuration – Port Based

Traffic is forwarded to the member ports of the same VLAN group. VLAN port based startup, set in the same group of the port, can be a normal transmission packet, without restricting the types of packets.



VLAN Configuration – Port Base interface-1

The following table describes the labels in this screen.

Label	Description
Add	Select to enter VLAN add interface.
Edit	Select to edit an existing VLAN from the list.
Delete	Delete exist VLAN
Help	Show help file.

VLAN Configuration – Port Base interface-2

The following table describes the labels in this screen.

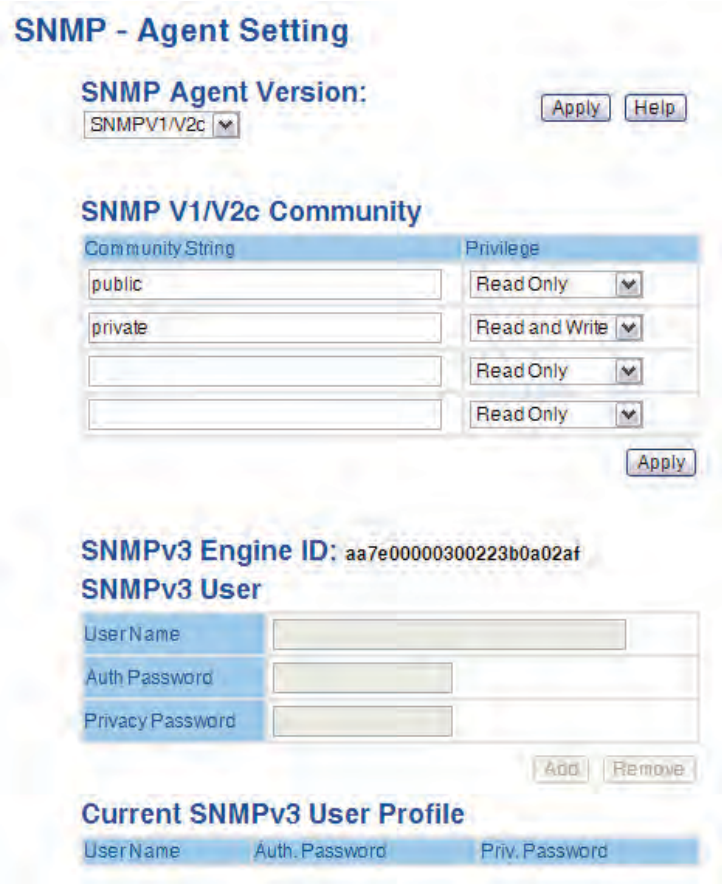
Label	Description
Group Name	VLAN name.
VLAN ID	Specify the VLAN ID
Add	Select port to join the VLAN group.
Remove	Remove port of the VLAN group
Apply	Select **Apply** to activate the configurations.
Help	Show help file.

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 – Agent Setting

You can set SNMP agent related information by Agent Setting Function.



SNMP Agent Setting interface

The following table describes the labels in this screen.

Label	Description
SNMP agent Version	Three SNMP versions are supported such as SNMP V1/SNMP V2c, and SNMP V3. SNMP V1/SNMP V2c agent use a community string match for authentication, that means SNMP servers access objects with read-only or read/write permissions with the community default string public/private. SNMP V3 requires an authentication level of MD5 or DES to encrypt data to enhance data security.
SNMP V1/V2c Community	SNMP Community should be set for SNMP V1/V2c. Four sets of "Community String/Privilege" are supported. Each Community String is maximum 32 characters. Keep empty to remove this Community string.
SNMPv3User	If SNMP V3 agent is selected, the SNMPv3 you profiled should be set for authentication. The Username is necessary. The Auth Password is encrypted by MD5 and the Privacy Password which is encrypted by DES. There are maximum 8 sets of SNMPv3 User and maximum 16 characters in username, and password. When SNMP V3 agent is selected, you can: 1. Input SNMPv3 username only. 2. Input SNMPv3 username and Auth Password. 3. Input SNMPv3 username, Auth Password and Privacy Password, which can be different with Auth Password. To remove a current user profile: 1. Input SNMPv3 user name you want to remove. 2. Select **Remove** button
Current SNMPv3 User Profile	Show all SNMPv3 user profiles.
Apply	Select **Apply** to activate the configurations.
Help	Show help file.

SNMP – Trap Setting

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.

SNMP Trap Setting interface

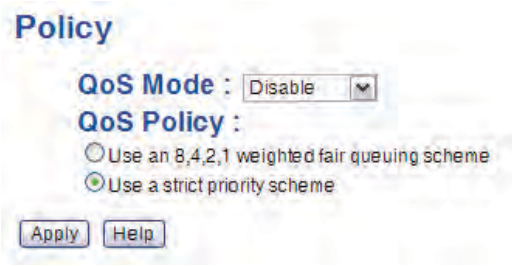
The following table describes the labels in this screen.

Label	Description
Server IP	The server IP address to receive Trap
Community	Community for authentication
Trap Version	Trap Version supports V1 and V2c.
Add	Add trap server profile.
Remove	Remove trap server profile.
Help	Show help file.

Traffic Prioritization

Traffic Prioritization includes 3 modes: port base, 802.1p/COS, and TOS/DSCP. By traffic prioritization function, you can classify the traffic into four classes for differential network application. CNGE5MS supports 4 priority queues.

QoS policy

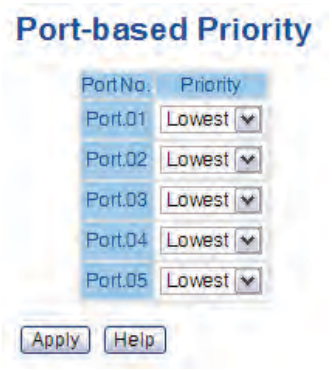


Traffic Prioritization interface

The following table describes the labels in this screen.

Label	Description
QOS policy	• **Using the 8,4,2,1 weight fair queue scheme:** the output queues will follow 8:4:2:1 ratio to transmit packets from the highest to lowest queue. For example: 8 high queue packets, 4 middle queue packets, 2 low queue packets, and the one lowest queue packets are transmitted in one turn. • **Using the strict priority scheme:** always the packets in higher queue will be transmitted first until higher queue is empty.
Priority Mode	Port-base: the output priority is determined by ingress port. • COS only: the output priority is determined by COS only. • TOS only: the output priority is determined by TOS only. • COS first: the output priority is determined by COS and TOS, but COS first. • TOS first: the output priority is determined by COS and TOS, but TOS first.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

Port-based priority



Port-based Priority interface

The following table describes the labels in this screen

Label	Description
Port base Priority	Assign Port with a priority queue. 4 priority queues can be assigned: High, Middle, Low, and Lowest.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

COS/802.1p

COS/802.1p interface

The following table describes the labels in this screen

Label	Description
COS/802.1p	COS (Class Of Service) is better known as 802.1p. It describes that the output priority of a packet is determined by user priority field in 802.1Q VLAN tag. The priority value is supported 0to7.COS value map to 4 priority queues: High, Middle, Low, and Lowest.
COS Port Default	When an ingress packet has not VLAN tag, a default priority value is considered and determined by ingress port.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

TOS/DSCP

TOS/DSCP interface

The following table describes the labels in this screen

Label	Description
TOS/DSCP	TOS (Type of Service) is a field in IP header of a packet. This TOS field is also used by Differentiated Services and is calLED the Differentiated Services Code Point (DSCP). The output priority of a packet can be determined by this field and the priority value is supported 0 to 63. DSCP value map to 4 priority queues: High, Middle, Low, and Lowest.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

IGMP

IGMP Snooping

Internet Group Management Protocol (IGMP) is used by IP hosts to register their dynamic multicast group membership. IGMP has 3 versions, IGMP v1, v2c and v3. Please refer to RFC 1112, 2236 and 3376. IGMP Snooping improves the performance of networks that carry multicast traffic. It provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic and reduces the amount of traffic on the Ethernet LAN.

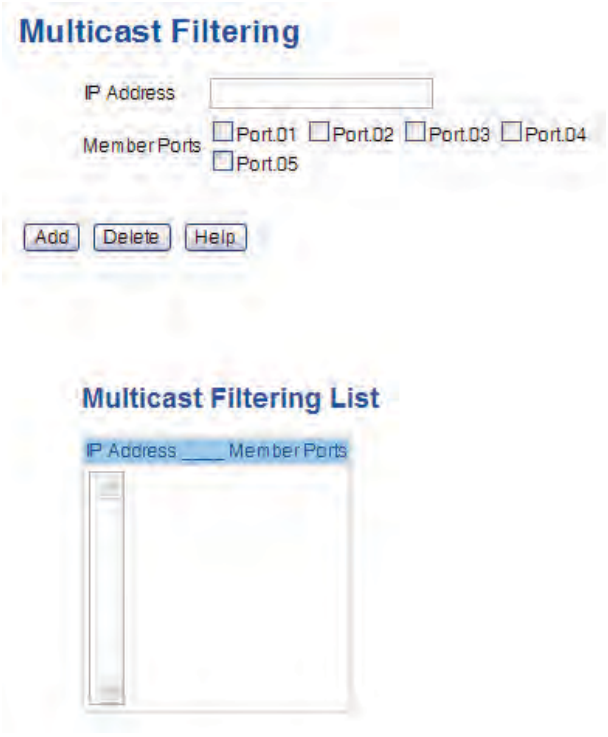
IGMP Snooping interface

The following table describes the labels in this screen.

Label	Description
IGMP Snooping	Enable/Disable IGMP snooping.
IGMP Query Mode	Switch will be IGMP querier or not. There should exist one and only one IGMP querier in an IGMP application. The "Auto" mode means that the querier is the one with lower IP address.
IGMP Snooping Table	Show current IP multicast list
Apply	Select **Apply** to set the configurations.
Help	Show help file.

Multicast Filter

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 ports that are connected to registered end stations.



Multicast Filtering interface

The following table describes the labels in this screen.

Label	Description
IP Address	Assign a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255
Member Ports	Tick the check box beside the port number to include them as the member ports in the specific multicast group IP address.
Add	Show current IP multicast list
Delete	Delete an entry from table
Help	Show help file.

Security

Five useful functions can enhance security of switch: IP Security, Port Security, MAC Blacklist, and MAC address Aging and 802.1x protocol.

IP Security

Only IP in the Secure IP List can manage the switch through your defined management mode. (WEB, Telnet, SNMP)

IP Security interface

The following table describes the labels in this screen.

Label	Description
IP security MODE	Enable/Disable the IP security function.
Enable WEB Management	Mark the blank to enable WEB Management.
Enable Telnet Management	Mark the blank to enable Telnet Management.
Enable SNMP Management	Mark the blank to enable SNMP Management.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

Port Security

Port security is to add static MAC addresses to hardware forwarding database. If port security is enabled at Port Control page, only the frames with MAC addresses in this list will be forwarded, otherwise will be discarded.

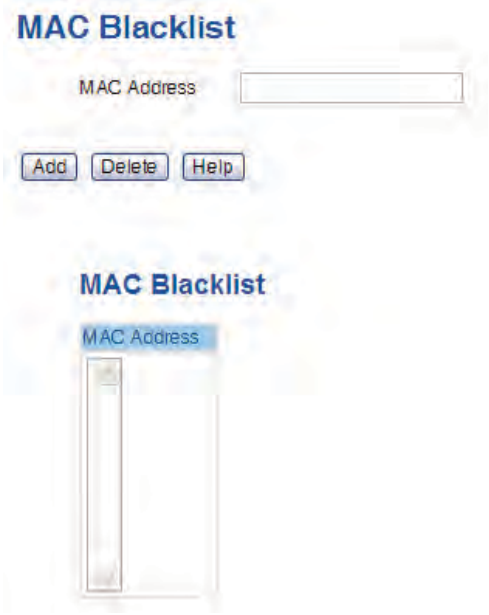
Port Security interface

The following table describes the labels in this screen.

Label	Description
MAC Address	Input MAC Address to a specific port.
Port NO.	Select port of switch.
Add	Add an entry of MAC and port information.
Delete	Delete the entry.
Help	Show help file.

MAC Blacklist

MAC Blacklist can eliminate the traffic forwarding to specific MAC addresses in list. Any frames forwarding to MAC addresses in this list will be discarded. Thus the target device will never receive any frame.



MAC Blacklist interface

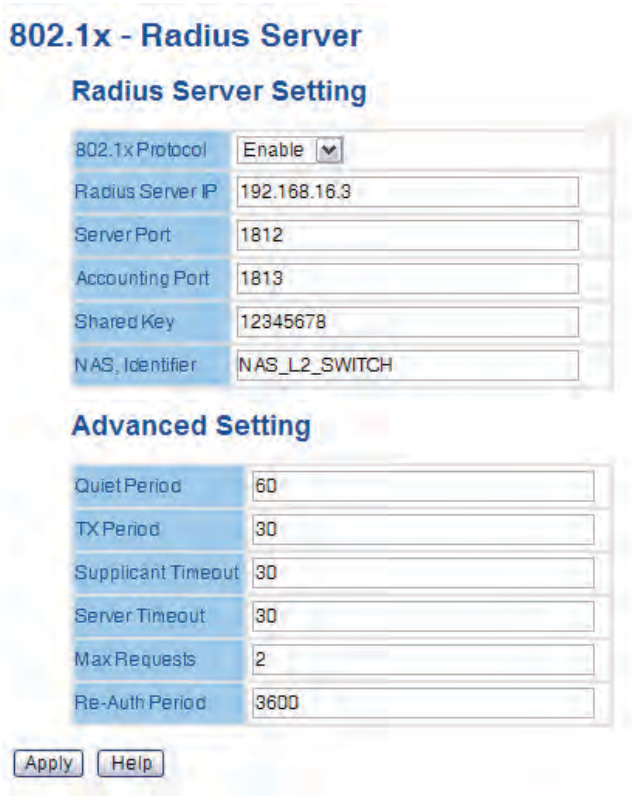
The following table describes the labels in this screen.

Label	Description
MAC Address	Input MAC Address to add to MAC Blacklist.
Port NO.	Select port of switch.
Add	Add an entry to Blacklist table.
Delete	Delete the entry.
Help	Show help file.

802.1x

802.1x - Radius Server

802.1x makes the use of the physical access characteristics of IEEE802 LAN infrastructures in order to provide an authenticated and authorized devices attached to a LAN port. Please refer to IEEE 802.1X - Port Based Network Access Control.



802.1x Radius Server interface

The following table describes the labels in this screen.

Label	Description
Radius Server Setting	
Radius Server IP	The IP address of the authentication server.
Server port	Set the UDP port number used by the authentication server to authenticate.
Account port	Set the UDP destination port for accounting requests to the specified Radius Server.
Shared Key	A key shared between this switch and authentication server.
NAS, Identifier	A string used to identify this switch.
Advanced Setting	
Quiet Period	Set the time interval between authentication failure and the start of a new authentication attempt.
Tx Period	Set the time that the switch can wait for response to an EAP request/ identity frame from the client before resending the request.
Supplicant Timeout	Set the period of time the switch waits for a supplicant response to an EAP request.
Server Timeout	Set the period of time the switch waits for a Radius server response to an authentication request.
Max Requests	Set the maximum number of times to retry sending packets to the supplicant.
Re-Auth Period	Set the period of time after which clients connected must be re-authenticated.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

802.1x-Port Authorized Mode

Set the 802.1x authorized mode of each port.

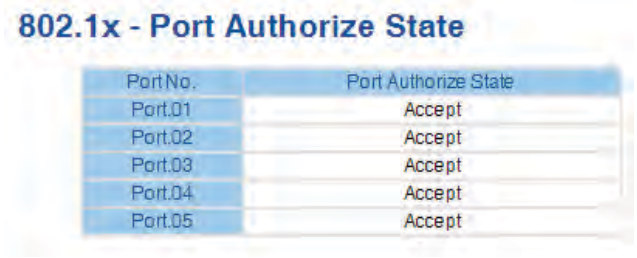
802.1x Port Authorize interface

The following table describes the labels in this screen.

Label	Description
Port Authorized Mode	Reject: force this port to be unauthorized. • Accept: force this port to be authorized. • Authorize: the state of this port was determined by the outcome of the 802.1x authentication. • Disable: this port will not participate in 802.1x.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

802.1x-Port Authorized Mode

Show 802.1x port authorized state.



802.1x Port Authorize State interface

Warning

This warning function is very important for managing the switch. You can manage switch by SYSLOG, Email, and Fault Relay. It helps you to monitor the switch status on remote site. When events occur, the warning message will send to your appointed server, Email, or relay fault to switch panel.

Fault Alarm

When any selected fault event happens, the Fault LED in switch panel will light up and the relay will signal at the same time.

Fault Alarm interface

The following table describes the labels in this screen.

Label	Description
Power Failure	Mark the blank of PWR 1 or PWR 2 to monitor.
Port Link Down/ Broken	Mark the blank of port 1 to port 5 to monitor.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

System Warning

System alarm support two warning mode: 1. SYSLOG. 2. E-MAIL. You can monitor switch through selected system events.

System Warning – SYSLOG Setting

The SYSLOG is a protocol to transmit event notification messages across networks. Please refer to RFC 3164 - The BSD SYSLOG Protocol

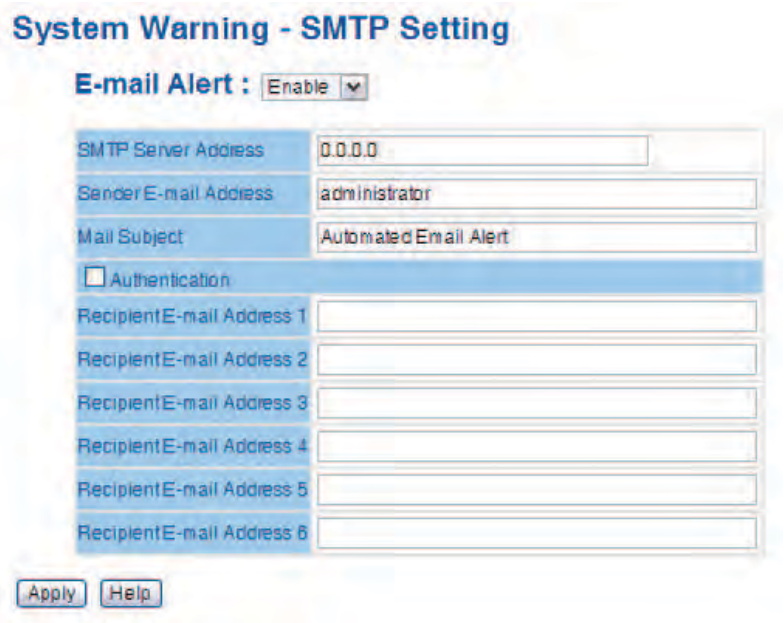
System Warning – SYSLOG Setting interface

The following table describes the labels in this screen.

Label	Description
SYSLOG Mode	• Disable: disable SYSLOG. • Client Only: log to local system. • Server Only: log to a remote SYSLOG server. • Both: log to both of local and remote server.
SYSLOG Server IP Address	The remote SYSLOG Server IP address.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

System Warning – SMTP Setting.

The acronym SMTP is short for Simple Mail Transfer Protocol. It is a protocol for e-mail transmission across the Internet. Please refer to RFC 821 - Simple Mail Transfer Protocol.



System Warning – SMTP Setting interface

The following table describes the labels in this screen.

Label	Description
E-mail Alarm	Enable/Disable transmission system warning events by e-mail.
Sender E-mail Address	The SMTP server IP address
Mail Subject	The Subject of the mail
Authentication	Username: the authentication username. Password: the authentication password. Confirm Password: re-enter password.
Recipient E-mail Address	The recipient's E-mail address. It supports 6 recipients for a mail.
Apply	Select **Apply** to set the configurations.
Help	Show help file.

System Warning – Event Selection

SYSLOG and SMTP are the two warning methods that are supported by the system. Check the corresponding box to enable system event warning method you wish to choose. Please note that the checkbox cannot be checked when SYSLOG or SMTP is disabled.

System Warning – Event Selection interface

The following table describes the labels in this screen.

Label	Description
System Event	
System Cold Start	Alert when system restart
Power Status	Alert when a power up or down
SNMP Authentication Failure	Alert when SNMP authentication failure.
Ring Topology Change	Alert when Ring topology changes.
Port Event	Disable Link Up Link Down Link Up & Link Down
Apply	Select **Apply** to set the configurations.
Help	Show help file.

Monitor and Diagnosis

MAC Address Table

Refer to IEEE 802.1 D Sections 7.9. The MAC Address Table, that is Filtering Database, supports queries by the Forwarding Process, as to whether a frame received by a given port with a given destination MAC address is to be forwarded through a given potential transmission port.

MAC Address Table interface

The following table describes the labels in this screen.

Label	Description
Port No	Show all MAC addresses mapping to a selected port in table.
Clear MAC Table	Clear all MAC addresses in table
Help	Show help file.

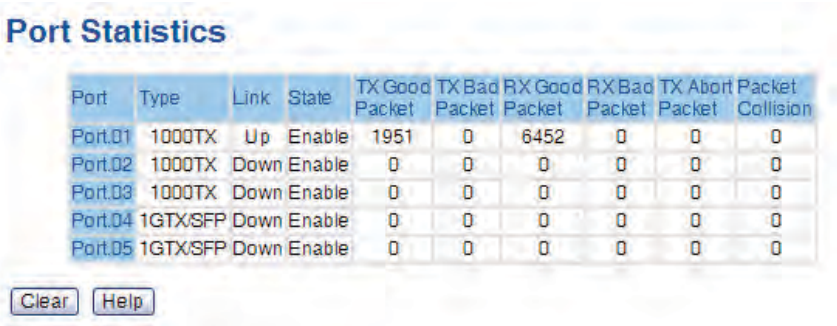
MAC Address Aging

You can set MAC Address aging timer, as time expired, the unused MAC will be cleared from MAC table. CNGE5MS also supports Auto Flush MAC Address Table When ports Link Down.

MAC Address Aging interface

Port Statistics

Port statistics show several statistics counters for all ports



Port Statistics interface

The following table describes the labels in this screen.

Label	Description
Type	Show port speed and media type.
Link	Show port link status.
State	Show ports enable or disable.
TX GOOD Packet	The number of good packets sent by this port.
TX Bad Packet	The number of bad packets sent by this port.
RX GOOD Packet	The number of good packets received by this port.
RX Bad Packet	The number of bad packets received by this port.
TX Abort Packet	The number of packets aborted by this port.
Packet Collision	The number of times a collision detected by this port.
Clear	Clear all counters.
Help	Show help file.

Port Monitoring

Port monitoring supports TX (egress) only, RX (ingress) only, and TX/RX monitoring. TX monitoring sends any data that egress out checked TX source ports to a selected TX destination port as well. RX monitoring sends any data that ingress in checked RX source ports out to a selected RX destination port as well as sending the frame where it normally would have gone. Note that keep all source ports unchecked in order to disable port monitoring.

Port monitoring interface

The following table describes the labels in this screen.

Label	Description
Destination Port	The port will receive a copied frame from source port for monitoring purpose.
Source Port	The port will be monitored. Mark the blank of TX or RX to be monitored.
TX	The frames come into switch port.
RX	The frames receive by switch port.
Apply	Select **Apply** to set the configurations.
Clear	Clear all marked blank. (disable the function)
Help	Show help file.

System Event Log

If system log client is enabled, the system event logs will show in this table.

System event log interface

The following table describes the labels in this screen.

Label	Description
Page	Select log page.
Reload	To get the newest event logs and refresh this page.
Clear	Clear log.
Help	Show help file.

Save Configuration

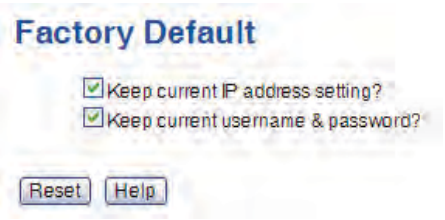
If any configuration changed, "Save Configuration" should be selected to save current configuration data to the permanent flash memory. Otherwise, the current configuration will be lost when power off or system reset.

System Configuration interface

The following table describes the labels in this screen.

Label	Description
Save	Save all configurations.
Help	Show help file.

Factory Default



Factory Default interface

Reset switch to default configuration. Select **Reset** to reset all configurations to the default value. You can select **Keep current IP address setting** and **Keep current username & password** to keep current IP and username and password.

System Reboot

System Reboot interface

Command Line Interface Management

Configuration by Command Line Interface (CLI).

About CLI Management

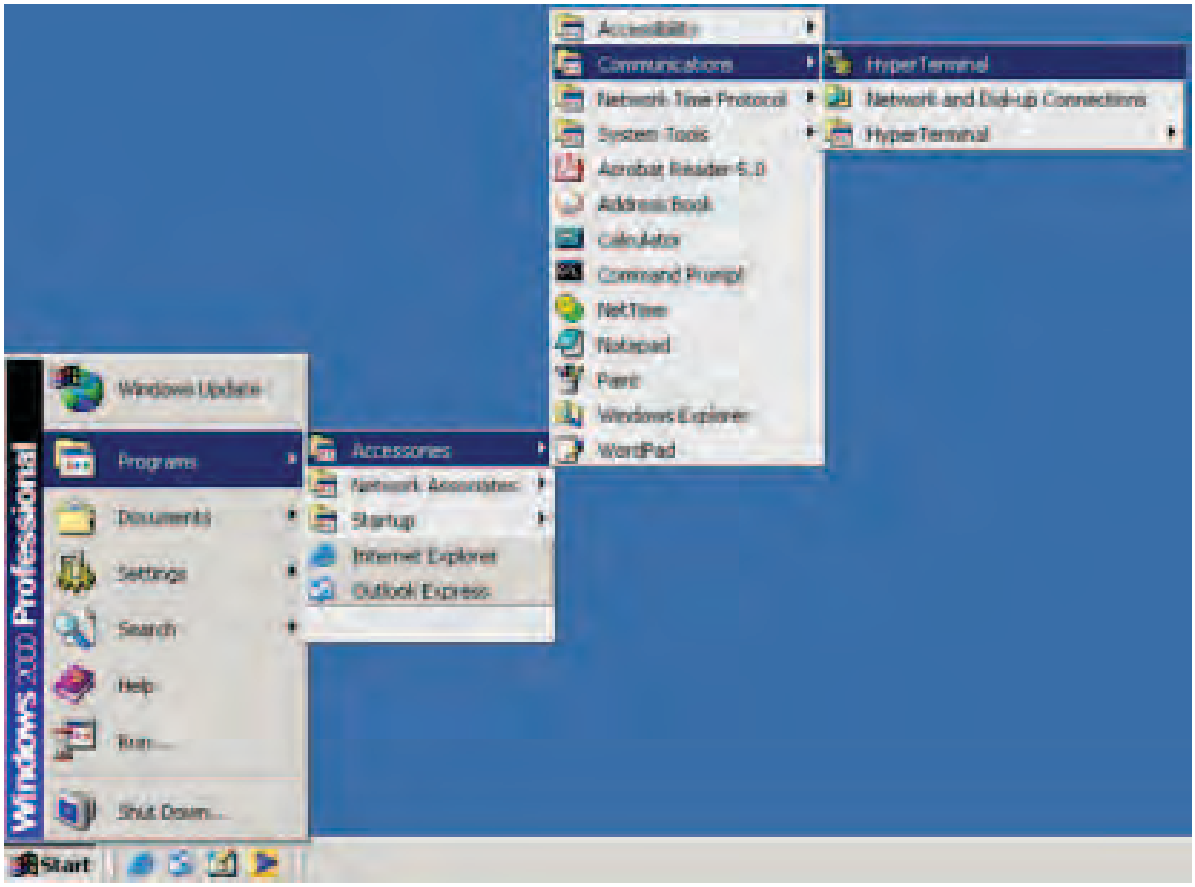
Besides WEB-base management, the CNGE8MS also supports CLI management. You can use console or telnet to manage the switch by CLI.

CLI Management by RS-232 Serial Console (9600, 8, none, 1, none)

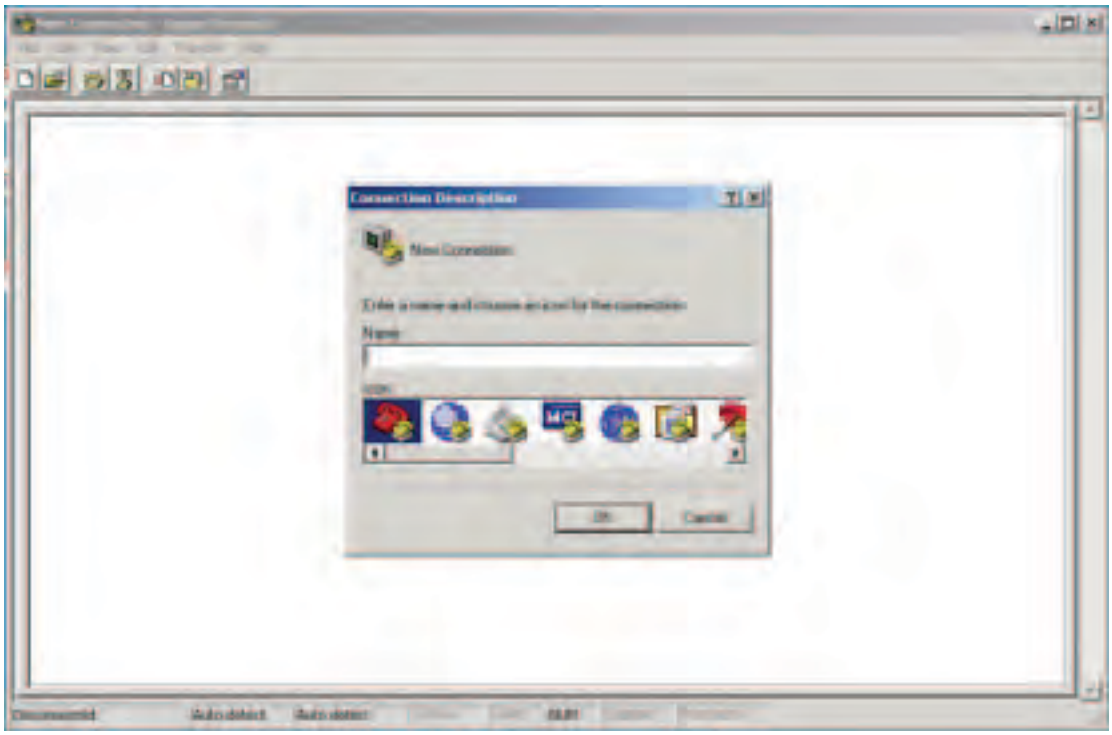
Before configuring by RS-232 serial console, use an RJ45 to DB9-F cable to connect the switches' RS-232 Console port to your PC's COM port.

Follow the steps below to access the console via RS-232 serial cable.

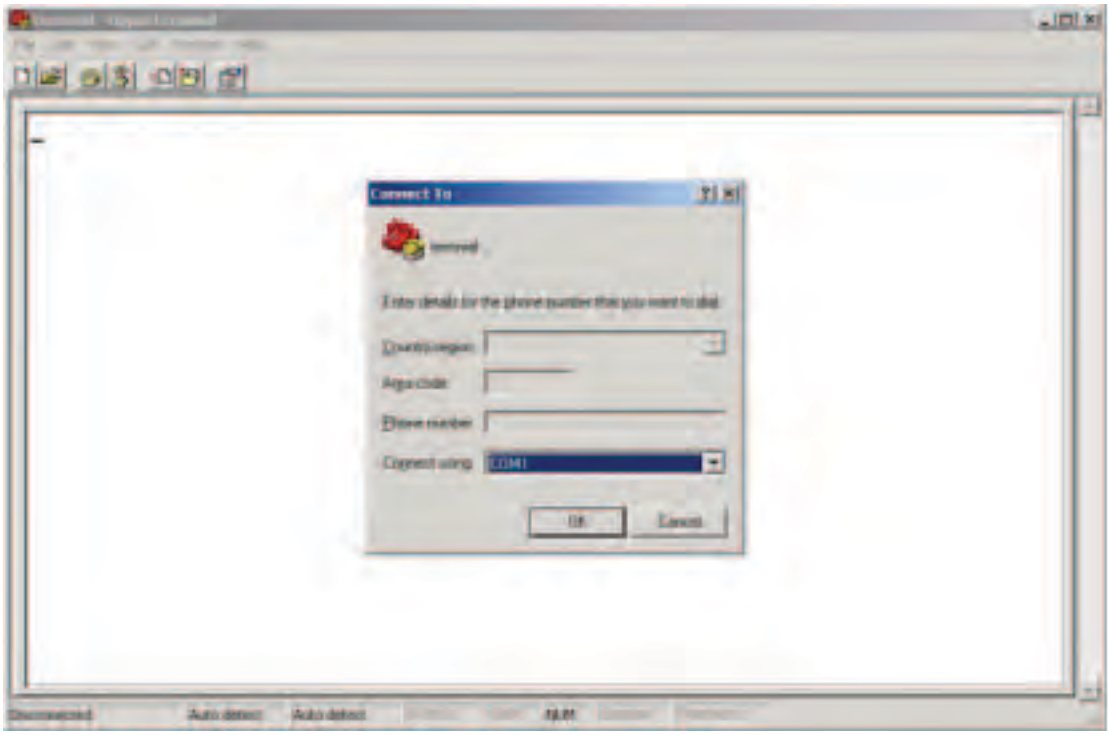
Step 1. From the Windows desktop, select on Start -> Programs -> Accessories -> Communications -> Hyper Terminal



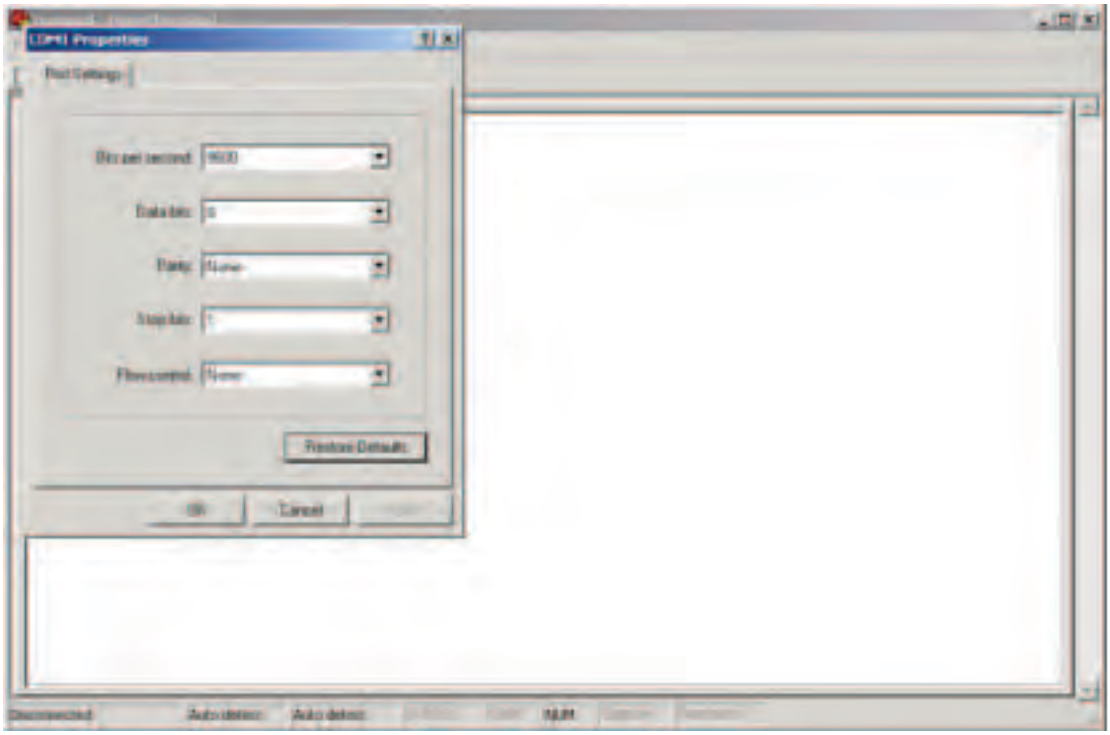
Step 2. Input a name for new connection



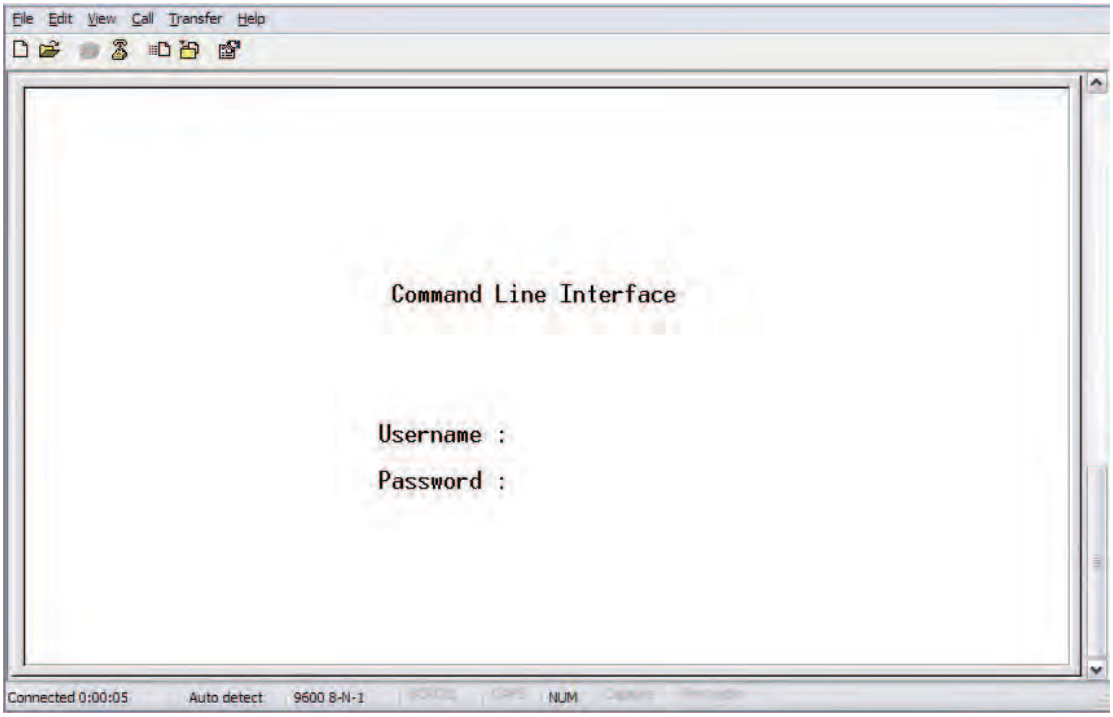
Step 3. Select the COM port number



Step 4. The COM port properties setting, 115200 for Bits per second, 8 for Data bits, None for Parity, 1 for Stop bits and none for Flow control.



Step 5. The Console login screen will appear. Use the keyboard to enter the Username and Password (The same with the password for Web Browser), then press **Enter**.



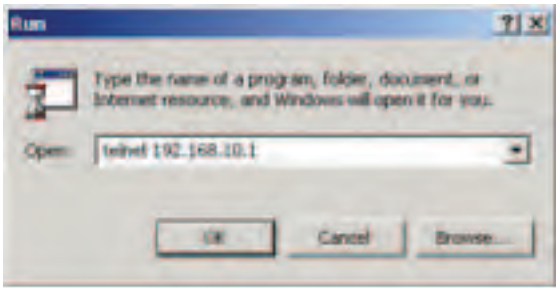
CLI Management by Telnet.

Users can use telnet to configure the switches.

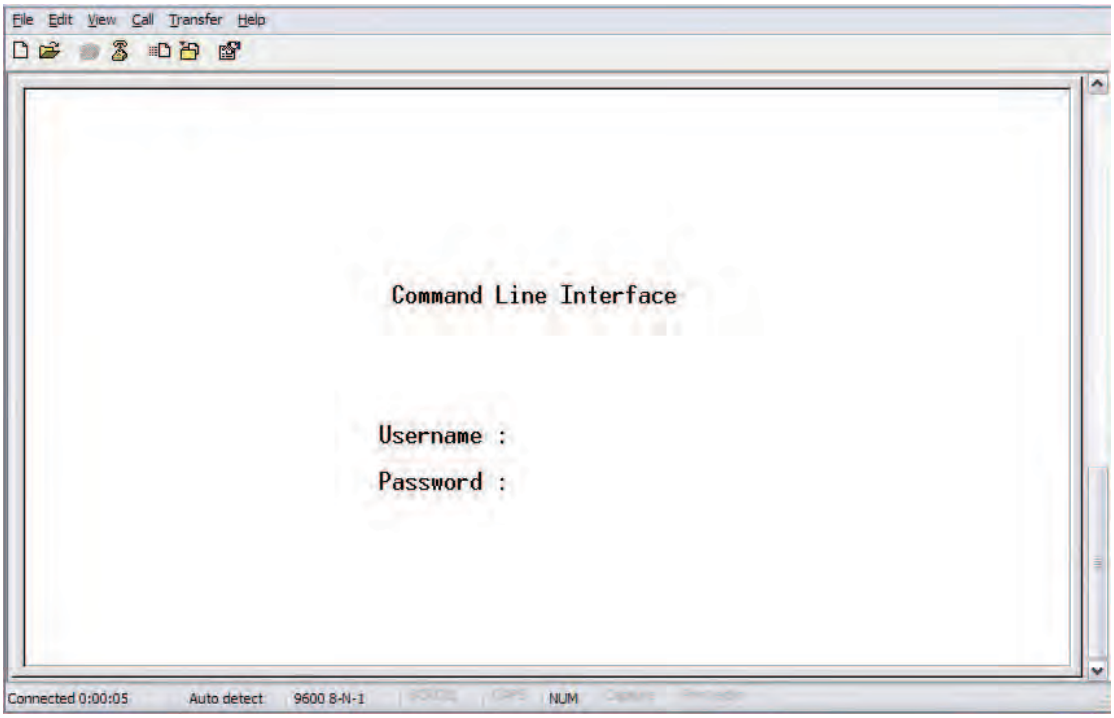
The default value is as below:
IP Address: **192.168.10.1**
Subnet Mask: **255.255.255.0**
Default Gateway: **192.168.10.254**
User Name: **admin**
Password: **admin**

Follow the steps below to access the console via Telnet.

Step 1. Telnet to the IP address of the switch from the Windows **Run** command (or from the MS-DOS prompt).



Step 2. The Login screen will appear. Use the keyboard to enter the Username and Password (The same with the password for Web Browser), and then press **Enter.**



Command Level

Modes	Access Method	Prompt	Exit Method	About This Model
User EXEC	Begin a session with your switch.	switch>	Enter logout or quit.	The user command available at the level of user is the subset of those available at the privileged level. Use this mode to • Enter menu mode. • 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 • 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 exit privileged EXEC mode or end.	Use this mode to configure parameters for the switch and Ethernet ports.

Symbol of Command Level.

Mode	Symbol of Command Level
User EXEC	E
Privileged EXEC	P
Global configuration	G
VLAN database	V
Interface configuration	I

Commands Set List–System Commands Set

CNGE5MS Commands	Level	Description	Example
show config	E	Show switch configuration	switch>show config
show terminal	P	Show console information	switch#show terminal
menu	E	Enter MENU mode	switch>menu
write memory	P	Save your configuration into permanent memory (flash rom)	switch#write memory
system name [System Name]	G	Configure system name	switch(config)#system name xxx
system location [System Location]	G	Set switch system location string	switch(config)#system location xxx
system description [System Description]	G	Set switch system description string	switch(config)#system description xxx
system contact [System Contact]	G	Set switch system contact window string	switch(config)#system contact xxx
show system-info	E	Show system information	switch>show system-info
ip address [Ip-address] [Subnet-mask] [Gateway]	G	Configure the IP address of switch	switch(config)#ip address 192.168.1.1 255.255.255.0 192.168.1.254
ip dhcp	G	Enable DHCP client function of switch	switch(config)#ip dhcp
show ip	P	Show IP information of switch	switch#show ip
no ip dhcp	G	Disable DHCP client function of switch	switch(config)#no ip dhcp
reload	G	Halt and perform a cold restart	switch(config)#reload
default	G	Restore to default	Switch(config)#default
admin username [Username]	G	Changes a login username. (maximum 10 words)	switch(config)#admin username xxxxxx
admin password [Password]	G	Specifies a password (maximum 10 words)	switch(config)#admin password xxxxxx
show admin	P	Show administrator information	switch#show admin
dhcpserver enable	G	Enable DHCP Server	switch(config)#dhcpserver enable
dhcpserver lowip [Low IP]	G	Configure low IP address for IP pool	switch(config)# dhcpserver lowip 192.168.1.1
dhcpserver highip [High IP]	G	Configure high IP address for IP pool	switch(config)# dhcpserver highip 192.168.1.50
dhcpserver subnetmask [Subnet mask]	G	Configure subnet mask for DHCP clients	switch(config)#dhcpserver subnetmask 255.255.255.0

dhcpserver gateway [Gateway]	G	Configure gateway for DHCP clients	switch(config)#dhcpserver gateway 192.168.1.254
dhcpserver dnsip [DNS IP]	G	Configure DNS IP for DHCP clients	switch(config)# dhcpserver dnsip 192.168.1.1
dhcpserver leasetime [Hours]	G	Configure lease time (in hour)	switch(config)#dhcpserver leasetime 1
dhcpserver ipbinding [IP address]	I	Set static IP for DHCP clients by port	switch(config)#interface fastEthernet 2 switch(config-if)#dhcpserver ipbinding 192.168.1.1
show dhcpserver configuration	P	Show configuration of DHCP server	switch#show dhcpserver configuration
show dhcpserver clients	P	Show client entries of DHCP server	switch#show dhcpserver clinets
show dhcpserver ip-binding	P	Show IP-Binding information of DHCP server	switch#show dhcpserver ip-binding
no dhcpserver	G	Disable DHCP server function	switch(config)#no dhcpserver
security enable	G	Enable IP security function	switch(config)#security enable
security http	G	Enable IP security of HTTP server	switch(config)#security http
security telnet	G	Enable IP security of telnet server	switch(config)#security telnet
security ip [Index(1..10)] [IP Address]	G	Set the IP security list	switch(config)#security ip 1 192.168.1.55
show security	P	Show the information of IP security	switch#show security
no security	G	Disable IP security function	switch(config)#no security
no security http	G	Disable IP security of HTTP server	switch(config)#no security http
no security telnet	G	Disable IP security of telnet server	switch(config)#no security telnet

Commands Set List–Port Commands Set

CNGE5MS Commands	Level	Description	Example
interface fastEthernet [Portid]	G	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex [full | half]	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#duplex
full speed [10|100|1000|auto]	I	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
flowcontrol mode [Symmetric|Asymmetric]	I	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion.	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol mode Asymmetric
no flowcontrol	I	Disable flow control of interface	switch(config-if)#no flowcontrol
security enable	I	Enable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#security enable
no security	I	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
bandwidth type all	I	Set interface ingress limit frame type to "accept all frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to "accept broadcast, multicast, and flooded unicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to "accept broadcast and multicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast
bandwidth type broadcast-only	I	Set interface ingress limit frame type to "only accept broadcast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only
bandwidth in [Value]	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config-if)#bandwidth in 100 switch(config)#interface fastEthernet 2

bandwidth out [Value]	I	Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth out 100
show bandwidth	I	Show interfaces bandwidth control	switch(config)#interface fastEthernet 2 switch(config-if)#show bandwidth
state [Enable | Disable]	I	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#interface fastEthernet 2 switch(config-if)#state Disable
show interface configuration	I	show interface configuration status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface configuration
show interface status	I	show interface actual status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface status
show interface accounting	I	show interface statistic counter	switch(config)#interface fastEthernet 2 switch(config-if)#show interface accounting
no accounting	I	Clear interface accounting information	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting

Commands Set List–Trunk command set

CNGE5MS Commands	Level	Description	Example
aggregator priority [1to65535]	G	Set port group system priority	switch(config)#aggregator priority 22
aggregator activityport [Port Numbers]	G	Set activity port	switch(config)#aggregator activityport 2
aggregator group [GroupID] [Port-list] lacp workp [Workport]	G	Assign a trunk group with LACP active. [GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	switch(config)#aggregator group 1 1-4 lacp workp 2 or switch(config)#aggregator group 2 1,4,3 lacp workp 3
aggregator group [GroupID] [Port-list] nolacp	G	Assign a static trunk group. [GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#aggregator group 1 2-4 nolacp or switch(config)#aggregator group 1 3,1,2 nolacp
show aggregator	P	Show the information of trunk groups	switch#show aggregator
no aggregator lacp [GroupID]	G	Disable the LACP function of trunk group	switch(config)#no aggregator lacp 1
no aggregator group [GroupID]	G	Remove a trunk group	switch(config)#no aggregator group 2

Commands Set List–VLAN command set

CNGE5MS Commands	Level	Description	Example
VLAN database	P	Enter VLAN configure mode	switch#VLAN database
VLAN [8021q | gvrp]	V	To set switch VLAN mode.	switch(VLAN)# VLANmode 8021q or switch(VLAN)# VLANmode gvrp
no VLAN [VID]	V	Disable VLAN group(by VID)	switch(VLAN)#no VLAN 2
no gvrp	V	Disable GVRP	switch(VLAN)#no gvrp
IEEE 802.1Q VLAN VLAN 8021q port [PortNumber] access-link untag [UntaggedVID]	V	Assign a access link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(VLAN)#VLAN 8021q port 3 access-link untag 33
VLAN 8021q port [PortNumber] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(VLAN)#VLAN 8021q port 3 trunk-link tag 2,3,6,99 or switch(VLAN)#VLAN 8021q port 3 trunk-link tag 3-20
VLAN 8021q port [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(VLAN)# VLAN 8021q port 3 hybrid-link untag 4 tag 3,6,8 or switch(VLAN)# VLAN 8021q port 3 hybrid-link untag 5 tag 6-8
VLAN 8021q aggregator [TrunkID] access-link untag [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(VLAN)#VLAN 8021q aggregator 3 access-link untag 33
VLAN 8021q aggregator [TrunkID] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VLAN by trunk group	switch(VLAN)#VLAN 8021q aggregator 3 trunk-link tag 2,3,6,99 or switch(VLAN)#VLAN 8021q aggregator 3 trunk-link tag 3-20
VLAN 8021q aggregator [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for VLAN by trunk group	switch(VLAN)# VLAN 8021q aggregator 3 hybrid-link untag 4 tag 3,6,8 or switch(VLAN)# VLAN 8021q aggregator 3 hybrid-link untag 5 tag 6-8
show VLAN [VID] or show VLAN	V	Show VLAN information	switch(VLAN)#show VLAN 23

Commands Set List–Spanning Tree command set

CNGE5MS Commands	Level	Description	Example
spanning-tree enable	G	Enable spanning tree	switch(config)#spanning-tree enable
spanning-tree priority [0 to 61440]	G	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
spanning-tree max-age [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)# spanning-tree max-age 15
spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
spanning-tree forward-time [seconds]	G	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)# spanning-tree forward-time 20
stp-path-cost [1 to 200000000]	I	Use the spanning-tree cost interface configuration command to set the path cost for Spanning TreeProtocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20
stp-path-priority [Port Priority]	I	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-path-priority 127
stp-admin-p2p [Auto|True|False]	I	Admin P2P of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-p2p Auto

stp-admin-edge [True|False]	I	Admin Edge of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-edge True
stp-admin-non-stp [True|False]	I	Admin NonSTP of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-non-stp False
Show spanning-tree	E	Display a summary of the spanning-tree states.	switch>show spanning-tree
no spanning-tree	G	Disable spanning-tree.	switch(config)#no spanning-tree

Commands Set List–QoS command set

CNGE5MS Commands	Level	Description	Example
qos policy [weighted-fair|strict]	G	Select QOS policy scheduling	switch(config)#qos policy weighted-fair
qos prioritytype [port-based|cos-only|tos-only|cos-first|tos-first]	G	Setting of QOS priority type	switch(config)#qos prioritytype
qos priority portbased [Port] [lowest|low|middle|high]	G	Configure Port-based Priority	switch(config)#qos priority portbased 1 low
qos priority cos [Priority] [lowest|low|middle|high]	G	Configure COS Priority	switch(config)#qos priority cos 22 middle
qos priority tos [Priority] [lowest|low|middle|high]	G	Configure TOS Priority	switch(config)#qos priority tos 3 high
show qos	P	Display the information of QoS configuration	switch>show qos
no qos	G	Disable QoS function	switch(config)#no qos

Commands Set List–IGMP command set

CNGE5MS Commands	Level	Description	Example
igmp enable	G	Enable IGMP snooping function	switch(config)#igmp enable
Igmp-query auto	G	Set IGMP query to auto mode	switch(config)#Igmp-query auto
Igmp-query force	G	Set IGMP query to force mode	switch(config)#Igmp-query force
show igmp configuration	P	Displays the details of an IGMP configuration.	switch#show igmp configuration
show igmp multi	P	Displays the details of an IGMP snooping entries.	switch#show igmp multi
no igmp	G	Disable IGMP snooping function	switch(config)#no igmp
no igmp-query	G	Disable IGMP query	switch#no igmp-query

Commands Set List–MAC/Filter Table command set

CNGE5MS Commands	Level	Description	Example
mac-address-table static hwaddr [MAC]	I	Configure MAC address table of interface (static).	switch(config)#interface fastEthernet 2 switch(config-if)#mac-address-table static hwaddr 000012345678
mac-address-table filter hwaddr [MAC]	G	Configure MAC address table(filter)	switch(config)#mac-address-table filter hwaddr 000012348678
show mac-address-table	P	Show all MAC address table	switch#show mac-address-table
show mac-address-table static	P	Show static MAC address table	switch#show mac-address-table static
show mac-address-table filter	P	Show filter MAC address table.	switch#show mac-address-table filter
no mac-address-table static hwaddr [MAC]	I	Remove an entry of MAC address table of interface (static)	switch(config)#interface fastEthernet 2 switch(config-if)#no mac-address-table static hwaddr 000012345678
no mac-address-table filter hwaddr [MAC]	G	Remove an entry of MAC address table (filter)	switch(config)#no mac-address-table filter hwaddr 000012348678
no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#no mac-address-table

Commands Set List–SNMP command set

CNGE5MS Commands	Level	Description	Example
snmp agent-mode [v1v2c | v3]	G	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2c
snmp-server host [IP address] community [Community-string] trap-version [v1|v2c]	G	Configure SNMP server host information and community string	switch(config)#snmp-server host 192.168.10.50 community public trap-version v1 (remove) Switch(config)# no snmp-server host 192.168.10.50
snmp community-strings [Community-string] right [RO|RW]	G	Configure the community string right	switch(config)#snmp community-strings public right RO or switch(config)#snmp community-strings public right RW
snmp snmpv3-user [User Name] password [Authentication Password] [Privacy Password]	G	Configure the user profile for SNMPV3 agent. Privacy password could be empty.	switch(config)#snmp snmpv3-user test01 password AuthPW PrivPW
show snmp	P	Show SNMP configuration	switch#show snmp
show snmp-server	P	Show specified trap server information	switch#show snmp-server
no snmp community-strings [Community]	G	Remove the specified community.	switch(config)#no snmp community-strings public
no snmp snmpv3-user [User Name] password [Authentication Password] [Privacy Password]	G	Remove specified user of SNMPv3 agent. Privacy password could be empty.	switch(config)# no snmp snmpv3-user test01 password AuthPW PrivPW
no snmp-server host [Host-address]	G	Remove the SNMP server host.	switch(config)#no snmp-server 192.168.10.50

Commands Set List–Port Mirroring command set

CNGE5MS Commands	Level	Description	Example
monitor rx	G	Set RX destination port of monitor function	switch(config)#monitor rx
monitor tx	G	Set TX destination port of monitor function	switch(config)#monitor tx
show monitor	P	Show port monitor information	switch#show monitor
monitor [RX|TX|Both]	I	Configure source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#monitor RX
show monitor	I	Show port monitor information	switch(config)#interface fastEthernet 2 switch(config-if)#show monitor
no monitor	I	Disable source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#no monitor

Commands Set List–802.1x command set

CNGE5MS Commands	Level	Description	Example
8021x enable	G	Enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radius ip [IP address]	G	Change the radius server IP.	switch(config)# 8021x system radiusip 192.168.1.1
8021x system server port [port ID]	G	Change the radius server port	switch(config)# 8021x system serverport 1815
8021x system account port [port ID]	G	Change the accounting port	switch(config)# 8021x system account port 1816
8021x system share key [ID]	G	Change the shared key value.	switch(config)# 8021x system share key 123456
8021x system nasid [words]	G	Change the NAS ID	switch(config)# 8021x system nasid test1
8021x misc quiet period [sec.]	G	Specify the quiet period value of the switch.	switch(config)# 8021x misc quiet period 10
8021x misc tx period [sec.]	G	Set the TX period.	switch(config)# 8021x misc tx period 5
8021x misc support timeout [sec.]	G	Set the supplicant timeout.	switch(config)# 8021x misc support timeout 20
8021x misc server timeout [sec.]	G	Set the server timeout.	switch(config)#8021x misc server timeout 20

8021x misc max request [number]	G	Set the MAX requests.	switch(config)# 8021x misc max request 3
8021x misc reauth period [sec.]	G	Set the reauth period.	switch(config)# 8021x misc reauth period 3000
8021x port state [disable | reject | accept | authorize]	I	Set the state of the selected port.	switch(config)#interface fast Ethernet 3 switch(config-if)#8021x port state accept
show 8021x	E	Display a summary of the 802.1x properties and also the port sates.	switch>show 8021x
no 8021x	G	Disable 802.1x function	switch(config)#no 8021x

Commands Set List–TFTP command set

CNGE5MS Commands	Level	Description	Defaults Example
backup flash:backup_cfg	G	Save configuration to TFTP 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	G	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
upgrade flash:upgrade_fw	G	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

Commands Set List–SYSLOG, SMTP, EVENT command set

CNGE5MS Commands	Level	Description	Example
systemlog ip [IP address]	G	Set System log server IP address.	switch(config)# systemlog ip 192.168.1.100
systemlog mode [client|server|both]	G	Specified the log mode	switch(config)# systemlog mode both
show systemlog	E	Display system log.	Switch>show systemlog
show systemlog	P	Show system log client & server information	switch#show systemlog
no systemlog	G	Disable systemlog functon	switch(config)#no systemlog
smtp enable	G	Enable SMTP function	switch(config)#smtp enable
smtp serverip [IP address]	G	Configure SMTP server IP	switch(config)#smtp serverip 192.168.1.5

smtp authentication	G	Enable SMTP authentication	switch(config)#smtp authentication
smtp account [account]	G	Configure authentication account	switch(config)#smtp account User
smtp password [password]	G	Configure authentication password	switch(config)#smtp password
smtp rcpt email [Index] [Email address]	G	Configure Rcpt e-mail Address	switch(config)#smtp rcpt email 1 Alert@test.com
show smtp	P	Show the information of SMTP	switch#show smtp
no smtp	G	Disable SMTP function	switch(config)#no smtp
event device-cold-start [Systemlog|SMTP|Both]	G	Set cold start event type	switch(config)#event device-cold-start both
event authentication-failure [Systemlog|SMTP|Both]	G	Set Authentication failure event type	switch(config)#event authentication-failure both
event Ring-topology-change [Systemlog|SMTP|Both]	G	Set s ring topology changed event type	switch(config)#event ring-topology-change both
event systemlog [Link-UP|Link-Down|Both]	I	Set port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#event systemlog both
event smtp [Link-UP|Link-Down|Both]	I	Set port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#event smtp both
show event	P	Show event selection	switch#show event
no event device-cold-start	G	Disable cold start event type	switch(config)#no event device-cold-start
no event authentication-failure	G	Disable Authentication failure event typ	switch(config)#no event authentication-failure
no event ring-topology-change	G	Disable ring topology changed event type	switch(config)#no event ring-topology-change
no event system log	I	Disable port event for system log	switch(config)#interface fast Ethernet 3 switch(config-if)#no event system log
no event smpt	I	Disable port event for SMTP	switch(config)#interface fast Ethernet 3 switch(config-if)#no event smtp
show system log	P	Show system log client & server information	switch#show system log

Commands Set List–SNTP command set

CNGE5MS Commands	Level	Description	Example
sntp enable	G	Enable SNTP function	switch(config)#sntp enable
sntp daylight	G	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight
sntp daylight-period [Start time] [End time]	G	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# sntp daylight-period 20060101-01:01 20060202-01-01
sntp daylight-offset [Minute]	G	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight-offset 3
sntp ip [IP]	G	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp ip 192.169.1.1
sntp timezone [Timezone]	G	Set time zone index, use "show sntp timzezone" command to get more information of index number	switch(config)#sntp timezone 22
show sntp	P	Show SNTP information	switch#show sntp
show sntp time zone	P	Show index number of time zone list	switch#show sntp time zone
no sntp	G	Disable SNTP function	switch(config)#no sntp
no sntp daylight	G	Disable daylight saving time	switch(config)#no sntp daylight

Commands Set List– Ring command set

CNGE5MS Commands	Level	Description	Example
Ring enable	G	Enable Ring	switch(config)# Ring enable
Ring master	G	Enable ring master	switch(config)# Ring master
Ring couple ring	G	Enable couple ring	switch(config)# Ring couple ring
Ring dual homing	G	Enable dual homing	switch(config)# Ring dual homing
Ring ring port [1st Ring Port] [2nd Ring Port]	G	Configure 1st/2nd Ring Port	switch(config)# Ring ring port 7 8
Ring coupling port [Coupling Port]	G	Configure Coupling Port	switch(config)# Ring coupling port 1
Ring control port [Control Port]	G	Configure Control Port	switch(config)# Ring control port 2
Ring homing port [Dual Homing Port]	G	Configure Dual Homing Port	switch(config)# Ring homing port 3
show Ring	P	Show the information of Ring	switch#show Ring
no Ring	G	Disable Ring	switch(config)#no Ring
no Ring master	G	Disable ring master	switch(config)# no Ring master
no Ring couple ring	G	Disable couple ring	switch(config)# no Ring couple ring
no Ring dual homing	G	Disable dual homing	switch(config)# no Ring dual homing

Technical Specifications

Technology	
Ethernet Standards	IEEE 802.3 for 10Base-T, IEEE 802.3u for 100Base-T(X) and 100Base-FX IEEE 802.3z for 1000Base-X IEEE 802.3ab for 1000Base-T(X), IEEE 802.3x for Flow control IEEE 802.3ad for LACP (Link Aggregation Control Protocol) IEEE 802.1D for STP (Spanning Tree Protocol) IEEE 802.1p for COS (Class of Service) IEEE 802.1Q for VLAN Tagging IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol) IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol) IEEE 802.1x for Authentication IEEE 802.1AB for LLDP (Link Layer Discovery Protocol)
MAC addresses	8192
Priority Queues	4
Flow Control	IEEE 802.3x Flow Control and Back-pressure
Processing	Store-and-Forward
Interface	
Gigabit Combo Ports	2 × 100/1000Base-X SFP + 2 × 10/100/1000Base-T(X) RJ45 Ports
Gigabit RJ45 Ports	3 × 10/100/1000Base-T(X), Auto MDI/MDIX
LED Indicators	Per Unit : Power × 3 (Green) Gigabit RJ45 Ports: Per Port : Link/Activity(Green/Blinking Green), 100Mbps indicator (Amber) Gigabit SFP Ports: Per Port : Link/Activity(Green/Blinking Green)
Power Requirements	
Power Input Voltage	PWR1/2: 12 – 48VDC on 7-pin Terminal Block PWR3 : 12 – 45VDC on DC-Jack
Reverse Polarity Protection	Present (On Terminal Block Only)
Power Consumption	10 Watts
Environmental	
Operating Temperature	-40 – +75 °C
Storage Temperature	-40 – +85 °C
Operating Humidity	5% – 95%, non-condensing

Mechanical	
Dimension (W × D × H)	54.1 × 106.1 × 145.4mm (2.13 × 4.18 × 5.72in)
Casing	IP-30 protection
Regulatory Approvals	
EMI	FCC Part 15, CISPR(EN55022) class A
EMS	EN61000-4-2 (ESD) EN61000-4-3 (RS) EN61000-4-4 (EFT) EN61000-4-5 (Surge) EN61000-4-6 (CS) EN61000-4-8 EN61000-4-11
Shock	IEC60068-2-27
Free Fall	IEC 60068-2-32
Vibration	IEC 60068-2-6
Safety	EN60950
Warranty	Lifetime

ComNet Customer Service
Customer Care is ComNet Technology's global service center, where our professional staff is ready to answer your questions at any time.

Email ComNet Global Service Center: customercare@comnet.net

comnet
Communication Networks

3 CORPORATE DRIVE | DANBURY, CT 06810 | USA
T: 203.796.5300 | F: 203.796.5303 | TECH SUPPORT: 1.888.678.9427 | INFO@COMNET.NET

8 TURNBERRY PARK ROAD | GILDERSOME | MORLEY | LEEDS, UK LS27 7LE
T: +44 (0)113 307 6400 | F: +44 (0)113 253 7462 | INFO-EUROPE@COMNET.NET