



INSTALLATION AND OPERATION MANUAL

CNGE12MS

12-PORT MANAGED GIGABIT SWITCH

v1.2 Sept 2012

The ComNet™ CNGE12MS is a 12-port Managed Ethernet Switch designed to reliably operate in harsh, environmentally challenging applications. It features four (4) 1000BASE-X and eight (8) gigabit combo ports. The eight combo ports are 10/100/1000Mbps configurable for either CAT5-e copper, or multimode or single-mode optical fiber by the use of optional ComNet SFPs*. Exclusive to ComNet is C-Ring, a feature that protects the network from interruptions or temporary malfunctions with fast recovery technology. Legacy ring allows the switch to be used in an existing ring of ComNet X-Ring enabled switches. Redundant DC inputs are included for uninterrupted operation in the event of a power supply failure. The electrical ports support the 10/100/1000Mbps Ethernet IEEE802.3 protocol, and auto-negotiating and auto-MDi/MDiX features are provided. These network-managed layer 2 switches are optically and electrically compatible with any IEEE802.3 compliant Ethernet device. The CNGE12MS is DIN-rail or wall-mountable.

Contents

Regulatory Compliance Statement	3
Warranty	3
Disclaimer	3
Safety Information	3
Overview	4
Introduction	4
Software Features	5
Hardware Features	5
Hardware Installation	6
Installing the Switch on DIN-Rail	6
Wall Mounting Installation	8
Hardware Overview	9
Front Panel	9
Front Panel LEDs	10
Top View Panel	10
Rear Panel	11
Cables	12
Ethernet Cables	12
SFP	14
Console Cable	14
WEB Management	16
Command Line Interface Management	85
About CLI Management	85
Technical Specifications	98

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 Information

- » Only ComNet service personnel can service the equipment. Please contact ComNet Technical Support.
- » The equipment should be installed in locations with controlled access, or other means of security, and controlled by persons of authority.

Overview

Introduction

The CNGE12MS is powerful managed Ethernet switch that has many features. These switches can work under a wide temperature range, dusty environment and humidity condition They can be managed by Windows Utility, WEB, TELNET and Console or other third-party SNMP software as well.

Software Features

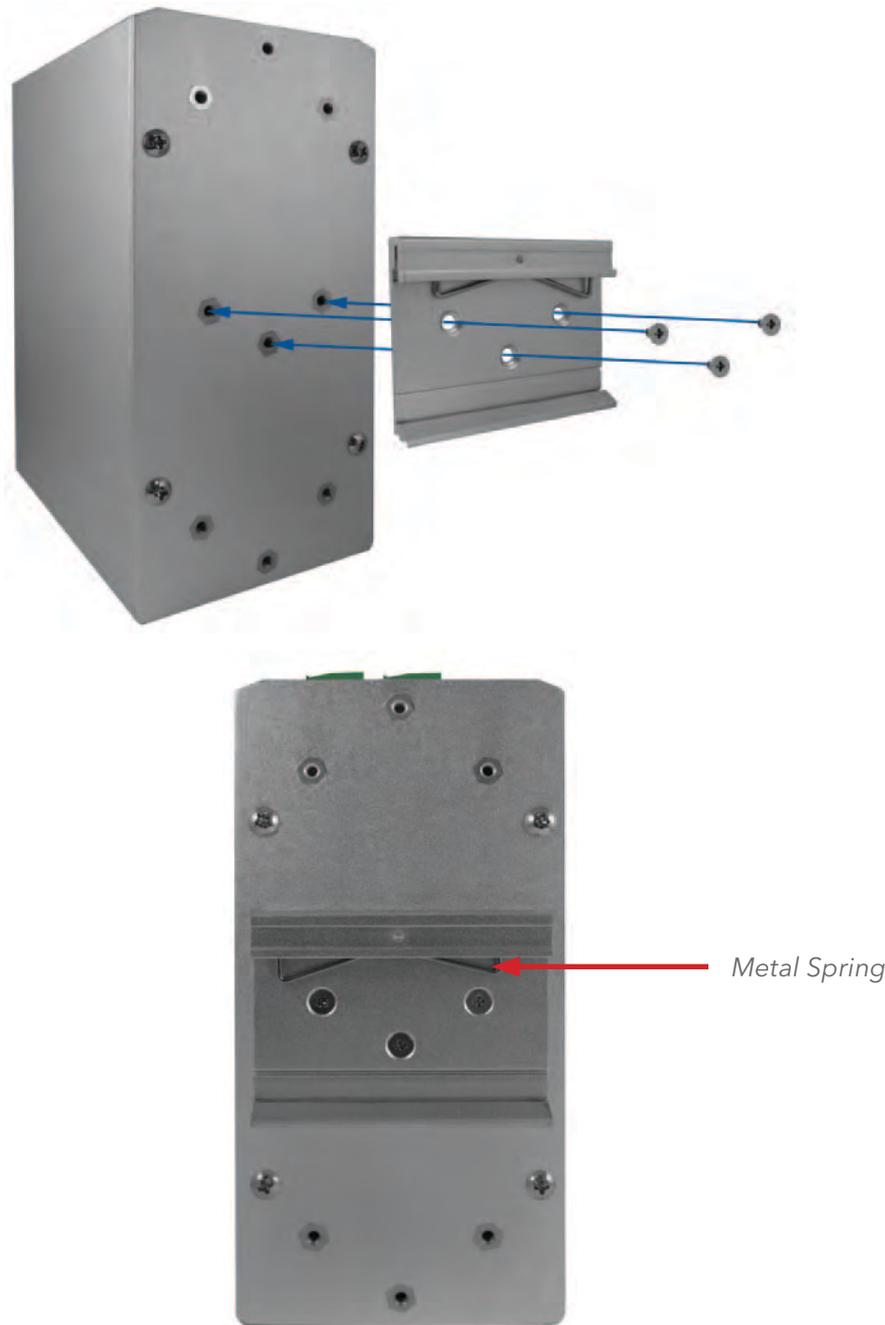
- » Redundant Ethernet Ring (Recovery time < 30ms over 250 unit connection)
- » Supports Ring Coupling, Dual Homing, RSTP over Ring
- » Supports SNMPv1/v2c/v3 & RMON & Port base/IEEE 802.1Q VLAN Network Management
- » Event notification by Email, SNMP trap and Relay Output
- » Windows Utility, Web-based, Telnet and Console (CLI) configuration
- » Enable/disable ports, MAC based port security
- » Port based network access control (IEEE 802.1x)
- » VLAN (IEEE 802.1q) to segregate and secure network traffic
- » Radius centralized password management
- » SNMPv3 encrypted authentication and access security
- » RSTP (IEEE 802.1w)
- » Quality of Service (IEEE 802.1p) for real-time traffic
- » VLAN (IEEE 802.1q) with double tagging and GVRP supported
- » IGMP Snooping for multicast filtering
- » Port configuration, status, statistics, mirroring, security
- » Remote Monitoring (RMON)

Hardware Features

- » Redundant dual DC power inputs
- » Wide Operating Temperature Range: -40° to 75°C
- » Storage Temperature: -40° to 85°C
- » Operating Humidity: 5% to 95%, non-condensing
- » Casing: Aluminum
- » 8 x Gigabit combo ports with 100/1000BASE-X SFP & 10/100/1000BASE-T(X)
- » 4 x 1000BASE-X SFP
- » Console Port
- » Dimensions (W × D × H) 96.4 × 108.5 × 154 mm (3.8 × 4.2.7 × 6.06 in)

Hardware Installation

Installing the Switch on DIN-Rail



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



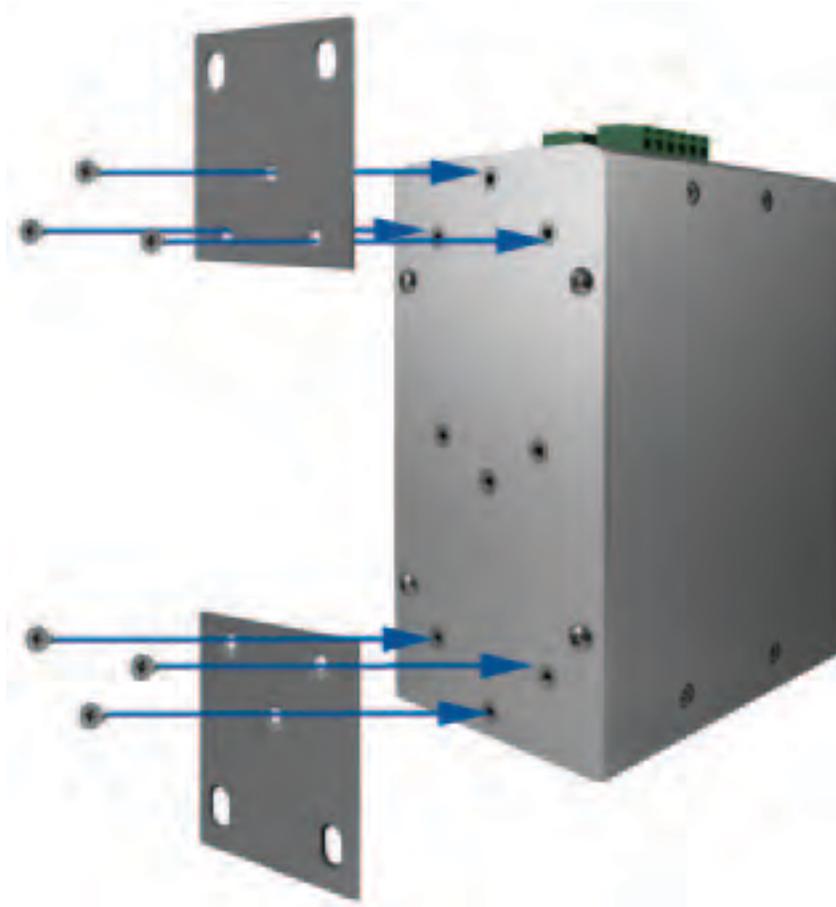
Wall Mounting Installation

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

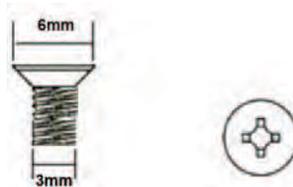
Mounting the CNGE12MS on a Wall

Step 1: Remove Din-Rail kit.

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



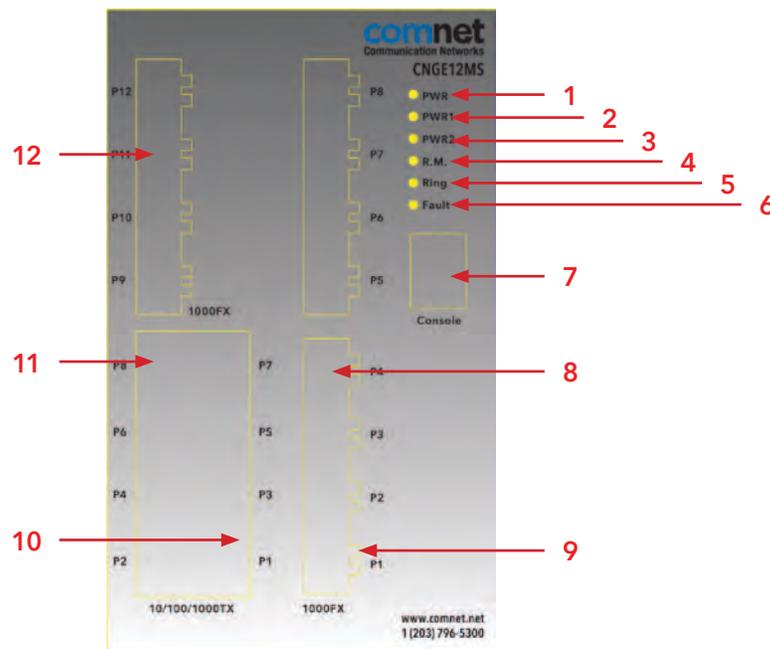
The screw specifications are shown in the following two pictures. In order to prevent switches from being damaged, the screws should not be larger than the size that used in CNGE12MS switch.



Hardware Overview

Front Panel

Port	Description
SFP ports	4 1000BASE-X on SFP port
Combo Port	8 100/1000BASE-X on SFP port and 8 10/100/1000BASE-T(X)
Console	Use RS-232 with RJ-45 connector to manage switch.



CNGE12MS

1. LED for PWR. With PWR UP, the green LED will be light on
2. LED for PWR1
3. LED for PWR2
4. LED for R.M (Ring master). When the LED light is on, it means that this switch is the master.
5. LED for Ring. When the led light is on, it means that C-Ring is activated.
6. LED for Fault. When the light on, it means Power failure or Port down/fail.
7. Console port (RJ-45)
8. 100/1000BASE-X SFP ports (combo)
9. LED for SFP ports link status.
10. LED for Ethernet ports link status.
11. 10/100/1000BASE-T(X) ports (combo)
12. 1000 BASE-X SFP ports

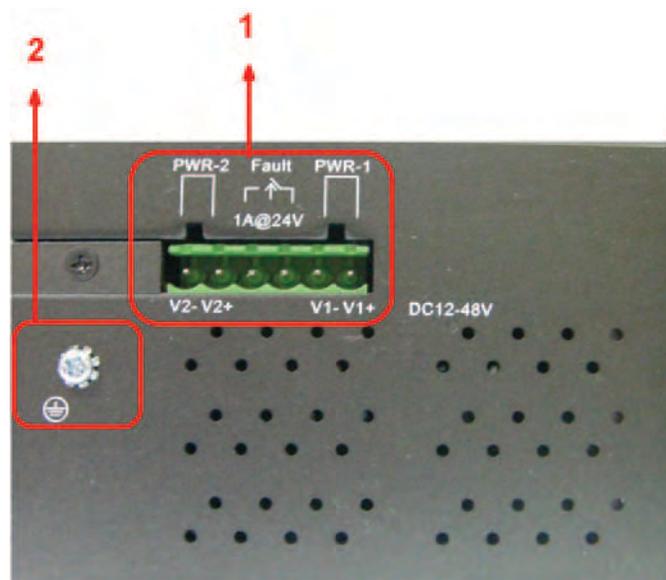
Front Panel LEDs

LED	Color	Status	Description
PWR	Green	On	DC power module up
PW1	Green	On	DC power module 1 activated.
PW2	Green	On	DC Power module 2 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.)
		Fast blinking	Ring is working normally.
Fault	Amber	On	Fault relay. Power failure or Port down/fail.
Gigabit Ethernet ports			
LNK/ACT	Green	Blinking	Data transmitted.
Full Duplex	Amber	On	Port works under full duplex.
Gigabit SFP ports			
LNK/ACT	Green	Blinking	Data transmitted.
		On	Port link up.

Top View Panel

The bottom panel component of CNGE12MS is shown as below:

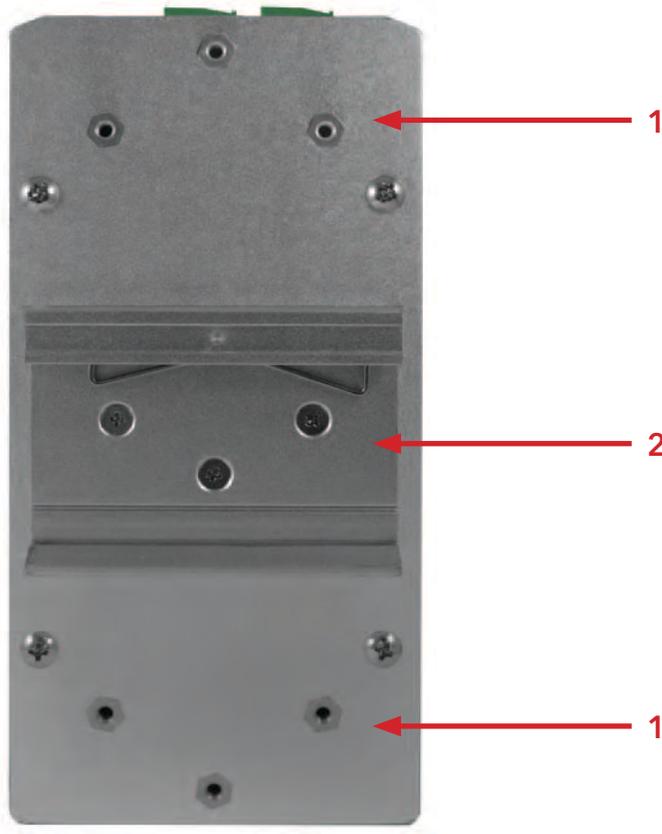
1. Terminal block includes: PWR1, PWR2 (12-48V DC)
2. Ground wire



Rear Panel

The rear panel components of CNGE12MS are shown below:

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



Cables

Ethernet Cables

The CNGE12MS switch has standard Ethernet ports. According to the link type, the switch uses CAT3, CAT4, CAT5 or CAT5-e 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	Type	Max. Length	Connector
10BASE-T	CAT3, CAT4, CAT5 100Ω	UTP 100m (328ft)	RJ-45
100BASE-TX	CAT5 100Ω UTP	UTP 100m (328ft)	RJ-45
1000BASE-TX	CAT5/CAT5-e 100Ω UTP	UTP 100m (328ft)	RJ-45

Cable Types and Specifications

10/100BASE-T(X) Pin Assignments

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

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

10/100 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-

1000 BASE-T RJ-45 Pin Assignments

The CNGE12MS switch supports auto MDI/MDI-X operation. You can use a straight-through cable to connect a PC to the switch. The table below shows the 10/100BASE-T(X) MDI and MDI-X port pin outs.

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

10/100 BASE-T MDI/MDI-X pins assignment

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-

1000 BASE-T MDI/MDI-X pins assignment

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

SFP

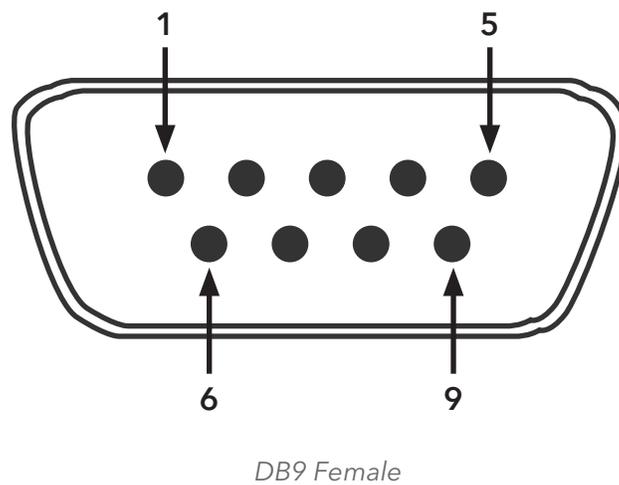
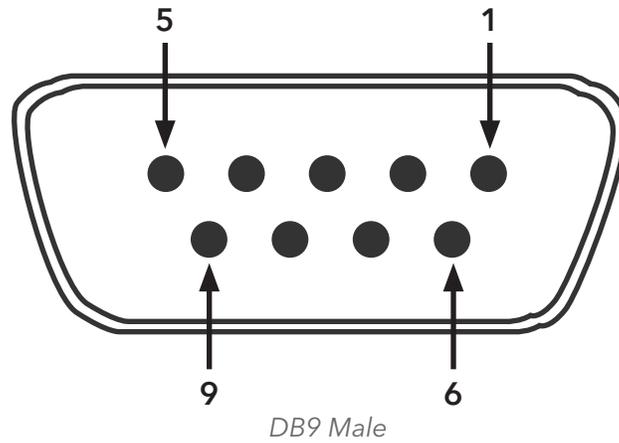
The switch has fiber optic ports with SFP connectors. The fiber optical ports are available with multi-mode and single-mode fiber with various distance and connector types. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.



Console Cable

CNGE12MS switch can be managed by the console port. The DB-9 to RJ-45 cable can be found in the package. You can connect them to the PC via a RS-232 cable with DB-9 female connector and the other end (RJ-45 connector) connects to console port of switch.

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



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 details 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 is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

Note: *By default, IE5.0 or later version does not allow Java Applets to open sockets. 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**

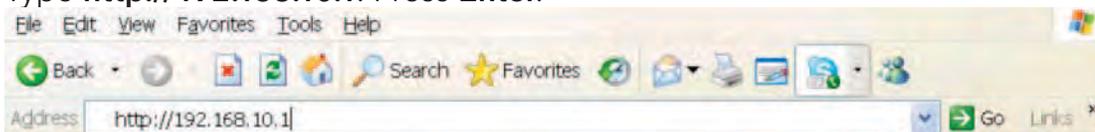
Default Gateway: **192.168.10.254**

User Name: **admin**

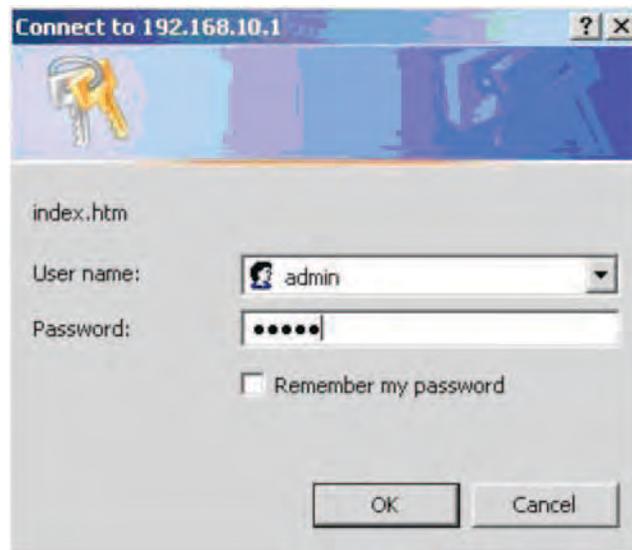
Password: **admin**

System Login

1. Launch Internet Explorer.
2. Type **http://192.168.10.1**. Press **Enter**.

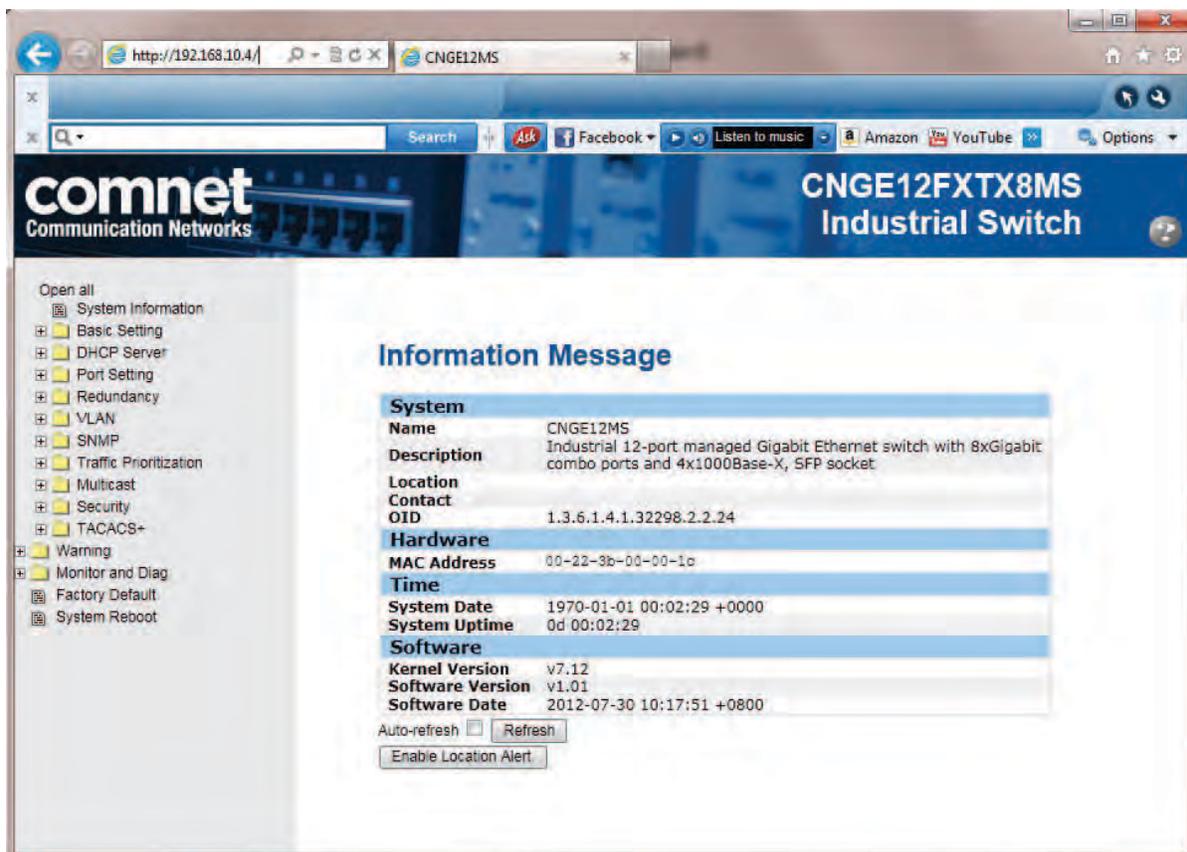


3. The login screen appears.
4. Key in the username and password. The default username and password is **admin**.
5. Select **Enter** or **OK** button, then the main interface of the Web-based management appears.



Login screen

Main Interface



Main interface

Basic Setting

System Information

The switch system information is provided here.



System Information interface

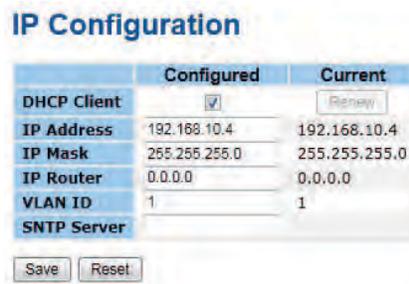
Label	Description
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
System Name	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z, a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
System Location	The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
Timezone Offset	Enter the name of contact person or organization Provide the time zone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes.
Save	Select to save changes.
Reset	Select to undo any changes made locally and revert to previously saved values.

Admin & Password

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

Label	Description
Old Password	Enter the current system password. If this is incorrect, the new password will not be set.
New Password	The system password. The allowed string length is 0 to 31, and the allowed content is the ASCII characters from 32 to 126.
Confirm New password	Re-type the new password.
Save	Select to save changes.

IP Setting



Configure the managed switch IP information on this page.

Label	Description
DHCP Client	Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
IP Address	Assign the IP address that the network is using. If DHCP client function is enabling, 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 display in this column. The default IP is 192.168.10.1
IP Mask	Assign the subnet mask of the IP address. If DHCP client function is enabling, you do not need to assign the subnet mask
IP Router	Assign the network gateway for the switch. The default gateway is 192.168.10.254
VLAN ID	Provide the managed VLAN ID. The allowed range is 1 through 4095.
SNTP Server	SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.
Save	Select to save changes.
Reset	Select to undo any changes made locally and revert to previously saved values.
Renew	Select to renew DHCP. This button is only available if DHCP is enabled.

HTTPS

HTTPS Configuration

Mode 

Label	Description
Mode	Indicates the HTTPS mode operation. Possible modes are: Enabled: Enable HTTPS mode operation. Disabled: Disable HTTPS mode operation.
Automatic Redirect	Indicates the HTTPS redirect mode operation. Automatic redirect web browser to HTTPS during HTTPS mode enabled. Possible modes are: Enabled: Enable HTTPS redirect mode operation. Disabled: Disable HTTPS redirect mode operation.
Save	Select to save changes.
Reset	Select to undo any changes made locally and revert to previously saved values.

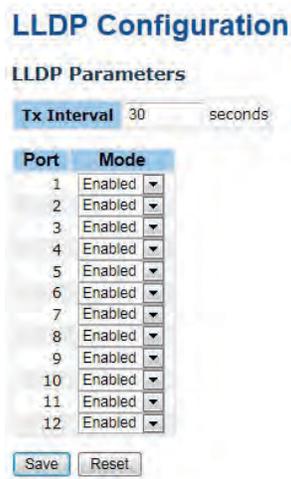
SSH

SSH Configuration

Mode 

Label	Description
Mode	Indicates the SSH mode operation. Possible modes are: Enabled: Enable SSH mode operation. Disabled: Disable SSH mode operation.
Save	Select to save changes.
Reset	Select to undo any changes made locally and revert to previously saved values.

LLDP



LLDP Parameters

This page allows the user to inspect and configure the current LLDP port settings.

Label	Description
Tx Interval	The switch is periodically transmitting LLDP frames to its neighbors for keeping the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds.
Tx Hold	Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.
Tx Delay	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds.
Tx Reinit	When a port is disabled, LLDP is disabled or the switch is rebooted a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Port Configuration

Label	Description
Port	The switch port number of the logical LLDP port.
Mode	<p>Select LLDP mode.</p> <p>Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.</p> <p>Tx only The switch will drop LLDP information received from neighbors, but will send out LLDP information.</p> <p>Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors.</p> <p>Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbors.</p>
CDP Aware	<p>Select CDP awareness.</p> <p>The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP for the port is enabled. Only CDP TLVs that can be mapped into a corresponding field in the LLDP neighbors table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frame are not shown in the LLDP statistic.). CDP TLVs are mapped into LLDP neighbors table as shown below.</p> <p>CDP TLV "Device ID" is mapped into the LLDP "Chassis ID" field.</p> <p>CDP TLV "Address" is mapped into the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table.</p> <p>CDP TLV "Port ID" is mapped into the LLDP "Port ID" field.</p> <p>CDP TLV "Version and Platform" is mapped into the LLDP "System Description" field.</p> <p>Both the CDP and LLDP supports "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors table.</p> <p>If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.</p> <p>Note: When CDP awareness for a port is disabled the CDP information isn't removed immediately, but will be removed when the hold time is exceeded.</p>
Port Descr	Optional TLV: When checked the "port description" is included in LLDP information transmitted.
Sys Name	Optional TLV: When checked the "system name" is included in LLDP information transmitted.
Sys Descr	Optional TLV: When checked the "system description" is included in LLDP information transmitted.
Sys Capa	Optional TLV: When checked the "system capability" is included in LLDP information transmitted.
Mgmt Addr	Optional TLV: When checked the "management address" is included in LLDP information transmitted.

LLDP Neighbor Information

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The columns hold the following information:

LLDP Neighbor Information

Auto-refresh Refresh Open in new window

Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	Management Address
Port.1	00-1E-94-01-10-B4	Port.02	CNGE8MS	1000TX	Bridge(+)	192.168.10.5 (IPv4) O/D:

Label	Description
Local Port	The port on which the LLDP frame was received.
Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.
Remote Port ID	The Remote Port ID is the identification of the neighbor port.
System Name	System Name is the name advertised by the neighbor unit.
Port Description	Port Description is the port description advertised by the neighbor unit.
System Capabilities	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: <ol style="list-style-type: none"> 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
Management Address	Management Address is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address.
Refresh	Select to refresh the page immediately.
Auto-Refresh	Check this box to enable an automatic refresh of the page at regular intervals.

LLDP Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole stack, switch, while local counters refer to counters for the currently selected switch.

Auto-refresh Refresh Clear

Global Counters	
Neighbor entries were last changed at 1970-01-01 21:45:58 +0000 (68 sec. ago)	
Total Neighbors Entries Added	2
Total Neighbors Entries Deleted	1
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

Local Counters								
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	7	3	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	2612	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	6	4	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	2616	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0

Global Counters

Label	Description
Neighbor entries were last changed at	Shows the time for when the last entry was last deleted or added. It is also shows the time elapsed since last change was detected.
Total Neighbors Entries Added	Shows the number of new entries added since switch reboot.
Total Neighbors Entries Deleted	Shows the number of new entries deleted since switch reboot.
Total Neighbors Entries Dropped	Shows the number of LLDP frames dropped due to that the entry table was full.
Total Neighbors Entries Aged Out	Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

Label	Description
Local Port	The port on which LLDP frames are received or transmitted.
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.
Rx Errors	The number of received LLDP frames containing some kind of error.
Frames Discarded	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.
Org. Discarded	The number of organizationally TLVs received.
Age-Outs	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.
Refresh	Select to refresh the page immediately.
Clear	Clears the local counters. All counters (including global counters) are cleared upon reboot.
Auto-Refresh	Check this box to enable an automatic refresh of the page at regular intervals.

Backup/Restore Configuration

You can save/view or load the switch configuration. The configuration file is in XML format with a hierarchy of tags:



Firmware Update

This page facilitates an update of the firmware controlling the switch.



DHCP Server

Setting

The system provides with DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.

DHCP Server Configuration

Enabled	<input type="checkbox"/>
Start IP Address	192.168.10.100
End IP Address	192.168.10.200
Subnet Mask	255.255.255.0
Router	192.168.10.254
DNS	192.168.10.254
Lease Time (sec.)	86400
TFTP Server	0.0.0.0
Boot File Name	

Save Reset

DHCP Dynamic Client List

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

DHCP Dynamic Client List

No.	Select	Type	MAC Address	IP Address	Surplus Lease
-----	--------	------	-------------	------------	---------------

Select/Clear All Add to static Table

DHCP Client List

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

DHCP Client List

MAC Address

IP Address

Add as Static

No.	Select	Type	MAC Address	IP Address	Surplus Lease
-----	--------	------	-------------	------------	---------------

Delete Select/Clear All

Port Setting

Port Control

This page displays current port configurations. Ports can also be configured here.

Port Configuration

Refresh

Auto Detect 100/1000 SFP Enabled

Port	Link	Speed		Flow Control			Maximum Frame	Power Control
		Current	Configured	Current Rx	Current Tx	Configured		
1	1Gfdx	Auto	Auto	X	X	<input type="checkbox"/>	9600	Disabled
2	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600	Disabled
3	1Gfdx	Auto	Auto	X	X	<input type="checkbox"/>	9600	Disabled
4	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600	Disabled
5	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600	Disabled
6	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600	Disabled
7	1Gfdx	Auto	Auto	X	X	<input type="checkbox"/>	9600	Disabled
8	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600	Disabled
9	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600	
10	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600	
11	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600	
12	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600	

Save Reset

Label	Description
Port	This is the logical port number for this row.
Link	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
Current Link Speed	Provides the current link speed of the port.
Configured Link Speed	Select any available link speed for the given switch port. Auto Speed selects the highest speed that is compatible with a link partner. Disabled disables the switch port operation.
Flow Control	When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
Maximum Frame	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 9600 bytes.
Excessive Collision Mode	Configure port transmit collision behavior. Discard: Discard frame after 16 collisions (default). Restart: Restart back-off algorithm after 16 collisions.
Power Control	The Usage column shows the current percentage of the power consumption per port. The Configured column allows for changing the power savings mode parameters per port. Disabled: All power savings mechanisms disabled. ActiPHY: Link down power savings enabled. PerfectReach: Link up power savings enabled. Enabled: Both link up and link down power savings enabled.
Total Power Usage	Total power usage in board, measured in percent.
Select	Select to save changes.
Reset	Select to undo any changes made locally and revert to previously saved values.
Auto-Refresh	Select to refresh the page. Any changes made locally will be undone.

Rate Limit

Configure the switch port rate limit for Policers and Shapers on this page.

Port	Policer Enabled	Policer Rate	Policer Unit	Shaper Enabled	Shaper Rate	Shaper Unit
1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
8	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
9	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
10	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
11	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
12	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps

Save Reset

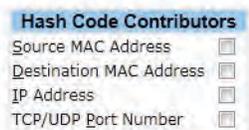
Label	Description
Port	The logical port for the settings contained in the same row.
Policer Enabled	Enable or disable the port policer. The default value is "Disabled".
Policer Rate	Configure the rate for the port policer. The default value is "500". This value is restricted to 500-1000000 when the "Policer Unit" is "kbps", and it is restricted to 1-1000 when the "Policer Unit" is "Mbps"
Policer Unit	Configure the unit of measure for the port policer rate as kbps or Mbps. The default value is "kbps".
Shaper Enabled	Enable or disable the port shaper. The default value is "Disabled".
Shaper Rate	Configure the rate for the port shaper. The default value is "500". This value is restricted to 500-1000000 when the "Policer Unit" is "kbps", and it is restricted to 1-1000 when the "Policer Unit" is "Mbps"
Shaper Unit	Configure the unit of measure for the port shaper rate as kbps or Mbps. The default value is "kbps".
Save	Select to save changes.
Reset	Select to undo any changes made locally and revert to previously saved values.

Port Trunk

Trunk Configuration

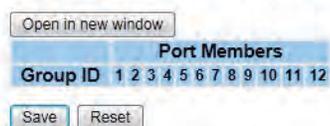
This page is used to configure the Aggregation hash mode and the aggregation group.

Aggregation Mode Configuration



Label	Description
Source MAC Address	The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.
Destination MAC Address	The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.
IP Address	The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.
TCP/UDP Port Number	The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.

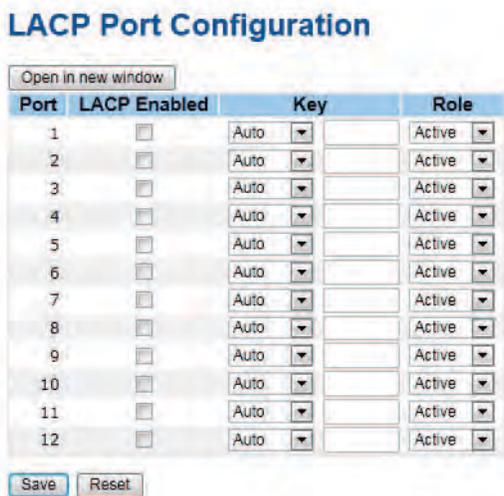
Aggregation Group Configuration



Label	Description
Group ID	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
Port Members	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

LACP Port Configuration

This page allows the user to inspect the current LACP port configurations, and possibly change them as well.



Label	Description
Port	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
LACP Enabled	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.
Key	The Key value incurred by the port, range 1-65535. The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
Role	The Role shows the LACP activity status. Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).
Save	Select to save changes.
Reset	Select to undo any changes made locally and revert to previously saved values.

LACP System Status

This page provides a status overview for all LACP instances.



Label	Description
Aggr ID	The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
Partner System ID	The system ID (MAC address) of the aggregation partner.
Partner Key	The Key that the partner has assigned to this aggregation ID.
Last Changed	The time since this aggregation changed.
Last Changed	Shows which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID:Port".
Refresh	Select to refresh the page immediately.
Auto-Refresh	Check this box to enable an automatic refresh of the page at regular intervals.

LACP Status

This page provides a status overview for LACP status for all ports.

LACP Status

Auto-refresh Refresh Open in new window

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	No	-	-	-	-
6	No	-	-	-	-
7	No	-	-	-	-
8	No	-	-	-	-
9	No	-	-	-	-
10	No	-	-	-	-
11	No	-	-	-	-
12	No	-	-	-	-

Label	Description
Port	The switch port number.
LACP	'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.
Key	The key assigned to this port. Only ports with the same key can aggregate together.
Aggr ID	The Aggregation ID assigned to this aggregation group.
Partner System ID	The partners System ID (MAC address).
Partner Port	The partners port number connected to this port.
Refresh	Select to refresh the page immediately.
Auto-Refresh	Check this box to enable an automatic refresh of the page at regular intervals.

LACP Statistics

This page provides an overview for LACP statistics for all ports.

LACP Statistics

Auto-refresh Refresh Clear

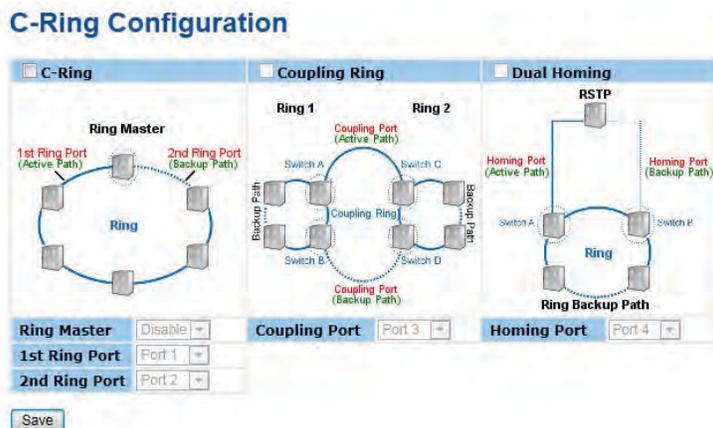
Port	LACP Transmitted	LACP Received	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0

Label	Description
Port	The switch port number
LACP Transmitted	Shows how many LACP frames have been sent from each port
LACP Received	Shows how many LACP frames have been received at each port.
Discarded	Shows how many unknown or illegal LACP frames have been discarded at each port.
Refresh	Select to refresh the page immediately.
Auto-Refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Clear	Clears the counters for all ports

Redundancy

C-Ring

C-Ring is the most powerful Ring in the world. The recovery time of C-Ring is less than 30ms. It can reduce unexpected damage caused by network topology change. C-Ring Supports 3 Ring topologies: C-Ring, Coupling Ring and Dual Homing.

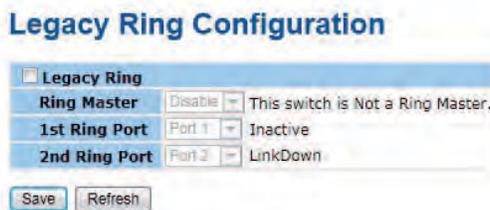


Ring interface

Label	Description
C-Ring	Mark to enable C-Ring.
Ring Master	There should be only one Ring Master in a ring. However if there are two or more switches that 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	The primary port, when this switch is Ring Master.
2nd Ring Port	The backup port, when this switch is Ring Master.
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 switch 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.
Save	Select Save to set the configurations.

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

Legacy Ring



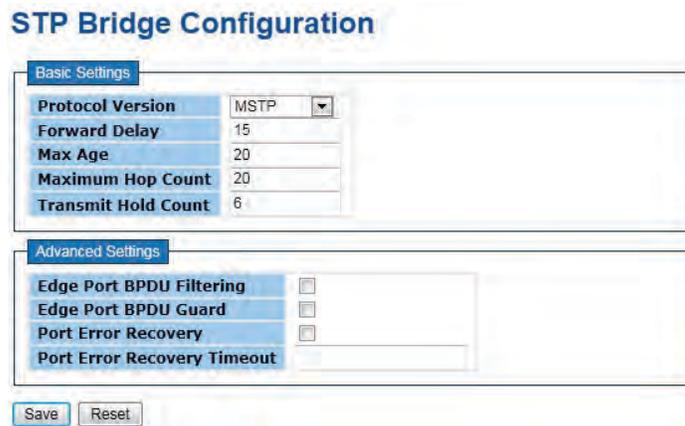
Legacy ring provides support for the switch to be used in an existing ring of ComNet X-Ring enabled switches.

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.

MSTP



Bridge Settings

This page allows you to configure RSTP system settings. The settings are used by all RSTP Bridge instances in the Switch Stack.

Label	Description
Protocol Version	The STP protocol version setting. Valid values are STP, RSTP and MSTP.
Forward Delay	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be $\leq (FwdDelay-1)*2$.
Maximum Hop Count	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range 4 to 30 seconds, and MaxAge must be $\leq (FwdDelay-1)*2$.
Transmit Hold Count	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.
Save	Select to save changes.
Reset	Select to undo any changes made locally and revert to previously saved values.

MSTI Mapping

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

MSTI Configuration

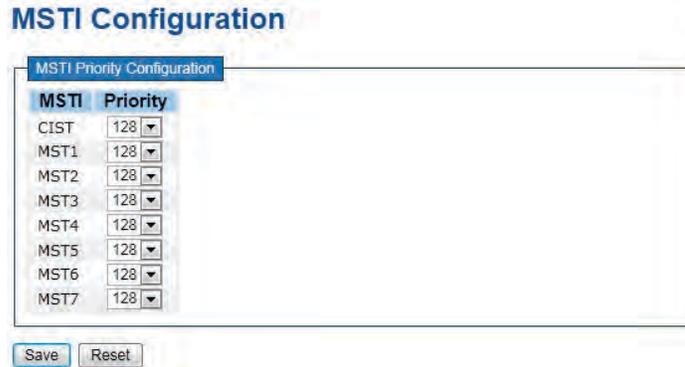
Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Label	Description
Configuration Name	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name can have a maximum of 32 characters.
Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
MSTI	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
VLANs Mapped	The list of VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)
Save	Select to save changes.
Reset	Select to undo any changes made locally and revert to previously saved values.

MSTI Priorities

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.



Label	Description
MSTI	The bridge instance. The CIST is the default instance, which is always active.
Priority	Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.
Save	Select to save changes.
Reset	Select to undo any changes made locally and revert to previously saved values.

CIST Ports

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well. This page contains settings for physical and aggregated ports. The aggregation settings are stack global.

STP CIST Ports Configuration

CIST Aggregated Ports Configuration									
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
-	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True

CIST Normal Ports Configuration									
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
1	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
5	<input checked="" type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
7	<input checked="" type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
8	<input checked="" type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
9	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
10	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
11	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
12	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Save Reset

Label	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
OpenEdge (state flag)	Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transitioning to the forwarding state is faster for edge ports (having operEdge true) than for other ports.
AdminEdge	Controls whether the operEdge flag should start as being set or cleared. (The initial operEdge state when a port is initialized).
AutoEdge	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

Restricted Role	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
Restricted TCN	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or is the physical link state for the attached LANs transitions frequently.
Point-to-Point	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.
Save	Select to save changes.
Reset	Select to undo any changes made locally and revert to previously saved values.

MSTI Ports

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well. A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are stack global.

MSTI Port Configuration

Select MSTI

MST1

- MST1
- MST2
- MST3
- MST4
- MST5
- MST6
- MST7

MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost	Priority
-	Auto <input type="text"/>	128 <input type="text"/>

MSTI Normal Ports Configuration

Port	Path Cost	Priority
1	Auto <input type="text"/>	128 <input type="text"/>
2	Auto <input type="text"/>	128 <input type="text"/>
3	Auto <input type="text"/>	128 <input type="text"/>
4	Auto <input type="text"/>	128 <input type="text"/>
5	Auto <input type="text"/>	128 <input type="text"/>
6	Auto <input type="text"/>	128 <input type="text"/>
7	Auto <input type="text"/>	128 <input type="text"/>
8	Auto <input type="text"/>	128 <input type="text"/>
9	Auto <input type="text"/>	128 <input type="text"/>
10	Auto <input type="text"/>	128 <input type="text"/>
11	Auto <input type="text"/>	128 <input type="text"/>
12	Auto <input type="text"/>	128 <input type="text"/>

Label	Description
Port	The switch port number of the corresponding STP CIST (and MSTI) port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
Save	Select to save changes.
Clear	Select to undo any changes made locally and revert to previously saved values.

STP Bridges

This page provides a status overview for all STP bridge instances.

The displayed table contains a row for each STP bridge instance, where the column displays the following information:

STP Bridges

Auto-refresh Refresh

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	80:00-00:22:3B:00:00:1C	80:00-00:22:3B:00:00:1C	-	0	Steady	1d 20:03:50

Label	Description
MSTI	The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
Bridge ID	The Bridge ID of this Bridge instance.
Root ID	The Bridge ID of the currently elected root bridge.
Root Port	The switch port currently assigned the root port role.
Root Cost	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Topology Flag	The current state of the Topology Change Flag for this Bridge instance.
Topology Change Last	The time since last Topology Change occurred.
Refresh	Select to refresh the page immediately.
Auto-Refresh	Check this box to enable an automatic refresh of the page at regular intervals.

STP Port Status

This page displays the STP CIST port status for port physical ports in the currently selected switch.

STP Port Status

Auto-refresh Refresh

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Disabled	Discarding	-
6	Non-STP	Forwarding	-
7	DesignatedPort	Forwarding	0d 21:47:41
8	Disabled	Discarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding	-

Label	Description
Port	The switch port number of the logical STP port.
CIST Role	The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort.
State	The current STP port state of the CIST port. The port state can be one of the following values: Blocking Learning Forwarding.
Uptime	The time since the bridge port was last initialized.
Refresh	Select to refresh the page immediately.
Auto-Refresh	Check this box to enable an automatic refresh of the page at regular intervals.

STP Statistics

This page displays the RSTP port statistics counters for bridge ports in the currently selected switch.

STP Statistics

Auto-refresh Refresh Clear

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
7	39255	40113	0	0	0	0	0	0	0	0

Label	Description
Port	The switch port number of the logical RSTP port.
RSTP	The number of RSTP Configuration BPDU's received/transmitted on the port.
STP	The number of legacy STP Configuration BPDU's received/transmitted on the port.
TCN	The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
Discarded Unknown	The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
Discarded Illegal	The number of illegal Spanning Tree BPDU's received (and discarded) on the port.
Refresh	Select to refresh the page immediately.
Auto-Refresh	Check this box to enable an automatic refresh of the page at regular intervals.

VLAN

VLAN Membership Configuration

The VLAN membership configuration for the selected stack switch unit switch can be monitored and modified here. Up to 64 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

VLAN Membership Configuration



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

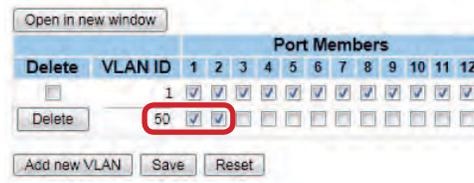
Adding a New Static Entry Select **Add New VLAN** to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The VLAN is enabled on the selected stack switch unit when you select on **Save**. The VLAN is thereafter present on the other stack switch units, but with no port members. A VLAN without any port members on any stack unit will be deleted when you select **Save**. The **Delete** button can be used to undo the addition of new VLANs.

Example: Portbased VLAN Setting

(For ingress port)

1. VLAN Membership Configuration setting port 1 & VID=50

VLAN Membership Configuration



2. VLAN Port 1 Configuration-->Disable VLAN Aware

VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	<input type="checkbox"/>	All	Specific	50
2	<input type="checkbox"/>	All	Specific	50
3	<input type="checkbox"/>	All	Specific	1
4	<input type="checkbox"/>	All	Specific	1

3. VLAN Port 1 Configuration-->Mode=specific, ID=50

VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	<input type="checkbox"/>	All	Specific	50
2	<input type="checkbox"/>	All	Specific	50
3	<input type="checkbox"/>	All	Specific	1
4	<input type="checkbox"/>	All	Specific	1

(For egress port)

1. VLAN Membership Configuration setting port 2 & VID=50

VLAN Membership Configuration



2. VLAN Port 2 Configuration-->VLAN Aware has no effect

VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	<input type="checkbox"/>	All	Specific	50
2	<input type="checkbox"/>	All	Specific	50
3	<input type="checkbox"/>	All	Specific	1
4	<input type="checkbox"/>	All	Specific	1

3. VLAN Port 2 Configuration-->Mode=specific, ID=50

(any packet can enter egress port)

VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	<input type="checkbox"/>	All	Specific	50
2	<input type="checkbox"/>	All	Specific	50
3	<input type="checkbox"/>	All	Specific	1
4	<input type="checkbox"/>	All	Specific	1

802.1Q Access port Setting

(For ingress port)

1. VLAN Membership Configuration setting port & VID=50

VLAN Membership Configuration

Open in new window

		Port Members											
Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>											
<input type="checkbox"/>	50	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add new VLAN Save Reset

2. VLAN Port Configuration-->Enable VLAN Aware

VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	<input checked="" type="checkbox"/>	All	Specific	50
2	<input type="checkbox"/>	All	Specific	1
3	<input type="checkbox"/>	All	Specific	1
4	<input type="checkbox"/>	All	Specific	1
5	<input type="checkbox"/>	All	Specific	1

3. VLAN Port Configuration-->Mode=specific, ID=50

VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	<input checked="" type="checkbox"/>	All	Specific	50
2	<input type="checkbox"/>	All	Specific	1
3	<input type="checkbox"/>	All	Specific	1
4	<input type="checkbox"/>	All	Specific	1
5	<input type="checkbox"/>	All	Specific	1

(For egress port)

1. VLAN Membership Configuration setting port & VID=50

VLAN Membership Configuration

Open in new window

		Port Members											
Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>											
<input type="checkbox"/>	50	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add new VLAN Save Reset

2. VLAN Port Configuration-->Disable VLAN Aware

VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	<input checked="" type="checkbox"/>	All	Specific	50
2	<input type="checkbox"/>	All	Specific	1
3	<input type="checkbox"/>	All	Specific	1
4	<input type="checkbox"/>	All	Specific	1
5	<input type="checkbox"/>	All	Specific	1

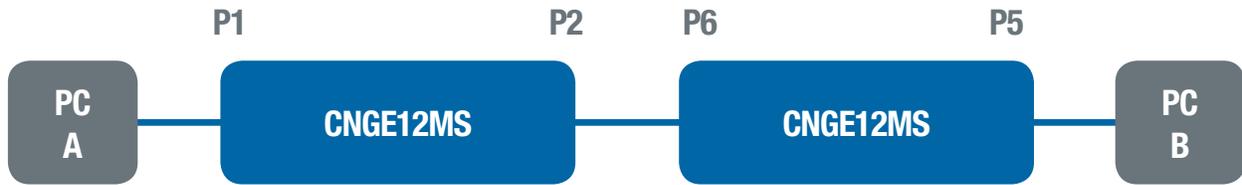
3. VLAN Port Configuration-->Mode=specific, ID=50

(untagged & tag=50 packet can enter egress port)

VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	<input type="checkbox"/>	All	Specific	50
2	<input type="checkbox"/>	All	Specific	1
3	<input type="checkbox"/>	All	Specific	1
4	<input type="checkbox"/>	All	Specific	1
5	<input type="checkbox"/>	All	Specific	1

802.1Q Trunk port setting (multi-tag)



(For ingress port)

1. VLAN Membership Configuration setting port & VID=11, 22, 33

VLAN Membership Configuration

Open in new window

Delete	VLAN ID	Port Members											
		1	2	3	4	5	6	7	8	9	10	11	12
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>											
<input type="checkbox"/>	11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	22	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	33	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. VLAN Port Configuration-->Enable VLAN Aware

VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	<input checked="" type="checkbox"/>	All	Specific	11
2	<input checked="" type="checkbox"/>	All	Specific	
3	<input checked="" type="checkbox"/>	All	Specific	1
4	<input checked="" type="checkbox"/>	All	Specific	1
5	<input type="checkbox"/>	All	Specific	1

3. VLAN Port Configuration-->Mode=specific, ID=11

(when entering packet is untagged frame, added tag = 11

When entering the tagged frame, only VID = 11, 22, 33 three kinds of packets can pass)

VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	<input checked="" type="checkbox"/>	All	Specific	11
2	<input checked="" type="checkbox"/>	All	Specific	
3	<input checked="" type="checkbox"/>	All	Specific	1
4	<input checked="" type="checkbox"/>	All	Specific	1
5	<input type="checkbox"/>	All	Specific	1

(For egress port)

1. VLAN Membership Configuration setting port, VID=11, 22, 33

VLAN Membership Configuration

Open in new window

		Port Members											
Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>											
<input type="checkbox"/>	11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	22	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	33	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. VLAN Port Configuration-->Enable VLAN Aware

VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN Mode	ID
1	<input type="checkbox"/>	All	Specific	50
2	<input type="checkbox"/>	All	Specific	50
3	<input type="checkbox"/>	All	Specific	1
4	<input type="checkbox"/>	All	Specific	1
5	<input checked="" type="checkbox"/>	All	Specific	11
6	<input checked="" type="checkbox"/>	All	Specific	1
7	<input checked="" type="checkbox"/>	All	Specific	1
8	<input checked="" type="checkbox"/>	All	Specific	1
9	<input type="checkbox"/>	All	Specific	1
10	<input type="checkbox"/>	All	Specific	1
11	<input type="checkbox"/>	All	Specific	1

3. VLAN Port Configuration-->Mode=none

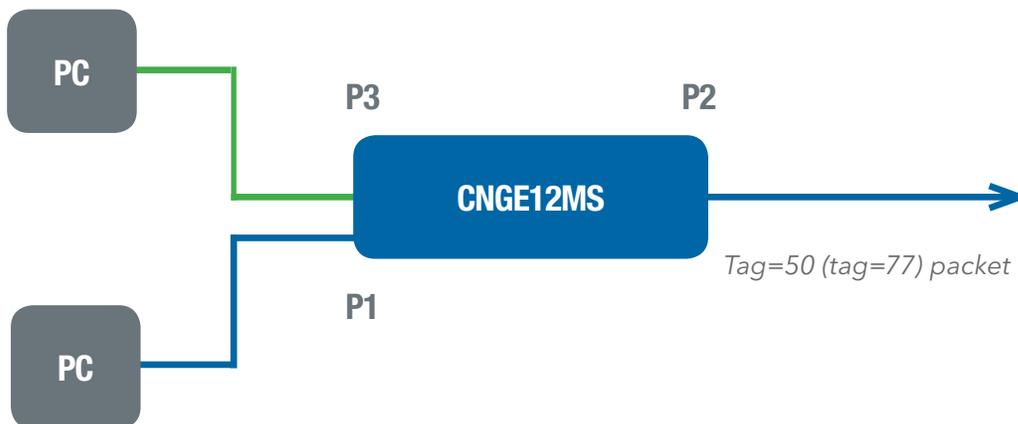
(egress port can receive tag=11, 22, 33 packet

In addition, only tag=11 packet can enter egress port)

VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN Mode	ID
1	<input type="checkbox"/>	All	Specific	50
2	<input type="checkbox"/>	All	Specific	50
3	<input type="checkbox"/>	All	Specific	1
4	<input type="checkbox"/>	All	Specific	1
5	<input checked="" type="checkbox"/>	All	Specific	11
6	<input checked="" type="checkbox"/>	All	Specific	1
7	<input checked="" type="checkbox"/>	All	Specific	1
8	<input checked="" type="checkbox"/>	All	Specific	1
9	<input type="checkbox"/>	All	Specific	1
10	<input type="checkbox"/>	All	Specific	1
11	<input type="checkbox"/>	All	Specific	1

Q-in-Q VLAN Setting



Ingress Port 1----->Egress Port 2

(For ingress port-----Port 1)

1. VLAN Membership Configuration setting port 1, 2 and 3 & VID=50

VLAN Membership Configuration

Open in new window

		Port Members											
Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>											
<input type="checkbox"/>	50	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add new VLAN Save Reset

2. VLAN Port Configuration-->Disable Port 1 VLAN Aware

VLAN Port Configuration

Port	VLAN Aware	Frame Type	Port VLAN Mode	ID
1	<input type="checkbox"/>	All	Specific	50
2	<input checked="" type="checkbox"/>	All	None	1
3	<input checked="" type="checkbox"/>	All	None	1
4	<input type="checkbox"/>	All	Specific	1
5	<input type="checkbox"/>	All	Specific	1

3. VLAN Port Configuration-->Port 1 Mode=specific, ID=50

VLAN Port Configuration

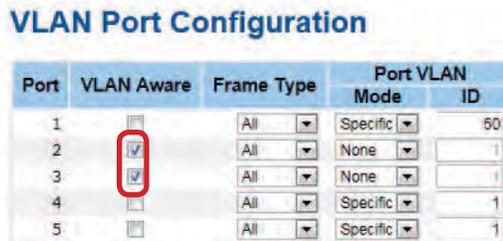
Port	VLAN Aware	Frame Type	Port VLAN Mode	ID
1	<input type="checkbox"/>	All	Specific	50
2	<input checked="" type="checkbox"/>	All	None	1
3	<input checked="" type="checkbox"/>	All	None	1
4	<input type="checkbox"/>	All	Specific	1
5	<input type="checkbox"/>	All	Specific	1

(For egress port ----Port 2)

1. VLAN Membership Configuration setting port & VID=50

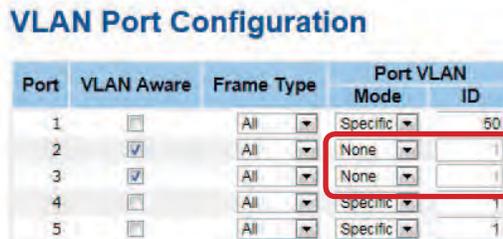


2. VLAN Port Configuration-->Enable Port 2 and 3 VLAN Aware.



3. VLAN Port Configuration-->Mode=none

(only tag=50 packet can enter egress port)



Private VLAN

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Private VLAN ID	Indicates the ID of this particular private VLAN.
MAC Address	The MAC address for the entry.
Port Members	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New Static Entry Select **Add New Private VLAN** to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Select **OK** to discard the incorrect entry, or select **Cancel** to return to the editing and make a correction.

The Private VLAN is enabled when you select **Save**.

The **Delete** button can be used to undo the addition of new Private VLANs.

Private VLAN Membership Configuration



Label	Description
Port Members	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled for that port. When unchecked, port isolation is disabled for that port. By default, port isolation is disabled for all ports.

SNMP

SNMP-System

SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e50171990001

Label	Description
Mode	Indicates the SNMP mode operation. Possible modes are: Enabled: Enable SNMP mode operation. SNMP v2c: Set SNMP supported version 2c. Disabled: Disable SNMP mode operation.
Version	Indicates the SNMP supported version. Possible versions are: SNMP v1: Set SNMP supported version 1. SNMP v3: Set SNMP supported version 3.
Read Community	Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using USM for authentication and privacy and the community string will associated with SNMPv3 communities table
Write Community	Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using USM for authentication and privacy and the community string will associated with SNMPv3 communities table.
Engine ID	Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

SNMP Trap Configuration

Trap Mode	Disabled
Trap Version	SNMP v1
Trap Community	public
Trap Destination Address	
Trap Authentication Failure	Enabled
Trap Link-up and Link-down	Enabled
Trap Inform Mode	Enabled
Trap Inform Timeout (seconds)	
Trap Inform Retry Times	

Save Reset

Label	Description
Trap Mode	Indicates the SNMP trap mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.
Trap Version	Indicates the SNMP trap supported version. Possible versions are: SNMP v1: Set SNMP trap supported version 1. SNMP v2c: Set SNMP trap supported version 2c. SNMP v3: Set SNMP trap supported version 3.
Trap Community	Indicates the community access string when send SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.
Trap Destination Address	Indicates the SNMP trap destination address. Trap Destination IPv6 Address
Trap Destination IPv6 Address	Provide the trap destination IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80:215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example, ':::192.1.2.34'.
Trap Authentication Failure	Indicates the SNMP entity is permitted to generate authentication failure traps. Possible modes are: Enabled: Enable SNMP trap authentication failure. Disabled: Disable SNMP trap authentication failure.
Trap Link-up and Link-down	Indicates the SNMP trap link-up and link-down mode operation. Possible modes are: Enabled: Enable SNMP trap link-up and link-down mode operation. Disabled: Disable SNMP trap link-up and link-down mode operation.
Trap Inform Mode	Indicates the SNMP trap inform mode operation. Possible modes are: Enabled: Enable SNMP trap inform mode operation. Disabled: Disable SNMP trap inform mode operation.
Trap Inform Timeout(seconds)	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.
Trap Inform Retry Times	Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.
Trap Probe Security Engine ID	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: Enabled: Enable SNMP trap probe security engine ID mode of operation. Disabled: Disable SNMP trap probe security engine ID mode of operation.
Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed.
Trap Security Name	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

SNMP-Communities

Configure SNMPv3 communities table on this page. The entry index key is Community.

SNMPv3 Communities Configuration

Delete	Community	Source IP	Source Mask
<input type="checkbox"/>	public	0.0.0.0	0.0.0.0
<input type="checkbox"/>	private	0.0.0.0	0.0.0.0

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Community	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Source IP	Indicates the SNMP access source address.
Source Mask	Indicates the SNMP access source address mask.

SNMP-Users

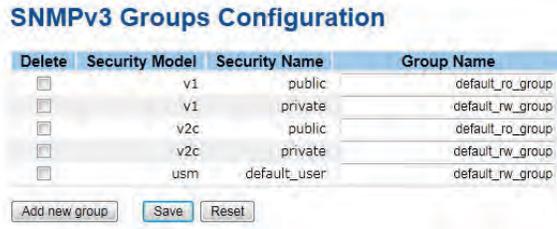
Configure SNMPv3 users table on this page. The entry index keys are Engine ID and User Name.



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equals system engine ID then it is local user; otherwise it is remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: None authentication and none privacy. Auth, NoPriv: Authentication and none privacy. Auth, Priv: Authentication and privacy. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: None: None authentication protocol. MD5: An optional flag to indicate that this user using MD5 authentication protocol. SHA: An optional flag to indicate that this user using SHA authentication protocol. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
Authentication Password	A string identifying the authentication pass phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is the ASCII characters from 33 to 126.
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are: None: None privacy protocol. DES: An optional flag to indicate that this user using DES authentication protocol.
Privacy Password	A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126.

SNMP-Groups

Configure SNMPv3 groups table on this page. The entry index keys are Security Model and Security Name.



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: v1: Reserved for SNMPv1. v2c: Reserved for SNMPv2c. usm: User-based Security Model (USM).
Security Name	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

SNMP-Views

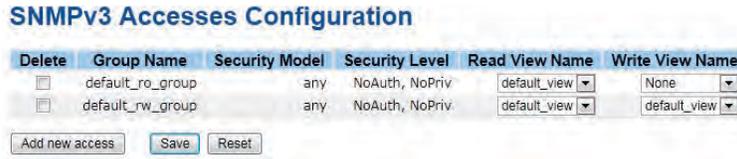
Configure SNMPv3 views table on this page. The entry index keys are View Name and OID Subtree.



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
View Type	Indicates the view type that this entry should belong to. Possible view types are: included: An optional flag to indicate that this view subtree should be included. excluded: An optional flag to indicate that this view subtree should be excluded. Generally, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID subtree overstep the 'excluded' view entry.
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is a digital number or an asterisk(*).

SNMP-Accesses

Configure SNMPv3 accesses table on this page. The entry index keys are Group Name, Security Model and Security Level.



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: any: Accepted any security model (v1 v2c usm). v1: Reserved for SNMPv1. v2c: Reserved for SNMPv2c. usm: User-based Security Model (USM).
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: None authentication and none privacy. Auth, NoPriv: Authentication and none privacy. Auth, Priv: Authentication and privacy.
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Write View Name	The name of the MIB view defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

Traffic Prioritization

Port Configuration

This page allows you to configure QoS settings for each port.

Frames can be classified by 4 different QoS classes: Low, Normal, Medium, and High.

The classification is controlled by a QCL that is assigned to each port.

A QCL consists of an ordered list of up to 12 QCEs.

Each QCE can be used to classify certain frames to a specific QoS class.

This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority.

Frames not matching any of the QCEs are classified to the default QoS class for the port.

Port QoS Configuration

Port QoS Configuration

Ingress Configuration				Egress Configuration				
Port	Default Class	QCL #	Tag Priority	Queuing Mode	Queue Weighted			
					Low	Normal	Medium	High
1	Low	1	0	Strict Priority	1	2	3	4
2	Low	1	0	Strict Priority	1	3	4	5
3	High	1	0	Strict Priority	1	3	4	5
4	Low	1	0	Strict Priority	1	2	4	2
5	Low	1	0	Strict Priority	1	3	4	5
6	Low	1	0	Strict Priority	1	2	4	5
7	Low	1	0	Strict Priority	1	2	3	3
8	Low	1	0	Strict Priority	1	2	4	5
9	Low	1	0	Strict Priority	1	2	4	5
10	Low	1	0	Strict Priority	1	2	4	5
11	Low	1	0	Strict Priority	1	2	4	5
12	Low	1	0	Strict Priority	1	2	4	5

Save Reset

Label	Description
Port	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled for that port. When unchecked, port isolation is disabled for that port. By default, port isolation is disabled for all ports.
Default Class	Configure the default QoS class for the port, that is, the QoS class for frames not matching any of the QCEs in the QCL.
QCL#	Select which QCL to use for the port.
Tag Priority	Select the default tag priority for this port when adding a Tag to the untagged frames.
Queuing Mode	Select which Queuing mode for this port.
Queue Weighted	Setting Queue weighted (Low = Normal, Medium = High) if the "Queuing Mode" is "Weighted".

QoS Control List

This page lists the QCEs for a given QCL.

Frames can be classified by 4 different QoS classes: Low, Normal, Medium, and High.

The classification is controlled by a QoS assigned to each port.

A QCL consists of an ordered list of up to 12 QCEs.

Each QCE can be used to classify certain frames to a specific QoS class.

This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority. Frames not matching any of the QCEs are classified to the default QoS Class for the port.



Label	Description
QCL#	Select a QCL to display a table that lists all the QCEs for that particular QCL.
QCE Typ	Specifies which frame field the QCE processes to determine the QoS class of the frame. The following QCE types are supported: Ethernet Type: The Ethernet Type field. If frame is tagged, this is the Ethernet Type that follows the tag header. VLAN ID: VLAN ID. Only applicable if the frame is VLAN tagged. TCP/UDP Port: IPv4 TCP/UDP source/destination port. DSCP: IPv4 and IPv6 DSCP. ToS: The 3 precedence bit in the ToS byte of the IPv4/IPv6 header (also known as DS field). Tag Priority: User Priority. Only applicable if the frame is VLAN tagged or priority tagged.
Type Value	Indicates the value according to its QCE type. Ethernet Type: The field shows the Ethernet Type value. VLAN ID: The field shows the VLAN ID. TCP/UDP Port: The field shows the TCP/UDP port range. DSCP: The field shows the IPv4/IPv6 DSCP value.
Traffic Class	The QoS class associated with the QCE.
Modification Buttons	You can modify each QCE in the table using the following buttons: + : Inserts a new QCE before the current row. e : Edits the QCE. /\ : Moves the QCE up the list. \/ : Moves the QCE down the list. x : Deletes the QCE. + : The lowest plus sign adds a new entry at the bottom of the list of QCL.

Storm Control

Storm control for the switch is configured on this page.

Storm Control Configuration

Frame Type	Status	Rate (pps)
Unicast	<input type="checkbox"/>	1K
Multicast	<input type="checkbox"/>	1K
Broadcast	<input type="checkbox"/>	1K

Save Reset

There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

The rate is 2^n , where n is equal to or less than 15, or "No Limit". The unit of the rate can be either pps (packets per second) or kpps (kilopackets per second). The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

(Note: Frames, which are sent to the CPU of the switch are always limited to approximately 4 kpps. For example, broadcasts in the management VLAN are limited to this rate. The management VLAN is configured on the IP setup page.)

Label	Description
Frame Type	The settings in a particular row apply to the frame type listed here: unicast, multicast, or broadcast.
Status	Enable or disable the storm control status for the given frame type.
Rate	The rate unit is packet per second (pps), configure the rate as 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. The 1 kpps is actually 1002.1 pps.

Wizard

This handy wizard helps you set up a QCL quickly.

Welcome to the QCL Configuration Wizard!

Please select an action:

- Set up IP Cam High Performance**
Increase IP Cam performance.
- Set up Port Policies**
Group ports into several types according to different QCL policies.
- Set up Typical Network Application Rules**
Set up the specific QCL for different typical network application quality control.
- Set up ToS Precedence Mapping**
Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.
- Set up VLAN Tag Priority Mapping**
Set up the traffic class mapping to the user priority value (3 bits) when receiving VLAN tagged packets.

To continue, click Next.

Next >

Label	Description
Set up Port Policies	Group ports into several types according to different QCL policies.
Set up Typical Network Application Rules	Set up the specific QCL for different typical network application quality control.
Set up ToS Precedence Mapping	Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.
Set up VLAN Tag Priority Mapping	Set up the traffic class mapping to the User Priority value (3 bits) when receiving VLAN tagged packets.

IGMP Snooping

This page provides IGMP Snooping related configuration.

Label	Description
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMC Flooding enabled	Enable unregistered IPMC traffic flooding.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping.
IGMP Querier	Enable the IGMP Query in the VLAN. The Query will send out if no Query received in 255 seconds after IGMP Query Enabled. Each Querier's interval is 125 seconds, and it will stop and act as an IGMP Querier if received any Query from other devices.
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP query. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port.

IGMP Snooping Status

Auto-refresh Refresh Clear Open in new window

IGMP Snooping Status

Statistics

VLAN ID	Querier Status	Querier Transmit	Querier Receive	V1 Reports Receive	V2 Reports Receive	V3 Reports Receive	V2 Leave Receive
1	IDLE	0	0	0	0	0	0

IGMP Groups

VLAN ID	Groups	Port Members											
		1	2	3	4	5	6	7	8	9	10	11	12
No IGMP groups													

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-

Label	Description
VLAN ID	The VLAN ID of the entry.
Groups	The present IGMP groups. Max. are 128 groups for each VLAN.
Port Members	The ports that are members of the entry.
Querier Status	Show the Querier status is "ACTIVE" or "IDLE".
Querier Receive	The number of Transmitted Queries.
V1 Reports Receive	The number of Received V1 Reports.
V2 Reports Receive	The number of Received V2 Reports.
V3 Reports Receive	The number of Received V3 Reports.
V2 Leave Receive	The number of Received V2 Leave.
Refresh	Select to refresh the page immediately.
Clear	Clears all Statistics counters.
Auto-Refresh	Check this box to enable an automatic refresh of the page at regular intervals.

Security

ACL

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Copy	Logging	Shutdown	Counter
1	1	Permit	Disabled	Disabled	Disabled	Disabled	54367
2	1	Permit	Disabled	Disabled	Disabled	Disabled	0
3	1	Permit	Disabled	Disabled	Disabled	Disabled	15255
4	1	Permit	Disabled	Disabled	Disabled	Disabled	0
5	1	Permit	Disabled	Disabled	Disabled	Disabled	67
6	1	Permit	Disabled	Disabled	Disabled	Disabled	1153
7	1	Permit	Disabled	Disabled	Disabled	Disabled	6874
8	1	Permit	Disabled	Disabled	Disabled	Disabled	0
9	1	Permit	Disabled	Disabled	Disabled	Disabled	0
10	1	Permit	Disabled	Disabled	Disabled	Disabled	0
11	1	Permit	Disabled	Disabled	Disabled	Disabled	0
12	1	Permit	Disabled	Disabled	Disabled	Disabled	0

Label	Description
Port	The logical port for the settings contained in the same row.
Policy ID	Select the policy to apply to this port. The allowed values are 1 through 8. The default value is 1.
Action	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
Rate Limiter ID	Select which rate limiter to apply to this port. The allowed values are Disabled or the values 1 through 15. The default value is "Disabled".
Port Copy	Select which port frames are copied to. The allowed values are Disabled or a specific port number. The default value is "Disabled".
Logging	Specify the logging operation of this port. The allowed values are: Enabled: Frames received on the port are stored in the System Log. Disabled: Frames received on the port are not logged. The default value is "Disabled". Please note that the System Log memory size and logging rate is limited.
Shutdown	Specify the port shut down operation of this port. The allowed values are: Enabled: If a frame is received on the port, the port will be disabled. Disabled: Port shut down is disabled. The default value is "Disabled".
Counter	Counts the number of frames that match this ACE.

802.1x

This page allows you to configure how an administrator is authenticated when he logs into the switch stack via TELNET, SSH or the web pages.

Authentication Configuration

Client Configuration

Client	Authentication Method	Fallback
telnet	local	<input type="checkbox"/>
web	local	<input type="checkbox"/>
console	local	<input type="checkbox"/>

RADIUS Authentication Server Configuration

#	Enabled	IP Address	Port	Secret
1	<input type="checkbox"/>		1812	
2	<input type="checkbox"/>		1812	
3	<input type="checkbox"/>		1812	
4	<input type="checkbox"/>		1812	
5	<input type="checkbox"/>		1812	

RADIUS Accounting Server Configuration

#	Enabled	IP Address	Port	Secret
1	<input type="checkbox"/>		1813	
2	<input type="checkbox"/>		1813	
3	<input type="checkbox"/>		1813	
4	<input type="checkbox"/>		1813	
5	<input type="checkbox"/>		1813	

Client Configuration

The table has one row for each Client and a number of columns, which are:

Label	Description
Client	The Client for which the configuration below applies.
Authentication Method	Authentication Method can be set to one of the following values: none: authentication is disabled and login is not possible. local: use the local user database on the switch stack for authentication. radius: use a remote RADIUS server for authentication. tacacs+ : use a remote TACACS+ server for authentication.
Fallback	Enable fallback to local authentication by checking this box. If none of the configured authentication servers are alive, the local user database is used for authentication. This is only possible if the Authentication Method is set to something else than 'none' or 'local'.
Save	Select to save changes.
Reset	Select to undo any changes made locally and revert to previously saved values.

Common Server Configuration

These setting are common for all of the Authentication Servers.

Label	Description
Timeout	The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any). RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.
Dead Time	The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

RADIUS Authentication Server Configuration

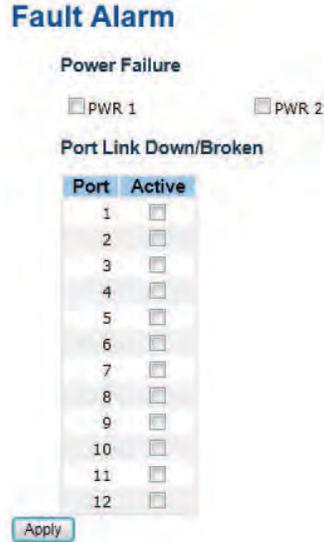
The table has one row for each RADIUS Authentication Server and a number of columns, which are:

Label	Description
#	The RADIUS Authentication Server number for which the configuration below applies.
Enable	Enable the RADIUS Authentication Server by checking this box.
IP Address	Enable fallback to local authentication by checking this box. If none of the configured authentication servers are alive, the local user database is used for authentication. This is only possible if the Authentication Method is set to something else than 'none' or 'local'.
Port	The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.
Secret	The secret - up to 29 characters long - shared between the RADIUS Accounting Server and the switchstack.

Warning

Fault Alarm

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



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 8 to monitor.
Apply	Select Apply to set the configurations.

System Warning

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



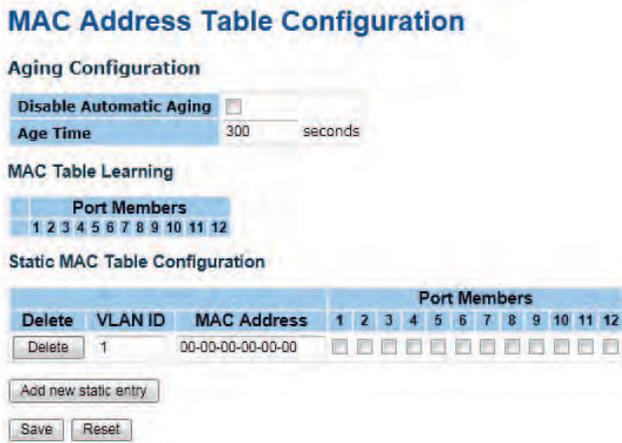
The following table describes the labels in this screen.

Label	Description
IP Address	The remote SYSLOG Server IP address.
Save	Select Save to set the configurations.
Reset	Select to reset the IP Address to the last saved entry.

Monitor and Diag

MAC Table

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.



Aging Configuration

By default, dynamic entries are removed from the MAC after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds; for example, Age time seconds.

The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking **Disable automatic aging**.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The maximum of 64 entries is for the whole stack, and not per switch.

The MAC table is sorted first by VLAN ID and then by MAC address.

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Adding a New Static Entry Select **Add new static entry** to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Select "Save".

Mirroring

Configure port Mirroring on this page.

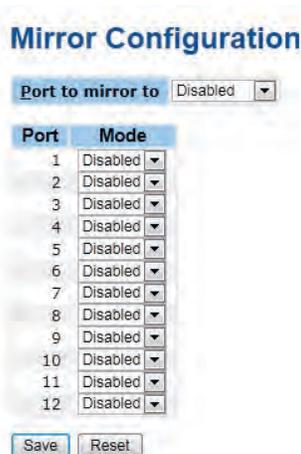
To debug network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow.

The traffic to be copied to the mirror port is selected as follows:

All frames received on a given port (also known as ingress or source mirroring).

All frames transmitted on a given port (also known as egress or destination mirroring).

Port to mirror also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this port. Disabled disables mirroring.



Label	Description
Port	The logical port for the settings contained in the same row.
Mode	Select mirror mode: Rx only: Frames received at this port are mirrored to the mirror port. Frames transmitted are not mirrored. Tx only: Frames transmitted from this port are mirrored to the mirror port. Frames received are not mirrored. Disabled: Neither frames transmitted nor frames received are mirrored. Enabled: Frames received and frames transmitted are mirrored to the mirror port.

Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames for the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

System Log Information

The switch system log information is provided here.



Label	Description
ID	The ID (>= 1) of the system log entry.
Level	The level of the system log entry. The following level types are supported: Info: Information level of the system log. Warning: Warning level of the system log. Error: Error level of the system log. All: All levels.
Time	The time of the system log entry.
Message	The MAC Address of this switch.
Auto-Refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Updates the system log entries, starting from the current entry ID.
Clear	Flushes all system log entries.
<<	Updates the system log entries, starting from the first available entry ID.
<<	Updates the system log entries, ending at the last entry currently displayed.
>>	Updates the system log entries, starting from the last entry currently displayed.
>>	Updates the system log entries, ending at the last available entry ID.

Detailed Log

The switch system detailed log information is provided here.



Label	Description
ID	The ID (>= 1) of the system log entry.
Message	The detailed messages of the system log entry.
Refresh	Updates the system log entries, starting from the current entry ID.
Clear	Flushes all system log entries.
<<	Updates the system log entries, starting from the first available entry ID.
<<	Updates the system log entries, ending at the last entry currently displayed.
>>	Updates the system log entries, starting from the last entry currently displayed.
>>	Updates the system log entries, ending at the last available entry ID.

Traffic Overview

This page provides an overview of general traffic statistics for all switch ports.

Port Statistics Overview

Auto-refresh Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive
1	55570	16116	4171313	2140694	1	0	0	0	130
2	0	0	0	0	0	0	0	0	0
3	15280	15080	1648096	2957465	25	0	0	0	15
4	0	0	0	0	0	0	0	0	0
5	69	204	6410	34194	2	0	2	0	0
6	2073	2407	382623	664119	0	0	0	0	0
7	6961	110259	1082601	11217650	1	0	0	0	5
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0

Label	Description
Port	The logical port for the settings contained in the same row.
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions per port.
Drops	The number of frames discarded due to ingress or egress congestion.
Filtered	The number of received frames filtered by the forwarding process.
Auto-Refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Updates the counters entries, starting from the current entry ID.
Clear	Flushes all counters entries.

Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Detailed Statistics-Receive & Transmit Total

Detailed Port Statistics Port 1

Receive Total		Transmit Total	
Rx Packets	55597	Tx Packets	16130
Rx Octets	4173222	Tx Octets	2143090
Rx Unicast	0	Tx Unicast	98
Rx Multicast	55511	Tx Multicast	11116
Rx Broadcast	85	Tx Broadcast	4916
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	52123	Tx 64 Bytes	1
Rx 65-127 Bytes	87	Tx 65-127 Bytes	8812
Rx 128-255 Bytes	3384	Tx 128-255 Bytes	7081
Rx 256-511 Bytes	3	Tx 256-511 Bytes	228
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	8
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Low	130	Tx Low	12586
Rx Normal	0	Tx Normal	0
Rx Medium	0	Tx Medium	0
Rx High	55466	Tx High	3544
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	1	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	130		

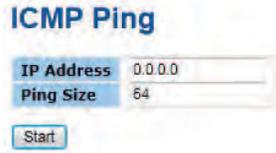
Label	Description
Rx and Tx Packets	The number of received and transmitted (good and bad) packets.
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
Rx and Tx Unicast	The number of received and transmitted (good and bad) unicast packets.
Rx and Tx Multicast	The number of received and transmitted (good and bad) multicast packets.
Rx and Tx Broadcast	The number of received and transmitted (good and bad) broadcast packets.
Rx and Tx Pause	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
Rx Drops	The number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short 1 frames received with valid CRC.
Rx Oversize	The number of long 2 frames received with valid CRC.
Rx Fragments	The number of short 1 frames received with invalid CRC.
Rx Jabber	The number of long 2 frames received with invalid CRC.
Rx Filtered	The number of received frames filtered by the forwarding process.
Tx Drops	The number of frames dropped due to output buffer congestion.
Tx Late / Exc.Coll.	The number of frames dropped due to excessive or late collisions.

Short frames are frames that are smaller than 64 bytes.

Long frames are frames that are longer than the configured maximum frame length for this port.

Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.



After you press **Start**, 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING6 server ::10.10.132.20
```

```
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
```

```
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
```

```
64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms
```

```
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms
```

```
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms
```

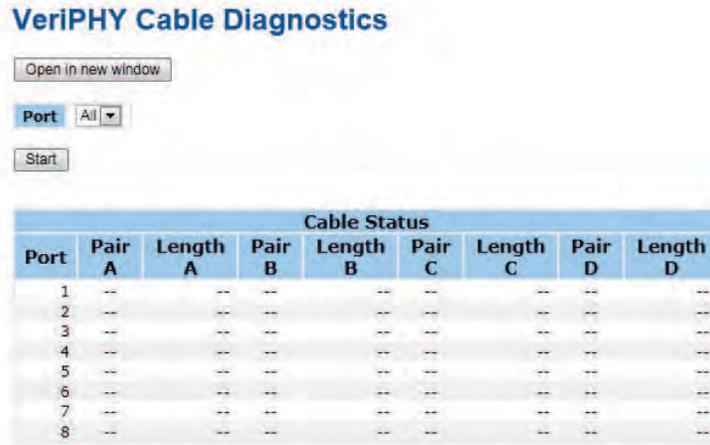
```
Sent 5 packets, received 5 OK, 0 bad
```

You can configure the following properties of the issued ICMP packets:

Label	Description
IP Address	The destination IP Address.
Ping Size	The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.

VeriPHY

This page is used for running the VeriPHY Cable Diagnostics.



Press **Start** to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Label	Description
Port	The port where you are requesting VeriPHY Cable Diagnostics.
Cable Status	Port: Port number. Pair: The status of the cable pair. Length: The length (in meters) of the cable pair.

System Reboot

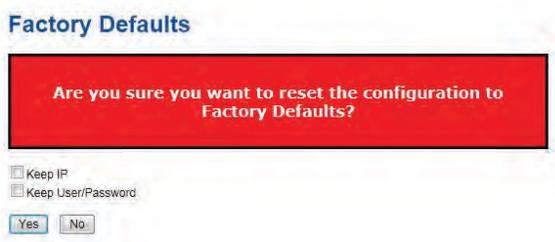
You can reset the stack switch on this page. After reset, the system will boot normally as if you had powered-on the devices



Label	Description
Yes	Select to reboot device.
No	Select to return to the Port State page without rebooting.

Factory Defaults

You can reset the configuration of the stack switch on this page. Only the IP configuration is retained.



Label	Description
Keep IP	Mark this box to retain current IP settings upon reset
Keep User/Password	Mark this box to retain current Username and Password
Yes	Select to reset the configuration to Factory Defaults.
No	Select to return to the Port State page without resetting the configuration

Command Line Interface Management

About CLI Management

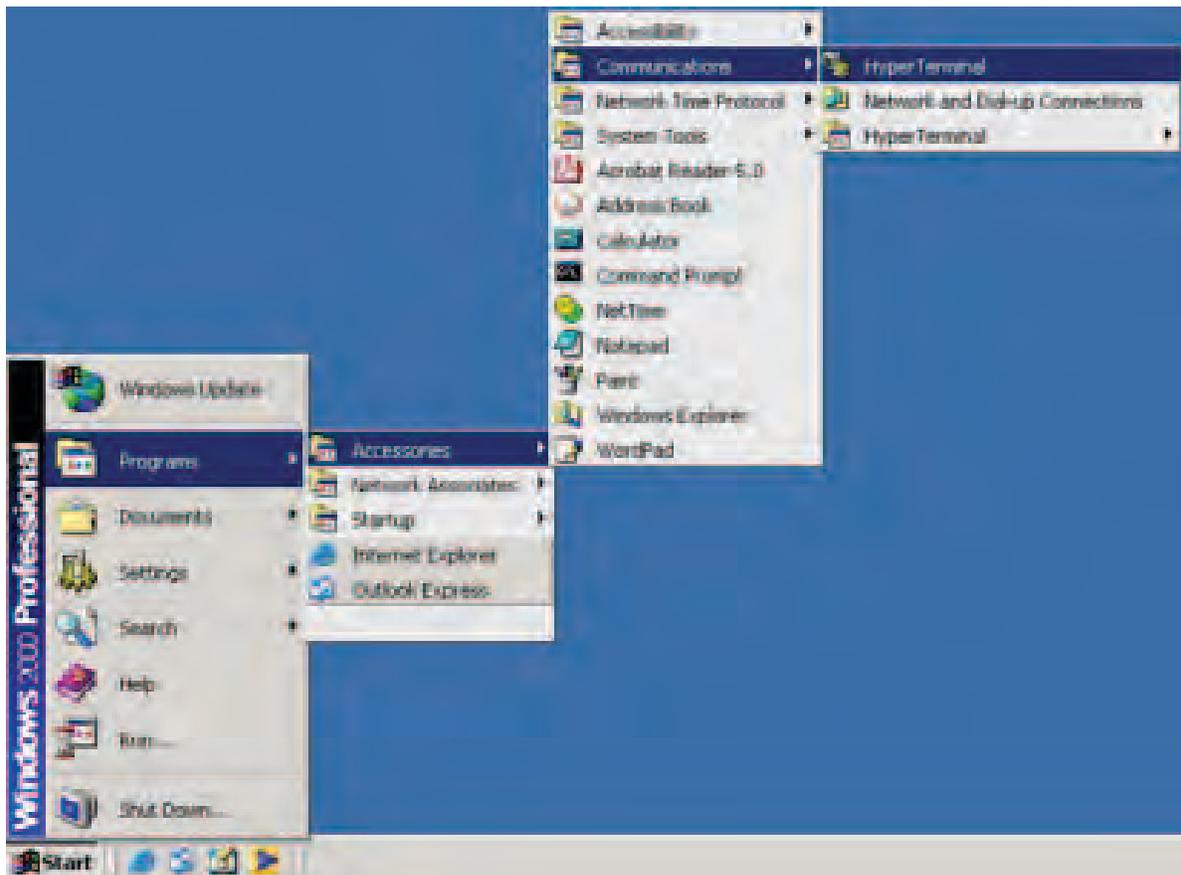
Besides WEB-base management, CNGE12MS also support CLI management. You can use console or telnet to management switch by CLI.

CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

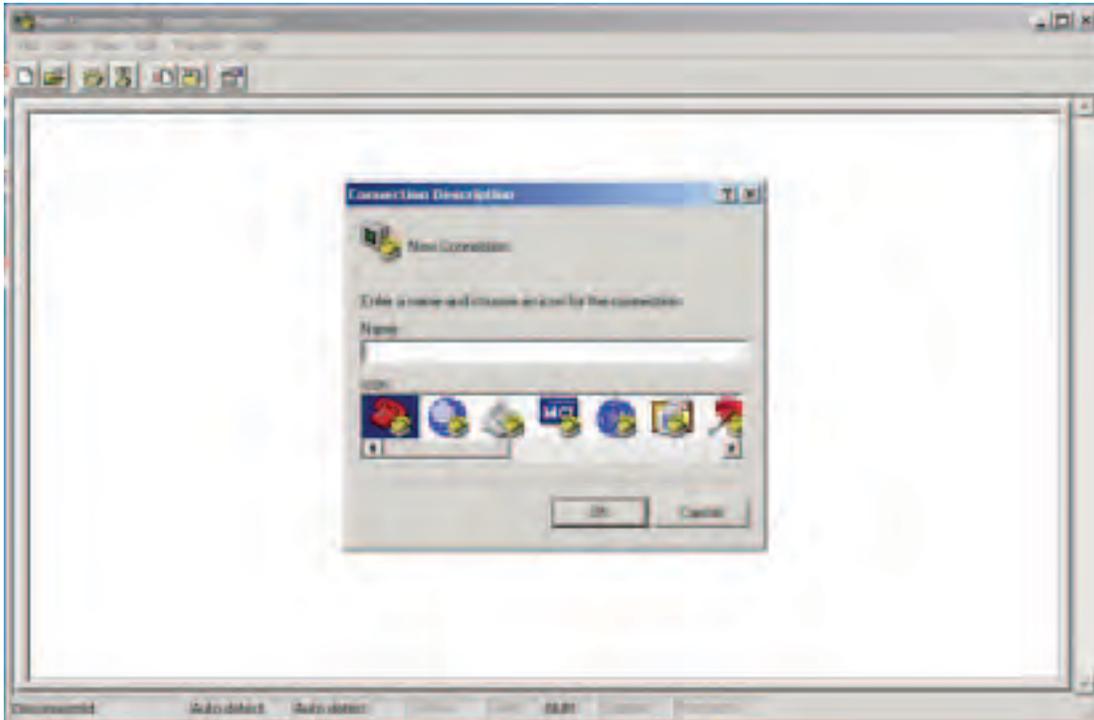
Before Configuring by RS-232 serial console, use an RJ45 to DB9-F cable to connect the Switches' RS-232 Console port to your PC's COM port.

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

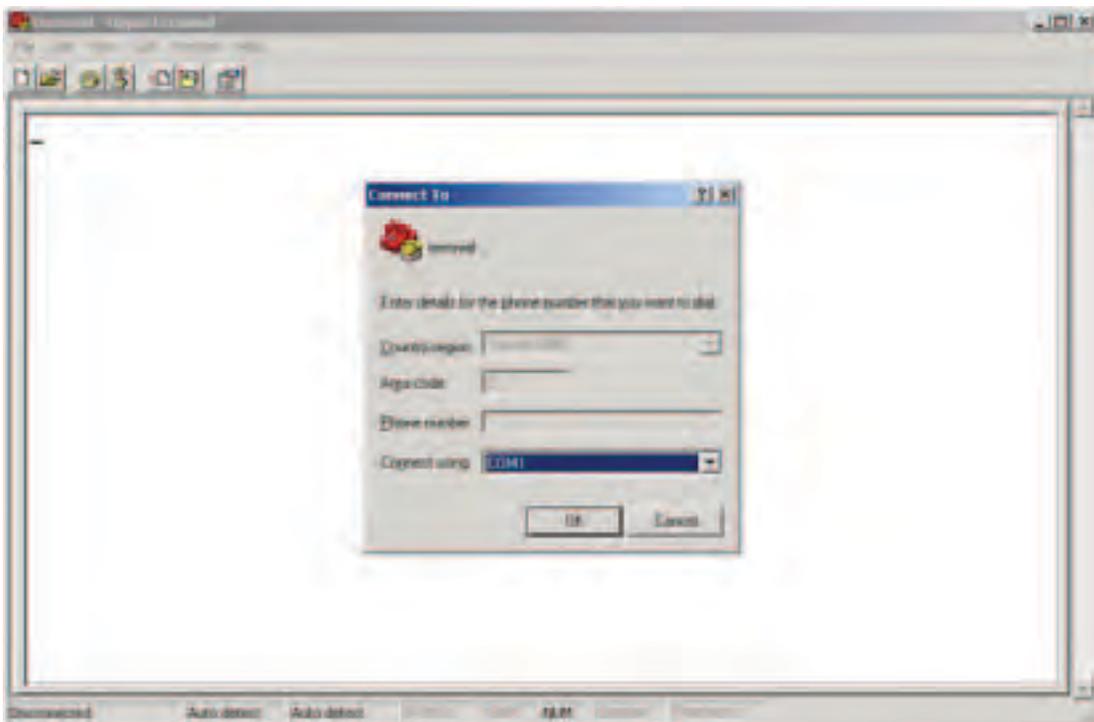
Step 1. From the Windows desktop, select on Start -> Programs -> Accessories -> Communications -> Hyper Terminal



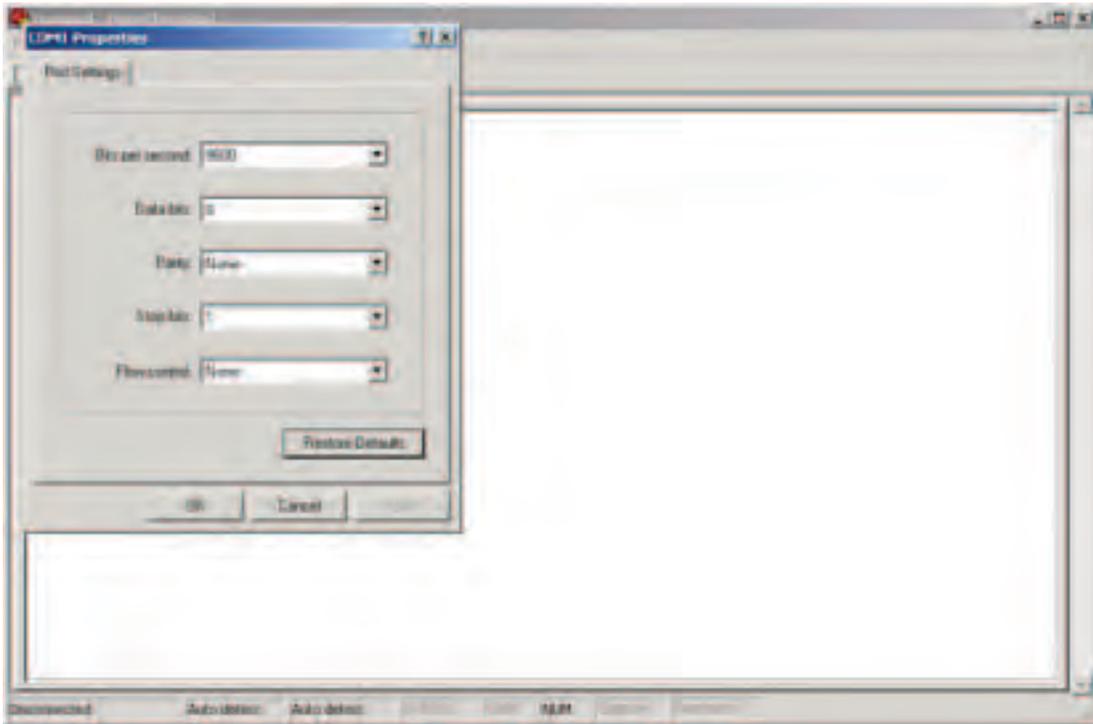
Step 2. Input a name for new connection



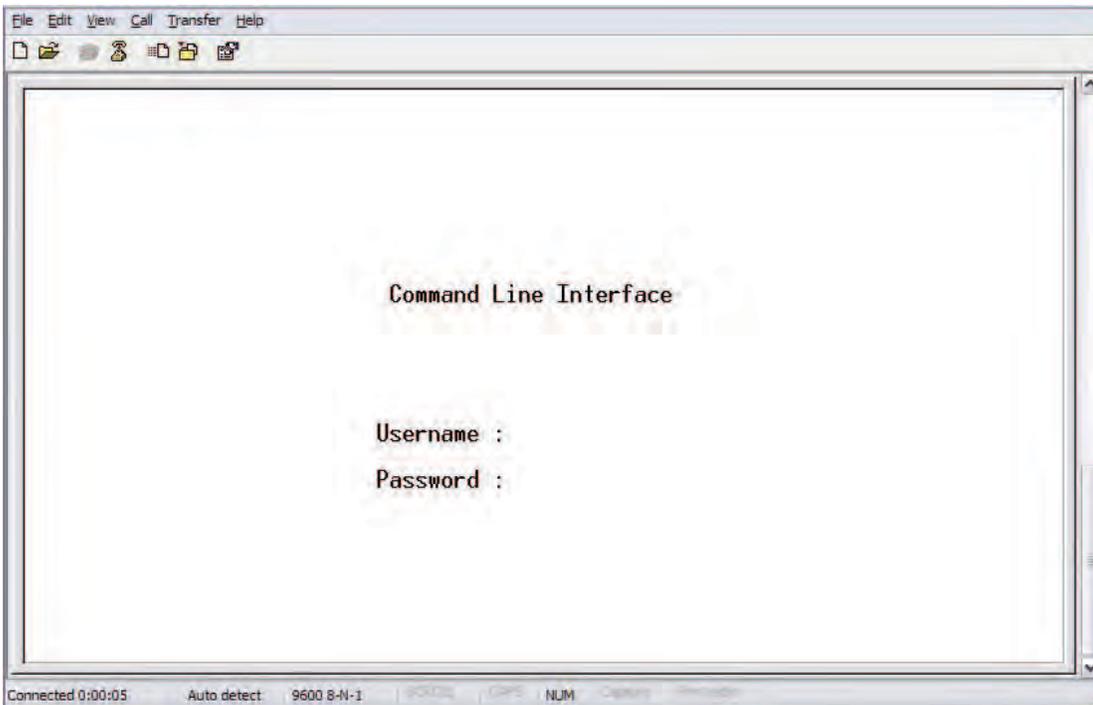
Step 3. Select the COM port number



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**

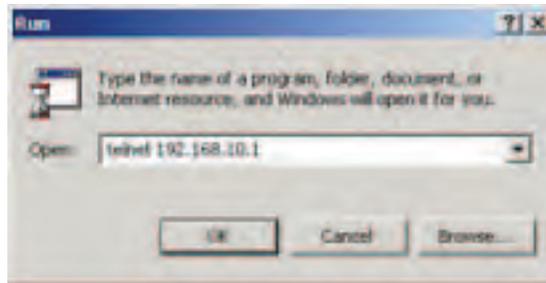
Default Gateway: **192.168.10.254**

User Name: **admin**

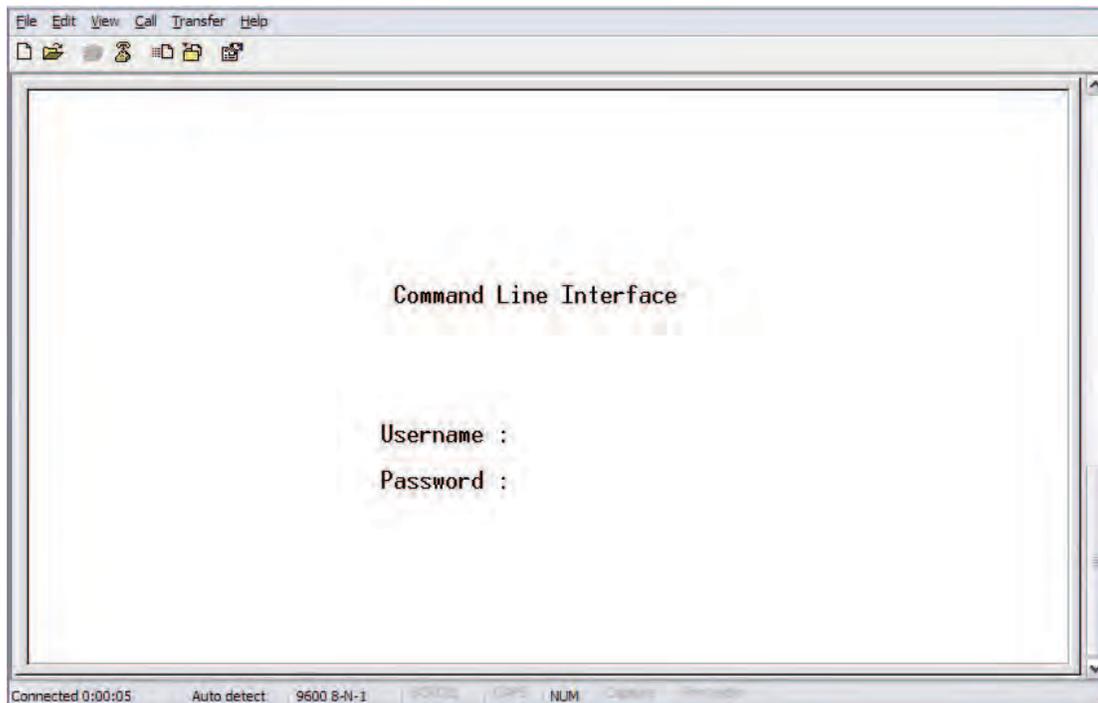
Password: **admin**

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) as below.



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 Sets

System

```

System> Configuration [all] [<port_list>]
System> Reboot
System> Restore Default [keep_ip]
System> Contact [<contact>]
System> Name [<name>]
System> Location [<location>]
System> Description [<description>]
System> Password <password>
System> Username [<username>]
System> Timezone [<offset>]
System> Log [<log_id>] [all|info|warning|error] [clear]

```

Syslog

```

Syslog> ServerConfiguration [<ip_addr>]

```

IP

```

IP> Configuration
IP> DHCP [enable|disable]
IP> Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]
IP> Ping <ip_addr_string> [<ping_length>]
IP> SNTP [<ip_addr_string>]

```

Auth

```

Auth> Configuration
Auth> Timeout [<timeout>]
Auth> Deadtime [<dead_time>]
Auth> RADIUS [<server_index>] [enable|disable] [<ip_addr_string>]
Auth> [<secret>] [<server_port>]
Auth> ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>]
Auth> [<secret>] [<server_port>]
Auth> Client [console|telnet|ssh|web] [none|local|radius] [enable|disable]
Auth> Statistics [<server_index>]

```

Port

```

Port> Configuration [<port_list>]
      State [<port_list>] [enable|disable]
      Mode [<port_list>] [10hdx|10fdx|100hdx|100fdx|1000fdx|auto]
      Flow Control [<port_list>] [enable|disable]
      MaxFrame [<port_list>] [<max_frame>]
      Power [<port_list>] [enable|disable|actiphy|dynamic]
      Excessive [<port_list>] [discard|restart]
      Statistics [<port_list>] [<command>]
      VeriPHY [<port_list>]
    
```

Aggr

```

Aggr> Configuration
      Add <port_list> [<aggr_id>]
      Delete <aggr_id>
      Lookup [<aggr_id>]
      Mode [smac|dmac|ip|port] [enable|disable]
    
```

LACP

```

LACP> Configuration [<port_list>]
      Mode [<port_list>] [enable|disable]
      Key [<port_list>] [<key>]
      Role [<port_list>] [active|passive]
      Status [<port_list>]
      Statistics [<port_list>] [clear]
    
```

STP

```
Configuration
Version [<stp_version>]
Non-certified release, v
Txhold [<holdcount>]lt 15:15:15, Dec 6 2007
MaxAge [<max_age>]
FwdDelay [<delay>]
bpduFilter [enable|disable]
bpduGuard [enable|disable]
recovery [<timeout>]
CName [<config-name>] [<integer>]
Status [<msti>] [<port_list>]
Msti Priority [<msti>] [<priority>]
Msti Map [<msti>] [clear]
STP> Msti Add <msti> <vid>
Port Configuration [<port_list>]
Port Mode [<port_list>] [enable|disable]
Port Edge [<port_list>] [enable|disable]
Port AutoEdge [<port_list>] [enable|disable]
Port P2P [<port_list>] [enable|disable|auto]
Port RestrictedRole [<port_list>] [enable|disable]
Port RestrictedTcn [<port_list>] [enable|disable]
Port bpduGuard [<port_list>] [enable|disable]
Port Statistics [<port_list>]
Port Mcheck [<port_list>]
Msti Port Configuration [<msti>] [<port_list>]
Msti Port Cost [<msti>] [<port_list>] [<path_cost>]
Msti Port Priority [<msti>] [<port_list>] [<priority>]
```

Dot1x

```

Dot1x> Configuration [<port_list>]
Mode [enable|disable]
State [<port_list>] [macbased|auto|authorized|unauthorized]
Authenticate [<port_list>] [now]
Reauthentication [enable|disable]
Period [<reauth_period>]
Timeout [<eapol_timeout>]
Statistics [<port_list>] [clear|eapol|radius]
Clients [<port_list>] [all|<client_cnt>]
Agetime [<age_time>]
Holdtime [<hold_time>]
    
```

IGMP

```

IGMP> Configuration [<port_list>]
Mode [enable|disable]
State [<vid>] [enable|disable]
Querier [<vid>] [enable|disable]
Fastleave [<port_list>] [enable|disable]
Router [<port_list>] [enable|disable]
Flooding [enable|disable]
Groups [<vid>]
Status [<vid>]
    
```

LLDP

```

LLDP> Configuration [<port_list>]
Mode [<port_list>] [enable|disable|rx|tx]
Optional_TLV [<port_list>][port_descr|sys_name|sys_descr|sys_
capa|mgmt_addr] [enable|disable]
Interval [<interval>]
Hold [<hold>]
Delay [<delay>]
Reinit [<reinit>]
Info [<port_list>]
Statistics [<port_list>] [clear]
    
```

MAC

```

MAC> Configuration [<port_list>]
      Add <mac_addr> <port_list> [<vid>]
      Delete <mac_addr> [<vid>]
      Lookup <mac_addr> [<vid>]
      Agetime [<age_time>]
      Dump [<mac_max>] [<mac_addr>] [<vid>]
      Statistics [<port_list>]
      Flush
    
```

VLAN

```

VLAN> Configuration [<port_list>]
      Aware [<port_list>] [enable|disable]
      PVID [<port_list>] [<vid>|none]
      FrameType [<port_list>] [all|tagged]
      Add <vid> [<port_list>]
      Delete <vid>
      Lookup [<vid>]
    
```

PVLAN

```

PVLAN> Configuration [<port_list>]
      Add <pvlan_id> [<port_list>]
      Delete <pvlan_id>
      Lookup [<pvlan_id>]
      Isolate [<port_list>] [enable|disable]
    
```

QOS

```

Configuration [<port_list>]
Classes [<class>]
Default [<port_list>] [<class>]
Tagprio [<port_list>] [<tag_prio>]
QCL Port [<port_list>] [<qcl_id>]
QCL Add [<qcl_id>] [<qce_id>] [<qce_id_next>]
(etype <etype>) |
(vid <vid>) |
(port <udp_tcp_port>) |
(dscp <dscp>) |
(tos <tos_list>) |
(tag_prio <tag_prio_list>)
<class>
QCL Delete <qcl_id> <qce_id>
QCL Lookup [<qcl_id>] [<qce_id>]
Mode [<port_list>] [strict|weighted]
Weight [<port_list>] [<class>] [<weight>]
Rate Limiter [<port_list>] [enable|disable] [<bit_rate>]
Shaper [<port_list>] [enable|disable] [<bit_rate>]
Storm Unicast [enable|disable] [<packet_rate>]
Storm Multicast [enable|disable] [<packet_rate>]
Storm Broadcast [enable|disable] [<packet_rate>]

```

ACL

```

ACL> Configuration [<port_list>]
Action [<port_list>] [permit|deny] [<rate_limiter>] [<port_copy>]
[<logging>] [<shutdown>]
Policy [<port_list>] [<policy>]
Rate [<rate_limiter_list>] [<packet_rate>]
Add [<ace_id>] [<ace_id_next>] [switch | (port <port>) | (policy
<policy>)]
[<vid>] [<tag_prio>] [<dmac_type>]
[(etype [<etype>] [<smac>] [<dmac>])] |
(arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) |
(ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) |
(icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) |
(udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) |
(tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])
[permit|deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]
Delete <ace_id>
Lookup [<ace_id>]
Clear
    
```

Mirror

```

Mirror> Configuration [<port_list>]
Port [<port>] [disable]
Mode [<port_list>] [enable|disable|rx|tx]
    
```

Config

```

Config> Save <ip_server> <file_name>
Load <ip_server> <file_name> [check]
    
```

SNMP

```

Trap Inform Retry Times [<retries>]
Trap Probe Security Engine ID [enable|disable]
Trap Security Engine ID [<engineid>]
Trap Security Name [<security_name>]
Engine ID [<engineid>]
Community Add <community> [<ip_addr>] [<ip_mask>]
Community Delete <index>
Community Lookup [<index>]
User Add <engineid> <user_name> [MD5|SHA] [<auth_password>]
[DES]
[<priv_password>]
User Delete <index>
SNMP> User Changekey <engineid> <user_name> <auth_password> [<priv_
password>]
User Lookup [<index>]
Group Add <security_model> <security_name> <group_name>
Group Delete <index>
Group Lookup [<index>]
View Add <view_name> [included|excluded] <oid_subtree>
View Delete <index>
View Lookup [<index>]
Access Add <group_name> <security_model> <security_level>
[<read_view_name>] [<write_view_name>]
Access Delete <index>
Access Lookup [<index>]
    
```

Firmware

```

Firmware> Load <ip_addr_string> <file_name>
    
```

fault

```

Fault> Alarm PortLinkDown [<port_list>] [enable|disable]
Alarm PowerFailure [pwr1|pwr2|pwr3] [enable|disable]
    
```

SFLOW

```
SFLOW> mode [enable|disable]
        version [v2|v5]
        rate [<integer>]
        interval [<integer>]
        coladdr [<ip_addr>]
        colport [<integer>]
        show
```

Technical Specifications

Switch Model	CNGE12MS
Physical Ports	
Gigabit Combo Port	8 × 10/100/1000BASE-T(X) and 100/1000BASE-X SFP ports
1000BASE-X SFP Port	4
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, 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 Table	8k
Priority Queues	4
Processing	Store-and-Forward
Switch Properties	Switching latency: 7 us Switching bandwidth: 24Gbps Max. Number of Available VLANs: 4096 IGMP multicast groups: 128 for each VLAN Port rate limiting: User Define
Jumbo frame	Up to 9K Bytes
Security Features	IP Police security feature Enable/disable ports, MAC based port security Port based network access control (IEEE 802.1x) VLAN (IEEE 802.1Q) to segregate and secure network traffic Radius centralized password management SNMPv3 encrypted authentication and access security

Software Features	STP/RSTP/MSTP (IEEE 802.1D/w/s) Redundant ComRing C-Ring with recovery time < 30ms over 250 units TOS/Diffserv supported Quality of Service (IEEE 802.1p) for real-time traffic VLAN (IEEE 802.1Q) with VLAN tagging and GVRP supported IGMP Snooping IP based bandwidth management Application based QoS management DOS/DDOS auto prevention Port configuration, status, statistics, monitoring, security DHCP Client/Server
Network Redundancy	C-Ring Legacy Ring STP / RSTP / MSTP compatible
RS-232 Serial Console Port	RS-232 in RJ45 connector with console cable. 115200bps, 8, N, 1
LED indicators	
Power indicator	Green : Power LED x 3
R.M. indicator	Green : indicate system operated in ITS-Ring Master mode
Ring indicator	Green : indicate system operated in ITS-Ring mode
Fault indicator	Amber : Indicate unexpected event occurred
RJ45 port indicator	Green for port Link/Act. Amber for Duplex/Collision
Fiber port indicator	Green for port Link/Act.
Fault contact	
Relay	Relay output to carry capacity of 1A at 24VDC
Power	
Redundant Input power	Dual DC inputs. 12~48VDC on 6-pin terminal block
Power consumption (Typ.)	22 Watts
Overload current protection	Present
Reverse polarity protection	Present
Physical Characteristic	
Enclosure	Aluminum
Dimension (W × D × H)	96.4 × 108.5 × 154 mm (3.8 × 4.2.7 × 6.06 inch)
Weight (g)	3.13 pounds / 1420 grams
Environmental	
Storage Temperature	-40° to 85°C (-40° to 185°F)
Operating Temperature	-40° to 75°C (-40° to 167°F)
Operating Humidity	5% to 95% Non-condensing

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	IEC60068-2-32
Vibration	IEC60068-2-6
Safety	EN60950-1
Warranty	Lifetime

MECHANICAL INSTALLATION INSTRUCTIONS

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: customer care@comnet.net



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