

INSTALLATION AND OPERATION MANUAL



CWGE28FX4TX24MS

**(24) 10/100/1000 BASE-TX + (4) 1000BASE-FX
MANAGED ETHERNET SWITCH**

The ComNet™ CWGE28FX4TX24MS Layer 2 Managed 28 Port Ethernet Switch supports twenty-four (24) 10/100/1000BASE-TX ports and four (4) 1000BASE-FX ports of Ethernet data. The four 1000BASE-FX ports are SFP configurable for fiber type (multimode or single-mode), connector type and distance. The exclusive C-Ring redundant ring feature protects networks from interruptions or temporary malfunctions with its fast recovery technology. The electrical ports support the 10/100/1000 Mbps Ethernet IEEE 802.3 protocol, and auto-negotiating and auto-MDI/MDIX features are included. The CWGE28FX4TX24MS are optically (1000BASE-FX) and electrically compatible with any IEEE 802.3 compliant Ethernet device.

Contents

About This Guide	3
Related Documentation	3
About ComNet	3
Website	3
Support	3
Safety	3
Overview	4
Introduction	4
Software Features	5
Hardware Features	6
Hardware Installation	7
Rear Panel	8
Rack mount kit assembly	8
Cables	10
Ethernet Cables	10
SFP (Small Form-Factor Pluggable) Optical Connectors	12
Console Cable	13
WEB Management	14
Configuration by Web Browser	14
Command Line Interface Management	102
About CLI Management	102
Commander Groups	106
Technical Specifications	114

About This Guide

This guide is intended for different users such as engineers, integrators, developers, IT managers, and technicians.

It assumes that users have some PC competence and are familiar with Microsoft Windows operating systems and web browsers such as Windows Internet Explorer and Mozilla Firefox, as well as have knowledge of the following:

- » Installation of electronic equipment
- » Electrical regulations and guidelines
- » Knowledge of Local Area Network technology

Related Documentation

The following documentation is also available:

- » CWGE28FX4TX24MS Datasheet

About ComNet

ComNet develops and markets the next generation of video solutions for the CCTV, defense, and homeland security markets. At the core of ComNet's solutions are a variety of high-end video servers and the ComNet IVS software, which provide the industry with a standard platform for analytics and security management systems enabling leading performance, compact and cost effective solutions.

ComNet's products are available in commercial and rugged form.

Website

For information on ComNet's entire product line, please visit the ComNet website at <http://www.comnet.net>

Support

For any questions or technical assistance, please contact your sales person (sales@comnet.net) or the customer service support center (techsupport@comnet.net)

Safety

- » 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 ComNet CWGE28FX4TX24MS is a managed redundant ring Ethernet switch with 24x10/100/1000Base-(TX) ports and 4x1000Base-X SFP ports. The Ethernet Redundancy protocol, C-Ring (Gigabit model recovery time < 30ms over 250 units of connection) and MSTP/RSTP/STP (IEEE 802.1s/w/D) can protect your applications from network interruptions or temporary malfunctions with its fast recovery technology.

ComNet's Ethernet switches provide advanced IP-based bandwidth management which can limit the maximum bandwidth for each IP device. The User can configure IP cameras and Network Video Recorders with more bandwidth and limit other device's bandwidth.

ComNet's Ethernet switches also support application-based QoS. Application-based QoS can set the highest priority for data stream according to TCP/UDP port number. The ComNet special IP police function can permit only allowed IP address with MAC address to access the networking. Unintended access is eliminated, as a user cannot access the IP surveillance network without permission. Moreover, the ComNet CWGE28FX4TX24MS switch provides advanced DoS/DDoS auto prevention. If an IP flow rises quickly, the CWGE28FX4TX24MS switch will lock the source IP address for a certain time to prevent the attack. It is hardware-based prevention so it can prevent DDOS attack immediately and completely. And all functions of the CWGE28FX4TX24MS can also be centrally managed conveniently by eConsole, the Web-based interface, Telnet and console (CLI) configuration. Therefore, the switch is one of the most reliable choices for highly managed and Gigabit Fiber Optic Ethernet applications.

Software Features

- » Industry's fastest Redundant Ethernet Ring (Gigabit model recovery time < 30ms over 250 units connection)
- » Support for Ring Coupling, Dual Homing over Ring and standard STP/RSTP
- » Support for SNMPv1/v2c/v3 & RMON & Port base/802.1Q VLAN Network Management
- » Event notification by Email and SNMP trap
- » Windows Utility eConsole, Web-based ,Telnet and Console(CLI) configuration
- » Enable/disable ports, MAC based port security
- » Port based network access control (802.1x)
- » VLAN (802.1q) to segregate and secure network traffic
- » RADIUS centralized password management
- » SNMPv3 encrypted authentication and access security
- » Quality of Service (802.1p) for real-time traffic
- » VLAN (802.1q) with double tagging and GVRP supported
- » IGMP Snooping for multicast filtering
- » Port configuration, status, statistics, mirror, security
- » Remote Monitoring (RMON)

Hardware Features

- » One 100~240VAC power input
- » Operating Temperature: -10° to +60° C (+14° to +140° F)
- » Storage Temperature: -40 to 85°C (-40 to 185°F)
- » Operating Humidity: 5% to 95%, non-condensing
- » Casing: IP-20
- » 24 x 10/100/1000Base -T(X) RJ-45 ports
- » 4 x 1000 Base-X SFP ports
- » Console Port (DB9 Female connector)
- » Dimensions (W × D × H): 17.50 × 7.88 × 1.75 inch (44.45 × 20.00 × 4.45 cm)

Hardware Installation



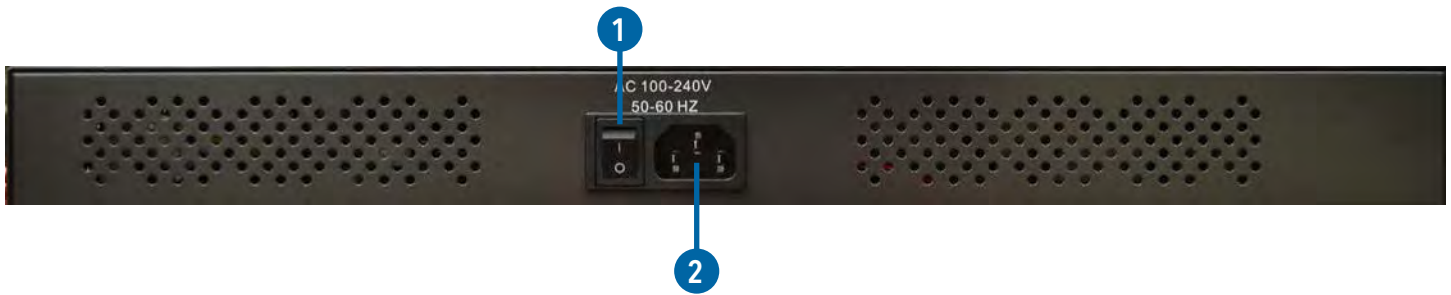
CWGE28FX4TX24MS Front Panel

The following table describes the labels that are on the CWGE28FX4TX24MS switch

Port	Description
Gigabit SFP ports	4 × 1000Base-X on SFP port
Gigabit Ethernet Port	24 × 10/100/1000Base-T(X)
Console	Use RS-232 with DB9 connector to manage switch.

1. Console port (DB9 Female connector)
2. 10/100/1000Base-T(X) gigabits Ethernet port
3. 1000Base-X Fiber port on SFP port
4. LED for Ethernet ports Link/Act status: Left Green for 1000Mbps indicator, Amber for 10/100Mbps indicator
5. LED for Ethernet ports Duplex status.
6. LED for SFP ports Link/Act status.
7. Front panel Indicating LEDs:
 - › STA: Solid Green indicates that the system is ready. The LED is blinking when the system is upgrading firmware
 - › PWR: The LED lights on when the power module is activated.
 - › R.M.: (Ring Master). When the LED light is on, the switch is the ring master of Ring.
 - › Ring: When the LED light is on, it means the C-Ring is activated.
 - › DEF: System resets to default configuration.
 - › Ping: System is processing “PING” request.
 - › RUN: System is operating continuously.
 - › RMT: System is accessed remotely.

Rear Panel



CWGE28FX4TX24MS Rear Panel

1. Power Switch
2. Power input for AC 100V~240V / 50~60Hz

Rack mount kit assembly

You can find the rack mount kit and the screws in the packing box. Please assembly the rack mount kit on the switch with screws as shown below:



Front Panel LEDs

LED	Color	Status	Description
PWR	Green	On	DC power module activated.
STA	Green	On	Power module is in PWR UP state
		Blinking	The system is upgrading firmware
DEF	Green	On	System resets to default configuration.
RUN	Green	Slowly blinking	System is operating continuously.
Ping	Green	Blinking	System is processing "PING" request
RMT	Green	Blinking	System is being accessed remotely.
Ring	Green	On	Ring enabled.
		Slowly blinking	Ring has only One link. (lacks one link to build the ring)
		Fast blinking	Ring work normally.
R.M	Green	On	When the system is operating in C-Ring Master mode
Fault	Amber	On	Indicates unexpected event occurred.
10/100/1000Base-T(X) Gigabit Ethernet ports			
LINK/ACT (Left)	Green	On	Port speed 1000M link up
		Blinking	Data Transmitted on 1000M
	Amber	On	Port speed 10/100M link up
		Blinking	Data Transmitted on 10/100M
Full-Duplex (Right)	Amber	On	Full-Duplex
		Blinking	Half-Duplex
SFP			
LINK/ACT	Green	On	Port link up.
		Blinking	Data transmitted

Cables

Ethernet Cables

The CWGE28FX4TX24MS series switches have standard Ethernet ports. According to the link type, the switches use CAT 3, 4, 5, 5e UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

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

100BASE-TX/10BASE-T Pin Assignment

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

10/100 Base-T RJ-45 Pin Assignments

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

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

1000 Base-T RJ-45 Pin Assignments

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

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

The CWGE28FX4TX24MS switch support auto MDI/MDI-X operation. You can use a straight-through cable to connect a PC to the switch. The following table below shows the 10BASE-T/100BASE-TX MDI and MDI-X port pin outs.

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

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

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

1000 Base-T MDI/MDI-X 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-

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

SFP (Small Form-Factor Pluggable) Optical Connectors

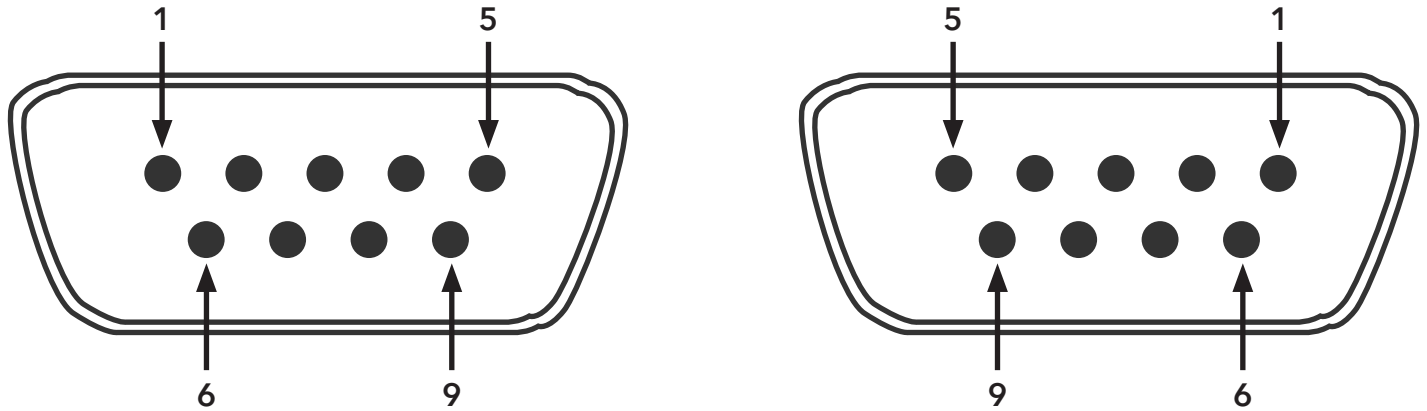
The Switch has fiber optic ports for use with with SFP connectors. There are many ComNet SFP modules available with either multimode or single-mode fiber, connector type and distance available. Contact ComNet for availability to meet your requirement. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.



Switch A Switch B

Console Cable

CWGE28FX4TX24MS switch can be managed through the console port. The DB-9 to RJ-45 cable can be found in the package. You can connect them to PC via a RS-232 cable with DB-9 female connector and the other end (RJ-45 connector) connects to console port of switch.



DB-9 Male DB-9 Female

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

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 introduces the configuration by Web browser.

About Web-based Management

An embedded HTML web site resides in 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 intentionally 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

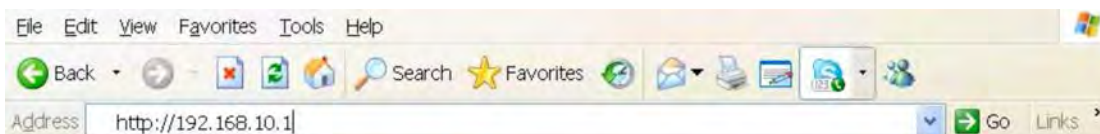
Default Gateway: 192.168.10.254

User Name: admin

Password: admin

System Login

1. Launch the browser: Internet Explorer.
2. Type http:// and the IP address of the switch. Press "Enter".



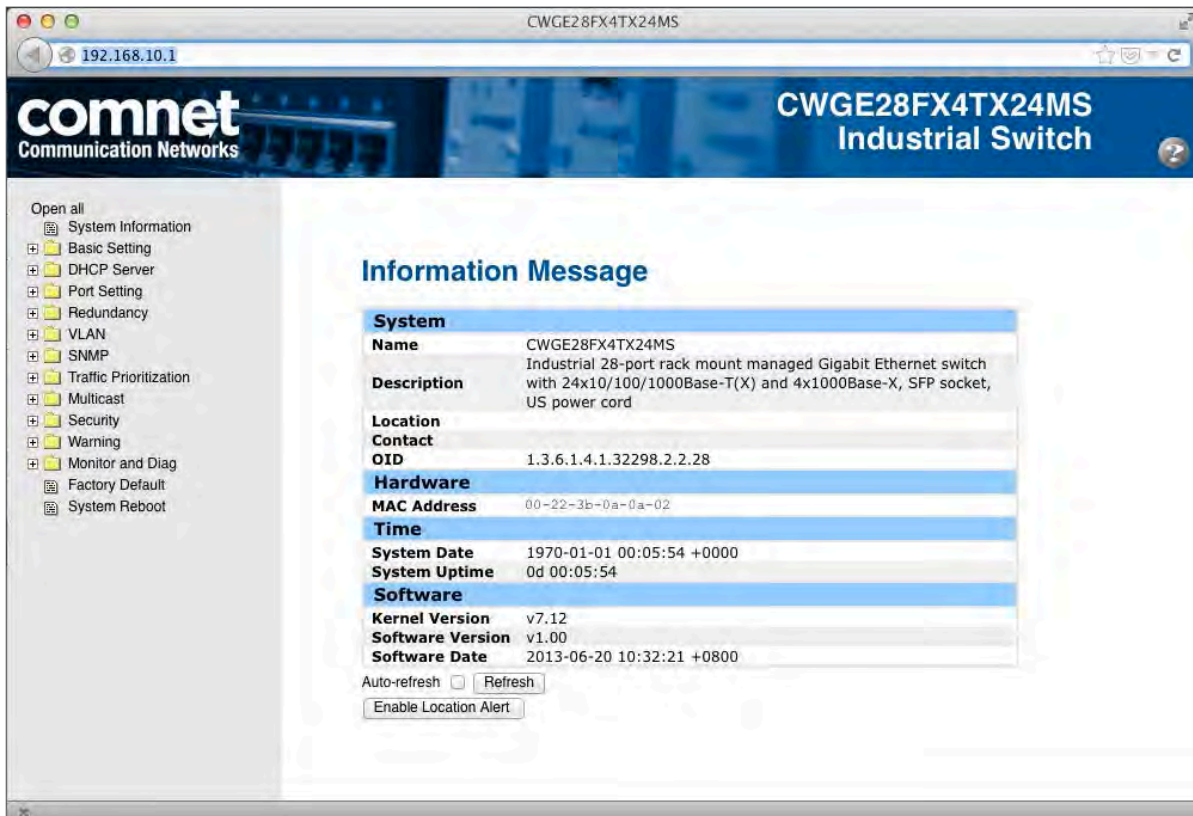
3. The login screen appears.
4. Key in the username and password. The default username and password is "admin".

5. Click "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 Configuration	
System Name	CWGE28FX4TX24MS
System Description	Industrial 28-port rack mount managed
System Location	
System Contact	
System Timezone Offset (minutes)	0

Save Reset

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	A name must be assigned by the network administrator 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-Za-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.
System Contact	Enter the name of contact person or organization
Timezone Offset	Provide the timezone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes.
Save	Click to save changes.
Reset	Click 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 CLI.

The screenshot shows a web interface titled "System Password". It features four input fields stacked vertically, each with a blue header: "Username", "Old Password", "New Password", and "Confirm New Password". The "Username" field contains the text "admin". Below these fields is a "Save" button.

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 password	Re-type the new password.
Save	Click to save changes.

IP Setting

Configure the switch-managed IP information on this page.

	Configured	Current
DHCP Client	<input type="checkbox"/>	Renew
IP Address	192.168.10.1	192.168.10.1
IP Mask	255.255.255.0	255.255.255.0
IP Router	0.0.0.0	0.0.0.0
VLAN ID	1	1
SNTP Server		

Save Reset

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	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Renew	Click to renew DHCP. This button is only available if DHCP is enabled.

HTTPS



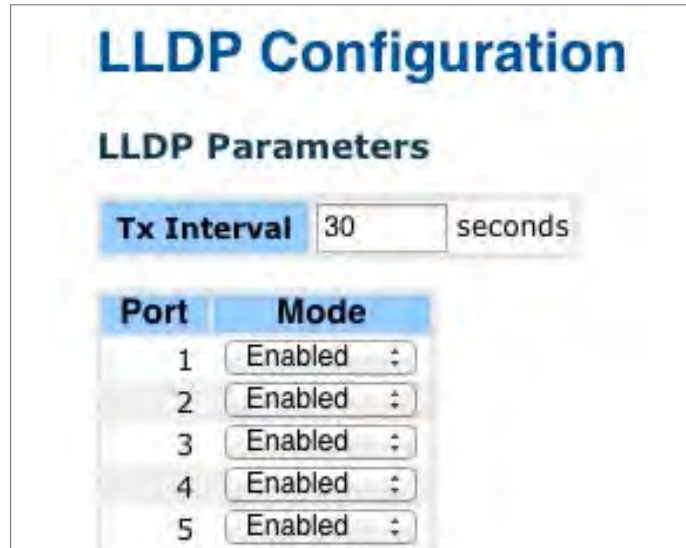
Label	Description
Mode	Indicates the HTTPS mode operation. Possible modes are: Enabled: Enable HTTPS mode operation. Disabled: Disable HTTPS mode operation.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

SSH



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

LLDP



LLDP Configuration

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

Label	Description
Port	The switch port number of the logical LLDP port.
Mode	Select LLDP mode. Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed. Tx only The switch will drop LLDP information received from neighbors, but will send out LLDP information. Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors. Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

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
------------	------------	----------------	-------------	------------------	---------------------	--------------------

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:

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 Capabilites	<p>System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:</p> <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 <p>When a switch capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).</p>
Management Address	Management Address is the next unit's address that is used for higher layer entities to assist in the network nodes discovery process by the network management. This could identify the neighbor's IP address.
Refresh	Click to immediately refresh the page .
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.



Global Counters

Label	Description
Neighbor entries were last changed at	Shows the time when the entry was last deleted or added. It also shows the time elapsed since last change was detected.
Total Neighbors Entries Added	Shows the number of new entries added since the switch rebooted.
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.

LLDP Statistics

Local Counters								
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	31	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	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
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0

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	Click 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:

Configuration Save

Configuration Upload

 No file selected.

Firmware Update

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

Firmware Update

 No file selected.

DHCP Server

Setting

The system supports DHCP server function. Enable the DHCP server function and the switch system will become 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	

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
-----	--------	------	-------------	------------	---------------

DHCP Client List

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

DHCP Client List

MAC Address	
IP Address	

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

Port Setting

Port Control

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

Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame	Power Control
		Current	Configured	Current Rx	Current Tx	Configured		
1	● Down	Down	Auto	×	×	<input type="checkbox"/>	9600	Disabled
2	● 1Gfdx	1Gfdx	Auto	×	×	<input type="checkbox"/>	9600	Disabled
3	● Down	Down	Auto	×	×	<input type="checkbox"/>	9600	Disabled
⋮								
25	● Down	Down	Auto	×	×	<input type="checkbox"/>	9600	
26	● Down	Down	Auto	×	×	<input type="checkbox"/>	9600	
27	● Down	Down	Auto	×	×	<input type="checkbox"/>	9600	
28	● Down	Down	Auto	×	×	<input type="checkbox"/>	9600	

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.
Save	Save changes.
Reset	Undo any changes made locally and revert to previously saved values.
Refresh	Click to refresh the page. Any changes made locally will be undone.

Rate Limit

Configure the switch port rate limit for traffic policing and shaping 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
...						
26	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
27	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
28	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps

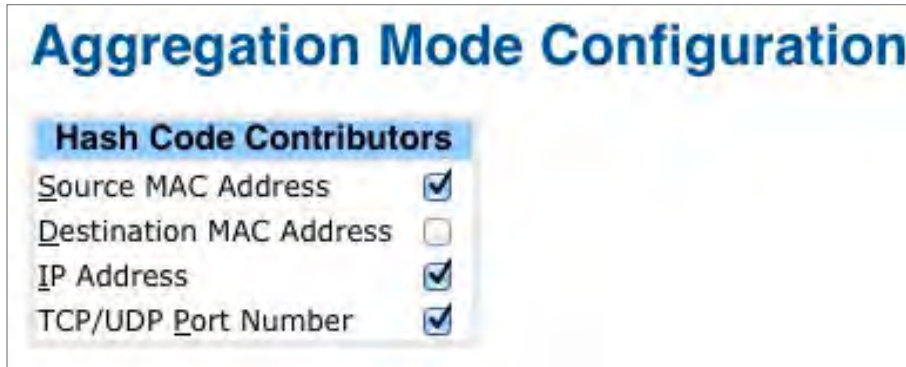
Save Reset

Label	Description
Port	The logical port for the settings contained in the same row.
Traffic policing Enabled	Enable or disable the port traffic policing. The default value is "Disabled".
Traffic policing Rate	Configure the rate for the port traffic policing. The default value is "500". This value is restricted to 500-1000000 when the "Traffic policing Unit" is "kbps", and it is restricted to 1-1000 when the "Traffic policing Unit" is "Mbps"
Traffic policing Unit	Configure the unit of measure for the port traffic-policing 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 "Traffic policing Unit" is "kbps", and it is restricted to 1-1000 when the "Traffic policing 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	Save changes.
Reset	Click 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.



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

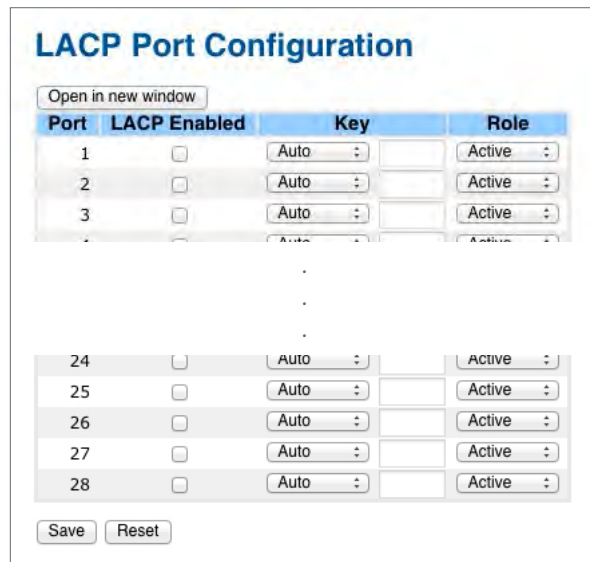
[Open in new window](#)

Group ID	Port Members																											
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Normal	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
9	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
10	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
11	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
12	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
13	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
14	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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 change as required.



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. The active will transmit LACP packets each second, while passive will wait for a LACP packet from a partner (communicate if communicated to).
Save	Save changes.
Reset	Click 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.

LACP System Status

Auto-refresh Refresh Open in new window

Aggr ID	Partner System ID	Partner Key	Last Changed	Local Ports
No ports enabled or no existing partners				

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	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.

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	-	-	-	-
13	No	-	-	-	-
14	No	-	-	-	-
15	No	-	-	-	-
16	No	-	-	-	-
17	No	-	-	-	-
18	No	-	-	-	-
19	No	-	-	-	-
20	No	-	-	-	-
21	No	-	-	-	-
22	No	-	-	-	-
23	No	-	-	-	-
24	No	-	-	-	-
25	No	-	-	-	-
26	No	-	-	-	-
27	No	-	-	-	-
28	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	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

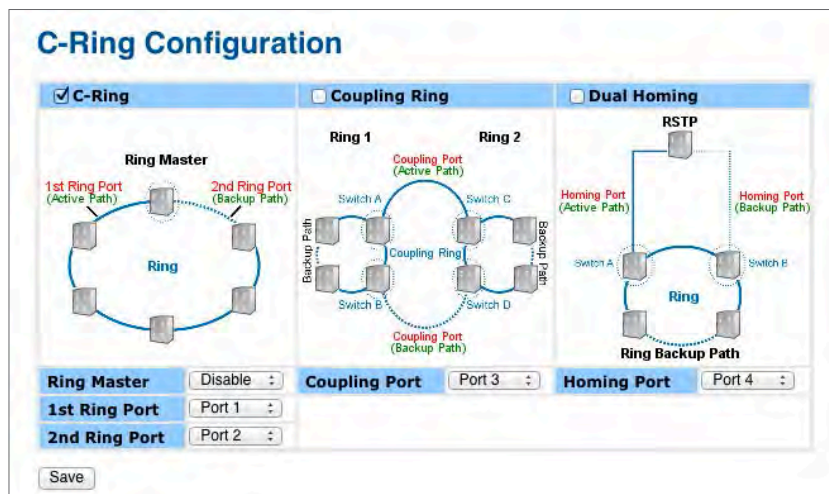
Port	LACP	LACP	Discarded	
	Transmitted	Received	Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	0	0
24	0	0	0	0
25	0	0	0	0
26	0	0	0	0
27	0	0	0	0
28	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	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 Redundant Ring in the world. The recovery time of C-Ring is less than 30 ms. It can reduce unexpected damage caused by network topology change. C-Ring Supports 3 Ring topology: C-Ring, Coupling Ring and Dual Homing.



Ring interface

The following table describes the labels in this screen.

Label	Description
Redundant Ring	Mark to enable C-Ring.
Ring Master	There should be one and 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, C-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 C-Ring to the normal switches in RSTP mode.
Save	Save 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	Save changes.
Reset	Click 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.

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 is at most 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	Save changes.
Reset	Click 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.

MSTI Configuration

MSTI	Priority
CIST	128
MST1	128
MST2	128
MST3	128
MST4	128
MST5	128
MST6	128
MST7	128

Save Reset

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	Save changes.
Reset	Click 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 needed. 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

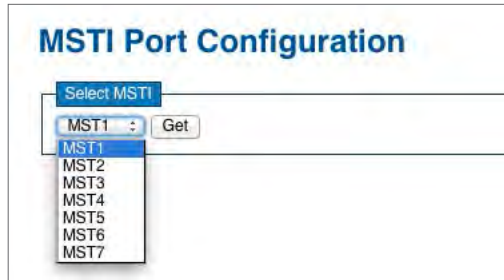
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
1	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input type="checkbox"/>	Auto	128	Edge	<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 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 type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
8	<input 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
13	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
14	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
15	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
16	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
17	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
18	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
19	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
20	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
21	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
22	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
23	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
24	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
25	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
26	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
27	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
28	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

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 know 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.
Point2Point	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	Save changes.
Reset	Click 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 needed. 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.



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	Save changes.
Reset	Click 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.

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	80:00-00:22:3B:0A:0A:02	80:00-00:22:3B:0A:0A:02	-	0	Steady	-

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

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	Click 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.

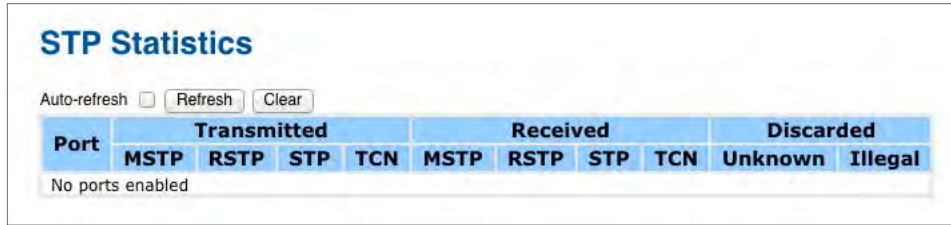
The screenshot shows a web interface titled "STP Port Status". At the top, there is an "Auto-refresh" checkbox (unchecked) and a "Refresh" button. Below this is a table with the following data:

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding	-
13	Non-STP	Forwarding	-
14	Non-STP	Forwarding	-
15	Non-STP	Forwarding	-
16	Non-STP	Forwarding	-
17	Non-STP	Forwarding	-
18	Non-STP	Forwarding	-
19	Non-STP	Forwarding	-
20	Non-STP	Forwarding	-
21	Non-STP	Forwarding	-
22	Non-STP	Forwarding	-
23	Non-STP	Forwarding	-
24	Non-STP	Forwarding	-
25	Non-STP	Forwarding	-
26	Non-STP	Forwarding	-
27	Non-STP	Forwarding	-
28	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	Refreshes 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.



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	Refreshes 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

	Delete	VLAN ID	Port Members																											
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
	<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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	Click 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 click 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 click **Save**.

The Reset 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

Open in new window

		Port Members																											
Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delete	50	<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"/>	<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"/>	<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 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
5	<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
5	<input type="checkbox"/>	All	Specific	1

Portbased VLAN Setting (For egress port)

1. VLAN Membership Configuration setting port 2 & 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	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delete	50	<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"/>	<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"/>	<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 2 Configuration-->don't care 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	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 checked="" 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	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<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"/>	<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"/>	<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

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

802.1Q Access port Setting (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	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<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"/>	<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"/>	<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

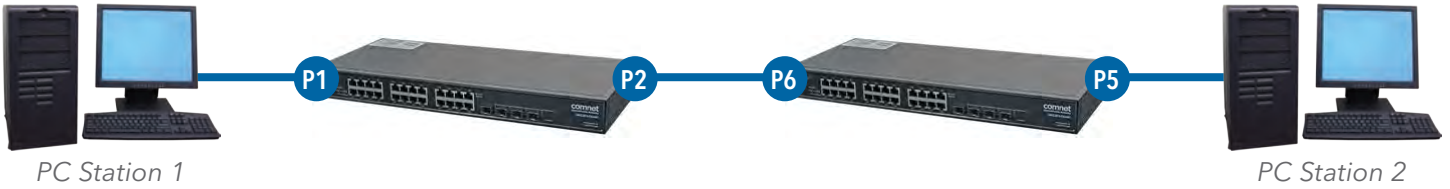
Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	<input type="checkbox"/>	All	Specific	50
2	<input type="checkbox"/>	All	Specific	1
3	<input type="checkbox"/>	All	Specific	1
4	<input type="checkbox"/>	All	Specific	1

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

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

		Port Members																											
Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	11	<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"/>	<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"/>	<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 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"/>	<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"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	33	<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"/>	<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"/>	<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	11
2	<input checked="" type="checkbox"/>	All	Specific	1
3	<input checked="" type="checkbox"/>	All	Specific	1
4	<input checked="" type="checkbox"/>	All	Specific	1
5	<input type="checkbox"/>	All	Specific	1
6	<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	1
3	<input checked="" type="checkbox"/>	All	Specific	1
4	<input checked="" type="checkbox"/>	All	Specific	1
5	<input type="checkbox"/>	All	Specific	1
6	<input type="checkbox"/>	All	Specific	1

Table 5 - UTC Time Zones

(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	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	11	<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"/>	<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"/>	<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 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"/>	<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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	33	<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"/>	<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"/>	<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

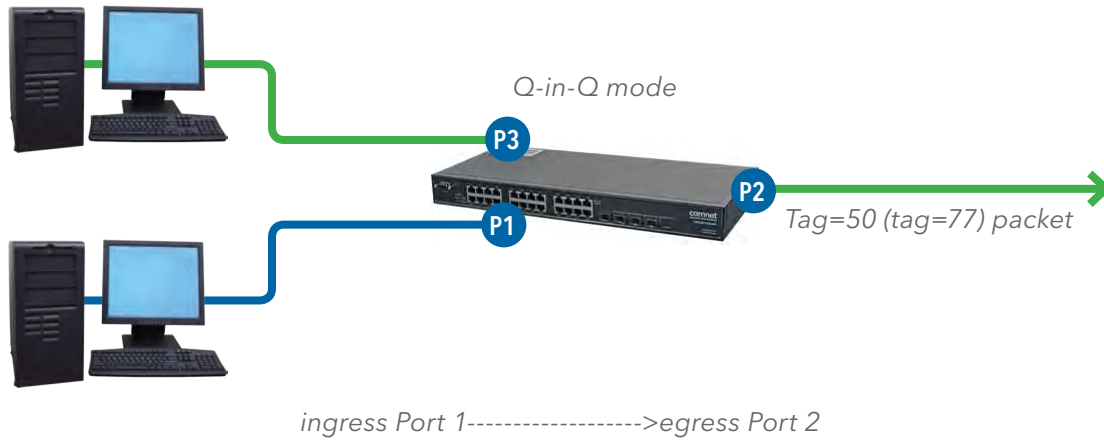
Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	<input type="checkbox"/>	All	Specific	1
2	<input type="checkbox"/>	All	Specific	1
3	<input type="checkbox"/>	All	Specific	1
4	<input type="checkbox"/>	All	Specific	1
5	<input checked="" type="checkbox"/>	All	Specific	11
6	<input checked="" type="checkbox"/>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

3. VLAN Port Configuration-->Mode=none
 Egress port can receive tag=11,22,33 packet
 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	1
2	<input type="checkbox"/>	All	Specific	1
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

QinQ VLAN Setting



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

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

VLAN Membership Configuration

Open in new window

Delete	VLAN ID	Port Members																											
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	50	<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"/>	<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"/>	<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	
			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	
			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

VLAN Membership Configuration

Open in new window

		Port Members																											
Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<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"/>	<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"/>	<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 Port 2, 3 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-->Mode=none
(only tag=50 packet can enter egress port)

VLAN Port Configuration

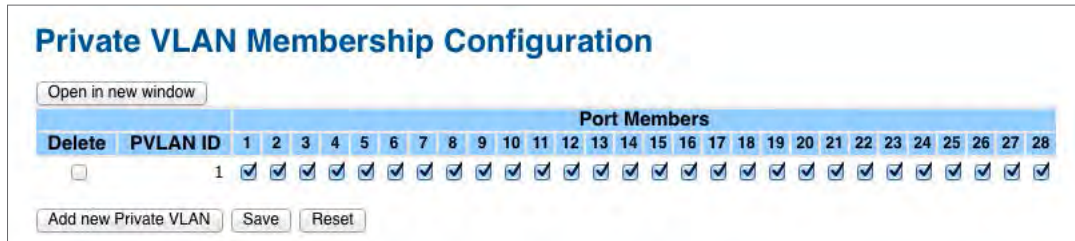
Port	VLAN Aware	Frame Type	Port VLAN	
			Mode	ID
1	<input type="checkbox"/>	All	Specific	50
2	<input checked="" type="checkbox"/>	All	None	1
3	<input checked="" type="checkbox"/>	All	None	1
4	<input type="checkbox"/>	All	Specific	1
5	<input type="checkbox"/>	All	Specific	1

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.

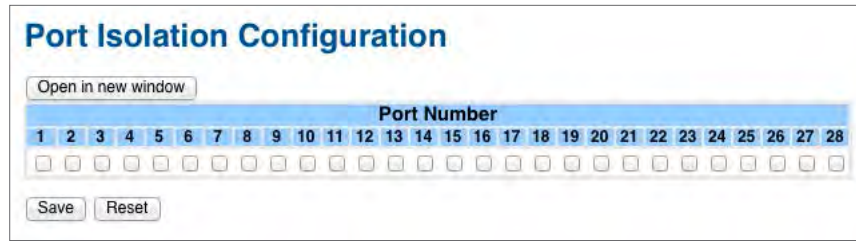
A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.



Label	Description
Delete	Check the box next to an ID 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	Click Add a 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. Click OK to discard the incorrect entry, or click Cancel to return to the editing and make a correction.

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

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



Label	Description
Port Members	A check box is provided for each port of a private VLAN.

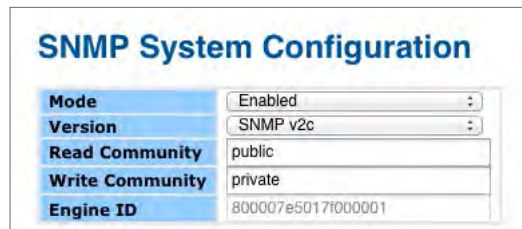
When checked, port isolation is enabled for that port.

When unchecked, port isolation is disabled for that port.

By default, port isolation is disabled for all ports.

SNMP

SNMP - System



Label	Description
Mode	Indicates the SNMP mode operation. Possible modes are: Enabled: Enable SNMP mode operation. Disabled: Disable SNMP mode operation.
Version	Indicates the SNMP supported version. Possible versions are: SNMP v1: Set SNMP supported version 1. SNMP v2c: Set SNMP supported version 2c. 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)	1
Trap Inform Retry Times	5

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 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.

SNMP - Communities

Configure SNMPv3 community's table on this page. The entry index key is Community.

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.

SNMPv3 Users Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

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 equal system engine ID then it is local user; otherwise it's 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: No 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: No 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: No 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.

SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group
<input type="checkbox"/>	usm	default_user	default_rw_group

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.

SNMPv3 Views Configuration

Delete	View Name	View Type	OID Subtree
<input type="checkbox"/>	default_view	included	.1

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. General, 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 digital number or asterisk (*).

SNMP - Accesses

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

SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	default_ro_group	any	NoAuth, NoPriv	default_view ▾	None ▾
<input type="checkbox"/>	default_rw_group	any	NoAuth, NoPriv	default_view ▾	default_view ▾

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: No authentication and no 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.

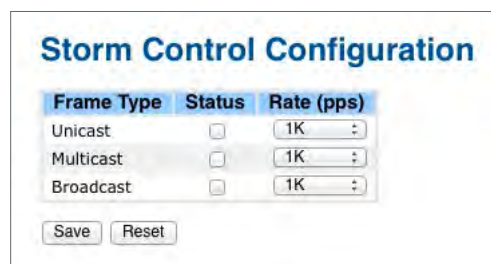
Traffic Prioritization

Storm Control

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 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. The 1 kpps is actually 1002.1 pps.

Port QoS

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	4	8
2	Low	1	0	Strict Priority	1	2	4	8
3	Low	1	0	Strict Priority	1	2	4	8
4	Low	1	0	Strict Priority	1	2	4	8
5	Low	1	0	Strict Priority	1	2	4	8
6	Low	1	0	Strict Priority	1	2	4	8
7	Low	1	0	Strict Priority	1	2	4	8
8	Low	1	0	Strict Priority	1	2	4	8
9	Low	1	0	Strict Priority	1	2	4	8
10	Low	1	0	Strict Priority	1	2	4	8
11	Low	1	0	Strict Priority	1	2	4	8
12	Low	1	0	Strict Priority	1	2	4	8
13	Low	1	0	Strict Priority	1	2	4	8
14	Low	1	0	Strict Priority	1	2	4	8
15	Low	1	0	Strict Priority	1	2	4	8
16	Low	1	0	Strict Priority	1	2	4	8
17	Low	1	0	Strict Priority	1	2	4	8
18	Low	1	0	Strict Priority	1	2	4	8
19	Low	1	0	Strict Priority	1	2	4	8
20	Low	1	0	Strict Priority	1	2	4	8
21	Low	1	0	Strict Priority	1	2	4	8
22	Low	1	0	Strict Priority	1	2	4	8
23	Low	1	0	Strict Priority	1	2	4	8
24	Low	1	0	Strict Priority	1	2	4	8
25	Low	1	0	Strict Priority	1	2	4	8
26	Low	1	0	Strict Priority	1	2	4	8
27	Low	1	0	Strict Priority	1	2	4	8
28	Low	1	0	Strict Priority	1	2	4	8

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.

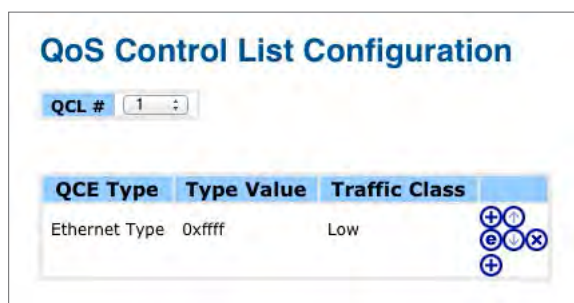
Frames can be classified by 4 different QoS classes: Low, Normal, Medium, and High.

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 Type	Specifies which frame fields 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. × : Deletes the QCE. + : The lowest plus sign adds a new entry at the bottom of the list of QCL.

Queuing Counters

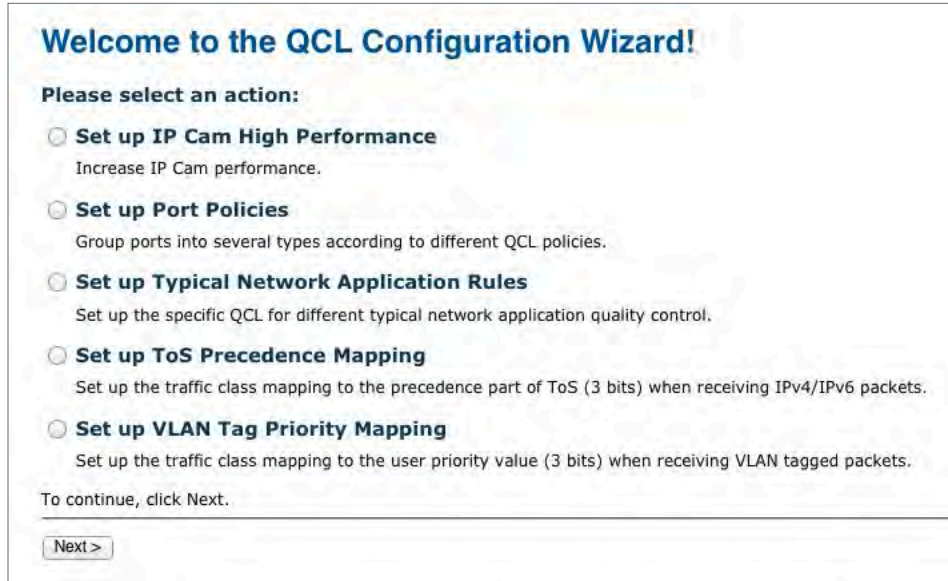
This page provides statistics for the different queues for all switch ports.

Queuing Counters									
Auto-refresh <input type="checkbox"/> Refresh Clear									
Port	Low Queue		Normal Queue		Medium Queue		High Queue		
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit	
1	0	0	0	0	0	0	0	0	0
2	44644	0	0	0	0	0	0	0	30436
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
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
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0	0

Label	Description
Port	The logical port for the settings contained in the same row.
Low Queue	There are 4 QoS queues per port with strict or weighted queuing scheduling. This is the lowest priority queue.
Normal Queue	This is the normal priority queue of the 4 QoS queues. It has higher priority than the "Low Queue".
Medium Queue	This is the medium priority queue of the 4 QoS queues. It has higher priority than the "Normal Queue".
High Queue	This is the highest priority queue of the 4 QoS queues.
Receive / Transmit	The number of received and transmitted packets per port.

Wizard

This handy wizard helps you set up a QCL quickly.



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.

Multicast

IGMP Snooping

This page provides IGMP Snooping related configuration.

The screenshot shows the 'IGMP Snooping Configuration' interface. It is divided into two main sections: 'Global Configuration' and 'Port Related Configuration'.
Global Configuration: Contains two checkboxes: 'Snooping Enabled' (unchecked) and 'Unregistered IPMC Flooding enabled' (unchecked).
Port Related Configuration: Contains a table with columns 'VLAN ID', 'Snooping Enabled', and 'IGMP Querier'.

VLAN ID	Snooping Enabled	IGMP Querier
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
50	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Port Related Configuration: Contains a table with columns 'Port', 'Router Port', and 'Fast Leave'.

Port	Router Port	Fast Leave
1	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>
...		
26	<input type="checkbox"/>	<input type="checkbox"/>
27	<input type="checkbox"/>	<input type="checkbox"/>
28	<input type="checkbox"/>	<input type="checkbox"/>

At the bottom of the configuration area are 'Save' and 'Reset' buttons.

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 Querier in the VLAN. The Querier will send out if no Querier received in 255 seconds after IGMP Querier Enabled. Each Querier's interval is 125 second, and it will stop act as an IGMP Querier if received any Querier 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 querier. 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
50	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	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
	No IGMP groups																												

Router Port

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

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 Querier.
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	Click 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.

ACL

Ports

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

Refresh Clear

Port	Policy ID	Action	Rate Limiter ID	Port Copy	Logging	Shutdown	Counter
1	1	Permit	Disabled	Disabled	Disabled	Disabled	0
2	1	Permit	Disabled	Disabled	Disabled	Disabled	50591
3	1	Permit	Disabled	Disabled	Disabled	Disabled	0
4	1	Permit	Disabled	Disabled	Disabled	Disabled	0
5	1	Permit	Disabled	Disabled	Disabled	Disabled	0
6	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.

Rate Limiters

Configure the rate limiter for the ACL of the switch.

Rate Limiter ID	Rate (pps)
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1

Save Reset

Label	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
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.

ACL Configuration

Configure an ACE (Access Control Entry) on this page.

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type that you selected.

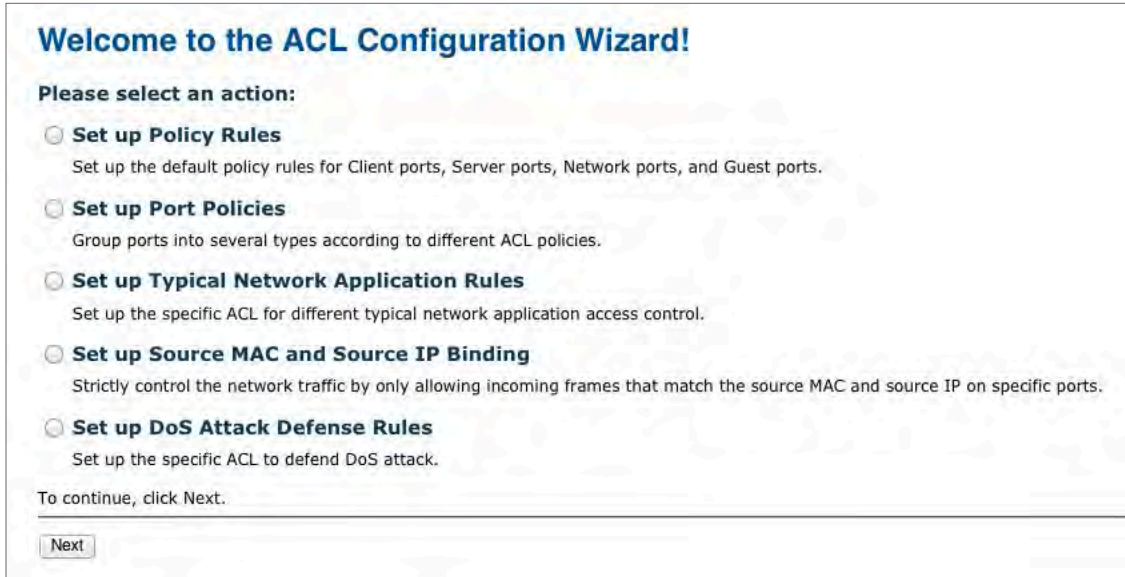
A frame that hits this ACE matches the configuration that is defined here.



Label	Description
Ingress Port	Select the ingress port for which this ACE applies. Any: The ACE applies to any port. Port n: The ACE applies to this port number, where n is the number of the switch port. Policy n: The ACE applies to this policy number, where n can range from 1 through 8.
Frame Type	Select the frame type for this ACE. These frame types are mutually exclusive. Any: Any frame can match this ACE. Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications should be greater than or equal to 1536 decimal (equal to 0600 hexadecimal). ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with Ethernet type. IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with Ethernet type.
Action	Specify the action to take with a frame that hits this ACE. Permit: The frame that hits this ACE is granted permission for the ACE operation. Deny: The frame that hits this ACE is dropped.
Rate Limiter	Specify the rate limiter in number of base units. The allowed range is 1 to 15. Disabled indicates that the rate limiter operation is disabled.
Port Copy	Frames that hit the ACE are copied to the port number specified here. The allowed range is the same as the switch port number range. Disabled indicates that the port copy operation is disabled.
Logging	Specify the logging operation of the ACE. The allowed values are: Enabled: Frames matching the ACE are stored in the System Log. Disabled: Frames matching the ACE are not logged. Please note that the System Log memory size and logging rate is limited.
Shutdown	Specify the port shut down operation of the ACE. The allowed values are: Enabled: If a frame matches the ACE, the ingress port will be disabled. Disabled: Port shut down is disabled for the ACE.
Counter	The counter indicates the number of times the ACE was hit by a frame.

Wizard

This handy wizard helps you set up an ACL quickly



Label	Description
Set up Policy Rules	Set up the default policy rules for Client ports, Server ports, Network ports and Guest ports.
Set up Port Policies	Group ports into several types according to different ACL policies.
Set up Typical Network Application Rules	Set up the specific ACL for different typical network application access control.
Set up Source MAC and Source IP Binding	Strictly control the network traffic by only allowing incoming frames that match the source IP and source MAC on specific port.
Set up DoS Attack Defense Rules	Set up the specific ACL to defend DoS attack.

802.1x

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the Authentication configuration page.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

Overview of 802.1X (Port-Based) Authentication

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note: *Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the Authentication configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.*

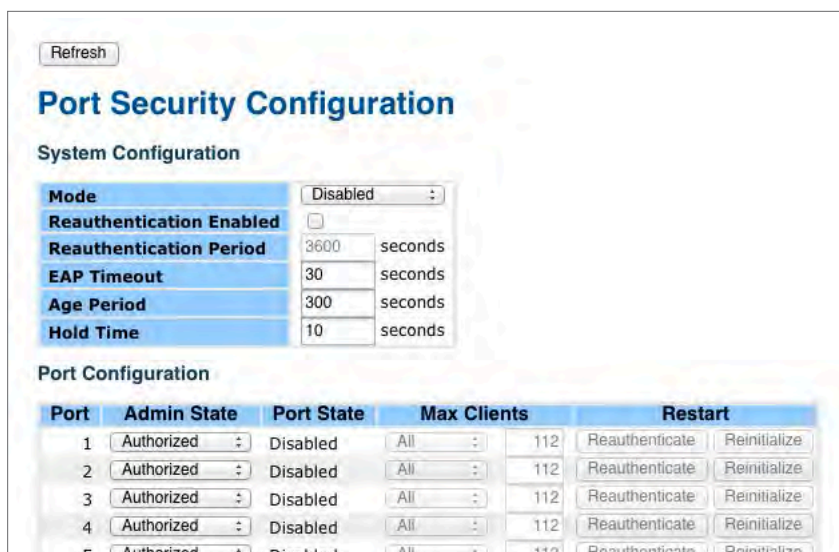
Overview of MAC-Based Authentication

Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client’s MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form “xx-xx-xx-xx-xx-xx”, that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using static entries into the MAC Table. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don’t need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users, equipment whose MAC address is a valid RADIUS user can be used by anyone, and only the MD5-Challenge method is supported.

The 802.1X and MAC-Based Authentication configuration consists of two sections, System Configuration and Port Configuration.



Label	Description
System Configuration	
Mode	<p>Indicates if 802.1X and MAC-based authentication is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.</p> <p>If checked, clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port.</p> <p>For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Age Period below).</p> <p>Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.</p>
EAP Timeout	<p>Determines the time the switch shall wait for the supplicant response before retransmitting a packet. Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.</p>
Age Period	<p>This setting applies to ports running MAC-based authentication, only.</p> <p>Suppose a client is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch that runs MAC-based authentication, and suppose the client gets successfully authenticated. Now assume that the client powers down his PC. What should make the switch forget about the authenticated client? Reauthentication will not solve this problem, since this doesn't require the client to be present, as discussed under Reauthentication Enabled above. The solution is aging of authenticated clients. The Age Period, which can be set to a number between 10 and 1000000 seconds, works like this: A timer is started when the client gets authenticated. After half the age period, the switch starts looking for frames sent by the client. If another half age period elapses and no frames are seen, the client is considered removed from the system, and it will have to authenticate again the next time a frame is seen from it. If, on the other hand, the client transmits a frame before the second half of the age period expires, the switch will consider the client alive, and leave it authenticated. Therefore, an age period of T will require the client to send frames more frequent than T/2 for him to stay authenticated.</p>
Hold Time	<p>This setting applies to ports running MAC-based authentication, only.</p> <p>If the RADIUS server denies a client access, or a RADIUS server request times out (according to the timeout specified on the Authentication configuration page), the client is put on hold in the unauthorized state. In this state, frames from the client will not cause the switch to attempt to re-authenticate the client. The Hold Time, which can be set to a number between 10 and 1000000 seconds, determines the time after an EAP Failure indication or RADIUS timeout that a client is not allowed access.</p>

Label	Description
System Configuration	
Port	The port number for which the configuration below applies.
Admin State	<p>Sets the authentication mode to one of the following options (only used when 802.1X or MAC-based authentication is globally enabled):</p> <p>Auto: Requires an 802.1X-aware client (supplicant) to be authorized by the authentication server. Clients that are not 802.1X-aware will be denied access.</p> <p>Authorized: Forces the port to grant access to all clients, 802.1X-aware or not. The switch transmits an EAPOL Success frame when the port links up.</p> <p>Unauthorized: Forces the port to deny access to all clients, 802.1X-aware or not. The switch transmits an EAPOL Failure frame when the port links up.</p> <p>MAC-Based: Enables MAC-based authentication on the port. The switch does not transmit or accept EAPOL frames on the port. Flooded frames and broadcast traffic will be transmitted on the port, whether or not clients are authenticated on the port, whereas unicast traffic against an unsuccessfully authenticated client will be dropped. Clients that are not yet successfully authenticated will not be allowed to transmit frames of any kind.</p>
Port State	<p>The current state of the port. It can undertake one of the following values:</p> <p>Disabled: 802.1X and MAC-based authentication is globally disabled.</p> <p>Link Down: 802.1X or MAC-based authentication is enabled, but there is no link on the port.</p> <p>Authorized: The port is authorized. This is the case when 802.1X authentication is enabled, the port has link, and the Admin State is "Auto" and the supplicant is authenticated or the Admin State is "Authorized".</p> <p>Unauthorized: The port is unauthorized. This is the case when 802.1X authentication is enabled, the port has link, and the Admin State is "Auto", but the supplicant is not (yet) authenticated or the Admin State is "Unauthorized".</p> <p>X Auth/Y Unauth: X clients are currently authorized and Y are unauthorized. This state is shown when 802.1X and MAC-based authentication is globally enabled and the Admin State is set to "MAC-Based".</p>
Max Clients	<p>This setting applies to ports running MAC-based authentication, only.</p> <p>The maximum number of clients allowed on a given port can be configured through the list-box and edit-control for this setting. Choosing the value "All" from the list-box allows the port to consume up to 48 client state-machines. Choosing the value "Specific" from the list-box opens up for entering a specific number of maximum clients on the port (1 to 48).</p> <p>The switch is "born" with a pool of state-machines, from which all ports draw whenever a new client is seen on the port. When a given port's maximum is reached (both authorized and unauthorized clients count), further new clients are disallowed access. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available state-machines.</p>

Restart	<p>Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is "Auto" or "MAC-Based".</p> <p>Clicking these buttons will not cause settings changed on the page to take effect.</p> <p>Reauthenticate: Schedules a reauthentication to whenever the quiet-period of the port runs out (port-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.</p> <p>The button only has effect for successfully authenticated ports/clients and will not cause the port/client to get temporarily unauthorized.</p> <p>Reinitialize: Forces a reinitialization of the port/clients and thereby a re-authentication immediately. The port/clients will transfer to the unauthorized state while the reauthentication is ongoing.</p>
---------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Port Security Status

Auto-refresh Refresh

Port	State	Last Source	Last ID
1	Disabled		
2	Disabled		
3	Disabled		
4	Disabled		
5	Disabled		
6	Disabled		
7	Disabled		
8	Disabled		
9	Disabled		
10	Disabled		
11	Disabled		
12	Disabled		
13	Disabled		
14	Disabled		
15	Disabled		
16	Disabled		
17	Disabled		
18	Disabled		
19	Disabled		
20	Disabled		
21	Disabled		
22	Disabled		
23	Disabled		
24	Disabled		
25	Disabled		
26	Disabled		
27	Disabled		
28	Disabled		

Label	Description
Port	The switch port number. Click to navigate to detailed 802.1X statistics for this port.
State	The current state of the port. Refer to IEEE 802.1X Port State for a description of the individual states.
Last Source	The source MAC address carried in the most recently received EAPOL frame for port-based authentication, and the most recently received frame from a new client for MAC-based authentication.
Last ID	The user name (supplicant identity) carried in the most recently received Resp/ID EAPOL frame for port-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

802.1X Statistics

802.1X Statistics Port 1

Port 1 : Auto-refresh Refresh Clear

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	Total	0
Response ID	0	Request ID	0
Responses	0	Requests	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		
Receive Backend Server Counters		Transmit Backend Server Counters	
Access Challenges	0	Responses	0
Other Requests	0		
Auth. Successes	0		
Auth. Failures	0		
Last Supplicant Info			
Version			0
Source			
Identity			

This page provides detailed IEEE 802.1X statistics for a specific switch port running port-based authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only. Use the port select box to select which port details to be displayed.

Label	Description
<p>EAPOL Counters (Receive / Transmit)</p>	<p>These counters are not available for MAC-based ports. Supplicant frame counter statistics. There are seven receive frame counters and three transmit frame counters. RX Direction: Total: Number of valid EAPOL frames of any type that have been received by the switch Response ID: Number of valid EAP Resp/ID frames that have been received by the switch Responses: Number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch Start: Number of EAPOL Start frames that have been received by the switch Logoff: Number of valid EAPOL logoff frames that have been received by the switch Invalid Type: Number of EAPOL frames that have been received by the switch in which the frame type is not recognized TX Direction: Total: Number of EAPOL frames of any type that have been transmitted by the switch Request ID: Number of EAP initial request frames that have been transmitted by the switch Requests: Number of valid EAP Request frames (other than initial request) that have been transmitted by the switch.</p>
<p>Backend Server Counters (Receive / Transmit)</p>	<p>Backend server frame counter statistics. For MAC-based ports there are two tables containing backend server counters. The left most shows a summary of all backend server counters on this port. The right most shows backend server counters for the currently selected client, or dashes if no client is selected or available. A client can be selected from the list of authorized/unauthorized clients below the two counter tables. There are slight differences in the interpretation of the counters between port- and MAC-based authentications.</p>
<p>Last Supplicant Info</p>	<p>For MAC-based ports, this section is embedded in the backend server counter's section. Information about the last supplicant/client that attempted to authenticate.</p>
<p>Clients attached to this port</p>	<p>This table is only available for MAC-based ports Each row in the table represents a MAC-based client on the port, and there are three parameters for each client: MAC Address: Shows the MAC address of the client, which is also used as the password in the authentication process against the backend server. Clicking the link causes the client's backend server counters to be shown in the right-most backend server counters table above. If no clients are attached, it shows No clients attached. State: Shows whether the client is authorized or unauthorized. As long as the backend server hasn't successfully authenticated a client, it is unauthorized Last Authentication: Show the date and time of the last authentication of the client. This gets updated for every re-authentication of the client.</p>

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	

Save Reset

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'.

RADIUS Authentication Server Status Overview

Auto-refresh Refresh

#	IP Address	Status
1	0.0.0.0:1812	Disabled
2	0.0.0.0:1812	Disabled
3	0.0.0.0:1812	Disabled
4	0.0.0.0:1812	Disabled
5	0.0.0.0:1812	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:1813	Disabled
2	0.0.0.0:1813	Disabled
3	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
5	0.0.0.0:1813	Disabled

Label	Description
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
State	The current state of the server. This field takes one of the following values: Disabled: The server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Authentication Statistics for Server #1 (0.0.0.0:1812)

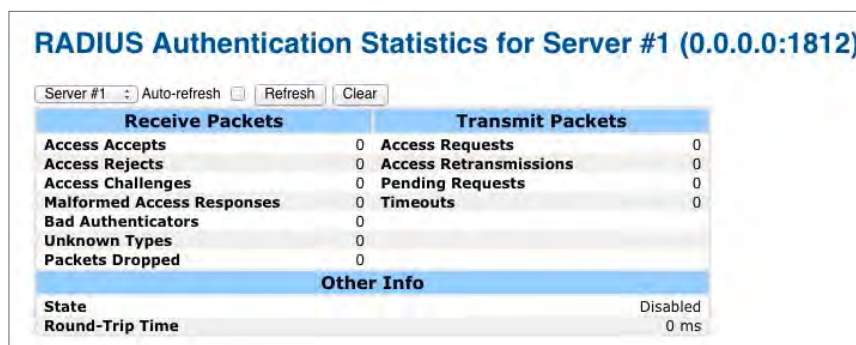
Server #1 : Auto-refresh Refresh Clear

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
State		Disabled	
Round-Trip Time		0 ms	

RADIUS Accounting Statistics for Server #1 (0.0.0.0:1813)

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
State		Disabled	
Round-Trip Time		0 ms	

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for.



Label	Description
Packet Counters	<p>RADIUS authentication server packet counter. There are seven receive and four transmit counters.</p> <p>RX Direction:</p> <p>Access Accepts: The number of RADIUS Access-Accept packets (valid or invalid) received from the server.</p> <p>Access Rejects: The number of RADIUS Access-Reject packets (valid or invalid) received from the server.</p> <p>Access Challenges: The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.</p> <p>Malformed Access Responses: The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.</p> <p>Bad Authenticators: The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.</p> <p>Unknown Types: The number of RADIUS packets that were received from the server on the authentication port and dropped as unknown.</p> <p>Packets Dropped: The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.</p> <p>TX Direction:</p> <p>Access Requests: The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.</p> <p>Access Retransmissions: The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.</p> <p>Pending Requests: The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout or retransmission.</p> <p>Timeouts: The number of authentication timeouts to the server After a timeout, the client may retry to the same server, send to a different server. or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Rrequest as well as a timeout.</p>

Other Info	<p>This section contains information about the state of the server and the latest round-trip time.</p> <p>State: Shows the state of the server as one of the following values. Disabled: The selected server is disabled. Not Ready: The server is enabled but IP Communication is not yet up and running. Ready: The server is enabled, IP Communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to the server but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead time expires. The number of seconds left before this occurs is displayed in parenthesis. The state is only reachable when more than one server is enabled.</p> <p>Round Trip Time: The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicated that there hasn't been round-trip communication with the server yet.</p>
------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

RADIUS Accounting Statistics for Server #1 (0.0.0.0:1813)			
Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
State			Disabled
Round-Trip Time			0 ms

Label	Description
Packet Counters	<p>RADIUS accounting server packet counter. There are five receive and four transmit counters.</p> <p>RX Direction:</p> <p>Responses: The number of RADIUS packets (valid or invalid) received from the server.</p> <p>Malformed Access Responses: The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.</p> <p>Bad Authenticators: The number of RADIUS packets containing invalid authenticators or Message Authenticator attributes received from the server.</p> <p>Unknown Types: The number of RADIUS packets that were received from the server on the accounting port and dropped as unknown.</p> <p>Packets Dropped: The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.</p> <p>TX Direction:</p> <p>Requests: The number of RADIUS packets sent to the server. This does not include retransmissions.</p> <p>Retransmissions: The number of RADIUS packets retransmitted to the RADIUS authentication server.</p> <p>Pending Requests: The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Response, timeout or retransmission.</p> <p>Timeouts: The number of accounting timeouts to the server After a timeout, the client may retry to the same server, send to a different server. or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Rrequest as well as a timeout.</p>

Other Info	<p>This section contains information about the state of the server and the latest round-trip time.</p> <p>State: Shows the state of the server as one of the following values. Disabled: The selected server is disabled. Not Ready: The server is enabled but IP Communication is not yet up and running. Ready: The server is enabled, IP Communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to the server but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead time expires. The number of seconds left before this occurs is displayed in parenthesis. The state is only reachable when more than one server is enabled.</p> <p>Round Trip Time: The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicated that there hasn't been round-trip communication with the server yet.</p>
------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

TACACS+

Server Configuration

#	Enabled	IP Address	Port	Secret
1	<input type="checkbox"/>		49	
2	<input type="checkbox"/>		49	
3	<input type="checkbox"/>		49	
4	<input type="checkbox"/>		49	
5	<input type="checkbox"/>		49	

Save Reset

Use this page to enable TACACS+ by IP Address.

Warning

System Warning

SYSLOG Setting

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

Syslog Server

IP Address: 0.0.0.0

Save Reset

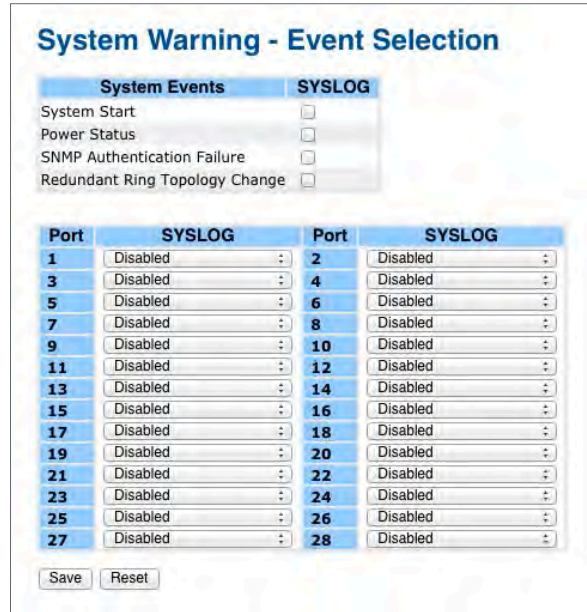
System Warning - SYSLOG Setting interface

The following table describes the labels in this screen.

Label	Description
SYSLOG Server IP Address	The remote SYSLOG Server IP address.

Event Selection

SYSLOG is the warning method supported by the system. Click on the dropdown selection to enable system event warning.



System Warning - Event Selection interface

The following table describes the labels in this screen.

Section		Description
System Event	System Cold Start	Alert when system restart
	Power Status	Alert when a power up or down
	SNMP Authentication Failure	Alert when SNMP authentication failure.
	Redundant Ring Topology Change	Alert when C-Ring topology changes.
Port Event	SYSLOG	Disable Link Up Link Down Link Up & Link Down
Save		Activate the configurations.
Reset		Clear your changes without saving.

Monitor and Diag

MAC Table

Configuration

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. The allowed range is 10 to 1000000 seconds.

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

MAC Table Learning

If the learning mode for a given port is grayed out, another module is in control of the mode, so that the user cannot change it. An example of such a module is the MAC-Based Authentication under 802.1X.

Each port can perform learning based upon the following settings:

Label	Description
Auto	Learning is performed automatically as soon as a frame with unknown SMAC is received.
Disable	No learning is performed.
Secure	Only static MAC entries are learned, all other frames are dropped.

Note: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

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.

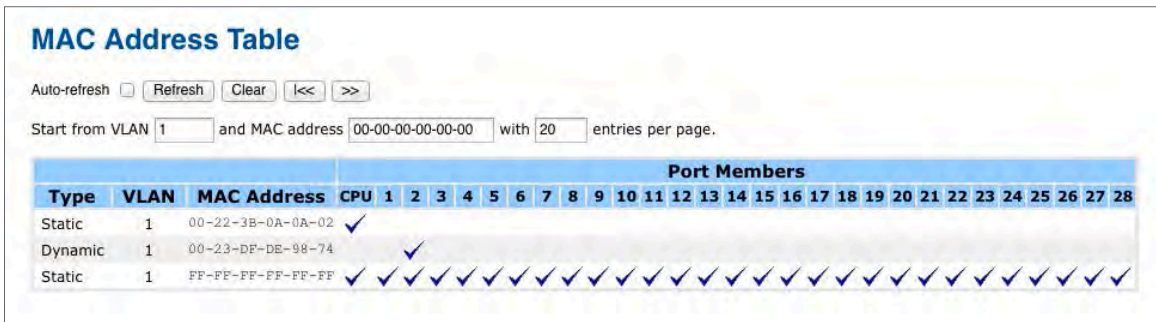
Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Adding a New Static Entry	Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click Save .

MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the “entries per page” input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The “Start from MAC address” and “VLAN” input fields allow the user to select the starting point in the MAC Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text “no more entries” is shown in the displayed table. Use the << button to start over.



Label	Description
Type	Indicates whether the entry is a static or dynamic entry.
MAC address	The MAC address of the entry.
VLAN	The VLAN ID of the entry.
Port Members	The ports that are members of the entry.

Port Statistic

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	0	0	0	0	0	0	0	0	0
2	26232	14932	4723854	3353893	0	0	0	0	1142
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
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
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0	0
28	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 Port Statistics Port 1			
Port 1		Auto-refresh <input type="checkbox"/> Refresh Clear	
Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Low	0	Tx Low	0
Rx Normal	0	Tx Normal	0
Rx Medium	0	Tx Medium	0
Rx High	0	Tx High	0
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

Detailed Statistics-Receive & Transmit Total

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 received 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.

Port 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

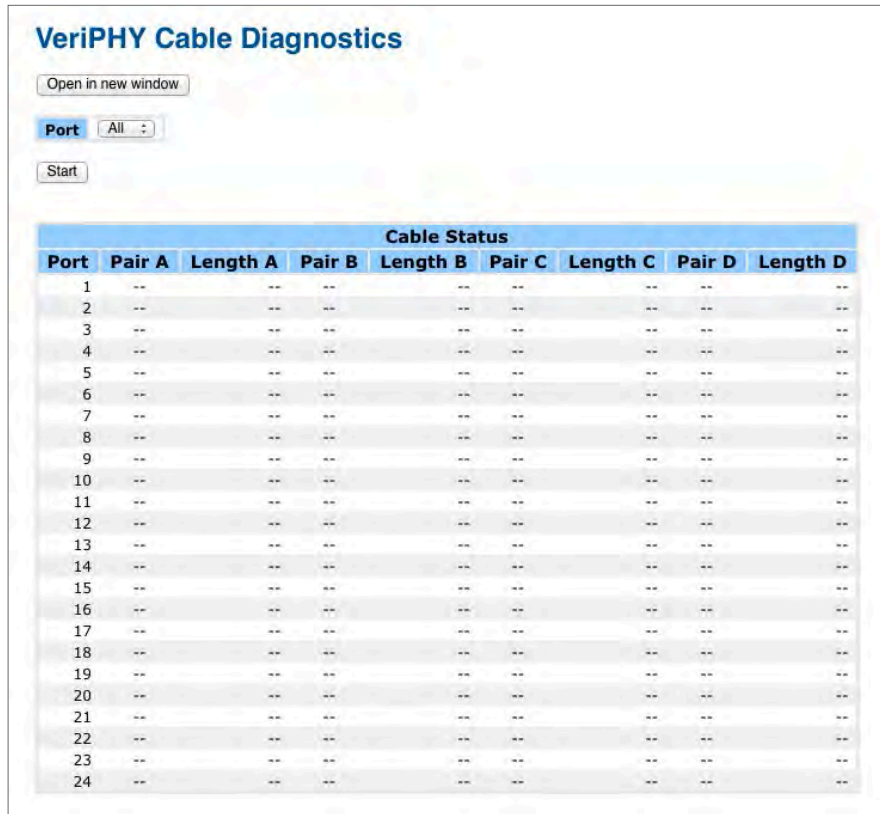
The switch system log information is provided here.



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.

Cable Diagnostics

This page is used for running the VeriPHY Cable Diagnostics.



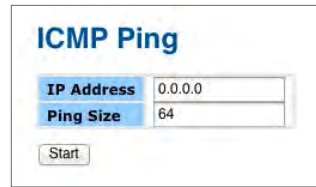
Press **Start** to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate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

Ping

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



The image shows a web-based interface for performing an ICMP Ping. It has a title 'ICMP Ping' in blue. Below the title are two input fields: 'IP Address' with the value '0.0.0.0' and 'Ping Size' with the value '64'. At the bottom of the form is a 'Start' button.

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.

Factory Defaults

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

Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?

Keep IP
 Keep User/Password

Label	Description
Yes	Click to reset the configuration to Factory Defaults.
No	Click to return to the Port State page without resetting the configuration

System Reboot

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

Warm Reset

Are you sure you want to perform a Warm Restart?

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

Command Line Interface Management

About CLI Management

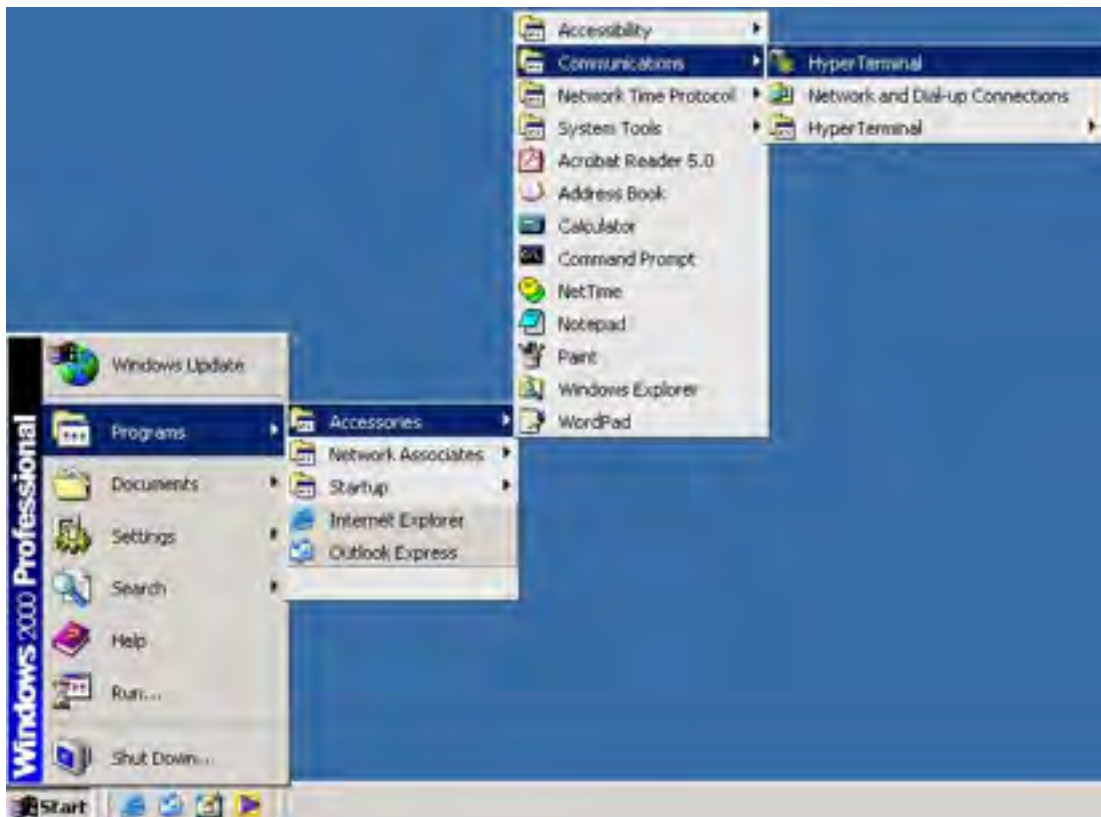
In addition to WEB-base management, the CWGE28FX4TX24MS also supports CLI management. You can use console or telnet to management the switch by CLI.

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

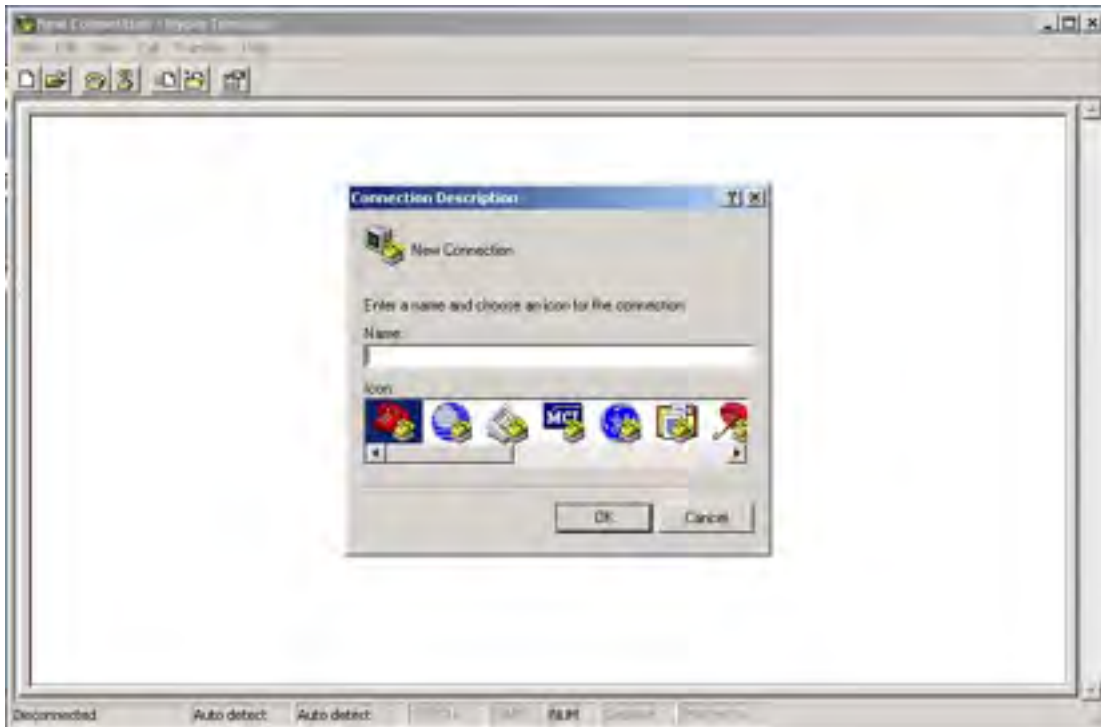
Before Configuring by RS-232 serial console, use an DB-9-M to DB-9-F cable to connect the switches' RS-232 Console port to your PC COM port.

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

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



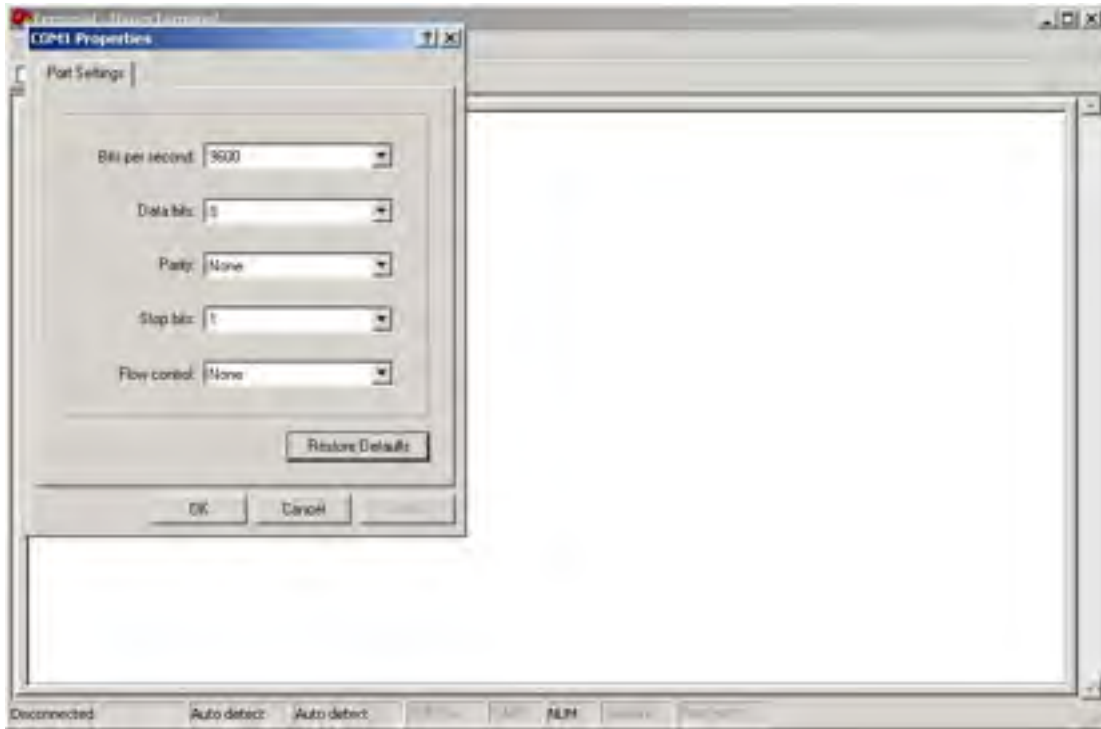
Step 2. Input a name for new connection



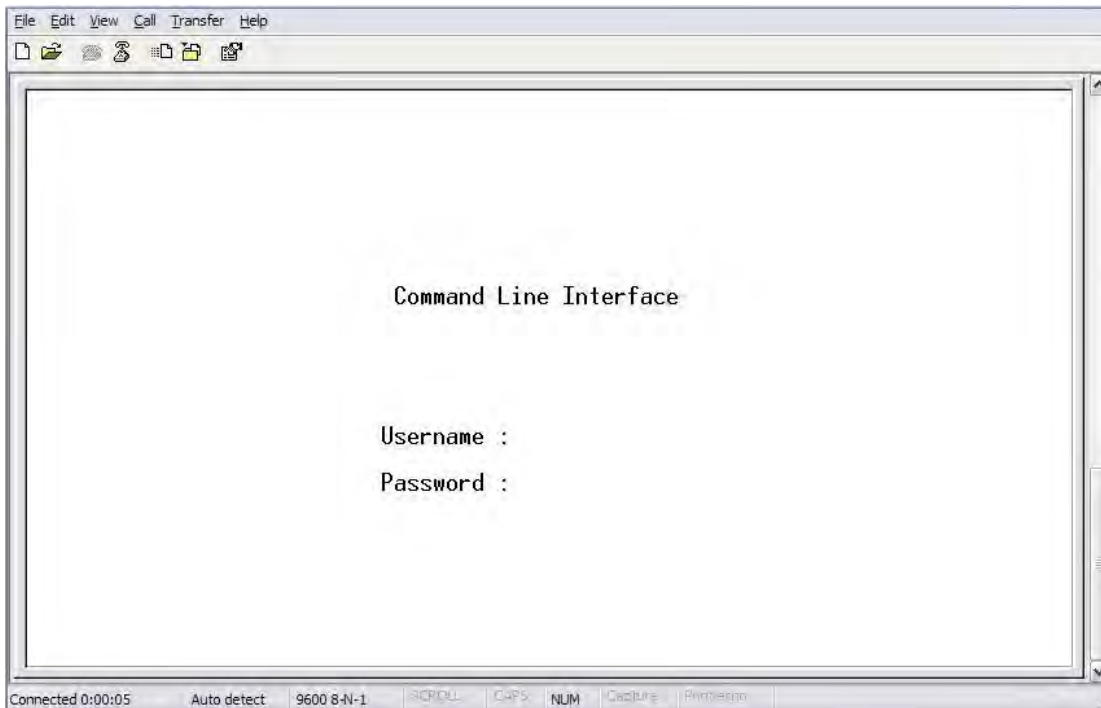
Step 3. Select to use COM port number



Step 4. The COM port properties setting, 115200 for baud rate, 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 (these are the same as the credentials for Web Browser), and 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

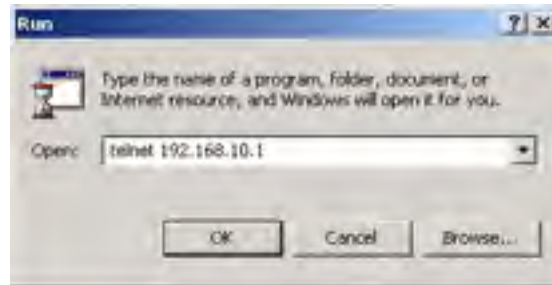
Default Gateway: 192.168.10.254

User Name: admin

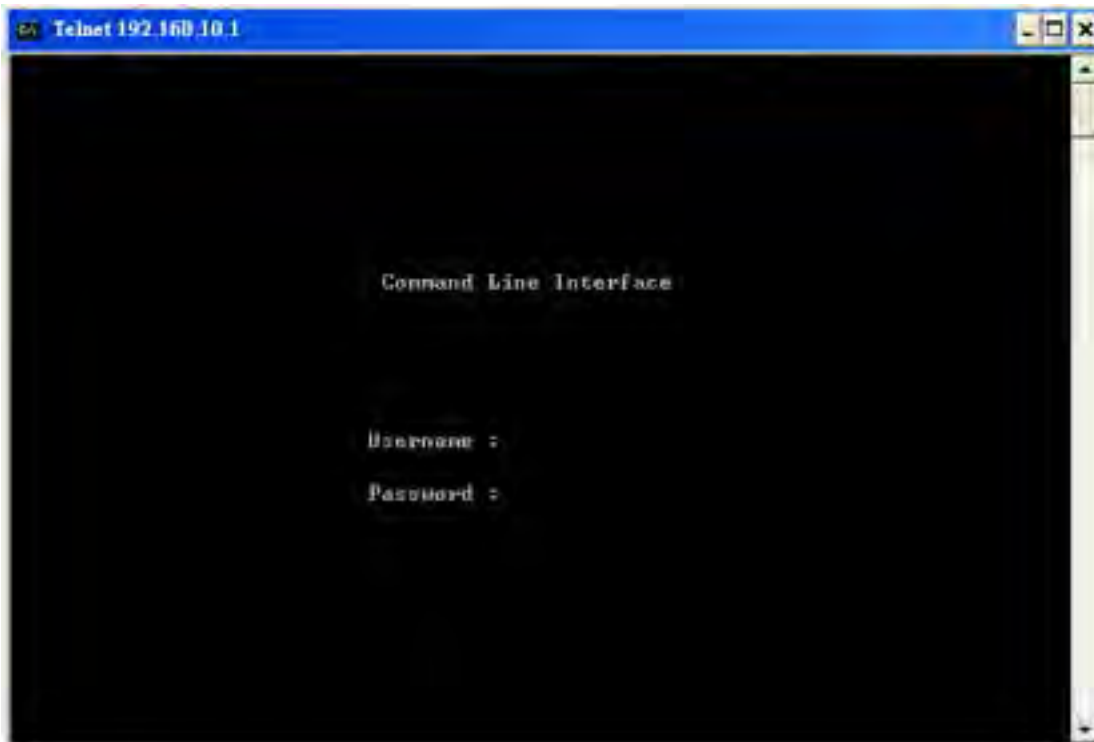
Password: admin

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**



Commander Groups

System

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

Syslog

Syslog>	ServerConfiguration [<ip_addr>]
---------	---------------------------------

IP

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

Auth

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

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]
	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>]
	Learning [<port_list>] [auto disable secure]
	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

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

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>
	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>
-----------	-----------------------------------

SFLOW

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

Technical Specifications

ComNet Switch Model	CWGE28FX4TX24MS
Physical Ports	
Gigabit Ports 10/100/1000Base-T(X)	24
1000Base-X SFP Port	4
Technology	
Ethernet Standards	<p>IEEE 802.3 for 10Base-T</p> <p>IEEE 802.3u for 100Base-TX and 100Base-FX</p> <p>IEEE 802.3z for 1000Base-X</p> <p>IEEE 802.3ab for 1000Base-T</p> <p>IEEE 802.3x for Flow control</p> <p>IEEE 802.3ad for LACP (Link Aggregation Control Protocol)</p> <p>IEEE 802.1D for STP (Spanning Tree Protocol)</p> <p>IEEE 802.1p for COS (Class of Service)</p> <p>IEEE 802.1Q for VLAN Tagging</p> <p>IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol)</p> <p>IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol)</p> <p>IEEE 802.1x for Authentication</p> <p>IEEE 802.1AB for LLDP (Link Layer Discovery Protocol)</p>
MAC Table	8k
Priority Queues	4
Processing	Store-and-Forward
Switch Properties	<p>Switching latency: 7 us</p> <p>Switching bandwidth: 56Gbps</p> <p>Max. Number of Available VLANs: 4096</p> <p>IGMP multicast groups: 128 for each VLAN</p> <p>Port rate limiting: User Defined</p>
Jumbo frame	Up to 9.6K Bytes
Security Features	<p>Device Binding security feature</p> <p>Enable/disable ports, MAC based port security</p> <p>Port based network access control (802.1x)</p> <p>VLAN (802.1Q) to segregate and secure network traffic</p> <p>Radius centralized password management</p> <p>SNMPv3 encrypted authentication and access security</p> <p>Https / SSH enhance network security</p>

Software Features	STP/RSTP/MSTP (IEEE 802.1D/w/s) Redundant Ring (C-Ring) with recovery time less than 30ms over 250 units TOS/Diffserv supported Quality of Service (802.1p) for real-time traffic VLAN (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 SMTP Client
Network Redundancy	C-Ring Legacy Ring STP / RSTP compatible MSTP
RS-232 Serial Console Port	RS-232 in RJ45 connector with console cable. 115200bps, 8, N, 1
LED indicators	
Power indicator	Green Power LED × 3
R.M. indicator	Green - system operating in C-Ring Master mode
Ring indicator	Green - system operating in C-Ring mode
Fault indicator	Amber indicates unexpected event
10/100/1000Base-T(X) RJ45 port indicator	Green for port Link/Act. Amber for Duplex/Collision
SFP fiber port indicator	Green for port Link/Act.
Power	
Input power	100~240VAC, 50~60Hz
Power consumption (Typ.)	36 Watts
Overload current protection	Present
Mechanical	
Enclosure	IP-20
Dimension (W × D × H)	17.50 × 7.88 × 1.75 in (44.45 × 20.00 × 4.45 cm)
Weight	<13 lbs/ 6kg
Environmental	
Storage Temperature	-40 to 85°C (-40 to 185°F)
Operating Temperature	-10° to +60° C (+14° to +140° 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	5 years

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