comnet
Communication Networks

INSTALLATION AND OPERATION MANUAL

CNGE12FX4TX8MS[POE]/TS

TRAFFIC DETECTOR RACK INDUSTRIALLY HARDENED MANAGED SWITCH WITH (8) 10/100/1000BASE-TX & (4) 100/1000BASE-FX PORTS & OPTIONAL POE+

This manual serves the following ComNet Model Numbers:

CNGE12FX4TX8MS/TS
CNGE12FX4TX8MSPOE/TS

The ComNet CNGE12FX4TX8MS[POE]/TS is a twelve port, managed Ethernet switch. The switch is mechanically designed to fit into the input file of a NEMA TS2 traffic detector rack and derives power and ground from the backplane. The small form factor allows the user to take advantage of existing rack space already dedicated within an already space limited traffic cabinet making installation clean and easy. The four SFP ports are 100/1000Mbps capable, allowing single-mode or multimode optical fiber transmission with the use of optional SFPs. The density of the SFP ports allows for an optical drop-and-repeat, ring or star (north-south-east-west) topology to address the majority of traffic applications. The remaining eight RJ-45 ports allow for high-throughput 10/100/1000TX Gigabit connectivity on the local copper Ethernet access ports. The CNGE12FX4TX8MSPOE/TS features IEEE 802.3at (30W) PoE on all eight RJ-45 Ethernet ports for PoE-compliant devices such as wireless radios or IP cameras. The ideal solution when footprint within the traffic cabinet is limited.

Contents

About This Guide 5
Related Documentation 5
About ComNet 5
Website 5
Support 5
Safety 5
Overview 6
Introduction 6
Software Features 7
Hardware Features 7
Hardware Overview 8
Front Panel 8
Ethernet Cables 9
1000/100BASE-TX/10BASE-T Pin Assignments 9
SFP 11
Console Cable 12
WEB Management 13
Configuration by Web Browser 13
About Web-based Management 13
Basic Setting 16
System Information 16
Admin & Password 17
Auth Method 18
IPv6 Setting 19
IP Setting 20
HTTPS 21
SSH 21
LLDP 22
LLDP Neighbor Information 23
LLDP Neighbor Information 24
Modbus TCP 26
Backup/Restore Configuration 26
Firmware Update 26

DHCP Server 26
Port Setting 30
Port Alias 31
Port Trunk 32
LACP 33
Loop Protection 37
Loop Protection Status Help 38
Redundancy 39
Legacy Ring 40
G.8032 - MEP 41
G.8032 - ERPS 42
MSTP 43
STP 49
Fast Recovery mode 52
VLAN 53
VLAN Setting Example 58
Voice VLAN - Configuration 64
Voice VLAN - OUI 66
SNMP 67
Traffic Prioritization 73
Multicast 86
Security Remote Control 90
Device Binding 91
Advanced Configuration 92
Alias IP Address 92
Alive Check 92
DDoS Prevention 93
Device Description 94
Stream Check 95
AAA 99
RADIUS Overview 101
System Warning 112
SMTP Setting 113
Monitor and Diag 115
Port Statistic 118
System Log Information 122
Cable Diagnostics 123

SFP Monitor 124
Ping 125
Syncronization-PTP 126
PoE Configuration (PoE Models Only) 128
Status 130
Factory Defaults 131
System Reboot 131
Command Line Interface Management 132
About CLI Management 132
Commander Groups 136
Technical Specifications 150

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:

- CNGE12FX4TX8MS[POE]TS Data sheet
- SFP Modules Data sheet

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 CNGE12FX4TX8MS[POE]/TS is a twelve port, managed Ethernet switch. The switch is mechanically designed to fit into the input file of a NEMA TS2 traffic detector rack and derives power and ground from the backplane. The small form factor allows the user to take advantage of existing rack space already dedicated within an already space limited traffic cabinet making installation clean and easy. The four SFP ports are 100/1000Mbps capable, allowing single-mode or multimode optical fiber transmission with the use of optional SFPs. The density of the SFP ports allows for an optical drop-and-repeat, ring or star (north-south-east-west) topology to address the majority of traffic applications. The remaining eight RJ-45 ports allow for high-throughput 10/100/1000TX Gigabit connectivity on the local copper Ethernet access ports. The CNGE12FX4TX8MSPOE/TS features IEEE 802.3at (30W) PoE on all eight RJ-45 Ethernet ports for PoE-compliant devices such as wireless radios or IP cameras. The ideal solution when footprint within the traffic cabinet is limited.

Software Features

- C-Ring (recovery time < 30ms over 250 units of connection)
- MSTP (RSTP/STP compatible) for Ethernet Redundancy
- G.8032 Ethernet Ring protection System (ERPS)
- Optional 8 ports PSE fully compliant with IEEE802.3at standard, providing up to 30 Watts per port
- IEEE 1588v2 clock synchronization
- Provides HTTPS/SSH protocol to enhance network security
- IP-based bandwidth management
- application-based QoS management
- Device Binding security function
- IGMP v2/v3 (IGMP snooping support) for filtering multicast traffic
- SNMP v1/v2c/v3 & RMON & 802.1Q VLAN Network Management
- ACL, TACACS+ and 802.1x User Authentication for security
- 9.6K Bytes Jumbo Frame
- SFP ports support DDM function
- Supports Modbus TCP Protocol
- Multiple notification for warning of unexpected event
- Web-based Telnet, Console (CLI), and Windows utility (eConsole) configuration
- LLDP Protocol
- NEMA TS2 traffic detector rack design

Hardware Features

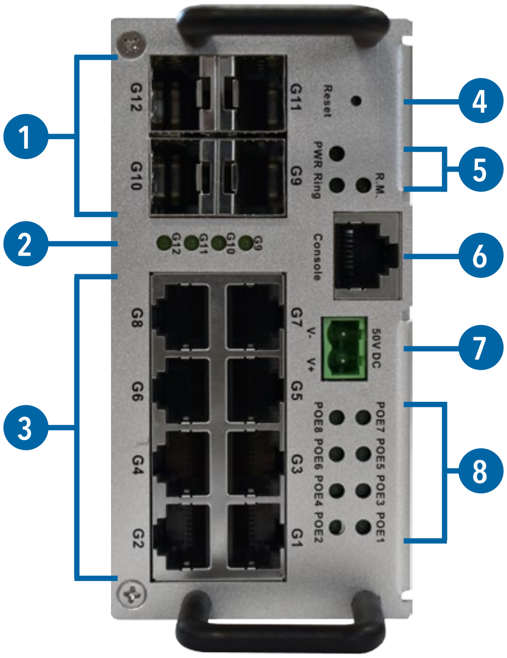
- Operating Temperature: -40° to +75° C
- Storage Temperature: – 40° to 85°C
- Operating Humidity: 5% to 97%, non-condensing
- 8 × 10/100/1000Base–T(X)
- 4 × 100/1000 Base-X SFP
- Console Port
- Dimensions: 2.23 × 4.51 × 8.08 in (5.67 × 11.45 × 20.53 cm)

Hardware Overview

Front Panel

The following table describes the labels on the CNGE12FX4TX8MS[POE]/TS series switches.

Port	Description
Gigabit SFP ports	4 x 100/1000Base-X on SFP port
Gigabit Ethernet Ports	8 x 10/100/1000Base-T(X)
Console	Use RS-232 with RJ-45 connecter to manage switch.



CNGE12FX4TX8MSPOE/TS - Typical Front Panel

1. 100/1000Base-X SFP Ports
2. Indicator LEDs for SFP Ports Link/Activity
3. 10/100/1000BaseT(X) RJ-45 Ports and Indicator LEDs for Link/Activity and Speed.
4. Reset Button
5. Indicator LEDs for Power, C-Ring and Ring Master status
6. RJ-45 Console Port
7. PoE Power Input for 48-57 V External Power Input
8. PoE Indicator LEDs

Ethernet Cables

The CNGE12FX4TX8MS[POE]/TS 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

1000/100BASE-TX/10BASE-T Pin Assignments

With 1000/100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

10/100Base-T(X) PSE RJ-45 port

Pin Number	Assignment
#1	TD+ with PoE Power input +
#2	TD – with PoE Power input +
#3	RD+ with PoE Power input –
#6	RD – with PoE Power input –

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

1000Base-T PSE RJ-45 port

Pin Number	Assignment
#1	BI_DA+ with PoE Power input +
#2	BI_DA – with PoE Power input +
#3	BI_DB+ with PoE Power input –
#4	BI_DC+
#5	BI_DC-
#6	BI_DB – with PoE Power input –
#7	BI_DD+
#8	BI_DD-

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-

The CNGE12FX4TX8MS[POE]/TS series switches support auto MDI/MDI-X operation. You can use a straight-through cable to connect PC to switch. The following table below shows the 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

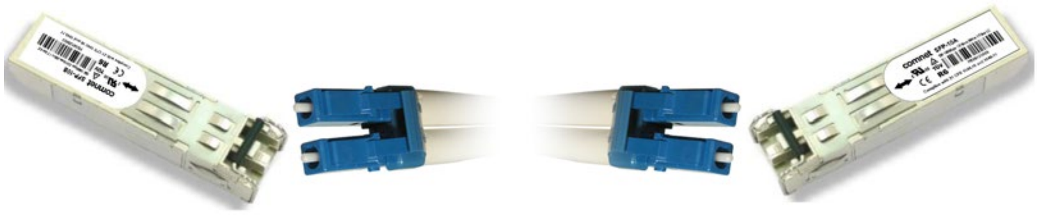
1000 Base-T MDI/MDI-X pins assignment

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

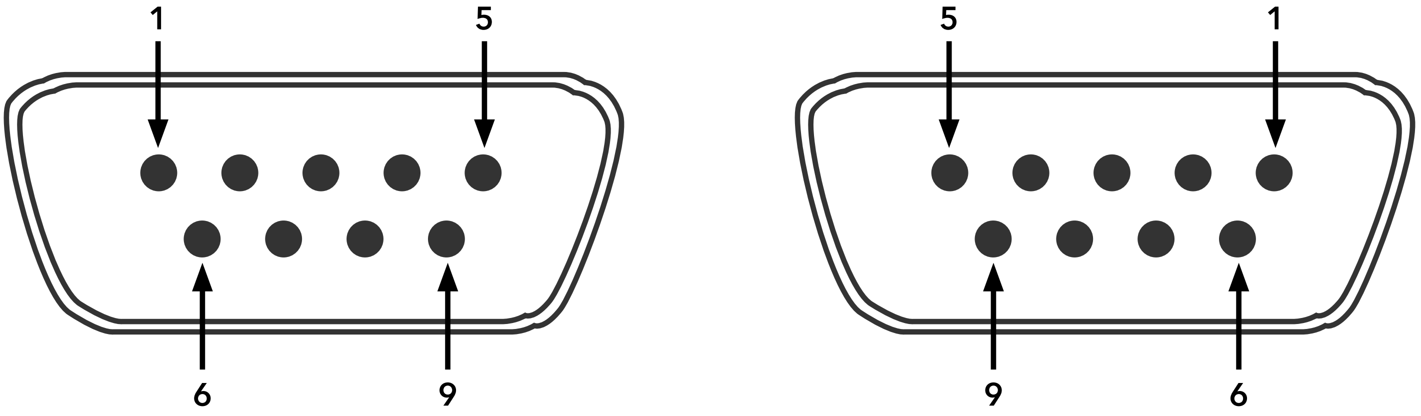
The Switch has fiber optical ports with SFP connectors. The fiber optical ports are in multi-mode (0 to 550M, 850 nm with 50/125 μm, 62.5/125 μm fiber) and single-mode with LC connector. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.



Switch A *Switch B*

Console Cable

CNGE12FX4TX8MS[POE]/TS series switches can be managed via a console port located on the front of the switch. The RJ-45 to DB-9 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 male connector) connects to console port of switch.



DB-9 Male DB-9 Female

PC pin out (male) assignment	RS-232 with DB-9 female connector	DB9 to RJ 45
Pin #2 RD	Pin #2 TD	Pin #2
Pin #3 TD	Pin #3 RD	Pin #3
Pin #5 GD	Pin #5 GD	Pin #5

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

WEB Management

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

Configuration by Web Browser

This section 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.

Preparing for Web Management

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0

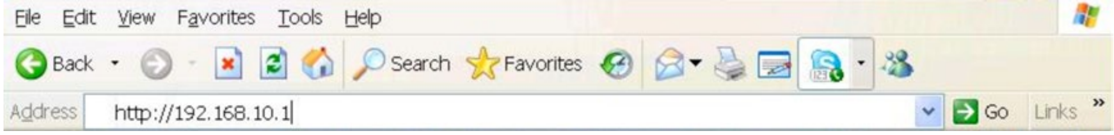
Default Gateway: 192.168.10.254

User Name: admin

Password: admin

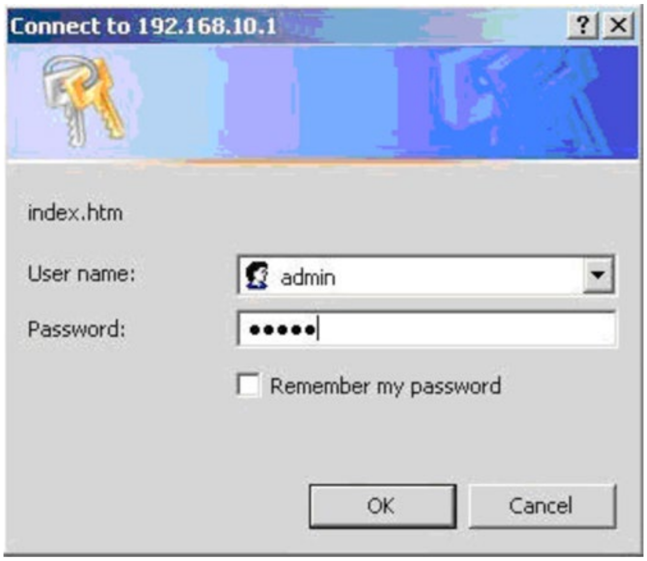
System Login

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



Address http://192.168.10.1

3. The login screen appears.



index.htm

User name: admin

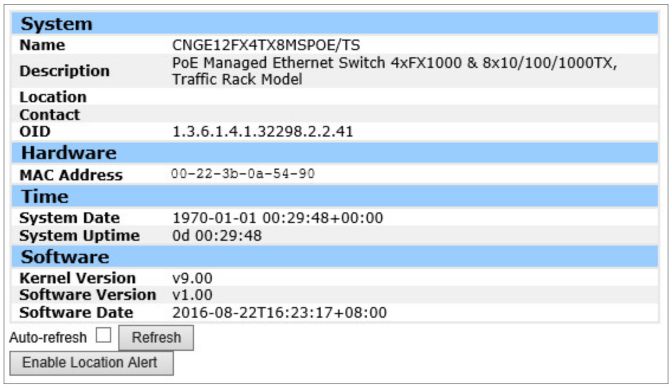
Password: •••••

□ Remember my password

Login screen

4. Key in the username and password. The default username and password is admin.
5. Press OK button, then the main interface of the Web-based management appears.

Main Interface



System	
Name	CNGE12FX4TX8MSPOE/TS
Description	PoE Managed Ethernet Switch 4xFX1000 & 8x10/100/1000TX, Traffic Rack Model
Location	
Contact	
OID	1.3.6.1.4.1.32298.2.2.41

Hardware	
MAC Address	00-22-3b-0a-54-90

Time	
System Date	1970-01-01 00:29:48+00:00
System Uptime	0d 00:29:48

Software	
Kernel Version	v9.00
Software Version	v1.00
Software Date	2016-08-22T16:23:17+08:00

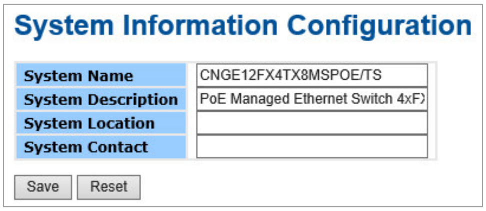
Auto-refresh ☐

Main interface

Basic Setting

System Information

The switch system information is provided here.



System Information Configuration

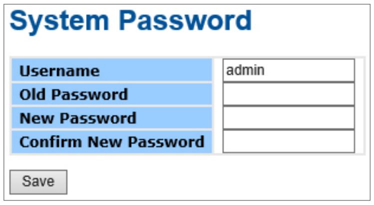
System Name	CNGE12FX4TX8MSPOE/TS
System Description	PoE Managed Ethernet Switch 4xF
System Location	
System Contact	

System Information interface

Label	Description
System Name	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-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 Description	The device Description.
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	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.
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.



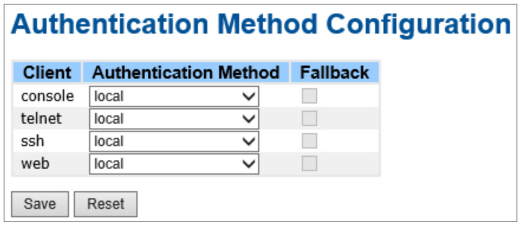
System Password

Username	admin
Old Password	
New Password	
Confirm New Password	

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.

Auth Method

This page allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.



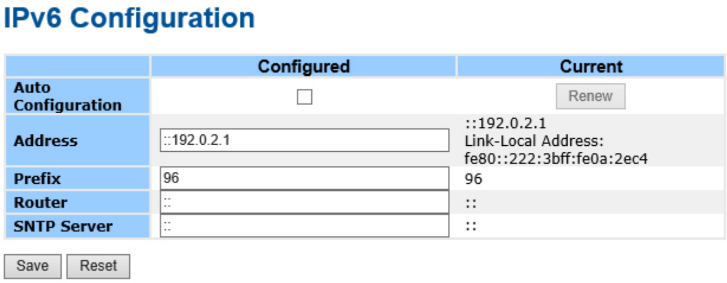
Authentication Method Configuration

Client	Authentication Method	Fallback
console	local	□
telnet	local	□
ssh	local	□
web	local	□

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

IPv6 Setting

Configure the switch-management IPv6 information on this page.



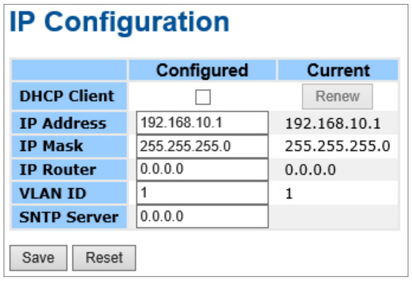
IPv6 Configuration

	Configured	Current
Auto Configuration	□	Renew
Address	::192.0.2.1	::192.0.2.1 Link-Local Address: fe80::222:3bff:fe0a:2ec4
Prefix	96	96
Router	::	::
SNTP Server	::	::

Label	Description
Auto Configuration	Enable IPv6 auto-configuration by checking this box. If the system cannot obtain the stateless address in time, the configured IPv6 settings will be used. The router may delay responding to a router solicitation for a few seconds, the total time needed to complete auto-configuration can be significantly longer.
Address	Provide the IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
Prefix	Provide the IPv6 Prefix of this switch. The allowed range is 1 to 128.
Router	Provide the IPv6 gateway address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

IP Setting

Configure the switch-managed IP information on this page.

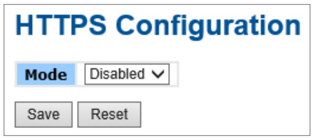


IP Configuration

	Configured	Current
DHCP Client	□	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	0.0.0.0	

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	Provide the IP address of the SNTP Server in dotted decimal notation.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

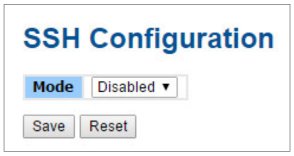
HTTPS


HTTPS Configuration

Mode Disabled

Label	Description
Mode	Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. 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.

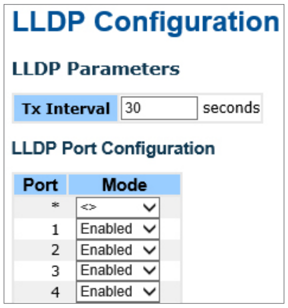
SSH


SSH Configuration

Mode Disabled

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

LLDP Parameters

Tx Interval: 30 seconds

LLDP Port Configuration

Port	Mode
*	<>
1	Enabled
2	Enabled
3	Enabled
4	Enabled

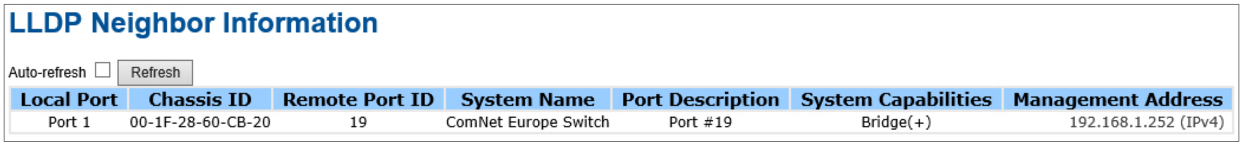
LLDP Configuration

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. 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

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:



Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	Management Address
Port 1	00-1F-28-60-CB-20	19	ComNet Europe Switch	Port #19	Bridge(+)	192.168.1.252 (IPv4)

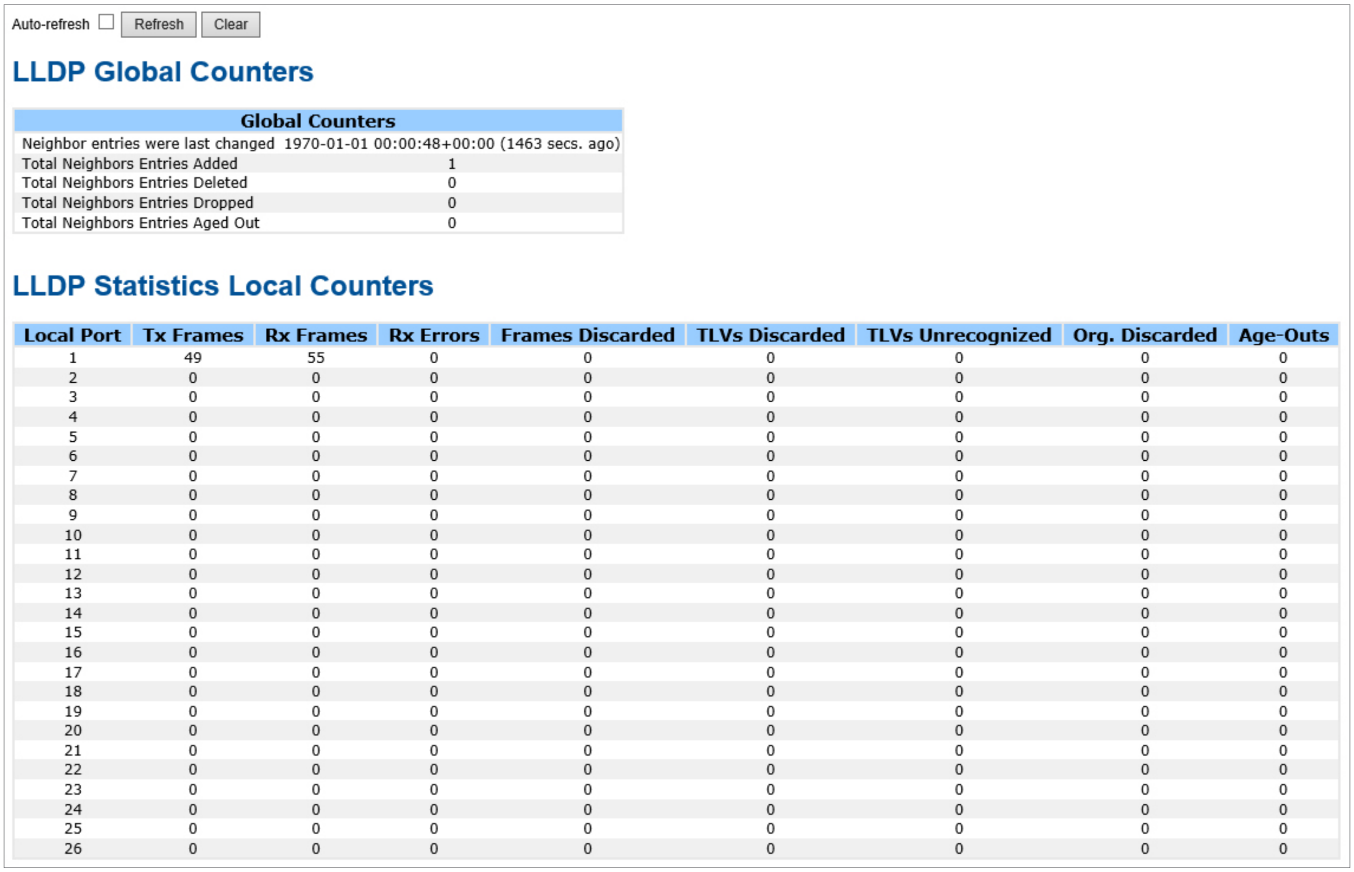
LLDP Neighbor Information

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 Capabilities	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
Management Address	Management Address is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address.
Refresh	Click to refresh the page immediately.
Auto-Refresh	Check this box to enable an automatic refresh of the page at regular intervals.

LLDP Neighbor Information

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.



LLDP Global Counters

Global Counters	
Neighbor entries were last changed	1970-01-01 00:00:48+00:00 (1463 secs. ago)
Total Neighbors Entries Added	1
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	49	55	0	0	0	0	0	0
2	0	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

Port Statistics

Global Counters

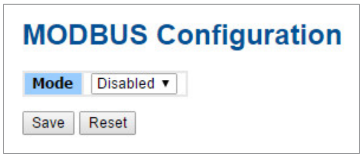
Label	Description
Neighbor entries were last changed at	Shows the time for when the last entry was last deleted or added. It is also shows the time elapsed since last change was detected.
Total Neighbors Entries Added	Shows the number of new entries added since switch reboot.
Total Neighbors Entries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

Local Counters

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

Modbus TCP

This page shows Modbus TCP support of the switch. (For more information regarding Modbus, please visit http://www.modbus.org/)

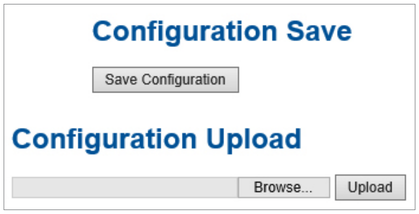


MODBUS Configuration

Mode: Disabled ▾

Label	Description
Mode	Shows the existing status of the Modbus TCP function

Backup/Restore Configuration



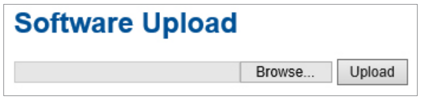
Configuration Save

Configuration Upload

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

Firmware Update

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

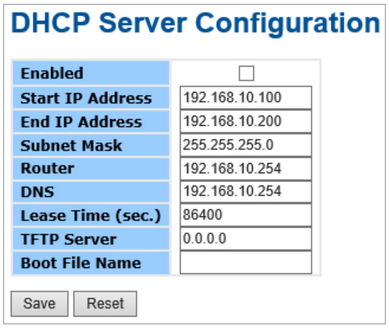


Software Upload

DHCP Server

Setting

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

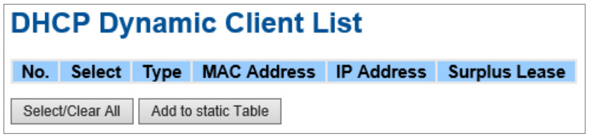


DHCP Server Configuration

Enabled	□
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.

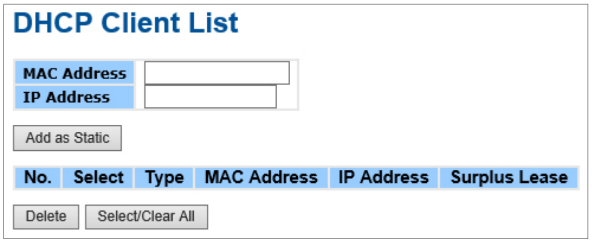


DHCP Dynamic Client List

No.	Select	Type	MAC Address	IP Address	Surplus Lease

DHCP Client List

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



DHCP Client List

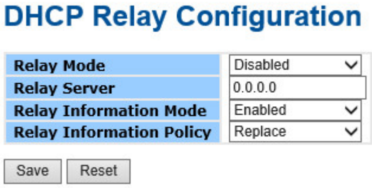
MAC Address	
IP Address	

No.	Select	Type	MAC Address	IP Address	Surplus Lease

DHCP Relay Agent

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

Relay



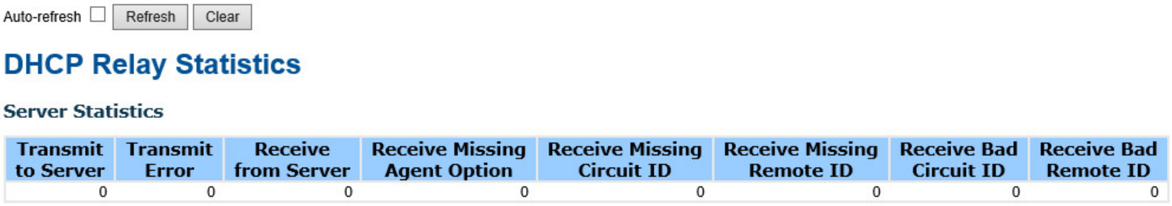
DHCP Relay Configuration

Relay Mode	Disabled
Relay Server	0.0.0.0
Relay Information Mode	Enabled
Relay Information Policy	Replace

Label	Description
Relay Mode	Indicates the DHCP relay mode operation. Possible modes are: Enabled: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations. Disabled: Disable DHCP relay mode operation.
Relay Server	Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain.

Label	Description
Relay Information Mode	Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID).), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address. Possible modes are: Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled. Disabled: Disable DHCP relay information mode operation.
Relay Information Policy	Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' option is invalid when relay information mode is disabled. Possible policies are: Replace: Replace the original relay information when a DHCP message that already contains it is received. Keep: Keep the original relay information when a DHCP message that already contains it is received. Drop: Drop the package when a DHCP message that already contains relay information is received.

Relay Statistics

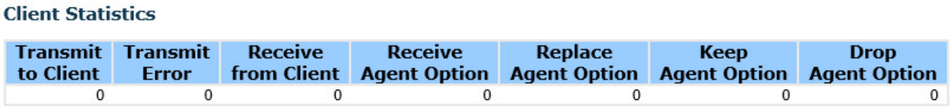


DHCP Relay Statistics

Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

Label	Description
Transmit to Server	The number of packets that are relayed from client to server.
Transmit Error	The number of packets that resulted in errors while being sent to clients.
Receive from Server	The number of packets received from server.
Receive Missing Agent Option	The number of packets received without agent information options.
Receive Missing Cirucit ID	The number of packets received with the Circuit ID option missing.
Receive Missing Remote ID	The number of packets received with the Remote ID option missing.
Receive Bad Circuit ID	The number of packets whose Circuit ID option did not match known circuit ID.
Receive Bad Remote ID	The number of packets whose Remote ID option did not match known Remote ID.



Client Statistics

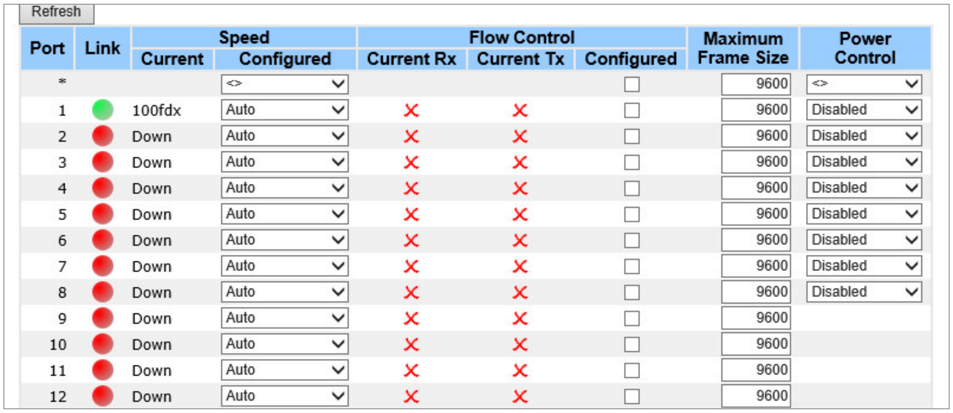
Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

Label	Description
Transmit to Client	The number of relayed packets from server to client.
Transmit Error	The number of packets that resulted in error while being sent to servers.
Receive from Client	The number of received packets from server.
Receive Agent Option	The number of received packets with relay agent information option.
Replace Agent Option	The number of packets which were replaced with relay agent information option.
Keep Agent Option	The number of packets whose relay agent information was retained.
Drop Agent Option	The number of packets that were dropped which were received with relay agent information.

Port Setting

Port Control

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



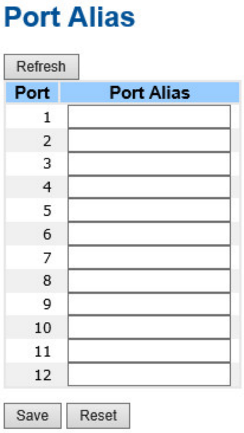
Port	Link	Speed		Flow Control			Maximum Frame Size	Power Control
		Current	Configured	Current Rx	Current Tx	Configured		
*			<>			□	9600	<>
1	🟢	100fdx	Auto	✗	✗	□	9600	Disabled
2	🔴	Down	Auto	✗	✗	□	9600	Disabled
3	🔴	Down	Auto	✗	✗	□	9600	Disabled
4	🔴	Down	Auto	✗	✗	□	9600	Disabled
5	🔴	Down	Auto	✗	✗	□	9600	Disabled
6	🔴	Down	Auto	✗	✗	□	9600	Disabled
7	🔴	Down	Auto	✗	✗	□	9600	Disabled
8	🔴	Down	Auto	✗	✗	□	9600	Disabled
9	🔴	Down	Auto	✗	✗	□	9600	
10	🔴	Down	Auto	✗	✗	□	9600	
11	🔴	Down	Auto	✗	✗	□	9600	
12	🔴	Down	Auto	✗	✗	□	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	Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are: Disabled - Disables the switch port operation. Auto - Cu port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner. **10Mbps HDX** - Force the Cu port to 10Mbps half duplex mode. **10Mbps FDX** - Force the Cu port to 10Mbps full duplex mode. **100Mbps HDX** - Force the Cu port to 100Mbps half duplex mode. **100Mbps FDX** - Force the Cu port to 100Mbps full duplex mode. **1Gbps FDX** - Force the Cu port to 1Gbps full duplex mode.
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.

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

Port Alias

Configure the port alias name for each port.

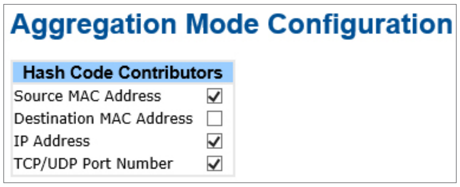


Port	Port Alias
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	

Label	Description
Port	This is the logical port number for this row.
Port Alias	Enter the port name you wish to use for this port.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Port Trunk

Trunk Configuration

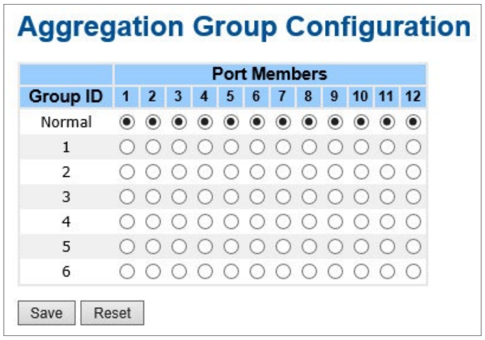


Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	☑
Destination MAC Address	□
IP Address	☑
TCP/UDP Port Number	☑

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

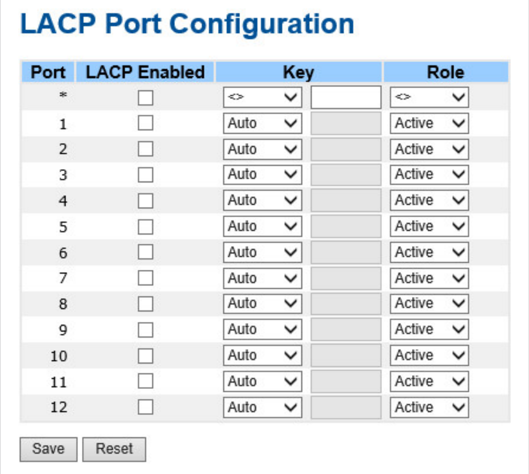
	Port Members											
Group ID	1	2	3	4	5	6	7	8	9	10	11	12
Normal	●	●	●	●	●	●	●	●	●	●	●	●
1	○	○	○	○	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○	○	○	○	○
5	○	○	○	○	○	○	○	○	○	○	○	○
6	○	○	○	○	○	○	○	○	○	○	○	○

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

LACP

Port Configuration

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



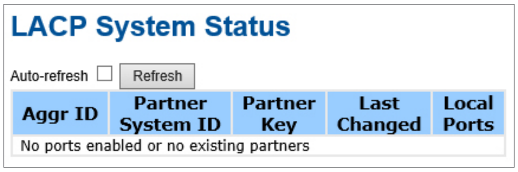
LACP Port Configuration

Port	LACP Enabled	Key		Role
*	□	<>		<>
1	□	Auto		Active
2	□	Auto		Active
3	□	Auto		Active
4	□	Auto		Active
5	□	Auto		Active
6	□	Auto		Active
7	□	Auto		Active
8	□	Auto		Active
9	□	Auto		Active
10	□	Auto		Active
11	□	Auto		Active
12	□	Auto		Active

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 (speak if spoken to).
Save	Click to 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.

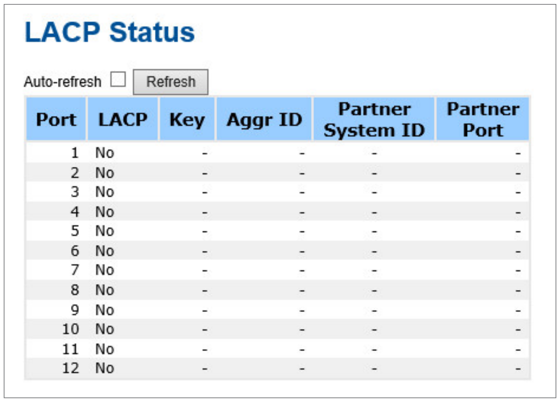


Aggr ID	Partner System ID	Partner Key	Last Changed	Local Ports
No ports enabled or no existing partners				

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.
Local Ports	Shows which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID:Port".
Refresh	Click to refresh the page immediately.
Auto-Refresh	Check this box to enable an automatic refresh of the page at regular intervals.

LACP Status

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



LACP Status

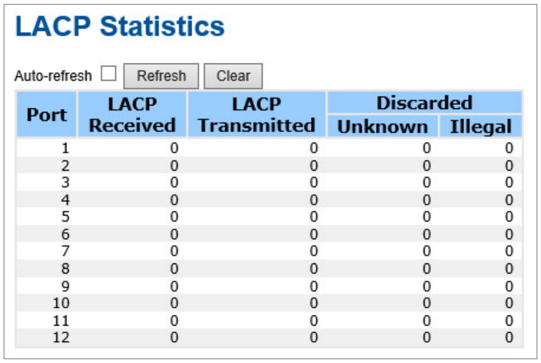
Auto-refresh □ Refresh

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

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

LACP Statistics

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



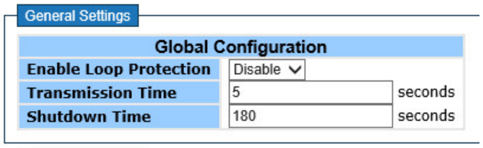
LACP Statistics

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

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

Loop Protection

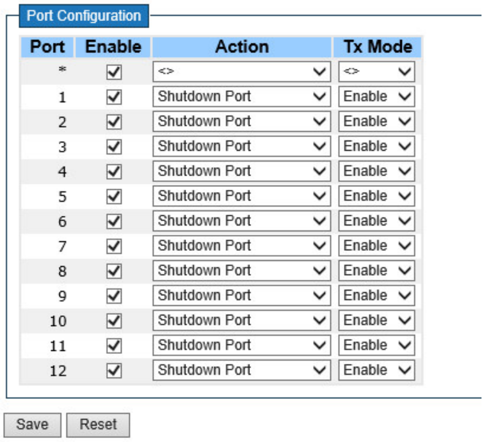
This feature prevents the loop attack. When the port receives loop packet. This port will auto disable, prevent the "loop attack" affect other network devices.



General Settings

Global Configuration		
Enable Loop Protection	Disable	
Transmission Time	5	seconds
Shutdown Time	180	seconds

Label	Description
Enable Loop Protection	Controls whether loop protections is enabled (as a whole).
Transmission Time	The interval between each loop protection PDU sent on each port. valid values are 1 to 10 seconds.
Shutdown Time	The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).

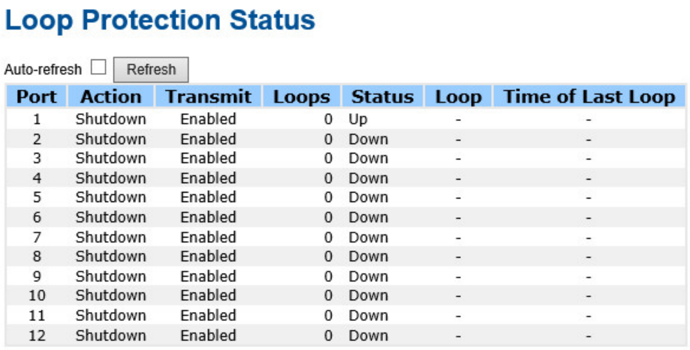


Port Configuration

Port	Enable	Action	Tx Mode
*	☑	<>	<>
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port	Enable
3	☑	Shutdown Port	Enable
4	☑	Shutdown Port	Enable
5	☑	Shutdown Port	Enable
6	☑	Shutdown Port	Enable
7	☑	Shutdown Port	Enable
8	☑	Shutdown Port	Enable
9	☑	Shutdown Port	Enable
10	☑	Shutdown Port	Enable
11	☑	Shutdown Port	Enable
12	☑	Shutdown Port	Enable

Label	Description
Port	The switch port number of the port.
Enable	Controls whether loop protection is enabled on this switch port.
Action	Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log 43 or Log Only.
Tx Mode	Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Loop Protection Status Help



Loop Protection Status

Auto-refresh □ Refresh

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Up	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Down	-	-
10	Shutdown	Enabled	0	Down	-	-
11	Shutdown	Enabled	0	Down	-	-
12	Shutdown	Enabled	0	Down	-	-

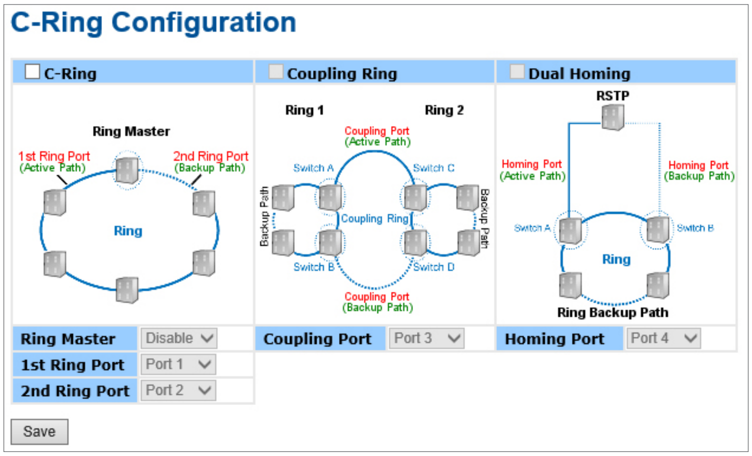
This page displays the loop protection port status the ports of the switch.
Loop protection port status is:

Label	Description
Port	The switch port number of the logical port.
Action	The currently configured port action.
Transmit	The currently configured port transmit mode.
Loops	The number of loops detected on this port.
Status	The current loop protection status of the port.
Loop	Whether a loop is currently detected on the port.
Time of Last Loop	The time of the last loop event detected.
Buttons	Refresh : Click to refresh the page immediately. Auto-refresh : Check this box to enable an automatic refresh of the page at regular intervals.

Redundancy

C-Ring

C-Ring is one of the most powerful Ring technologies 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 different Ring topologies: Ring, Coupling Ring and Dual Homing.



C-Ring Configuration

□ C-Ring		□ Coupling Ring		□ Dual Homing	
Ring Master	Disable	Coupling Port	Port 3	Homing Port	Port 4
1st Ring Port	Port 1				
2nd Ring Port	Port 2				

Ring Master
1st Ring Port (Active Path)
2nd Ring Port (Backup Path)
Ring
Ring 1
Ring 2
Coupling Port (Active Path)
Switch A
Switch C
Switch B
Switch D
Coupling Ring
Backup Path
Backup Path
Coupling Port (Backup Path)
RSTP
Homing Port (Active Path)
Homing Port (Backup Path)
Switch A
Switch B
Ring
Ring Backup Path
Save

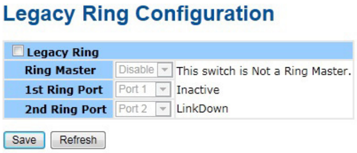
C-Ring interface

The following table describes the labels in this screen.

Label	Description
C-Ring	Mark to enable Ring.
Ring Master	There should be one and only one Ring Master in a ring. However if there are two or more switches which set Ring Master to enable, the switch with the lowest MAC address will be the actual Ring Master and others will be Backup Masters.
1st Ring Port	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 needs four switches to build an active and a backup link. Set a port as coupling port. The coupled four ports of four switches will be run in active/backup mode.
Dual Homing	Mark to enable Dual Homing. By selecting Dual Homing mode, Ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work as active/backup mode, and connect each Ring to the normal switches in RSTP mode.
Apply	Click “Apply” to set the configurations.

Note: It is not recommended to set one switch as a Ring Master and a Coupling Ring at the same time due to heavy load.

Legacy Ring



Legacy Ring Configuration

☐ Legacy Ring		
Ring Master	Disable	This switch is Not a Ring Master.
1st Ring Port	Port 1	Inactive
2nd Ring Port	Port 2	LinkDown

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

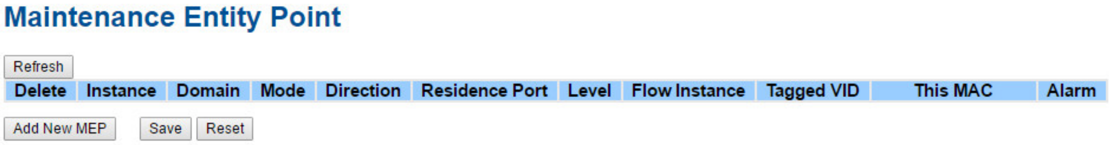
X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same. In the X-Ring topology, every switch should be enabled with X-Ring or Legacy Ring function and two ports should be assigned as the member ports 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.

G.8032 - MEP

The Maintenance Entity Point instances are configured here.



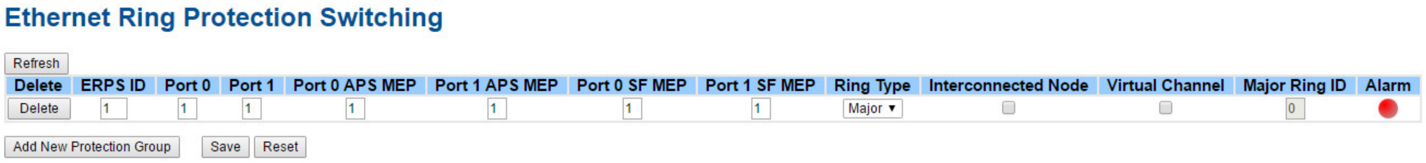
Maintenance Entity Point

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm

Label	Description
Delete	This box is used to mark a MEP for deletion in next Save operation.
Instance	The ID of the MEP. Click on the ID of a MEP to enter the configuration page.
Domain	Port: This is a MEP in the Port Domain. 'Flow Instance' is a Port. Esp: Future use Evc: This is a MEP in the EVC Domain. 'Flow Instance' is a EVC Mpls: Future use
Mode	MEP: This is a Maintenance Entity End Point. MIP: This is a Maintenance Entity Intermediate Point.
Direction	Ingress: This is a Ingress (down) MEP - monitoring ingress traffic on 'Residence Port'. Egress: This is a Egress (up) MEP - monitoring egress traffic on 'Residence Port'.
Residence Port	The port where MEP is monitoring - see 'Direction'.
Level	The MEG level of this MEP.
Flow Instance	The MEP is related to this flow - See 'Domain'.
Tagged VID	Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.
This MAC	The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).
Alarm	There is an active alarm on the MEP.
Buttons	Add New MEP: Click to add a new MEP entry Refresh: Click to refresh the page immediately Save: Click to save changes Reset: Click to undo any changes made locally and revert to previously saved values.

G.8032 - ERPS

The Ethernet Ring Protection Switch instances are configured here.



Ethernet Ring Protection Switching

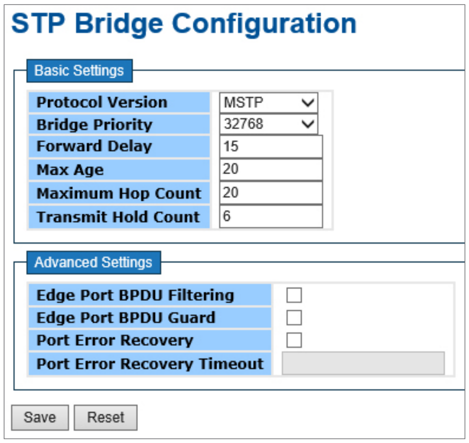
Delete	ERPS ID	Port 0	Port 1	Port 0 APS MEP	Port 1 APS MEP	Port 0 SF MEP	Port 1 SF MEP	Ring Type	Interconnected Node	Virtual Channel	Major Ring ID	Alarm
Delete	1	1	1	1	1	1	1	Major ▾	□	□	0	●

Label	Description
Delete	This box is used to mark an ERPS for deletion in next Save operation.
Protection group ID	The ID of the created Protection group. Click on the ID of an Protection group to enter the configuration page.
Port 0	This will create a Port 0 of the switch in the ring.
Port 1	This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance
Port 0 SF MEP	The Port 0 Signal Fail reporting MEP.
Port 1 SF MEP	The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.
Port 0 APS MEP	The Port 0 APS PDU handling MEP.
Port 1 APS MEP	The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.
Ring Type	Type of Protecting ring. It can be either major ring or sub-ring.
Interconnected Node	Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.
Virtual Channel	Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel.
Major Ring ID	Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.
Alarm	There is an active alarm on the ERPS.
Buttons	Add New Protection Group: Click to add a new Protection group entry Refresh: Click to refresh the page immediately Save: Click to save changes Reset: Click to undo any changes made locally and revert to previously saved values.

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.



STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Bridge Priority	32768
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

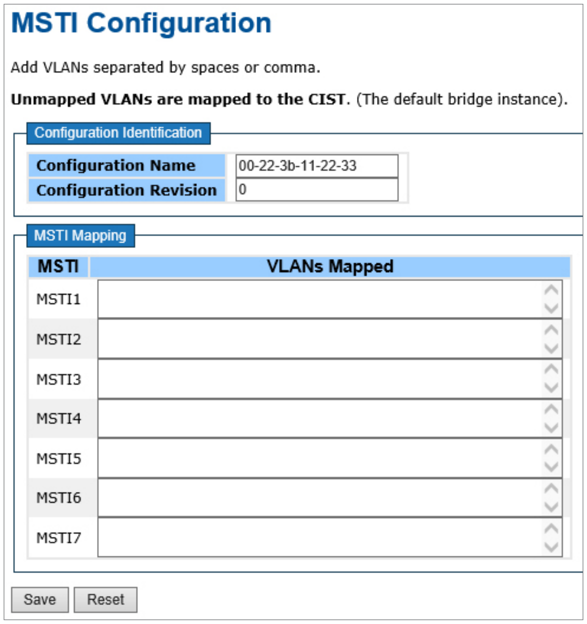
Advanced Settings

Edge Port BPDU Filtering	□
Edge Port BPDU Guard	□
Port Error Recovery	□
Port Error Recovery Timeout	

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 <= (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 <= (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	Click to 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.



MSTI Configuration

Add VLANs separated by spaces or comma.

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

Configuration Identification

Configuration Name	00-22-3b-11-22-33
Configuration Revision	0

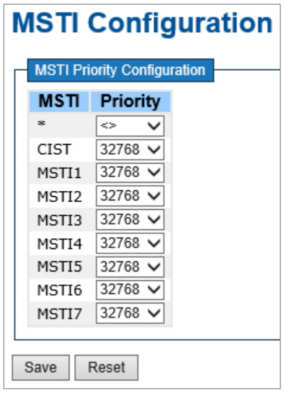
MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

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	Click to 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

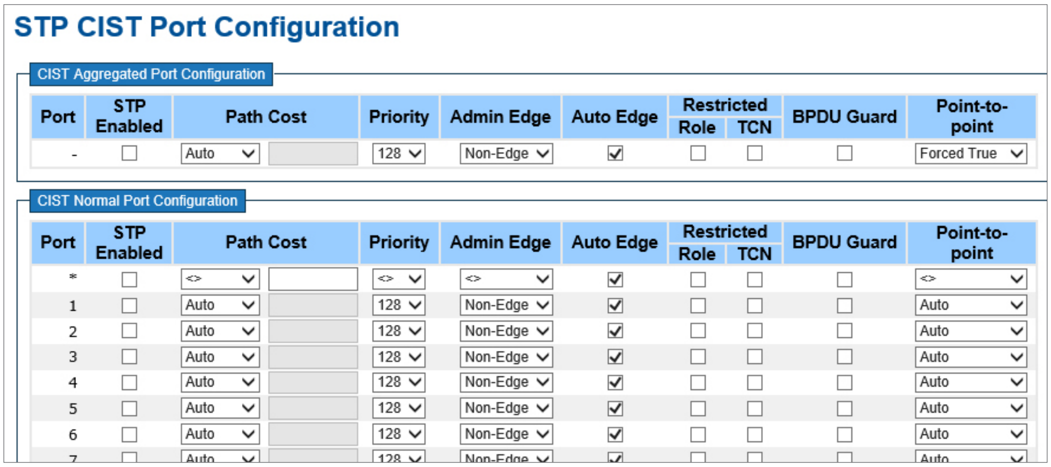
MSTI Priority Configuration

MSTI	Priority
*	<>
CIST	32768
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

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	Click to 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 well. This page contains settings for physical and aggregated ports. The aggregation settings are stack global.



STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
-	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
*	☐	<>		<>	<>	☑	☐	☐	☐	<>
1	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
2	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
3	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
4	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
5	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
6	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
7	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto

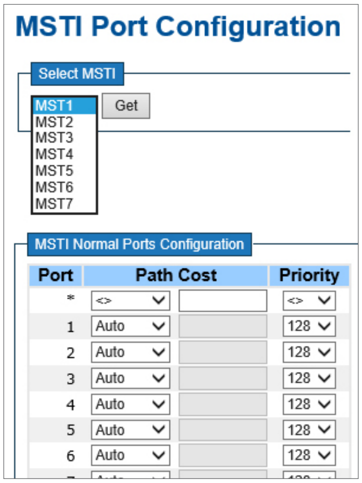
Label	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended 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 openEdge true) than for other ports.
AdminEdge	Controls whether the openEdge flag should start as being set or cleared. (The initial openEdge state when a port is initialized).
AutoEdge	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows openEdge 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.

Label	Description
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	Click to 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 well. A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

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



Port	Path Cost		Priority
*	<>		<>
1	Auto		128
2	Auto		128
3	Auto		128
4	Auto		128
5	Auto		128
6	Auto		128

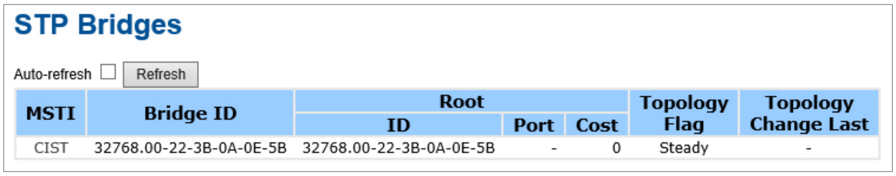
Label	Description
Port	The switch port number of the corresponding STP CIST (and MSTI) port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined 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	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

STP

STP Bridges

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

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



STP Bridges

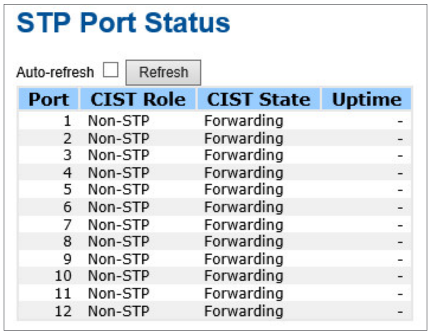
Auto-refresh □ Refresh

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-22-3B-0A-0E-5B	32768.00-22-3B-0A-0E-5B	-	0	Steady	-

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.



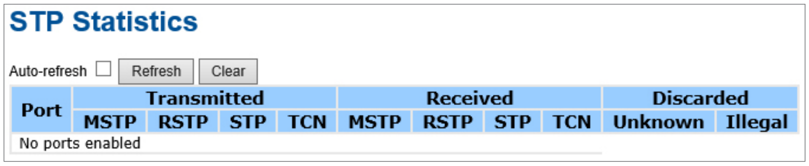
STP Port Status

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	-

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	Click to refresh the page immediately.
Auto-Refresh	Check this box to enable an automatic refresh of the page at regular intervals.

STP Statistics

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



STP Statistics

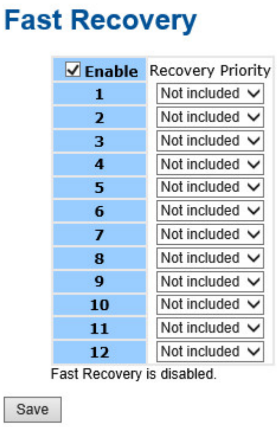
Auto-refresh □ Refresh Clear

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
No ports enabled										

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	Click to refresh the page immediately.
Auto-Refresh	Check this box to enable an automatic refresh of the page at regular intervals.

Fast Recovery mode

The Fast Recovery Mode can be set to connect multiple ports to one or more switches. The CNGE12FX4TX8MS[POE]/TS with its fast recovery mode will provide redundant links. Fast Recovery mode supports 12 priorities, only the first priority will be the active port, the other ports configured with other priorities will be the backup ports.



Fast Recovery

☑ Enable	Recovery Priority
1	Not included
2	Not included
3	Not included
4	Not included
5	Not included
6	Not included
7	Not included
8	Not included
9	Not included
10	Not included
11	Not included
12	Not included

Fast Recovery is disabled.

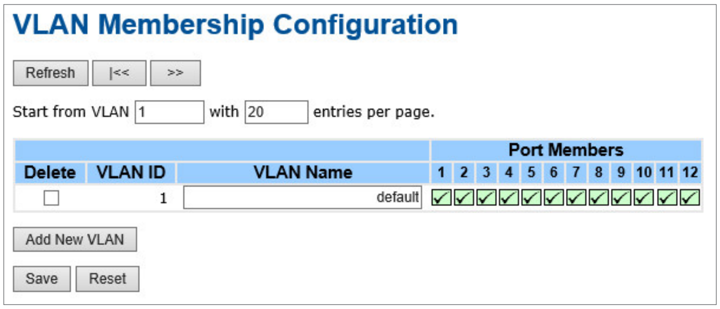
Fast Recovery Mode interface

Label	Description
Active	Activate the fast recovery mode.
port	Port can be configured as 12 priorities. Only the port with highest priority will be the active port. 1st Priority is the highest.
Apply	Click **Apply** to activate the configurations.

VLAN

VLAN Membership Configuration

The VLAN membership configuration for the selected stack switch unit switch can be monitored and modified here. Up to 256 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.



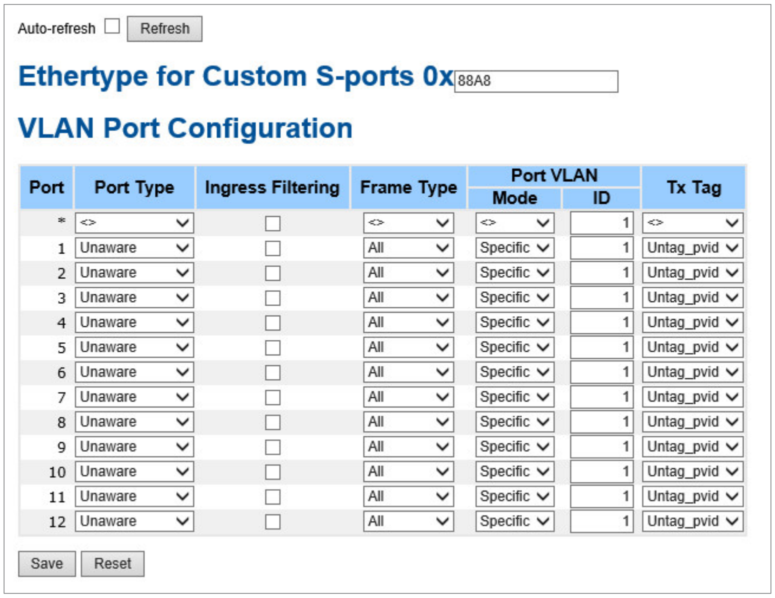
VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page.

			Port Members											
Delete	VLAN ID	VLAN Name	1	2	3	4	5	6	7	8	9	10	11	12
□	1	default	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

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	Check marks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Adding a New Static Entry	Click **Add New VLAN** to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The VLAN is enabled on the selected stack switch unit when you 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 **Delete** button can be used to undo the addition of new VLANs.

VLAN Port Configuration



Auto-refresh □ Refresh

Ethertype for Custom S-ports 0x 88A8

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN		Tx Tag
				Mode	ID	
*	<>	□	<>	<>	1	<>
1	Unaware	□	All	Specific	1	Untag_pvid
2	Unaware	□	All	Specific	1	Untag_pvid
3	Unaware	□	All	Specific	1	Untag_pvid
4	Unaware	□	All	Specific	1	Untag_pvid
5	Unaware	□	All	Specific	1	Untag_pvid
6	Unaware	□	All	Specific	1	Untag_pvid
7	Unaware	□	All	Specific	1	Untag_pvid
8	Unaware	□	All	Specific	1	Untag_pvid
9	Unaware	□	All	Specific	1	Untag_pvid
10	Unaware	□	All	Specific	1	Untag_pvid
11	Unaware	□	All	Specific	1	Untag_pvid
12	Unaware	□	All	Specific	1	Untag_pvid

Save Reset

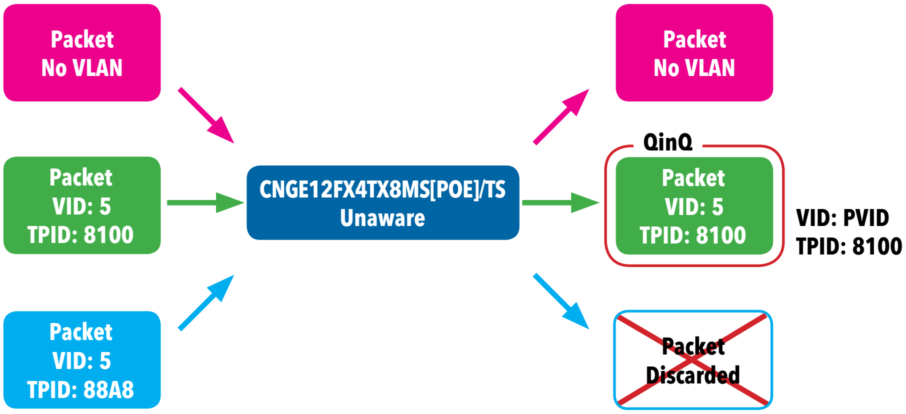
Label	Description
Ethertype for customer S-Ports	This field specifies the ether type used for Custom S-ports. This is a global setting for all the Custom S-ports.
Port	This is the logical port number of this row.
Port type	Port can be one of the following types: Unaware, Customer port (C-port), Service port (S-port), Custom Service port (S-custom-port) If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed.
Ingress Filtering	Enable ingress filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no check mark).
Frame Type	Determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to All.
Port VLAN Mode	Configures the Port VLAN Mode. The allowed values are None or Specific. This parameter affects VLAN ingress and egress processing. If None is selected, a VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN aware switches. Tx tag should be set to Untag_pvid when this mode is used. If Specific (the default value) is selected, a Port VLAN ID can be configured (see below). Untagged frames received on the port are classified to the Port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.

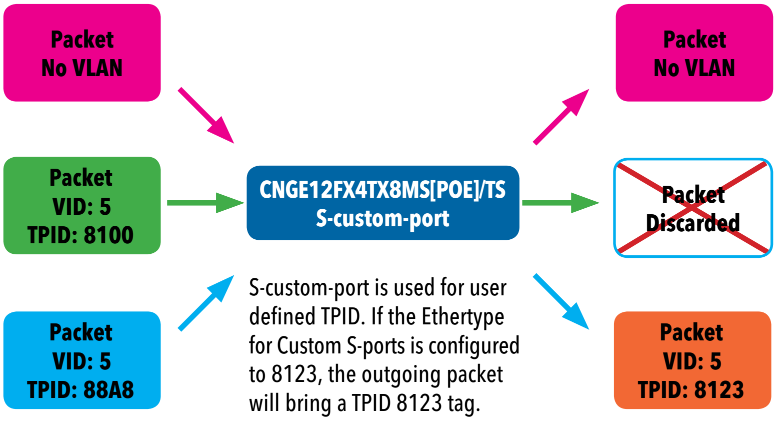
Label	Description
Port VLAN ID	Configures the VLAN identifier for the port. The allowed values are from 1 through 4095. The default value is 1. ***Note: The port must be a member of the same VLAN as the Port VLAN ID.***
Tx Tag	Determines egress tagging of a port. Untag_pvid – All VLANs except the configured PVID will be tagged. Tag_all – All VLANs are tagged. Untag_all – All VLANs are untagged.

How to use Unaware / C-Port / S-Port / S-Custom-Port

Port can be one of the following types: Unaware, C-port, S-port, and S-custom-port.

	Ingress action	**Egress action**
Unaware The function of Unaware can be used for 802.1QinQ (double tag).	When the port received untagged frames, an untagged frame obtain a tag (based on PVID) and is forwarded. When the port received tagged frames, 1. If the tagged frame with TPID=0x8100, it become a double-tag frame, and is forwarded. 2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of frame transmitted by Unaware port will be set to 0x8100. The final status of the frame after egressing are also effected by Egress Rule.
C-port	When the port received untagged frames, an untagged frame obtain a tag (based on PVID) and is forwarded. When the port received tagged frames, 1. If a tagged frame with TPID=0x8100, it is forwarded. 2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of frame transmitted by C-port will be set to 0x8100.
S-port	When the port received untagged frames, an untagged frame obtain a tag (based on PVID) and is forwarded. When the port received tagged frames, 1. If a tagged frame with TPID=0x88A8, it is forwarded. 2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8100), it will be discarded.	The TPID of frame transmitted by S-port will be set to 0x88A8.
S-custom-port	When the port received untagged frames, an untagged frame obtain a tag (based on PVID) and is forwarded. When the port received tagged frames, 1. If a tagged frame with TPID=0x88A8, it is forwarded. 2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8100), it will be discarded.	The TPID of frame transmitted by S-custom-port will be set to an self-customized value, which can be set by the user using the column of Ethertype for Custom S-ports.

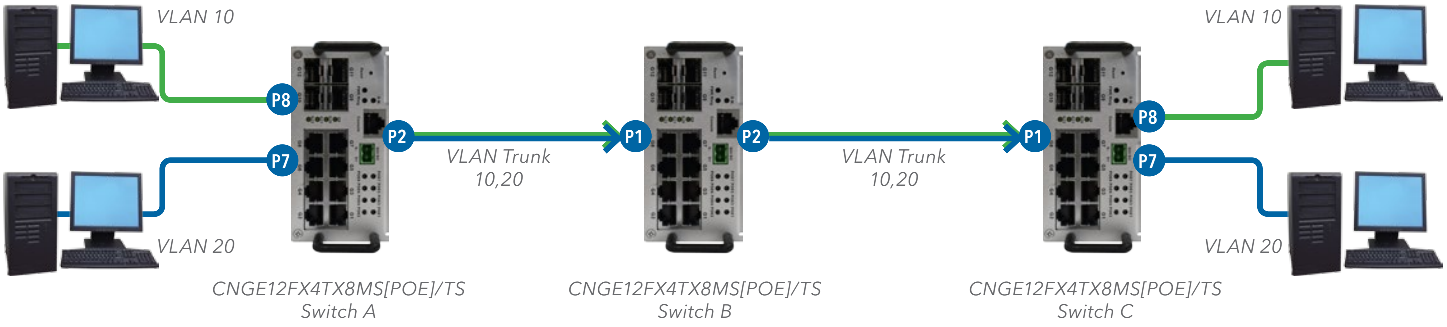




S-custom-port is used for user defined TPID. If the Ethertype for Custom S-ports is configured to 8123, the outgoing packet will bring a TPID 8123 tag.

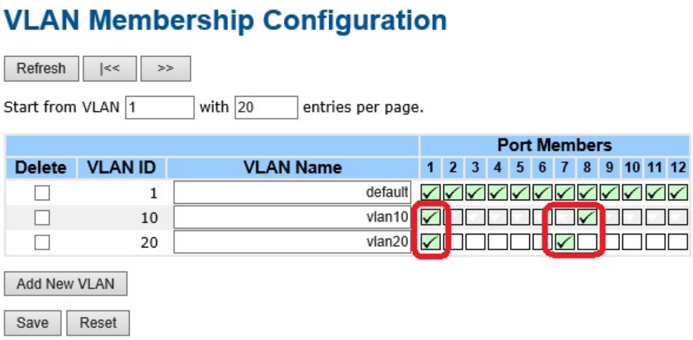
VLAN Setting Example

VLAN Access Mode Setting



In the topology above, for Switch A,
Port 7 is VLAN Access mode = Untagged 20
Port 8 is VLAN Access mode = Untagged 10

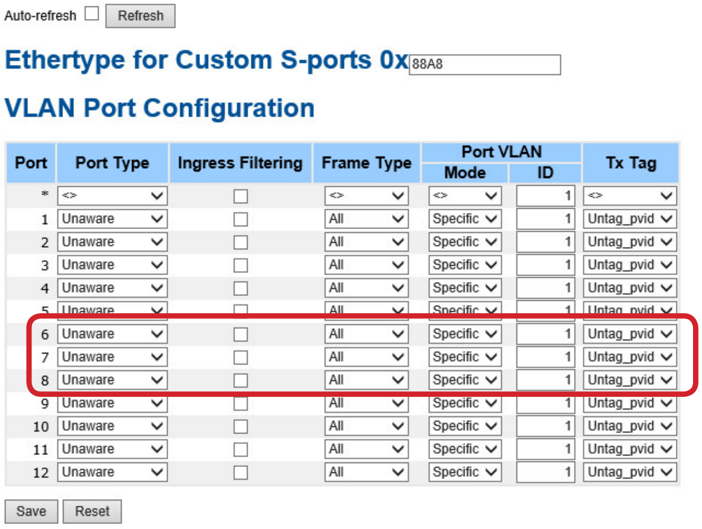
Configure the VLAN for Switch A as shown



VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page.

			Port Members											
Delete	VLAN ID	VLAN Name	1	2	3	4	5	6	7	8	9	10	11	12
□	1	default	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
□	10	vlan10	☑	□	□	□	□	□	□	☑	□	□	□	□
□	20	vlan20	☑	□	□	□	□	□	☑	□	□	□	□	□



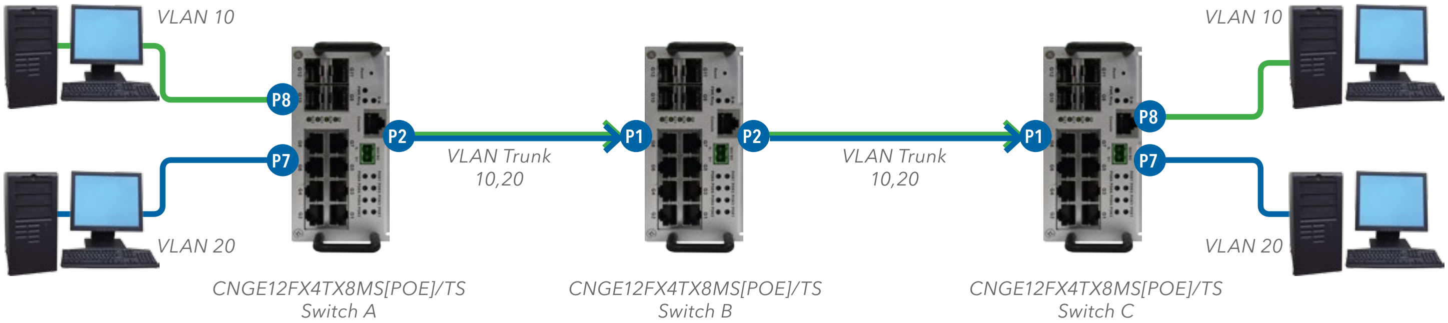
Auto-refresh □

Ethertype for Custom S-ports 0x 88A8

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN		Tx Tag
				Mode	ID	
*	<>	□	<>	<>	1	<>
1	Unaware	□	All	Specific	1	Untag_pvid
2	Unaware	□	All	Specific	1	Untag_pvid
3	Unaware	□	All	Specific	1	Untag_pvid
4	Unaware	□	All	Specific	1	Untag_pvid
5	Unaware	□	All	Specific	1	Untag_pvid
6	Unaware	□	All	Specific	1	Untag_pvid
7	Unaware	□	All	Specific	1	Untag_pvid
8	Unaware	□	All	Specific	1	Untag_pvid
9	Unaware	□	All	Specific	1	Untag_pvid
10	Unaware	□	All	Specific	1	Untag_pvid
11	Unaware	□	All	Specific	1	Untag_pvid
12	Unaware	□	All	Specific	1	Untag_pvid

VLAN 1Q Trunk mode

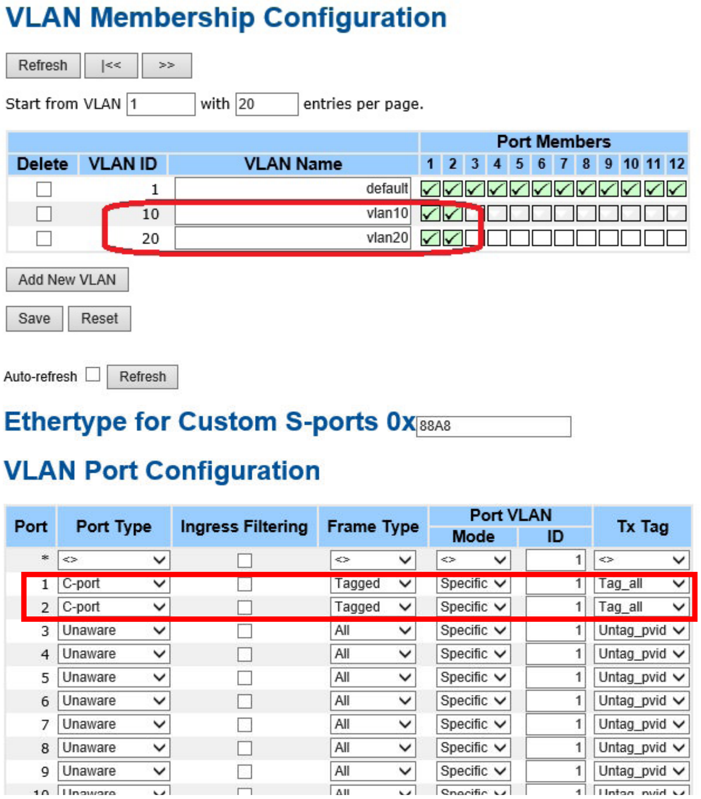

VLAN 10
VLAN 20
P8
P7
P2
VLAN Trunk 10,20
P1
P2
VLAN Trunk 10,20
P1
P8
P7
VLAN 10
VLAN 20
CNGE12FX4TX8MS[POE]/TS Switch A
CNGE12FX4TX8MS[POE]/TS Switch B
CNGE12FX4TX8MS[POE]/TS Switch C

In the topology above, for Switch B,

Port 1 = VLAN 1Qtrunk mode = tagged 10,20

Port 2 = VLAN 1Qtrunk mode = tagged 10,20

Configure the VLAN for Switch B as shown



VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	VLAN Name	Port Members											
			1	2	3	4	5	6	7	8	9	10	11	12
☐	1	default	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
☐	10	vlan10	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐	20	vlan20	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Ethertype for Custom S-ports 0x 88A8

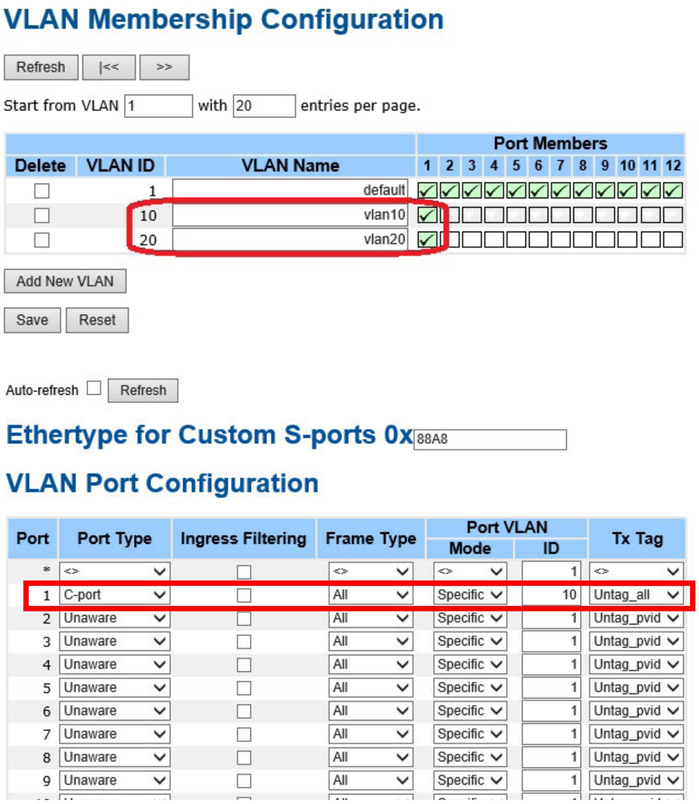
VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN		Tx Tag
				Mode	ID	
*	<>	☐	<>	<>	1	<>
1	C-port	☐	Tagged	Specific	1	Tag_all
2	C-port	☐	Tagged	Specific	1	Tag_all
3	Unaware	☐	All	Specific	1	Untag_pvid
4	Unaware	☐	All	Specific	1	Untag_pvid
5	Unaware	☐	All	Specific	1	Untag_pvid
6	Unaware	☐	All	Specific	1	Untag_pvid
7	Unaware	☐	All	Specific	1	Untag_pvid
8	Unaware	☐	All	Specific	1	Untag_pvid
9	Unaware	☐	All	Specific	1	Untag_pvid
10	Unaware	☐	All	Specific	1	Untag_pvid

VLAN Hybrid mode

To set Port 1 VLAN Hybrid mode = untagged 10
Tagged 10,20

Configure the VLAN for the Switch as shown



VLAN Membership Configuration

Refresh |<< >>

Start from VLAN 1 with 20 entries per page.

			Port Members											
Delete	VLAN ID	VLAN Name	1	2	3	4	5	6	7	8	9	10	11	12
□	1	default	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
□	10	vlan10	☑	□	□	□	□	□	□	□	□	□	□	□
□	20	vlan20	☑	□	□	□	□	□	□	□	□	□	□	□

Add New VLAN

Save Reset

Auto-refresh □ Refresh

Ethertype for Custom S-ports 0x 88A8

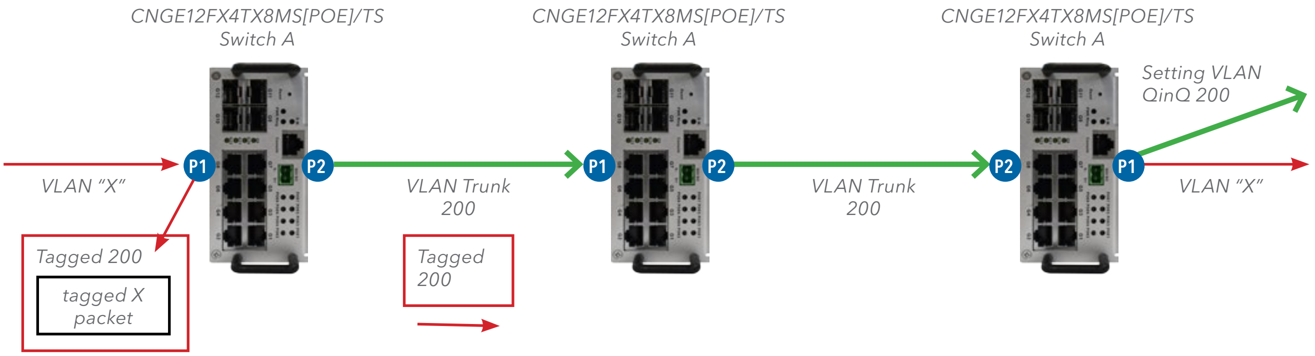
VLAN Port Configuration

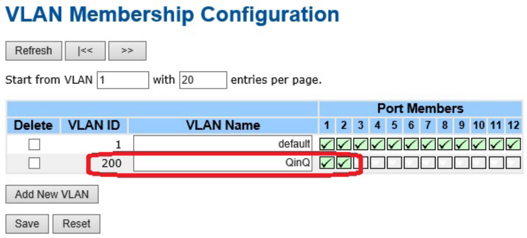
Port	Port Type	Ingress Filtering	Frame Type	Port VLAN		Tx Tag
				Mode	ID	
*	<>	□	<>	<>	1	<>
1	C-port	□	All	Specific	10	Untag_all
2	Unaware	□	All	Specific	1	Untag_pvid
3	Unaware	□	All	Specific	1	Untag_pvid
4	Unaware	□	All	Specific	1	Untag_pvid
5	Unaware	□	All	Specific	1	Untag_pvid
6	Unaware	□	All	Specific	1	Untag_pvid
7	Unaware	□	All	Specific	1	Untag_pvid
8	Unaware	□	All	Specific	1	Untag_pvid
9	Unaware	□	All	Specific	1	Untag_pvid

VLAN QinQ mode

Below is an example of the VLAN QinQ Mode, which is typically used in an environment with unknown VLAN.

VLAN "X" = Unknown VLAN

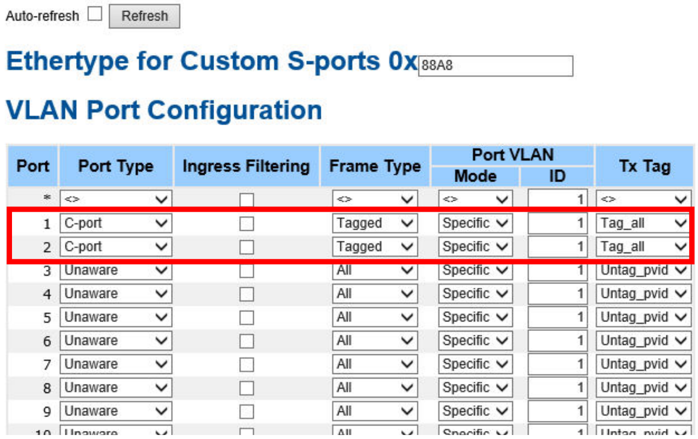




VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page.

			Port Members											
Delete	VLAN ID	VLAN Name	1	2	3	4	5	6	7	8	9	10	11	12
□	1	default	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
□	200	QinQ	☑	☑	□	□	□	□	□	□	□	□	□	□



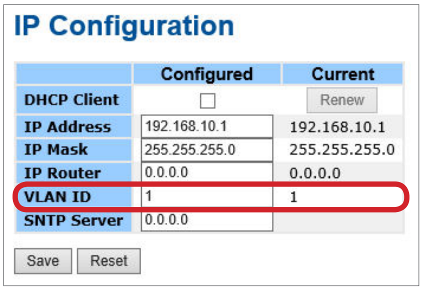
Ethertype for Custom S-ports 0x 88A8

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN		Tx Tag
				Mode	ID	
*	<>	□	<>	<>	1	<>
1	C-port	□	Tagged	Specific	1	Tag_all
2	C-port	□	Tagged	Specific	1	Tag_all
3	Unaware	□	All	Specific	1	Untag_pvid
4	Unaware	□	All	Specific	1	Untag_pvid
5	Unaware	□	All	Specific	1	Untag_pvid
6	Unaware	□	All	Specific	1	Untag_pvid
7	Unaware	□	All	Specific	1	Untag_pvid
8	Unaware	□	All	Specific	1	Untag_pvid
9	Unaware	□	All	Specific	1	Untag_pvid
10	Unaware	□	All	Specific	1	Untag_pvid

VLAN Management VLAN ID Setting

If Management VLAN is set, only the same VLAN ID port can control the switch.



IP Configuration

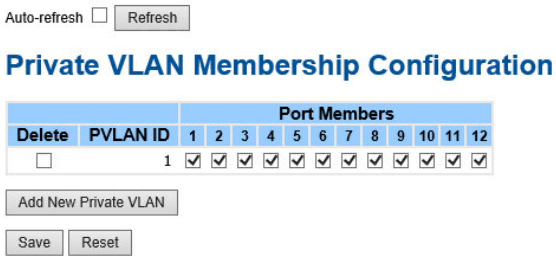
	Configured	Current
DHCP Client	□	Renew
IP Address	192.168.10.1	192.168.10.1
IP Mask	255.255.255.0	255.255.255.0
IP Router	0.0.0.0	0.0.0.0
VLAN ID	1	1
SNTP Server	0.0.0.0	

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.

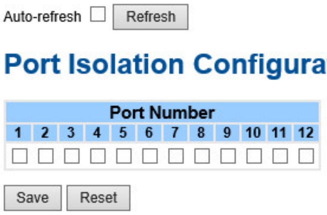
A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.



Private VLAN Membership Configuration

		Port Members											
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Private VLAN ID	Indicates the ID of this particular private VLAN.
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 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 **Delete** button can be used to undo the addition of new Private VLANs.



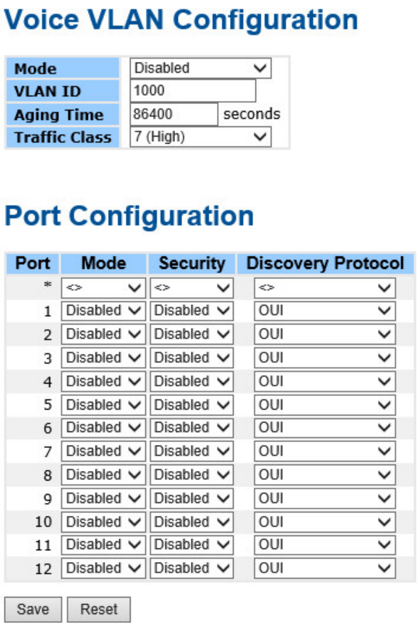
Port Isolation Configuration

Port Number											
1	2	3	4	5	6	7	8	9	10	11	12
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Label	Description
Port Number	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.

Voice VLAN - Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.



Voice VLAN Configuration

Mode	Disabled
VLAN ID	1000
Aging Time	86400 seconds
Traffic Class	7 (High)

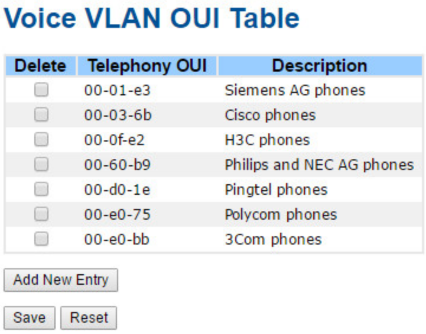
Port Configuration

Port	Mode	Security	Discovery Protocol
*	<>	<>	<>
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI
4	Disabled	Disabled	OUI
5	Disabled	Disabled	OUI
6	Disabled	Disabled	OUI
7	Disabled	Disabled	OUI
8	Disabled	Disabled	OUI
9	Disabled	Disabled	OUI
10	Disabled	Disabled	OUI
11	Disabled	Disabled	OUI
12	Disabled	Disabled	OUI

Label	Description
Mode	Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are: Enabled: Enable Voice VLAN mode operation. Disabled: Disable Voice VLAN mode operation.
VLAN ID	Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.
Aging Time	Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.
Traffic Class	Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.
Port Mode	Indicates the Voice VLAN port mode. When the port mode isn't equal disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible port modes are: Disabled: Disjoin from Voice VLAN. Auto: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically. Forced: Force join to Voice VLAN.
Port Security	Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are: Enabled: Enable Voice VLAN security mode operation. Disabled: Disable Voice VLAN security mode operation.
Port Discovery Protocol	Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are: OUI: Detect telephony device by OUI address. LLDP: Detect telephony device by LLDP. Both: Both OUI and LLDP.
Buttons	Save: Click to save changes Reset: Click to undo any changes made locally and revert to previously saved values.

Voice VLAN - OUI

Configure VOICE VLAN OUI table on this page. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of the OUI process.



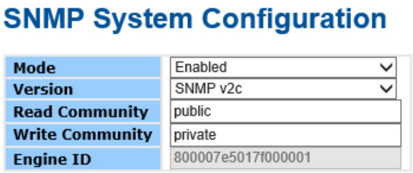
Voice VLAN OUI Table

Delete	Telephony OUI	Description
□	00-01-e3	Siemens AG phones
□	00-03-6b	Cisco phones
□	00-0f-e2	H3C phones
□	00-60-b9	Philips and NEC AG phones
□	00-d0-1e	Pingtel phones
□	00-e0-75	Polycom phones
□	00-e0-bb	3Com phones

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Telephony OUI	A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is “xx-xx-xx” (x is a hexadecimal digit).
Description	The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.
Buttons	Add New Entry: Click to add a new access management entry. Save: Click to save changes Reset: Click to undo any changes made locally and revert to previously saved values.

SNMP

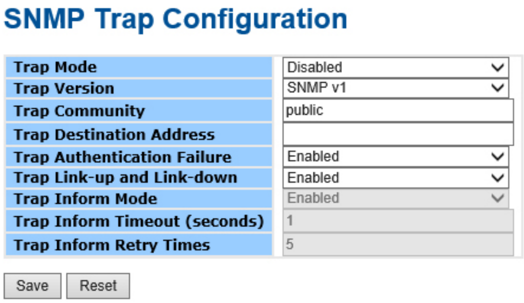
SNMP-System



SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

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

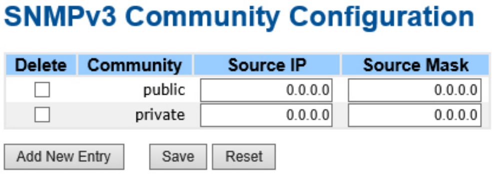
Trap Mode	Disabled
Trap Version	SNMP v1
Trap Community	public
Trap Destination Address	
Trap Authentication Failure	Enabled
Trap Link-up and Link-down	Enabled
Trap Inform Mode	Enabled
Trap Inform Timeout (seconds)	1
Trap Inform Retry Times	5

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.
Trap Probe Security Engine ID	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: Enabled: Enable SNMP trap probe security engine ID mode of operation. Disabled: Disable SNMP trap probe security engine ID mode of operation.

Label	Description
Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed.
Trap Security Name	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

SNMP-Communities

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



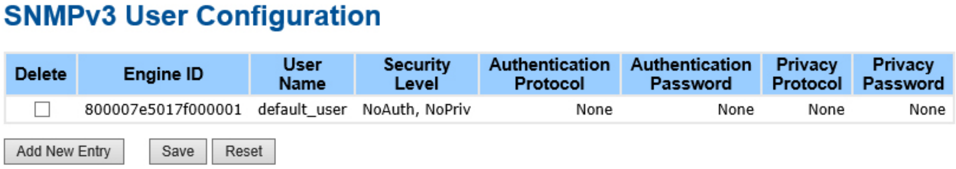
SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
□	public	0.0.0.0	0.0.0.0
□	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.



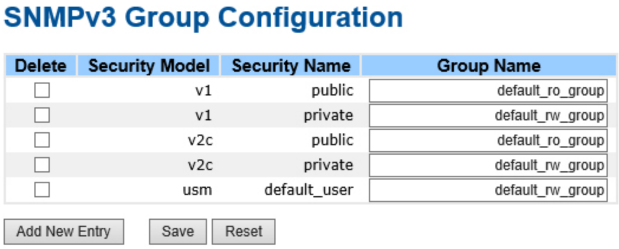
SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
□	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 a local user; otherwise it's a remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: None authentication and none privacy. Auth, NoPriv: Authentication and none privacy. Auth, Priv: Authentication and privacy. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: None: 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.



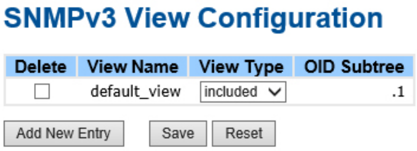
SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
□	v1	public	default_ro_group
□	v1	private	default_rw_group
□	v2c	public	default_ro_group
□	v2c	private	default_rw_group
□	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.



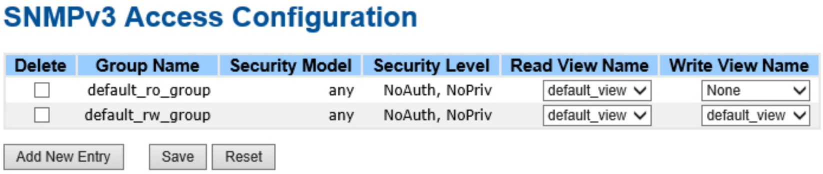
SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
□	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. Generally, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID subtree overstep the 'excluded' view entry.
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is 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 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	default_ro_group	any	NoAuth, NoPriv	default_view	None
□	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: None authentication and none privacy. Auth, NoPriv: Authentication and none privacy. Auth, Priv: Authentication and privacy.
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Write View Name	The name of the MIB view defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

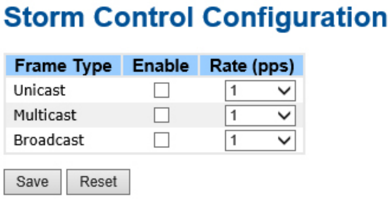
Traffic Prioritization

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.



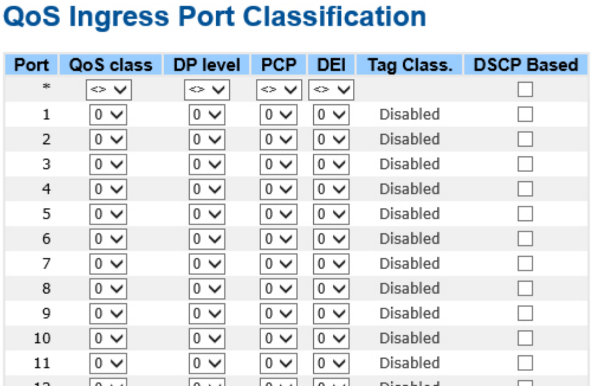
Storm Control Configuration

Frame Type	Enable	Rate (pps)
Unicast	□	1
Multicast	□	1
Broadcast	□	1

Label	Description
Frame Type	The settings in a particular row apply to the frame type listed here: unicast, multicast, or broadcast.
Enable	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 Classification

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.



QoS Ingress Port Classification

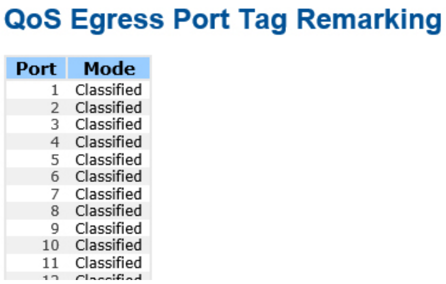
Port	QoS class	DP level	PCP	DEI	Tag Class.	DSCP Based
*	<>	<>	<>	<>		□
1	0	0	0	0	Disabled	□
2	0	0	0	0	Disabled	□
3	0	0	0	0	Disabled	□
4	0	0	0	0	Disabled	□
5	0	0	0	0	Disabled	□
6	0	0	0	0	Disabled	□
7	0	0	0	0	Disabled	□
8	0	0	0	0	Disabled	□
9	0	0	0	0	Disabled	□
10	0	0	0	0	Disabled	□
11	0	0	0	0	Disabled	□

Label	Description
Port	The port number for which the configuration below applies
QoS Class	Controls the default QoS class. All frames are classified to a QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority. If the port is VLAN aware and the frame is tagged, then the frame is classified to a QoS class that is based on the PCP value in the tag as shown below. Otherwise the frame is classified to the default QoS class. PCP value: 0 1 2 3 4 5 6 7 QoS class: 1 0 2 3 4 5 6 7 If the port is VLAN aware, the frame is tagged and Tag Class is enabled, then the frame is classified to a QoS class that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default QoS class. The classified QoS class can be overruled by a QCL entry. Note: If the default QoS class has been dynamically changed, then the actual default QoS class is shown in parentheses after the configured default QoS class.
DP level	Controls the default Drop Precedence Level. All frames are classified to a DP level. If the port is VLAN aware and the frame is tagged, then the frame is classified to a DP level that is equal to the DEI value in the tag. Otherwise the frame is classified to the default DP level. If the port is VLAN aware, the frame is tagged and Tag Class is enabled, then the frame is classified to a DP level that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DP level. The classified DP level can be overruled by a QCL entry.
PCP	Controls the default PCP value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.

Label	Description
DEI	Controls the default DEI value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.
Tag Class	Shows the classification mode for tagged frames on this port. Disabled: Use default QoS class and DP level for tagged frames. Enabled: Use mapped versions of PCP and DEI for tagged frames. Click on the mode in order to configure the mode and/or mapping. Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default QoS class and DP level.
DSCP Based	Click to Enable DSCP Based QoS Ingress Port Classification.

Port Tag Remarking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.



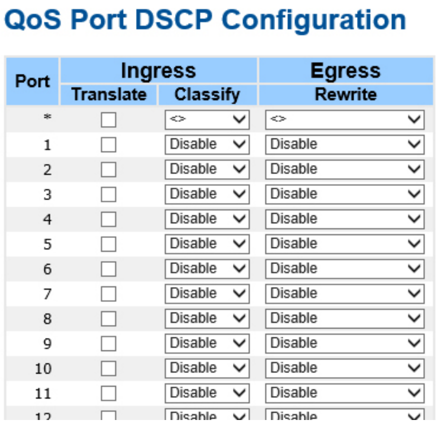
QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified

Label	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking
Mode	Shows the tag remarking mode for this port. Classified: Use classified PCP/DEI values. Default: Use default PCP/DEI values. Mapped: Use mapped versions of QoS class and DP level.

Port DSCP

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports.



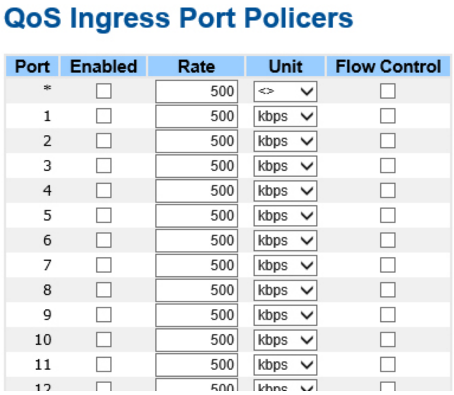
QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	□	<>	<>
1	□	Disable	Disable
2	□	Disable	Disable
3	□	Disable	Disable
4	□	Disable	Disable
5	□	Disable	Disable
6	□	Disable	Disable
7	□	Disable	Disable
8	□	Disable	Disable
9	□	Disable	Disable
10	□	Disable	Disable
11	□	Disable	Disable
12	□	Disable	Disable

Label	Description
Port	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
Ingress	In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: 1. Translate 2. Classify
1. Translate	To Enable the Ingress Translation click the checkbox.
2. Classify	Classification for a port have 4 different values. • Disable: No Ingress DSCP Classification. • DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0. • Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP. • All: Classify all DSCP.
Egress	Port Egress Rewriting can be one of – • Disable: No Egress rewrite. • Enable: Rewrite enabled without remapping. • Remap DP Unaware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table. • Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.

Port Policing

This page allows you to configure the Policer settings for all switch ports.



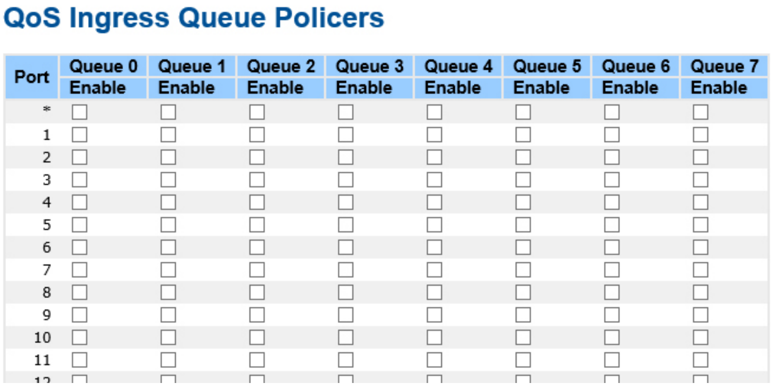
QoS Ingress Port Policers

Port	Enabled	Rate	Unit	Flow Control
*	□	500	<>	□
1	□	500	kbps	□
2	□	500	kbps	□
3	□	500	kbps	□
4	□	500	kbps	□
5	□	500	kbps	□
6	□	500	kbps	□
7	□	500	kbps	□
8	□	500	kbps	□
9	□	500	kbps	□
10	□	500	kbps	□
11	□	500	kbps	□
12	□	500	kbps	□

Label	Description
Port	The port number for which the configuration below applies
Enable	Controls whether the policer is enabled on this switch port.
Rate	Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the “Unit” is “kbps” or “fps”, and it is restricted to 1-3300 when the “Unit” is “Mbps” or “kfps”.
Unit	Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is “kbps”.
Flow Control	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Queue Policing

This page allows you to configure the Queue Policer settings for all switch ports.



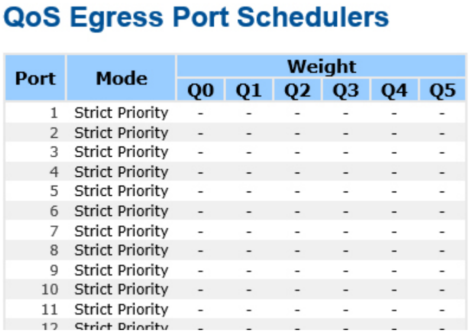
QoS Ingress Queue Policers

Port	Queue 0 Enable	Queue 1 Enable	Queue 2 Enable	Queue 3 Enable	Queue 4 Enable	Queue 5 Enable	Queue 6 Enable	Queue 7 Enable
*	□	□	□	□	□	□	□	□
1	□	□	□	□	□	□	□	□
2	□	□	□	□	□	□	□	□
3	□	□	□	□	□	□	□	□
4	□	□	□	□	□	□	□	□
5	□	□	□	□	□	□	□	□
6	□	□	□	□	□	□	□	□
7	□	□	□	□	□	□	□	□
8	□	□	□	□	□	□	□	□
9	□	□	□	□	□	□	□	□
10	□	□	□	□	□	□	□	□
11	□	□	□	□	□	□	□	□
12	□	□	□	□	□	□	□	□

Label	Description
Port	The port number for which the configuration below applies.
Enable(E)	Controls whether the queue policer is enabled on this switch port.
Rate	Controls the rate for the queue policer. The default value is 500. This value is restricted to 100-1000000 when the “Unit” is “kbps”, and it is restricted to 1-3300 when the “Unit” is “Mbps”. This field is only shown if at least one of the queue policers are enabled.
Unit	Controls the unit of measure for the queue policer rate as kbps or Mbps. The default value is “kbps”. This field is only shown if at least one of the queue policers are enabled.

Port Scheduler

This page provides an overview of QoS Egress Port Schedulers for all switch ports.



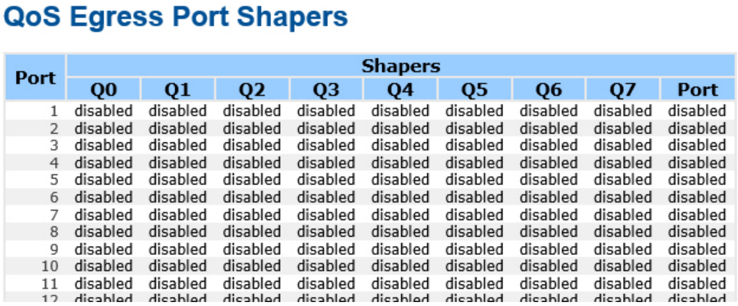
QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-

Label	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.
Mode	Shows the scheduling mode for this port.
Qn	Shows the weight for this queue and port.

Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports.



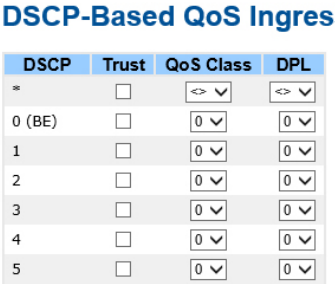
QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
11	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
12	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

Label	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.
Mode	Shows "disabled" or actual queue shaper rate – e.g. "800 Mbps".
Qn	Shows "disabled" or actual port shaper rate – e.g. "800 Mbps".

DSCP Based QoS

This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.



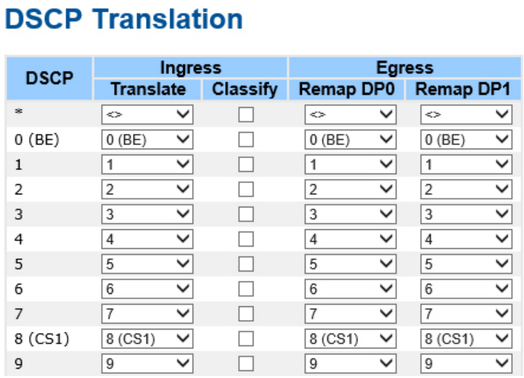
DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*	□	<>	<>
0 (BE)	□	0	0
1	□	0	0
2	□	0	0
3	□	0	0
4	□	0	0
5	□	0	0

Label	Description
DSCP	Maximum number of supported DSCP values are 64.
Trust	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.
QoS Class	QoS class value can be any of (0-7)
DPL	Drop Precedence Level (0-1)

DSCP Translation

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.



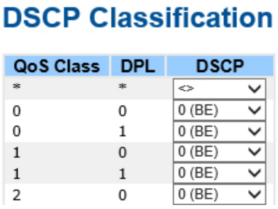
DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	□	<>	<>
0 (BE)	0 (BE)	□	0 (BE)	0 (BE)
1	1	□	1	1
2	2	□	2	2
3	3	□	3	3
4	4	□	4	4
5	5	□	5	5
6	6	□	6	6
7	7	□	7	7
8 (CS1)	8 (CS1)	□	8 (CS1)	8 (CS1)
9	9	□	9	9

Label	Description
DSCP	Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.
Ingress	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation – 1. Translate 2. Classify
1. Translate	DSCP at Ingress side can be translated to any of (0-63) DSCP values.
2. Classify	Click to enable Classification at Ingress side.
Egress	There are the following configurable parameters for Egress side – 1. Remap DP0 Controls the remapping for frames with DP level 0. 2. Remap DP1 Controls the remapping for frames with DP level 1.
1. Remap DP0	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.
2. Remap DP1	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

DSCP Classification

This page allows you to configure the mapping of QoS class and Drop Precedence Level to DSCP value.



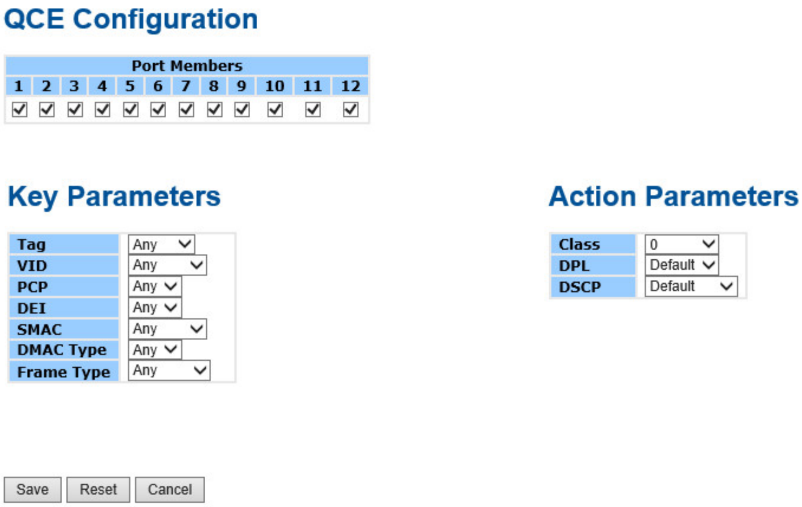
DSCP Classification

QoS Class	DPL	DSCP
*	*	<>
0	0	0 (BE)
0	1	0 (BE)
1	0	0 (BE)
1	1	0 (BE)
2	0	0 (BE)

Label	Description
QoS Class	Actual QoS class
DPL	Actual Drop Precedence Level.
DSCP	Select the classified DSCP value (0-63).

QoS Control List

This page allows to edit|insert a single QoS Control Entry at a time. A QCE consists of several parameters. These parameters vary according to the frame type that you select.



QCE Configuration

Port Members											
1	2	3	4	5	6	7	8	9	10	11	12
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Key Parameters

Tag	Any
VID	Any
PCP	Any
DEI	Any
SMAC	Any
DMAC Type	Any
Frame Type	Any

Action Parameters

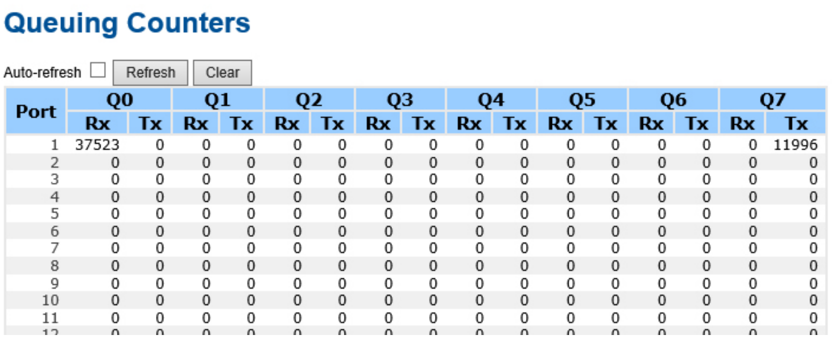
Class	0
DPL	Default
DSCP	Default

Label	Description
Port Members	Check the checkbox button to include the port in the QCL entry. By default all ports are included.
Key Parameters	Key configuration is described as below: **Tag** Value of Tag field can be 'Any', 'Untag' or 'Tag'. VID Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs. **PCP** Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'. **DEI** Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'. **SMAC** Source MAC address: 24 MS bits (OUI) or 'Any'. **DMAC** Type Destination MAC type: possible values are unicast(UC), multicast(MC), broadcast(BC) or 'Any'. **Frame Type** Frame Type can have any of the following values: 1. Any 2. Ethernet 3. LLC 4. SNAP 5. IPv4 6. IPv6 Note: All frame types are explained below.
1. Any	Allow all types of frames.
2. Ethernet	Ethernet Type Valid Ethernet type can have a value within 0x600-0xFFFF or 'Any' but excluding 0x800(IPv4) and 0x86DD(IPv6), default value is 'Any'.

Label	Description
3. LLC	SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'. DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'. Control Valid Control field can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'.
4. SNAP	PID Valid PID(a.k.a Ethernet type) can have value within 0x00-0xFFFF or 'Any', default value is 'Any'.
5. IPv4	Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'. Source IP Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero. DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43. IP Fragment Ipv4 frame fragmented option: yes|no|any. Sport Source TCP/UDP port(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP. Dport Destination TCP/UDP port(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP
6.IPv6	Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'. Source IP IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits. DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43. Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP. Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
Action Parameters	Class QoS class: (0-7) or 'Default'. DP Valid Drop Precedence Level can be (0-1) or 'Default'. DSCP Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'. 'Default' means that the default classified value is not modified by this QCE.

QoS Counters

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



Queuing Counters

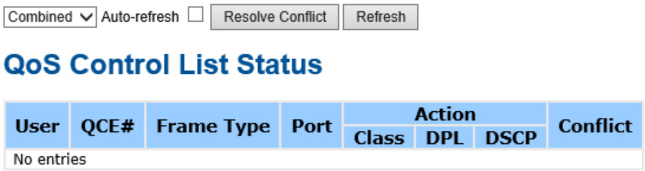
Auto-refresh □ Refresh Clear

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	37523	0	0	0	0	0	0	0	0	0	0	0	0	0	0	11996
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Label	Description
Port	The logical port for the settings contained in the same row.
Qn	There are 8 QoS queues per port. Q0 is the lowest priority queue.
Rx / Tx	The number of received and transmitted packets per queue.

QCL Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.



QoS Control List Status

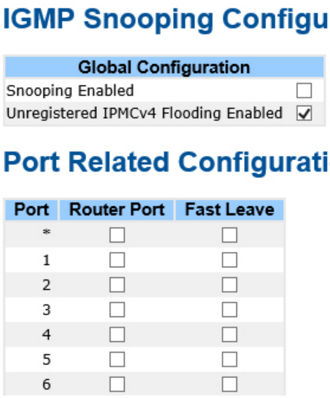
User	QCE#	Frame Type	Port	Action			Conflict
				Class	DPL	DSCP	
No entries							

Label	Description
User	Indicates the QCL user.
QCE#	Indicates the index of QCE.
Frame Type	Indicates the type of frame to look for incoming frames. Possible frame types are: Any: The QCE will match all frame type. Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. LLC: Only (LLC) frames are allowed. SNAP: Only (SNAP) frames are allowed. IPv4: The QCE will match only IPV4 frames. IPv6: The QCE will match only IPV6 frames.
Port	Indicates the list of ports configured with the QCE.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP. Class: Classified QoS class; if a frame matches the QCE it will be put in the queue. DPL: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column. DSCP: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.
Conflict	Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

Multicast

IGMP Snooping

This page provides IGMP Snooping related configuration.



IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	□
Unregistered IPMCv4 Flooding Enabled	☑

Port Related Configuration

Port	Router Port	Fast Leave
*	□	□
1	□	□
2	□	□
3	□	□
4	□	□
5	□	□
6	□	□

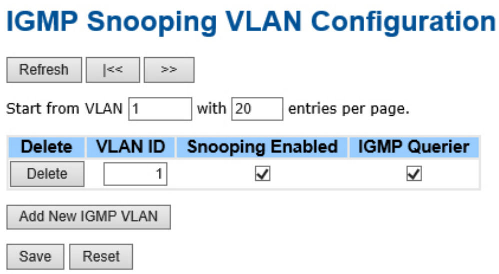
Label	Description
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMCv4Flooding enabled	Enable unregistered IPMC traffic flooding.
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP 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 – VLAN Configuration

Each page shows up to 99 entries from the VLAN 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 VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The “VLAN” input fields allow the user to select the starting point in the VLAN Table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest VLAN Table match.

The **>>** will use the last entry of the currently displayed entry 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.



IGMP Snooping VLAN Configuration

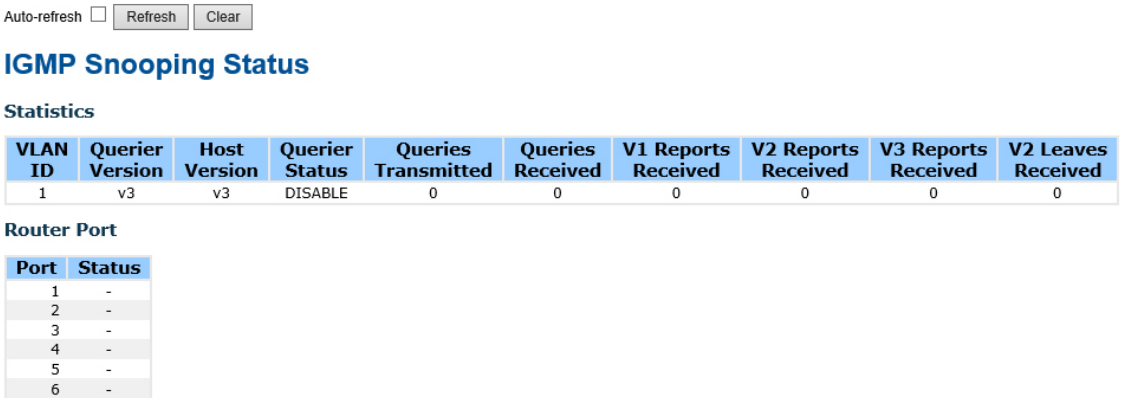
Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Snooping Enabled	IGMP Querier
Delete	1	☑	☑

Label	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enable	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
IGMP Querier	Enable the IGMP Querier in the VLAN.

IGMP Snooping Status

This page provides IGMP Snooping status.



IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
1	v3	v3	DISABLE	0	0	0	0	0	0

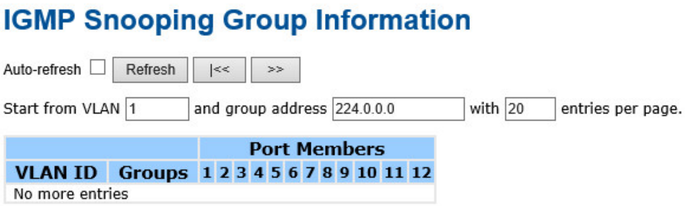
Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-

Label	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	Working Querier Version currently.
Host Version	Working Host Version currently.
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.
Port	Switch Port number
Status	Indicate whether specific port is a router port or not .

IGMP Snooping Groups Information

Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group.



IGMP Snooping Group Information

Auto-refresh □ Refresh |<< >>

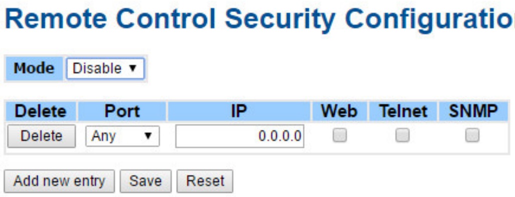
Start from VLAN 1 and group address 224.0.0.0 with 20 entries per page.

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

Label	Description
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group..

Security Remote Control

Remote Control Security allows you limit the remote access of management interface. When enabled, the request of client which is not in the allow list will be rejected.



Remote Control Security Configuration

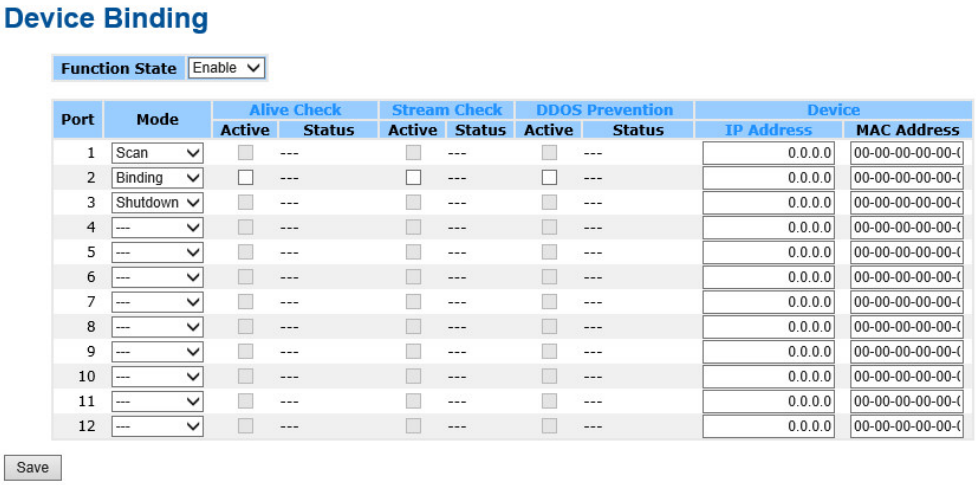
Mode: Disable

Delete	Port	IP	Web	Telnet	SNMP
Delete	Any	0.0.0.0	□	□	□

Label	Description
Port	Port number of remote client.
IP Address	IP address of remote client. Keeps this field “0.0.0.0” means “Any IP”.
Web	Check this item to enable Web management interface.
Telnet	Check this item to enable Telnet management interface.
SNMP	Check this item to enable SNMP management interface.
Delete	Check this item to delete.
Buttons	Save: Click to save changes. Reset: Click to undo any changes made locally and revert to previously saved values. Add New Entry: Click to add a new client.

Device Binding

This page provides Device Binding related configuration. Device Binding is a powerful monitor for devices and network security.



Device Binding

Function State: Enable

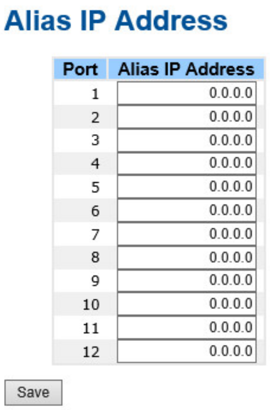
Port	Mode	Alive Check		Stream Check		DDOS Prevention		Device	
		Active	Status	Active	Status	Active	Status	IP Address	MAC Address
1	Scan	□	---	□	---	□	---	0.0.0.0	00-00-00-00-00-(
2	Binding	□	---	□	---	□	---	0.0.0.0	00-00-00-00-00-(
3	Shutdown	□	---	□	---	□	---	0.0.0.0	00-00-00-00-00-(
4	---	□	---	□	---	□	---	0.0.0.0	00-00-00-00-00-(
5	---	□	---	□	---	□	---	0.0.0.0	00-00-00-00-00-(
6	---	□	---	□	---	□	---	0.0.0.0	00-00-00-00-00-(
7	---	□	---	□	---	□	---	0.0.0.0	00-00-00-00-00-(
8	---	□	---	□	---	□	---	0.0.0.0	00-00-00-00-00-(
9	---	□	---	□	---	□	---	0.0.0.0	00-00-00-00-00-(
10	---	□	---	□	---	□	---	0.0.0.0	00-00-00-00-00-(
11	---	□	---	□	---	□	---	0.0.0.0	00-00-00-00-00-(
12	---	□	---	□	---	□	---	0.0.0.0	00-00-00-00-00-(

Label	Description
Mode	Indicates the per-port Device Binding operation. Possible modes are: ---: Disable. Scan: Scan IP/MAC automatically, but no binding function. Binding: Enable binding function. Under this mode, any IP/MAC doesn't match the entry will not be allowed to access the network. Shutdown: Shutdown the port (No Link).
Alive Check Active	Enable/Disable Alive Check. When enabled, switch will ping the device continually.
Alive Check Status	Indicates the Alive Check status. Possible statuses are: ---: Disable. Got Reply: Got ping reply from device, that means the device is still alive. Lost Reply: Lost ping reply from device, that means the device might have hanged.
Stream Check Active	Enable/Disable Stream Check. When enabled, switch will detect the stream change(getting low) from device.
Stream Check Status	Indicates the Stream Check status. Possible statuses are: ---: Disable. Normal: The stream is normal. Low: The stream is getting low.
DDoS Prevention Action	Enable/Disable DDOS Prevention. When enabled, switch will monitor the device to against DDOS attack (from device).
DDoS Prevention Status	Indicates the DDOS Prevention status. Possible statuses are: ---: Disable. Analysing: Analyse the packet throughput for initialization. Running: Function ready. Attacked: DDOS attack happened.
Device IP	Address Specify the IP Address of device.
Device MAC Address	Specify the MAC Address of device.

Advanced Configuration

Alias IP Address

This page provides Alias IP Address related configuration. Some devices might have more than one IP address, you could specify the other IP address here.



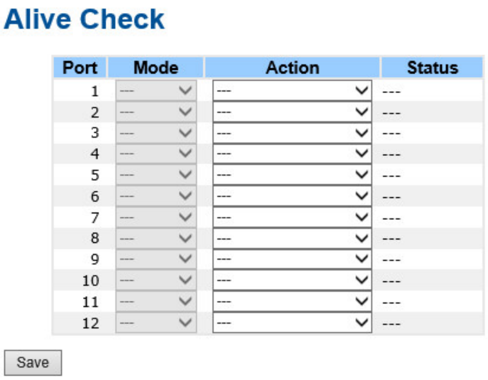
Alias IP Address

Port	Alias IP Address
1	0.0.0.0
2	0.0.0.0
3	0.0.0.0
4	0.0.0.0
5	0.0.0.0
6	0.0.0.0
7	0.0.0.0
8	0.0.0.0
9	0.0.0.0
10	0.0.0.0
11	0.0.0.0
12	0.0.0.0

Label	Description
Alias IP Address	Specify Alias IP address. Keep "0.0.0.0" if the device doesn't have alias IP address.

Alive Check

Using a constant ping command the switch will check for a possible port link failure. If the port link fails then the switch will complete the requested action field setting.



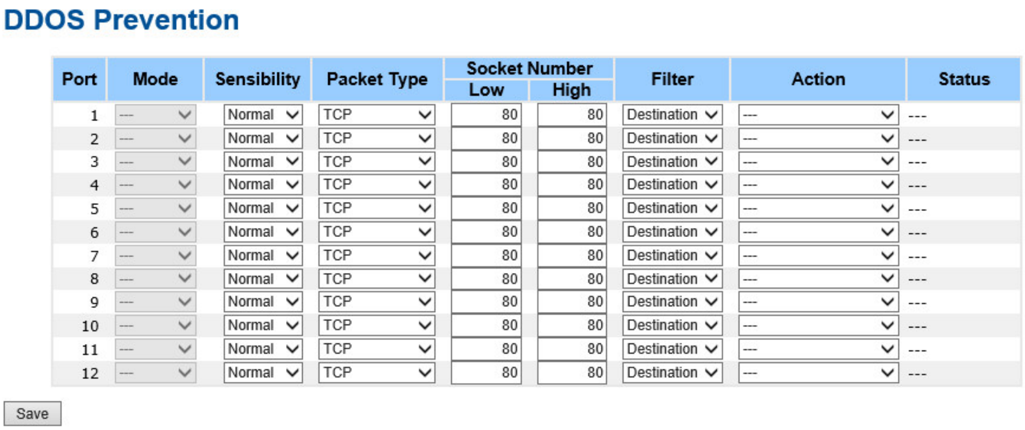
Alive Check

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

Label	Description
Link Change	Disable and enable port
Only log it	Only send log to log server
Shut Down the Port	Disable this port
Reboot Device	Disable and Enable P.O.E Power

DDoS Prevention

This page provides DDOS Prevention related configuration. The switch monitors the ingress packets and will take the selected action when a DDOS attack happens on the particular port.



DDOS Prevention

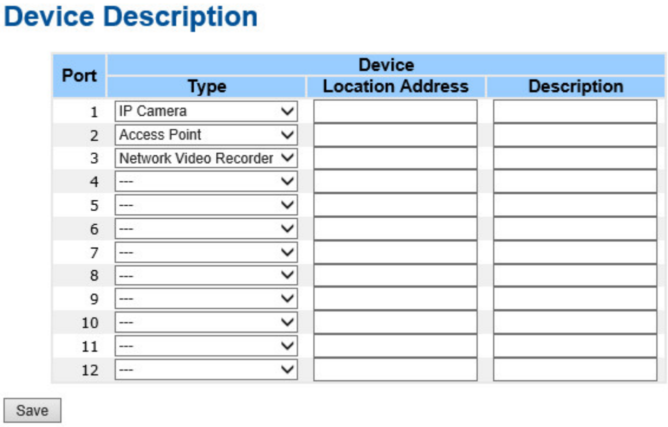
Port	Mode	Sensibility	Packet Type	Socket Number		Filter	Action	Status
				Low	High			
1	---	Normal	TCP	80	80	Destination	---	---
2	---	Normal	TCP	80	80	Destination	---	---
3	---	Normal	TCP	80	80	Destination	---	---
4	---	Normal	TCP	80	80	Destination	---	---
5	---	Normal	TCP	80	80	Destination	---	---
6	---	Normal	TCP	80	80	Destination	---	---
7	---	Normal	TCP	80	80	Destination	---	---
8	---	Normal	TCP	80	80	Destination	---	---
9	---	Normal	TCP	80	80	Destination	---	---
10	---	Normal	TCP	80	80	Destination	---	---
11	---	Normal	TCP	80	80	Destination	---	---
12	---	Normal	TCP	80	80	Destination	---	---

Label	Description
Mode	Enable/Disable DDOS Prevention of the port.
Sensibility	Indicates the level of DDOS detection. Possible levels are: Low: Low sensibility. Normal: Normal sensibility. Medium: Medium sensibility. High: High sensibility.
Packet Type	Indicates the packet type of DDOS monitor. Possible types are: RX Total: Total ingress packets. RX Unicast: Unicast ingress packets. RX Multicast: Multicast ingress packets. RX Broadcast: Broadcast ingress packets. TCP: TCP ingress packets. UDP: UDP ingress packets.
Socket Number	If packet type is UDP(or TCP), please specify the socket number here. The socket number could be a range, from low to high. If the socket number is only one, please fill the same number in low field and high field.
Filiter	If packet type is UDP(or TCP), please choose the socket direction (Destination/Source).
Action	Indicates the action when DDOS attack happened. Possible actions are: ---: Do nothing. Blocking 1 minute: To block the forwarding for 1 mintue, and log the event. Blocking 10 minute: To block the forwarding for 10 mintues, and log the event. Blocking: Just blocking, and log the event. Shut Down the Port: Shut down the port (No Link), and log the event. Only Log it: Just log the event. Reboot Device: If POE supported, the device could be rebooted. And log the event.

Label	Description
Status	Indicates the DDOS Prevention status. Possible statuses are: ---: Disable. Analysing: Analyse the packet throughput for initialization. Running: Function ready. Attacked: DDOS attack happened.

Device Description

This page provides Device Description related configuration.



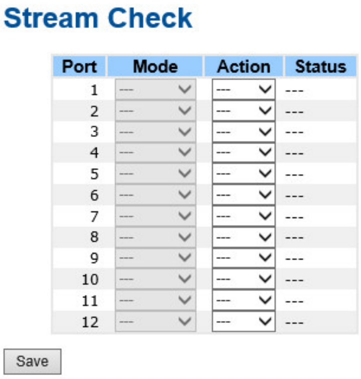
Device Description

Port	Device		
	Type	Location Address	Description
1	IP Camera		
2	Access Point		
3	Network Video Recorder		
4	---		
5	---		
6	---		
7	---		
8	---		
9	---		
10	---		
11	---		
12	---		

Label	Description
Device Type	Indicates the type of device. Possible types are: ---: No specification. IP Camera: IP Camera. IP Phone: IP Phone. Access Point: Access Point. PC: PC. PLC: PLC. Network Video Recorder: Network Video Recorder.
Location Address	Location information of device, this information could be used for Google Mapping.
Description	Device description.

Stream Check

This page provides Stream Check related configuration.



Stream Check

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

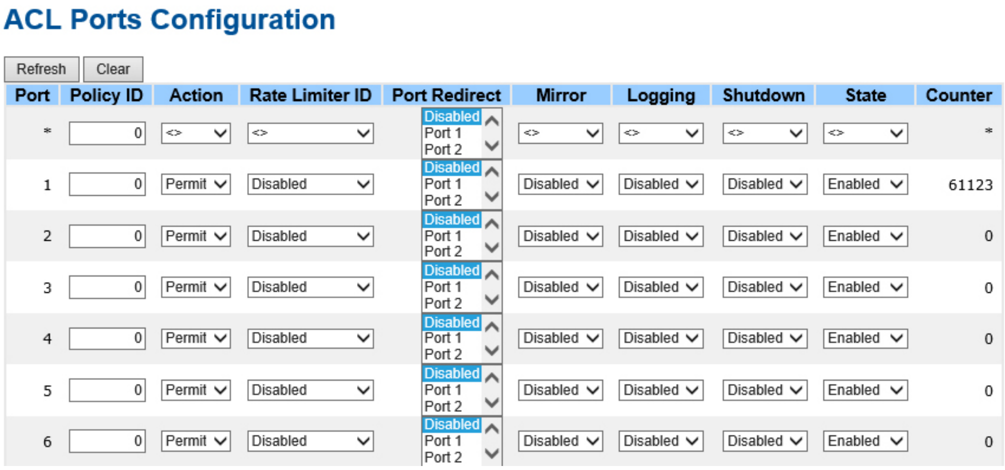
Label	Description
Mode	Enable/Disable stream monitor of the port.
Action	Indicates the action when stream getting low. Possible actions are: ---: Do nothing. Log it: Just log the event

Security

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.



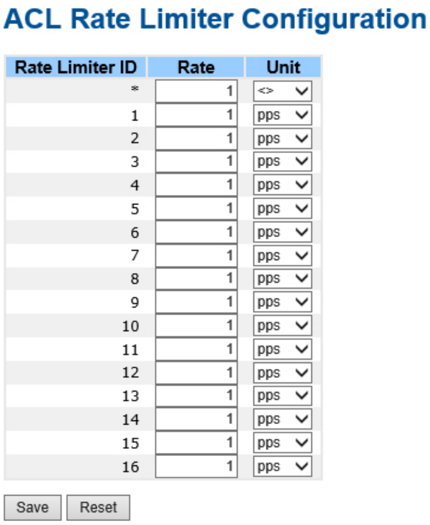
ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	61123
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	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.



ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	1	<>
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

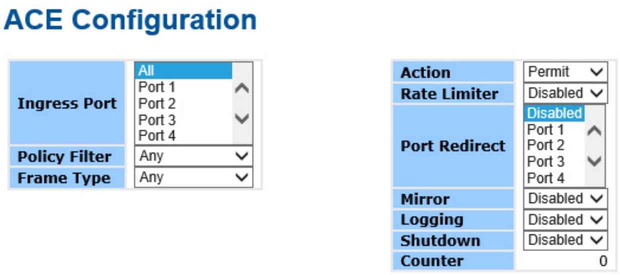
Label	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate	The rate unit is packet per second (pps), configure the rate as 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. The 1 kpps is actually 1002.1 pps.

ACL Control List

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.

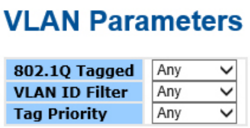


ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Any
Frame Type	Any

Action	Permit
Rate Limiter	Disabled
Port Redirect	Disabled Port 1 Port 2 Port 3 Port 4
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

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 specifies 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.



VLAN Parameters

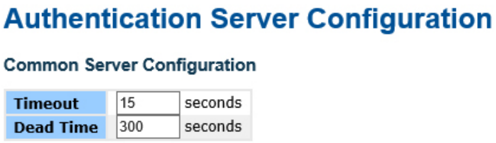
802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Label	Description
VLAN ID Filter	Specify the VLAN ID filter for this ACE. Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".) Specific: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.
VLAN ID	When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.
Tag Priority	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value Any means that no tag priority is specified (tag priority is "don't-care".)

AAA

Common Server Configuration

This page allows you to configure the Authentication Servers



Authentication Server Configuration

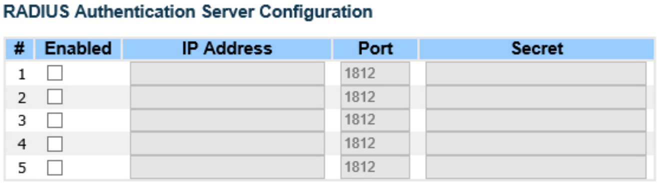
Common Server Configuration

Timeout	15	seconds
Dead Time	300	seconds

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

RADIUS Authentication Server Configuration

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

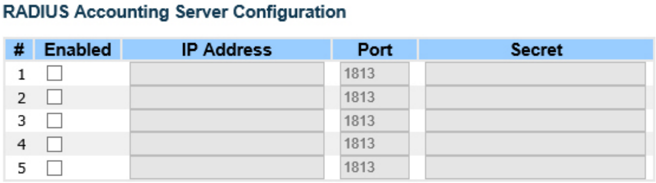


RADIUS Authentication Server Configuration

#	Enabled	IP Address	Port	Secret
1	□		1812	
2	□		1812	
3	□		1812	
4	□		1812	
5	□		1812	

Label	Description
#	The RADIUS Authentication Server number for which the configuration below applies.
Enabled	Enable the RADIUS Authentication Server by checking this box.
IP Address	The IP address or hostname of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation.
Port	The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.
Secret	The secret – up to 29 characters long – shared between the RADIUS Authentication Server and the switch stack.

RADIUS Accounting Server Configuration



RADIUS Accounting Server Configuration

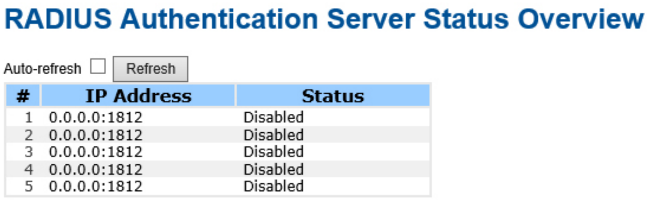
#	Enabled	IP Address	Port	Secret
1	□		1813	
2	□		1813	
3	□		1813	
4	□		1813	
5	□		1813	

Label	Description
#	The RADIUS Accounting Server number for which the configuration below applies.
Enabled	Enable the RADIUS Accounting Server by checking this box.
IP Address	The IP address or hostname of the RADIUS Accounting Server. IP address is expressed in dotted decimal notation.
Port	The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.
Secret	The secret – up to 29 characters long – shared between the RADIUS Accounting Server and the switch stack.

RADIUS Overview

This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page.

RADIUS Authentication Servers



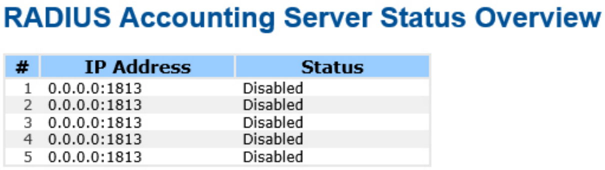
RADIUS Authentication Server Status Overview

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

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.
Status	The current status 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 Accounting Servers



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.
Status	The current status 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 accounting attempts. Dead (X seconds left): Accounting 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.

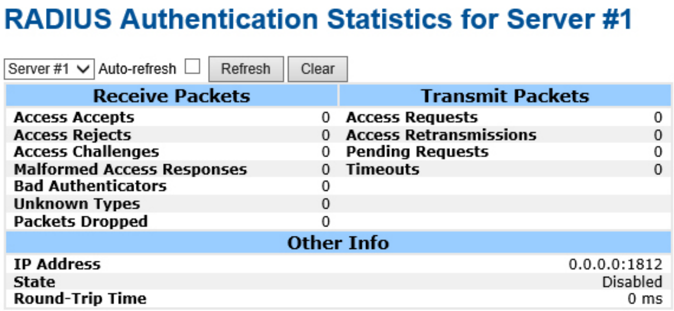
RADIUS Details

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.

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.

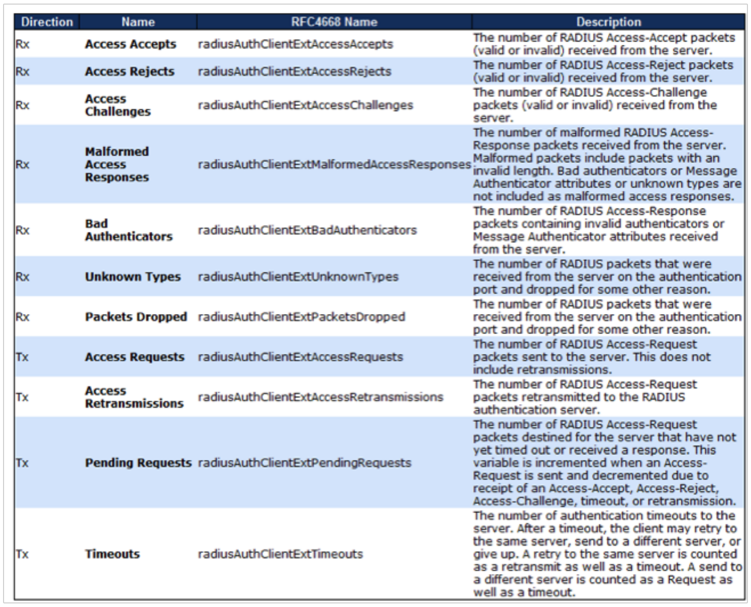
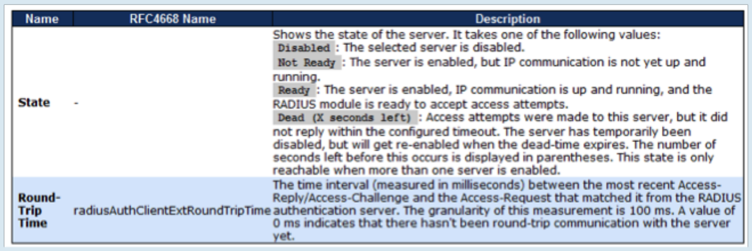


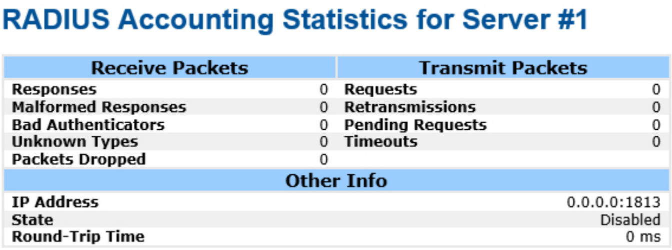
RADIUS Authentication Statistics for Server #1

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		

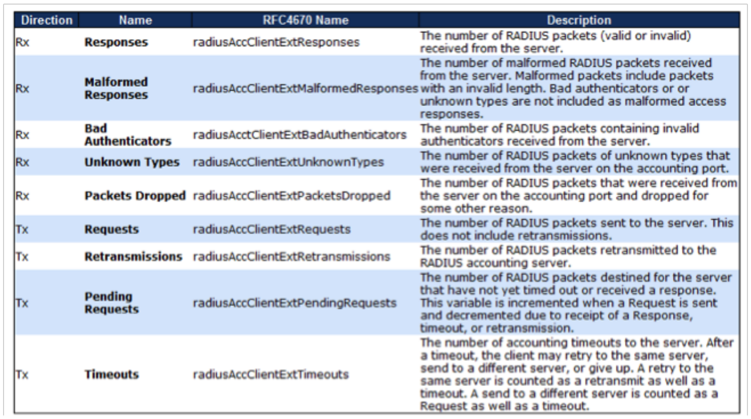
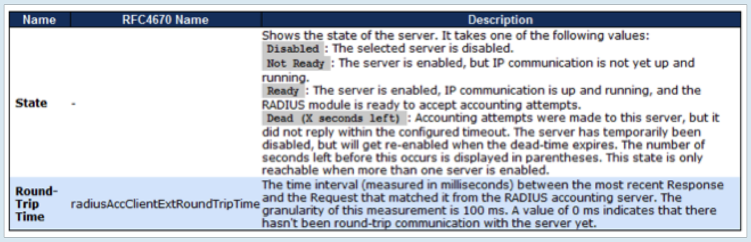
Other Info	
IP Address	0.0.0.0:1812
State	Disabled
Round-Trip Time	0 ms

<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td>Packet Counters</td><td>RADIUS authentication server packet counter. There are seven receive and four transmit counters.

<table>
<tr><th>Direction</th><th>Name</th><th>RFC4668 Name</th><th>Description</th></tr>
<tr><td>Rx</td><td>Access Accepts</td><td>radiusAuthClientExtAccessAccepts</td><td>The number of RADIUS Access-Accept packets (valid or invalid) received from the server.</td></tr>
<tr><td>Rx</td><td>Access Rejects</td><td>radiusAuthClientExtAccessRejects</td><td>The number of RADIUS Access-Reject packets (valid or invalid) received from the server.</td></tr>
<tr><td>Rx</td><td>Access Challenges</td><td>radiusAuthClientExtAccessChallenges</td><td>The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.</td></tr>
<tr><td>Rx</td><td>Malformed Access Responses</td><td>radiusAuthClientExtMalformedAccessResponses</td><td>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.</td></tr>
<tr><td>Rx</td><td>Bad Authenticators</td><td>radiusAuthClientExtBadAuthenticators</td><td>The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.</td></tr>
<tr><td>Rx</td><td>Unknown Types</td><td>radiusAuthClientExtUnknownTypes</td><td>The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.</td></tr>
<tr><td>Rx</td><td>Packets Dropped</td><td>radiusAuthClientExtPacketsDropped</td><td>The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.</td></tr>
<tr><td>Tx</td><td>Access Requests</td><td>radiusAuthClientExtAccessRequests</td><td>The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.</td></tr>
<tr><td>Tx</td><td>Access Retransmissions</td><td>radiusAuthClientExtAccessRetransmissions</td><td>The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.</td></tr>
<tr><td>Tx</td><td>Pending Requests</td><td>radiusAuthClientExtPendingRequests</td><td>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.</td></tr>
<tr><td>Tx</td><td>Timeouts</td><td>radiusAuthClientExtTimeouts</td><td>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 Request as well as a timeout.</td></tr>
</table>
</td></tr>
<tr><td>Other Info</td><td>This section contains information about the state of the server and the latest round-trip time.

<table>
<tr><th>Name</th><th>RFC4668 Name</th><th>Description</th></tr>
<tr><td>State</td><td>-</td><td>Shows the state of the server. It takes 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 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.</td></tr>
<tr><td>Round-Trip Time</td><td>radiusAuthClientExtRoundTripTime</td><td>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 indicates that there hasn't been round-trip communication with the server yet.</td></tr>
</table>
</td></tr>
</table>



RADIUS Accounting Statistics for Server #1

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			
IP Address			0.0.0.0:1813
State			Disabled
Round-Trip Time			0 ms

<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td>Packet Counters</td><td>RADIUS accounting server packet counter. There are five receive and four transmit counters.
<table><tr><th>Direction</th><th>Name</th><th>RFC4670 Name</th><th>Description</th></tr><tr><td>Rx</td><td><b>Responses</b></td><td>radiusAccClientExtResponses</td><td>The number of RADIUS packets (valid or invalid) received from the server.</td></tr><tr><td>Rx</td><td><b>Malformed Responses</b></td><td>radiusAccClientExtMalformedResponses</td><td>The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or or unknown types are not included as malformed access responses.</td></tr><tr><td>Rx</td><td><b>Bad Authenticators</b></td><td>radiusAcctClientExtBadAuthenticators</td><td>The number of RADIUS packets containing invalid authenticators received from the server.</td></tr><tr><td>Rx</td><td><b>Unknown Types</b></td><td>radiusAccClientExtUnknownTypes</td><td>The number of RADIUS packets of unknown types that were received from the server on the accounting port.</td></tr><tr><td>Rx</td><td><b>Packets Dropped</b></td><td>radiusAccClientExtPacketsDropped</td><td>The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.</td></tr><tr><td>Tx</td><td><b>Requests</b></td><td>radiusAccClientExtRequests</td><td>The number of RADIUS packets sent to the server. This does not include retransmissions.</td></tr><tr><td>Tx</td><td><b>Retransmissions</b></td><td>radiusAccClientExtRetransmissions</td><td>The number of RADIUS packets retransmitted to the RADIUS accounting server.</td></tr><tr><td>Tx</td><td><b>Pending Requests</b></td><td>radiusAccClientExtPendingRequests</td><td>The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.</td></tr><tr><td>Tx</td><td><b>Timeouts</b></td><td>radiusAccClientExtTimeouts</td><td>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 Request as well as a timeout.</td></tr></table></td></tr>
<tr><td>Other Info</td><td>This section contains information about the state of the server and the latest
<table><tr><th>Name</th><th>RFC4670 Name</th><th>Description</th></tr><tr><td><b>State</b></td><td>-</td><td>Shows the state of the server. It takes one of the following values:
<code>Disabled</code> : The selected server is disabled.
<code>Not Ready</code> : The server is enabled, but IP communication is not yet up and running.
<code>Ready</code> : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.
<code>Dead (X seconds left)</code> : Accounting 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.</td></tr><tr><td><b>Round-Trip Time</b></td><td>radiusAccClientExtRoundTripTime</td><td>The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.</td></tr></table></td></tr>
</table>

NAS(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.

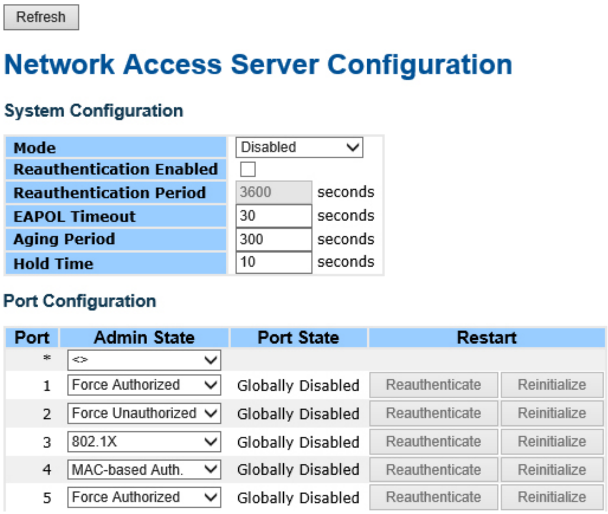
Overview of MAC-Based Authentication

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, a system – and a port-wide



Network Access Server Configuration

System Configuration

Mode	Disabled	
Reauthentication Enabled	☐	
Reauthentication Period	3600	seconds
EAPOL Timeout	30	seconds
Aging Period	300	seconds
Hold Time	10	seconds

Port Configuration

Port	Admin State	Port State	Restart	
*	<>			
1	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
2	Force Unauthorized	Globally Disabled	Reauthenticate	Reinitialize
3	802.1X	Globally Disabled	Reauthenticate	Reinitialize
4	MAC-based Auth.	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize

Label	Description
Mode	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.
Reauthentication Enabled	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. 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).
Reauthentication Period	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.
EAPOL Timeout	Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.

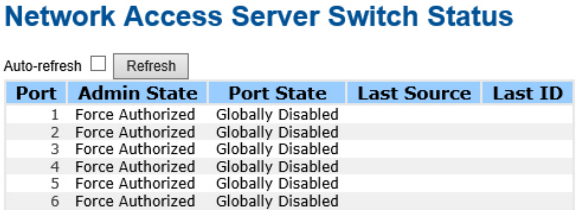
Label	Description
Age Period	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: • MAC-Based Auth. When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.
Hold Time	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: • MAC-Based Auth. If a client is denied access – either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration>Security>AAA" page) – the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. The switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.
Port	The port number for which the configuration below applies.

Label	Description
Admin State	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available: **Force Authorized** In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication. **Force Unauthorized** In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access. **Port-based 802.1X** 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 authenticator 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 AAA 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. Single 802.1X In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated. Multi 802.1X In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant. Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is – like Single 802.1X – not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module. In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination – to wake up any supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality. **MAC-based Auth.** Unlike port-based 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 the Port Security module. 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 port-based 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 advantage of MAC-based authentication over 802.1X-based authentication is 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. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

Label	Description
Port State	The current state of the port. It can undertake one of the following values: **Globally Disabled:** NAS is globally disabled. Link Down: NAS is globally enabled, but there is no link on the port. **Authorized:** The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. **Unauthorized:** The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. **X Auth/Y Unauth:** The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.
Restart	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect. **Reauthenticate:** Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized. **Reinitialize:** Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

Switch

This page provides an overview of the current NAS port states.



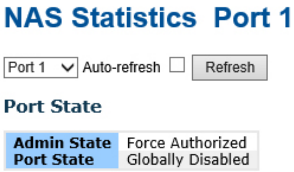
Network Access Server Switch Status

Auto-refresh □ Refresh

Port	Admin State	Port State	Last Source	Last ID
1	Force Authorized	Globally Disabled		
2	Force Authorized	Globally Disabled		
3	Force Authorized	Globally Disabled		
4	Force Authorized	Globally Disabled		
5	Force Authorized	Globally Disabled		
6	Force Authorized	Globally Disabled		

Label	Description
Port	The switch port number. Click to navigate to detailed 802.1X statistics for this port.
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
Last Source	The source MAC address carried in the most recently received EAPOL frame for EAPOL-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 Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

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.



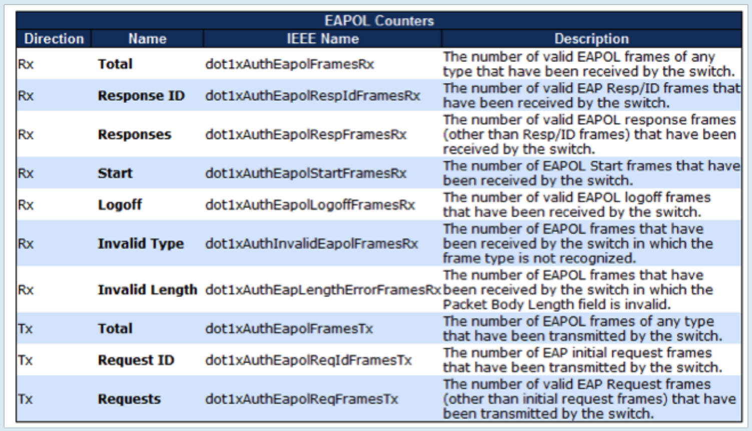
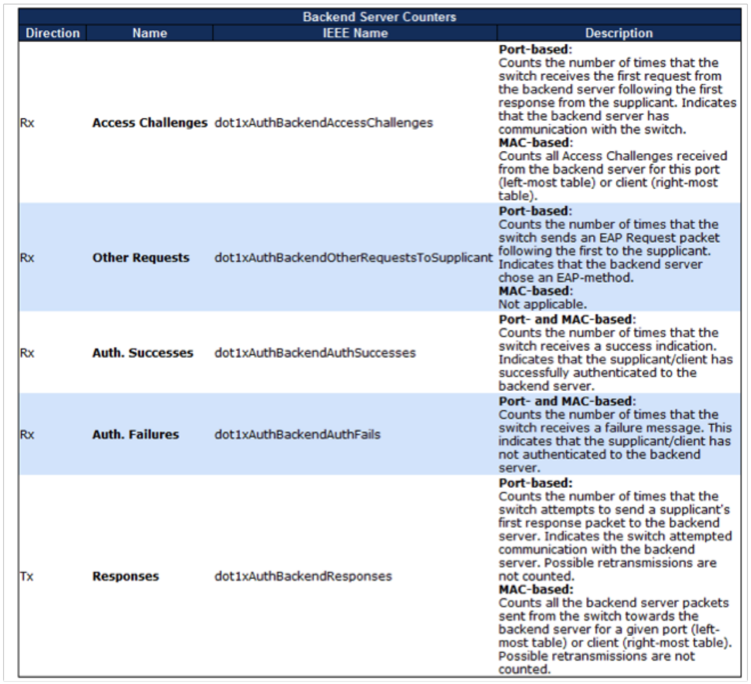
NAS Statistics Port 1

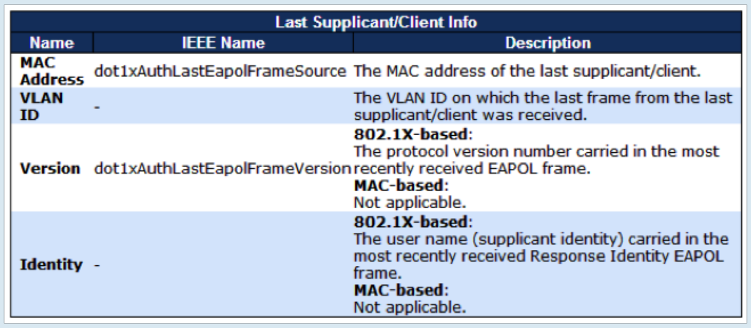
Port 1 ▾ Auto-refresh □ Refresh

Port State

Admin State	Force Authorized
Port State	Globally Disabled

Label	Description
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.

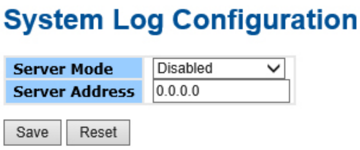
<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td>EAPOL Counters</td><td>These supplicant frame counters are available for the following administrative states:
• Force Authorized
• Force Unauthorized
• 802.1X

<table>
<tr><th colspan="4">EAPOL Counters</th></tr>
<tr><th>Direction</th><th>Name</th><th>IEEE Name</th><th>Description</th></tr>
<tr><td>Rx</td><td><b>Total</b></td><td>dot1xAuthEapolFramesRx</td><td>The number of valid EAPOL frames of any type that have been received by the switch.</td></tr>
<tr><td>Rx</td><td><b>Response ID</b></td><td>dot1xAuthEapolRespIdFramesRx</td><td>The number of valid EAP Resp/ID frames that have been received by the switch.</td></tr>
<tr><td>Rx</td><td><b>Responses</b></td><td>dot1xAuthEapolRespFramesRx</td><td>The number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch.</td></tr>
<tr><td>Rx</td><td><b>Start</b></td><td>dot1xAuthEapolStartFramesRx</td><td>The number of EAPOL Start frames that have been received by the switch.</td></tr>
<tr><td>Rx</td><td><b>Logoff</b></td><td>dot1xAuthEapolLogoffFramesRx</td><td>The number of valid EAPOL logoff frames that have been received by the switch.</td></tr>
<tr><td>Rx</td><td><b>Invalid Type</b></td><td>dot1xAuthInvalidEapolFramesRx</td><td>The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.</td></tr>
<tr><td>Rx</td><td><b>Invalid Length</b></td><td>dot1xAuthEapLengthErrorFramesRx</td><td>The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.</td></tr>
<tr><td>Tx</td><td><b>Total</b></td><td>dot1xAuthEapolFramesTx</td><td>The number of EAPOL frames of any type that have been transmitted by the switch.</td></tr>
<tr><td>Tx</td><td><b>Request ID</b></td><td>dot1xAuthEapolReqIdFramesTx</td><td>The number of EAP initial request frames that have been transmitted by the switch.</td></tr>
<tr><td>Tx</td><td><b>Requests</b></td><td>dot1xAuthEapolReqFramesTx</td><td>The number of valid EAP Request frames (other than initial request frames) that have been transmitted by the switch.</td></tr>
</table></td></tr>
<tr><td>Backend Server Counters</td><td>These backend (RADIUS) frame counters are available for the following administrative states:
• 802.1X
• MAC-based Auth.

<table>
<tr><th colspan="4">Backend Server Counters</th></tr>
<tr><th>Direction</th><th>Name</th><th>IEEE Name</th><th>Description</th></tr>
<tr><td>Rx</td><td><b>Access Challenges</b></td><td>dot1xAuthBackendAccessChallenges</td><td><b>Port-based</b>:
Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch.
<b>MAC-based</b>:
Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).</td></tr>
<tr><td>Rx</td><td><b>Other Requests</b></td><td>dot1xAuthBackendOtherRequestsToSupplicant</td><td><b>Port-based</b>:
Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method.
<b>MAC-based</b>:
Not applicable.</td></tr>
<tr><td>Rx</td><td><b>Auth. Successes</b></td><td>dot1xAuthBackendAuthSuccesses</td><td><b>Port- and MAC-based</b>:
Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.</td></tr>
<tr><td>Rx</td><td><b>Auth. Failures</b></td><td>dot1xAuthBackendAuthFails</td><td><b>Port- and MAC-based</b>:
Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.</td></tr>
<tr><td>Tx</td><td><b>Responses</b></td><td>dot1xAuthBackendResponses</td><td><b>Port-based:</b>
Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted.
<b>MAC-based:</b>
Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td>Last Supplicant/ Client Info</td><td>Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:
• 802.1X
• MAC-based Auth.

<table>
<tr><th colspan="3">Last Supplicant/Client Info</th></tr>
<tr><th>Name</th><th>IEEE Name</th><th>Description</th></tr>
<tr><td><b>MAC Address</b></td><td>dot1xAuthLastEapolFrameSource</td><td>The MAC address of the last supplicant/client.</td></tr>
<tr><td><b>VLAN ID</b></td><td>-</td><td>The VLAN ID on which the last frame from the last supplicant/client was received.</td></tr>
<tr><td><b>Version</b></td><td>dot1xAuthLastEapolFrameVersion</td><td><b>802.1X-based</b>:
The protocol version number carried in the most recently received EAPOL frame.
<b>MAC-based</b>:
Not applicable.</td></tr>
<tr><td><b>Identity</b></td><td>-</td><td><b>802.1X-based</b>:
The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame.
<b>MAC-based</b>:
Not applicable.</td></tr>
</table>
</td></tr>
</table>

System Warning

SYSLOG Setting

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


System Log Configuration

Server Mode	Disabled
Server Address	0.0.0.0

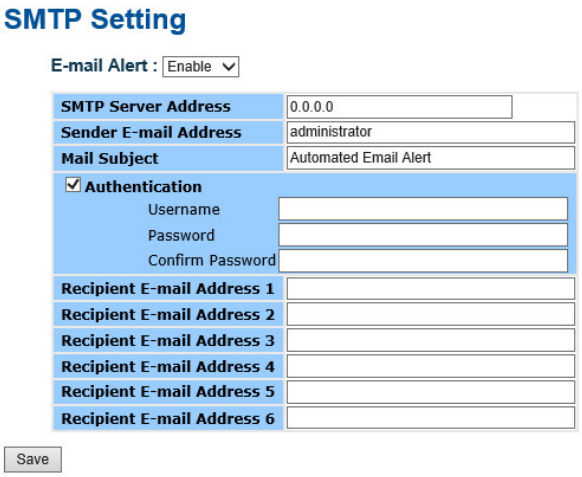
System Warning – SYSLOG Setting interface

The following table describes the labels in this screen.

Label	Description
Server Mode	Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are: Enabled: Enable server mode operation. Disabled: Disable server mode operation.
SYSLOG Server IP Address	Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name.

SMTP Setting

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



SMTP Setting

E-mail Alert : Enable

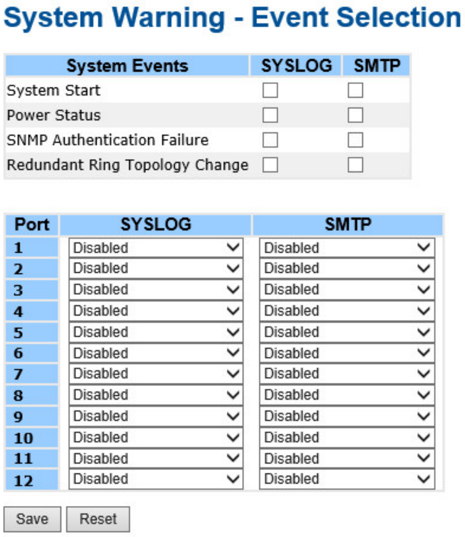
SMTP Server Address	0.0.0.0
Sender E-mail Address	administrator
Mail Subject	Automated Email Alert
☑ Authentication	
Username	
Password	
Confirm Password	
Recipient E-mail Address 1	
Recipient E-mail Address 2	
Recipient E-mail Address 3	
Recipient E-mail Address 4	
Recipient E-mail Address 5	
Recipient E-mail Address 6	

System Warning – SMTP Setting interface

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

Event Selection

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



System Warning - Event Selection

System Events	SYSLOG	SMTP
System Start	□	□
Power Status	□	□
SNMP Authentication Failure	□	□
Redundant Ring Topology Change	□	□

Port	SYSLOG	SMTP
1	Disabled	Disabled
2	Disabled	Disabled
3	Disabled	Disabled
4	Disabled	Disabled
5	Disabled	Disabled
6	Disabled	Disabled
7	Disabled	Disabled
8	Disabled	Disabled
9	Disabled	Disabled
10	Disabled	Disabled
11	Disabled	Disabled
12	Disabled	Disabled

System Warning – Event Selection interface

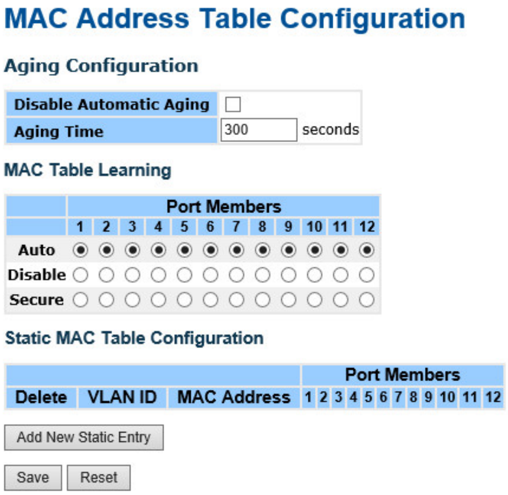
The following table describes the labels in this screen.

Label	Description
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 = event	› Disable › Link Up › Link Down › Link Up & Link Down
Save	Click to save the configurations.
Reset	Click to reset the configurations.

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.



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

MAC Table Learning

	Port Members											
	1	2	3	4	5	6	7	8	9	10	11	12
Auto	●	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○

Static MAC Table Configuration

			Port Members											
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12

Aging Configuration

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

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

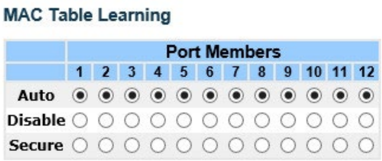
The allowed range is 10 to 1000000 seconds.

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

MAC Table Learning

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

Each port can do learning based upon the following settings:



MAC Table Learning

	Port Members											
	1	2	3	4	5	6	7	8	9	10	11	12
Auto	●	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○

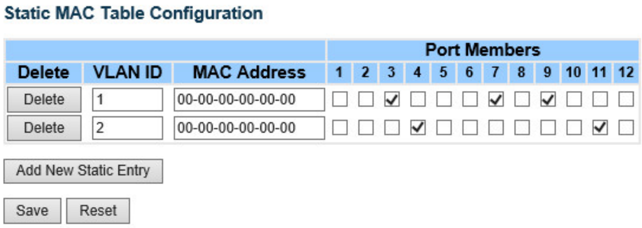
Label	Description
Auto	Learning is done automatically as soon as a frame with unknown SMAC is received.
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped. Note: Make sure that the link used for managing the switch is added to the Static Mac Table before 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.



Static MAC Table Configuration

			Port Members											
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12
Delete	1	00-00-00-00-00-00	□	□	☑	□	□	□	☑	□	☑	□	□	□
Delete	2	00-00-00-00-00-00	□	□	□	☑	□	□	□	□	□	□	☑	□

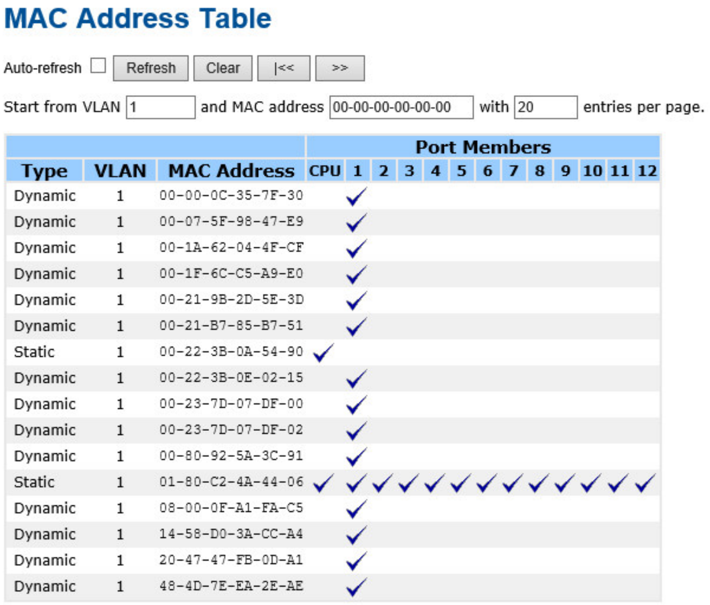
Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Add a New Static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



MAC Address Table

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

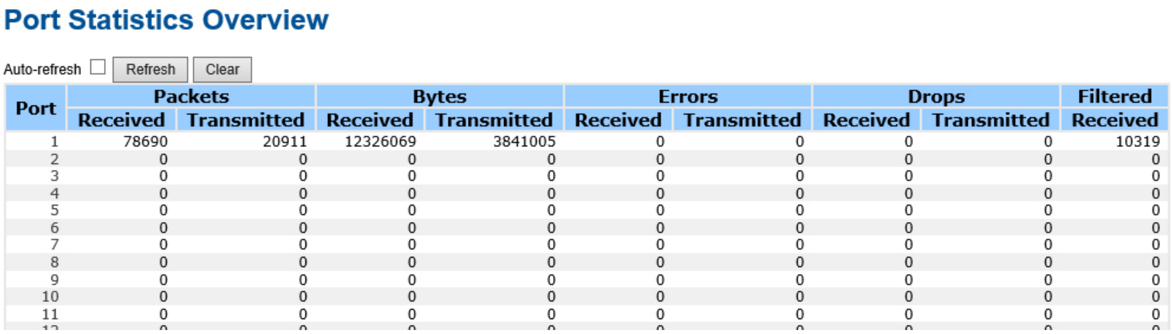
			Port Members												
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12
Dynamic	1	00-00-0C-35-7F-30		✓											
Dynamic	1	00-07-5F-98-47-E9		✓											
Dynamic	1	00-1A-62-04-4F-CF		✓											
Dynamic	1	00-1F-6C-C5-A9-E0		✓											
Dynamic	1	00-21-9B-2D-5E-3D		✓											
Dynamic	1	00-21-B7-85-B7-51		✓											
Static	1	00-22-3B-0A-54-90	✓												
Dynamic	1	00-22-3B-0E-02-15		✓											
Dynamic	1	00-23-7D-07-DF-00		✓											
Dynamic	1	00-23-7D-07-DF-02		✓											
Dynamic	1	00-80-92-5A-3C-91		✓											
Static	1	01-80-C2-4A-44-06	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic	1	08-00-0F-A1-FA-C5		✓											
Dynamic	1	14-58-D0-3A-CC-A4		✓											
Dynamic	1	20-47-47-FB-0D-A1		✓											
Dynamic	1	48-4D-7E-EA-2E-AE		✓											

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
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	78690	20911	12326069	3841005	0	0	0	0	10319
2	0	0	0	0	0	0	0	0	0
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

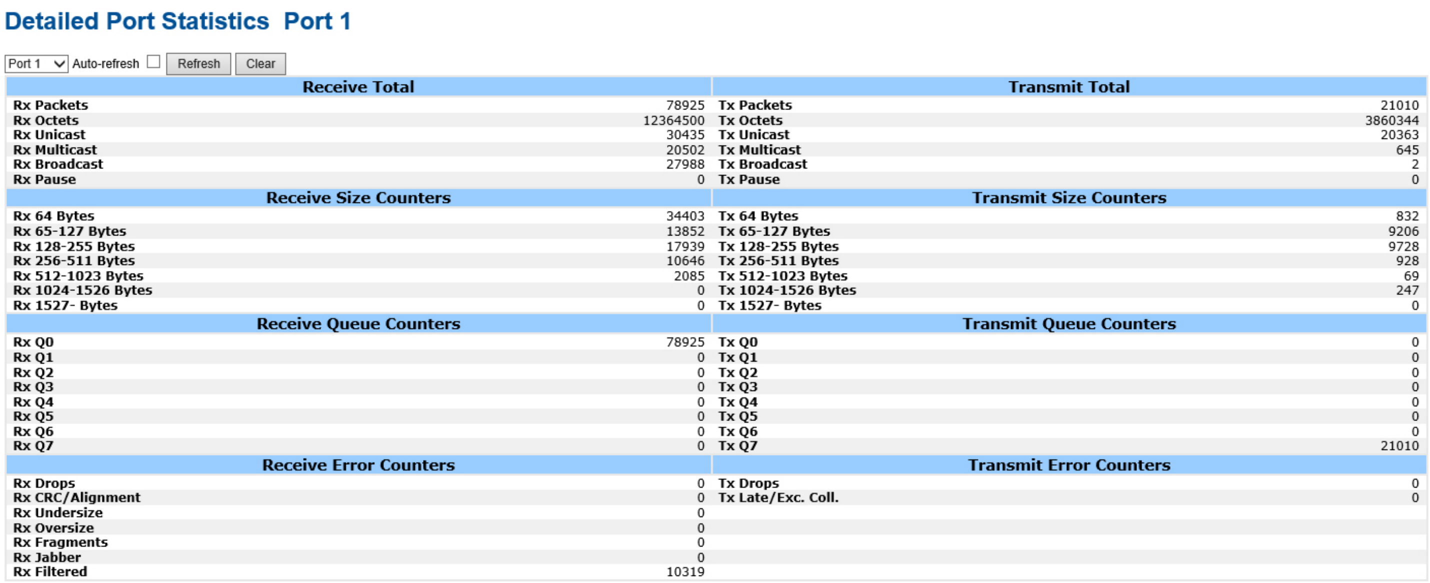
Label	Description
Port	The logical port for the settings contained in the same row.
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions per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

Detailed Statistics

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

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

Detailed Statistics-Receive & Transmit Total



Detailed Port Statistics Port 1

Receive Total		Transmit Total	
Rx Packets	78925	Tx Packets	21010
Rx Octets	12364500	Tx Octets	3860344
Rx Unicast	30435	Tx Unicast	20363
Rx Multicast	20502	Tx Multicast	645
Rx Broadcast	27988	Tx Broadcast	2
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	34403	Tx 64 Bytes	832
Rx 65-127 Bytes	13852	Tx 65-127 Bytes	9206
Rx 128-255 Bytes	17939	Tx 128-255 Bytes	9728
Rx 256-511 Bytes	10646	Tx 256-511 Bytes	928
Rx 512-1023 Bytes	2085	Tx 512-1023 Bytes	69
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	247
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	78925	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	21010
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	10319		

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

Label	Description
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 Monitoring

Configure port Mirroring on this page.

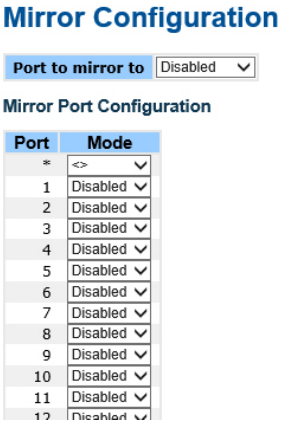
To debug network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow.

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.



Mirror Configuration

Port to mirror to: Disabled

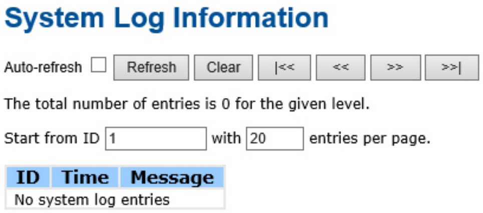
Mirror Port Configuration

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled

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.



System Log Information

The total number of entries is 0 for the given level.

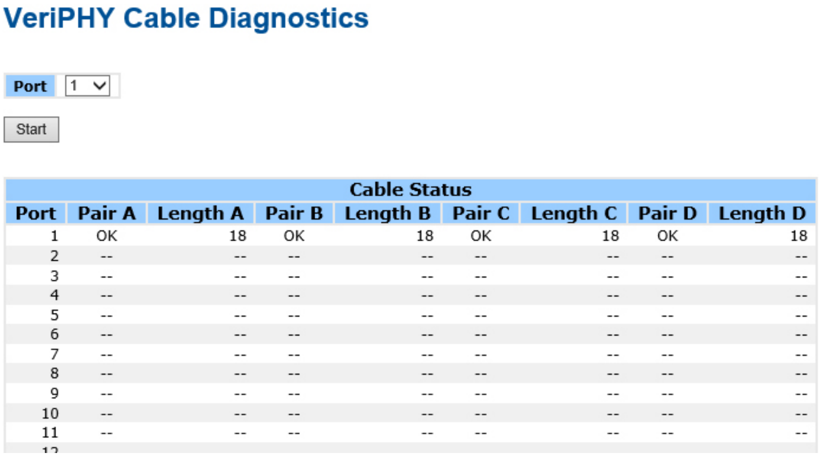
Start from ID 1 with 20 entries per page.

ID	Time	Message
No system log entries		

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.



Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	OK	18	OK	18	OK	18	OK	18
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--
7	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--
9	--	--	--	--	--	--	--	--
10	--	--	--	--	--	--	--	--
11	--	--	--	--	--	--	--	--
12								

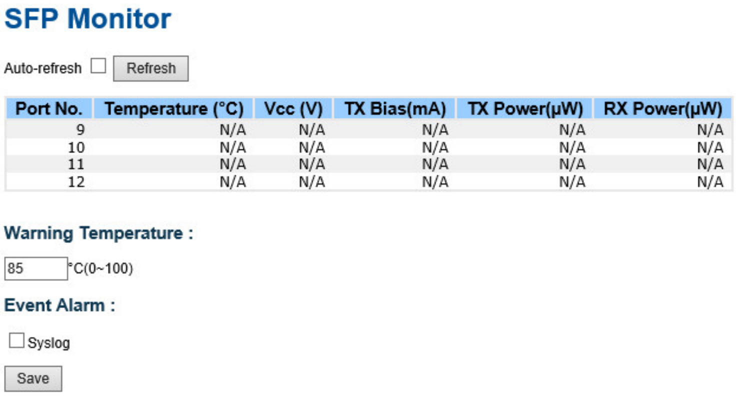
Press **Start** to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate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

SFP Monitor

DDM function, can pass SFP module which supports DDM function, measure the temperature of the apparatus and manage and set up event alarm module through DDM WEB



SFP Monitor

Auto-refresh □ Refresh

Port No.	Temperature (°C)	Vcc (V)	TX Bias(mA)	TX Power(μW)	RX Power(μW)
9	N/A	N/A	N/A	N/A	N/A
10	N/A	N/A	N/A	N/A	N/A
11	N/A	N/A	N/A	N/A	N/A
12	N/A	N/A	N/A	N/A	N/A

Warning Temperature :

85 °C(0~100)

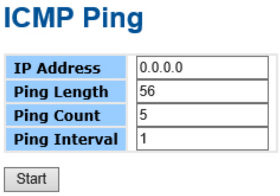
Event Alarm :

□ Syslog

Save

Ping

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



ICMP Ping

IP Address	0.0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1

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:

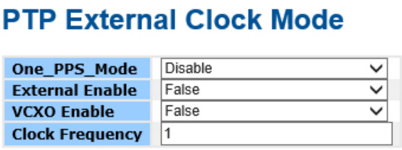
Label	Description
IP Address	The destination IP Address.
Ping Size	The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.

Syncronization-PTP

Overview of MAC-Based Authentication

This page allows the user to configure and inspect the current PTP clock settings.

PTP External Clock Mode

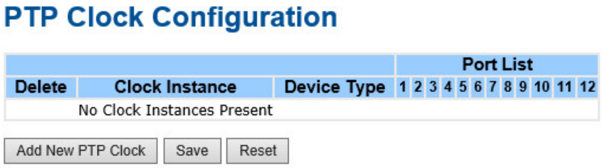


PTP External Clock Mode

One_PPS_Mode	Disable
External Enable	False
VCXO Enable	False
Clock Frequency	1

Label	Description
One_pps_mode	This Selection box will allow you to select the One_pps_mode configuration. The following values are possible: 1. Output : Enable the 1 pps clock output 2. Input : Enable the 1 pps clock input 3. Disable : Disable the 1 pps clock in/out-put
External Enable	This Selection box will allow you to configure the External Clock output. The following values are possible: 1. True : Enable the external clock output 2. False : Disable the external clock output
VCXO_Enable	This Selection box will allow you to configure the External VCXO rate adjustment. The following values are possible: 1. True : Enable the external VCXO rate adjustment 2. False : Disable the external VCXO rate adjustment
Clock Frequency	This will allow to set the Clock Frequency. The possible range of values are 1 – 25000000 (1 – 25MHz)

PTP Clock Configuration



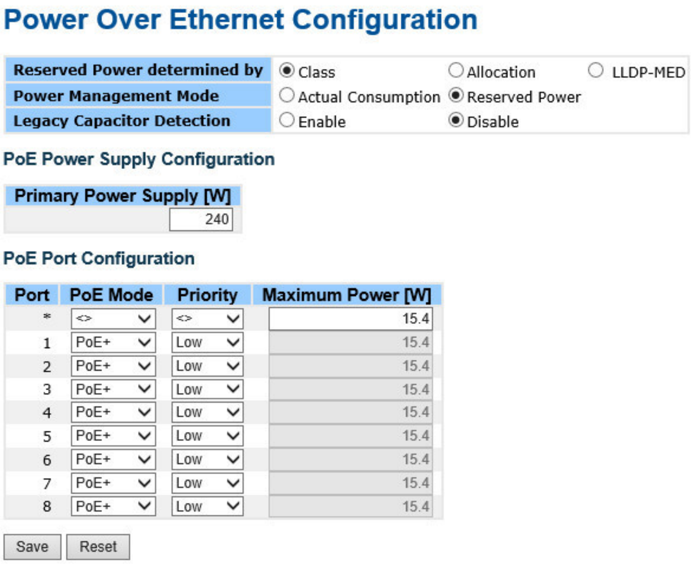
PTP Clock Configuration

Delete	Clock Instance	Device Type	Port List											
			1	2	3	4	5	6	7	8	9	10	11	12
	No Clock Instances Present													

Label	Description
Delete	Check this box and click on 'Save' to delete the clock instance.
Clock Instance	Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to edit the Clock details.
Device Type	Indicates the Type of the Clock Instance. There are five Device Types. 1. Ord-Bound - clock's Device Type is Ordinary-Boundary Clock. 2. P2p Transp - clock's Device Type is Peer to Peer Transparent Clock. 3. E2e Transp - clock's Device Type is End to End Transparent Clock. 4. Master Only - clock's Device Type is Master Only. 5. Slave Only - clock's Device Type is Slave Only.
Port List	Set check mark for each port configured for this Clock Instance.
2 Step Flag	Static member: defined by the system, true if two-step Sync events and Pdelay_Resp events are used
Clock Identity	It shows unique clock identifier
One Way	If true, one-way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.
Protocol	Transport protocol used by the PTP protocol engine Ethernet PTP over Ethernet multicast ip4multi PTP over IPv4 multicast ip4uni PTP over IPv4 unicast Note : IPv4 unicast protocol only works in Master only and Slave only clocks See parameter Device Type In a unicast Slave only clock you also need configure which master clocks to request Announce and Sync messages from. See: Unicast Slave Configuration
VLAN Tag Enable	Enables the VLAN tagging for the PTP frames. Note: Packets are only tagged if the port is configured for vlan tagging. i.e: Port Type != Unaware and PortVLAN mode == None, and the port is member of the VLAN.
VID	VLAN Identifier used for tagging the PTP frames.
PCP	Priority Code Point value used for PTP frames.

PoE Configuration (PoE Models Only)

PoE is an acronym for Power Over Ethernet. Power Over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.



Power Over Ethernet Configuration

Reserved Power determined by	● Class	○ Allocation	○ LLDP-MED
Power Management Mode	○ Actual Consumption	● Reserved Power	
Legacy Capacitor Detection	○ Enable	● Disable	

PoE Power Supply Configuration

Primary Power Supply [W]
240

PoE Port Configuration

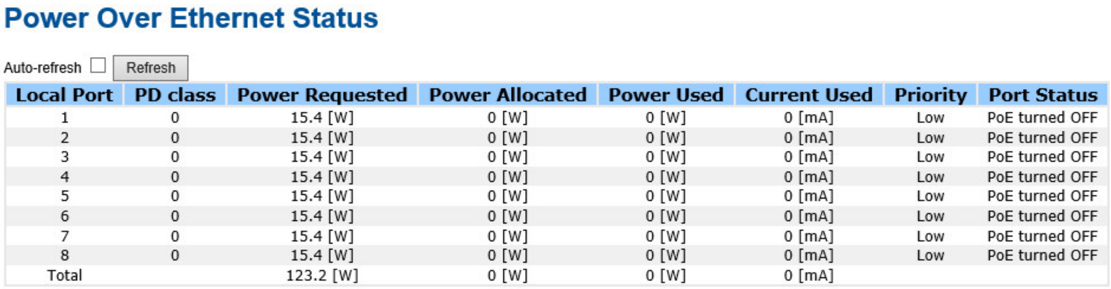
Port	PoE Mode	Priority	Maximum Power [W]
*	<>	<>	15.4
1	PoE+	Low	15.4
2	PoE+	Low	15.4
3	PoE+	Low	15.4
4	PoE+	Low	15.4
5	PoE+	Low	15.4
6	PoE+	Low	15.4
7	PoE+	Low	15.4
8	PoE+	Low	15.4

Label	Description
Reserved Power determined by	There are three modes for configuring how the ports/PDs may reserve power. 1. Allocated mode: In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields. 2. Class mode: In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode the Maximum Power fields have no effect. 3. LLDP-MED mode: This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode In this mode the Maximum Power fields have no effect For all modes: If a port uses more power than the reserved power for the port, the port is shut down.

Label	Description
Power Management Mode	There are 2 modes for configuring when to shut down the ports: 1. Actual Consumption: In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down. 2. Reserved Power: In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.
Primary Power Source	For being able to determine the amount of power the PD may use, it must be defined what amount of power the primary power source can deliver. Valid values are 0 - 240 Watts
Port	This is the logical port number for this row. Ports that are not PoE-capable are grayed out and thus impossible to configure PoE for.
PoE Mode	The PoE Mode represents the PoE operating mode for the port. Disabled: PoE disabled for the port. PoE : Enables PoE IEEE 802.3af (Class 4 PDs limited to 15.4W) PoE+ : Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 30W)
Priority	The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical. The priority is used in the case where the remote devices requires more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.
Maximum Power	The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device. (The maximum allowed value is 30 W.)

Status

This page allows the user to inspect the current status for all PoE ports.



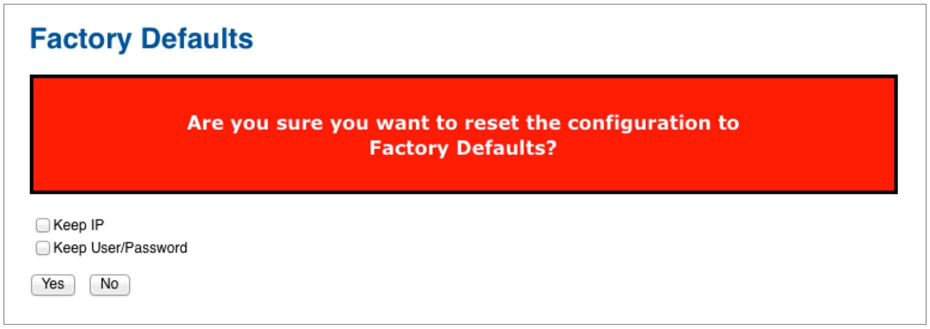
Power Over Ethernet Status

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	0	15.4 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
2	0	15.4 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
3	0	15.4 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
4	0	15.4 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
5	0	15.4 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
6	0	15.4 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
7	0	15.4 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
8	0	15.4 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF
Total		123.2 [W]	0 [W]	0 [W]	0 [mA]		

Label	Description
Local Port	This is the logical port number for this row.
PD Class	Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the PDs class. Five Classes are defined: Class 0: Max. power 15.4 W Class 1: Max. power 4.0 W Class 2: Max. power 7.0 W Class 3: Max. power 15.4 W Class 4: Max. power 30.0 W
Power Requested	The Power Requested shows the requested amount of power the PD wants to be reserved.
Power Allocated	The Power Allocated shows the amount of power the switch has allocated for the PD.
Power Used	The Power Used shows how much power the PD currently is using.
Current Used	The Power Used shows how much current the PD currently is using.
Priority	The Priority shows the port's priority configured by the user.
Port Status	The Port Status shows the port's status. The status can be one of the following values: PoE not available – No PoE chip found – PoE not supported for the port. PoE turned OFF – PoE disabled : PoE is disabled by user. PoE turned OFF – Power budget exceeded – The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down. No PD detected – No PD detected for the port. PoE turned OFF – PD overload – The PD has requested or used more power than the port can deliver, and is powered down. PoE turned OFF – PD is off. Invalid PD – PD detected, but is not working correctly.

Factory Defaults

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



Factory Defaults

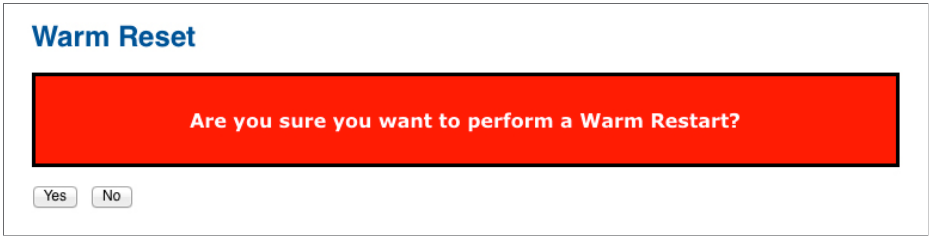
Are you sure you want to reset the configuration to Factory Defaults?

□ 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

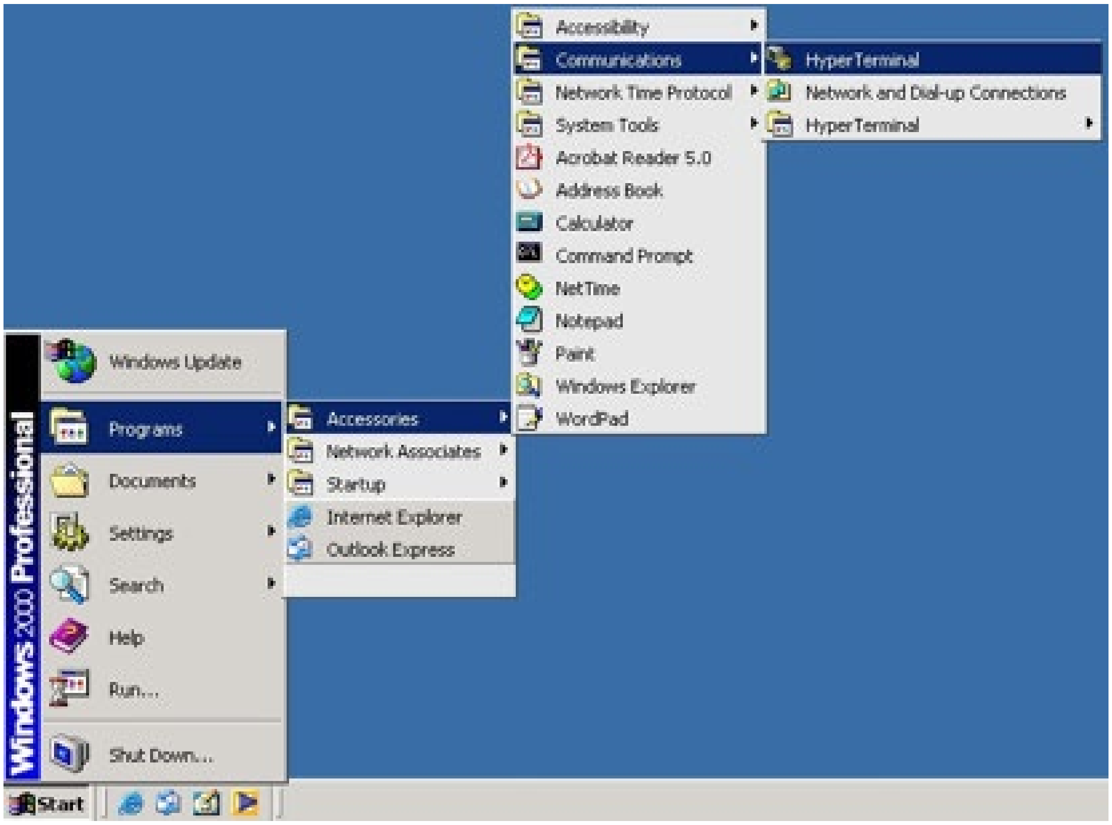
In addition to WEB-base management, the switch also supports CLI management. You can use console or telnet to management the switch by CLI.

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

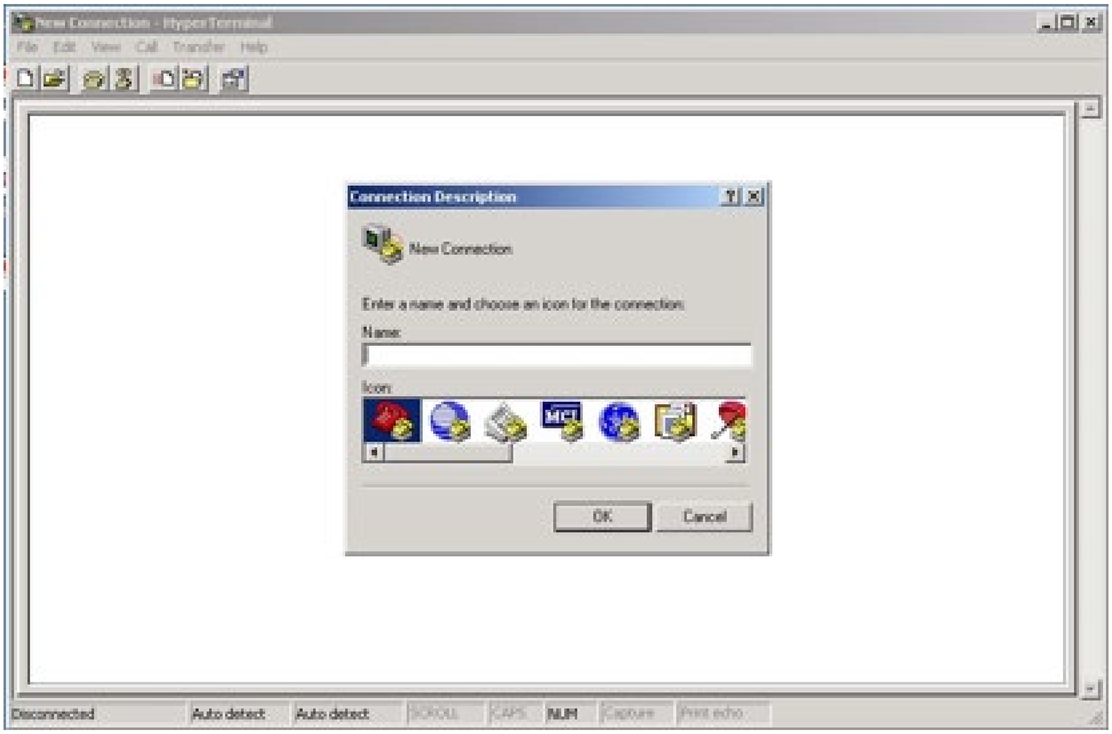
Before Configuring by RS-232 serial console, use an DB-9-M to RJ-45 cable to connect the switches' RS-232 Console port to your PC COM port.

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



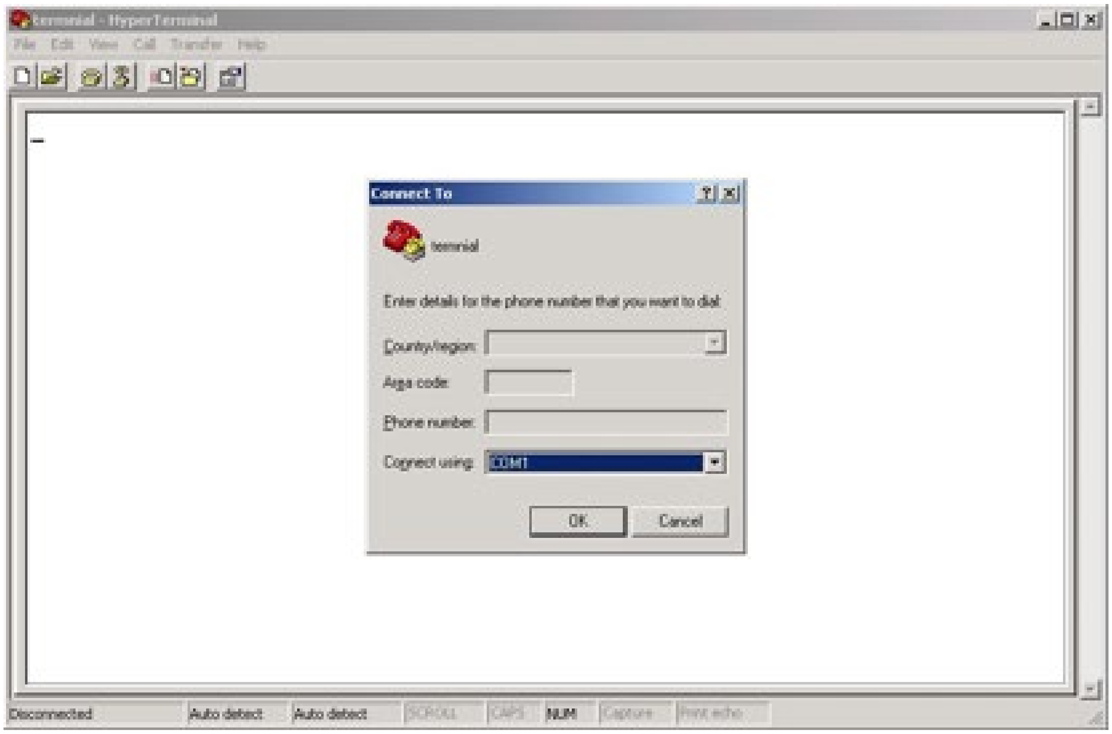
New Connection

Enter a name and choose an icon for the connection:

Name:

Icon:

Step 3. Select to use COM port number



termnial

Enter details for the phone number that you want to dial:

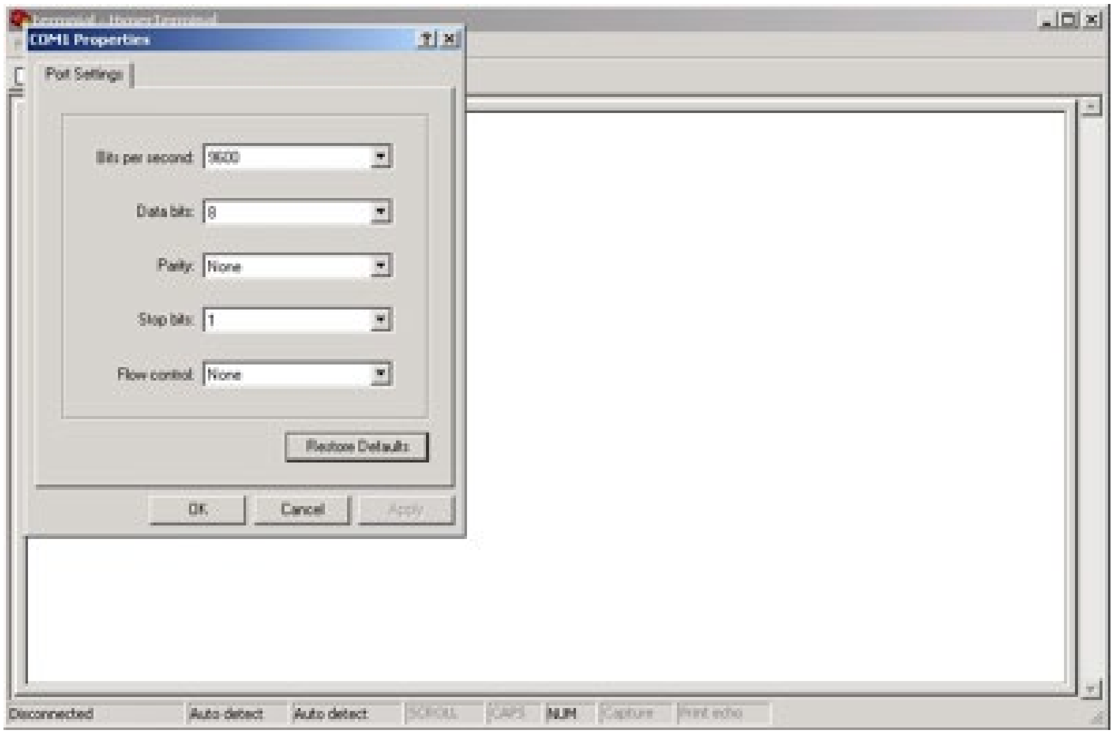
Country/region:

Area code:

Phone number:

Connect using: COM1

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.



Bits per second: 9600

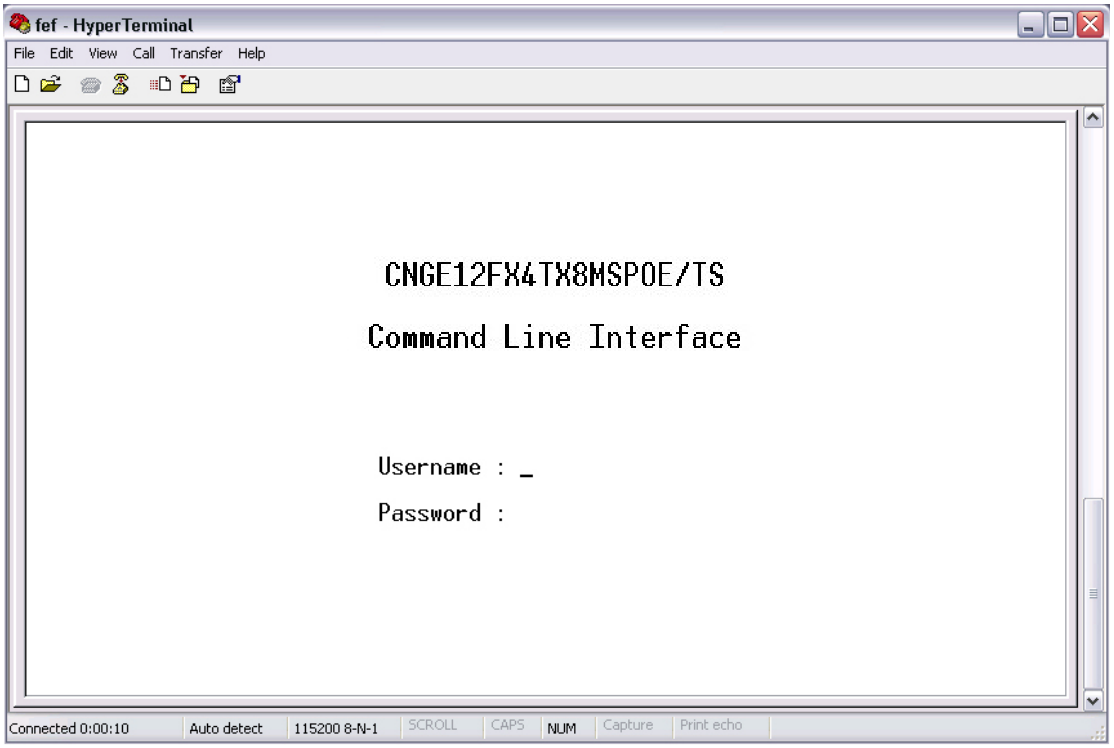
Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

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**.



```
        CNGE12FX4TX8MSPOE/TS

       Command Line Interface


       Username : _

       Password :
```

CLI Management by Telnet

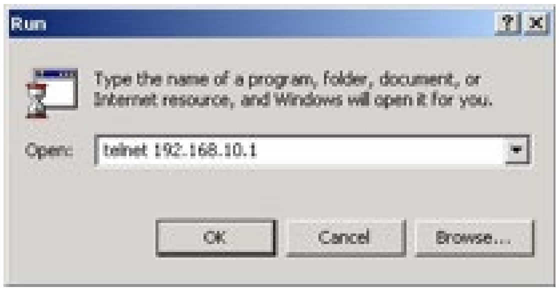
Users can use “**TELNET**” to configure the switches.

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**

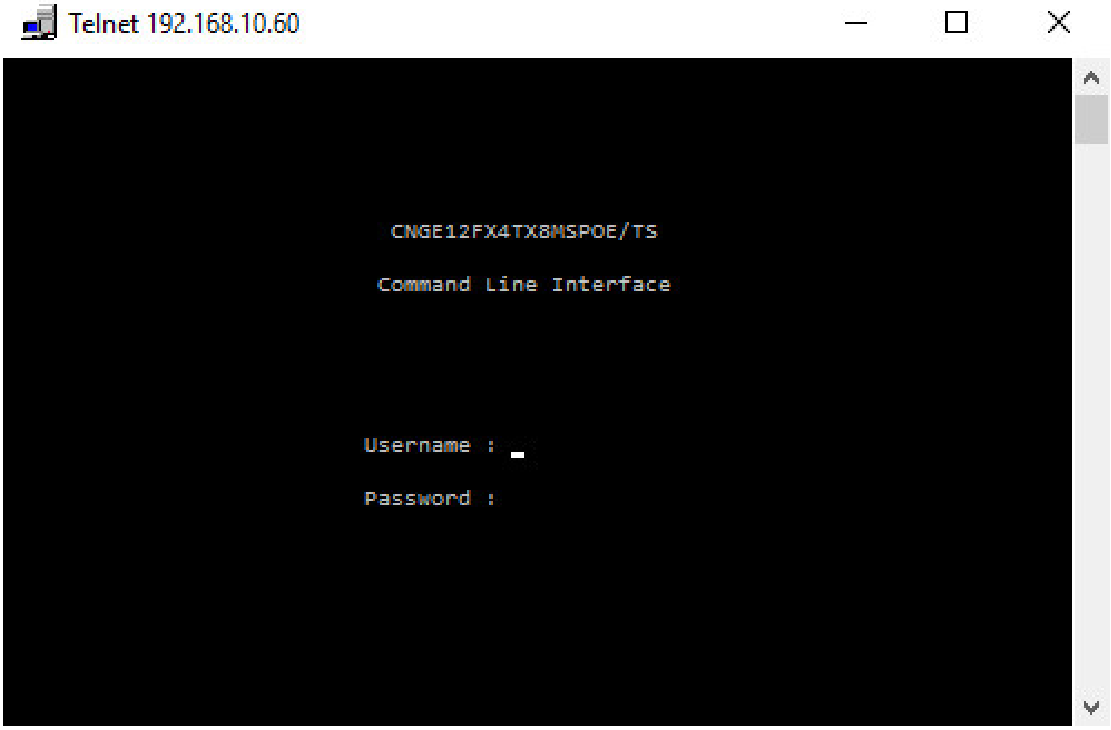
Follow the steps below to access the console via Telnet.

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


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

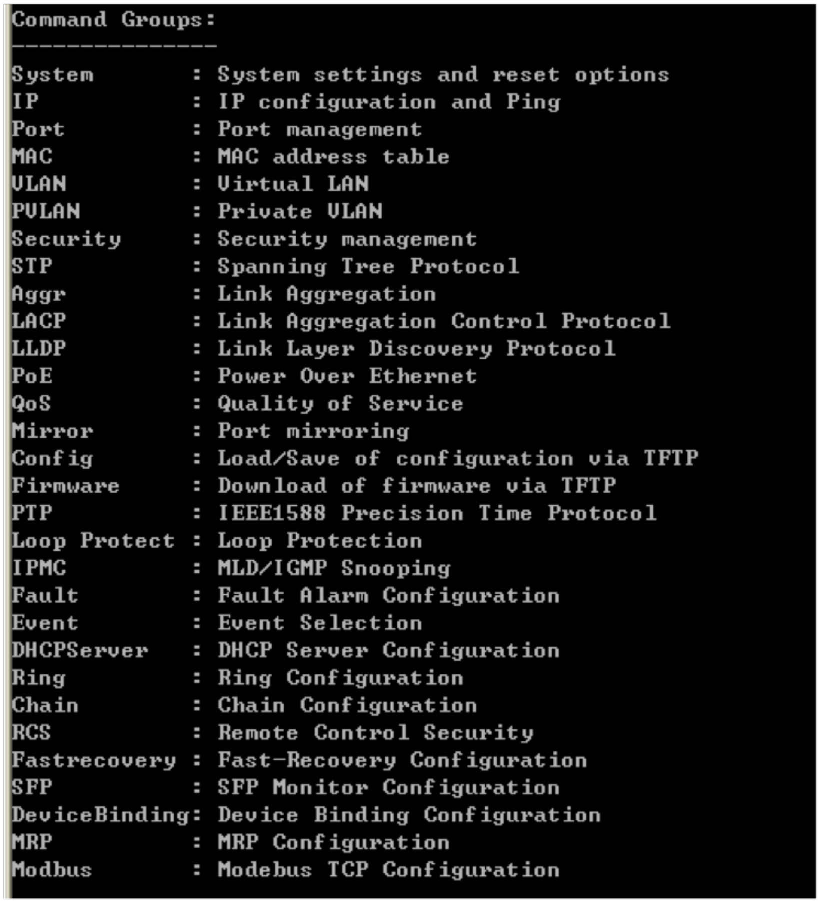
```
telnet 192.168.10.1
```

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**



```
CNGE12FX4TX8MSPOE/TS

Command Line Interface



Username :

Password :
```

Commander Groups



```
Command Groups:
---------------

System       : System settings and reset options
IP           : IP configuration and Ping
Port         : Port management
MAC          : MAC address table
VLAN         : Virtual LAN
PVLAN        : Private VLAN
Security     : Security management
STP          : Spanning Tree Protocol
Aggr         : Link Aggregation
LACP         : Link Aggregation Control Protocol
LLDP         : Link Layer Discovery Protocol
PoE          : Power Over Ethernet
QoS          : Quality of Service
Mirror       : Port mirroring
Config       : Load/Save of configuration via TFTP
Firmware     : Download of firmware via TFTP
PTP          : IEEE1588 Precision Time Protocol
Loop Protect : Loop Protection
IPMC         : MLD/IGMP Snooping
Fault        : Fault Alarm Configuration
Event        : Event Selection
DHCPServer   : DHCP Server Configuration
Ring         : Ring Configuration
Chain        : Chain Configuration
RCS          : Remote Control Security
Fastrecovery : Fast-Recovery Configuration
SFP          : SFP Monitor Configuration
DeviceBinding: Device Binding Configuration
MRP          : MRP Configuration
Modbus       : Modebus TCP Configuration
```

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]

IP

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

Port

Port>	Configuration [<port_list>] [up|down]
	State [<port_list>] [enable|disable]
	Mode [<port_list>] [auto|10hdx|10fdx|100hdx|100fdx|1000fdx|sfp_auto_ams]
	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>] [up|down]
	VeriPHY [<port_list>]
	SFP [<port_list>]

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>]
	PVID [<port_list>] [<vid>|none]
	FrameType [<port_list>] [all|tagged|untagged]
	IngressFilter [<port_list>] [enable|disable]
	tx_tag [<port_list>] [untag_pvid|untag_all|tag_all]
	PortType [<port_list>] [unaware|c-port|s-port|s-custom-port]
	EtypeCustomSport [<etype>]
	Add <vid>|<name> [<ports_list>]
	Forbidden Add <vid>|<name> [<port_list>]
	Delete <vid>|<name>
	Forbidden Delete <vid>|<name>
	Forbidden Lookup [<vid>] [(name <name>)]
	Lookup [<vid>] [(name <name>)] [combined|static|nas|all]
	Name Add <name> <vid>
	Name Delete <name>
	Name Lookup [<name>]
	Status [<port_list>] [combined|static|nas|mstp|all|conflicts]

Private VLAN

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

Security

Security >	Switch Switch security setting
	Network Network security setting
	AAA Authentication, Authorization and Accounting setting

Security Switch

Security/switch>	Password <password>
	Auth Authentication
	SSH Secure Shell
	HTTPS Hypertext Transfer Protocol over Secure Socket Layer
	RMON Remote Network Monitoring

Security Switch Authentication

Security/switch/auth>	Configuration
	Method [console|telnet|ssh|web] [none|local|radius] [enable|disable]

Security Switch SSH

Security/switch/ssh>	Configuration
	Mode [enable|disable]

Security Switch HTTPS

Security/switch/ssh>	Configuration
	Mode [enable|disable]

Security Switch RMON

Security/switch/rmon>	Statistics Add <stats_id> <data_source>
	Statistics Delete <stats_id>
	Statistics Lookup [<stats_id>]
	History Add <history_id> <data_source> [<interval>] [<buckets>]
	History Delete <history_id>
	History Lookup [<history_id>]
	Alarm Add <alarm_id> <interval> <alarm_variable> [absolute|delta]<rising_ threshold> <rising_event_index> <falling_threshold> <falling_event_index> [rising|falling|both]
	Alarm Delete <alarm_id>
	Alarm Lookup [<alarm_id>]

Security Network

Security/Network>	Psec Port Security Status
	NAS Network Access Server (IEEE 802.1X)
	ACL Access Control List
	DHCP Dynamic Host Configuration Protocol

Security Network Psec

Security/Network/ Psec>	Switch [<port_list>]
	Port [<port_list>]

Security Network NAS

Security/Network/NAS>	Configuration [<port_list>]
	Mode [enable|disable]
	State [<port_list>] [auto|authorized|unauthorized|macbased]
	Reauthentication [enable|disable]
	ReauthPeriod [<reauth_period>]
	EapolTimeout [<eapol_timeout>]
	Agetime [<age_time>]
	Holdtime [<hold_time>]
	Authenticate [<port_list>] [now]
	Statistics [<port_list>] [clear|eapol|radius]

Security Network ACL

Security/Network/ACL>	Configuration [<port_list>]
	Action [<port_list>] [permit|deny] [<rate_limiter>][<port_redirect>] [<mirror>] [<logging>] [<shutdown>]
	Policy [<port_list>] [<policy>]
	Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]
	Add [<ace_id>] [<ace_id_next>][(port <port_list>)] [(policy <policy> <policy_bitmask>)][<tagged>] [<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_redirect>] [<mirror>] [<logging>][<shutdown>]
	Delete <ace_id>
	Lookup [<ace_id>]
	Clear
	Status [combined|static|loop_protect|dhcp|ptp|ipmc|conflicts]
	Port State [<port_list>] [enable|disable]

Security Network DHCP

Security/Network/DHCP>	Configuration
	Mode [enable|disable]
	Server [<ip_addr>]
	Information Mode [enable|disable]
	Information Policy [replace|keep|drop]
	Statistics [clear]

Security Network AAA

Security/Network/AAA>	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>]
	Statistics [<server_index>]

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>]

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]

LLDP

LLDP>	Configuration [<port_list>]
	Mode [<port_list>] [enable|disable]
	Statistics [<port_list>] [clear]
	Info [<port_list>]

PoE

PoE>	Configuration [<port_list>]
	Mode [<port_list>] [disabled|poe|poe+]
	Priority [<port_list>] [low|high|critical]
	Mgmt_mode [class_con|class_res|al_con|al_res|lldp_res|lldp_con]
	Maximum_Power [<port_list>] [<port_power>]
	Status
	Primary_Supply [<supply_power>]
	Schedule Configuration [<port_list>]
	Schedule Mode [<port_list>] [enable|disable]
	Schedule Port [<port_list>] [enable|disable] [sun|mon|tue|wed|thu|fri|sat] [<hour>]
	AutoPing Configuration [<port_list>]
	AutoPing Log [clear]
	AutoPing Mode [enable|disable]
	AutoPing Port [<port>] [<ip_addr>] [<ping_interval>] [<retry>] [nothing|restart-forever|restart-once|power-on|power-off] [<reboot>] PoE>

QoS

QoS>	DSCP Map [<dscp_list>] [<class>] [<dpl>]
	DSCP Translation [<dscp_list>] [<trans_dscp>]
	DSCP Trust [<dscp_list>] [enable|disable]
	DSCP Classification Mode [<dscp_list>] [enable|disable]
	DSCP Classification Map [<class_list>] [<dpl_list>] [<dscp>]
	DSCP EgressRemap [<dscp_list>] [<dpl_list>] [<dscp>]
	Storm Unicast [enable|disable] [<packet_rate>]
	Storm Multicast [enable|disable] [<packet_rate>]
	Storm Broadcast [enable|disable] [<packet_rate>]
	QCL Add [<qce_id>] [<qce_id_next>] [<port_list>] [<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type>] [(etype [<etype>]) | (LLC [<DSAP>] [<SSAP>] [<control>]) | (SNAP [<PID>]) | (ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) | (ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])] [<class>] [<dp>] [<classified_dscp>]
	QCL Delete <qce_id>
	QCL Lookup [<qce_id>]
	QCL Status [combined|static|conflicts]
	QCL Refresh

Mirror

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

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>]

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]

Firmware

Firmware>	Load <ip_addr_string> <file_name>

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>]

PTP

PTP>	Configuration [<clockinst>]
	PortState <clockinst> [<port_list>] [enable|disable|internal]
	ClockCreate <clockinst> [<devtype>] [<twostep>] [<protocol>] [<oneway>] [<clockid>] [<tag_enable>] [<vid>] [<prio>]
	ClockDelete <clockinst> [<devtype>]
	DefaultDS <clockinst> [<priority1>] [<priority2>] [<domain>]
	CurrentDS <clockinst>
	ParentDS <clockinst>
	Timingproperties <clockinst> [<utcoffset>] [<valid>] [<leap59>] [<leap61>] [<timetrac>] [<freqtrac>] [<ptptimescale>] [<timesource>]
	PTP PortDataSet <clockinst> [<port_list>] [<announceintv>] [<announceto>] [<syncintv>] [<delaymech>] [<minpdelayreqintv>] [<delayasymmetry>] [<ingressLatency>]
	LocalClock <clockinst> [update|show|ratio] [<clockratio>]
	Filter <clockinst> [<def_delay_filt>] [<period>] [<dist>]
	Servo <clockinst> [<displaystates>] [<ap_enable>] [<ai_enable>] [<ad_enable>] [<ap>] [<ai>] [<ad>]
	SlaveTableUnicast <clockinst>
	UniConfig <clockinst> [<index>] [<duration>] [<ip_addr>]
	ForeignMasters <clockinst> [<port_list>]
	EgressLatency [show|clear]
	MasterTableUnicast <clockinst>
	ExtClockMode [<one_pps_mode>] [<ext_enable>] [<clockfreq>] [<vcxo_enable>]
	OnePpsAction [<one_pps_clear>]
	DebugMode <clockinst> [<debug_mode>]
	Wireless mode <clockinst> [<port_list>] [enable|disable]
	Wireless pre notification <clockinst> <port_list>
	Wireless delay <clockinst> [<port_list>] [<base_delay>] [<incr_delay>]

IPMC

IPMC>	Configuration [igmp]
	Mode [igmp] [enable|disable]
	Flooding [igmp] [enable|disable]
	VLAN Add [igmp] <vid>
	VLAN Delete [igmp] <vid>
	State [igmp] [<vid>] [enable|disable]
	Querier [igmp] [<vid>] [enable|disable]
	Fastleave [igmp] [<port_list>] [enable|disable]
	Router [igmp] [<port_list>] [enable|disable]
	Status [igmp] [<vid>]
	Groups [igmp] [<vid>]
	Version [igmp] [<vid>]

Fault

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

Event

Event>	Configuration
	Syslog SystemStart [enable|disable]
	Syslog PowerStatus [enable|disable]
	Syslog SnmpAuthenticationFailure [enable|disable]
	Syslog RingTopologyChange [enable|disable]
	Syslog Port [<port_list>] [disable|linkup|linkdown|both]
	SMTP SystemStart [enable|disable]
	SMTP PowerStatus [enable|disable]
	SMTP SnmpAuthenticationFailure [enable|disable]
	SMTP RingTopologyChange [enable|disable]
	SMTP Port [<port_list>] [disable|linkup|linkdown|both]

DHCPServer

DHCPServer>	Mode [enable|disable]
	Setup [<ip_start>] [<ip_end>] [<ip_mask>] [<ip_router>] [<ip_dns>] [<ip_tftp>] [<lease>] [<bootfile>]

Ring

Ring>	Mode [enable|disable]
	Master [enable|disable]
	1stRingPort [<port>]
	2ndRingPort [<port>]
	Couple Mode [enable|disable]
	Couple Port [<port>]
	Dualhoming Mode [enable|disable]
	Dualhoming Port [<port>]

SFP

SFP>	syslog [enable|disable]
	temp [<temperature>]
	Info

Technical Specifications

ComNet Switch Model	CNGE12FX4TX8MS/TS	CNGE12FX4TX8MSPOE/TS
Physical Ports		
RJ-45 ports	8 10/100/1000Base-T(X) Auto MDI/ MDIX	8 10/100/1000Base-T(X) Auto MDI/ MDIX with PSE Ports
SFP ports	4 100/1000Base-X	
Technology		
Ethernet Standards	IEEE 802.3 for 10Base-T IEEE 802.3u for 100Base-TX and 100Base-FX IEEE 802.3ab for 1000Base-T IEEE 802.z for 1000Base-X IEEE 802.3x for Flow control IEEE 802.3ad for LACP (Link Aggregation Control Protocol) IEEE 802.1p for COS (Class of Service) IEEE 802.1Q for VLAN Tagging IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol) IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol) IEEE 802.1x for Authentication IEEE 802.1AB for LLDP (Link Layer Discovery Protocol)	
PoE Support	No PoE Support	IEEE 802.3at PoE specification (up to 30 Watts per port for PSE). Total power budget is 240 Watts
MAC Table	8k	
Priority Queues	8	
Processing	Store-and-Forward	
Switch Properties	Switching latency: 7 us Switching bandwidth: 24 Gbps Max. Number of Available VLANs: 256 IGMP multicast groups: 128 for each VLAN Port rate limiting: User Define	
Jumbo frame	Up to 9.6K Bytes	

ComNet Switch Model	CNGE12FX4TX8MS/TS	CNGE12FX4TX8MSPOE/TS
Security Features	Device Binding security feature Enable/disable ports, MAC based port security Port based network access control (802.1x) Single 802.1x and Multiple 802.1x MAC-based authentication QoS assignment Guest VLAN MAC address limit TACACS+ VLAN (802.1Q) to segregate and secure network traffic Radius centralized password management SNMPv3 encrypted authentication and access security Https / SSH enhance network security Web and CLI authentication and authorization IP source guard	
Software Features	IEEE 1588v2 clock synchronization IEEE 802.1D Bridge, auto MAC address learning/aging and MAC address (static) MSTP (RSTP/STP compatible) 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 Modbus TCP IGMP v2/v3 Snooping IP-based bandwidth management Application-based QoS management Port configuration, status, statistics, monitoring, security DHCP Server/Client/Relay SMTP Client DOS/DDOS auto prevention	
Network Redundancy	C-Ring MSTP (RSTP/STP compatible) Legacy Ring G.8032 ERPS	
RS-232 Serial Console Port	RS-232 in RJ-45 connector with console cable. 115200bps, 8, N, 1	

ComNet Switch Model	CNGE12FX4TX8MS/TS	CNGE12FX4TX8MSPOE/TS
LED indicators		
Power (PWR)	Green: Power indicator	
Ring Master (R.M.)	Green: Indicates that the system is operating in C-Ring Master mode	
C-Ring (Ring)	Green: Indicates that the system operating in C-Ring mode Green Blinking: Indicates that the Ring is broken.	
RJ-45 Port	Green for Link/Act indicator	
SFP Port	Green for port Link/Act.	
PoE	N/A	Blue : PoE enabled LED × 8
Power		
Power Input	12-24 VDC from traffic detector rack	
PoE Power Input	N/A	48-57 VDC (2-pin screw terminal connector on front panel)
Power consumption	18 Watts (Typ., PoE Load Not Included)	
Overload current protection	Present	
Physical Characteristic		
Enclosure	NEMA TS2 traffic detector rack design	
Dimension (W x D x H)	2.23 × 4.51 × 8.08 in (5.67 × 11.45 × 20.53 cm)	
Weight	750 g	
Environmental		
Storage Temperature	-40° to 85°C	
Operating Temperature	-40° to +75°C	
Operating Humidity	5% to 97% Non-condensing	

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

comnet
Communication Networks

3 CORPORATE DRIVE | DANBURY, CT 06810 | USA
T: 203.796.5300 | F: 203.796.5303 | TECH SUPPORT: 1.888.678.9427 | INFO@COMNET.NET
8 TURNBERRY PARK ROAD | GILDERSOME | MORLEY | LEEDS, UK LS27 7LE
T: +44 (0)113 307 6400 | F: +44 (0)113 253 7462 | INFO-EUROPE@COMNET.NET