comnet
Communication Networks

INSTALLATION AND OPERATION MANUAL

RLXE4GE24MODMS

HARDENED LAYER 3 MANAGED 10 GIGABIT MODULAR ETHERNET SWITCH

The ComNet RLXE4GE24MODMS is a Layer-3 modular managed redundant ring configurable Ethernet switch. It has four slots that can accommodate individual modules that feature different combinations of SFP and electrical TX ports. One of the slots can accommodate a 10 gigabit module with either 2 or 4 10 Gbps or 1 Gbps SFP ports. The switch is designed for security, ITS, power substation and rolling stock applications, and is fully compliant with the requirement of IEC 61850-3 and IEEE 1613 as well as NEMA TS1/TS2. The RLXE4GE24MODMS switch supports multiple Ethernet Redundancy protocols, including C-Ring (recovery time < 30ms over 250 units of connection) and MSTP (RSTP/STP compatible). This switch can protect critical applications from network interruptions or temporary malfunctions with its fast recovery technology. This environmentally hardened switch is designed for direct deployment in difficult out-of-plant or roadside operating environments.

Contents

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:

» RLXE4GE24MODMS 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 RLXE4GE24MODMS is a Layer-2/3 modular managed redundant ring Ethernet switch with 4 slots. This switch is designed for industrial applications, power substation applications and rolling stock applications, RLXE4GE24MODMS is compliant with the requirement of IEC 61850-3 and IEEE 1613. RLXE4GE24MODMS supports Ethernet Redundancy protocol, C-Ring (recovery time < 30ms over 250 units of connection) and MSTP (RSTP/STP compatible). It can protect your mission-critical applications from network interruptions or temporary malfunctions with its fast recovery technology. Wide operating temperature ranges of -40 to +75°C (when the proper 10 Gbps module is in use) are supported.

RLXE4GE24MODMS can also be managed centrally and conveniently by using eConsole software or via the Web-based interface, Telnet or console (CLI) configuration. The RLXE4GE24MODMS switch is one of the most reliable choices for highly-managed and Fiber Ethernet power substation and rolling stock applications..

Software Features

» Designed for power substation / Railway application and fully compliant with the requirement of IEC 61850-3 and IEEE 1613
» Modular design makes network planning and upgrades easy
» Supports Layer 3 static routing, and RIP function
» C-Ring (recovery time < 30ms over 250 units of connection)
» MSTP (RSTP/STP compatible) for Ethernet Redundancy
» 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
» 10K Bytes Jumbo Frame
» SFP ports support DDM function
» Multiple notification for warning of unexpected event
» Web-based Telnet, Console (CLI), and Windows utility (eConsole) configuration
» LLDP Protocol

Hardware Features

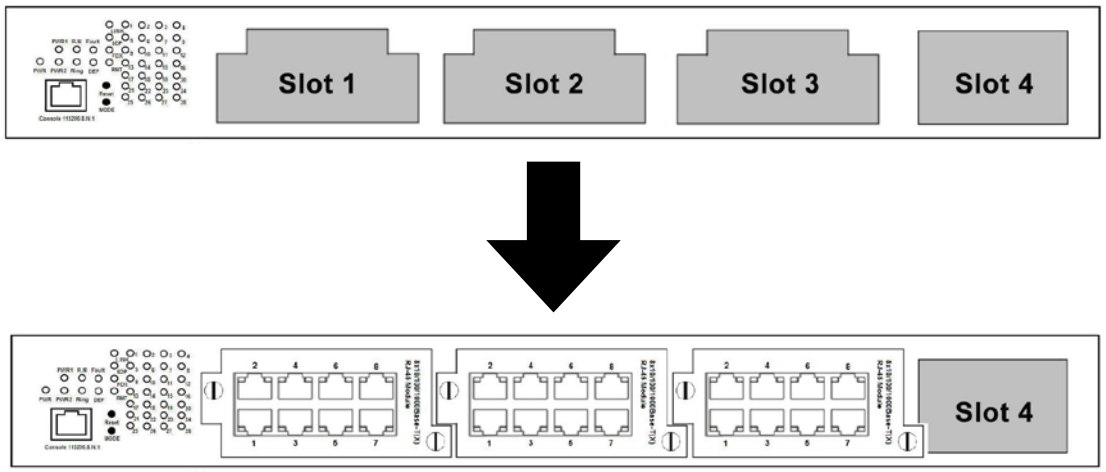
- » Supports redundant Power Inputs (Modular DC/AC Power, supports two power modules in redundant operation)
- » Supports maximum 3 slots 8 x 10/100/1000Base-T(X) RJ-45 Module
- » Supports maximum 3 slots 8 x 100/1000Base-X SFP Module
- » Supports maximum 1 slot 2/4 x 10G SFP+ Module or 2/4 x 1G SFP+ Module
- » 19 inch rack mountable design
- » Operating Temperature: -40 to +75° C (Proper 10 Gbps SFP+ module used) or -40 to 85° C (10 Gbps SFP+ module absent)
- » Storage Temperature: -40 to 85° C
- » Operating Humidity: 5% to 95%, non-condensing
- » Console Port (RJ45) : Baud Rate 115200 bps, 8, N, 1
- » Dimensions : 440(W) × 325 (D) × 44 (H) mm

Hardware Installation

Installing RJ-45 Module in RLXE4GE24MODMS

Each RLXE4GE24MODMS Switch supports a maximum of three RJ-45 Modules. To install the module users must turn off the RLXE4GE24MODMS Power and plug-in the RJ-45 Module into Slot 1 ~ Slot 3.

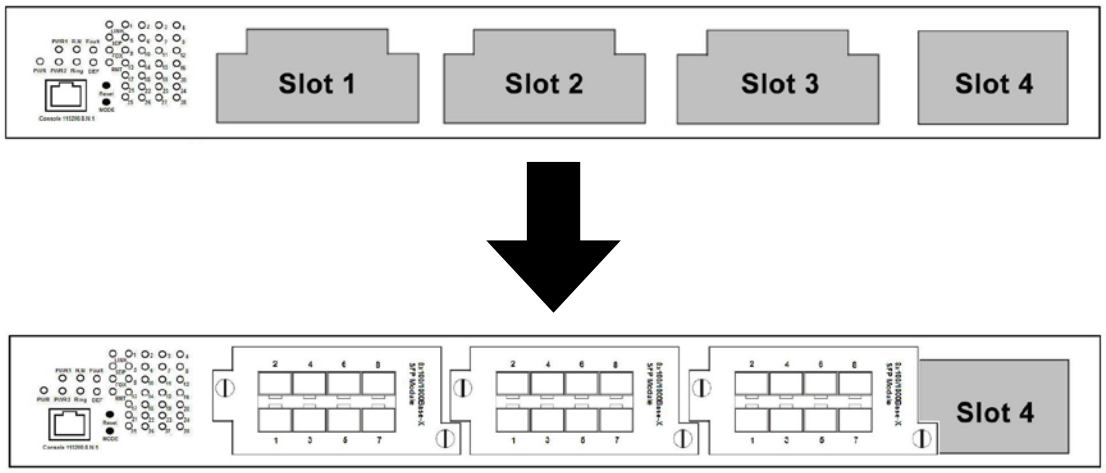
Once installed turn on the power.



Installing SFP Module in RLXE4GE24MODMS

Each RLXE4GE24MODMS Switch supports a maximum of three SFP Modules. To install the module users must turn off the RLXE4GE24MODMS Power and plug-in the SFP Module into Slot 1 ~ Slot 3.

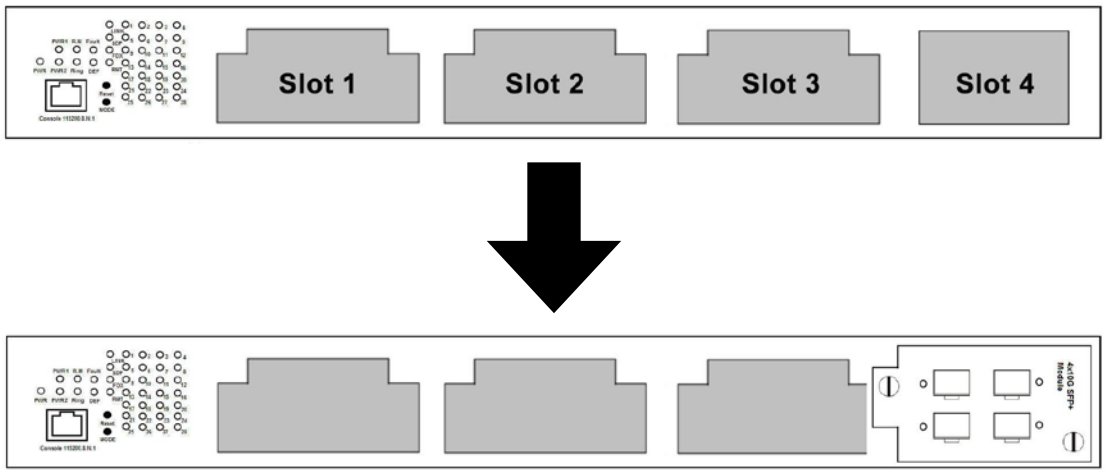
Once installed turn on the power.



Installing 10 Gbps SFP+ Module in RLXE4GE24MODMS

Each RLXE4GE24MODMS Switch supports a maximum of one 10G SFP+ Module. To install the module users must turn off the RLXE4GE24MODMS Power and plug-in the SFP Module into Slot 4.

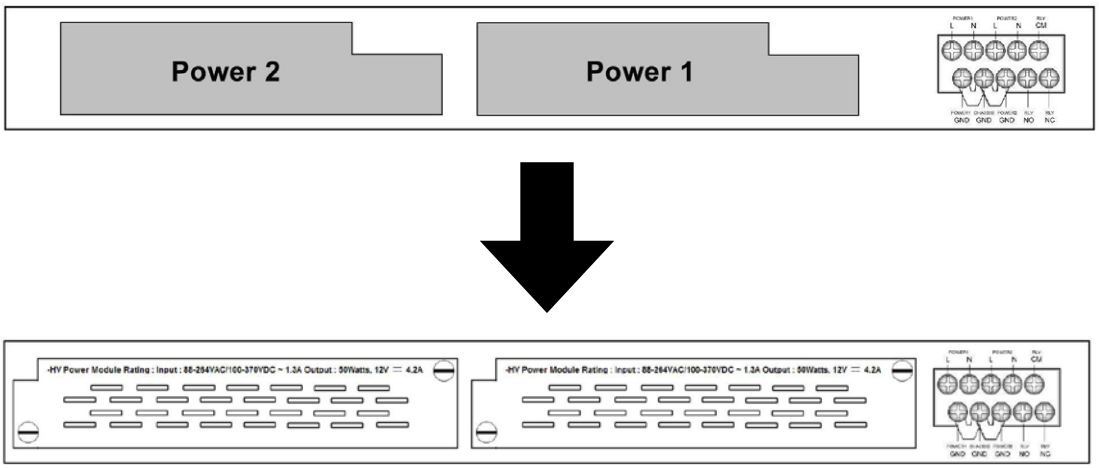
Once installed turn on the power.



Installing Power Module in RLXE4GE24MODMS

Each RLXE4GE24MODMS Switch supports a maximum of two Power Modules. To install the power module users must turn off the RLXE4GE24MODMS Power and plug-in the Power Module to Slot 1 or or Slot 2 (Either one or two modules can be installed).

Once installed turn on the power.

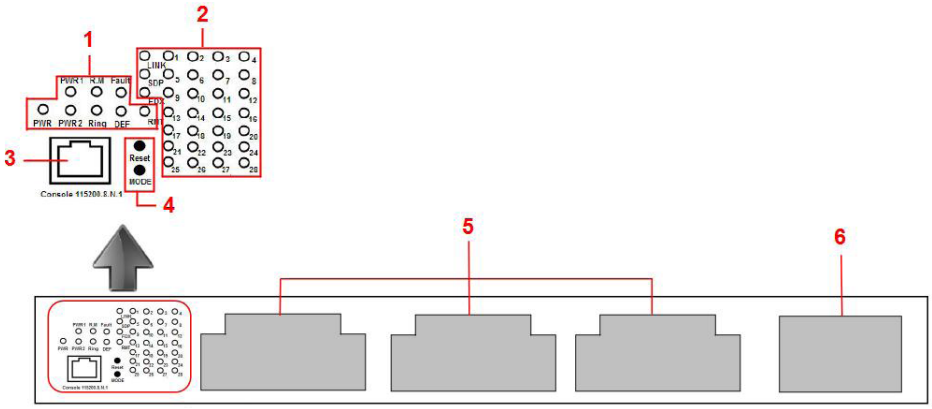


Hardware Overview

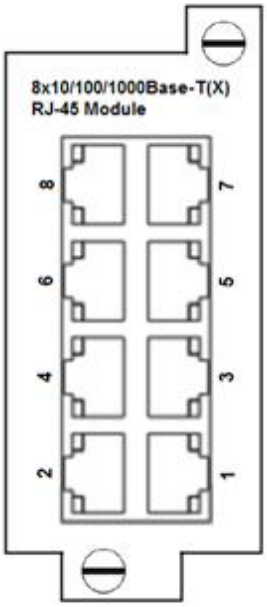
Front Panel

RLXE4GE24MODMS supports four different module types.

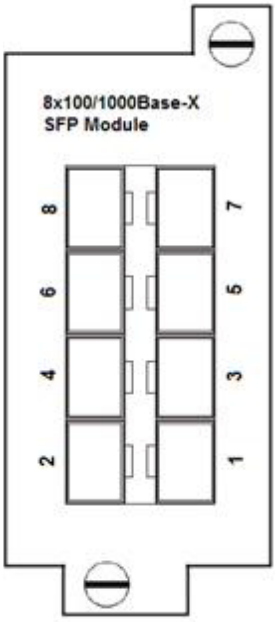
Module	Description
RLXE4GE24MODMS/HV	RLXE4GE24MODMS Chassis With Dual High Voltage Power Supplies
RLXE4GE24MODMS/LV	RLXE4GE24MODMS Chassis With Dual Low Voltage Power Supplies
RLXE4GE24MODMS/8TX	8 x 10/100/1000Base-T(X)
RLXE4GE24MODMS/8SFP	8 x 100 / 1000 Base-X
RLXE4GE24MODMS/XE2SFP	2 x 10G SFP+
RLXE4GE24MODMS/XE4SFP	4 x 10G SFP+



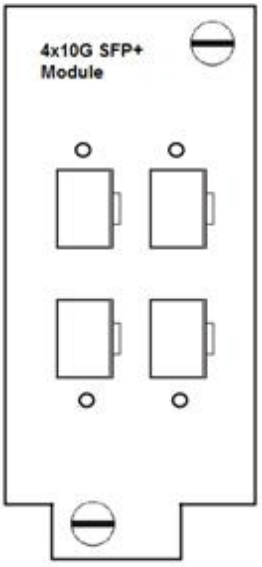
1. Front Panel LED Status:
   LED for PW1: When the PWR1 links, the green led will be light on.
   LED for PW2: When the PWR2 links, the green led will be light on.
   LED for PWR: This LED lights on when the power module is activated.
   LED for R.M. (Ring master): When the LED lights on, this switch is designated as the ring master of the C-Ring topology.
   LED for Ring: When the LED light on, the C-Ring is activated.
   LED for Fault: Indicates unexpected event occurred.
   LED for DEF: System resets to default configuration.
   LED for RMT: System resets to default configuration.
2. Status by port LED , support three types LED Status .
   LINK Status : Port show link status
   SPD Status : Port LED show Speed status
   FDX Status : Port LED show Duplex status
3. Console port (RJ-45)
4. Buttons
   Reset Button : Push the button 3 seconds for reset; 5 seconds for factory default.
   Mode Button : Push the button to change the Port LED Mode .
5. RJ-45 / SFP Module Slot.
6. 10G SFP+ Module Slot.



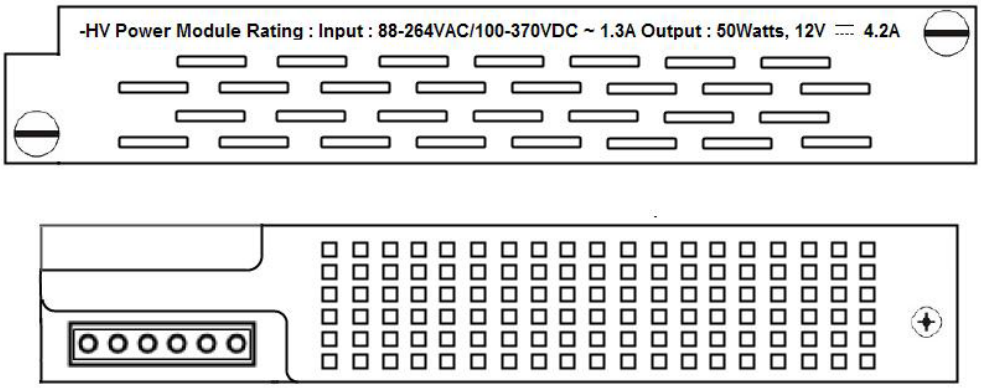
RJ-45 Module
8 × 10/100/1000Base-T(X)



SFP Module
8 × 100/1000Base-X SFP



10 Gbps Module
4 × 10 Gigbit SFP

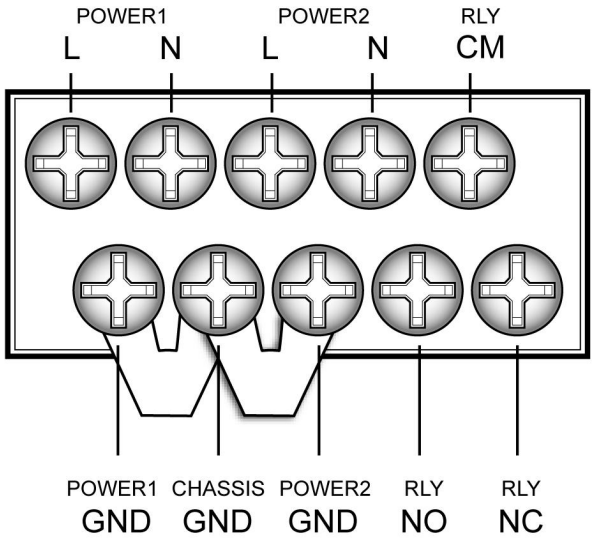


Power Module

Power Panel

RLXE4GE24MODMS are redundant power switches with support for two power inputs.

Note: At the factory, power GND and chassis GND are connected as shown in the picture below.



RLY CM: Relay Common
RLY NO: Relay Normally Open
RLY NC: Relay Normally Closed

Rack mount kit assembly

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

Ethernet Cables

The RLXE4GE24MODMS 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.

10/100 Base-T(X) 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

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 RLXE4GE24MODMS 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

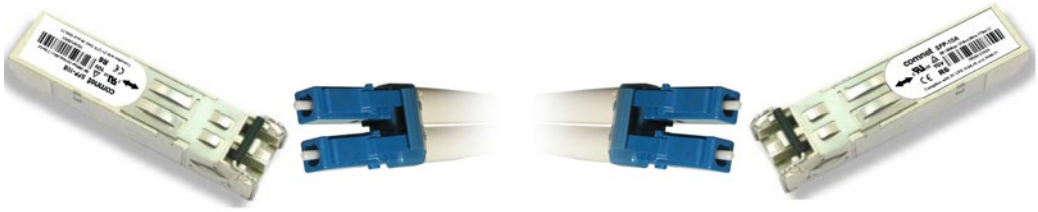
1000 Base-T MDI/MDI-X pins assignment

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

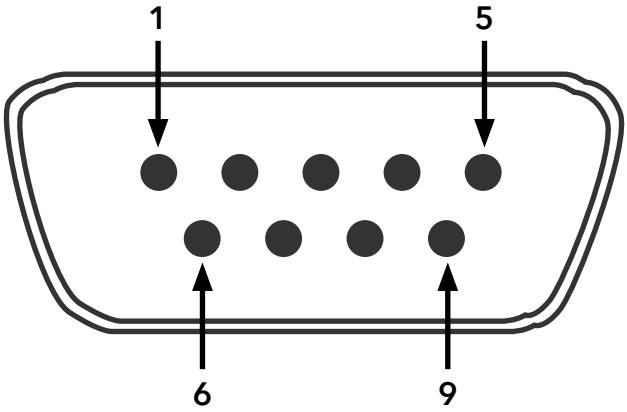
The Switch has fiber optical ports with SFP connectors. The fiber optical ports are in 100/1000Base-X multi-mode (0 to 550M, 850 nm with 50/125 μm, 62.5/125 μm fiber) , single-mode and 10 Gbps SFP+ Module with LC connector. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.



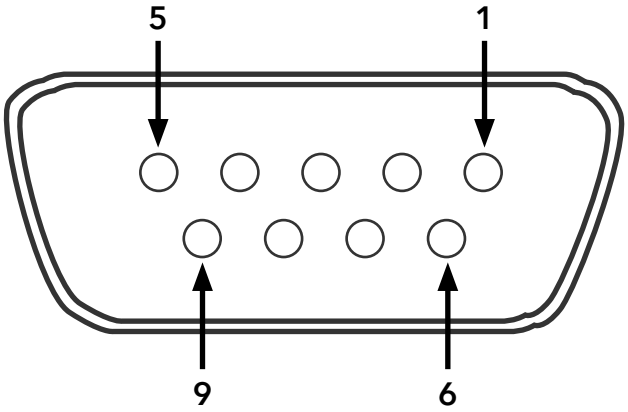
Switch A *Fiber Cord* *Switch B*

Console Cable

RLXE4GE24MODMS switches can be managed by the console port. The DB-9 to RJ-45 cable can be found in the package. You can connect them to a PC via a RS-232 cable with DB-9 female connector and the other end (RJ-45 connector) connects to console port of the switch.



DB-9 Male



DB-9 Female

PC pin out (male) assignment	RS-232 with DB-9 female connector	DB-9 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. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

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

Preparing for Web Management

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

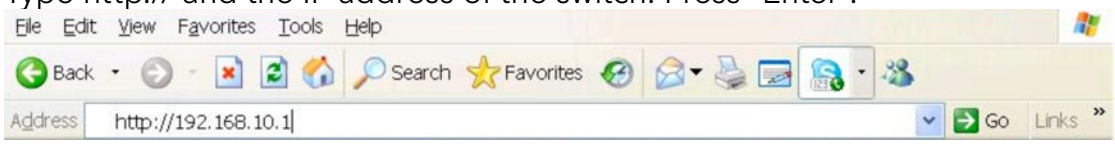
Default Gateway: **192.168.10.254**

User Name: **admin**

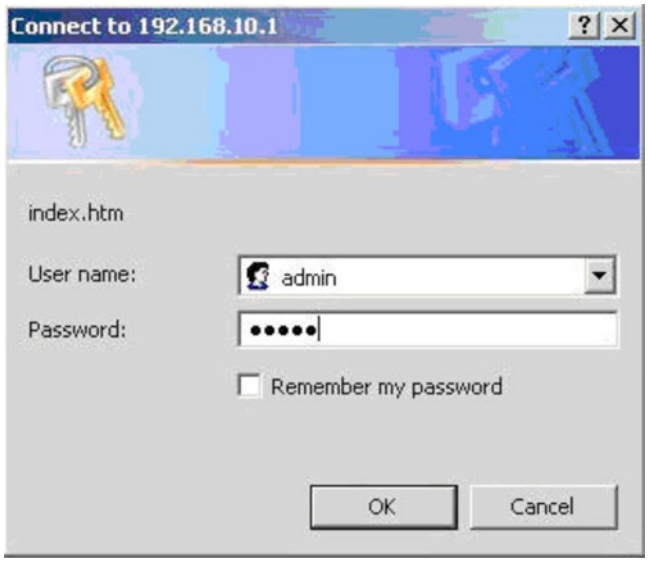
Password: **admin**

System Login

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



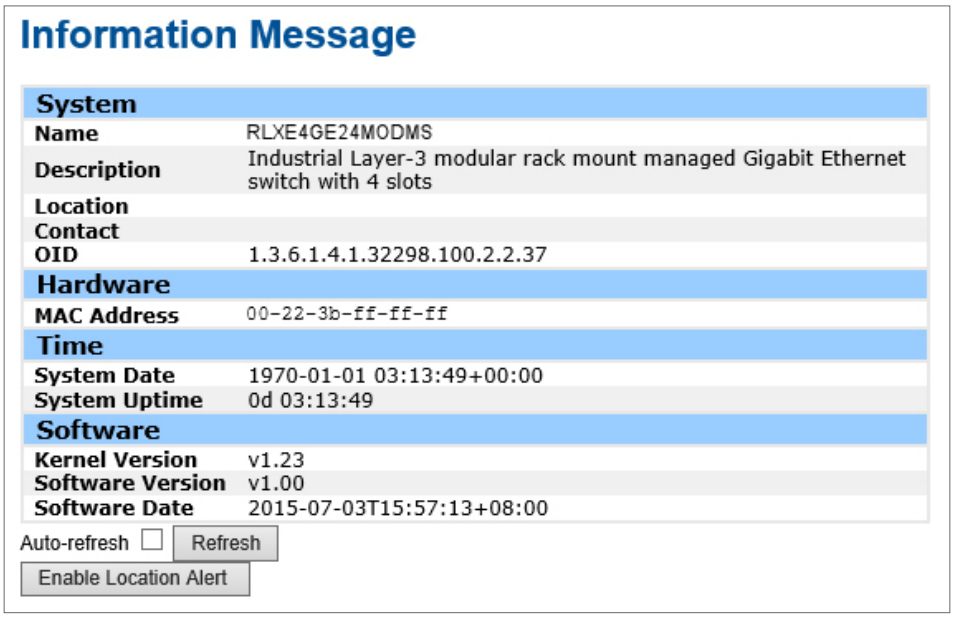
3. The login screen appears.



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

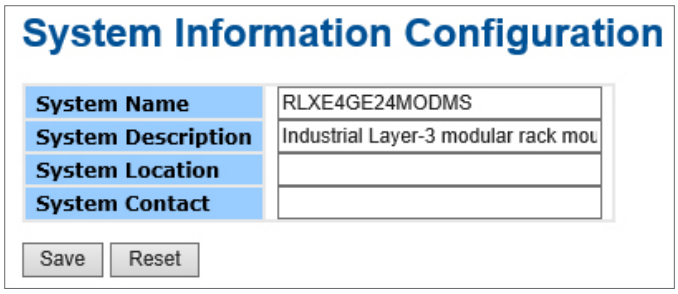


Main interface

Basic Setting

System Information

The switch system information is provided here.

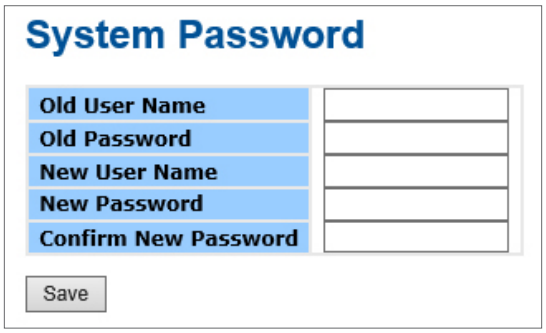


System Information interface

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

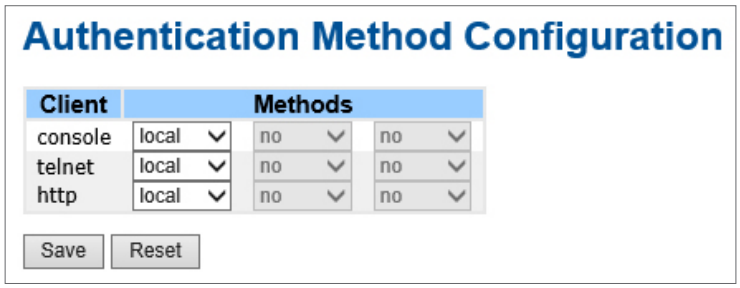
This page allows you to configure the system password required to access the web pages or log in from CLI.



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.

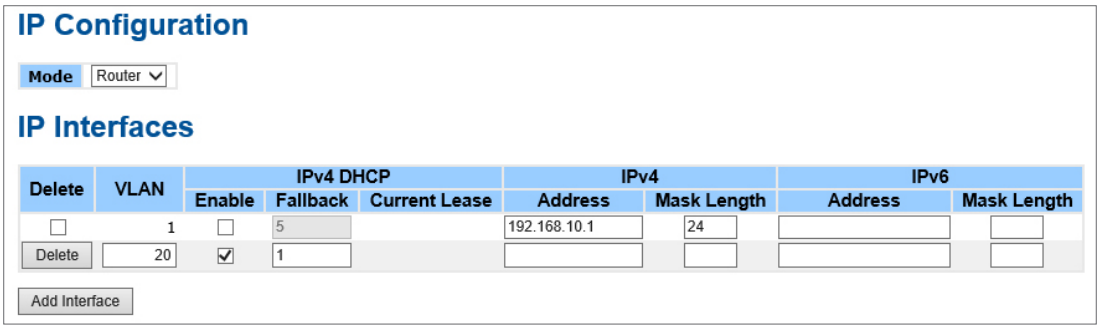


Label	Description
Client	The management client for which the configuration below applies.
Authentication Method	Authentication Methods can be set to one of the following values: none: authentication is disabled and login is not possible. local: use the local user database on the switch for authentication. radius: use a remote RADIUS server for authentication. tacas: use a remote TACAS server for authentication
Fallback	Two additional fallback options are also available by using the additional Methods selection boxes. This is only possible if the first 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.

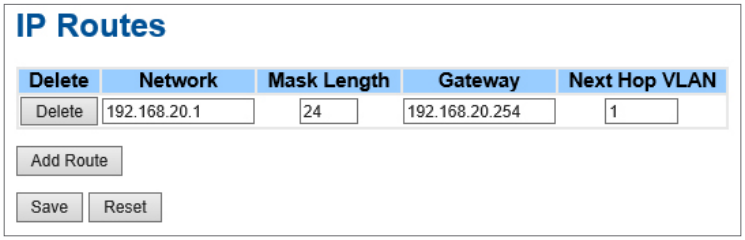
IP Setting

Configure IP basic settings, control IP interfaces and IP routes.

The maximum number of interfaces supported is 128 and the maximum number of routes is 1024.



Label	Description
Mode	Configure whether the IP stack should act as a Host or a Router. In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces.
Delete	Select this option to delete an existing IP interface.
VLAN	The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating an new interface.
IPv4 DHCP Enable	The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating an new interface.
IPv4 DHCP Fallback Timeout	The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.
IPv4 DHCP Current Lease	For DHCP interfaces with an active lease, this column show the current interface address, as provided by the DHCP server.
IPv4 Address	The IPv4 address of the interface in dotted decimal notation. If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.
IPv4 Mask	The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address. If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.
IPv6 Address	The IPv6 address of the interface. A 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. The field may be left blank if IPv6 operation on the interface is not desired.
IPv6 Mask	The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for a IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.



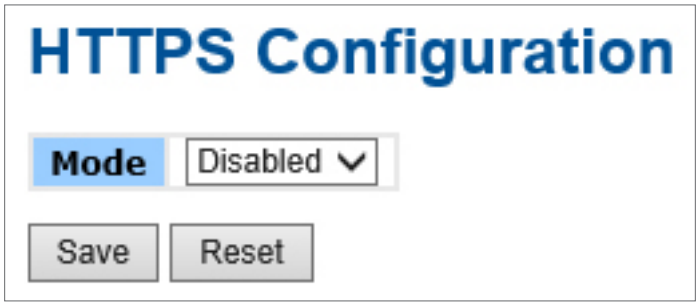
Label	Description
Delete	Select this option to delete an existing IP route.
Network	The destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0or IPv6 :: notation.
Mask Length	The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).
Gateway	The IP address of the IP gateway. Valid format is dotted decimal notationor a valid IPv6 notation. Gateway and Network must be of the same type.
Next Hop VLAN (Only for IPv6)	The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway. If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.

RIP

The user can configure RIP Function on this page.

Label	Description
Mode	Indicates the RIP mode operation. Possible modes are: Enabled: Enable RIP mode operation. Disabled: Disable RIP mode operation.

HTTPS

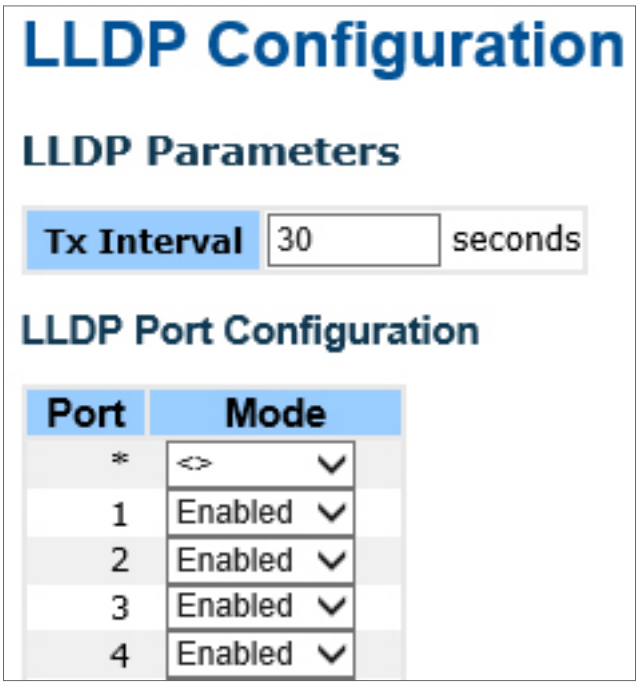


Label	Description
Mode	Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are: Enabled: Enable HTTPS mode operation. Disabled: Disable HTTPS mode operation.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

SSH

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

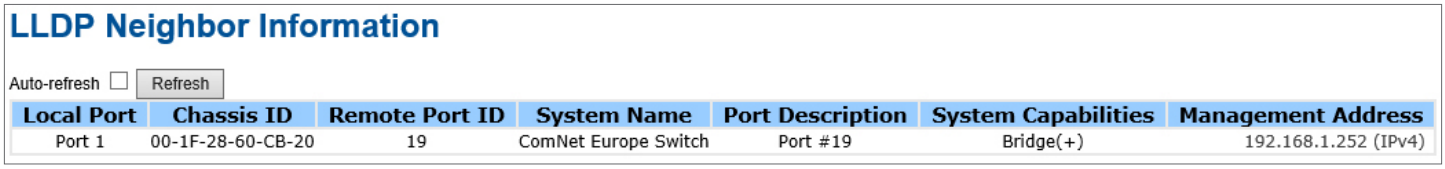
LLDP



LLDP Configuration

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

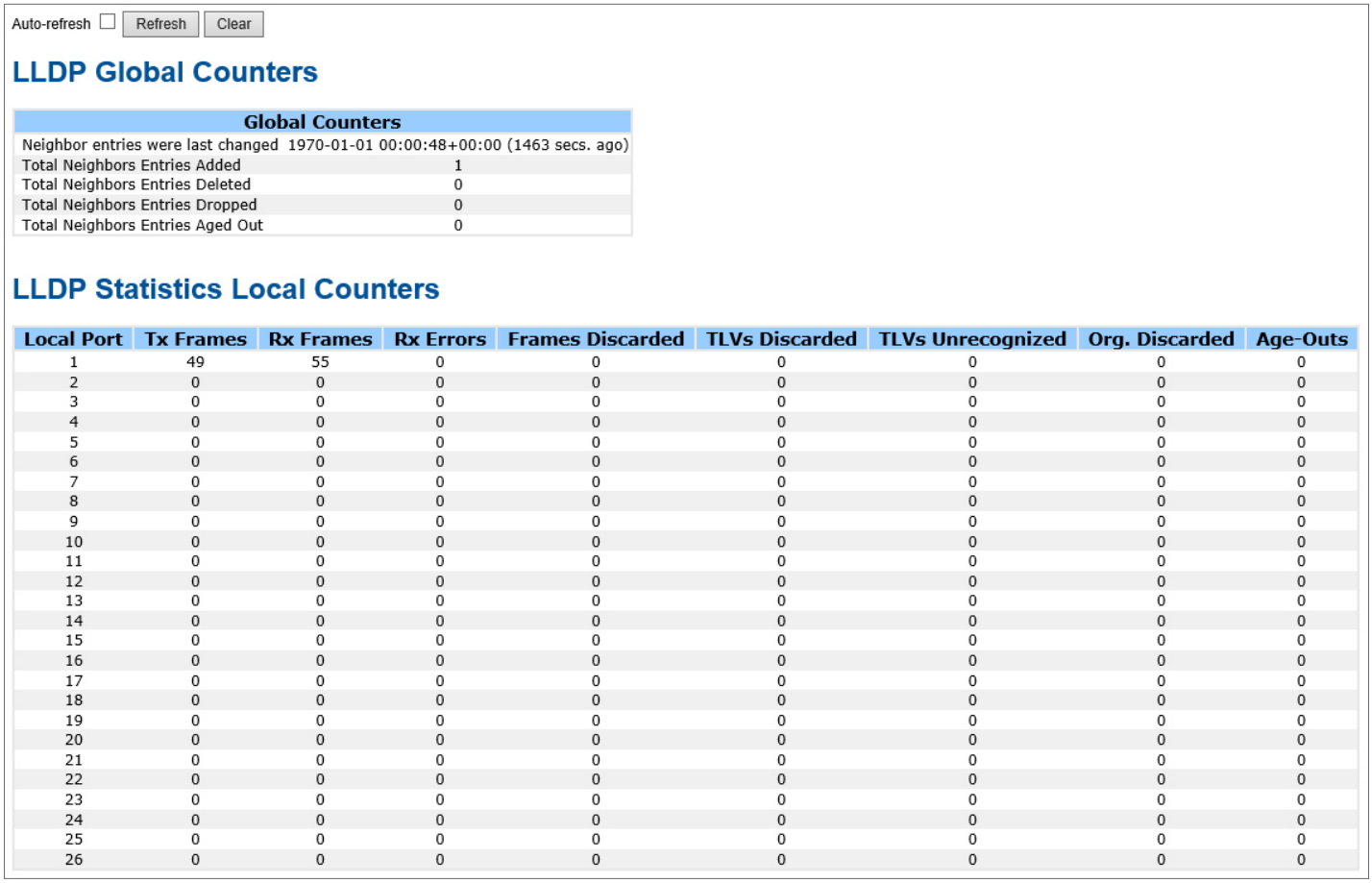
Label	Description
Port	The switch port number of the logical LLDP port.
Mode	Select LLDP mode. Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors. Enabled The switch will send out LLDP information, and will analyze LLDP information received 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:

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.



Auto-refresh ☐ Refresh Clear

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

This page provides an overview of all LLDP traffic.

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

Global Counters

Label	Description
Neighbor entries were last changed at	Shows the time 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.

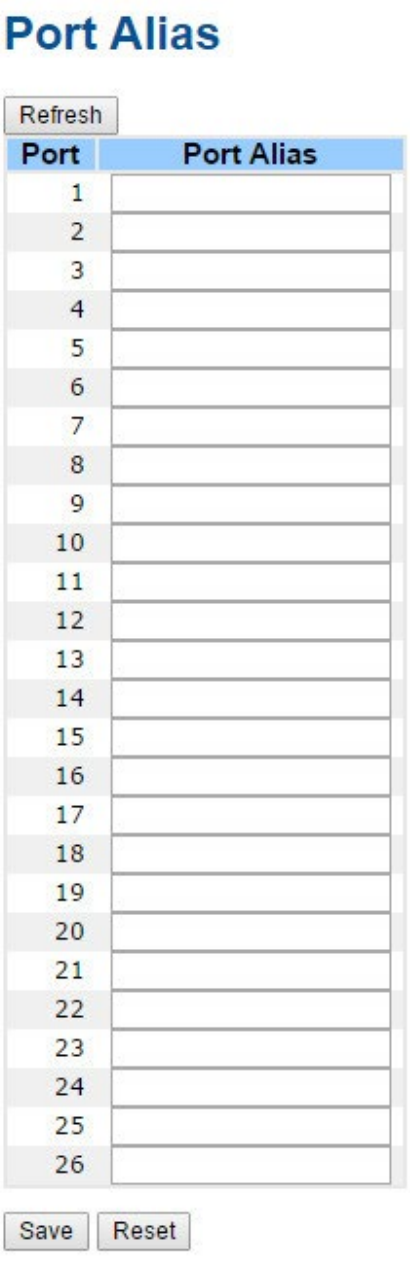
Modbus TCP

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

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

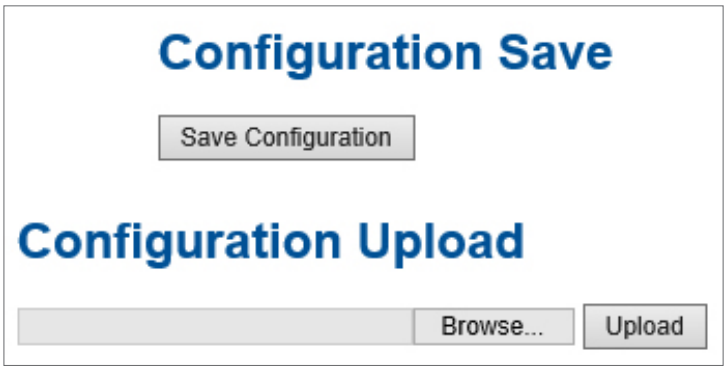
Port Alias

Configure the port alias name for each port.



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.

Backup/Restore Configuration



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

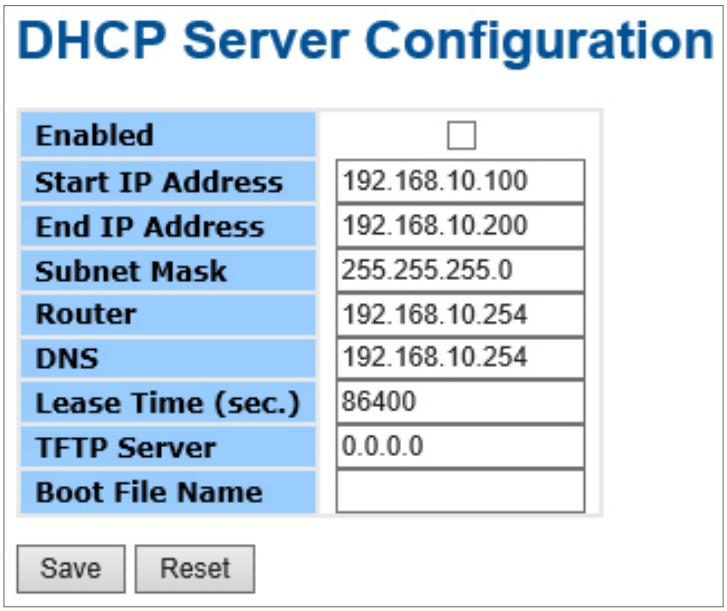
Firmware Update

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

DHCP Server

Setting

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

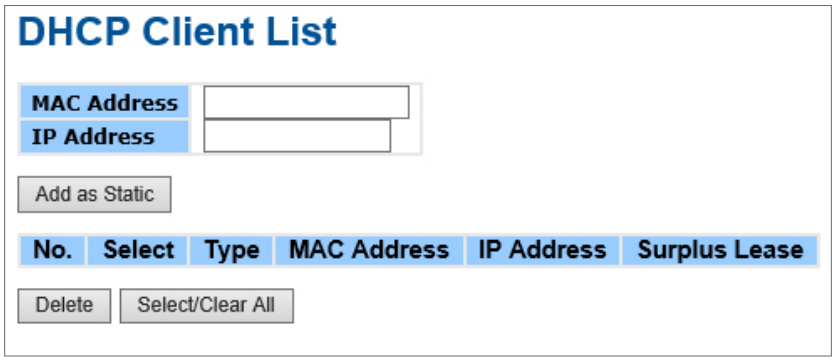


DHCP Dynamic Client List

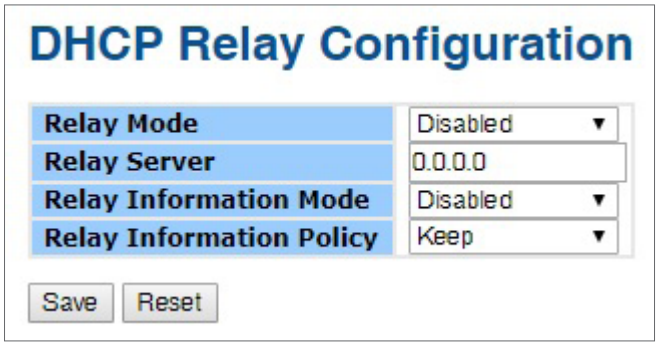
When the DHCP server function is activated, the system will collect the DHCP client information and display in here.

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 Relay Configuration



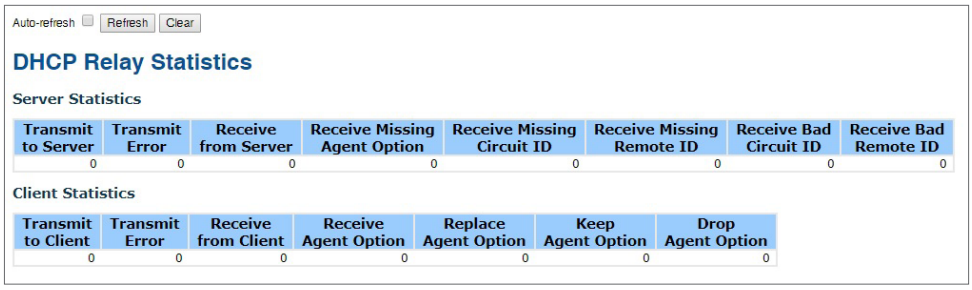
Configure DHCP Relay on this page.

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.
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 the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy 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.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

DHCP Relay Statistics

This page provides statistics for DHCP relay.



Server Statistics

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 Circuit 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.

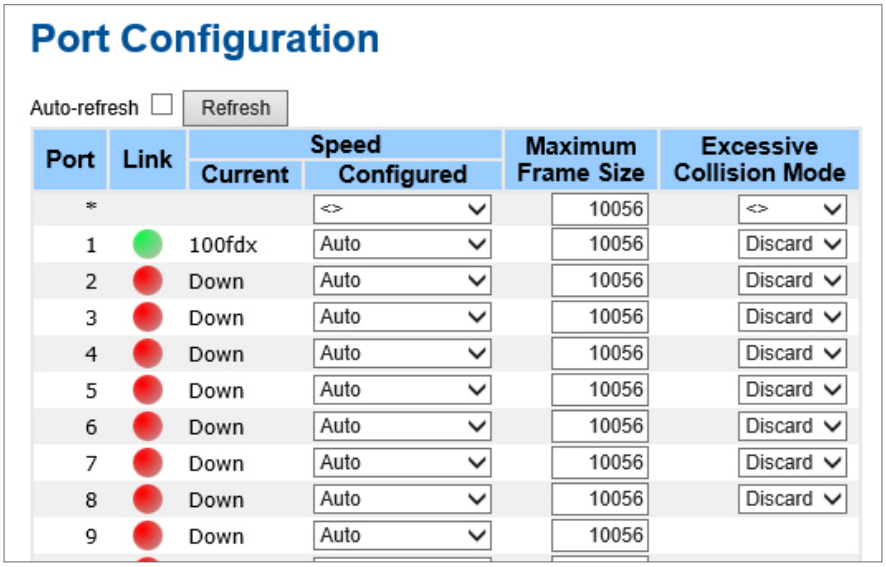
Client Statistics

Transmit to Client	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.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page immediately.
Clear	Clear all statistics.

Port Setting

Port Control

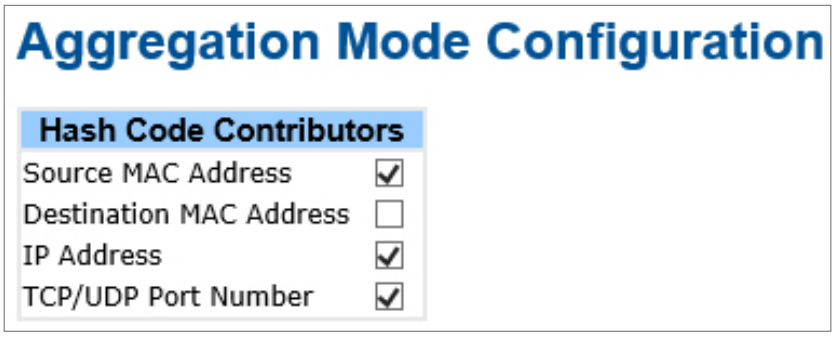
This page displays current port configurations. Ports can also be configured here.



Label	Description
Port	This is the logical port number for this row.
Link	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
Current Link Speed	Provides the current link speed of the port.
Configured Link Speed	Select any available link speed for the given switch port. Auto Speed selects the highest speed that is compatible with a link partner. Disabled disables the switch port operation. <> : configuration of all ports.
Maximum Frame	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 10056 bytes.
Excessive Collision Mode	Configure port transmit collision behavior. Discard: Discard frame after 16 collisions (default). Restart: Restart backoff algorithm after 16 collisions
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.

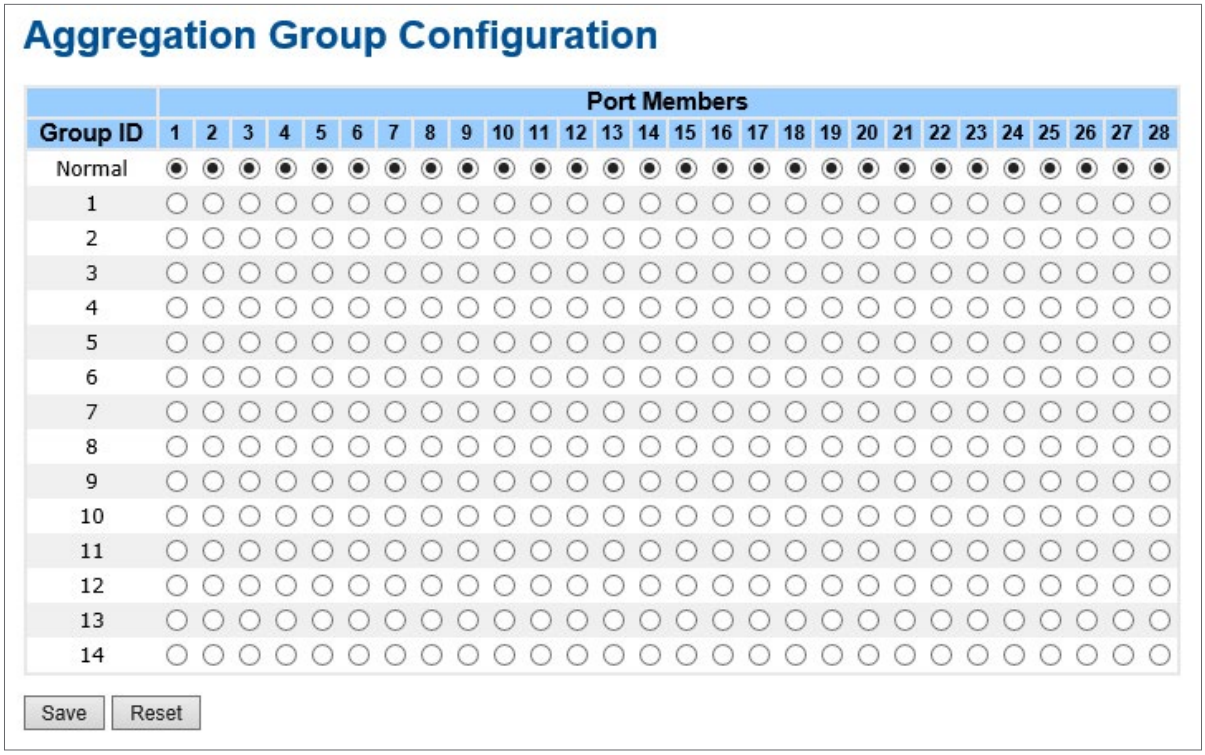
Port Trunk

Trunk Configuration



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

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

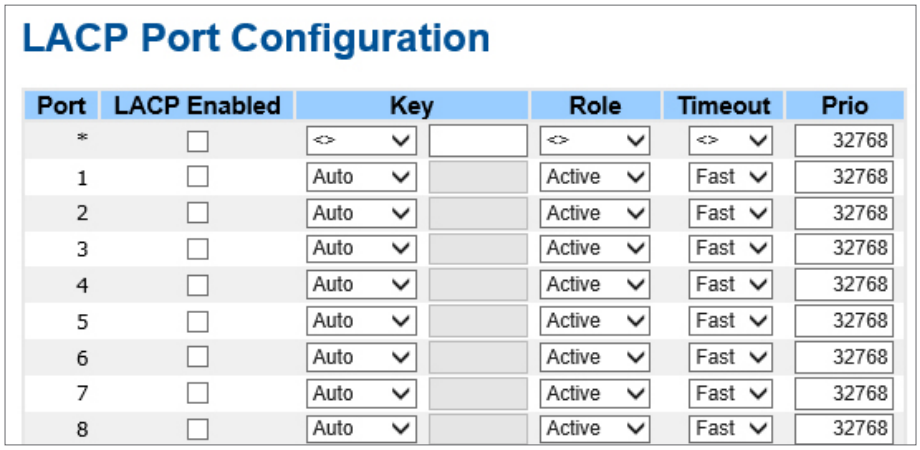


Label	Description
Group ID	Indicates the group ID for the settings contained in the same row. Group ID “Normal” indicates there is no aggregation. Only one group ID is valid per port.
Port Members	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation,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

LACP

Port Configuration

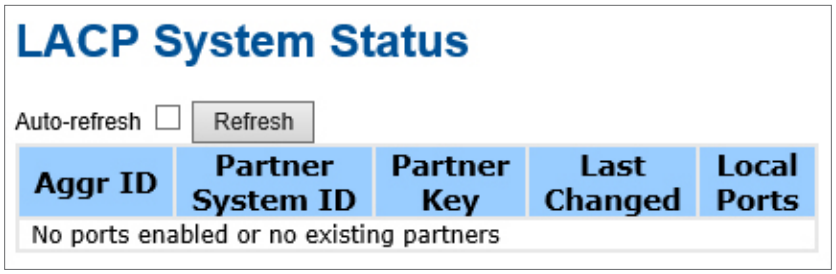
This page allows the user to inspect the current LACP port configurations, and possibly change them as well.



Label	Description
Port	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
LACP Enabled	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.
Key	The Key value incurred by the port, range 1-65535. The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
Role	The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).
Timeout	The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.
Prio	The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

LACP System Status

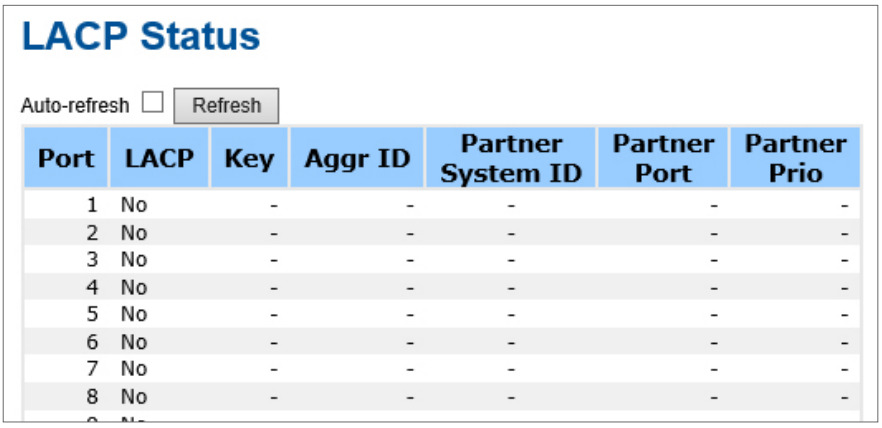
This page provides a status overview for all LACP instances.



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

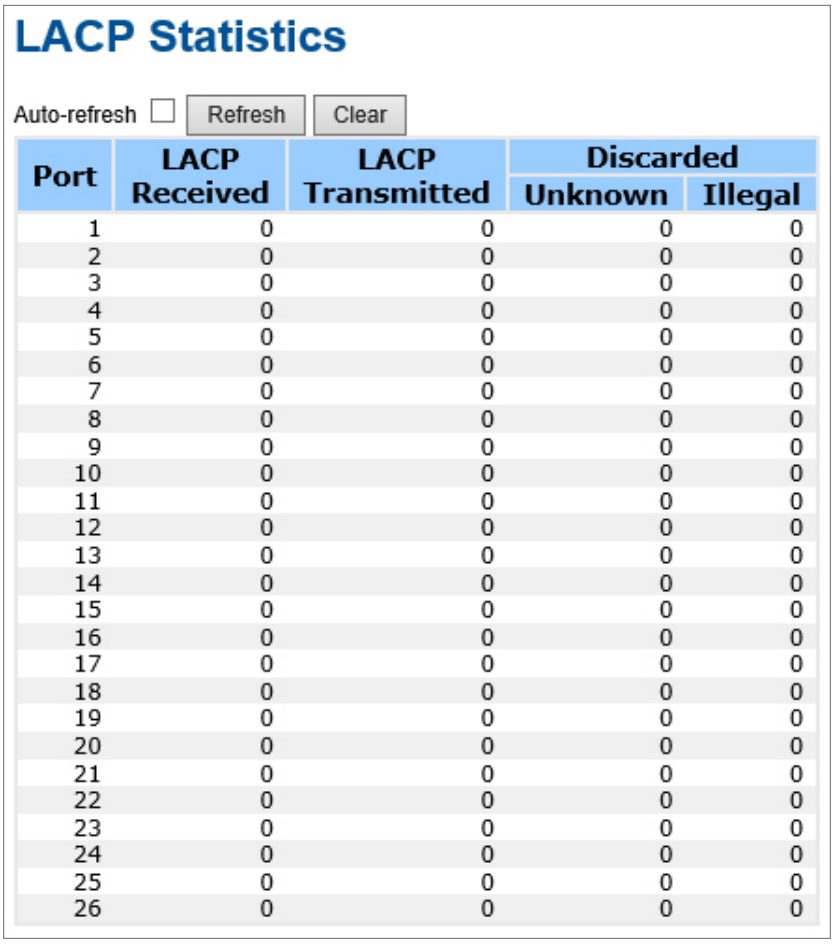
This page provides a status overview for LACP status for all ports.



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.
Partner Prio	The Partner's port priority
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

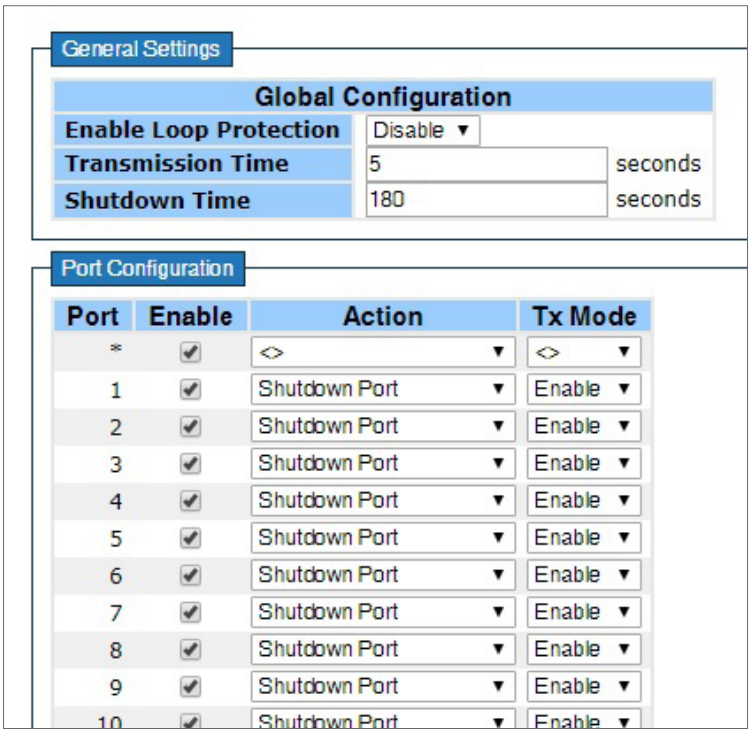
Auto-refresh ☐ Refresh Clear

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
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	0	0
24	0	0	0	0
25	0	0	0	0
26	0	0	0	0

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 Configuration

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



General Settings

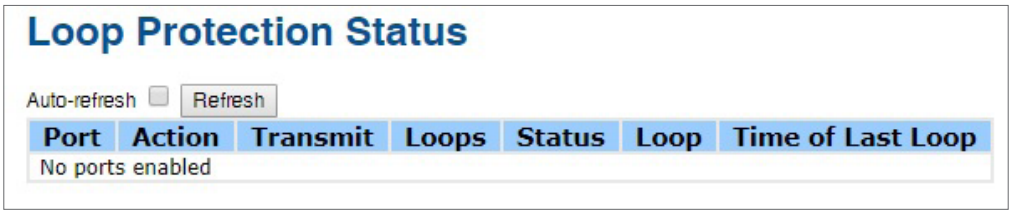
Enable Loop Protection	Controls whether loop protections is enabled (as a whole).
Transmission Time	The interval between each loop protection PDU sent on each port. valid values are 1 to 10 seconds.
Shutdown Time	The period (in seconds) for which a port will be kept disabled in the event of a loop is 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	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 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.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Loop Protection Status

This page displays the loop protection port status the ports of the currently selected switch.

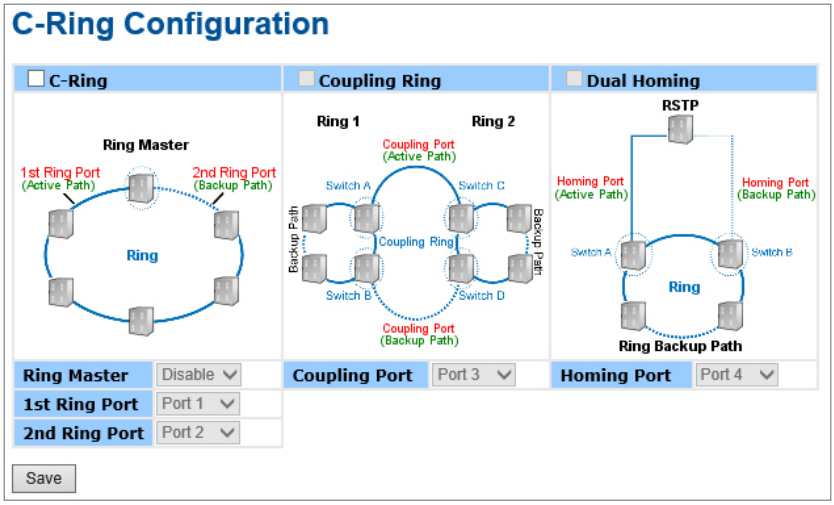


Loop protection port status is:

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

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 interface

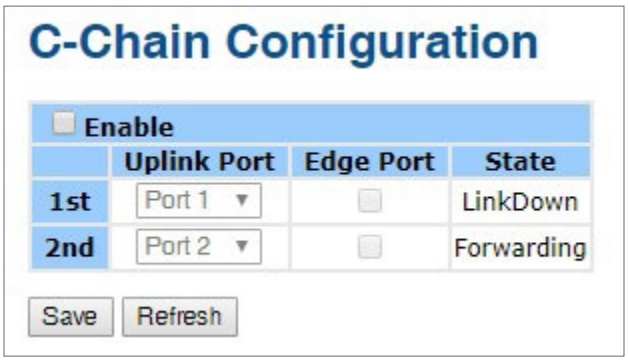
The following table describes the labels in this screen.

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.

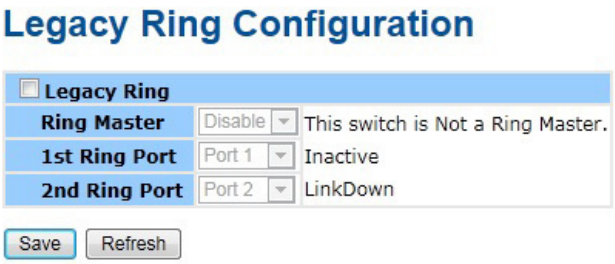
C-Chain Configuration

C-Chain is an easy use and powerful network redundancy protocol. The recovery speed of C-Chain is very quickly. It provides the add-on network redundancy topology for any backbone network, the upper LAN could be C-Ring, RSTP, Single Switch, or any backbone.



Label	Description
Enable	Check this box to enable C-Chain.
Uplink Port	There are two uplink ports for every devices in the chain. The user must specify the ports according to topology of network.
Edge Port	Only the edge (head or tail) device needs to specify edge port. The user must specify the edge port according to topology of network.
State	There three states for uplink port: Link Down, Blocking, and Forwarding.
Save	Click to save changes.
Refresh	Click to refresh the page.

Legacy Ring



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

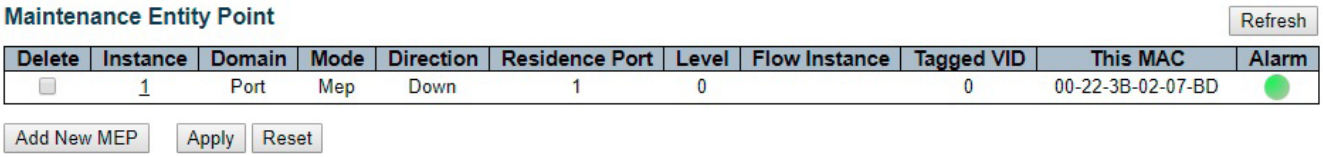
X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same. In the X-Ring topology, every switch should be enabled with X-Ring or Legacy Ring function and two ports should be assigned as the member ports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

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

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

MEP

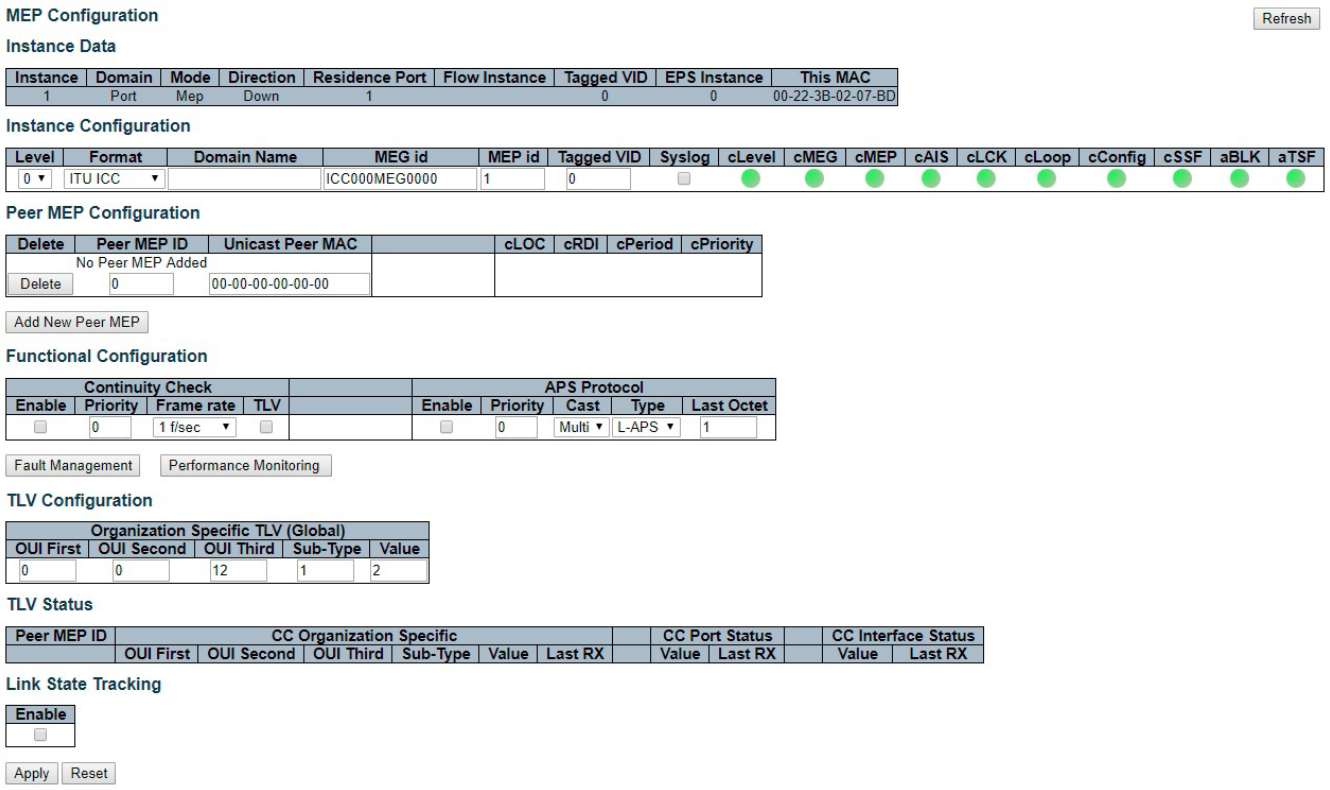
The Maintenance Entity Point instances are configured here.



Object	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. The range is from 1 through 100.
Domain	Port: This is a MEP in the Port Domain. EVC: This is a MEP in the EVC Domain. 'Flow Instance' is an EVC. The EVC must be created VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In case of Up-MEP the VLAN must be created MPLS Link: This is a MEP in the MPLS Link Domain. MPLS Tunnel: This is a MEP in the MPLS Tunnel Domain. MPLS PW: This is a MEP in the MPLS Pseudo Wires Domain. MPLS LSP: This is a MEP in the MPLS LSP Domain.
Mode	MEP: This is a Maintenance Entity End Point. MIP: This is a Maintenance Entity Intermediate Point.
Direction	Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'. Up: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.
Residence Port	The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.
Level	The MEG level of this MEP.
Flow Instance	The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.
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. EVC MEP: This is not used. VLAN MEP: This is not used. EVC MIP: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active.
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.
Add New MEP	Click to add a new MEP entry.
Refresh	Click to refresh the page immediately.
Apply	Click to apply changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Maintenance Entity End Point Configuration

This page allows the user to inspect and configure the current MEP Instance.



Object	Description
Instance Data	
MEP Instance	The ID of the MEP.
Domain	Port: This is a MEP in the Port Domain. EVC: This is a MEP in the EVC Domain. 'Flow Instance' is an EVC. The EVC must be created VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In case of Up-MEP the VLAN must be created MPLS Link: This is a MEP in the MPLS Link Domain. MPLS Tunnel: This is a MEP in the MPLS Tunnel Domain. MPLS PW: This is a MEP in the MPLS Pseudo Wires Domain. MPLS LSP: This is a MEP in the MPLS LSP Domain.
Mode	MEP: This is a Maintenance Entity End Point. MIP: This is a Maintenance Entity Intermediate Point.
Direction	Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'. Up: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.
Residence Port	The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.
Flow Instance	The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.

Object	Description
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. EVC MEP: This is not used. VLAN MEP: This is not used. EVC MIP: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active.
This MAC	The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).
Instance Configuration	
EVC Policy ID	This is the Policy number of the relevant ECE. Policy ID is used to assure that received OAM PDU is able to hit a IS2 entry. If this value is '0' IS2 rules will be created on classified VID. If this is NOT '0' IS2 rules will be created on this Policy (PAG). This must be equal to ECE Policy Number if OAM PDU will hit the ECE IS0. This is the case if an ECE is created with 'tag_type' as 'any'.
EVC QoS	This is only relevant for a EVC MEP. This is the Qos of the EVC and used for getting QoS counters for Loss Measurement.
Level	See help on MEP create WEB.
Format	This is the configuration of the two possible Maintenance Association Identifier formats. ITU ICC: This is defined by ITU (Y1731 Fig. A3). 'Domain Name' is not used. 'MEG id' must be max. 13 char. IEEE String: This is defined by IEEE (802.1ag Section 21.6.5). 'Domain Name' can be max. 16 char. 'MEG id' (Short MA Name) can be max. 16 char. ITU CC ICC: This is defined by ITU (Y1731 Fig. A5). 'Domain Name' is not used. 'MEG id' must be max. 15 char.
Domain Name	This is the IEEE Maintenance Domain Name and is only used in case of 'IEEE String' format. This string can be empty giving Maintenance Domain Name Format 1 - Not present. This can be max 16 char.
MEG Id	This is either ITU MEG ID or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this must be 13 char. In case of ITU CC ICC format this must be 15 char. In case of IEEE String format this can be max 16 char.
MEP Id	This value will become the transmitted two byte CCM MEP ID.
Tagged VID	This value will be the VID of a TAG added to the OAM PDU.
VOE	This will attempt to utilize VOE HW for MEP implementation. Not all platforms support VOE.
cLevel	Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP.
cMEG	Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP.
cMEP	Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP.
cAIS	Fault Cause indicating that AIS PDU is received.
cLCK	Fault Cause indicating that LCK PDU is received.
cSSF	Fault Cause indicating that server layer is indicating Signal Fail.

Object	Description
aBLK	The consequent action of blocking service frames in this flow is active.
aTSF	The consequent action of indicating Trail Signal Fail to-wards protection is active.
Peer MEP Configuration	
Delete	This box is used to mark a Peer MEP for deletion in next Save operation.
Peer MEP ID	This value will become an expected MEP ID in a received CCM - see 'cMEP'.
Unicast Peer MAC	This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.
cLOC	Fault Cause indicating that no CCM has been received (in 3,5 periods) - from this peer MEP.
cRDI	Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP.
cPeriod	Fault Cause indicating that a CCM is received with a period different what is configured for this MEP - from this peer MEP.
cPriority	Fault Cause indicating that a CCM is received with a priority different what is configured for this MEP - from this peer MEP.
Add New Peer MEP	Click to add a new peer MEP.
Functional Configuration	
Continuity Check	
Enable	Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1.
Priority	The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.
Frame rate	Selecting the frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731. This value has the following uses: * The transmission rate of the CCM PDU. * Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see 'cLOC'. * Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see 'cPeriod'. Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.
TLV	Enable/disable of TLV insertion in the CCM PDU.
APS Protocol	
Enable	Automatic Protection Switching protocol information transportation based on transmitting/receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured.
Priority	The priority to be inserted as PCP bits in TAG (if any).

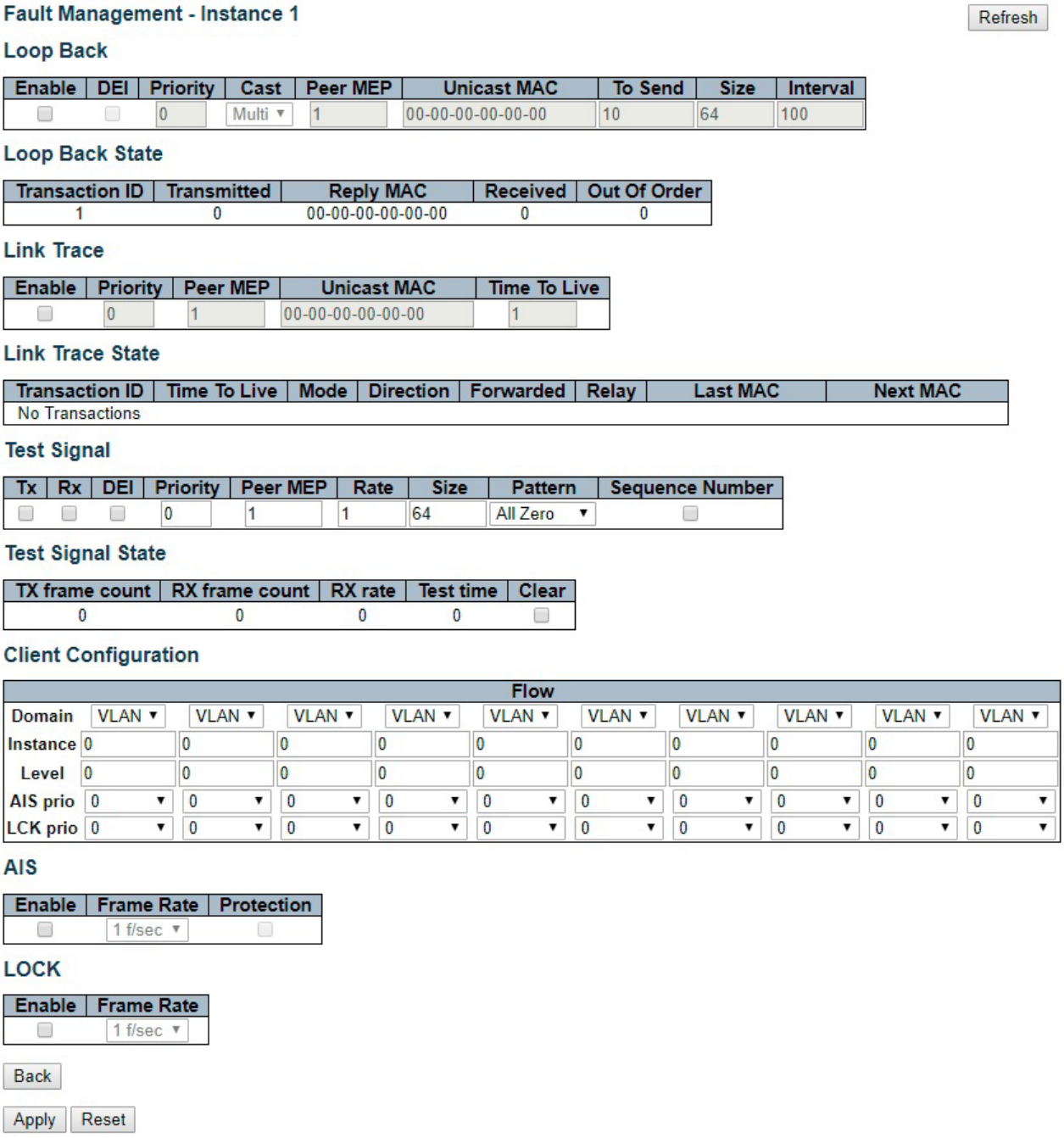
Object	Description
Cast	Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. Unicast is only valid for L-APS - see 'Type'. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032.
Type	R-APS: APS PDU is transmitted as R-APS - this is for ERPS. L-APS: APS PDU is transmitted as L-APS - this is for ELPS.
Last Octet	This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 (03/2010) a RAPS multi-cast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is '01' and the usage of other values is for further study.
TLV Configuration	Configuration of the OAM PDU TLV. Currently only TLV in the CCM is supported.
Organization Specific - OUI First	The transmitted first value in the OS TLV OUI field.
Organization Specific - OUI Second	The transmitted second value in the OS TLV OUI field.
Organization Specific - OUI Third	The transmitted third value in the OS TLV OUI field.
Organization Specific - Sub-Type	The transmitted value in the OS TLV Sub-Type field.
Organization Specific - Value	The transmitted value in the OS TLV Value field.
TLV Status	Display of the last received TLV. Currently only TLV in the CCM is supported.
CC Organization Specific - OUI First	The last received first value in the OUI field.
CC Organization Specific - OUI Second	The last received second value in the OS TLV OUI field.
CC Organization Specific - OUI Third	The last received third value in the OS TLV OUI field.
CC Organization Specific - Sub-Type	The last received value in the OS TLV Sub-Type field.
CC Organization Specific - Value	The last received value in the OS TLV Value field.
CC Organization Specific - Last RX	OS TLV was received in the last received CCM PDU.

Object	Description
CC Port Status - Value	The last received value in the PS TLV Value field.
CC Port Status - Last RX	PS TLV was received in the last received CCM PDU.
CC Interface Status - Value	The last received value in the IS TLV Value field.
CC Interface Status - Last RX	IS TLV was received in the last received CCM PDU.
Link State Tracking	
Enable	When LST is enabled in an instance, Local SF or received 'isDown' in CCM Interface Status TLV, will bring down the residence port. Only valid in Up-MEP.
Fault Management	Click to go to Fault Management page.
Performance Monitoring	Click to go to Performance Monitor page.
Refresh	Click to refresh the page immediately.
Apply	Click to apply changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

MEP Fault Management Configuration

This page allows the user to inspect and configure the Fault Management of the current MEP Instance.

Note that the sub-tables of Link Trace, Link Trace State, Client, AIS and LOCK are not supported while the MEP entry is in MPLS(Link/Tunnel/PW/LSP) domain.



Object	Description
Loop Back	
Enable	Loop Back based on transmitting/receiving LBM/LBR PDU can be enabled/disabled. Loop Back is automatically disabled when all 'To Send' LBM PDU has been transmitted - waiting 5 sec. for all LBR from the end.
DEI	The DEI to be inserted as PCP bits in TAG (if any).
Priority	The priority to be inserted as PCP bits in TAG (if any).
Cast	Selection of LBM PDU transmitted unicast or multi-cast. The unicast MAC will be configured through 'Peer MEP' or 'Unicast Peer MAC'. To-wards MIP only unicast Loop Back is possible.
Peer MEP	This is only used if the 'Unicast MAC' is configured to all zero. The LBM unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.
Unicast MAC	This is only used if NOT configured to all zero. This will be used as the LBM PDU unicast MAC. This is the only way to configure Loop Back to-wards a MIP.
MPLS TTL	The Time-To-Live value to be used for the MPLS OAM LBM PDU. It is insignificant when this MEP domain type is MPLS Link/Tunnel/PW/LSP. The allowed value is from 0 through 255.
To Send	The number of LBM PDU to send in one loop test. The value 0 indicate infinite transmission (test behaviour). This is HW based LBM/LBR and Requires VOE.
Size	The LBM frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing LBM OAM PDU - including CRC (four bytes). Example when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + LBM PDU LENGTH(46) + CRC(4) = 64 bytes The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC. There are two frame MAX sizes to consider. Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 96009600 Bytes CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 15261526 Bytes Consider that the Peer MEP must be able to handle the selected frame size. Consider that In case of SW based MEP, the received LBR PDU must be copied to CPU Warning will be given if selected frame size exceeds the CPU RX frame MAX size Frame MIN Size is 64 Bytes.
Interval	The interval between transmitting LBM PDU. In 10ms. in case 'To Send' != 0 (max 100 - '0' is as fast as possible) In 1us. in case 'To Send' == 0 (max 10.000)",
Loop Back State	
Transaction ID	The transaction id of the first LBM transmitted. For each LBM transmitted the transaction id in the PDU is incremented.
Transmitted	The total number of LBM PDU transmitted.
Reply MAC	The MAC of the replying MEP/MIP. In case of multi-cast LBM, replies can be received from all peer MEP in the group. This MAC is not shown in case of 'To Send' == 0.
Received	The total number of LBR PDU received from this 'Reply MAC'.

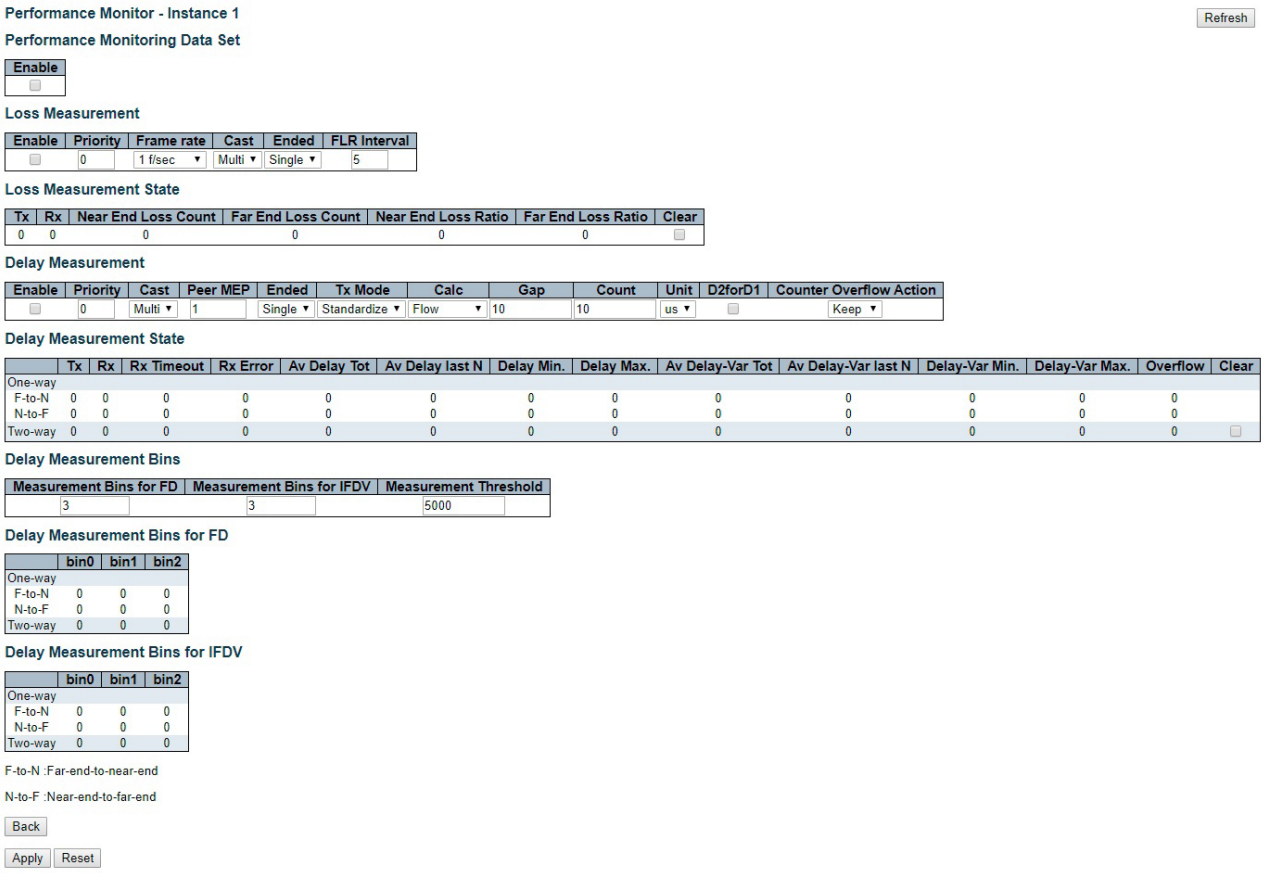
Object	Description
Out Of Order	The number of LBR PDU received from this 'Reply MAC' with incorrect 'Transaction ID'.
Link Trace	
Enable	Link Trace based on transmitting/receiving LTM/LTR PDU can be enabled/disabled. Link Trace is automatically disabled when all 5 transactions are done with 5 sec. interval - waiting 5 sec. for all LTR in the end. The LTM PDU is always transmitted as Multi-cast Class 2.
Priority	The priority to be inserted as PCP bits in TAG (if any).
Peer MEP	This is only used if the 'Unicast MAC' is configured to all zero. The Link Trace Target MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.
Unicast MAC	This is only used if NOT configured to all zero. This will be used as the Link Trace Target MAC. This is the only way to configure a MIP as Target MAC.
Time To Live	This is the LTM PDU TTL value as described in Y.1731. This value is decremented each time forwarded by a MIP. Will not be forwarded reaching zero.
Link Trace State	
Transaction ID	The transaction id is incremented for each LTM send. This value is inserted the transmitted LTM PDU and is expected to be received in the LTR PDU. Received LTR with wrong transaction id is ignored. There are five transactions in one Link Trace activated.
Time To Live	This is the TTL value taken from the LTM received by the MIP/MEP sending this LTR - decremented as if forwarded.
Mode	Indicating if is was a MEP/MIP sending this LTR.
Direction	Indicating if MEP/MIP sending this LTR is ingress/egress.
Forwarded	Indicating if MEP/MIP sending this LTR has forwarded the LTM.
Relay	The Relay action can be one of the following MAC: The was a hit on the LT Target MAC FDB: LTM is forwarded based on hit in the Filtering DB MFDB: LTM is forwarded based on hit in the MIP CCM DB
Last MAC	The MAC identifying the last sender of the LBM causing this LTR - initiating MEP or previous MIP forwarding.
Next MAC	The MAC identifying the next sender of the LBM causing this LTR - MIP forwarding or terminating MEP.
Test Signal	
Enable	Test Signal based on transmitting TST PDU can be enabled/disabled.
DEI	The DEI to be inserted as PCP bits in TAG (if any).
Priority	The priority to be inserted as PCP bits in TAG (if any).
Peer MEP	The TST frame destination MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Object	Description
Rate	The TST frame transmission bit rate - in Mega bits pr. second. Limit is 2.5Gbps. This is the bit rate of a standard frame without any encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will give a higher bitrate on the wire. The TST frame transmission bit rate - in Mega bits pr. second. Limit is 400 Mbps. This is the bit rate of a standard frame without any encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will give a higher bitrate on the wire. The TST frame transmission bit rate - in Mega bits pr. second. Limit is 400 Mbps. This is the bit rate of a standard frame without any encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will give a higher bitrate on the wire.
Size	The TST frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing TST OAM PDU - including CRC (four bytes). Example when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC. There are two frame MAX sizes to consider. Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 96009600 Bytes CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 15261526 Bytes Consider that the Peer MEP must be able to handle the selected frame size. Consider that in order to calculate the 'RX rate' a received TST PDU must be copied to CPU Warning will be given if selected frame size exceeds the CPU RX frame MAX size Frame MIN Size is 64 Bytes.
Pattern	The 'empty' TST PDU has the size of 12 bytes. In order to achieve the configured frame size a data TLV will be added with a pattern. Example when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes The TST PDU needs to be 46 bytes so a pattern of 46-12=34 bytes will be added. All Zero: Pattern will be '00000000' All One: Pattern will be '11111111' 10101010: Pattern will be '10101010'
Test Signal State	
TX frame count	The number of transmitted TST frames since last 'Clear'.
RX frame count	The number of received TST frames since last 'Clear'.
RX rate	The current received TST frame bit rate in Kbps. This is calculated on a 1 s. basis, starting when first TST frame is received after 'Clear'. The frame size used for this calculation is the first received after 'Clear'
Test time	The number of seconds passed since first TST frame received after last 'Clear'.
Clear	This will clear all Test Signal State. Transmission of TST frame will be restarted. Calculation of 'Rx frame count', 'RX rate' and 'Test time' will be started when receiving first TST frame.
Client Configuration	Only a Port MEP is able to be a server MEP with flow configuration. The Priority in the client flow is always the highest priority configured in the EVC.

Object	Description
Domain	The domain of the client layer flow. For a MPLS MEP, the client domain can only be EVC or LSP. For a non-MPLS MEP, the client flow domain can not be LSP. For a non-MPLS MEP, the client flow domain can not be mixed VLAN and EVC.
Instance	Client layer flow instance numbers.
Level	Client layer level - AIS and LCK PDU transmitted in this client layer flow will be on this level.
AIS Prio	The priority to be used when transmitting AIS in each client flow. Priority resulting in highest possible PCP can be selected.
LCK Prio	The priority to be used when transmitting LCK in each client flow. Priority resulting in highest possible PCP can be selected.
AIS	
Enable	Insertion of AIS signal (AIS PDU transmission) in client layer flows, can be enable/disabled.
Frame Rate	Selecting the frame rate of AIS PDU. This is the inverse of transmission period as described in Y.1731.
Protection	Selecting this means that the first 3 AIS PDU is transmitted as fast as possible - in case of using this for protection in the end point.
LOCK	
Enable	Insertion of LOCK signal (LCK PDU transmission) in client layer flows, can be enable/disabled.
Frame Rate	Selecting the frame rate of LCK PDU. This is the inverse of transmission period as described in Y.1731.:
Refresh	Click to refresh the page immediately.
Back	Click to go back to this MEP instance main page.
Apply	Click to apply changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

MEP Performance Monitor Configuration

This page allows the user to inspect and configure the performance monitor of the current MEP Instance.



Performance Monitoring Data Set	
Enable	When enabled this MEP instance will contribute to the 'PM Data Set' gathered by the PM Session.
Loss Measurement	
Enable	Loss Measurement based on transmitting/receiving CCM or LMM/LMR PDU can be enabled/disabled - see 'Ended'. This is only valid with one Peer MEP configured.
Priority	The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.
Frame rate	Selecting the frame rate of CCM/LMM PDU. This is the inverse of transmission period as described in Y.1731. Selecting 300f/sec or 100f/sec is not valid. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.
Cast	Selection of CCM or LMM PDU transmitted unicast or multicast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. In case of enable of Continuity Check and dual ended Loss Measurement both implemented on SW based CCM, 'Cast' has to be the same.

Ended	Single: Single ended Loss Measurement implemented on LMM/LMR. Dual: Dual ended Loss Measurement implemented on SW based CCM.
FLR Interval	This is the interval in seconds where the Frame Loss Ratio is calculated.
Flow Counting	Traffic (service frames) are counted per flow - all priority in one.
Oam Counting	Loss Measurement can count OAM frames in different ways. Y1713: Loss Measurement is counting OAM frames as service frames as described in Y1731. None: Loss Measurement is NOT counting OAM frames as service frames. All: Loss Measurement is counting all OAM frames as service frames.
Loss Measurement State	
Near End Loss Count	The accumulated near end frame loss count - since last 'clear'.
Far End Loss Count	The accumulated far end frame loss count - since last 'clear'.
Near End Loss Ratio	The near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted - in the latest 'FLR Interval'. The result is given in percent.
Far End Loss Ratio	The far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted - in the latest 'FLR Interval'. The result is given in percent.
Clear	Set of this check and save will clear the accumulated counters and restart ratio calculation.
Delay Measurement	
Enable	Delay Measurement based on transmitting 1DM/DMM PDU can be enabled/ disabled. Delay Measurement based on receiving and handling 1DM/DMR PDU is always enabled.
Priority	The priority to be inserted as PCP bits in TAG (if any).
Cast	Selection of 1DM/DMM PDU transmitted unicast or multicast. The unicast MAC will be configured through 'Peer MEP'.
Peer MEP	This is only used if the 'Cast' is configured to Uni. The 1DM/DMR unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.
Way	One-Way: One-Way Delay Measurement implemented on 1DM. Two-Way: Two-Way Delay Measurement implemented on DMM/DMR.
Tx Mode	Standardize: Y.1731 standardize way to transmit 1DM/DMR. Proprietary: Vitesse proprietary way with follow-up packets to transmit 1DM/DMR.
Calc	This is only used if the 'Way' is configured to Two-way. Round trip: The frame delay calculated by the transmitting and receiving timestamps of initiators. Frame Delay = RxTimeb-TxTimeStampf Flow: The frame delay calculated by the transmitting and receiving timestamps of initiators and remotes. Frame Delay = (RxTimeb-TxTimeStampf)-(TxTimeStampb-RxTimeStampf)
Gap	The gap between transmitting 1DM/DMM PDU in 10ms. The range is 10 to 65535.
Count	The number of last records to calculate. The range is 10 to 2000.
Unit	The time resolution.

D2forD1	Enable to use DMM/DMR packet to calculate one-way DM. If the option is enabled, the following action will be taken. When DMR is received, two-way delay (roundtrip or flow) and both near-end-to-far-end and far-end-to-near-end one-way delay are calculated. When DMM or 1DM is received, only far-end-to-near-end one-way delay is calculated.
Counter Overflow Action	The action to counter when overflow happens.
Delay Measurement State	
Tx	The accumulated transmit count - since last 'clear'.
Rx	The accumulated receive count - since last 'clear'.
Rx Timeout	The accumulated receive timeout count for two-way only - since last 'clear'.
Rx Error	The accumulated receive error count - since last 'clear'. This is counting if the frame delay is larger than 1 second or if far end residence time is larger than the round trip time.
Av Delay Tot	The average total delay - since last 'clear'.
Av Delay last N	The average delay of the last n packets - since last 'clear'.
Delay Min.	The minimum delay - since last 'clear'.
Delay Max.	The maximum delay - since last 'clear'.
Av Delay-Var Tot	The average total delay variation - since last 'clear'.
Av Delay-Var last N	The average delay variation of the last n packets - since last 'clear'.
Delay-Var Min.	The minimum delay variation - since last 'clear'.
Delay-Var Max.	The maximum delay variation - since last 'clear'.
Overflow	The number of counter overflow - since last 'clear'.
Clear	Set of this check and save will clear the accumulated counters.
Far-end-to-near-end one-way delay	The one-way delay is from remote devices to the local devices. Here are the conditions to calculate this delay. 1. 1DM received. 2. DMM received with D2forD1 enabled. 3. DMR received with D2forD1 enabled.
Near-end-to-far-end one-way delay	The one-way delay is from the local devices to remote devices. The only case to calculate this delay is below. DMR received with D2forD1 enabled.
Delay Measurement Bins	
A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.	
Measurement Bins for FD	Configurable number of Frame Delay Measurement Bins per Measurement Interval. The minimum number of FD Measurement Bins per Measurement Interval supported is 2. The maximum number of FD Measurement Bins per Measurement Interval supported is 10. The default number of FD Measurement Bins per Measurement Interval supported is 3.

Measurement Bins for IFDV	Configurable number of Inter-Frame Delay Variation Measurement Bins per Measurement Interval. The minimum number of FD Measurement Bins per Measurement Interval supported is 2. The maximum number of FD Measurement Bins per Measurement Interval supported is 10. The default number of FD Measurement Bins per Measurement Interval supported is 2.
Measurement Threshold	Configurable the Measurement Threshold for each Measurement Bin. The unit for a measurement threshold is in microseconds (us). The default configured measurement threshold for a Measurement Bin is an increment of 5000 us.

Delay Measurement Bins for FD

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.
If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us
bin1	5,000 us	5,000 us <= measurement < 10,000 us
bin2	10,000 us	10,000 us <= measurement < 15,000 us
bin3	15,000 us	15,000 us <= measurement < infinite us

Delay Measurement Bins for IFDV

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.
If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us
bin1	5,000 us	5,000 us <= measurement < 10,000 us
bin2	10,000 us	10,000 us <= measurement < 15,000 us
bin3	15,000 us	15,000 us <= measurement < infinite us

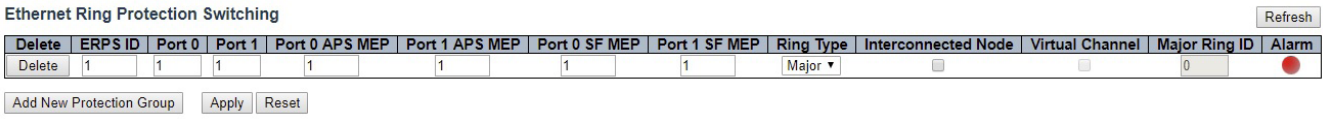
Refresh	Click to refresh the page immediately.
Back	Click to go back to this MEP instance main page.
Apply	Click to apply changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

ERPS

The ERPS instances are configured here.

Please note that ERPS cannot be used in conjunction with Spanning Tree or Loop Protection on the same switch

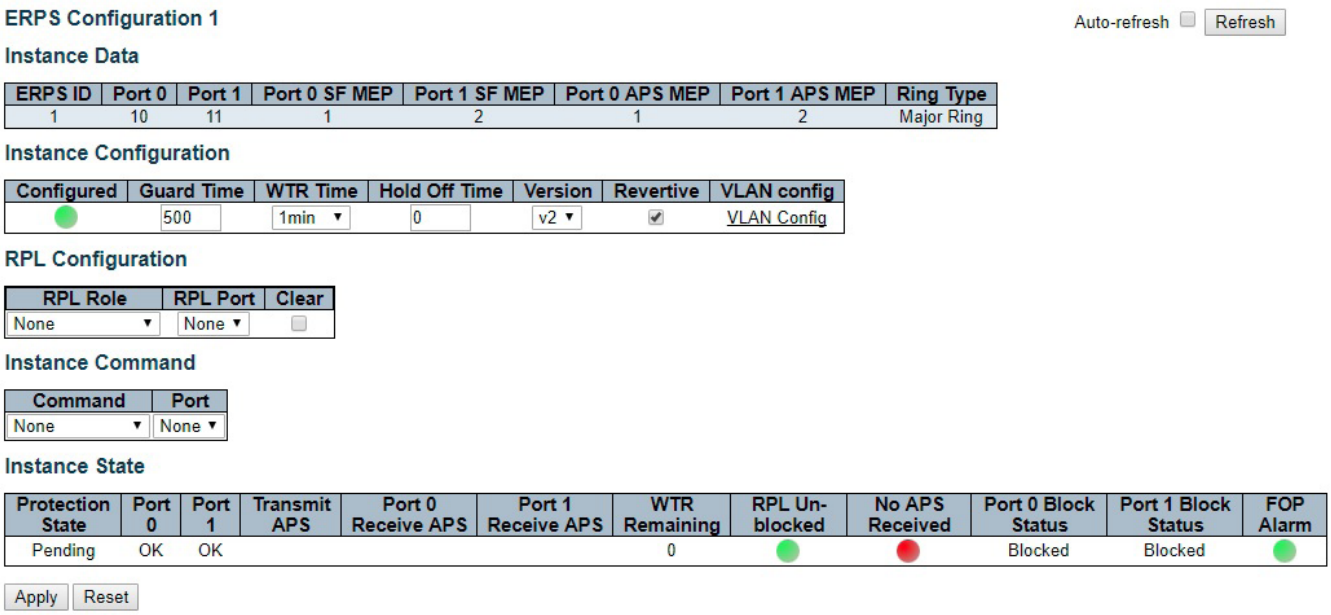
Note: For an example of how to configure an ERPS ring please refer to appendix A at the rear of this document.



Object	Description
Delete	This box is used to mark an ERPS for deletion in next Save operation.
ERPS ID	The ID of the created Protection group, It must be an integer value between 1 and 64. The maximum number of ERPS Protection Groups that can be created are 64. 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.

Add New Protection Group	Click to add a new Protection group entry.
Refresh	Click to refresh the page immediately.
Apply	Click to apply changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Ethernet Ring Protection Switch Configuration

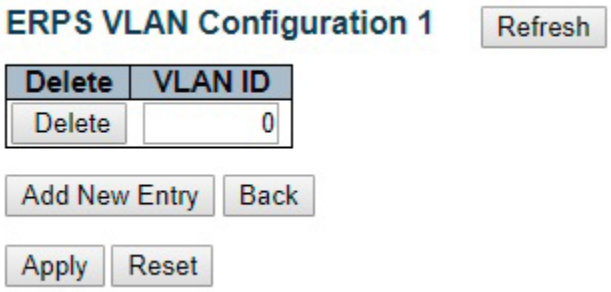


Object	Description
Instance Data	
ERPS ID	The ID of the Protection group.
Port 0	This will create a Port 0 of the switch in the ring.
Port 1	This will create “Port 1” of the switch in the Ring. As interconnected sub-ring will have only one ring port, “Port 1” is configured as “0” for interconnected sub-ring. “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.
Instance Configuration	
Configured	Red: This ERPS is only created and has not yet been configured - is not active. Green: This ERPS is configured - is active.

Object	Description
Guard Time	Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds, with a default value of 500 ms
WTR Time	The Wait To Restore timing value to be used in revertive switching. The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes with a default value of 5 minutes.
Hold Off Time	The timing value to be used to make persistent check on Signal Fail before switching. The range of the hold off timer is 0 to 10 seconds in steps of 100 ms
Version	ERPS Protocol Version - v1 or v2
Revertive	In Revertive mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL. In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.
VLAN config	VLAN configuration of the Protection Group. Click on the "VLAN Config" link to configure VLANs for this protection group.
RPL Configuration	
RPL Role	It can be either RPL owner or RPL Neighbor.
RPL Port	This allows to select the east port or west port as the RPL block.
Clear	If the owner has to be changed, then the clear check box allows to clear the RPL owner for that ERPS ring.
Sub-Ring Configuration	
Topology Change	Clicking this checkbox indicates that the topology changes in the sub-ring are propagated in the major ring.
Instance Command	
Command	Administrative command. A port can be administratively configured to be in either manual switch or forced switch state.
Forced Switch	Forced Switch command forces a block on the ring port where the command is issued.
Manual Switch	In the absence of a failure or FS, Manual Switch command forces a block on the ring port where the command is issued.
Clear	The Clear command is used for clearing an active local administrative command (e.g., Forced Switch or Manual Switch).
Port	Port selection - Port0 or Port1 of the protection Group on which the command is applied.
Instance State	
Protection State	ERPS state according to State Transition Tables in G.8032.
Port 0	OK: State of East port is ok SF: State of East port is Signal Fail
Port 1	OK: State of West port is ok SF: State of West port is Signal Fail

Object	Description
Transmit APS	The transmitted APS according to State Transition Tables in G.8032.
Port 0 Receive APS	The received APS on Port 0 according to State Transition Tables in G.8032.
Port 1 Receive APS	The received APS on Port 1 according to State Transition Tables in G.8032.
WTR Remaining	Remaining WTR timeout in milliseconds.
RPL Un-blocked	APS is received on the working flow.
No APS Received	RAPS PDU is not received from the other end.
Port 0 Block Status	Block status for Port 0 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.
Port 1 Block Status	Block status for Port 1 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.
FOP Alarm	Failure of Protocol Defect(FOP) status. If FOP is detected, red LED glows; else green LED glows.
Apply	Click to apply changes.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page immediately.
Reset	Click to undo any changes made locally and revert to previously saved values.

VLAN Membership Configuration

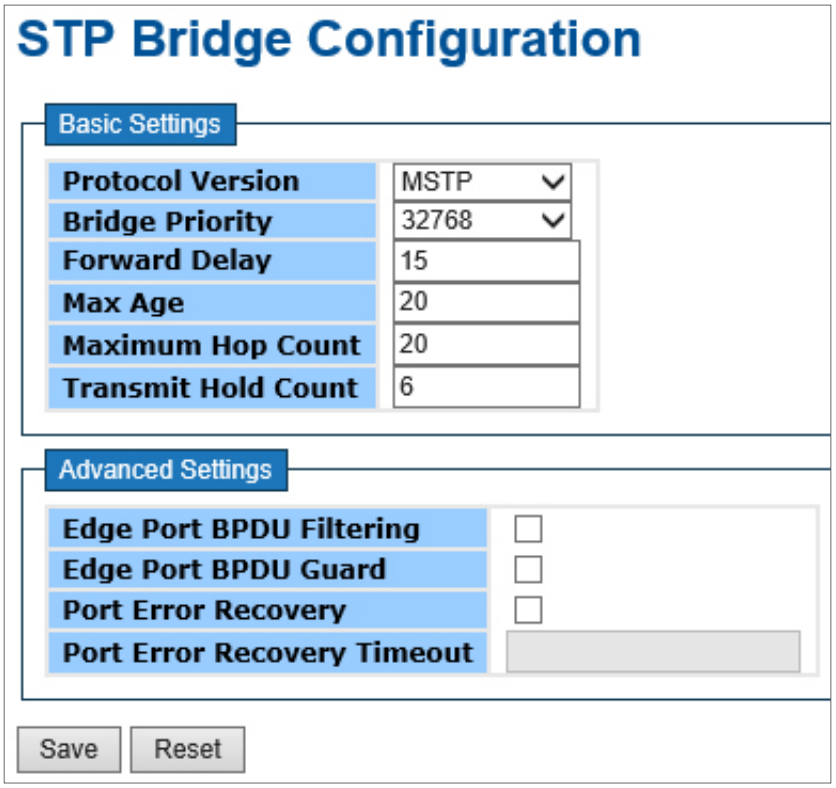


Object	Description
Delete	To delete a VLAN entry, check this box. The entry will be deleted on all stack switch units during the next Save.
VLAN ID	Indicates the ID of this particular VLAN.
Adding a New VLAN	Click "Add New Entry" to add a new VLAN ID. Legal values for a VLAN ID are 1 through 4095. The VLAN is enabled on the selected switch unit when you click on "Save". A VLAN without any port members will be deleted when you click "Save". The "Delete" button can be used to undo the addition of new VLANs.
Apply	Click to apply changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Back	Click to go back to this MEP instance main page.
Refresh	Refreshes the displayed table starting from the "VLAN ID" input fields.

MSTP

Bridge Settings

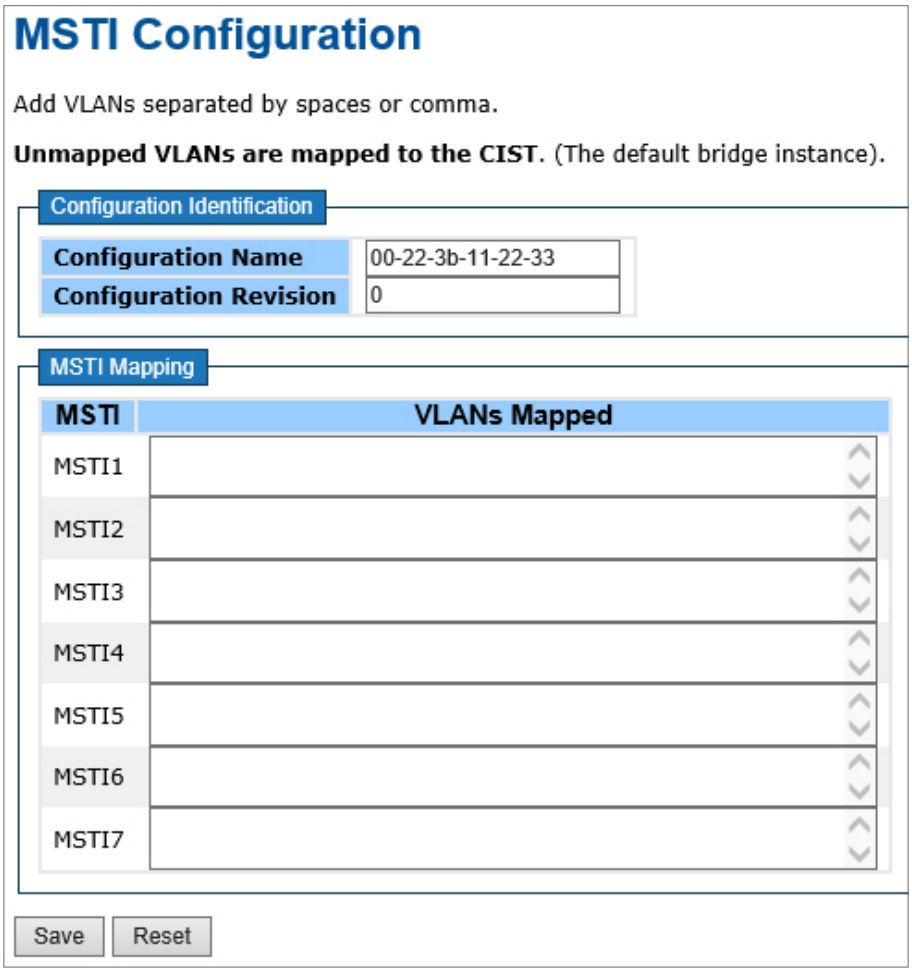
This page allows you to configure RSTP system settings. The settings are used by all RSTP Bridge instances in the Switch Stack.



Label	Description
Protocol Version	The STP protocol version setting. Valid values are STP, RSTP and MSTP.
Forward Delay	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (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

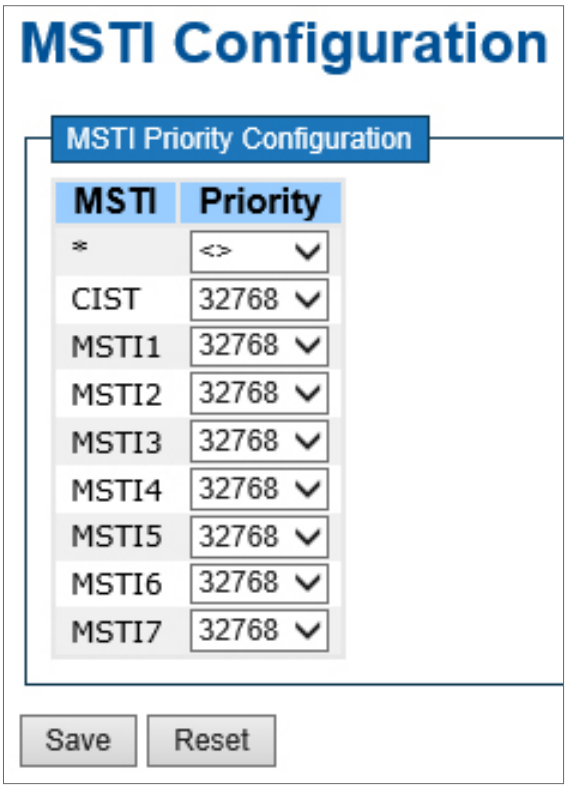
This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.



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

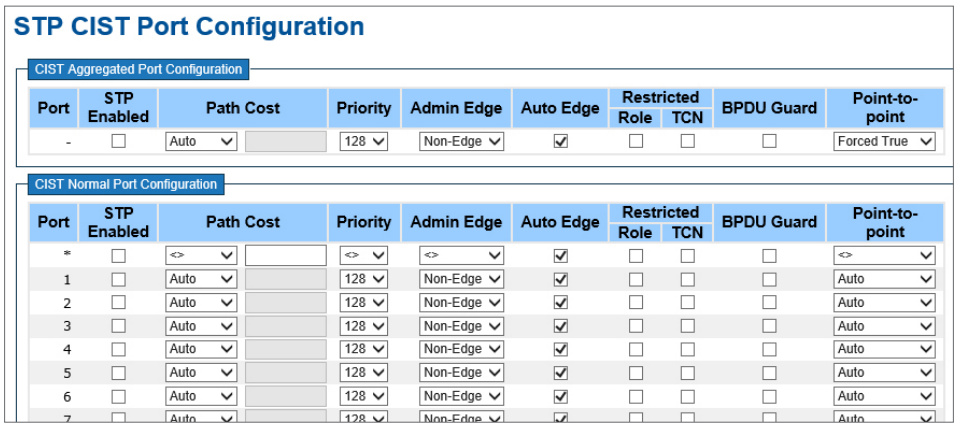
This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.



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.



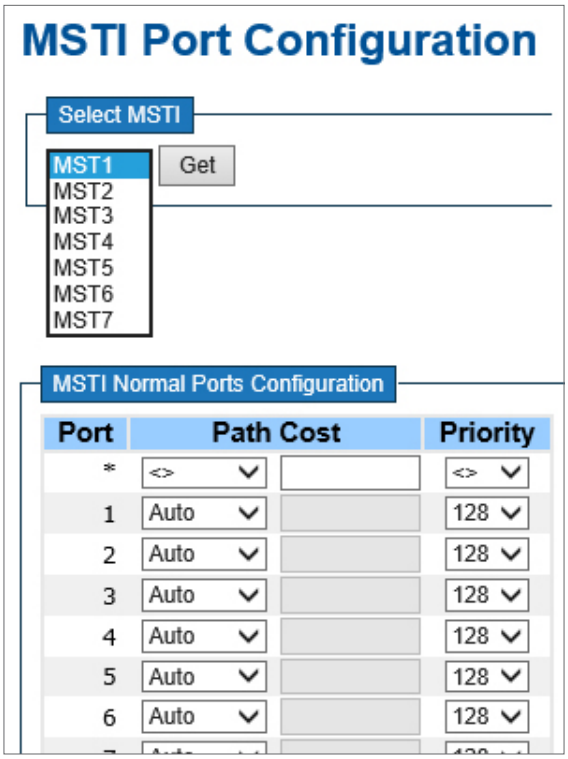
Label	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended 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.

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.



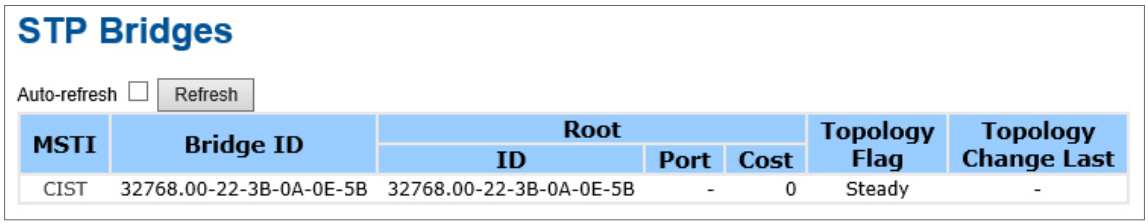
Label	Description
Port	The switch port number of the corresponding STP CIST (and MSTI) port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined 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.

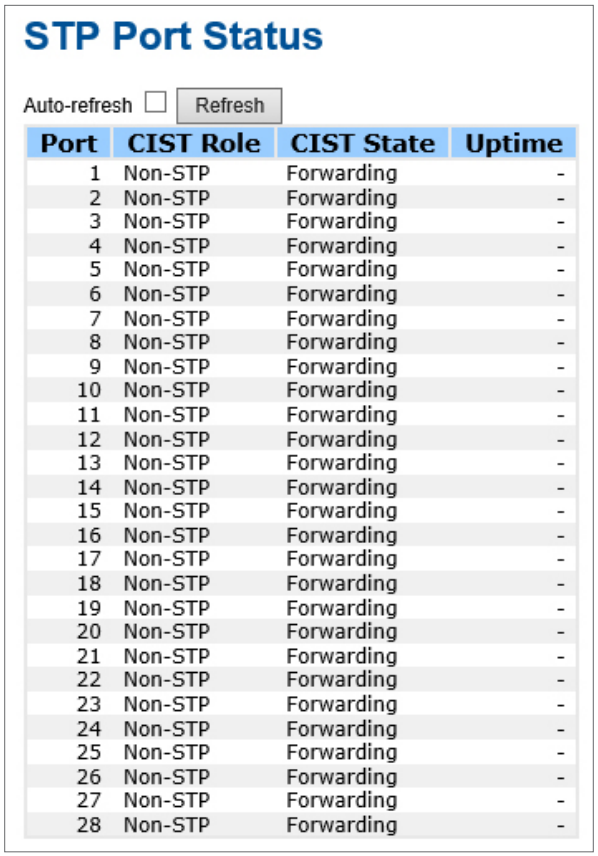
The displayed table contains a row for each STP bridge instance, where the column displays the following information:



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

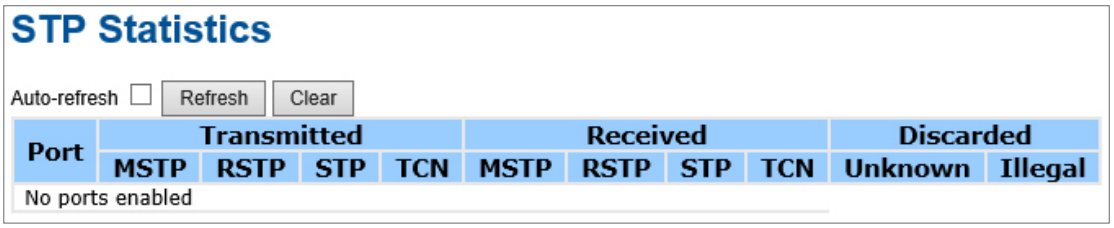
This page displays the STP CIST port status for port physical ports in the currently selected switch.



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

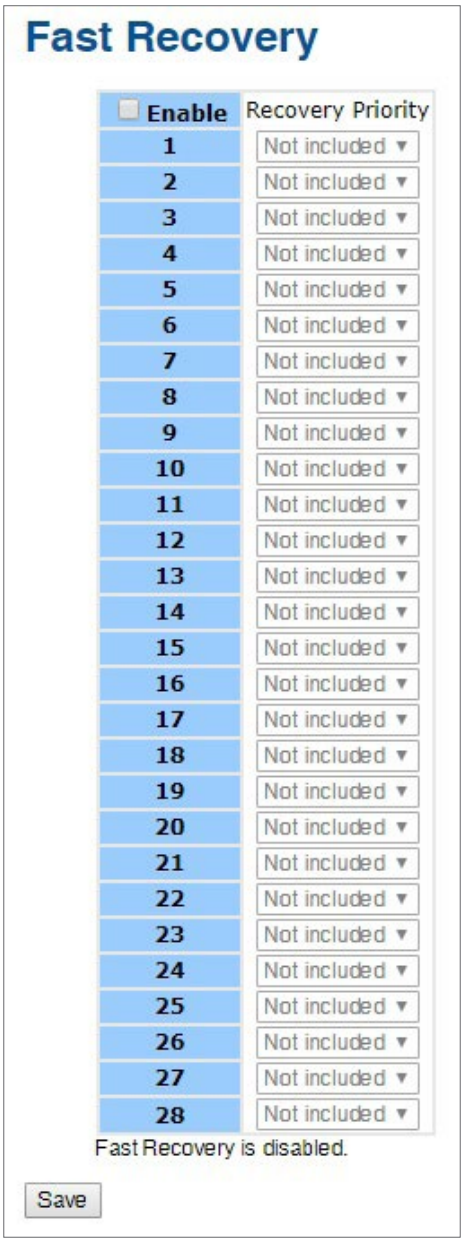
This page displays the RSTP port statistics counters for bridge ports in the currently selected switch.



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 Configuration

Fast Recovery is a function for port redundancy. The port has the highest recovery priority (the lowest number) will be the active port, others will be blocked (if included).

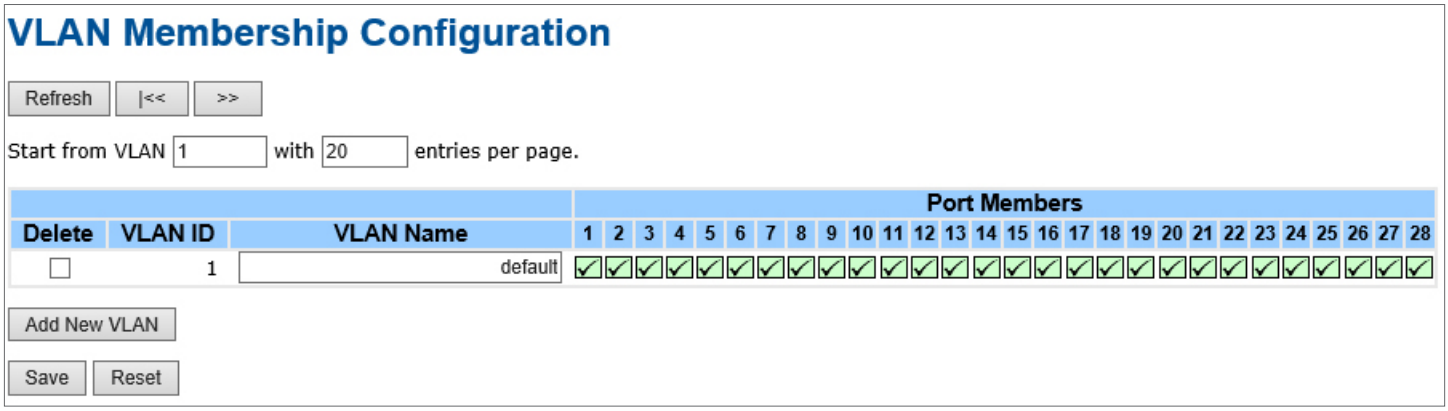


Enable	Enable Fast Recovery function.
Recovery Priority	The port has the highest recovery priority (the lowest number) will be the active port, others will be blocked (if included).
Save	Click to save changes.

VLAN

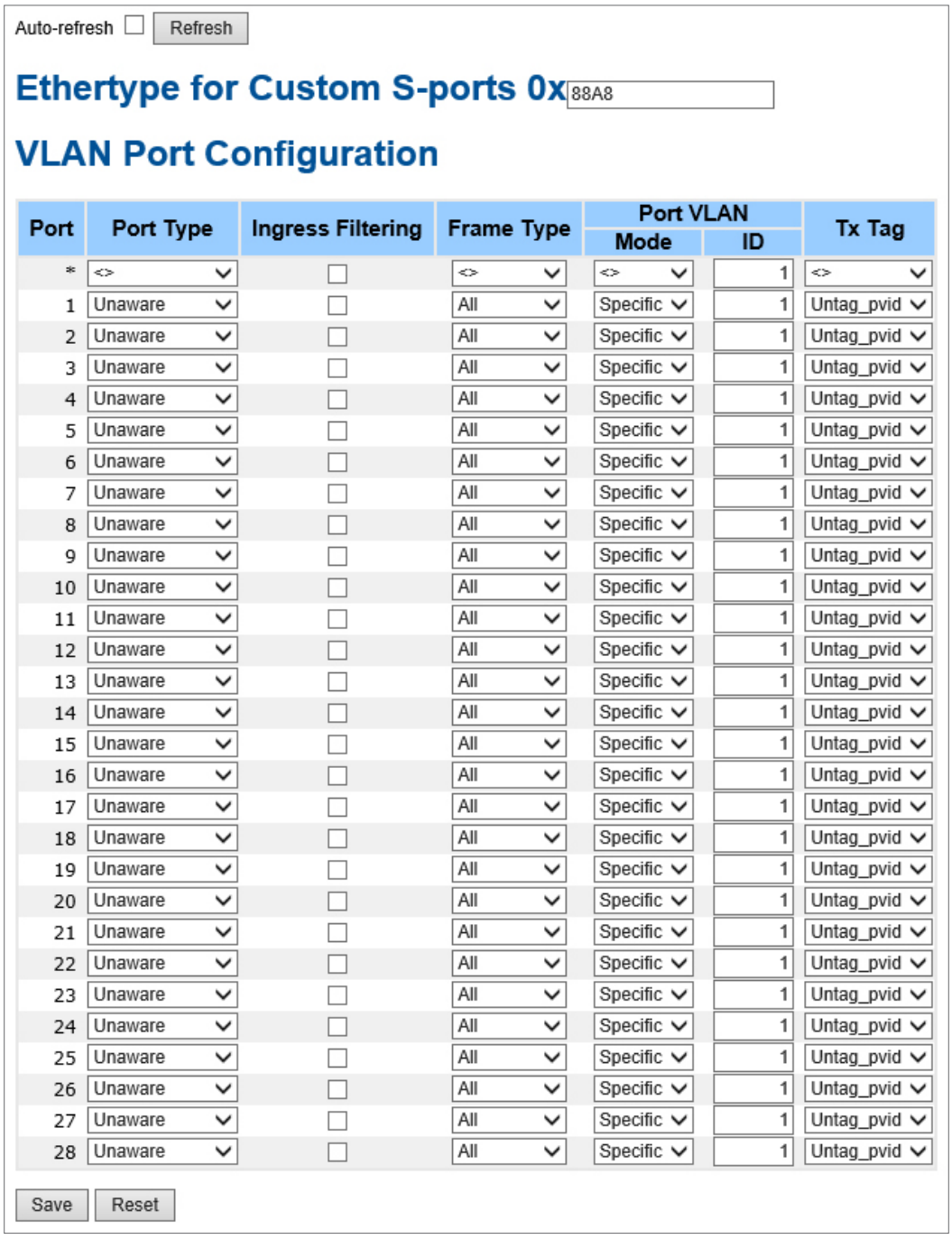
VLAN Membership Configuration

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



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
VLAN Name	The descriptive name for the VLAN 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 Mode	Port VLAN ID	Tx Tag
*	<>	☐	<>	<>	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
13	Unaware	☐	All	Specific	1	Untag_pvid
14	Unaware	☐	All	Specific	1	Untag_pvid
15	Unaware	☐	All	Specific	1	Untag_pvid
16	Unaware	☐	All	Specific	1	Untag_pvid
17	Unaware	☐	All	Specific	1	Untag_pvid
18	Unaware	☐	All	Specific	1	Untag_pvid
19	Unaware	☐	All	Specific	1	Untag_pvid
20	Unaware	☐	All	Specific	1	Untag_pvid
21	Unaware	☐	All	Specific	1	Untag_pvid
22	Unaware	☐	All	Specific	1	Untag_pvid
23	Unaware	☐	All	Specific	1	Untag_pvid
24	Unaware	☐	All	Specific	1	Untag_pvid
25	Unaware	☐	All	Specific	1	Untag_pvid
26	Unaware	☐	All	Specific	1	Untag_pvid
27	Unaware	☐	All	Specific	1	Untag_pvid
28	Unaware	☐	All	Specific	1	Untag_pvid

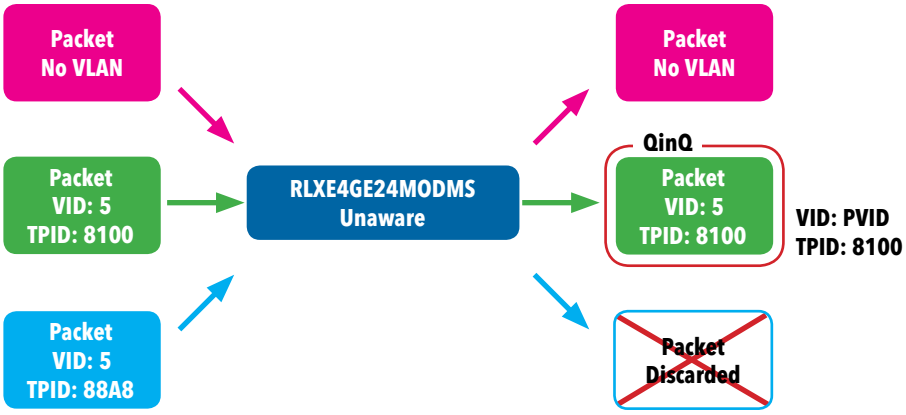
Save Reset

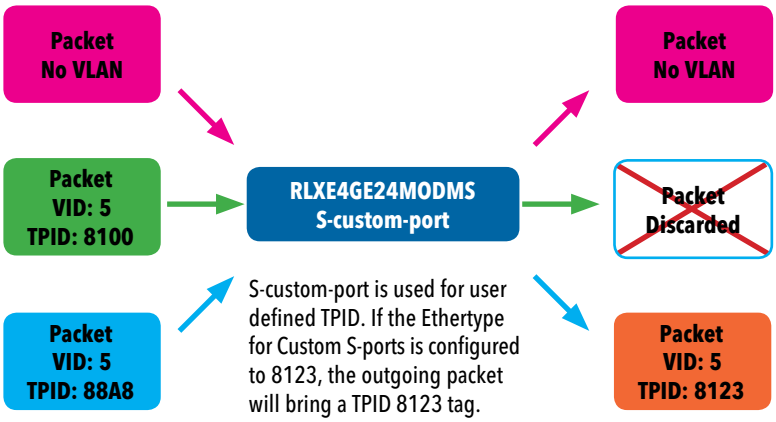
Label	Description
Ethertype for customer S-Ports	This field specifies the ether type used for Custom S-ports. This is a global setting for all the Custom S-ports.
Port	This is the logical port number of this row.
Port type	Port can be one of the following types: Unaware, Customer port (C-port), Service 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.
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.

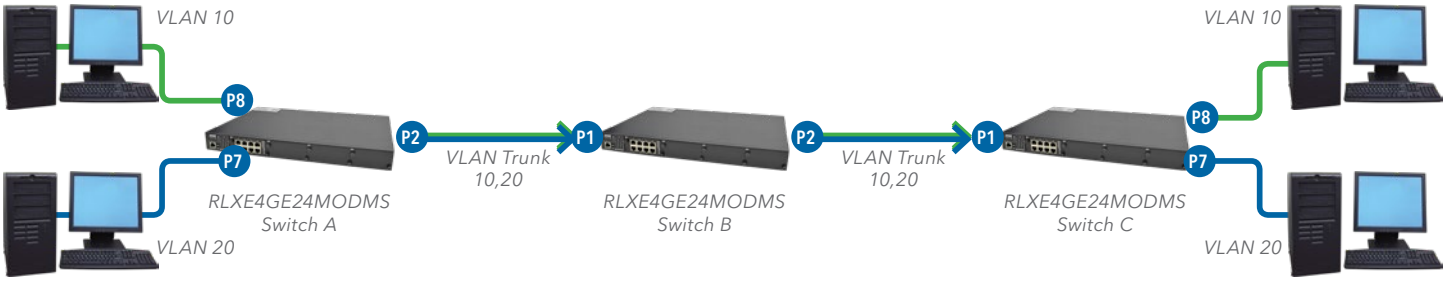
	Ingress action	Egress action
Unaware The function of Unaware can be used for 802.1QinQ (double tag).	When the port received untagged frames, an untagged frame obtain a tag (based on PVID) and is forwarded. When the port received tagged frames, 1. If the tagged frame with TPID=0x8100, it become a double-tag 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.


Packet
No VLAN
Packet
VID: 5
TPID: 8100
Packet
VID: 5
TPID: 88A8
RLXE4GE24MODMS
Unaware
Packet
No VLAN
QinQ
Packet
VID: 5
TPID: 8100
VID: PVID
TPID: 8100
Packet
Discarded


Packet
No VLAN
Packet
VID: 5
TPID: 8100
Packet
VID: 5
TPID: 88A8
RLXE4GE24MODMS
S-custom-port
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.
Packet
No VLAN
Packet
Discarded
Packet
VID: 5
TPID: 8123

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

Refresh |<< >>

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	13	14	15	16	17	18	19	20	21	22	23	24	25	26
☐	1	default	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
☐	10	vlan10	☑	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐	20	vlan20	☑	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Add New VLAN

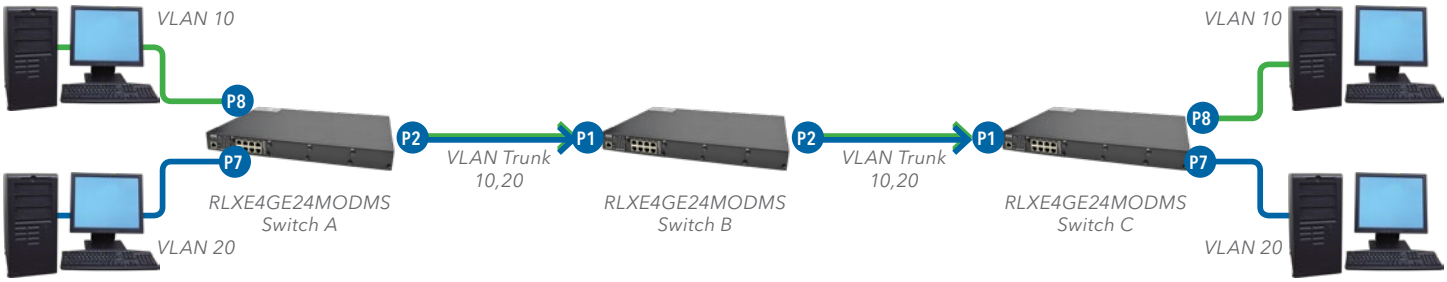
Auto-refresh ☐ Refresh

Ethertype for Custom S-ports 0x 88A8

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN Mode	Port VLAN ID	Tx Tag
*	<>	☐	<>	<>	1	<>
1	C-port	☐	Tagged	Specific	1	Tag_all
2	Unaware	☐	All	None	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	☐	Untagged	Specific	10	Untag_pvid
7	Unaware	☐	Untagged	Specific	20	Untag_pvid
8	Unaware	☐	Untagged	Specific	30	Untag_pvid
9	Unaware	☐	All	Specific	1	Untag_pvid
10	Unaware	☐	All	Specific	1	Untag_pvid

VLAN 1Q Trunk mode



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

Refresh |<< >>

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 13 14 15 16 17 18 19 20 21 22 23 24 25 26
☐	1	default	☑ ☑
☐	10	vlan10	☑ ☑ ☐
☐	20	vlan20	☑ ☑ ☐

Add New VLAN

Auto-refresh ☐ Refresh

Ethertype for Custom S-ports 0x 88A8

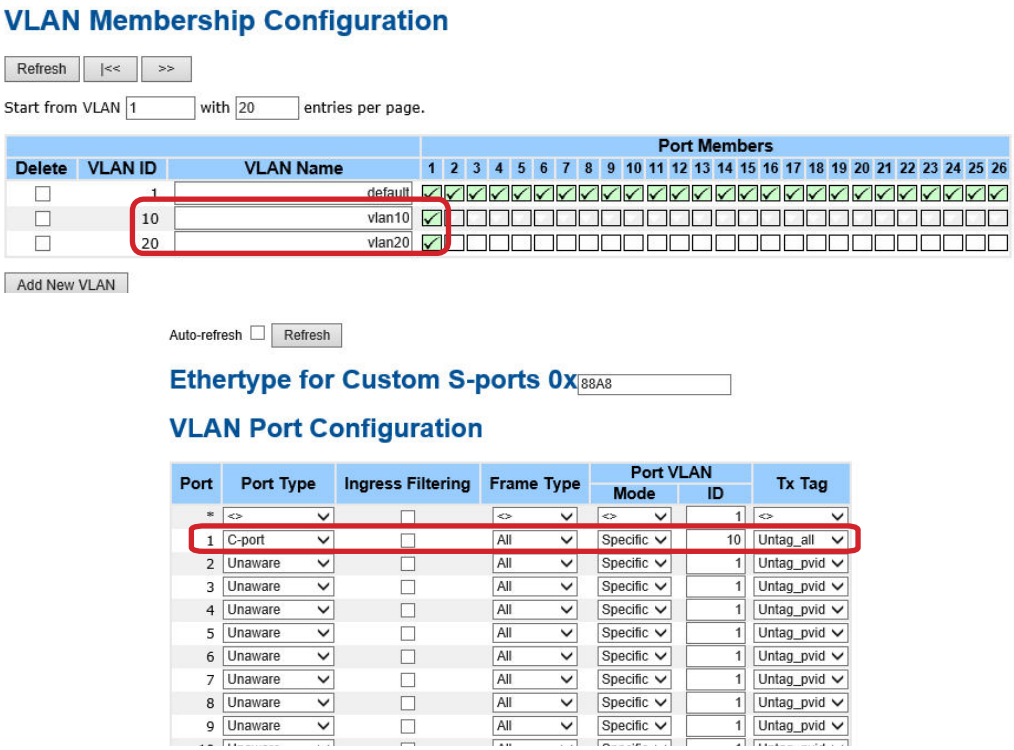
VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN Mode	Port VLAN ID	Tx Tag
*	<>	☐	<>	<>	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

VLAN Hybrid mode

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

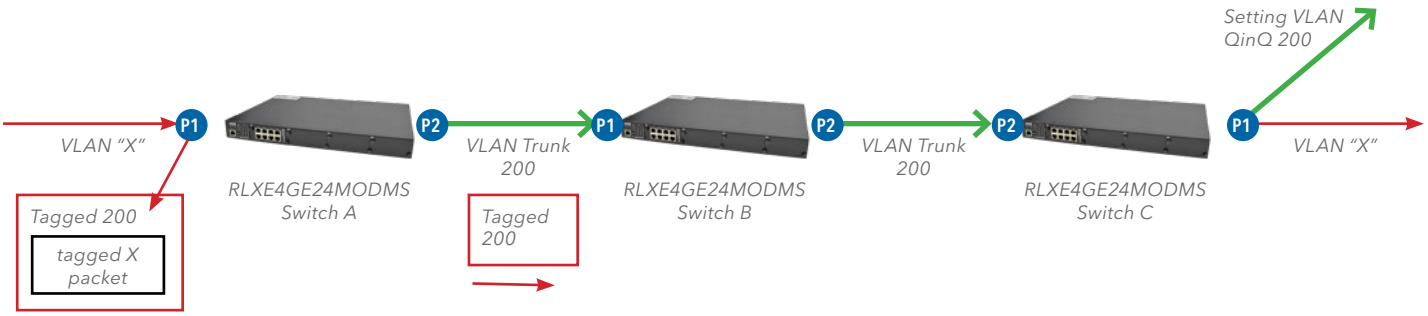
Configure the VLAN for the Switch as shown



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

Refresh |<< >>

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	VLAN Name	Port Members
☐	1	default	☑ ☑
☐	200	QinQ	☑ ☑ ☐

Add New VLAN

Auto-refresh ☐ Refresh

Ethertype for Custom S-ports 0x 88A8

VLAN Port Configuration

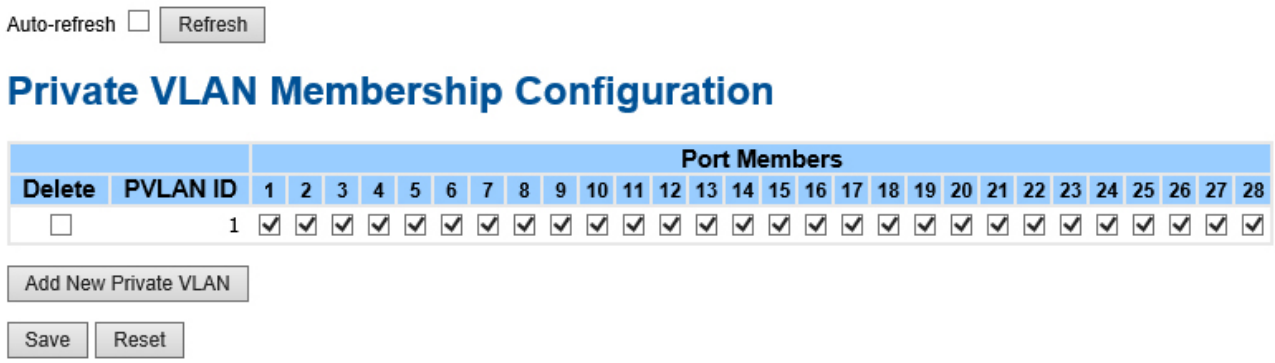
Port	Port Type	Ingress Filtering	Frame Type	Port VLAN Mode	Port VLAN ID	Tx Tag
*	<>	☐	<>	<>	1	<>
1	Unaware	☐	All	Specific	200	Untag_all
2	C-port	☐	Tagged	None	1	Tag_all
3	Unaware	☐	All	Specific	1	Untag_pvid
4	Unaware	☐	All	Specific	1	Untag_pvid
5	Unaware	☐	All	Specific	1	Untag_pvid
6	Unaware	☐	All	Specific	1	Untag_pvid
7	Unaware	☐	All	Specific	1	Untag_pvid
8	Unaware	☐	All	Specific	1	Untag_pvid
9	Unaware	☐	All	Specific	1	Untag_pvid

Private VLAN

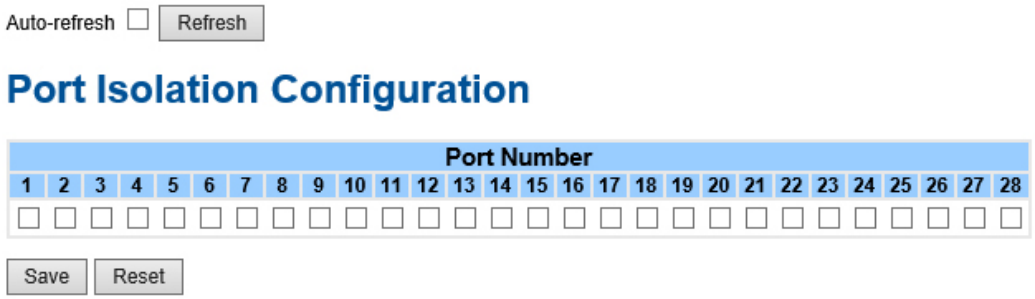
The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means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

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

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



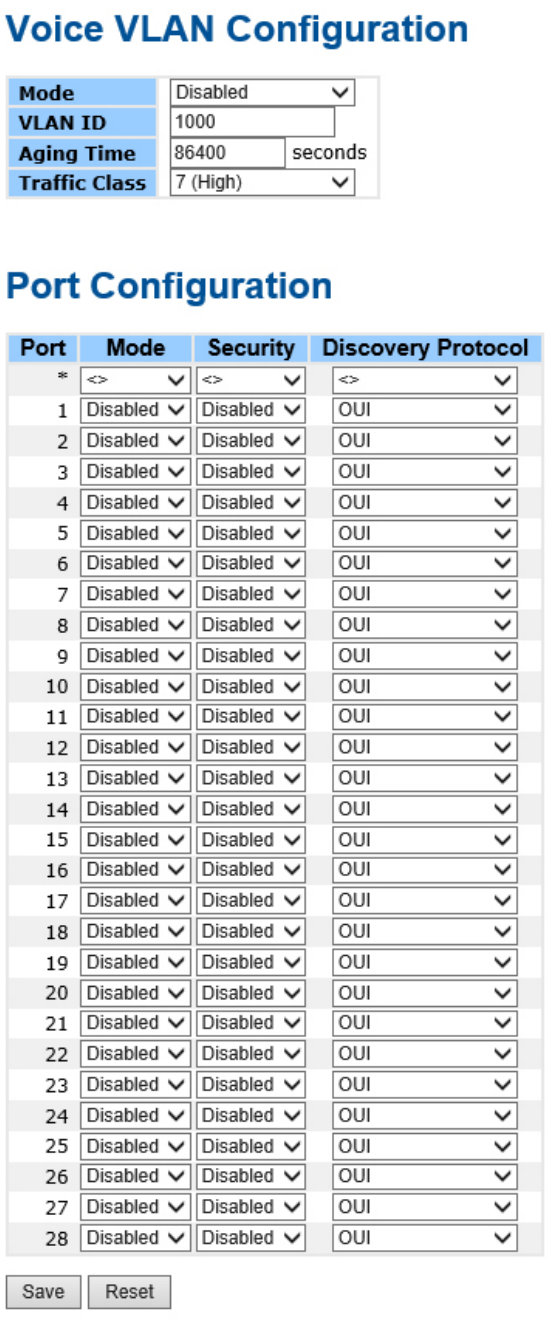
Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Private VLAN ID	Indicates the ID of this particular private VLAN.
Port Members	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To 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.



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

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.



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. 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

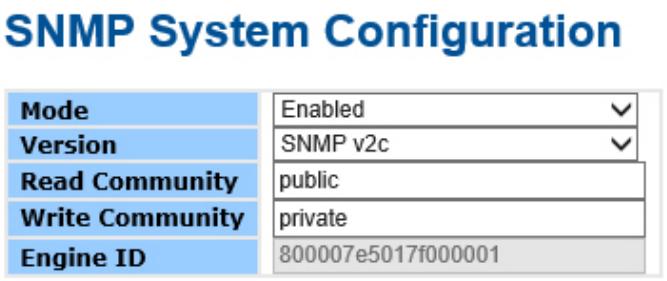
Voice VLAN OUI

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

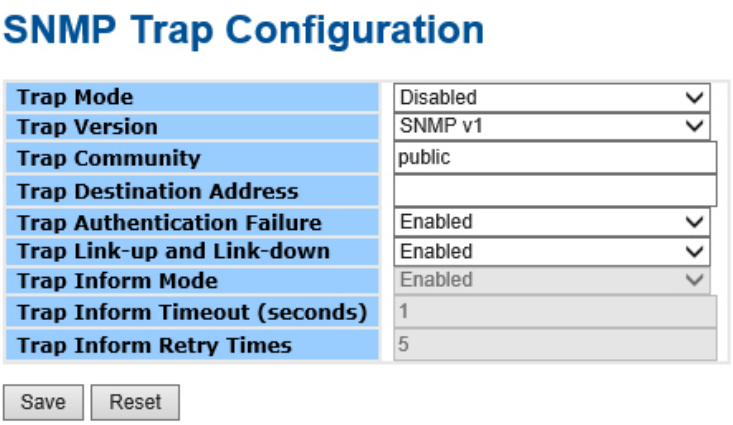
Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Telephony OUI	A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is “xx-xx-xx” (x is a hexadecimal digit).
Description	The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.
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



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.

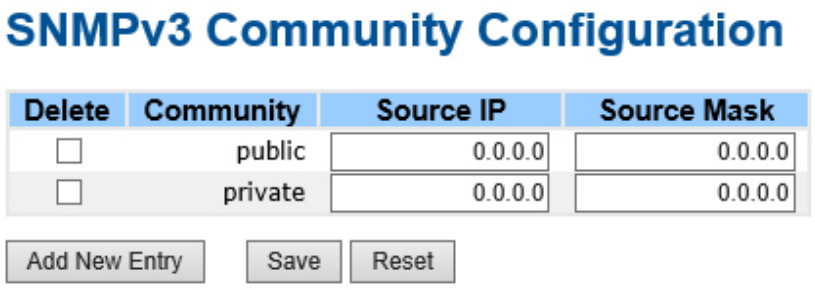


Label	Description
Trap Mode	Indicates the SNMP trap mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.
Trap Version	Indicates the SNMP trap supported version. Possible versions are: SNMP v1: Set SNMP trap supported version 1. SNMP 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

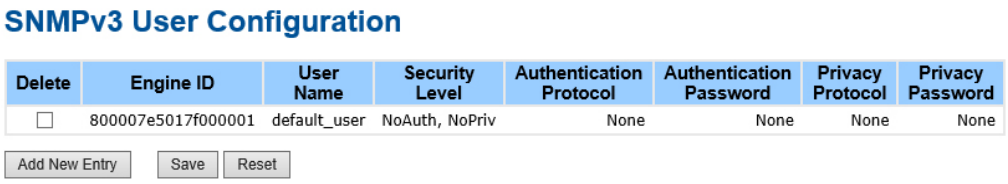
Configure SNMPv3 communities table on this page. The entry index key is Community.



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

SNMP-Users

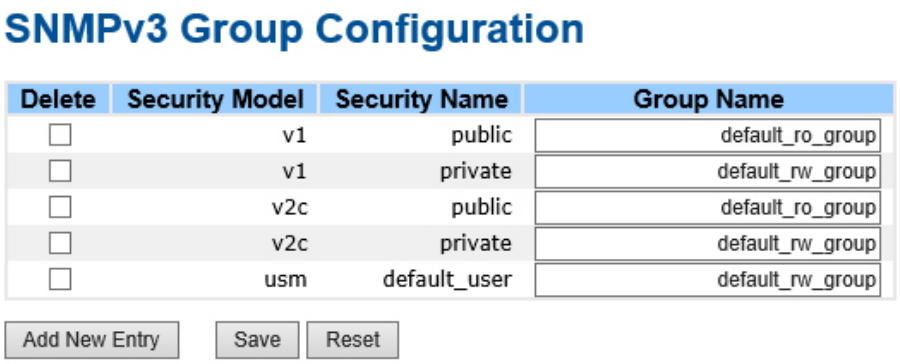
Configure SNMPv3 users table on this page. The entry index keys are Engine ID and User Name.



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID 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

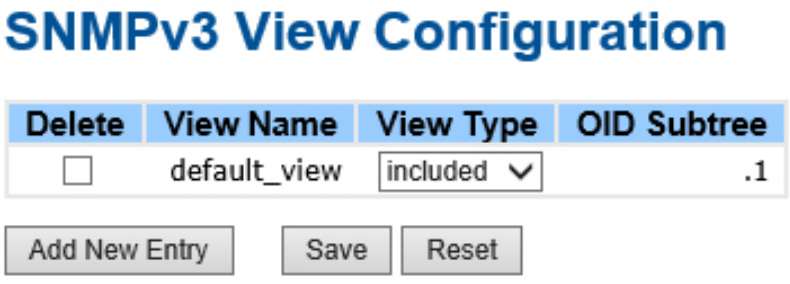
Configure SNMPv3 groups table on this page. The entry index keys are Security Model and Security Name.



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

SNMP-Views

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

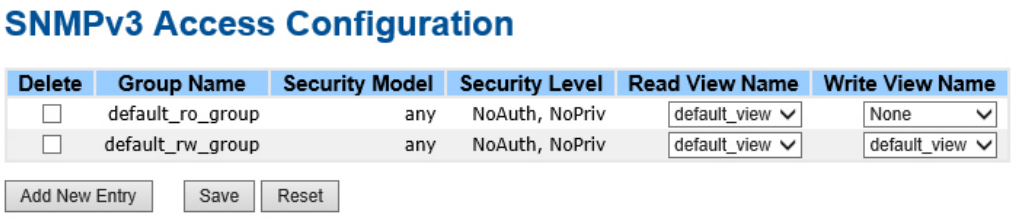


Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

View Type	Indicates the view type that this entry should belong to. Possible view types are: included: An optional flag to indicate that this view subtree should be included. excluded: An optional flag to indicate that this view subtree should be excluded. Generally, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID subtree overstep the 'excluded' view entry.
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is 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.



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.

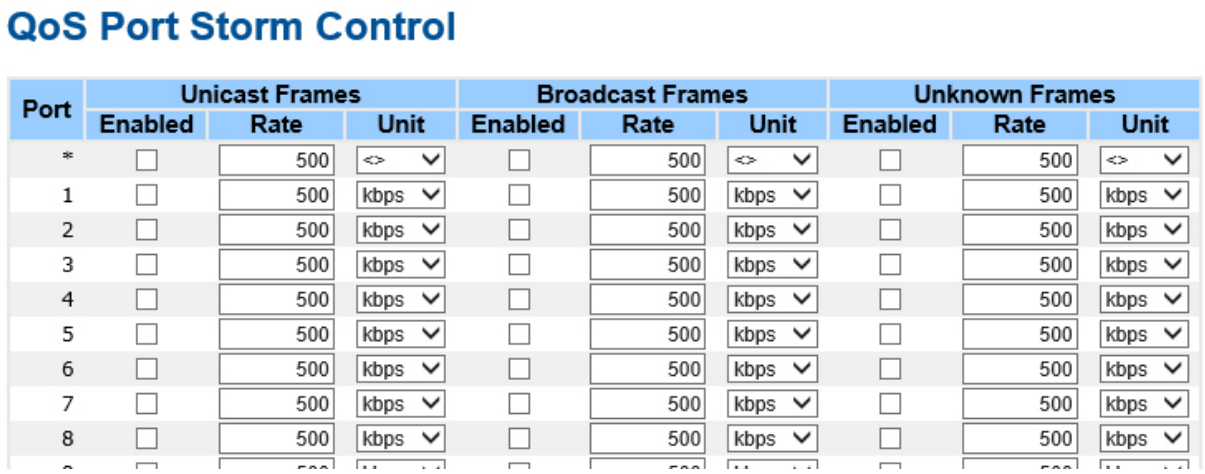
Traffic Prioritization

Storm Control

There is a unicast storm rate control, broadcast storm rate control, and an unknown 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 a numerical figure. The unit of the rate can be either kbps, Mbps, fps or kfps. The configuration indicates the permitted packet rate for unicast, broadcast, or unknown traffic across the switch.

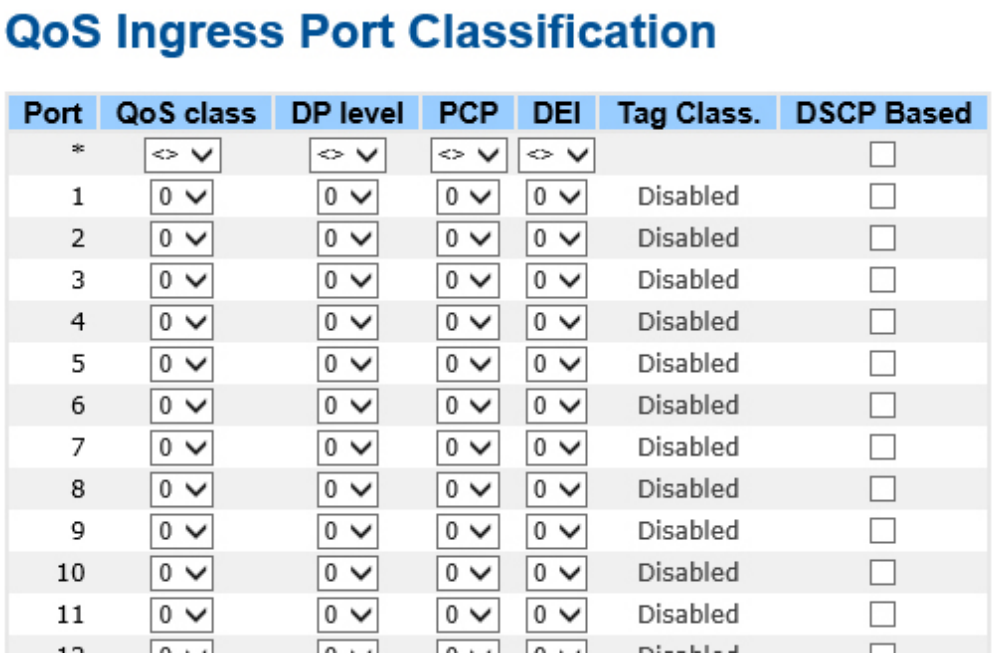
Note: Frames, which are sent to the CPU of the switch are always limited to approximately 4 kpps. For example, broadcasts in the management VLAN are limited to this rate.



Label	Description
Frame Type	The settings in a particular column apply to the frame type listed here: unicast, broadcast, or unknown.
Enable	Enable or disable the storm control status for the given frame type on the given port.
Rate/Unit	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”.

Port Classification

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

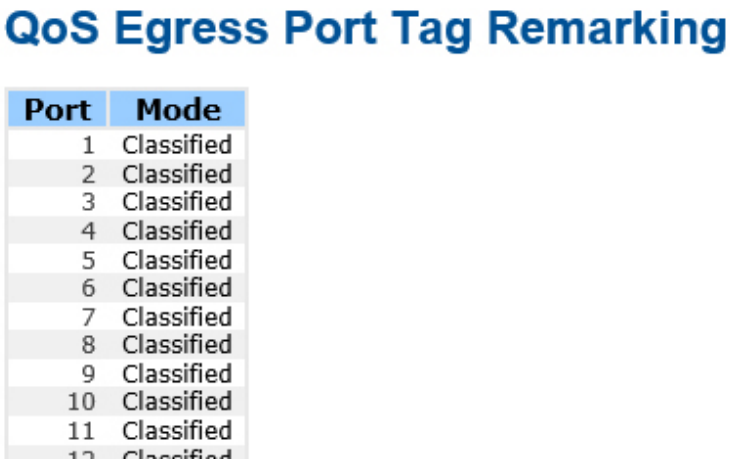


Label	Description
Port	The port number for which the configuration below applies
QoS Class	Controls the default QoS class. All frames are classified to a QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority. If the port is VLAN 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.
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

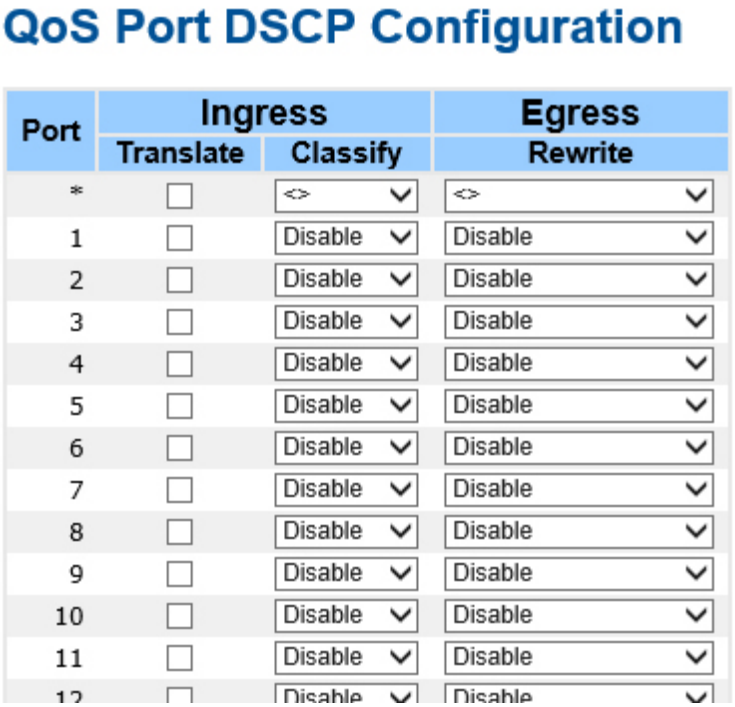
This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.



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.

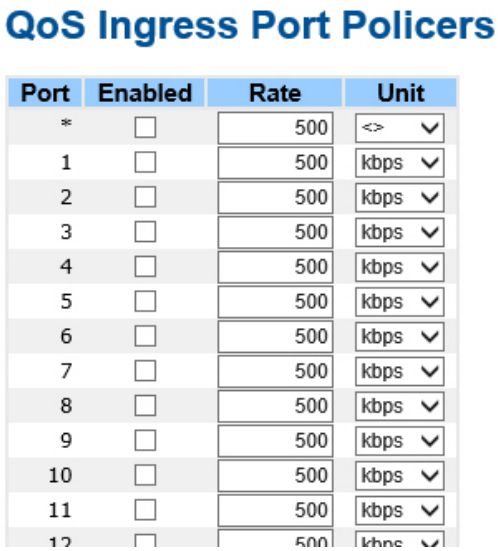


Label	Description
Port	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
Ingress	In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: 1. 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

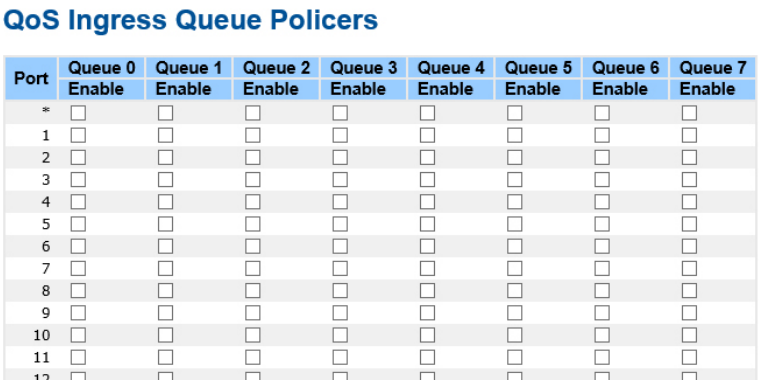
This page allows you to configure the Policer settings for all switch ports.



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".

Queue Policing

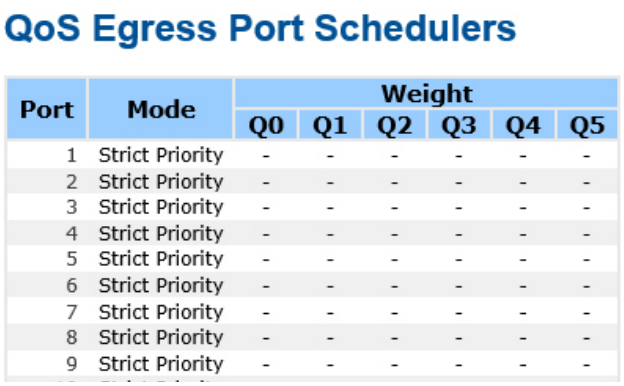
This page allows you to configure the Queue Policer settings for all switch ports.



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

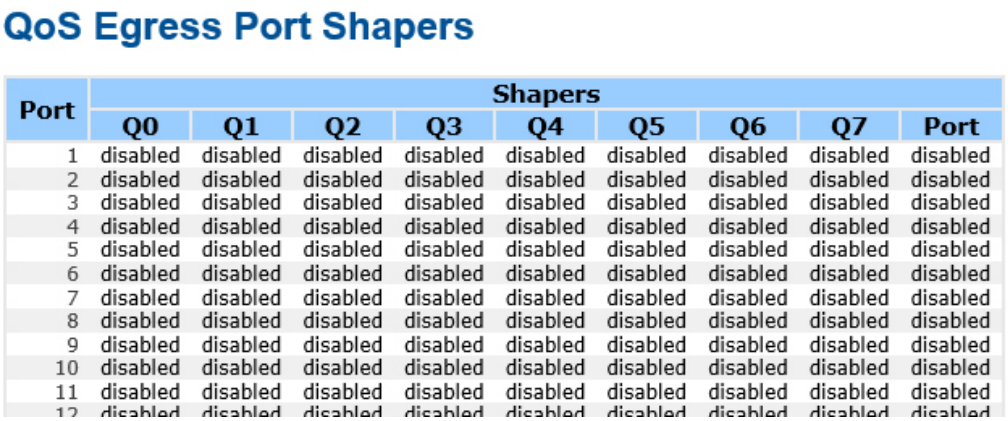
This page provides an overview of QoS Egress Port Schedulers for all switch ports.



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.



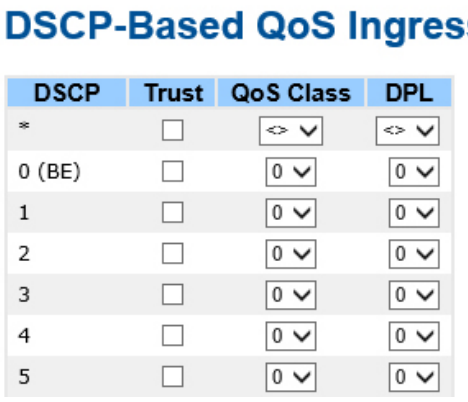
QoS Egress Port Shapers

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.



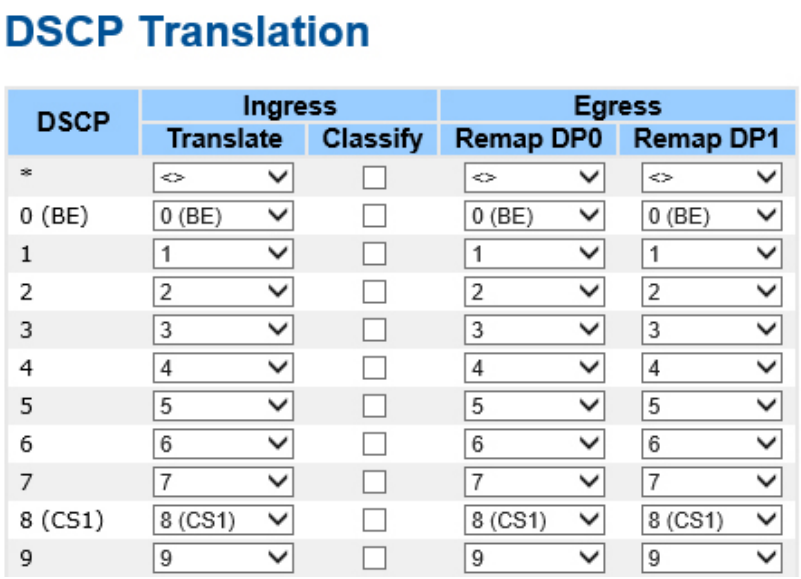
DSCP-Based QoS Ingress Classification

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

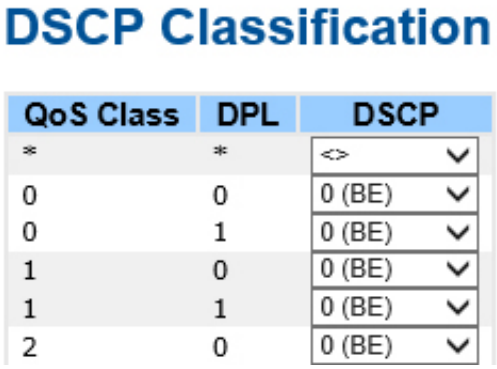
This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.



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

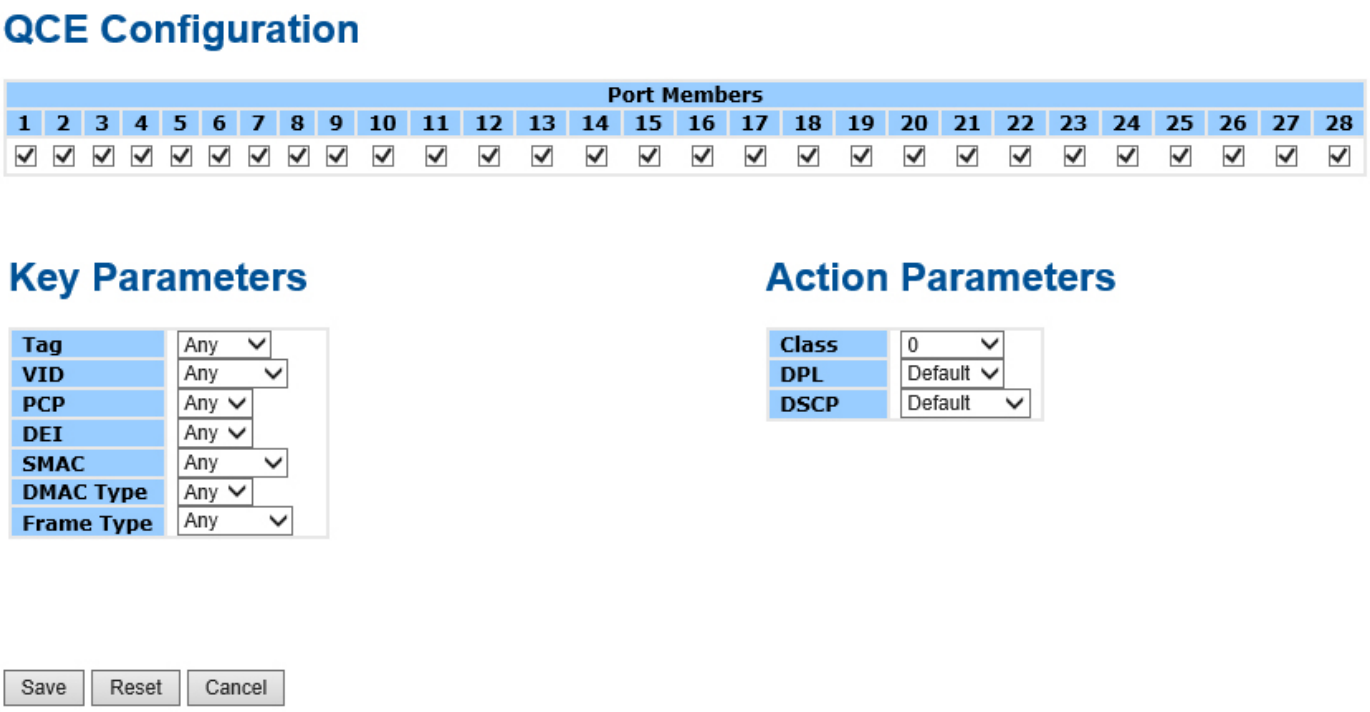
This page allows you to configure the mapping of QoS class and Drop Precedence Level to DSCP value.



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.

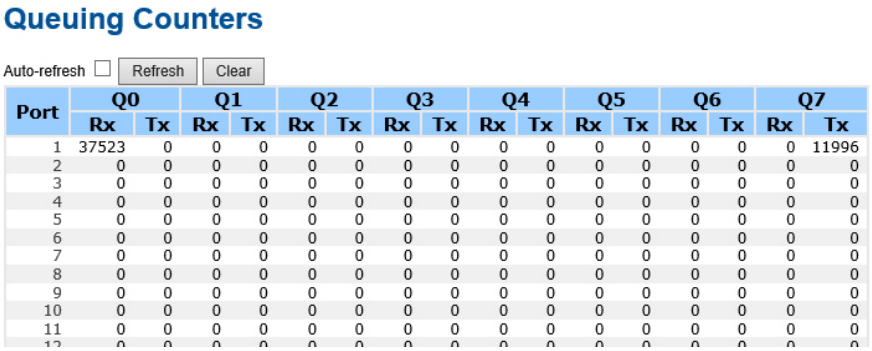


Label	Description
Port Members	Check the checkbox button to include the port in the QCL entry. By default all ports are included.
Key Parameters	Key configuration is described as below: **Tag** Value of Tag field can be 'Any', 'Untag' or 'Tag'. VID Valid value of VLAN ID can be any value in the range 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'.
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.

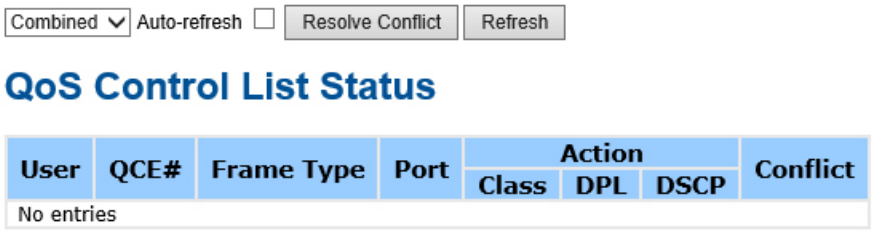


Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	37523	0	0	0	0	0	0	0	0	0	0	0	0	0	0	11996
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0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

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.

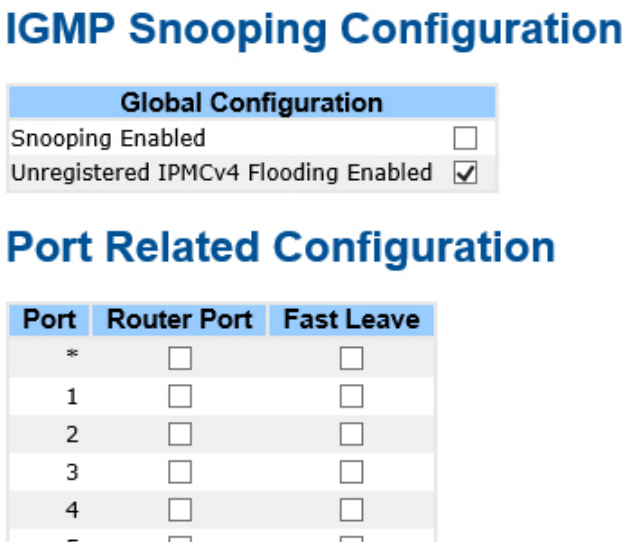


Label	Description
User	Indicates the QCL user.
QCE#	Indicates the index of QCE.
Frame Type	Indicates the type of frame to look for incoming frames. Possible frame types are: Any: The QCE will match all frame type. Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. LLC: Only (LLC) 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.



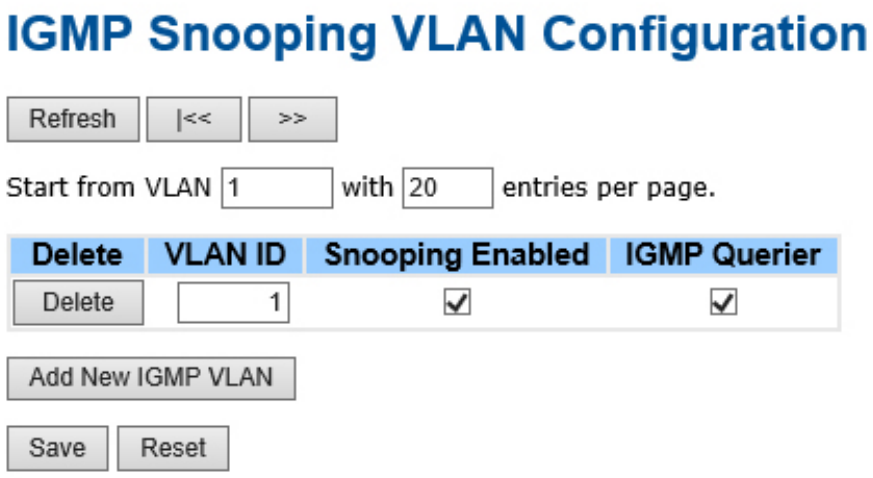
Label	Description
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMCv4Flooding enabled	Enable unregistered IPMC traffic flooding.
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP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

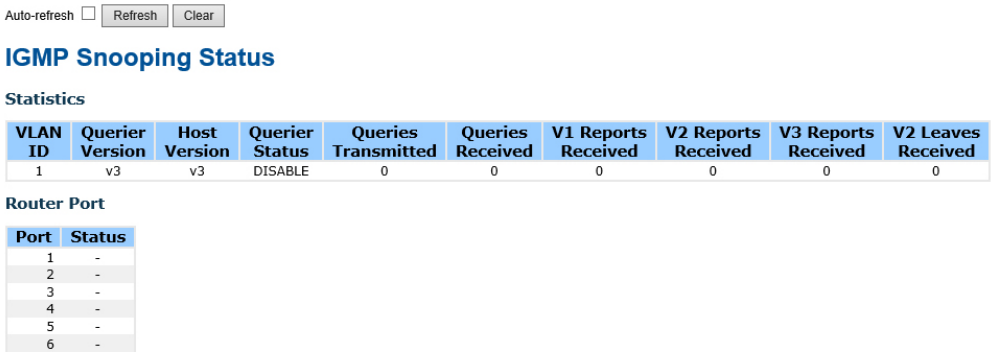
The **>>** will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the **|<<** button to start over.



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

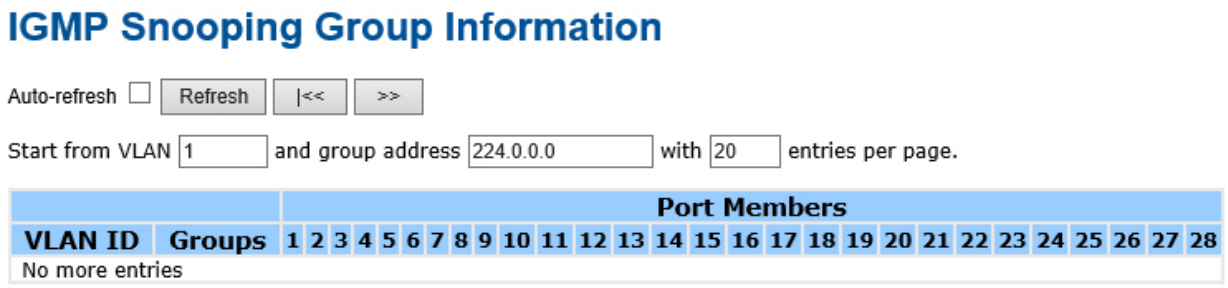
This page provides IGMP Snooping status.



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.



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

Remote Control Security

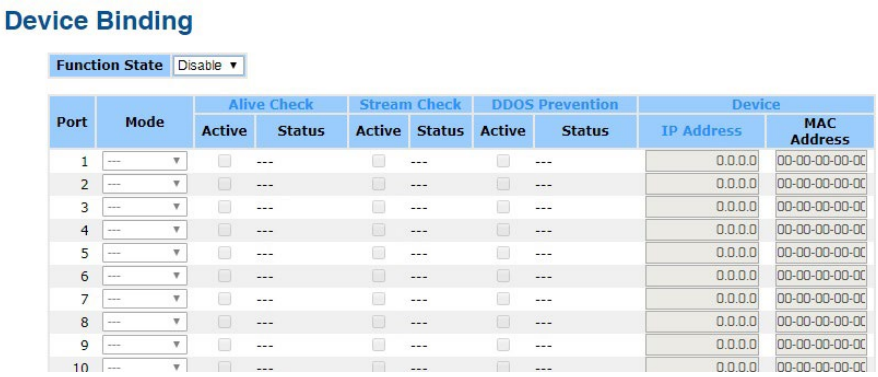
Remote Control Security allows you limit the remote access of management interface. When enabled, the request of client which is not in the allow list will be rejected.

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

Device Binding Configuration

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

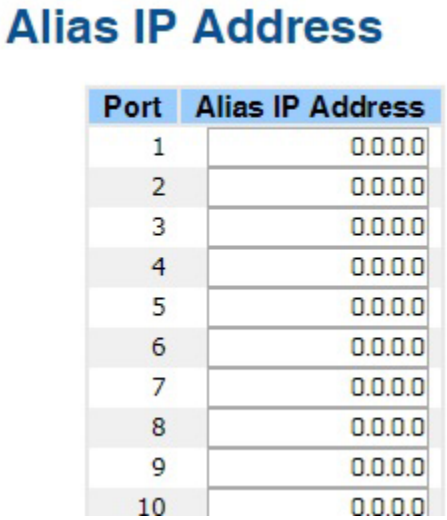


Label	Description
Function State	Enable/Disable Device Binding.
Mode	Indicates the per-port Device Binding operation. Possible modes are: ---: Disable. Scan: Scan IP/MAC automatically, but no binding function. Binding: Enable binding function. Under this mode, any IP/MAC doesn't match the entry will 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 been 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 Active	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.

Label	Description
Device IP Address	Specify the IP Address of device.
Device MAC Address	Specify the MAC Address of device.
Save	Click to save changes.

Alias IP Address Configuration

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



Label	Description
Alias IP Address	Specify Alias IP address. Keeps “0.0.0.0”, if the device doesn’t have alias IP address.
Save	Click to save changes.

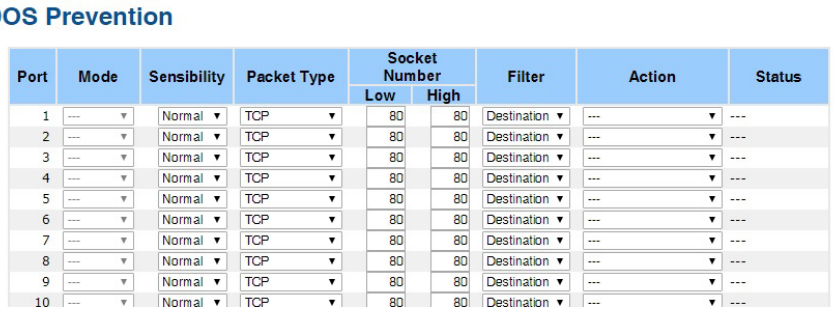
Alive Check Configuration

This page provides Alive Check related configuration.

Label	Description
Mode	Enable/Disable Alive Check of the port.
Action	Indicates the action when alive check failed. Possible actions are: ---: Do nothing. Link Change: Link down the port, and link up once. Shunt 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.
Status	Indicates the Alive Check status. Possible statuses are: ---: Disable. Analysing: Analyse the packet throughput for initialization. Running: Function ready. Attacked: DDOS attack happened.
Save	Click to save changes.

DDOS Prevention Configuration

This page provides DDOS Prevention related configuration. Switch could monitor the ingress packets, and do some actions when DDOS attack happened on this port. Configure these setting helps the prevention become more suitable.

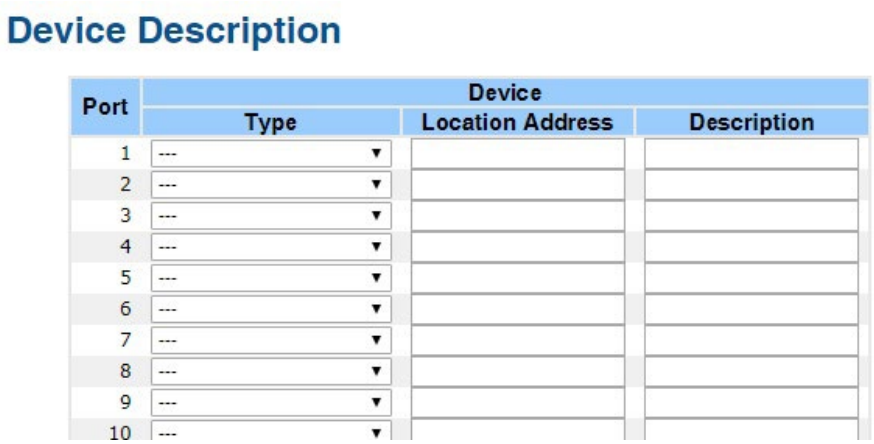


Label	Description
Mode	Enable/Disable DDOS Prevention of the port.
Sensibility	Indicates the level of DDOS detection. Possible levels are: Low: Low sensibility. Normal: Normal sensibility. Medium: Medium sensibility. High: High sensibility.
Packet Type	Indicates the packet type of DDOS monitor. Possible 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.
Filter	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. Shunt 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.
Save	Click to save changes.

Device Description Configuration

This page provides Device Description related configuration.



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.
Save	Click to save changes.

Stream Check Configuration

This page provides Stream Check related configuration.

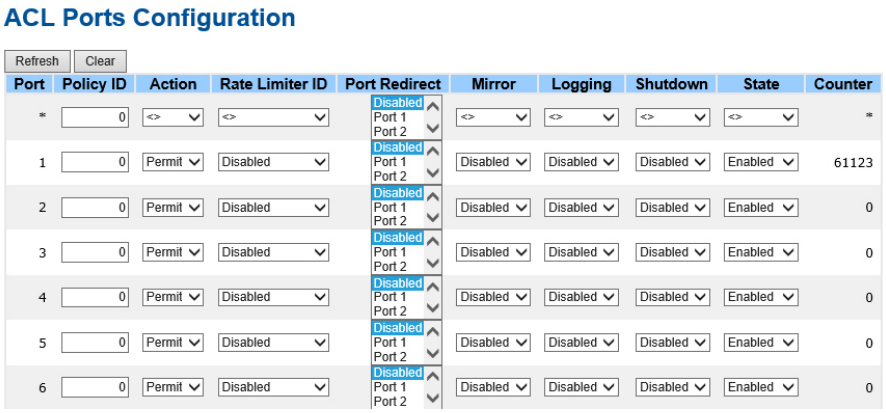
Label	Description
Mode	Enable/Disable stream monitor of the port.
Action	Indicates the action when stream getting low. Possible actions are: ---: Do nothing. Log it: Just log the event.
Save	Click to save changes.

Security

ACL

Ports

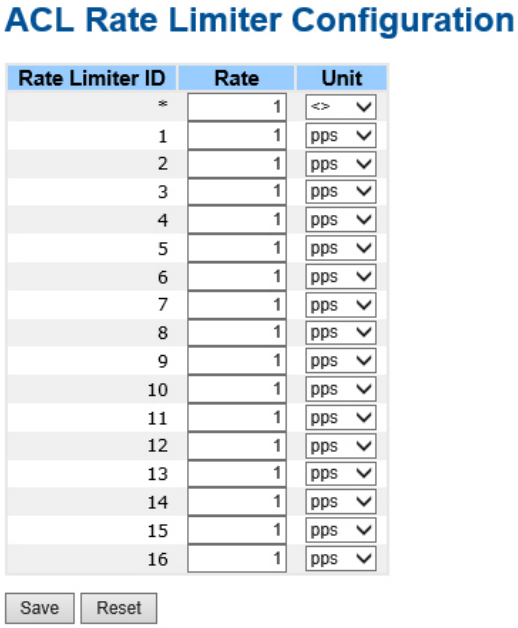
Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.



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.



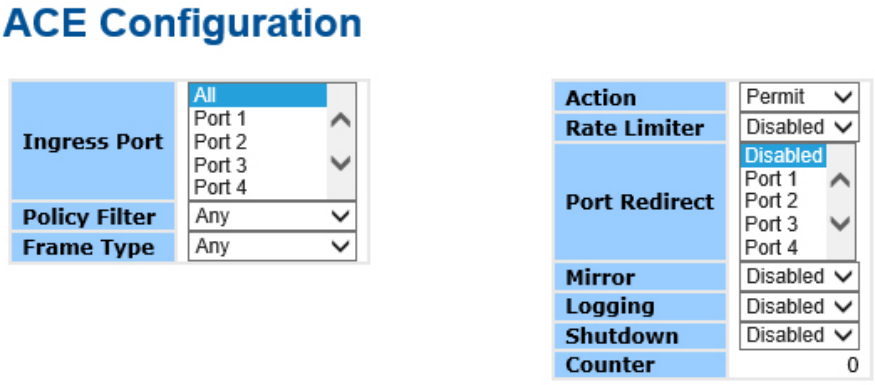
Label	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate	The rate unit is packet per second (pps), configure the rate as 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. The 1 kpps is actually 1002.1 pps.

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.



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

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

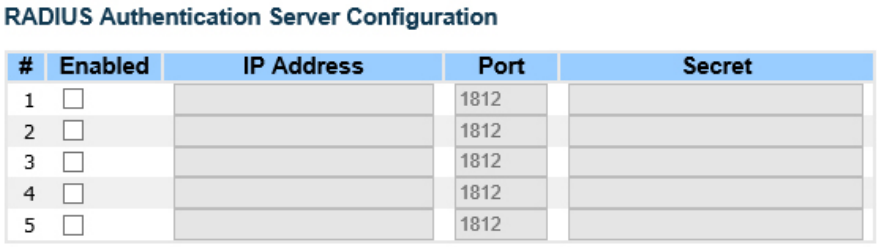
Common Server Configuration

This page allows you to configure the Authentication Servers

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

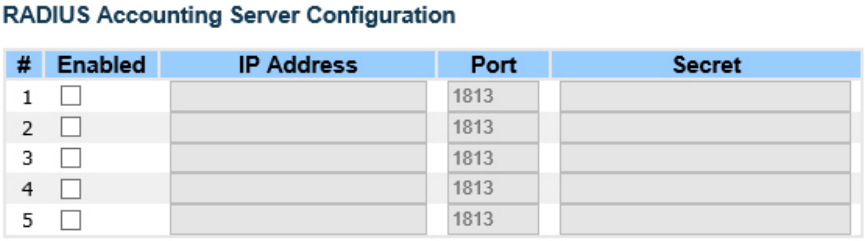
The table has one row for each RADIUS Authentication Server and a number of columns, which are:


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

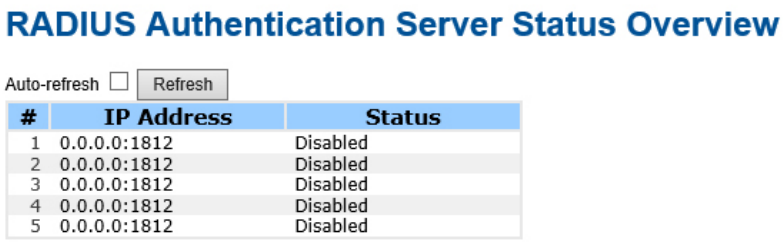
#	Enabled	IP Address	Port	Secret
1	☐		1813	
2	☐		1813	
3	☐		1813	
4	☐		1813	
5	☐		1813	

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

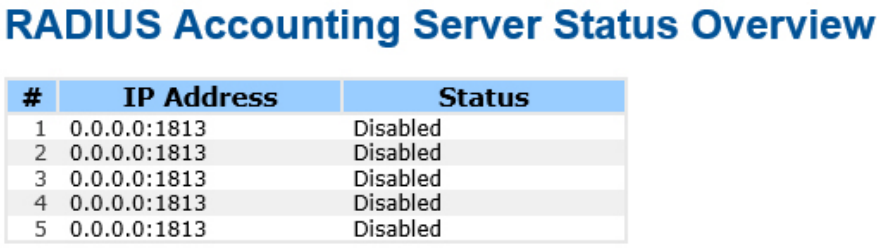
This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page.

RADIUS Authentication Servers



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



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

Label	Description
Packet Counters	RADIUS authentication server packet counter. There are seven receive and four transmit counters.
Other Info	This section contains information about the state of the server and the latest round-trip time.

Direction	Name	RFC4668 Name	Description
Rx	**Access Accepts**	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	**Access Rejects**	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	**Access Challenges**	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	**Malformed Access Responses**	radiusAuthClientExtMalformedAccessResponses	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.
Rx	**Bad Authenticators**	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	**Unknown Types**	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Rx	**Packets Dropped**	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx	**Access Requests**	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	**Access Retransmissions**	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx	**Pending Requests**	radiusAuthClientExtPendingRequests	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.
Tx	**Timeouts**	radiusAuthClientExtTimeouts	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.

Name	RFC4668 Name	Description
State	-	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.
Round-Trip Time	radiusAuthClientExtRoundTripTime	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.

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

Label	Description
Packet Counters	RADIUS accounting server packet counter. There are five receive and four transmit counters.
Other Info	This section contains information about the state of the server and the latest

Direction	Name	RFC4670 Name	Description
Rx	Responses	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	Malformed Responses	radiusAccClientExtMalformedResponses	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.
Rx	Bad Authenticators	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	Unknown Types	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	Packets Dropped	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	Requests	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	Retransmissions	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	Pending Requests	radiusAccClientExtPendingRequests	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.
Tx	Timeouts	radiusAccClientExtTimeouts	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.

Name	RFC4670 Name	Description
State	-	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 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.
Round-Trip Time	radiusAccClientExtRoundTripTime	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.

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.

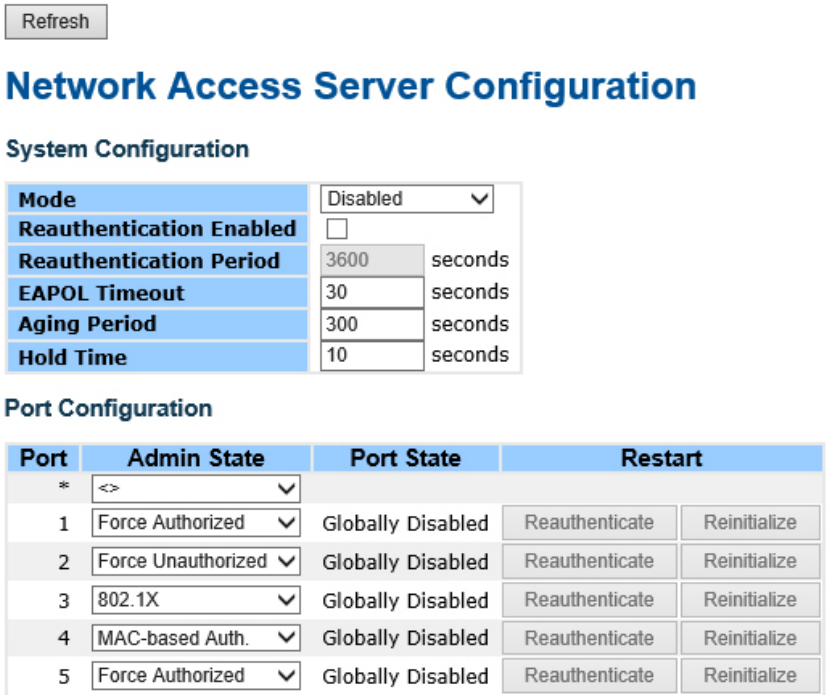
Overview of MAC-Based Authentication

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.



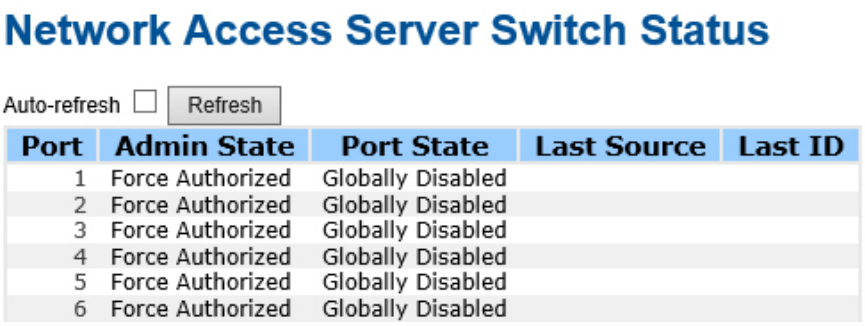
Label	Description
Mode	Indicates if 802.1X and MAC-based authentication is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
Reauthentication Enabled	If checked, clients are reauthenticated after the interval specified by the Reauthentication 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.
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.

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.

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.



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.

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.
EAPOL Counters	These supplicant frame counters are available for the following administrative states: • Force Authorized • Force Unauthorized • 802.1X

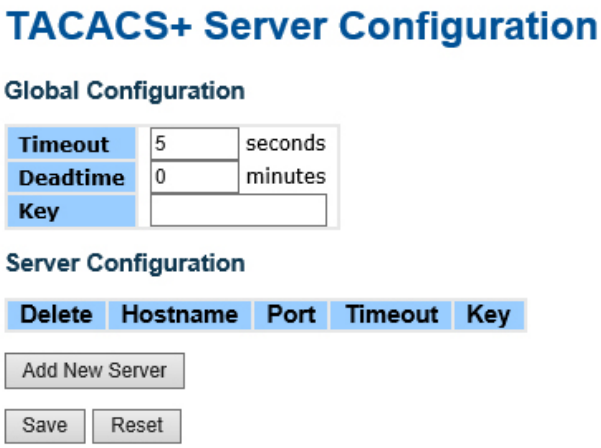
EAPOL Counters

Direction	Name	IEEE Name	Description
Rx	**Total**	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	**Response ID**	dot1xAuthEapolRespIdFramesRx	The number of valid EAP Resp/ID frames that have been received by the switch.
Rx	**Responses**	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch.
Rx	**Start**	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	**Logoff**	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL logoff frames that have been received by the switch.
Rx	**Invalid Type**	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	**Invalid Length**	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	**Total**	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	**Request ID**	dot1xAuthEapolReqIdFramesTx	The number of EAP initial request frames that have been transmitted by the switch.
Tx	**Requests**	dot1xAuthEapolReqFramesTx	The number of valid EAP Request frames (other than initial request frames) that have been transmitted by the switch.

<table>
<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>Access Challenges</td><td>dot1xAuthBackendAccessChallenges</td><td>Port-based:
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.
MAC-based:
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>Other Requests</td><td>dot1xAuthBackendOtherRequestsToSupplicant</td><td>Port-based:
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.
MAC-based:
Not applicable.</td></tr>
<tr><td>Rx</td><td>Auth. Successes</td><td>dot1xAuthBackendAuthSuccesses</td><td>Port- and MAC-based:
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>Auth. Failures</td><td>dot1xAuthBackendAuthFails</td><td>Port- and MAC-based:
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>Responses</td><td>dot1xAuthBackendResponses</td><td>Port-based:
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.
MAC-based:
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>
<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>MAC Address</td><td>dot1xAuthLastEapolFrameSource</td><td>The MAC address of the last supplicant/client.</td></tr>
<tr><td>VLAN ID</td><td>-</td><td>The VLAN ID on which the last frame from the last supplicant/client was received.</td></tr>
<tr><td>Version</td><td>dot1xAuthLastEapolFrameVersion</td><td>802.1X-based:
The protocol version number carried in the most recently received EAPOL frame.
MAC-based:
Not applicable.</td></tr>
<tr><td>Identity</td><td>-</td><td>802.1X-based:
The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame.
MAC-based:
Not applicable.</td></tr>
</table>
</td>
</tr>
</table>

TACACS+ Server Configuration Help

This page allows you to configure the TACACS+ servers.



Global Configuration

These settings are common for all of the TACACS+ servers.

Label	Description
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.
Deadtime	Deadtime, which can be set to a number between 0 to 1440 minutes, 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 Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
Key	The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Configuration

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

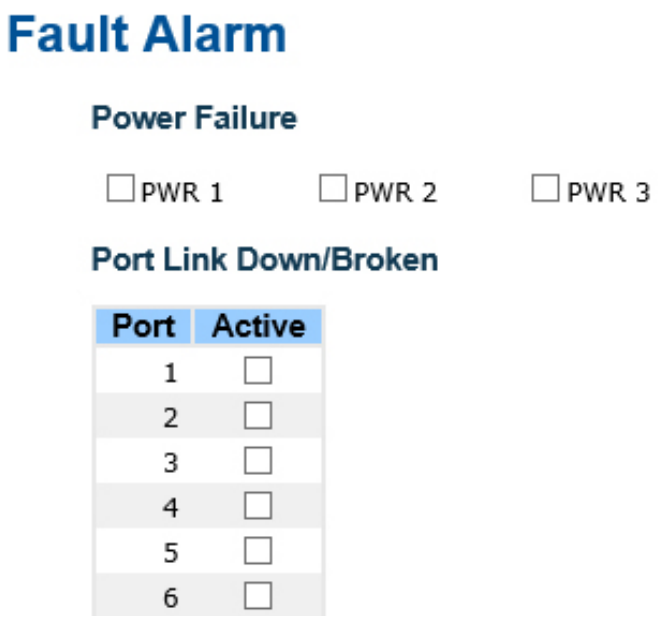
Label	Description
Delete	To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.
Hostname	The IP address of the TACACS+ server.
Port	The TCP port to use on the TACACS+ server for authentication.
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
Key	This optional setting overrides the global key. Leaving it blank will use the global key.

Label	Description
Adding a New Server	Click to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported. The button can be used to undo the addition of the new server.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Warning

Fault Alarm

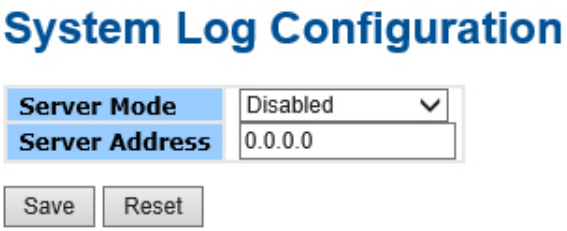
When any selected fault event is happened, the Fault LED in switch panel will light up and the electric relay will signal at the same time.



System Warning

SYSLOG Setting

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



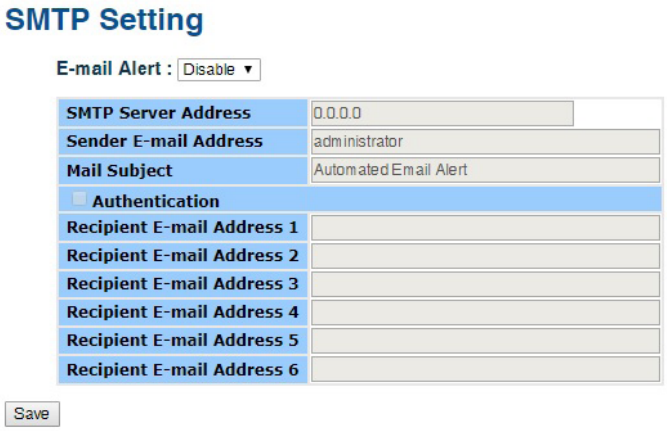
System Warning – SYSLOG Setting interface

The following table describes the labels in this screen.

Label	Description
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 Configuration

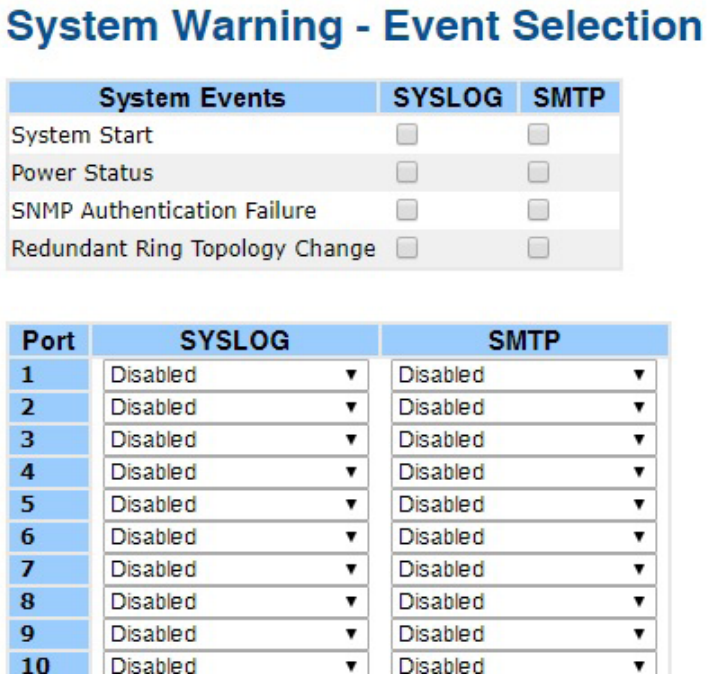
The SMTP is Short for Simple Mail Transfer Protocol. It's a protocol for e-mail transmission across the Internet. Please refer to RFC 821 - Simple Mail Transfer Protocol.



Label	Description
E-mail Alert	Enable/Disable transmission system warning events by e-mail.
SMTP Server Address	The SMTP server IP address(or domain name address).
Sender E-mail Address	The sender's E-mail address of the mail.
Mail Subject	The Subject of the mail.
Authentication	Checked if the SMTP server needs authentication.
Username	The authentication username.
Password	The authentication password.
Confirm Password	Re-enter password.
Recipient E-mail Address	The recipient's E-mail address. It supports 6 recipients for a mail.
Save	Click to save changes.

Event Selection

SYSLOG is the warning method 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 is disabled.



System Warning – Event Selection interface

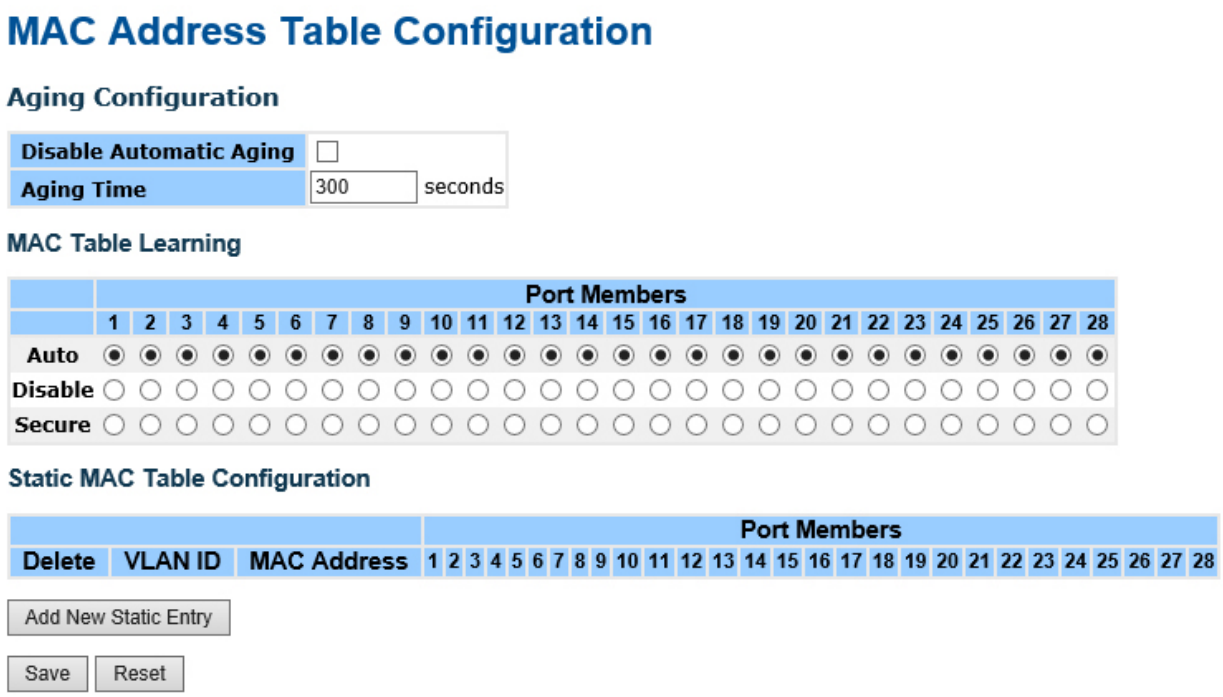
The following table describes the labels in this screen.

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.



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.

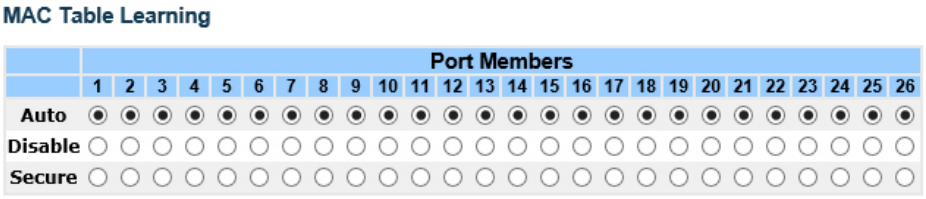
The allowed range is 10 to 1000000 seconds.

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:



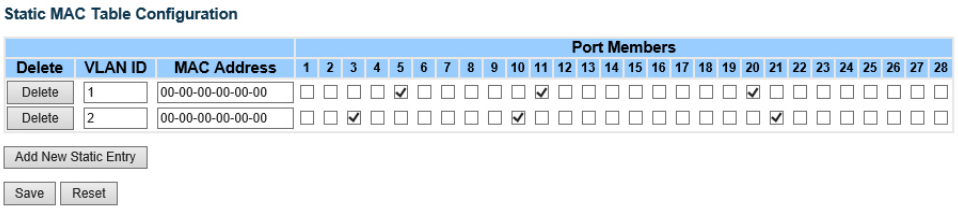
Label	Description
Auto	Learning is done automatically as soon as a frame with unknown SMAC is received.
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped. Note: Make sure that the link used for managing the switch is added to the Static Mac Table before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



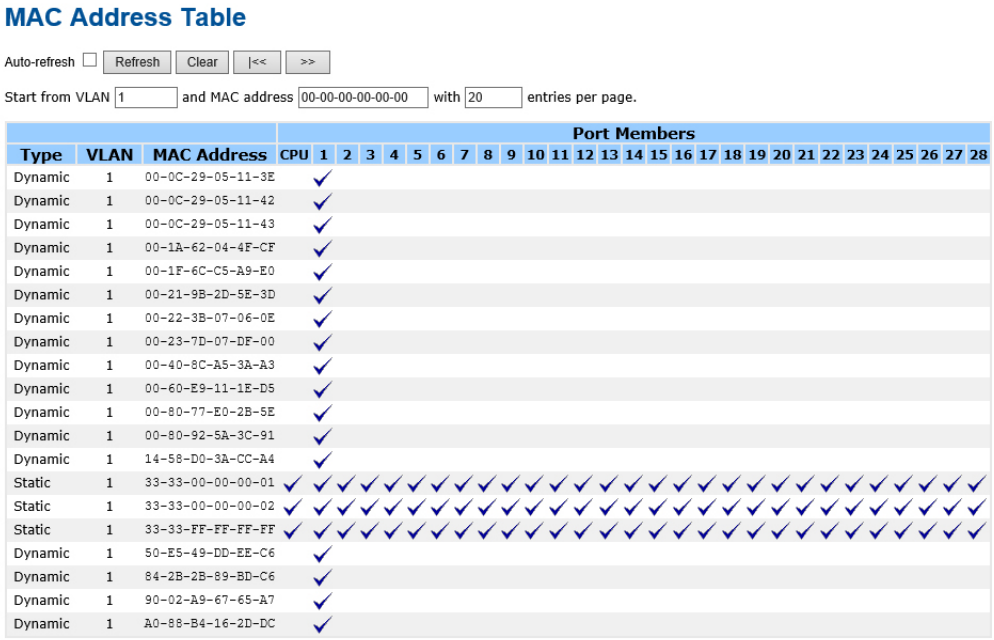
Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Add a New Static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

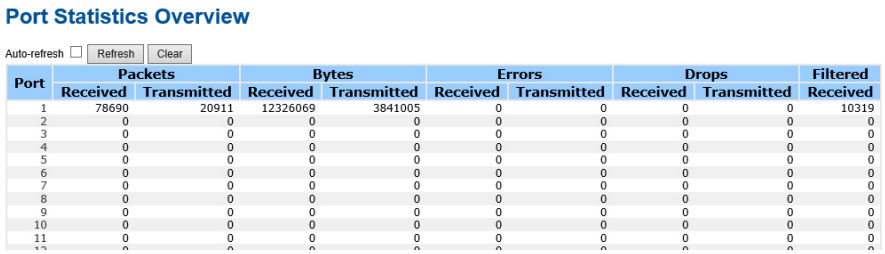


Label	Description
Type	Indicates whether the entry is a static or dynamic entry.
MAC address	The MAC address of the entry.
VLAN	The VLAN ID of the entry.
Port Members	The ports that are members of the entry.

Port Statistic

Traffic Overview

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



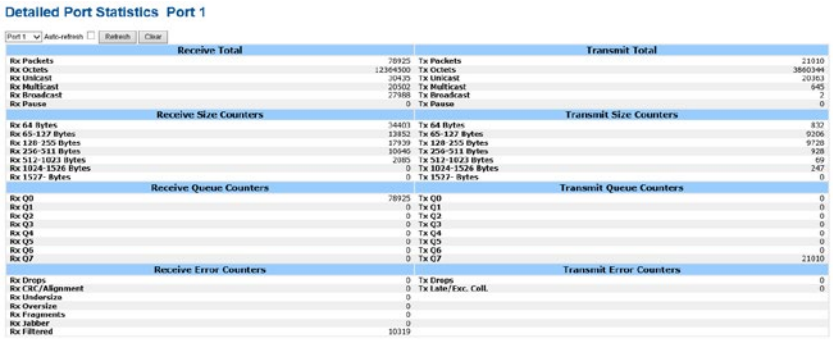
Label	Description
Port	The logical port for the settings contained in the same row.
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions per 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



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

Short frames are frames that are smaller than 64 bytes.

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

Port Monitoring

Configure port Mirroring on this page.

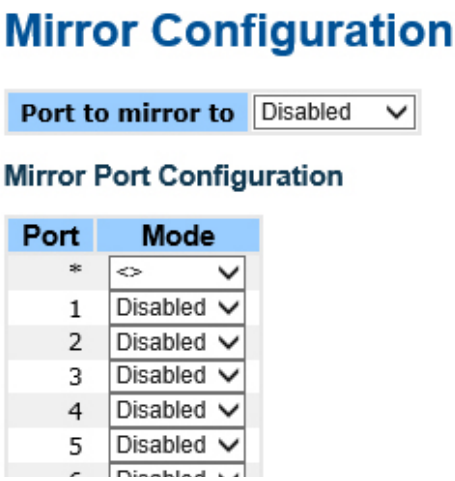
To debug network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow.

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.



Label	Description
Port	The logical port for the settings contained in the same row.
Mode	Select mirror mode. Rx only : Frames received at this port are mirrored to the mirror port. Frames transmitted are not mirrored. Tx only :Frames transmitted from this port are mirrored to the mirror port. Frames received are not mirrored. Disabled : Neither frames transmitted nor frames received are mirrored. Enabled : Frames received and frames transmitted are mirrored to the mirror port. Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames for the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

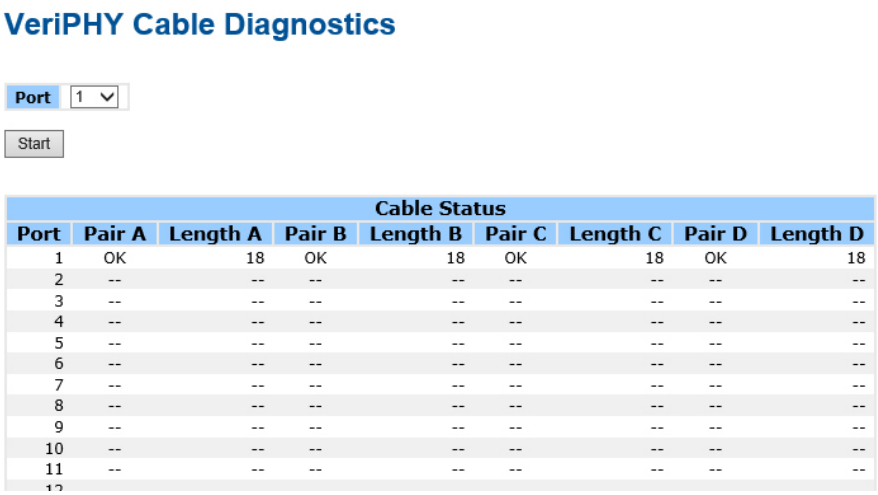
System Log Information

The switch system log information is provided here.

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

Cable Diagnostics

This page is used for running the VeriPHY Cable Diagnostics.



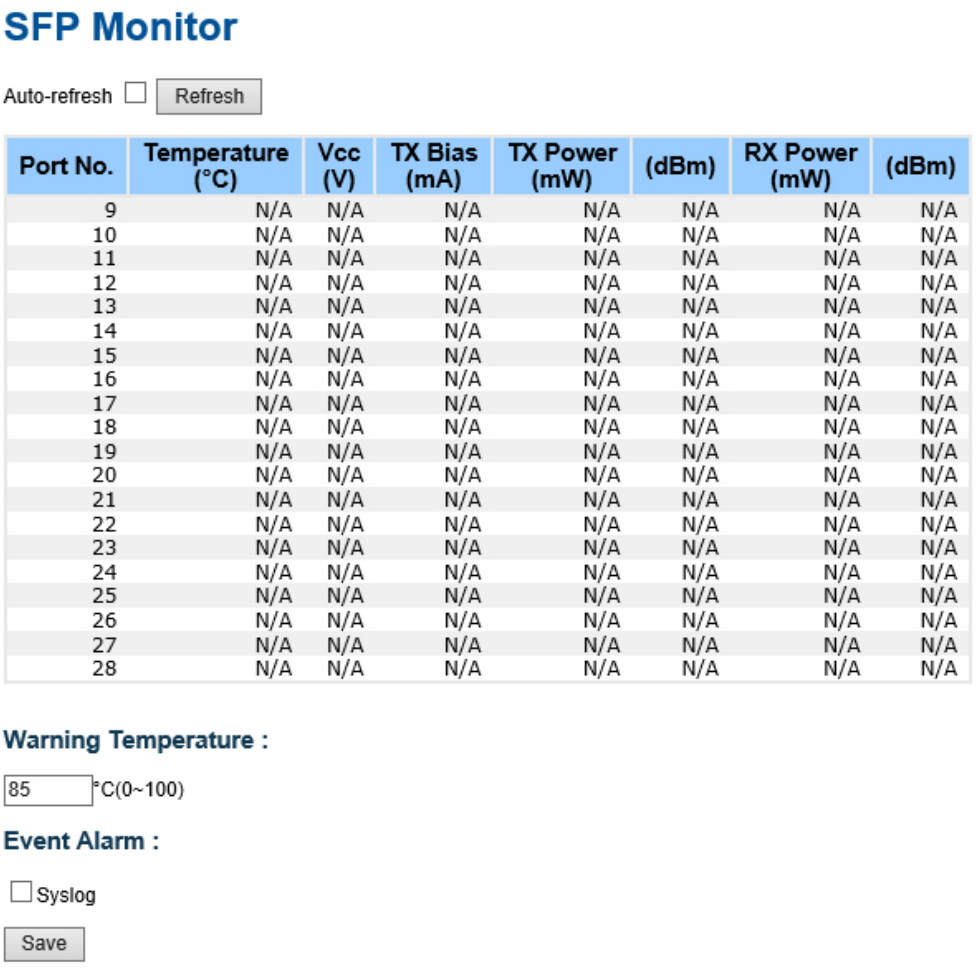
Press **Start** to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate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

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

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

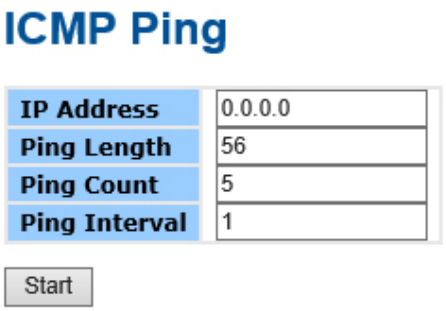
SFP Monitor

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



Ping

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



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

PING6 server ::10.10.132.20

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

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

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

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

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

Sent 5 packets, received 5 OK, 0 bad

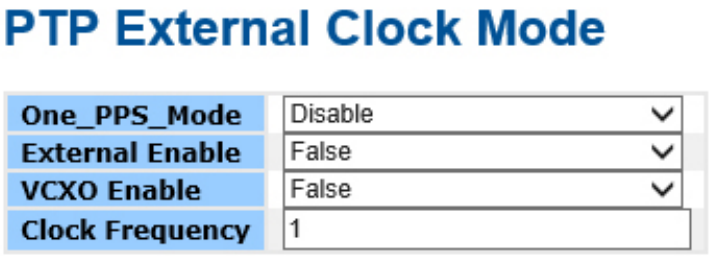
You can configure the following properties of the issued ICMP packets:

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

Syncronization-PTP

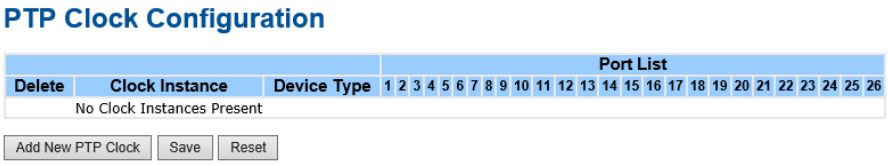
This page allows the user to configure and inspect the current PTP clock settings.

PTP External Clock Mode



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)

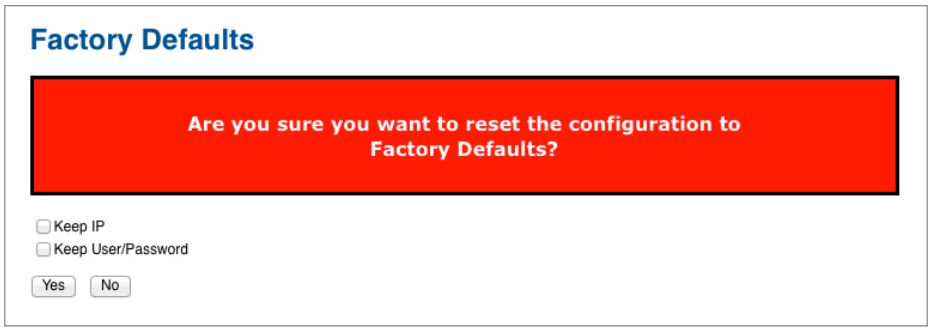
PTP Clock Configuration



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.

Factory Defaults

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



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.

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

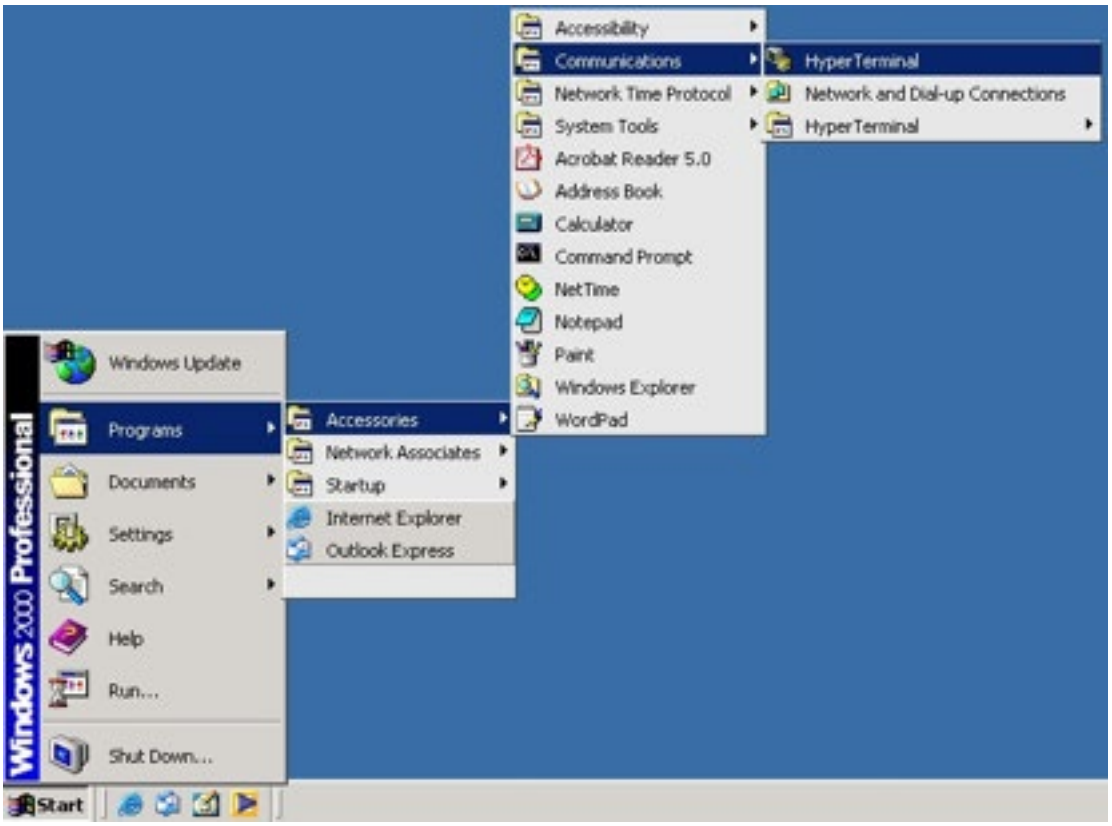
In addition to WEB-base management, the RLXE4GE24MODMS also supports CLI management. You can use console or telnet to management the switch by CLI.

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

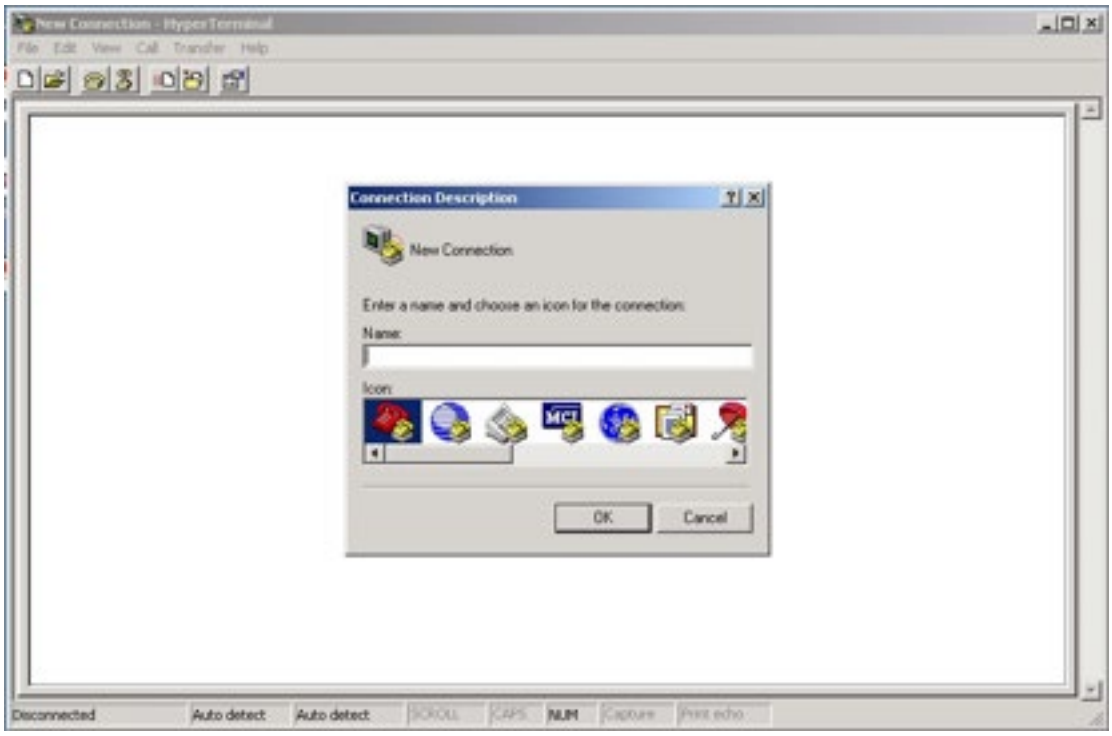
Before Configuring by RS-232 serial console, use an DB-9-M to DB-9-F cable to connect the switches' RS-232 Console port to your PC COM port.

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

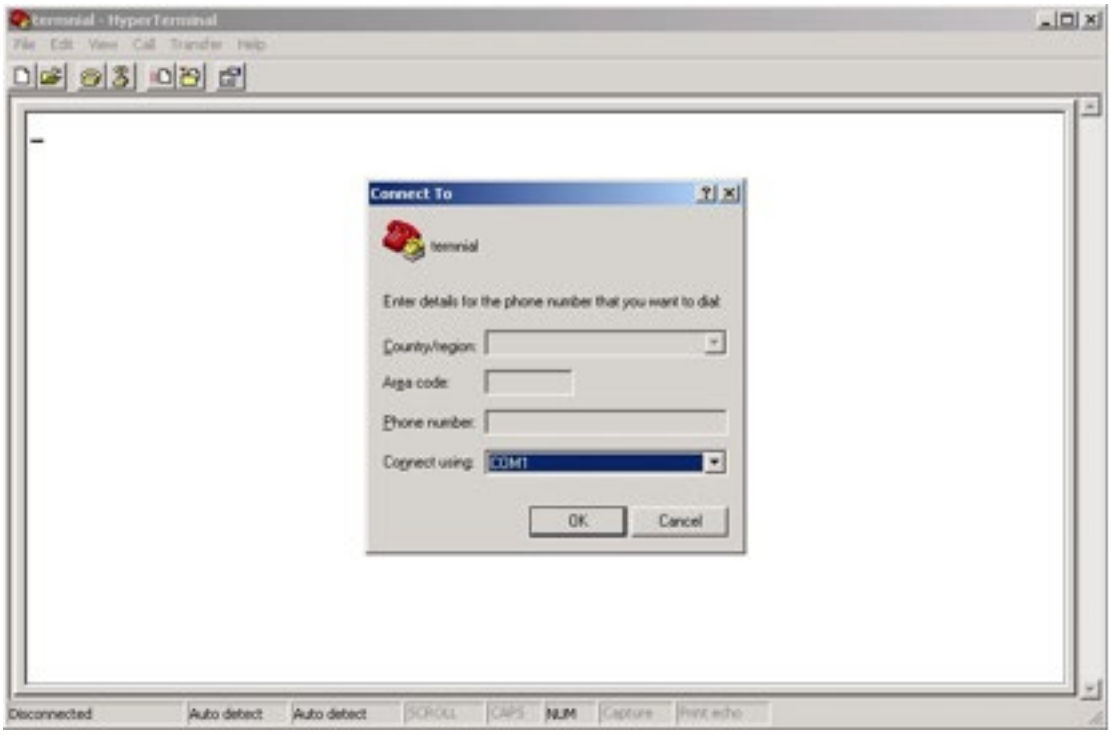
Step 1. From the Windows desktop, Select Start – > Programs – > Accessories – > Communications – > Hyper Terminal



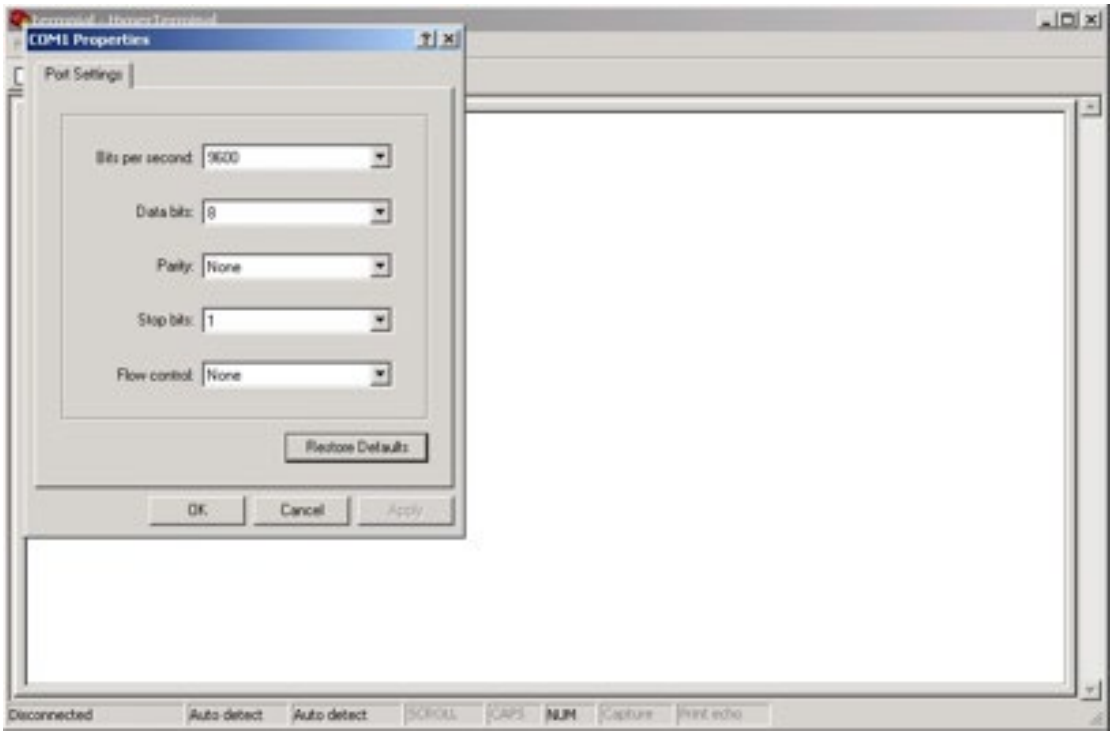
Step 2. Input a name for new connection



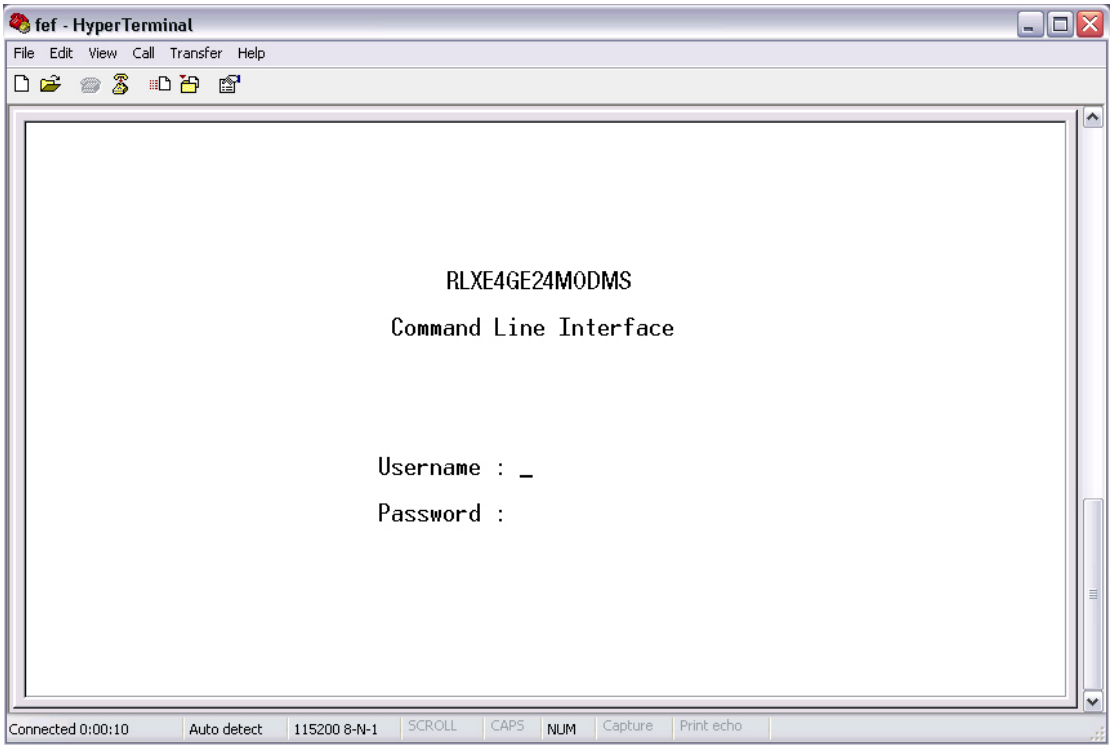
Step 3. Select to use COM port number



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



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



CLI Management by Telnet

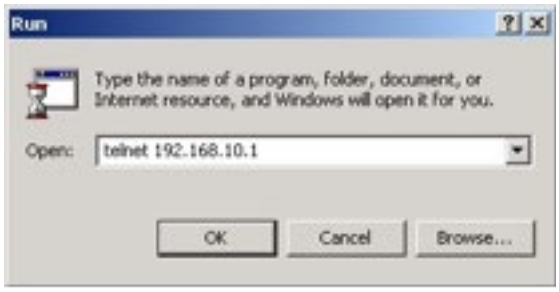
Users can use "TELNET" to configure the switches.

The default value is as below:

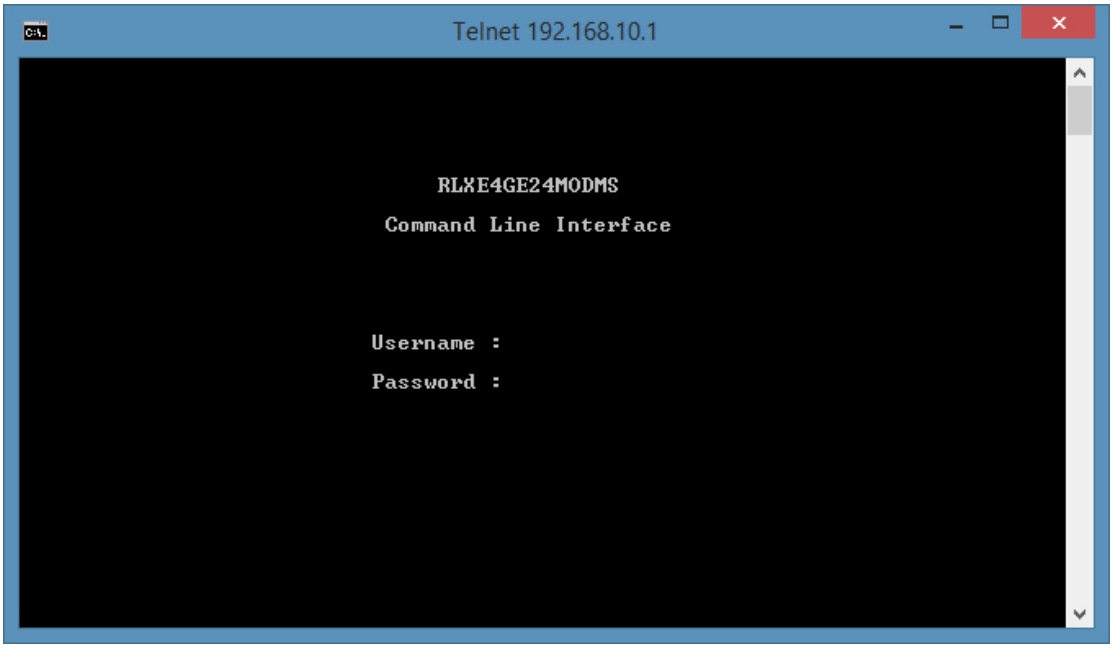
IP Address: 192.168.10.1
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.10.254
User Name: admin
Password: admin

Follow the steps below to access the console via Telnet.

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



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



Commander Groups

```
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>]

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]

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

Using the Routing Function

Static Routing Setting Example

Two PCs in different subnets, use static route function for routing between the two subnets.

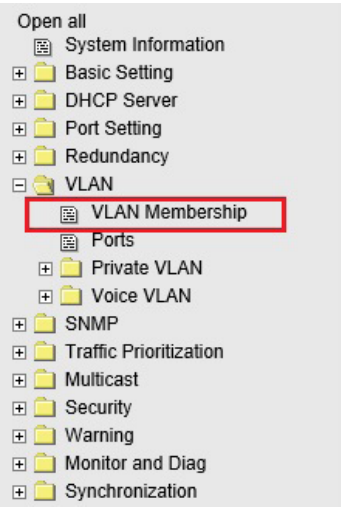
L3 Switch by VLAN Routing two subnets, the user needs to set two VLANs in the switch.

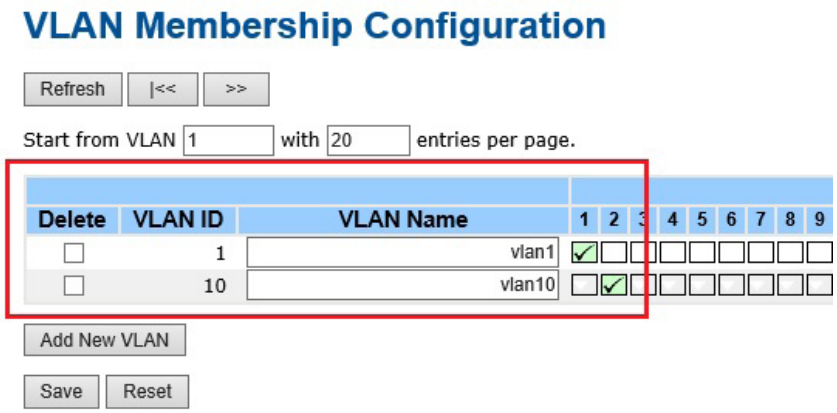
Example - Set VLAN 1 = 192.168.10.X , VLAN 10 = 192.168.20.X

Detail settings as follows:

1. VLAN Setting

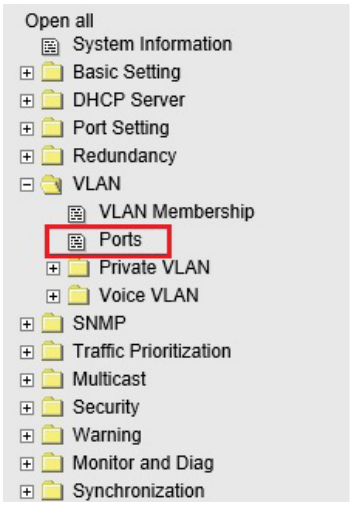
Port 1 = VLAN Group 1
Port 2 = VLAN Group 10

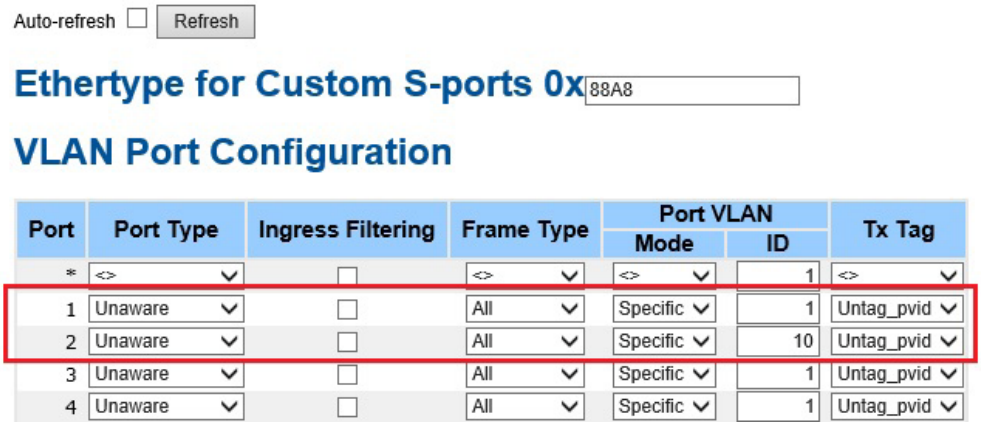




Port 1 PVID = 1

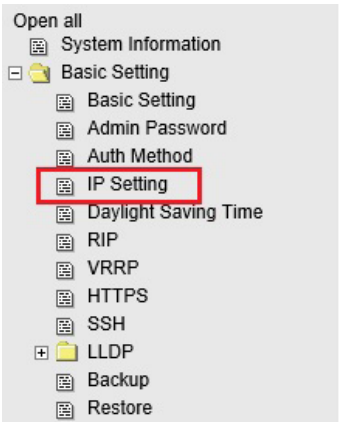
Port 2 PVID = 10

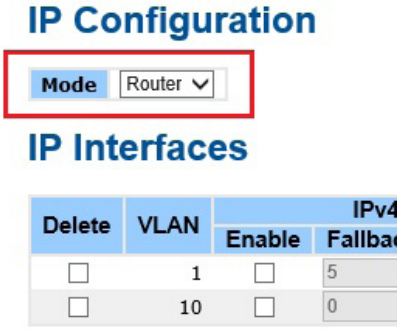




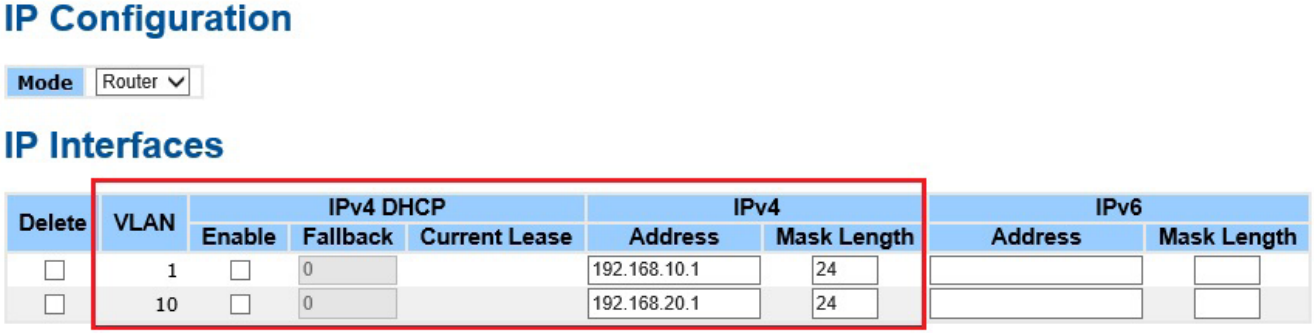
2. Static Routing Setting

Mode = Router





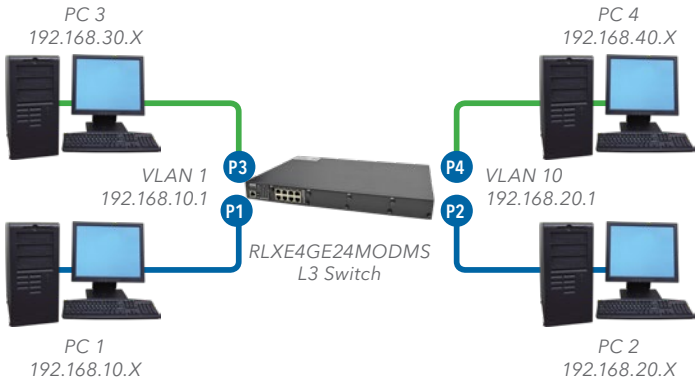
Create IP interfaces
VLAN 1 = 192.168.10.1
VLAN 10 = 192.168.20.1



Setup is complete
PC 1 = 192.168.10.X
PC 2 = 192.168.20.X

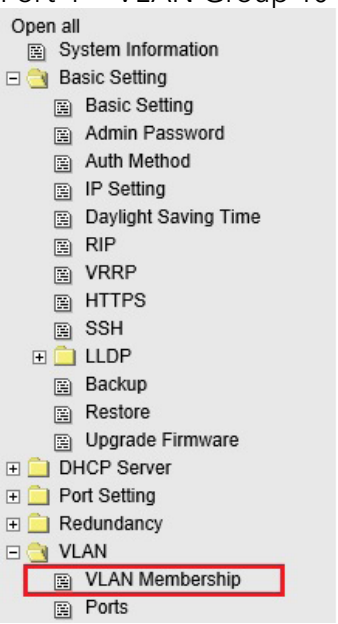
PC 1 can ping to PC 2 (192.168.10.X routing to 192.168.20.X)

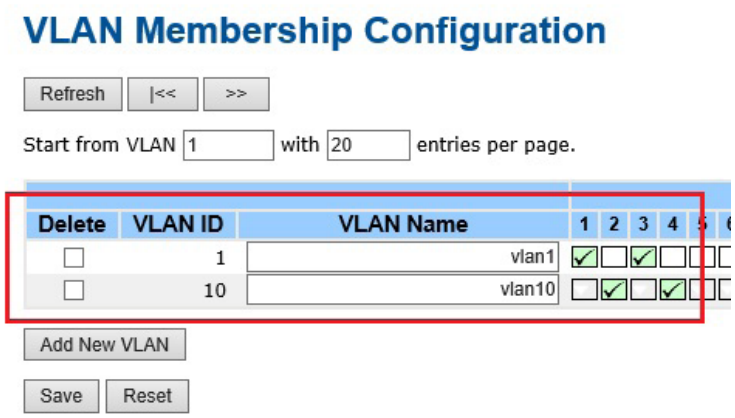
RIP Routing Setting Example:



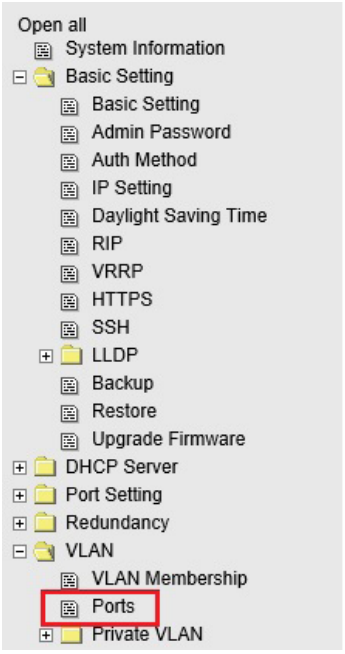
1. VLAN Setting

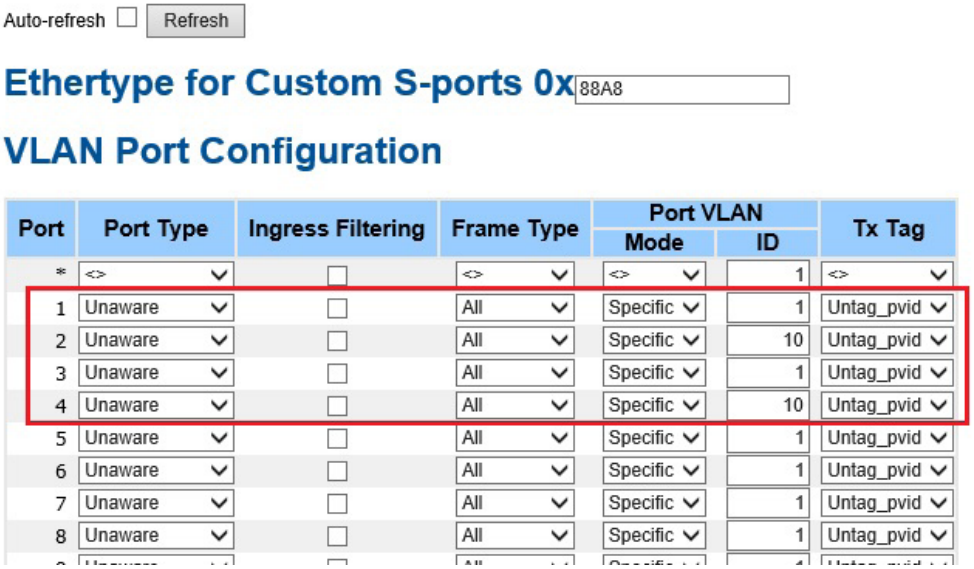
Port 1 = VLAN Group 1
Port 2 = VLAN Group 10
Port 3 = VLAN Group 1
Port 4 = VLAN Group 10





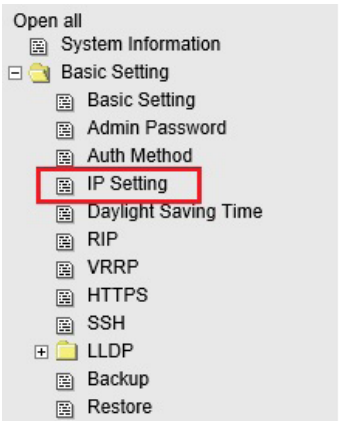
Port 1 PVID = 1
Port 2 PVID = 10
Port 3 PVID = 1
Port 4 PVID =10

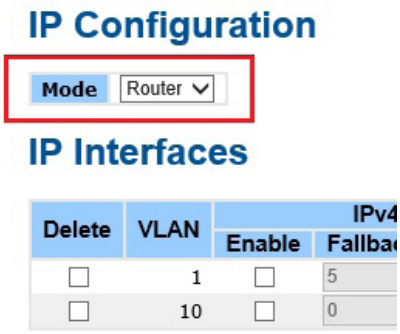




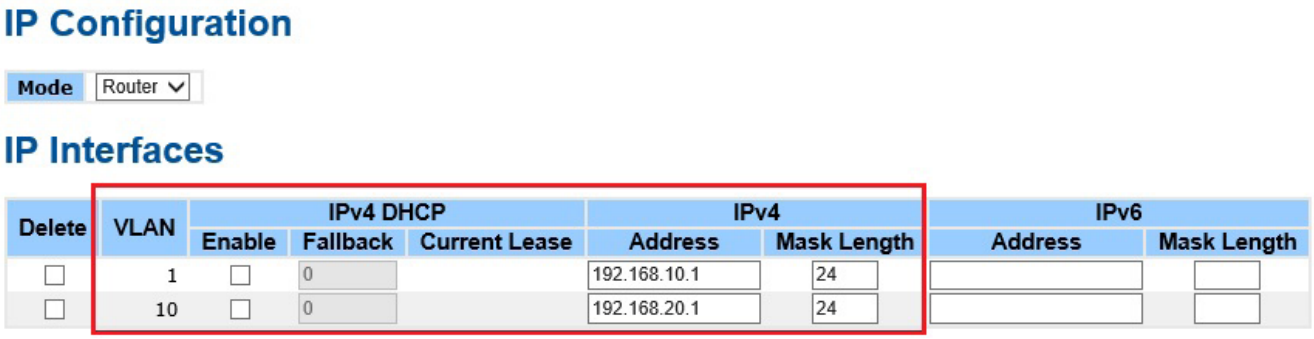
2. Static Routing Setting

Mode = Router



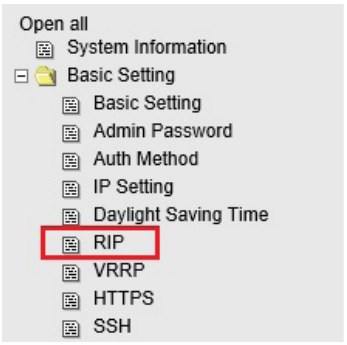


Create IP interfaces
VLAN 1 = 192.168.10.1
VLAN 10 = 192.168.20.1



3. RIP Routing Setting

RIP Mode = Enabled



Setup is complete
PC 1 = 192.168.10.X
PC 2 = 192.168.20.X
PC 3 = 192.168.30.X
PC 4 = 192.168.40.X
PC 1 can ping to PC2 , PC3 , PC4
PC 2 can ping to PC1 , PC3 , PC4
PC 3 can ping to PC1 , PC2 , PC4
PC 4 can ping to PC1 , PC2 , PC3

Technical Specifications

ComNet Switch Model	RLXE4GE24MODMS
Physical Ports	
Slot Number 1-3	8 × 1Gb Ports Per Slot
Slot Number 4	4 × 10Gb SFP+ Ports
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 802.3ae for 10Gigabit Ethernet 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)
MAC Table	32k
Priority Queues	8
Processing	Store-and-Forward
Switch Properties	Switching latency: 7 us Switching bandwidth: 128 Gbps Max. Number of Available VLANs: 256 IGMP multicast groups: 128 for each VLAN Port rate limiting: User Define
Jumbo frame	Up to 10K Bytes
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	Hardware routing, RIP, and static routing 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 IGMP v2/v3 Snooping IP-based bandwidth management Application-based QoS management Port configuration, status, statistics, monitoring, security DHCP Server/Client
Network Redundancy	C-Ring C-Chain Legacy Ring ERPS MSTP (RSTP/STP compatible)
RS-232 Serial Console Port	RS-232 in RJ-45 connector with console cable. 115200bps, 8, N, 1

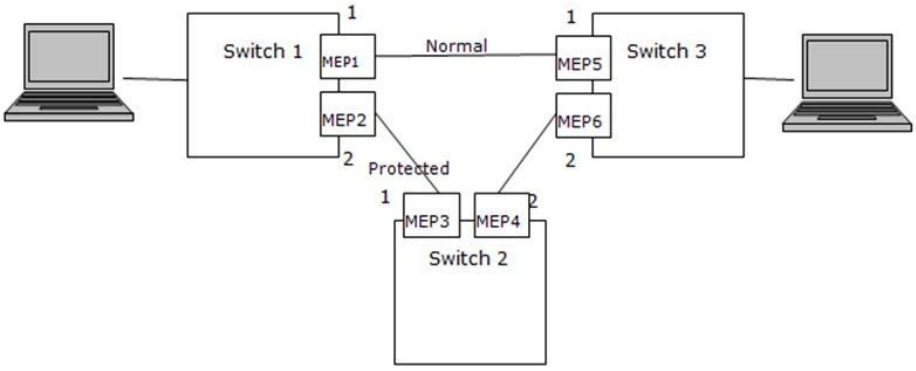
LED indicators	
System Ready (PWR)	Green: System is ready. Blinking: System is upgrading firmware.
Power (PWR1 / PWR2)	Green: Power is connected
Ring Master (R.M.)	Green: System is operating in C-Ring Master Mode
C-Ring (Ring)	Green: System is operating in C-Ring Mode Green Blinking: Ring is broken
Fault	Amber: Unexpected event has occurred
Reset to Default Running (DEF)	Green: System is resetting to default configuration
Supervisor Login (RMT)	Green: System is being accessed remotely
Smart LED Display system	Link/Act(LINK)/Speed(SPD)/Duplex(FDX)/Remote(RMT) Green LED × 4 Mode Select Button (MODE): Link/Act(LINK)/Speed(SPD)/ Duplex(FDX)/Remote(RMT) select button Ports 1 through 28 Link/Act(LK/ACT) Green LED × 28
Fault contact	
Relay	Relay output to carry capacity of 1 A at 24 VDC
Power	
Power Input	LV Chassis: Dual 24/48VDC (20~72VDC) power inputs at terminal block HV Chassis: Dual 88~264VAC / 100~370VDC power inputs at terminal block
Power consumption	46 Watts Max
Overload current protection	Present
Physical Characteristic	
Enclosure	19 inches rack mountable
Dimension (W x D x H)	440 (W) × 325 (D) × 44 (H) mm (17.32 × 12.8 × 1.73 inch)
Weight (g)	6600 g
Environmental	
Storage Temperature	-40 to 85°C (-40 to 185°F)
Operating Temperature	10G SFP+ module absent : -40 to 85° C Proper 10G SFP+ module used: -40 to 75° C
Operating Humidity	5% to 95% Non-condensing

Appendix A

Ethernet Ring Protection Switching Example Configuration

Introduction

This section shows how to configure the Ethernet Ring Protection Switching (ERPS) for ComNet switches using the Web GUI and the CLI commands. The following figure shows a simple three switch network constructed to demonstrate these features.



Ethernet Ring Protection Switching (ERPS) Model

Configuring ERPS from the Web GUI

Initial Switch Configuration

Use the following steps to configure the ERPS features through the Web.

1. Set the proper static IP for each switch. In this example, switch 1 is 192.168.10.1, switch 2 is 192.168.10.2 and switch 3 is 192.168.10.3.
2. Connect switch 1 to switch 2 and switch 1 to switch3. Do not connect switch 2 to switch 3 to avoid creating a loop. The web client is connected to switch 1.
3. To avoid conflict with ERPS disable spanning tree on all switches if it is enabled.
4. Enable VLAN tag aware on all three switches. In VLAN configuration page, set port mode to Hybrid port and port type to C-Port on port 1 and port 2 for each of the three switches, as screen shot below.

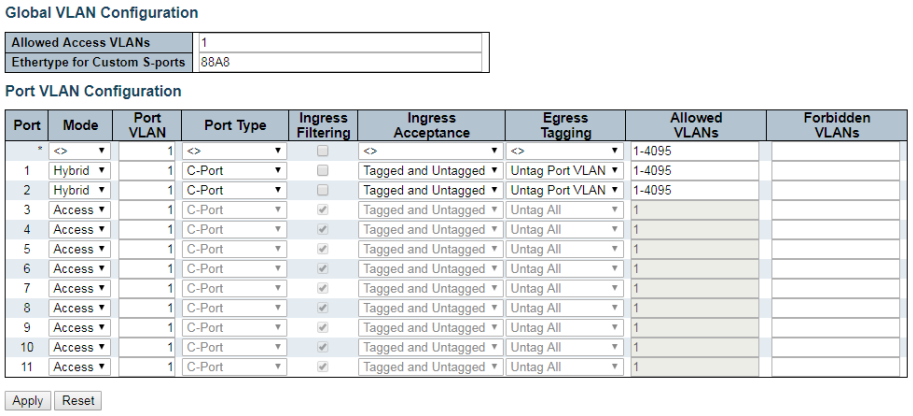


Figure 1 – Switch 1, 2, & 3 VLAN Configuration

Creating a MEP on Switch 1

1. On switch 1, add a new MEP on port 1 and 2 by clicking MEP. Configure the MEP as shown, and click Add New MEP.

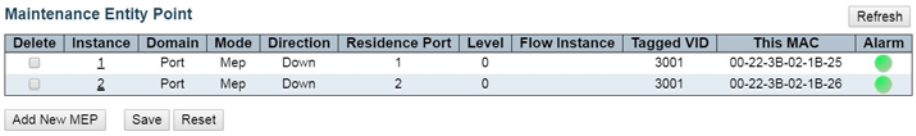


Figure 2 – Switch 1 Port 1 and 2 MEP Configuration

2. Edit MEP1 by clicking 1 under Instance of the MEP table. Configure the page as shown, and click Save or Apply.

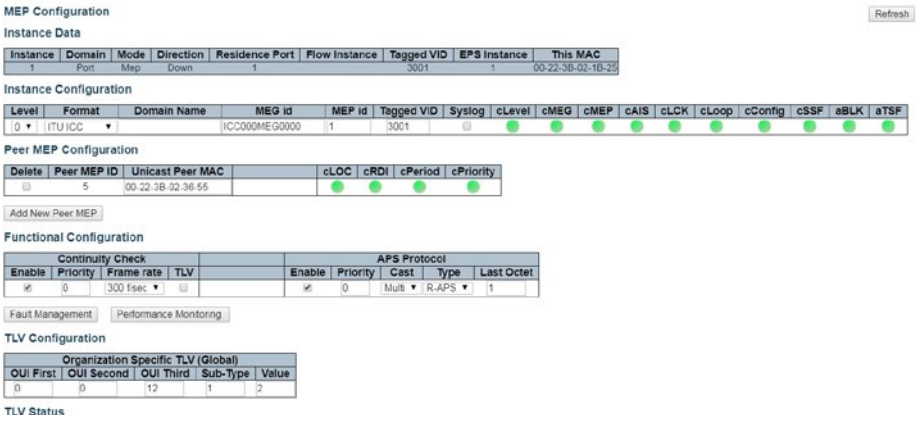


Figure 3 – Switch 1 MEP 1 Configuration

The Unicast Peer MAC can remain empty because it will be learned by receiving the CCM from the peer side. On ComNet switches, before they are learned, the CCM frame rate cannot be changed to above 100/sec. If known, enter the peer MAC address manually.

3. Edit MEP2 by clicking 2 under Instance of the MEP table. Configure the MEP as shown, and click Save or Apply.

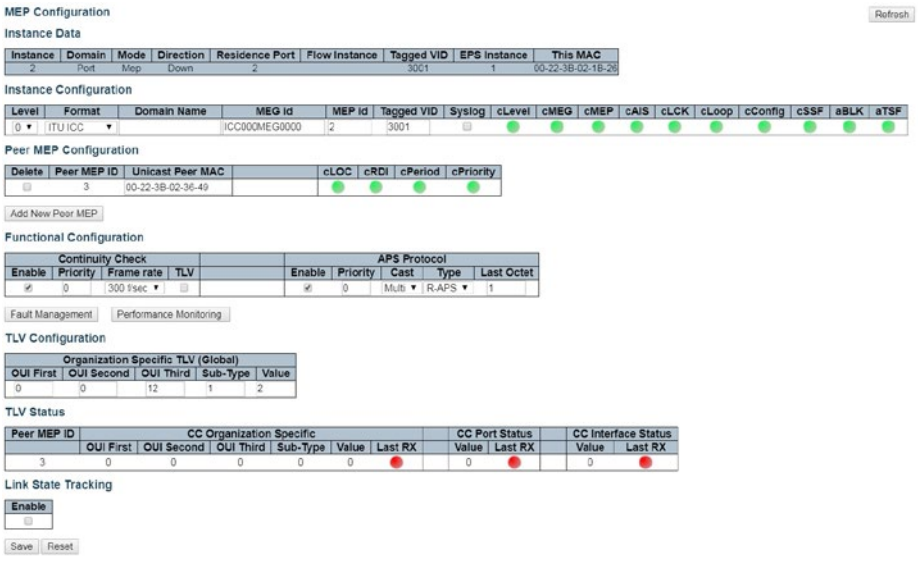


Figure 4 – Switch 1 MEP 2 Configuration

Configuring Switch 2

1. Add a new MEP on port 1 and 2 of switch 2.

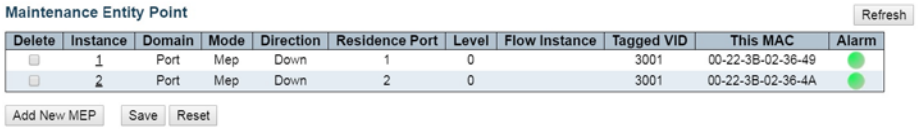


Figure 5 – Switch 2 Port 1 and 2 MEP Configuration

2. Edit MEP1 of switch 2 by clicking 1 under Instance of the MEP table. Configure the MEP as shown, and click Save or Apply.

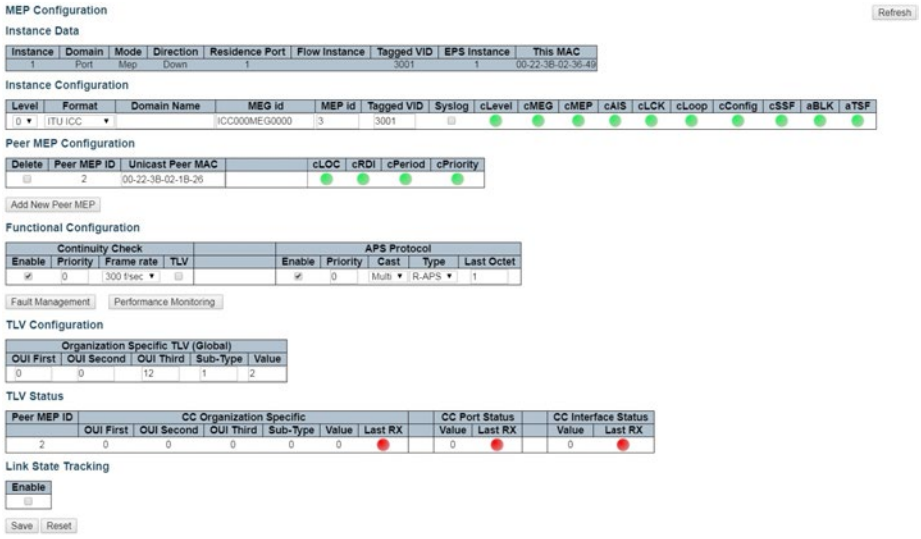


Figure 6 – Switch 2 MEP 1 Configuration

3. Edit MEP2 of switch 2 by clicking 2 under Instance of the MEP table. Configure the MEP as shown, and click Save or Apply.

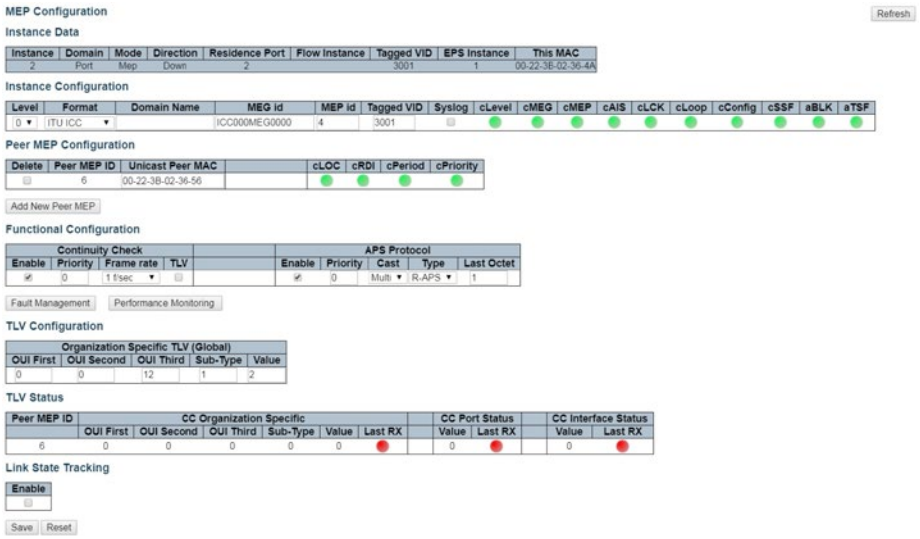


Figure 7 – Switch 2 MEP 2 Configuration

Configuring Switch 3

1. Add a new MEP on port 1 and 2 of switch 3.

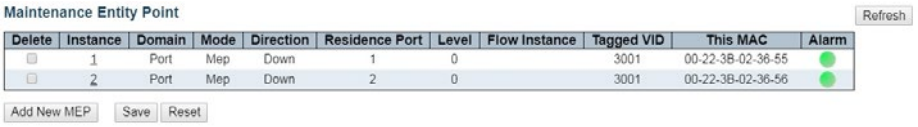


Figure 8 – Switch 3 Port 1 and 2 MEP Configuration

2. Edit MEP1 of switch 3 by clicking 1 under Instance of the MEP table. Configure the MEP as shown, and click Save or Apply.

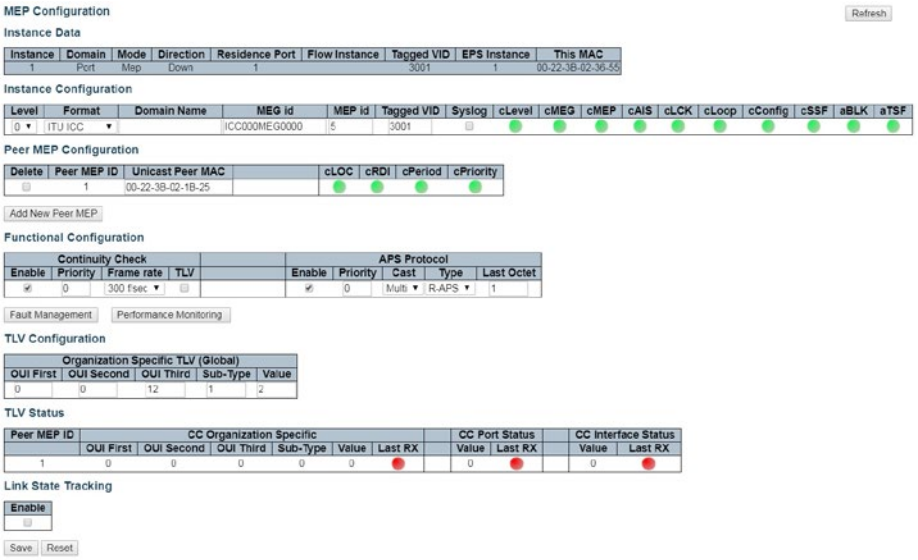


Figure 9 – Switch 3 MEP 1 Configuration

3. Edit MEP2 of switch 3 by clicking 2 and configuring the MEP as shown, and click Save or Apply.

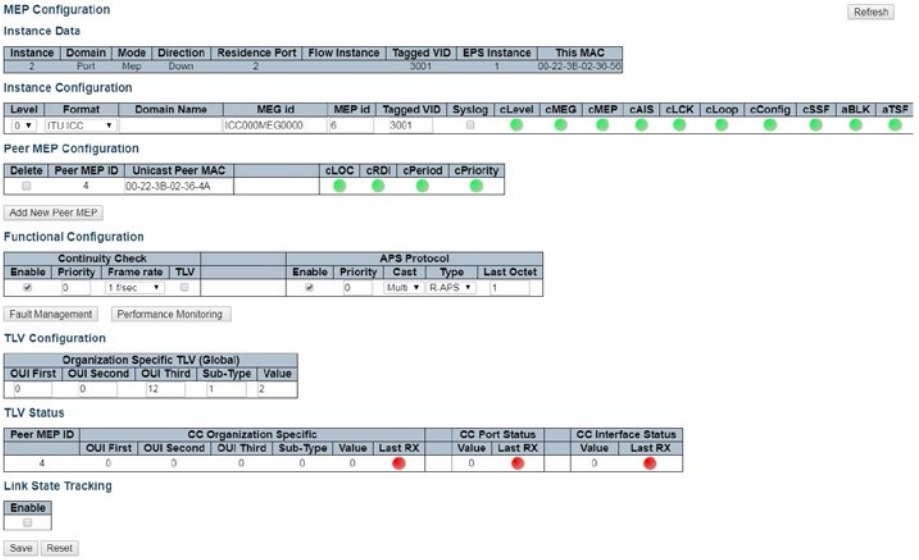


Figure 10 – Switch 3 MEP 2 Configuration

Configuring ERPS on Switch 1

1. On switch 1, click ERPS to go to the Ethernet Ring Protection switching page. Add the Ring Protection Link (RPL) owner as shown, and click Add New Protection Group.

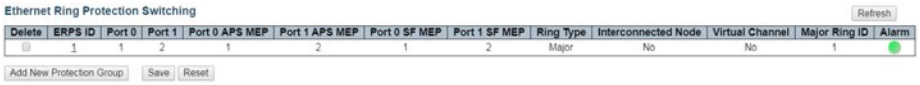


Figure 11 – Add New Protection Group (Switch 1) Configuration

2. Edit ERPS1 by clicking 1. Set the configuration as shown, and click Save or Apply.

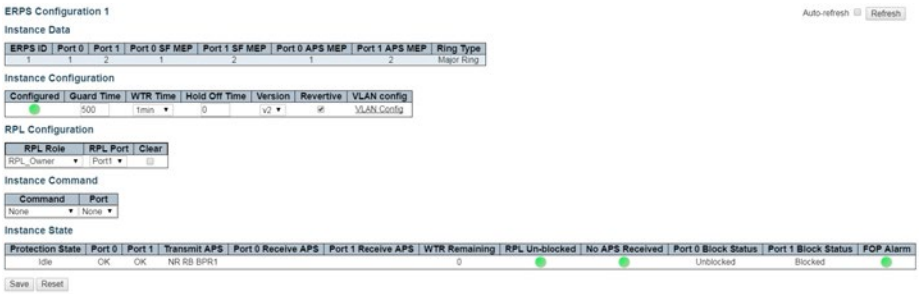


Figure 12 – ERPS 1 (Switch 1) Configuration

3. Click VLAN Config to edit the protected VLAN.

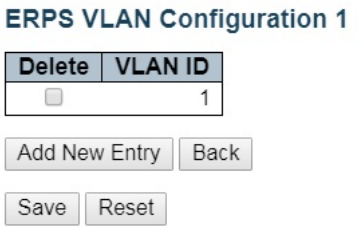


Figure 13 – Protected VLAN (Switch 1) Configuration

4. After clicking Save or Apply, remember to connect switch 2 and switch 3. Because the RPL is disconnected, the user will not be able to access switch 2 from switch 1.

5. Check the MEP table on switch 1, switch 2, and switch 3. Alarms should show green.

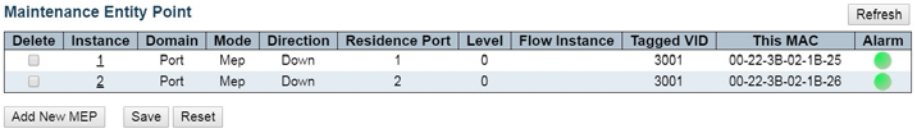


Figure 14 – MEP Status

Configuring ERPS on Switch 2, the RPL Neighbor

1. On switch 2, click ERPS followed by Add New Protection Group.

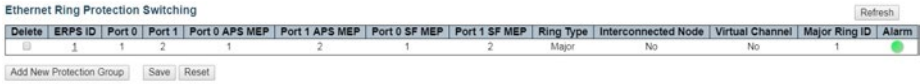


Figure 15 – Add New Protection Group (Switch 2) Configuration

2. Edit ERPS1 by clicking 1. Configure the device as shown, and click Save or Apply.

Figure 16 – ERPS 1 (Switch 2) Configuration

3. Click VLAN Config to edit the VLAN.

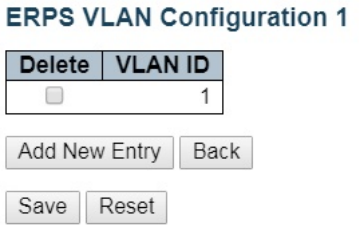


Figure 17 – ERPS VLAN (Switch 2) Configuration

Configuring ERPS on Switch 3

1. On switch 3, click ERPS followed by Add New Protection Group.

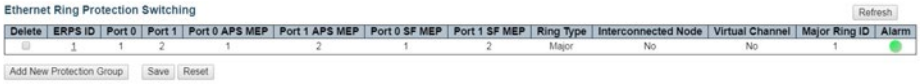


Figure 18 – Add New Protection Group (Switch3)

2. Edit ERPS1 by clicking 1. No action is required on switch 3. Keep the RPL owner at none.

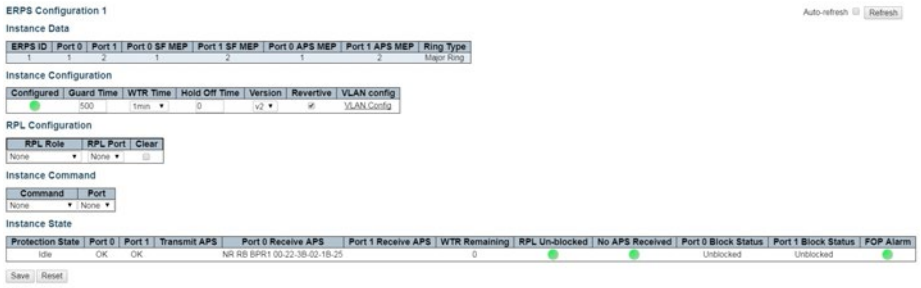


Figure 19 – ERPS 1 (Switch 2) Configuration

3. Click VLAN Config to edit the VLAN.

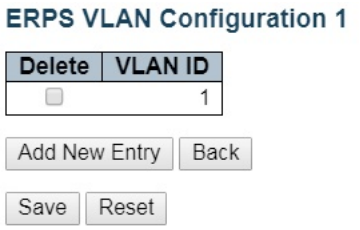


Figure 20 – ERPS VLAN (Switch 3) Configuration

Ethernet Ring Protection Switching Configuration

Verifying ERPS

1. Change the CCM rate starting from switch 3. Click on MEP > 2 and then use the frame rate pull down to select 300 f/sec.

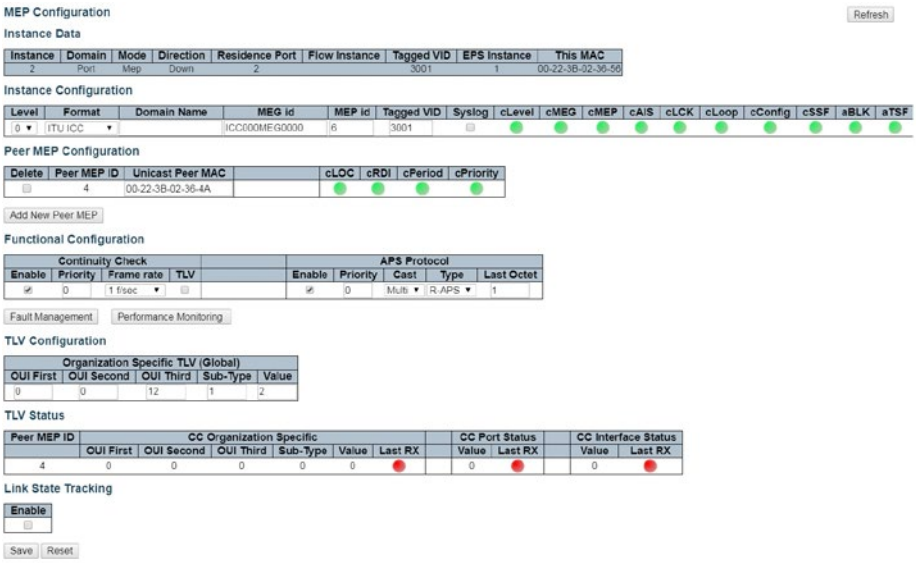


Figure 21 – Edit MEP 2 CCM Rate (Switch 3)

2. Change the CCM rate for MEP 1.

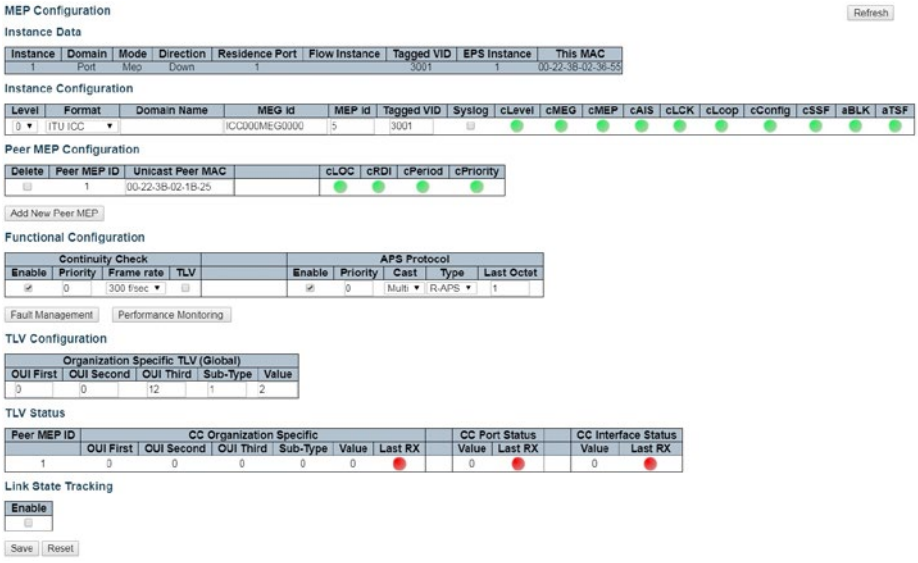


Figure 22 – Edit MEP 1 CCM Rate (Switch 3)

3. Change the CCM rate on switch 1. Click on MEP > 1 and then use the frame rate pull down to select 300 f/sec.

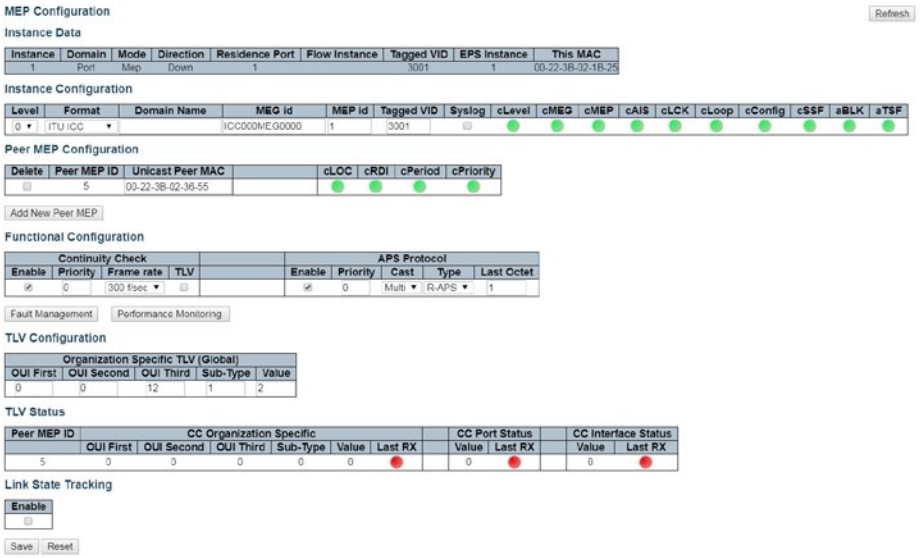


Figure 23 – Edit MEP 1 CCM Rate (Switch 1)

4. Change the CCM rate for MEP 2.

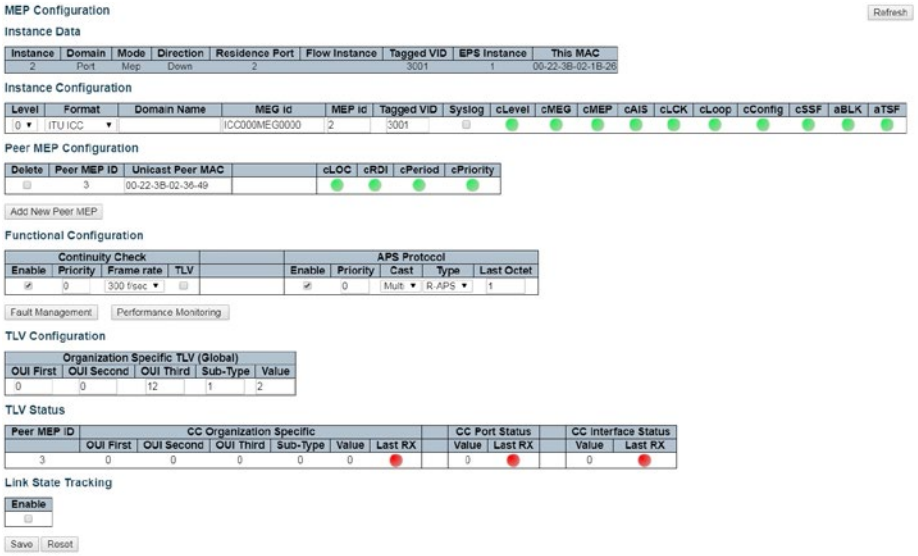


Figure 24 – Edit MEP 2 CCM Rate (Switch 1)

5. Change the CCM rate on switch 2. Click on MEP > 1 and then use the frame rate pull down to select 300 f/sec.

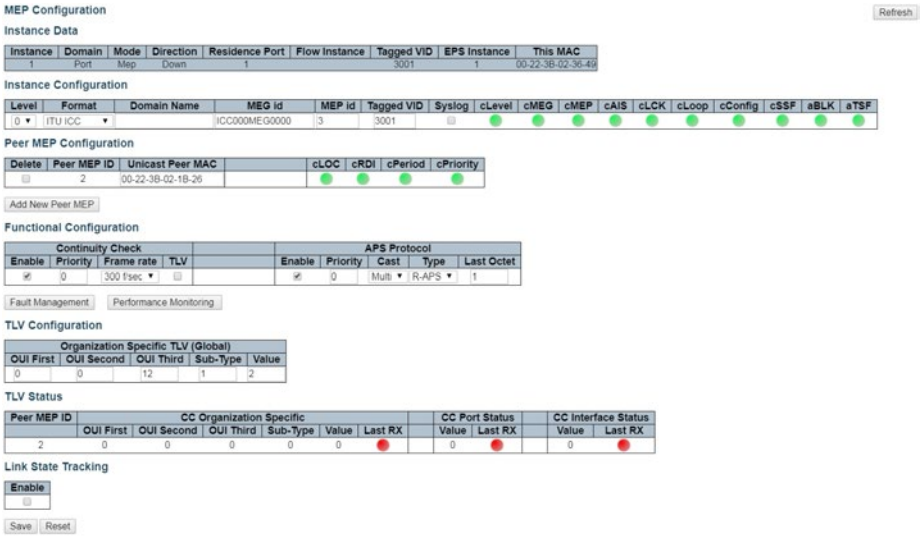


Figure 25 – Edit MEP 1 CCM Rate (Switch 2)

6. Change the CCM rate for MEP 2.

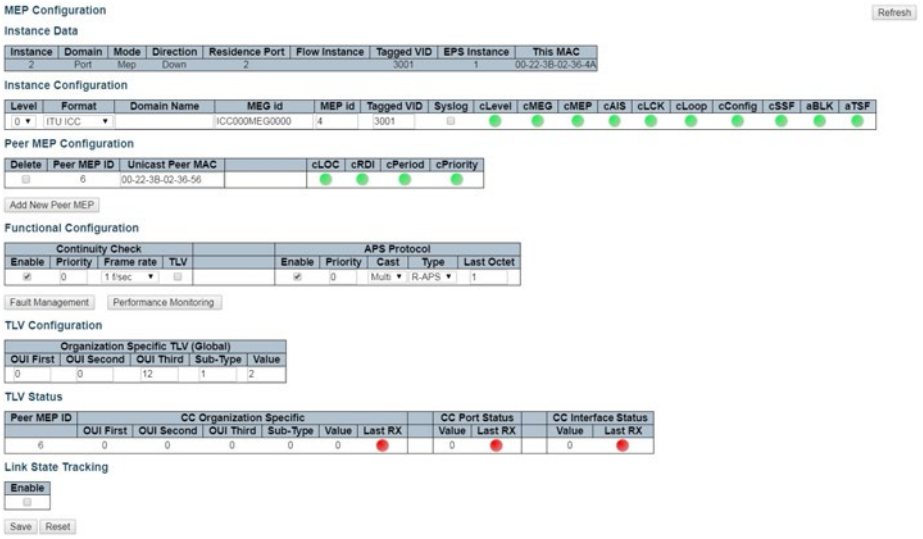


Figure 26 – Edit MEP 2 CCM Rate (Switch 2)

7. On Switch 1, check ERPS status by clicking ERPS to ensure normal link status

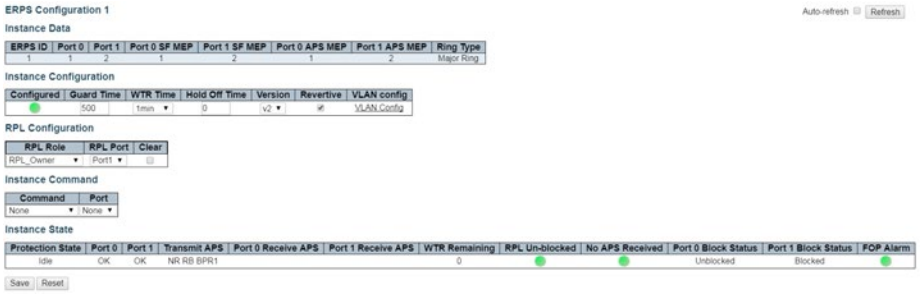


Figure 27 – Switch 1 ERPS Status

8. Disconnect the normal link for switch 1 and switch 3.

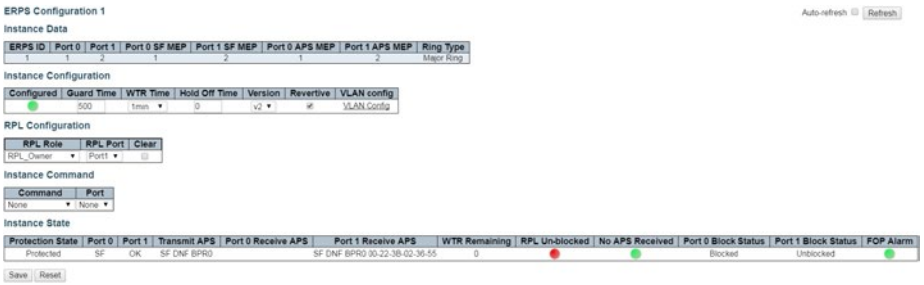


Figure 28 – Disconnect Normal Link

9. Restore the normal link for switch 1 and switch 3 to display the protection state as Pending.

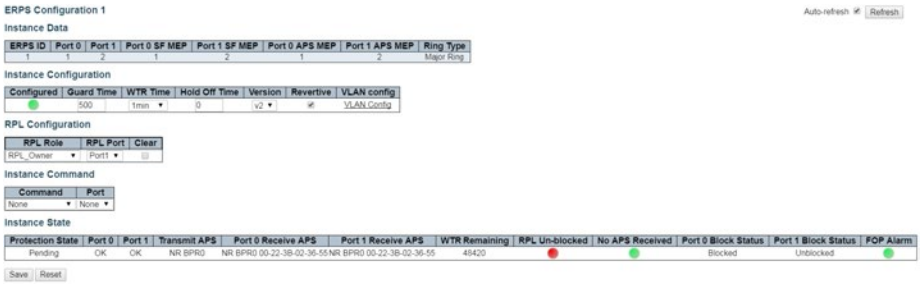


Figure 29 – Restore Normal Link

10. After WTR timeout, and clicking Refresh, it should show as Idle.

Figure 30 – Refresh ERPS Status

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