# RES-P9242GC Series

## Industrial Rack-Mount Ethernet Switch

# User Manual

**Version 1.0**

**July, 2017**

**www.oringnet.com**

## COPYRIGHT NOTICE

Copyright © 2016 ORing Industrial Networking Corp.
All rights reserved.
No part of this publication may be reproduced in any form without the prior written consent of ORing Industrial Networking Corp.

## TRADEMARKS

ORing is a registered trademark of ORing Industrial Networking Corp.
All other trademarks belong to their respective owners.

## REGULATORY COMPLIANCE STATEMENT

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

## WARRANTY

ORing warrants that all ORing products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). ORing will repair or replace products found by ORing to be defective within this warranty period, with shipment expenses apportioned by ORing and the distributor. This warranty does not cover product modifications or repairs done by persons other than ORing-approved personnel, and this warranty does not apply to ORing products that are misused, abused, improperly installed, or damaged by accidents.
Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

## DISCLAIMER

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

## CONTACT INFORMATION

**ORing Industrial Networking Corp.**
3F., NO.542-2, JhongJheng Rd., Sindian District, New Taipei City 231, Taiwan, R.O.C.
Tel: + 886 2 2218 1066 // Fax: + 886 2 2218 1014
Website: www.oring-networking.com

**Technical Support**
E-mail: support@oring-networking.com

**Sales Contact**
E-mail: sales@oring-networking.com (Headquarters)
sales@oring-networking.com.cn (China)

# Table of Content

**Getting Started ..... 7**
1.1 About the RES-P9242GCL ..... 7
1.2 Software Features ..... 7
1.3 Hardware Specifications ..... 8

**Hardware Overview ..... 9**
2.1 Front Panel ..... 9
2.1.1 Ports and Connectors ..... 9
2.1.2 LED ..... 9

**Hardware Installation ..... 11**
3.1 Rack-mount Installation ..... 11
3.2 Wiring ..... 12
3.2.1 Grounding ..... 12
3.2.2 Fault Relay ..... 12
3.2.3 Redundant Power Inputs ..... 12
3.3 Connection ..... 13
3.3.1 Cables ..... 13
10/100/1000BASE-T(X) Pin Assignments ..... 13
RS-232 Console Port Wiring ..... 15
3.3.2 SFP ..... 15
3.3.3 O-Ring/O-Chain ..... 16

**Redundancy ..... 19**
4.1 O-Ring ..... 19
4.1.1 Introduction ..... 19
4.1.2 Configurations ..... 19
4.2 Open-Ring ..... 20
4.2.1 Introduction ..... 20
4.2.2 Configurations ..... 21
4.3 O-Chain ..... 21
4.3.1 Introduction ..... 21
4.3.2 Configurations ..... 22
4.4 MSTP ..... 23
STP/RSTP ..... 23
4.4.1 Bridge Setting ..... 24

4.4.2 MSTI Mapping ..... 25
4.4.3 MSTI Priorities ..... 26
4.4.4 CIST Ports ..... 27
4.4.5 MSTI Ports ..... 29
4.4.6 Bridge Status ..... 31
4.4.7 Port Status ..... 33
4.4.8 Port Statistics ..... 34
4.5 Fast Recovery ..... 34

**Management ..... 36**
5.1 Basic Settings ..... 37
5.1.1 System Information ..... 37
5.1.2 Admin & Password ..... 38
5.1.3 Authentication ..... 39
5.1.4 IP Settings ..... 40
5.1.5 IPv6 Settings ..... 40
5.1.6 Daylight Saving Time ..... 42
5.1.7 HTTPS ..... 43
5.1.8 SSH ..... 44
5.1.9 DBU01 ..... 45
5.1.10 LLDP ..... 45
5.1.10.1 LLDP Configurations ..... 45
5.1.10.2 LLDP Neighbor Information ..... 46
5.1.10.3 Port Statistics ..... 47
5.1.11 NTP ..... 48
5.1.12 Modbus TCP ..... 49
5.1.13 Backup/Restore Configurations ..... 50
5.1.14 Firmware Update ..... 50
5.2 DHCP Server ..... 50
5.2.1 Settings ..... 50
5.2.2 Dynamic Client List ..... 51
5.2.3 Client List ..... 51
5.2.4 Relay Agent ..... 52
5.2.4.1 Settings ..... 52
5.2.4.2 Statistics ..... 53
5.3 Port Setting ..... 55
5.3.1 Port Control ..... 55
5.3.2 Port Alias ..... 56

5.3.3 Port Trunk ..... 57
5.3.3.1 Configuration ..... 57
5.3.3.2 LACP Port ..... 58
5.3.3.3 System Status ..... 60
5.3.3.4 Port Status ..... 60
5.3.3.5 LACP Statistics ..... 61
5.3.4 Loop Protection ..... 62
5.3.4.1 Configuration ..... 62
5.3.4.1 Status ..... 63
5.4 VLAN ..... 63
5.4.1 VLAN Membership ..... 63
5.4.2 Ports ..... 64
5.4.3 Private VLAN ..... 73
5.4.3.1 PVLAN Membership ..... 73
5.4.3.2 Port Isolation ..... 74
5.5 SNMP ..... 74
5.5.1 System ..... 74
5.5.2 Communities ..... 77
5.5.3 Users ..... 78
5.5.4 Groups ..... 79
5.5.5 Views ..... 80
5.5.6 Access ..... 81
5.6 Traffic Prioritization ..... 82
5.6.1 Storm Control ..... 82
5.6.2 Port Classification ..... 83
5.6.3 Port Tag Remaking ..... 85
5.6.4 Port DSCP ..... 86
5.6.5 Port Policing ..... 87
5.6.6 Queue Policing ..... 88
5.6.7 Port Scheduler ..... 89
5.6.8 Port Shaping ..... 92
5.6.9 DSCP Based QoS ..... 93
5.6.10 DSCP Translation ..... 93
5.6.11 DSCP Classification ..... 94
5.6.12 QoS Control List ..... 95
5.6.13 QoS Statisitics ..... 97
5.6.14 QCL Status ..... 98

5.7 Multicast ..... 99
5.7.1 IGMP Snooping ..... 99
5.7.1.1 Basic Settings ..... 99
5.7.1.2 VLAN Configurations ..... 100
5.7.1.3 Status ..... 101
5.7.1.4 Groups Information ..... 102
5.8 Security ..... 102
5.8.1 Remote Control Security ..... 102
5.8.2 Device Binding ..... 103
5.8.2.1 Basic Configuration ..... 103
5.8.2.2 Advanced Configurations ..... 104
Alias IP Address ..... 104
Alive Check ..... 105
DDoS Prevention ..... 106
Device Description ..... 107
Stream Check ..... 108
5.8.3 ACL ..... 108
5.8.3.1 Ports ..... 108
5.8.3.2 Rate Limiters ..... 110
5.8.3.3 ACL Control List ..... 110
5.8.4 AAA ..... 123
5.8.4.1 Configurations ..... 123
5.8.4.2 RADIUS Overview ..... 124
Authentication and Accounting Server Status Overview ..... 126
5.8.4.3 RADIUS Details ..... 128
5.8.5 NAS (802.1x) ..... 130
5.8.5.1 Configuration ..... 132
5.8.5.2 Switch ..... 139
5.8.5.3 Port ..... 140
5.9 Warning ..... 142
5.9.1 Fault Alarm ..... 142
5.9.2 System Warning ..... 142
5.9.2.1 SYSLOG Setting ..... 142
5.9.2.2 SMTP Setting ..... 143
5.9.2.3 Event Selection ..... 144
5.10 Monitor and Diag ..... 145
5.10.1 MAC Table ..... 145

5.10.1.1 MAC Address Table Configuration ..... 145
5.10.1.2 MAC Table ..... 147
5.10.2 Port Statistics ..... 148
5.10.2.1 Traffic Overview ..... 148
5.10.2.2 Detailed Statistics ..... 148
5.10.3 Port Mirroring ..... 150
5.10.4 System Log Information ..... 151
5.10.5 SFP Monitor ..... 152
5.10.6 Traffic Monitor ..... 153
5.10.7 Ping ..... 154
5.10.8 Ping6 ..... 155
5.11 Troubleshooting ..... 155
5.11.1 Factory Defaults ..... 155
5.11.2 System Reboot ..... 156

**Command Line Interface Management ..... 157**

# Getting Started

## 1.1 About the RES-P9242GCL

RES-P9242GCL series are 26-port rack mount managed redundant ring Ethernet switch with 24x10/100Base-T(X) and 2xGigabit Combo ports, SFP socket. These switches are designed for power substation application, and it is fully compliant with the requirement of IEC 61850-3 and IEEE 1613. These switches support Ethernet Redundancy protocol, O-Ring (recovery time < 30ms), O-Chain, MRP*NOTE, Fast Recovery and MSTP (RSTP/STP compatible) can protect your mission-critical applications from network interruptions or temporary malfunctions with its fast recovery technology. RES-P9242GCL series can also be managed centralized and convenient by Open-Vision, as well as the Web-based interface, Telnet and console (CLI) configuration. Therefore, the switch is one of the most reliable choice for highly-managed and Fiber Ethernet application.

## 1.2 Software Features

- Supports Open-Ring to interoperate with other vendors' ring technology in open architecture
- Support O-Ring (recovery time < 30ms over 250 units of connection) and MSTP(RSTP/STP compatible) for Ethernet Redundancy
- Supports O-Chain to allow multiple redundant network rings
- Supports hardware IEEE 1588v2 clock synchronization
- Supports IPV6 new Internet protocol
- Supports Modbus TCP protocol
- Supports IEEE 802.3az Energy-Efficient Ethernet technology
- Supports HTTPS/SSH protocols to enhance network security
- Supports SMTP client and NTP server protocol
- Supports IP-based bandwidth management
- Supports application-based QoS management
- Supports Device Binding security function
- Supports DOS/DDOS auto prevention
- Supports IGMP v2/v3 (IGMP snooping support) to filter multicast traffic
- Supports SNMP v1/v2c/v3 & RMON & 802.1Q VLAN network management
- Supports ACL, TACACS+ and 802.1x user authentication for security
- Supports 9.6K Bytes Jumbo Frame
- Supports multiple notifications for incidents

- Supports management via Web-based interfaces, Telnet, Console (CLI), and Windows utility (Open-Vision)
- Supports LLDP Protocol
- Support DBU-01 backup unit device for fast configuration backup/restore

## 1.3 Hardware Specifications

- 19-inch rack mountable design
- Compliant with IEC 61850-3 and IEEE 1613
- 24 x 10/100Base-T(X) RJ-45 ports
- 2xGigabit combo ports consisting of one copper and and one SFP port (DDM supported)
- Dual VAC power supplies
- Operating temperature: -40 to 75$^{o}$C
- Storage temperature: -40 to 85$^{o}$C
- Operating humidity: 5% to 95%, non-condensing
- Dimensions: 440 (W) x 200 (D) x 44 (H) mm (17.32 x 7.87 x 1.73 inch)

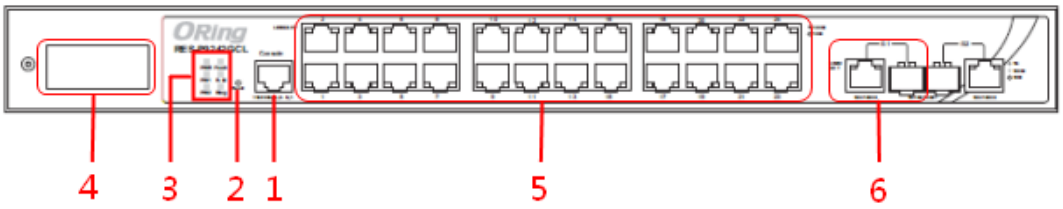
# Hardware Overview

## 2.1 Front Panel

### 2.1.1 Ports and Connectors

The device comes with the following ports and connectors on the front panel.

| Port | Description |
|---|---|
| **Ethernet ports** | 24 x 10/100Base-T(X) copper ports |
| **Combo ports** | 2 x Gigabit Combo ports with one copper port and one SFP port each. |
| **Console port** | 1 x console port |
| **Reset button** | 1 x reset button. Press the button for 3 seconds to reset and 5 seconds to return to factory default. |




1. Console port
2. Reset button
3. LED Status
   - Power indicator
   - Ring status LED
   - RM status LED
   - Fault indicator
4. Power input
5. LAN ports
6. Combo ports

### 2.1.2 LED

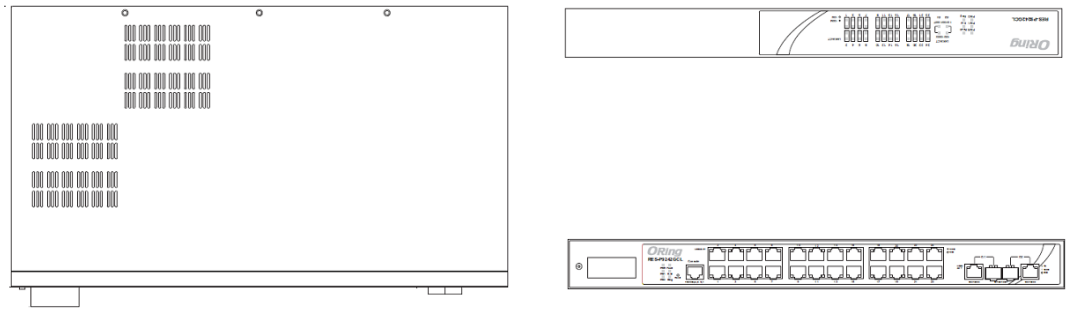
| LED | Color | Status | Description |
|---|---|---|---|
| **PWR** | Green | On | System power is on |
| **R.M** | Green | On | Port is operated as Ring Master. |
| **Ring** | Green | On | Port is operated in Ring mode |
| **Fault** | Amber | On | Errors occur (power failure or port malfunctioning) |
| 10/100Base-T(X) RJ45 port | | | |
| **Link/ACT** | Green | On | Port is connected |

| | | | |
|---|---|---|---|
| **Speed** | Amber | On | Port is running at 100Mbps |
| | | Off | Port is running at 10Mbps |
| 10/100/1000Base-T(X) RJ45 Port | | | |
| **Link/ACT** | Green | On | Port is connected |
| **Speed** | Amber | On | Port is running at 1000Mbps |
| | | Off | Port is running at 10/100Mbps |
| 1G/10GBase-X SFP port | | | |
| **Link/ACT** | Green | On | Port is connected |

# Hardware Installation

## 3.1 Rack-mount Installation

The switch comes with two rack-mount kits to allow you to fasten the switch to a rack in any environments.

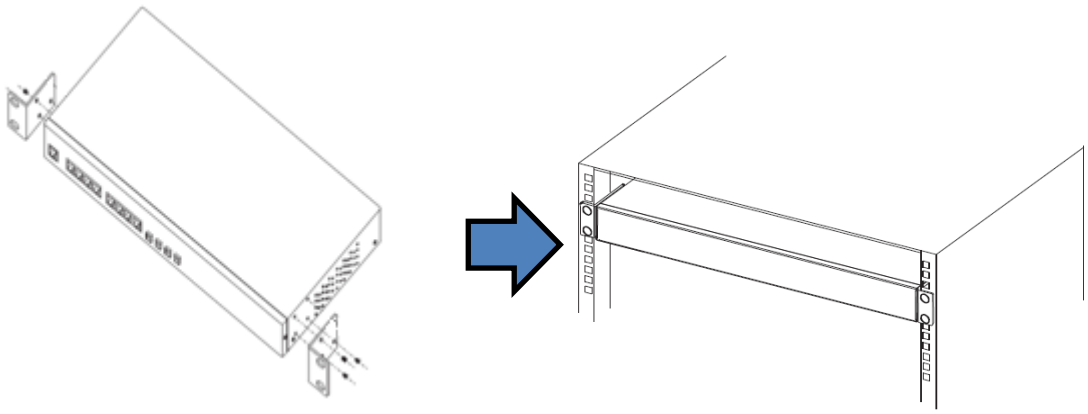


**Rack-mount measurement (Unit = mm)**

Follow the following steps to install the switch to a rack.

Step 1: Attach the mounting brackets to the front left and right sides of the switch using 4 screws

Step 2: With front brackets orientated in front of the rack, fasten the brackets to the rack using two more screws.



# 3.2 Wiring

**WARNING**

Do not disconnect modules or wires unless power has been switched off or the area is known to be non-hazardous. The devices may only be connected to the supply voltage shown on the type plate.

**ATTENTION**

1. Be sure to disconnect the power cord before installing and/or wiring your switches.
2. Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.
3. If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.
4. Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.
5. Do not run signal or communications wiring and power wiring through the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.
6. You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring sharing similar electrical characteristics can be bundled together
7. You should separate input wiring from output wiring
8. It is advised to label the wiring to all devices in the system

## 3.2.1 Grounding

Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screws to the grounding surface prior to connecting devices.

## 3.2.2 Fault Relay

The relay contact of the terminal block connector is used to detect user-configured events. The switch provides fail open and fail close options for you to form relay circuits based on your needs. If you want the relay device to start operating at power failure, attach the two wires to COM and fail close to form a close circuit, vice versa. The relay contact of the 2-pin terminal block connector will respond to user-configured events according to the wiring.

## 3.2.3 Redundant Power Inputs

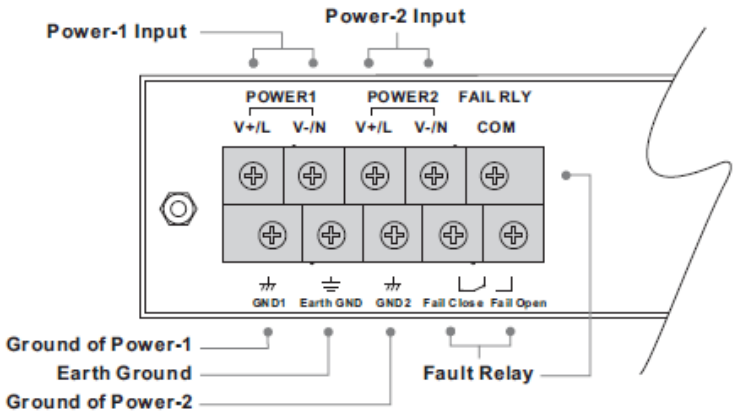
The switch supports dual redundant power supplies, Power Supply 1 (PWR1) and Power Supply 2 (PWR2). The connections for PWR1 and PWR2 are located on the terminal block.

**Step 1**: Remove the transparent cover designed for protection from the terminal block.

**Step 2**: Insert the negative/positive wires into the V-/V+ terminals, respectively.

**Step 3**: To keep the wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.

**Step 4**: After wiring is completed, put the transparent cover back to the terminal block.




# 3.3 Connection

## 3.3.1 Cables

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

The device comes with standard Ethernet ports. According to the link type, the switch uses CAT 3, 4, 5,5e UTP cables to connect to any other network devices (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable 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-T | Cat. 5/Cat. 5e 100-ohm UTP | UTP 100 m (328ft) | RJ-45 |

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

10/100Base-T(X) RJ-45 ports

| Pin Number | Assignment |
|---|---|
| #1 | TD+ |
| #2 | TD- |
| #3 | RD+ |

| | |
|---|---|
| #6 | RD- |

1000Base-T RJ-45 Port 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- |

10/100 Base-T(X) MDI/MDI-X Pin Assignments:

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

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

1000Base-T MDI/MDI-X Pin Assignments:

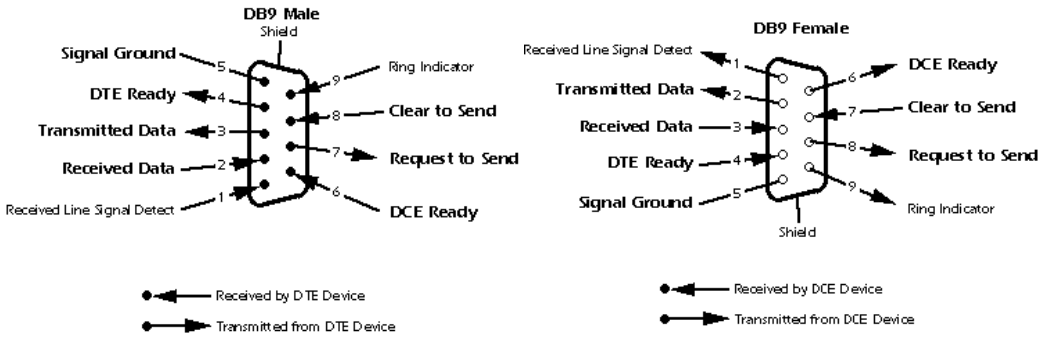
| Pin Number | MDI port | MDI-X port |
|---|---|---|
| 1 | BI_DA+ | BI_DB+ |
| 2 | BI_DA- | BI_DB- |
| 3 | BI_DB+ | BI_DA+ |
| 4 | BI_DC+ | BI_DD+ |
| 5 | BI_DC- | BI_DD- |
| 6 | BI_DB- | BI_DA- |
| 7 | BI_DD+ | BI_DC+ |
| 8 | BI_DD- | BI_DC- |

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

### RS-232 Console Port Wiring

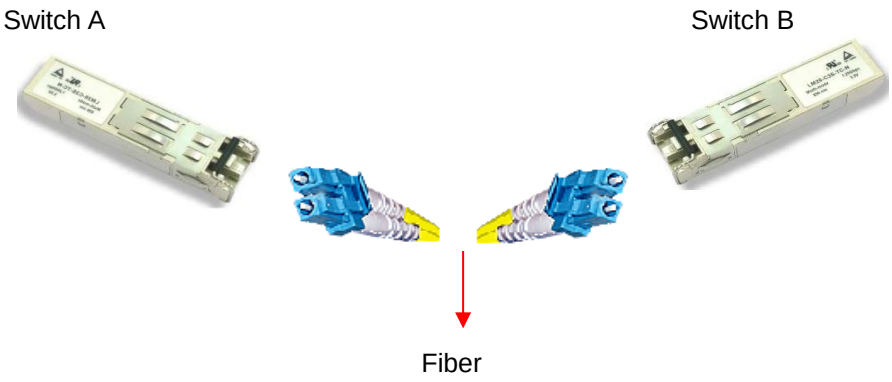
The device can be managed via the console port using a RS-232 cable which can be found in the package. Connect each end of the RS-232 cable to the switch and a PC respectively.

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




## 3.3.2 SFP

The switch comes with two combo ports which include a SFP port that can connect to other devices using SFP modules. The SFP modules are hot-swappable input/output devices that can be plugged into the SFP ports to connect the switch with the fiber-optic network. Remember that the TX port of Switch A should be connected to the RX port of Switch B.




1. Insert clean dust plugs into the SFPs after the cables are extracted from them.
2. Clean the optic surfaces of the fiber cables before you plug them back into the optical bores of another SFP module.

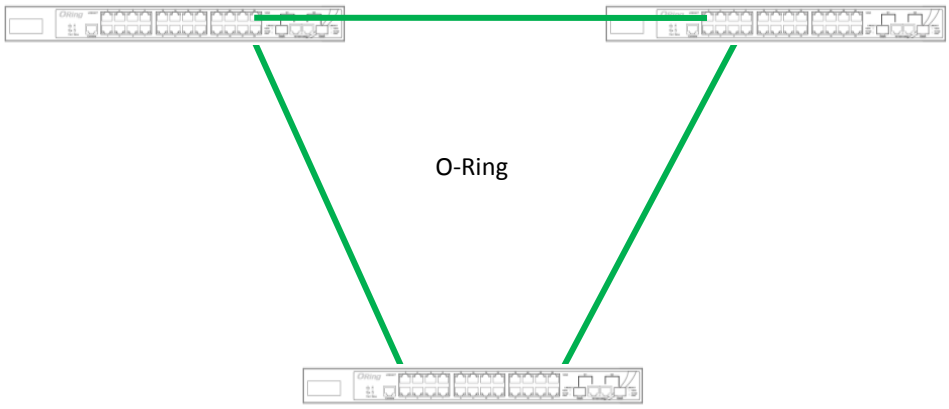
3. Avoid getting dust and other contaminants into the optical bores of your SFP modules in cases of malfunction

### 3.3.3 O-Ring/O-Chain

#### O-Ring

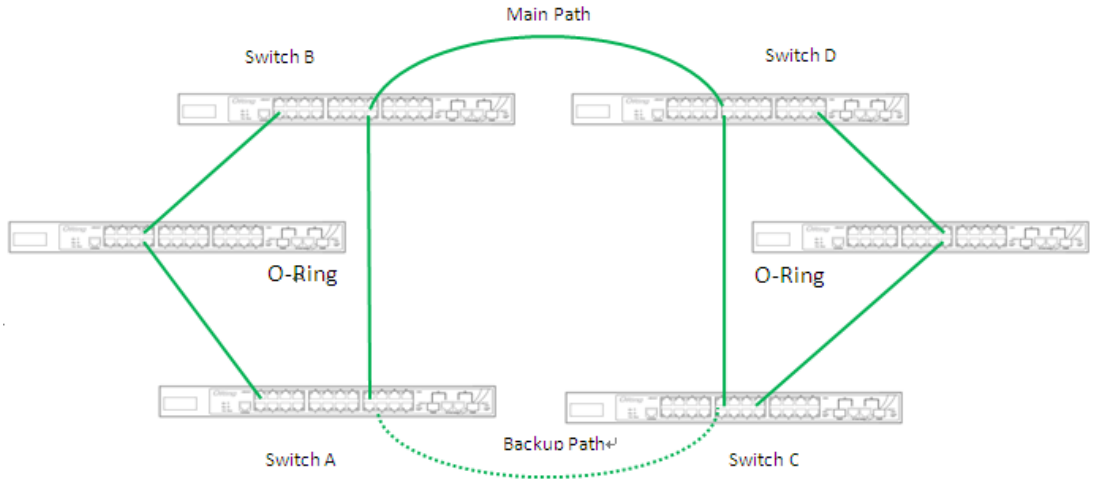
You can connect three or more switches to form a ring topology to gain network redundancy capabilities through the following steps.

1. Connect each switch to form a daisy chain using an Ethernet cable.
2. Set one of the connected switches to be the master and make sure the port setting of each connected switch on the management page corresponds to the physical ports connected. For information about the port setting, please refer to 4.1.2 Configurations.
3. Connect the last switch to the first switch to form a ring topology.



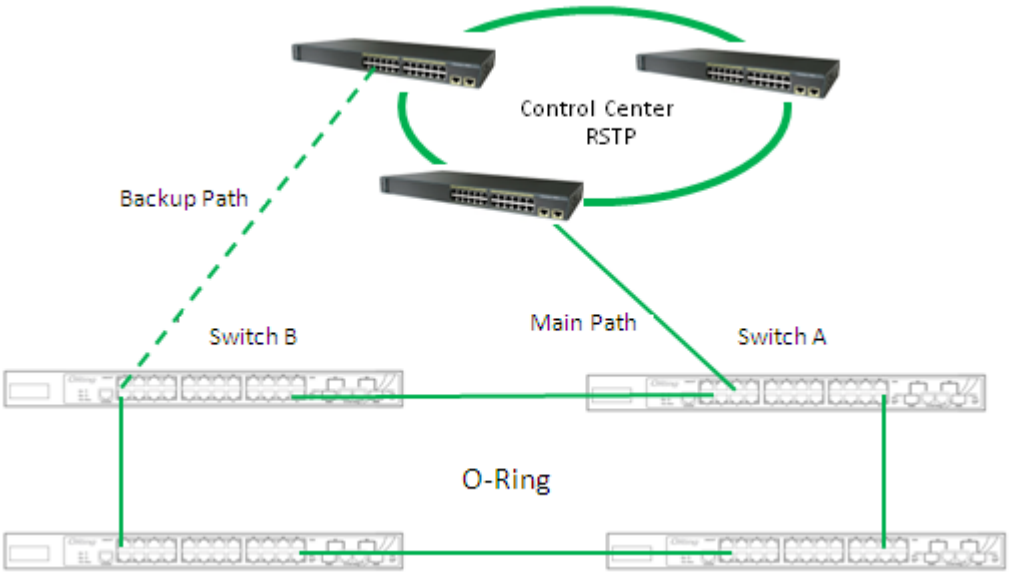

#### Coupling Ring

If you already have two O-Ring topologies and would like to connect the rings, you can form them into a coupling ring. All you need to do is select two switches from each ring to be connected, for example, switch A and B from Ring 1 and switch C and D from Ring 2. Decide which port on each switch to be used as the coupling port and then link them together, for example, port 1 of switch A to port 2 of switch C and port 1 of switch B to port 2 of switch D. Then, enable Coupling Ring on the management page and select the coupling ring in correspondence to the connected port. For more information on port setting, please refer to 4.1.2 Configurations. Once the setting is completed, one of the connections will act as the main path while the other will act as the backup path.




## Dual Homing

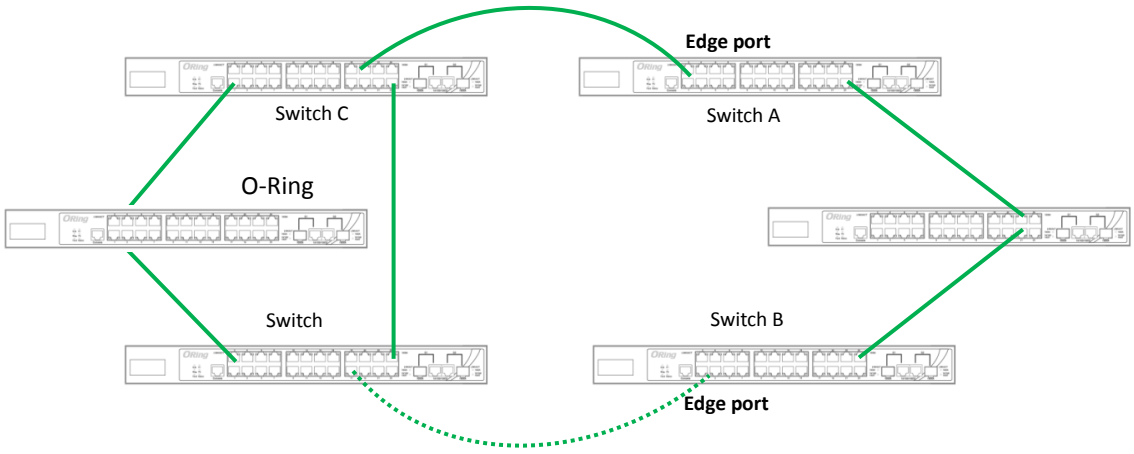
If you want to connect your ring topology to a RSTP network environment, you can use dual homing. Choose two switches (Switch A & B) from the ring for connecting to the switches in the RSTP network (backbone switches). The connection of one of the switches (Switch A or B) will act as the primary path, while the other will act as the backup path that is activated when the primary path connection fails.




## O-Chain

When connecting multiple O-Rings to meet your expansion demand, you can create an O-Chain topology through the following steps.

1. Select two switches from the chain (Switch A & B) that you want to connect to the O-Ring and connect them to the switches in the ring (Switch C & D).
2. In correspondence to the ports connected to the ring, configure an edge port for both of the connected switches in the chain by checking the box in the management page (see 4.1.2 Configurations).
3. Once the setting is completed, one of the connections will act as the main path, and the other as the backup path.



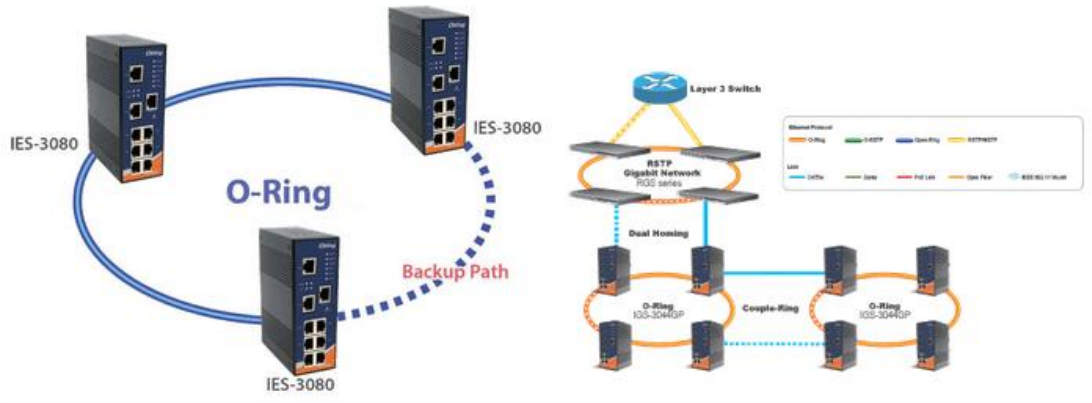
# Redundancy

Redundancy for minimized system downtime is one of the most important concerns for industrial networking devices. Hence, ORing has developed proprietary redundancy technologies including O-Ring and Open-Ring featuring faster recovery time than existing redundancy technologies widely used in commercial applications, such as STP, RSTP, and MSTP. ORing's proprietary redundancy technologies not only support different networking topologies, but also assure the reliability of the network.

## 4.1 O-Ring

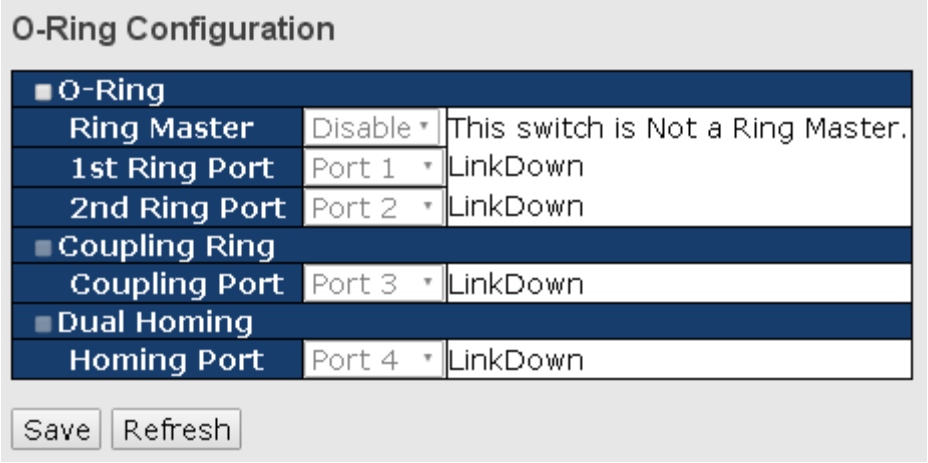
### 4.1.1 Introduction

O-Ring is ORing's proprietary redundant ring technology, with recovery time of less than 30 milliseconds (in full-duplex Gigabit operation) or 10 milliseconds (in full-duplex Fast Ethernet operation) and up to 250 nodes. The ring protocols identify one switch as the master of the network, and then automatically block packets from traveling through any of the network's redundant loops. In the event that one branch of the ring gets disconnected from the rest of the network, the protocol automatically readjusts the ring so that the part of the network that was disconnected can reestablish contact with the rest of the network. The O-Ring redundant ring technology can protect mission-critical applications from network interruptions or temporary malfunction with its fast recover technology.




### 4.1.2 Configurations

O-Ring supports three ring topologies: **Ring Master**, **Coupling Ring**, and **Dual Homing**. You can configure the settings in the interface below.




| Label | Description |
|---|---|
| **O-Ring** | Check to enable O-Ring topology. |
| **Ring Master** | Only one ring master is allowed in a ring. However, if more than one switches are set to enable **Ring Master**, the switch with the lowest MAC address will be the active ring master and the others will be backup masters. |
| **1st Ring Port** | The primary port when the switch is ring master |
| **2nd Ring Port** | The backup port when the switch is ring master |
| **Coupling Ring** | Check to enable **Coupling Ring**. **Coupling Ring** can divide a big ring into two smaller rings to avoid network topology changes affecting all switches. It is a good method for connecting two rings. |
| **Coupling Port** | Ports for connecting multiple rings. A coupling ring needs four switches to build an active and a backup link. Links formed by the coupling ports will run in active/backup mode. |
| **Dual Homing** | Check to enable **Dual Homing**. When **Dual Homing** is enabled, the ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work in active/backup mode, and connect each ring to the normal switches in RSTP mode. |
| **Apply** | Click to activate the configurations. |

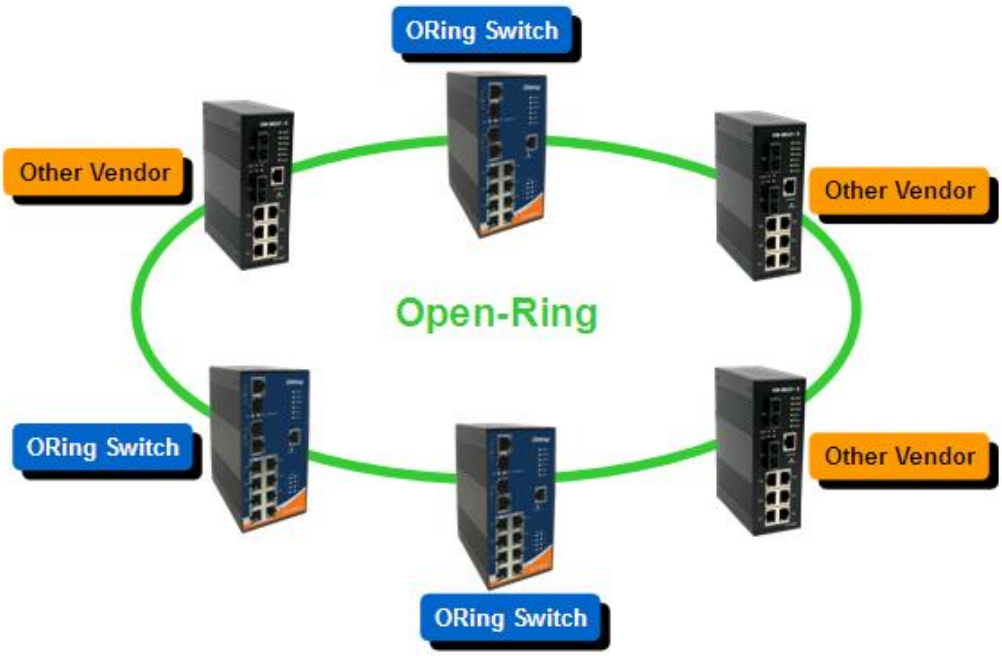
**Note:** due to heavy loading, setting one switch as ring master and coupling ring at the same time is not recommended.

# 4.2 Open-Ring

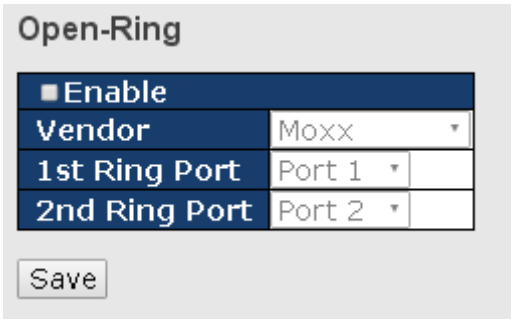
## 4.2.1 Introduction

Open-Ring is a technology developed by ORing to enhance ORing switches' interoperability

with other vendors' products. With this technology, you can add any ORing switches to the network based on other ring technologies.




## 4.2.2 Configurations




| Label | Description |
|---|---|
| **Enable** | Check to enable Open-Ring topology |
| **Vender** | Choose the venders that you want to join in their rings |
| **1st Ring Port** | The first port to connect to the ring |
| **2nd Ring Port** | The second port to connect to the ring |

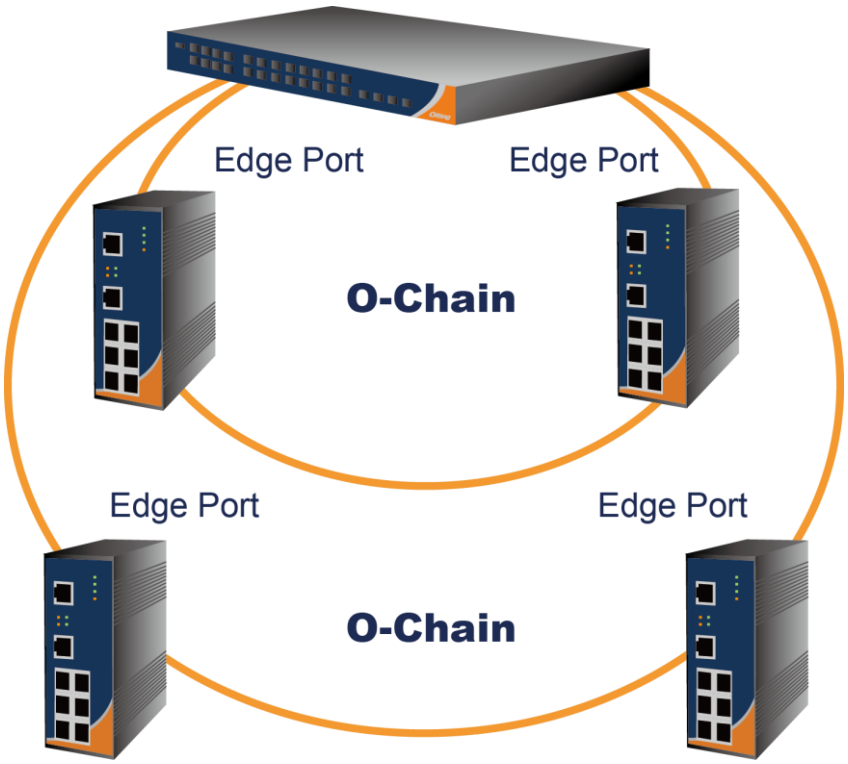
# 4.3 O-Chain

## 4.3.1 Introduction

O-Chain is ORing's revolutionary network redundancy technology which enhances network redundancy for any backbone networks, providing ease-of-use and maximum fault-recovery

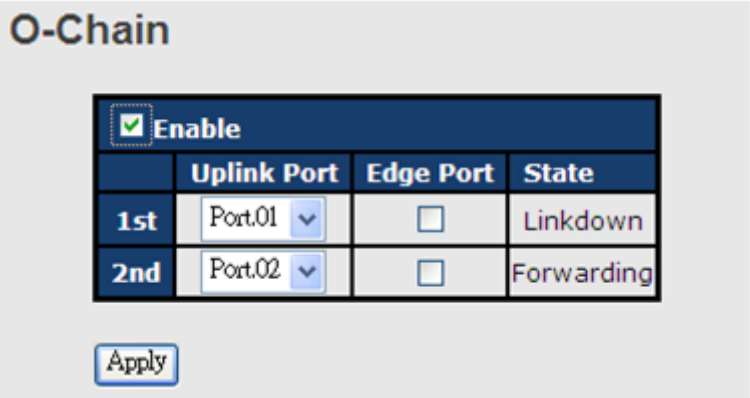
swiftness, flexibility, compatibility, and cost-effectiveness in a set of network redundancy topologies. The self-healing Ethernet technology designed for distributed and complex industrial networks enables the network to recover in less than 30 milliseconds (in full-duplex Gigabit operation) or 10 milliseconds (in full-duplex Fast Ethernet operation) for up to 250 switches if at any time a segment of the chain fails.

O-Chain allows multiple redundant rings of different redundancy protocols to join and function together as a large and the most robust network topologies. It can create multiple redundant networks beyond the limitations of current redundant ring technologies.




## 4.3.2 Configurations

O-Chain is very easy to configure and manage. Only one edge port of the edge switch needs to be defined. Other switches beside them just need to have O-Chain enabled.



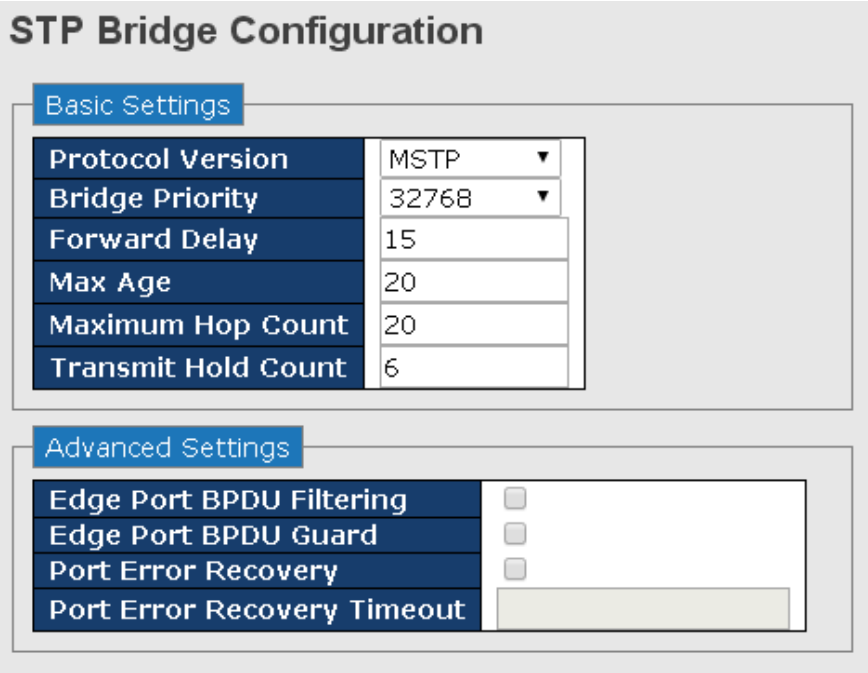

| Label | Description |
|---|---|
| **Enable** | Check to enable O-Chain function |
| **1st Ring Port** | The first port connecting to the ring |
| **2nd Ring Port** | The second port connecting to the ring |
| **Edge Port** | An O-Chain topology must begin with edge ports. The ports with a smaller switch MAC address will serve as the backup link and RM LED will light up. |

# 4.4 MSTP

## STP/RSTP

STP (Spanning Tree Protocol), and its advanced versions RSTP (Rapid Spanning Tree Protocol) and MSTP (Multiple Spanning Tree Protocol), are designed to prevent network loops and provide network redundancy. Network loops occur frequently in large networks as when two or more paths run to the same destination, broadcast packets may get in to an infinite loop and hence causing congestion in the network. STP can identify the best path to the destination, and block all other paths. The blocked links will stay connected but inactive. When the best path fails, the blocked links will be activated. Compared to STP which recovers a link in 30 to 50 seconds, RSTP can shorten the time to 5 to 6 seconds. In other words, RSTP provides faster spanning tree convergence after a topology changes. The switch supports STP and will auto detect the connected device running on STP or RSTP protocols.

## 4.4.1 Bridge Setting




| Label | Description |
|---|---|
| **Protocol Version** | Select Spanning Tree type , support STP / RSTP / MSTP |
| **Bridge Priority** | A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, you must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule |
| **Forwarding Delay Time** | The time of a port waits before changing from RSTP learning and listening states to forwarding state. The valid value is between 4 through 30. |
| **Max Age** | The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. The valid value is between 6 through 40. |
| **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 to. Valid values are in the range 6 to 40 hops. |
| **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. |
| **Edge Port BPDU Filtering** | Control whether a port explicitly configured as Edge will transmit and receive BPDUs. |

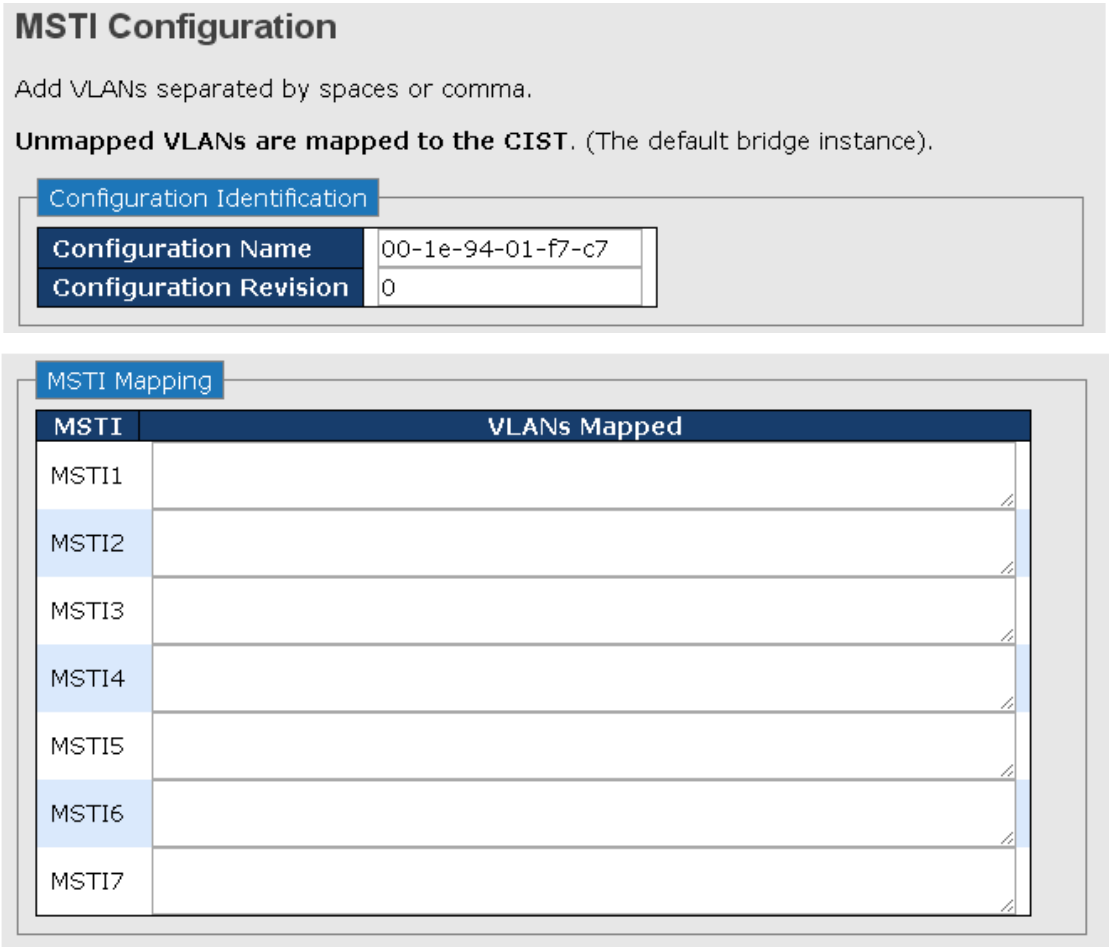
| | |
|---|---|
| **Edge Port BPDU Guard** | Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology. |
| **Port Error Recovery** | Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot. |
| **Port Error Recovery Timeout** | The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours). |

**NOTE**: the calculation of the MAX Age, Hello Time, and Forward Delay Time is as follows:

2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)

## 4.4.2 MSTI Mapping

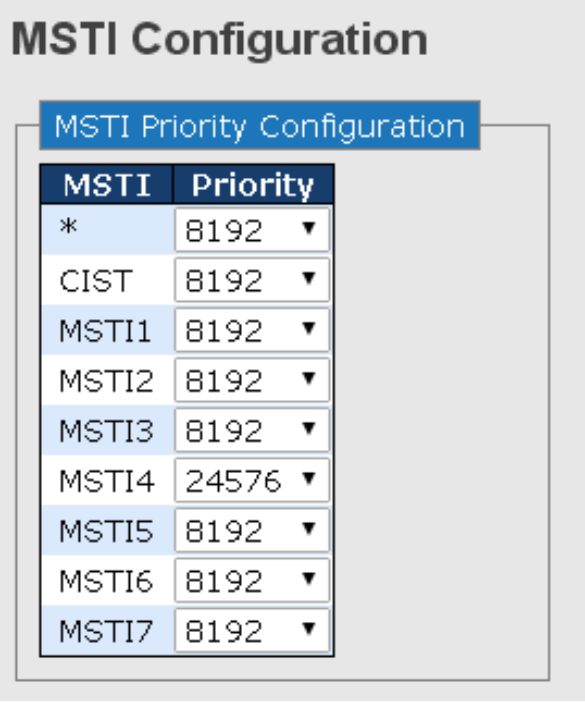
This page allows you to examine and adjust the configuration of STP MSTI. This function will map VLANs to a specific MSTP instance. .



| Label | Description |
|---|---|
| **Configuration Name** | The name for this MSTI. Maximum characters allowed are 32. The default name is the switch's MAC address. |
| **Configuration Revision** | The revision for this MSTI. |
| **MSTI** | Instance identifier to configure. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. (Range: 1-7) |
| **VLANs Mapped** | VLANs to assign to this MST instance. Note that the VLANs must be separated with comma and/or space and one VLAN can only be mapped to one MSTI. (Range: 1-4094) |

## 4.4.3 MSTI Priorities

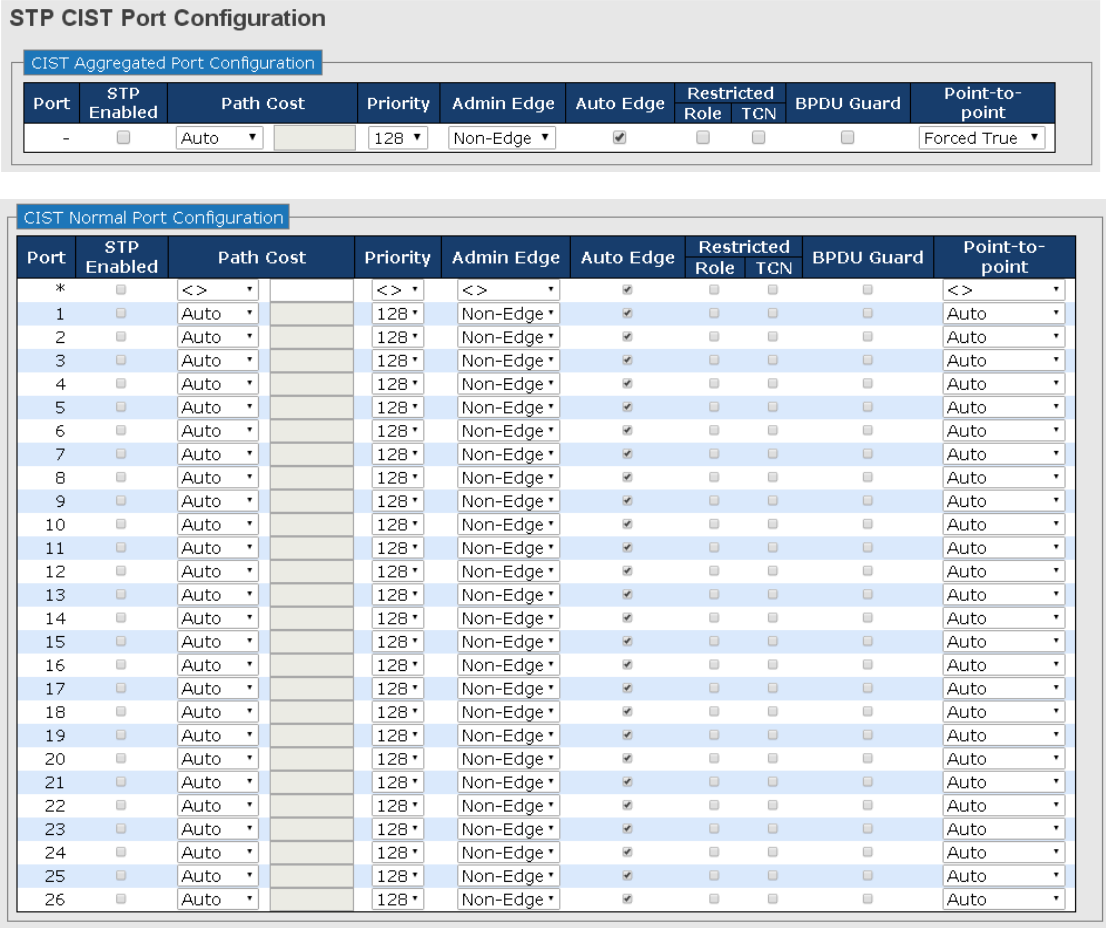
You can configure the bridge priority for the CIST and any configured MSTI. Remember that RSTP will look up each MST Instance as a single bridge node.




| Label | Description |
|---|---|
| **MSTI** | Instance identifier to configure. |
| **Priority** | The priority of a spanning tree instance. |

## 4.4.4 CIST Ports

This page allows you to configure CIST ports including physical and aggregated ports.



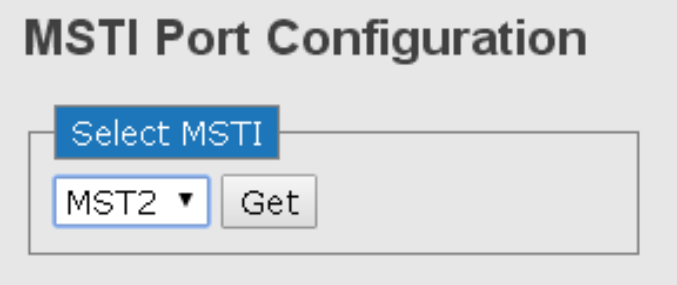

| Label | Description |
|---|---|
| **Port** | The port identifier |
| **STP Enabled** | Check to enable STP Function |
| **Path Cost** | This parameter allows you to control the path cost for each port. **Auto** will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. **Specific** will allow you to enter a user-defined value. |
| **Path Cost Value (1-200000000)** | If you choose Specific from the drop-down list, you can specify a value ranging from 1 to 200000000. As STA determines the best path between devices based on path cost, lower values are suggested for ports attached to faster media, and higher values for ports with slower media. |
| **Priority** | Specify the priority for a port in the Spanning Tree Algorithm. If |

| | |
|---|---|
| | the path cost for all ports on a switch are the same, the port with the highest priority (usually with the lowest value) will be used as an active link in the Spanning Tree. In this way, a port with higher priority is less likely to be blocked if the Spanning Tree Algorithm discovers network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. |
| **Admin Edge** | When an interface is attached to a LAN segment at the end of a bridged LAN or to an end node, you can enable this function so forwarding loops can pass directly through to the spanning tree forwarding state. Since end nodes cannot cause forwarding loops, enabling this function allows for quicker convergence for devices such as workstations or servers. The current forwarding database will be retained to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events. The spanning tree will not initiate reconfiguration when the interface changes state. It also overcomes other STA-related timeout problems. Keep in mind that this feature should only be used for ports connected to an end node device. |
| **Auto Edge** | Check to enable automatic edge detection on a bridge port. The bridge will then determine that a port is at the edge of the network if no BPDU's are received on the port. |
| **Restricted – Role** | Enabling this function will prevent the port from being selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. This port will be selected as an Alternate Port after the Root Port has been selected. The function 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 influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard. |
| **Restricted -TCN** | Enabling this function will prevent the port from propagating received topology change notifications and topology changes to other ports. The function can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location |

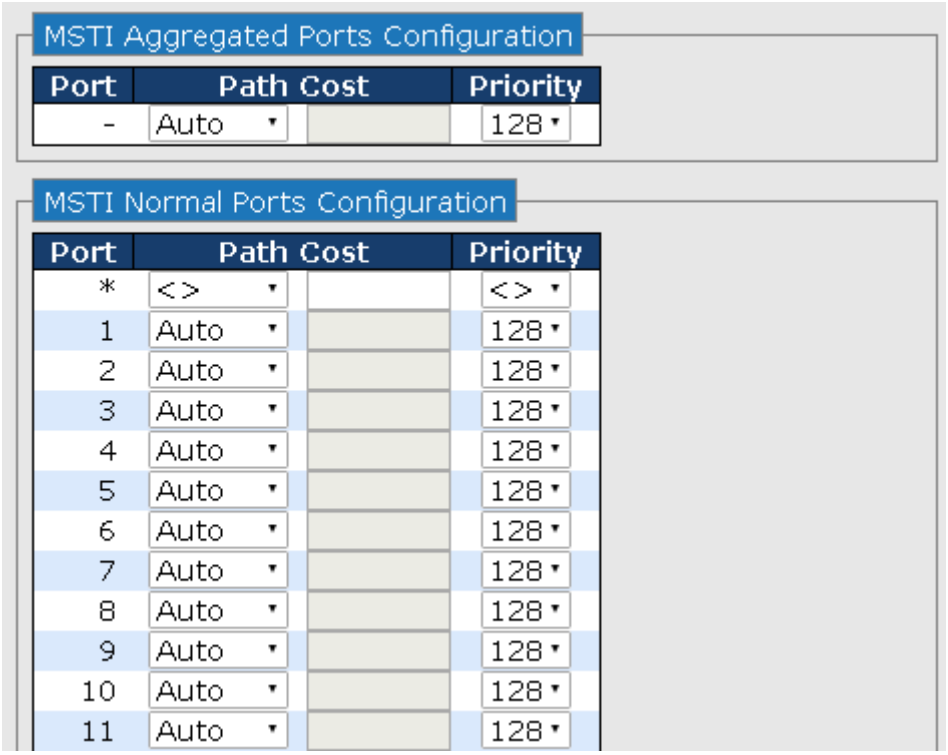
| | |
|---|---|
| | information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently. |
| **BPDU Guard** | If enabled, the port will disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting. |
| **Point to Point** | Controls whether the port connects to a point-to-point LAN rather than to 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 the configurations. |

## 4.4.5 MSTI Ports

This page allows you to configure STA attributes for interfaces in a specific MSTI, including path cost, and port priority. You may use a different priority or path cost for ports of the same media type to indicate the preferred path.



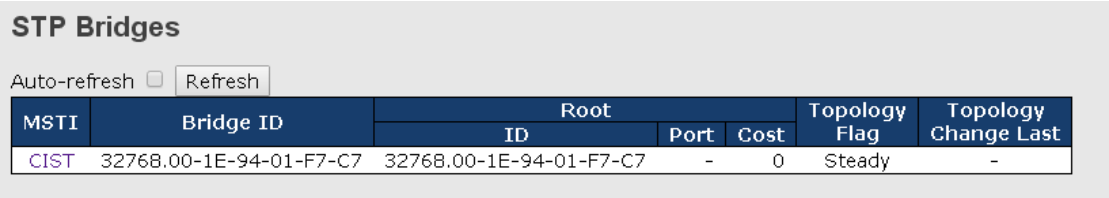

Choose a MSTI and click on **Get** will bring you to the following page.




| Label | Description |
|---|---|
| **Port** | The port identifier |
| **Path Cost** | As this parameter is used by the STA to determine the best path between devices, lower values are suggested for ports attached to faster media, and higher values for ports with slower media. (Path cost takes precedence over port priority.) The value will control the path cost incurred by the port. Auto will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Specific will allow you to enter a user-defined value. |
| **Priority** | Specify the priority for a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (usually with the lowest value) will be used as an active link in the Spanning Tree. In this way, a port with higher priority is less likely to be blocked if the Spanning Tree Algorithm discovers network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. |

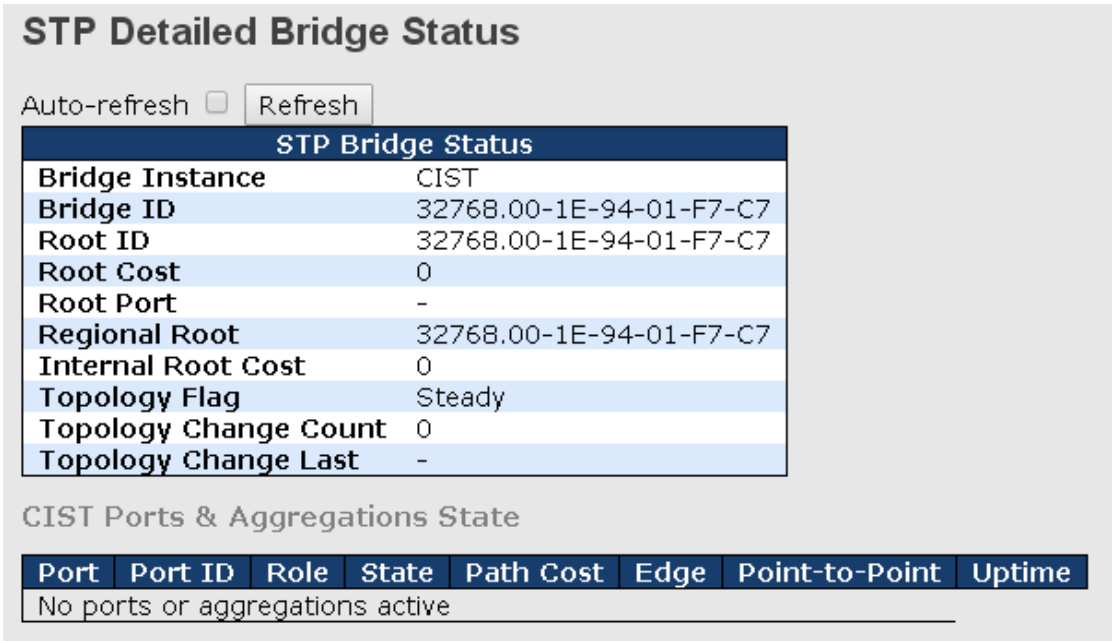
## 4.4.6 Bridge Status

This page will show STA information on the global bridge such as the switch and individual ports.




| Label | Description |
|---|---|
| **MSTI** | Indicates the bridge instance. |
| **Bridge ID** | A unique identifier for this bridge, consisting of the bridge priority, and MAC address (where the address is taken from the switch system). |
| **Root** | Root ID: A unique identifier of the device in the Spanning Tree that this switch has been accepted as the root device, consisting of the priority and MAC address.<br>Root Port: the number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If no root port is designated, it means this switch has been accepted as the root device of the Spanning Tree network.<br>Root Cost: the path cost from the root port on this switch to the root device. The cost for the root bridge zero. For all other bridges, it is the sum of the port path costs on the least cost path to the root bridge. |
| **Technology Flag** | The current state of the Topology Change Notification flag (TCN) for this bridge instance. |
| **Technology Change Last** | Time since the Spanning Tree was last reconfigured. |

Click on CIST will bring out the following information window. Regional Root is the bridge ID of the designated regional root bridge, inside the MSTP region of this bridge. Internal Root Path is the path cost regional root path cost. The cost for the Regional Root Bridge is zero, and for all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. Note that these parameters only apply to the CIST instance.

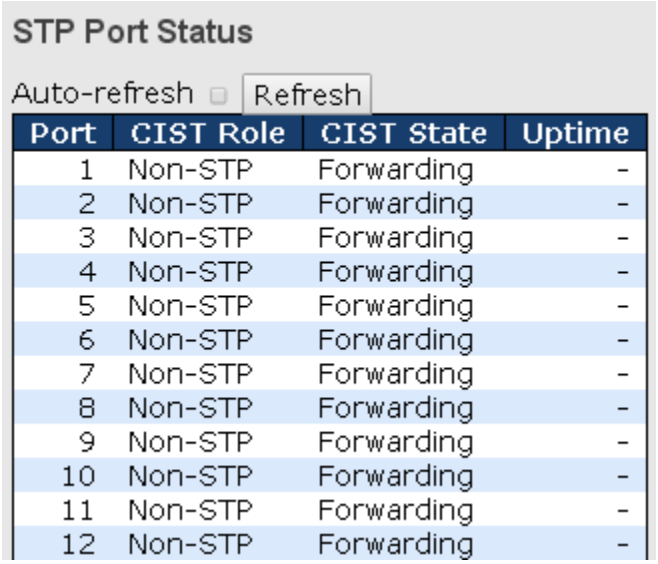



| Label | Description |
|---|---|
| **Port** | The port identifier. |
| **Port ID** | The port identifier used by the RSTP protocol, consisting of the priority and the logical port index of the bridge port. |
| **Role** | The role of a port is assigned based on whether it is part of the active topology connecting the bridge to the root bridge (i.e., root port), connecting a LAN through the bridge to the root bridge (i.e., designated port); or is an alternate or backup port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. |
| **State** | Displays the current state of this port in the Spanning Tree. |
| **Path Cost** | The path cost of the port contributed to the paths towards the spanning tree root which include this port. It can be a value assigned by the Auto setting or any explicitly configured value. |
| **Edge** | The current RSTP port (operational) Edge Flag. An Edge Port is a switch port to which no bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transitions directly to the Forwarding Port State, since there is no possibility of it participating in a loop. |
| **Point-to-Point** | Indicates a connection to exactly one other bridge. The flag may be automatically computed or explicitly configured. The |

| | |
|---|---|
| | point-to-point properties of a port affect how fast it can transition RSTP states. |
| **Uptime** | The time since the bridge port was last initialized. |

## 4.4.7 Port Status

This page shows the STA functional status of participating ports.

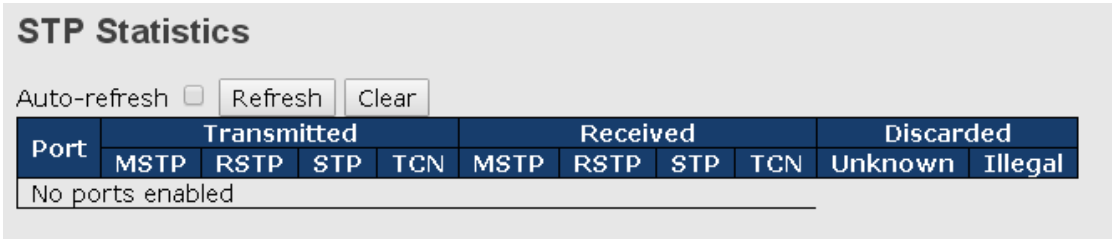



| Label | Description |
|---|---|
| **Port** | The port identifier. |
| **CIST Role** | The role of a port is assigned based on whether it is part of the active topology connecting the bridge to the root bridge (i.e., root port), connecting a LAN through the bridge to the root bridge (i.e., designated port); or is an alternate or backup port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. |
| **CIST State** | Displays the current state of this port in the Spanning Tree. There are three states.<br>**Blocking**: the port will receive STA configuration messages, but will not forward packets.<br>**Learning**: The port transmits configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. The port address table will be cleared, and the port will learn addresses.<br>**Forwarding**: The port will forward packets while learning addresses. |

| | |
|---|---|
| **Uptime** | The time since the bridge port was last initialized. |

## 4.4.8 Port Statistics

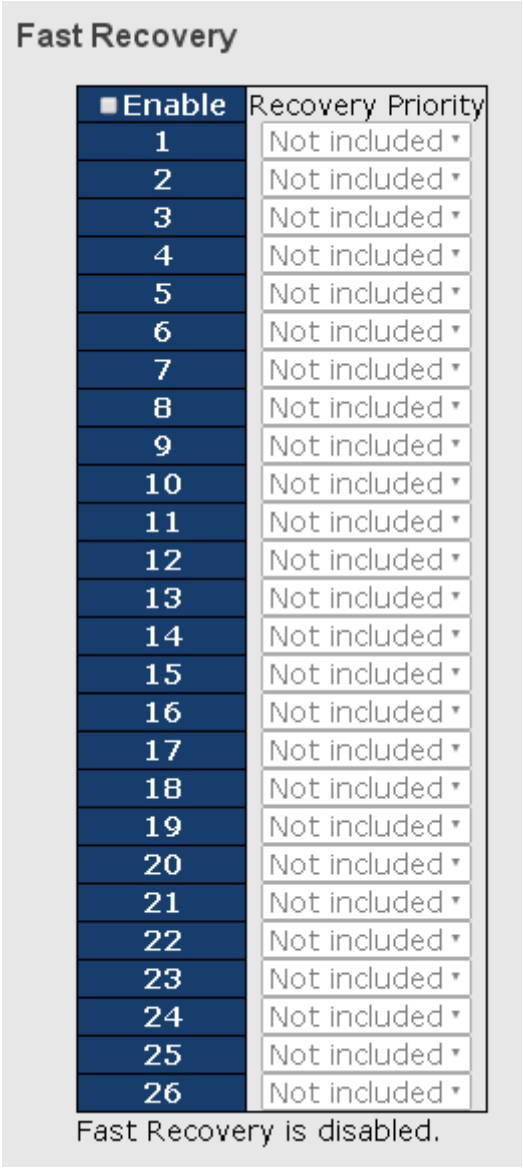
This page shows statistics on spanning tree protocol packets crossing each port.




| Label | Description |
|---|---|
| **Port** | The port identifier. |
| **Transmitted/Received** | MSTP: the number of MSTP Configuration BPDUs received/ transmitted on a port.<br>RSTP: the number of RSTP Configuration BPDUs received/ transmitted on a port.<br>RTP: the number of legacy STP Configuration BPDU's received/ transmitted on a port.<br>TCN: the number of (legacy) Topology Change Notification BPDUs received/transmitted on a port. |
| **Discarded** | Unknown: the number of unknown Spanning Tree BPDUs received (and discarded) on a port.<br>Illegal: the number of illegal Spanning Tree BPDUs received (and discarded) on a port. |

# 4.5 Fast Recovery

Fast recovery mode can be set to connect multiple ports to one or more switches, thereby providing redundant links. Fast recovery mode supports 5 priorities. Only the first priority will be the active port, and the other ports with different priorities will be backup ports.




| Label | Description |
|---|---|
| **Enable** | Activate fast recovery mode. |
| **Recovery Priority** | Specify the recovery priority for each port. |
| **Save** | Click to save the configurations. |

# Management

The switch can be controlled via a built-in web server which supports Internet Explorer (Internet Explorer 5.0 or above versions) and other Web browsers such as Chrome. Therefore, you can manage and configure the switch easily and remotely. You can also upgrade firmware via a web browser. The Web management function not only reduces network bandwidth consumption, but also enhances access speed and provides a user-friendly viewing screen.

By default, IE5.0 or later version do not allow Java applets to open sockets. You need to modify the browser setting separately in order to enable Java applets for network ports.

## Preparing for Web Management

You can access the management page of the switch via the following default values:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

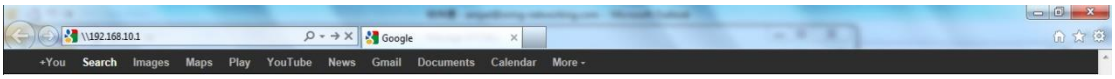
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

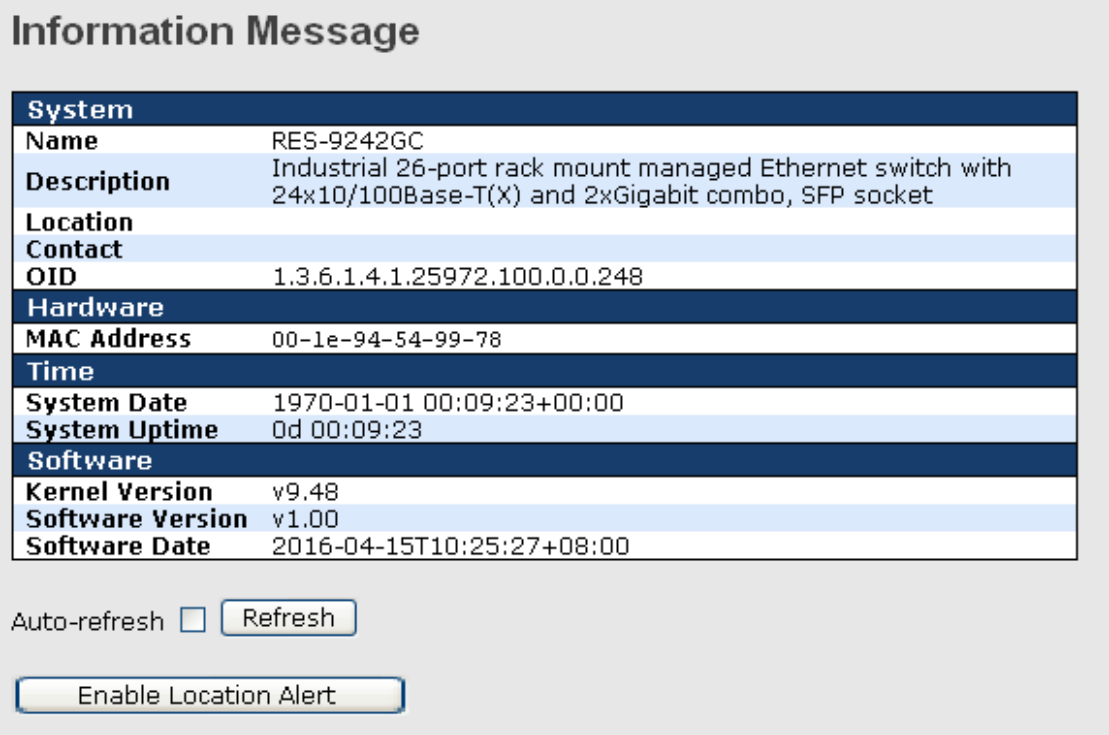
## System Login

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




3. A login screen appears.
4. Type in the username and password. The default username and password is **admin**.
5. Click **Enter** or **OK** button, the management Web page appears.

After logging in, you can see the information of the switch as below.



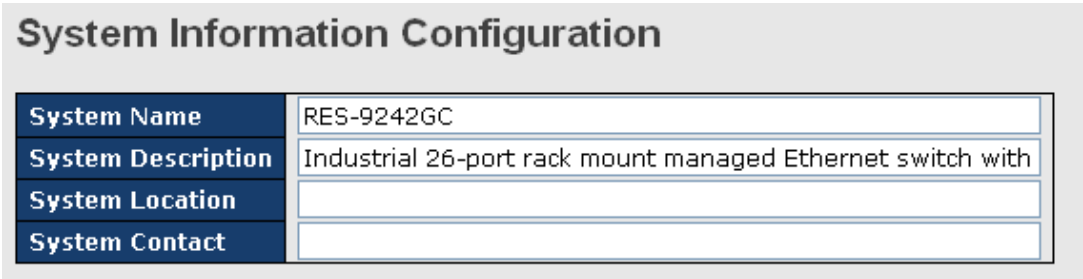

On the left hand side of the management interface shows links to various settings. You can click on the links to access the configuration pages of different functions.

# 5.1 Basic Settings

Basic Settings allow you to configure the basic functions of the switch.

## 5.1.1 System Information

This page shows the general information of the switch.

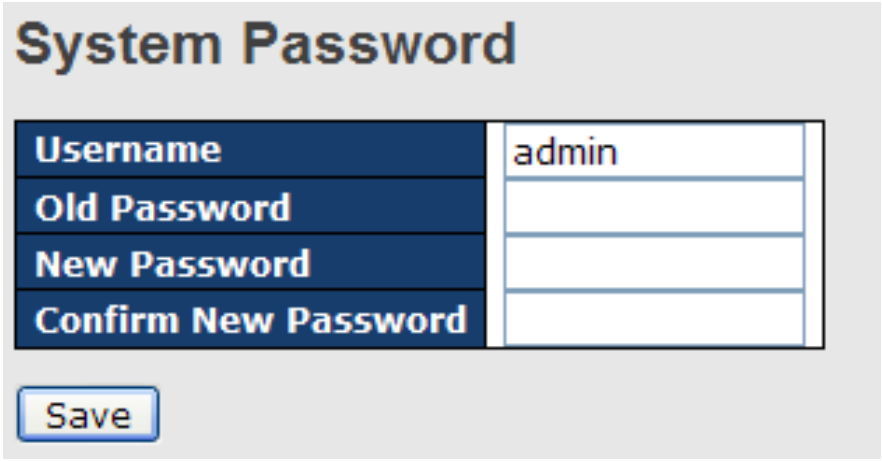



| Label | Description |
|---|---|
| **System Name** | An administratively assigned name for the managed node. By convention, this is the node's fully-qualified domain name. |

| | |
|---|---|
| | A domain name is a text string consisting of alphabets (A-Z, a-z), digits (0-9), and minus sign (-). Space is not allowed to be part of the 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** | Description of the device |
| **System Location** | The physical location of the node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and only ASCII characters from 32 to 126 are allowed. |
| **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 only ASCII characters from 32 to 126 are allowed. |
| **Save** | Click to save changes. |
| **Reset** | Click to undo any changes made locally and revert to previously saved values. |

## 5.1.2Admin & Password

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

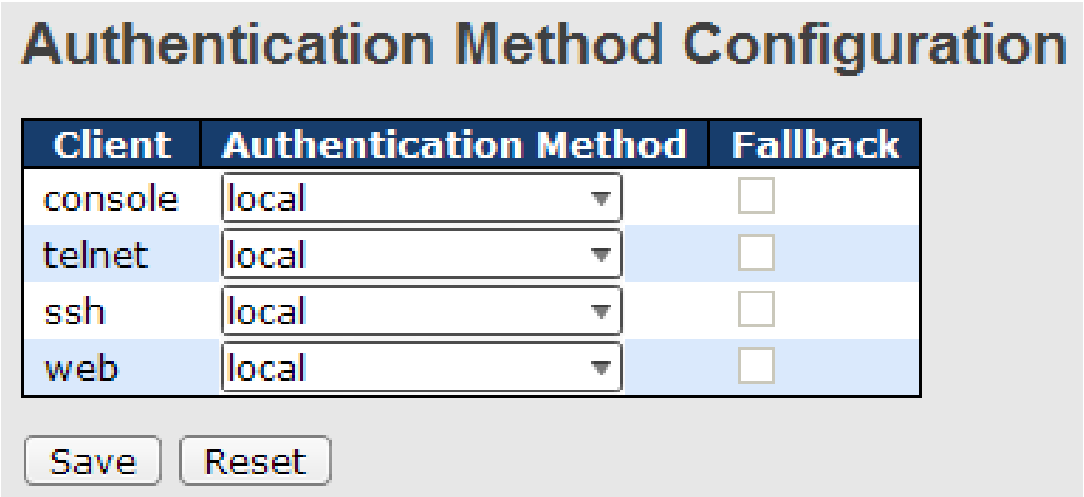



| Label | Description |
|---|---|
| **Old Password** | The existing password. If this is incorrect, you cannot set the new password. |
| **New Password** | The new system password. The allowed string length is 0 to |

| | |
|---|---|
| | 31, and only ASCII characters from 32 to 126 are allowed. |
| **Confirm New Password** | Re-type the new password. |
| **Save** | Click to save changes. |

## 5.1.3 Authentication

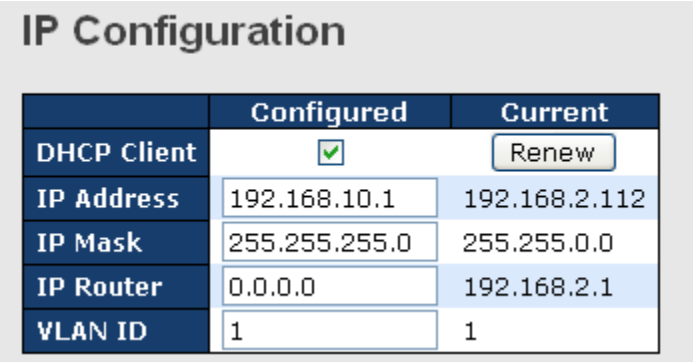
This page allows you to configure how a user is authenticated when he/she logs into the switch via one of the management interfaces.




| Label | Description |
|---|---|
| **Client** | The management client for which the configuration below applies. |
| **Authentication Method** | Authentication Method can be set to one of the following values:<br>**None**: authentication is disabled and login is not possible.<br>**Local**: local user database on the switch is used for authentication.<br>**Radius**: a remote RADIUS server is used for authentication. |
| **Fallback** | Check to enable fallback to local authentication.<br>If none of the configured authentication servers are active, the local user database is used for authentication.<br>This is only possible if **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 |

## 5.1.4 IP Settings

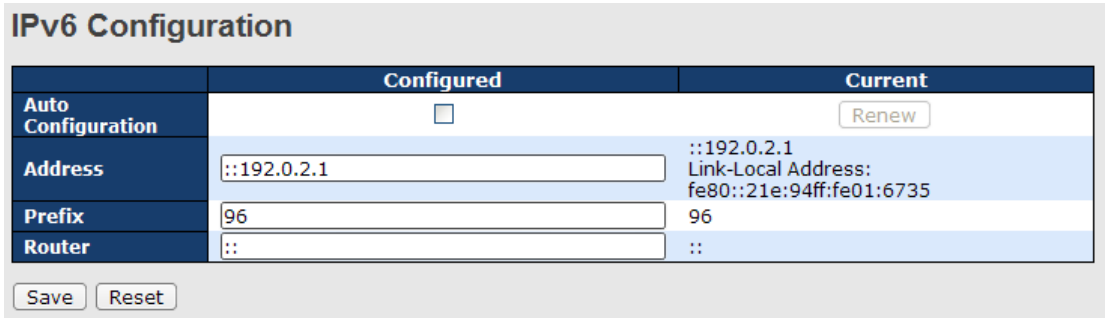
You can configure IP information of the switch in this page.




| Label | Description |
|---|---|
| **DHCP Client** | Enable the DHCP client by checking this box. If DHCP fails or the configured IP address is zero, DHCP will retry. If DHCP retry fails, DHCP will stop trying and the configured IP settings will be used. |
| **IP Address** | Assigns the IP address of the network in use. If DHCP client function is enabled, you do not need to assign the IP address. The network DHCP server will assign the IP address to the switch and it will be displayed in this column. The default IP is 192.168.10.1. |
| **IP Mask** | Assigns the subnet mask of the IP address. If DHCP client function is enabled, you do not need to assign the subnet mask. |
| **IP Router** | Assigns the network gateway for the switch. The default gateway is 192.168.10.254. |
| **VLAN ID** | Provides the managed VLAN ID. The allowed range is 1 through 4095. |
| **Save** | Click to save changes. |
| **Reset** | Click to undo any changes made locally and revert to previously saved values. |

## 5.1.5 IPv6 Settings

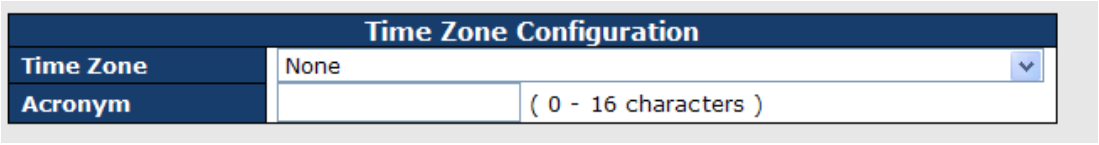
You can configure IPv6 information of the switch in the page.




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

## 5.1.6 Daylight Saving Time

### Time Zone Configuration

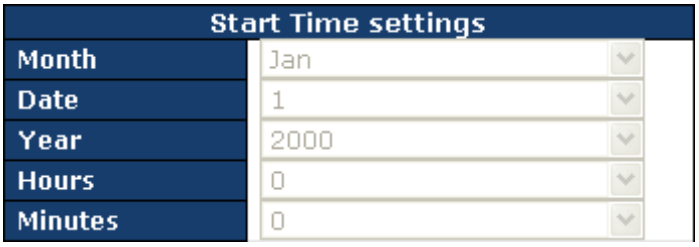



| Label | Description |
|---|---|
| **Time Zone** | Select the time zone from the dropdown list according to the location of the switch and click **Save**. |
| **Acronym** | Set an acronym for the time zone. This is a user configurable acronym for identifying the time zone. Up to 16 alpha-numeric characters can be input. The acronym can contain '-', '_' or '.' |

### Daylight Saving Time Configuration

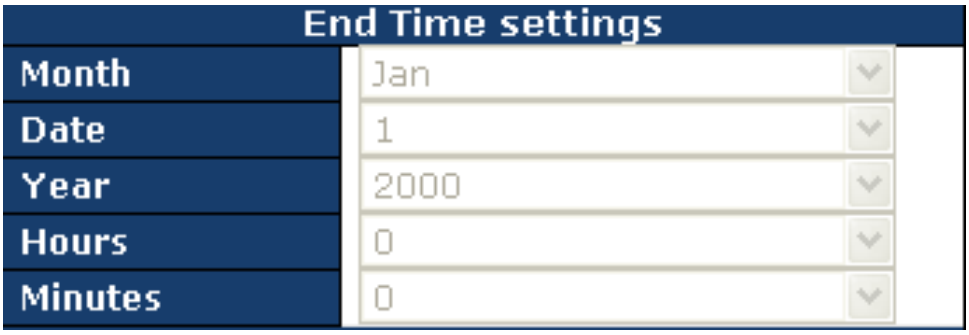
| Label | Description |
|---|---|
| **Daylight Saving Time** | This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select **Disable** to disable the configuration or **Recurring** to configure the duration to repeat every year. Select **Non-Recurring** to configure the duration for single time configuration. Default is **Disabled.** |

### Start Time Settings



| Label | Description |
|---|---|
| **Year** | Select the starting year |
| **Date** | Select the starting day. |
| **Month** | Select the starting month. |
| **Hours** | Select the starting hour. |
| **Minutes** | Select the starting minute. |

### End Time Settings



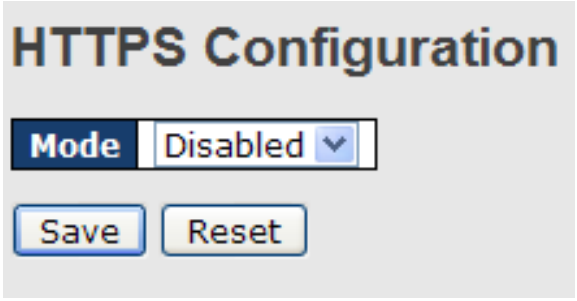

| Label | Description |
|---|---|
| **Year** | Select the ending year |
| **Day** | Select the ending day. |
| **Month** | Select the ending month. |
| **Hours** | Select the ending hour. |
| **Minutes** | Select the ending minute. |

### Offset Settings

| Label | Description |
|---|---|
| **Offset** | Configures the offset time. The time is measured by minute. |

## 5.1.7 HTTPS

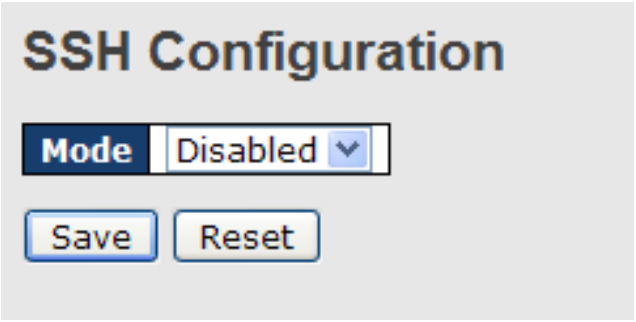
You can configure HTTPS settings in the following page.




| Label | Description |
|---|---|
| **Mode** | Indicates the selected HTTPS mode. When the current connection is HTTPS, disabling HTTPS will automatically redirect web browser to an HTTP connection. The modes include:<br>**Enabled**: enable HTTPS.<br>**Disabled**: disable HTTPS. |
| **Save** | Click to save changes |
| **Reset** | Click to undo any changes made locally and revert to previously saved values |

### 5.1.8 SSH

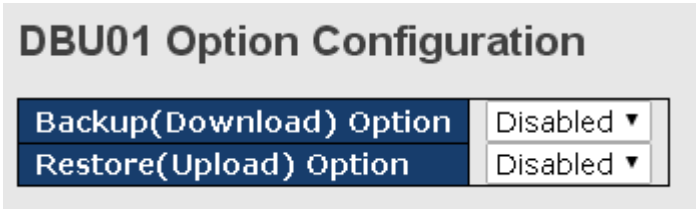
You can configure SSH settings in the following page.




| Label | Description |
|---|---|
| **Mode** | Indicates the selected SSH mode. The modes include:<br>**Enabled**: enable SSH.<br>**Disabled**: disable SSH. |
| **Save** | Click to save changes |
| **Reset** | Click to undo any changes made locally and revert to previously saved values |

## 5.1.9 DBU01

DBU01 is an embedded configuration backup/restore function. It allows you to store and restore device configurations without using a PC.

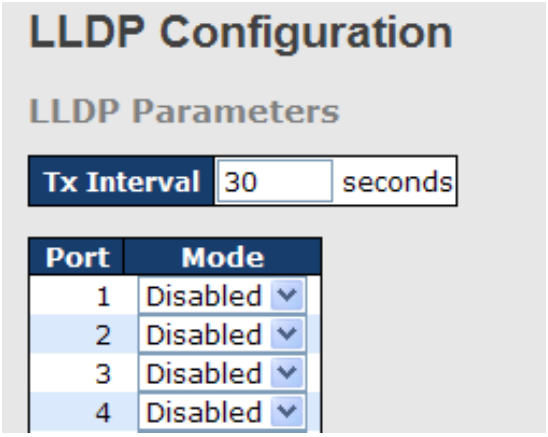



| Label | Description |
|---|---|
| **Backup Option** | Enable or disable backup function. If enabled, existing configurations will be stored as a backup file. |
| **Restore Option** | Enable or disable backup function. If enabled, the system will apply saved configurations to the device. |

## 5.1.10 LLDP

### 5.1.10.1 LLDP Configurations

This page allows you to examine and configure LLDP port settings.

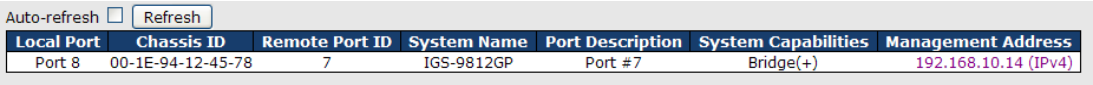



| Label | Description |
|---|---|
| **Port** | The switch port number to which the following settings will be applied. |
| **Mode** | Indicates the selected LLDP mode<br>**Rx only**: the switch will not send out LLDP information, but LLDP information from its neighbors will be analyzed.<br>**Tx only**: the switch will drop LLDP information received from |

| | |
|---|---|
| | its neighbors, but will send out LLDP information.<br>**Disabled**: the switch will not send out LLDP information, and will drop LLDP information received from its neighbors.<br>**Enabled**: the switch will send out LLDP information, and will analyze LLDP information received from its neighbors. |

## 5.1.10.2 LLDP Neighbor Information

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

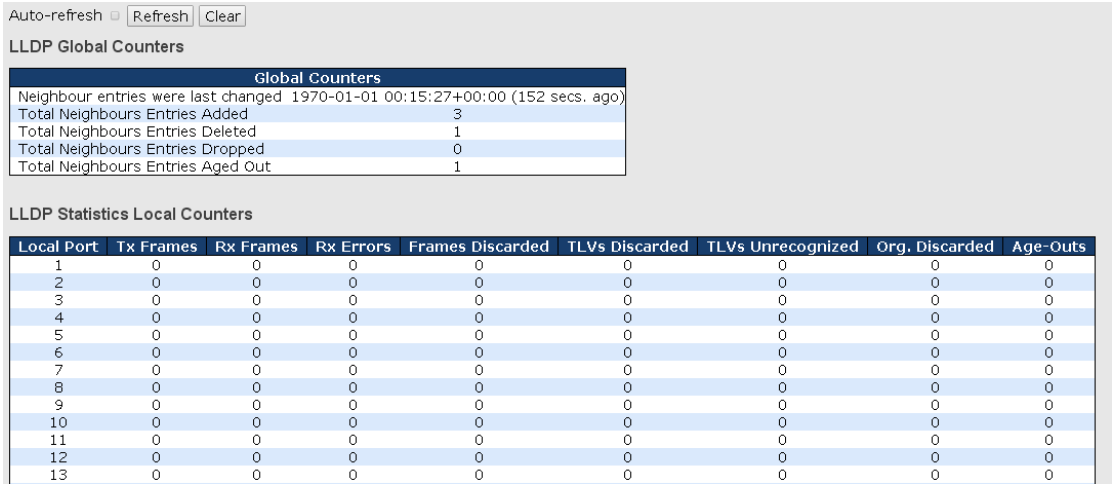



| Label | Description |
|---|---|
| **Local Port** | The port that you use to transmits and receives LLDP frames. |
| **Chassis ID** | The identification number of the neighbor sending out the LLDP frames. |
| **Remote Port ID** | The identification of the neighbor port |
| **System Name** | The name advertised by the neighbor. |
| **Port Description** | The description of the port advertised by the neighbor. |
| **System Capabilities** | Description of the neighbor's capabilities. The capabilities include:<br>1. **Other**<br>2. **Repeater**<br>3. **Bridge**<br>4. **WLAN Access Point**<br>5. **Router**<br>6. **Telephone**<br>7. **DOCSIS Cable Device**<br>8. **Station Only**<br>9. **Reserved**<br>When a capability is enabled, a (+) will be displayed. If the capability is disabled, a (-) will be displayed. |
| **Management Address** | The neighbor's address which can be used to help network management. This may contain the neighbor's IP address. |

| | |
|---|---|
| **Refresh** | Click to refresh the page immediately |
| **Auto-refresh** | Check to enable an automatic refresh of the page at regular intervals |

## 5.1.10.3 Port Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters will apply settings to the whole switch stack, while local counters will apply settings to specified switches.




### Global Counters

| Label | Description |
|---|---|
| **Neighbor entries were last changed at** | Shows the time when the last entry was deleted or added. |
| **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 full entry table |
| **Total Neighbors Entries Aged Out** | Shows the number of entries deleted due to expired time-to-live |

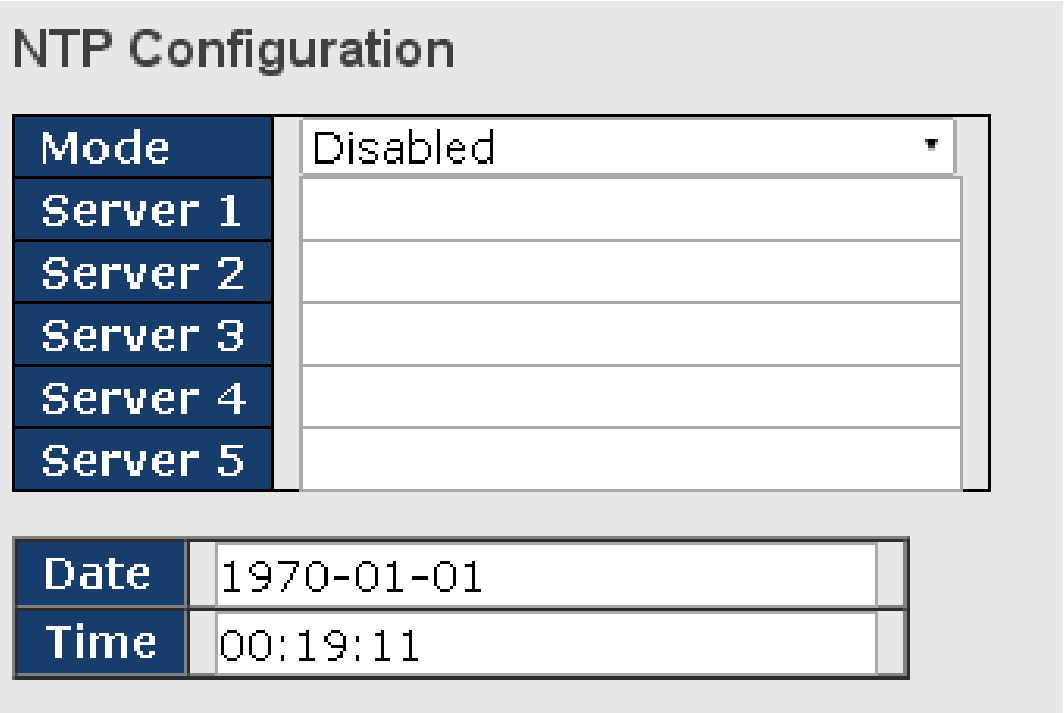
### Local Counters

| Label | Description |
|---|---|
| **Local Port** | The port that receives or transmits LLDP frames |
| **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 errors |
| **Frames Discarded** | If a port receives an LLDP frame, and the switch's internal table is full, the LLDP frame will be counted and discarded. This situation is known as "too many neighbors" in the LLDP standard. LLDP frames require a new entry in the table if Chassis ID or Remote Port ID is not included in 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 (Type Length Value). If a TLV is malformed, it will be 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 the LLDP information is valid (age-out time). If no new LLDP frame is received during the age-out time, the LLDP information will be removed, and the value of the age-out counter will be incremented. |
| **Refresh** | Click to refresh the page immediately |
| **Clear** | Click to clear the local counters. All counters (including global counters) are cleared upon reboot. |
| **Auto-refresh** | Check to enable an automatic refresh of the page at regular intervals |

### 5.1.11 NTP

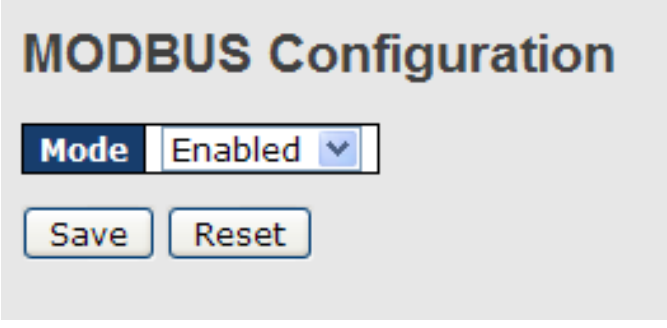
The function allows you to specify the Network Time Protocol (NTP) servers to query for the current time to maintain an accurate time on the switch, ensuring the system log record meaningful dates and times for event entries. With NTP, the switch can set its internal clock periodically according to an NTP time server. Otherwise, the switch will only record the time from the factory default set at the last bootup. When the NTP client is enabled, the switch regularly sends a request for a time update to a configured time server. A maximum of five time servers are supported. The switch will attempt to poll each server in the configured sequence.




| Label | Description |
|---|---|
| **Mode** | Select a NTP mode from the drop down list. |
| **Server** | Sets the IP address for up to five time servers. The switch will update the time from the servers, starting from the first to the fifth in sequence if any of them fails. The polling interval is fixed at 15 minutes. |

## 5.1.12 Modbus TCP

Modbus TCP uses TCP/IP and Ethernet to carry the data of the Modbus message structure between compatible devices. The protocol is commonly used in SCADA systems for communications between a human-machine interface (HMI) and programmable logic controllers. This page enables you to enable and disable Modbus TCP support of the switch.



| Label | Description |
|---|---|
| **Mode** | Shows the existing status of the Modbus TCP function |

### 5.1.13 Backup/Restore Configurations

You can save/view or load switch configurations. The configuration file is in XML format.

### 5.1.14 Firmware Update

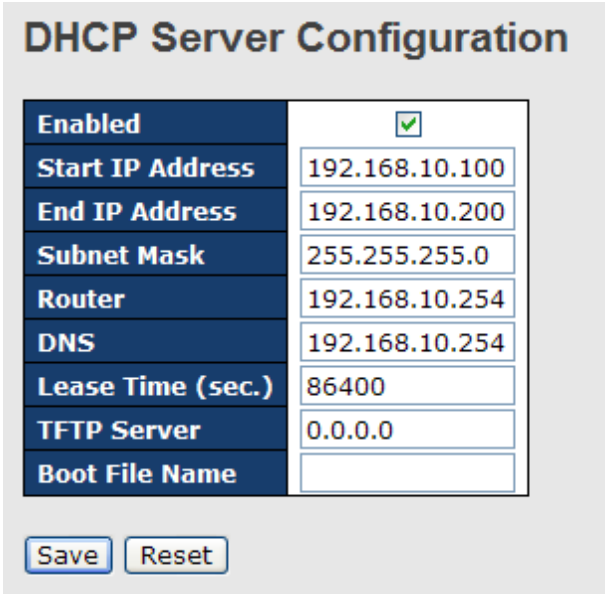
This page allows you to update the firmware of the switch.

## 5.2 DHCP Server

The switch provides DHCP server functions. By enabling DHCP, the switch will become a DHCP server and dynamically assigns IP addresses and related IP information to network clients.

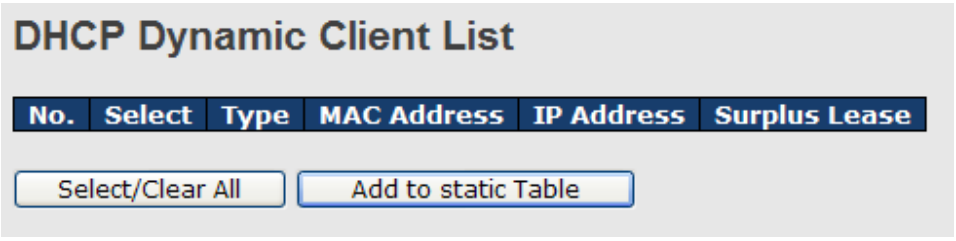
### 5.2.1 Settings

This page allows you to set up DHCP settings for the switch. You can check the **Enabled** checkbox to activate the function. Once the box is checked, you will be able to input information in each column.



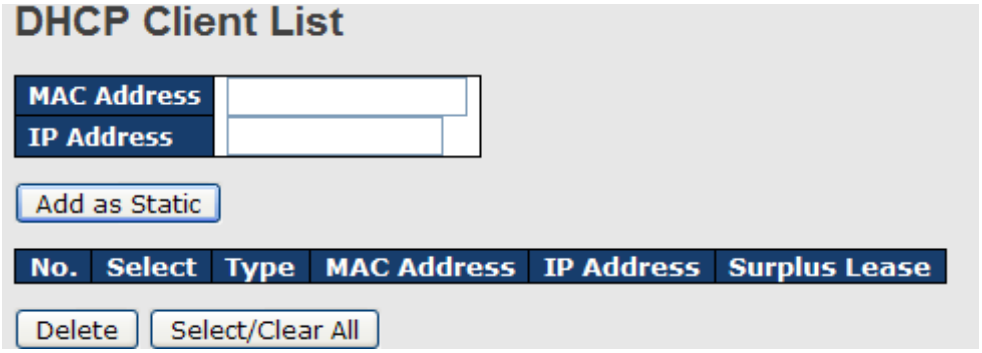

## 5.2.2 Dynamic Client List

When DHCP server functions are activated, the switch will collect DHCP client information and display in the following table.




## 5.2.3 Client List

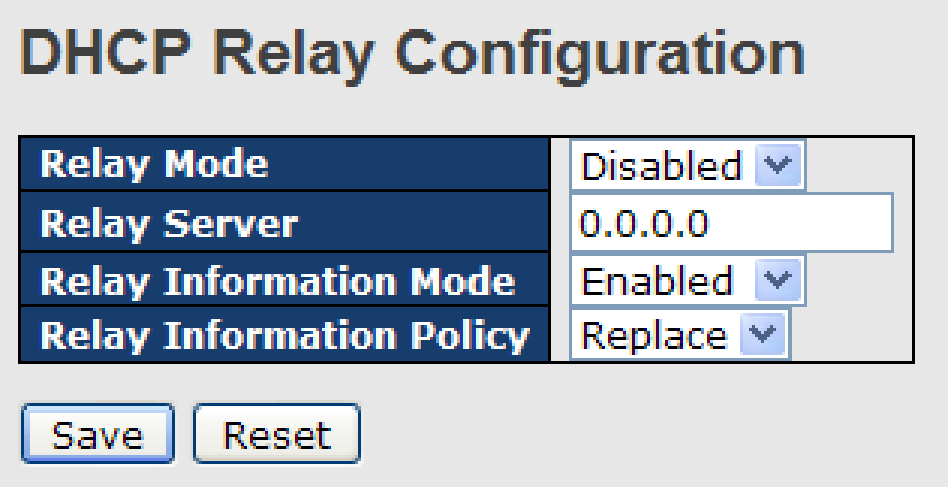
You can assign a specific IP address within the dynamic IP range to a specific port. When a device is connected to the port and requests for dynamic IP assigning, the switch will assign the IP address that has previously been assigned to the connected device.



## 5.2.4 Relay Agent

### 5.2.4.1 Settings

DHCP relay is used to forward and transfer DHCP messages between the clients and the server when they are not in the same subnet domain. You can configure the function in this page.

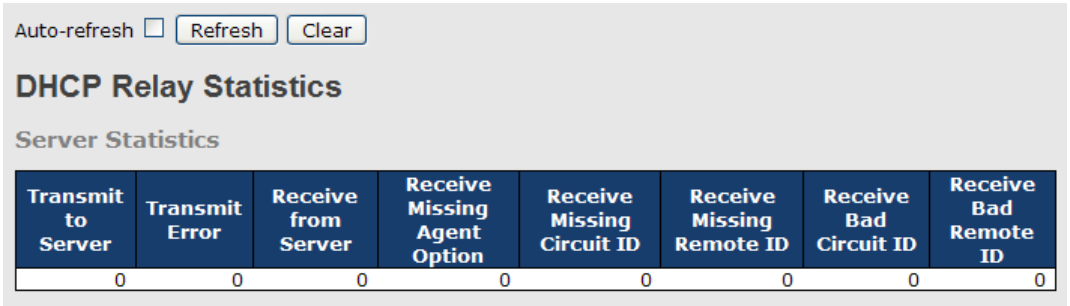



| Label | Description |
|---|---|
| **Relay Mode** | Indicates the existing DHCP relay mode. The modes include:<br>**Enabled**: activate DHCP relay. When DHCP relay is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain to prevent the DHCP broadcast message from flooding for security considerations.<br>**Disabled**: disable DHCP relay. |
| **Relay Server** | Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and transfer DHCP messages between the clients and the server when they are not in the same subnet domain. |
| **Relay Information Mode** | Indicates the existing DHCP relay information mode. The format of DHCP option 82 circuit ID format is "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, and the fifth and sixth characters are the module ID. In stand-alone devices, the module ID |

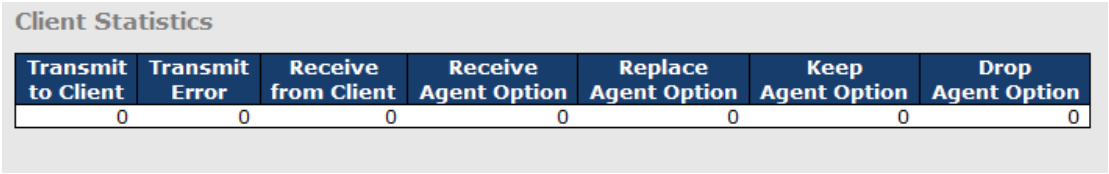
| | |
|---|---|
| | always equals to 0; in stacked devices, it means switch ID. The last two characters are the port number. For example, "00030108" means the DHCP message received form VLAN ID 3, switch ID 1, and port No. 8. The option 82 remote ID value equals to the switch MAC address.<br>The modes include:<br>Enabled: activate DHCP relay information. When DHCP relay information is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to a DHCP server and removes it from a DHCP message when transferring to a DHCP client. It only works when DHCP relay mode is enabled.<br>Disabled: disable DHCP relay information. |
| **Relay Information Policy** | Indicates the policies to be enforced when receiving DHCP relay information. When DHCP relay information mode is enabled, if the agent receives a DHCP message that already contains relay agent information, it will enforce the policy. The Replace option is invalid when relay information mode is disabled. The policies includes:<br>Replace: replace the original relay information when a DHCP message containing the information is received.<br>Keep: keep the original relay information when a DHCP message containing the information is received.<br>Drop: drop the package when a DHCP message containing the information is received. |

## 5.2.4.2 Statistics

The relay statistics shows the information of relayed packet of the switch.



| Label | Description |
|---|---|
| **Transmit to Sever** | The number of packets relayed from the client to the server. |
| **Transmit Error** | The number of packets with errors when being sent to clients. |
| **Receive from Server** | The number of packets received from the server. |
| **Receive Missing Agent Option** | The number of packets received without agent information. |
| **Receive Missing Circuit ID** | The number of packets received with Circuit ID. |
| **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 do not match the known circuit ID. |
| **Receive Bad Remote ID** | The number of packets whose Remote ID do not match the known Remote ID. |



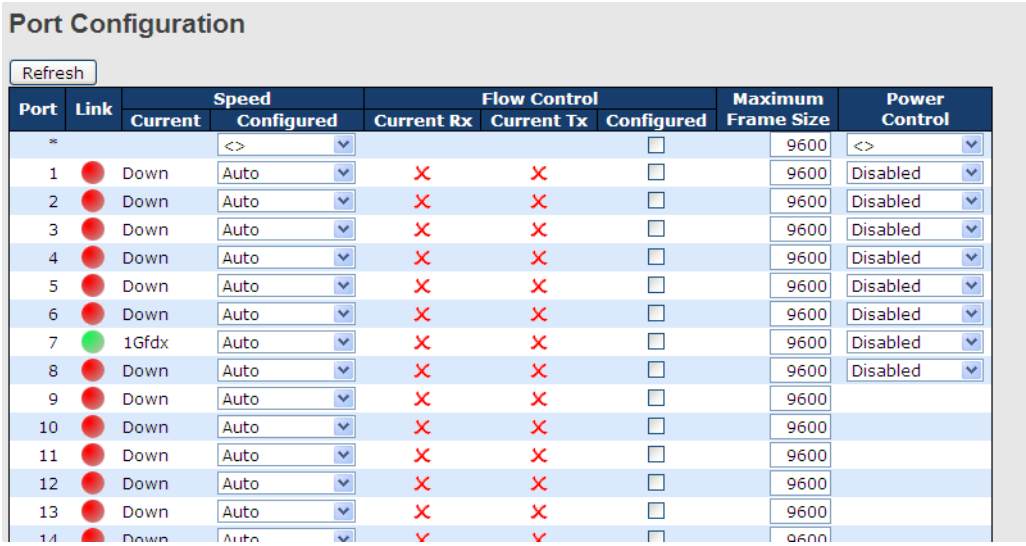

| Label | Description |
|---|---|
| **Transmit to Client** | The number of packets relayed from the server to the client. |
| **Transmit Error** | The number of packets with errors when being sent to servers. |
| **Receive from Client** | The number of packets received from the server. |
| **Receive Agent Option** | The number of received packets containing relay agent information. |
| **Replace Agent Option** | The number of packets replaced when received messages contain relay agent information. |
| **Keep Agent Option** | The number of packets whose relay agent information is retained. |
| **Drop Agent Option** | The number of packets dropped when received messages contain relay agent information. |

# 5.3 Port Setting

Port Setting allows you to manage individual ports of the switch, including traffic, power, and trunks.

## 5.3.1 Port Control

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

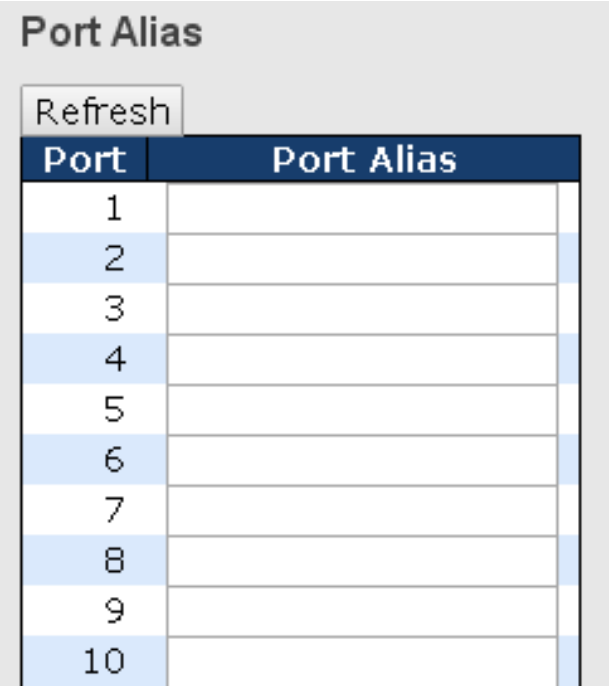



| Label | Description |
|---|---|
| **Port** | The switch port number to which the following settings will be applied. |
| **Link** | The current link state is shown by different colors. Green indicates the link is up and red means the link is down. |
| **Current Link Speed** | Indicates the current link speed of the port. |
| **Configured Link Speed** | The drop-down list provides available link speed options for a given switch port.<br>**Auto** selects the highest speed supported by the link partner.<br>**Disabled** disables switch port configuration.<br>**<>** configures all ports. |
| **Flow Control** | When **Auto** is selected for the speed, the flow control will be negotiated to the capacity advertised by the link partner. When a fixed-speed setting is selected, that is what is used. **Current Rx** indicates whether pause frames on the port are obeyed, and **Current Tx** indicates whether pause |

| | |
|---|---|
| | frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last auto-negotiation. You can check the Configured column to use flow control. This setting is related to the setting of **Configured Link Speed**. |
| **Maximum Frame** | You can enter the maximum frame size allowed for the switch port in this column, including FCS. The allowed range is 1518 bytes to 9600 bytes. |
| **Power Control** | Shows the current power consumption of each port in percentage. The **Configured** column allows you to change power saving parameters for each port.<br>**Disabled**: all power savings functions are disabled.<br>**ActiPHY**: link down and power savings enabled.<br>**PerfectReach**: link up and power savings enabled.<br>**Enabled**: both link up and link down power savings enabled. |
| **Total Power Usage** | Total power consumption of the board, measured in percentage. |
| **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. |

## 5.3.2 Port Alias

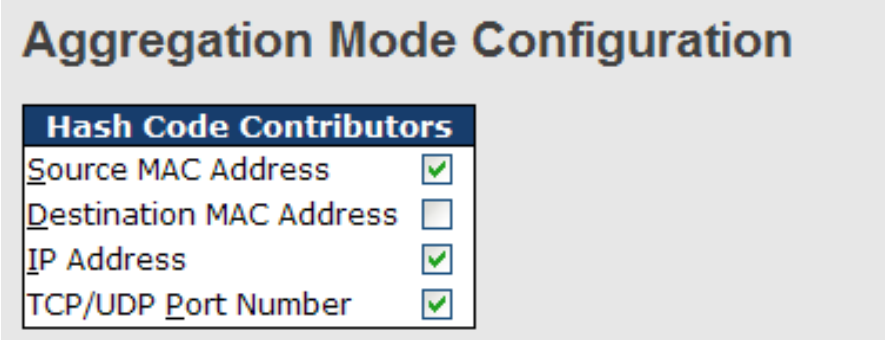
You can assign a port alias name for each port to enable easy identification of the devices connected to the port.




## 5.3.3 Port Trunk

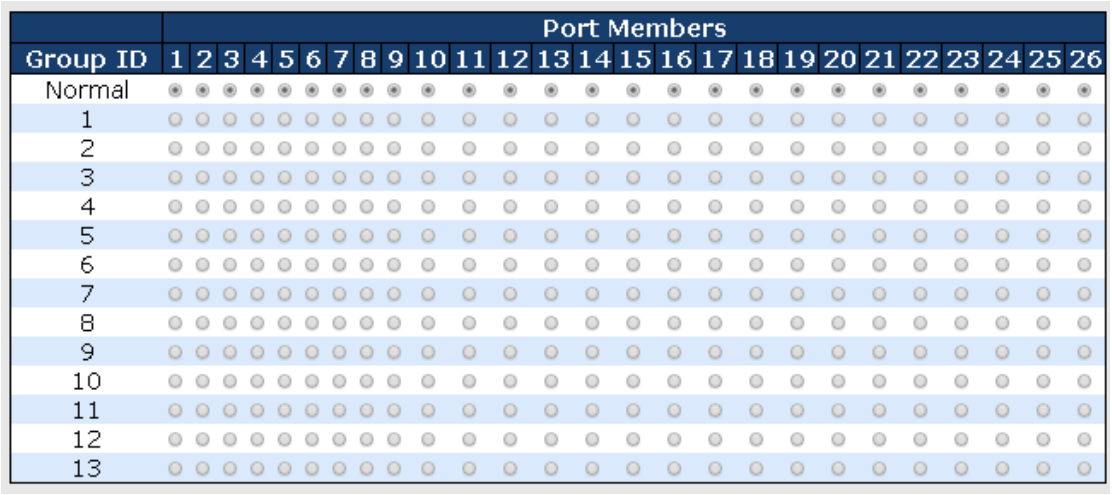
### 5.3.3.1 Configuration

This page allows you to configure the aggregation hash mode and the aggregation group.




| Label | Description |
|---|---|
| **Source MAC Address** | Calculates the destination port of the frame. You can check this box to enable the source MAC address, or uncheck to disable. By default, **Source MAC Address** is enabled. |
| **Destination MAC Address** | Calculates the destination port of the frame. You can check this box to enable the destination MAC address, or uncheck to disable. By default, **Destination MAC Address** is disabled. |

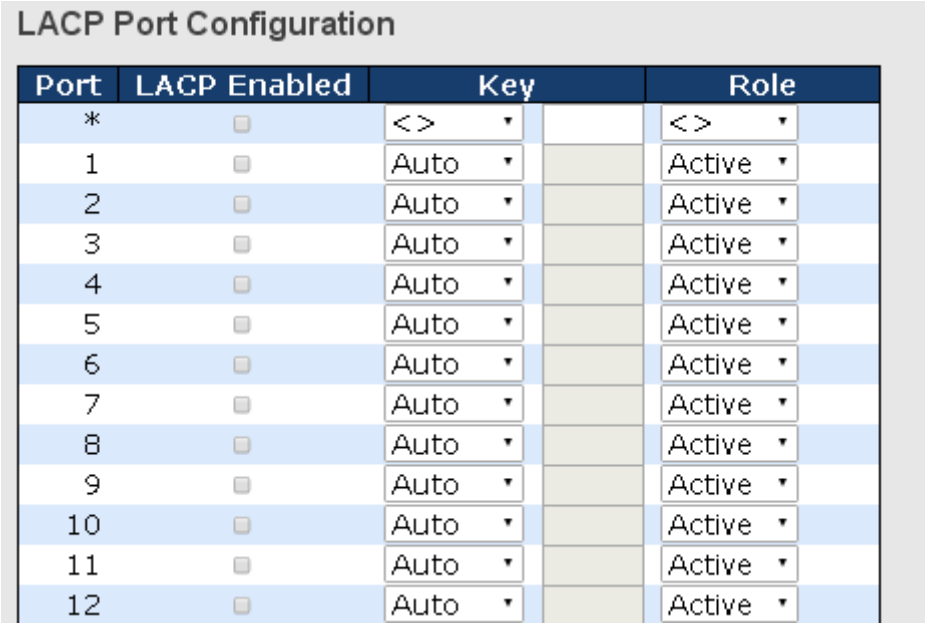
| | |
|---|---|
| **IP Address** | Calculates the destination port of the frame. You can check this box to enable the IP address, or uncheck to disable. By default, **IP Address** is enabled. |
| **TCP/UDP Port Number** | Calculates the destination port of the frame. You can check this box to enable the TCP/UDP port number, or uncheck to disable. By default, **TCP/UDP Port Number** is enabled. |




| Label | Description |
|---|---|
| **Group ID** | Indicates the ID of each aggregation group. **Normal** means no aggregation. Only one group ID is valid per port. |
| **Port Members** | Lists each switch port 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 the ports must be in the same speed in each group. |

### 5.3.3.2 LACP Port

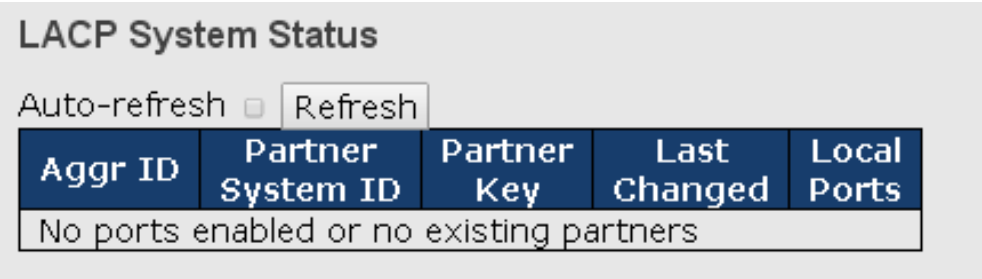
This page allows you to enable LACP functions to group ports together to form single virtual links, thereby increasing the bandwidth between the switch and other LACP-compatible devices. LACP trunks are similar to static port trunks, but they are more flexible because LACP is compliant with the IEEE 802.3ad standard. Hence, it is interoperable with equipment from other vendors that also comply with the standard. You can change LACP port settings in this page.




| Label | Description |
|---|---|
| **Port** | Indicates the ID of each aggregation group. **Normal** indicates there is no aggregation. Only one group ID is valid per port. |
| **LACP Enabled** | Lists each switch port for each group ID. Check to include a port in an aggregation, or clear the box 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 the ports must be in the same speed in each group. |
| **Key** | The **Key** value varies with the port, ranging from 1 to 65535. **Auto** will set the key according to the physical link speed (10Mb = 1, 100Mb = 2, 1Gb = 3). **Specific** allows you to enter a user-defined value. Ports with the same key value can join in the same aggregation group, while ports with different keys cannot. |
| **Role** | Indicates LACP activity status. **Active** will transmit LACP packets every second, while **Passive** will wait for a LACP packet from a partner (speak if spoken to). |
| **Save** | Click to save changes |
| **Reset** | Click to undo any changes made locally and revert to previously saved values |

### 5.3.3.3 System Status

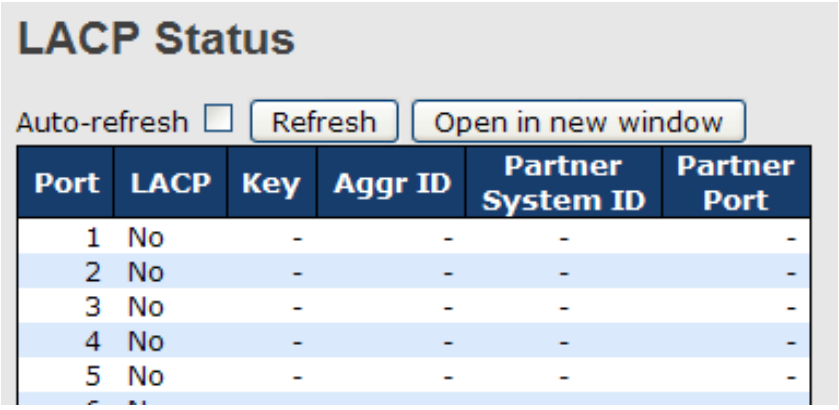
This page provides a status overview for all LACP instances.




| Label | Description |
|---|---|
| **Aggr ID** | The aggregation ID is associated with the aggregation instance. For LLAG, the ID is shown as '**isid:aggr-id**' and for GLAGs as '**aggr-id**'. |
| **Partner System ID** | System ID (MAC address) of the aggregation partner. |
| **Partner Key** | The key assigned by the partner to the aggregation ID. |
| **Last Changed** | The time since this aggregation changed. |
| **Last Channged** | Indicates which ports belong to the aggregation of the switch/stack. The format is: "**Switch ID:Port**". |
| **Refresh** | Click to refresh the page immediately. |

### 5.3.3.4 Port Status

This page provides an overview of the LACP status for all ports.

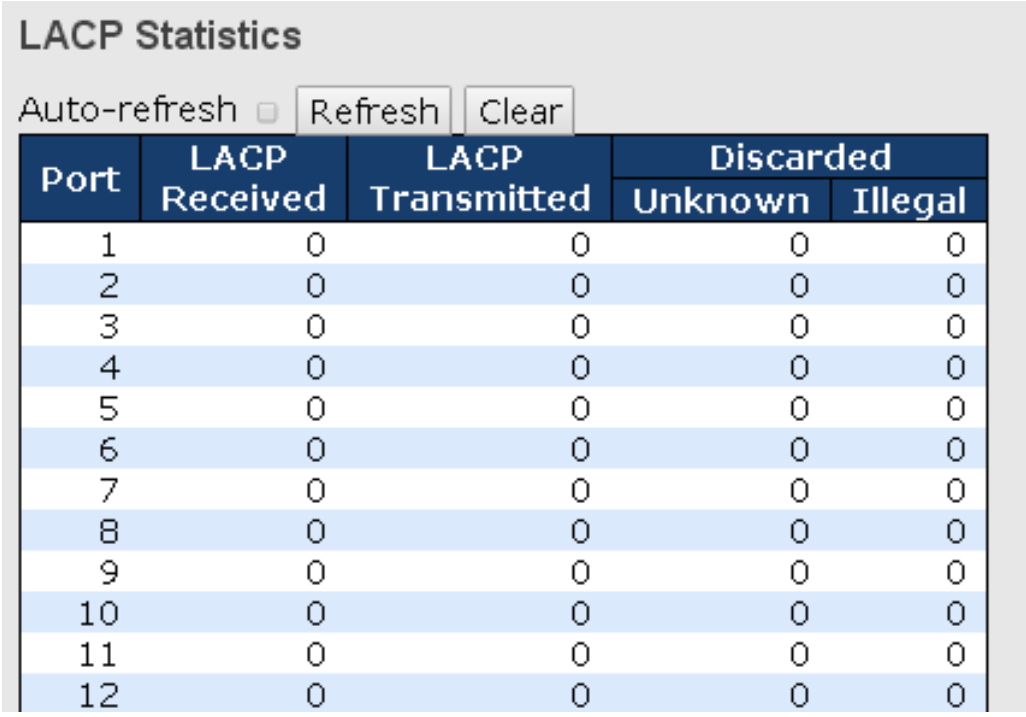



| Label | Description |
|---|---|
| **Port** | Switch port number |
| **LACP** | **Yes** means LACP is enabled and the port link is up. **No** means LACP is not enabled or the port link is down. |

| | |
|---|---|
| | **Backup** means the port cannot join in the aggregation group unless other ports are removed. The LACP status is disabled. |
| **Key** | The key assigned to the port. Only ports with the same key can be aggregated |
| **Aggr ID** | The aggregation ID assigned to the aggregation group |
| **Partner System ID** | The partner's system ID (MAC address) |
| **Partner Port** | The partner's port number associated with the port |
| **Refresh** | Click to refresh the page immediately |

### 5.3.3.5 LACP Statistics

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

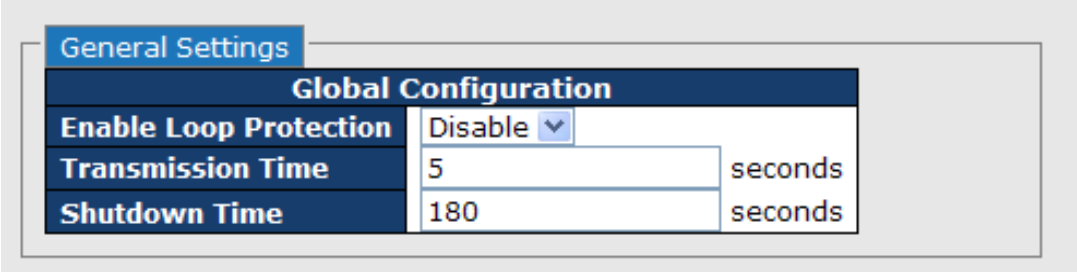



| Label | Description |
|---|---|
| **Port** | Switch port number. |
| **LACP Transmitted** | The number of LACP frames sent from each port. |
| **LACP Received** | The number of LACP frames received at each port. |
| **Discarded** | The number of unknown or illegal LACP frames discarded at each port. |
| **Refresh** | Click to refresh the page immediately. |
| **Clear** | Click to clear the counters for all ports |

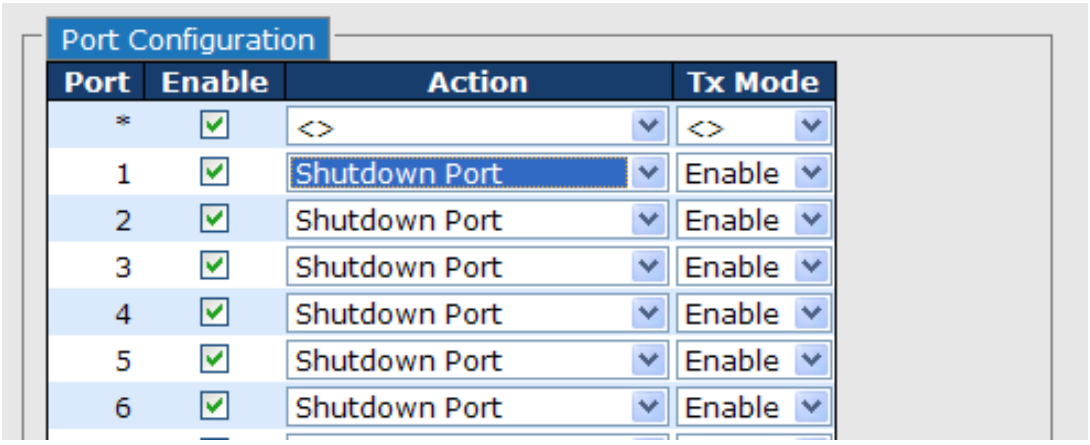
## 5.3.4 Loop Protection

### 5.3.4.1 Configuration

This feature prevents loop attack. When receiving loop packets, the port will be disabled automatically, preventing the loop attack from affecting other network devices.



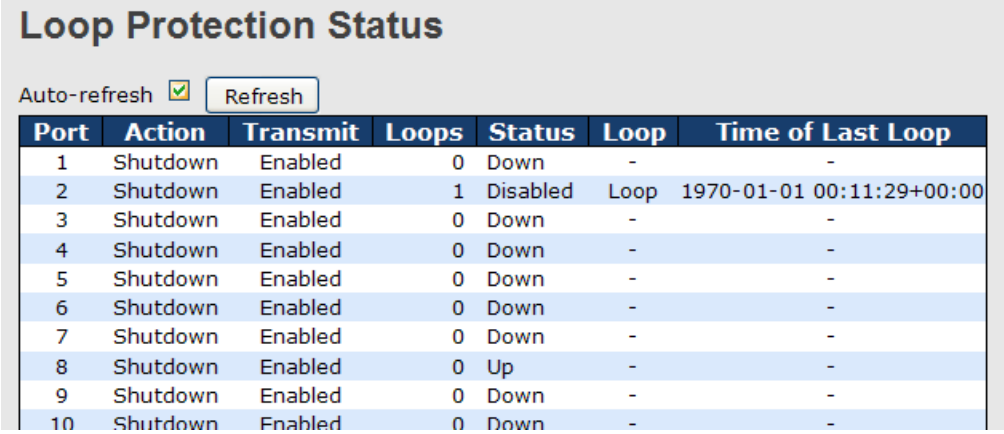

| Label | Description |
|---|---|
| **Enable Loop Protection** | Activate loop protection functions (as a whole) |
| **Transmission Time** | The interval between each loop protection PDU sent on each port. The valid value is 1 to 10 seconds. |
| **Shutdown Time** | The period (in seconds) for which a port will be kept disabled when a loop is detected (shutting down the port). The valid value is 0 to 604800 seconds (7 days). A value of zero will keep a port disabled permanently (until the device is restarted). |




| Label | Description |
|---|---|
| **Port** | Switch port number. |
| **Enable** | Activate loop protection functions (as a whole). |
| **Action** | Configures the action to take when a loop is detected. Valid |

| | |
|---|---|
| | values include **Shutdown Port**, **Shutdown Port**, and **Log or Log Only**. |
| **Tx Mode** | Controls whether the port is actively generating loop protection PDUs or only passively look for looped PDUs. |

### 5.3.4.1 Status

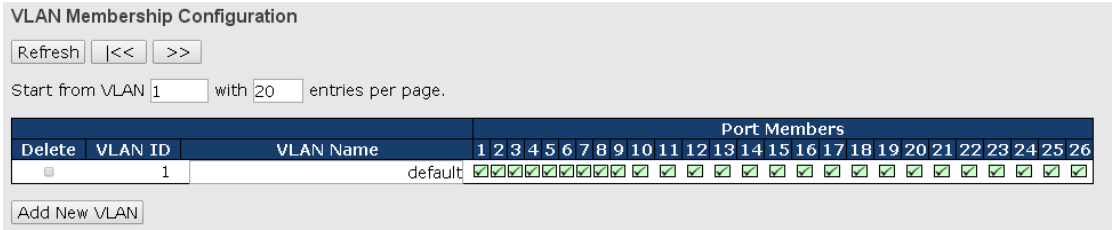



| Label | Description |
|---|---|
| **Port** | The switch port number of the logical port. |
| **Action** | The currently configured port action. |
| **Transmit** | The currently configured port transmit mode. |
| **Loops** | The number of loops detected on this port. |
| **Status** | The current loop 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. |

# 5.4 VLAN

## 5.4.1 VLAN Membership

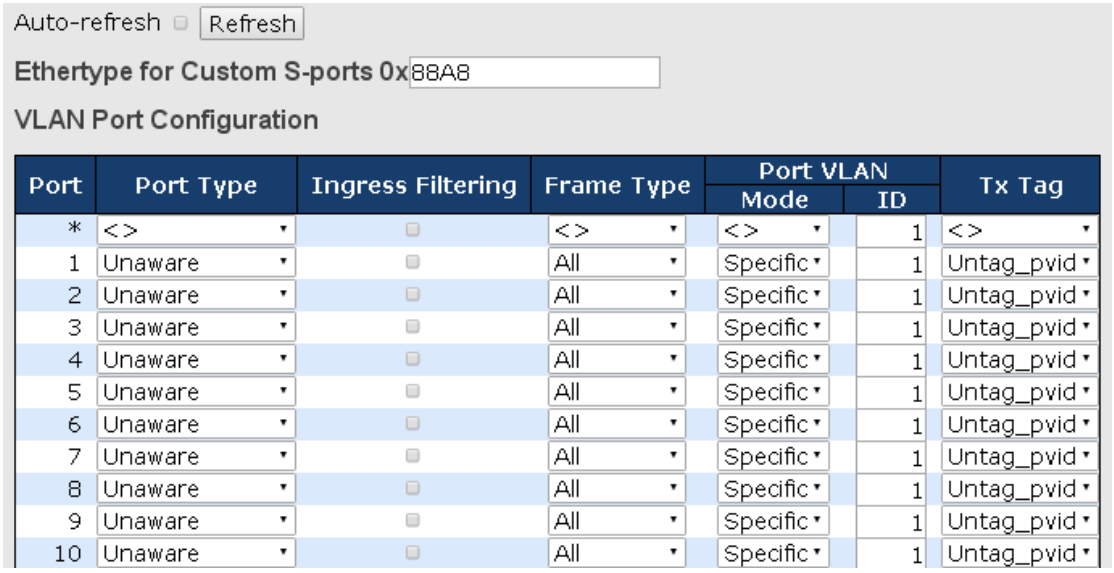
You can view and change VLAN membership configurations for a selected switch stack in this page. Up to 64 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.



| Label | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **VLAN ID** | The VLAN ID for the entry. |
| **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 New VLAN** | Click to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Valid values for a VLAN ID are 1 through 4095.<br>After clicking **Save**, the new VLAN will be enabled on the selected switch stack but contains no port members.<br>A VLAN without any port members on any stack will be deleted when you click **Save**.<br>Click **Delete** to undo the addition of new VLANs. |

## 5.4.2 Ports

This page allows you to set up VLAN ports individually.




| 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 custom S-ports. |
| **Port** | The switch port number to which the following settings will be |

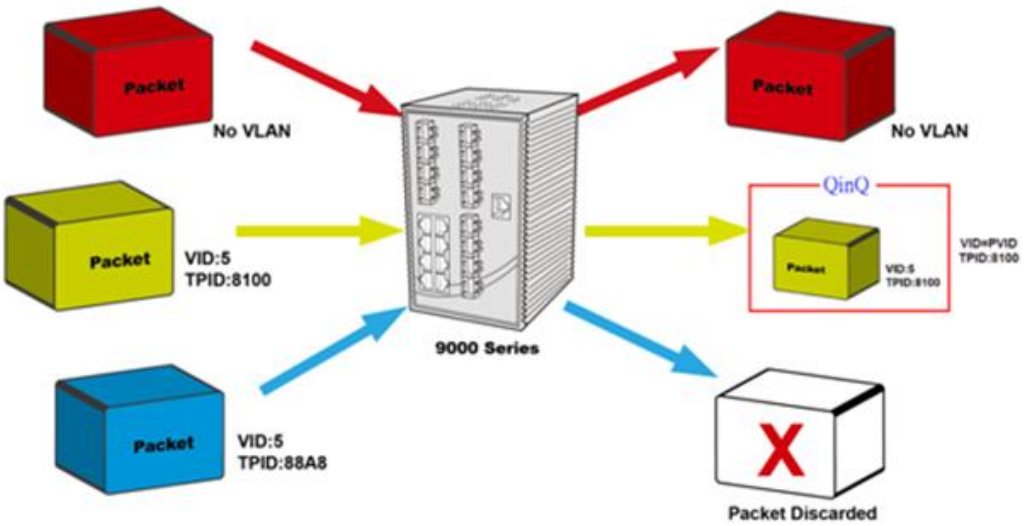
| | |
|---|---|
| | applied. |
| **Port type** | Port can be one of the following types: **Unaware**, **Customer** (**C-port**), **Service** (**S-port**), **Custom Service** (**S-custom-port**). If port type is **Unaware**, all frames are classified to the port VLAN ID and tags are not removed. |
| **Ingress 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 will be 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 will be discarded. By default, the field is set to **All**. |
| **Port VLAN Mode** | The allowed values are **None** or **Specific**. This parameter affects VLAN ingress and egress processing.<br>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.<br>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 will be inserted in the frame. |
| **Port VLAN ID** | Configures the VLAN identifier for the port. The allowed range of the values is 1 through 4095. The default value is 1. 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. |

## Introduction of Port Types

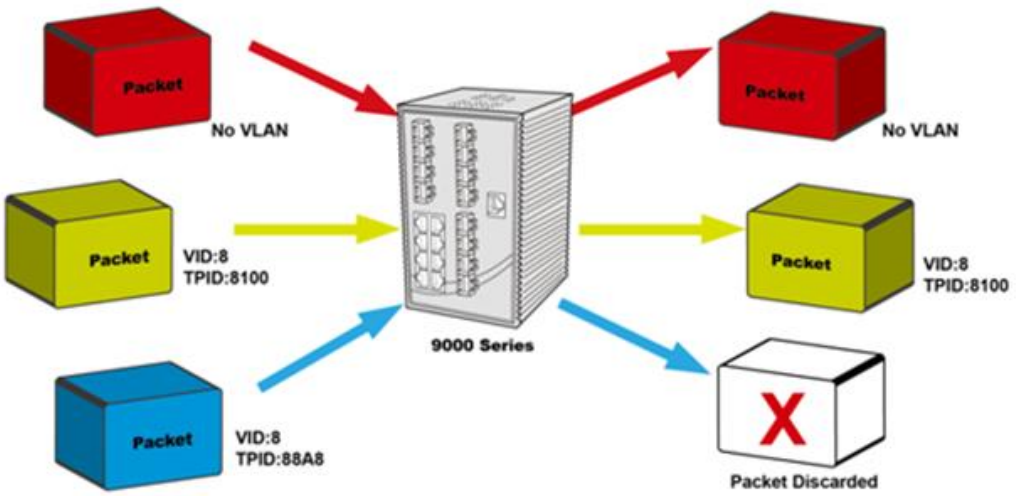
Below is a detailed description of each port type, including Unaware, C-port, S-port, and

S-custom-port.

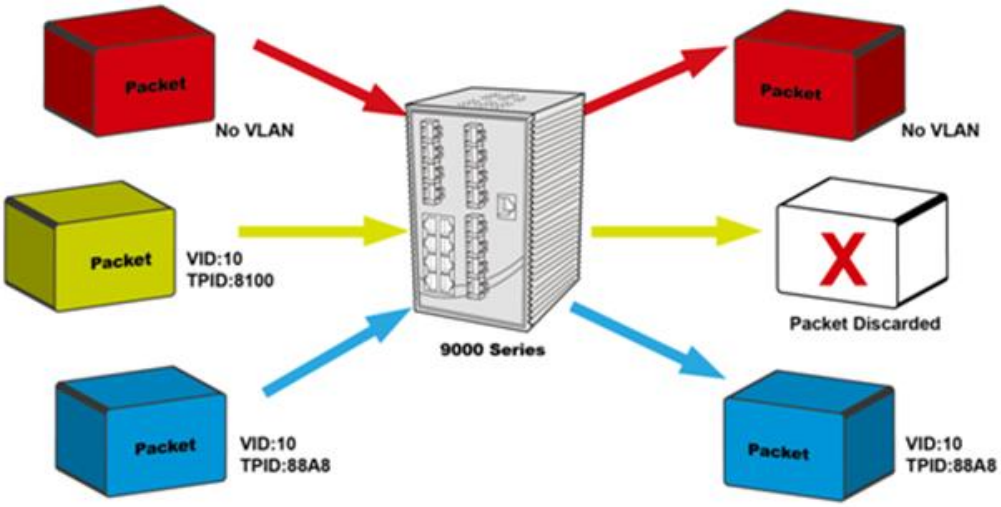
| | Ingress action | Egress action |
|---|---|---|
| **Unaware**<br><br>**The function of Unaware can be used for 802.1QinQ (double tag).** | When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded.<br>When the port receives tagged frames:<br>1. If the tagged frame contains a TPID of 0x8100, it will become a double-tag frame and will be forwarded.<br>2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded. | The TPID of a frame transmitted by Unaware port will be set to 0x8100.<br>The final status of the frame after egressing will also be affected by the Egress Rule. |
| **C-port** | When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded.<br>When the port receives tagged frames:<br>1. If the tagged frame contains a TPID of 0x8100, it will be forwarded.<br>2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded. | The TPID of a frame transmitted by C-port will be set to 0x8100. |
| **S-port** | When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded.<br>When the port receives tagged frames:<br>1. If the tagged frame contains a TPID of 0x8100, it will be forwarded.<br>2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8100), it will be discarded. | The TPID of a frame transmitted by S-port will be set to 0x88A8. |
| **S-custom-port** | When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded.<br>When the port receives tagged frames:<br>1. If the tagged frame contains a TPID of 0x8100, it will be forwarded.<br>2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8100), it will be discarded. | The TPID of a frame transmitted by S-custom-port will be set to a self-customized value, which can be set by the user via **Ethertype for Custom S-ports.** |



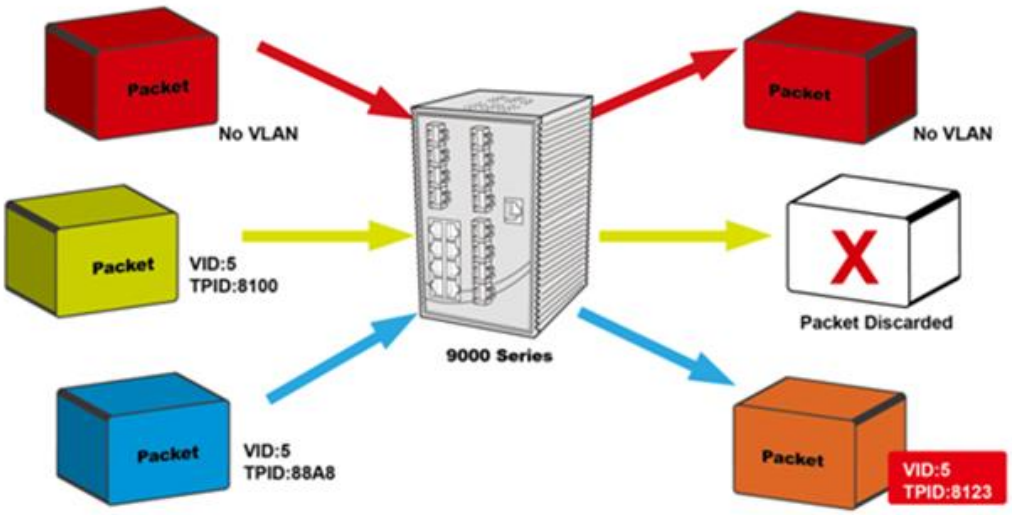

Unaware




C-port




S-port

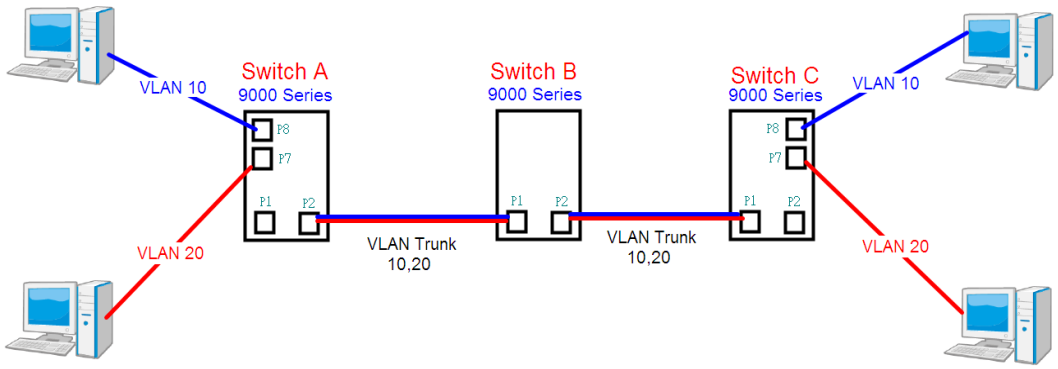



S-custom-port

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

# Examples of VLAN Settings

## VLAN Access Mode:

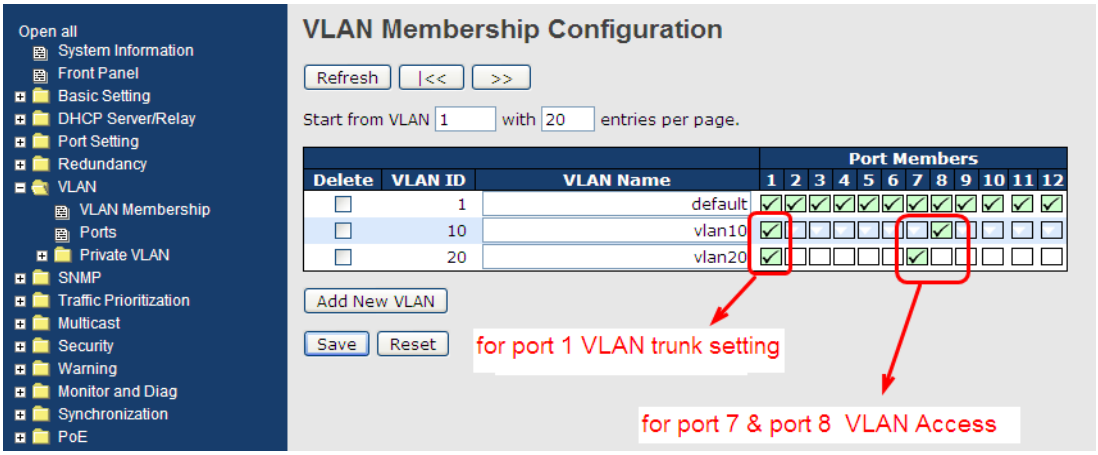


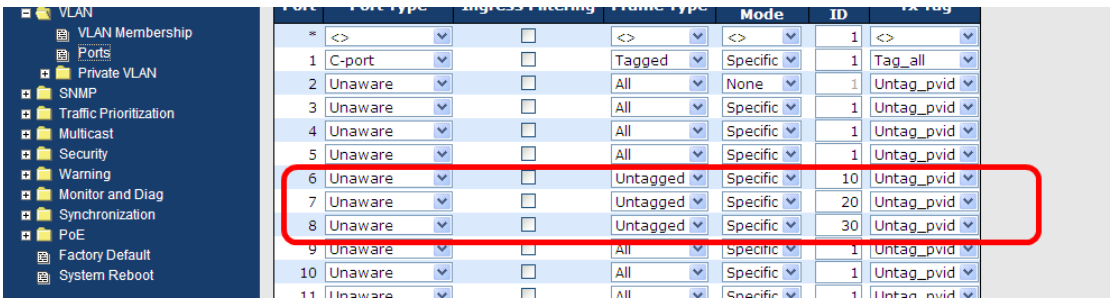

**Switch A**,

Port 7 is VLAN Access mode = Untagged 20

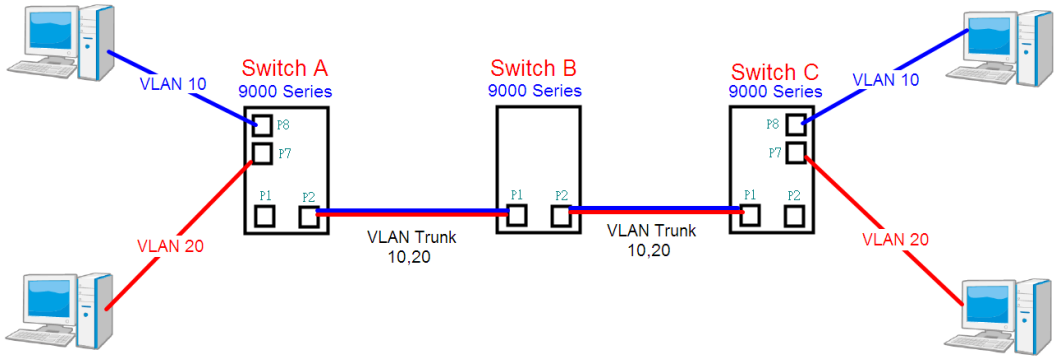
Port 8 is VLAN Access mode = Untagged 10

Below are the switch settings.



## VLAN 1Q Trunk Mode:

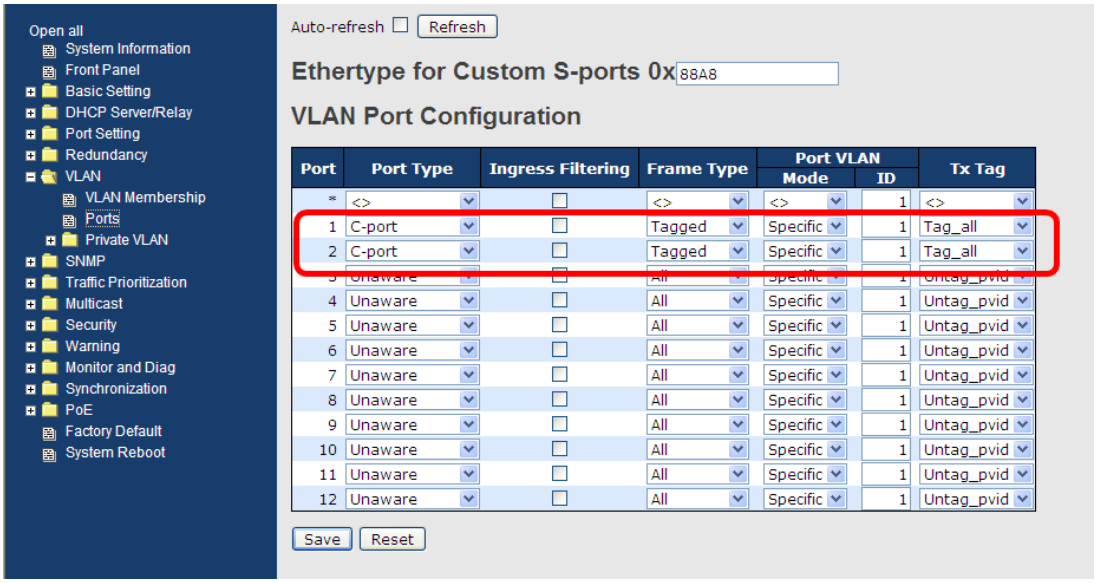



**Switch B**,

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

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

Below are the switch settings.

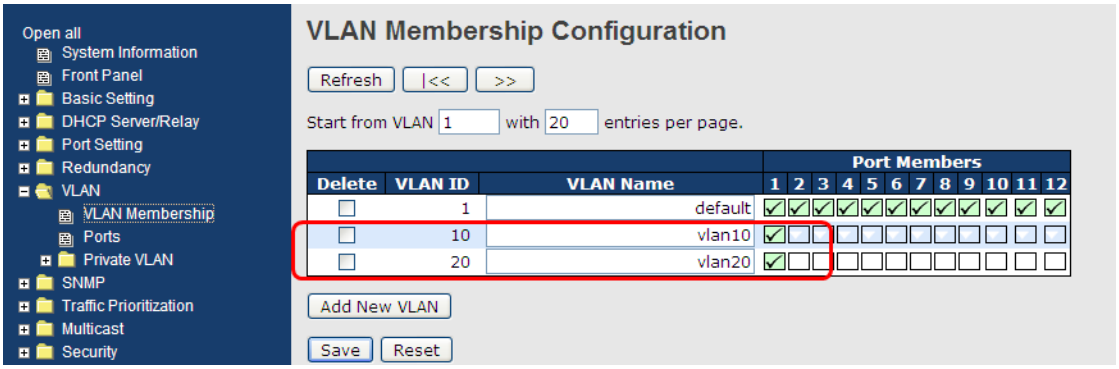


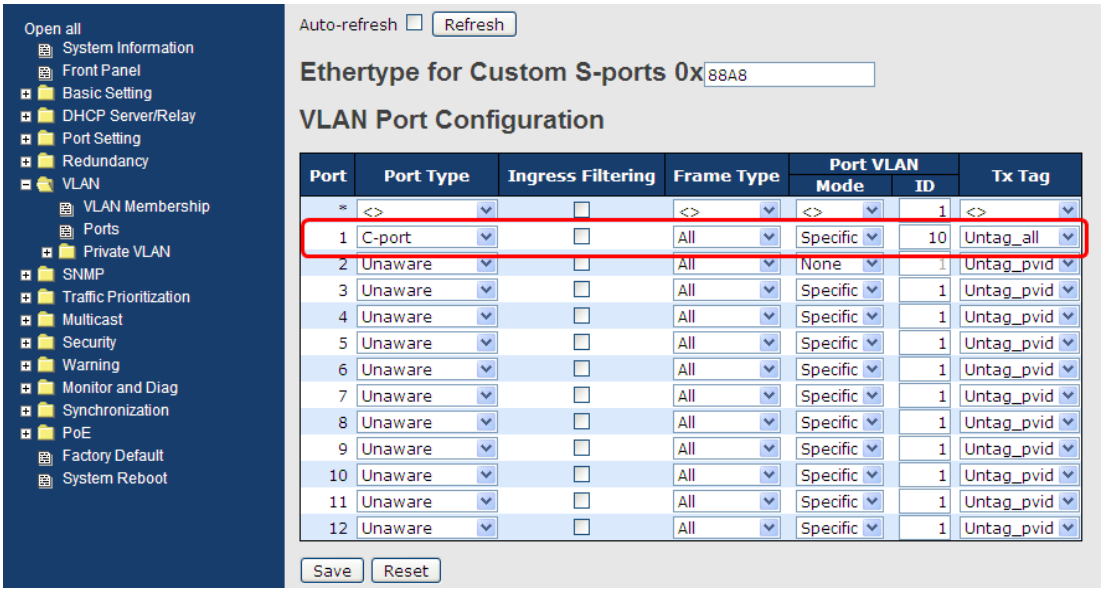
**VLAN Hybrid Mode:**

Port 1 VLAN Hybrid mode = untagged 10

Tagged 10, 20

Below are the switch settings.

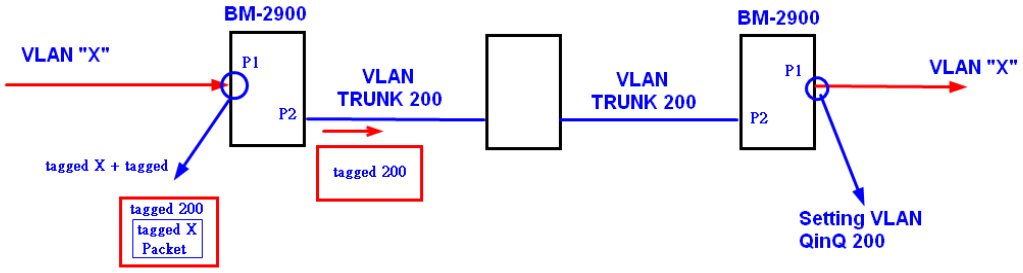


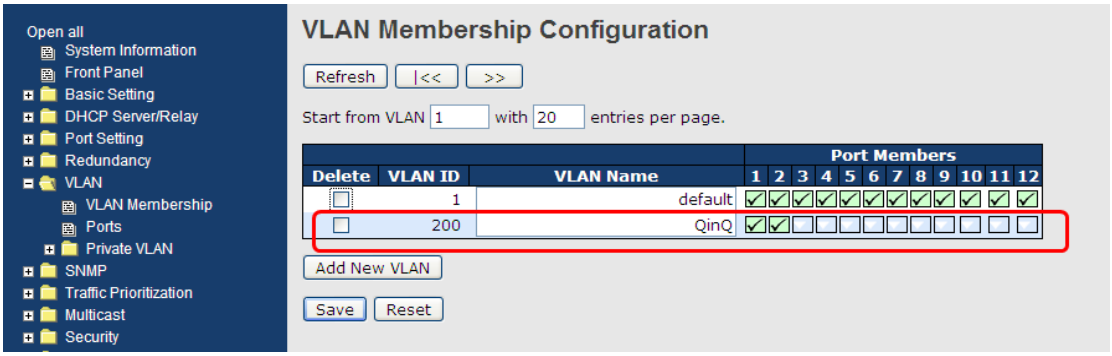

**VLAN QinQ Mode:**

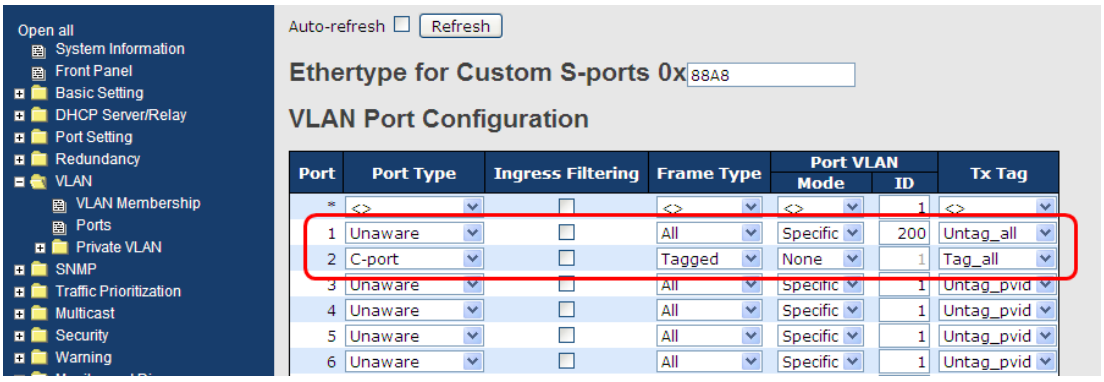
VLAN QinQ mode is usually adopted when there are unknown VLANs, as shown in the figure below.

VLAN “X” = Unknown VLAN




## 9000 Series Port 1 VLAN Settings:

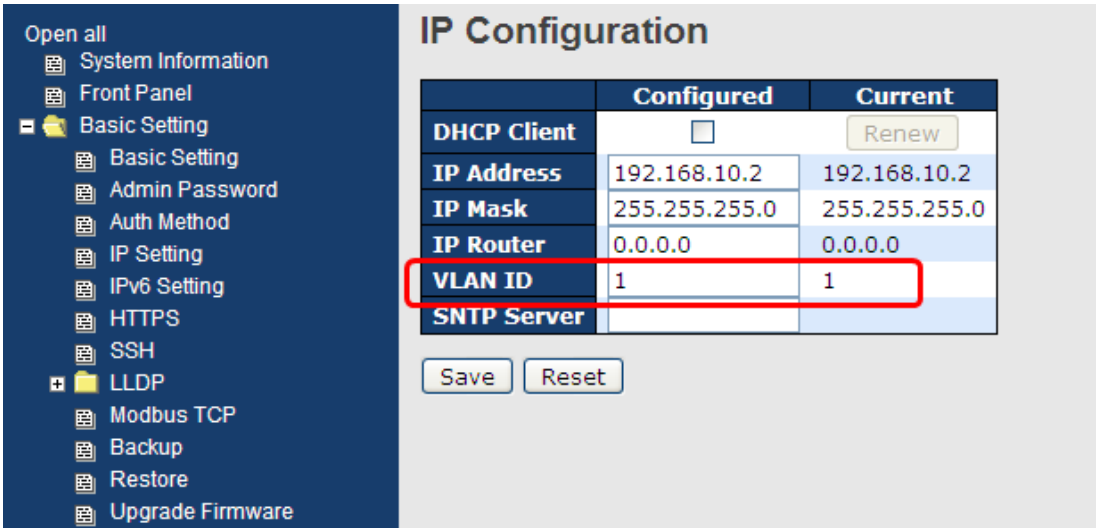



## VLAN ID Settings

When setting the management VLAN, only the same VLAN ID port can be used to control the switch.

## series VLAN Settings:

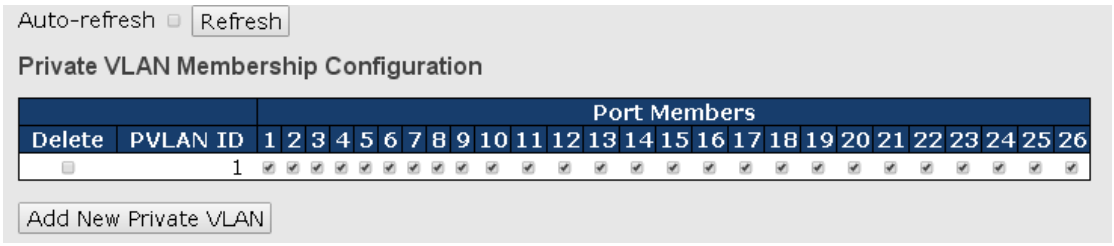



## 5.4.3 Private VLAN

### 5.4.3.1 PVLAN Membership

The private VLAN membership configuration 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.

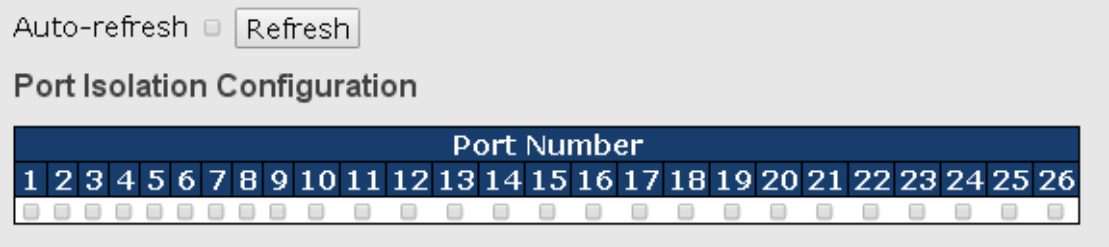
A port must be a member of both a VLAN and a private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and private VLAN 1. A VLAN-unaware port can only be a member of one VLAN, but it can be a member of multiple private VLANs.




| Label | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **PVLAN 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. You can check the box to include a port in a private VLAN. 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 New Private VLAN** | Click the button 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.<br>The private VLAN is enabled when you click Save.<br>The **Delete** button can be used to undo the addition of new private VLANs. |

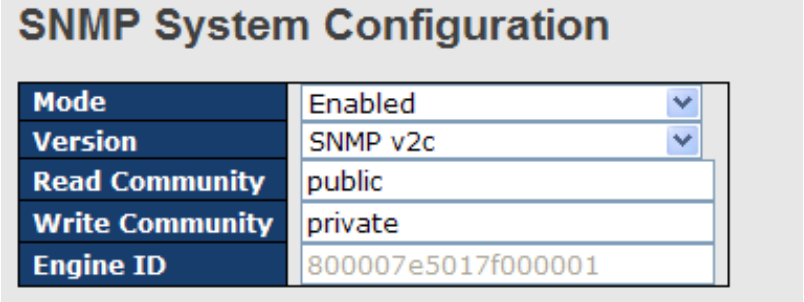
### 5.4.3.2 Port Isolation



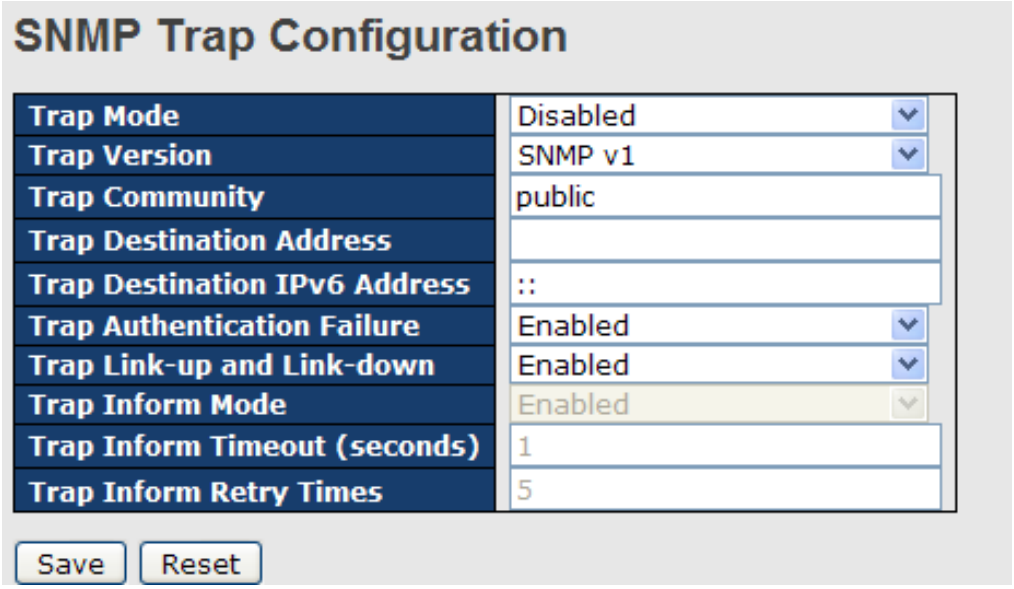

| Label | Description |
|---|---|
| **Port Member** | A check box is provided for each port of a private VLAN.<br>When checked, port isolation is enabled for that port.<br>When unchecked, port isolation is disabled for that port.<br>By default, port isolation is disabled for all ports. |

# 5.5 SNMP

## 5.5.1 System



| Label | Description |
|---|---|
| **Mode** | Indicates existing SNMP mode. Possible modes include:<br>**Enabled**: enable SNMP mode<br>**Disabled**: disable SNMP mode |
| **Version** | Indicates the supported SNMP version. Possible versions include:<br>**SNMP v1**: supports SNMP version 1.<br>**SNMP v2c**: supports SNMP version 2c.<br>**SNMP v3**: supports SNMP version 3. |
| **Read Community** | Indicates the read community string to permit access to SNMP agent. The allowed string length is 0 to 255, and only ASCII characters from 33 to 126 are allowed.<br>The field only suits to SNMPv1 and SNMPv2c. SNMPv3 uses USM for authentication and privacy and the community string will be associated with SNMPv3 community table. |
| **Write Community** | Indicates the write community string to permit access to SNMP agent. The allowed string length is 0 to 255, and only ASCII characters from 33 to 126 are allowed.<br>The field only suits to SNMPv1 and SNMPv2c. SNMPv3 uses USM for authentication and privacy and the community string will be associated with SNMPv3 community 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. |

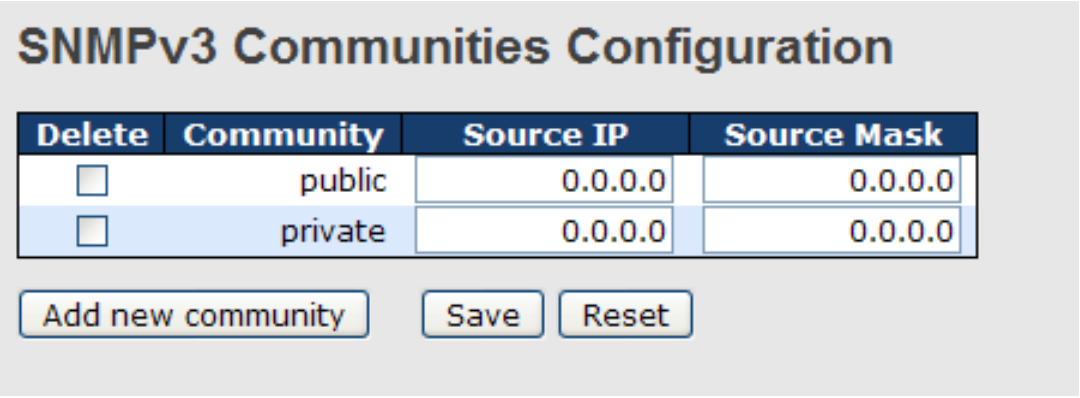



| Label | Description |
|---|---|
| **Trap Mode** | Indicates existing SNMP trap mode. Possible modes include:<br>**Enabled**: enable SNMP trap mode<br>**Disabled**: disable SNMP trap mode |
| **Trap Version** | Indicates the supported SNMP trap version. Possible versions include:<br>**SNMP v1**: supports SNMP trap version 1<br>**SNMP v2c**: supports SNMP trap version 2c<br>**SNMP v3**: supports SNMP trap version 3 |
| **Trap Community** | Indicates the community access string when sending SNMP trap packets. The allowed string length is 0 to 255, and only ASCII characters from 33 to 126 are allowed. |
| **Trap Destination Address** | Indicates the SNMP trap destination address |
| **Trap Destination IPv6 Address** | Provides the trap destination IPv6 address of this switch. IPv6 address consists of 128 bits represented as eight groups of four hexadecimal digits with a colon separating each field (:). For example, in 'fe80::215:c5ff:fe03:4dc7', the symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also uses a following legally IPv4 address. For example, '::192.1.2.34'. |

| | |
|---|---|
| **Trap Authentication Failure** | Indicates the SNMP entity is permitted to generate authentication failure traps. Possible modes include:<br>**Enabled**: enable SNMP trap authentication failure.<br>**Disabled**: disable SNMP trap authentication failure. |
| **Trap Link-up and Link-down** | Indicates the SNMP trap link-up and link-down mode. Possible modes include:<br>**Enabled**: enable SNMP trap link-up and link-down mode.<br>**Disabled**: disable SNMP trap link-up and link-down mode. |
| **Trap Inform Mode** | Indicates the SNMP trap inform mode. Possible modes include:<br>**Enabled**: enable SNMP trap inform mode.<br>**Disabled**: disable SNMP trap inform mode. |
| **Trap Inform Timeout(seconds)** | Configures the SNMP trap inform timeout. The allowed range is 0 to 2147. |
| **Trap Inform Retry Times** | Configures the retry times for SNMP trap inform. The allowed range is 0 to 255. |

## 5.5.2 Communities

This page allows you to configure SNMPv3 community table. The entry index key is **Community**.

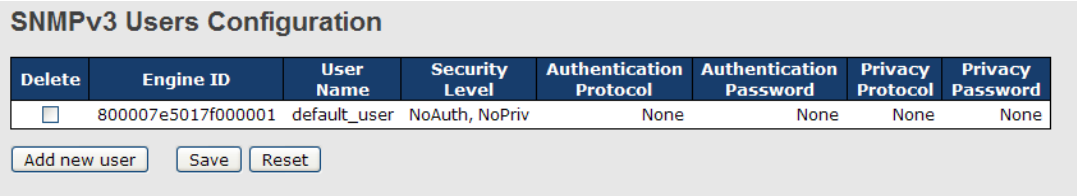



| Label | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Community** | Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed. |

| | |
|---|---|
| **Source IP** | Indicates the SNMP source address |
| **Source Mask** | Indicates the SNMP source address mask |

## 5.5.3 Users

This page allows you to configure SNMPv3 user table. The entry index keys are **Engine ID** and **User Name**.

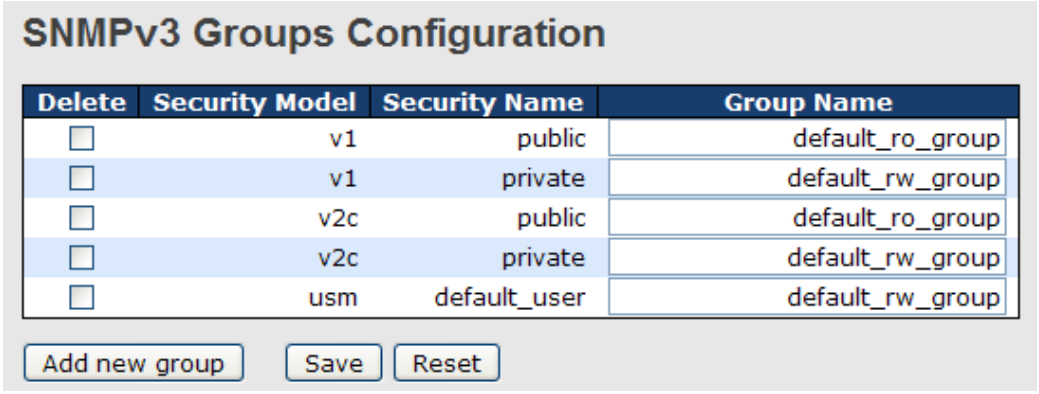



| Label | Description |
|---|---|
| **Delete** | Check to delete the entry. It will be deleted during the next save. |
| **Engine ID** | An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses User-based Security Model (USM) for message security and View-based Access Control Model (VACM) for access control. For the USM entry, the **usmUserEngineID** and **usmUserName** are the entry 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 is the same as system engine ID, then it is local user; otherwise it's remote user. |
| **User Name** | A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed. |
| **Security Level** | Indicates the security model that this entry should belong to. Possible security models include:<br>**NoAuth, NoPriv**: no authentication and no privacy<br>**Auth, NoPriv**: Authentication without privacy |

| | |
|---|---|
| | **Auth, Priv**: Authentication with privacy<br>The value of security level cannot be modified if the entry already exists, which means the value must be set correctly at the time of entry creation. |
| **Authentication Protocol** | Indicates the authentication protocol that this entry should belong to. Possible authentication protocols include:<br>**None**: no authentication protocol<br>**MD5**: an optional flag to indicate that this user is using MD5 authentication protocol<br>**SHA**: an optional flag to indicate that this user is using SHA authentication protocol<br>The value of security level cannot be modified if the entry already exists, which means the value must be set correctly at the time of entry creation. |
| **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. Only ASCII characters from 33 to 126 are allowed. |
| **Privacy Protocol** | Indicates the privacy protocol that this entry should belong to. Possible privacy protocols include:<br>**None**: no privacy protocol<br>**DES**: an optional flag to indicate that this user is using DES authentication protocol |
| **Privacy Password** | A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and only ASCII characters from 33 to 126 are allowed. |

### 5.5.4 Groups

This page allows you to configure SNMPv3 group table. 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 included:<br>**v1**: Reserved for SNMPv1.<br>**v2c**: Reserved for SNMPv2c.<br>**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 only ASCII characters from 33 to 126 are allowed. |
| **Group Name** | A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed. |

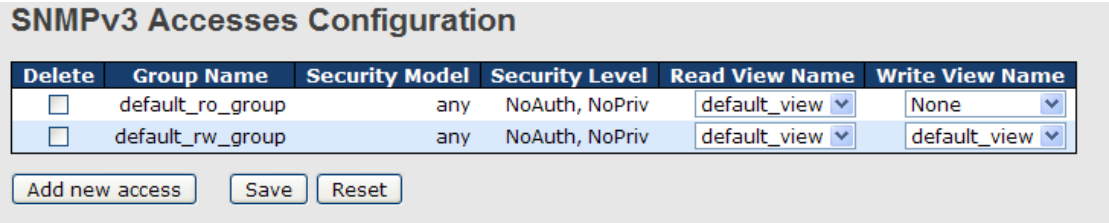
## 5.5.5 Views

This page allows you to configure SNMPv3 view table. 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 only ASCII characters from 33 to 126 are allowed. |
| **View Type** | Indicates the view type that this entry should belong to. Possible view types include:<br>**Included**: an optional flag to indicate that this view subtree should be included.<br>**Excluded**: An optional flag to indicate that this view subtree should be excluded.<br>Generally, if an entry's view type is **Excluded**, it should exist another entry whose view type is **Included, and** its OID subtree oversteps the **Excluded** 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 (*). |

## 5.5.6 Access

This page allows you to configure SNMPv3 access table. 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 only ASCII characters from 33 to 126 are allowed. |
| **Security Model** | Indicates the security model that this entry should belong |

| | |
|---|---|
| | to. Possible security models include:<br>**any**: Accepted any security model (v1\|v2c\|usm).<br>**v1**: Reserved for SNMPv1.<br>**v2c**: Reserved for SNMPv2c.<br>**usm**: User-based Security Model (USM). |
| **Security Level** | Indicates the security model that this entry should belong to. Possible security models include:<br>**NoAuth, NoPriv**: no authentication and no privacy<br>**Auth, NoPriv**: Authentication without privacy<br>**Auth, Priv**: Authentication with 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 only ASCII characters from 33 to 126 are allowed. |
| **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 only ASCII characters from 33 to 126 are allowed. |

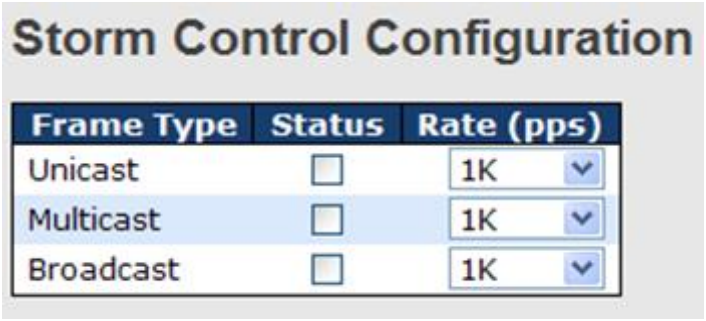
# 5.6 Traffic Prioritization

## 5.6.1Storm Control

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

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

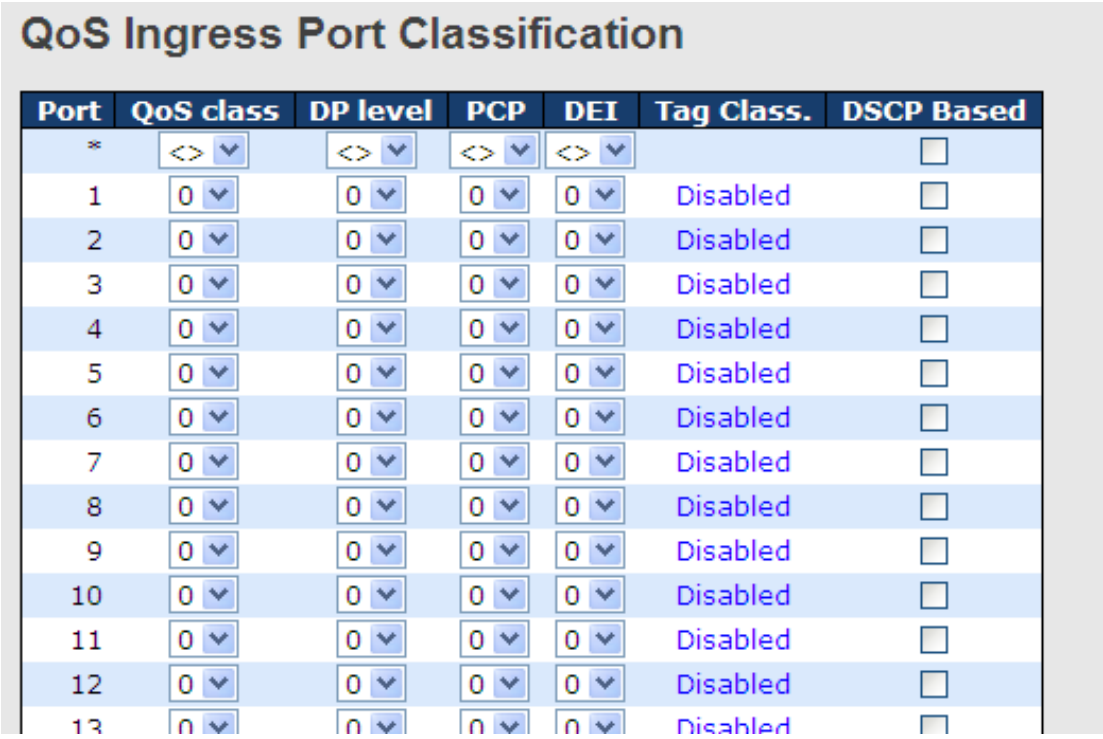
Note: frames sent to the CPU of the switch are always limited to approximately 4 kpps. For example, broadcasts in the management VLAN are limited to this rate. The management VLAN is configured on the IP setup page.




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

## 5.6.2 Port Classification

QoS is an acronym for Quality of Service. It is a method to achieve efficient bandwidth utilization between individual applications or protocols.

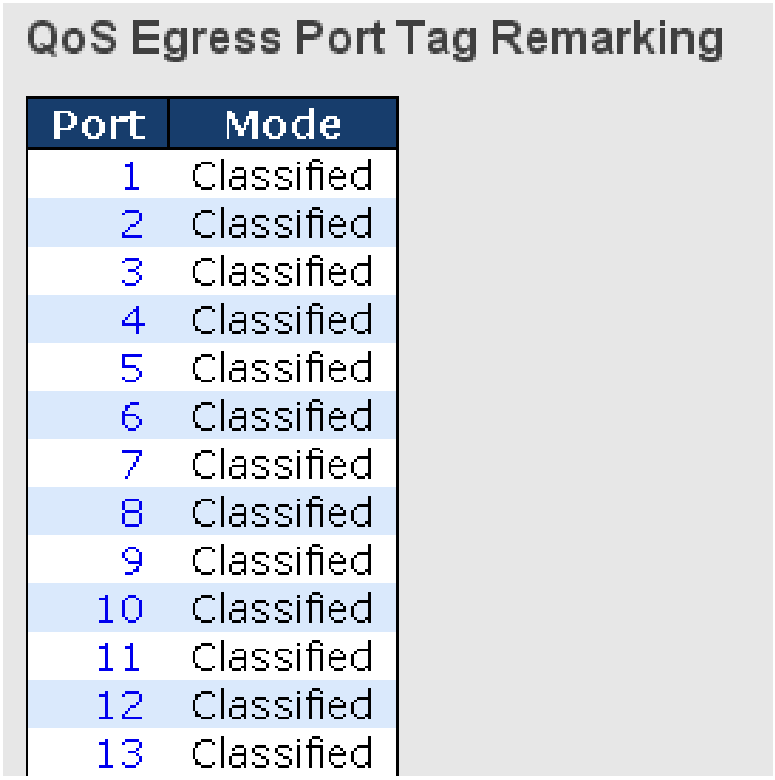


| Label | Description |
|---|---|
| **Port** | The port number for which the configuration below applies |
| **QoS Class** | Controls the default QoS class<br>All frames are classified to a QoS class. There is a one to one mapping between QoS class, queue, and priority. A QoS class of 0 (zero) has the lowest priority.<br>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.<br>PCP value: 0 1 2 3 4 5 6 7<br>QoS class: 1 0 2 3 4 5 6 7<br>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.<br>The classified QoS class can be overruled by a QCL entry.<br>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<br>All frames are classified to a DP level.<br>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.<br>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.<br>The classified DP level can be overruled by a QCL entry. |
| **PCP** | Controls the default PCP value<br>All frames are classified to a PCP value.<br>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.<br>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<br>**Disabled**: Use default QoS class and DP level for tagged frames<br>**Enabled**: Use mapped versions of PCP and DEI for tagged frames<br>Click on the mode to configure the mode and/or mapping<br>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 |

## 5.6.3 Port Tag Remaking

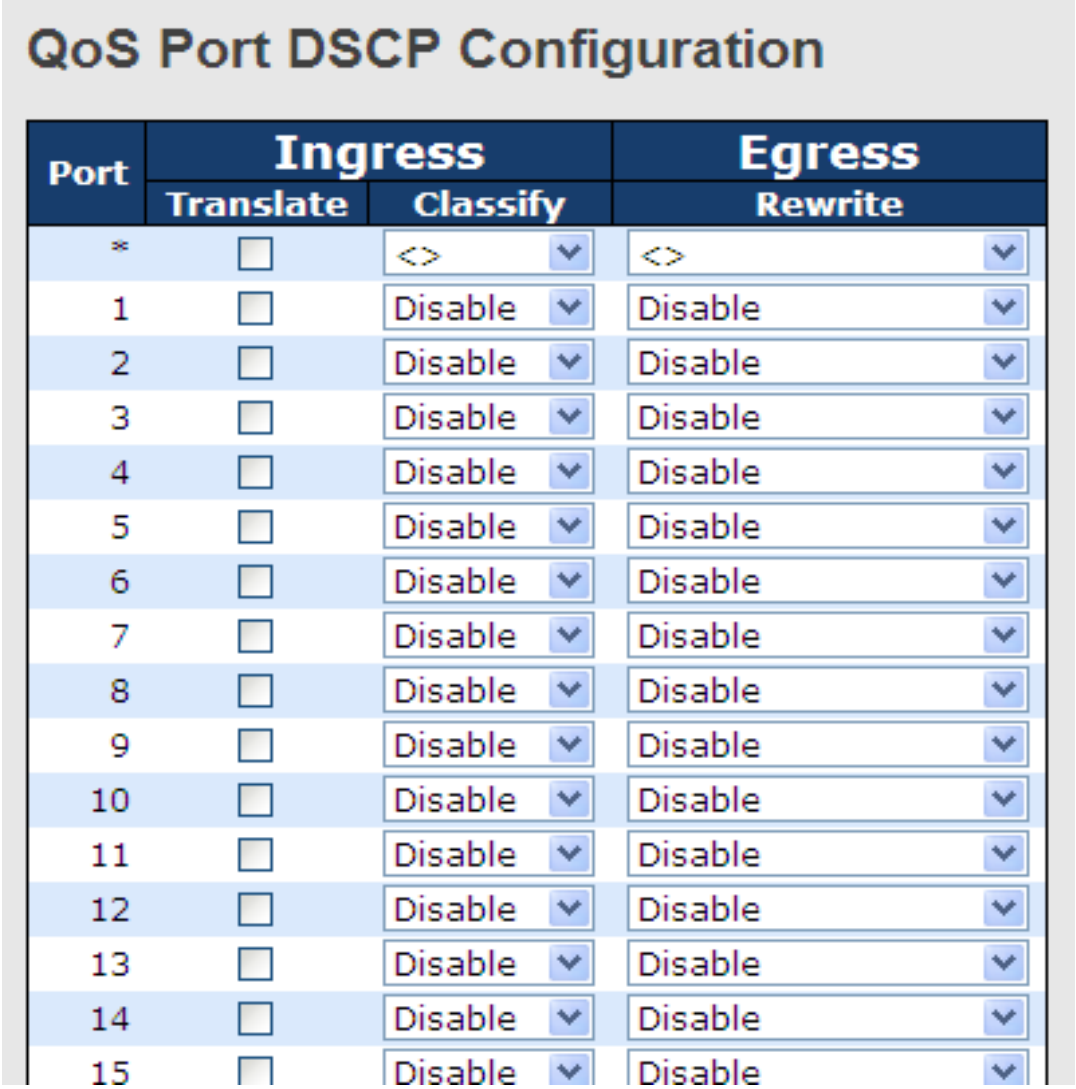
This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.



| Label | Description |
|---|---|
| **Port** | The switch port number to which the following settings will be applied. Click on the port number to configure tag remarking |
| **Mode** | Shows the tag remarking mode for this port<br>**Classified**: use classified PCP/DEI values<br>**Default**: use default PCP/DEI values<br>**Mapped**: use mapped versions of QoS class and DP level |

## 5.6.4 Port DSCP

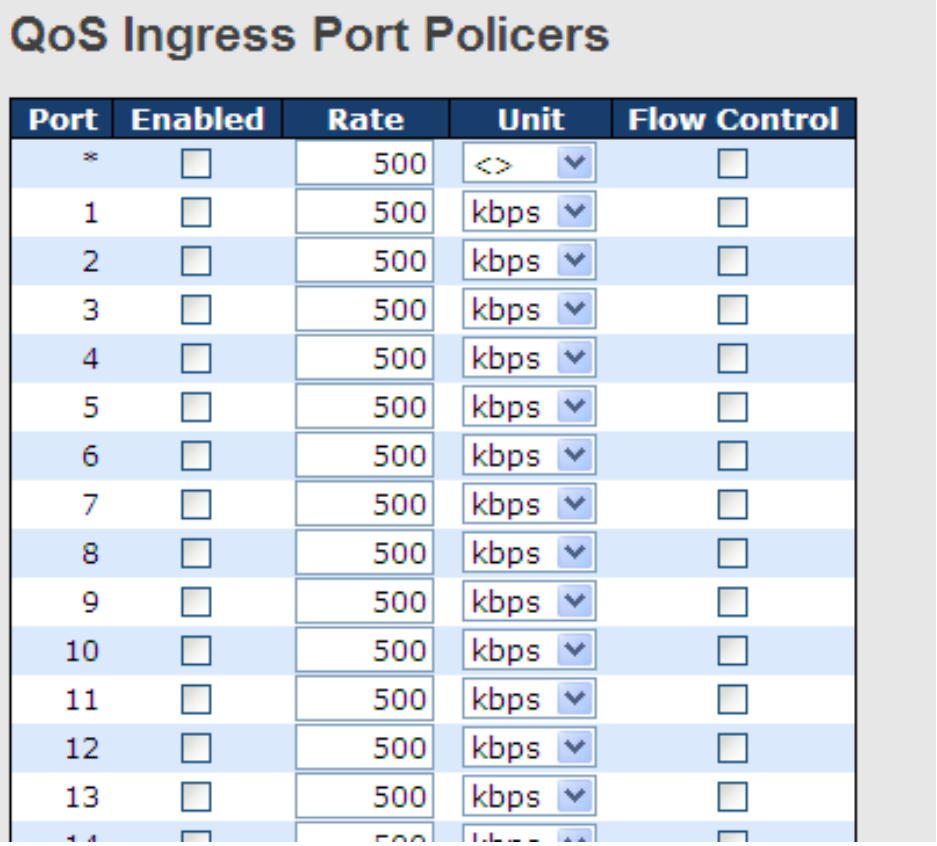
This page allows you to configure basic QoS Port DSCP settings for all switch ports.



| Label | Description |
|---|---|
| **Port** | 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.<br>There are two configuration parameters available in Ingress:<br>1. **Translate**<br>2. **Classify** |
| **1. Translate** | Check to enable ingress translation |
| **2. Classify** | Classification has 4 different values.<br>**Disable**: no Ingress DSCP classification<br>**DSCP=0**: classify if incoming (or translated if enabled) DSCP is 0.<br>**Selected**: classify only selected DSCP whose classification is enabled as specified in **DSCP Translation** window for the specific DSCP.<br>**All**: classify all DSCP |
| **Egress** | Port egress rewriting can be one of the following options:<br>**Disable**: no Egress rewrite<br>**Enable**: rewrite enabled without remapping<br>**Remap DP Unaware**: DSCP from the analyzer is remapped and the frame is remarked with a remapped DSCP value. The remapped DSCP value is always taken from the '**DSCP Translation->Egress Remap DP0**' table.<br>**Remap DP Aware**: DSCP from the analyzer is remapped and the frame is remarked with a 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. |

## 5.6.5 Port Policing

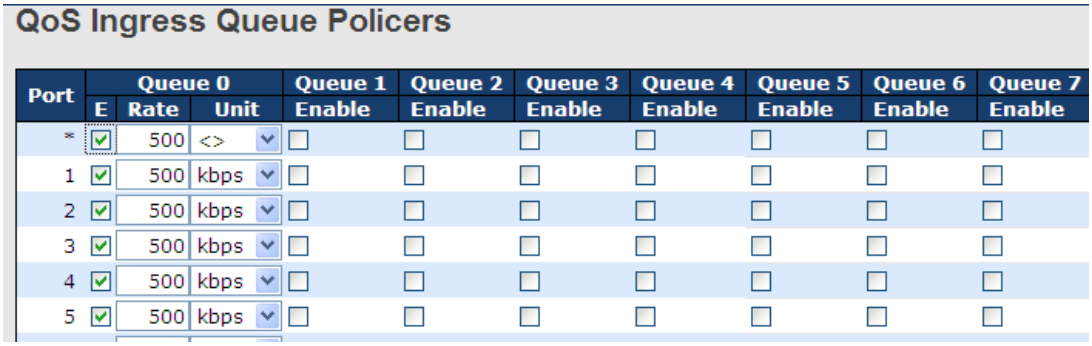
This page allows you to configure Policer settings for all switch ports.




| Label | Description |
|---|---|
| **Port** | The port number for which the configuration below applies |
| **Enable** | Check to enable the policer for individual switch ports |
| **Rate** | Configures the rate of each policer. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps** or **fps**, and is restricted to 1 to 3300 when the **Unit** is **Mbps** or **kfps**. |
| **Unit** | Configures the unit of measurement for each policer rate as **kbps**, **Mbps**, **fps**, or **kfps**. The default value is **kbps**. |
| **Flow Control** | If **Flow Control** is enabled and the port is in **Flow Control** mode, then pause frames are sent instead of being discarded. |

## 5.6.6 Queue Policing

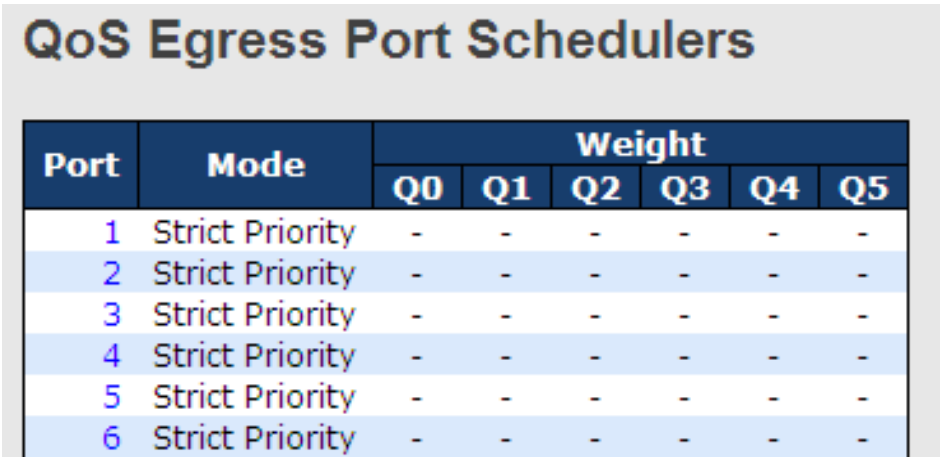
This page allows you to configure Queue Policer settings for all switch ports.




| Label | Description |
|---|---|
| **Port** | The port number for which the configuration below applies. |
| **Enable(E)** | Check to enable queue policer for individual switch ports. |
| **Rate** | Configures the rate of each queue policer. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps**, and is restricted to 1 to 3300 when the **Unit** is **Mbps**.<br>This field is only shown if at least one of the queue policers is enabled. |
| **Unit** | Configures the unit of measurement for each queue policer rate as kbps or Mbps. The default value is **kbps**.<br>This field is only shown if at least one of the queue policers is enabled. |

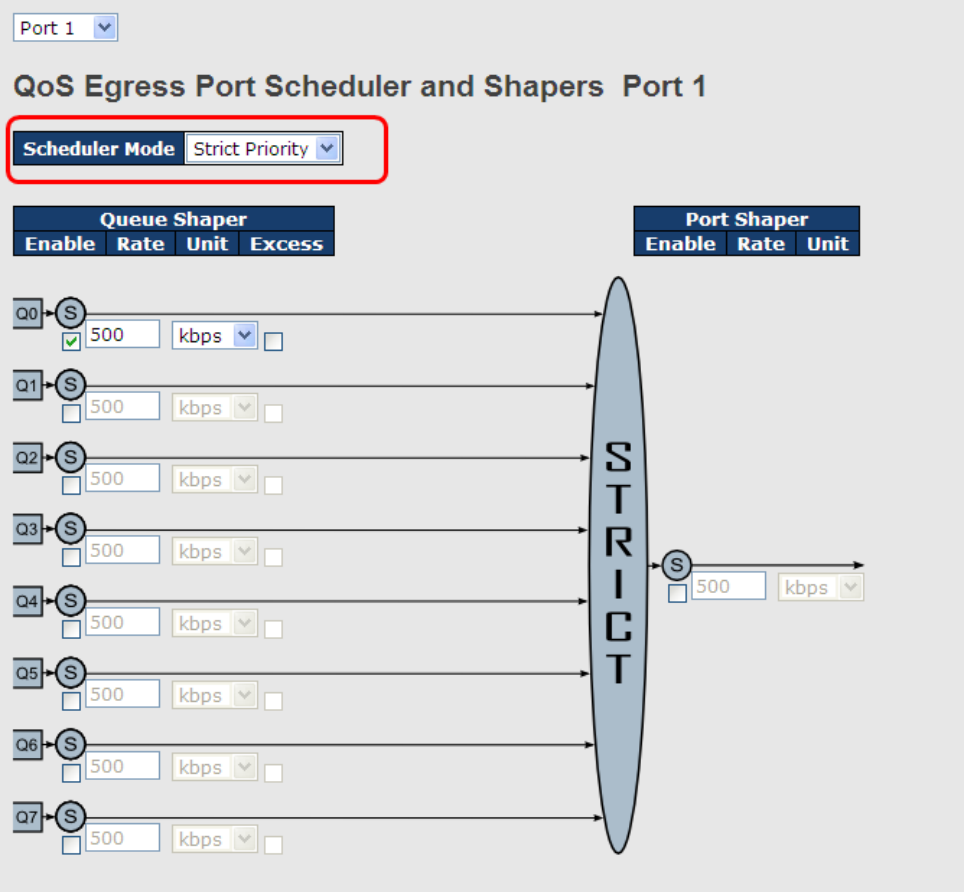
## 5.6.7 Port Scheduler

This page allows you to configure Scheduler and Shapers for a specific port. Clicking the port number in this page will bring up another page with detailed settings for port priority.



| Label | Description |
|---|---|
| **Port** | The switch port number to which the following settings will be applied.<br>Click on the port number to configure the schedulers |
| **Mode** | Shows the scheduling mode for this port |
| **Weight** | Shows the weight for this queue and port |

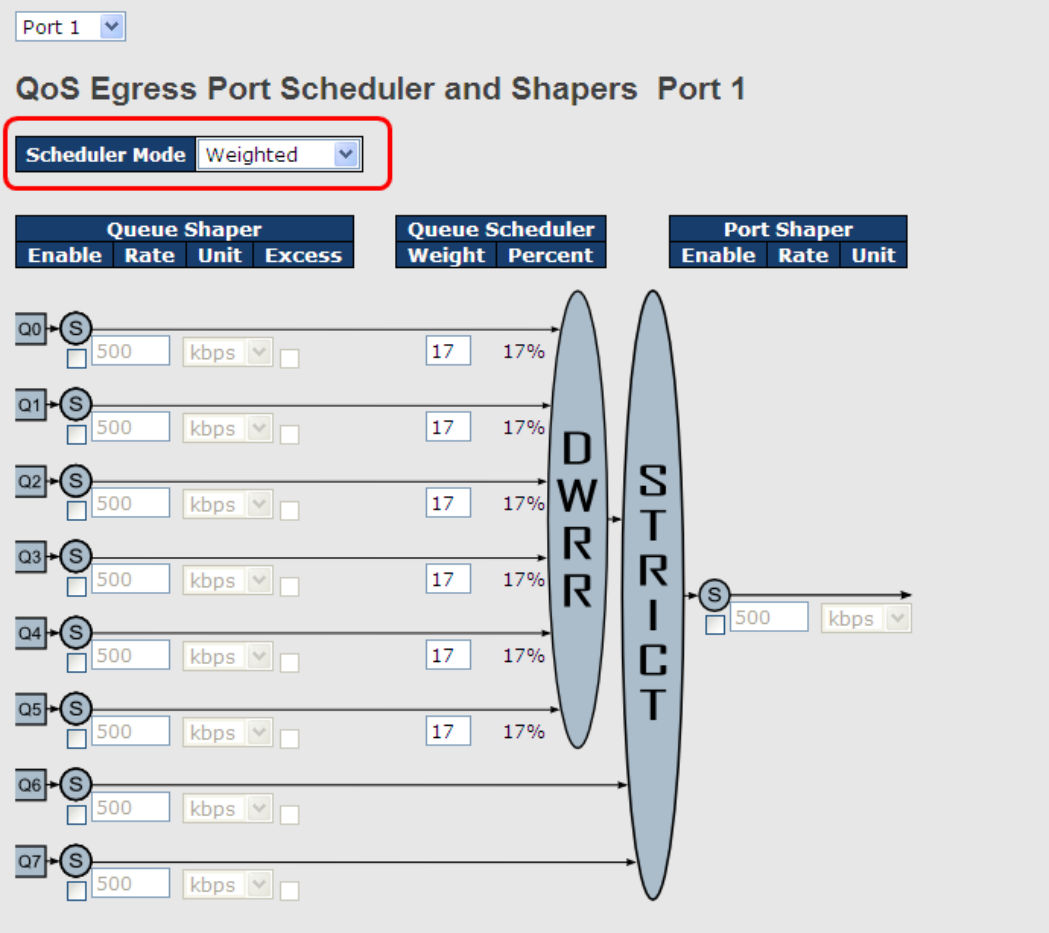
## Strict Priority




| Label | Description |
|---|---|
| **Scheduler Mode** | Controls whether the scheduler mode is **Strict Priority** or **Weighted** on this switch port. |
| **Queue Shaper Enable** | Check to enable queue shaper for individual switch ports. |
| **Queue Shaper Rate** | Configures the rate of each queue shaper. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps**", and it is restricted to 1 to 3300 when the **Unit** is **Mbps**. |
| **Queues Shaper Unit** | Configures the rate for each queue shaper. The default |

| | |
|---|---|
| | value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps**, and it is restricted to 1 to 3300 when the **Unit** is **Mbps**. |
| **Queue Shaper Excess** | Allows the queue to use excess bandwidth. |
| **Port Shaper Enable** | Check to enable port shaper for individual switch ports. |
| **Port Shaper Rate** | Configures the rate of each port shaper. The default value is **500** This value is restricted to 100 to 1000000 when the **Unit** is **kbps**, and it is restricted to 1 to 3300 when the **Unit** is **Mbps**. |
| **Port Shaper Unit** | Configures the unit of measurement for each port shaper rate as **kbps** or **Mbps**. The default value is **kbps**. |

## Weighted

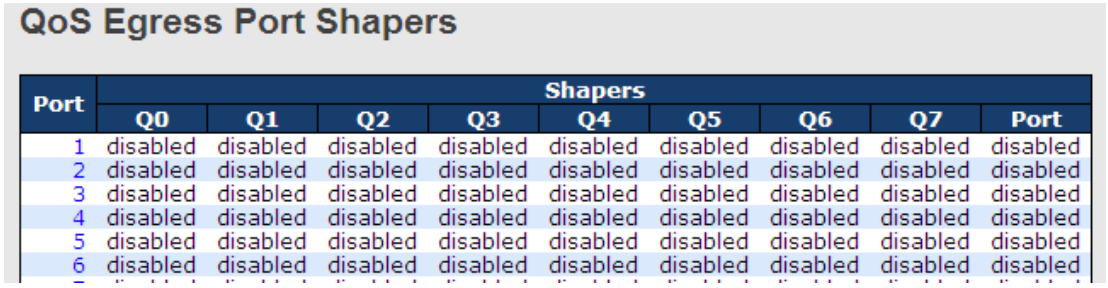



| Label | Description |
|---|---|
| **Scheduler Mode** | Controls whether the scheduler mode is **Strict Priority** or **Weighted** on this switch port |

| | |
|---|---|
| **Queue Shaper Enable** | Check to enable queue shaper for individual switch ports |
| **Queue Shaper Rate** | Configures the rate of each queue shaper. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps**, and it is restricted to 1 to 3300 when the **Unit** is **Mbps**. |
| **Queues Shaper Unit** | Configures the rate of each queue shaper. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit**" is **kbps**, and it is restricted to 1 to 3300 when the **Unit** is **Mbps**. |
| **Queue Shaper Excess** | Allows the queue to use excess bandwidth |
| **Queue Scheduler Weight** | Configures the weight of each queue. The default value is **17**. This value is restricted to 1 to 100. This parameter is only shown if **Scheduler Mode** is set to **Weighted**. |
| **Queue Scheduler Percent** | Shows the weight of the queue in percentage. This parameter is only shown if **Scheduler Mode** is set to **Weighted**. |
| **Port Shaper Enable** | Check to enable port shaper for individual switch ports |
| **Port Shaper Rate** | Configures the rate of each port shaper. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps**, and it is restricted to 1 to 3300 when the **Unit** is **Mbps**. |
| **Port Shaper Unit** | Configures the unit of measurement for each port shaper rate as **kbps** or **Mbps**. The default value is **kbps**. |

## 5.6.8 Port Shaping

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

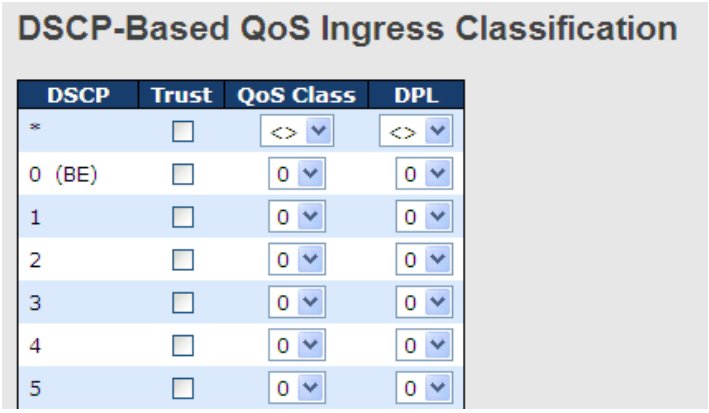



| Label | Description |
|---|---|
| **Port** | The switch port number to which the following settings will |

| | |
|---|---|
| | be applied. Click on the port number 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" |

## 5.6.9 DSCP Based QoS

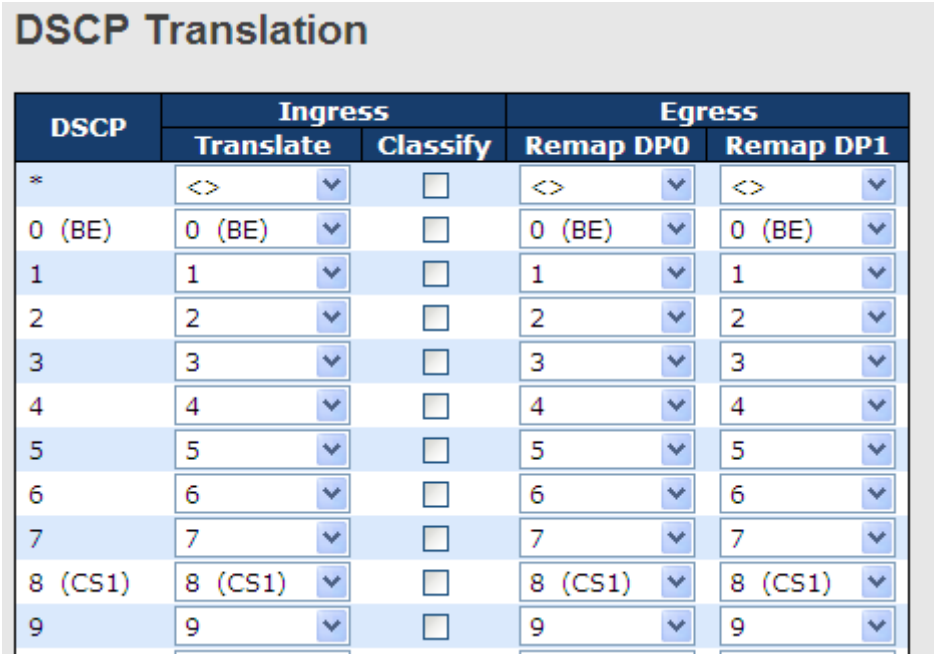
This page allows you to configure basic QoS DSCP-based QoS Ingress Classification settings for all switches.




| Label | Description |
|---|---|
| **DSCP** | Maximum number of supported DSCP values is 64 |
| **Trust** | Check to trust a specific DSCP value. 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 number from 0-7. |
| **DPL** | Drop Precedence Level (0-1) |

## 5.6.10 DSCP Translation

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

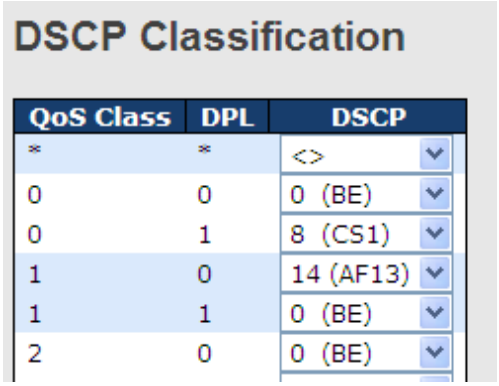



| Label | Description |
|---|---|
| **DSCP** | Maximum number of supported DSCP values is 64 and valid DSCP value ranges from 0 to 63. |
| **Ingress** | Ingress DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.<br>There are two configuration parameters for DSCP Translation -<br>1. **Translate:** DSCP can be translated to any of (0-63) DSCP values.<br>2. **Classify:** check to enable ingress classification |
| **Egress** | Configurable engress parameters include;<br>**Remap DP0**: controls the remapping for frames with DP level 0. You can select the DSCP value from a selected menu to which you want to remap. DSCP value ranges from 0 to 63.<br>**Remap DP1**: controls the remapping for frames with DP level 1. You can select the DSCP value from a selected menu to which you want to remap. DSCP value ranges from 0 to 63. |

## 5.6.11 DSCP Classification

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

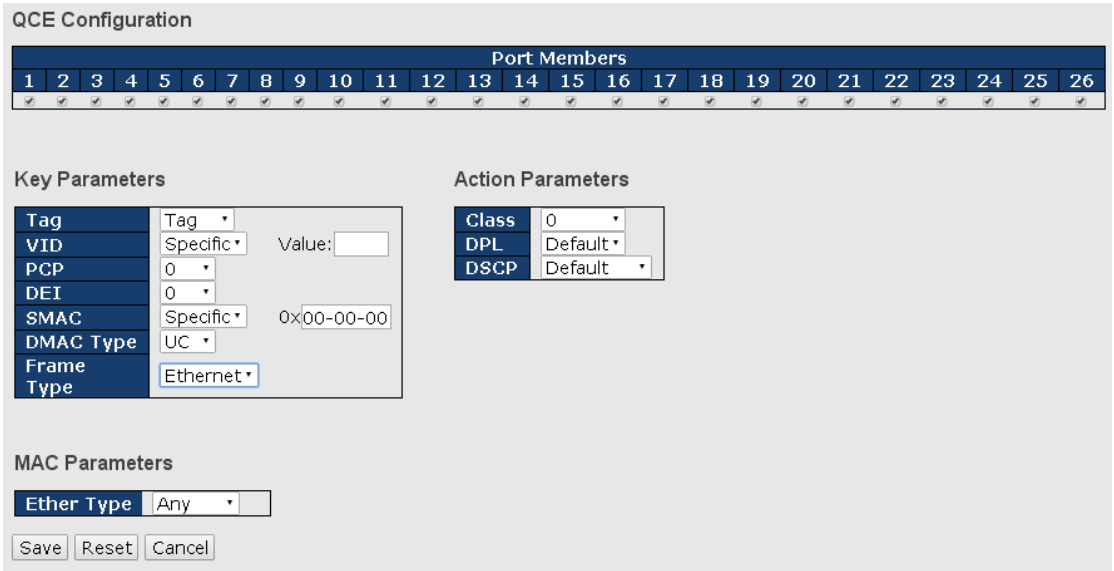
DSCP value.




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

## 5.6.12 QoS Control List

This page allows you to edit or insert a single QoS control entry at a time. A QCE consists of several parameters. These parameters vary with the frame type you select.



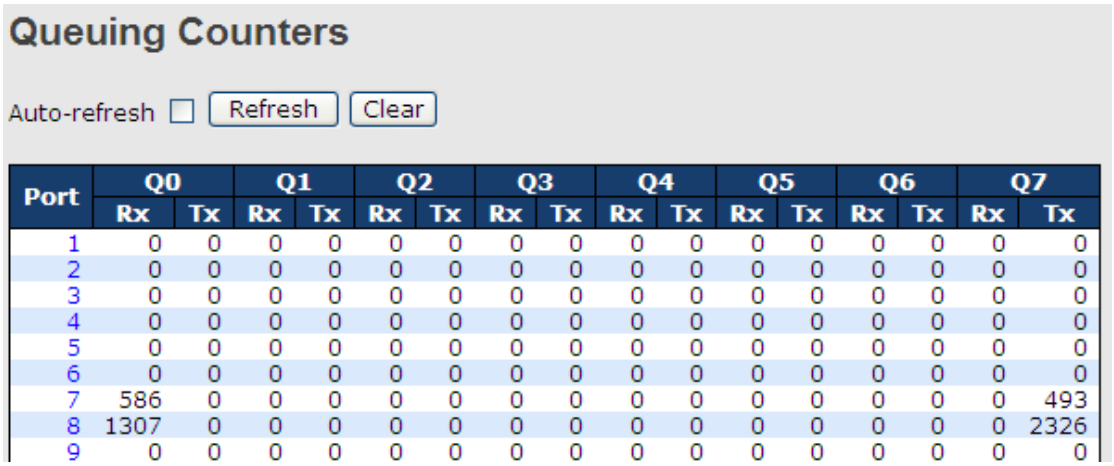

| Label | Description |
|---|---|
| Port Members | Check to include the port in the QCL entry. By default, all ports are included. |
| Key Parameters | Key configurations include:<br>**Tag**: value of tag, can be **Any**, **Untag** or **Tag**. |

| | |
|---|---|
| | **VID**: valid value of VLAN ID, can be any value from 1 to 4095 **Any**: user can enter either a specific value or a range of VIDs.<br>**PCP**: Priority Code Point, can be specific numbers (0, 1, 2, 3, 4, 5, 6, 7), a range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or **Any.**<br>**DEI**: Drop Eligible Indicator, can be any of values between 0 and 1 or **Any**<br>**SMAC**: Source MAC Address, can be 24 MS bits (OUI) or **Any.**<br>**DMAC Type**: Destination MAC type, can be **unicast** (**UC**), **multicast** (**MC**), **broadcast** (**BC**) or **Any.**<br>Frame Type can be the following values:<br>**Any**<br>**Ethernet**<br>**LLC**<br>**SNAP**<br>**IPv4**<br>**IPv6**<br>Note: all frame types are explained below. |
| Any | Allow all types of frames |
| Ethernet | Valid Ethernet values can range from 0x600 to 0xFFFF or Any' but excluding 0x800(IPv4) and 0x86DD (IPv6). The default value is **Any**. |
| LLC | SSAP Address: valid SSAP (Source Service Access Point) values can range from 0x00 to 0xFF or **Any**. The default value is **Any**.<br>DSAP Address: valid DSAP (Destination Service Access Point) values can range from 0x00 to 0xFF or **Any**. The default value is **Any**.<br>Control Valid Control: valid values can range from 0x00 to 0xFF or **Any**. The default value is **Any**. |
| SNAP | PID: valid PID (a.k.a ethernet type) values can range from 0x00 to 0xFFFF or Any. The default value is Any. |
| IPv4 | Protocol IP Protocol Number: (0-255, TCP or UDP) or **Any**<br>Source IP: specific Source IP address in value/mask format or **Any**. IP and mask are in the format of x.y.z.w |

| | |
|---|---|
| | where x, y, z, and w are decimal numbers between 0 and 255. When the 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.<br>DSCP (Differentiated Code Point): can be a specific value, a range, or **Any**. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.<br>IP Fragment: Ipv4 frame fragmented options include **'yes'**, **'no'**, and **'any'**.<br>Sport Source TCP/UDP Port: (0-65535) or **Any**, specific value or port range applicable for IP protocol UDP/TCP.<br>Dport Destination TCP/UDP Port: (0-65535) or **Any**, specific value or port range applicable for IP protocol UDP/TCP. |
| IPv6 | Protocol IP protocol number: (0-255, TCP or UDP) or **Any.**<br>Source IP IPv6 source address: (a.b.c.d) or **Any**, 32 LS bits.<br>DSCP (Differentiated Code Point): can be a specific value, a range, or **Any**. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.<br>Sport Source TCP/UDP port: (0-65535) or **Any**, specific value or port range applicable for IP protocol UDP/TCP.<br>Dport Destination TCP/UDP port: (0-65535) or **Any**, specific value or port range applicable for IP protocol UDP/TCP. |
| Action Parameters | Class QoS class: (0-7) or **Default**<br>Valid Drop Precedence Level value can be (0-1) or **Default**.<br>Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or **Default**.<br>Default means that the default classified value is not modified by this QCE. |

## 5.6.13 QoS Statisitics

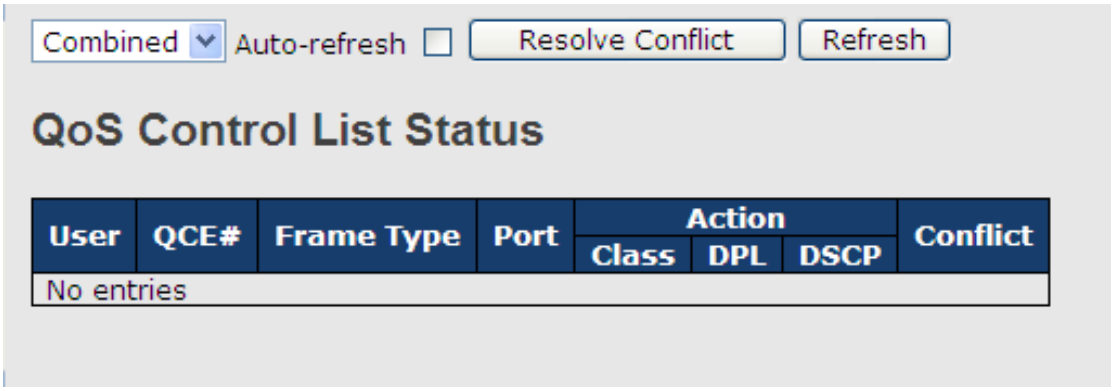
This page provides the statistics of individual queues for all switch ports.




| Label | Description |
|---|---|
| **Port** | The switch port number to which the following settings will be applied. |
| **Qn** | There are 8 QoS queues per port. Q0 is the lowest priority |
| **Rx / Tx** | The number of received and transmitted packets per queue |

## 5.6.14 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: |

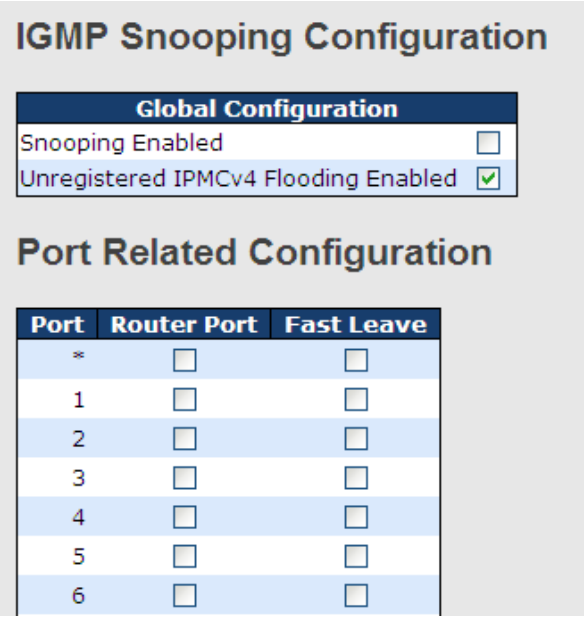
| | |
|---|---|
| | **Any**: the QCE will match all frame type.<br>**Ethernet**: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.<br>**LLC**: Only (LLC) frames are allowed.<br>**SNAP**: Only (SNAP) frames are allowed.<br>**IPv4**: the QCE will match only IPV4 frames.<br>**IPv6**: the 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.<br>There are three action fields: **Class**, **DPL**, and **DSCP**.<br>**Class**: Classified QoS; if a frame matches the QCE, it will be put in the queue.<br>**DPL**: Drop Precedence Level; if a frame matches the QCE, then DP level will set to a value displayed under DPL column.<br>**DSCP**: if a frame matches the QCE, then DSCP will be classified with the value displayed under DSCP column. |
| **Conflict** | Displays the conflict status of QCL entries. As hardware resources are shared by multiple applications, 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 hardware resources required to add the QCL entry by pressing **Resolve Conflict** button**.** |

# 5.7 Multicast

## 5.7.1 IGMP Snooping

### 5.7.1.1 Basic Settings

This page provides IGMP Snooping related configurations.




| Label | Description |
|---|---|
| **Snooping Enabled** | Check to enable global IGMP snooping |
| **Unregistered IPMCv4Flooding enabled** | Check to enable unregistered IPMC traffic flooding |
| **Router Port** | Specifies 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.<br>If an aggregation member port is selected as a router port, the whole aggregation will act as a router port. |
| **Fast Leave** | Check to enable fast leave on the port |

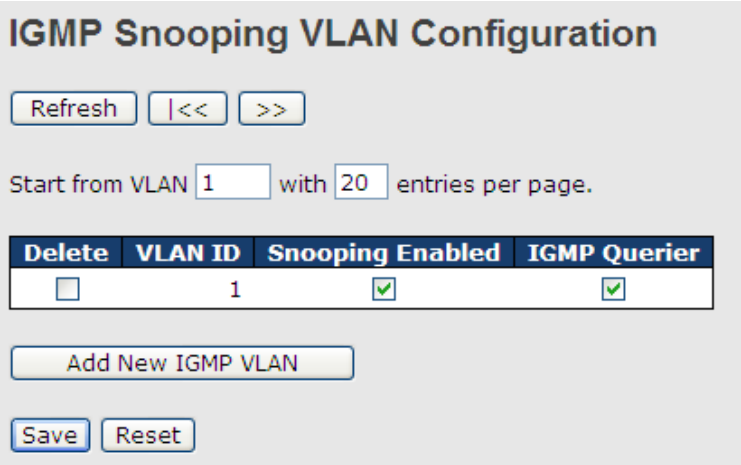
### 5.7.1.2 VLAN Configurations

Each page shows up to 99 entries from the VLAN table, with a default value of 20, selected by 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 field allows 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.

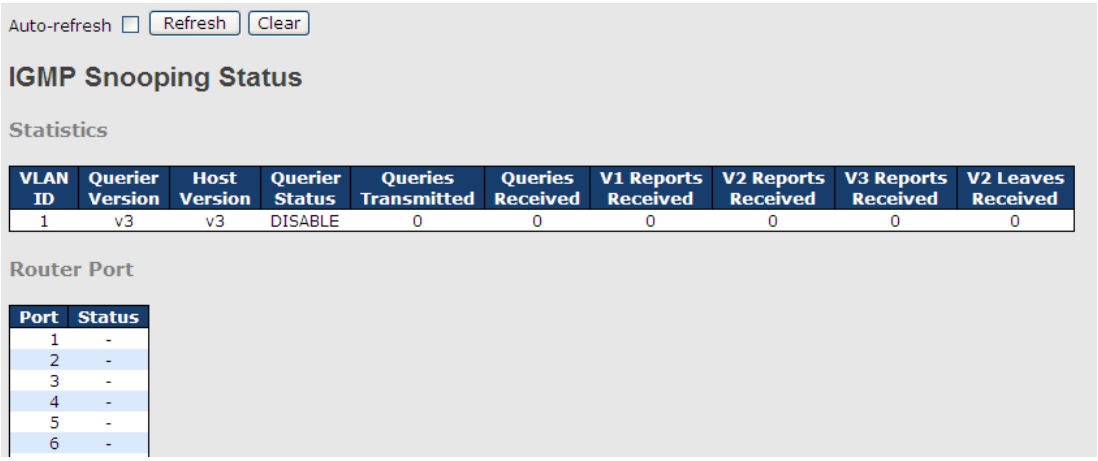
When the end is reached, the text **No more entries** is shown in the displayed table. Use the **|<<** button to start over.




| 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** | Check to enable IGMP snooping for individual VLAN. Up to 32 VLANs can be selected. |
| **IGMP Querier** | Check to enable the IGMP Querier in the VLAN |

### 5.7.1.3 Status

This page provides IGMP snooping status.

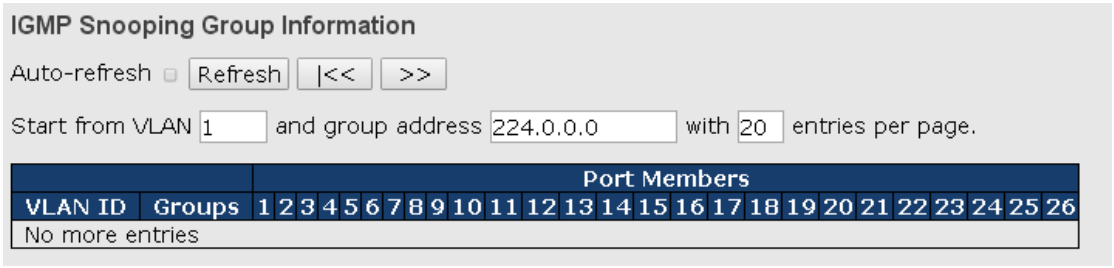



| Label | Description |
|---|---|
| **VLAN ID** | The VLAN ID of the entry |

| | |
|---|---|
| **Querier Version** | Active Querier version |
| **Host Version** | Active Host version |
| **Querier Status** | Shows the Querier status as **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 packets |
| **Refresh** | Click to refresh the page immediately |
| **Clear** | Clear all statistics counters |
| **Auto-refresh** | Check to enable an automatic refresh of the page at regular intervals |
| **Port** | Switch port number |
| **Status** | Indicates whether a specific port is a router port or not |

#### 5.7.1.4 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.

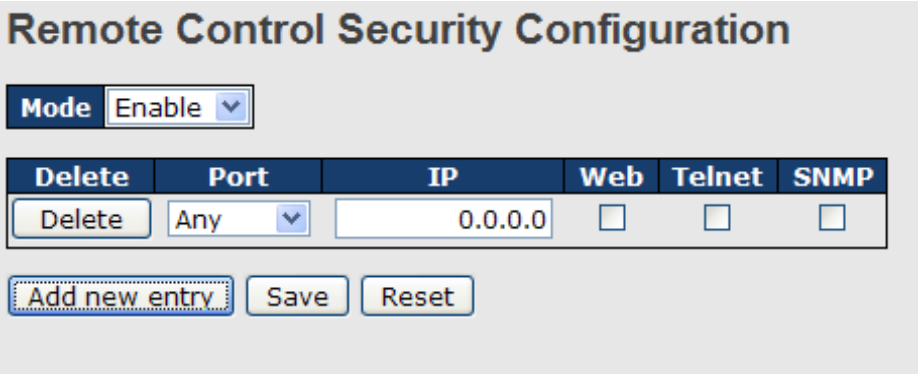



| Label | Description |
|---|---|
| **VLAN ID** | The VLAN ID of the group |
| **Groups** | The group address of the group displayed |
| **Port Members** | Ports under this group |

# 5.8 Security

## 5.8.1 Remote Control Security

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

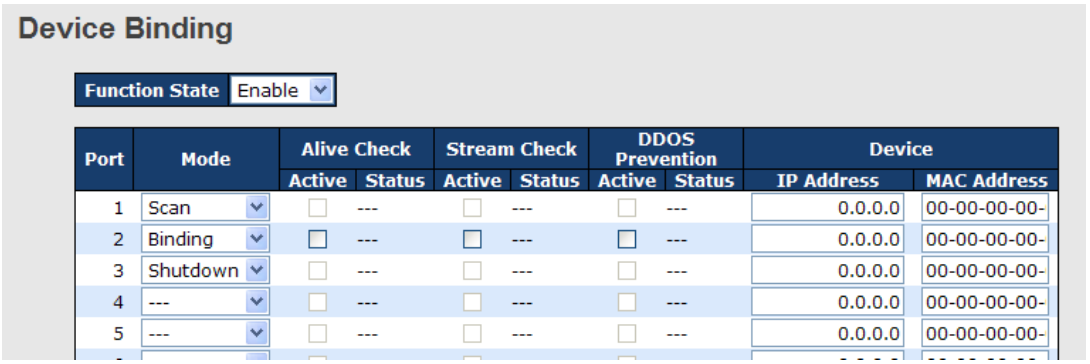



| Label | Description |
|---|---|
| **Port** | Port number of the remote client |
| **IP Address** | IP address of the remote client. **0.0.0.0** means "any IP". |
| **Web** | Check to enable management via a Web interface |
| **Telnet** | Check to enable management via a Telnet interface |
| **SNMP** | Check to enable management via a SNMP interface |
| **Delete** | Check to delete entries |

## 5.8.2 Device Binding

### 5.8.2.1 Basic Configuration

This page provides device binding configurations. Device binding is a powerful way to monitor devices and network security.



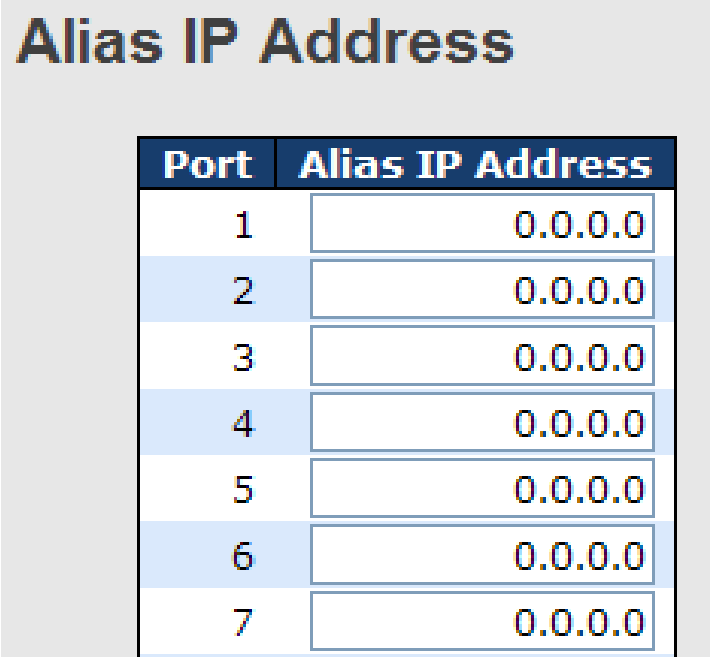

| Label | Description |
|---|---|
| **Mode** | Indicates the device binding operation for each port. Possible modes are:<br>**---**: disable<br>**Scan**: scans IP/MAC automatically, but no binding function |

| | |
|---|---|
| | **Binding**: enables binding. Under this mode, any IP/MAC that does not match the entry will not be allowed to access the network.<br>**Shutdown**: shuts down the port (No Link) |
| **Alive Check Active** | Check to enable alive check. When enabled, switch will ping the device continually. |
| **Alive Check Status** | Indicates alive check status. Possible statuses are:<br>**---**: disable<br>**Got Reply**: receive ping reply from device, meaning the device is still alive<br>**Lost Reply**: not receiving ping reply from device, meaning the device might have been dead. |
| **Stream Check Active** | Check to enable stream check. When enabled, the switch will detect the stream change (getting low) from the device. |
| **Stream Check Status** | Indicates stream check status. Possible statuses are:<br>**---**: disable<br>**Normal**: the stream is normal.<br>**Low**: the stream is getting low. |
| **DDoS Prevention Acton** | Check to enable DDOS prevention. When enabled, the switch will monitor the device against DDOS attacks. |
| **DDoS Prevention Status** | Indicates DDOS prevention status. Possible statuses are:<br>**---**: disable<br>**Analyzing**: analyzes packet throughput for initialization<br>**Running**: analysis completes and ready for next move<br>**Attacked**: DDOS attacks occur |
| **Device IP Address** | Specifies IP address of the device |
| **Device MAC Address** | Specifies MAC address of the device |

### 5.8.2.2 Advanced Configurations

#### Alias IP Address

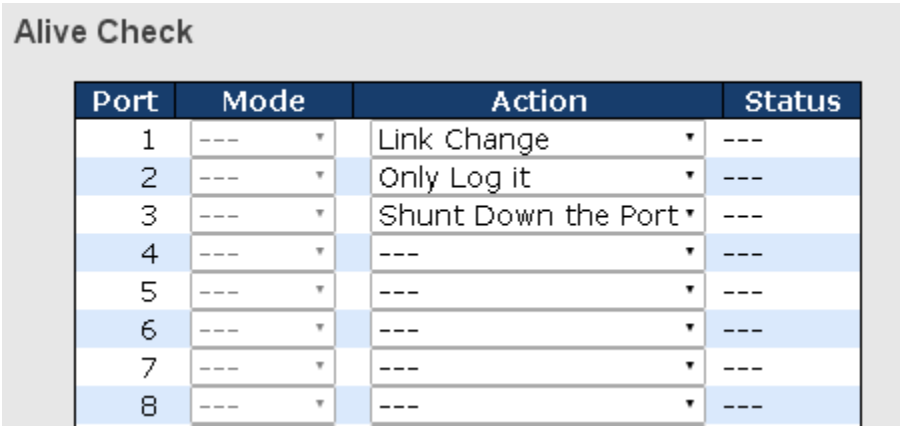
This page provides Alias IP Address configuration. Some devices might have more than one IP addresses. You could specify the other IP address here.




| Label | Description |
|---|---|
| **Alias IP Address** | Specifies alias IP address. Keep **0.0.0.0** if the device does not have an alias IP address. |

### Alive Check

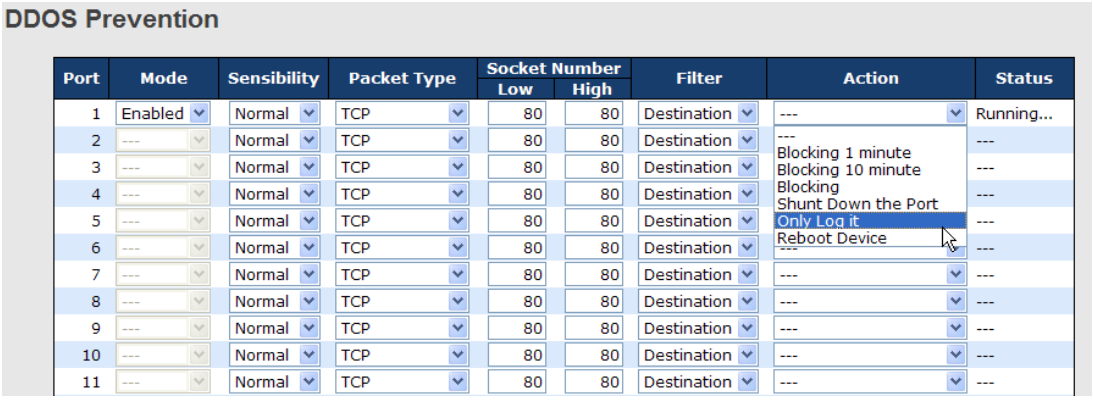
You can use ping commands to check port link status. If a port link fails, the system will take actions based on your settings.




| Label | Description |
|---|---|
| **Mode** | Disables or enables the port |
| **Action** | The action to be taken when the link fails, such as shutting down the port and logging the event, simply logging the event, and rebooting. |

## DDoS Prevention

This page provides DDOS Prevention configurations. The switch can monitor ingress packets, and perform actions when DDOS attack occurred on this port. You can configure the setting to achieve maximum protection.

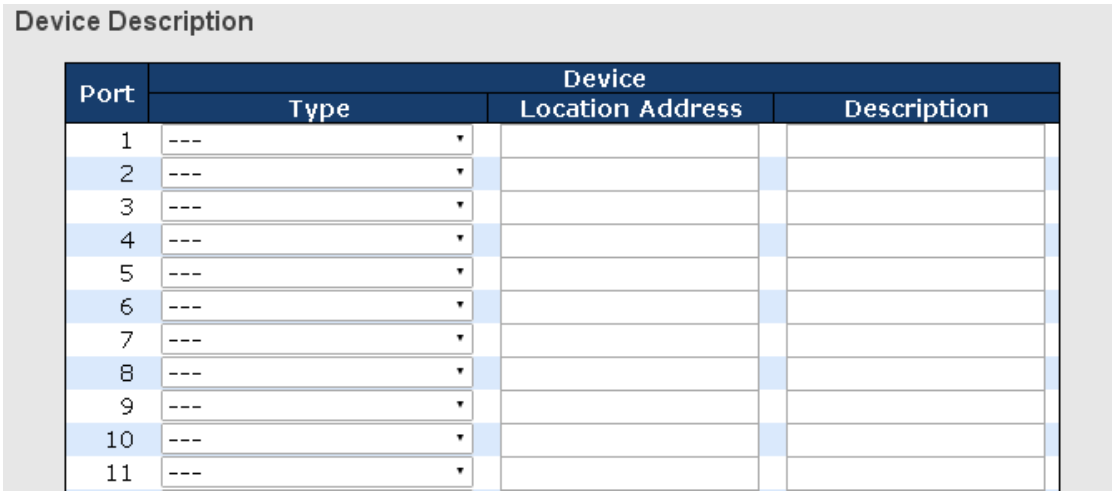



| Label | Description |
|---|---|
| **Mode** | Enables or disables DDOS prevention of the port |
| **Sensibility** | Indicates the level of DDOS detection. Possible levels are:<br>**Low**: low sensibility<br>**Normal**: normal sensibility<br>**Medium**: medium sensibility<br>**High**: high sensibility |
| **Packet Type** | Indicates the types of DDoS attack packets to be monitored. Possible types are:<br>**RX Total**: all ingress packets<br>**RX Unicast**: unicast ingress packets<br>**RX Multicast**: multicast ingress packets<br>**RX Broadcast**: broadcast ingress packets<br>**TCP**: TCP ingress packets<br>**UDP**: UDP ingress packets |
| **Socket Number** | If packet type is UDP (or TCP), please specify the socket number here. The socket number can be a range, from low to high. If the socket number is only one, please fill the same number in the low and high fields. |
| **Filter** | If packet type is UDP (or TCP), please choose the socket direction (**Destination**/**Source**). |
| **Action** | Indicates the action to take when DDOS attacks occur. |

| | |
|---|---|
| | Possible actions are:<br>**---**: no action<br>**Blocking 1 minute**: blocks the forwarding for 1 minute and log the event<br>**Blocking 10 minute**: blocks the forwarding for 10 minutes and log the event<br>**Blocking**: blocks and logs the event<br>**Shunt Down the Port**: shuts down the port (No Link) and logs the event<br>**Only Log it**: simply logs the event<br>**Reboot Device**: if PoE is supported, the device can be rebooted. The event will be logged. |
| **Status** | Indicates the DDOS prevention status. Possible statuses are:<br>**---**: disables DDOS prevention<br>**Analyzing**: analyzes packet throughput for initialization<br>**Running**: analysis completes and ready for next move<br>**Attacked**: DDOS attacks occur |

## Device Description

This page allows you to configure device description settings.

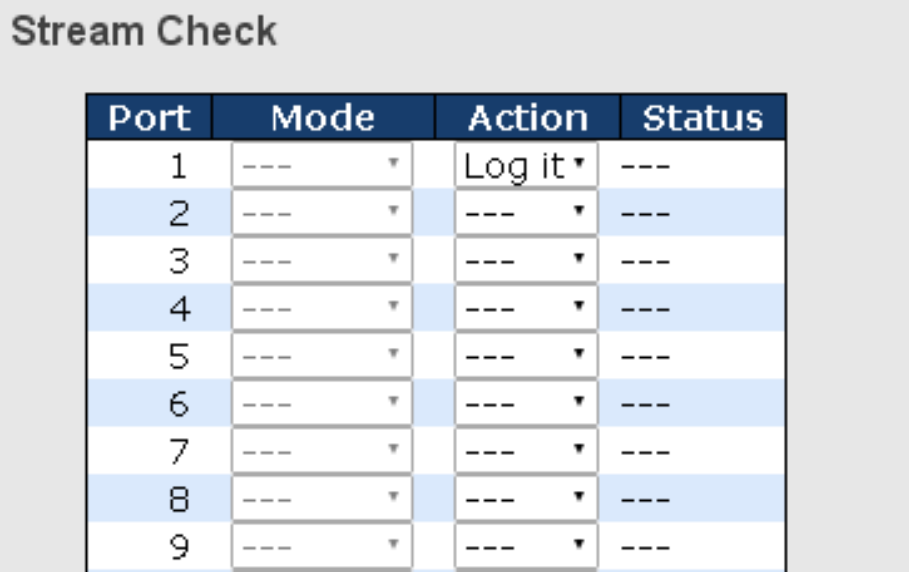



| Label | Description |
|---|---|
| **Device Type** | Indicates device types. Possible types are: **---** (no specification), **IP Camera**, **IP Phone**, **Access Point**, **PC**, **PLC**, and **Network Video Recorder** |

| | |
|---|---|
| **Location Address** | Indicates location information of the device. The information can be used for Google Mapping. |
| **Description** | Device descriptions |

### Stream Check

This page allows you to configure stream check settings.



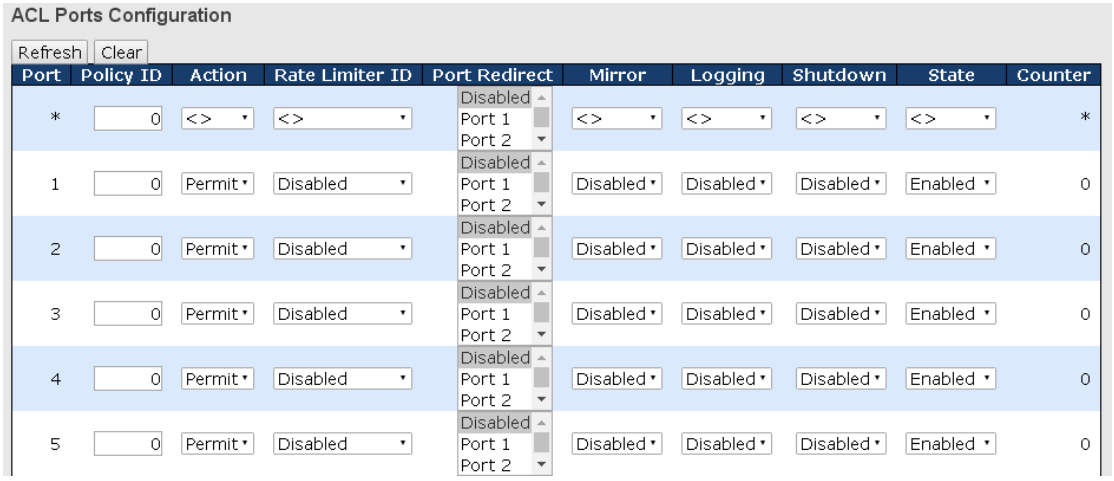

| Label | Description |
|---|---|
| **Mode** | Enables or disables stream monitoring of the port |
| **Action** | Indicates the action to take when the stream gets low. Possible actions are:<br>**---**: no action<br>**Log it**: simply logs the event |

## 5.8.3 ACL

An ACL (Access Control List) is a list of permissions attached to an object. An ACL specifies which users or system processes are authorized to access the objects and what operations are allowed on given objects.

### 5.8.3.1 Ports

This page allows you to 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.

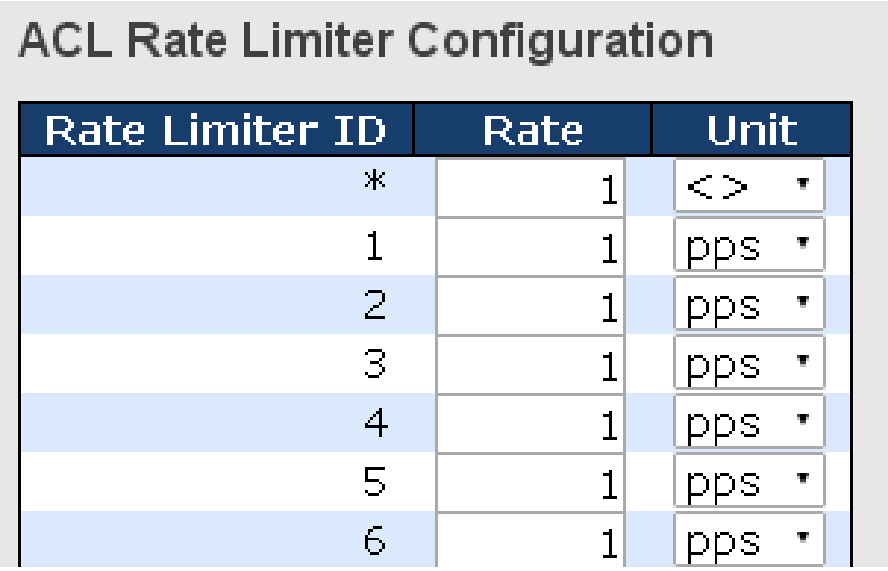



| Label | Description |
|---|---|
| **Port** | The switch port number to which the following settings will be applied |
| **Policy ID** | Select to apply a policy to the port. The allowed values are 1 to 8. The default value is **1**. |
| **Action** | Select to **Permit** to permit or **Deny** to deny forwarding. The default value is **Permit**. |
| **Rate Limiter ID** | Select a rate limiter for the port. The allowed values are Disabled or numbers from 1 to 15. The default value is Disabled. |
| **Port Redirect** | Indicates the port redirect operation implemented by the ACE. Frames matching the ACE are redirected to the listed port. |
| **Mirror** | Select which port frames are copied to. The allowed values are **Disabled** or a specific port number. The default value is **Disabled**. |
| **Logging** | Specifies the logging operation of the port. The allowed values are:<br>**Enabled**: frames received on the port are stored in the system log<br>**Disabled**: frames received on the port are not logged.<br>The default value is **Disabled**. Please note that system log memory capacity and logging rate is limited. |
| **Shutdown** | Specifies the shutdown operation of this port. The allowed values are:<br>**Enabled**: if a frame is received on the port, the port will be |

| | |
|---|---|
| | disabled.<br>**Disabled**: port shut down is disabled.<br>The default value is **Disabled**. |
| **Counter** | Counts the number of frames that match this ACE. |

### 5.8.3.2 Rate Limiters

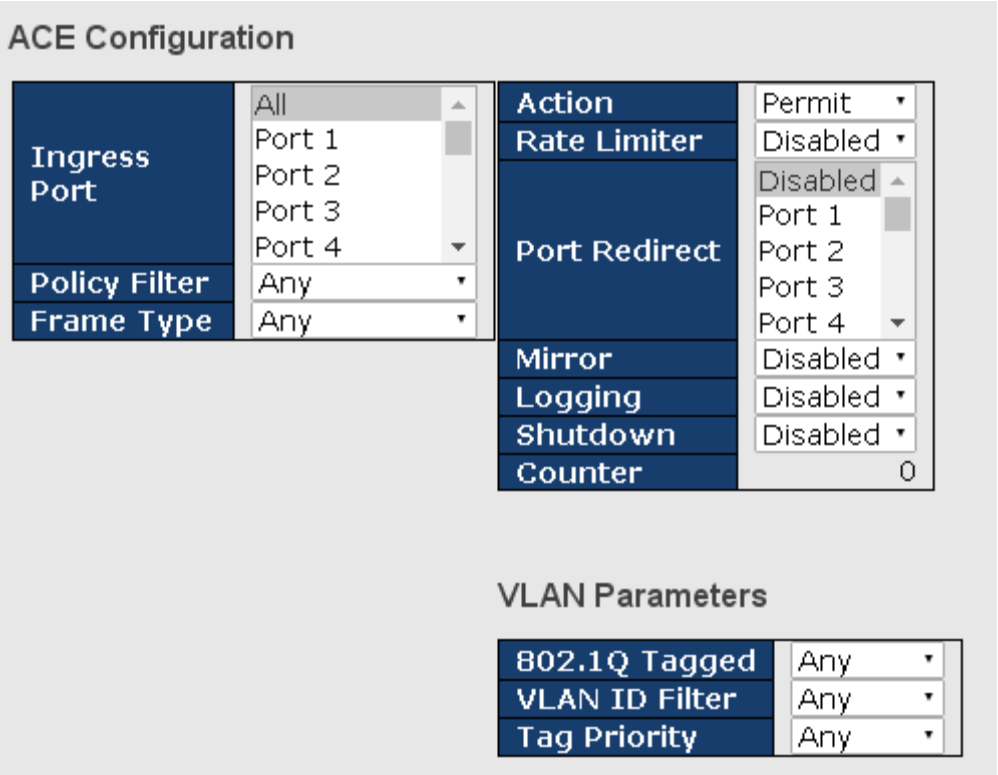
This page allows you to configure the rate limiter for the ACL of the switch.



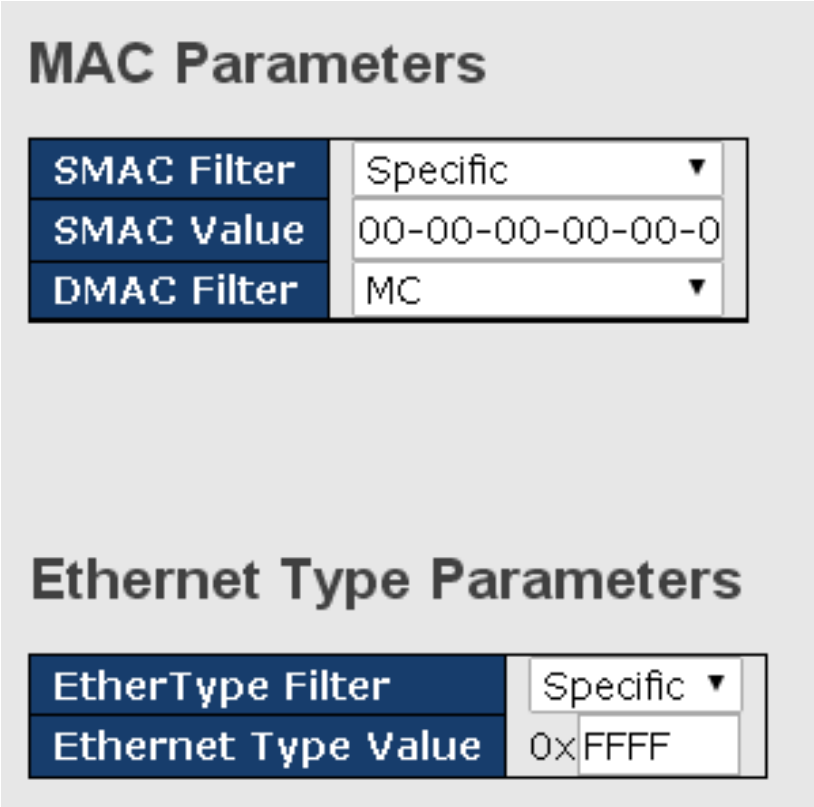

| Label | Description |
|---|---|
| **Rate Limiter ID** | The rate limiter ID for the settings contained in the same row. |
| **Rate** | The rate unit is packet per second (pps), which can be configured as 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K.<br>The 1 kpps is actually 1002.1 pps. |
| **Unit** | Specify the unit for the rate. |

### 5.8.3.3 ACL Control List

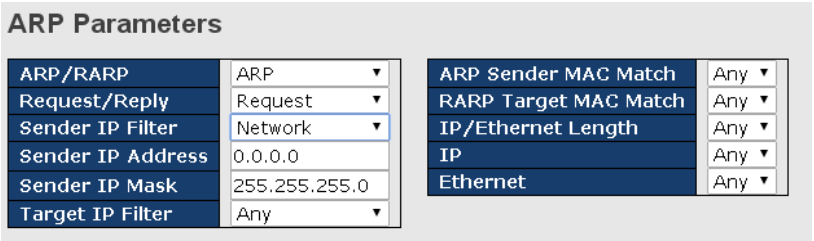
An ACE (Access Control Entry) is an element in an access control list (ACL). An ACL can have zero or more ACEs. Each ACE controls or monitors access to an object based on user-defined configurations. Each ACE consists of several parameters which vary with the frame type you have selected.



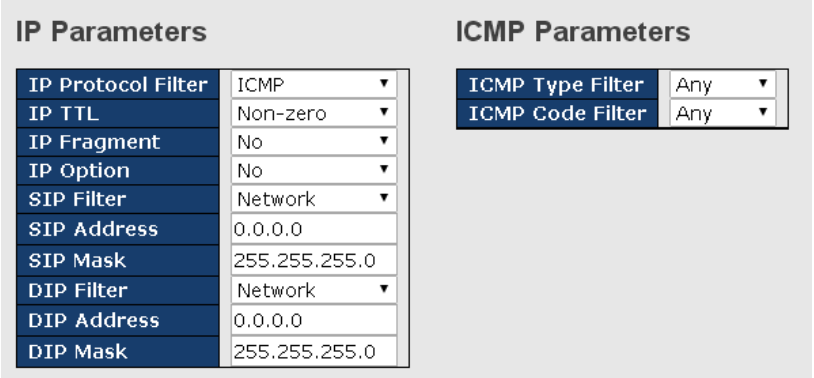

| Label | Description |
|---|---|
| **Ingress Port** | Indicates the ingress port to which the ACE will apply.<br>**Any**: the ACE applies to any port.<br>**Port n**: the ACE applies to this port number, where n is the number of the switch port.<br>**Policy n**: the ACE applies to this policy number, where n can range from 1 to 8. |
| **Policy Filter** | Indicates the policy number filter for this ACE. Choose any will not specify any policy filter. Choose Specific will allow you to filter a specific policy with this ACE. You can enter an policy value and bitmask then. |
| **Frame Type** | Indicates the frame type of the ACE. These frame types are mutually exclusive.<br>**Any**: any frame can match the ACE.<br>**Ethernet Type**: only Ethernet type frames can match the ACE. The IEEE 802.3 descripts the value of length/types should be greater than or equal to 1536 decimal (equal to 0600 hexadecimal). |




**ARP**: only ARP frames can match the ACE. Notice the ARP frames will not match the ACE with Ethernet type.

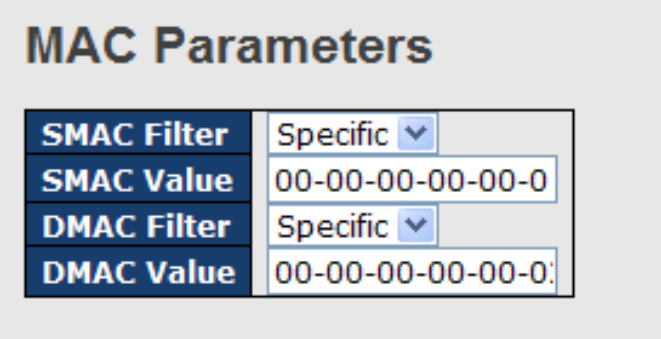



**IPv4**: only IPv4 frames can match the ACE. Notice the IPv4 frames will not match the ACE with Ethernet type.



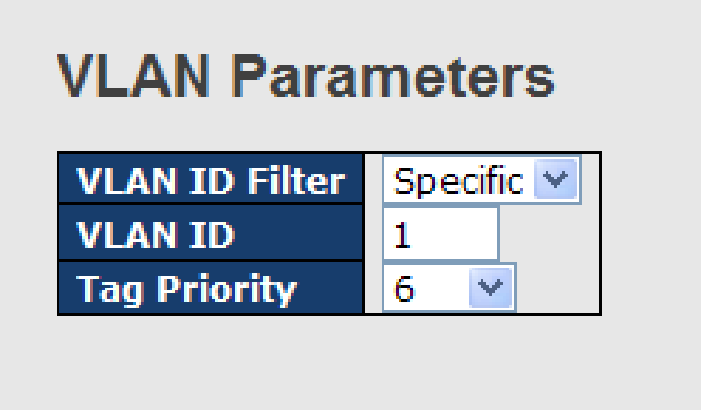

| | |
|---|---|
| **Action** | Specifies the action to take when a frame matches the ACE.<br>Permit: takes action when the frame matches the ACE.<br>Deny: drops the frame matching the ACE. |

| | |
|---|---|
| **Rate Limiter** | Specifies the rate limiter in number of base units. The allowed range is 1 to 15. **Disabled** means the rate limiter operation is disabled. |
| **Port Redirect** | Indicates the port redirect operation implemented by the ACE. Frames matching the ACE are redirected to the listed port. |
| **Port Copy** | Frames matching the ACE are copied to the port number specified here. The allowed range is the same as the switch port number range. Disabled means the port copy operation is disabled. |
| **Logging** | Specifies the logging operation of the ACE. The allowed values are:<br>**Enabled**: frames matching the ACE are stored in the system log.<br>**Disabled**: frames matching the ACE are not logged.<br>Please note that system log memory capacity and logging rate is limited. |
| **Shutdown** | Specifies the shutdown operation of the ACE. The allowed values are:<br>**Enabled**: if a frame matches the ACE, the ingress port will be disabled.<br>**Disabled**: port shutdown is disabled for the ACE. |
| **Counter** | Indicates the number of times the ACE matched by a frame. |



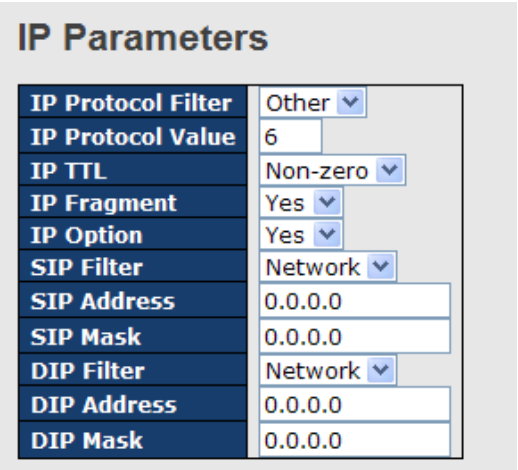

| Label | Description |
|---|---|
| **SMAC Filter** | (Only displayed when the frame type is Ethernet Type or ARP.)<br>Specifies the source MAC filter for the ACE.<br>**Any**: no SMAC filter is specified (SMAC filter status is "**don't-care**").<br>**Specific**: if you want to filter a specific source MAC address with the ACE, choose this value. A field for entering an SMAC value appears. |

| | |
|---|---|
| **SMAC Value** | When **Specific** is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". Frames matching the ACE will use this SMAC value. |
| **DMAC Filter** | Specifies the destination MAC filter for this ACE<br>**Any**: no DMAC filter is specified (DMAC filter status is "**don't-care**").<br>**MC**: frame must be multicast.<br>**BC**: frame must be broadcast.<br>**UC**: frame must be unicast.<br>**Specific**: If you want to filter a specific destination MAC address with the ACE, choose this value. A field for entering a DMAC value appears. |
| **DMAC Value** | When **Specific** is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". Frames matching the ACE will use this DMAC value. |




| Label | Description |
|---|---|
| **VLAN ID Filter** | Specifies the VLAN ID filter for the ACE<br>**Any**: no VLAN ID filter is specified (VLAN ID filter status is "**don't-care**").<br>**Specific**: if you want to filter a specific VLAN ID with the 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 |

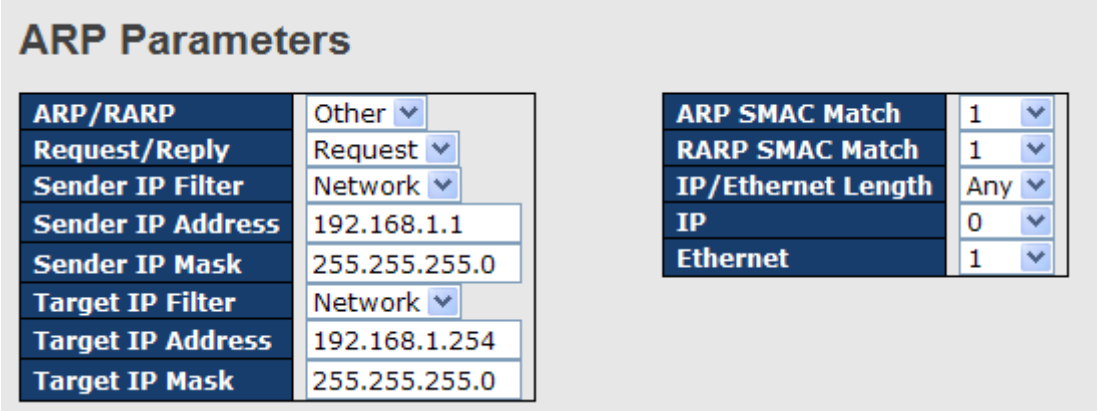
| | |
|---|---|
| | to 4095. Frames matching the ACE will use this VLAN ID value. |
| **Tag Priority** | Specifies the tag priority for the ACE. A frame matching the ACE will use this tag priority. The allowed number range is 0 to 7. **Any** means that no tag priority is specified (tag priority is "**don't-care**"). |




| Label | Description |
|---|---|
| **IP Protocol Filter** | Specifies the IP protocol filter for the ACE<br>**Any**: no IP protocol filter is specified ("**don't-care**").<br>**Specific**: if you want to filter a specific IP protocol filter with the ACE, choose this value. A field for entering an IP protocol filter appears.<br>ICMP: selects ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. For more details of these fields, please refer to the help file.<br>**UDP**: selects UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. For more details of these fields, please refer to the help file.<br>**TCP**: selects TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. For more details of these fields, please refer to the help file. |
| **IP Protocol Value** | **Specific** allows you to enter a specific value. The allowed range is 0 to 255. Frames matching the ACE will use this IP protocol value. |
| **IP TTL** | Specifies the time-to-live settings for the ACE |

| | |
|---|---|
| | **Zero**: IPv4 frames with a time-to-live value greater than zero must not be able to match this entry.<br>**Non-zero**: IPv4 frames with a time-to-live field greater than zero must be able to match this entry.<br>**Any**: any value is allowed ("**don't-care**"). |
| **IP Fragment** | Specifies the fragment offset settings for the ACE. This includes settings of More Fragments (MF) bit and Fragment Offset (FRAG OFFSET) for an IPv4 frame.<br>**No**: IPv4 frames whose MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.<br>**Yes**: IPv4 frames whose MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.<br>**Any**: any value is allowed ("**don't-care**"). |
| **IP Option** | Specifies the options flag settings for the ACE<br>**No**: IPv4 frames whose options flag is set must not be able to match this entry.<br>**Yes**: IPv4 frames whose options flag is set must be able to match this entry.<br>**Any**: any value is allowed ("**don't-care**"). |
| **SIP Filter** | Specifies the source IP filter for this ACE<br>**Any**: no source IP filter is specified (Source IP filter is "**don't-care**").<br>**Host**: source IP filter is set to **Host**. Specify the source IP address in the **SIP Address** field that appears.<br>**Network**: source IP filter is set to **Network**. Specify the source IP address and source IP mask in the **SIP Address** and **SIP Mask** fields that appear. |
| **SIP Address** | When **Host** or **Network** is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation. |
| **SIP Mask** | When **Network** is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation. |
| **DIP Filter** | Specifies the destination IP filter for the ACE<br>**Any**: no destination IP filter is specified (destination IP filter is "**don't-care**"). |

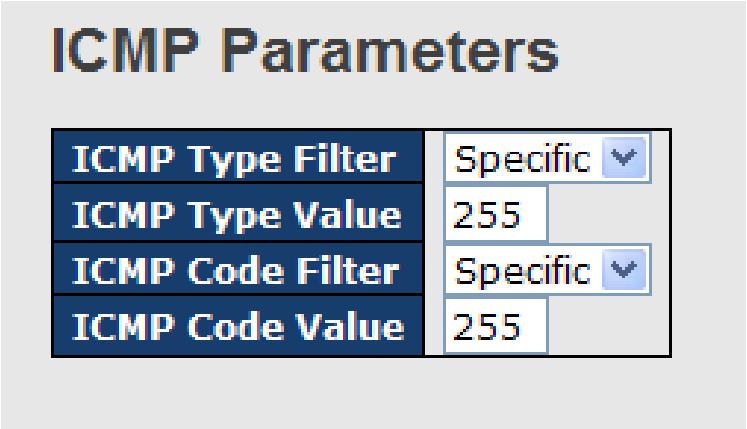
| | |
|---|---|
| | **Host**: destination IP filter is set to **Host**. Specify the destination IP address in the **DIP Address** field that appears.<br>**Network**: destination IP filter is set to **Network**. Specify the destination IP address and destination IP mask in the **DIP Address** and **DIP Mask** fields that appear. |
| **DIP Address** | When **Host** or **Network** is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation. |
| **DIP Mask** | When **Network** is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation. |



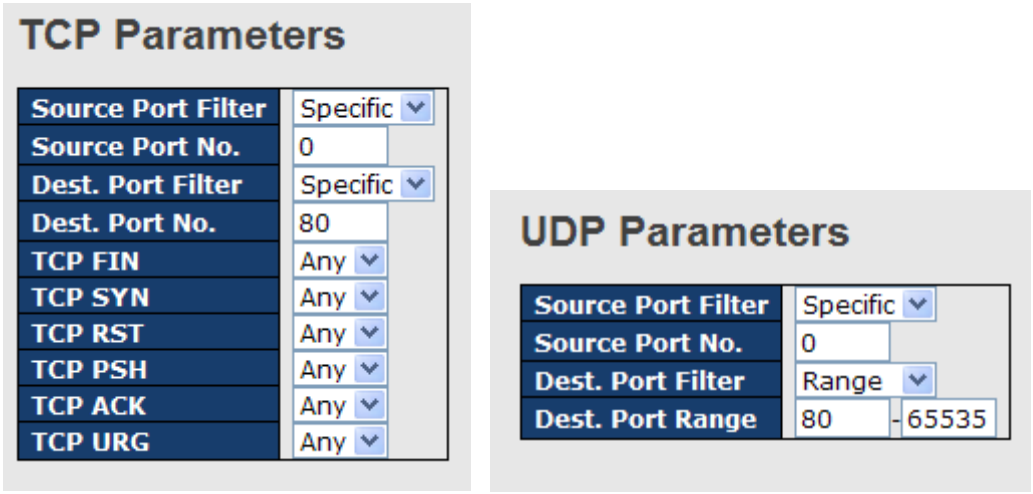

| Label | Description |
|---|---|
| **ARP/RARP** | Specifies the available ARP/RARP opcode (OP) flag for the ACE<br>**Any**: no ARP/RARP OP flag is specified (OP is "**don't-care**").<br>**ARP**: frame must have ARP/RARP opcode set to ARP<br>**RARP**: frame must have ARP/RARP opcode set to RARP.<br>**Other**: frame has unknown ARP/RARP Opcode flag. |
| **Request/Reply** | Specifies the available ARP/RARP opcode (OP) flag for the ACE<br>**Any**: no ARP/RARP OP flag is specified (OP is "**don't-care**").<br>**Request**: frame must have ARP Request or RARP Request OP flag set. |

| | |
|---|---|
| | **Reply**: frame must have ARP Reply or RARP Reply OP flag. |
| **Sender IP Filter** | Specifies the sender IP filter for the ACE<br>**Any**: no sender IP filter is specified (sender IP filter is "**don't-care**").<br>**Host**: sender IP filter is set to **Host**. Specify the sender IP address in the **SIP Address** field that appears.<br>**Network**: sender IP filter is set to **Network**. Specify the sender IP address and sender IP mask in the **SIP Address** and **SIP Mask** fields that appear. |
| **Sender IP Address** | When Host or Network is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation. |
| **Sender IP Mask** | When Network is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation. |
| **Target IP Filter** | Specifies the target IP filter for the specific ACE<br>**Any**: no target IP filter is specified (target IP filter is "**don't-care**").<br>**Host**: target IP filter is set to **Host**. Specify the target IP address in the **Target IP Address** field that appears.<br>**Network**: target IP filter is set to **Network**. Specify the target IP address and target IP mask in the **Target IP Address** and **Target IP Mask** fields that appear. |
| **Target IP Address** | When **Host** or **Network** is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation. |
| **Target IP Mask** | When **Network** is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation. |
| **ARP SMAC Match** | Specifies whether frames will meet the action according to their sender hardware address field (SHA) settings.<br>**0**: ARP frames where SHA is not equal to the SMAC address<br>**1**: ARP frames where SHA is equal to the SMAC address<br>**Any**: any value is allowed ("**don't-care**"). |
| **RARP SMAC Match** | Specifies whether frames will meet the action according to their target hardware address field (THA) settings. |

| | |
|---|---|
| | **0**: RARP frames where THA is not equal to the SMAC address<br>**1**: RARP frames where THA is equal to the SMAC address<br>**Any**: any value is allowed ("**don't-care**") |
| **IP/Ethernet Length** | Specifies whether frames will meet the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.<br>**0**: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must not match this entry.<br>**1**: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must match this entry.<br>**Any**: any value is allowed ("**don't-care**"). |
| **IP** | Specifies whether frames will meet the action according to their ARP/RARP hardware address space (HRD) settings.<br>**0**: ARP/RARP frames where the HLD is equal to Ethernet (1) must not match this entry.<br>**1**: ARP/RARP frames where the HLD is equal to Ethernet (1) must match this entry.<br>**Any**: any value is allowed ("**don't-care**"). |
| **Ethernet** | Specifies whether frames will meet the action according to their ARP/RARP protocol address space (PRO) settings.<br>**0**: ARP/RARP frames where the PRO is equal to IP (0x800) must not match this entry.<br>**1**: ARP/RARP frames where the PRO is equal to IP (0x800) must match this entry.<br>**Any**: any value is allowed ("**don't-care**"). |




| Label | Description |
|---|---|
| **ICMP Type Filter** | Specifies the ICMP filter for the ACE<br>**Any**: no ICMP filter is specified (ICMP filter status is "**don't-care**").<br>**Specific**: if you want to filter a specific ICMP filter with the ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears. |
| **ICMP Type Value** | When **Specific** is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is 0 to 255. A frame matching the ACE will use this ICMP value. |
| **ICMP Code Filter** | Specifies the ICMP code filter for the ACE<br>**Any**: no ICMP code filter is specified (ICMP code filter status is "**don't-care**").<br>**Specific**: if you want to filter a specific ICMP code filter with the ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears. |
| **ICMP Code Value** | When **Specific** is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is 0 to 255. A frame matching the ACE will use this ICMP code value. |




| Label | Description |
|---|---|
| **TCP/UDP Source Filter** | Specifies the TCP/UDP source filter for the ACE<br>**Any**: no TCP/UDP source filter is specified (TCP/UDP source filter status is "**don't-care**").<br>**Specific**: if you want to filter a specific TCP/UDP source filter with the ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.<br>**Range**: if you want to filter a specific TCP/UDP source range filter with the ACE, you can enter a specific TCP/UDP source range. A field for entering a TCP/UDP source value appears. |
| **TCP/UDP Source No.** | When **Specific** is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame matching the ACE will use this TCP/UDP source value. |
| **TCP/UDP Source Range** | When **Range** is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame matching the ACE will use this TCP/UDP source value. |
| **TCP/UDP Destination Filter** | Specifies the TCP/UDP destination filter for the ACE<br>**Any**: no TCP/UDP destination filter is specified (TCP/UDP destination filter status is "**don't-care**").<br>**Specific**: if you want to filter a specific TCP/UDP destination filter with the ACE, you can enter a specific |

| | |
|---|---|
| | TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.<br>**Range**: if you want to filter a specific range TCP/UDP destination filter with the ACE, you can enter a specific TCP/UDP destination range. A field for entering a TCP/UDP destination value appears. |
| **TCP/UDP Destination Number** | When **Specific** is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame matching the ACE will use this TCP/UDP destination value. |
| **TCP/UDP Destination Range** | When **Range** is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame matching the ACE will use this TCP/UDP destination value. |
| **TCP FIN** | Specifies the TCP FIN ("no more data from sender") value for the ACE.<br>**0**: TCP frames where the FIN field is set must not be able to match this entry.<br>**1**: TCP frames where the FIN field is set must be able to match this entry.<br>**Any**: any value is allowed ("**don't-care**"). |
| **TCP SYN** | Specifies the TCP SYN ("synchronize sequence numbers") value for the ACE<br>**0**: TCP frames where the SYN field is set must not be able to match this entry.<br>**1**: TCP frames where the SYN field is set must be able to match this entry.<br>**Any**: any value is allowed ("**don't-care**"). |
| **TCP PSH** | Specifies the TCP PSH ("push function") value for the ACE<br>**0**: TCP frames where the PSH field is set must not be able to match this entry.<br>**1**: TCP frames where the PSH field is set must be able to match this entry.<br>**Any**: any value is allowed ("**don't-care**"). |
| **TCP ACK** | Specifies the TCP ACK ("acknowledgment field significant") value for the ACE |

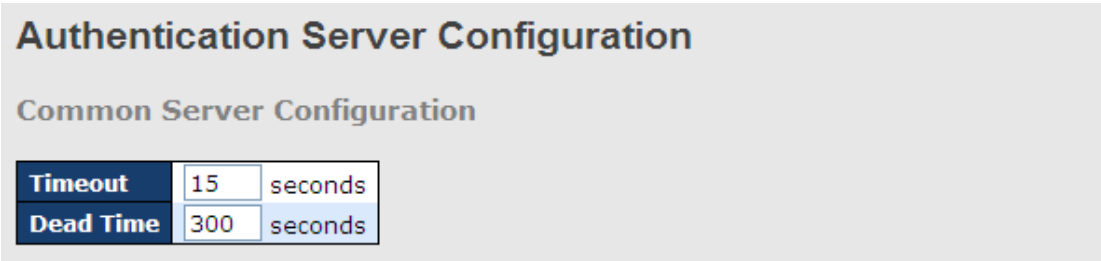
| | |
|---|---|
| | **0**: TCP frames where the ACK field is set must not be able to match this entry.<br>**1**: TCP frames where the ACK field is set must be able to match this entry.<br>**Any**: any value is allowed ("**don't-care**"). |
| **TCP URG** | Specifies the TCP URG ("urgent pointer field significant") value for the ACE<br>**0**: TCP frames where the URG field is set must not be able to match this entry.<br>**1**: TCP frames where the URG field is set must be able to match this entry.<br>**Any**: any value is allowed ("**don't-care**"). |

## 5.8.4 AAA

An AAA server is an application that provides authentication, authorization, and accounting services for attempted access to a network. An AAA server can reside in a dedicated computer, an Ethernet switch, an access point or a network access server. The current standard by which devices or applications communicate with an AAA server is RADIUS (Remote Authentication Dial-In User Service). RADIUS is a protocol used between the switch and the authentication server. This page allows you to configure common settings for an authentication server.

### 5.8.4.1 Configurations

This page allows you to configure 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.<br>If the server does not reply within this time frame, we will consider it to be dead and continue with the next enabled |

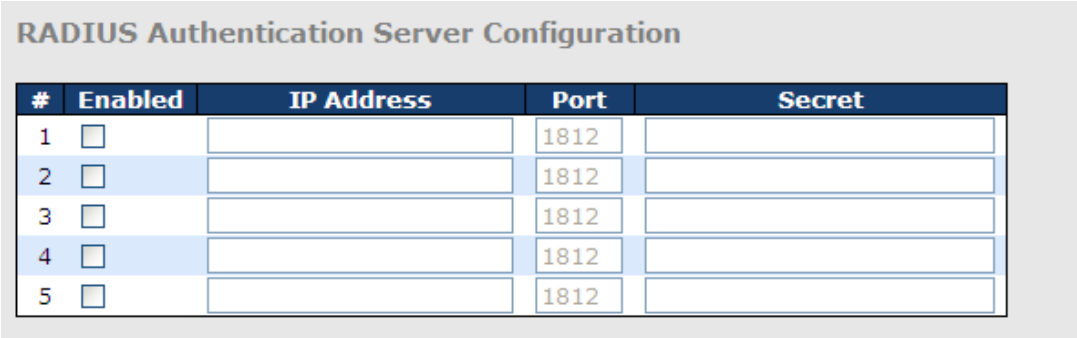
| | |
|---|---|
| | server (if any).<br><br>RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. 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.<br>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. |

### 5.8.4.2 RADIUS Overview

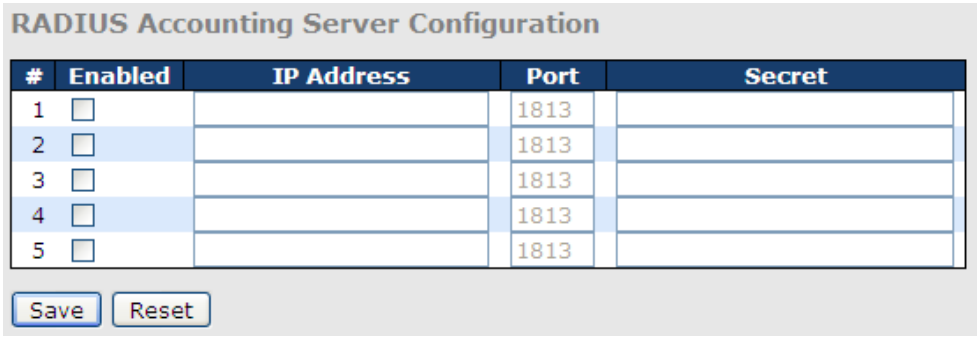
#### Authentication and Accounting Server Configurations

When a user requests network connection, a RADIUS client which receives the request will perform an initial access negotiation with the user to obtain identity/password information. The client then passes the information to a RADIUS server as part of an authentication/authorization request.

The RADIUS server matches data from the authentication/authorization request with information in a trusted database. If a match is found and the user's credentials are correct, the RADIUS server sends an accept message to the client to grant access. If a match is not found or a problem is found with the user's credentials, the server returns a reject message to deny access. The NAD then establishes or terminates the user's connection. The NAD may then forward accounting information to the RADIUS server to document the transaction; the RADIUS server may store or forward this information as needed to support billing for the services provided.

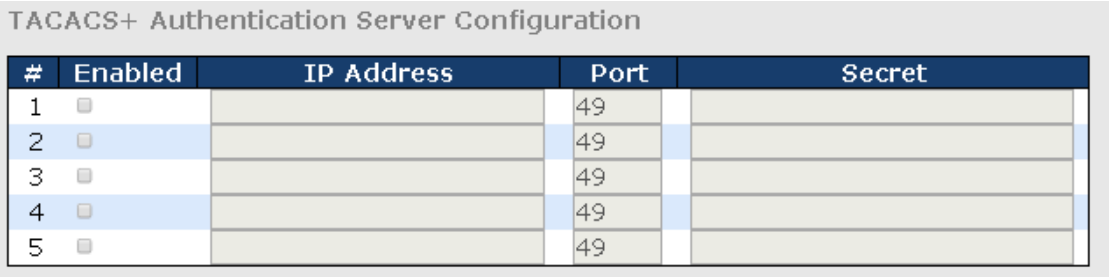



| Label | Description |
|---|---|
| # | The RADIUS authentication server number for which the configuration below applies. |
| **Enabled** | Check to enable the RADIUS authentication server. |
| **IP Address** | The IP address or hostname of the RADIUS authentication server. IP address is expressed in 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. |




| Label | Description |
|---|---|
| # | The RADIUS accounting server number for which the configuration below applies. |
| **Enabled** | Check to enable the RADIUS accounting server |
| **IP Address** | The IP address or hostname of the RADIUS accounting server. IP address is expressed in dotted decimal notation. |

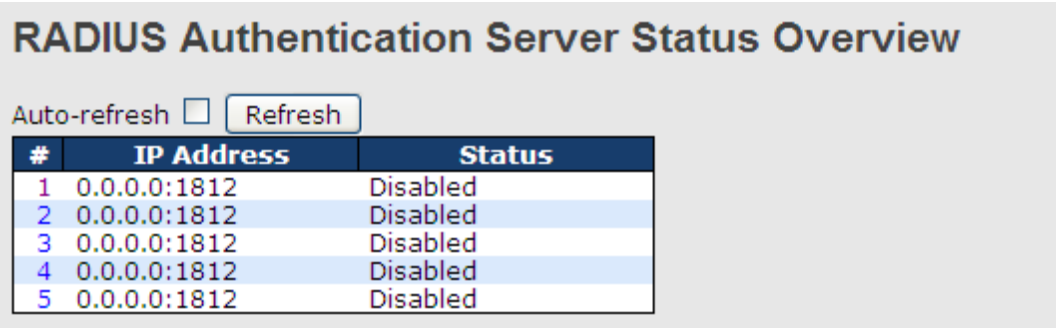
| | |
|---|---|
| **Port** | The UDP port to use on the RADIUS accounting server. If the port is set to **0** (zero), the default port (1813) is used on the RADIUS accounting server. |
| **Secret** | The secret - up to 29 characters long - shared between the RADIUS accounting server and the switch stack. |



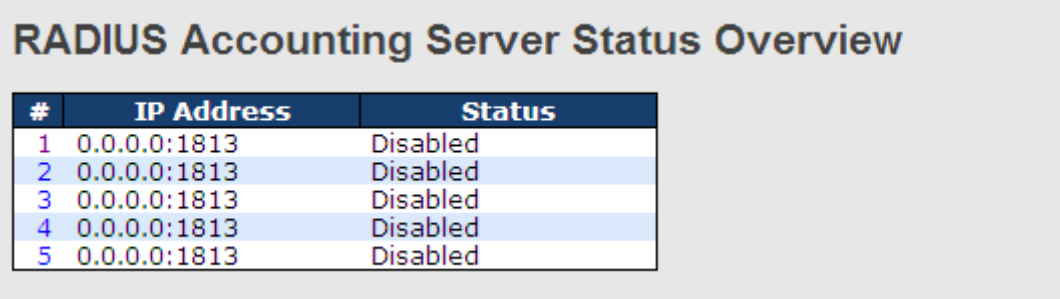

| Label | Description |
|---|---|
| # | The TACACS+ authentication server number for which the configuration below applies. |
| **Enabled** | Check to enable the TACACS+ authentication server |
| **IP Address** | The IP address or hostname of the TACACS+ authentication server. IP address is expressed in dotted decimal notation. |
| **Port** | The UDP port to use on the TACACS+ authentication server. If the port is set to **0** (zero), the default port (49) is used on the RADIUS accounting server. |
| **Secret** | The secret - up to 29 characters long - shared between the TACACS+ authentication server and the switch stack. |

## Authentication and Accounting Server Status Overview

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



| Label | Description |
|---|---|
| # | The RADIUS server number. Click to navigate to detailed statistics of the server |
| **IP Address** | The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of the server |
| **Status** | The current status of the server. This field has one of the following values:<br>**Disabled**: the server is disabled.<br>**Not Ready**: the server is enabled, but IP communication is not yet up and running.<br>**Ready**: the server is enabled, IP communications are built, and the RADIUS module is ready to accept access attempts.<br>**Dead** (X seconds left): access attempts are made to this server, but it does not reply within the configured timeout. The server has temporarily been disabled, but will be 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. |



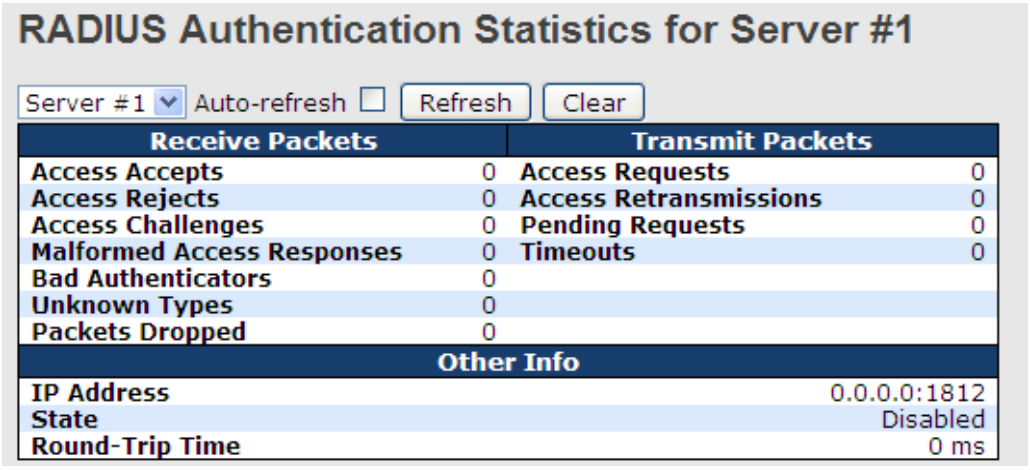

| Label | Description |
|---|---|
| # | The RADIUS server number. Click to navigate to detailed statistics of the server |
| **IP Address** | The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of the server |
| **Status** | The current status of the server. This field has one of the following values:<br>Disabled: the server is disabled. |

| | |
|---|---|
| | **Not Ready**: the server is enabled, but IP communication is not yet up and running.<br>**Ready**: the server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.<br>**Dead (X seconds left)**: accounting attempts are made to this server, but it does not reply within the configured timeout. The server has temporarily been disabled, but will be 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. |

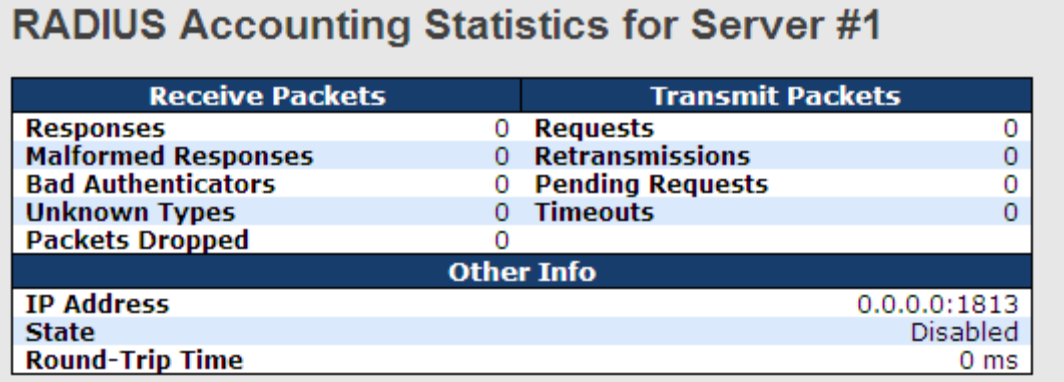
### 5.8.4.3 RADIUS Details

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

Use the server drop-down list to switch between the backend servers to show related details.



<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td>Packet Counters</td><td>RADIUS authentication server packet counters. There are seven ‘receive’ and four ‘transmit’ counters.
<table>
<tr><th>Direction</th><th>Name</th><th>RFC4668 Name</th><th>Description</th></tr>
<tr><td>Rx</td><td>Access Accepts</td><td>radiusAuthClientExtAccessAccepts</td><td>The number of RADIUS Access-Accept packets (valid or invalid) received from the server.</td></tr>
<tr><td>Rx</td><td>Access Rejects</td><td>radiusAuthClientExtAccessRejects</td><td>The number of RADIUS Access-Reject packets (valid or invalid) received from the server.</td></tr>
<tr><td>Rx</td><td>Access Challenges</td><td>radiusAuthClientExtAccessChallenges</td><td>The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.</td></tr>
<tr><td>Rx</td><td>Malformed Access Responses</td><td>radiusAuthClientExtMalformedAccessResponses</td><td>The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.</td></tr>
<tr><td>Rx</td><td>Bad Authenticators</td><td>radiusAuthClientExtBadAuthenticators</td><td>The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.</td></tr>
<tr><td>Rx</td><td>Unknown Types</td><td>radiusAuthClientExtUnknownTypes</td><td>The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.</td></tr>
<tr><td>Rx</td><td>Packets Dropped</td><td>radiusAuthClientExtPacketsDropped</td><td>The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.</td></tr>
<tr><td>Tx</td><td>Access Requests</td><td>radiusAuthClientExtAccessRequests</td><td>The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.</td></tr>
<tr><td>Tx</td><td>Access Retransmissions</td><td>radiusAuthClientExtAccessRetransmissions</td><td>The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.</td></tr>
<tr><td>Tx</td><td>Pending Requests</td><td>radiusAuthClientExtPendingRequests</td><td>The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.</td></tr>
<tr><td>Tx</td><td>Timeouts</td><td>radiusAuthClientExtTimeouts</td><td>The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.</td></tr>
</table></td></tr>
<tr><td>Other Info</td><td>This section contains information about the state of the server and the latest round-trip time.
<table>
<tr><th>Name</th><th>RFC4668 Name</th><th>Description</th></tr>
<tr><td>State</td><td>-</td><td>Shows the state of the server. It takes one of the following values:<br><code>Disabled</code> : The selected server is disabled.<br><code>Not Ready</code> : The server is enabled, but IP communication is not yet up and running.<br><code>Ready</code> : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.<br><code>Dead (X seconds left)</code> : Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.</td></tr>
<tr><td>Round-Trip Time</td><td>radiusAuthClientExtRoundTripTime</td><td>The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.</td></tr>
</table></td></tr>
</table>



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

## 5.8.5 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 does not require the users to have special 802.1X software installed on their system. The switch uses the users' MAC addresses to authenticate against the backend server. As intruders can create counterfeit MAC addresses, MAC-based authentication is less secure than 802.1X authentication.

### Overview of 802.1X (Port-Based) Authentication

In an 802.1X network environment, 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 which 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 as it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) does not 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 the result to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note: in an environment where two backend servers are enabled, the server timeout is configured to X seconds (using the authentication configuration page), and the first server in the list is currently down (but not considered dead), if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, it will never be authenticated because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. Since the server has not failed (because the X seconds have not expired), the same server will be contacted when the next backend authentication server requests 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 in 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

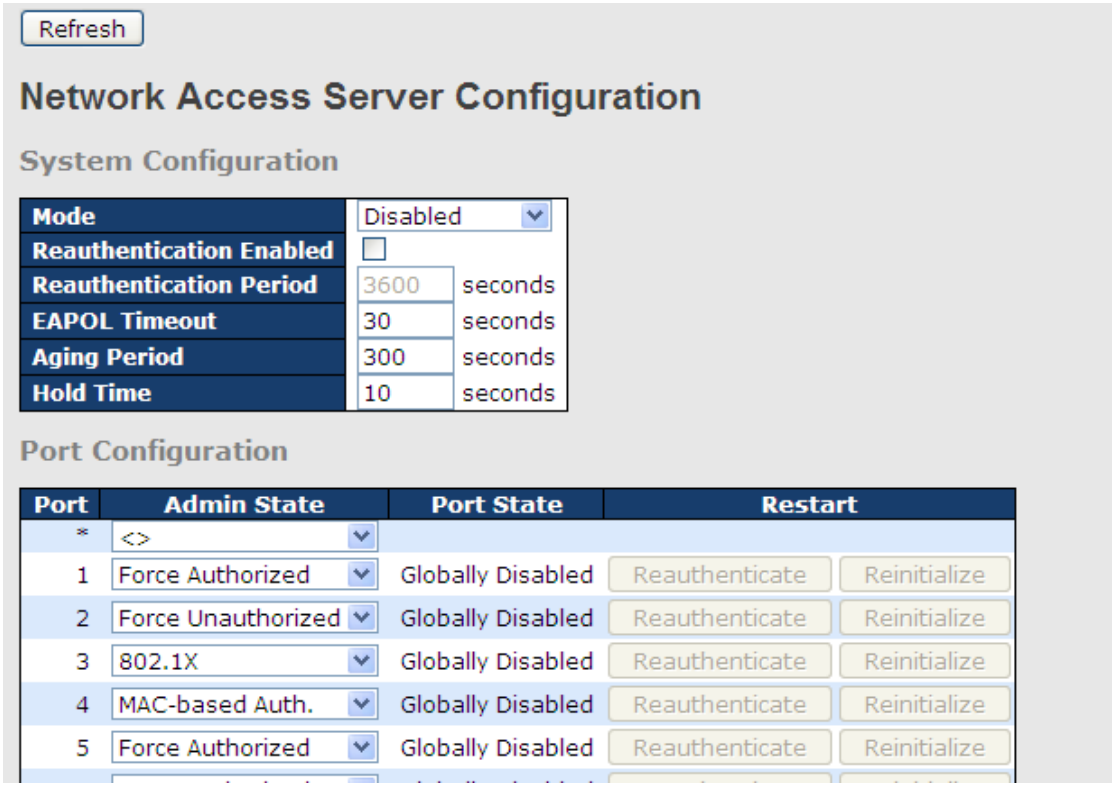
configured accordingly.

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 do npt 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.

802.1X and MAC-Based authentication configurations consist of two sections: system- and port-wide.

### 5.8.5.1 Configuration



| 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 to forward 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.<br>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 does not 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 re-authenticated. This is only active if the **Reauthentication Enabled** checkbox is checked. Valid range of the value is 1 to 3600 seconds. |
| **EAPOL Timeout** | Determines the time for retransmission of Request Identity EAPOL frames.<br>Valid range of the value is 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:<br>**MAC-Based Auth**.:<br>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.<br>For ports in **MAC-based Auth.** mode, reauthentication does not cause direct communications 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:<br>**MAC-Based Auth**.:<br>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 Unauthorized state. The hold timer does not count during an on-going authentication.<br>The switch will ignore new frames coming from the client during the hold time.<br>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:<br><br>**Force Authorized**<br>In this mode, the switch will send one EAPOL Success frame when the port link is up, and any client on the port will be allowed network access without authentication.<br>**Force Unauthorized**<br>In this mode, the switch will send one EAPOL Failure frame when the port link is up, and any client on the port will be disallowed network access.<br>**Port-based 802.1X**<br>In an 802.1X network environment, 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 which encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server is 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 as it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) does not 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.<br>When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding the result to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.<br>Note: in an environment where two backend servers are enabled, the server timeout is configured to X seconds (using the authentication configuration page), and the first server in the list is currently down (but not considered dead), if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, it will never be authenticated because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. Since the server has not failed (because the X seconds have not expired), the same server will be contacted when 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.<br>**a. 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 are not authenticated individually. To overcome this security breach, use the Single 802.1X variant.<br>Single 802.1X is not yet an IEEE standard, but features many of the same characteristics as 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 communications between the supplicant and the switch. If more than one supplicant are connected to a port, the one that comes first when the port's link is connected will be the first one considered. If that supplicant does not provide valid credentials within a certain amount of time, the chance will be given to another supplicant. 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.<br>**b. Multi 802.1X**<br>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 are not authenticated individually. To overcome this security breach, use the Multi 802.1X variant.<br>Multi 802.1X is not yet an IEEE standard, but features many of the same characteristics as port-based 802.1X. In Multi 802.1X, one or more supplicants can be authenticated on the same port at the same time. Each |

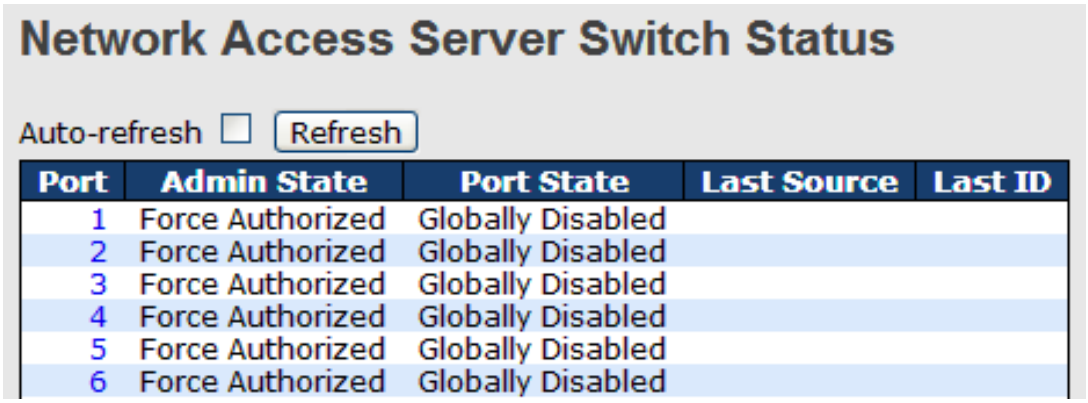
| | |
|---|---|
| | supplicant is authenticated individually and secured in the MAC table using the Port Security module.<br>In Multi 802.1X it is not possible to use the multicast BPDU MAC address as the destination MAC address for EAPOL frames sent from the switch to the supplicant, since that would 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.<br>The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.<br>**MAC-based Auth.**<br>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 in 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.<br>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.<br>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 do not 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:<br>**Globally Disabled**: NAS is globally disabled.<br>**Link Down**: NAS is globally enabled, but there is no link on the port.<br>**Authorized**: the port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.<br>**Unauthorized:** the port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.<br>**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.<br>Clicking these buttons will not cause settings changed on the page to take effect.<br>**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.<br>The button only has effect on successfully authenticated clients on the port and will not cause the clients to be temporarily unauthorized.<br>**Reinitialize**: forces a reinitialization of the clients on the port and hence a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress. |

### 5.8.5.2 Switch

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

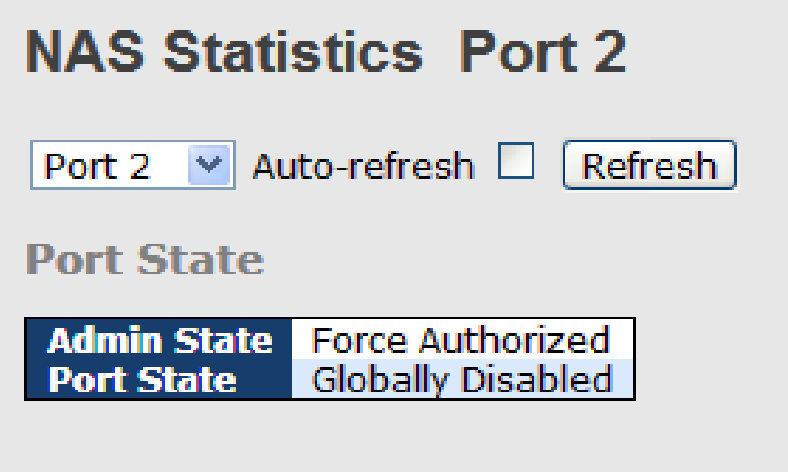



| Label | Description |
|---|---|
| **Port** | The switch port number. Click to navigate to detailed 802.1X statistics of each port. |
| **Admin State** | The port's current administrative state. Refer to **NAS Admin State** for more details regarding each value. |
| **Port State** | The current state of the port. Refer to **NAS Port State** for more details regarding each value. |
| **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. |

### 5.8.5.3 Port

This page provides detailed IEEE 802.1X statistics for a specific switch port using port-based authentication. For MAC-based ports, only selected backend server (RADIUS Authentication Server) statistics is showed. Use the port drop-down list to select which port details to be displayed.



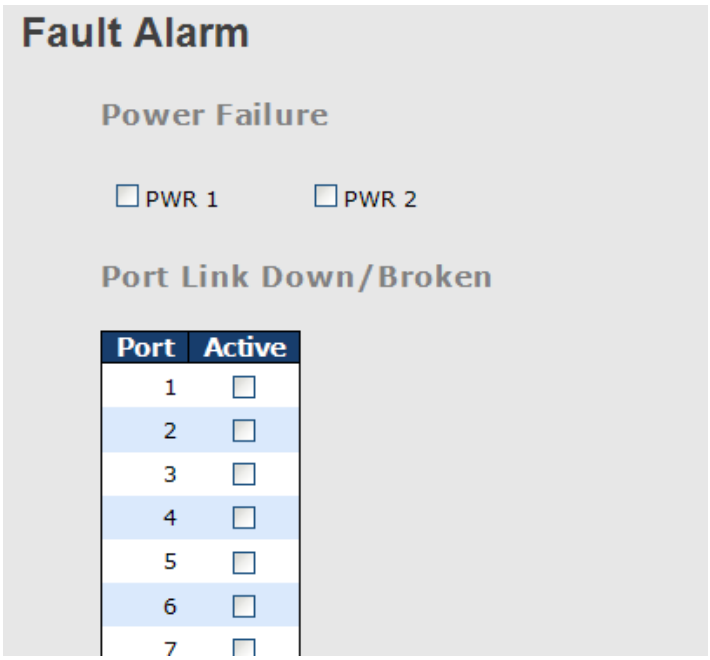

| Label | Description |
|---|---|
| **Admin State** | The port's current administrative state. Refer to **NAS Admin State** for more details regarding each value. |
| **Port State** | The current state of the port. Refer to **NAS Port State** for more details regarding each value. |
| **EAPOL Counters** | These supplicant frame counters are available for the following administrative states:<br>• **Force Authorized**<br>• **Force Unauthorized**<br>• 802.1X |

| | |
|---|---|
| | **EAPOL Counters**<br>Direction / Name / IEEE Name / Description<br>Rx / **Total** / dot1xAuthEapolFramesRx / The number of valid EAPOL frames of any type that have been received by the switch.<br>Rx / **Response ID** / dot1xAuthEapolRespIdFramesRx / The number of valid EAP Resp/ID frames that have been received by the switch.<br>Rx / **Responses** / dot1xAuthEapolRespFramesRx / The number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch.<br>Rx / **Start** / dot1xAuthEapolStartFramesRx / The number of EAPOL Start frames that have been received by the switch.<br>Rx / **Logoff** / dot1xAuthEapolLogoffFramesRx / The number of valid EAPOL logoff frames that have been received by the switch.<br>Rx / **Invalid Type** / dot1xAuthInvalidEapolFramesRx / The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.<br>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.<br>Tx / **Total** / dot1xAuthEapolFramesTx / The number of EAPOL frames of any type that have been transmitted by the switch.<br>Tx / **Request ID** / dot1xAuthEapolReqIdFramesTx / The number of EAP initial request frames that have been transmitted by the switch.<br>Tx / **Requests** / dot1xAuthEapolReqFramesTx / The number of valid EAP Request frames (other than initial request frames) that have been transmitted by the switch. |
| **Backend Server Counters** | These backend (RADIUS) frame counters are available for the following administrative states:<br>• **802.1X**<br>• **MAC-based Auth.**<br>**Backend Server Counters**<br>Direction / Name / IEEE Name / Description<br>Rx / **Access Challenges** / dot1xAuthBackendAccessChallenges / **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).<br>Rx / **Other Requests** / dot1xAuthBackendOtherRequestsToSupplicant / **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.<br>Rx / **Auth. Successes** / dot1xAuthBackendAuthSuccesses / **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.<br>Rx / **Auth. Failures** / dot1xAuthBackendAuthFails / **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.<br>Tx / **Responses** / dot1xAuthBackendResponses / **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. |
| **Last Supplicant/Client Info** | Information about the last supplicant/client that attempts to authenticate. This information is available for the following administrative states:<br>• **802.1X**<br>• **MAC-based Auth.**<br>**Last Supplicant/Client Info**<br>Name / IEEE Name / Description<br>**MAC Address** / dot1xAuthLastEapolFrameSource / The MAC address of the last supplicant/client.<br>**VLAN ID** / - / The VLAN ID on which the last frame from the last supplicant/client was received.<br>**Version** / dot1xAuthLastEapolFrameVersion / **802.1X-based**: The protocol version number carried in the most recently received EAPOL frame. **MAC-based**: Not applicable.<br>**Identity** / - / **802.1X-based**: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. **MAC-based**: Not applicable. |

# 5.9 Warning

## 5.9.1 Fault Alarm

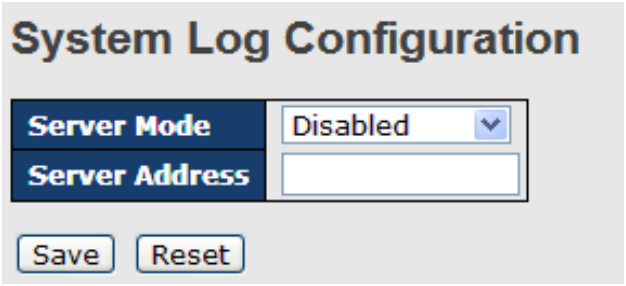
When any selected fault event happens, the Fault LED on the switch panel will light up and the electric relay will signal at the same time.




## 5.9.2 System Warning

### 5.9.2.1 SYSLOG Setting

The SYSLOG is a protocol that transmits event notifications across networks. For more details, please refer to RFC 3164 - The BSD SYSLOG Protocol.

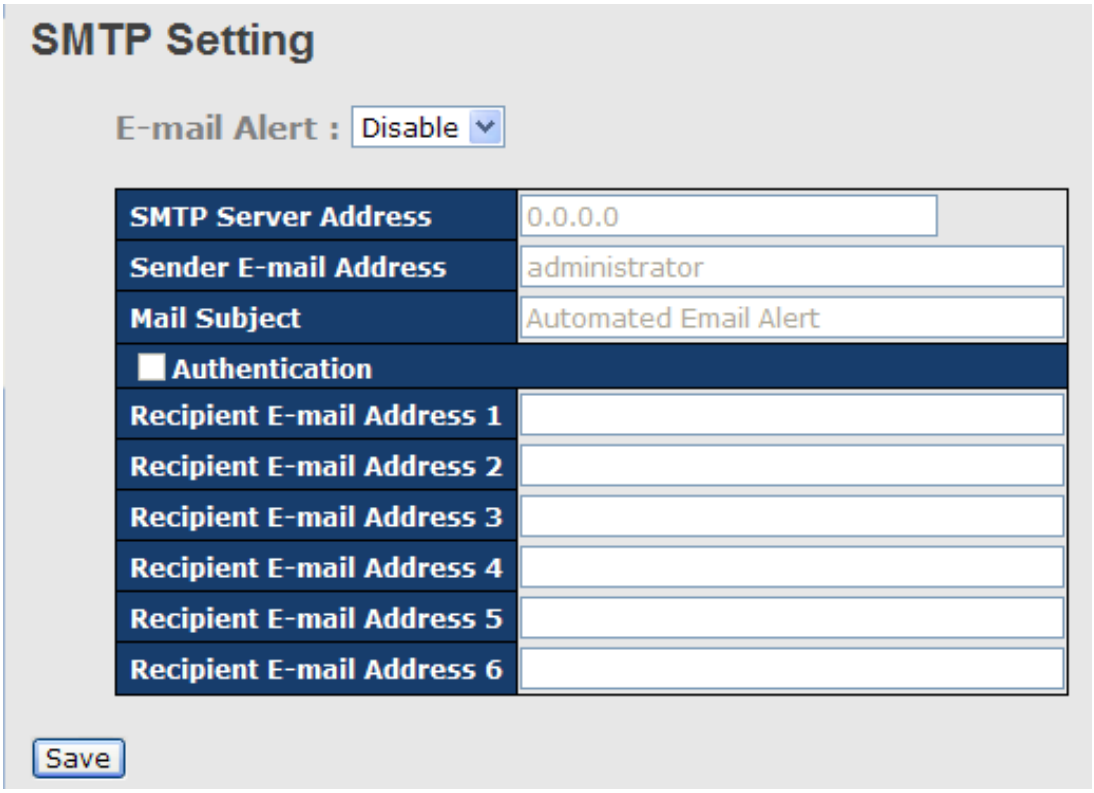



| Label | Description |
|---|---|
| Server Mode | Indicates existing server mode. When the mode |

| | |
|---|---|
| | operation is enabled, the syslog message will be sent to syslog server. The syslog protocol is based on UDP communications and received on UDP port 514 and the syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always be sent even if the syslog server does not exist. Possible modes are:<br>**Enabled**: enable server mode<br>**Disabled**: disable server mode |
| **SYSLOG Server IP Address** | Indicates the IPv4 host address of syslog server. If the switch provides DNS functions, it also can be a host name. |

### 5.9.2.2 SMTP Setting

SMTP (Simple Mail Transfer Protocol) is a protocol for transmitting e-mails across the Internet. For more information, please refer to RFC 821 - Simple Mail Transfer Protocol.

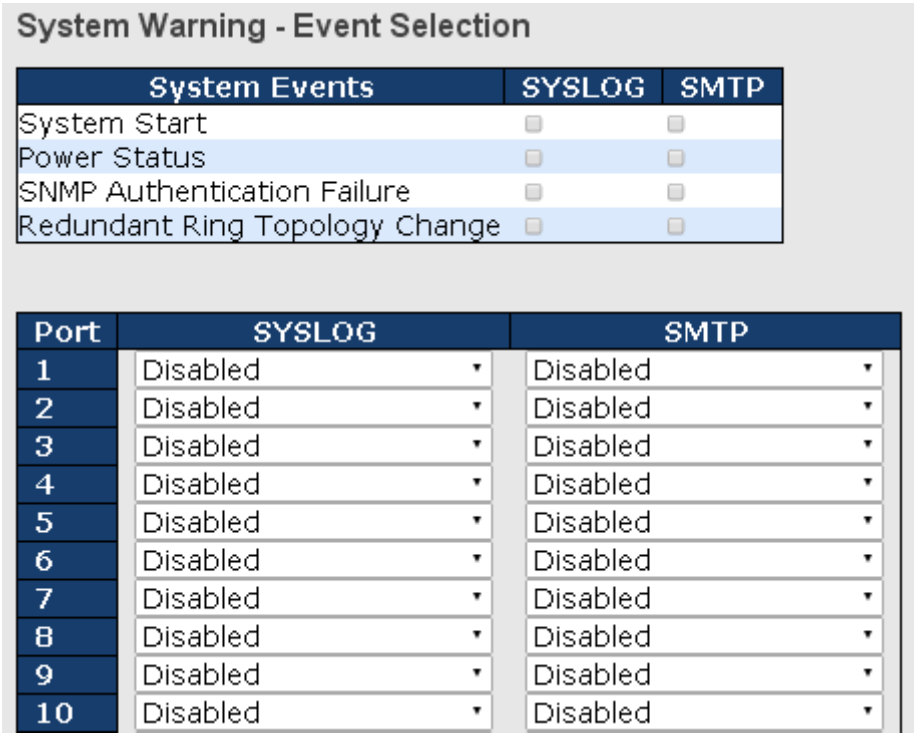



| Label | Description |
|---|---|
| **E-mail Alarm** | Enables or disables transmission of system warnings |

| | |
|---|---|
| | by e-mail |
| **Sender E-mail Address** | SMTP server IP address |
| **Mail Subject** | Subject of the mail |
| **Authentication** | ■ **Username:** the authentication username<br>■ **Password:** the authentication password<br>■ **Confirm Password:** re-enter password |
| **Recipient E-mail Address** | The recipient's e-mail address. A mail allows for 6 recipients. |
| **Apply** | Click to activate the configurations |
| **Help** | Shows help file |

### 5.9.2.3 Event Selection

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




| Label | Description |
|---|---|
| **System Cold Start** | Sends out alerts when the system is restarted |
| **Power Status** | Sends out alerts when power is up or down |
| **SNMP Authentication Failure** | Sends out alert when SNMP authentication fails |

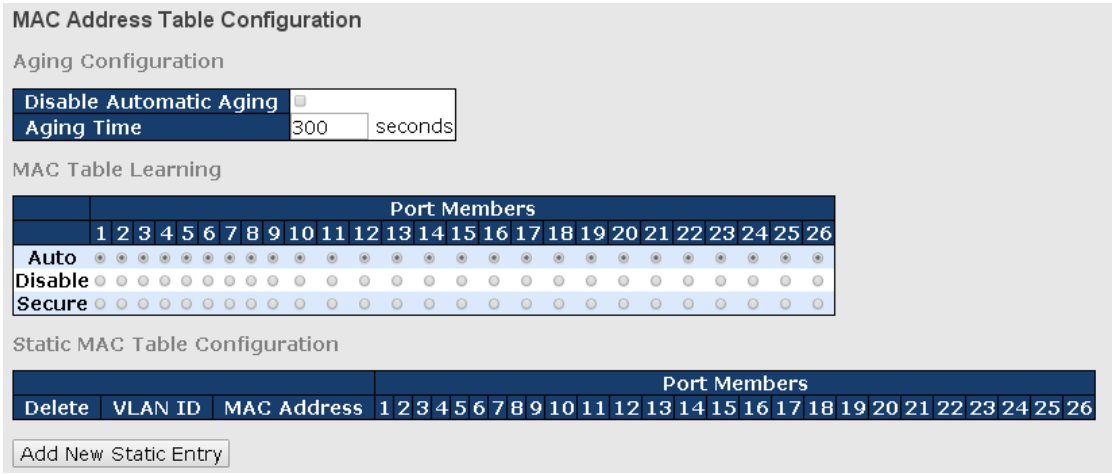
| | |
|---|---|
| **O-Ring Topology Change** | Sends out alerts when O-Ring topology changes |
| **Port Event**<br>**SYSLOG / SMTP event** | ■ Disable<br>■ Link Up<br>■ Link Down<br>■ Link Up & Link Down |
| **Apply** | Click to activate the configurations |
| **Help** | Shows help file |

# 5.10 Monitor and Diag

## 5.10.1 MAC Table

### 5.10.1.1 MAC Address Table Configuration

The MAC address table can be configured on this page. You can set timeouts for entries in the dynamic MAC table and configure the static MAC table here.




#### Aging Configuration

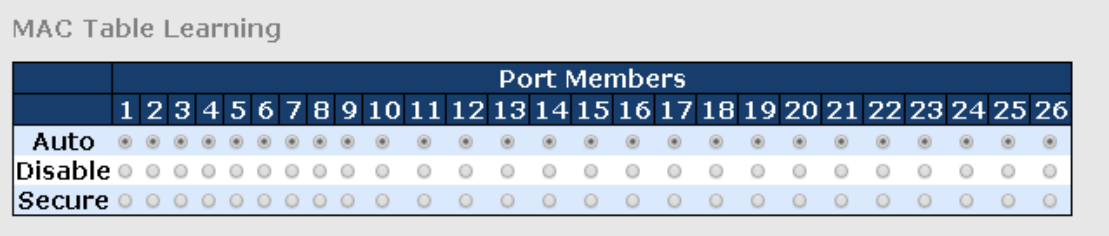
By default, dynamic entries are removed from the MAC after 300 seconds. This removal is called aging. You can configure aging time by entering a value in the box of **Age Time**. The allowed range is 10 to 1000000 seconds. You can also disable the automatic aging of dynamic entries by checking **Disable Automatic Aging**.

#### MAC Table Learning

If the learning mode for a given port is grayed out, it means another module is in control of the mode, and thus the user cannot change the configurations. An example of such a module is MAC-Based authentication under 802.1X.

You can configure the port to dynamically learn the MAC address based upon the following

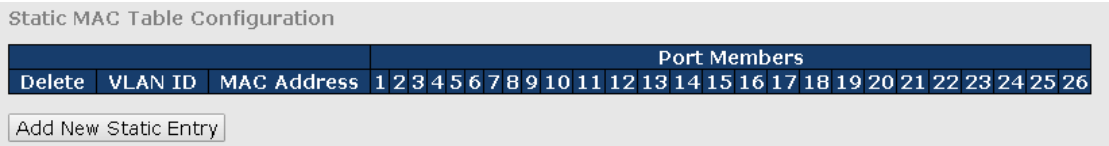
settings:




| 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.<br>Note: make sure the link used for managing the switch is added to the static Mac table before changing to secure learning mode, otherwise the management link will be 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 Configurations

The static entries in the MAC table are shown in this table. The static MAC table can contain up to 64 entries. The entries are for the whole stack, not for individual switches. The MAC table is sorted first by VLAN ID and then by MAC address.




| Label | Description |
|---|---|
| **Delete** | Check to delete an 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 to modify the entry. |
| **Adding New Static Entry** | Click to add a new entry to the static MAC table. You can |

| | |
|---|---|
| | specify the VLAN ID, MAC address, and port members for the new entry. Click **Save** to save the changes. |

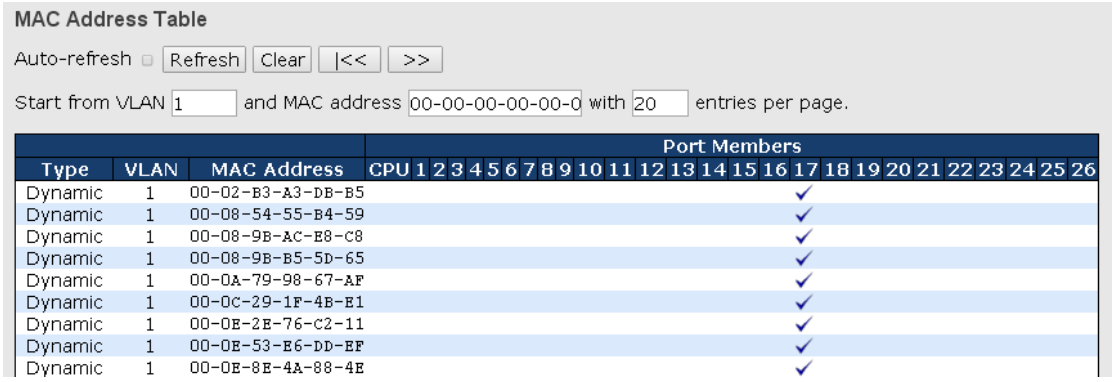
### 5.10.1.2 MAC Table

Each page shows up to 999 entries from the MAC table, with a default value of 20, selected by 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.

Each page shows up to 999 entries from the MAC table, with a default value of 20, selected by 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** 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 clicking **Refresh** - assume the value of the first displayed entry, allows 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 it reaches the end, the text "**no more entries**" is shown in the displayed table. Use the **|<<** button to start over.

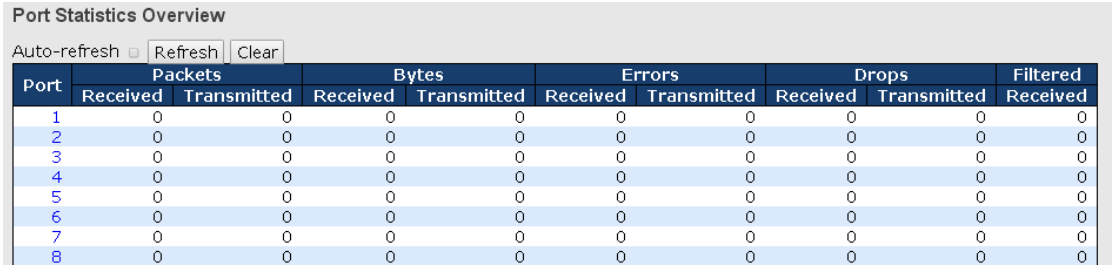



| Label | Description |
|---|---|
| **Type** | Indicates whether the entry is a static or dynamic entry |
| **MAC address** | The MAC address of the entry |
| **VLAN** | The VLAN ID of the entry |
| **Port Members** | The ports that are members of the entry. |

# 5.10.2 Port Statistics

## 5.10.2.1 Traffic Overview

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



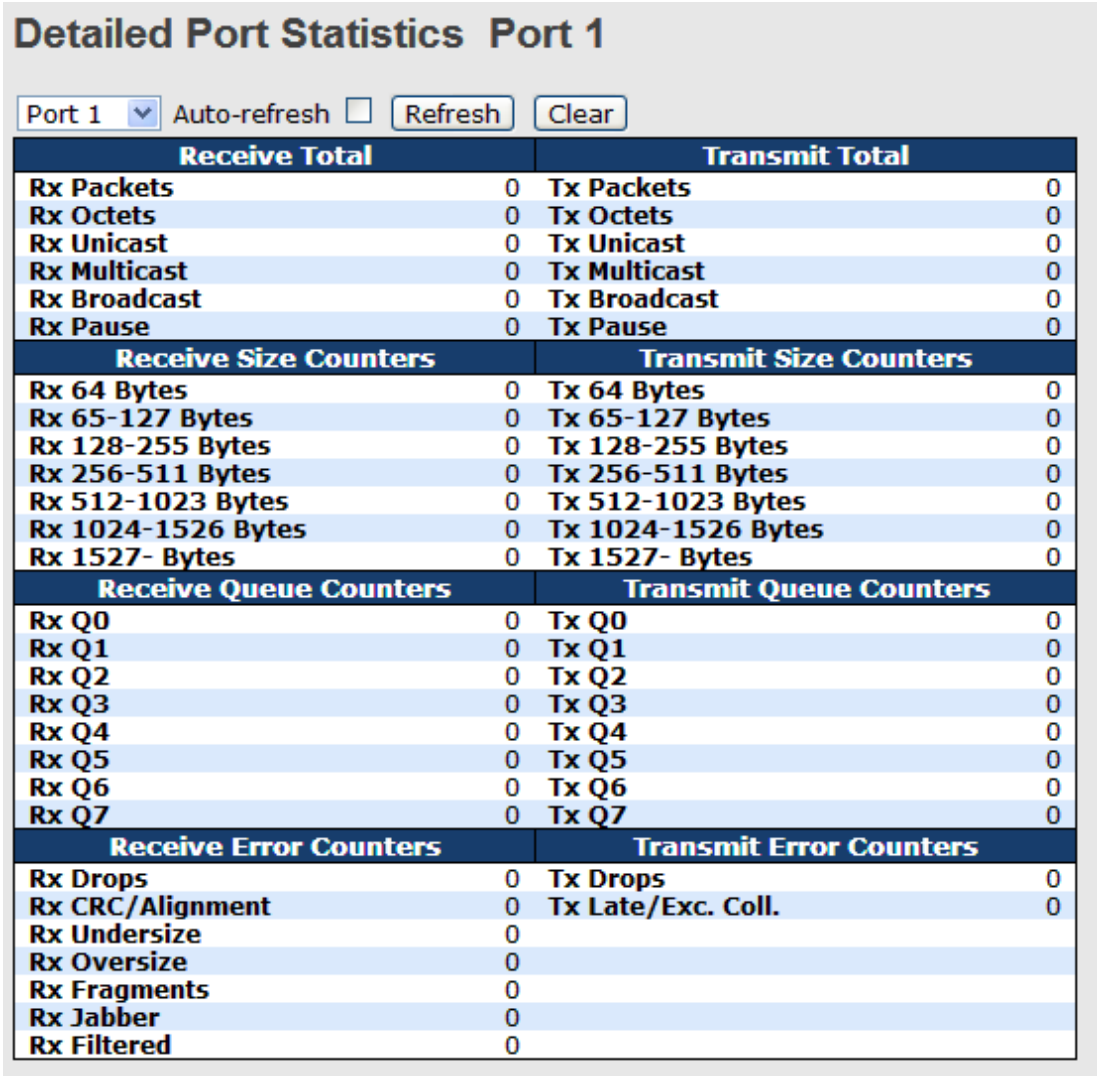

| Label | Description |
|---|---|
| **Port** | The switch port number to which the following settings will be applied. |
| **Packets** | The number of received and transmitted packets per port. |
| **Bytes** | The number of received and transmitted bytes per port. |
| **Errors** | The number of frames 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 to enable an automatic refresh of the page at regular intervals. |
| **Refresh** | Updates the counter entries, starting from the current entry ID. |
| **Clear** | Flushes all counters entries. |

## 5.10.2.2 Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port drop-down list to decide the details of which switch port to be displayed.

The displayed counters include the total number for receive and transmit, the size for receive and transmit, and the errors for receive and transmit.

### Detailed Statistics – Total Receive & Transmit




| 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, including FCS, except 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** | The number of 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 insufficient receive buffer 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 a valid CRC |
| **Rx Oversize** | The number of long[2] frames received with a valid CRC |
| **Rx Fragments** | The number of short[1] frames received with an invalid CRC |
| **Rx Jabber** | The number of long[2] frames received with an 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 |

1. Short frames are frames smaller than 64 bytes.
2. Long frames are frames longer than the maximum frame length configured for this port.

## 5.10.3 Port Mirroring

You can configure port mirroring on this page.

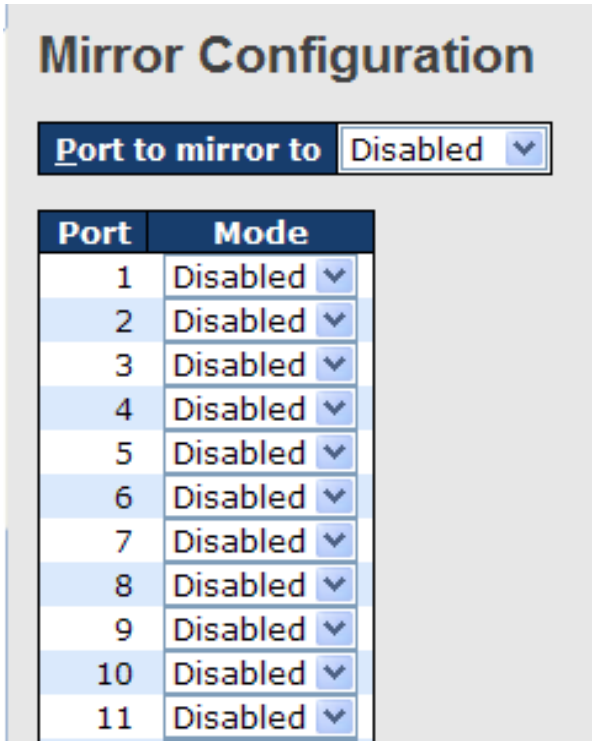
To solve network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow.

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).

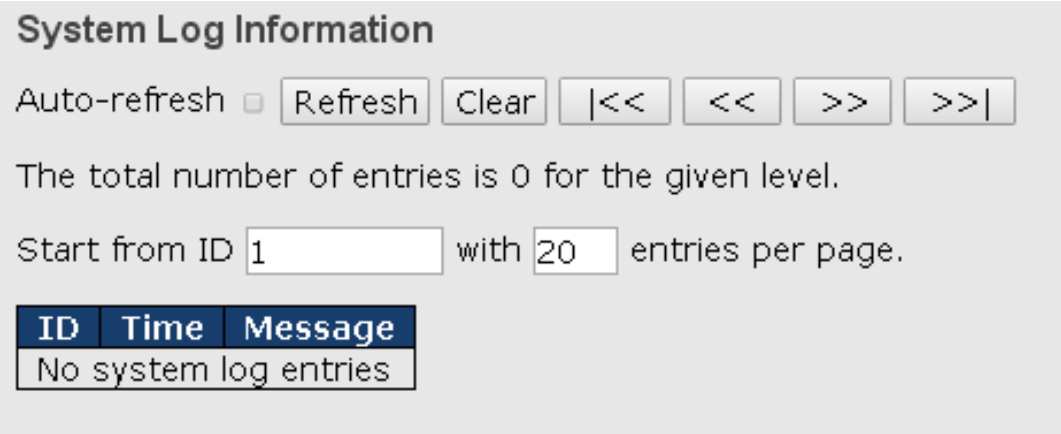
Port to mirror is also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this port. Disabled option disables mirroring.




| Label | Description |
|---|---|
| **Port** | The switch port number to which the following settings will be applied. |
| **Mode** | Drop-down list for selecting a mirror mode.<br>**Rx only**: only frames received on this port are mirrored to the mirror port. Frames transmitted are not mirrored.<br>**Tx only**: only frames transmitted from this port are mirrored to the mirror port. Frames received are not mirrored.<br>**Disabled**: neither transmitted nor received frames are mirrored.<br>**Enabled**: both received and transmitted frames are mirrored to the mirror port.<br>Note: for a given port, a frame is only transmitted once. Therefore, you cannot mirror Tx frames to the mirror port. In this case, mode for the selected mirror port is limited to **Disabled** or **Rx nly**. |

## 5.10.4 System Log Information

This page provides switch system log information.




| Label | Description |
|---|---|
| **ID** | The ID (>= 1) of the system log entry |
| **Time** | The time of the system log entry. |
| **Message** | The MAC address of the switch. |
| **Auto-refresh** | Check this box to enable an automatic refresh of the page at regular intervals. |
| **Refresh** | Updates system log entries, starting from the current entry ID. |
| **Clear** | Flushes all system log entries. |
| **\|<<** | Updates system log entries, starting from the first available entry ID. |
| **<<** | Updates system log entries, ending at the last entry currently displayed. |
| **>>** | Updates system log entries, starting from the last entry currently displayed.. |
| **>>\|** | Updates system log entries, ending at the last available entry ID. |

## 5.10.5 SFP Monitor

SFP modules with DDM (Digital Diagnostic Monitoring) function can measure the temperature of the apparatus, helping you monitor the status of connection and detect errors immediately. You can manage and set up event alarms through DDM Web interface.

**SFP Monitor**

Auto-refresh ☐ Refresh

| Port No. | Temperature (°C) | Vcc (V) | TX Bias (mA) | TX Power (mW) | (dBm) | RX Power (mW) | (dBm) |
|---|---|---|---|---|---|---|---|
| 25 | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| 26 | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

Warning Temperature :

85 °C(0~100)

Event Alarm :

☐ Syslog

Save

## 5.10.6 Traffic Monitor

By enabling traffic monitoring function, the switch will send out an SYSLOG event notification or SMTP e-mail when the traffic becomes too large.

**Traffic Monitor**

| Port | Monitor-Counter | Time-Interval | Increasing-Quantity |
|---|---|---|---|
| 1 | Disable | 3 | 1000 |
| 2 | Disable | 3 | 1000 |
| 3 | Disable | 3 | 1000 |
| 4 | Disable | 3 | 1000 |
| 5 | Disable | 3 | 1000 |
| 6 | Disable | 3 | 1000 |
| 7 | Disable | 3 | 1000 |
| 8 | Disable | 3 | 1000 |
| 9 | Disable | 3 | 1000 |
| 10 | Disable | 3 | 1000 |
| 11 | Disable | 3 | 1000 |
| 12 | Disable | 3 | 1000 |
| 13 | Disable | 3 | 1000 |
| 14 | Disable | 3 | 1000 |
| 15 | Disable | 3 | 1000 |
| 16 | Disable | 3 | 1000 |
| 17 | Disable | 3 | 1000 |
| 18 | Disable | 3 | 1000 |
| 19 | Disable | 3 | 1000 |
| 20 | Disable | 3 | 1000 |
| 21 | Disable | 3 | 1000 |
| 22 | Disable | 3 | 1000 |
| 23 | Disable | 3 | 1000 |
| 24 | Disable | 3 | 1000 |
| 25 | Disable | 3 | 1000 |
| 26 | Disable | 3 | 1000 |

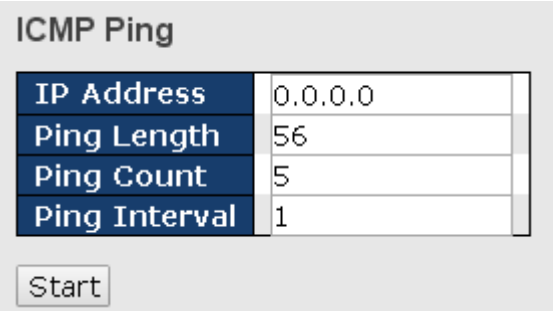
Event Alarm

☐ Syslog ☐ SMTP

| Label | Description |
|---|---|
| **Monitor–Counter** | Monitor the incoming traffic by bandwidth or number of packets. Available options include:<br>**RX Octet**: calculates the total bandwidth consumed by incoming traffic<br>**RX Broadcast**: calculates the number of broadcast packets<br>**RX Multicast**: calculates the number of multicast packets<br>**RX Unicast**: calculates the number of unicast packets<br>**RX Non-Unicast**: calculates the total number of multicast and broadcast packets<br>**Disable**: disables the function |
| **Time-Interval** | Sets the time interval of counting |
| **Increasing Quantity** – | Specify a threshold for the counter. When the result of calculation exceeds the value, an alert will be issued. |
| **Event Alarm** | Specifies alarm type (SYSLOG or SMTP) |

## 5.10.7 Ping

This command sends ICMP echo request packets to another node on the network. Using the ping command, you can see if another site on the network can be reached.




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

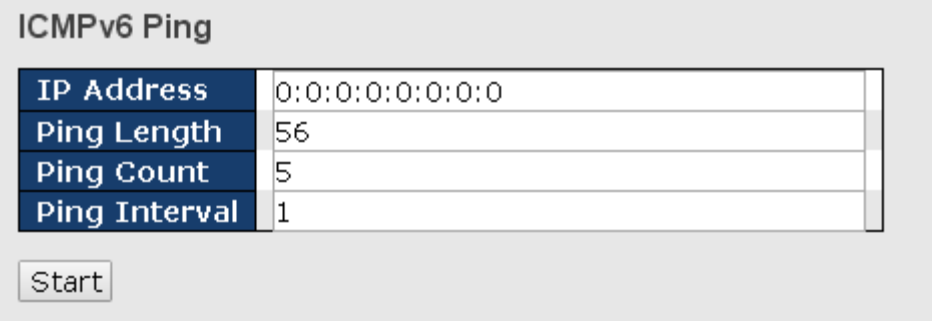
PING6 server ::10.10.132.20
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms

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 Length** | The payload size of the ICMP packet. Values range from 8 to 1400 bytes. |
| **Ping Count** | The number of ICMP packets to be sent. |
| **Ping Interval** | The interval at which ICMP packets will be sent. |

### 5.10.8 Ping6




PING6 server ::192.168.10.1

sendto

sendto

sendto

sendto

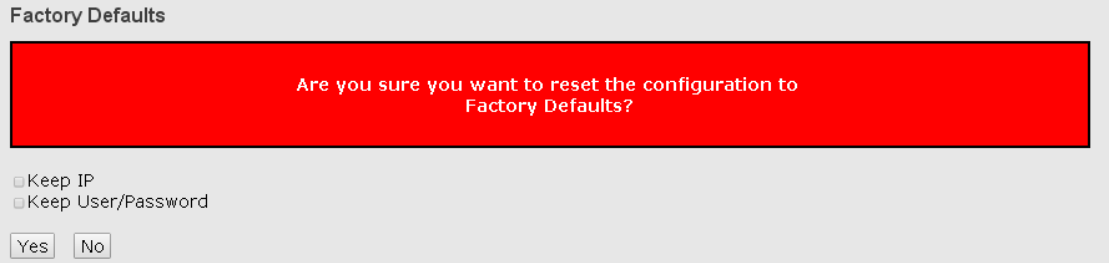
sendto

Sent 5 packets, received 0 OK, 0 bad

## 5.11 Troubleshooting

### 5.11.1 Factory Defaults

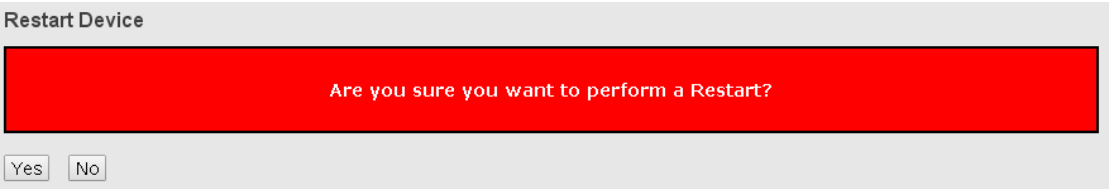
You can reset the configuration of the stack switch on this page. Only the IP configuration is retained.




| Label | Description |
|---|---|
| **Keep IP** | Check the box if you want the device to keep the IP address after restoring to factory settings |
| **Keep User/Password** | Check the box if you want the device to keep the username and password after restoring to factory settings |
| **Yes** | Click to reset the configuration to factory defaults |
| **No** | Click to return to the Port State page without resetting |

## 5.11.2 System Reboot

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




| Label | Description |
|---|---|
| **Yes** | Click to reboot device |
| **No** | Click to return to the **Port State** page without rebooting |

# Command Line Interface Management

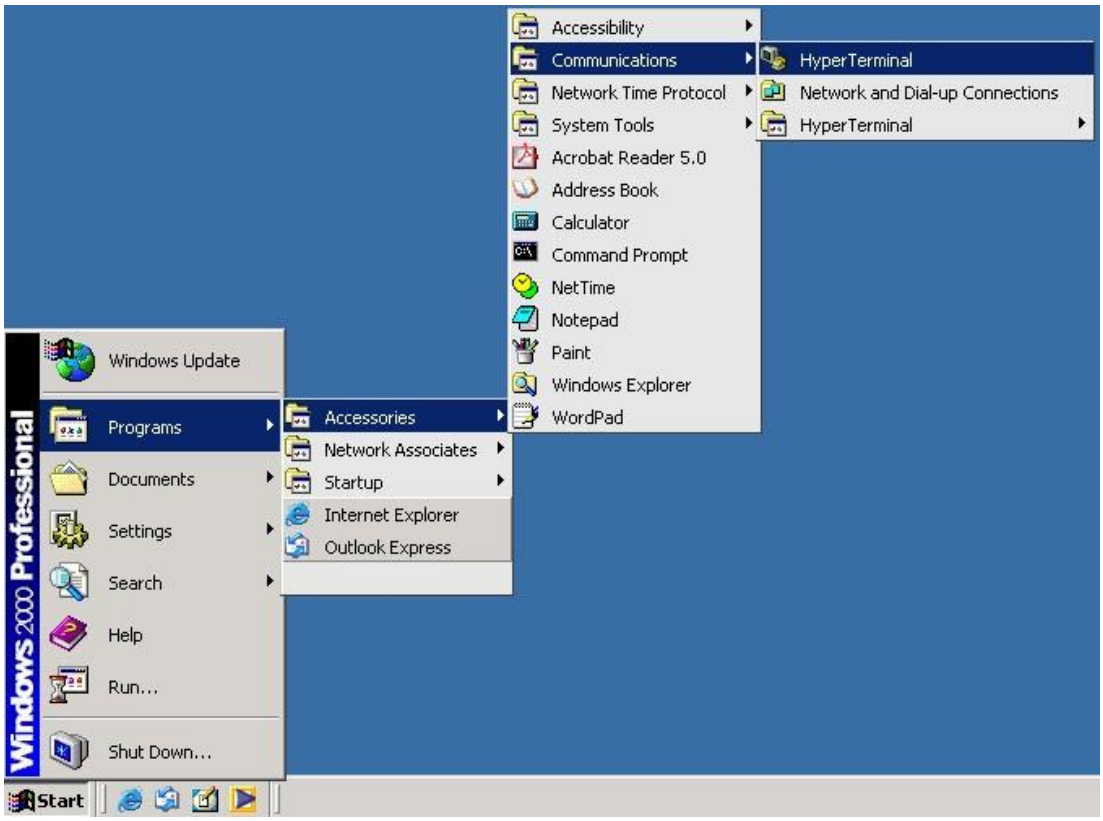
Besides Web-based management, the device also support CLI management. You can use console or telnet to manage the switch by CLI.

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

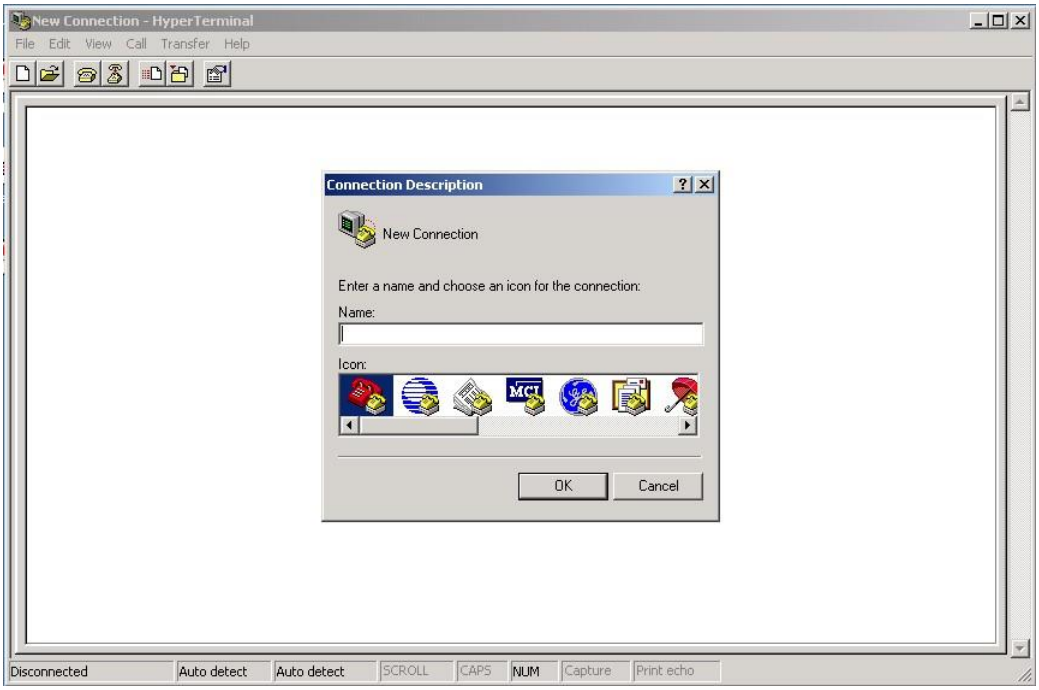
Before configuring RS-232 serial console, connect the RS-232 port of the switch to your PC Com port using a RJ45 to DB9-F cable.

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

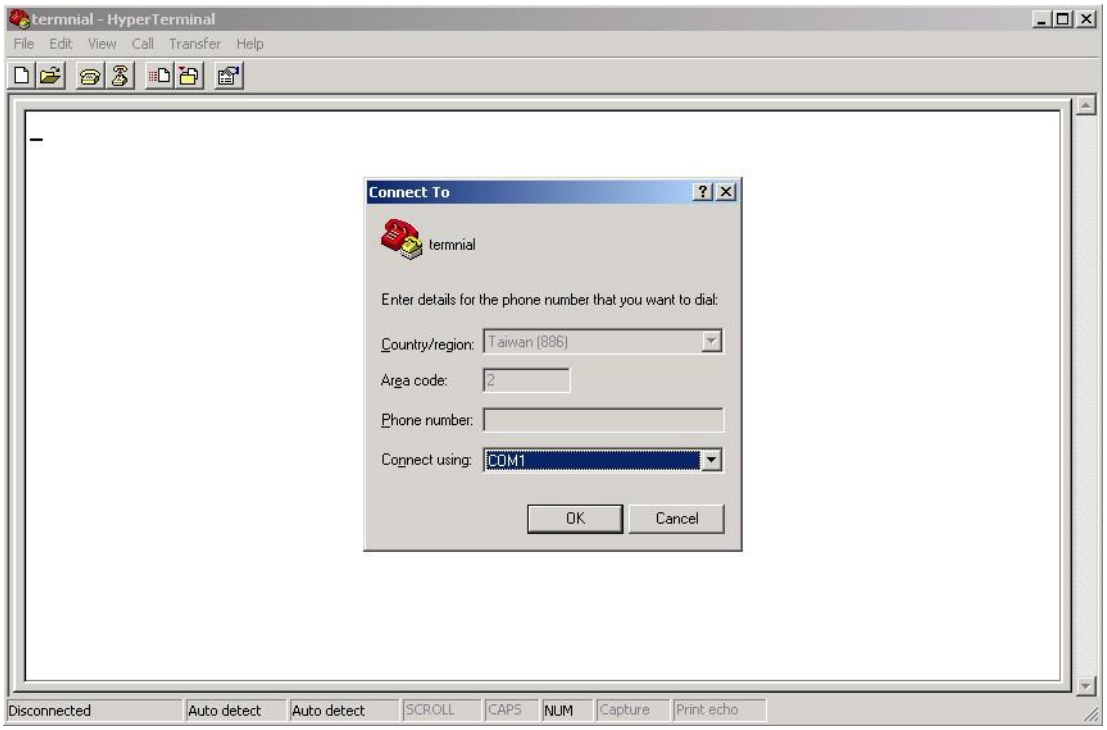
Step 1: On Windows desktop, click on **Start** -> **Programs** -> **Accessories** -> **Communications** -> **Hyper Terminal**



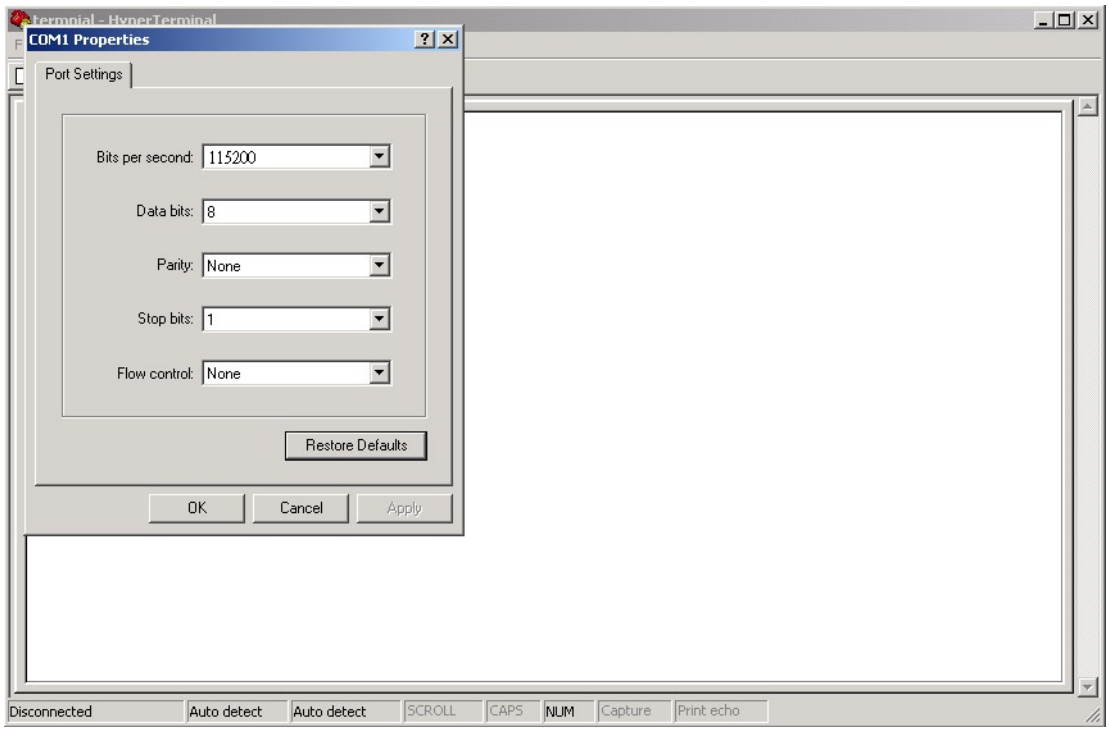
Step 2: Input a name for the new connection.



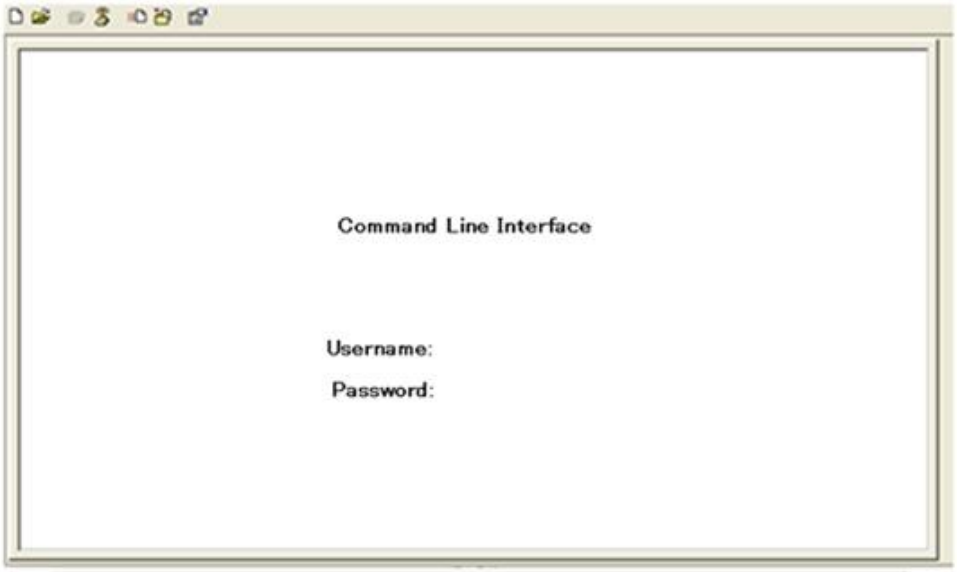

Step 3: Select a COM port in the drop-down list.



Step 4: A pop-up window that indicates COM port properties appears, including bits per second, data bits, parity, stop bits, and flow control.




Step 5: The console login screen will appear. Use the keyboard to enter the Username and Password (same as the password for Web browsers), then press **Enter**.




**CLI Management by Telnet**

You can can use **TELNET**to configure the switch. The default values are:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

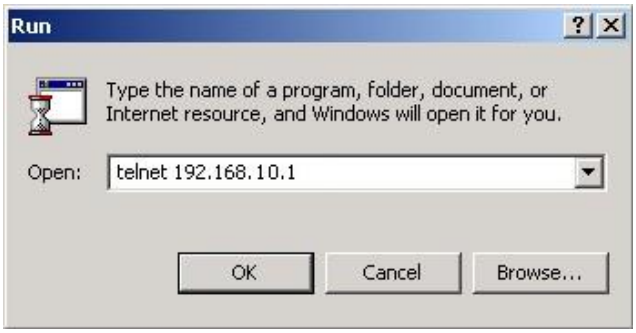
Default Gateway: **192.168.10.254**

User Name: **admin**

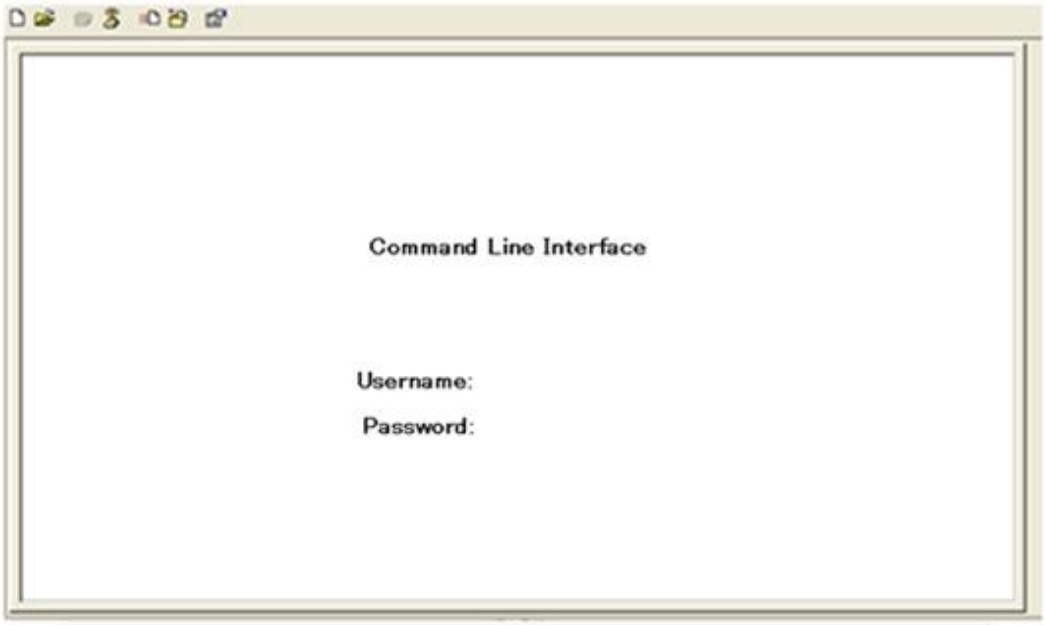
Password: **admin**

Follow the steps below to access console via Telnet.

Step 1: Telnet to the IP address of the switch from the **Run** window by inputting commands (or from the MS-DOS prompt) as below.




Step 2: The Login screen will appear. Use the keyboard to enter the Username and Password (same as 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] |
| | Mode [<port_list>] [auto\|10hdx\|10fdx\|100hdx\|100fdx\|1000fdx\|sfp_auto_ams] |
| | Flow Control [<port_list>] [enable\|disable] |
| | State [<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>]<br>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>]<br>[<port_list>]<br>[<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type>]<br>[(etype [<etype>]) \| |

| | |
|---|---|
| | (LLC [<DSAP>] [<SSAP>] [<control>]) \|<br>(SNAP [<PID>]) \|<br>(ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) \|<br>(ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])]<br>[<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>]<br>[<logging>] [<shutdown>]<br>Policy [<port_list>] [<policy>] |
| | Rate [<rate_limiter_list>] [<packet_rate>] |
| | Add [<ace_id>] [<ace_id_next>] [switch \| (port <port>) \| (policy <policy>)]<br>[<vid>] [<tag_prio>] [<dmac_type>]<br>[(etype [<etype>] [<smac>] [<dmac>]) \|<br>(arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) \|<br>(ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) \|<br>(icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) \|<br>(udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) \|<br>(tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])]<br>[permit\|deny] [<rate_limiter>] [<port_copy>]<br>[<logging>] [<shutdown>]<br>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>] |

### Firmware

| | |
|---|---|
| Firmware> | Load <ip_addr_string> <file_name> |

### 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>] |

**Loop Protect**

| | |
|---|---|
| Loop Protect> | Configuration |
| | Mode [enable\|disable] |
| | Transmit [<transmit-time>] |
| | Shutdown [<shutdown-time>] |
| | Port Configuration [<port_list>] |
| | Port Mode [<port_list>] [enable\|disable] |
| | Port Action [<port_list>] [shutdown\|shut_log\|log] |
| | Port Transmit [<port_list>] [enable\|disable] |
| | Status [<port_list>] |

**IPMC**

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

**Fault**

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

### Event

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

### DHCPServer

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

### Ring

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

### Chain

| | |
|---|---|
| Chain> | Configuration |
| | Mode [enable\|disable] |
| | 1stUplinkPort [<port>] |
| | 2ndUplinkPort [<port>] |
| | EdgePort [1st\|2nd\|none] |

### RCS

| | |
|---|---|
| RCS> | Mode [enable\|disable] |
| | Add [<ip_addr>] [<port_list>] [web_on\|web_off] [telnet_on\|telnet_off] [snmp_on\|snmp_off] |
| | Del <index> |
| | Configuration |

### FastReocvery

| | |
|---|---|
| FastRecovery> | Mode [enable\|disable] |
| | Port [<port_list>] [<fr_priority>] |

### SFP

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

### DeviceBinding

| | |
|---|---|
| Devicebinding> | Mode [enable\|disable] |
| | Port Mode [<port_list>] [disable\|scan\|binding\|shutdown] |
| | Port DDOS Mode [<port_list>] [enable\|disable] |
| | Port DDOS Sensibility [<port_list>] [low\|normal\|medium\|high] |
| | Port DDOS Packet [<port_list>] [rx_total\|rx_unicast\|rx_multicast\|rx_broadcast\|tcp\|udp] |
| | Port DDOS Low [<port_list>] [<socket_number>] |
| | Port DDOS High [<port_list>] [<socket_number>] |
| | Port DDOS Filter [<port_list>] [source\|destination] |
| | Port DDOS Action [<port_list>] [do_nothing\|block_1_min\|block_10_mins\|block\|shutdown\|only_log\|reboot_device] |
| | Port DDOS Status [<port_list>] |
| | Port Alive Mode [<port_list>] [enable\|disable] |
| | Port Alive Action [<port_list>] [do_nothing\|link_change\|shutdown\|only_log\|reboot_device] |
| | Port Alive Status [<port_list>] |
| | Port Stream Mode [<port_list>] [enable\|disable] |

| | |
|---|---|
| | Port Stream Action [<port_list>] [do_nothing\|only_log] |
| | Port Stream Status [<port_list>] |
| | Port Addr [<port_list>] [<ip_addr>] [<mac_addr>] |
| | Port Alias [<port_list>] [<ip_addr>] |
| | Port DeviceType [<port_list>] [unknown\|ip_cam\|ip_phone\|ap\|pc\|plc\|nvr] |
| | Port Location [<port_list>] [<device_location>] |
| | Port Description [<port_list>] [<device_description>] |

**MRP**

| | |
|---|---|
| MRP> | Configuration |
| | Mode [enable\|disable] |
| | Manager [enable\|disable] |
| | React [enable\|disable] |
| | 1stRingPort [<mrp_port>] |
| | 2ndRingPort [<mrp_port>] |
| | Parameter MRP_TOPchgT [<value>] |
| | Parameter MRP_TOPNRmax [<value>] |
| | Parameter MRP_TSTshortT [<value>] |
| | Parameter MRP_TSTdefaultT [<value>] |
| | Parameter MRP_TSTNRmax [<value>] |
| | Parameter MRP_LNKdownT [<value>] |
| | Parameter MRP_LNKupT [<value>] |
| | Parameter MRP_LNKNRmax [<value>] |

**Modbus**

| | |
|---|---|
| Modbus> | Status |
| | Mode [enable\|disable] |

# Technical Specifications

| ORing Switch Model | RES-P9242GCL-LV | RES-P9242GCL-HV |
|---|---|---|
| **Physical Ports** | | |
| 10/100 Base-T(X) Ports in RJ45 Auto MDI/MDIX | **24** | |
| Gigabit combo port with 10/100/1000Base-T(X) and 1000Base-X SFP | **2** | |
| **Technology** | | |
| Ethernet Standards | IEEE 802.3 for 10Base-T<br>IEEE 802.3u for 100Base-TX<br>IEEE 802.3ab for 1000Base-T<br>IEEE 802.3z for 1000Base-X<br>IEEE 802.3x for Flow control<br>IEEE 802.3ad for LACP (Link Aggregation Control Protocol )<br>IEEE 802.1D for STP (Spanning Tree Protocol)<br>IEEE 802.1p for COS (Class of Service)<br>IEEE 802.1Q for VLAN Tagging<br>IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol)<br>IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol)<br>IEEE 802.1X for Authentication<br>IEEE 802.1AB for LLDP (Link Layer Discovery Protocol) | |
| MAC Table | 8k | |
| Priority Queues | 8 | |
| Processing | Store-and-Forward | |
| Switch Properties | Switching latency: 7 us<br>Switching bandwidth: 8.8Gbps<br>Max. Number of Available VLANs: 4095<br>VLAN ID Range : VID 1 to 4094<br>IGMP multicast groups: 256 for each VLAN<br>Port rate limiting: User Define | |
| Security Features | Device Binding security feature<br>Enable/disable ports, MAC based port security<br>Port based network access control (802.1x)<br>MAC-based authentication (802.1x)<br>Guest VLAN<br>VLAN (802.1Q ) to segregate and secure network traffic<br>Radius centralized password management<br>SNMPv3 encrypted authentication and access security<br>Https / SSH enhance network security<br>Web and CLI authentication and authorization<br>IP source guard | |
| Software Features | IEEE 802.1D Bridge, auto MAC address learning/aging and MAC address (static)<br>Multiple Registration Protocol (MRP)<br>MSTP (RSTP/STP compatible)<br>TOS/Diffserv supported<br>Quality of Service (802.1p) for real-time traffic<br>VLAN (802.1Q) with VLAN tagging<br>IGMP v2/v3 Snooping<br>Application-based QoS management<br>DOS/DDOS auto prevention<br>Port configuration, status, statistics, monitoring, security<br>DHCP Server/Client/Relay<br>Modbus TCP<br>SMTP Client<br>NTP server | |
| Network Redundancy | O-Ring<br>O-Chain<br>MRP*Note<br>Fast Recovery | |

| | | |
|---|---|---|
| | MSTP (RSTP/STP compatible) | |
| RS-232 Serial Console Port | RS-232 in DB-9 connector with console cable. 115200bps, 8, N, 1 | |
| **LED indicators** | | |
| Power Indicator | Green : Power LED x 3 | |
| Ring Master Indicator | Green : Indicates that the system is operating in O-Ring Master mode | |
| O-Ring Indicator | Green : Indicates that the system operating in O-Ring mode<br>Green Blinking: Indicates that the Ring is broken. | |
| Fault Indicator | Amber : Indicate unexpected event occurred | |
| 10/100Base-T(X) RJ45 port indicator | Green at left for port Link/Act.<br>Amber at right for speed indicator (On for 100Mbps, Off for 10Mbps indicator) | |
| 10/100/1000Base-T(X) RJ45 Port Indicator | Green for Link/Act indicator.<br>Dual color LED for speed indicator : Green for 1000Mbps, Amber for 100Mbps, Off-light for 10Mbps | |
| 100/1000Base-X SFP Port Indicator | Green for port Link/Act. | |
| **Fault contact** | | |
| Relay | Relay output to carry capacity of 1A at 24VDC | |
| **Power** | | |
| Power Input | Dual 24/48VDC (24~72VDC) power inputs at terminal block | Dual 125~370VDC / 100~240VAC power inputs |
| Power consumption (Typ.) | 19W | 19.8W |
| Overload current protection | Present | |
| Reverse Polarity Protection | Present | |
| **Physical Characteristic** | | |
| Enclosure | 19 inches rack mountable | |
| Dimension (W x D x H) | 443.7(W) x 262.7(D) x 44(H) mm (17.46x10.34x1.73 inch) | |
| Weight (g) | 3,535g | 4,050g |
| **Environmental** | | |
| Storage Temperature | -40 to 85°C (-40 to 185°F) | |
| Operating Temperature | -40 to 85°C (-40 to 185°F ) | |
| Operating Humidity | 5% to 95% Non-condensing | |
| **Regulatory approvals** | | |
| EMC | CE EMC (EN 55024, EN 55032), FCC Part 15 B, IEC 61850/ IEEE1613 | |
| EMI | EN 55032, CISPR32, EN 61000-3-2, EN 61000-3-3, FCC Part 15B class A | |
| EMS | EN 55024 (IEC/EN 61000-4-2 (ESD), IEC/EN 61000-4-3 (RS),IEC/EN 61000-4-4 (EFT),<br>IEC/EN 61000-4-5 (Surge), IEC/EN 61000-4-6 (CS), IEC/EN 61000-4-8(PFMF), IEC/EN 61000-4-11 (DIP)) | |
| Shock | IEC 60068-2-27 | |
| Free Fall | IEC 60068-2-31 | |
| Vibration | IEC 60068-2-6 | |
| Safety | EN 60950-1 | |
| Other | IEC 61850/ IEEE1613 | |
| MTBF | 297,924 hrs | 262,968 hrs |
| **Warranty** | 5 years | |