



CPGS-9120-M12-C

Industrial Managed Ethernet Switch

User Manual

Version 3.0
December, 2013

www.oring-networking.com



COPYRIGHT NOTICE

Copyright © 2013 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



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 23148, Taiwan, R.O.C.

Tel: + 886 2 2918 1066 // Fax: + 886 2 2918 2368

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 | 5 |
| 1.1 About CPGS-9120-M12-C Series | 5 |
| 1.2 Software Features | 5 |
| 1.3 Hardware Features..... | 6 |
| Hardware Overview..... | 7 |
| 2.1 Front Panel..... | 7 |
| 2.1.1 Ports and Connectors | 7 |
| 2.1.2 LEDs | 8 |
| Hardware Installation..... | 9 |
| 3.1 Installation | 9 |
| 3.2 Connection | 9 |
| 3.2.1 Cables | 9 |
| Redundancy | 12 |
| 4.1 O-Ring | 12 |
| 4.1.1 Introduction | 12 |
| 4.1.2 Configurations..... | 12 |
| 4.2 O-Chain | 14 |
| 4.2.1 Introduction | 14 |
| 4.2.2 Configurations..... | 14 |
| 4.3 MRP..... | 15 |
| 4.3.1 Introduction | 15 |
| 4.3.2 Configurations..... | 15 |
| 4.4 STP/RSTP/MSTP..... | 16 |
| 4.4.1 STP/RSTP | 16 |
| 4.4.2 MSTP | 19 |
| 4.4.3 CIST..... | 22 |
| 4.5 Fast Recovery | 24 |
| Management..... | 26 |
| 5.1 Basic Settings..... | 27 |
| 5.1.1 System Information | 27 |
| 5.1.2 Admin & Password..... | 28 |
| 5.1.3 Authentication | 29 |



- 5.1.4 IP Settings 29
- 5.1.5 IPv6 Settings 30
- 5.1.6 HTTPS 32
- 5.1.7 SSH 32
- 5.1.8 LLDP 33
- 5.1.9 Modbus TCP 36
- 5.1.10 Backup/Restore Configurations 37
- 5.1.11 Firmware Update 37
- 5.2 DHCP Server 37
 - 5.2.1 Basic Settings 37
 - 5.2.2 Dynamic Client List 38
 - 5.2.3 Client List 38
 - 5.2.4 DHCP Relay 39
- 5.3 Port Setting 41
 - 5.3.1 Port Control 41
 - 5.3.2 Port Trunk 43
 - 5.3.3 LACP 43
 - 5.3.4 Loop Guard 47
- 5.4 VLAN 49
 - 5.4.1 VLAN Membership 49
 - 5.4.2 Port Configurations 50
 - 5.4.3 Private VLAN 59
- 5.5 SNMP 61
 - 5.5.1 SNMP System Configurations 61
 - 5.5.2 SNMP Community Configurations 63
 - 5.5.3 SNMP User Configurations 64
 - 5.5.4 SNMP Group Configurations 66
 - 5.5.5 SNMP View Configurations 67
 - 5.5.6 SNMP Access Configurations 67
- 5.6 Traffic Prioritization 68
 - 5.6.1 Storm Control 68
 - 5.6.2 Port Classification 69
 - 5.6.3 Port Tag Remaking 71
 - 5.6.4 Port DSCP 72
 - 5.6.5 Policing 73
 - 5.6.6 Scheduling and Shaping 75
 - 5.6.7 Port Scheduler 78



| | | |
|--------|---|-----|
| 5.6.8 | Port Shaping | 78 |
| 5.6.9 | DSCP-based QoS | 79 |
| 5.6.10 | DSCP Translation | 80 |
| 5.6.11 | DSCP Classification | 81 |
| 5.6.12 | QoS Control List..... | 82 |
| 5.6.13 | QoS Counters | 84 |
| 5.6.14 | QCL Status..... | 85 |
| 5.7 | Multicast | 86 |
| 5.7.1 | IGMP Snooping..... | 86 |
| 5.7.2 | VLAN Configurations of IGMP Snooping..... | 87 |
| 5.7.3 | IGMP Snooping Status | 88 |
| 5.7.4 | Groups Information of IGMP Snooping..... | 89 |
| 5.8 | Security | 89 |
| 5.8.1 | Remote Control Security Configurations | 89 |
| 5.8.2 | Device Binding | 90 |
| 5.8.3 | ACL | 95 |
| 5.8.4 | Authentication, Authorization, and Accounting | 107 |
| 5.8.5 | RADIUS..... | 107 |
| 5.8.6 | NAS (802.1x) | 114 |
| 5.9 | Alerts | 124 |
| 5.9.1 | Fault Alarm..... | 124 |
| 5.9.2 | System Warning..... | 125 |
| 5.10 | Monitor and Diag..... | 128 |
| 5.10.1 | MAC Table..... | 128 |
| 5.10.2 | Port Statistics | 131 |
| 5.10.3 | Port Mirroring | 133 |
| 5.10.4 | System Log Information..... | 134 |
| 5.10.5 | Cable Diagnostics | 135 |
| 5.10.6 | Ping | 136 |
| 5.11 | Synchronization..... | 138 |
| 5.12 | Troubleshooting..... | 140 |
| 5.12.1 | Factory Defaults | 140 |
| 5.12.2 | System Reboot | 140 |
| 5.13 | Command Line Interface Management..... | 141 |

Getting Started

1.1 About CPGS-9120-M12-C Series

ORing's CPGS-9120-M12-C series are compact Ethernet switches on a highly integrated 3U Compact PCI card form factor. Featuring eight 10/100/1000Base-T(X) ports and four 10/100/1000Base-T(X) M12 connectors, the CPGS-9120-M12-C series are fully compliant with the EN50155 standard, and are ideal for harsh industrial applications, such as factory automation, vehicle, and railway applications. The four M12 connectors make the card a perfect fit for factory rolling stock applications. With complete support for Ethernet redundancy protocols such as O-Ring (recovery time < 30ms over 250 units of connection) and MSTP (RSTP/STP compatible), the switch can protect your mission-critical applications from network interruptions or temporary malfunctions with its fast recovery technology. Featuring a wide operating temperature from -40°C to 70°C, the CPGS-9120-M12-C series can be managed centrally and conveniently via Open-Vision, web browsers, Telnet and console (CLI) configuration, making it one of the most reliable choices for power substation and rolling stock applications. Since the switch card is hot swappable, you do not need to turn off the system power during installation.



1.2 Software Features

- Supports O-Ring (recovery time < 30ms over 250 units of connection), MSTP/RSTP/STP (IEEE 802.1s/w/D) for Ethernet Redundancy
- Supports O-Chain to allow multiple redundant network rings
- Supports standard IEC 62439 MRP (Media Redundancy Protocol) function
- Supports IPV6 new internet protocol version
- Support Modbus TCP protocol
- Supports IEEE 802.3az Energy-Efficient Ethernet technology
- Supports HTTPS/SSH protocols to enhance network security
- Supports SMTP client
- Supports IP-based bandwidth management
- Supports application-based QoS management



- Supports Device Binding security function
- Supports DOS/DDOS auto prevention
- Supports 9.6K Bytes Jumbo frame
- Supports multiple notifications for incidents
- IGMP v2/v3 (IGMP snooping support) for filtering multicast traffic
- Supports SNMP v1/v2c/v3 & RMON & 802.1Q VLAN network management
- Supports ACL, TACACS+ and 802.1x user authentication for security
- Supports management via Web-based interfaces, Telnet, Console (CLI), and Windows utility (Open-Vision)
- Supports LLDP protocol

1.3 Hardware Features

- Supports 3U and 8HP CompactPCI form factor and hot swapping
- PICMG 2.0 Rev. 3.0 compatible, universal 5V and 3.3V PCI signaling voltage supported
- 8x10/100/1000Base-T(X) ports for connecting to other CompactPCI sockets and 4x10/100/1000Base-T(X) M12 connector ports
- 1 x console port (RJ-45)
- M12 connectors for reliable operation against environmental disturbances
- Operating Temperature: -40 to 70°C
- Storage Temperature: -40 to 85°C
- Operating Humidity: 5% to 95%, non-condensing
- Dimensions: 40 (W) x 130.7 (H) x 209.0 (D) mm

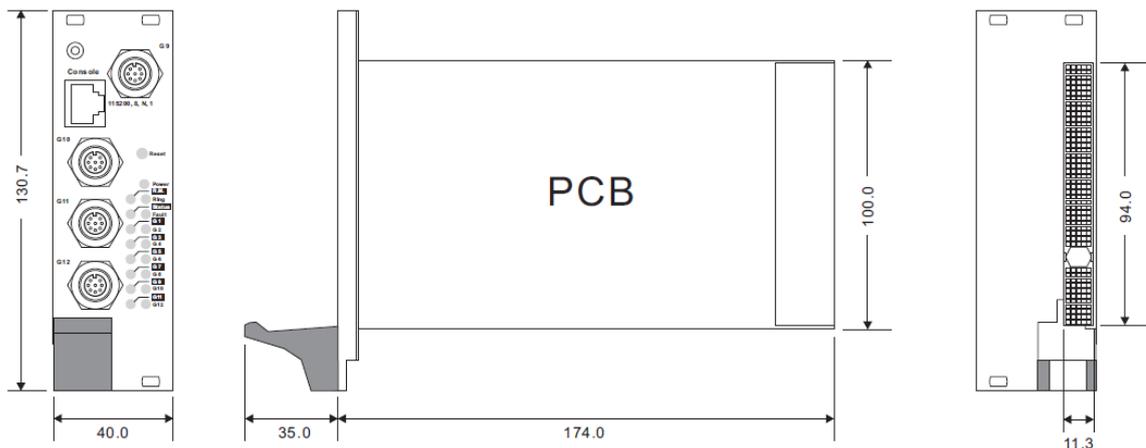
Hardware Overview

2.1 Front Panel

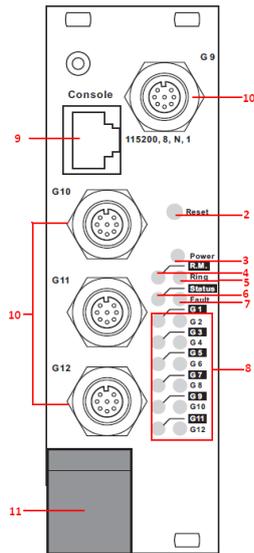
2.1.1 Ports and Connectors

The CPGS-9120-M12-C series provide the following ports on the front panel.

| Port | Description |
|---|--|
| 10/100/1000 Fast Ethernet ports in M12 connector | Four 10/100/1000 Base-T(X) Fast Ethernet ports in M12 connectors support auto-negotiation. Default settings as below: Speed: auto Duplex: auto Flow control: disable |
| Console port | One console port for with RS-232 to RJ-45 connector |
| Reset button | Press reset button 2 to 3 seconds to reset the switch. Press reset button 5 seconds to reset the switch to factory defaults. |



CPGS-9120-M12-C



1. Ejection lever
2. Reset button
3. Power status LED
4. R.M. status LED
5. Ring status LED
6. System status LED
7. Fault LED
8. Port status LEDs
9. Console port
10. M12 Ethernet connectors

2.1.2 LEDs

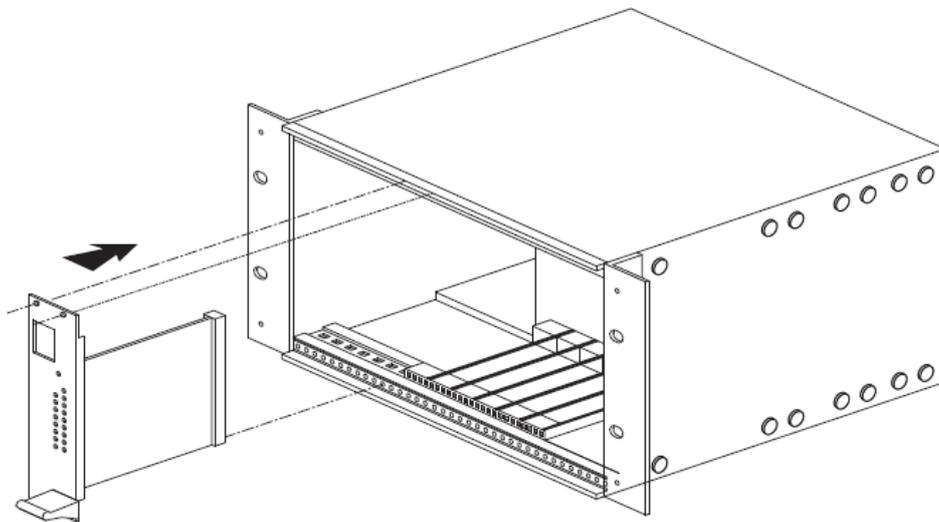
| LED | Color | Status | Description |
|---------------|-------|----------|--|
| PWR | Green | On | DC power on |
| G1-G12 | Green | On | Port is linked |
| | | Blinking | Transmitting data |
| R.M | Green | On | Operating as Ring Master. |
| Ring | Green | On | Operating in Ring mode |
| | | Blinking | Ring broken |
| Status | Green | On | Ethernet link on |
| Fault | Amber | On | Faulty indication (power failure or ports down/fail) |

Hardware Installation

3.1 Installation

Follow the steps below to install the card to the CPCI chassis.

1. Remove the metal cover plate on the back of an available CPCI slot.
2. Insert the card into the slot and use the bracket screws to secure it firmly in place.
3. Connect the card to the desired network devices.



3.2 Connection

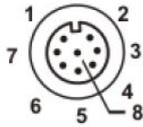
3.2.1 Cables

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

The CPGS-9120-M12-C series use M12 connectors for network connection. 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) | 8-pin female M12 A-coding connector |
| 100BASE-TX | Cat. 5 100-ohm UTP | UTP 100 m (328 ft) | 8-pin female M12 A-coding connector |
| 1000BASE-T | Cat. 5e, 6 | UTP 100 m (328ft) | 8-pin female M12 A-coding connector |

M12/8P Pin Definition



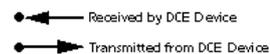
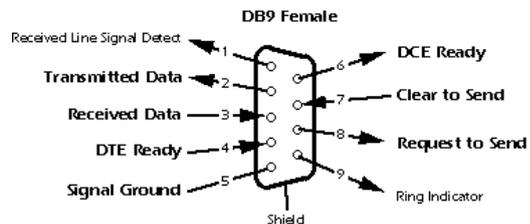
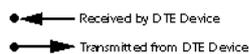
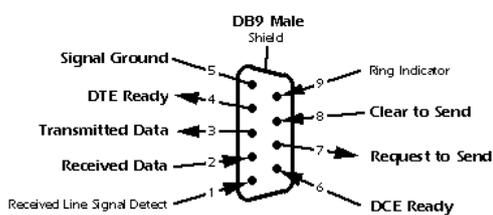
| 10/100Base-T(X) | |
|-----------------|-------------|
| PIN No. | Description |
| #6 | TD+ |
| #4 | TD- |
| #5 | RD+ |
| #8 | RD- |

| 1000Base-T | |
|------------|-------------|
| PIN No. | Description |
| #1 | BI_DC+ |
| #2 | BI_DD+ |
| #3 | BI_DD- |
| #4 | BI_DA- |
| #5 | BI_DB+ |
| #6 | BI_DA+ |
| #7 | BI_DC- |
| #8 | BI_DB- |

RS-232 console port wiring

The CPGS-9120-M12-C series can be managed via console ports using a RS-232 cable which can be found in the package. You can connect the port to a PC via the RS-232 cable with a DB-9 female connector. The DB-9 female connector of the RS-232 cable should be connected to the PC while the other end of the cable (RJ-45 connector) should be connected to the console port of the switch.

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



Backplane Pin Definition

The table below provides information of each pin on the backplane of the card. Please refer to the table for the pin assignment of each serial port.



| Pin | Z | A | B | C | D | E | F | |
|-----|-----|--------|--------|--------|--------|--------|-----|-------|
| 22 | GND | NC | STxD | NC | NC | SRxD | GND | J2/P2 |
| 21 | GND | NC | NC | NC | NC | NC | GND | |
| 20 | GND | LED5_0 | LED5_1 | GND | LED7_0 | LED7_1 | GND | |
| 19 | GND | LED4_0 | LED4_1 | GND | LED6_0 | LED6_1 | GND | |
| 18 | GND | LED1_0 | LED1_1 | GND | LED3_0 | LED3_1 | GND | |
| 17 | GND | LED0_0 | LED0_1 | GND | LED2_0 | LED2_1 | GND | |
| 16 | GND | P8_RX+ | P8_RX- | GND | NC | NC | GND | |
| 15 | GND | P8_TX+ | P8_TX- | GND | NC | NC | GND | |
| 14 | GND | P7_RX+ | P7_RX- | GND | NC | NC | GND | |
| 13 | GND | P7_TX+ | P7_TX- | GND | NC | NC | GND | |
| 12 | GND | P6_RX+ | P6_RX- | GND | NC | NC | GND | |
| 11 | GND | P6_TX+ | P6_TX- | GND | NC | NC | GND | |
| 10 | GND | P5_RX+ | P5_RX- | GND | NC | NC | GND | |
| 9 | GND | P5_TX+ | P5_TX- | GND | NC | NC | GND | |
| 8 | GND | P4_RX+ | P4_RX- | GND | NC | NC | GND | |
| 7 | GND | P4_TX+ | P4_TX- | GND | NC | NC | GND | |
| 6 | GND | P3_RX+ | P3_RX- | GND | NC | NC | GND | |
| 5 | GND | P3_TX+ | P3_TX- | GND | NC | NC | GND | |
| 4 | GND | P2_RX+ | P2_RX- | GND | NC | NC | GND | |
| 3 | GND | P2_TX+ | P2_TX- | GND | NC | NC | GND | |
| 2 | GND | P1_RX+ | P1_RX- | GND | NC | NC | GND | |
| 1 | GND | P1_TX+ | P1_TX- | GND | NC | NC | GND | |
| | | | | | | | | |
| 25 | GND | +5V | NC | NC | +3.3V | +5V | GND | J1/P1 |
| 24 | GND | NC | +5V | 5V(MO) | NC | NC | GND | |
| 23 | GND | +3.3V | NC | NC | +5V | NC | GND | |
| 22 | GND | NC | GND | +3.3V | NC | NC | GND | |
| 21 | GND | +3.3V | NC | NC | NC | NC | GND | |
| 20 | GND | NC | GND | 5V(MO) | NC | NC | GND | |
| 19 | GND | +3.3V | NC | NC | GND | NC | GND | |
| 18 | GND | NC | GND | +3.3V | NC | NC | GND | |
| 17 | GND | +3.3V | NC | NC | GND | NC | GND | |
| 16 | GND | NC | GND | 5V(MO) | NC | NC | GND | |
| 15 | GND | +3.3V | NC | NC | GND | NC | GND | |
| 14 | | | | | | | | |
| 13 | | | | | | | | |
| 12 | | | | | | | | |

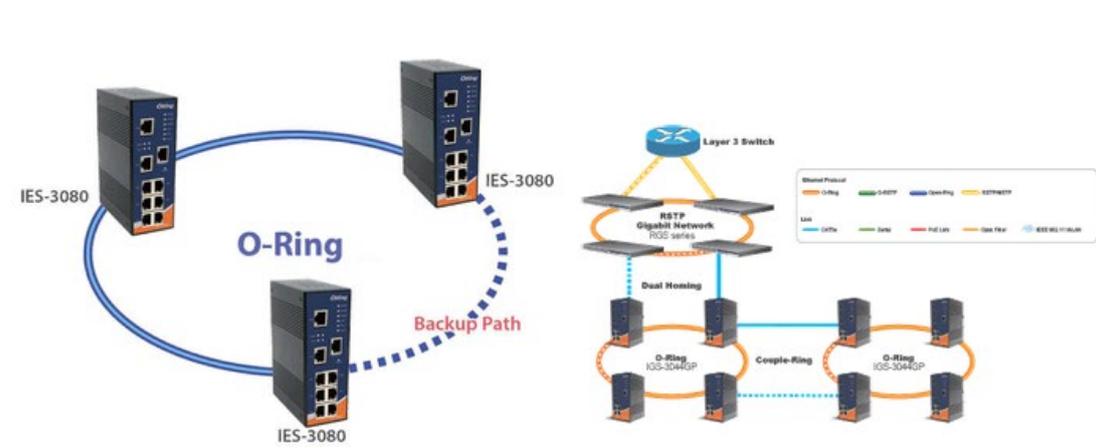
Redundancy

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.



O-Ring Configuration

| | | |
|---|-----------|-----------------------------------|
| <input checked="" type="checkbox"/> O-Ring | | |
| Ring Master | Disable ▾ | This switch is Not a Ring Master. |
| 1st Ring Port | Port 1 ▾ | LinkDown |
| 2nd Ring Port | Port 2 ▾ | LinkDown |
| <input type="checkbox"/> Coupling Ring | | |
| Coupling Port | Port 3 ▾ | LinkDown |
| <input type="checkbox"/> Dual Homing | | |
| Homing Port | Port 4 ▾ | LinkDown |

| Label | Description |
|-----------------------|---|
| Redundant 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 apply the configurations. |

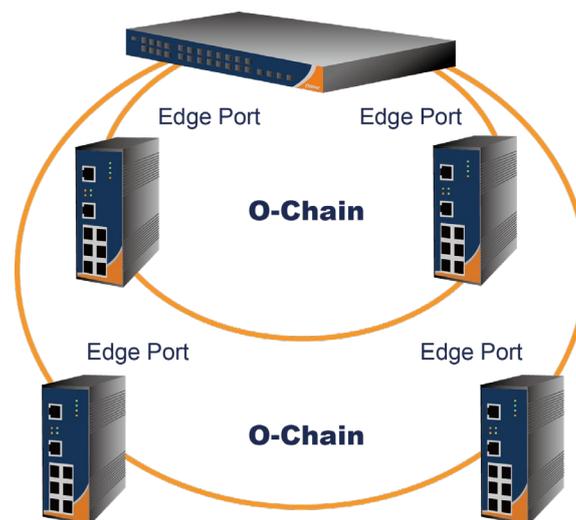
Note: due to heavy computing loading, setting one switch as ring master and coupling ring at the same time is not recommended.

4.2 O-Chain

4.2.1 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.



4.2.2 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.

O-Chain

| <input checked="" type="checkbox"/> Enable | | | |
|--|-------------|--------------------------|------------|
| | Uplink Port | Edge Port | State |
| 1st | Port.01 | <input type="checkbox"/> | Linkdown |
| 2nd | Port.02 | <input type="checkbox"/> | Forwarding |

Apply

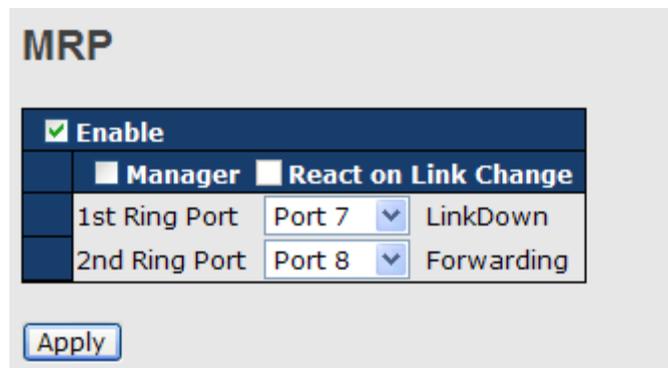
| Label | Description |
|---------------------------------|---|
| Enable | Check to enable O-Chain function |
| 1st Ring Port | The first port connecting to the ring |
| 2nd Ring Port | The second port connecting to the ring |
| Edge Port | An O-Chain topology must begin with edge ports. The ports with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

4.3 MRP

4.3.1 Introduction

MRP (Media Redundancy Protocol) is an industry standard for high-availability Ethernet networks. MRP allowing Ethernet switches in ring configuration to recover from failure rapidly to ensure seamless data transmission. A MRP ring (IEC 62439) can support up to 50 devices and will enable a back-up link in 80ms (adjustable to max. 200ms/500ms).

4.3.2 Configurations



| Label | Description |
|---|--|
| Enable | Enables the MRP function |
| Manager | Every MRP topology needs a MRP manager. One MRP topology can only have a Manager. If two or more switches are set to be Manager, the MRP topology will fail. |
| React on Link Change (Advanced mode) | Faster mode. Enabling this function will cause MRP topology to converge more rapidly. This function only can be set in MRP manager switch. |
| 1st Ring Port | Chooses the port which connects to the MRP ring |
| 2nd Ring Port | Chooses the port which connects to the MRP ring |

4.4 STP/RSTP/MSTP

4.4.1 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.

STP Bridge Status

This page shows the status for all STP bridge instance.

STP Bridges

Auto-refresh

| MSTI | Bridge ID | Root | | | Topology Flag | Topology Change Last |
|------|-------------------------|-------------------------|------|------|---------------|----------------------|
| | | ID | Port | Cost | | |
| | 80:00-00:1E:94:FF:FF:FF | 80:00-00:1E:94:FF:FF:FF | - | 0 | Steady | - |

| Label | Description |
|-----------------------------|---|
| MSTI | The bridge instance. You can also link to the STP detailed bridge status. |
| Bridge ID | The bridge ID of this bridge instance. |
| Root ID | The bridge ID of the currently selected root bridge. |
| Root Port | The switch port currently assigned the root port role. |
| Root Cost | Root path cost. For a root bridge, this is zero. For other bridges, it is the sum of port path costs on the least cost path to the Root Bridge. |
| Topology Flag | The current state of the Topology Change Flag for the bridge instance. |
| Topology Change Last | The time since last Topology Change occurred. |
| Refresh | Click to refresh the page immediately. |
| Auto-refresh | Check this box to enable an automatic refresh of the page at regular intervals. |



STP Port Status

This page displays the STP port status for the currently selected switch.

STP Port Status

Auto-refresh

| Port | CIST Role | CIST State | Uptime |
|------|-----------|------------|--------|
| 1 | Non-STP | Forwarding | - |
| 2 | Non-STP | Forwarding | - |
| 3 | Non-STP | Forwarding | - |
| 4 | Non-STP | Forwarding | - |
| 5 | Non-STP | Forwarding | - |
| 6 | Non-STP | Forwarding | - |
| 7 | Non-STP | Forwarding | - |
| 8 | Non-STP | Forwarding | - |
| 9 | Non-STP | Forwarding | - |
| 10 | Non-STP | Forwarding | - |
| 11 | Non-STP | Forwarding | - |
| 12 | Non-STP | Forwarding | - |

| Label | Description |
|---------------------|--|
| Port | The switch port number to which the following settings will be applied. |
| CIST Role | The current STP port role of the CIST port. The values include: AlternatePort , BackupPort , RootPort , and DesignatedPort . |
| State | The current STP port state of the CIST port. The values include: Blocking , Learning , and Forwarding . |
| Uptime | The time since the bridge port is last initialized |
| Refresh | Click to refresh the page immediately. |
| Auto-refresh | Check this box to enable an automatic refresh of the page at regular intervals. |

STP Statistics

This page displays the STP port statistics for the currently selected switch.

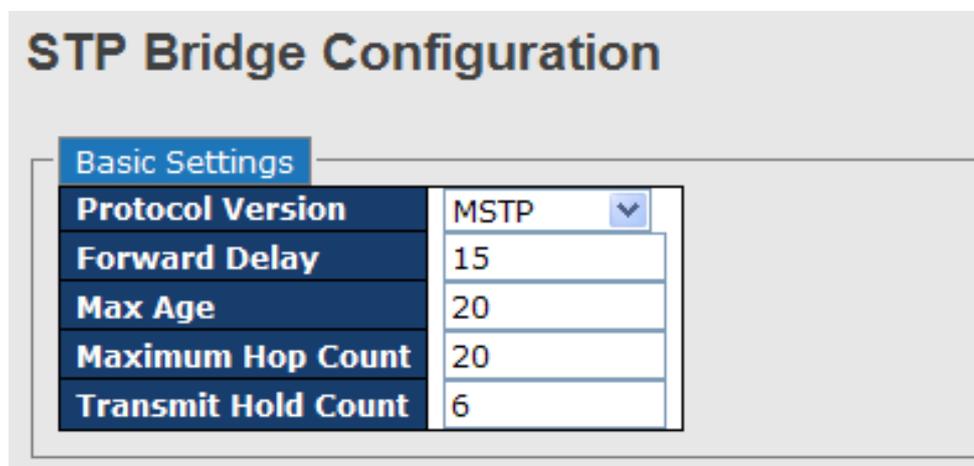
STP Statistics

Auto-refresh

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

| Label | Description |
|--------------------------|--|
| Port | The switch port number to which the following settings will be applied. |
| RSTP | The number of RSTP configuration BPDUs received/transmitted on the port |
| STP | The number of legacy STP configuration BPDUs received/transmitted on the port |
| TCN | The number of (legacy) topology change notification BPDUs received/transmitted on the port |
| Discarded Unknown | The number of unknown spanning tree BPDUs received (and discarded) on the port. |
| Discarded Illegal | The number of illegal spanning tree BPDUs received (and discarded) on the port. |
| Refresh | Click to refresh the page immediately |
| Auto-refresh | Check to enable an automatic refresh of the page at regular intervals |

STP Bridge Configurations



STP Bridge Configuration

Basic Settings

| | |
|----------------------------|------|
| Protocol Version | MSTP |
| Forward Delay | 15 |
| Max Age | 20 |
| Maximum Hop Count | 20 |
| Transmit Hold Count | 6 |

| Label | Description |
|-------------------------|---|
| Protocol Version | The version of the STP protocol. Valid values include STP, RSTP and MSTP. |
| Forward Delay | The delay used by STP bridges to transit root and designated ports to forwarding (used in STP compatible mode). The range of valid values is 4 to 30 seconds. |
| Max Age | The maximum time the information transmitted by the root bridge is considered valid. The range of valid values is 6 to 40 seconds, |

| | |
|----------------------------|--|
| | and Max Age must be $\leq (\text{FwdDelay}-1)*2$. |
| Maximum Hop Count | This defines the initial value of remaining hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. The range of valid values is 4 to 30 seconds, and MaxAge must be $\leq (\text{FwdDelay}-1)*2$. |
| Transmit Hold Count | The number of BPDUs a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. The range of valid values is 1 to 10 BPDUs per second. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

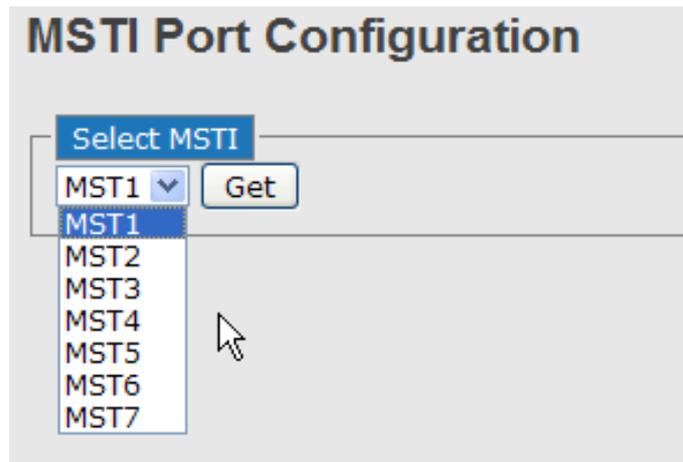
4.4.2 MSTP

Since the recovery time of STP and RSTP takes seconds, which are unacceptable in some industrial applications, MSTP was developed. The technology supports multiple spanning trees within a network by grouping and mapping multiple VLANs into different spanning-tree instances, known as MSTIs, to form individual MST regions. Each switch is assigned to an MST region. Hence, each MST region consists of one or more MSTP switches with the same VLANs, at least one MST instance, and the same MST region name. Therefore, switches can use different paths in the network to effectively balance loads.

Port Settings

This page allows you to examine and change the configurations of current MSTI ports. A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before MSTI port configuration options are displayed.

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



| MSTI Normal Ports Configuration | | | |
|---------------------------------|-----------|--|----------|
| Port | Path Cost | | Priority |
| 1 | Auto | | 128 |
| 2 | Auto | | 128 |
| 3 | Auto | | 128 |
| 4 | Auto | | 128 |
| 5 | Auto | | 128 |
| 6 | Auto | | 128 |

| Label | Description |
|------------------|--|
| Port | The switch port number of the corresponding STP CIST (and MSTI) port |
| Path Cost | Configures the path cost incurred by the port. Auto will set the path cost according to the physical link speed by using the 802.1D-recommended values. Specific allows you to enter a user-defined value. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range of valid values is 1 to 200000000. |
| Priority | Configures the priority for ports having identical port costs. (See above). |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

Mapping

This page allows you to examine and change the configurations of current STP MSTI bridge instance.



MSTI Configuration

Add VLANs separated by spaces or comma.

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

Configuration Identification

| | |
|-------------------------------|-------------------|
| Configuration Name | 00-1e-94-ff-ff-ff |
| Configuration Revision | 0 |

MSTI Mapping

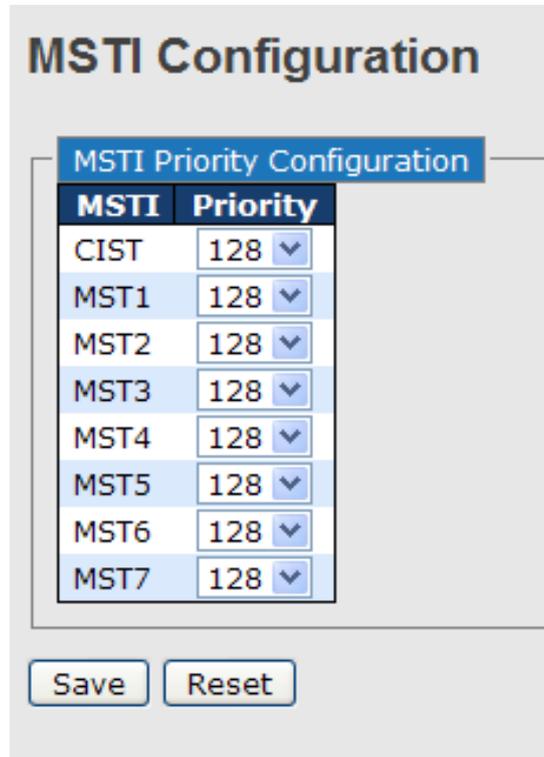
| MSTI | VLANs Mapped |
|------|--------------|
| MST1 | |
| MST2 | |
| MST3 | |
| MST4 | |
| MST5 | |
| MST6 | |
| MST7 | |

Save Reset

| Label | Description |
|-------------------------------|---|
| Configuration Name | The name which identifies the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configurations in order to share spanning trees for MSTIs (intra-region). The name should not exceed 32 characters. |
| Configuration Revision | Revision of the MSTI configuration named above. This must be an integer between 0 and 65535. |
| MSTI | The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. |
| VLANs Mapped | The list of VLANs mapped to the MSTI. The VLANs must be separated with commas and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI will be left empty (ex. without any mapped VLANs). |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

Priority

This page allows you to examine and change the configurations of current STP MSTI bridge instance priority.



The screenshot shows the 'MSTI Configuration' page. At the top, there is a title 'MSTI Configuration'. Below it is a section titled 'MSTI Priority Configuration' which contains a table with two columns: 'MSTI' and 'Priority'. The table lists instances from CIST to MST7, each with a priority of 128 and a dropdown arrow. Below the table are two buttons: 'Save' and 'Reset'.

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

| Label | Description |
|-----------------|---|
| MSTI | The bridge instance. CIST is the default instance, which is always active. |
| Priority | Indicates bridge priority. The lower the value, the higher the priority. The bridge priority, MSTI instance number, and the 6-byte MAC address of the switch forms a bridge identifier. |
| Save | Click to save changes |
| Reset | Click to undo any changes made locally and revert to previously saved values |

4.4.3 CIST

With the ability to cross regional boundaries, CIST is used by MSTP to communicate with other MSTP regions and with any RSTP and STP single-instance spanning trees in the network. Any boundary port, that is, if it is connected to another region, will automatically belong solely to CIST, even if it is assigned to an MSTI. All VLANs that are not members of particular MSTIs are members of the CIST.



Port Settings

STP CIST Ports Configuration

CIST Aggregated Ports Configuration

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

CIST Normal Ports Configuration

| Port | STP Enabled | Path Cost | Priority | Admin Edge | Auto Edge | Restricted Role | TCN | BPDU Guard | Point-to-point |
|------|--------------------------|-----------|----------|------------|-------------------------------------|--------------------------|--------------------------|--------------------------|----------------|
| 1 | <input type="checkbox"/> | Auto | 128 | Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 2 | <input type="checkbox"/> | Auto | 128 | Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 3 | <input type="checkbox"/> | Auto | 128 | Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 4 | <input type="checkbox"/> | Auto | 128 | Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 5 | <input type="checkbox"/> | Auto | 128 | Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 6 | <input type="checkbox"/> | Auto | 128 | Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |

| Label | Description |
|-------------------------------|--|
| Port | The switch port number to which the following settings will be applied. |
| STP Enabled | Check to enable STP for the port |
| Path Cost | Configures the path cost incurred by the port. Auto will set the path cost according to the physical link speed by using the 802.1D-recommended values. Specific allows you to enter a user-defined value. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range of valid values is 1 to 200000000. |
| Priority | Configures the priority for ports having identical port costs. (See above). |
| OpenEdge (setate flag) | A flag indicating whether the port is connected directly to edge devices or not (no bridges attached). Transiting to the forwarding state is faster for edge ports (operEdge set to true) than other ports. |
| AdminEdge | Configures the operEdge flag to start as set or cleared.(the initial operEdge state when a port is initialized). |
| AutoEdge | Check to enable the bridge to detect edges at the bridge port automatically. This allows operEdge to be derived from whether BPDUs are received on the port or not. |
| Restricted Role | When enabled, the port will not be selected as root port for CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an alternate port after the root port |

| | |
|-----------------------|--|
| | has been selected. If set, spanning trees will lose connectivity. It can be set by a network administrator to prevent bridges outside a core region of the network from influencing the active spanning tree topology because those bridges are not under the full control of the administrator. This feature is also known as Root Guard. |
| Restricted TCN | When enabled, the port will not propagate received topology change notifications and topology changes to other ports. If set, it will cause temporary disconnection after changes in an active spanning trees topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges outside a core region of the network from causing address flushing in that region because those bridges are not under the full control of the administrator or is the physical link state for the attached LANs transitions frequently. |
| Point2Point | Configures whether the port connects to a point-to-point LAN rather than a shared medium. This can be configured automatically or set to true or false manually. Transitioning to forwarding state is faster for point-to-point LANs than for shared media. |
| Save | Click to save changes. |
| Reset | Click to undo any changes made locally and revert to previously saved values. |

4.5 Fast Recovery

Fast recovery mode can be set to connect multiple ports to one or more switches. The CPGS-9120-M12-C with fast recovery mode will provide redundant links. Fast recovery mode supports 12 priorities. Only the first priority will be the active port, and the other ports with different priorities will be backup ports.

Fast Recovery Mode

| | |
|---|---|
| <input checked="" type="checkbox"/> Active | |
| Port.01 | Not included <input type="button" value="v"/> |
| Port.02 | Not included <input type="button" value="v"/> |
| Port.03 | Not included <input type="button" value="v"/> |
| Port.04 | Not included <input type="button" value="v"/> |
| Port.05 | Not included <input type="button" value="v"/> |

| Label | Description |
|---------------|--|
| Active | Activate fast recovery mode |
| port | Ports can be set to 12 priorities. Only the port with the highest priority will be the active port. 1st Priority is the highest. |
| Apply | Click to activate 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.

Note: 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.

Management via Web Browser

Follow the steps below to manage your switch via a Web browser

System Login

1. Launch an 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. Press **Enter** or click **OK**, the management page appears.



Note: you can use 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**

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

Information Message

| System | |
|-------------------------|---|
| Name | CPGS-9120-M12-C |
| Description | Industrial 12-port CompactPCI managed Gigabit Ethernet switch with 12x10/100/1000Base-T(X), M12 connector |
| Location | |
| Contact | |
| OID | 1.3.6.1.4.1.25972.100.0.11.120 |
| Hardware | |
| MAC Address | 00-1e-94-01-67-35 |
| Time | |
| System Date | 1970-01-01T00:03:58+00:00 |
| System Uptime | 0d 00:03:58 |
| Software | |
| Kernel Version | v9.00 |
| Software Version | v1.00 |
| Software Date | 2013-03-13T14:14:08+08:00 |

Auto-refresh

On the right hand side of the management interface shows links to various settings. Clicking on the links will bring you to individual configuration pages.

5.1 Basic Settings

The Basic Settings page allows you to configure the basic functions of the switch.

5.1.1 System Information

This page shows the general information of the switch.

System Information Configuration

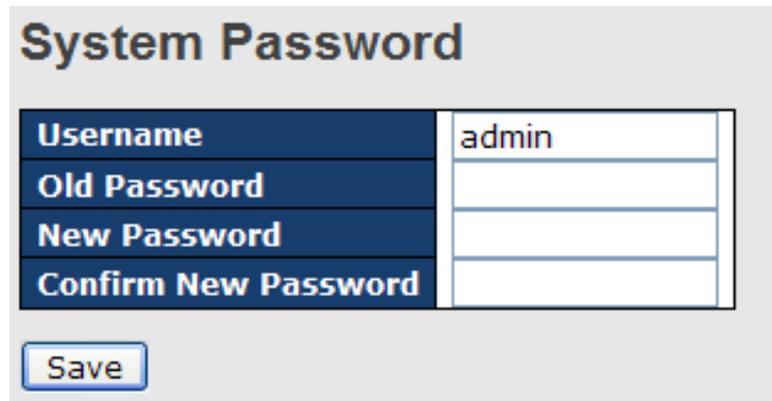
| | |
|---------------------------|--|
| System Name | <input type="text" value="CPGS-9120-M12-C"/> |
| System Description | <input type="text" value="Industrial 12-port CompactPCI"/> |
| System Location | <input type="text"/> |
| System Contact | <input type="text"/> |

| 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. |

5.1.2 Admin & Password

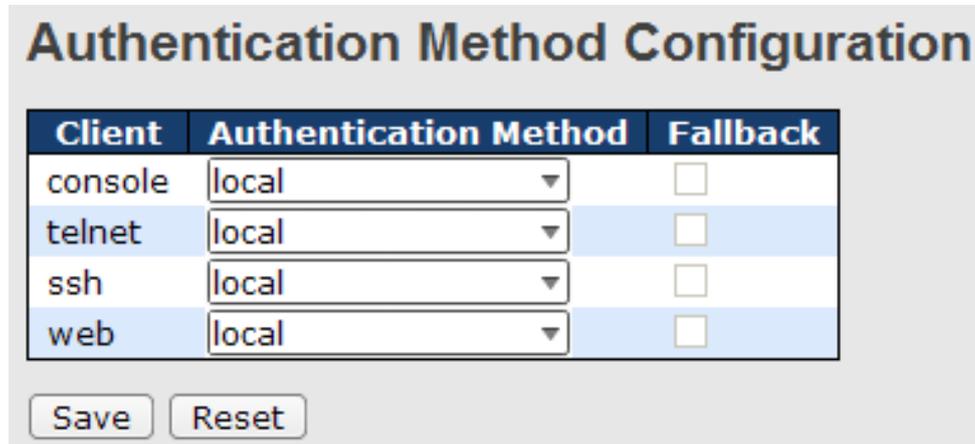
This page allows you to configure the system password required to access the web pages or log in from CLI.



| Label | Description |
|-------------------------|--|
| Old Password | 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 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.



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

Save Reset

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

This page allows you to configure IP information for the switch. You can specify configure the settings manually by disabling DHCP Client. After inputting the values, click **Renew** and the new values will be applied, which will be displayed under **Current**.

IP Configuration

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

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

5.1.5 IPv6 Settings

IPv6 is the next-generation IP that uses a 128-bit address standard. It is developed to supplement, and eventually replace the IPv4 protocol. You can configure IPv6 information of the switch on the following page.

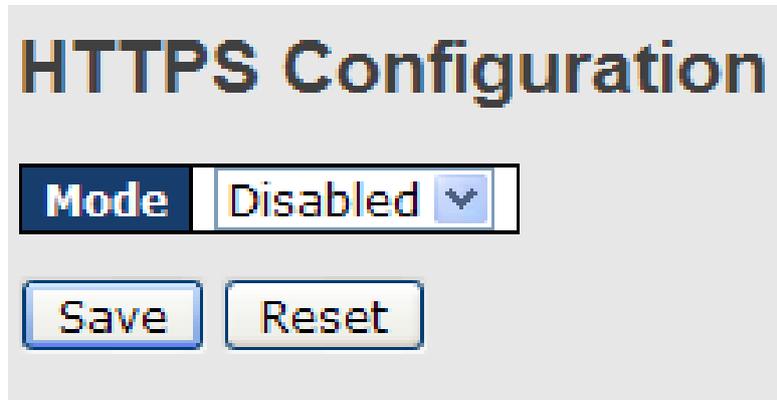
IPv6 Configuration

| | Configured | Current |
|--------------------|--|--|
| Auto Configuration | <input type="checkbox"/> | <input type="button" value="Renew"/> |
| Address | <input type="text" value="::192.0.2.1"/> | ::192.0.2.1 Link-Local Address: fe80::21e:94ff:fe01:6735 |
| Prefix | <input type="text" value="96"/> | 96 |
| Router | <input type="text" value="::"/> | :: |

| 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 | Specify an IPv6 address for 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 | Specify an IPv6 prefix for the switch. The allowed range is 1 to 128. |
| Router | Specify an IPv6 address for 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 HTTPS

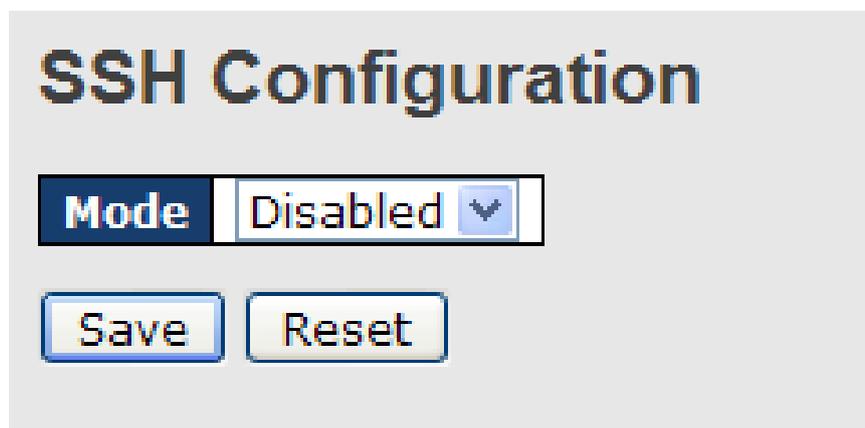
You can configure the HTTPS mode in the following page.



| 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: Enabled: enable HTTPS. Disabled: disable HTTPS. |
| Save | Click to save changes |
| Reset | Click to undo any changes made locally and revert to previously saved values |

5.1.7 SSH

SSH (Secure Shell) is a cryptographic network protocol intended for secure data transmission and remote access by creating a secure channel between two networked PCs. You can configure the SSH mode in the following page.

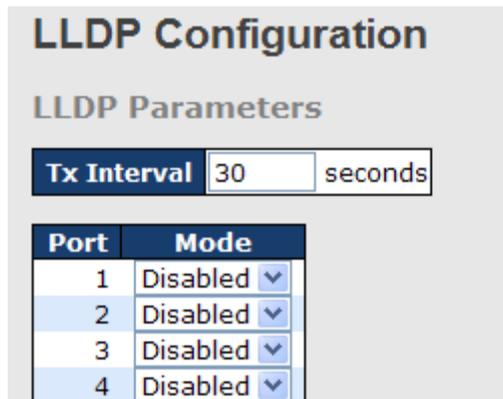


| Label | Description |
|--------------|---|
| Mode | Indicates the selected SSH mode. The modes include: Enabled: enable SSH. Disabled: disable SSH. |
| Save | Click to save changes |
| Reset | Click to undo any changes made locally and revert to previously saved values |

5.1.8 LLDP

LLDP Configurations

LLDP (Link Layer Discovery Protocol) provides a method for networked devices to receive and/or transmit their information to other connected devices on the network that are also using the protocols, and to store the information that is learned about other devices. This page allows you to examine and configure current LLDP port settings.



LLDP Configuration

LLDP Parameters

Tx Interval seconds

| Port | Mode |
|------|----------|
| 1 | Disabled |
| 2 | Disabled |
| 3 | Disabled |
| 4 | Disabled |

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



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:

| | |
|----------------------------|--|
| 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: <ol style="list-style-type: none">1. Other2. Repeater3. Bridge4. WLAN Access Point5. Router6. Telephone7. DOCSIS Cable Device8. Station Only9. Reserved 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 |

LLDP 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.



Auto-refresh Refresh Clear

| Global Counters | |
|---|---|
| Neighbor entries were last changed at 1970-01-01 04:03:03 +0000 (26 sec. ago) | |
| Total Neighbors Entries Added | 1 |
| Total Neighbors Entries Deleted | 0 |
| Total Neighbors Entries Dropped | 0 |
| Total Neighbors Entries Aged Out | 0 |

LLDP Statistics

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

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 |

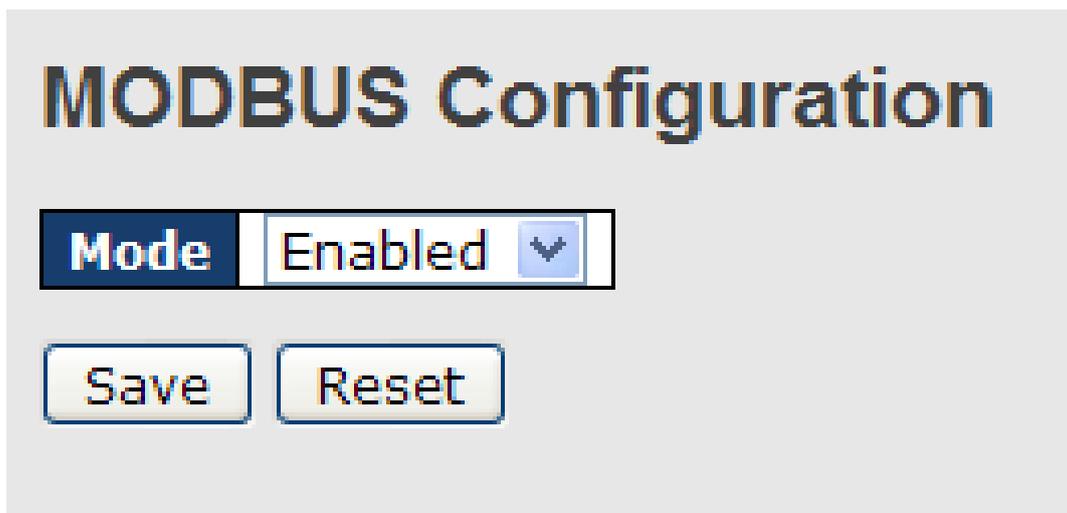
Local Counters

| 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 |

5.1.9 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 | Enable or Disable Modbus TCP function |

5.1.10 Backup/Restore Configurations

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



5.1.11 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 Basic 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.

DHCP Server Configuration

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

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.

DHCP Dynamic Client List

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

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.

DHCP Client List

| | |
|--------------------|----------------------|
| MAC Address | <input type="text"/> |
| IP Address | <input type="text"/> |

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

5.2.4 DHCP Relay

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.

DHCP Relay Configuration

| | |
|---------------------------------|------------|
| Relay Mode | Disabled ▾ |
| Relay Server | 0.0.0.0 |
| Relay Information Mode | Enabled ▾ |
| Relay Information Policy | Replace ▾ |

| Label | Description |
|-------------------------------|--|
| Relay Mode | <p>Indicates the existing DHCP relay mode. The modes include:</p> <p>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.</p> <p>Disabled: disable DHCP relay</p> |
| Relay Server | <p>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.</p> |
| Relay Information Mode | <p>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</p> |



| | |
|--|---|
| | <p>ID 1, and port No. 8. The option 82 remote ID value equals to the switch MAC address.</p> <p>The modes include:</p> <p>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.</p> <p>Disabled: disable DHCP relay information</p> |
| <p>Relay Information Policy</p> | <p>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:</p> <p>Replace: replace the original relay information when a DHCP message containing the information is received.</p> <p>Keep: keep the original relay information when a DHCP message containing the information is received.</p> <p>Drop: drop the package when a DHCP message containing the information is received.</p> |

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

Auto-refresh

DHCP Relay Statistics

Server Statistics

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

| Label | Description |
|----------------------------|--|
| Transmit to 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 |

Client Statistics

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

| Label | Description |
|-----------------------------|--|
| Transmit to Client | The number of 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.



Port Configuration

Refresh

| Port | Link | Speed | | Flow Control | | | Maximum Frame Size | Power Control |
|------|--------|---------|------------|--------------|------------|--------------------------|--------------------|---------------|
| | | Current | Configured | Current Rx | Current Tx | Configured | | |
| * | | | <> | | | <input type="checkbox"/> | 9600 | <> |
| 1 | ● Down | Down | Auto | ✗ | ✗ | <input type="checkbox"/> | 9600 | Disabled |
| 2 | ● Down | Down | Auto | ✗ | ✗ | <input type="checkbox"/> | 9600 | Disabled |
| 3 | ● Down | Down | Auto | ✗ | ✗ | <input type="checkbox"/> | 9600 | Disabled |
| 4 | ● Down | Down | Auto | ✗ | ✗ | <input type="checkbox"/> | 9600 | Disabled |
| 5 | ● Down | Down | Auto | ✗ | ✗ | <input type="checkbox"/> | 9600 | Disabled |
| 6 | ● Down | Down | Auto | ✗ | ✗ | <input type="checkbox"/> | 9600 | Disabled |
| 7 | ● Down | Down | Auto | ✗ | ✗ | <input type="checkbox"/> | 9600 | Disabled |
| 8 | ● Down | Down | Auto | ✗ | ✗ | <input type="checkbox"/> | 9600 | Disabled |

| 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 Auto selects the highest speed supported by the link partner Disabled disables switch port configuration <> 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. |

| | |
|----------------|---|
| | <p>Disabled: all power savings functions are disabled</p> <p>ActiPHY: link down and power savings enabled</p> <p>PerfectReach: link up and power savings enabled</p> <p>Enabled: both link up and link down power savings enabled</p> |
| 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 Trunk

A port trunk is a group of ports that have been grouped together to function as one logical path. This method provides an economical way for you to increase the bandwidth between the switch and another networking device. In addition, it is useful when a single physical link between the devices is insufficient to handle the traffic load. This page allows you to configure the aggregation hash mode and the aggregation group.

Aggregation Mode Configuration

| Hash Code Contributors | |
|-------------------------|-------------------------------------|
| Source MAC Address | <input checked="" type="checkbox"/> |
| Destination MAC Address | <input type="checkbox"/> |
| IP Address | <input checked="" type="checkbox"/> |
| TCP/UDP Port Number | <input checked="" type="checkbox"/> |

| 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 Number | Port | 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. |
|-----------------------|-------------|---|

Aggregation Group Configuration

| Group ID | Port Members | | | | | | | | | | | |
|----------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Normal | <input checked="" type="radio"/> |
| 1 | <input type="radio"/> |
| 2 | <input type="radio"/> |
| 3 | <input type="radio"/> |
| 4 | <input type="radio"/> |
| 5 | <input type="radio"/> |
| 6 | <input type="radio"/> |

| 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 LACP

LACP (Link Aggregation Control Protocol) 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. This page allows you to enable LACP functions to group ports together to form single virtual links and change associated settings, thereby increasing the bandwidth between the switch and other LACP-compatible devices.

LACP Port Configuration

Open in new window

| Port | LACP Enabled | Key | Role |
|------|--------------------------|------|--------|
| 1 | <input type="checkbox"/> | Auto | Active |
| 2 | <input type="checkbox"/> | Auto | Active |
| 3 | <input type="checkbox"/> | Auto | Active |
| 4 | <input type="checkbox"/> | Auto | Active |

| 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 changes made locally and revert to previous values |

LACP System Status

This page provides a status overview for all LACP instances.

LACP System Status

Auto-refresh Refresh Open in new window

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



| Label | Description |
|--------------------------|--|
| Aggr ID | The aggregation ID 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. |
| Local Ports | Indicates which ports belong to the aggregation of the switch/stack. The format is: " Switch ID:Port ". |
| Refresh | Click to refresh the page immediately |
| Auto-refresh | Check to enable an automatic refresh of the page at regular intervals |

LACP Status

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

LACP Status

Auto-refresh Refresh Open in new window

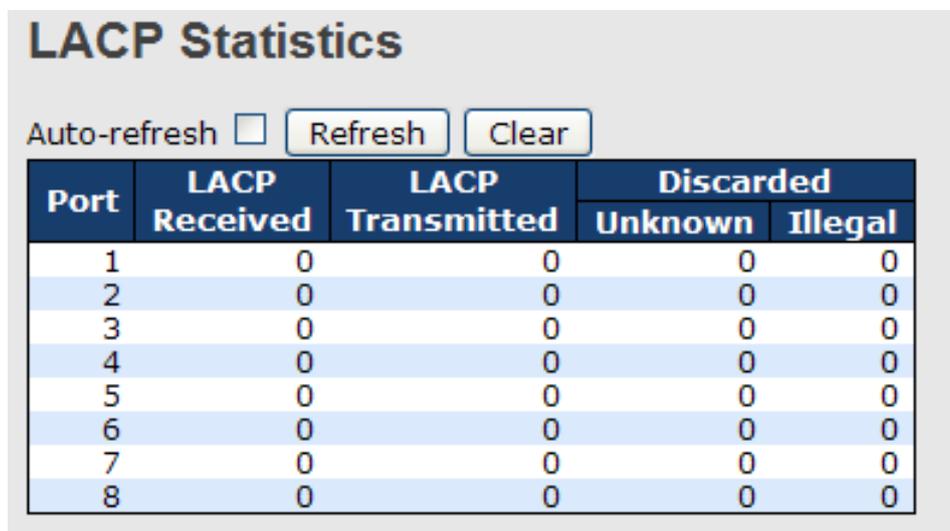
| Port | LACP | Key | Aggr ID | Partner System ID | Partner Port |
|------|------|-----|---------|-------------------|--------------|
| 1 | No | - | - | - | - |
| 2 | No | - | - | - | - |
| 3 | No | - | - | - | - |
| 4 | No | - | - | - | - |
| 5 | No | - | - | - | - |

| 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 |
| Auto-refresh | Check to enable an automatic refresh of the page at regular intervals |

LACP Statistics

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



| Port | LACP Received | LACP Transmitted | Discarded | |
|------|---------------|------------------|-----------|---------|
| | | | Unknown | Illegal |
| 1 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 |

| 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 |
| Auto-refresh | Check to enable an automatic refresh of the page at regular intervals |
| Clear | Click to clear the counters for all ports |

5.3.4 Loop Guard

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

General Settings

Global Configuration

| | |
|-------------------------------|-------------|
| Enable Loop Protection | Disable ▾ |
| Transmission Time | 5 seconds |
| Shutdown Time | 180 seconds |

| 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). |

Port Configuration

| Port | Enable | Action | Tx Mode |
|------|-------------------------------------|-----------------|----------|
| * | <input checked="" type="checkbox"/> | <> ▾ | <> ▾ |
| 1 | <input checked="" type="checkbox"/> | Shutdown Port ▾ | Enable ▾ |
| 2 | <input checked="" type="checkbox"/> | Shutdown Port ▾ | Enable ▾ |
| 3 | <input checked="" type="checkbox"/> | Shutdown Port ▾ | Enable ▾ |
| 4 | <input checked="" type="checkbox"/> | Shutdown Port ▾ | Enable ▾ |
| 5 | <input checked="" type="checkbox"/> | Shutdown Port ▾ | Enable ▾ |
| 6 | <input checked="" type="checkbox"/> | Shutdown Port ▾ | Enable ▾ |

| 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. |

5.4 VLAN

5.4.1 VLAN Membership

A VLAN (Virtual LAN) is a logical LAN based on a physical LAN with links that does not consist of a physical (wired or wireless) connection between two computing devices but is implemented using methods of network virtualization. A VLAN can be created by partitioning a physical LAN into multiple logical LANs using a VLAN ID. You can assign switch ports to a VLAN and add new VLANs in this page.

VLAN Membership Configuration

Start from VLAN with entries per page.

| Delete | VLAN ID | VLAN Name | Port Members | | | | | | | | |
|--------------------------|---------|-----------|--------------|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | |
| <input type="checkbox"/> | 1 | default | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Label | Description |
|---------------------|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| VLAN ID | The VLAN ID for the entry |
| MAC Address | The MAC address for the entry |
| Port Members | Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry |
| Add New VLAN | <p>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.</p> <p>After clicking Save, the new VLAN will be enabled on the selected switch stack but contains no port members.</p> <p>A VLAN without any port members on any stack will be deleted when you click Save.</p> <p>Click Delete to undo the addition of new VLANs.</p> |

5.4.2 Port Configurations

This page allows you to set up VLAN ports individually.

Auto-refresh

Ethertype for Custom S-ports 0x

VLAN Port Configuration

| Port | Port Type | Ingress Filtering | Frame Type | Port VLAN | | Tx Tag |
|------|-----------|--------------------------|------------|-----------|----|------------|
| | | | | Mode | ID | |
| * | <> | <input type="checkbox"/> | <> | <> | 1 | <> |
| 1 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 2 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 3 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 4 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 5 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 6 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 7 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 8 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |

| 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 |

| | |
|---------------------|---|
| | <p>VLAN ingress and egress processing.</p> <p>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.</p> <p>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.</p> |
| Port VLAN ID | <p>Configures the VLAN identifier for the port. The allowed range of the values is 1 through 4095. The default value is 1.</p> <p>Note: The port must be a member of the same VLAN as the port VLAN ID.</p> |
| Tx Tag | <p>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.</p> |

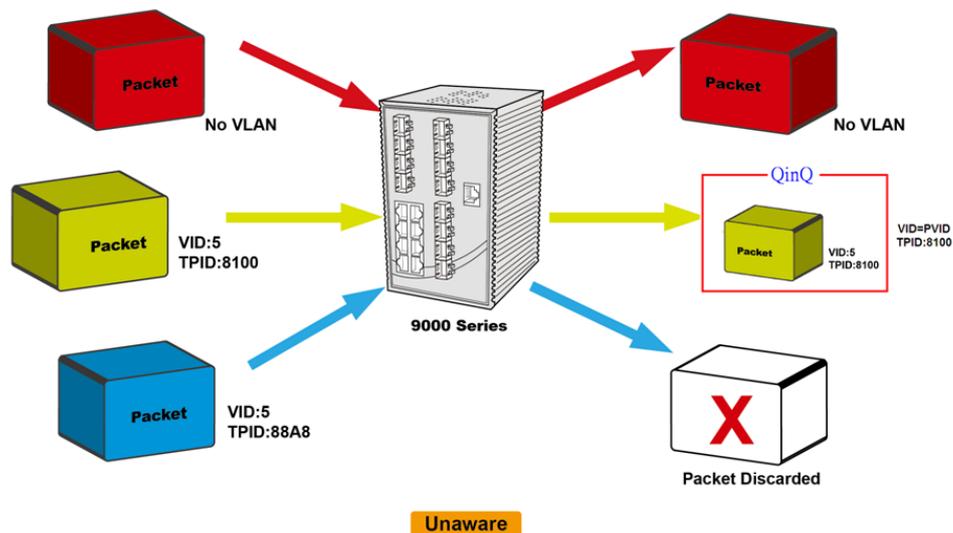
Introduction of Port Types

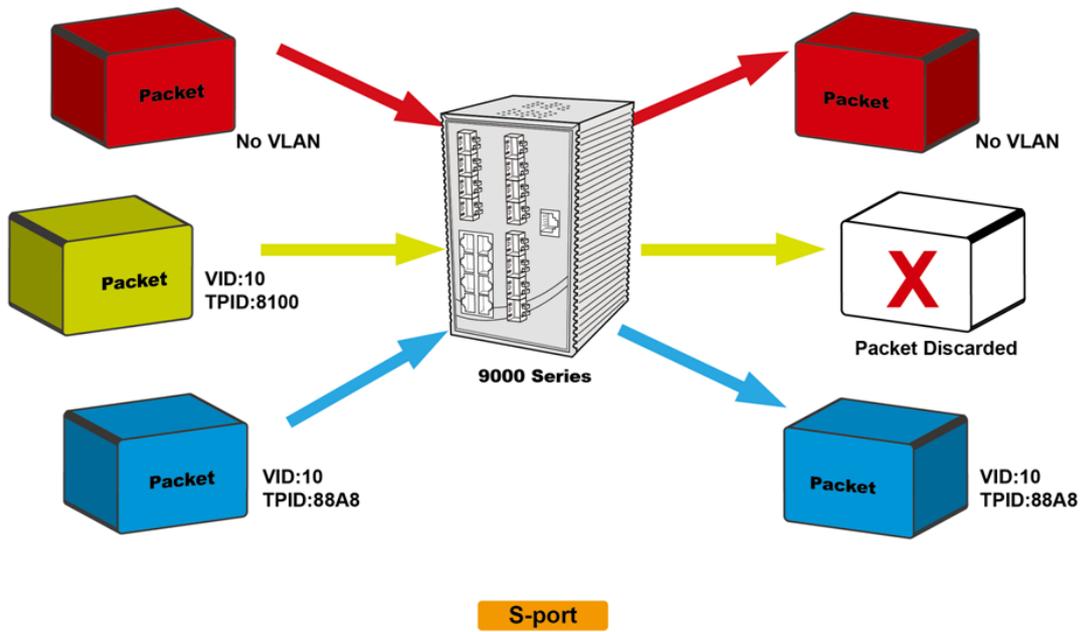
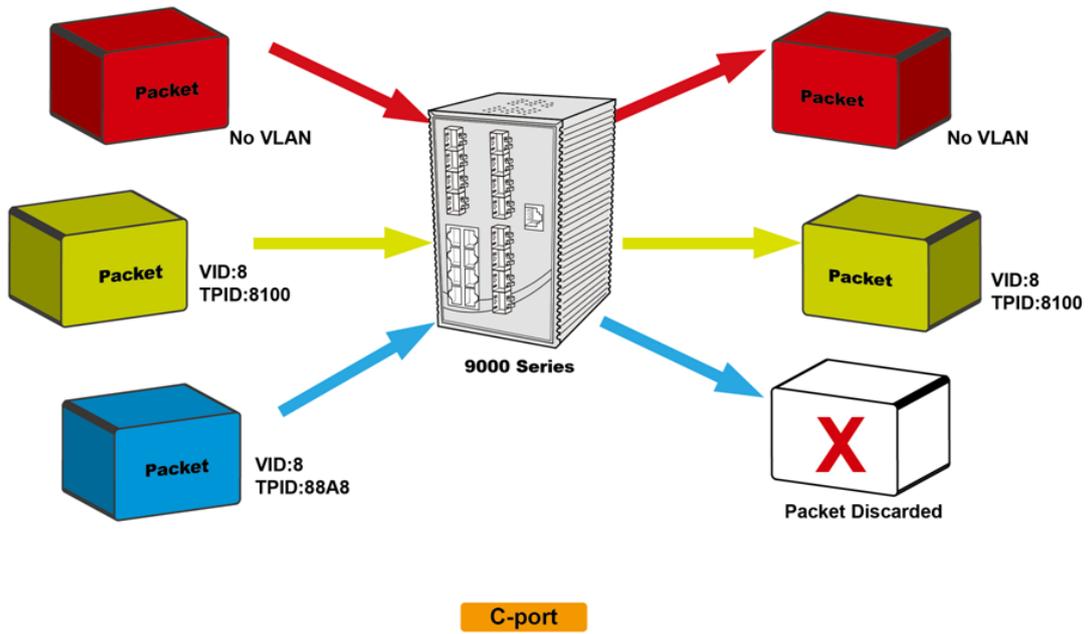
Below is a detailed description of each port type, including Unaware, C-port, S-port, and S-custom-port.

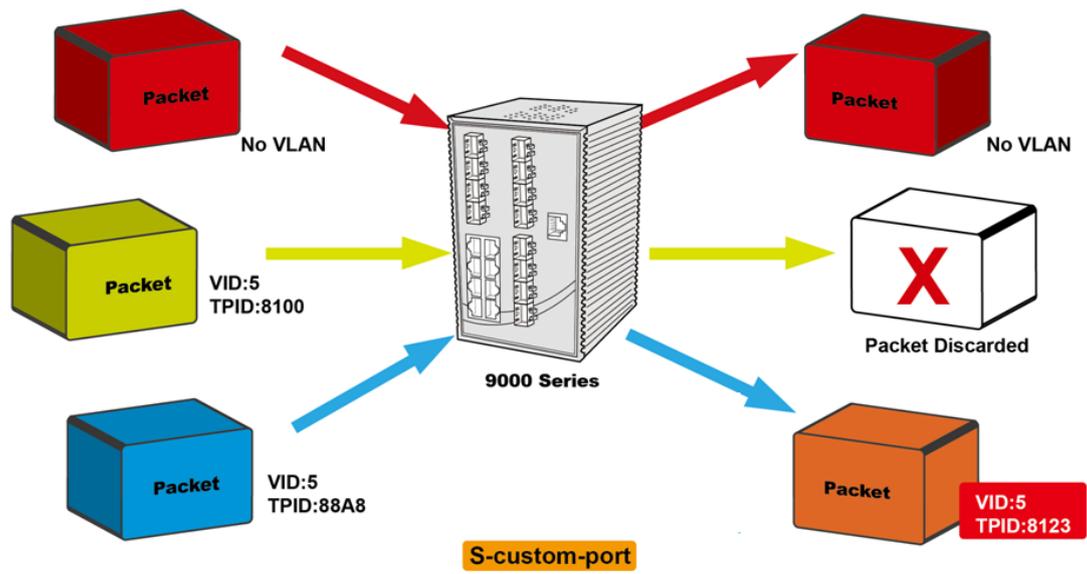
| | Ingress action | Egress action |
|--|--|--|
| Unaware The function of Unaware can be used for 802.1QinQ (double tag). | <p>When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded.</p> <p>When the port receives tagged frames:</p> <ol style="list-style-type: none"> 1. If the tagged frame contains a TPID of 0x8100, it will become a double-tag frame and will be forwarded. 2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded. | <p>The TPID of a frame transmitted by Unaware port will be set to 0x8100.</p> <p>The final status of the frame after egressing will also be affected by the Egress Rule.</p> |
| C-port | <p>When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded.</p> | <p>The TPID of a frame transmitted by C-port will be set to 0x8100.</p> |

| | | |
|----------------------|--|---|
| | When the port receives tagged frames: <ol style="list-style-type: none"> 1. If the tagged frame contains a TPID of 0x8100, it will be forwarded. 2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded. | |
| S-port | When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded. When the port receives tagged frames: <ol style="list-style-type: none"> 1. If the tagged frame contains a TPID of 0x8100, it will be forwarded. 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. When the port receives tagged frames: <ol style="list-style-type: none"> 1. If the tagged frame contains a TPID of 0x8100, it will be forwarded. 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 . |

Below are the illustrations of different port types:



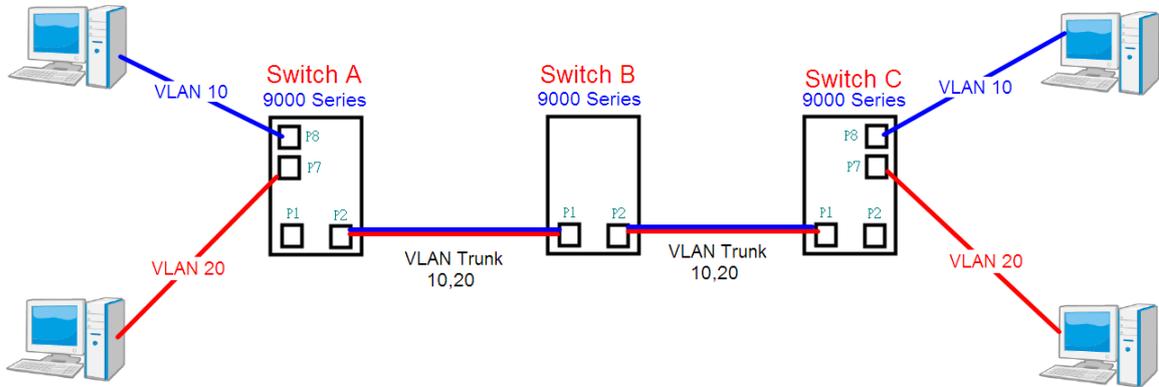




S-custom-port is used for user defined TPID .While Ethertype for Custom S-ports is configured to 8123 , outgoing packet will bring with TPID 8123 tag .

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.

- Open all
- System Information
- Front Panel
- Basic Setting
- DHCP Server/Relay
- Port Setting
- Redundancy
- VLAN
 - VLAN Membership
 - Ports
 - Private VLAN
- SNMP
- Traffic Prioritization
- Multicast
- Security
- Warning
- Monitor and Diag
- Synchronization
- PoE

VLAN Membership Configuration

Refresh | << | >>

Start from VLAN with entries per page.

| Delete | VLAN ID | VLAN Name | Port Members | | | | | | | | | | | | |
|--------------------------|---------|-----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | |
| <input type="checkbox"/> | 1 | default | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> | 10 | vlan10 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | 20 | vlan20 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Add New VLAN

Save Reset

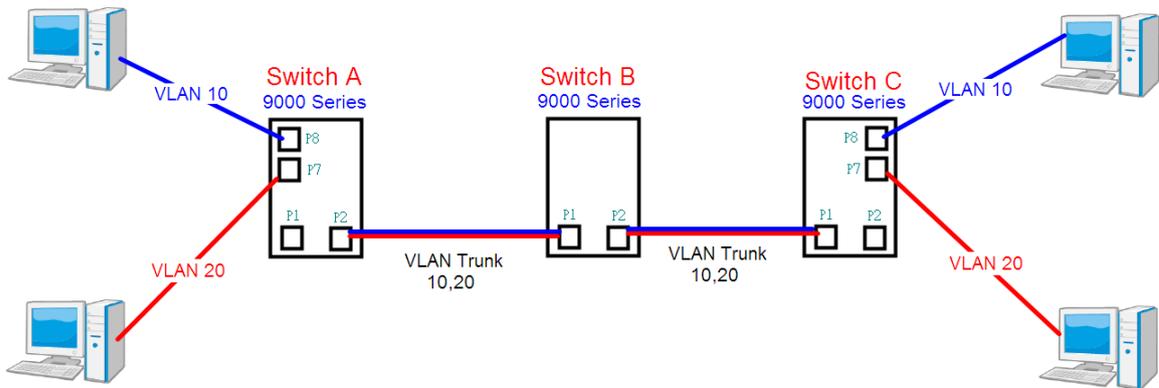
for port 1 VLAN trunk setting

for port 7 & port 8 VLAN Access

- VLAN
 - VLAN Membership
 - Ports
 - Private VLAN
- SNMP
- Traffic Prioritization
- Multicast
- Security
- Warning
- Monitor and Diag
- Synchronization
- PoE
- Factory Default
- System Reboot

| Port | Port Type | Ingress Filtering | Frame Type | Mode | ID | Px Tag |
|------|-----------|--------------------------|------------|----------|----|------------|
| * | <> | <input type="checkbox"/> | <> | <> | 1 | <> |
| 1 | C-port | <input type="checkbox"/> | Tagged | Specific | 1 | Tag_all |
| 2 | Unaware | <input type="checkbox"/> | All | None | 1 | Untag_pvid |
| 3 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 4 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 5 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 6 | Unaware | <input type="checkbox"/> | Untagged | Specific | 10 | Untag_pvid |
| 7 | Unaware | <input type="checkbox"/> | Untagged | Specific | 20 | Untag_pvid |
| 8 | Unaware | <input type="checkbox"/> | Untagged | Specific | 30 | Untag_pvid |
| 9 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 10 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 11 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |

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 Membership Configuration

Refresh | << >>

Start from VLAN 1 with 20 entries per page.

| Delete | VLAN ID | VLAN Name | Port Members | | | | | | | | | | | |
|--------------------------|---------|-----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| <input type="checkbox"/> | 1 | default | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> | 10 | VLAN10 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | 20 | VLAN20 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Add New VLAN

Save Reset

Auto-refresh Refresh

Ethertype for Custom S-ports 0x88A8

VLAN Port Configuration

| Port | Port Type | Ingress Filtering | Frame Type | Port VLAN | | Tx Tag |
|------|-----------|--------------------------|------------|-----------|----|------------|
| | | | | Mode | ID | |
| * | <> | <input type="checkbox"/> | <> | <> | 1 | <> |
| 1 | C-port | <input type="checkbox"/> | Tagged | Specific | 1 | Tag_all |
| 2 | C-port | <input type="checkbox"/> | Tagged | Specific | 1 | Tag_all |
| 3 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 4 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 5 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 6 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 7 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 8 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 9 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 10 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 11 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 12 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |

Save Reset

VLAN Hybrid Mode:

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

Below are the switch settings.

VLAN Membership Configuration

Refresh | << | >>

Start from VLAN 1 with 20 entries per page.

| Delete | VLAN ID | VLAN Name | Port Members | | | | | | | | | | | | |
|--------------------------|---------|-----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | |
| <input type="checkbox"/> | 1 | default | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> | 10 | vlan10 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | 20 | vlan20 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Add New VLAN

Save Reset

Auto-refresh Refresh

Ethertype for Custom S-ports 0x88A8

VLAN Port Configuration

| Port | Port Type | Ingress Filtering | Frame Type | Port VLAN | | Tx Tag |
|------|-----------|--------------------------|------------|-----------|----|------------|
| | | | | Mode | ID | |
| * | <> | <input type="checkbox"/> | <> | <> | 1 | <> |
| 1 | C-port | <input type="checkbox"/> | All | Specific | 10 | Untag_all |
| 2 | Unaware | <input type="checkbox"/> | All | None | 1 | Untag_pvid |
| 3 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 4 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 5 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 6 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 7 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 8 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 9 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 10 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 11 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |
| 12 | Unaware | <input type="checkbox"/> | All | Specific | 1 | Untag_pvid |

Save Reset

VLAN ID Settings

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

9000ies VLAN Settings:

Open all

- System Information
- Front Panel
- Basic Setting
 - Basic Setting
 - Admin Password
 - Auth Method
 - IP Setting
 - IPv6 Setting
 - HTTPS
 - SSH
 - LLDP
 - Modbus TCP
 - Backup
 - Restore
 - Upgrade Firmware

IP Configuration

| | Configured | Current |
|-------------|--------------------------|--------------------------------------|
| DHCP Client | <input type="checkbox"/> | <input type="button" value="Renew"/> |
| IP Address | 192.168.10.2 | 192.168.10.2 |
| IP Mask | 255.255.255.0 | 255.255.255.0 |
| IP Router | 0.0.0.0 | 0.0.0.0 |
| VLAN ID | 1 | 1 |
| SNTP Server | | |

5.4.3 Private VLAN

A private VLAN contains switch ports that can only communicate with a given "uplink". The restricted ports are called private ports. Each private VLAN typically contains many private ports and a single uplink. The switch forwards all frames received on a private port out the uplink port, regardless of VLAN ID or destination MAC address. A port must be a member of both a VLAN and a private VLAN to be able to forward packets. This page allows you to configure private VLAN memberships for the switch. By default, all ports are VLAN unaware and members of VLAN 1 and private VLAN 1.

Auto-refresh

Private VLAN Membership Configuration

| | | Port Members | | | | | | | |
|--------------------------|----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Delete | PVLAN ID | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| <input type="checkbox"/> | 1 | <input checked="" type="checkbox"/> |

| Label | Description |
|----------------------------------|--|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Private VLAN ID | Indicates the ID of this particular private VLAN. |
| MAC Address | The MAC address for the entry. |
| Port Members | A row of check boxes for each port is displayed for each private VLAN ID. 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 a New Static Entry | <p>Click Add new Private VLAN to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click OK to discard the incorrect entry, or click Cancel to return to the editing and make a correction.</p> <p>The private VLAN is enabled when you click Save.</p> <p>The Delete button can be used to undo the addition of new private VLANs.</p> |

A private VLAN is defined as a pairing of a primary VLAN with a secondary VLAN. A promiscuous port is a port that can communicate with all other private VLAN port types via the primary VLAN and any associated secondary VLANs, whereas isolated ports can communicate only with a promiscuous port.

Port Isolation Configuration

| Port Number | | | | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| <input type="checkbox"/> |

Save

Reset

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

5.5 SNMP

SNMP (Simple Network Management Protocol) is a protocol for managing devices on IP networks. It is mainly used network management systems to monitor the operational status of networked devices. In an event-triggered situation, traps and notifications will be sent to administrators.

5.5.1 SNMP System Configurations

SNMP System Configuration

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

| Label | Description |
|-----------------------|--|
| Mode | Indicates existing SNMP mode. Possible modes include: Enabled: enable SNMP mode Disabled: disable SNMP mode |
| Version | Indicates the supported SNMP version. Possible versions include: SNMP v1: supports SNMP version 1. SNMP v2c: supports SNMP version 2c. 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. 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 | <p>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.</p> <p>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.</p> |
| Engine ID | <p>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.</p> |

SNMP Trap Configuration

| | |
|--------------------------------------|----------|
| Trap Mode | Disabled |
| Trap Version | SNMP v1 |
| Trap Community | public |
| Trap Destination Address | |
| Trap Destination IPv6 Address | :: |
| Trap Authentication Failure | Enabled |
| Trap Link-up and Link-down | Enabled |
| Trap Inform Mode | Enabled |
| Trap Inform Timeout (seconds) | 1 |
| Trap Inform Retry Times | 5 |

| Label | Description |
|-----------------------|--|
| Trap Mode | <p>Indicates existing SNMP trap mode. Possible modes include:</p> <p>Enabled: enable SNMP trap mode</p> <p>Disabled: disable SNMP trap mode</p> |
| Trap Version | <p>Indicates the supported SNMP trap version. Possible versions include:</p> <p>SNMP v1: supports SNMP trap version 1</p> <p>SNMP v2c: supports SNMP trap version 2c</p> <p>SNMP v3: supports SNMP trap version 3</p> |
| 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: Enabled: enable SNMP trap authentication failure Disabled: disable SNMP trap authentication failure |
| Trap Link-up and Link-down | Indicates the SNMP trap link-up and link-down mode. Possible modes include: Enabled: enable SNMP trap link-up and link-down mode Disabled: disable SNMP trap link-up and link-down mode |
| Trap Inform Mode | Indicates the SNMP trap inform mode. Possible modes include: Enabled: enable SNMP trap inform mode 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 SNMP Community Configurations

You can define access to the SNMP data on your devices by creating one or more SNMP communities. An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. This page allows you to configure SNMPv3 community table. The entry index key is **Community**.

SNMPv3 Communities Configuration

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

| Label | Description |
|--------------------|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Community | Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and 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 SNMP User Configurations

Each SNMP user has a specified username, a group to which the user belongs, authentication password, authentication protocol, privacy protocol, and privacy password. When you create a user, you must associate it with an SNMP group. The user then inherits the security model of the group. This page allows you to configure the SNMPv3 user table. The entry index keys are **Engine ID** and **User Name**.

SNMPv3 Users Configuration

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

| Label | Description |
|------------------|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Engine ID | An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses User-based Security Model (USM) for |



| | |
|--------------------------------|--|
| | <p>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.</p> |
| User Name | <p>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.</p> |
| Security Level | <p>Indicates the security model that this entry should belong to. Possible security models include:</p> <p>NoAuth, NoPriv: no authentication and none privacy Auth, NoPriv: Authentication and no privacy Auth, Priv: Authentication and privacy</p> <p>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.</p> |
| Authentication Protocol | <p>Indicates the authentication protocol that this entry should belong to. Possible authentication protocols include:</p> <p>None: no authentication protocol MD5: an optional flag to indicate that this user is using MD5 authentication protocol SHA: an optional flag to indicate that this user is using SHA authentication protocol</p> <p>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.</p> |
| Authentication Password | <p>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.</p> |
| Privacy Protocol | <p>Indicates the privacy protocol that this entry should belong to. Possible privacy protocols include:</p> <p>None: no privacy protocol DES: an optional flag to indicate that this user is using DES</p> |

| | |
|-------------------------|---|
| | 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 SNMP Group Configurations

An SNMP group is an access control policy for you to add users. Each SNMP group is configured with a security model, and is associated with an SNMP view. A user within an SNMP group should match the security model of the SNMP group. These parameters specify what type of authentication and privacy a user within an SNMP group uses. Each SNMP group name and security model pair must be unique. This page allows you to configure the SNMPv3 group table. The entry index keys are **Security Model** and **Security Name**.

SNMPv3 Groups Configuration

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

| Label | Description |
|-----------------------|--|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Security Model | Indicates the security model that this entry should belong to. Possible security models included: v1 : Reserved for SNMPv1. v2c : Reserved for SNMPv2c. usm : User-based Security Model (USM). |
| Security Name | A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and 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 SNMP View Configurations

The SNMP v3 View table specifies the MIB object access requirements for each View Name. You can specify specific areas of the MIB that can be accessed or denied based on the entries or create and delete entries in the View table in this page. The entry index keys are **View Name** and **OID Subtree**.

SNMPv3 Views Configuration

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

Add new view
Save
Reset

| 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: Included: an optional flag to indicate that this view subtree should be included. Excluded: An optional flag to indicate that this view subtree should be excluded. Generally, if 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 SNMP Access Configurations

This page allows you to configure SNMPv3 access table. The entry index keys are **Group Name**, **Security Model**, and **Security Level**.

SNMPv3 Accesses Configuration

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

| Label | Description |
|------------------------|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Group Name | A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and 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: any : Accepted any security model (v1 v2c usm). v1 : Reserved for SNMPv1. v2c : Reserved for SNMPv2c. usm : User-based Security Model (USM). |
| Security Level | Indicates the security model that this entry should belong to. Possible security models include: NoAuth, NoPriv : no authentication and no privacy Auth, NoPriv : Authentication and no privacy Auth, Priv : Authentication and privacy |
| Read View Name | The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and 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

5.6.1 Storm Control

A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configuration, or users issuing a denial-of-service attack can cause a storm. Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port. In this page, you can specify the rate at which packets are received for unicast, multicast, and broadcast traffic. The unit of the rate can be either pps (packets per second) or

kpps (kilopackets per second).

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.

Storm Control Configuration

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

| Label | Description |
|-------------------|---|
| Frame Type | Frame types supported by the Storm Control function, including Unicast , Multicast , and Broadcast . |
| Status | Enables or disables the given frame type |
| Rate | The rate is packet per second (pps), configure the rate as 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. The 1 kpps is actually 1002.1 pps. |

5.6.2 Port Classification

QoS (Quality of Service) is a method to achieve efficient bandwidth utilization between devices by prioritizing frames according to individual requirements and transmit the frames based on their importance. Frames in higher priority queues receive a bigger slice of bandwidth than those in a lower priority queue.

QoS Ingress Port Classification

| Port | QoS class | DP level | PCP | DEI | Tag Class. | DSCP Based |
|------|-----------|----------|------|------|------------|--------------------------|
| * | <> ▼ | <> ▼ | <> ▼ | <> ▼ | | <input type="checkbox"/> |
| 1 | 0 ▼ | 0 ▼ | 0 ▼ | 0 ▼ | Disabled | <input type="checkbox"/> |
| 2 | 0 ▼ | 0 ▼ | 0 ▼ | 0 ▼ | Disabled | <input type="checkbox"/> |
| 3 | 0 ▼ | 0 ▼ | 0 ▼ | 0 ▼ | Disabled | <input type="checkbox"/> |
| 4 | 0 ▼ | 0 ▼ | 0 ▼ | 0 ▼ | Disabled | <input type="checkbox"/> |
| 5 | 0 ▼ | 0 ▼ | 0 ▼ | 0 ▼ | Disabled | <input type="checkbox"/> |
| 6 | 0 ▼ | 0 ▼ | 0 ▼ | 0 ▼ | Disabled | <input type="checkbox"/> |
| 7 | 0 ▼ | 0 ▼ | 0 ▼ | 0 ▼ | Disabled | <input type="checkbox"/> |



| Label | Description |
|------------------|--|
| Port | The port number for which the configuration below applies |
| QoS Class | <p>Controls the default QoS class</p> <p>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.</p> <p>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.</p> <p>PCP value: 0 1 2 3 4 5 6 7 QoS class: 1 0 2 3 4 5 6 7</p> <p>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.</p> <p>The classified QoS class can be overruled by a QCL entry.</p> <p>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.</p> |
| DP level | <p>Controls the default Drop Precedence Level</p> <p>All frames are classified to a DP level.</p> <p>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.</p> <p>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.</p> <p>The classified DP level can be overruled by a QCL entry.</p> |
| PCP | <p>Controls the default PCP value</p> <p>All frames are classified to a PCP value.</p> <p>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.</p> |
| DEI | <p>Controls the default DEI value</p> <p>All frames are classified to a DEI value.</p> |

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

5.6.3 Port Tag Remaking

You can set QoS egress queues on a port such as classifying data and marking it according to its priority and the policies. Packets will then travel across the switch's internal paths carrying their assigned QoS tag markers. At the egress port, these markers are read and used to determine which queue each data packet is forwarded to. When the traffic does not conform to the conditions set in a policer command, you can remark the traffic.

QoS Egress Port Tag Remarking

| Port | Mode |
|------|------------|
| 1 | Classified |
| 2 | Classified |
| 3 | Classified |
| 4 | Classified |
| 5 | Classified |
| 6 | Classified |
| 7 | Classified |
| 8 | Classified |

| 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 Classified: use classified PCP/DEI values Default: use default PCP/DEI values Mapped: use mapped versions of QoS class and DP level |

5.6.4 Port DSCP

DSCP (Differentiated Services Code Point) is a measure of QoS. It can classify data packets by using the 6-bit DS field in the IP header so you can manage each traffic class differently and efficiently, thereby achieving optimized use of network bandwidth. DSCP-enabled routers on the network will read the DSCP value of the data packet and put the packet into different queues before transmission, such as high priority and most efficient transmission. With such QoS functions, you can ensure low-latency for critical traffic. This page allows you to configure DSCP settings for each port.

QoS Port DSCP Configuration

| Port | Ingress | | Egress |
|------|--------------------------|----------|---------|
| | Translate | Classify | Rewrite |
| * | <input type="checkbox"/> | <> | <> |
| 1 | <input type="checkbox"/> | Disable | Disable |
| 2 | <input type="checkbox"/> | Disable | Disable |
| 3 | <input type="checkbox"/> | Disable | Disable |
| 4 | <input type="checkbox"/> | Disable | Disable |
| 5 | <input type="checkbox"/> | Disable | Disable |
| 6 | <input type="checkbox"/> | Disable | Disable |
| 7 | <input type="checkbox"/> | Disable | Disable |

| Label | Description |
|----------------|---|
| Port | Shows the list of ports for which you can configure DSCP Ingress and Egress settings. |
| Ingress | <p>In Ingress settings you can change ingress translation and classification settings for individual ports.</p> <p>There are two configuration parameters available in Ingress:</p> <p>Translate: check to enable the function</p> <p>Classify: includes four values</p> <p>Disable: no Ingress DSCP classification</p> <p>DSCP=0: classify if incoming (or translated if enabled) DSCP is 0.</p> <p>Selected: classify only selected DSCP whose classification is enabled as specified in DSCP Translation window for the specific DSCP.</p> <p>All: classify all DSCP</p> |
| Egress | <p>Port egress rewriting can be one of the following options:</p> <p>Disable: no Egress rewrite</p> <p>Enable: rewrite enabled without remapping</p> <p>Remap DP Unaware: DSCP from the analyzer is remapped and</p> |

| | |
|----------------|---|
| | <p>the frame is remarked with a remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table.</p> <p>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.</p> |
| Port | Shows the list of ports for which you can configure DSCP Ingress and Egress settings. |
| Ingress | <p>In Ingress settings you can change ingress translation and classification settings for individual ports.</p> <p>There are two configuration parameters available in Ingress:</p> <p>Translate: check to enable the function</p> <p>Classify: includes four values</p> <p>Disable: no Ingress DSCP classification</p> <p>DSCP=0: classify if incoming (or translated if enabled) DSCP is 0.</p> <p>Selected: classify only selected DSCP whose classification is enabled as specified in DSCP Translation window for the specific DSCP.</p> <p>All: classify all DSCP</p> |

5.6.5 Policing

Policing is a traffic regulation mechanism for limiting the rate of traffic streams, thereby controlling the maximum rate of traffic sent or received on an interface. When the traffic rate exceeds the configured maximum rate, policing drops or remarks the excess traffic. This page allows you to configure Policer for all switch ports.

Port Policing

| Port | Enabled | Rate | Unit | Flow Control |
|------|--------------------------|------|------|--------------------------|
| * | <input type="checkbox"/> | 500 | <> | <input type="checkbox"/> |
| 1 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> |
| - | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> |



| 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. |

Queue Policing

| QoS Ingress Queue Policers | | | | | | | | | | |
|----------------------------|-------------------------------------|------|------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Port | Queue 0 | | | Queue 1 | Queue 2 | Queue 3 | Queue 4 | Queue 5 | Queue 6 | Queue 7 |
| | E | Rate | Unit | Enable |
| * | <input checked="" type="checkbox"/> | 500 | <> | <input type="checkbox"/> |
| 1 | <input checked="" type="checkbox"/> | 500 | kbps | <input type="checkbox"/> |
| 2 | <input checked="" type="checkbox"/> | 500 | kbps | <input type="checkbox"/> |
| 3 | <input checked="" type="checkbox"/> | 500 | kbps | <input type="checkbox"/> |
| 4 | <input checked="" type="checkbox"/> | 500 | kbps | <input type="checkbox"/> |
| 5 | <input checked="" type="checkbox"/> | 500 | kbps | <input type="checkbox"/> |

| 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 . 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 . This field is only shown if at least one of the queue policers is enabled. |

5.6.6 Scheduling and Shaping

Port scheduling can solve performance degradation during network congestions. The schedulers allow switches to maintain separate queues for packets from each source and prevent specific traffic to use up all bandwidth. This page allows you to configure Scheduler and Shapers for individual ports.

QoS Egress Port Scheduler and Shaper Strict Priority

Strict Priority uses queues based only priority. When traffic arrives the device, traffic on the highest priority queue will be transmitted first, followed by traffic on lower priorities. If there is always some content in the highest priority queue, then the other packets in the rest of queues will not be sent until the highest priority queue is empty. The SP algorithm is preferred when the received packets contain high priority data, such as voice and video.

Port 1

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority

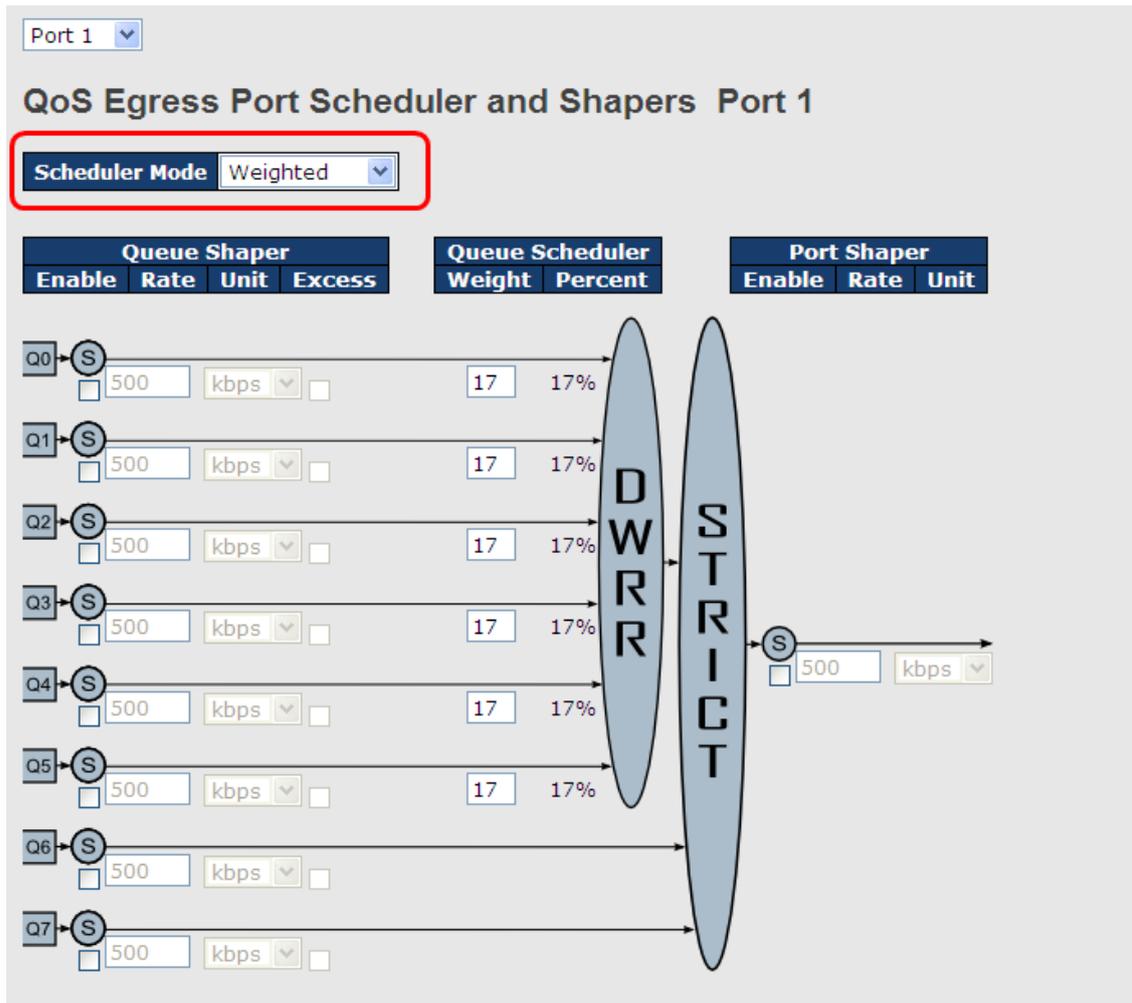
| Queue Shaper | | | | Port Shaper | | |
|-------------------------------------|------|------|--------------------------|--------------------------|------|------|
| Enable | Rate | Unit | Excess | Enable | Rate | Unit |
| <input checked="" type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | 500 | kbps |
| <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | | |
| <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | | |
| <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | | |
| <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | | |
| <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | | |
| <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | | |
| <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | | |



| Label | Description |
|----------------------------|---|
| Scheduler Mode | Two scheduling modes are available: Strict Priority or Weighted |
| 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

Weighted scheduling will deliver traffic on a rotating basis. It can guarantee each queue's minimum bandwidth based on their bandwidth weight when there is traffic congestion. Only when a port has more traffic than it can handle will this mode be activated. A queue is given an amount of bandwidth regardless of the incoming traffic on that port. Queue with larger weights will have more guaranteed bandwidth than others with smaller weights.



| Label | Description |
|-------------------------------|--|
| Scheduler Mode | Two scheduling modes are available: Strict Priority or Weighted |
| 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 . |

5.6.7 Port Scheduler

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

QoS Egress Port Schedulers

| Port | Mode | Weight | | | | | |
|------|-----------------|--------|----|----|----|----|----|
| | | Q0 | Q1 | Q2 | Q3 | Q4 | Q5 |
| 1 | Strict Priority | - | - | - | - | - | - |
| 2 | Strict Priority | - | - | - | - | - | - |
| 3 | Strict Priority | - | - | - | - | - | - |
| 4 | Strict Priority | - | - | - | - | - | - |
| 5 | Strict Priority | - | - | - | - | - | - |
| 6 | Strict Priority | - | - | - | - | - | - |

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

5.6.8 Port Shaping

Port shaping enables you to limit traffic on a port, thereby controlling the amount of traffic passing through the port. With port shaping, you can shape the aggregate traffic through an interface to a rate that is less than the line rate for that interface. When configuring port shaping on an interface, you specify a value indicating the maximum amount of traffic allowable for the interface. This value must be less than the maximum bandwidth for that interface.

QoS Egress Port Shapers

| Port | Shapers | | | | | | | | Port | |
|------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| | Q0 | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 | | |
| 1 | disabled |
| 2 | disabled |
| 3 | disabled |
| 4 | disabled |
| 5 | disabled |
| 6 | disabled |

| 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" |
| Q0~Q7 | Shows disabled or actual port shaper rate - e.g. "800 Mbps" |

5.6.9 DSCP-based QoS

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

DSCP-Based QoS Ingress Classification

| DSCP | Trust | QoS Class | DPL |
|--------|--------------------------|-----------|------|
| * | <input type="checkbox"/> | <> ▾ | <> ▾ |
| 0 (BE) | <input type="checkbox"/> | 0 ▾ | 0 ▾ |
| 1 | <input type="checkbox"/> | 0 ▾ | 0 ▾ |
| 2 | <input type="checkbox"/> | 0 ▾ | 0 ▾ |
| 3 | <input type="checkbox"/> | 0 ▾ | 0 ▾ |
| 4 | <input type="checkbox"/> | 0 ▾ | 0 ▾ |
| 5 | <input type="checkbox"/> | 0 ▾ | 0 ▾ |

| 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 apply to **Ingress** or **Egress**.

| DSCP | Ingress | | Egress | |
|---------|-----------|--------------------------|-----------|-----------|
| | Translate | Classify | Remap DP0 | Remap DP1 |
| * | <> | <input type="checkbox"/> | <> | <> |
| 0 (BE) | 0 (BE) | <input type="checkbox"/> | 0 (BE) | 0 (BE) |
| 1 | 1 | <input type="checkbox"/> | 1 | 1 |
| 2 | 2 | <input type="checkbox"/> | 2 | 2 |
| 3 | 3 | <input type="checkbox"/> | 3 | 3 |
| 4 | 4 | <input type="checkbox"/> | 4 | 4 |
| 5 | 5 | <input type="checkbox"/> | 5 | 5 |
| 6 | 6 | <input type="checkbox"/> | 6 | 6 |
| 7 | 7 | <input type="checkbox"/> | 7 | 7 |
| 8 (CS1) | 8 (CS1) | <input type="checkbox"/> | 8 (CS1) | 8 (CS1) |
| 9 | 9 | <input type="checkbox"/> | 9 | 9 |

| Label | Description |
|----------------|--|
| DSCP | Maximum number of supported DSCP values is 64 and valid DSCP value ranges from 0 to 63. |
| Ingress | <p>Ingress DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.</p> <p>There are two configuration parameters for DSCP Translation -</p> <ol style="list-style-type: none"> Translate: Enables ingress translation of DSCP values based on the specified classification method. DSCP can be translated to any of (0-63) DSCP values. Classify: Enable Classification at ingress side as defined in the QoS Port DSCP Configuration table. |
| Egress | <p>Configurable egress parameters include;</p> <p>Remap DP0: Re-maps DP0 field to selected DSCP value. DP0 indicates a drop precedence with a low priority. You can select the DSCP value from a selected menu to which you want to remap. DSCP value ranges form 0 to 63.</p> <p>Remap DP1: Re-maps DP1 field to selected DSCP value. DP1 indicates a drop precedence with a high priority. You can select</p> |

| | |
|----------------|---|
| | the DSCP value from a selected menu to which you want to remap. DSCP value ranges form 0 to 63. |
| DSCP | Maximum number of supported DSCP values is 64 and valid DSCP value ranges from 0 to 63. |
| Ingress | <p>Ingress DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.</p> <p>There are two configuration parameters for DSCP Translation -</p> <ol style="list-style-type: none"> 1. Translate: Enables ingress translation of DSCP values based on the specified classification method. DSCP can be translated to any of (0-63) DSCP values. 2. Classify: Enable Classification at ingress side as defined in the QoS Port DSCP Configuration table. |
| Egress | <p>Configurable egress parameters include;</p> <p>Remap DP0: Re-maps DP0 field to selected DSCP value. DP0 indicates a drop precedence with a low priority. You can select the DSCP value from a selected menu to which you want to remap. DSCP value ranges form 0 to 63.</p> <p>Remap DP1: Re-maps DP1 field to selected DSCP value. DP1 indicates a drop precedence with a high priority. You can select the DSCP value from a selected menu to which you want to remap. DSCP value ranges form 0 to 63.</p> |
| DSCP | Maximum number of supported DSCP values is 64 and valid 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.

| DSCP Classification | | |
|---------------------|-----|-----------|
| QoS Class | DPL | DSCP |
| * | * | <> |
| 0 | 0 | 0 (BE) |
| 0 | 1 | 8 (CS1) |
| 1 | 0 | 14 (AF13) |
| 1 | 1 | 0 (BE) |
| 2 | 0 | 0 (BE) |

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

5.6.12 QoS Control List

This page shows all the QCE (Quality Control Entries) for a given QCL. You can edit or add new QoS control entries in this page. A QCE consists of several parameters. These parameters vary with the frame type you select.

QCE Configuration

| Port Members | | | | | | | | | | | | | | | | | | | |
|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| <input checked="" type="checkbox"/> |

Key Parameters

| | | |
|-------------------|----------|-----------------------------|
| Tag | Tag | <input type="text"/> |
| VID | Specific | Value: <input type="text"/> |
| PCP | 2 | |
| DEI | 0 | |
| SMAC | Specific | 0x00-00-00 |
| DMAC Type | UC | |
| Frame Type | Ethernet | |

Action Parameters

| | |
|--------------|-----------|
| Class | 3 |
| DPL | 1 |
| DSCP | 28 (AF32) |

MAC Parameters

| | | |
|-------------------|----------|---------------|
| Ether Type | Specific | Value: 0xFFFF |
|-------------------|----------|---------------|

| Label | Description |
|-----------------------|--|
| Port Members | Check to include the port in the QCL entry. By default, all ports are included. |
| Key Parameters | Key configurations include: Tag: value of tag, can be Any , Untag or Tag . VID: valid value of VLAN ID from 1 to 4095 Any: can be a specific value or a range of VIDs. 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 |



| | |
|-----------------|--|
| | <p>DEI: Drop Eligible Indicator, can be any of values between 0 and 1 or Any</p> <p>SMAC: Source MAC Address, can be 24 MS bits (OUI) or Any</p> <p>DMAC Type: Destination MAC type, can be unicast (UC), multicast (MC), broadcast (BC) or Any</p> <p>Frame Type can be the following values: Any, Ethernet, LLC, SNAP, IPv4, and IPv6</p> <p>Note: all frame types are explained below.</p> |
| 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 | <p>SSAP Address: valid SSAP (Source Service Access Point) values can range from 0x00 to 0xFF or Any. The default value is Any.</p> <p>DSAP Address: valid DSAP (Destination Service Access Point) values can range from 0x00 to 0xFF or Any. The default value is Any.</p> <p>Control Valid Control: valid values can range from 0x00 to 0xFF or Any. The default value is Any.</p> |
| SNAP | PID: valid PID (a.k.a ethernet type) values can range from 0x00 to 0xFFFF or Any . The default value is Any . |
| IPv4 | <p>Protocol IP Protocol Number: (0-255, TCP or UDP) or Any</p> <p>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.</p> <p>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.</p> <p>IP Fragment: Ipv4 frame fragmented options include 'yes', 'no', and 'any'.</p> <p>Sport Source TCP/UDP Port: (0-65535) or Any, specific value or port range applicable for IP protocol UDP/TCP</p> <p>Dport Destination TCP/UDP Port: (0-65535) or Any, specific value or port range applicable for IP protocol UDP/TCP</p> |
| IPv6 | Protocol IP protocol number: (0-255, TCP or UDP) or Any |

| | |
|--------------------------|--|
| | <p>Source IP IPv6 source address: (a.b.c.d) or Any, 32 LS bits</p> <p>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.</p> <p>Sport Source TCP/UDP port: (0-65535) or Any, specific value or port range applicable for IP protocol UDP/TCP</p> <p>Dport Destination TCP/UDP port: (0-65535) or Any, specific value or port range applicable for IP protocol UDP/TCP</p> |
| Action Parameters | <p>Class QoS class: (0-7) or Default</p> <p>Valid Drop Precedence Level value can be (0-1) or Default.</p> <p>Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or Default.</p> <p>Default means that the default classified value is not modified by this QCE.</p> |

5.6.13 QoS Counters

This page shows information on the number of packets sent and received at each queue.

Queuing Counters

Auto-refresh Refresh Clear

| Port | Q0 | | Q1 | | Q2 | | Q3 | | Q4 | | Q5 | | Q6 | | Q7 | |
|------|------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------|
| | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 586 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 493 |
| 8 | 1307 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2326 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| 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. A conflict will occur if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

Combined ▾
Auto-refresh
Resolve Conflict
Refresh

QoS Control List Status

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

| Label | Description |
|-------------------|--|
| User | Indicates the QCL user |
| QCE# | Indicates the index of QCE |
| Frame Type | <p>Indicates the type of frame to look for incoming frames. Possible frame types are:</p> <p>Any: the QCE will match all frame type.</p> <p>Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.</p> <p>LLC: Only (LLC) frames are allowed.</p> <p>SNAP: Only (SNAP) frames are allowed.</p> <p>IPv4: the QCE will match only IPV4 frames.</p> <p>IPv6: the QCE will match only IPV6 frames.</p> |
| Port | Indicates the list of ports configured with the QCE. |
| Action | <p>Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.</p> <p>There are three action fields: Class, DPL, and DSCP.</p> <p>Class: Classified QoS; if a frame matches the QCE, it will be put in the queue.</p> <p>DPL: Drop Precedence Level; if a frame matches the QCE, then DP level will set to a value displayed under DPL column.</p> <p>DSCP: if a frame matches the QCE, then DSCP will be classified with the value displayed under DSCP column.</p> |
| 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

IGMP (Internet Group Management Protocol) snooping monitors the IGMP traffic between hosts and multicast routers. The switch uses what IGMP snooping learns to forward multicast traffic only to interfaces that are connected to interested receivers. This conserves bandwidth by allowing the switch to send multicast traffic to only those interfaces that are connected to hosts that want to receive the traffic, instead of flooding the traffic to all interfaces in the VLAN. This page allows you to set up IGMP snooping configurations.

IGMP Snooping Configuration

Global Configuration

Snooping Enabled

Unregistered IPMCv4 Flooding Enabled

Port Related Configuration

| Port | Router Port | Fast Leave |
|------|--------------------------|--------------------------|
| ∞ | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | <input type="checkbox"/> |

| Label | Description |
|---|---|
| Snooping Enabled | Check to enable global IGMP snooping |
| Unregistered IPMCv4 Flooding 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 |

| | |
|-------------------|---|
| | <p>Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.</p> <p>If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.</p> |
| Fast Leave | Check to enable fast leave on the port |

5.7.2 VLAN Configurations of IGMP Snooping

If a VLAN is not IGMP snooping-enabled, it floods multicast data and control packets to the entire VLAN in hardware. When snooping is enabled, IGMP packets are trapped to the CPU. Data packets are mirrored to the CPU in addition to being VLAN flooded. The CPU then installs hardware resources, so that subsequent data packets can be switched to desired ports in hardware without going to the CPU.

Each page shows up to 99 entries from the VLAN table, depending on the value in the Entries Per Page field. By default, the 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** field allows the user to select the starting point in the VLAN Table. Clicking **Refresh** will update the displayed table starting from that or the next closest VLAN Table match.

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

IGMP Snooping VLAN Configuration

Refresh
|<<
>>

Start from VLAN with entries per page.

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

Add New IGMP VLAN

Save
Reset



| 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 |

5.7.3 IGMP Snooping Status

This page provides IGMP snooping status.

Auto-refresh [Refresh](#) [Clear](#)

IGMP Snooping Status

Statistics

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

Router Port

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

| Label | Description |
|---------------------------|--|
| VLAN ID | The VLAN ID of the entry |
| Querier Version | 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 |

5.7.4 Groups Information of IGMP Snooping

Information about entries in the **IGMP Group Table** is shown in this page. The **IGMP Group Table** is sorted first by VLAN ID, and then by group.

IGMP Snooping Group Information

Auto-refresh Refresh |<< >>

Start from VLAN and group address with entries per page.

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

| Label | Description |
|---------------------|--|
| VLAN ID | 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 Configurations

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

Remote Control Security Configuration

Mode

| Delete | Port | IP | Web | Telnet | SNMP |
|---------------------------------------|----------------------------------|--------------------------------------|--------------------------|--------------------------|--------------------------|
| <input type="button" value="Delete"/> | <input type="text" value="Any"/> | <input type="text" value="0.0.0.0"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |



| 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

Device binding is ORing's proprietary technology which binds the IP/MAC address of a device with a specified Ethernet port. If the IP/MAC address of the device connected to the Ethernet port does not conform to the binding requirements, the device will be locked for security concerns. Device Binding also provides security functions via alive checking, streaming check, and DoS/DDoS prevention.

Device Binding

Function State: Enable

| Port | Mode | Alive Check | | Stream Check | | DDOS Prevention | | Device | |
|------|----------|--------------------------|--------|--------------------------|--------|--------------------------|--------|------------|--------------|
| | | Active | Status | Active | Status | Active | Status | IP Address | MAC Address |
| 1 | Scan | <input type="checkbox"/> | --- | <input type="checkbox"/> | --- | <input type="checkbox"/> | --- | 0.0.0.0 | 00-00-00-00- |
| 2 | Binding | <input type="checkbox"/> | --- | <input type="checkbox"/> | --- | <input type="checkbox"/> | --- | 0.0.0.0 | 00-00-00-00- |
| 3 | Shutdown | <input type="checkbox"/> | --- | <input type="checkbox"/> | --- | <input type="checkbox"/> | --- | 0.0.0.0 | 00-00-00-00- |
| 4 | --- | <input type="checkbox"/> | --- | <input type="checkbox"/> | --- | <input type="checkbox"/> | --- | 0.0.0.0 | 00-00-00-00- |
| 5 | --- | <input type="checkbox"/> | --- | <input type="checkbox"/> | --- | <input type="checkbox"/> | --- | 0.0.0.0 | 00-00-00-00- |

| Label | Description |
|---------------------------|---|
| Mode | Indicates the device binding operation for each port. Possible modes are: ---: disable 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. 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: ---: disable Got Reply : receive ping reply from device, meaning the device is still |

| | | |
|--------------------------|-------------------|--|
| | | alive Lost Reply: not receiving ping reply from device, meaning the device might have been dead. |
| Stream Active | Check | Check to enable stream check. When enabled, the switch will detect the stream change (getting low) from the device. |
| Stream Status | Check | Indicates stream check status. Possible statuses are: ---: disable Normal: the stream is normal. Low: the stream is getting low. |
| DDoS Acton | Prevention | Check to enable DDOS prevention. When enabled, the switch will monitor the device against DDOS attacks. |
| DDoS Status | Prevention | Indicates DDOS prevention status. Possible statuses are: ---: disable Analyzing: analyzes packet throughput for initialization Running: analysis completes and ready for next move Attacked: DDOS attacks occur |
| Device IP Address | | Specifies IP address of the device |
| Device Address | MAC | Specifies MAC address of the device |

Advanced Configurations

Alias IP Address

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

Alias IP Address

| Port | Alias IP Address |
|------|------------------|
| 1 | 0.0.0.0 |
| 2 | 0.0.0.0 |
| 3 | 0.0.0.0 |
| 4 | 0.0.0.0 |
| 5 | 0.0.0.0 |
| 6 | 0.0.0.0 |
| 7 | 0.0.0.0 |

| 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

Alive Checking monitors the real-time status of the device connected to the port. Alive-checking packets will be sent to the device to probe if the device is running. If the switch receives no response from the device, actions will be taken according to your configurations.

Alive Check

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

The image shows a screenshot of a web interface for configuring Alive Check. A dropdown menu is open for port 2, showing the following options: Link Change, Only Log it, Shunt Down the Port, and Reboot Device. The status for all ports is currently '---'.

| Label | Description |
|----------------------------|-------------------------------------|
| Link Change | Disables or enables the port |
| Only log it | Simply sends logs to the log server |
| Shunt Down the Port | Disables the port |
| Reboot Device | Disables or enables PoE power |

DDoS Prevention

The switch can monitor ingress packets, and perform actions when DDOS attack occurred on this port. When network traffic from a specific device increases significantly in a short period of time, the switch will lock the IP address of that device to protect the network from attacks. You can configure DDoS prevention on this page to achieve maximum protection.



DDOS Prevention

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

| | |
|----------------------|---|
| Mode | Enables or disables DDOS prevention of the port |
| Sensibility | Indicates the level of DDOS detection. Possible levels are: Low: low sensibility Normal: normal sensibility Medium: medium sensibility High: high sensibility |
| Packet Type | Indicates the types of DDoS attack packets to be monitored. Possible types are: RX Total: all ingress packets RX Unicast: unicast ingress packets RX Multicast: multicast ingress packets RX Broadcast: broadcast ingress packets TCP: TCP ingress packets UDP: UDP ingress packets |
| Socket Number | If packet type is UDP (or TCP), please specify the socket number here. The socket number 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: ---: no action Blocking 1 minute: blocks the forwarding for 1 minute and log the event Blocking 10 minute: blocks the forwarding for 10 minutes and log the event |



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

Device Description

This page allows you to configure device description settings.

Device Description

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

| Label | Description |
|--------------------|---|
| Device Type | <p>Indicates device types. Possible types are:</p> <p>---: no specification</p> <p>IP Camera</p> <p>IP Phone</p> <p>Access Point</p> |

| | |
|-------------------------|---|
| | PC PLC Network Video Recorder |
| Location Address | Indicates location information of the device. The information can be used for Google Mapping. |
| Description | Device descriptions |

Stream Check

Stream check monitors the consistency of real-time network traffic from the device bound with the port. When the traffic changes sharply all of a sudden, an alert will be issued. This page allows you to configure stream check settings.

| Stream Check | | | |
|--------------|-----------|----------|--------|
| Port | Mode | Action | Status |
| 1 | Enabled ▾ | Log it ▾ | Normal |
| 2 | --- ▾ | --- ▾ | --- |
| 3 | --- ▾ | --- ▾ | --- |
| 4 | --- ▾ | --- ▾ | --- |
| 5 | --- ▾ | --- ▾ | --- |
| 6 | --- ▾ | --- ▾ | --- |
| 7 | --- ▾ | --- ▾ | --- |
| 8 | --- ▾ | --- ▾ | --- |
| 9 | --- ▾ | --- ▾ | --- |
| 10 | --- ▾ | --- ▾ | --- |
| 11 | --- ▾ | --- ▾ | --- |
| 12 | --- ▾ | --- ▾ | --- |

| 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: ---: no action 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.



Port Configuration

ACL Ports Configuration

Refresh Clear

| Port | Policy ID | Action | Rate Limiter ID | Port Copy | Logging | Shutdown | Counter |
|------|-----------|--------|-----------------|-----------|----------|----------|----------|
| 1 | 1 | Permit | Disabled | Disabled | Disabled | Disabled | 108498 |
| 2 | 1 | Permit | Disabled | Disabled | Disabled | Disabled | 0 |
| 3 | 1 | Permit | Disabled | Disabled | Disabled | Disabled | 68732984 |
| 4 | 1 | Permit | Disabled | Disabled | Disabled | Disabled | 0 |
| 5 | 1 | Permit | Disabled | Disabled | Disabled | Disabled | 0 |
| 6 | 1 | Permit | Disabled | Disabled | Disabled | Disabled | 68732984 |
| 7 | 1 | Permit | Disabled | Disabled | Disabled | Disabled | 0 |
| 8 | 1 | Permit | Disabled | Disabled | Disabled | Disabled | 0 |

| 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 Copy | 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: Enabled : frames received on the port are stored in the system log Disabled : frames received on the port are not logged The default value is Disabled . Please note that system log memory capacity and logging rate is limited. |
| Shutdown | Specifies the shutdown operation of this port. The allowed values are: Enabled : if a frame is received on the port, the port will be disabled. Disabled : port shut down is disabled. The default value is Disabled . |
| Counter | Counts the number of frames that match this ACE. |

Rate Limiters

This page allows you to define the rate limits applied to a port.

ACL Rate Limiter Configuration

| Rate Limiter ID | Rate (pps) |
|-----------------|------------|
| 1 | 1 |
| 2 | 1 |
| 3 | 1 |
| 4 | 1 |
| 5 | 1 |
| 6 | 1 |
| 7 | 1 |
| 8 | 1 |
| 9 | 1 |
| 10 | 1 |
| 11 | 1 |
| 12 | 1 |

| 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. The 1 kpps is actually 1002.1 pps. |

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.

ACE Configuration

| | | | |
|---------------------|--------|---------------------|----------|
| Ingress Port | Port 1 | Action | Permit |
| Frame Type | IPv4 | Rate Limiter | Disabled |
| | | Port Copy | Disabled |
| | | Logging | Disabled |
| | | Shutdown | Disabled |
| | | Counter | 5197 |



| Label | Description |
|---------------------|---|
| Ingress Port | Indicates the ingress port to which the ACE will apply. Any: the ACE applies to any port Port n: the ACE applies to this port number, where n is the number of the switch port. Policy n: the ACE applies to this policy number, where n can range from 1 to 8. |
| Frame Type | Indicates the frame type of the ACE. These frame types are mutually exclusive. Any: any frame can match the ACE. Ethernet Type: only Ethernet type frames can match the ACE. The IEEE 802.3 describes 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. Permit: takes action when the frame matches the ACE. 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 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: Enabled: frames matching the ACE are stored in the system log. Disabled: frames matching the ACE are not logged. Please note that system log memory capacity and logging rate is limited. |
| Shutdown | Specifies the shutdown operation of the ACE. The allowed values are: Enabled: if a frame matches the ACE, the ingress port will be disabled. Disabled: port shutdown is disabled for the ACE. |
| Counter | Indicates the number of times the ACE matched by a frame. |

MAC Parameters

| | |
|--------------------|------------------|
| SMAC Filter | Specific ▼ |
| SMAC Value | 00-00-00-00-00-0 |
| DMAC Filter | Specific ▼ |
| DMAC Value | 00-00-00-00-00-0 |

| Label | Description |
|--------------------|--|
| SMAC Filter | <p>(Only displayed when the frame type is Ethernet Type or ARP.) Specifies the source MAC filter for the ACE.</p> <p>Any: no SMAC filter is specified (SMAC filter status is "don't-care"). 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.</p> |
| SMAC Value | <p>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.</p> |
| DMAC Filter | <p>Specifies the destination MAC filter for this ACE</p> <p>Any: no DMAC filter is specified (DMAC filter status is "don't-care"). MC: frame must be multicast. BC: frame must be broadcast. UC: frame must be unicast.</p> <p>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.</p> |
| DMAC Value | <p>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.</p> |

VLAN Parameters

| | |
|----------------|------------|
| VLAN ID Filter | Specific ▾ |
| VLAN ID | 1 |
| Tag Priority | 6 ▾ |

| Label | Description |
|----------------|---|
| VLAN ID Filter | <p>Specifies the VLAN ID filter for the ACE</p> <p>Any: no VLAN ID filter is specified (VLAN ID filter status is "don't-care").</p> <p>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.</p> |
| VLAN ID | <p>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.</p> |
| Tag Priority | <p>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").</p> |

IP Parameters

| | |
|--------------------|------------|
| IP Protocol Filter | Other ▾ |
| IP Protocol Value | 6 |
| IP TTL | Non-zero ▾ |
| IP Fragment | Yes ▾ |
| IP Option | Yes ▾ |
| SIP Filter | Network ▾ |
| SIP Address | 0.0.0.0 |
| SIP Mask | 0.0.0.0 |
| DIP Filter | Network ▾ |
| DIP Address | 0.0.0.0 |
| DIP Mask | 0.0.0.0 |



| | |
|---------------------------|---|
| IP Protocol Filter | <p>Specifies the IP protocol filter for the ACE</p> <p>Any: no IP protocol filter is specified ("don't-care").</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> |
| IP Protocol Value | <p>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.</p> |
| IP TTL | <p>Specifies the time-to-live settings for the ACE</p> <p>Zero: IPv4 frames with a time-to-live value greater than zero must not be able to match this entry.</p> <p>Non-zero: IPv4 frames with a time-to-live field greater than zero must be able to match this entry.</p> <p>Any: any value is allowed ("don't-care").</p> |
| IP Fragment | <p>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.</p> <p>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.</p> <p>Yes: IPv4 frames whose MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.</p> <p>Any: any value is allowed ("don't-care").</p> |
| IP Option | <p>Specifies the options flag settings for the ACE</p> <p>No: IPv4 frames whose options flag is set must not be able to match this entry.</p> <p>Yes: IPv4 frames whose options flag is set must be able to match this entry.</p> <p>Any: any value is allowed ("don't-care").</p> |
| SIP Filter | <p>Specifies the source IP filter for this ACE</p> |

| | |
|--------------------|---|
| | <p>Any: no source IP filter is specified (Source IP filter is "don't-care").</p> <p>Host: source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.</p> <p>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.</p> |
| 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 | <p>Specifies the destination IP filter for the ACE</p> <p>Any: no destination IP filter is specified (destination IP filter is "don't-care").</p> <p>Host: destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.</p> <p>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.</p> |
| 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. |

ARP Parameters

| | | | |
|--------------------------|---------------|---------------------------|-------|
| ARP/RARP | Other ▾ | ARP SMAC Match | 1 ▾ |
| Request/Reply | Request ▾ | RARP SMAC Match | 1 ▾ |
| Sender IP Filter | Network ▾ | IP/Ethernet Length | Any ▾ |
| Sender IP Address | 192.168.1.1 | IP | 0 ▾ |
| Sender IP Mask | 255.255.255.0 | Ethernet | 1 ▾ |
| Target IP Filter | Network ▾ | | |
| Target IP Address | 192.168.1.254 | | |
| Target IP Mask | 255.255.255.0 | | |

| Label | Description |
|-----------------|---|
| ARP/RARP | <p>Specifies the available ARP/RARP opcode (OP) flag for the ACE</p> <p>Any: no ARP/RARP OP flag is specified (OP is "don't-care").</p> <p>ARP: frame must have ARP/RARP opcode set to ARP</p> |



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

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

ICMP Parameters

| | |
|-------------------------|------------|
| ICMP Type Filter | Specific ▾ |
| ICMP Type Value | 255 |
| ICMP Code Filter | Specific ▾ |
| ICMP Code Value | 255 |

| Label | Description |
|-------------------------|--|
| ICMP Type Filter | Specifies the ICMP filter for the ACE Any: no ICMP filter is specified (ICMP filter status is "don't-care"). 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 Any: no ICMP code filter is specified (ICMP code filter status is "don't-care"). 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. |

TCP Parameters

| | |
|--------------------|------------|
| Source Port Filter | Specific ▾ |
| Source Port No. | 0 |
| Dest. Port Filter | Specific ▾ |
| Dest. Port No. | 80 |
| TCP FIN | Any ▾ |
| TCP SYN | Any ▾ |
| TCP RST | Any ▾ |
| TCP PSH | Any ▾ |
| TCP ACK | Any ▾ |
| TCP URG | Any ▾ |

UDP Parameters

| | |
|--------------------|------------|
| Source Port Filter | Specific ▾ |
| Source Port No. | 0 |
| Dest. Port Filter | Range ▾ |
| Dest. Port Range | 80 - 65535 |

| Label | Description |
|------------------------------|--|
| TCP/UDP Source Filter | Specifies the TCP/UDP source filter for the ACE Any: no TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care"). 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 |



| | |
|-----------------------------------|--|
| | <p>entering a TCP/UDP source value appears.</p> <p>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.</p> |
| TCP/UDP Source No. | <p>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.</p> |
| TCP/UDP Source Range | <p>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.</p> |
| TCP/UDP Destination Filter | <p>Specifies the TCP/UDP destination filter for the ACE</p> <p>Any: no TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").</p> <p>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.</p> <p>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.</p> |
| TCP/UDP Destination Number | <p>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.</p> |
| TCP/UDP Destination Range | <p>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.</p> |
| TCP FIN | <p>Specifies the TCP FIN ("no more data from sender") value for the ACE.</p> <p>0: TCP frames where the FIN field is set must not be able to match this entry.</p> <p>1: TCP frames where the FIN field is set must be able to match this entry.</p> <p>Any: any value is allowed ("don't-care").</p> |
| TCP SYN | <p>Specifies the TCP SYN ("synchronize sequence numbers") value for</p> |

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

5.8.4 Authentication, Authorization, and Accounting

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.

Authentication Server Configuration

Common Server Configuration

| | | |
|------------------|-----|---------|
| Timeout | 15 | seconds |
| Dead Time | 300 | seconds |

| Label | Description |
|------------------|---|
| Timeout | <p>The timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this time frame, we will consider it to be dead and continue with the next enabled server (if any).</p> <p>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.</p> |
| Dead Time | <p>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.</p> <p>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.</p> |

5.8.5 RADIUS

Authentication and Accounting Server

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.

RADIUS Authentication Server Configuration

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

| 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 is a text string used by RADIUS to encrypt the client and server authenticator field during exchanges between the router and a RADIUS authentication server. The router encrypts PPP PAP passwords using this text string. The secret - up to 29 characters long - shared between the RADIUS authentication server and the switch stack. |

RADIUS Accounting Server Configuration

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

| 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 is a text string used by RADIUS to encrypt the client and server authenticator field during exchanges between the router and a RADIUS authentication server. The router encrypts PPP PAP passwords using this text string. The secret - up to 29 characters long - shared between the RADIUS authentication server and the switch stack. |

Authentication and Accounting Server Status

This page provides information about the status of the RADIUS server configurable on the authentication configuration page.

RADIUS Authentication Server Status Overview

Auto-refresh

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

| Label | Description |
|-------------------|--|
| # | The RADIUS server number. Click to navigate to detailed statistics 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: Disabled: the server is disabled. Not Ready: the server is enabled, but IP communication is not yet up |

| | |
|--|--|
| | <p>and running.</p> <p>Ready: the server is enabled, IP communications are built, and the RADIUS module is ready to accept access attempts.</p> <p>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.</p> |
|--|--|

RADIUS Accounting Server Status Overview

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

| Label | Description |
|------------|--|
| # | The RADIUS server number. Click to navigate to detailed statistics of the server |
| IP Address | The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of the server |
| Status | <p>The current status of the server. This field has one of the following values:</p> <p>Disabled: the server is disabled.</p> <p>Not Ready: the server is enabled, but IP communication is not yet up and running.</p> <p>Ready: the server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.</p> <p>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.</p> |



Authentication and Accounting Server Statistics

This page shows the access statistics of the authentication and accounting servers. Use the server drop-down list to switch between the backend servers to show related details.

RADIUS Authentication Statistics for Server #1

Server #1 ▾
Auto-refresh
Refresh
Clear

| Receive Packets | | Transmit Packets | |
|----------------------------|---|------------------------|---|
| Access Accepts | 0 | Access Requests | 0 |
| Access Rejects | 0 | Access Retransmissions | 0 |
| Access Challenges | 0 | Pending Requests | 0 |
| Malformed Access Responses | 0 | Timeouts | 0 |
| Bad Authenticators | 0 | | |
| Unknown Types | 0 | | |
| Packets Dropped | 0 | | |
| Other Info | | | |
| IP Address | | 0.0.0.0:1812 | |
| State | | Disabled | |
| Round-Trip Time | | 0 ms | |

| Label | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-----------------|---|--|---|--|-------------|----|----------------|----------------------------------|---|----|----------------|----------------------------------|---|----|-------------------|-------------------------------------|--|----|----------------------------|---|--|----|--------------------|--------------------------------------|--|----|---------------|---------------------------------|---|----|-----------------|-----------------------------------|---|----|-----------------|-----------------------------------|--|----|------------------------|--|--|----|------------------|------------------------------------|--|----|----------|-----------------------------|---|
| Packet Counters | RADIUS authentication server packet counters. There are seven 'receive' and four 'transmit' counters. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #003366; color: white;"> <th>Direction</th> <th>Name</th> <th>RFC4668 Name</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </table> | Direction | Name | RFC4668 Name | Description | Rx | Access Accepts | radiusAuthClientExtAccessAccepts | The number of RADIUS Access-Accept packets (valid or invalid) received from the server. | Rx | Access Rejects | radiusAuthClientExtAccessRejects | The number of RADIUS Access-Reject packets (valid or invalid) received from the server. | Rx | Access Challenges | radiusAuthClientExtAccessChallenges | The number of RADIUS Access-Challenge packets (valid or invalid) received from the server. | Rx | Malformed Access Responses | radiusAuthClientExtMalformedAccessResponses | The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses. | Rx | Bad Authenticators | radiusAuthClientExtBadAuthenticators | The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server. | Rx | Unknown Types | radiusAuthClientExtUnknownTypes | The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason. | Rx | Packets Dropped | radiusAuthClientExtPacketsDropped | The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason. | Tx | Access Requests | radiusAuthClientExtAccessRequests | The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions. | Tx | Access Retransmissions | radiusAuthClientExtAccessRetransmissions | The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server. | Tx | Pending Requests | radiusAuthClientExtPendingRequests | The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission. | Tx | Timeouts | radiusAuthClientExtTimeouts | The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout. |
| | Direction | Name | RFC4668 Name | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Rx | Access Accepts | radiusAuthClientExtAccessAccepts | The number of RADIUS Access-Accept packets (valid or invalid) received from the server. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Rx | Access Rejects | radiusAuthClientExtAccessRejects | The number of RADIUS Access-Reject packets (valid or invalid) received from the server. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Rx | Access Challenges | radiusAuthClientExtAccessChallenges | The number of RADIUS Access-Challenge packets (valid or invalid) received from the server. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Rx | Malformed Access Responses | radiusAuthClientExtMalformedAccessResponses | The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Rx | Bad Authenticators | radiusAuthClientExtBadAuthenticators | The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Rx | Unknown Types | radiusAuthClientExtUnknownTypes | The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Rx | Packets Dropped | radiusAuthClientExtPacketsDropped | The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Tx | Access Requests | radiusAuthClientExtAccessRequests | The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Tx | Access Retransmissions | radiusAuthClientExtAccessRetransmissions | The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Tx | Pending Requests | radiusAuthClientExtPendingRequests | The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Tx | Timeouts | radiusAuthClientExtTimeouts | The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |



| Other Info | <p>This section contains information about the state of the server and the latest round-trip time.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>RFC4668 Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>State</td> <td>-</td> <td>Shows the state of the server. It takes one of the following values: Disabled : The selected server is disabled. Not Ready : The server is enabled, but IP communication is not yet up and running. Ready : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left) : Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.</td> </tr> <tr> <td>Round-Trip Time</td> <td>radiusAuthClientExtRoundTripTime</td> <td>The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.</td> </tr> </tbody> </table> | Name | RFC4668 Name | Description | State | - | Shows the state of the server. It takes one of the following values: Disabled : The selected server is disabled. Not Ready : The server is enabled, but IP communication is not yet up and running. Ready : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left) : Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled. | Round-Trip Time | radiusAuthClientExtRoundTripTime | The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet. |
|------------------------|---|--|--------------|-------------|--------------|---|--|------------------------|----------------------------------|--|
| Name | RFC4668 Name | Description | | | | | | | | |
| State | - | Shows the state of the server. It takes one of the following values: Disabled : The selected server is disabled. Not Ready : The server is enabled, but IP communication is not yet up and running. Ready : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left) : Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled. | | | | | | | | |
| Round-Trip Time | radiusAuthClientExtRoundTripTime | The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet. | | | | | | | | |

RADIUS Accounting Statistics for Server #1

| Receive Packets | | Transmit Packets | |
|----------------------------|--------------|-------------------------|---|
| Responses | 0 | Requests | 0 |
| Malformed Responses | 0 | Retransmissions | 0 |
| Bad Authenticators | 0 | Pending Requests | 0 |
| Unknown Types | 0 | Timeouts | 0 |
| Packets Dropped | 0 | | |
| Other Info | | | |
| IP Address | 0.0.0.0:1813 | | |
| State | Disabled | | |
| Round-Trip Time | 0 ms | | |

| Label | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-----------------|--|--------------------------------------|---|--------------|-------------|----|------------------|-----------------------------|---|----|----------------------------|--------------------------------------|--|----|---------------------------|-------------------------------------|--|----|----------------------|--------------------------------|--|----|------------------------|----------------------------------|---|----|-----------------|----------------------------|---|----|------------------------|-----------------------------------|---|----|-------------------------|-----------------------------------|--|----|-----------------|----------------------------|---|
| Packet Counters | <p>RADIUS accounting server packet counters. There are five 'receive' and four 'transmit' counters.</p> <table border="1"> <thead> <tr> <th>Direction</th> <th>Name</th> <th>RFC4670 Name</th> <th>Description</th> </tr> </thead> <tbody> <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 unknown types are not included as malformed access responses.</td> </tr> <tr> <td>Rx</td> <td>Bad Authenticators</td> <td>radiusAccClientExtBadAuthenticators</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> </tbody> </table> | Direction | Name | RFC4670 Name | Description | Rx | Responses | radiusAccClientExtResponses | The number of RADIUS packets (valid or invalid) received from the server. | Rx | Malformed Responses | radiusAccClientExtMalformedResponses | The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses. | Rx | Bad Authenticators | radiusAccClientExtBadAuthenticators | The number of RADIUS packets containing invalid authenticators received from the server. | Rx | Unknown Types | radiusAccClientExtUnknownTypes | The number of RADIUS packets of unknown types that were received from the server on the accounting port. | Rx | Packets Dropped | radiusAccClientExtPacketsDropped | The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason. | Tx | Requests | radiusAccClientExtRequests | The number of RADIUS packets sent to the server. This does not include retransmissions. | Tx | Retransmissions | radiusAccClientExtRetransmissions | The number of RADIUS packets retransmitted to the RADIUS accounting server. | Tx | Pending Requests | radiusAccClientExtPendingRequests | The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission. | Tx | Timeouts | radiusAccClientExtTimeouts | The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout. |
| Direction | Name | RFC4670 Name | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Rx | Responses | radiusAccClientExtResponses | The number of RADIUS packets (valid or invalid) received from the server. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Rx | Malformed Responses | radiusAccClientExtMalformedResponses | The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Rx | Bad Authenticators | radiusAccClientExtBadAuthenticators | The number of RADIUS packets containing invalid authenticators received from the server. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Rx | Unknown Types | radiusAccClientExtUnknownTypes | The number of RADIUS packets of unknown types that were received from the server on the accounting port. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Rx | Packets Dropped | radiusAccClientExtPacketsDropped | The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Tx | Requests | radiusAccClientExtRequests | The number of RADIUS packets sent to the server. This does not include retransmissions. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Tx | Retransmissions | radiusAccClientExtRetransmissions | The number of RADIUS packets retransmitted to the RADIUS accounting server. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Tx | Pending Requests | radiusAccClientExtPendingRequests | The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Tx | Timeouts | radiusAccClientExtTimeouts | The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | | | |
|------------|---|---------------------------------|--|
| Other Info | This section contains information about the state of the server and the latest round-trip time. | | |
| | Name | RFC4670 Name | Description |
| | State | | Shows the state of the server. It takes one of the following values: Disabled : The selected server is disabled. Not_Ready : The server is enabled, but IP communication is not yet up and running. Ready : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left) : Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled. |
| | Round-Trip Time | radiusAccClientExtRoundTripTime | The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet. |

5.8.6 NAS (802.1x)

A NAS (Network Access Server) is an access gateway between an external communications network and an internal network. For example, when the user dials into the ISP, he/she will be given access to the Internet after being authorized by the access server. The authentication between the client and the server include IEEE 802.1X- and MAC-based.

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 backend servers (RADIUS) determine whether the user is allowed access to the network.

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 request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Overview of MAC-Based Authentication

Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string 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 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, and only the MD5-Challenge method is supported.

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

Network Access Server Configuration

System Configuration

| | | |
|---------------------------------|---|---------|
| Mode | Disabled <input type="button" value="v"/> | |
| Reauthentication Enabled | <input type="checkbox"/> | |
| Reauthentication Period | 3600 | seconds |
| EAPOL Timeout | 30 | seconds |
| Aging Period | 300 | seconds |
| Hold Time | 10 | seconds |

Port Configuration

| Port | Admin State | Port State | Restart | |
|------|---|-------------------|---|---|
| * | <> | | | |
| 1 | Force Authorized <input type="button" value="v"/> | Globally Disabled | <input type="button" value="Reauthenticate"/> | <input type="button" value="Reinitialize"/> |
| 2 | Force Unauthorized <input type="button" value="v"/> | Globally Disabled | <input type="button" value="Reauthenticate"/> | <input type="button" value="Reinitialize"/> |
| 3 | 802.1X <input type="button" value="v"/> | Globally Disabled | <input type="button" value="Reauthenticate"/> | <input type="button" value="Reinitialize"/> |
| 4 | MAC-based Auth. <input type="button" value="v"/> | Globally Disabled | <input type="button" value="Reauthenticate"/> | <input type="button" value="Reinitialize"/> |
| 5 | Force Authorized <input type="button" value="v"/> | Globally Disabled | <input type="button" value="Reauthenticate"/> | <input type="button" value="Reinitialize"/> |

| Label | Description |
|---------------------------------|--|
| Mode | Indicates if 802.1X and MAC-based authentication is globally enabled or disabled on the switch. If globally disabled, all ports are allowed 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. 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. |



| | |
|--------------------|---|
| | <p>Valid range of the value is 1 to 65535 seconds. This has no effect for MAC-based ports.</p> |
| Age Period | <p>This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:</p> <p>MAC-Based Auth.:</p> <p>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.</p> <p>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.</p> |
| Hold Time | <p>This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:</p> <p>MAC-Based Auth.:</p> <p>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.</p> <p>The switch will ignore new frames coming from the client during the hold time.</p> <p>The hold time can be set to a number between 10 and 1000000 seconds.</p> |
| Port | <p>The port number for which the configuration below applies</p> |
| Admin State | <p>If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:</p> <p>Force Authorized</p> <p>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.</p> <p>Force Unauthorized</p> <p>In this mode, the switch will send one EAPOL Failure frame when</p> |

the port link is up, and any client on the port will be disallowed network access.

Port-based 802.1X

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.

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 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.

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.

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.

b. Multi 802.1X

In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they are not authenticated individually. To overcome this security breach, use the Multi 802.1X variant.

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.

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.

The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

MAC-based Auth.

Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string 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 the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special

| | |
|--------------------------|--|
| | <p>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.</p> |
| <p>Port State</p> | <p>The current state of the port. It can undertake one of the following values:</p> <p>Globally Disabled: NAS is globally disabled.</p> <p>Link Down: NAS is globally enabled, but there is no link on the port.</p> <p>Authorized: the port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.</p> <p>Unauthorized: the port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.</p> <p>X Auth/Y Unauth: the port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.</p> |
| <p>Restart</p> | <p>Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect.</p> <p>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.</p> <p>The button only has effect on successfully authenticated clients on the port and will not cause the clients to be temporarily unauthorized.</p> <p>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.</p> |



NAS Status

This page shows the information on current NAS port statuses.

Network Access Server Switch Status

Auto-refresh

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

| Label | Description |
|--------------------|--|
| Port | The switch port number. Click to navigate to detailed 802.1X statistics 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. |

This page provides detailed IEEE 802.1X statistics for a specific switch port using port-based authentication. For MAC-based ports, only the statistics of selected backend server statistics will be shown. Use the drop-down list to select which port details to be displayed.

NAS Statistics Port 2

Port 2 Auto-refresh

Port State

Admin State Force Authorized
Port State Globally Disabled

| Label | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-------------------------|--|-----------------------------------|--|--|--|-----------|------|-----------|-------------|----|--------------|------------------------|---|----|--------------------|------------------------------|---|----|------------------|----------------------------|--|----|--------------|-----------------------------|---|----|---------------|------------------------------|--|----|---------------------|-------------------------------|---|----|-----------------------|-----------------------------------|--|----|--------------|------------------------|--|----|-------------------|-----------------------------|--|----|-----------------|---------------------------|--|
| Admin State | The port's current administrative state. Refer to NAS Admin State for 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 | <p>These supplicant frame counters are available for the following administrative states:</p> <ul style="list-style-type: none"> • Force Authorized • Force Unauthorized • 802.1X <table border="1"> <thead> <tr> <th colspan="4">EAPOL Counters</th> </tr> <tr> <th>Direction</th> <th>Name</th> <th>IEEE Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Rx</td> <td>Total</td> <td>dot1xAuthEapolFramesRx</td> <td>The number of valid EAPOL frames of any type that have been received by the switch.</td> </tr> <tr> <td>Rx</td> <td>Response ID</td> <td>dot1xAuthEapolRespIdFramesRx</td> <td>The number of valid EAP Resp/ID frames that have been received by the switch.</td> </tr> <tr> <td>Rx</td> <td>Responses</td> <td>dot1xAuthEapolRespFramesRx</td> <td>The number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch.</td> </tr> <tr> <td>Rx</td> <td>Start</td> <td>dot1xAuthEapolStartFramesRx</td> <td>The number of EAPOL Start frames that have been received by the switch.</td> </tr> <tr> <td>Rx</td> <td>Logoff</td> <td>dot1xAuthEapolLogoffFramesRx</td> <td>The number of valid EAPOL logoff frames that have been received by the switch.</td> </tr> <tr> <td>Rx</td> <td>Invalid Type</td> <td>dot1xAuthInvalidEapolFramesRx</td> <td>The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.</td> </tr> <tr> <td>Rx</td> <td>Invalid Length</td> <td>dot1xAuthEapolLengthErrorFramesRx</td> <td>The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.</td> </tr> <tr> <td>Tx</td> <td>Total</td> <td>dot1xAuthEapolFramesTx</td> <td>The number of EAPOL frames of any type that have been transmitted by the switch.</td> </tr> <tr> <td>Tx</td> <td>Request ID</td> <td>dot1xAuthEapolReqIdFramesTx</td> <td>The number of EAP initial request frames that have been transmitted by the switch.</td> </tr> <tr> <td>Tx</td> <td>Requests</td> <td>dot1xAuthEapolReqFramesTx</td> <td>The number of valid EAP Request frames (other than initial request frames) that have been transmitted by the switch.</td> </tr> </tbody> </table> | EAPOL Counters | | | | Direction | Name | IEEE Name | Description | Rx | Total | dot1xAuthEapolFramesRx | The number of valid EAPOL frames of any type that have been received by the switch. | Rx | Response ID | dot1xAuthEapolRespIdFramesRx | The number of valid EAP Resp/ID frames that have been received by the switch. | Rx | Responses | dot1xAuthEapolRespFramesRx | The number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch. | Rx | Start | dot1xAuthEapolStartFramesRx | The number of EAPOL Start frames that have been received by the switch. | Rx | Logoff | dot1xAuthEapolLogoffFramesRx | The number of valid EAPOL logoff frames that have been received by the switch. | Rx | Invalid Type | dot1xAuthInvalidEapolFramesRx | The number of EAPOL frames that have been received by the switch in which the frame type is not recognized. | Rx | Invalid Length | dot1xAuthEapolLengthErrorFramesRx | The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid. | Tx | Total | dot1xAuthEapolFramesTx | The number of EAPOL frames of any type that have been transmitted by the switch. | Tx | Request ID | dot1xAuthEapolReqIdFramesTx | The number of EAP initial request frames that have been transmitted by the switch. | Tx | Requests | dot1xAuthEapolReqFramesTx | The number of valid EAP Request frames (other than initial request frames) that have been transmitted by the switch. |
| EAPOL Counters | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Direction | Name | IEEE Name | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Rx | Total | dot1xAuthEapolFramesRx | The number of valid EAPOL frames of any type that have been received by the switch. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Rx | Response ID | dot1xAuthEapolRespIdFramesRx | The number of valid EAP Resp/ID frames that have been received by the switch. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Rx | Responses | dot1xAuthEapolRespFramesRx | The number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Rx | Start | dot1xAuthEapolStartFramesRx | The number of EAPOL Start frames that have been received by the switch. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Rx | Logoff | dot1xAuthEapolLogoffFramesRx | The number of valid EAPOL logoff frames that have been received by the switch. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Rx | Invalid Type | dot1xAuthInvalidEapolFramesRx | The number of EAPOL frames that have been received by the switch in which the frame type is not recognized. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Rx | Invalid Length | dot1xAuthEapolLengthErrorFramesRx | The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Tx | Total | dot1xAuthEapolFramesTx | The number of EAPOL frames of any type that have been transmitted by the switch. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Tx | Request ID | dot1xAuthEapolReqIdFramesTx | The number of EAP initial request frames that have been transmitted by the switch. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Tx | Requests | dot1xAuthEapolReqFramesTx | The number of valid EAP Request frames (other than initial request frames) that have been transmitted by the switch. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Backend Server Counters | <p>These backend (RADIUS) frame counters are available for the following administrative states:</p> <ul style="list-style-type: none"> • 802.1X • MAC-based Auth. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | <table border="1"> <thead> <tr> <th colspan="4">Backend Server Counters</th> </tr> <tr> <th>Direction</th> <th>Name</th> <th>IEEE Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Rx</td> <td>Access Challenges</td> <td>dot1xAuthBackendAccessChallenges</td> <td> Port-based: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. MAC-based: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table). </td> </tr> <tr> <td>Rx</td> <td>Other Requests</td> <td>dot1xAuthBackendOtherRequestsToSupplicant</td> <td> Port-based: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. MAC-based: Not applicable. </td> </tr> <tr> <td>Rx</td> <td>Auth. Successes</td> <td>dot1xAuthBackendAuthSuccesses</td> <td> Port- and MAC-based: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server. </td> </tr> <tr> <td>Rx</td> <td>Auth. Failures</td> <td>dot1xAuthBackendAuthFails</td> <td> Port- and MAC-based: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server. </td> </tr> <tr> <td>Tx</td> <td>Responses</td> <td>dot1xAuthBackendResponses</td> <td> Port-based: Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. MAC-based: Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted. </td> </tr> </tbody> </table> | Backend Server Counters | | | | Direction | Name | IEEE Name | Description | 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). | 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. | 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. | 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. | 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. |
|-----------------------------|---|--|--|--|------|-----------|-------------|--------------------|-------------------------------|--|--------------------------|----------------------------------|--|----------------|--------------------------------|--|--|----|--|-------------------------------|---|----|-----------------------|---------------------------|--|----|------------------|---------------------------|--|
| Backend Server Counters | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Direction | Name | IEEE Name | Description | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 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). | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 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. | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 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. | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 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. | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 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 | <p>Information about the last supplicant/client that attempts to authenticate. This information is available for the following administrative states:</p> <ul style="list-style-type: none"> • 802.1X • MAC-based Auth. <table border="1"> <thead> <tr> <th colspan="3">Last Supplicant/Client Info</th> </tr> <tr> <th>Name</th> <th>IEEE Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>MAC Address</td> <td>dot1xAuthLastEapolFrameSource</td> <td>The MAC address of the last supplicant/client.</td> </tr> <tr> <td>VLAN ID</td> <td>-</td> <td>The VLAN ID on which the last frame from the last supplicant/client was received.</td> </tr> <tr> <td>Version</td> <td>dot1xAuthLastEapolFrameVersion</td> <td> The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable. 802.1X-based: </td> </tr> <tr> <td>Identity</td> <td>-</td> <td> The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. MAC-based: Not applicable. </td> </tr> </tbody> </table> | Last Supplicant/Client Info | | | Name | IEEE Name | Description | MAC Address | dot1xAuthLastEapolFrameSource | The MAC address of the last supplicant/client. | VLAN ID | - | The VLAN ID on which the last frame from the last supplicant/client was received. | Version | dot1xAuthLastEapolFrameVersion | The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable. 802.1X-based: | Identity | - | The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. MAC-based: Not applicable. | | | | | | | | | | |
| Last Supplicant/Client Info | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Name | IEEE Name | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| MAC Address | dot1xAuthLastEapolFrameSource | The MAC address of the last supplicant/client. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| VLAN ID | - | The VLAN ID on which the last frame from the last supplicant/client was received. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Version | dot1xAuthLastEapolFrameVersion | The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable. 802.1X-based: | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Identity | - | The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. MAC-based: Not applicable. | | | | | | | | | | | | | | | | | | | | | | | | | | | |

5.9 Alerts

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. The following pages allow you to set up alert conditions based on your needs for individual switch ports, including actions to be taken during disconnection and power failure.

Fault Alarm

Port Link Down/Broken

| Port | Active |
|------|--------------------------|
| 1 | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> |
| 9 | <input type="checkbox"/> |
| 10 | <input type="checkbox"/> |
| 11 | <input type="checkbox"/> |
| 12 | <input type="checkbox"/> |

5.9.2 System Warning

SYSLOG Setting

SYSLOG is a protocol that allows a device to send event notification messages across IP networks to event message collectors. It permits separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. As Syslog messages are UDP-based, the sender and receiver will not be aware of it if the packet is lost due to network disconnection and no UDP packet will be resent.

System Log Configuration

| | |
|-----------------------|---|
| Server Mode | Disabled <input type="button" value="v"/> |
| Server Address | <input type="text"/> |

| Label | Description |
|---------------------------------|--|
| Server Mode | <p>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.</p> <p>Possible modes are:</p> <p>Enabled: enable server mode</p> <p>Disabled: disable server mode</p> |
| 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. |

SMTP Setting

SMTP (Simple Mail Transfer Protocol) is a protocol for transmitting e-mails across the Internet. By setting up SMTP alert, the device will send a notification e-mail when a user-defined event occurs.

SMTP Setting

E-mail Alert : ▼

| | |
|--|--|
| SMTP Server Address | <input type="text" value="0.0.0.0"/> |
| Sender E-mail Address | <input type="text" value="administrator"/> |
| Mail Subject | <input type="text" value="Automated Email Alert"/> |
| <input type="checkbox"/> Authentication | |
| Recipient E-mail Address 1 | <input type="text"/> |
| Recipient E-mail Address 2 | <input type="text"/> |
| Recipient E-mail Address 3 | <input type="text"/> |
| Recipient E-mail Address 4 | <input type="text"/> |
| Recipient E-mail Address 5 | <input type="text"/> |
| Recipient E-mail Address 6 | <input type="text"/> |

| 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 | <ul style="list-style-type: none"> ■ Username: the authentication username ■ Password: the authentication password ■ 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 |

Event Selection

The device supports both SYSLOG and SMTP alerts. Check the corresponding box to enable the system event warning method you want. Please note that the checkboxes will gray out if SYSLOG or SMTP is disabled.

System Warning - Event Selection

| System Events | SYSLOG | SMTP |
|--------------------------------|--------------------------|--------------------------|
| System Start | <input type="checkbox"/> | <input type="checkbox"/> |
| Power Status | <input type="checkbox"/> | <input type="checkbox"/> |
| SNMP Authentication Failure | <input type="checkbox"/> | <input type="checkbox"/> |
| Redundant Ring Topology Change | <input type="checkbox"/> | <input type="checkbox"/> |

| Port | SYSLOG | SMTP |
|------|---|--|
| 1 | Disabled ▼ | Link Up and Link Down ▼ |
| 2 | Disabled ▼ | Link Up ▼ |
| 3 | Disabled ▼ | Link Down ▼ |
| 4 | Disabled ▼ | Disabled ▼ |
| 5 | Disabled ▼ | Disabled ▼ |
| 6 | Disabled ▼ | 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 Change | Topology | Sends out alerts when O-Ring topology changes |
| Port Event | SYSLOG / SMTP event | <ul style="list-style-type: none"> ■ Disable ■ Link Up ■ Link Down ■ Link Up & Link Down |
| Apply | | Click to activate the configurations |
| Help | | Shows help file |

5.10 Monitor and Diag

5.10.1 MAC Table

A MAC address table is a table in a network switch that maps MAC addresses to ports. The switch uses the table to determine which port the incoming packet should be forwarded to. Entries in a MAC address table fall into two types: dynamic and static entries. Entries in a static MAC table are added or removed manually and cannot age out by themselves. Entries in a dynamic MAC table will age out after a configured aging time. Such entries can be added by learning or manual configuration.

MAC Address Table Configuration

Aging Configuration

| | |
|--------------------------------|---|
| Disable Automatic Aging | <input type="checkbox"/> |
| Aging Time | <input style="width: 50px;" type="text" value="300"/> seconds |

MAC Table Learning

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

Static MAC Table Configuration

| | | | Port Members | | | | | | | | | | | |
|--|---------|-------------|--------------|---|---|---|---|---|---|---|---|----|----|----|
| Delete | VLAN ID | MAC Address | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| <input type="button" value="Add New Static Entry"/> | | | | | | | | | | | | | | |
| <input type="button" value="Save"/> <input type="button" value="Reset"/> | | | | | | | | | | | | | | |

Aging Configuration

Aging enables the switch to track only active MAC addresses on the network and flush out MAC addresses that are no longer used, thereby keeping the table current. By default, aged entries are removed after 300 seconds. You can configure aging time by entering a value in the **Age Time** box in seconds. 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

The switch can add the address and port on which the packet was received to the MAC table if the address does not exist in the table by examining the source address of each packet received on a port. This is called learning. It allows the MAC table to expand dynamically. 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.

MAC Table Learning

| | Port Members | | | | | | | | | | | |
|----------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Auto | <input checked="" type="radio"/> |
| Disable | <input type="radio"/> |
| Secure | <input type="radio"/> |

| Label | Description |
|----------------|---|
| Auto | Learning is done automatically as soon as a frame with unknown SMAC is received. |
| Disable | No learning is done. |
| Secure | Only static MAC entries are learned, all other frames are dropped. Note: make sure 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

This tablet shows the static entries in the MAC table which can contain up to 64 entries. Using static MAC address entries can reduce broadcast packets remarkably and are suitable for networks where network devices seldom change. You can manage the entries in this page. The MAC table is sorted first by VLAN ID and then by MAC address.

Static MAC Table Configuration

| Delete | VLAN ID | MAC Address | Port Members | | | | | | | | | | | |
|----------------------|---------|-------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Delete | 1 | 00-00-00-00-00-00 | <input type="checkbox"/> |
| Add New Static Entry | | | | | | | | | | | | | | |
| Save | | | Reset | | | | | | | | | | | |

| 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. |

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 **Refresh** 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.



| | |
|---------------------|--|
| 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 |

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

Detailed Port Statistics Port 1

Port 1 ▼
 Auto-refresh
 Refresh Refresh
 Clear Clear

| Receive Total | | Transmit Total | |
|------------------------|---|-------------------------|---|
| Rx Packets | 0 | Tx Packets | 0 |
| Rx Octets | 0 | Tx Octets | 0 |
| Rx Unicast | 0 | Tx Unicast | 0 |
| Rx Multicast | 0 | Tx Multicast | 0 |
| Rx Broadcast | 0 | Tx Broadcast | 0 |
| Rx Pause | 0 | Tx Pause | 0 |
| Receive Size Counters | | Transmit Size Counters | |
| Rx 64 Bytes | 0 | Tx 64 Bytes | 0 |
| Rx 65-127 Bytes | 0 | Tx 65-127 Bytes | 0 |
| Rx 128-255 Bytes | 0 | Tx 128-255 Bytes | 0 |
| Rx 256-511 Bytes | 0 | Tx 256-511 Bytes | 0 |
| Rx 512-1023 Bytes | 0 | Tx 512-1023 Bytes | 0 |
| Rx 1024-1526 Bytes | 0 | Tx 1024-1526 Bytes | 0 |
| Rx 1527- Bytes | 0 | Tx 1527- Bytes | 0 |
| Receive Queue Counters | | Transmit Queue Counters | |
| Rx Q0 | 0 | Tx Q0 | 0 |
| Rx Q1 | 0 | Tx Q1 | 0 |
| Rx Q2 | 0 | Tx Q2 | 0 |
| Rx Q3 | 0 | Tx Q3 | 0 |
| Rx Q4 | 0 | Tx Q4 | 0 |
| Rx Q5 | 0 | Tx Q5 | 0 |
| Rx Q6 | 0 | Tx Q6 | 0 |
| Rx Q7 | 0 | Tx Q7 | 0 |
| Receive Error Counters | | Transmit Error Counters | |
| Rx Drops | 0 | Tx Drops | 0 |
| Rx CRC/Alignment | 0 | Tx Late/Exc. Coll. | 0 |
| Rx Undersize | 0 | | |
| Rx Oversize | 0 | | |
| Rx Fragments | 0 | | |
| Rx Jabber | 0 | | |
| Rx Filtered | 0 | | |



| 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

Port mirroring function will copy the traffic of one port to another port on the same switch to allow the network analyzer attached to the mirror port to monitor and analyze packets. The function is useful for troubleshooting. 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 can be all frames received on a given port (also known as ingress or source mirroring) or all frames transmitted on a given port (also known as egress or destination mirroring). The port to which the monitored traffic is copied is called mirror port.

Mirror Configuration

Port to mirror to Disabled ▾

| Port | Mode |
|------|------------|
| 1 | Disabled ▾ |
| 2 | Disabled ▾ |
| 3 | Disabled ▾ |
| 4 | Disabled ▾ |
| 5 | Disabled ▾ |
| 6 | Disabled ▾ |

| Label | Description |
|-------------|--|
| Port | The switch port number to which the following settings will be applied. |
| Mode | Drop-down list for selecting a mirror mode. Rx only: only frames received on this port are mirrored to the mirror port. Frames transmitted are not mirrored. Tx only: only frames transmitted from this port are mirrored to the mirror port. Frames received are not mirrored. Disabled: neither transmitted nor received frames are mirrored. Enabled: both received and transmitted frames are mirrored to the mirror port. 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 only . |

5.10.4 System Log Information

This page provides switch system log information.

System Log Information

Auto-refresh Refresh Clear |<< << >> >>| Open in new window

Level All ▾

The total number of entries is 1 for the given level.

Start from ID with entries per page.

| ID | Level | Time | Message |
|----|-------|---------------------------|--|
| 1 | Info | 1970-01-01 00:01:09 +0000 | Port. 1 Device(192.168.10.66): Alive Check got reply again. |

| Label | Description |
|---------------------|--|
| ID | The ID (>= 1) of the system log entry |
| Level | <p>The level of the system log entry. The following level types are supported:</p> <p>Info: provides general information</p> <p>Warning: provides warning for abnormal operation</p> <p>Error: provides error message</p> <p>All: enables all levels</p> |
| 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 Cable Diagnostics

You can perform cable diagnostics for all ports or selected ports to diagnose any cable faults (short, open etc.) and feedback a distance to the fault. Simply select the port from the drop-down list and click Start to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY diagnostics is only accurate for cables 7 - 140 meters long. 10 and 100 Mbps ports will be disconnected while running VeriPHY diagnostics. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is completed.

VeriPHY Cable Diagnostics

Port

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

| Label | Description |
|---------------------|---|
| Port | The port for which VeriPHY Cable Diagnostics is requested |
| Cable Status | Port: port number Pair: the status of the cable pair Length: the length (in meters) of the cable pair |

5.10.6 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.

ICMP Ping

| | |
|-------------------|--------------------------------------|
| IP Address | <input type="text" value="0.0.0.0"/> |
| Ping Size | <input type="text" value="64"/> |

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

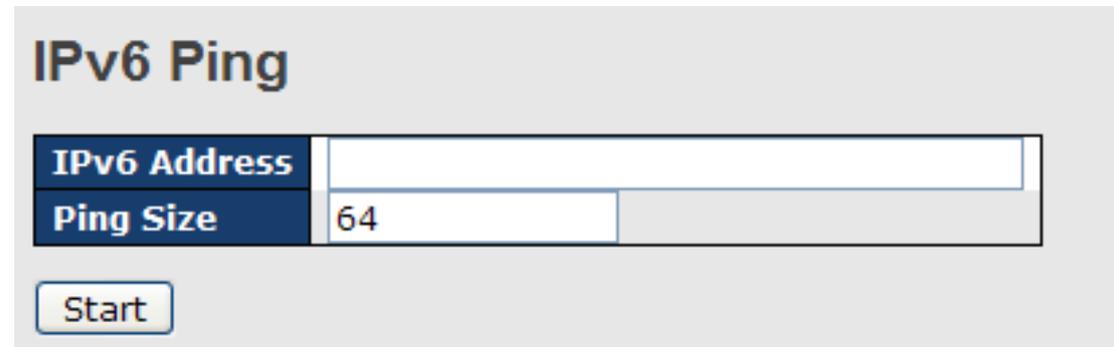
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms

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 Size | The payload size of the ICMP packet. Values range from 8 to 1400 bytes. |

IPv6 Ping



The screenshot shows a web interface for IPv6 Ping. At the top, the title "IPv6 Ping" is displayed. Below the title, there are two input fields: "IPv6 Address" and "Ping Size". The "Ping Size" field contains the value "64". Below these fields is a "Start" button.

PING v6 server ::192.168.10.1

sendto

sendto

sendto

sendto

sendto

Sent 5 packets, received 0 OK, 0 bad

5.11 Synchronization

PTP External Clock Mode

PTP External Clock Mode is a protocol for synchronizing clocks throughout a computer network. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems.

PTP External Clock Mode

| | |
|------------------------|---------|
| One_PPS_Mode | Disable |
| External Enable | False |
| VCXO Enable | False |
| Clock Frequency | 1 |

| Label | Description |
|------------------------|--|
| One_pps_mode | <p>The box allows you to select One_pps_mode configurations.</p> <p>The following values are possible:</p> <p>Output: enable the 1 pps clock output</p> <p>Input: enable the 1 pps clock input</p> <p>Disable: disable the 1 pps clock in/out-put</p> |
| External Enable | <p>The box allows you to configure external clock output.</p> <p>The following values are possible:</p> <p>True: enable external clock output</p> <p>False: disable external clock output</p> |
| VCXO_Enable | <p>The box allows you to configure the external VCXO rate adjustment.</p> <p>The following values are possible:</p> <p>True: enable external VCXO rate adjustment</p> <p>False: disable external VCXO rate adjustment</p> |
| Clock Frequency | <p>The box allows you to set clock frequency.</p> <p>The range of values is 1 - 25000000 (1 - 25MHz).</p> |



PTP Clock Configurations

PTP Clock Configuration

| Delete | Clock Instance | Device Type | Port List | | | | | | | |
|----------------------------|----------------|-------------|-------------|-------------------------|---------|----------|--------------------------|-----|-----|---|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| No Clock Instances Present | | | | | | | | | | |
| Delete | Clock Instance | Device Type | 2 Step Flag | Clock Identity | One Way | Protocol | VLAN Tag Enable | VID | PCP | |
| Delete | 0 | Ord-Bound | True | 00:1e:94:ff:fe:ff:ff:ff | False | Ethernet | <input type="checkbox"/> | 0 | 0 | |

| Label | Description |
|------------------------|---|
| Delete | Check this box and click Save to delete the clock instance |
| Clock Instance | Indicates the instance of a particular clock instance [0..3] Click on the clock instance number to edit the clock details |
| Device Type | Indicates the type of the clock instance. There are five device types. Ord-Bound : ordinary/boundary clock P2p Transp : peer-to-peer transparent clock E2e Transp : end-to-end transparent clock Master Only : master only Slave Only : slave only |
| Port List | Set check mark for each port configured for this Clock Instance. |
| 2 Step Flag | Static member defined by the system; true if two-step Sync events and Pdelay_Resp events are used |
| Clock Identity | Shows a unique clock identifier |
| One Way | If true , one-way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests. |
| Protocol | Transport protocol used by the PTP protocol engine Ethernet PTP over Ethernet multicast ip4multi PTP over IPv4 multicast ip4uni PTP over IPv4 unicast Note: IPv4 unicast protocol only works in Master Only and Slave Only clocks For more information, please refer to Device Type . In a unicast Slave Only clock, you also need to configure which master clocks to request Announce and Sync messages from. For more information, please refer to Unicast Slave Configuration |
| VLAN Tag Enable | Enables VLAN tagging for PTP frames |

| | |
|------------|---|
| | Note: Packets are only tagged if the port is configured for vlan tagging. i.e: Port Type != Unaware and PortVLAN mode == None, and the port is member of the VLAN. |
| VID | VLAN identifiers used for tagging the PTP frames |
| PCP | Priority code point values used for PTP frames |

5.12 Troubleshooting

5.12.1 Factory Defaults

This function is to force the switch back to the original factory settings. To reset the switch, select **Reset to Factory Defaults** from the drop-down list and click **Yes**. Only the IP configuration is retained.

Factory Defaults

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

| Label | Description |
|------------|--|
| Yes | Click to reset the configuration to factory defaults |
| No | Click to return to the Port State page without resetting |

5.12.2 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.

Warm Reset

Are you sure you want to perform a Warm Restart?

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

5.13 Command Line Interface Management

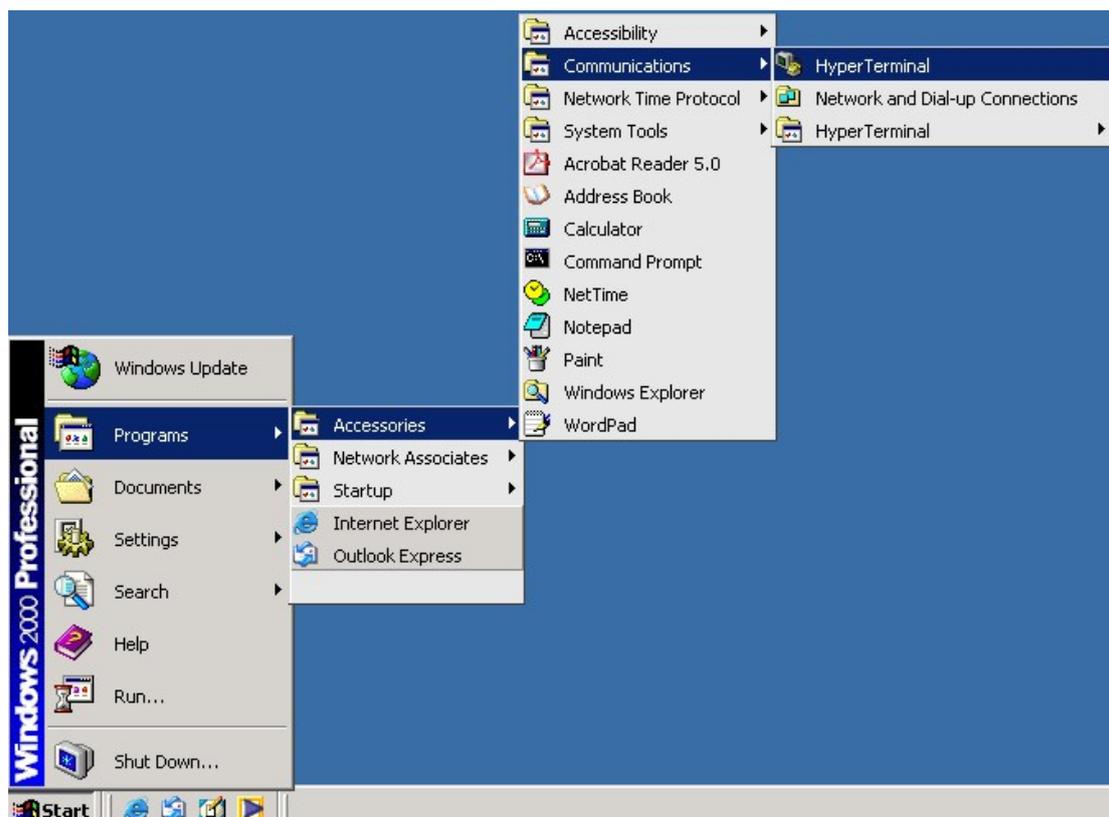
Besides Web-based management, the switch also supports CLI management. You can use console or telnet to manage the switch by CLI.

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

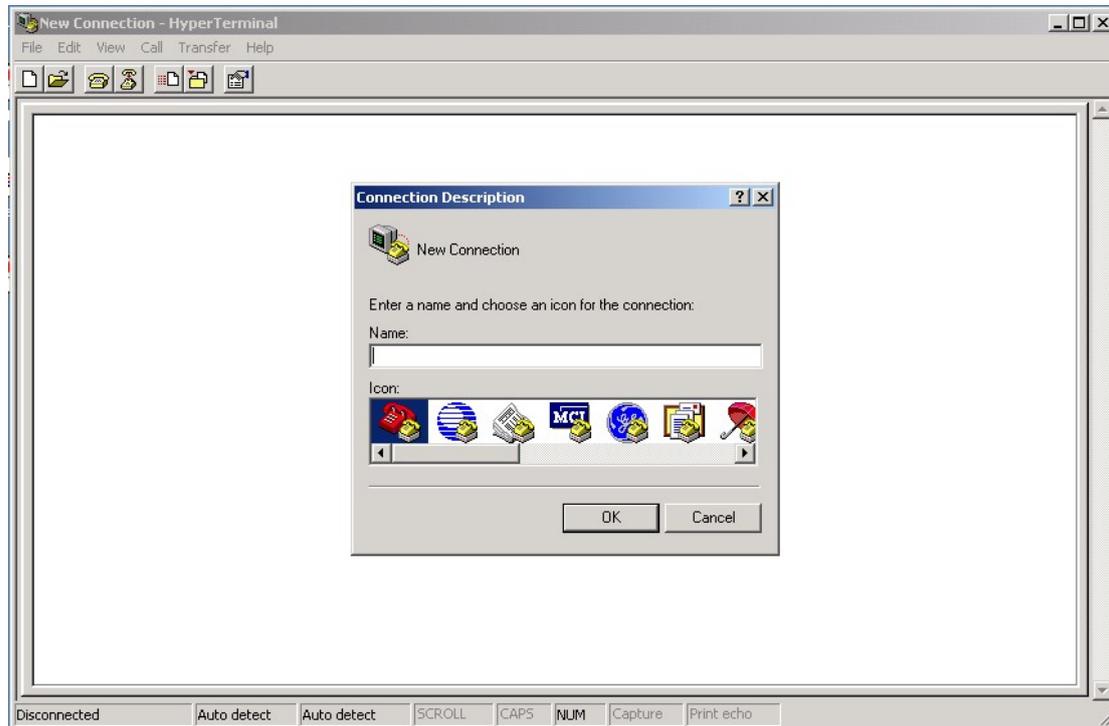
Before configuring RS-232 serial console, connect the RS-232 port of the switch to your PC Com port using a RJ45 to DB9-F cable.

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

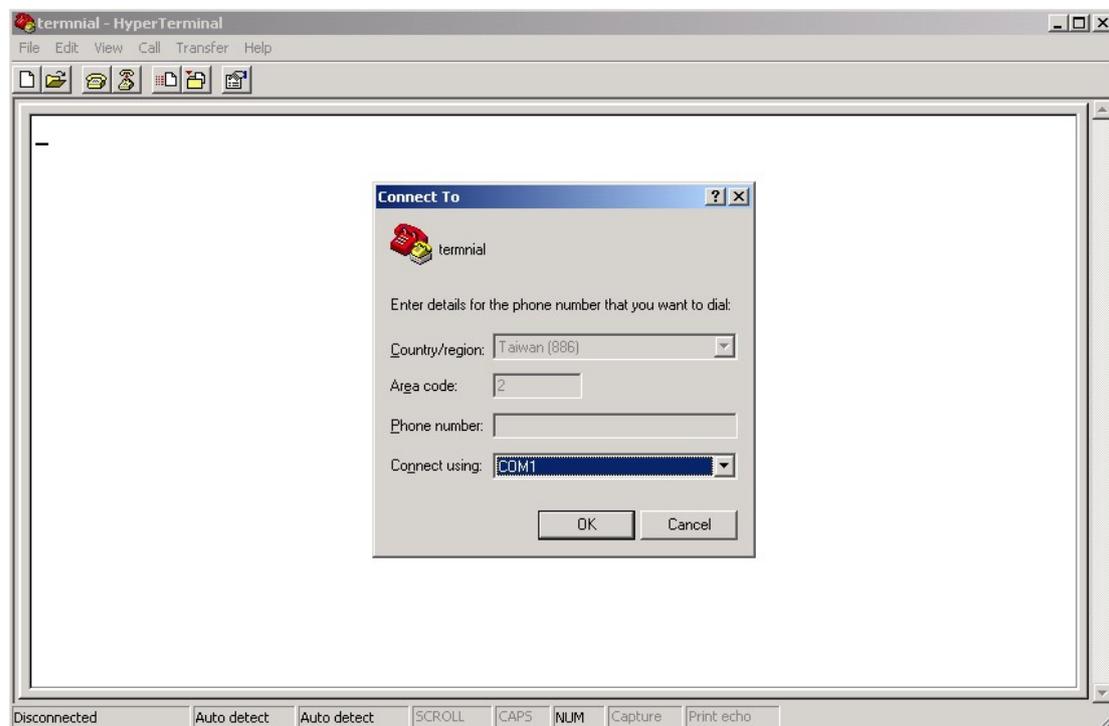
Step 1: On Windows desktop, click on **Start -> Programs -> Accessories -> Communications -> Hyper Terminal**



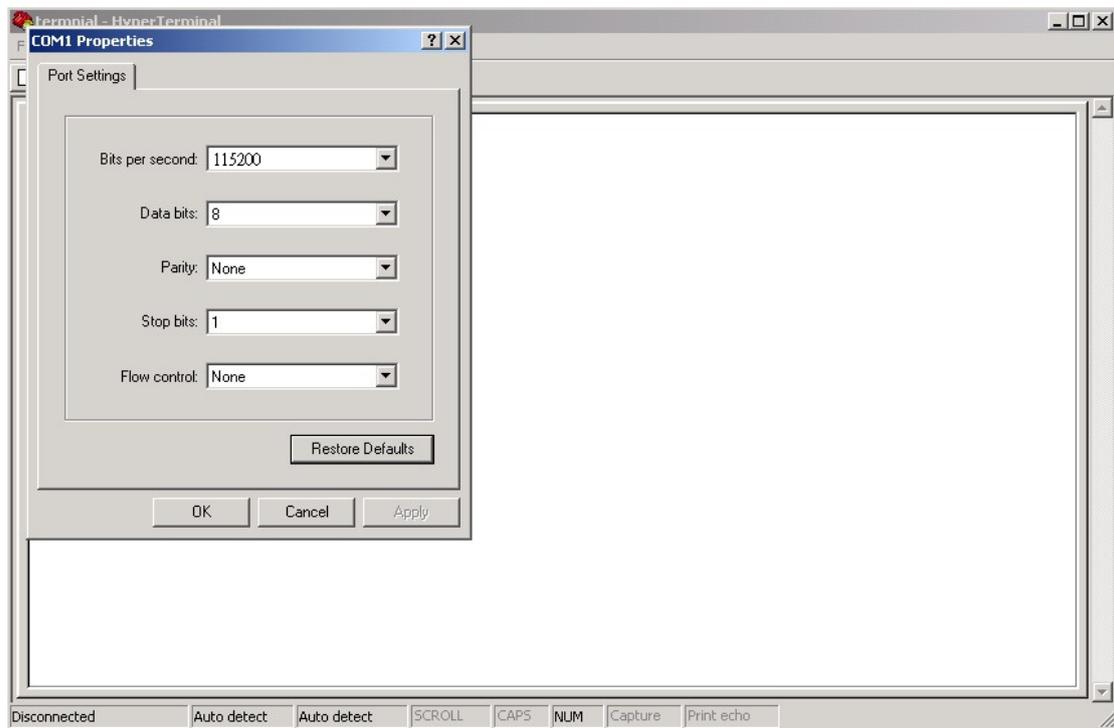
Step 2. Input a name for the new connection.



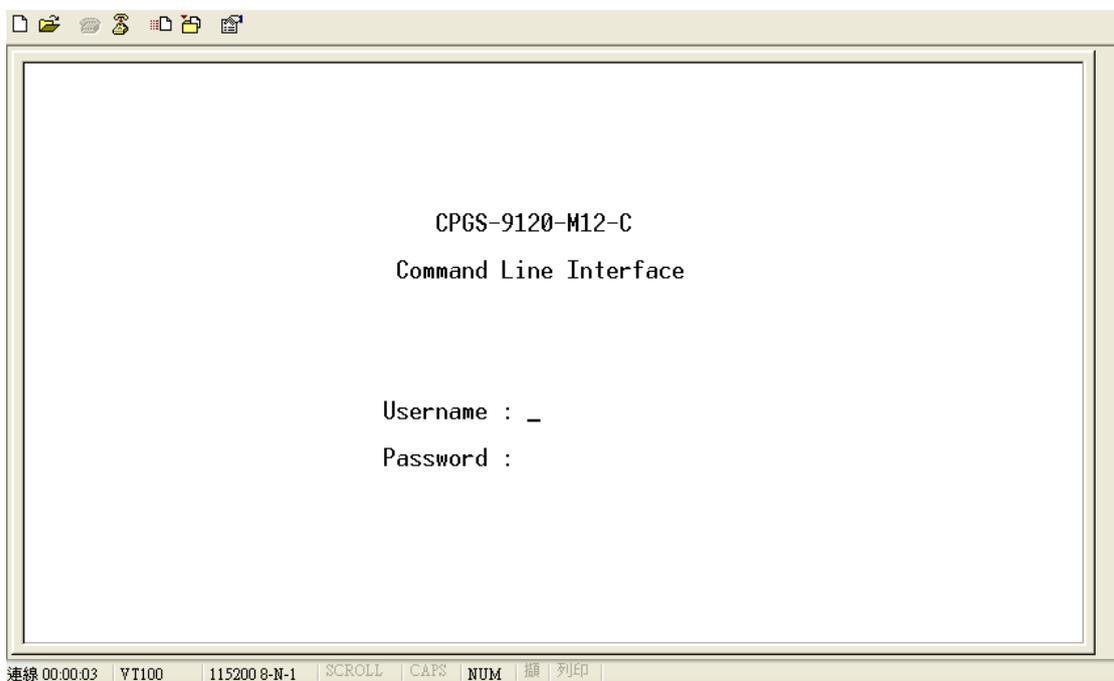
Step 3. Select a COM port in the drop-down list.



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

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

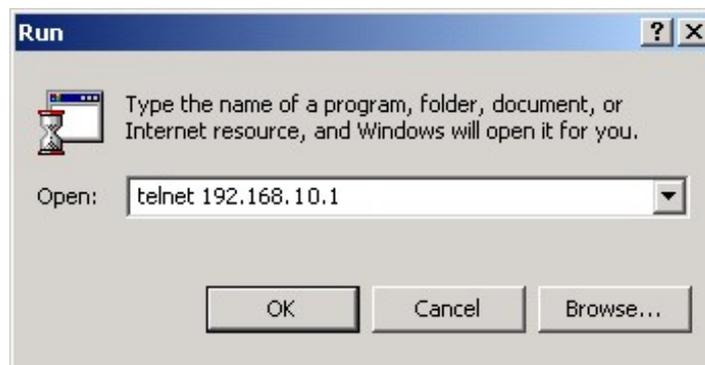
Default Gateway: **192.168.10.254**

User Name: **admin**

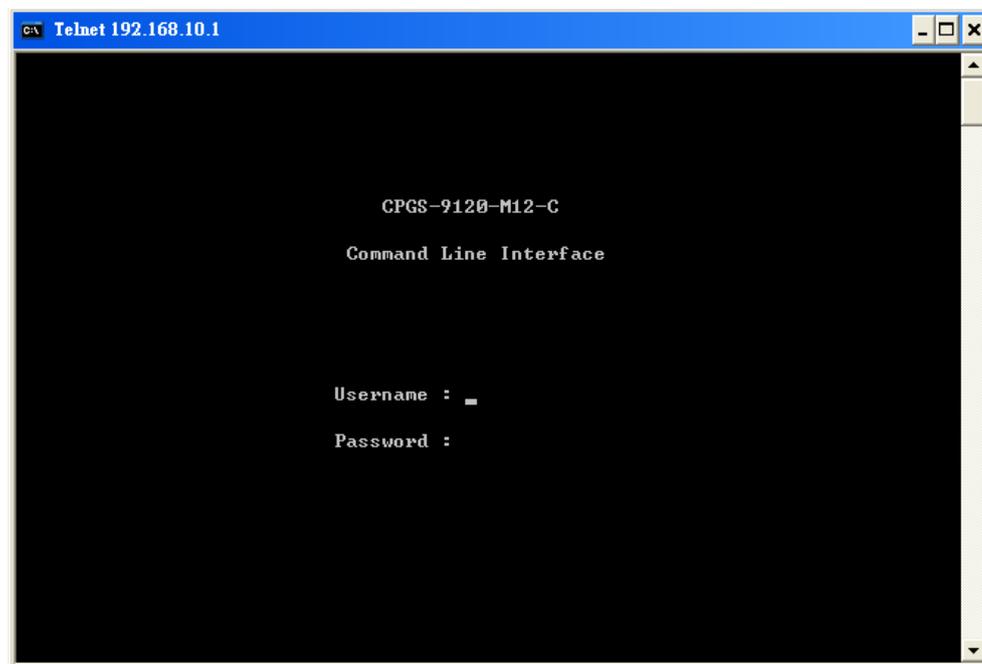
Password: **admin**

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
Syslog      : Syslog Server Configuration
IP          : IP configuration and Ping
Auth        : Authentication
Port        : Port management
Aggr        : Link Aggregation
LACP        : Link Aggregation Control Protocol
STP         : Spanning Tree Protocol
Dot1x       : IEEE 802.1X port authentication
IGMP        : Internet Group Management Protocol snooping
LLDP        : Link Layer Discovery Protocol
MAC         : MAC address table
ULAN        : Virtual LAN
PULAN       : Private ULAN
QoS         : Quality of Service
ACL         : Access Control List
Mirror      : Port mirroring
Config      : Load/Save of configuration via TFTP
SNMP        : Simple Network Management Protocol
Firmware    : Download of firmware via TFTP
Fault       : Fault Alarm Configuration
SFLOW       : SFLOW
```

**System**

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

Syslog

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

IP

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

Auth

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

Port

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

Aggr

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

LACP

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

STP

| | |
|------|---|
| STP> | Configuration |
| | Version [<stp_version>] |
| | Non-certified release, v |
| | Txhold [<holdcount>]lt 15:15:15, Dec 6 2007 |
| | MaxAge [<max_age>] |
| | FwdDelay [<delay>] |
| | bpduFilter [enable disable] |
| | bpduGuard [enable disable] |

| | |
|--|--|
| | recovery [<timeout>] |
| | CName [<config-name>] [<integer>] |
| | Status [<msti>] [<port_list>] |
| | Msti Priority [<msti>] [<priority>] |
| | Msti Map [<msti>] [clear] |
| | Msti Add <msti> <vid> |
| | Port Configuration [<port_list>] |
| | Port Mode [<port_list>] [enable disable] |
| | Port Edge [<port_list>] [enable disable] |
| | Port AutoEdge [<port_list>] [enable disable] |
| | Port P2P [<port_list>] [enable disable auto] |
| | Port RestrictedRole [<port_list>] [enable disable] |
| | Port RestrictedTcn [<port_list>] [enable disable] |
| | Port bpduGuard [<port_list>] [enable disable] |
| | Port Statistics [<port_list>] |
| | Port Mcheck [<port_list>] |
| | Msti Port Configuration [<msti>] [<port_list>] |
| | Msti Port Cost [<msti>] [<port_list>] [<path_cost>] |
| | Msti Port Priority [<msti>] [<port_list>] [<priority>] |

Dot1x

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

IGMP

| | |
|-------|-----------------------------|
| IGMP> | Configuration [<port_list>] |
| | Mode [enable disable] |

| | |
|--|--|
| | State [<vid>] [enable disable] |
| | Querier [<vid>] [enable disable] |
| | Fastleave [<port_list>] [enable disable] |
| | Router [<port_list>] [enable disable] |
| | Flooding [enable disable] |
| | Groups [<vid>] |
| | Status [<vid>] |

LLDP

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

MAC

| | |
|------|--|
| | Configuration [<port_list>] |
| | Add <mac_addr> <port_list> [<vid>] |
| | Delete <mac_addr> [<vid>] |
| | Lookup <mac_addr> [<vid>] |
| MAC> | Agetime [<age_time>] |
| | Learning [<port_list>] [auto disable secure] |
| | Dump [<mac_max>] [<mac_addr>] [<vid>] |
| | Statistics [<port_list>] |
| | Flush |

VLAN

| | |
|-------|--------------------------------------|
| | Configuration [<port_list>] |
| VLAN> | Aware [<port_list>] [enable disable] |
| | PVID [<port_list>] [<vid> none] |

| | |
|--|--------------------------------------|
| | FrameType [<port_list>] [all tagged] |
| | Add <vid> [<port_list>] |
| | Delete <vid> |
| | Lookup [<vid>] |

PVLAN

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

QOS

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



ACL

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

Mirror

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

Config

| | |
|---------|--------------------------------------|
| Config> | Save <ip_server> <file_name> |
| | Load <ip_server> <file_name> [check] |

SNMP

| | |
|-------|---|
| 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> |
|-----------|-----------------------------------|

fault

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

SFLOW

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



Technical Specifications

| ORing Switch Model | CPGS-9120-M12-C |
|--|--|
| Physical Ports | |
| 10/100/1000Base-T(X) Ports Auto MDI/MDIX | 12-port (8-port with CompactPCI interface, 4-port with M12 A-coding connector) (PICMG 2.0 compatible) |
| Technology | |
| Ethernet Standards | IEEE 802.3 for 10Base-T IEEE 802.3u for 100Base-TX IEEE 802.3ab for 1000Base-T IEEE 802.3x for Flow control IEEE 802.3ad for LACP (Link Aggregation Control Protocol) IEEE 802.1D for STP (Spanning Tree Protocol) IEEE 802.1p for COS (Class of Service) IEEE 802.1Q for VLAN Tagging IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol) IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol) IEEE 802.1x for Authentication IEEE 802.1AB for LLDP (Link Layer Discovery Protocol) |
| MAC Table | 8k |
| Priority Queues | 8 |
| Processing | Store-and-Forward |
| Switch Properties | Switching latency: 7 us Switching bandwidth: 24Gbps Max. Number of Available VLANs: 4096 IGMP multicast groups: 128 for each VLAN Port rate limiting: User Define |
| Jumbo frame | Up to 9.6K Bytes |
| Security Features | Device Binding security feature Enable/disable ports, MAC based port security Port based network access control (802.1x) VLAN (802.1Q) to segregate and secure network traffic Radius centralized password management SNMPv3 encrypted authentication and access security Https / SSH enhance network security |
| Software Features | STP/RSTP/MSTP (IEEE 802.1D/w/s) Redundant Ring (O-Ring) with recovery time less than 30ms over 250 units TOS/Diffserv supported Quality of Service (802.1p) for real-time traffic VLAN (802.1Q) with VLAN tagging supported IGMP Snooping IP-based bandwidth management Application-based QoS management DOS/DDOS auto prevention Port configuration, status, statistics, monitoring, security DHCP Server/Client/Relay SMTP Client Modbus TCP |
| Network Redundancy | O-Ring Open-Ring O-Chain MRP MSTP (STP / RSTP compatible) |
| RS-232 Serial Console Port | RS-232 in RJ45 connector with console cable. 115200bps, 8, N, 1 |
| LED indicators | |
| Power indicator (Power) | Green : Power LED x 1 |
| Status Indicator (STA) | Green : Ethernet status indicator |
| R.M. indicator (R.M) | Green : indicate system operated in O-Ring Master mode |
| Ring indicator (Ring) | Green : indicate system operated in O-Ring mode |



| | |
|-------------------------------------|--|
| Fault indicator (Fault) | Amber : Indicate unexpected event occurred |
| 10/100/1000Base-T(X) port indicator | Green for port Link/Act. |
| Power | |
| Power Input | CompactPCI bus powered (12VDC) |
| Power Consumption (Typ.) | TBD |
| Overload Current Protection | Present |
| Physical Characteristic | |
| Dimension (W x D x H) | TBD |
| Weight (g) | 340 g |
| Environmental | |
| Storage Temperature | -40 to 85°C (-40 to 185°F) |
| Operating Temperature | -40 to 70°C (-40 to 158°F) |
| Operating Humidity | 5% to 95% Non-condensing |
| Regulatory approvals | |
| EMI | FCC Part 15, CISPR (EN55022) class A, EN50155 (EN50121-3-2, EN55011, EN50121-4) |
| EMS | EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11 |
| Shock | IEC60068-2-27 |
| Free Fall | IEC60068-2-32 |
| Vibration | IEC60068-2-6 |
| Safety | EN60950-1 |
| Warranty | 5 years |