WoMaster

COVER

User Manual

DS410F

Industrial 10-port Full Gigabit L2 Managed Fiber/Ethernet Switch

Nov.23.2018 V.1.0

WOM ASIA Co., Ltd

1F., No.185-3, Kewang Rd., Longtan Dist., Taoyuan 325, Taiwan

www.womaster.eu

WoMaster

DS410F Industrial 10-port Full Gigabit L2 Managed Fiber/Ethernet Switch

User Manual

Copyright Notice

© WoMaster. All rights reserved.

About This Manual

This user manual is intended to guide a professional installer to install and to configure the DS410F switch. It includes procedures to assist you in avoiding unforeseen problems.

NOTE:

Only qualified and trained personnel should be involved with installation, inspection, and repairs of this switch.

Disclaimer

WoMaster reserves the right to make changes to this Manual or to the product hardware at any time without notice. Information provided here is intended to be accurate and reliable. However, it might not cover all details and variations in the equipment and does not claim to provide for every possible contingency met in the process of installation, operation, or maintenance. Should further information be required or should particular problem arise which are not covered sufficiently for the user's purposes, the matter should be referred to WoMaster. Users must be aware that updates and amendments will be made from time to time to add new information and/or correct possible unintentional technical or typographical mistakes. It is the user's responsibility to determine whether there have been any such updates or amendments of the Manual. WoMaster assumes no responsibility for its use by the third parties.

WoMaster Online Technical Services

At WoMaster, you can use the online service forms to request the support. The submitted forms are stored in server for WoMaster team member to assign tasks and monitor the status of your service. Please feel free to write to help@womaster.eu if you encounter any problems.

TABLE OF CONTENTS

COVER 1

TABLE OF CONTENTS 3

1. INTRODUCTION 5

1.1 OVERVIEW 5

1.2 MAJOR FEATURES 6

2. HARDWARE INSTALLATION 7

2.1HARDWARE DIMENSION 7

2.2WIRING THE POWER INPUTS 9

2.3WIRING THE ALARM RELAY OUTPUT (DO) 10

2.4WIRING THE DIGITAL INPUT (DI) 11

2.5CONNECTING THE GROUDING SCREW 12

2.6 DIN RAIL MOUNTING 12

3. DEVICE INTERFACE MANAGEMENT 13

3.1 CONFIGURATION 22

3.1.1 SYSTEM 22

3.1.2 GREEN ETHERNET 28

3.1.3 THERMAL PROTECTION 30

3.1.4 PORTS 31

3.1.5 SECURITY 33

3.1.6 AGGREGATION 63

3.1.7 LOOP PROTECTION 67

3.1.8 SPANNING TREE 68

3.1.9 IPMC 71

3.1.10 LLDP 73

3.1.11 MAC TABLE 75

3.1.12 VLAN 77

3.1.13 PRIVATE VLANS 82

3.1.14 QoS 83

3.1.14.1 QOS CLASSIFICATION 84

3.1.14.2 POLICERS 84

3.1.14.3 SHAPERS 84

3.1.14.4 SCHEDULING ALGORITHM 84

3.1.14.5 WEIGHTED RANDOM EARLY DETECTION(WRED) 84

3.1.14.6 STORM POLICING 85

3.1.14.7 INGRESS MAP 85
3.1.14.8 EGRESS MAP 85
3.1.15 MIRRORING 113
3.2 MONITOR 116
3.2.1 SYSTEM 116
3.2.2 GREEN ETHERNET 123
3.2.3 THERMAL PROTECTION 124
3.2.4 PORTS 125
3.2.5 SECURITY 130
3.2.6 AGGREGATION 131
3.2.7 LOOP PROTECTION 132
3.2.8 SPANNING TREE 133
3.2.9 IPMC 137
3.2.10 LLDP 139
3.2.11 MAC ADDRESS 145
3.2.12 VLANS 146
3.3 DIAGNOSTICS 149
3.3.1 PING (IPv4) 149
3.3.2 TRACEROUTE (IPv4) 151
3.3.3 VeryPHY 153
3.4 MAINTANANCE 153
3.4.1 RESTART 154
3.4.2 FACTORY DEFAULT 154
3.4.3 SOFTWARE 155
3.4.4 CONFIGURATION 156
3.5 FRONT PANEL 159

1. INTRODUCTION

1.1 OVERVIEW

DS410F/DS410 series is designed for industrial environments requiring high quality fiber communication such as industrial automation, road traffic control, etc. DS410F provides 10-port **full-gigabit** Ethernet including 6-port SFP, 2-port SFP/RJ45 combo and 2-port RJ45 (up to 8-port SFP); while DS410 provides 6-port RJ45, 2-port SFP/RJ45 combo and 2-port SFP for multi-port Giga copper requirement. Full Gigabit capability and rugged industrial design ensures system high performance and reliability in harsh environments, that has excellent heat dissipation design for operating in -40~75°C environments. For convenient traffic control and zero packet loss data transmission, DS410F/DS410 offer contemporary management and security functions. For the best traffic control, the switch management side features have been utilized: LACP, VLAN, QinQ, QoS, IGMP snooping v2, and etc.

In order to uplink connection, the DS410F provides 2 RJ45/SFP Gigabit Ethernet combo ports that can prioritize stream, such as video and also optimize VoIP. Gigabit Ethernet combo ports provides high speed uplink connection to higher level backbone switches with Ring Network Redundancy technology ensures the reliability of high-quality video transfer. High flexibility of cable types and distances for system integrators and DDM (Digital Diagnostic Monitoring) type SFP transceivers also equipped the switch for diagnosing transmission problem through maintenance and debugging of the signal quality.

WoMaster managed switch is designed to provide faster, secure, and more stable network. One advantage that makes it a powerful switch is that it supports network redundancy protocols/technologies such as Rapid Spanning Tree Protocol (RSTP). IEC 61000-6-2 / 61000-6-4 Heavy Industrial EMC certified design, rugged enclosure and -40~75°C wide operating temperature range, - all these features guarantee stable performance of the switch for surveillance data transmission under vibration and shock in rolling stocks, traffic control systems and other harsh environments.

This managed switch also can be smartly configured by WoMaster advanced management utility, Web Browser, SNMP, Telnet and RS-232 local console with its command like interface.

Excellent security features also provided, such as DHCP client, DHCP server with IP and MAC binding, 802.1X Port Based Network Access Control, SSH for Telnet security, IP Access table, port security and many other security features. All of these features in order to ensure the secure data communication.

The IP31-design aluminum case further strengthens the ability in harsh industrial environment. The event warning is notified to the network administrator via e-mail, system log, or by relay output. The Industrial Managed Gigabit Ethernet Switch has also passed CE/ FCC certifications to help ensure safe and reliable data transmission for industrial applications.

1.2 MAJOR FEATURES

Below are the major features of DS410F Series Switch:

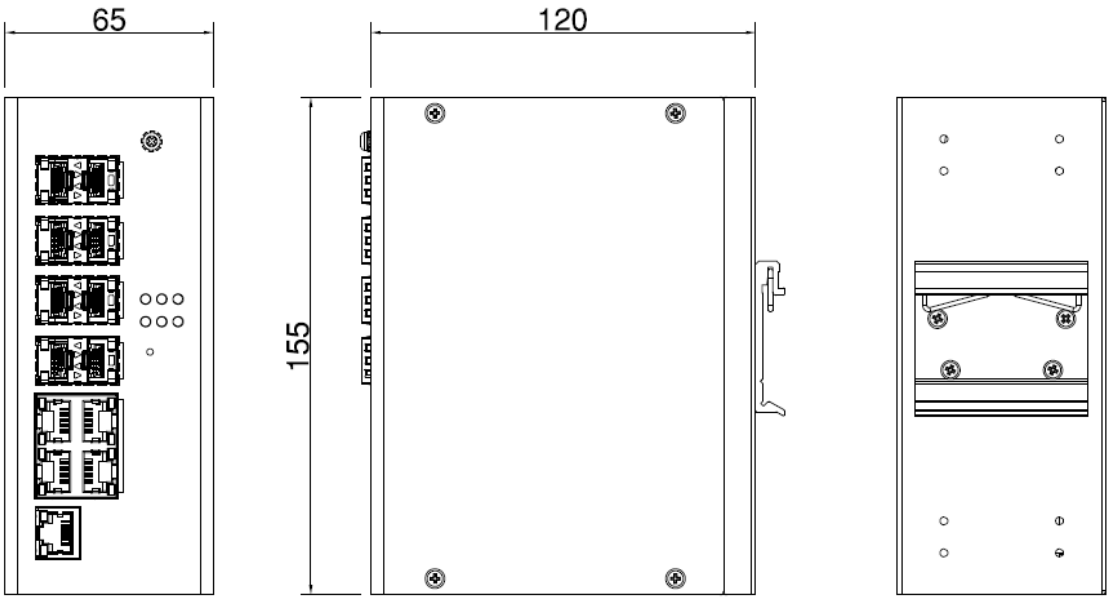
- 10-port Full Gigabit Ethernet, including 6 100/1000M SFP ports, 2 100/1000M SFP/RJ45 combo ports, and 2 RJ45 ports
- High flexibility of cable types and distances for system integrators
- DDM function for high quality fiber connectivity monitoring
- 4K MAC address table
- Stores and forwards with non-blocking switch fabric
- Advanced Management Features: Flow Control, Port Trunk/802.3ad LACP, VLAN, Private VLAN, Shared VLAN, Class of Service, Traffic Prioritize, Rate Control, Port Mirror, IGMP Snooping v2, Port classification, Port policing, Port scheduler, Port shaping, QoS control list, WRED, Port Security, ACL, Loop Protection.
- Advanced Security System: IEEE 802.1X/RADIUS, Management IP, Management VLAN, SSL
- Redundancy Technology: Rapid Spanning Tree Protocol (RSTP)
- Various configuration paths, including Web GUI, CLI, and SNMP
- LLDP topology control
- **10~60V** wide power range design with redundant
- power input NEMA-TS2 compliance for wayside traffic control assemblies
- Excellent heat dissipation design for operating in -40~75 ° C environments
- High level EMC protection exceeding traffic control and heavy industrial standards' requirements
- IEC 61000-6-2/4 Heavy Industrial Environment
- EN50121-4 railway trackside EMC Compliance
- IP31 ingress protection

2. HARDWARE INSTALLATION

This chapter introduces hardware, and contains information on installation and configuration procedures.

2.1 HARDWARE DIMENSION

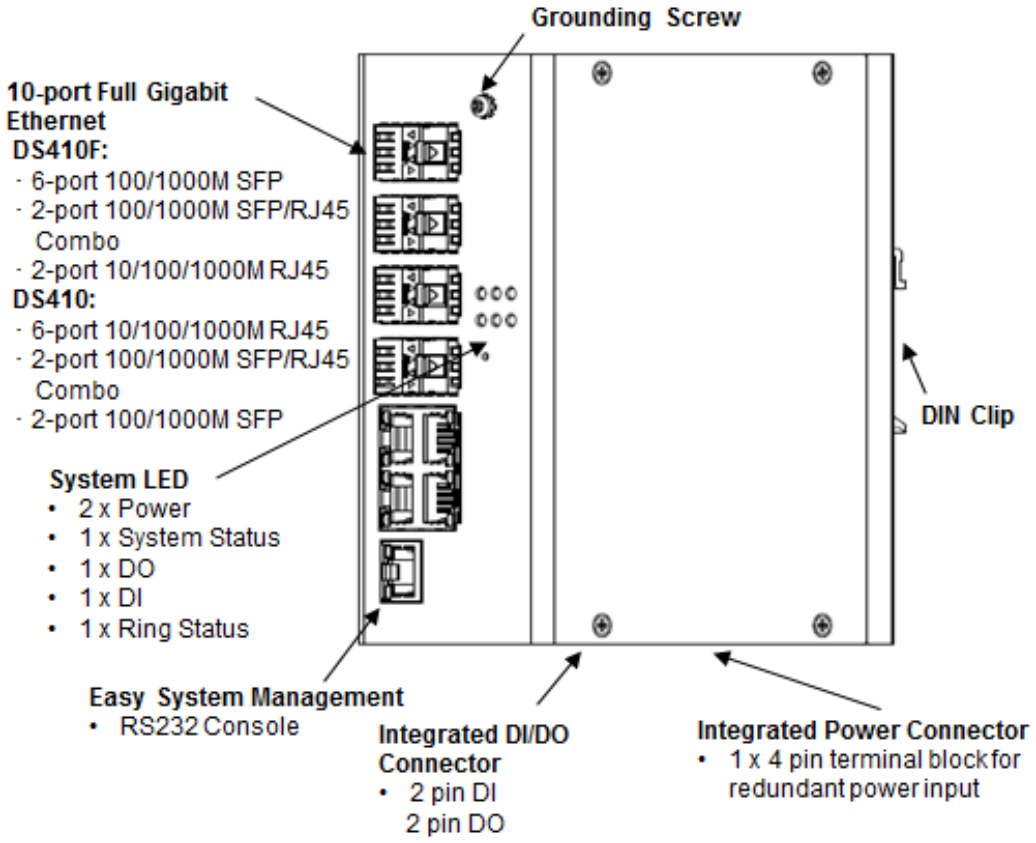
Dimensions of DS410F/DS410: 65 x 155 x 120 (W x H x D) / without DIN Rail Clip



Front Panel Layout

Below is the front panel from DS410F Series switches, for DS410F is included 6 ports 100/1000M SFP, 2 ports 100/1000M SFP/RJ45 Combo, 2 ports 10/100/1000M RJ45, and for DS410, it is included 6 ports 10/100/1000M SFP, 2 ports 100/1000M SFP/RJ45 Combo, 2 ports 100/1000M RJ45, System LED, USB for configuration/firmware management, RJ-45 diagnostic console, 2 x 4-pin terminal block connector (4 pin for power inputs, 2 pin for digital input and 2 pin for alarm relay output) and 1 chassis grounding screw. On the rear side of switch there is DIN rail clip attached.

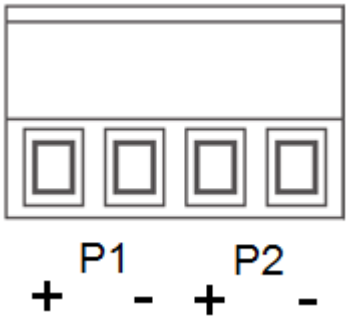
DS410F/DS410



2.2 WIRING THE POWER INPUTS

Power Input port in the switch provides 2 sets of power input connections (P1 and P2) on the terminal block. x

On the picture below is the power connector.



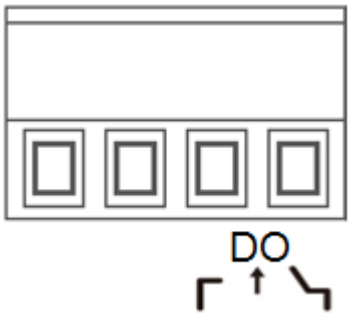
Wiring the Power Input

1. Insert the positive and negative wires into the V+ and V- contact on the terminal block connector.
2. Tighten the wire-clamp screws to prevent the power wires from being loosened.
3. Connect the power wires to suitable AC/DC Switching type power supply. The input DC voltage should be in the range of 10VDC to DC 60V DC.

> **WARNING:** Turn off AC power input source before connecting the Power to the terminal block connectors, for safety purpose. Don not turn-on the source of AC/DC power before all of the connections were well established.

2.3 WIRING THE ALARM RELAY OUTPUT (DO)

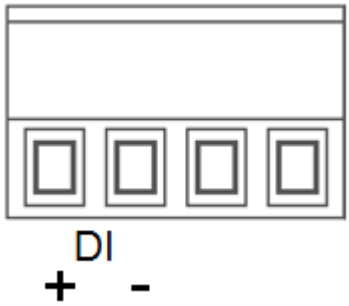
The relay output contacts are located on the front panel of the switch. The relay output consists of the 2-pin terminal block connector that used to detect user-configured events. The two wires attached to the fault contacts form a close circuit when a user-configured event is triggered. If a user-configured event does not occur, the fault circuit remains opened. The fault conditions such as power failure, Ethernet port link break or other pre-defined events which can be configured in the switch. Screw the DO wire tightly after digital output wire is connected.



NOTE: The relay contact only supports 0.5 A current, DC 24V. Do not apply voltage and current higher than the specifications.

2.4 WIRING THE DIGITAL INPUT (DI)

The Digital Input accepts one external DC type signal input that consists of two contacts on the terminal block connector on the switch's top panel. And can be configured to send alert message through Ethernet when the signal is changed. The signal may trigger and generated by external power switch, such as door open trigger switch for control cabinet. The switch's Digital Input accepts DC signal and can receive Digital High Level input DC 11V~30V and Digital Low Level input DC 0V~10V.



Here are the steps to wire the Digital Input:

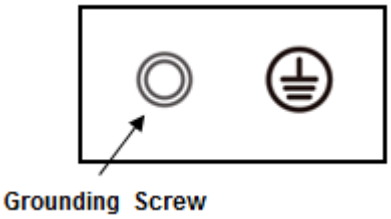
STEP 1: Insert the negative and positive wires into the -/+ terminals, respectively.

STEP 2: To keep the wires from pulling loose, tighten the wire-clamp screws on the front of the terminal block connector.

STEP 3: Insert the terminal block connector prongs into the terminal block receptor, which is located on the switch's top panel.

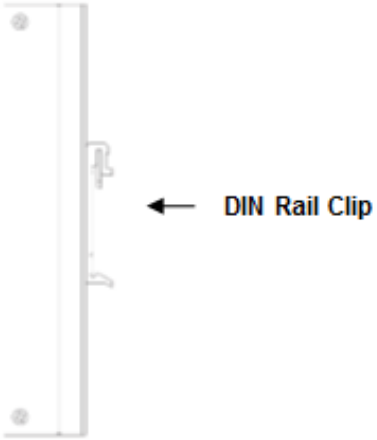
2.5 CONNECTING THE GROUDING SCREW

Grounding screw is located on the front side of the switch. Grounding Screw helps limit the effects of noise due to electromagnetic interference (EMI) such as lighting or surge protection. Run the ground connection from the ground screw to the grounding surface prior to connecting devices. And tighten and wire to chassis grounding for better durability.



2.6 DIN RAIL MOUNTING

The EN50022 DIN-Rail plate should already attached at the back panel of the switch screwed tightly. If you need to reattach the DIN-Rail attachment plate to the switch, make sure the plate is situated towards the top, as shown by the following figures.



To mount the switch on DIN Rail track, do the following instruction:

1. Insert the top side of DIN Rail track into the slot of DIN Rail clip.
2. Lightly clip the bottom of DIN-Rail to the track and make sure it attached well.
3. To remove the switch from the track, reverse the steps.

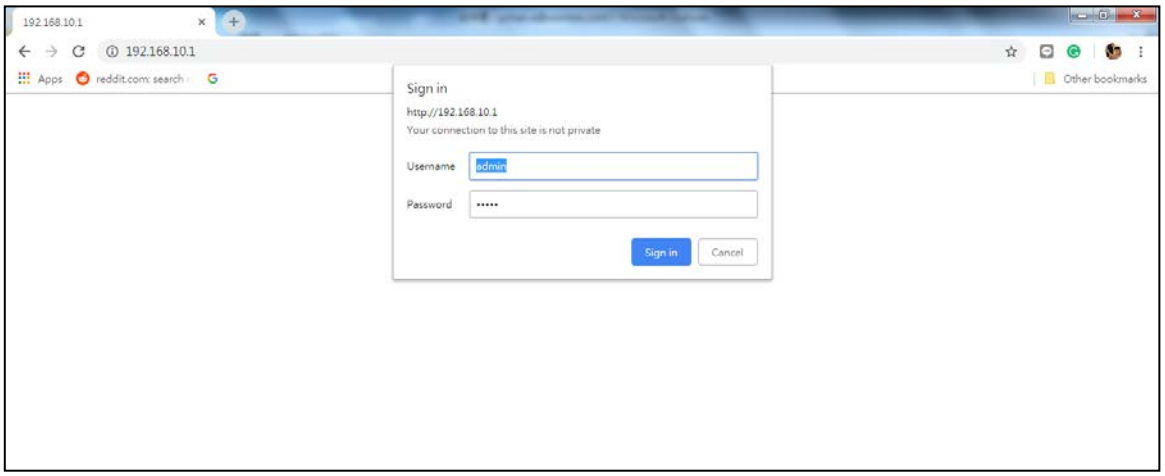
3. DEVICE INTERFACE MANAGEMENT

To access the management interface, WoMaster has several ways access mode through a network; they are web management and console management. Web interface management is the most common way and the easiest way to manage a network, through web interface management, a switch interface offering status information and a subset of switch commands through a standard web browser. If the network is down, another alternative to access the management interface can be used. The alternative way is by using console and telnet management which is offer configuration way through CLI Interface. WoMaster also provide excellent alternative by configure the switch via RS232 console cable if user doesn't attach user admin PC to the network, or if user loses network connection to Managed Switch. This manual describes the procedures for Web Interface and how to configure and monitor the managed switch only. For the CLI management interface please refers to the *CLI Command User Manual*.

PREPARATION FOR WEB INTERFACE MANAGEMENT

WoMaster provides Web interface management that allows user through standard web-browser such as Microsoft Internet Explorer, or Mozilla, or Google Chrome, to access and configure the switch management on the network.

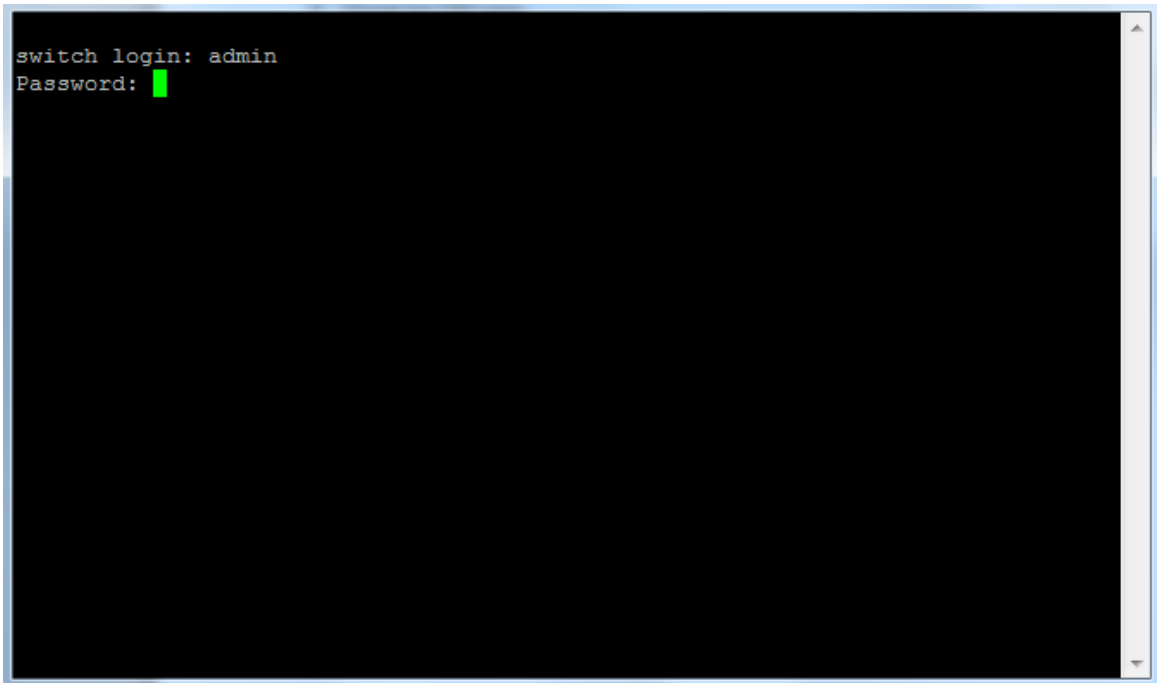
1. Plug the DC power to the switch and connect switch to computer.
2. Make sure that the switch default IP address is **192.168.10.1**.
3. Check that PC has an IP address on the same subnet as the switch. For example, the PC and the switch are on the same subnet if they both have addresses that start 192.168.1.x (Ex: **192.168.10.2)**. The subnet mask is 255.255.255.0.
4. Open command prompt and ping **192.168.10.1** to verify that the switch is reachable.
5. Launch the web browser (Internet Explorer or Mozilla Firefox or Google Chrome) on the PC.
6. Type **http://192.168.10.1** (or the IP address of the switch). And then press **Enter** and a pop up login page will appear.
7. Type user name and the password. Default user name: **admin** and password: **admin**. Then click **Login**.



PREPARATION FOR SERIAL CONSOLE

Attach RJ-45 to RS-232 DB-9 console cable to PC's COM port; connect RJ45 connector to the Console port of the WoMaster Managed Switch.

1. Go to Start -> Program -> Accessories -> Communication -> Hyper Terminal
2. Give a name to the new console connection.
3. Choose the COM name
4. Select correct serial settings. The serial settings of **WoMaster Managed switches** are as below:
   Baud Rate: 115200 / Parity: None / Data Bit: 8 / Stop Bit: 1
5. After connected, switch login screen can be seen.



6. Login the switch. The default username: **admin**; password: **admin.**

SSH (Secure Shell)

WoMaster managed SWITCH also supports SSH console. User can remotely connect to the switch by command line interface. The SSH connection can secure all the configuration commands user sent to the switch.

SSH is a client/server architecture while the switch is the SSH server. When user wants to make SSH connection with the switch, user should download the SSH client tool first.

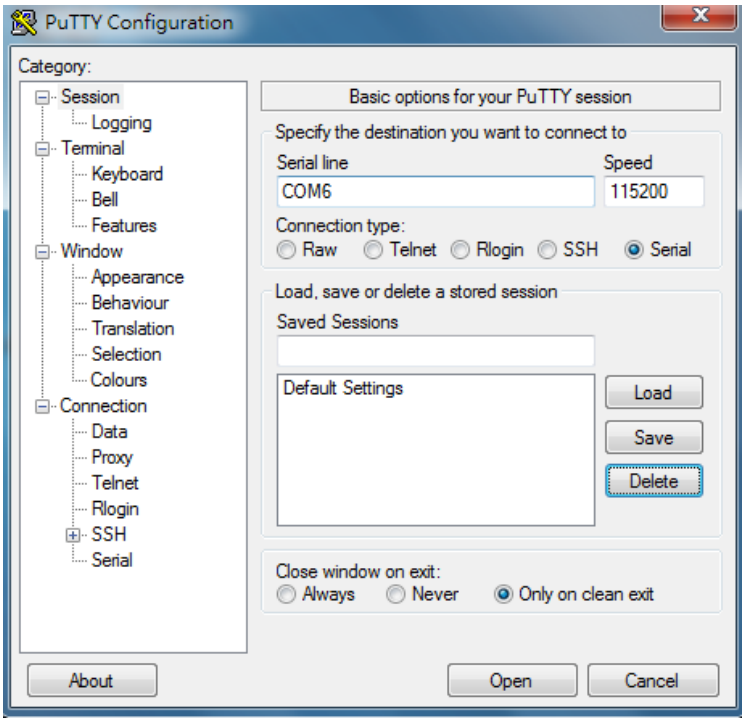
SSH Client

There are many free, sharewares, trials or charged SSH clients user can find on the internet, e.g., PuTTY is a free and popular Telnet/SSH client. We'll use this tool to demonstrate how to login by SSH. (PuTTY copyright 1997-2016 Simon Tatham).

Download PuTTY: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

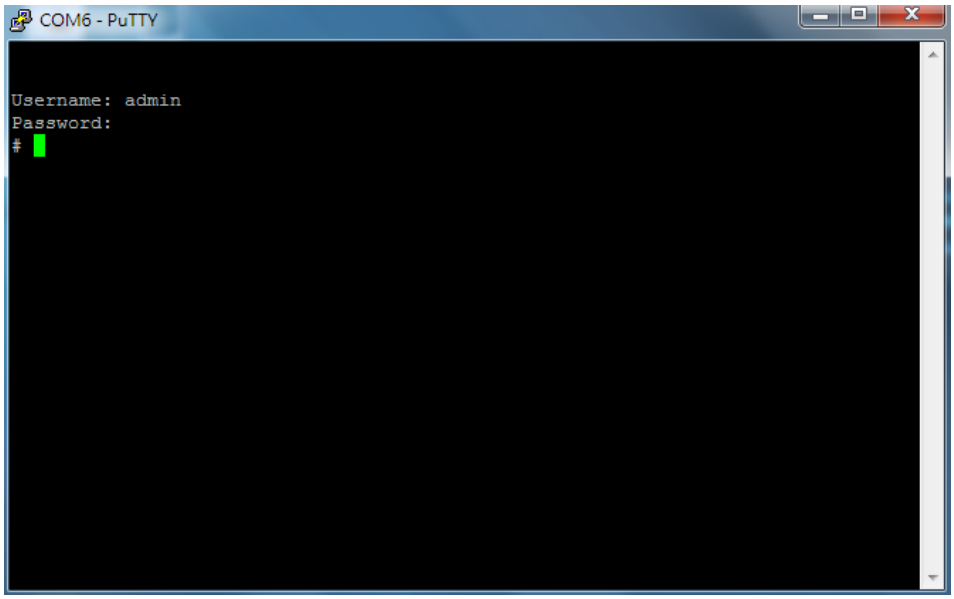
1. Open SSH Client/PuTTY

In the **Session** configuration, choose the **Serial** protocol then enter the **Serial line** and **Speed**. For the serial line, please check the device manager to make sure the serial line name. The speed should be 115200. Then click on **Open** to start the SSH session console.



2. After it user can see the CLI command screen is pop-up

3. Type the Switch Login name and its Password. The default settings are **admin / admin**.



4. All the commands user sees in Putty are the same as the CLI commands user sees via RS232 console.

The next chapter will introduce in detail how to use command line to configure some features in the switch.

For either type of connection, access to the command line interface is generally referred to as an EXEC session. There are some different command modes. Each command mode has its own access ability, available command lines and uses different command lines to enter and exit.

Privileged EXEC mode: In this mode, the system allows User to view current configuration, reset default, reload SWITCH, show system information, save configuration and enter the global configuration mode. Type **exit** to leave and press **?** to see the command list.

```
# ?
      clear            Clear
      configure        Enter configuration mode
      copy             Copy from source to destination
      delete           Delete one file in flash: file system
      dir              Directory of all files in flash: file system
      disable          Turn off privileged commands
      do               To run exec commands in the configuration mode
      dot1x            IEEE Standard for port-based Network Access Control
      enable           Turn on privileged commands
      exit             Exit from EXEC mode
      firmware         Firmware upgrade/swap
      help             Description of the interactive help system
      ip               IPv4 commands
      logout           Exit from EXEC mode
      more             Display file
      no               Delete trace hunt string
      ping             Send ICMP echo messages
      platform         Platform configuration
      reload           Reload system.
      send             Send a message to other tty lines
      show             Display statistics counters.
      terminal         Set terminal line parameters
      time             System time
      traceroute       Send IP Traceroute messages
      veriphy          VeriPHY keyword
```

Global Configuration Mode: Type configure terminal in privileged EXEC mode. Then User can enter the Global Configuration mode. In Global Configuration mode, User can configure all the features that the system provides. Type **exit** to leave and press **?** to see the command list.

The command lists of global configuration mode.

```
# configure terminal
(config)# ?
      aaa                  Authentication, Authorization and Accounting
      access               Access management
      access-list          Access list
      aggregation          Aggregation mode
      banner               Define a banner
      default              Set a command to its defaults
      do                   To run exec commands in the configuration mode
      dot1x                IEEE Standard for port-based Network Access Control
      enable               Modify enable password parameters
      end                  Go back to EXEC mode
      exit                 Exit from current mode
      green-ethernet       Green Ethernet (Power reduction)
      help                 Description of the interactive help system
      hostname             Set system's network name
      interface            Select an interface to configure
      ip                   IPv4 configurations
      lacp                 LACP settings
      line                 Configure a terminal line
      lldp                 LLDP configurations.
      logging              System logging message
      loop-protect         Loop protection configuration
      mac                  MAC table entries/configuration
      monitor              Monitoring different system events
      no                   Negate a command or set its defaults
      password             Specify the password for the administrator
      port-security        This command is obsolete.
      privilege            Command privilege parameters
      prompt               Set prompt
      qos
      radius-server        Configure RADIUS
      relay-output         Relay output configuration
      snmp-server          Set SNMP server's configurations
      spanning-tree        Spanning Tree protocol
      svl                  Shared VLAN Learning
      thermal-protect      Thermal protection configurations.
      time                 System time
      vlan                 VLAN commands
(config)#
```

Interface Configuration: Many features are enabled for a particular interface. The Interface commands enable or modify the operation of an interface. In this mode, a physical port is set up for a specific logical connection operation. The Interface Configuration mode provides access to the router interface configuration commands.

This section has three interface configuration, **Port interface, LLAG interface,** and **VLAN interface**. For Port interface, type **interface IFNAME** in global configuration mode. Then User can enter the interface configuration mode. In this mode, User can configure port settings. In port interface, the name of Gigabit Ethernet port 1 is GigabitEthernet 1/1, GigabitEthernet 1/2 and so on. Type **exit** to leave current level and press **?** to see the command list. The command lists of the global configuration mode.

```
(config)# interface ?
  *                    All switches or All ports
  GigabitEthernet      1 Gigabit Ethernet Port
  llag                 Local link aggregation interface configuration
  vlan                 VLAN interface configurations
(config)# interface GigabitEthernet ?
  <port_type_list>     Port list in 1/1-10
(config)# interface * / GigabitEthernet 1/1
(config-if)# ?
  access-list          Access list
  aggregation          Create an aggregation
  description          Description of the interface
  do                   To run exec commands in the configuration mode
  dot1x                IEEE Standard for port-based Network Access Control
  duplex               Interface duplex
  end                  Go back to EXEC mode
  excessive-restart    Restart backoff algorithm after 16 collisions (No
                       excessive-restart means discard frame after 16
                       collisions)
  exit                 Exit from current mode
  flowcontrol          Traffic flow control.
  frame-length-check   Drop frames with mismatch between EtherType/Length
                       field and actually payload size.
  green-ethernet       Green Ethernet (Power reduction)
  help                 Description of the interactive help system
  ip                   Interface Internet Protocol configuration commands
  lacp                 Enable LACP on this interface
  lldp                 LLDP configurations.
  loop-protect         Loop protection configuration on port
  mac                  MAC keyword
  media-type           Media type.
  mtu                  Maximum transmission unit
  no                   Set to default value.
  port-security        Enable/disable port security per interface.
  priority-flowcontrol Priority Flow Control (802.1Qbb)
  pvlan                Private VLAN
  qos                  Quality of Service
  shutdown             Shutdown of the interface.
  spanning-tree        Spanning Tree protocol
  speed                Configures interface speed. If you use 10, 100, or
                       1000 keywords with the auto keyword the port will
                       only advertise the specified speeds.
  switchport           Set VLAN switching mode characteristics
  thermal-protect      Thermal group for the interface.
```

The second section is LLAG/VLAN interface, press **interface LLAG (LLAG-ID)/VLAN (VLAN-ID)** in global configuration mode. User can then enter the interface configuration mode. In this mode, User can configure the settings for the specific LLAG/VLAN. To leave this interface mode type **exit**. Press **?** to see the available command list.

The command lists of the LLAG/ VLAN interface configuration mode.

```
#LLAG
(config)# interface llag ?
      1-5       ID of LLAG interface
(config)# interface llag 1
(config-llag)# ?
      do          To run exec commands in the configuration mode
      end         Go back to EXEC mode
      exit        Exit from current mode
      help        Description of the interactive help system
      lacp
      no

#VLAN
(config)# interface vlan ?
      <vlan_list>       List of VLAN interface numbers
(config)# interface vlan 1
(config-if-vlan)# ?
      do          To run exec commands in the configuration mode
      end         Go back to EXEC mode
      exit        Exit from current mode
      help        Description of the interactive help system
      ip          IPv4 configuration
      no          Negate a command or set its defaults
```

The table below presents the summary of the 5 command modes:

COMMAND MODE	MAIN FUNCTION	PROMPT
Privileged EXEC	In this mode, the system allows User to view current configuration, reset default, reload switch, show system information, save configuration…and enter global configuration mode.	#
Global Configuration	In global configuration mode, User can configure all the features that the system provides User	(config)#
Port Interface Configuration	In this mode, User can configure port related settings.	(config-if)#
LLAG / VLAN Interface Configuration	In this mode, User can configure settings for specific LLAG/VLAN.	(config-if)#

Here are some useful commands for User to see these available commands. Save User time in typing and avoid typing error. Press **?** to see all the available commands in this mode. It helps User to see the next command User can/should type as well.

```
(config)# interface ?
      *                    All switches or All ports
      GigabitEthernet      1 Gigabit Ethernet Port
      llag                 Local link aggregation interface configuration
      vlan                 VLAN interface configurations
```

(Character)? To see all the available commands starts from this character.

```
(config)# a?
      aaa              Authentication, Authorization and Accounting
      access           Access management
      access-list      Access list
      aggregation      Aggregation mode
```

The tab key helps User to input the command quicker. If there is only one available command in the next, clicking on tab key can help to finish typing soon.

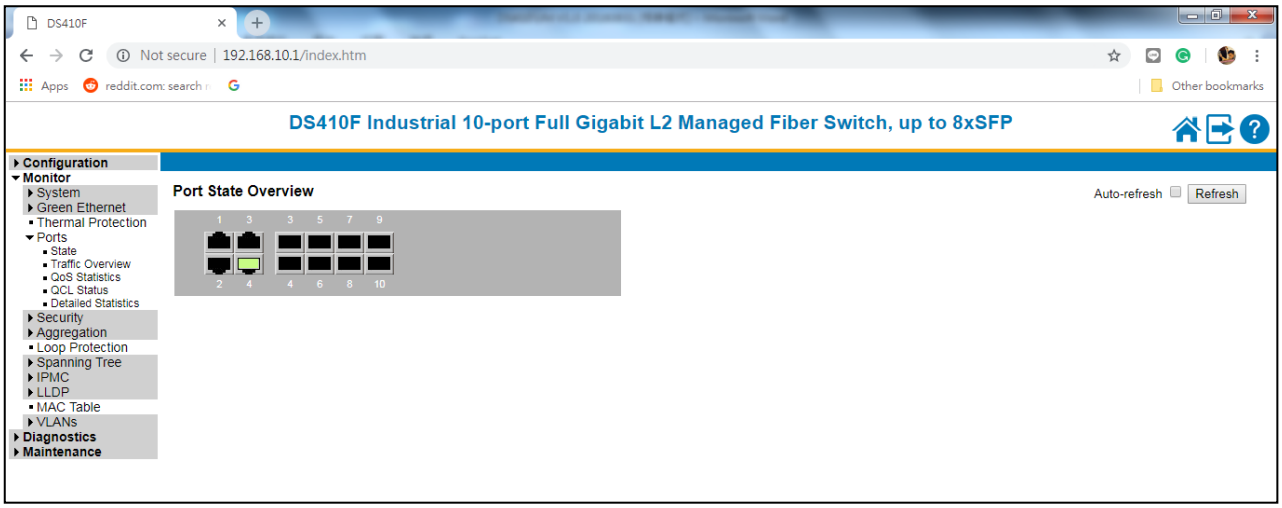
```
# co (tab)
configure copy
```

Ctrl+C To stop executing the unfinished command.

Ctrl+Q To show all of the command in the current mode.

Ctrl+Z To exit configuration mode.

Alert message when multiple users want to configure the switch. If the administrator is in configuration mode, then the Web users can't change the settings. This managed switch allows only one administrator to configure the switch at a time.



In this Web management for Featured Configuration, user will see all of WoMaster Switch's various configuration menus at the left side from the interface and a port state interface at the right side from the configuration page. Through this web management interface user can configure, monitoring, and set the administration functions. The whole information used web management interface to introduce the featured functions. User can use all of the standard web-browser to configure and access the switch on the network.

This web management has 4 big configuration functions:

- **Configuration**

This section will cover all of the configuration features for this switch.

- **Monitor**

This section will cover all of the monitoring sections include the traffic, QoS, Security, Aggregation, spanning tree, LLDP, VLAN and etc.

- **Diagnostics**

This section will cover the Ping, Traceroute and the VeriPHY features.

- **Maintenance**

This section will cover the firmware upgrade; restart the device, factory reset to defaults, upload and download the configuration file from the switch.

3.1 CONFIGURATION

When the user login to the switch, user will see the system section appear. This section provides all the basic setting and information or common setting from the switch that can be configured by the administrator.
Following topics is included:

3.1.1 System

3.1.2 Green Ethernet

3.1.3 Thermal Protection

3.1.4 Ports

3.1.5 Security

3.1.6 Aggregation

3.1.7 Loop Protection

3.1.8 Spanning Tree

3.1.9 IPMC

3.1.10 LLDP

3.1.11 MAC Table

3.1.12 VLANs

3.1.13 Private VLANs

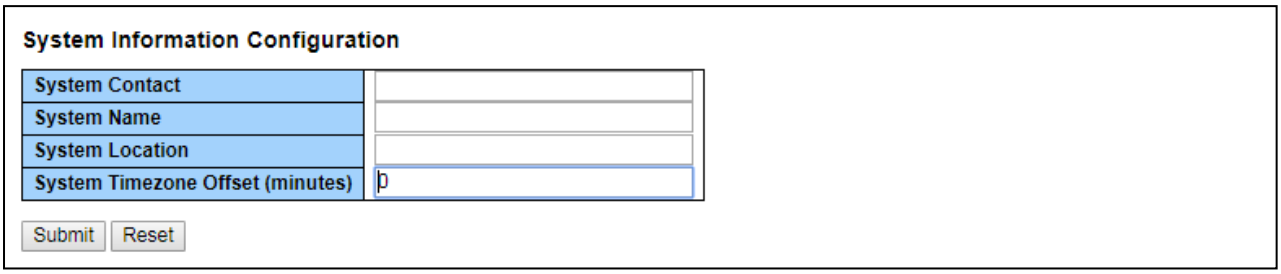
3.1.14 QoS

3.1.15 Mirroring

3.1.1 SYSTEM

Information section, this section shows the basic information from the switch to make it easier to identify different switches that are connected to User network. The figure below shows the interface of the Information section.

Information



The switch system information is provided here.

System Contact

The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

System Name

An admin assigned name for this managed node. By convention, this is the node's fully-qualified domain

name. A domain name is a text string drawn from the alphabet (A-Z a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.

System Location

The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Timezone Offset

Provide the timezone offset relative to UTC/GMT.

The offset is given in minutes east of GMT. The valid range is from **-1439** to **1439** minutes.

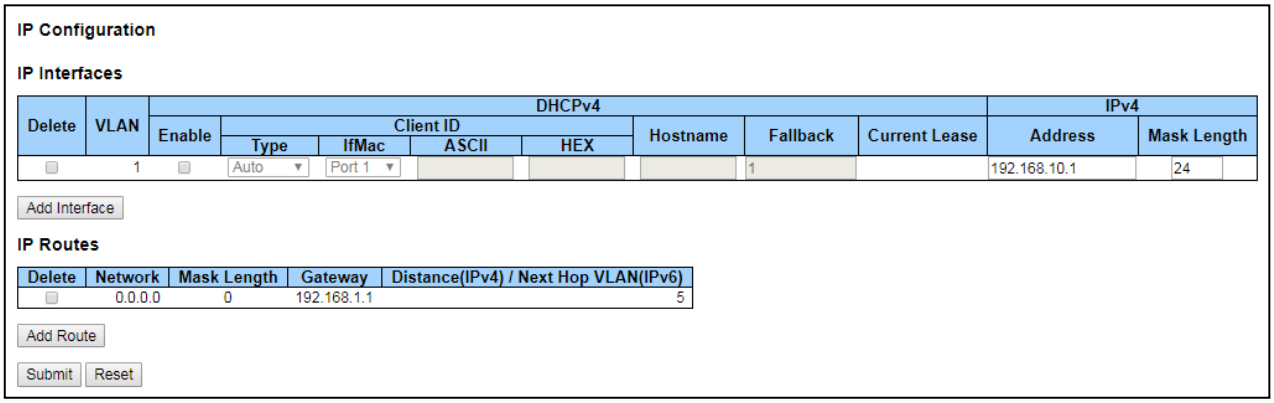
Buttons

Submit: Click to submit changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

IP Configuration

This IP Configuration page allows user to configure the device IP Address and in this page user able to set the IP Address according to the interface and VLAN. The second section is IP Routes, in this section user can configure the routing feature.



Configure IP basic settings, control IP interfaces and IP routes. The maximum number of interfaces supported is 8 and the maximum number of routes is 32.

IP Interfaces

Delete

Select this option to delete an existing IP interface.

VLAN

The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.

IPv4 DHCP Enabled

Enable the DHCPv4 client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol.

IPv4 DHCP Client Identifier Type

The type of DHCP client identifier. User can choose Auto, ifmac, ASCII, and HEX.

IPv4 DHCP Client Identifier IfMac

The interface name of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ifmac', the configured interface's hardware MAC address will be used in the DHCP option 61 field.

IPv4 DHCP Client Identifier ASCII

The ASCII string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ascii', the ASCII string will be used in the DHCP option 61 field.

IPv4 DHCP Client Identifier HEX

The hexadecimal string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type 'hex', the hexadecimal value will be used in the DHCP option 61 field.

IPv4 DHCP Hostname

The hostname of DHCP client. If DHCPv4 client is enabled, the configured hostname will be used in the DHCP option 12 field. When this value is empty string, the field uses the configured system name plus the latest three bytes of system MAC addresses as the hostname.

IPv4 DHCP Fallback Timeout

The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.

IPv4 DHCP Current Lease

For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.

IPv4 Address

The IPv4 address of the interface in dotted decimal notation. If **DHCP** is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

IPv4 Mask

The IPv4 network mask, in number of bits (*prefix length*). Valid values are between 0 and 30 bits for a IPv4 address. If **DHCP** is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

IP Routes

Delete

Select this option to delete an existing IP route.

Network

The destination IP network or host address of this route. Valid format is dotted decimal notation. A default route can use the value **0.0.0.0**.

Mask Length

The destination IP network or host mask, in number of bits (*prefix length*). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits. Only a default route will have a mask length of **0** (as it will match anything).

Gateway

The IP address of the IP gateway. Valid format is dotted decimal notation.

Distance (Only for IPv4)

The distance value of route entry is used to provide the priority information of the routing protocols to routers. When there are two or more different routing protocols are involved and have the same destination, the distance value can be used to select the best path.

Next Hop VLAN (Only for IPv6)

The VLAN ID (VID) of the specific IPv6 interface associated with the gateway.

The given VID ranges from 1 to 4095 and will be effective only when the corresponding IPv6 interface is valid.

If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway.

If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.

Buttons

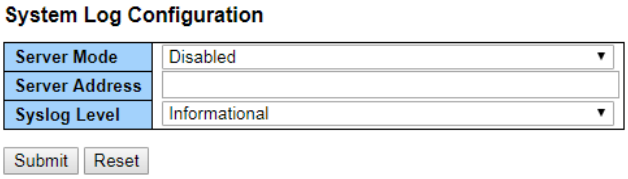
Add Interface: Click to add a new IP interface. A maximum of 8 interfaces is supported.

Add Route: Click to add a new IP route. A maximum of 32routes is supported.

Submit: Click to submit changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

LOG



System Log Configuration

Configure System Log on this page.

Server Mode

Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are:

Enabled: Enable server mode operation.

Disabled: Disable server mode operation.

Server Address

Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a domain name.

Syslog Level

Indicates what kind of message will send to syslog server. Possible modes are:

Error: Send the specific messages which severity code is less or equal than Error(3).

Warning: Send the specific messages which severity code is less or equal than Warning(4).

Notice: Send the specific messages which severity code is less or equal than Notice(5).

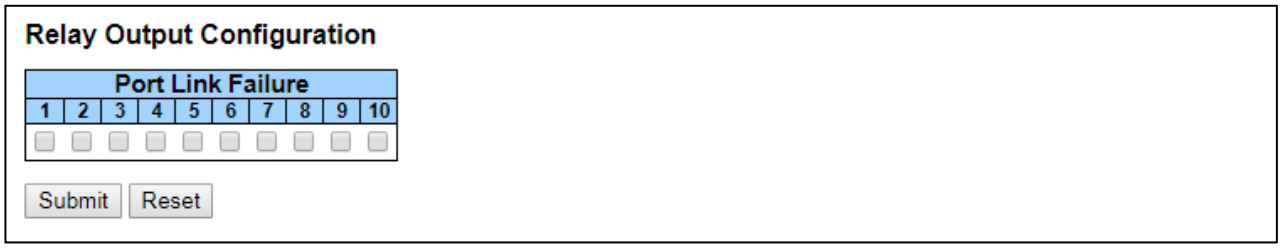
Informational: Send the specific messages which severity code is less or equal than Informational(6).

Buttons

Submit: Click to submit changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

RELAY OUTPUT



This page allows the user to inspect the current Relay Output configurations, and possibly change them as well. Relay Output Configuration:

Port Link Failure

A check box is provided for each port of a Port Link Failure.
When checked, port link failure will trigger relay status to "on".
When unchecked, port link failure will not trigger relay status to "on".
By default, port link failure is disabled on all ports.

Buttons

Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

3.1.2 GREEN ETHERNET

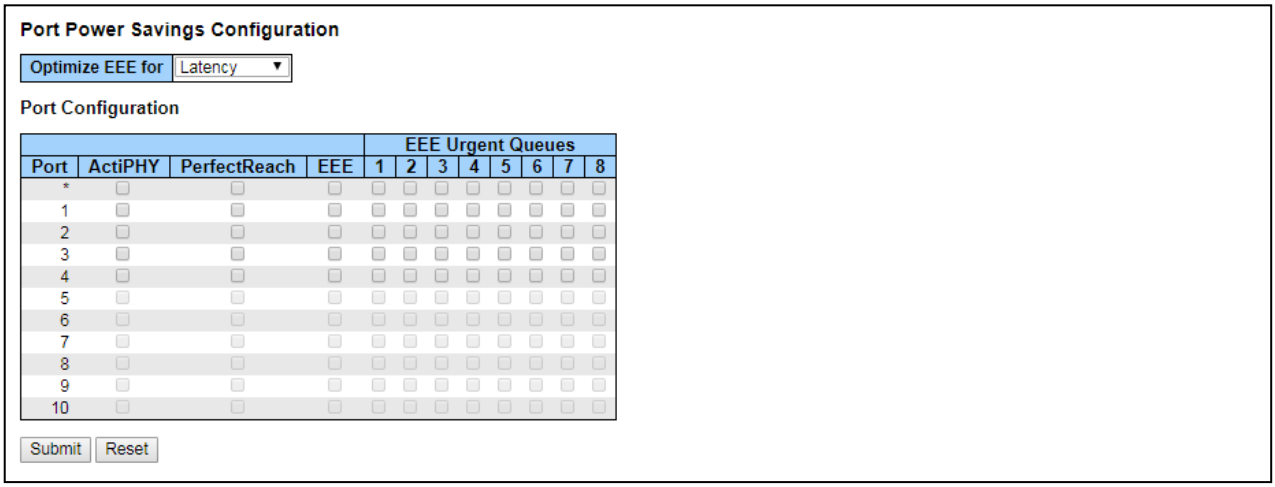
PORT POWER SAVINGS

What is EEE?

EEE is a power saving option that reduces the power usage when there is low or no traffic utilization.

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP protocol. EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode. For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for.

When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic.



Optimize EEE for

The switch can be set to optimize EEE for either best power saving or least traffic latency.

Port Configuration

Port

The switch port number of the logical port.

ActiPHY

Link down power savings enabled.

ActiPHY works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if cable is inserted.

PerfectReach

Cable length power savings enabled. Perfect Reach works by determining the cable length and lowering the power for ports with short cables.

EEE

Controls whether EEE is enabled for this switch port.

For maximizing power savings, the circuit isn't started at once transmit data is ready for a port, but is instead queued until a burst of data is ready to be transmitted. This will give some traffic latency.

If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

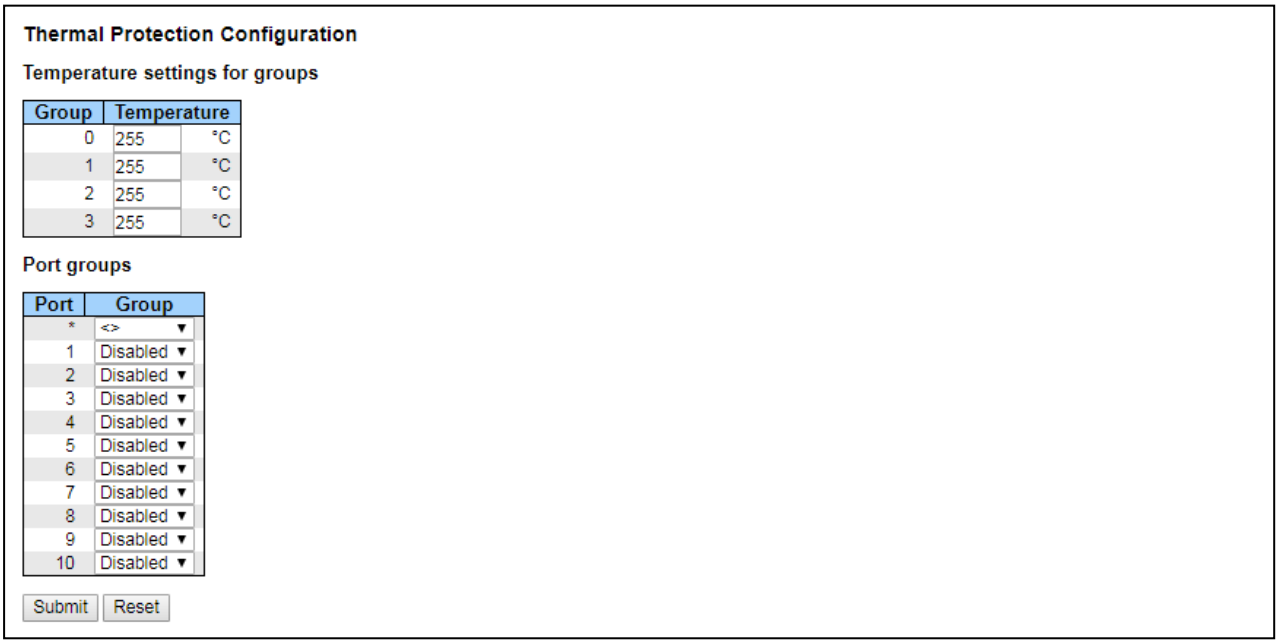
EEE Urgent Queues

Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

Buttons

Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

3.1.3 THERMAL PROTECTION



This page allows the user to inspect and configure the current setting for controlling thermal protection. Thermal protection is used to protect the chip from getting overheated.

When the temperature exceeds the configured thermal protection temperature, ports will be turned off in order to decrease the power consumption. It is possible to arrange the ports with different groups. Each group can be given a temperature at which the corresponding ports shall be turned off.

Temperature settings for groups

The temperature at which the ports with the corresponding group will be turned off. Temperatures between 0 and 255 C are supported.

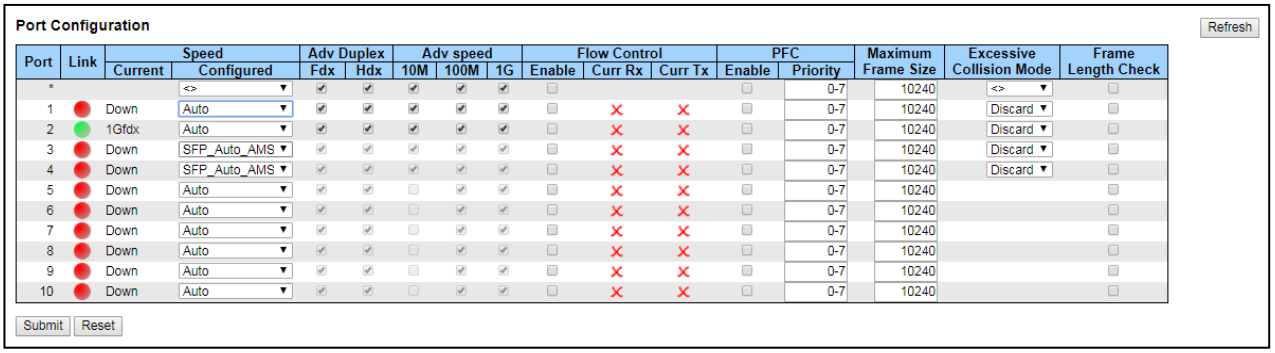
Port groups

The group the port belongs to. 4 groups are supported.

Buttons

Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

3.1.4 PORTS



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

Port

This is the logical port number for this row.

Link

The current link state is displayed graphically. Green indicates the link is up and red that it is down.

Current Link Speed

Provides the current link speed of the port.

Configured Link Speed

Selects any available link speed for the given switch port. Only speeds supported by the specific port are shown. Possible speeds are:
Disabled - Disables the switch port operation.
Auto - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.
10Mbps HDX - Forces the cu port in 10Mbps half-duplex mode.
10Mbps FDX - Forces the cu port in 10Mbps full duplex mode.
100Mbps HDX - Forces the cu port in 100Mbps half-duplex mode.
100Mbps FDX - Forces the cu port in 100Mbps full duplex mode.
1Gbps FDX - Forces the port in 1Gbps full duplex

SFP_Auto_AMS - Automatically determines the speed of the SFP. Note: There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFPs might not be detectable. The port is set in AMS mode. Cu port is set in **Auto** mode.
100-FX - SFP port in 100-FX speed. Cu port disabled.
1000-X - SFP port in 1000-X speed. Cu port disabled.
Ports in AMS mode with 1000-X speed has Cu port preferred.
Ports in AMS mode with 100-FX speed has Cu port preferred.

Advertise Duplex

When duplex is set as auto i.e auto negotiation, the port will only advertise the specified duplex as either **Fdx** or **Hdx**to the link partner. By default port will advertise all the supported duplexes if the Duplex is Auto.

Advertise Speed

When Speed is set as auto i.e auto negotiation, the port will only advertise the specified speeds (**10M** **100M** **1G2.5G** **5G** **10G**) to the link partner. By default port will advertise all the supported speeds if speed is set as Auto.

Flow Control

When **Auto Speed** is selected on a port, this section indicates the flow control capability that is advertised to the link partner.
When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto Negotiation.
Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
NOTICE: The 100FX standard doesn't support Auto Negotiation, so when in 100FX mode the flow control capabilities will always be shown as "disabled".

PFC

When PFC (802.1Qbb Priority Flow Control) is enabled on a port then flow control on a priority level is enabled. Through the **Priority** field, range (one or more) of priorities can be configured, e.g. '0-3,7' which equals '0,1,2,3,7'. PFC is not supported through auto negotiation. PFC and Flow control cannot both be enabled on the same port.

Maximum Frame Size

Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518-10240 bytes.

Excessive Collision Mode

Configure port transmit collision behavior.
Discard: Discard frame after 16 collisions (default).
Restart: Restart back off algorithm after 16 collisions.

Frame Length Check

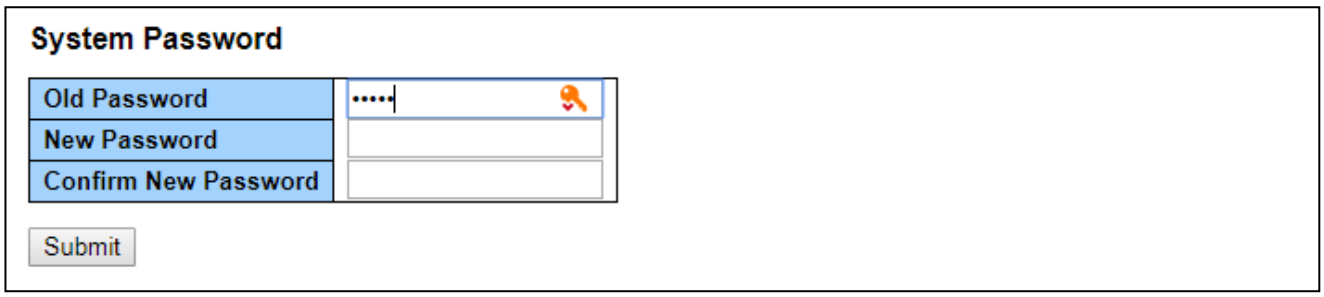
Configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actually payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch. Note: No drop counters count frames dropped due to frame length mismatch

Buttons

Submit: Click to submit 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.

3.1.5 SECURITY

Switch Password



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

Old Password

Enter the current system password. If this is incorrect, the new password will not be set.

New Password

The system password. The allowed string length is 0 to 31, and the allowed content is the ASCII characters from 32 to 126.

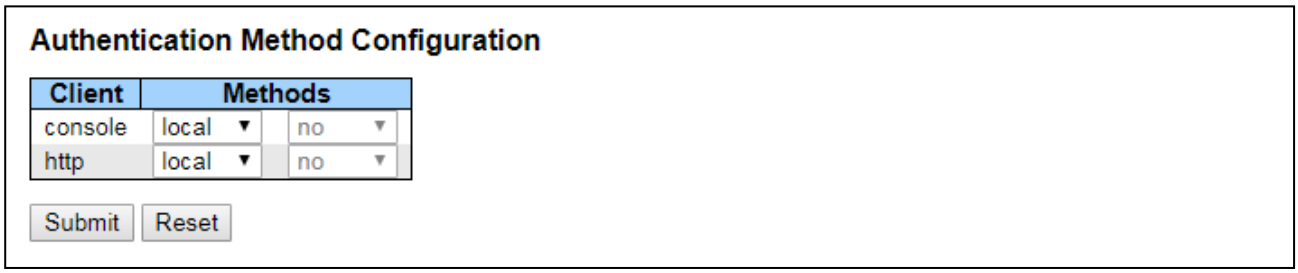
Confirm New Password

The new password must be entered twice to catch typing errors.

Buttons

Submit: Click to submit changes.

Authentication Method Configuration



The authentication section allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces. The table has one row for each client type and a number of columns, which are:

Client

The management client for which the configuration below applies.

Methods

Method can be set to one of the following values:

- no: Authentication is disabled and login is not possible.
- local: Use the local user database on the switch for authentication.
- radius: Use remote RADIUS server(s) for authentication.

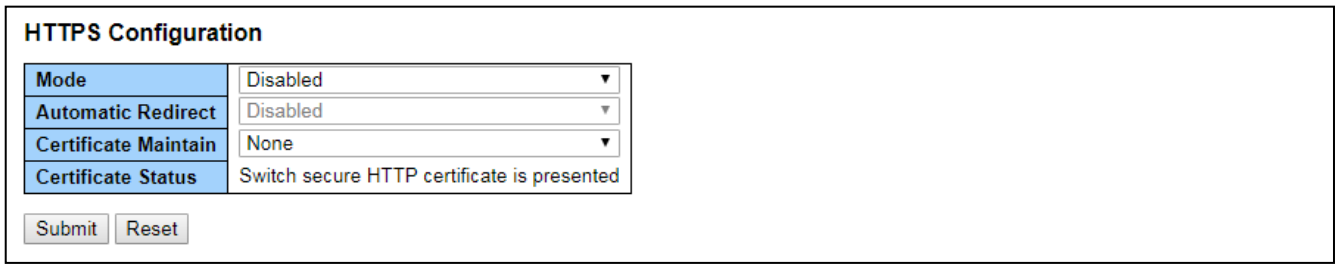
Methods that involves remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user

database if none of the configured authentication servers are alive.

Buttons

Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

HTTPS



This page allows you to configure the HTTPS settings and maintain the current certificate on the switch.

Mode

Indicate the HTTPS mode operation.
Possible modes are:
Enabled: Enable HTTPS mode operation.
Disabled: Disable HTTPS mode operation.

Automatic Redirect

Indicate the HTTPS redirect mode operation. It is only significant when "HTTPS Mode Enabled" is selected. When the redirect mode is enabled, the HTTP connection will be redirected to HTTPS connection automatically.
Notice that the browser may not allow the redirect operation due to the security consideration unless the switch certificate is trusted to the browser. You need to initialize the HTTPS connection manually for this case.
Possible modes are:
Enabled: Enable HTTPS redirect mode operation.
Disabled: Disable HTTPS redirect mode operation.

Certificate Maintain

The operation of certificate maintenance.
Possible operations are:
None: No operation.
Delete: Delete the current certificate.
Upload: Upload a certificate PEM file. Possible methods are: **Web Browser** or **URL**.
Generate: Generate a new self-signed RSA certificate.

Certificate Pass Phrase

Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.

Certificate Upload

Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem
Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g. Firefox v37 and Chrome v39.
Possible methods are:

Web Browser: Upload a certificate via Web browser.
URL: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is <protocol>://[<username>[:<password>]@]< host>[:<port>][/<path>]/<file_name>. For example, tftp://10.10.10.10/new_image_path/new_image.dat, http://username:password@10.10.10.10:80/new_image_path/new_image.dat. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score(_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.

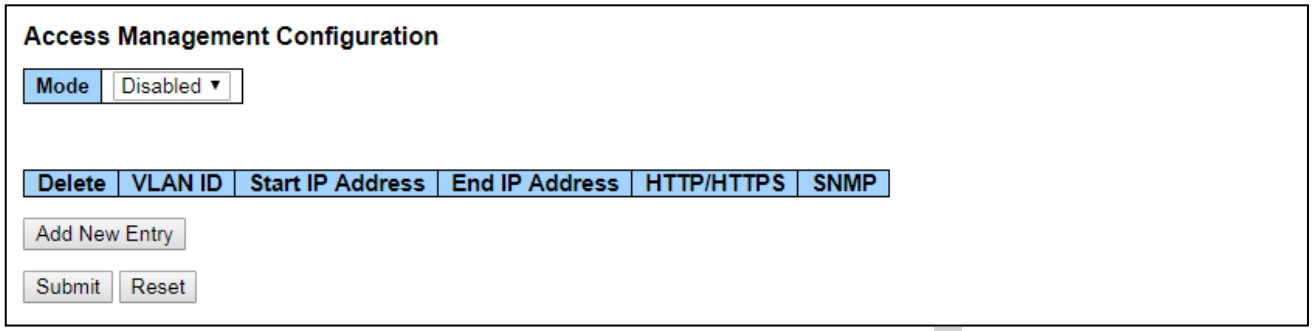
Certificate Status

Display the current status of certificate on the switch.
Possible statuses are:
Switch secure HTTP certificate is presented.
Switch secure HTTP certificate is not presented.
Switch secure HTTP certificate is generating ....

Buttons

Submit: Click to submit 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.

Access Management Configuration



Configure access management table on this page. The maximum number of entries is **16**. If the application's type match any one of the access management entries, it will allow access to the switch.

Mode

Indicates the access management mode operation. Possible modes are:
Enabled: Enable access management mode operation.
Disabled: Disable access management mode operation.

Delete

Check to delete the entry. It will be deleted during the next save.

VLAN ID

Indicates the VLAN ID for the access management entry.

Start IP address

Indicates the start IP unicast address for the access management entry.

End IP address

Indicates the end IP unicast address for the access management entry.

HTTP/HTTPS

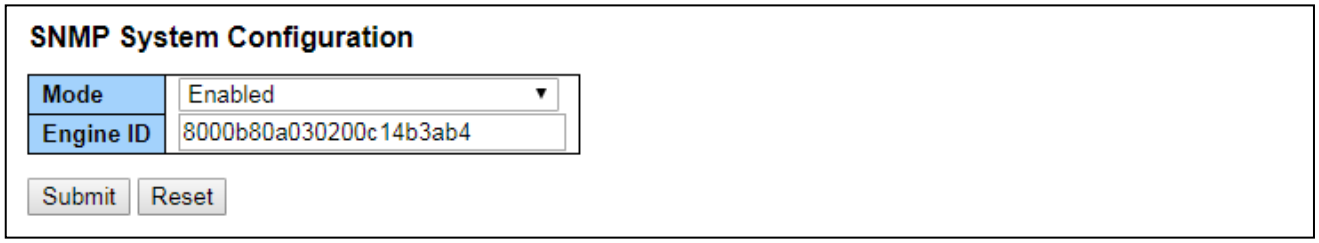
Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

SNMP

Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

Buttons

Add New Entry: Click to add a new access management entry.
Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.



SNMP System

Configure SNMP on this page.

Mode

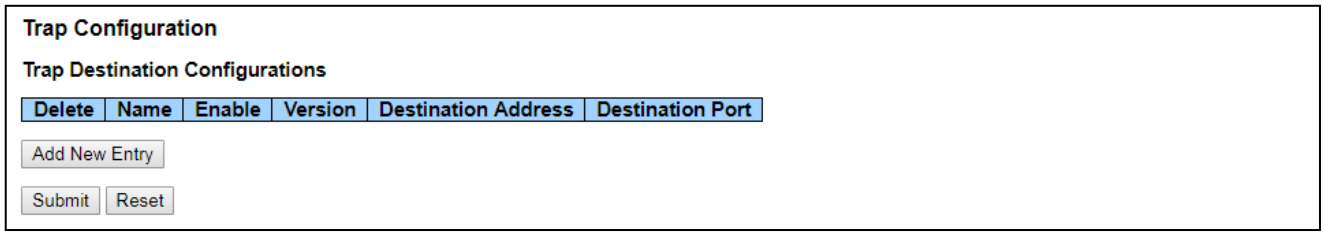
Indicates the SNMP mode operation. Possible modes are:
Enabled: Enable SNMP mode operation.
Disabled: Disable SNMP mode operation.

Engine ID

Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Only users on this Engine ID can access the device (local users), so changing the Engine ID will revoke access for all current local users.

Buttons

Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.



SNMP Trap

Configure SNMP trap on this page.

Trap Destination Configurations

Configure trap destinations on this page.

Name

Indicates the trap Configuration's name. Indicates the trap destination's name.

Enable

Indicates the trap destination mode operation. Possible modes are:
Enabled: Enable SNMP trap mode operation.
Disabled: Disable SNMP trap mode operation.

Version

Indicates the SNMP trap supported version. Possible versions are:
SNMPv1: Set SNMP trap supported version 1.
SNMPv2c: Set SNMP trap supported version 2c.
SNMPv3: Set SNMP trap supported version 3.

Destination Address

Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').

Destination port

Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

Buttons

Add New Entry: Click to add a new user.
Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

Trap Source Configurations

This page provides SNMP trap source configurations. A trap is sent for the given trap source if at least one filter with filter type included matches the filter, and no filters with filter type excluded matches.

Delete

Check to delete the entry. It will be deleted during the next save.

Name

Indicates the name for the entry.

Type

The filter type for the entry. Possible types are:
included: An optional flag to indicate a trap is sent for the given trap source is matched.
excluded: An optional flag to indicate a trap is not sent for the given trap source is matched.

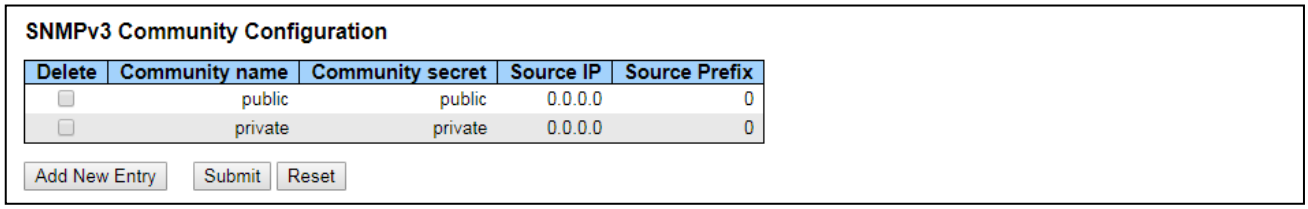
Subset OID

The subset OID for the entry. The value should depend on the what kind of trap name. For example, the ifIdex is the subset OID of linkUp and linkDown. A valid subset OID is one or more digital number(0-4294967295) or asterisk(*) which are separated by dots(.). The first character must not begin withasterisk(*) and the maximum of OID count must not exceed 128.

Buttons

Add New Entry: Click to add a new entry. The maximum entry count is **32**.
Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

Communities



SNMPv3 Community Configuration

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

Delete

Check to delete the entry. It will be deleted during the next save.

Community Name

Indicates the security name to map the community to the SNMP Groups configuration. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Community Secret

Indicates the community secret (access string) to permit access using SNMPv1 and SNMPv2c to the SNMP

agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Source IP

Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source prefix.

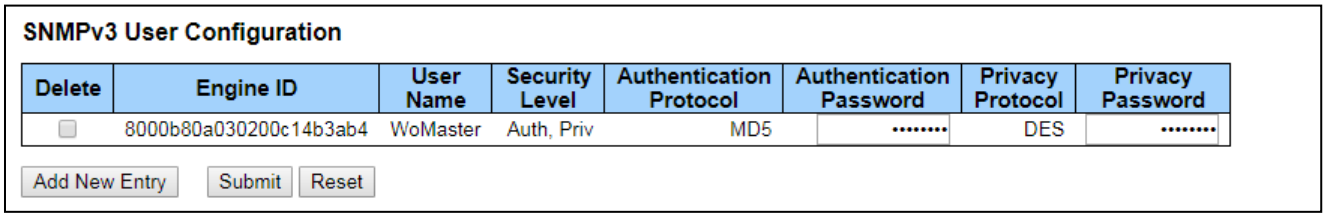
Source Prefix

Indicates the SNMP access source address prefix.

Buttons

Add New Entry: Click to add a new community entry.
Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

Users



SNMPv3 User Configuration

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

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(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.

User Name

A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Level

Indicates the security model that this entry should belong to. Possible security models are:
NoAuth, NoPriv: No authentication and no privacy.
Auth, NoPriv: Authentication and no privacy.
Auth, Priv: Authentication and privacy.
The value of security level cannot be modified if entry already exists. That means it must first be ensured

that the value is set correctly.

Authentication Protocol

Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:
None: No authentication protocol.
MD5: An optional flag to indicate that this user uses MD5 authentication protocol.
SHA: An optional flag to indicate that this user uses SHA authentication protocol.
The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.

Authentication Password

A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

Privacy Protocol

Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:
None: No privacy protocol.
DES: An optional flag to indicate that this user uses DES authentication protocol.
AES: An optional flag to indicate that this user uses AES authentication protocol.

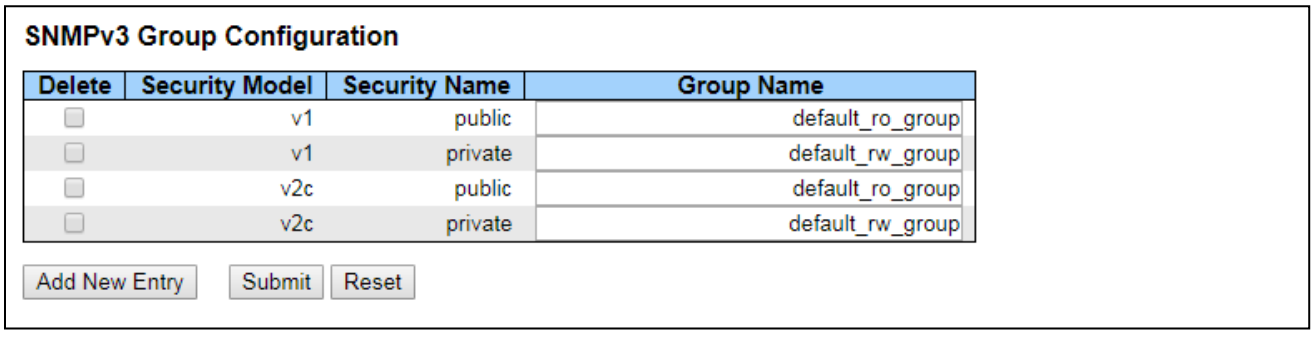
Privacy Password

A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

Add New Entry: Click to add a new user entry.
Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

GROUPS



SNMPv3 Group Configuration

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

Delete

Check to delete the entry. It will be deleted during the next save.

Security Model

Indicates the security model that this entry should belong to. Possible security models are:
v1: Reserved for SNMPv1.
v2c: Reserved for SNMPv2c.
usm: User-based Security Model (USM).

Security Name

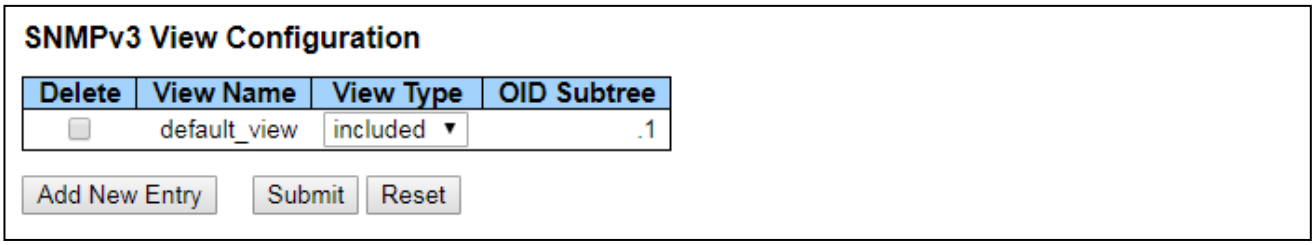
A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Group Name

A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

Add New Entry: Click to add a new group entry.
Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.



Views

SNMPv3 View Configuration

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

Delete

Check to delete the entry. It will be deleted during the next save.

View Name

A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

View Type

Indicates the view type that this entry should belong to. Possible view types are:
included: An optional flag to indicate that this view subtree should be included.
excluded: An optional flag to indicate that this view subtree should be excluded.
In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.

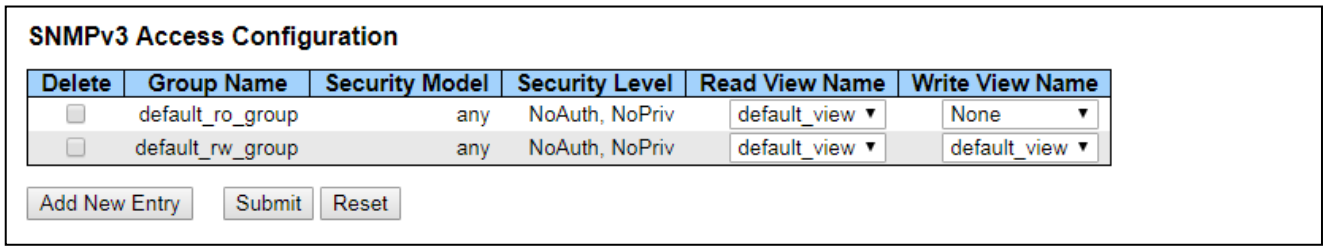
OID Subtree

The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Buttons

Add New Entry: Click to add a new view entry.
Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

Access



SNMPv3 Access Configuration

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

Delete

Check to delete the entry. It will be deleted during the next save.

Group Name

A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Model

Indicates the security model that this entry should belong to. Possible security models are:
any: Any security model accepted(v1|v2c|usm).
v1: Reserved for SNMPv1.
v2c: Reserved for SNMPv2c.
usm: User-based Security Model (USM).

Security Level

Indicates the security model that this entry should belong to. Possible security models are:
NoAuth, NoPriv: No authentication and no privacy.
Auth, NoPriv: Authentication and 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 the allowed content is ASCII characters from 33 to 126.

Write View Name

The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

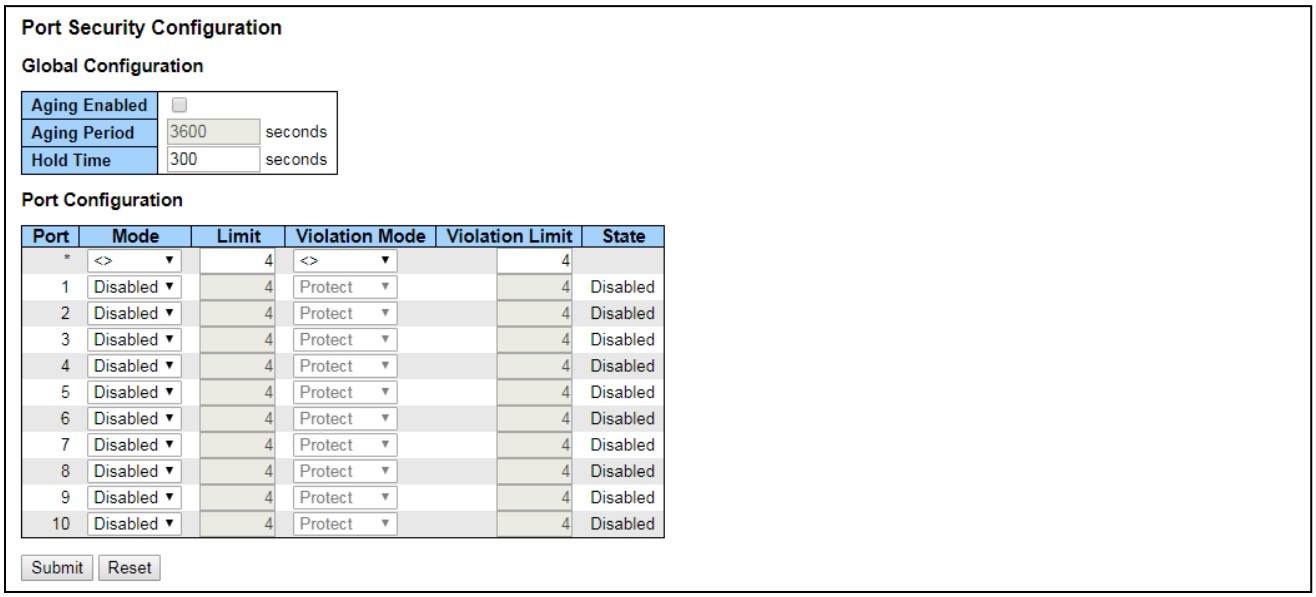
Buttons

Add New Entry: Click to add a new access entry.
Submit: Click to submit changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

NETWORKS

Port Security



This page allows you to configure the Port Security global and per-port settings. Port Security allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Port Security is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken depending on violation mode. The violation mode can be one of the four different described below.

The Port Security configuration consists of two sections, a global and a per-port.

Global Configuration

Aging Enabled

If checked, secured MAC addresses are subject to aging as discussed under Aging Period.

Aging Period

If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying functionality for securing MAC addresses, they may have other requirements to the aging period. The underlying functionality will use the shorter requested aging period of all modules that have aging enabled.
The Aging Period can be set to a number between 10 and 10000000 seconds with a default of 3600 seconds. To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Port Security is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Hold Time

The hold time - measured in seconds - is used to determine how long a MAC address is held in the MAC table if it has been found to violate the limit. Valid range is between 10 and 10000000 seconds with a default of 300 seconds. The reason for holding a violating MAC address in the MAC table is primarily to ensure that the same MAC address doesn't give rise to continuous notifications (if notifications on violation count is

enabled).

Port Configuration

The table has one row for each port on the switch and a number of columns, which are:

Port

The port number to which the configuration below applies.

Mode

Controls whether Port Security is enabled on this port. Notice that other modules may still use the underlying port security features without enabling Port Security on a given port.

Limit

The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1023. Default is 4. If the limit is exceeded, an action is taken corresponding to the violation mode.
The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

Violation Mode

If Limit is reached, the switch can take one of the following actions:
Protect: Do not allow more than Limit MAC addresses on the port, but take no further action.
Restrict: If Limit is reached, subsequent MAC addresses on the port will be counted and marked as violating. Such MAC addreses are removed from the MAC table when the hold time expires. At most Violation Limit MAC addresses can be marked as violating at any given time.
Shutdown: If Limit is reached, one additional MAC address will cause the port to be shut down. This implies that all secured MAC addresses be removed from the port, and no new addresses be learned. There are three ways to re-open the port:
1) In the "Configuration→Ports" page's "Configured" column, first disable the port, then restore the original mode.
2) Make a Port Security configuration change on the port.
3) Boot the switch.

Violation Limit

The maximum number of MAC addresses that can be marked as violating on this port. This number cannot exceed 1023. Default is 4. It is only used when Violation Mode is **Restrict**.

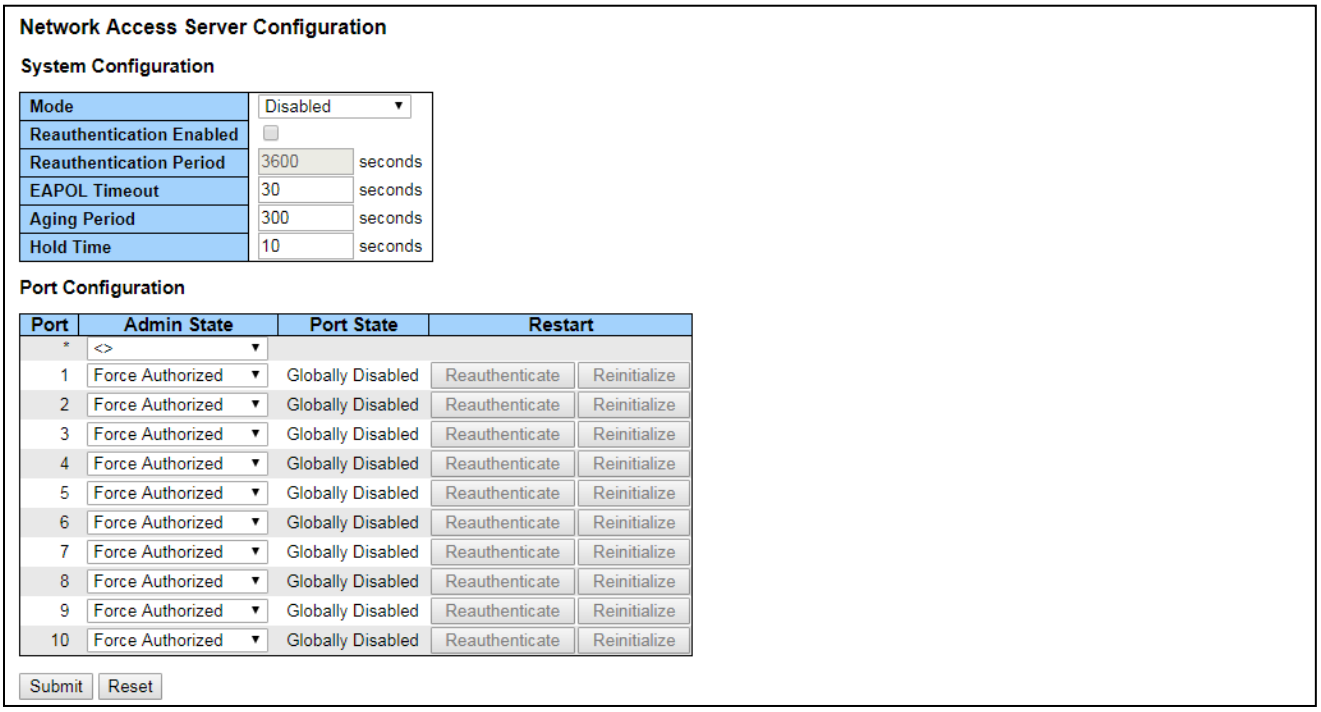
State

This column shows the current Port Security state of the port. The state takes one of four values:
Disabled: Port Security is disabled on the port.
Ready: The limit is not yet reached. This can be shown for all violation modes.
Limit Reached: Indicates that the limit is reached on this port. This can be shown for all violation modes.
Shutdown: Indicates that the port is shut down by Port Security. This state can only be shown if violation mode is set to **Shutdown**.

Buttons

Refresh: Click to refresh the page. Note that non-committed changes will be lost.
Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

NAS



This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings. The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Configuration→Security→AAA" page.

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

System Configuration

Mode

Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.

Reauthentication Enabled

If checked, successfully authenticated supplicants/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 or if a supplicant is no longer attached.
For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).

Reauthentication Period

Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.

EAPOL Timeout

Determines the time for retransmission of Request Identity EAPOL frames.
Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.

Aging Period

This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:
• MAC-Based Auth.
When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.
For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

Hold Time

This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:
• MAC-Based Auth.
If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.
The switch will ignore new frames coming from the client during the hold time.
The Hold Time can be set to a number between 10 and 1000000 seconds.

Port Configuration

The table has one row for each port on the switch and a number of columns, which are:

Port

The port number for which the configuration below applies.

Admin State

If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:

Force Authorized

In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

Force Unauthorized

In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

802.1X

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

encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.
When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

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

MAC-based Auth.

Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.
When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.
The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

Port State

The current state of the port. It can undertake one of the following values:
Globally Disabled: NAS is globally disabled.
Link Down: NAS is globally enabled, but there is no link on the port.
Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.
Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.
X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

Restart

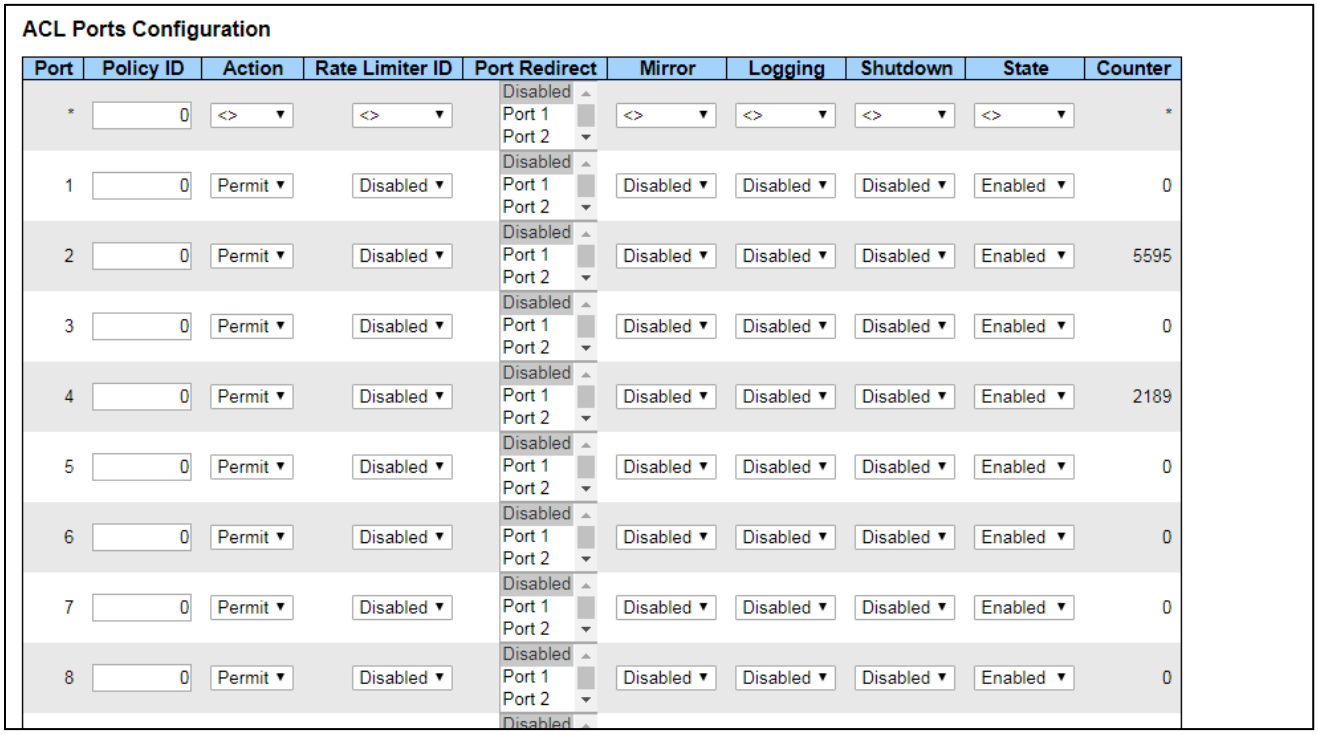
Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-basedmode.
Clicking these buttons will not cause settings changed on the page to take effect.
Reauthenticate: Schedules a reauthentication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

Buttons

Refresh: Click to refresh the page.
Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

ACL

Ports



ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled / Port 1 / Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	5595
3	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	2189
5	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0

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

Port

The logical port for the settings contained in the same row.

Policy ID

Select the policy to apply to this port. The allowed values are **0** through **63**. The default value is 0.

Action

Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".

Rate Limiter ID

Select which rate limiter to apply on this port. The allowed values are **Disabled** or the values **1** through **16**. The default value is "Disabled".

Port Redirect

Select which port frames are redirected on. The allowed values are **Disabled** or a specific port number and it can't be set when action is permitted. The default value is "Disabled".

Mirror

Specify the mirror operation of this port. The allowed values are:
Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored.
The default value is "Disabled".

Logging

Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC.
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". Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.

Shutdown

Specify the port shut down operation of this port. The allowed values are:
Enabled: If a frame is received on the port, the port will be disabled.
Disabled: Port shut down is disabled.
The default value is "Disabled".
Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).

State

Specify the port state of this port. The allowed values are:
Enabled: To reopen ports by changing the volatile port configuration of the ACL user module.
Disabled: To close ports by changing the volatile port configuration of the ACL user module.
The default value is "Enabled".

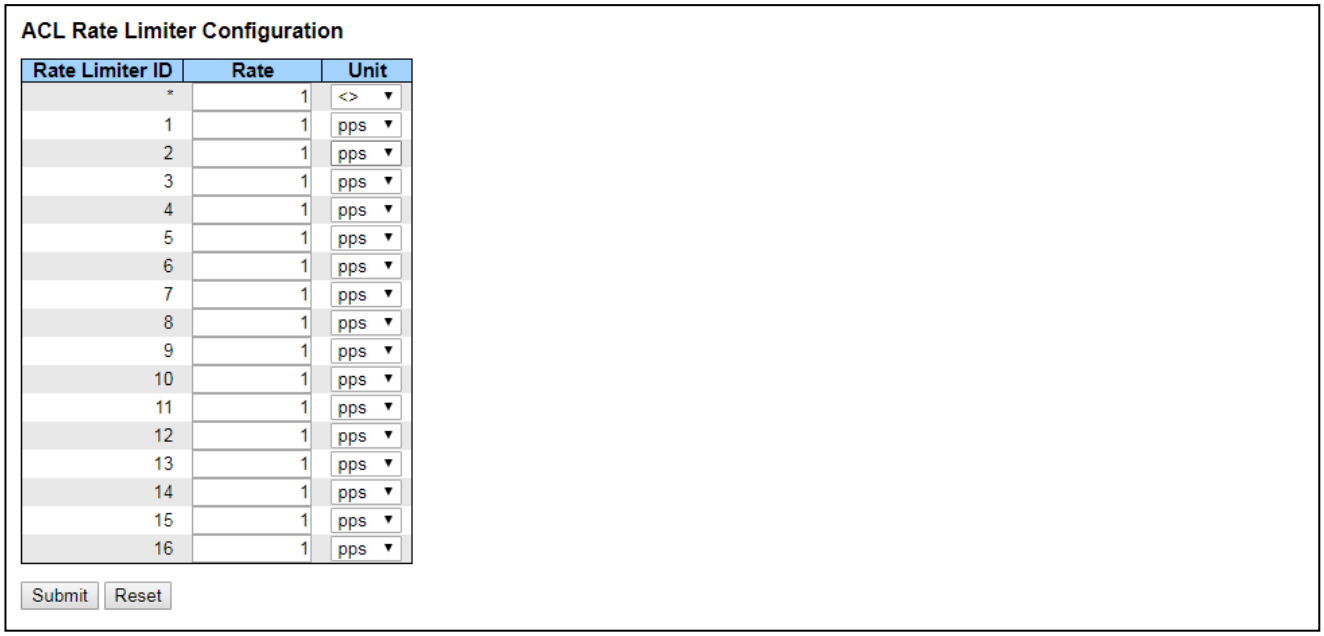
Counter

Counts the number of frames that match this ACE.

Buttons

Submit: Click to submit 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.
Clear: Click to clear the counters.

Rate Limiter



Configure the rate limiter for the ACL of the switch.

Rate Limiter ID

The rate limiter ID for the settings contained in the same row and its range is **1** to **16**.

Rate

The valid rate is **0 - 99, 100, 200, 300, ...,1092000** in pps
or **0, 100, 200, 300, ..., 1000000** in kbps.

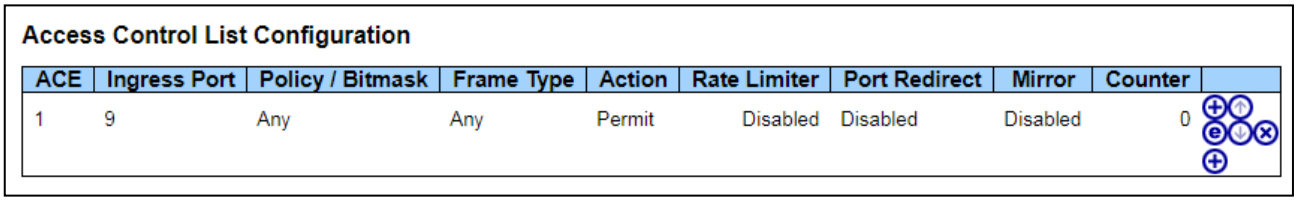
Unit

Specify the rate unit. The allowed values are:
pps: packets per second.
kbps: Kbits per second.

Buttons

Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

Access Control List



This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is **128** on each switch.

Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.

ACE

Indicates the ACE ID.

Ingress Port

Indicates the ingress port of the ACE. Possible values are:
All: The ACE will match all ingress port.
Port: The ACE will match a specific ingress port.

Policy / Bitmask

Indicates the policy number and bitmask of the ACE.

Frame Type

Indicates the frame type of the ACE. Possible values are:
Any: The ACE will match any frame type.
EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.
ARP: The ACE will match ARP/RARP frames.
IPv4: The ACE will match all IPv4 frames.
IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.
IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.
IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.
IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
IPv6: The ACE will match all IPv6 standard frames.

Action

Indicates the forwarding action of the ACE.
Permit: Frames matching the ACE may be forwarded and learned.
Deny: Frames matching the ACE are dropped.
Filter: Frames matching the ACE are filtered.

Rate Limiter

Indicates the rate limiter number of the ACE. The allowed range is **1** to **16**. When **Disabled** is displayed, the rate limiter operation is disabled.

Port Redirect

Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are **Disabled** or a specific port number. When **Disabled** is displayed, the port redirect operation is disabled.

Mirror

Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:
Enabled: Frames received on the port are mirrored.
Disabled: Frames received on the port are not mirrored.
The default value is "Disabled".

Counter

The counter indicates the number of times the ACE was hit by a frame.

Modification Buttons

You can modify each ACE (Access Control Entry) in the table using the following buttons:

: Inserts a new ACE before the current row.

: Edits the ACE row.

: Moves the ACE up the list.

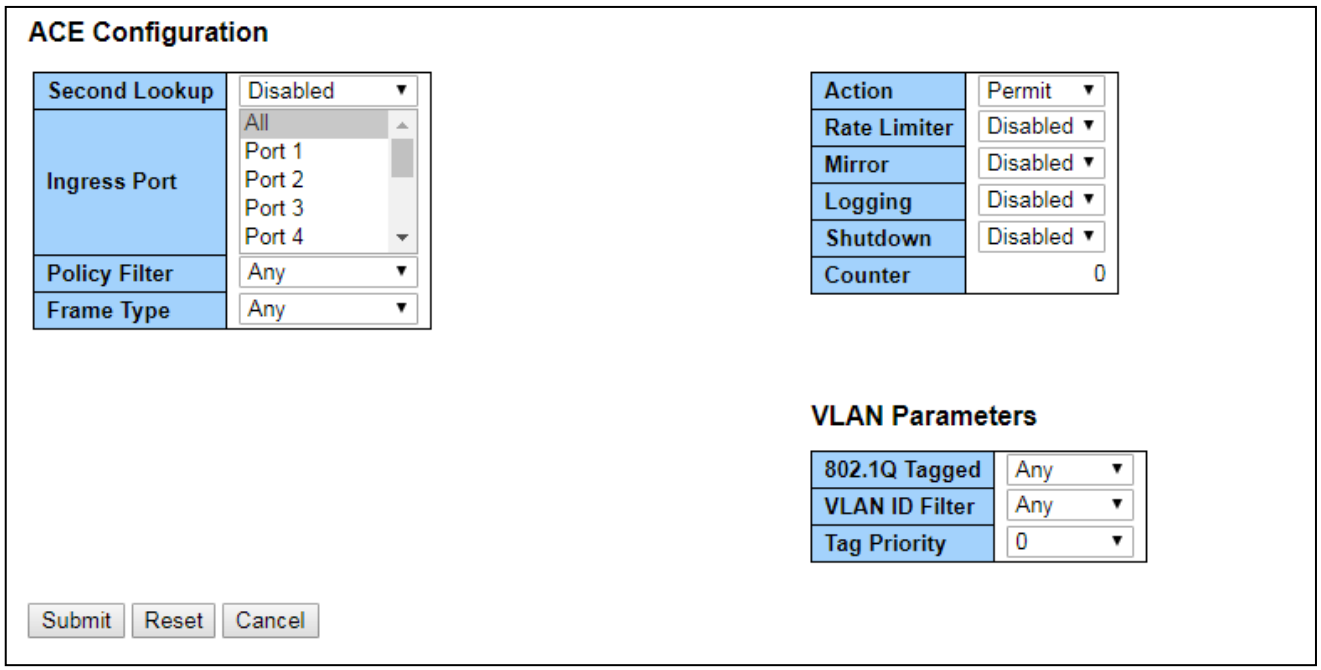
: Moves the ACE down the list.

: Deletes the ACE.

: The lowest plus sign adds a new entry at the bottom of the ACE listings.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page; any changes made locally will be undone.
Clear: Click to clear the counters.
Remove All: Click to remove all ACEs.



Configure an ACE (Access Control Entry) on this page. An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected. A frame that hits this ACE matches the configuration that is defined here.

Ingress Port

Select the ingress port for which this ACE applies.
All: The ACE applies to all port.
Port *n*: The ACE applies to this port number, where *n* is the number of the switch port.

Policy Filter

Specify the policy number filter for this ACE.
Any: No policy filter is specified. (policy filter status is "don't-care".)
Specific: If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears.

Policy Value

When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is **0** to **63**.

Policy Bitmask

When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is **0x0** to **0x3f**. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [policy_value & policy_bitmask]. For example, if the policy value is 3 and the policy bitmask is 0x10(bit 0 is "don't-care" bit), then policy 2 and 3 are applied to this rule.

Frame Type

Select the frame type for this ACE. These frame types are mutually exclusive.
Any: Any frame can match this ACE.
Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal) and the value should not be equal to 0x800(IPv4), 0x806(ARP) or 0x86DD(IPv6).
ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.
IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.
IPv6: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.

Action

Specify the action to take with a frame that hits this ACE.
Permit: The frame that hits this ACE is granted permission for the ACE operation.
Deny: The frame that hits this ACE is dropped.
Filter: Frames matching the ACE are filtered.

Rate Limiter

Specify the rate limiter in number of base units. The allowed range is **1** to **16**. **Disabled** indicates that the rate limiter operation is disabled.

Port Redirect

Frames that hit the ACE are redirected to the port number specified here. The rate limiter will affect these ports. The allowed range is the same as the switch port number range. **Disabled** indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted.

Mirror

Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port. The allowed values are:
Enabled: Frames received on the port are mirrored.
Disabled: Frames received on the port are not mirrored.
The default value is "Disabled".

Logging

Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information. The allowed values are:
Enabled: Frames matching the ACE are stored in the System Log.
Disabled: Frames matching the ACE are not logged.
Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.

Shutdown

Specify the port shut down operation of the ACE. The allowed values are:
Enabled: If a frame matches the ACE, the ingress port will be disabled.

Disabled: Port shut down is disabled for the ACE.
Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).

Counter

The counter indicates the number of times the ACE was hit by a frame.

MAC Parameters

SMAC Filter

(Only displayed when the frame type is Ethernet Type or ARP.)
Specify the source MAC filter for this ACE.
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 this ACE, choose this value. A field for entering an SMAC value appears.

SMAC Value

When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.

DMAC Filter

Specify the destination MAC filter for this ACE.
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.
Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.

DMAC Value

When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.

VLAN Parameters

802.1Q Tagged

Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are:
Any: Any value is allowed ("don't-care").
Enabled: Tagged frame only.
Disabled: Untagged frame only.
The default value is "Any".

VLAN ID Filter

Specify the VLAN ID filter for this ACE.
Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)
Specific: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.

VLAN ID

When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is **1** to **4095**. A frame that hits this ACE matches this VLAN ID value.

Tag Priority

Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is **0** to **7** or range **0-1**, **2-3**, **4-5**, **6-7**, **0-3** and **4-7**. The value **Any** means that no tag priority is specified (tag priority is "don't-care".)

ARP Parameters

The ARP parameters can be configured when Frame Type "ARP" is selected.

ARP/RARP

Specify the available ARP/RARP opcode (OP) flag for this ACE.
Any: No ARP/RARP OP flag is specified. (OP is "don't-care".)
ARP: Frame must have ARP opcode set to ARP.
RARP: Frame must have RARP opcode set to RARP.
Other: Frame has unknown ARP/RARP Opcode flag.

Request/Reply

Specify the available Request/Reply opcode (OP) flag for this ACE.
Any: No Request/Reply OP flag is specified. (OP is "don't-care".)
Request: Frame must have ARP Request or RARP Request OP flag set.
Reply: Frame must have ARP Reply or RARP Reply OP flag.

Sender IP Filter

Specify the sender IP filter for this ACE.
Any: No sender IP filter is specified. (Sender IP filter is "don't-care".)
Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.
Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.

Sender IP Address

When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

Sender IP Mask

When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.

Target IP Filter

Specify the target IP filter for this specific ACE.
Any: No target IP filter is specified. (Target IP filter is "don't-care".)
Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears.**Network**: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.

Target IP Address

When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

Target IP Mask

When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.

ARP Sender MAC Match

Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.
0: ARP frames where SHA is not equal to the SMAC address.
1: ARP frames where SHA is equal to the SMAC address.
Any: Any value is allowed ("don't-care").

RARP Target MAC Match

Specify whether frames can hit the action according to their target hardware address field (THA) settings.
0: RARP frames where THA is not equal to the target MAC address.
1: RARP frames where THA is equal to the target MAC address.
Any: Any value is allowed ("don't-care").

IP/Ethernet Length

Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.
0: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).
1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).
Any: Any value is allowed ("don't-care").

IP

Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.
0: ARP/RARP frames where the HLD is not equal to Ethernet (1).
1: ARP/RARP frames where the HLD is equal to Ethernet (1).
Any: Any value is allowed ("don't-care").

Ethernet

Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.
0: ARP/RARP frames where the PRO is not equal to IP (0x800).
1: ARP/RARP frames where the PRO is equal to IP (0x800).
Any: Any value is allowed ("don't-care").

IP Parameters

The IP parameters can be configured when Frame Type "IPv4" is selected.

IP Protocol Filter

Specify the IP protocol filter for this ACE.
Any: No IP protocol filter is specified ("don't-care").
Specific: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.
ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.
UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.
TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.

IP Protocol Value

When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is **0** to **255**. A frame that hits this ACE matches this IP protocol value.

IP TTL

Specify the Time-to-Live settings for this ACE.
zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.
non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.
Any: Any value is allowed ("don't-care").

IP Fragment

Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.
No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.
Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.
Any: Any value is allowed ("don't-care").

IP Option

Specify the options flag setting for this ACE.
No: IPv4 frames where the options flag is set must not be able to match this entry.
Yes: IPv4 frames where the options flag is set must be able to match this entry.
Any: Any value is allowed ("don't-care").

SIP Filter

Specify the source IP filter for this ACE.
Any: No source IP filter is specified. (Source IP filter is "don't-care".)
Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.
Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

SIP Address

When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

SIP Mask

When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.

DIP Filter

Specify the destination IP filter for this ACE.
Any: No destination IP filter is specified. (Destination IP filter is "don't-care".)
Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.
Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.

DIP Address

When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

DIP Mask

When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

IPv6 Parameters

The IPv6 parameters can be configured when Frame Type "IPv6" is selected.

Next Header Filter

Specify the IPv6 next header filter for this ACE.
Any: No IPv6 next header filter is specified ("don't-care").
Specific: If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears.
ICMP: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.
UDP: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.
TCP: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.

Next Header Value

When "Specific" is selected for the IPv6 next header value, you can enter a specific value. The allowed range is **0** to **255**. A frame that hits this ACE matches this IPv6 protocol value.

SIP Filter

Specify the source IPv6 filter for this ACE.
Any: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".)
Specific: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.

SIP Address

When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address.

SIP BitMask

When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFE(bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.

Hop Limit

Specify the hop limit settings for this ACE.
zero: IPv6 frames with a hop limit field greater than zero must not be able to match this entry.
non-zero: IPv6 frames with a hop limit field greater than zero must be able to match this entry.
Any: Any value is allowed ("don't-care").

ICMP Parameters

ICMP Type Filter

Specify the ICMP filter for this 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 this 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 that hits this ACE matches this ICMP value.

ICMP Code Filter

Specify the ICMP code filter for this 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 this 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 that hits this ACE matches this ICMP code value.

TCP/UDP Parameters

TCP/UDP Source Filter

Specify the TCP/UDP source filter for this 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 this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.
Range: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.

TCP/UDP Source No.

When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Source Range

When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Destination Filter

Specify the TCP/UDP destination filter for this ACE.
Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").
Specific: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.
Range: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.

TCP/UDP Destination Number

When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP destination value.

TCP/UDP Destination Range

When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP destination value.

TCP FIN

Specify the TCP "No more data from sender" (FIN) value for this ACE.
0: TCP frames where the FIN field is set must not be able to match this entry.
1: TCP frames where the FIN field is set must be able to match this entry.
Any: Any value is allowed ("don't-care").

TCP SYN

Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.
0: TCP frames where the SYN field is set must not be able to match this entry.
1: TCP frames where the SYN field is set must be able to match this entry.
Any: Any value is allowed ("don't-care").

TCP RST

Specify the TCP "Reset the connection" (RST) value for this ACE.
0: TCP frames where the RST field is set must not be able to match this entry.
1: TCP frames where the RST field is set must be able to match this entry.
Any: Any value is allowed ("don't-care").

TCP PSH

Specify the TCP "Push Function" (PSH) value for this ACE.
0: TCP frames where the PSH field is set must not be able to match this entry.
1: TCP frames where the PSH field is set must be able to match this entry.
Any: Any value is allowed ("don't-care").

TCP ACK

Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.
0: TCP frames where the ACK field is set must not be able to match this entry.
1: TCP frames where the ACK field is set must be able to match this entry.
Any: Any value is allowed ("don't-care").

TCP URG

Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.
0: TCP frames where the URG field is set must not be able to match this entry.
1: TCP frames where the URG field is set must be able to match this entry.
Any: Any value is allowed ("don't-care").

Ethernet Type Parameters

The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

EtherType Filter

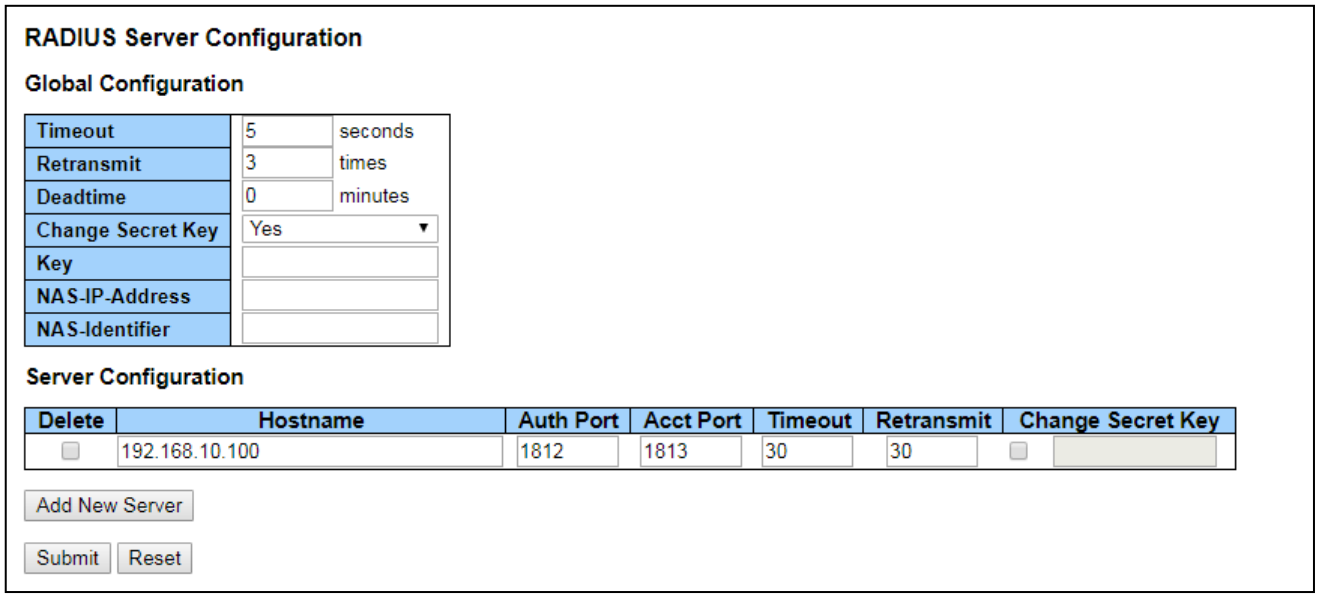
Specify the Ethernet type filter for this ACE.
Any: No EtherType filter is specified (EtherType filter status is "don't-care").
Specific: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.

Ethernet Type Value

When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is **0x600** to **0xFFFF** but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

Buttons

Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
Cancel: Return to the previous page.



AAA

This page allows you to configure up to 5 RADIUS servers.

Global Configuration

These setting are common for all of the RADIUS servers.

Timeout

Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.

Retransmit

Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.

Deadtime

Deadtime, which can be set to a number between 0 to 1440minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.
Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

Change Secret Key

Specify to change the secret key or not. When "Yes" is selected for the option, you can change the secret key - up to 63 characters long - shared between the RADIUS server and the switch.

NAS-IP-Address (Attribute 4)

The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-Identifier (Attribute 32)

The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this

field is left blank, the NAS-Identifier is not included in the packet.

Server Configuration

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

Delete

To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.

Hostname

The IPv4/IPv6 address of the RADIUS server.

Auth Port

The UDP port to use on the RADIUS server for authentication. Set to 0 to disable authentication.

Acct Port

The UDP port to use on the RADIUS server for accounting. Set to 0 to disable accounting.

Timeout

This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Retransmit

This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

Change Secret Key

Specify to change the secret key or not. When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key.

Adding a New Server

Click to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported.
The button can be used to undo the addition of the new server.

Buttons

Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

3.1.6 AGGREGATION

This document provides examples on how to configure Link Aggregation Control Protocol (LACP)/AGGR using the Command Line Interface (CLI). The commands apply to an enhanced version of the LACP. The examples used in this document pertain to WoMaster switches.

LACP ENHANCEMENT FEATURES

The following sections describe various LACP enhancement features.

Aggregation Groups

To create an aggregation a group type must be chosen on the interfaces that are participating in the group. This can be LACP active, LACP passive, or statically created aggregation “On”. No looping occurs even though the parallel links have links and have not formed an aggregation. Spanning tree is not needed for this but can be enabled to avoid loops between groups. LACP active initiates the LACP frames to partner. LACP passive does not initiate the LACP frames to partner, but answers if requested. “On” is a statically created aggregation without LACP.

Bundle Max

If there any exist suitable link partner, each LACP group automatically forms an aggregation for all of its members. The number of members can be restricted by setting the max bundle value to a number less than the number of group members. When the numbers of members who have formed aggregation reach the specified value, the remaining ports are set to standby and do not forward any frames. If an active member goes down, then a standby member will take over. The priority assignment controls to which member goes active/standby.

Revertive/Non-Revertive

The LACP group can be configured to be revertive (default) or non-revertive. When a higher priority port is in active/standby configuration comes back up, it becomes active again and the current active port (if it has lower priority) becomes standby, unless the group is configured to be non-revertive. In non-revertive mode, if a port comes back up, nothing changes and the traffic is not disturbed.

Note: Each time a link changes, the traffic is halted until the new aggregation (key) is fully set up.

1:1 Active (Standby) LACP

To achieve 1:1 active/standby configuration, create a group with two ports and configure one of the ports as bundle max. One of the ports, with higher priority, actively forwards traffic while the other remains in standby mode. The port, in standby mode, does not forward any frames other than BPDUs. The LACP state of the standby port is in no sync state. If the active port goes down, the standby port takes over. When the failed port becomes operational, it takes over the frame forwarding (unless configured not to - non-revertive) operation.

LACP State Information

The states of the LACP protocol (partner and actor) are visible through show lacp neighbor detail and show lacp internal detail commands.

CLI

The CLI syntax (for configuration and status) follows the Cisco IOS port-channel style. Port-channel is called aggregation in WoMaster terms.

ICLI Commands

The following sections describe the implementation of the preciously discussed LACP features through ICLI commands.

Creating an Aggregation Group

The following snippet shows how to create an active LACP group with ports Gig 1/1-2 as members.

```
# conf t
(config)# interface GigabitEthernet 1/1-2
(config-if)# aggregation group 1 mode ?
      active          Active LACP
      on              Static aggregation
      passive         Passive LACP
      <cr>
(config-if)# aggregation group 1 mode active
```

Active can be replaced with passive and on.

Showing the Status of an Aggregation Group

The following snippet shows the status of the active LACP group, created in the previous chapter.

```
# show  aggregation
Aggr ID     Name     Type            Speed        Configured      Aggregated
-------     ----       -----------     --------       ----------      ----------
                                LACP_ACTIV
1           LLAG1    E               Undefined    Gi 1/1-2        none
```

Show the internal configuration and status.

```
# show  lacp   internal
Port            State        Key     Priority
----------      --------   ----      --------
Gi 1/1          Down         1       32768
Gi 1/2          Down         1       32768
```

Where,
Port—is the local port.
State—indicates if a partner is seen and an aggregation created.
Key—is used as a term in the 802.1D standard. Here it equals the group id.
Priority—is used for active/standby purpose.

Showing the Detailed Status of an Aggregation Group

The following snippet shows the detailed status of the aggregation group.

```
# show lacp neighbor details
Port                    : The local port
State                   : The active/inactive state of this port
Aggr ID                 : The group id of this aggregation
Partner   Key           : The aggr key of the partner
Partner   Port          : The port of the partner
Partner   Port Prio : The       partner port priority
[Activ     Timeou    Aggrege    Synchro    Collect    Distrib    Defau    Expired]:
Booleans. The LACP protocol state seen from the link partner.

# show lacp internal details
Port          : The   local port
State         : The   active/inactive state of this port
Key           : The   key of this port, same as group id.
Priority : The        LACP priority of this port
               Timeo
[Activ         u            Aggrege   Synchro    Collect    Distrib    Defau    Expired]:
Booleans. The LACP protocol state seen from the actor (the local unit).
```

Statistics

The following snippet shows the statistics of the aggregation group.

```
# show lacp   statistics
Port            Rx Frames      Tx Frames      Rx Unknown    Rx Illegal
----------      ----------     ----------     ----------    ----------
Gi    1/1       2572           14067          0             0
Gi    1/2       2572           14068          0             0
```

System ID

The following snippet shows the system ID. The system ID is the combination of the priority and the MAC address.

```
(config)# lacp system-priority ?
      <1-65535>       Priority value, lower means higher priority
# show lacp system-id
System ID: 32768 - 00:01:c1:00:f6:90
```

Port LACP Commands

The following snippet shows how to configure LACP for each port.

```
# conf t
(config)# interface GigabitEthernet 1/1-2
(config-if)# lacp ?
port-priority       timeout             <cr>
```

Where,
port-priority—the LACP priority for the port.
Timeout—fast or slow protocol timeout.

Group LACP Commands

The following snippet shows how to perform an additional configuration of LACP based groups.

```
# conf t
(config)# interface llag 1
(config-llag)# lacp ?
failover
max-bundle
```

failover—revertive (default) /non-revertive
max-bundle—max size of the aggregation (1-max). All the default ports in the group can aggregate.

Forwarding Mode of the Aggregation

The forwarding distribution of the traffic can be affected by changing the aggregation mode. This is a global parameter and affects all aggregations. These mode parameters can be combined.
Note: Any change in the aggregation mode stops all forwarding until the key is fully setup.

```
config)# aggregation mode ?
        dmac            Destination MAC affects the distribution
        ip              IP address affects the distribution
        port            IP port affects the distribution
        smac            Source MAC affects the distribution
(config)# aggregation mode ?
aggregation mode { [ smac ] [ dmac ] [ ip ] [ port ] }
(config)# aggregation mode smac dmac
(config)# end
#
```

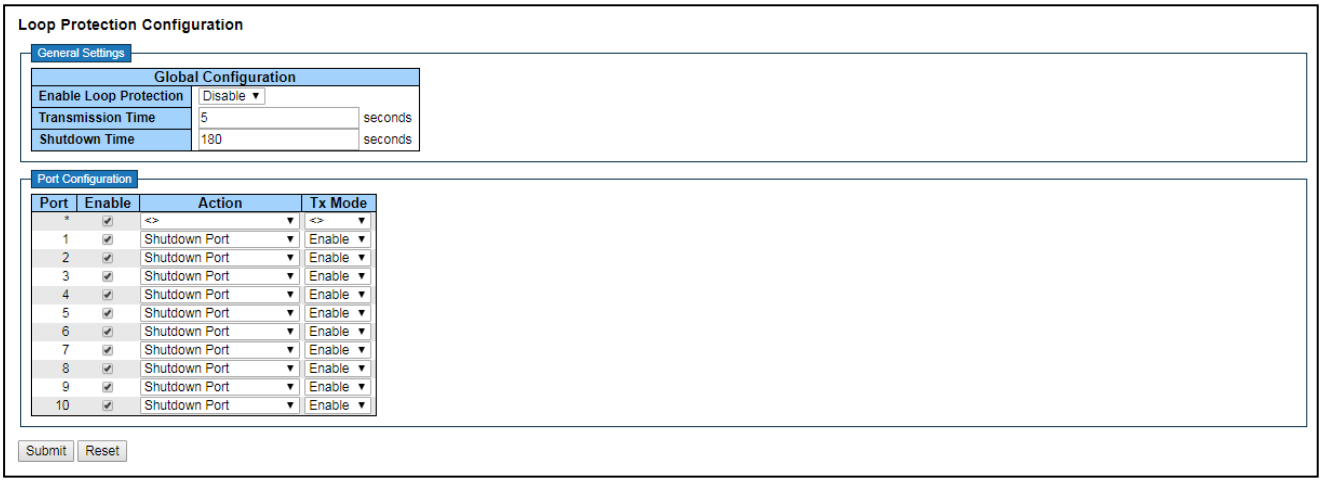
Delete an Aggregation Group

The following snippet shows how to delete an aggregation group.

```
# conf t
(config)# no interface llag 1
(config)#
```

3.1.7 LOOP PROTECTION

Since firmware of WoMaster switch supports loop elimination function that is based on per port or system configure. It prevents any communicate looping caused by RSTP and Ring when ring topology changes. The following figure shows the Loop Protection page.



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

General Settings

Enable Loop Protection

Controls whether loop protections is enabled (as a whole).

Transmission Time

The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds. Default value is 5 seconds.

Shutdown Time

The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart). Default value is 180 seconds.

Port Configuration

Port

The switch port number of the port.

Enable

Controls whether loop protection is enabled on this switch port.

Action

Configures the action performed when a loop is detected on a port. Valid values are **Shutdown Port**, **Shutdown Port and Log** or **Log Only**.

Tx Mode

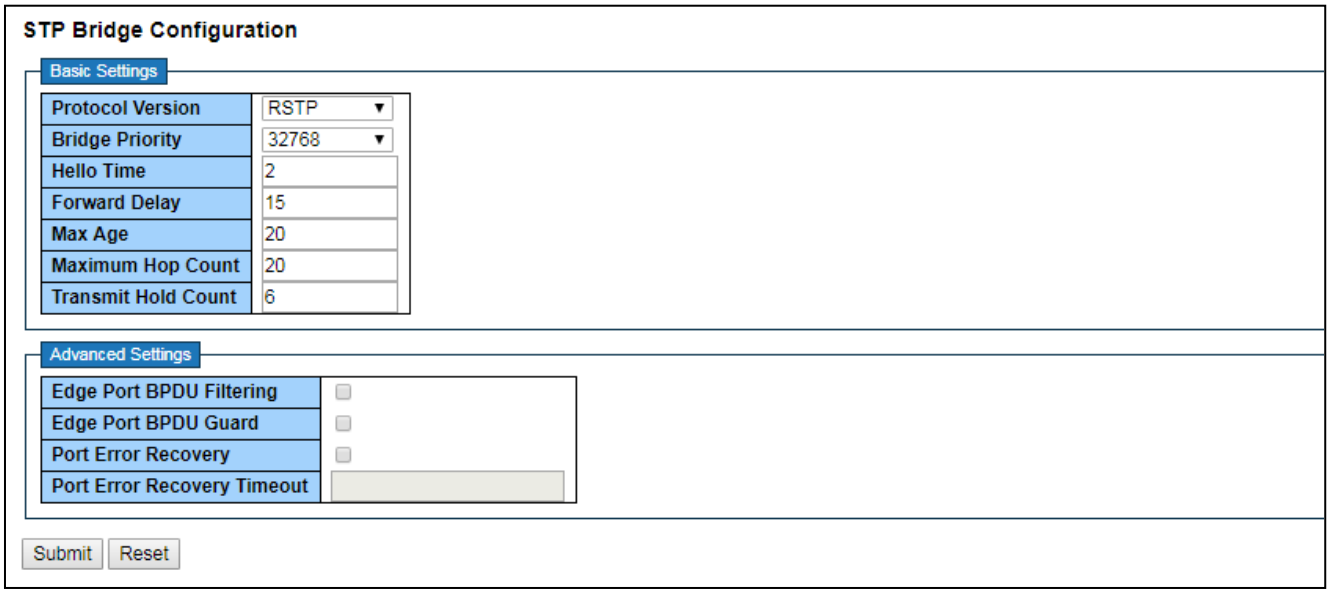
Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Buttons

Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

3.1.8 SPANNING TREE

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



Basic Settings

Protocol Version

The RSTP / STP protocol version setting. Valid values are **RSTP** and **STP**.

Bridge Priority

Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a *Bridge Identifier*.

Hello Time

The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds, default is 2 seconds.

Note: Changing this parameter from the default value is not recommended, and may have adverse effects on your network.

Forward Delay

The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age

The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, *and* MaxAge must be <= (FwdDelay-1)*2.

Maximum Hop Count

This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count

The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings

Edge Port BPDU Filtering

Control whether a port *explicitly* configured as **Edge**will transmit and receive BPDUs.

Edge Port BPDU Guard

Control whether a port *explicitly* configured as **Edge**will disable itself upon reception of a BPDU. The port will enter the *error-disabled* state, and will be removed from the active topology.

Port Error Recovery

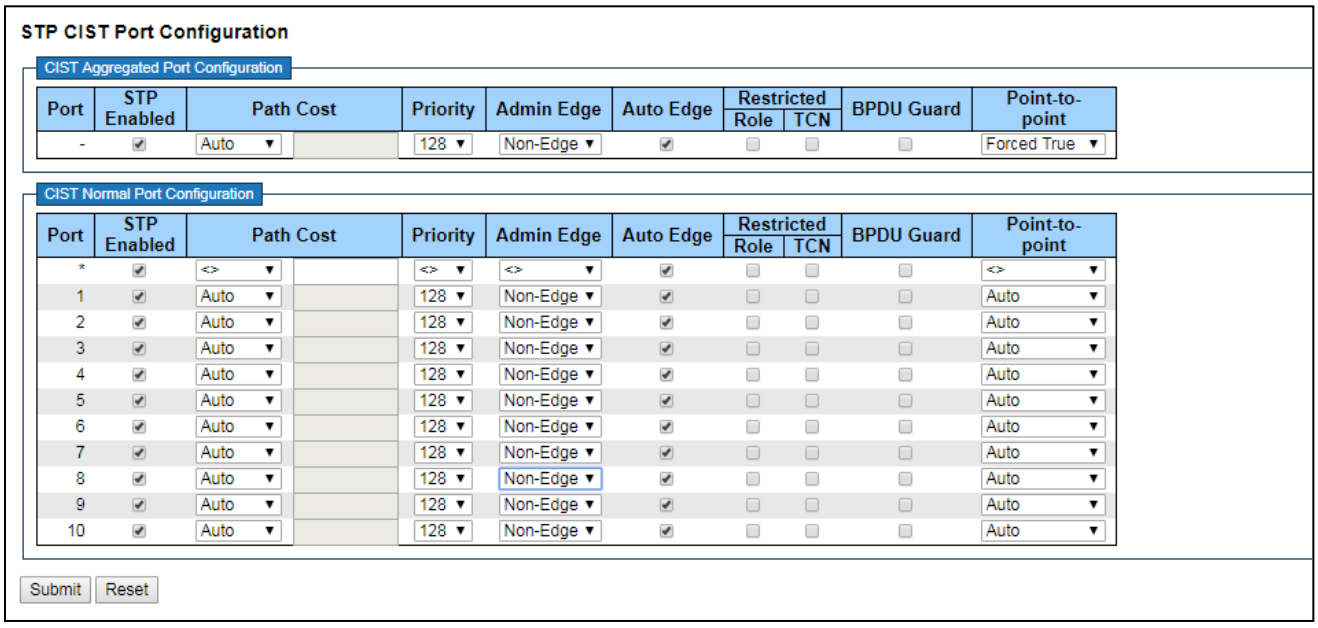
Control whether a port in the *error-disabled* state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

Port Error Recovery Timeout

The time to pass before a port in the *error-disabled* state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Buttons

Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.



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

This page contains settings for physical and aggregated ports.

Port

The switch port number of the logical STP port.

STP Enabled

Controls whether STP is enabled on this switch port.

Path Cost

Controls the path cost incurred by the port. The **Auto**setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority

Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

Lower priority is better.

operEdge (state flag)

Operational flag describing whether the port is connecting directly to edge devices. (*No* Bridges attached). Transition to the forwarding state is faster for edge ports (having *operEdgetrue*) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.

AdminEdge

Controls whether the *operEdge* flag should start as set or cleared. (The initial *operEdge* state when a port is initialized).

AutoEdge

Controls whether the bridge should enable automatic edge detection on the bridge port. This allows *operEdge* to be derived from whether BPDU's are received on the port or not.

Restricted Role

If enabled, causes the port not to be selected as Root Port for the CIST, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as **Root Guard**.

Restricted TCN

If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard

If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port **Edge** status does not effect this setting.

A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Point-to-Point

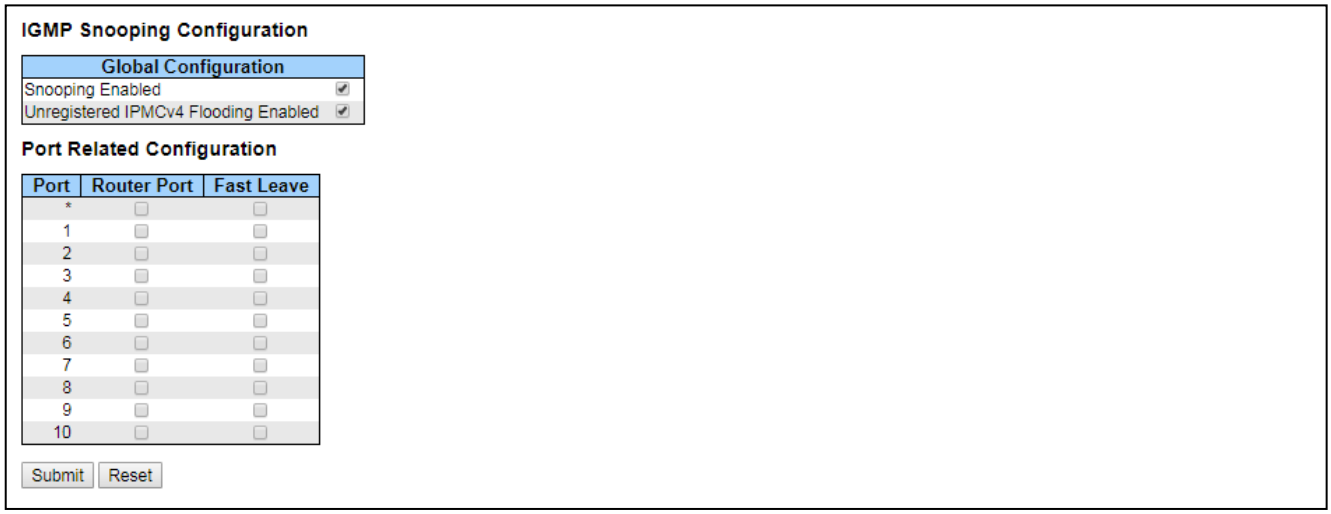
Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

3.1.9 IPMC

Basic Configuration



This page provides IGMP Snooping related configuration.

Snooping Enabled

Enable the Global IGMP Snooping.

Unregistered IPMCv4 Flooding Enabled

Enable unregistered IPMCv4 traffic flooding.
The flooding control takes effect only when IGMP Snooping is enabled.
When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.

Router Port

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.
If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Enable the fast leave on the port. System will remove group record and stop forwarding data upon receiving the IGMPv2 leave message without sending last member query messages.
It is recommended to enable this feature only when a single IGMPv2 host is connected to the specific port.

Buttons

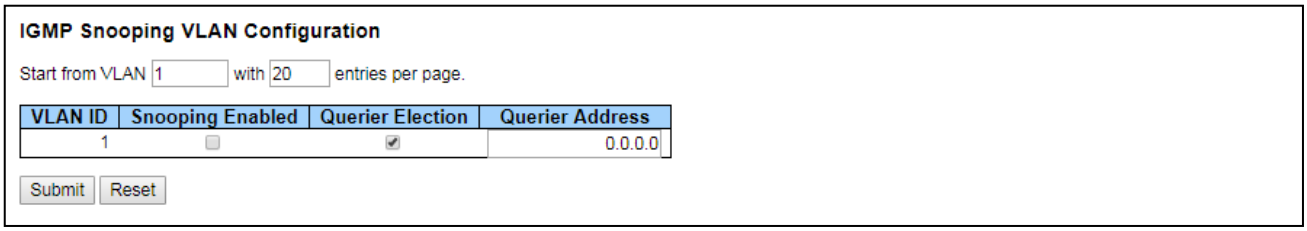
Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

VLAN Configuration

Navigating the IGMP Snooping VLANTable

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.
The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the next closest VLAN Table match.
The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the **|<<** button to start over.

IGMP Snooping VLAN Table Columns



For IGMP VLAN interface creation, you need to enter IP configuration page to setup IP interface first. **System** -> **IP** -> **Add IP interface**.

VLAN ID

The VLAN ID of the entry.

IGMP Snooping Enabled

Enable the per-VLAN IGMP Snooping. Up to **8** VLANs can be selected for IGMP Snooping.

Querier Election

Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Querier Address

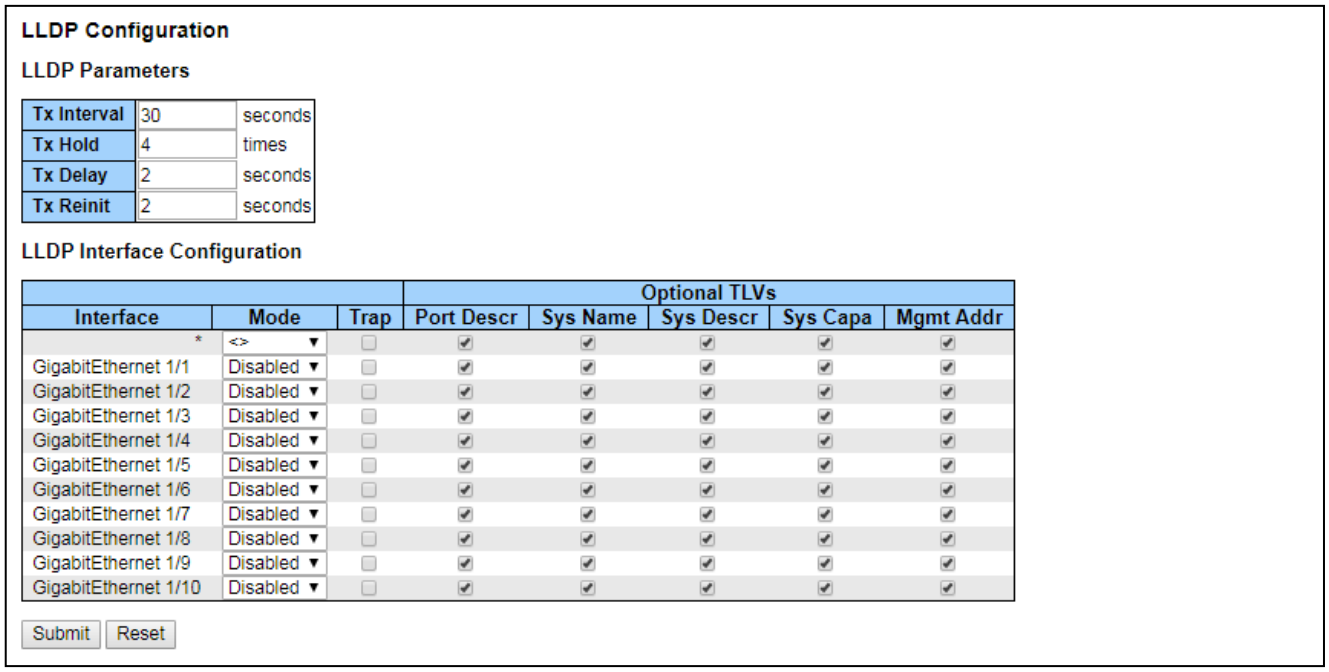
Define the IPv4 address as source address used in IP header for IGMP Querier election.
When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.
When the IPv4 management address is not set, system uses the first available IPv4 management address.
Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.
|<<: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
>>: Updates the table, starting with the entry after the last entry currently displayed.
Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

3.1.10 LLDP

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



LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

LLDP Interface Configuration

			Optional TLVs				
Interface	Mode	Trap	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>		☑	☑	☑	☑	☑
GigabitEthernet 1/1	Disabled		☑	☑	☑	☑	☑
GigabitEthernet 1/2	Disabled		☑	☑	☑	☑	☑
GigabitEthernet 1/3	Disabled		☑	☑	☑	☑	☑
GigabitEthernet 1/4	Disabled		☑	☑	☑	☑	☑
GigabitEthernet 1/5	Disabled		☑	☑	☑	☑	☑
GigabitEthernet 1/6	Disabled		☑	☑	☑	☑	☑
GigabitEthernet 1/7	Disabled		☑	☑	☑	☑	☑
GigabitEthernet 1/8	Disabled		☑	☑	☑	☑	☑
GigabitEthernet 1/9	Disabled		☑	☑	☑	☑	☑
GigabitEthernet 1/10	Disabled		☑	☑	☑	☑	☑

Submit Reset

LLDP Parameters

Tx Interval

The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds.

Tx Hold

Each LLDP frame contains information about how long time the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to **Tx Hold** multiplied by **Tx Interval** seconds. Valid values are restricted to 2 - 10 times.

Tx Delay

If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value. Valid values are restricted to 1 - 8192 seconds.

Tx Reinit

When a interface is disabled, LLDP is disabled or the switch is rebooted, a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. **Tx Reinit** controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Interface Configuration

Interface

The switch interface name of the logical LLDP interface.

Mode

Select LLDP mode.
Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.
Tx only The switch will drop LLDP information received from neighbors, but will send out LLDP information.
Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors.
Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

Port Descr

Optional TLV: When checked the "port description" is included in LLDP information transmitted.

Sys Name

Optional TLV: When checked the "system name" is included in LLDP information transmitted.

Sys Descr

Optional TLV: When checked the "system description" is included in LLDP information transmitted.

Sys Capa

Optional TLV: When checked the "system capability" is included in LLDP information transmitted.

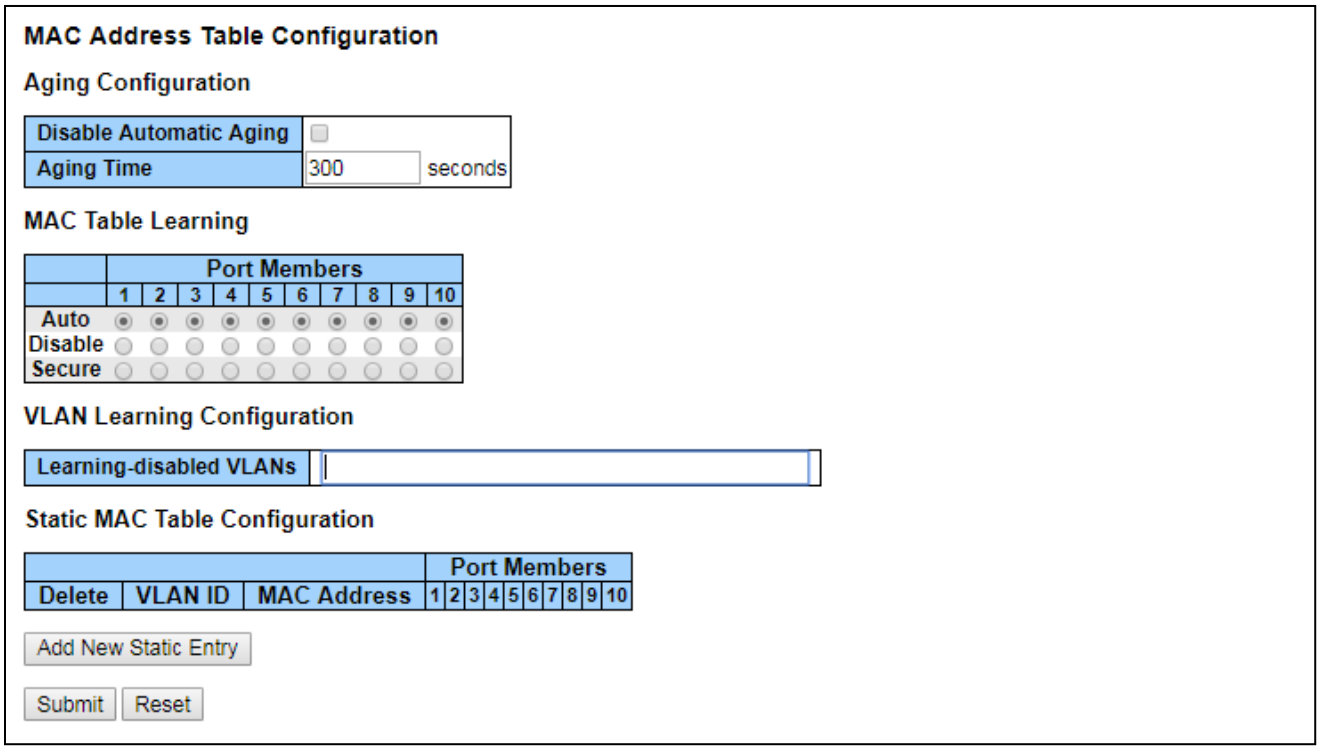
Mgmt Addr

Optional TLV: When checked the "management address" is included in LLDP information transmitted.

Buttons

Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

3.1.11 MAC TABLE



The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

Aging Configuration

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

Configure aging time by entering a value here in seconds; for example, **Age time** seconds.
The allowed range is **10** to **1000000** seconds.

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

MAC Table Learning

If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.
Each port can do learning based upon the following settings:

Auto

Learning is done automatically as soon as a frame with unknown SMAC is received.

Disable

No learning is done.

Secure

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

VLAN Learning Configuration

Learning-disabled VLANs

This field shows the Learning-disabled VLANs. When a NEW MAC arrives into a learning-disabled VLAN, the MAC won't be learnt. By the default, the field is empty. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.
The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: **1,10-13,200,300**. Spaces are allowed in between the delimiters.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The MAC table is sorted first by VLAN ID and then by MAC address.

Delete

Check to delete the entry. It will be deleted during the next save.

VLAN ID

The VLAN ID of the entry.

MAC Address

The MAC address of the entry.

Port Members

Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Adding a New Static Entry

Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Submit".

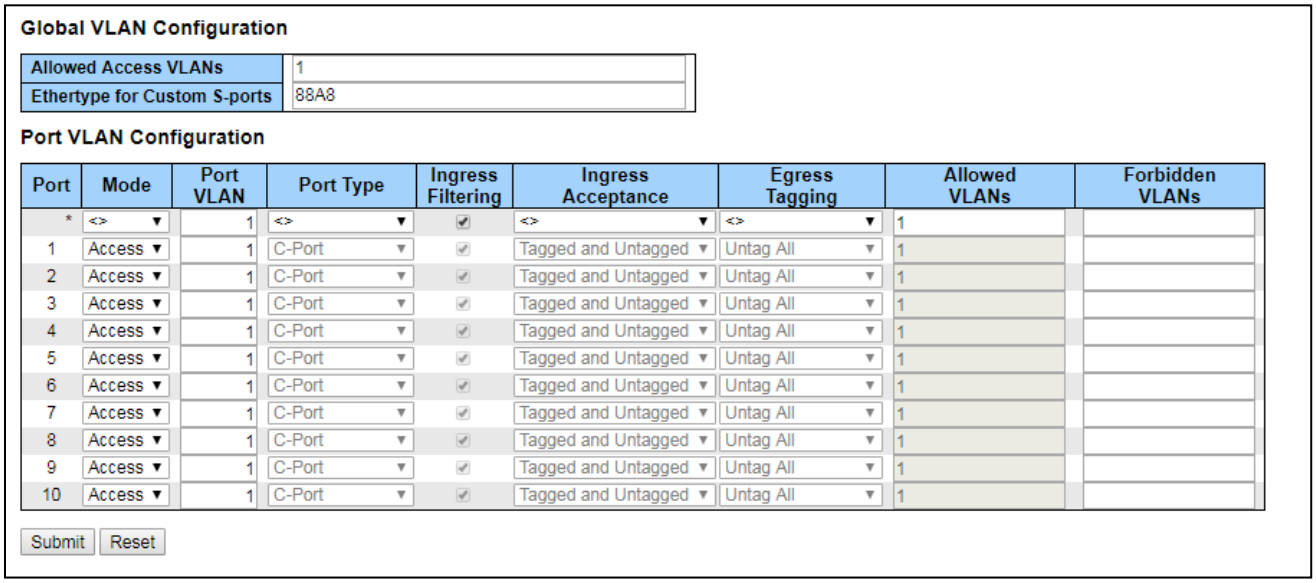
Buttons

Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

3.1.12 VLAN

Configuration

This page allows for controlling VLAN configuration on the switch. The page is divided into a global section and a per-port configuration section.



Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Submit Reset

Global VLAN Configuration

Allowed Access VLANs

This field shows the allowed Access VLANs, i.e. it only affects ports configured as Access ports. Ports in other modes are members of the VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.
The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: **1,10-13,200,300**. Spaces are allowed in between the delimiters.

Ethertype for Custom S-ports

This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

Port VLAN Configuration

Port

This is the logical port number of this row.

Mode

The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below. Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port will get when the mode is applied.

Access:
Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:

- Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1

- Accepts untagged and C-tagged frames
- Discards all frames not classified to the Access VLAN
- On egress all frames are transmitted untagged

Trunk:
Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:

- By default, a trunk port is member of all VLANs (1-4095)
- The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs
- Frames classified to a VLAN that the port is not a member of are discarded
- By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress
- Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress

Hybrid:
Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:

- Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware
- Ingress filtering can be controlled
- Ingress acceptance of frames and configuration of egress tagging can be configured independently

Port VLAN

Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1.
On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).
On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN. The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

Port Type

Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.

Unaware:
On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.

C-Port:
On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag.
If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN.
If frames must be tagged on egress, they will be tagged with a C-tag.

S-Port:
On egress, if frames must be tagged, they will be tagged with an S-tag.
On ingress, frames with a VLAN tag with TPID = 0x88A8 get classified to the VLAN ID embedded in the tag.
Priority-tagged frames are classified to the Port VLAN.
If the port is configured to accept **Tagged Only** frames (see Ingress Acceptance below), frames without this TPID are dropped.

Notice:
*If the S-port is configured to accept **Tagged and Untagged**frames (see Ingress Acceptance below), frames with a C-tag are treated like frames with an S-tag.*

*If the S-port is configured to accept **Untagged Only** frames, S-tagged frames will be discarded (except for priority S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID.*

S-Custom-Port:
On egress, if frames must be tagged, they will be tagged with the custom S-tag.
On ingress, frames with a VLAN tag with a TPID equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag.
Priority-tagged frames are classified to the Port VLAN.
If the port is configured to accept **Tagged Only** frames (see Ingress Acceptance below), frames without this TPID are dropped.

Notice:
*If the custom S-port is configured to accept **Tagged and Untagged** frames (see Ingress Acceptance below), frames with a C-tag are treated like frames with a custom S-tag.*

*If the Custom S-port is configured to accept **Untagged Only**frames, custom S-tagged frames will be discarded (except for priority custom S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID.*

Ingress Filtering

Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.
If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.
If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

Ingress Acceptance

Hybrid ports allow for changing the type of frames that are accepted on ingress.

Tagged and Untagged
Both tagged and untagged frames are accepted. See Port Type for a description of when a frame is considered tagged.
Tagged Only
Only frames tagged with the corresponding Port Type tag are accepted on ingress.

Untagged Only
Only untagged frames are accepted on ingress. See Port Type for a description of when a frame is considered untagged.

Egress Tagging

Ports in Trunk and Hybrid mode may control the tagging of frames on egress.

Untag Port VLAN
Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.

Tag All

All frames, whether classified to the Port VLAN or not, are transmitted with a tag.

Untag All
All frames, whether classified to the Port VLAN or not, are transmitted without a tag.
This option is only available for ports in Hybrid mode.

Allowed VLANs

Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN.
The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to **1-4095**.
The field may be left empty, which means that the port will not become member of any VLANs.

Forbidden VLANs

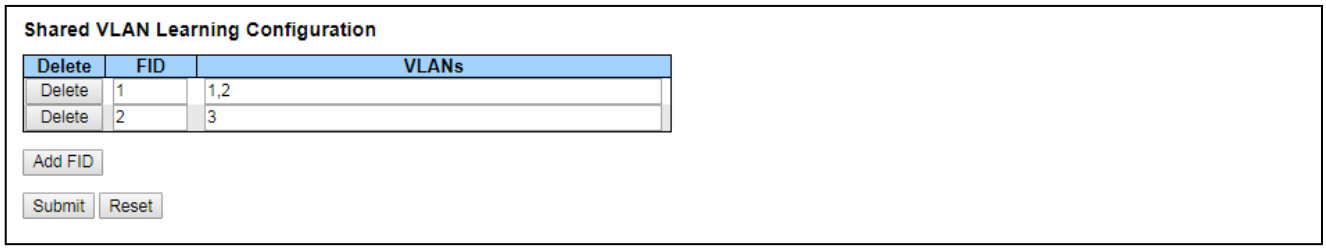
A port may be configured to never become member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.
The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field.
By default, the field is left blank, which means that the port may become a member of all possible VLANs.

Buttons

Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

SVL (Shared VLAN Learning)

Shared VLAN Learning allows for frames initially classified to a particular VLAN (based on Port VLAN ID or VLAN tag information) be bridged on a shared VLAN. In SVL two or more VLANs are grouped to share common source address information in the MAC table. The common entry in the MAC table is identified by a Filter ID (FID). SVL is useful for configuration of more complex, asymmetrical cross-VLAN traffic patterns, like E-TREE (Rooted-Multipoint) and Multi-netted Server. The alternative VLAN learning mode is IVL. The default VLAN learning mode is IVL and not all switches support SVL. In Independent VLAN Learning, every VLAN uses its own logical source address table as opposed to SVL where two or more VLANs share the same part of the MAC address table.



This page allows for controlling SVL configuration on the switch. In SVL, one or more VLANs map to a Filter ID (FID). By default, there is a one-to-one mapping from VLAN to FID, in which case the switch acts as an IVL bridge, but with SVL multiple VLANs may share the same MAC address table entries.

Delete

A previously allocated FID can be deleted by the use of this button.

FID

The Filter ID (FID) is the ID that VLANs get learned on in the MAC table when SVL is in effect.
No two rows in the table can have the same FID and the FID must be a number between 1 and 63.

VLANs

List of VLANs mapped into FID.
The syntax is as follows: Individual VLANs are separated by commas. Ranges are specified with a dash separating the lower and upper bound.
The following example will map VLANs 1, 10, 11, 12, 13, 200, and 300: **1,10-13,200,300**. Spaces are allowed in between the delimiters. The range of valid VLANs is 1 to 4095.
The same VLAN can only be a member of one FID. A message will be displayed if one VLAN is grouped into two or more FIDs.
All VLANs must map to a particular FID, and by default VLAN x maps to FID x. This implies that if FID x is defined, then VLAN x is implicitly a member of FID x unless it is specified for another FID. If FID x doesn't exist, a confirmation message will be displayed, asking whether to continue adding VLAN x implicitly to FID x.

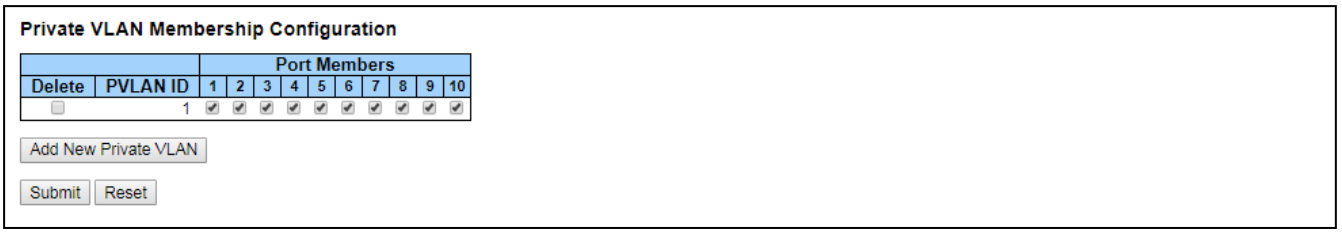
Buttons

Add FID: Add a new row to the SVL table. The FID will be pre-filled with the first unused FID.
Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

3.1.13 PRIVATE VLANS

This switch also has **private VLAN** functions; it helps to resolve the primary VLAN ID shortage, client ports' isolation and network security issues. A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains, allowing User to isolate the ports on the switch from each other. A subdomain consists of a primary VLAN and one or more secondary VLANs. All VLANs in a private VLAN domain share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another. The secondary VLANs may either be isolated VLANs or community VLANs. A host on an isolated VLAN can only communicate with the associated promiscuous port in its primary VLAN. Hosts on community VLANs can communicate among themselves and with their associated promiscuous port but not with ports in other community VLANs.

Membership



The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

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

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

Delete

To delete a private VLAN entry, check this box. The entry will be deleted during the next save.

Private VLAN ID

Indicates the ID of this particular private VLAN.

Port Members

A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New Private VLAN

Click **Add New Private VLAN** to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction.

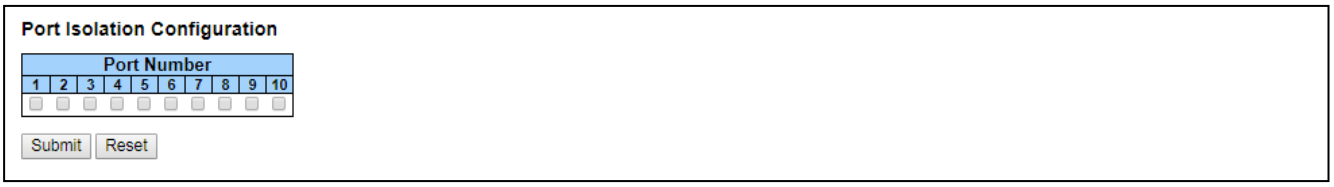
The Private VLAN is enabled when you click "Submit".

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

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

Port Isolation



This page is used for enabling or disabling port isolation on ports in a Private VLAN.

A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Configuration

Port Members

A check box is provided for each port of a private VLAN.
When checked, port isolation is enabled on that port.
When unchecked, port isolation is disabled on that port.
By default, port isolation is disabled on all ports.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
Submit: Click to submit changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

3.1.14 QoS

QoS is a mechanism for providing different priorities to different applications, users, or data flows, or to guarantee a certain level of performance for a data flow.

All incoming frames are classified into a Class of Service (CoS), which is used in the queue system when the assigning resources, in the arbitration from ingress to egress queues and in the egress scheduler when selecting the next frame for transmission.

There is a one-to-one mapping between the terms CoS, QoS class, queue, and priority. A CoS of zero has the lowest priority.

Bandwidth control in the queues can be done by using policers or shapers.

Apart from shapers and policers, different scheduling mechanisms can be configured based on how the different priority queues in the QoS system are handled.

Weighted Random Early Detection (WRED) can be configured globally to avoid congestion and drop the Yellow Frames (frames with DPL greater than zero) when the queues are filled.

The storm policers of the devices can be used at a global level to control the amount of flooded frames. It is also possible to configure per-port storm policers.

3.1.14.1 QOS CLASSIFICATION

QoS is classified as:

- Basic QoS - This enables predefined schemes for handling CoS, Drop Precedence Level (DPL), Priority Code Points (PCP), Drop Eligible Indicator (DEI), Class of Service ID (CoSID), and Differentiated Service Code Points (DSCP):
- CoS and DPL classification based on PCP and DEI for tagged frames. The mapping table from PCP and DEI to CoS and DPL is programmable per port.
- CoS and DPL classification based on DSCP values.
- DSCP translation.
- DSCP remarking based on CoS.
- Per-port CoS and DPL configuration for untagged and non-IP Frames.
- Per-port CoSID configuration. CoSID is a value that can be used as a selector in Egress Maps and Ethernet Services. It does not relate to CoS in any way.
- General classification using an Ingress Map.
- General remarking using an Egress Map.
- Advanced QoS - This uses the QoS Control Lists (QCLs), which provides a flexible classification:
- Higher layer protocol fields (Layer 2 through Layer 4) for rule matching.
- Actions include reclassification of CoS, DPL, PCP, DEI, DSCP, and ACL policy values. It is also possible to reclassify by using an Ingress Map.

3.1.14.2 POLICERS

Policers limit the bandwidth of received frames exceeding the configurable rates. Policers can be configured at queue level or at a port level. There is also a provision to add policers at the EVC level, although this provision is not discussed in this document.

3.1.14.3 SHAPERS

Egress traffic shaping can be achieved using bandwidth shapers. Shapers can be configured at queue level or at a port level.

3.1.14.4 SCHEDULING ALGORITHM

Two types of scheduling are possible on the device at a port level:

- Strict Priority: All queues follow strict priority scheduling.
- Deficit Weighted Round Robin (DWRR): Scheduling is based on the weights configured for each queue. Configuration is present to select the number of queues which can be under DWRR. It is possible to include from two to all eight queues in DWRR mode.

When the number of queues selected for DWRR is less than eight then the lowest priority queues are put in DWRR and higher priority queues are put in Strict Priority. For example if number of Queues is two for DWRR then Queue 0 and Queue 1 are set in DWRR mode, and the remaining Queues 2 to 7 are set in Strict Priority.

3.1.14.5 WEIGHTED RANDOM EARLY DETECTION (WRED)

Congestion can be avoided in the queue system by enabling and configuring the Weighted Random Early Detection (WRED) function. WRED can discard frames with DPL greater than zero.

There are three separate WRED groups, and each port belongs to one of these groups.

Configuration includes enabling WRED per group, queue, and DPL and setting the minimum and maximum Threshold. Minimum threshold is the queue fills level at which the WRED starts discarding the Frames. Maximum threshold can be configured as either Drop Probability or Fill Level. When the unit is Drop Probability, the mentioned threshold would be the Drop Probability with the queue fill level is just about 100%. When the unit is Fill Level, then it represents the queue fill level where Drop Probability is 100%.

3.1.14.6 STORM POLICING

Storm policers restrict the amount of flooded frames (frames coming with SMAC which are not learnt earlier) entering the device. The configurations are global per-device and not per-port. Storm policers can be applied separately on Unicast, Multicast, or Broadcast packets.

It is also possible to configure per-port storm policers. Port storm policers can be applied separately on Unicast, Broadcast, and flooded (unknown) packets.

3.1.14.7 INGRESS MAP

An Ingress Map is a mapping table created to classify values at ingress such as, CoS, DPL, PCP, DEI, DSCP, and CoSID based on the key values in the packet (PCP, PCP/DEI, DSCP, or PCP/DEI/DSCP).

In order to use an Ingress Map, it must first be created and configured. Configuration consists of the following

parameters:

- Key: Which part of the packet to use for lookup.
- Actions: Which kinds of values to classify.
- Mappings: The actual value to use for classification for each value of the key.

A specific Ingress Map can be associated with one or more ports, QCEs, or EVCs/ECEs. Using an Ingress Map will always take precedence over other kinds of port-based classification.

3.1.14.8 EGRESS MAP

An Egress Map is a mapping table created to control the rewriting of packets at egress. Values such as PCP, DEI, and DSCP can be updated based on the classified key values (CoSID, CoSID/DPL, DSCP, or DSCP/DPL).

In order to use an Egress Map, it must first be created and configured. Configuration consists of the following parameters:

- Key: This classified value(s) to use for lookup.
- Actions: Which kinds of values to rewrite in the packet.
- Mappings: The actual value to use for rewriting for each value of the key. A specific Egress Map can be associated with one or more ports or EVCs.

Configuration Examples

In the following sections, web interface and ICLI configuration examples are given according to the different QoS classifications.

Note: It is recommended to do a restore to default before starting to configure any of the examples in the following sections.

```
# reload defaults

#
```

Basic QoS: Port Classification

Basic QoS classification configuration can be done per port. Ingress traffic coming on each port can be assigned to a CoS, DPL, PCP, and DEI.

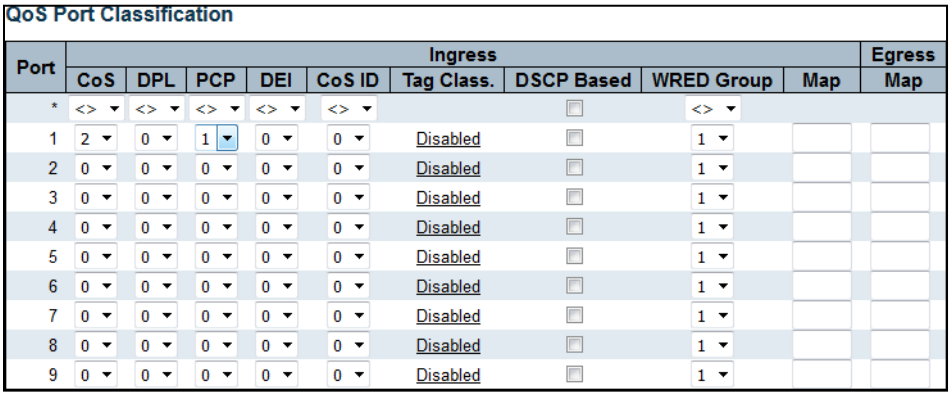
Example: All traffic coming on Port 1 is mapped to CoS 2, and PCP is set as 1.

Configuring Basic QoS Classification Using WebGUI

To configure all traffic coming on Port 1 is mapped to CoS 2 and PCP is set as 1, perform the following step.

- Click **Configuration** > **QoS** > **Port Classification**, and enter the settings as shown in the following illustration.

Set Up CoS and PCP for Ingress Traffic



The equivalent ICLI commands are:

configure terminal
(config)# interface GigabitEthernet 1/1
! Set CoS to 2 and PCP to 1
(config-if)# qos cos 2
(config-if)# qos pcp 1
(config-if)# end

Basic QoS: Tagged Frame Classification per Port

Ingress port tag classification can be done based on the PCP and DEI values received on the incoming packets. This is done by enabling tag classification for that port.

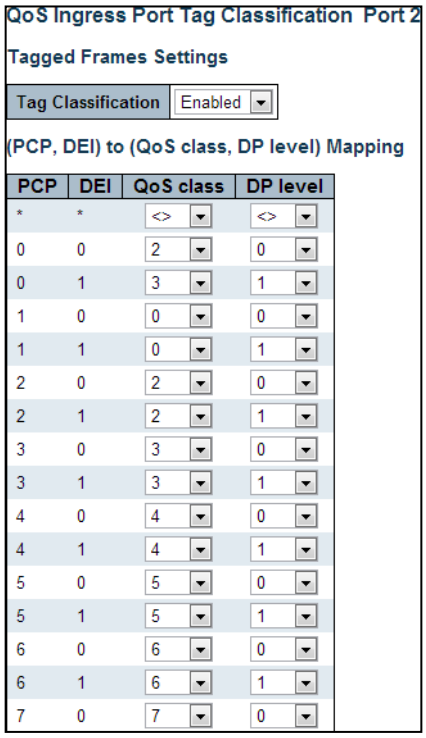
Example: Map PCP 0 and DEI 0 to CoS 2 and DPL 0, Map PCP 0 and DEI 1 to CoS 3 and DPL 1 on Port 2.

Configuring Ingress Port Tag Classification Using WebGUI

In order to configure the mapping from PCP 0 and DEI 0 to CoS 2 and DPL 0, and mapping from PCP 0 and DEI 1 to CoS 3 and DPL 1 on Port 2, please perform to the following steps.

1. Click **Configuration** > **QoS** > **Port Classification**.
2. On the **Port Classification** page, click the **Tag Class** corresponding to the port, and enter the parameters as shown in the following illustration.

Map PCP and DEI for Tagged Frames



The equivalent ICLI commands are:

```
# configure terminal
(config)# interface GigabitEthernet 1/2
! Enable Tag Classification
(config-if)# qos trust tag
! Map PCP 0 and DEI 0 to CoS 2 and DPL 0
(config-if)# qos map tag-cos pcp 0 dei 0 cos 2 dpl 0
! Map PCP 0 and DEL 1 to CoS 3 and DPL 1
(config-if)# qos map tag-cos pcp 0 dei 1 cos 3 dpl 1
(config-if)# end
```

Basic QoS: Tag Remarking per Port

Tag remarking on the egress frames can be done in three ways:

- Classified: PCP and DEI values on the egress frames are updated with the classified values at the ingress. By default, the PCP and DEI values are set to classified values.
- Default: PCP and DEI values on the egress frames are updated to default values defined per port.
- Mapped: PCP and DEI values on the egress frames are updated based on the tag remarking CoS/DPL to PCP/DEI mapping per port.

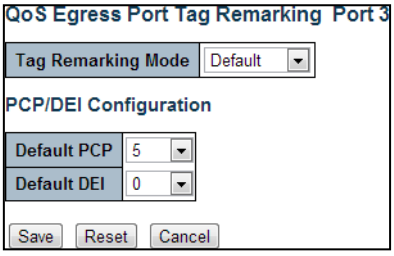
Example: Set Default PCP to 5 and DEI to 0 on Port 3.

Setting Up PCP Port Using WebGUI

To set the default PCP to 5 and DEI to 0 on Port 3, perform the following steps.

1. Click **Configuration** > **QoS** > **Port Tag Remarking**.
2. On the **Port Tag Remarking** page, click the **Port Number** corresponding to the port, and set the parameters as shown in the following illustration.

Set Up PCP and DEI for Default Tag Remarking



The equivalent ICLI commands are:

configure terminal
(config)# interface GigabitEthernet 1/3
! Set Default PCP to 5 and DEI to 0 (config-if)# qos tag-remark
pcp 5 dei 0 (config-if)# end

Example: Map CoS 2 and DPL 0 to PCP 3 and DEI 0. Map CoS 3 and DPL 1 to PCP 4 and DEI 1.

Mapping CoS and DPL Using WebGUI

To map CoS 2/DPL 0 to PCP 3/DEI 0 and CoS 3/DPL 1 to PCP 4/DEI 1, perform the following steps.

1. Click **Configuration** > **QoS** > **Port Tag Remarking**.
2. On the **Port Tag Remarking** page, click the **Port Number** corresponding to the port, and enter the parameters as shown in the following illustration.

Set Up CoS and DPL for Mapped Tag Remarking



The equivalent ICLI commands are:

configure terminal
(config)# interface GigabitEthernet 1/2
! Set Tag Remarking to Mapped
(config-if)# qos tag-remark mapped
! Map QoS Class 2 and DPL 0 to PCP 3 and DEI 0
(config-if)# qos map cos-tag cos 2 dpl 0 pcp 3 dei 0
! Map QoS Class 3 and DPL 1 to PCP 4 and DEI 1
(config-if)# qos map cos-tag cos 3 dpl 1 pcp 4 dei 1
(config-if)# end

Basic QoS: DSCP Configuration

The following DSCP Configuration settings are present per port for both the ingress and egress.

- DSCP-based QoS classification
- Selection of trusted DSCP values used for QoS Classification
- DSCP translation: DSCP translation is done based on the DSCP Translation table
- Classify (for rewriting if enabled):
  - No DSCP classification
  - Classify only DSCP = 0
  - Classify only selected (trusted) DSCP values based on the DSCP Classification table
  - Classify all DSCP
- Rewrite (on Egress):
  - No Egress rewrite
  - Rewrite enabled without remapping
  - Remap DSCP with DP unaware
  - Remap DSCP with DP aware

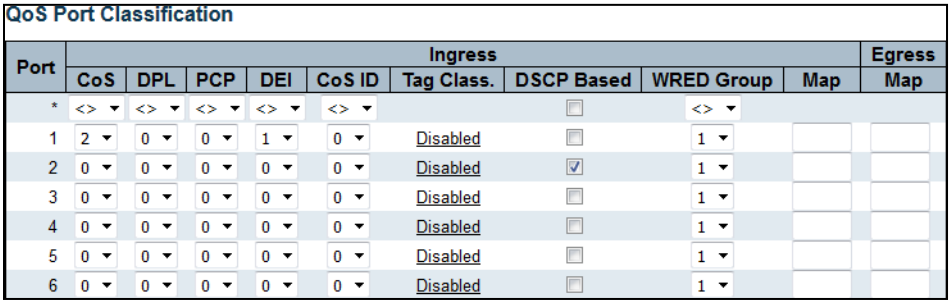
Example: DSCP (Only Trusted) to QoS Class/DPL classification at ingress on Port 2.

Configuring DSCP to QoS Classification Using WebGUI

To configure DSCP (only trusted) to QoS Class/DPL classification at ingress on Port 2, perform the following steps.

1. Click **Configuration** > **QoS** > **Port Classification**, and select the **DSCP Based** option as shown in the following illustration.

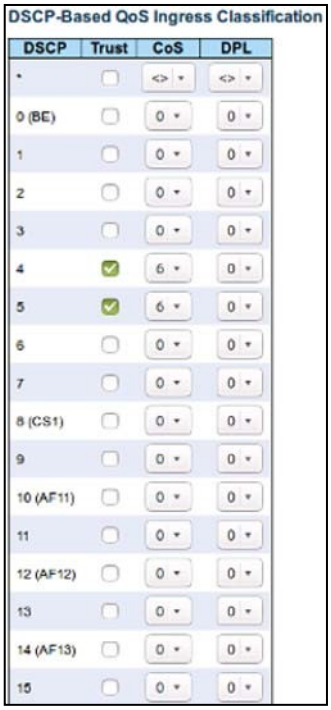
   Enable Trusted DSCP for Port


QoS Port Classification

Port	Ingress									Egress
	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	WRED Group	Map	Map
*	<>	<>	<>	<>	<>		☐	<>		
1	2	0	0	1	0	Disabled	☐	1		
2	0	0	0	0	0	Disabled	☑	1		
3	0	0	0	0	0	Disabled	☐	1		
4	0	0	0	0	0	Disabled	☐	1		
5	0	0	0	0	0	Disabled	☐	1		
6	0	0	0	0	0	Disabled	☐	1		

2. Click **Configuration** > **QoS** > **DSCP-Based QoS**, and configure as shown in the following illustration.

Map Trusted DSCP for Ingress Traffic



The equivalent ICLI commands are:

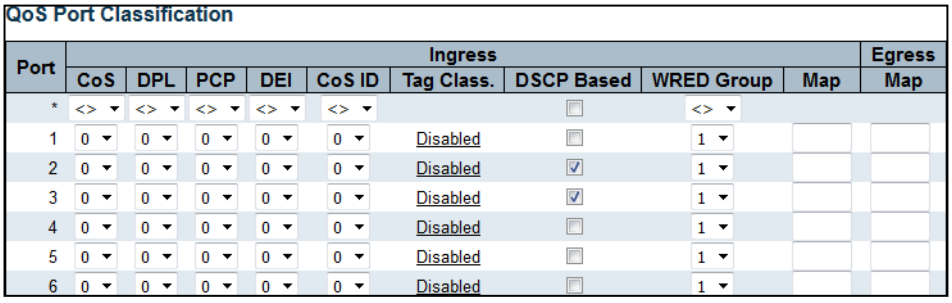
configure terminal
! Enable DSCP Trust for DSCP at Port2.
(config)# interface GigabitEthernet1/2
(config-if)# qos trust dscp
(config-if)# exit
! Map DSCP Values 4 and 5 to QoS Class 6.
(config)# qos map dscp-cos 4 cos 6 dpl 0
(config)# qos map dscp-cos 5 cos 6 dpl 0
(config)# end

Example: Translate DSCP at ingress on Port 2 and rewrite enabled on Port 3.

Translating DSCP at Ingress Using WebGUI

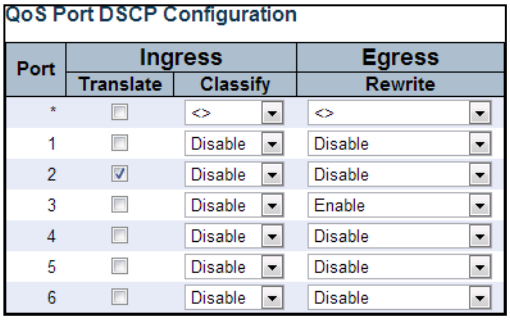
To translate DSCP at Ingress on Port 2 and rewrite enabled on Port 3, perform the following steps.

1. Click **Configuration** > **QoS** > **Port Classification**, and select the **DSCP Based** options as shown in the following illustration.
   Enable DSCP-Based QoS for Translation and DSCP Rewrite



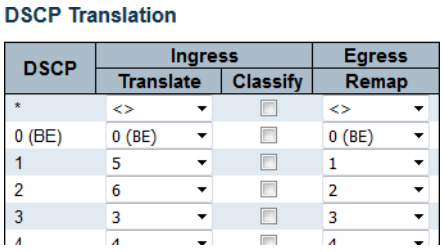
2. Click **Configuration** > **QoS** > **Port DSCP** and select the **Translate** option.

Config DSCP Ingress Translation and DSCP Egress Rewrite



3. Click **Configuration** > **QoS** > **DSCP Translation**, and configure translation mapping as shown in the following illustration.

Set Up Ingress Translation Map for DSCP



The equivalent ICLI commands are:

configure terminal
! Enable DSCP Translate at ingress on Port 2
(config)# interface GigabitEthernet 1/2
(config-if)# qos trust dscp
(config-if)# qos dscp-translate
(config-if)# exit
! Enable DSCP Remark at egress on Port 3
(config)# interface GigabitEthernet 1/3

(config-if)# qos trust dscp
(config-if)# qos dscp-remark rewrite
(config-if)# exit
! Create Ingress DSCP Translation Map
(config)# qos map dscp-ingress-translation 1 to5
(config)# qos map dscp-ingress-translation 2 to6
(config)# end

Example: Classify only DSCP as 0 at ingress on Port 2 and rewrite enabled on Port 3.

Configuring DSCP Classification at Ingress UsingWebGUI

To classify only DSCP as 0 at ingress on Port 2 and rewrite enabled on Port 3, perform the following steps.

1. Click **Configuration** > **QoS** > **Port Classification**, and select the **DSCP Based** options as shown in the following illustration.
   Enable DSCP-Based QoS for DSCP 0 Classification and DSCP Rewrite

QoS Port Classification

Port	Ingress								Egress
	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	WRED Group	Map
*	<>	<>	<>	<>	<>		☐	<>	
1	0	0	0	0	0	Disabled	☐	1	
2	0	0	0	0	0	Disabled	☑	1	
3	0	0	0	0	0	Disabled	☑	1	
4	0	0	0	0	0	Disabled	☐	1	
5	0	0	0	0	0	Disabled	☐	1	
6	0	0	0	0	0	Disabled	☐	1	

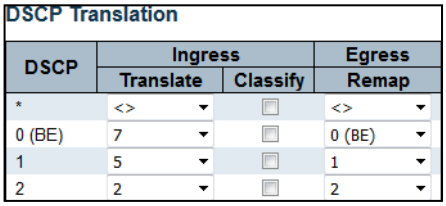
2. Click **Configuration** > **QoS** > **Port DSCP**, and set the Ingress values as shown in the following illustration.
   Set Up DSCP 0 Ingress Classification and DSCP Egress Rewrite

QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	☐	<>	<>
1	☐	Disable	Disable
2	☑	DSCP=0	Disable
3	☐	Disable	Enable
4	☐	Disable	Disable
5	☐	Disable	Disable
6	☐	Disable	Disable

3. Click **Configuration** > **QoS** > **DSCP Translation**, and enter translation mapping as shown in the following illustration.

Set Up Ingress Translation Map for DSCP 0



The equivalent ICLI commands are:

configure terminal
! Enable DSCP=0 Classification and Translation at ingress on Port2
(config)# interface GigabitEthernet 1/2
(config-if)# qos trust dscp
(config-if)# qos dscp-classify zero
(config-if)# qos dscp-translate
(config-if)# exit
! Create Ingress DSCP Translation Map.
(config)# qos map dscp-ingress-translation 0 to 7
(config)# qos map dscp-ingress-translation 1 to 5
! Note: Only DSCP=0 will be rewritten as these are only classified.
! Enable DSCP Remark at egress on Port 3
(config)# interface GigabitEthernet 1/3
(config-if)# qos trust dscp
(config-if)# qos dscp-remark rewrite
(config-if)# exit
(config)# end

Example: Classify Selected DSCP at ingress on Port 2, DSCP rewrite enabled on Port 3.

Classifying Selected DSCP at Ingress UsingWebGUI

To classify selected DSCP at ingress on Port 2, and DSCP rewrite enabled on Port 3, perform the following steps.

1. Click **Configuration** > **QoS** > **Port Classification**, and select the **DSCP Based** option.
   Enable Selected DSCP Classification and DSCP Rewrite

QoS Port Classification

Port	Ingress									Egress
	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	WRED Group	Map	Map
*	<>	<>	<>	<>	<>		☐	<>		
1	0	0	0	0	0	Disabled	☐	1		
2	0	0	0	0	0	Disabled	☑	1		
3	0	0	0	0	0	Disabled	☑	1		
4	0	0	0	0	0	Disabled	☐	1		
5	0	0	0	0	0	Disabled	☐	1		
6	0	0	0	0	0	Disabled	☐	1		

2. Click **Configuration** > **QoS** > **Port DSCP**, and set the values as shown in the followingillustration.
   Set Up Selected DSCP Ingress Classification and DSCP Egress Rewrite

QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	☐	<>	<>
1	☐	Disable	Disable
2	☑	Selected	Disable
3	☐	Disable	Enable
4	☐	Disable	Disable
5	☐	Disable	Disable
6	☐	Disable	Disable

3. Click **Configuration** > **QoS** > **DSCP Translation**, and configure translation mapping as shown in the following illustration.

Set Up Ingress Translation Map for Selected DSCP

DSCP Translation

DSCP	Ingress		Egress
	Translate	Classify	Remap
*	<>	☑	<>
0 (BE)	7	☑	0 (BE)
1	5	☑	1
2	8 (CS1)	☑	2
3	3	☐	3
4	4	☐	4

The equivalent ICLI commands are:

```
# configure terminal
! Enable DSCP classification for selected DSCP values at ingress Port2
(config)# interface GigabitEthernet 1/2
(config-if)# qos trust dscp
(config-if)# qos dscp-classify selected
(config-if)# exit
(config)# qos map dscp-classify 0
(config)# qos map dscp-classify 1
(config)# qos map dscp-classify 2
! Create Ingress DSCP Translation Map.
(config)# qos map dscp-ingress-translation 0 to 7
```

(config)# qos map dscp-ingress-translation 1 to 5

(config)# qos map dscp-ingress-translation 2 to 8

! Enable DSCP Remark at egress on Port 3

(config)# interface GigabitEthernet 1/3

(config-if)# qos trust dscp

(config-if)# qos dscp-remark rewrite

(config-if)# exit

(config-if)# end

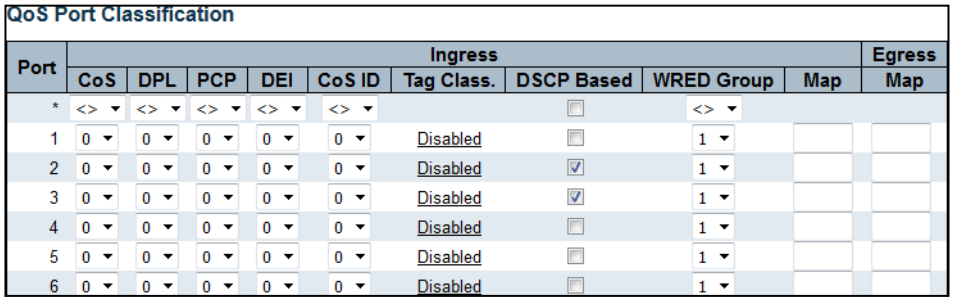
Example: Classify all DSCP values at ingress on Port 2, rewrite enabled on Port 3.

Classifying All DSCP at Ingress Using WebGUI

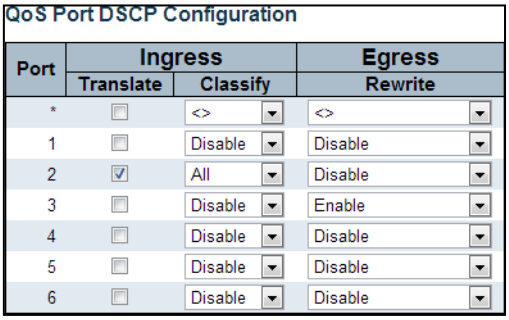
To classify all DSCP values at ingress on Port 2, rewrite enabled on Port 3, perform the following steps.

1. Click **Configuration** > **QoS** > **Port Classification**, and select the **DSCP Based** option as shown in the following illustration.

   Enable All DSCP Classification and DSCP Rewrite



2. Click **Configuration** > **QoS** > **Port DSCP**, and set the values as shown in the following illustration.
   Set Up All DSCP Ingress Classification and DSCP Egress Rewrite



The equivalent ICLI commands are:

configure terminal
! Enable DSCP classification for all DSCP values at ingress Port2
(config)# interface GigabitEthernet 1/2
(config-if)# qos trust dscp
(config-if)# qos dscp-classify any
(config-if)# exit
! Enable DSCP Remark at egress on Port 3
(config)# interface GigabitEthernet 1/3

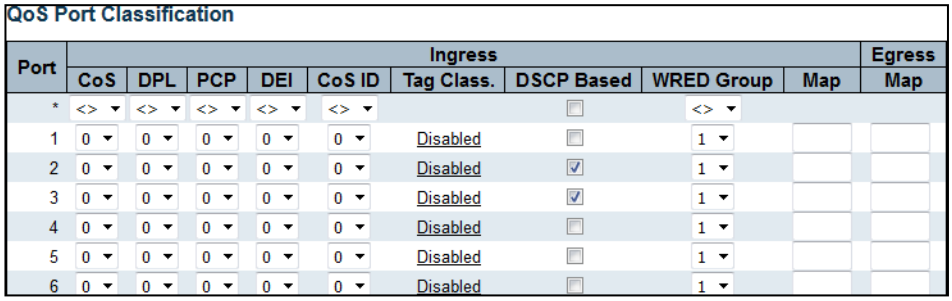
(config-if)# qos trust dscp
(config-if)# qos dscp-remark rewrite
(config-if)# exit
(config)# end

Example: QoS/DP to DSCP Classification enabled. Rewrite DSCP at egress on Port 3.

Enabling QoS/DP to DSCP Classification UsingWebGUI

To enable QoS/DP to DSCP Classification and rewrite DSCP at egress on Port 3, perform the following steps.

1. Click **Configuration** > **QoS** > **Port Classification**, and select the **DSCP Based** option as shown in the following illustration.
   Enable All DSCP Classification and DSCP Egress Remap

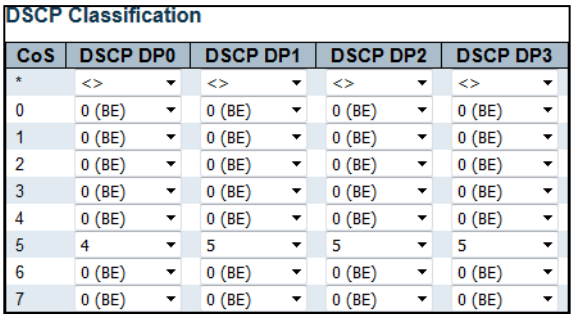


QoS Port Classification

Port	Ingress									Egress
	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	WRED Group	Map	Map
*	<>	<>	<>	<>	<>		☐	<>		
1	0	0	0	0	0	Disabled	☐	1		
2	0	0	0	0	0	Disabled	☑	1		
3	0	0	0	0	0	Disabled	☑	1		
4	0	0	0	0	0	Disabled	☐	1		
5	0	0	0	0	0	Disabled	☐	1		
6	0	0	0	0	0	Disabled	☐	1		

2. Click **Configuration** > **QoS** > **DSCP Classification**, and set the values as shown in the following illustration.

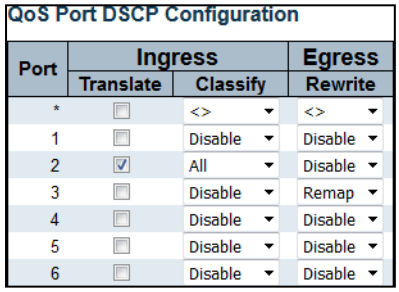
Map QoS/DP to DSCP Classification



DSCP Classification

CoS	DSCP DP0	DSCP DP1	DSCP DP2	DSCP DP3
*	<>	<>	<>	<>
0	0 (BE)	0 (BE)	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)	0 (BE)	0 (BE)
5	4	5	5	5
6	0 (BE)	0 (BE)	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)	0 (BE)	0 (BE)

3. Click **Configuration** > **QoS** > **Port DSCP**, and set the values as shown in the followingillustration.
   Set Up All DSCP Ingress Classification and DSCP Egress Remap



QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	☐	<>	<>
1	☐	Disable	Disable
2	☑	All	Disable
3	☐	Disable	Remap
4	☐	Disable	Disable
5	☐	Disable	Disable
6	☐	Disable	Disable

4. Click **Configuration** > **QoS** > **DSCP Translation**, and configure translation mapping as shown in the following illustration.

Remap DSCP from Ingress to Egress

DSCP Translation

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

The equivalent ICLI commands are:

configure terminal
! Enable DSCP Classification on all DSCP values on port2. (config)# interface GigabitEthernet 1/2
(config-if)# qos trust dscp (config-if)# qos dscp-classify
any (config-if)# exit
! Map QoS Class 5, DP 0 to DSCP 4, QoS Class 5, DP 1..3 to DSCP 5
(config)# qos map cos-dscp 5 dpl 0 dscp4
(config)# qos map cos-dscp 5 dpl 1 dscp5
(config)# qos map cos-dscp 5 dpl 2 dscp5
(config)# qos map cos-dscp 5 dpl 3 dscp5
! Remap DSCP 4 to DSCP = 8 and DSCP 5 to DSCP = 9 onEgress (config)# qos map
dscp-egress-translation 4 to 8
(config)# qos map dscp-egress-translation 5 to9
! Enable DSCP rewrite with DSCP Remap on Port 3 (config)# interface
GigabitEthernet 1/3
(config-if)# qos dscp-remark remap (config-if)# end

Advanced QoS: QCLs

Advanced QoS classification can be done by checking fields from Layer 2 to Layer 4 and mapping them to CoS, PCP/DEI, and DSCP values.

Example: Match on a particular Destination MAC on Port 2 and map these to CoS = 5.

Mapping a Particular MAC Destination to CoS Using WebGUI

To match on a particular destination MAC on Port 2 and map these to CoS = 5, perform the following steps.

1. Click **Configuration** > **QoS** > **QoS Control List** and click the **Add QCE to end of list** icon. The **QCE onfiguration** page opens.

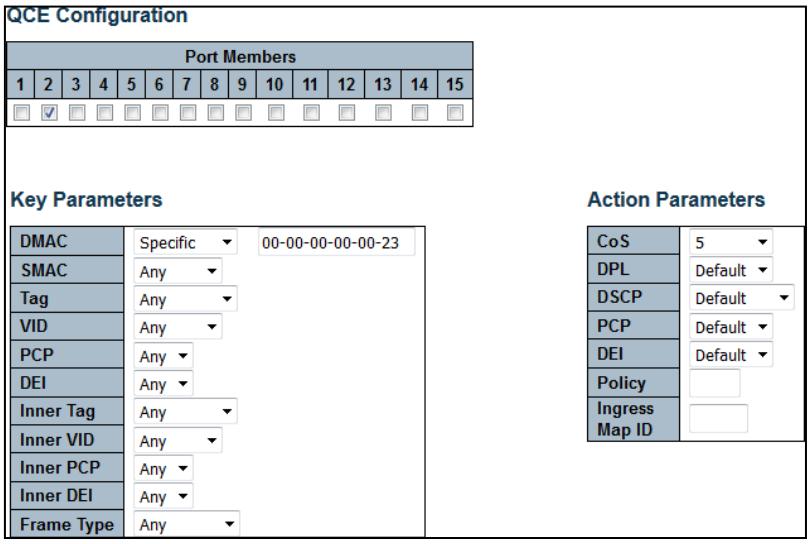
Create QCE Entry for Mapping MAC Address

QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action						
									CoS	DPL	DSCP	PCP	DEI	Policy	Ingress Map
															⊕

2. On the **QCE Configuration** page, set **Port**, **DMAC**, and **CoS** as shown in the followingillustration.

Map Frame with Particular Destination MAC to CoS



The equivalent ICLI commands are:

configure terminal
! Create QCL rule for matching particular destination MAC on Port 2 (config)#qosqce1interfaceGigabitEthernet 1/2dmac00-00-00-00-00-23action cos 5
(config-if)# end

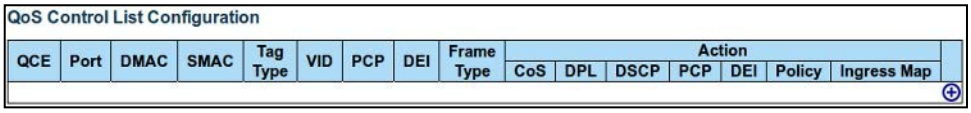
Example: Match on a particular VLAN Tag and PCP range on Port 2 and map these to CoS = 6. Also, map these frames to PCP = 6 and DEI = 0.

Mapping a Particular VLAN Tag and PCP Range to CoS Using WebGUI

To match on a particular VLAN Tag and PCP range on Port 2 and map these to CoS = 6, and also to map these frames to PCP = 6 and DEI = 0, perform the following steps.

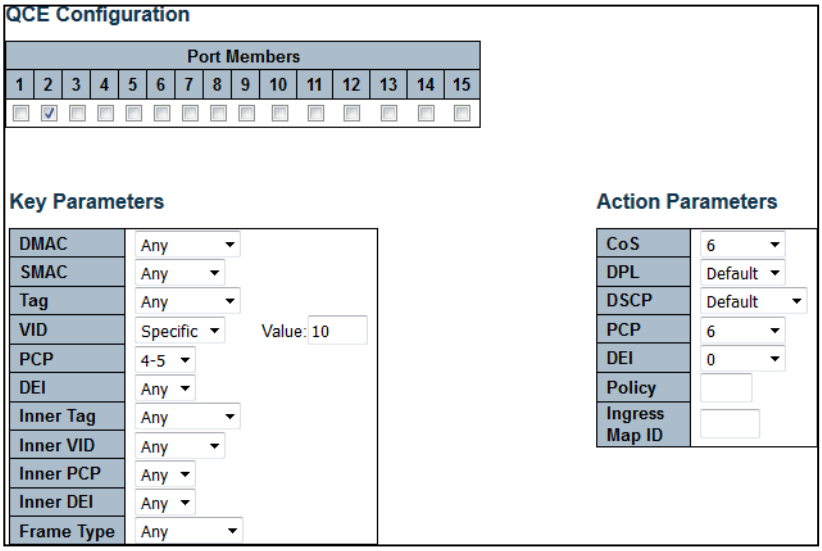
1. Click **Configuration** > **QoS** > **QoS Control List** and click the **Add QCE to end of list** icon. The **QCE Configuration** page opens.

Create QCE Entry for Mapping VLAN Tag and PCP



2. On the **QCE Configuration** page, set the appropriate values as shown in the following illustration.

Map Frame with Particular VLAN Tag and PCP to CoS, PCP, and DEI



The equivalent ICLI commands are:

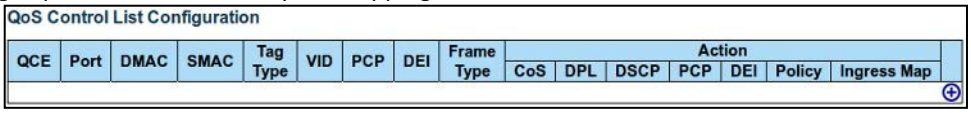
configure terminal
! Create QCL rule for matching particular VLAN ID and range of PCP values. (config)# qos qce 1 interface GigabitEthernet 1/2 tag vid 10 pcp 4-5action cos 6
pcp-dei 6 0 (config)# end

Example: Map on specific Dest MAC, Source IP, UDP Sport number on Port 2. Map these to CoS = 7, DP = 1 and, DSCP = 9.

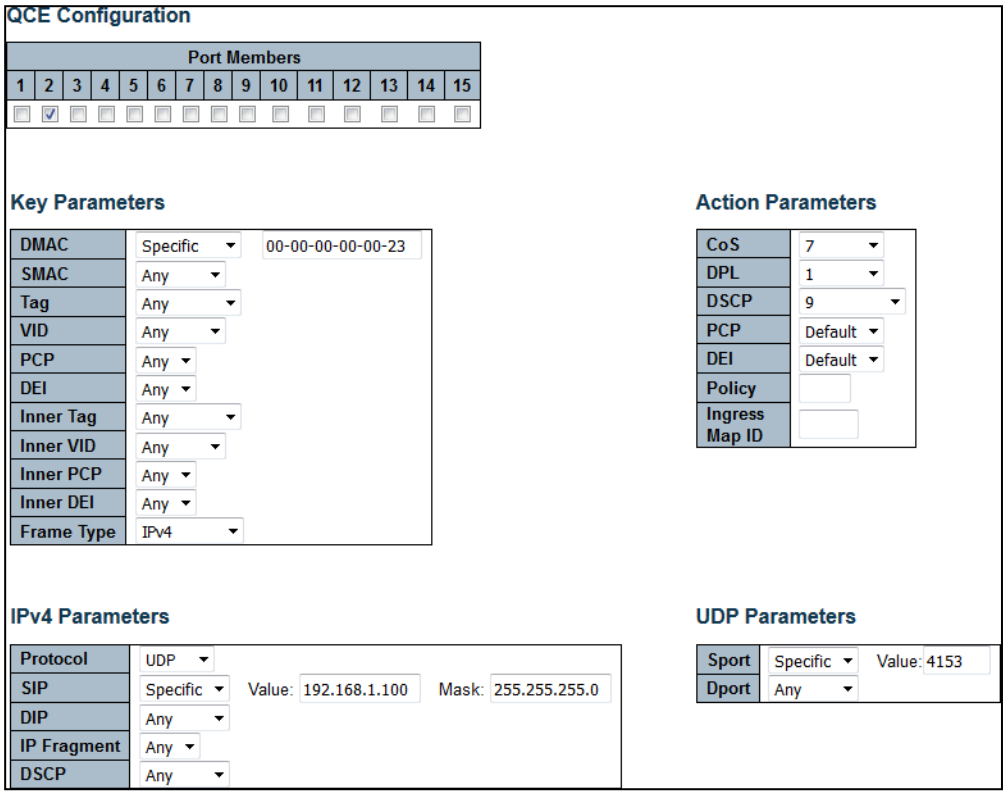
Mapping a Particular MAC Adress, Source IP, and UDP Sport Number Using WebGUI

To map specific destination MAC, Source IP, and UDP Sport number on Port 2, and map these to CoS = 7, DP = 1 and, DSCP = 9, perform the following steps.

1. Click **Configuration** > **QoS** > **QoS Control List** and click the **Add QCE to End of List** icon. The **QCE Configuration** page opens. Create QCE Entry for Mapping MAC Address, IP, and UDP Port



2. On the **QCE Configuration** page, set the appropriate values as shown in the followingillustration. Map Frame With Specifc MAC, IP, and UDP Port to CoS, DP, and DSCP



The equivalent ICLI commands are:

configure terminal
! Create QCL rule for matching DMAC, SIP, UDP Sport on Port 2. (config)# qos qce 1 interface GigabitEthernet 1/2 dmac00-00-00-00-00-23 frametype
ipv4 proto udp sip 192.168.1.100/24 sport 4154 action cos 7 dpl 1 dscp9 (config)# end

Policers

Port Policers

Enable policing at port level on a particular port.

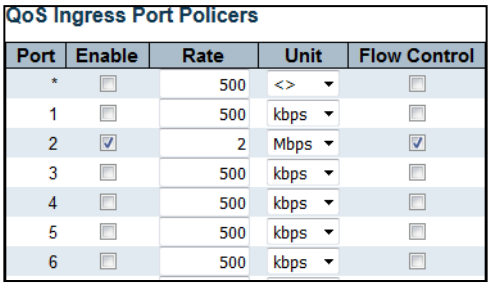
Example: Enable policer on Port 2 and set the policer rate to 2 Mbps. For better performance, we can optionally enable Flow control as well if the policed traffic is TCP traffic.

Configuring Policer Rate (Mbps) on aPort Using WebGUI

To configure policer on Port 2 and set the policer rate to 2 Mbps, perform the following step.

- Click **Configuration** > **QoS** > **Port Policing**, and set the policer rate as shown in the following illustration.

Set Up Port Policer Rate in Mbps Throughput



The equivalent ICLI commands are:

configure terminal
! Enable Policer on Port 2 with a rate set to 2 Mbps (config)# interface
GigabitEthernet 1/2
(config-if)# qos policer 2 mbps flowcontrol (config-if)# end

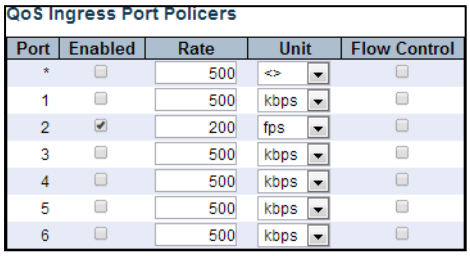
Example: Enable policer on Port 2 and set the policer rate to 200 Fps. The units are frames per second.

Configuring Policer Rate (Fps) on a Port Using WebGUI

To configure the policer on Port 2 and set the policer rate to 200 Fps, perform the following step.

- Click **Configuration** > **QoS** > **Port Policing**, and set the policer rate as shown in the following illustration.

Set Up Port Policer Rate in Fps Throughput



The equivalent ICLI commands are:

configure terminal
! Enable Policer on Port 2 with a rate set to 200fps (config)# interface
GigabitEthernet 1/2
(config-if)# qos policer 200 fps (config-if)# end

Queue Policers

Example: Enable policer on Queue 2 at Port 2. Set the policing rate to 20 Mbps.

Configuring Queue Policer on a Port Using WebGUI

To configure Queue Policer on Queue 2 at Port 2 and set the policing rate to 20 Mbps, perform the following steps.

1. Click **Configuration** > **QoS** > **Queue Policing**, and configure the policer as shown in the following illustration.

Set Up Queue Policer Rate in Mbps Throughput

QoS Ingress Queue Policers

Port	Queue 0	Queue 1	Queue 2			Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable	Enable	E	Rate	Unit	Enable	Enable	Enable	Enable	Enable
*	☐	☐	☐	500	<>	☐	☐	☐	☐	☐
1	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
2	☐	☐	☑	20	Mbps	☐	☐	☐	☐	☐
3	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
4	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
5	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
6	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐

The equivalent ICLI commands are:

configure terminal
! Enable Policer on Queue 2 at Port 2 with a rate set to 20Mbps (config)# interface GigabitEthernet 1/2
(config-if)# qos queue-policer queue 2 20 mbps (config-if)# end

Shapers

Port Shapers

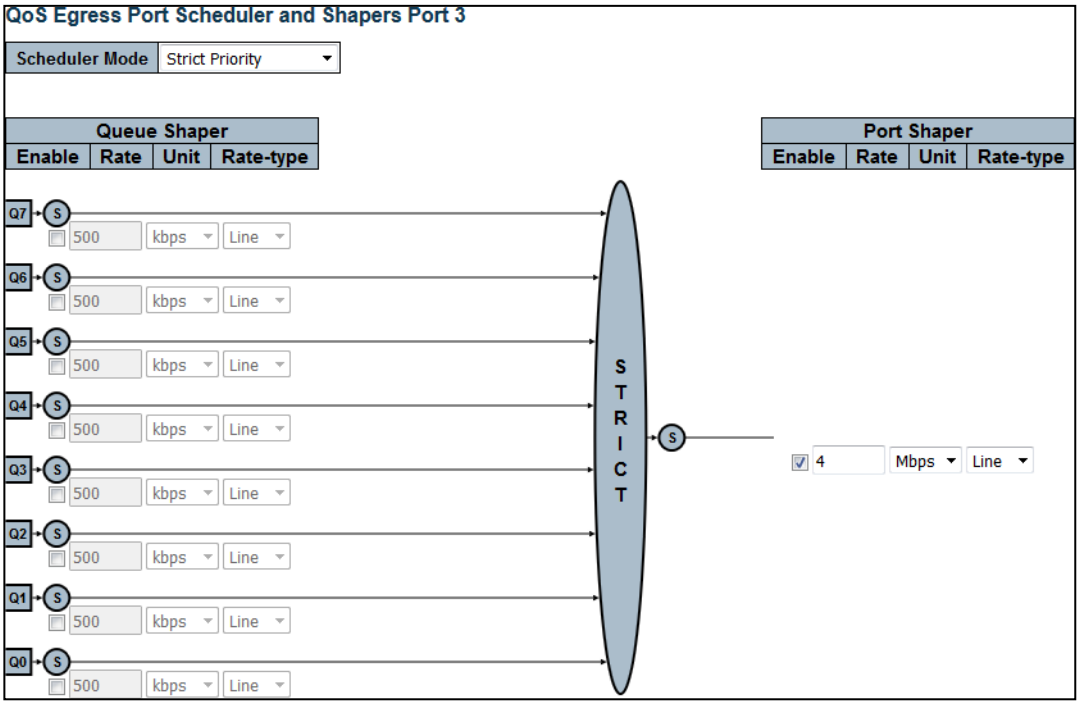
Enable shapers at port level to shape the egress traffic.
Example: Enable shaper on Port 3 and set the shaping rate to 4 Mbps.

Configuring Shaping Rate (Mbps) on a Port Using WebGUI

To enable a shaper on Port 3 and set the shaping rate to 4 Mbps, perform the following steps.

1. Click **Configuration** > **QoS** > **Port Shaping**.
2. **Port Shaping** page, click the **Port Number** corresponding to the port, and set the **Scheduler Mode** and **Rate** as shown in the following illustration.

Set Up Port Shaper Rate in Mbps Throughput



The equivalent ICLI commands are:

configure terminal
! Enable Shaper on Port 3 and set the rate to 4 Mbps (config)# interface
GigabitEthernet 1/3
(config-if)# qos shaper 4 mbps (config-if)# end

Queue Shapers

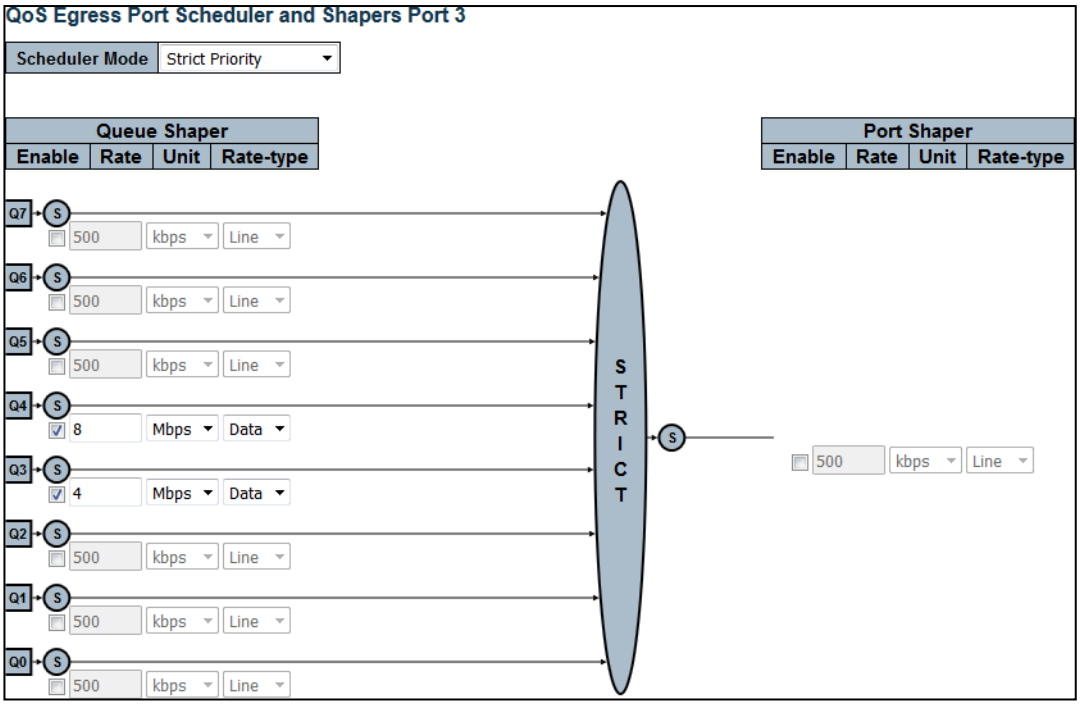
Example: Enable shaping on Queue 3 and Queue 4 at different rates on Port 3 and configure queue shapers to measure the data rate instead of the line rate.

Configuring Queue Shaper to Measure Data Rate UsingWebGUI

To configure shaping on Queue 3 and Queue 4 at different rates on Port 3, and to configure queue shapers to measure the data rate instead of the line rate, perform the following steps.

1. Click **Configuration** > **QoS** > **Port Shaping**.
2. On the **Port Shaping** page, click the **Port Number** corresponding to the port, and set **Queue Shaper** as seen in the following illustration.

Multiple Queues with Different Queue Shaper Rates



The equivalent ICLI commands are:

configure terminal
! Enable Queue Shaper on Queues 3 and 4 on Port 3 and set the rate to 4 and8
! Mbps. Use data rate.
(config)# interface GigabitEthernet 1/3
(config-if)# qos queue-shaper queue 3 4 mbps rate-type data (config-if)# qos queue-shaper queue 4 8 mbps rate-typedata (config-if)# end

Schedulers

DWRR

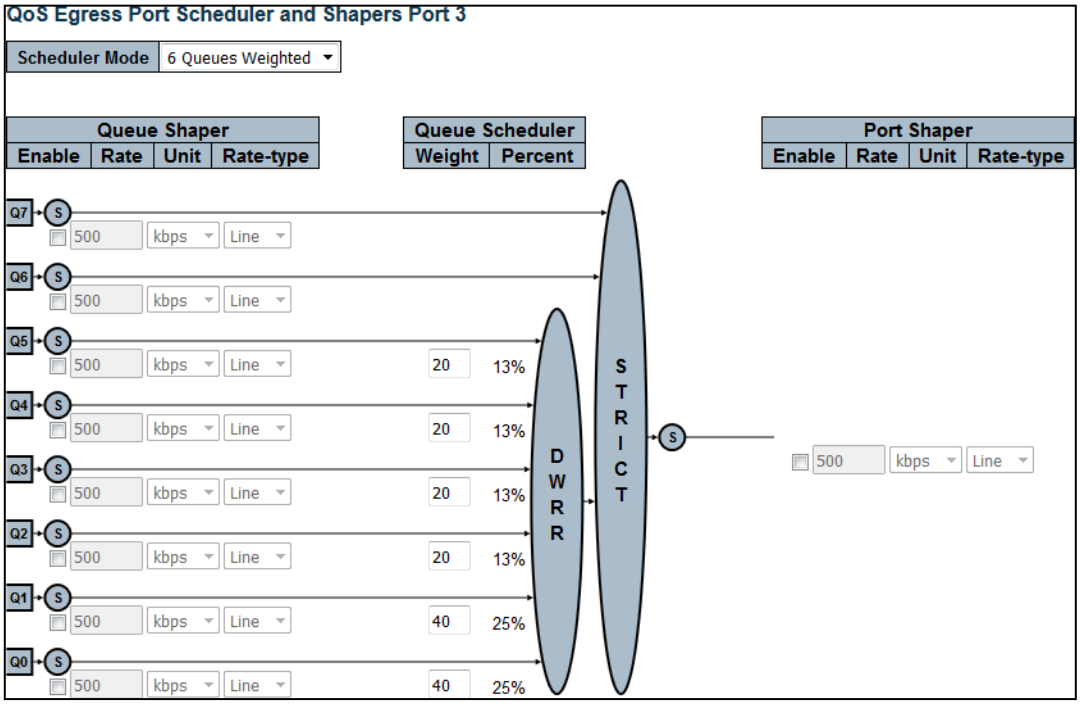
Example: Set the scheduling mode to DWRR (6 Queues Weighted) on Port 3 with the following weights: Queue0- 40, Queue1-40, Queue2-20, Queue3-20, Queue4-20, and Queue5-20.

Configuring Scheduling Mode to DWRR Using WebGUI

To configure Scheduling Mode to DWRR on Port 3 with the following weights: Queue0- 40, Queue1-40, Queue2-20, Queue3-20, Queue4-20, and Queue5-20, perform the following steps.

1. Click **Configuration** > **QoS** > **Port Shaping**.
2. On the **Port Shaping** page, click the **Port Number** corresponding to the port, and configure the **Queue Scheduler** as shown in the following illustration.

Set Up Scheduler Mode and Corresponding Queue Scheduler Weight



The equivalent ICLI commands are:

configure terminal
! Set Scheduler mode to DWRR Priority on Port 3 (config)# interface
GigabitEthernet 1/3
(config-if)# qos wrr 40 40 20 20 20 20 (config-if)# end

Weighted Random Early Detection (WRED)

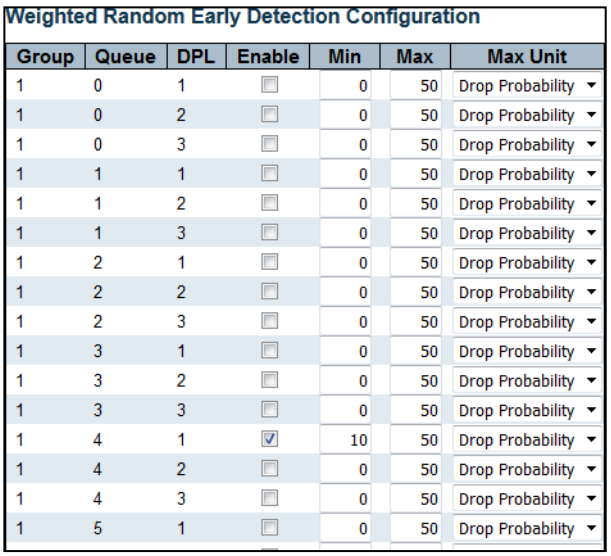
Example: Configure WRED on Group 1, Queue 4, and DPL 1 with a Minimum Threshold of 10% and Maximum Threshold of 50%. Maximum Threshold unit is Drop Probability.

Configuring WRED with Drop Probability Threshold Using WebGUI

To configure WRED on Group 1, Queue 4, and DPL 1 with a Minimum Threshold of 10% and Maximum Threshold of 50% (maximum Threshold unit is Drop Probability), perform the following step.

- Click **Configuration** > **QoS** > **WRED**, and configure WRED as shown in the following illustration.

Set Up WRED Group with Drop Probability Threshold



Weighted Random Early Detection Configuration

Group	Queue	DPL	Enable	Min	Max	Max Unit
1	0	1	☐	0	50	Drop Probability
1	0	2	☐	0	50	Drop Probability
1	0	3	☐	0	50	Drop Probability
1	1	1	☐	0	50	Drop Probability
1	1	2	☐	0	50	Drop Probability
1	1	3	☐	0	50	Drop Probability
1	2	1	☐	0	50	Drop Probability
1	2	2	☐	0	50	Drop Probability
1	2	3	☐	0	50	Drop Probability
1	3	1	☐	0	50	Drop Probability
1	3	2	☐	0	50	Drop Probability
1	3	3	☐	0	50	Drop Probability
1	4	1	☑	10	50	Drop Probability
1	4	2	☐	0	50	Drop Probability
1	4	3	☐	0	50	Drop Probability
1	5	1	☐	0	50	Drop Probability

The equivalent ICLI commands are:

configure terminal
!Set Minimum threshold as 10 and Maximum Threshold as 50 on Queue4. (config)# qos wred group 1 queue 4 dpl 1 min-fl 10 max 50

Note: Please note that ports are in WRED Group 1 by default. This is why further configuration is not necessary.

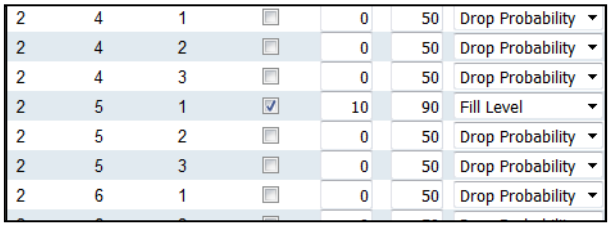
Example: Configure WRED on Group 2, Queue 5, DPL 1 with a Minimum Threshold of 10% and Maximum Threshold of 90%. Maximum Threshold unit is Fill Level. Assign Ports 1 and 2 to WRED Group 2.

Configuring WRED with Fill Level Threshold UsingWebGUI

To configure WRED on Group 2, Queue 5, DPL 1 with a Minimum Threshold of 10% and Maximum Threshold of 90% (maximum Threshold unit is Fill Level), perform the following steps.

1. Click **configuration** > **QoS** > **WRED**, and configure WRED as shown in the followingillustration.

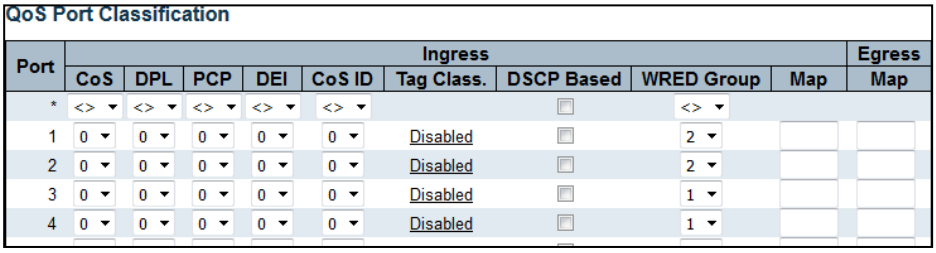
   Set Up WRED Group with Fill Level Threshold



2	4	1	☐	0	50	Drop Probability
2	4	2	☐	0	50	Drop Probability
2	4	3	☐	0	50	Drop Probability
2	5	1	☑	10	90	Fill Level
2	5	2	☐	0	50	Drop Probability
2	5	3	☐	0	50	Drop Probability
2	6	1	☐	0	50	Drop Probability

2. Click **Configuration** > **QoS** > **Port**, and configure Ports 1 and 2 to use WRED Group 2 as shown in the following illustration.

   Associate WRED Group with Port



QoS Port Classification

Port	Ingress								Egress
	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	WRED Group	Map
*	<>	<>	<>	<>	<>		☐	<>	
1	0	0	0	0	0	Disabled	☐	2	
2	0	0	0	0	0	Disabled	☐	2	
3	0	0	0	0	0	Disabled	☐	1	
4	0	0	0	0	0	Disabled	☐	1	

The equivalent ICLI commands are:

configure terminal
!Set Minimum threshold as 10 and Maximum Threshold as 90 on Queue5. (config)# qos wred group
2 queue 5 dpl 1 min-fl 10 max 90fill-level (config)# interface GigabitEthernet 1/1-2
(config-if)# qos wred-group 2

Storm Policing

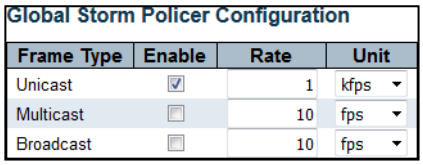
Example: Apply a global storm policer of 1 Kfps on a Unicast frame type.

Configuring Global Storm Policer (1 Kfps) UsingWebGUI

To configure a global storm policer of 1 Kfps on a Unicast frame type, perform the following step.

- Click **Configuration** > **QOS** > **Storm Policing**, and configure storm policer as shown in the following illustration.

Per System Unicast Storm Policing



Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast	☑	1	kfps
Multicast	☐	10	fps
Broadcast	☐	10	fps

The equivalent ICLI commands are:

configure terminal
(config)# qos storm unicast 1 kfps

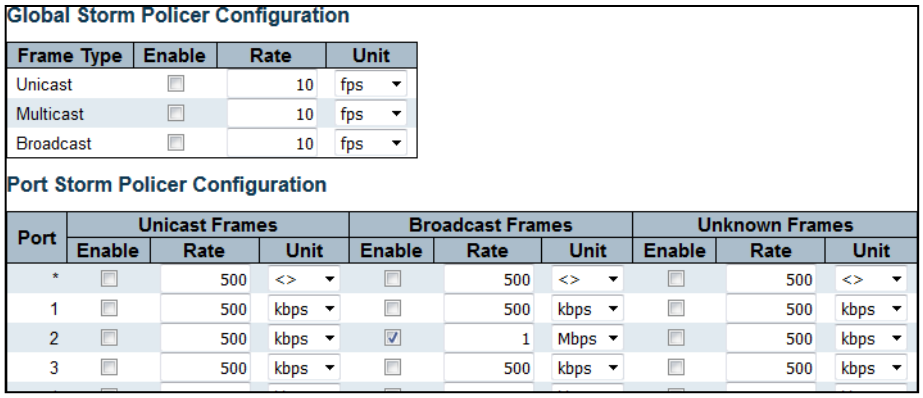
Example: Apply a port storm policer of 1 Mbps on Broadcast frames on Port 2.

Configuring Port Storm Policer (1 Mbps) UsingWebGUI

To configure storm policer of 1 Mbps on Broadcast frames on Port 2, perform the following step.

- Click **Configuration** > **QOS** > **Storm Policing**, and configure storm policer as shown in the following illustration.

Per Port Broadcast Storm Policing



Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast	☐	10	fps
Multicast	☐	10	fps
Broadcast	☐	10	fps

Port Storm Policer Configuration

Port	Unicast Frames			Broadcast Frames			Unknown Frames		
	Enable	Rate	Unit	Enable	Rate	Unit	Enable	Rate	Unit
*	☐	500	<>	☐	500	<>	☐	500	<>
1	☐	500	kbps	☐	500	kbps	☐	500	kbps
2	☐	500	kbps	☑	1	Mbps	☐	500	kbps
3	☐	500	kbps	☐	500	kbps	☐	500	kbps

The equivalent ICLI commands are:

configure terminal
(config)# interface GigabitEthernet 1/2 (config-if)# qos storm
broadcast 1mbps (config-if)# end

Ingress Map

Example: Create Ingress Map 20 with required properties.

Tagged frames with PCP 0-3 are mapped to CoS 0 and CoSID 0 (default mapping).
Tagged frames with PCP 4-7 are mapped to CoS 1 and CoSID 1.

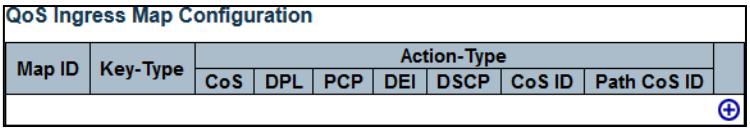
Configuring Ingress Map 20 Using WebGUI

To configure Ingress Map 20 with the following properties, perform the following steps.

- Tagged frames with PCP 0-3 are mapped to CoS 0 and CoSID 0 (default mapping).
- Tagged frames with PCP 4-7 are mapped to CoS 1 and CoSID 1.

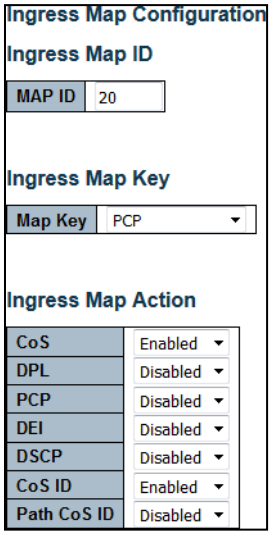
1. To create a new Ingress map, click **Configuration** > **QOS** > **Ingress Map**, and click the **Add New Map** icon.

   Create QoS Ingress Map Entry for PCP Key-Type



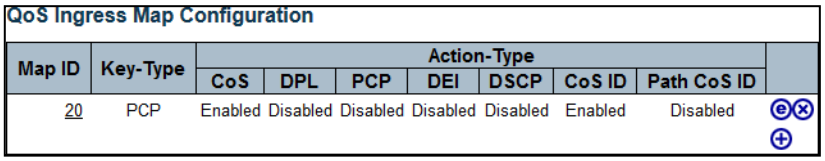
2. Enter the configuration details as shown in the following illustration.

   Set Up QoS Ingress Map with PCP Key-Type



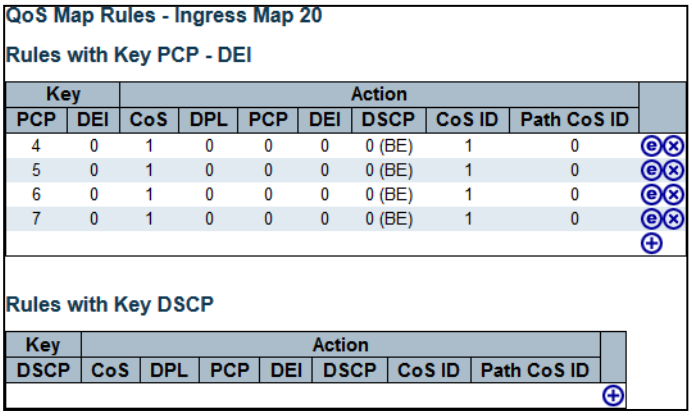
3. Click **Submit**.

   QoS Ingress Map PCP Key-Type Summary



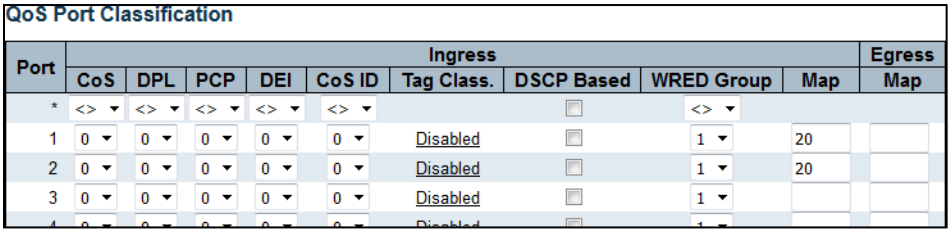
4. Under **Map ID**, click **20** and add these four entries (as shown in the illustration) by clicking the **Add New Map** icon.

Expand QoS Ingress Map PCP Entry and Rule Setup



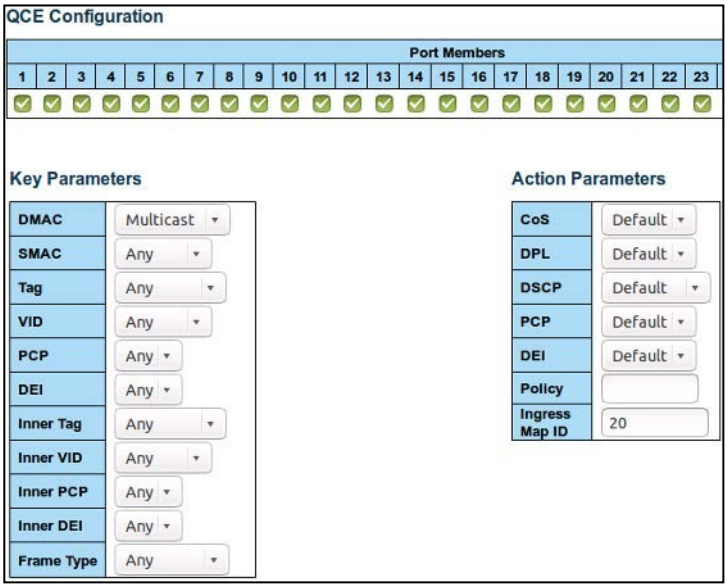
5. Associate Ports 1 and 2 with Ingress Map 20.

Associate PCP QoS Ingress Map with Port



6. Create a new QCE with ID 123 (for more information, see Advanced QoS: QCLs, page 14) that matches all packets from all ports where the destination MAC address is multicast; associate it with Ingress Map 20.

Associate PCP QoS Ingress Map with QCE



The equivalent ICLI commands are:

#configure terminal (config)# qos map ingress
20
(config-qos-map-ingress)# action cos class
(config-qos-map-ingress)# map pcp 4 to class 1 cos1

(config-qos-map-ingress)# map pcp 5 to class 1 cos1
(config-qos-map-ingress)# map pcp 6 to class 1 cos1

(config-qos-map-ingress)# map pcp 7 to class 1 cos 1
(config-qos-map-ingress)# end
!Associate port 1 and 2 with Ingress Map 20. # configure terminal
(config)# interface GigabitEthernet 1/1-2 (config-if)# qos
ingress-map 20
(config-if)# end
!Create a new QCE with ID 123 that matches all polackets from all ports where destination MAC address is multicast. Associate it with Ingress Map20.
configure terminal
(config)# qos qce 123 dmac multicast action ingress-map20 (config)# end

Example: Create Ingress Map 21 with the following properties:

- IP frames with DSCP 46 (Expedited Forwarding) are mapped to CoS 5 and CoSID 1.
- IP frames with all other DSCP values are mapped to CoS 0 and CoSID 0 (default mapping).

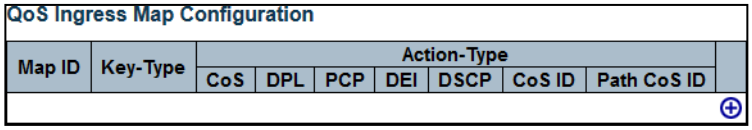
Configuring Ingress Map 21 Using WebGUI

To configure Ingress Map 21 with the following properties, perform the following steps.

- IP frames with DSCP 46 (expedited forwarding) are mapped to CoS 5 and CoSID 1.
- IP frames with all other DSCP values are mapped to CoS 0 and CoSID 0 (default mapping).

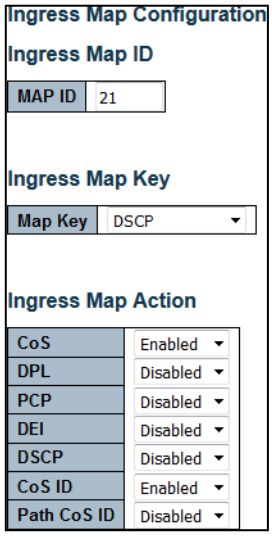
1. To create a new Ingress Map, click **Configuration** > **QOS** > **Ingress Map**, and click the **Add New Map** icon.

Create QoS Ingress Map Entry for DSCP Key-Type



2. Enter the configuration as shown in the following illustration.

Set up QoS Ingress Map with DSCP Key-Type



3. Click **Submit**.

QoS Ingress Map DSCP Key-Type Summary

QoS Ingress Map Configuration

Map ID	Key-Type	Action-Type						
		CoS	DPL	PCP	DEI	DSCP	CoS ID	Path CoS ID
21	DSCP	Enabled	Disabled	Disabled	Disabled	Disabled	Enabled	Disabled

4. Click the **Map ID 21** link and add these DSCP entries by clicking the **Add New Map** icon. Expand QoS Ingress Map DSCP Entry and Rule Setup

QoS Map Rules - Ingress Map 21

Rules with Key PCP - DEI

Key		Action						
PCP	DEI	CoS	DPL	PCP	DEI	DSCP	CoS ID	Path CoS ID

Rules with Key DSCP

Key	Action							
DSCP	CoS	DPL	PCP	DEI	DSCP	CoS ID	Path CoS ID	
46 (EF)	6	0	0	0	0 (BE)	1	0	

5. Associate Ports 3 and 4 with Ingress Map 21.

Associate DSCP QoS Ingress Map with Port

QoS Port Classification

Port	Ingress									Egress
	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	WRED Group	Map	Map
*	<>	<>	<>	<>	<>			<>		
1	0	0	0	0	0	Disabled		1		
2	0	0	0	0	0	Disabled		1		
3	0	0	0	0	0	Disabled		1	21	
4	0	0	0	0	0	Disabled		1	21	

The equivalent ICLI commands are:

#configure terminal. (config)# qos map ingress 21
(config-qos-map-ingress)# key dscp
(config-qos-map-ingress)# action cos class
(config-qos-map-ingress)# map dscp 46 to class 1 cos5 (config-qos-map-ingress)#
end
!Associate port 3 and 4 with Ingress Map 21. # configure terminal
(config)# interface GigabitEthernet 1/3-4 (config-if)# qos
ingress-map 21
(config-if)# end

Egress Map

Example: Create Egress Map 40 with the required properties:

- Set PCP to 7 and DSCP to 46 on frames classified to CoSID 1.
- Set PCP and DSCP to 0 on frames classified to all other CoSID values (defaultmapping).
-

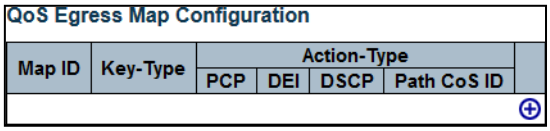
Configuring Egress Map 40 Using WebGUI

To configure Egress Map 40 with the following properties, perform the following steps.

- Set PCP to 7 and DSCP to 46 on frames classified to CoSID 1.
- Set PCP and DSCP to 0 on frames classified to all other CoSID values (default mapping).

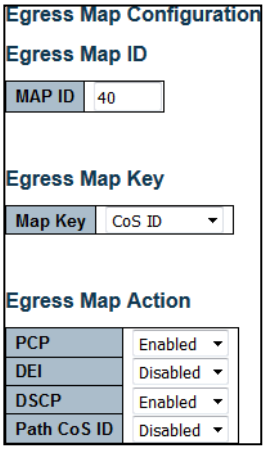
1. To create a new Egress Map, click **Configuration** > **QOS** > **Egress Map**, and click the **Add New Map** icon.

   Create QoS Egress Map Entry



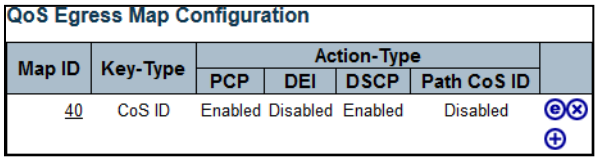
2. Enter the configuration as shown in the following illustration.

   Set Up QoS Egress Map with CoSID Key-Type



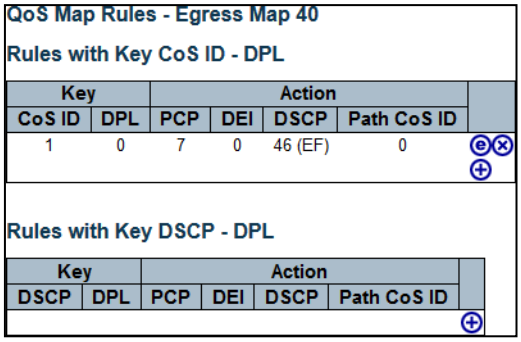
3. Click **Submit**.

   QoS Egress Map CoSID Key-Type Summary



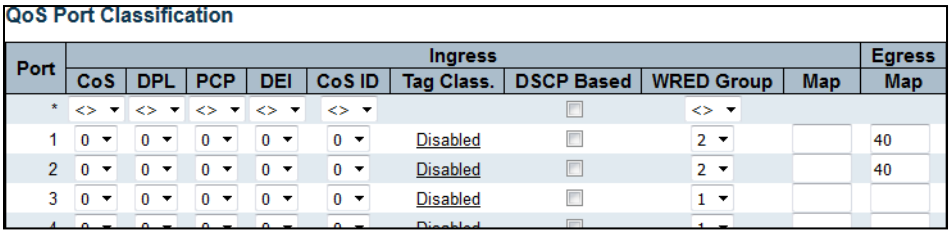
4. Click the **Map ID 40** link and add a single entry in the **CoS ID** table by clicking the **Add New Map** icon.

• Expand QoS Egress Map CoSID Entry and Rule Setup



5. Associate Ports 1 and 2 with Egress Map 40.

- **Associate CoSID QoS Egress Map with Port**


QoS Port Classification

Port	Ingress								Egress
	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	WRED Group	Map
*	<>	<>	<>	<>	<>			<>	
1	0	0	0	0	0	Disabled		2	40
2	0	0	0	0	0	Disabled		2	40
3	0	0	0	0	0	Disabled		1	

The equivalent ICLI commands are:

#Configure terminal (config)# qos map egress
40
(config-qos-map-ingress)# action dscp pcp
(config-qos-map-ingress)# map class 1 to dscp 46 pcp7
(config-qos-map-ingress)# end
!Associate port 1 and 2 with Egress Map 40. # configure terminal
(config)# interface GigabitEthernet 1/1-2 (config-if)# qos
egress-map 40
(config-if)# end

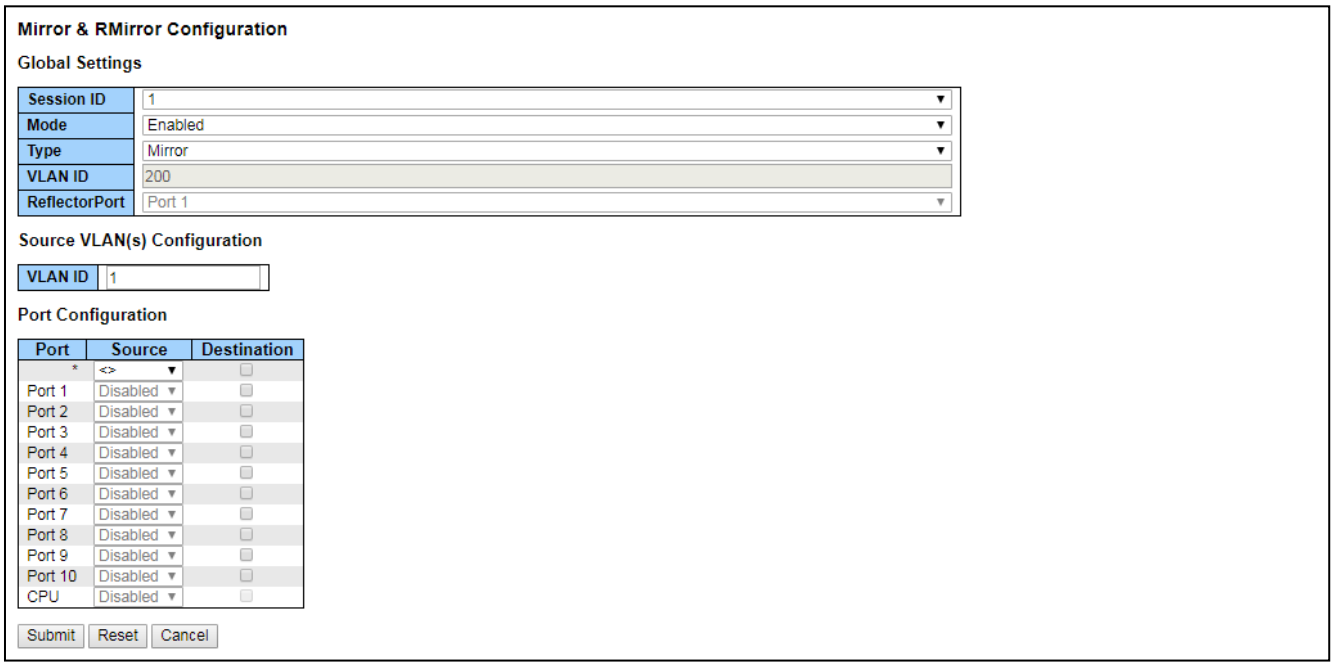
3.1.15 MIRRORING

Mirror & RMirror Configuration Table

Session ID	Mode	Type	VLAN ID	Reflector Port
1	Enabled	Mirror	-	-

Mirroring is a feature for switched port analyzer. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic. Remote Mirroring is an extend function of Mirroring. It can extend the destination port in other switch. So the administrator can analyze the network traffic on the other switches.

If you want to get the tagged mirrored traffic, you have to set VLAN egress tagging as "Tag All" on the reflector port. On the other hand, if you want to get untagged mirrored traffic, you have to set VLAN egress tagging as "Untag ALL" on the reflector port.



Session

Select session id to configure.

Mode

To **Enabled/Disabled** the mirror or Remote Mirroring function.

Type

Select switch type.

Mirror

The switch is running on mirror mode.
The source port(s) and destination port are located on this switch.

RMirror Source

The switch is a source node for monitor flow.
The source port(s), reflector port are located on this switch.

RMirror destination

The switch is an end node for monitor flow.

The destination port(s) is located on this switch.

VLAN ID

The VLAN ID points out where the monitor packet will copy to. The default VLAN ID is 200.

Reflector Port

The **reflector port** is a method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until the Remote Mirroring is disabled.
In the stacking mode, you need to select switch ID to select the correct device.
If you shut down a port, it cannot be a candidate for **reflector port**.
If you shut down the port which is a **reflector port**, the remote mirror function cannot work.

Note1: The reflector port needs to select only on Sourceswitch type.
Note2: The reflector port needs to disable MAC Table learning and STP.
Note3: The reflector port only supports on pure copper ports.

Source VLAN(s) Configuration

The switch can support VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field.
Note1: The Mirroring session shall have either ports or VLANs as sources, but not both.

Remote Mirroring Port Configuration

The following table is used for port role selecting.

Port

The logical port for the settings contained in the same row.

Source

Select mirror mode.
Disabled Neither frames transmitted nor frames received are mirrored.
Both Frames received and frames transmitted are mirrored on the **Destination port**.
Rx only Frames received on this port are mirrored on the **Destination port**. Frames transmitted are not mirrored.
Tx only Frames transmitted on this port are mirrored on the **Destination port**. Frames received are not mirrored.

Destination

Select destination port.
This checkbox is designed for mirror or Remote Mirroring.
The **destination port** is a switched port that you receive a copy of traffic from the source port.

Note1: On mirror mode, the device only supports one destination port.
Note2: The destination port needs to disable MAC Table learning.

Configuration Guideline for All Features

When the switch is running on Remote Mirroring mode, the administrator also needs to check whether or not other features are enabled or disabled.

For example, the administrator is not disabled the MSTP on reflector port. All monitor traffic will be blocked on reflector port. All recommended settings are described as follows.

	Impact	source port	reflector port	intermediate port	destination port	Remote Mirroring VLAN
arp_inspection	High		* disabled	* disabled		
acl	Critical		* disabled	* disabled	* disabled	
dhcp_relay	High		* disabled	* disabled		
dhcp_snooping	High		* disabled	* disabled		
ip_source_guard	Critical		* disabled	* disabled	* disabled	
ipmc/igmpsnp	Critical					un-conflict
ipmc/mldsnp	Critical					un-conflict
lacp	Low				o disabled	
lldp	Low				o disabled	
mac learning	Critical		* disabled	* disabled	* disabled	
mstp	Critical		* disabled		o disabled	
mvr	Critical					un-conflict
nas	Critical		* authorized	* authorized	* authorized	
psec	Critical		* disabled	* disabled	* disabled	
qos	Critical		* unlimited	* unlimited	* unlimited	
upnp	Low				o disabled	
mac-based vlan	Critical		* disabled	* disabled		
protocol-based vlan	Critical		* disabled	* disabled		
vlan_translation	Critical		* disabled	* disabled	* disabled	
voice_vlan	Critical		* disabled	* disabled		
mrp	Low				o disabled	
mvrp	Low				o disabled	

Note:

* -- must

o – optional

Impact: Critical/High/Low

Critical - 5 packets -> 0 packet

High - 5 packets -> 4 packets

Low - 5 packets -> 6 packets

Buttons

Submit: Click to submit changes.

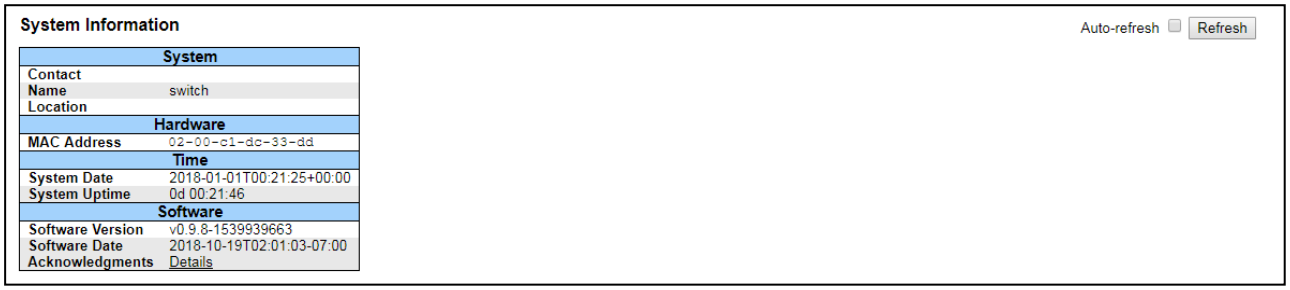
Reset: Click to undo any changes made locally and revert to previously saved values.

3.2 MONITOR

3.2.1 SYSTEM

INFORMATION

Port Settings section allows users to enable or disable each port function; state the speed/duplex of each port; and enable or disable the flow control of the port.



The switch system information is provided here.

Contact

The system contact configured in Configuration | System | Information | System Contact.

Name

The system name configured in Configuration | System | Information | System Name.

Location

The system location configured in Configuration | System | Information | System Location.

MAC Address

The MAC Address of this switch.

Chip ID

System Date

The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.

System Uptime

The period of time the device has been operational.

Software Version

The software version of this switch.

Software Date

The date when the switch software was produced.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

LED STATUS



The switch system LED status is provided here.

Clear Type

The types of system LED status clearing. Possible values are:

All: Clear all error status of the system LED and back to normal indication.

Fatal: Clear fatal error status of the system LED.

Software: Clear generic software error status of the system LED.

Description

The description of system LED.

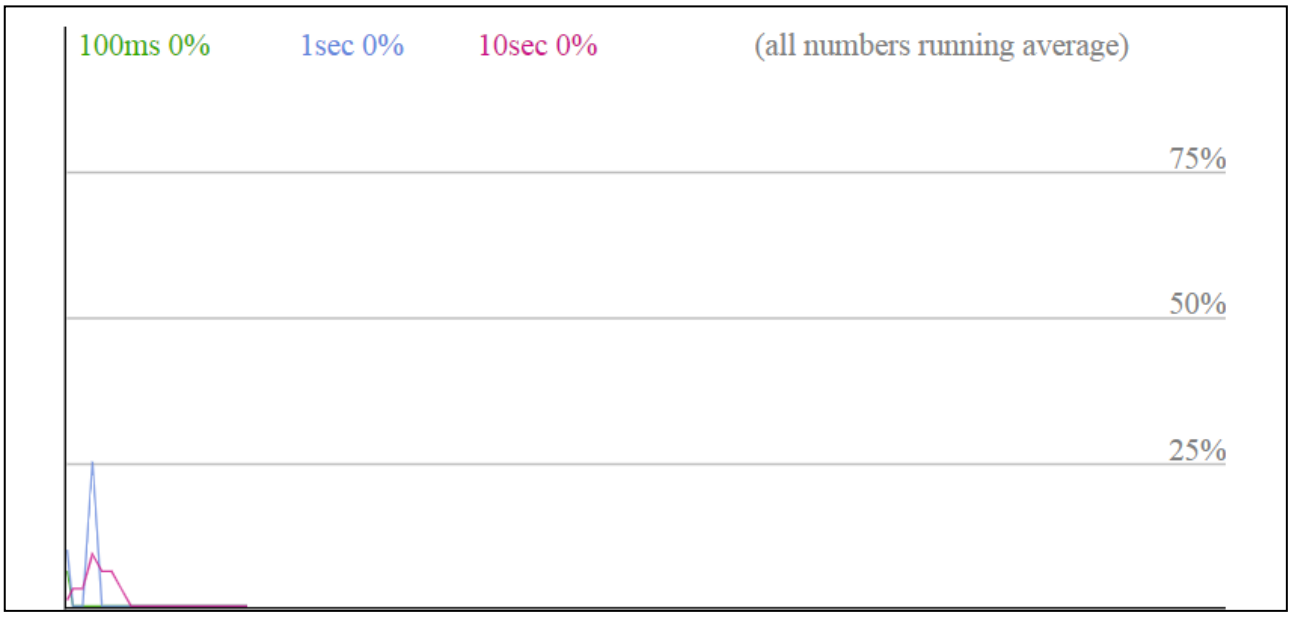
Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every second.

Refresh: Click to refresh the page.

Clear: Clear the selected error status of system LED.

CPU LOAD



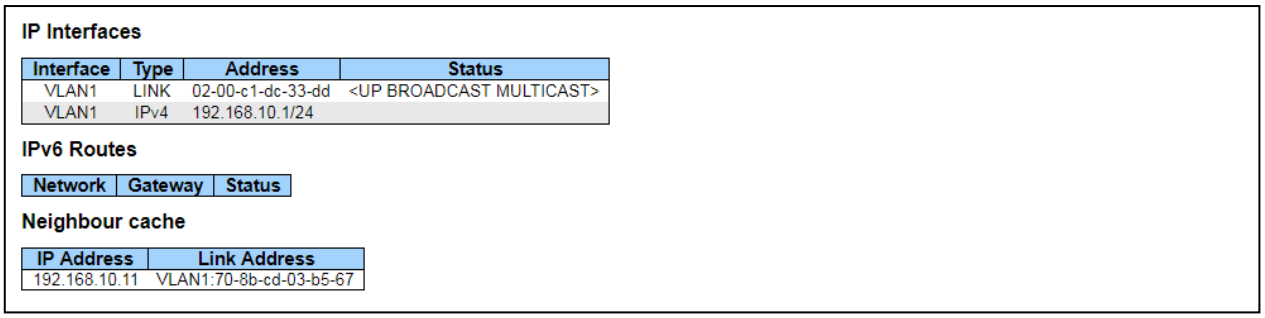
This page displays the CPU load, using an SVG graph. The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well. In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more

information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

IP STATUS



This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IPv6 routes and the neighbor cache (ARP cache) status.

IP Interfaces

Interface

The name of the interface.

Type

The address type of the entry. This may be **LINK** or **IPv4**.

Address

The current address of the interface (of the given type).

Status

The status flags of the interface (and/or address).

IPv6 Routes

Network

The destination IPv6 network or host address of this route.

Gateway

The gateway address of this route.

Status

The status flags of the route.

Neighbor cache

IP Address

The IP address of the entry.

Link Address

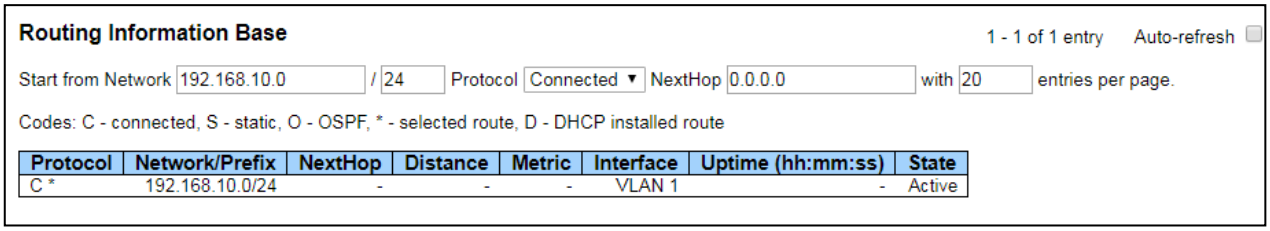
The Link (MAC) address for which a binding to the IP address given exist.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every second.

ROUTING INFORMATION BASE



This is IPv4 route entry table. It is used to provide the route entries status information.

Navigating the Routing Information Base Table

Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table.

The "Start from ID" input field allow the user to change the starting point in this table. Clicking the Refresh button will update the displayed table starting from that or the closest next entry match.

In addition, these input fields will upon a **|<<** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Protocol

The protocol of the route.

DHCP: The route is created by DHCP.

Connected: The destination network is connected directly.

Static: The route is created by user.

OSPF: The route is created by OSPF.

Network/Prefix

Network and prefix (example 10.0.0.0/16) of the given route entry.

NextHop

The IP address of nexthop. Value '0.0.0.0' indicates the link is directly connected.

Distance

The distance of the route.

Metric

The metric of the route.

Interface

The interface where the ip packet is outgoing.

Uptime (hh:ss:mm)

The time till the route is created. The unit is second.

State

Indicate if the destination network is reachable or not.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

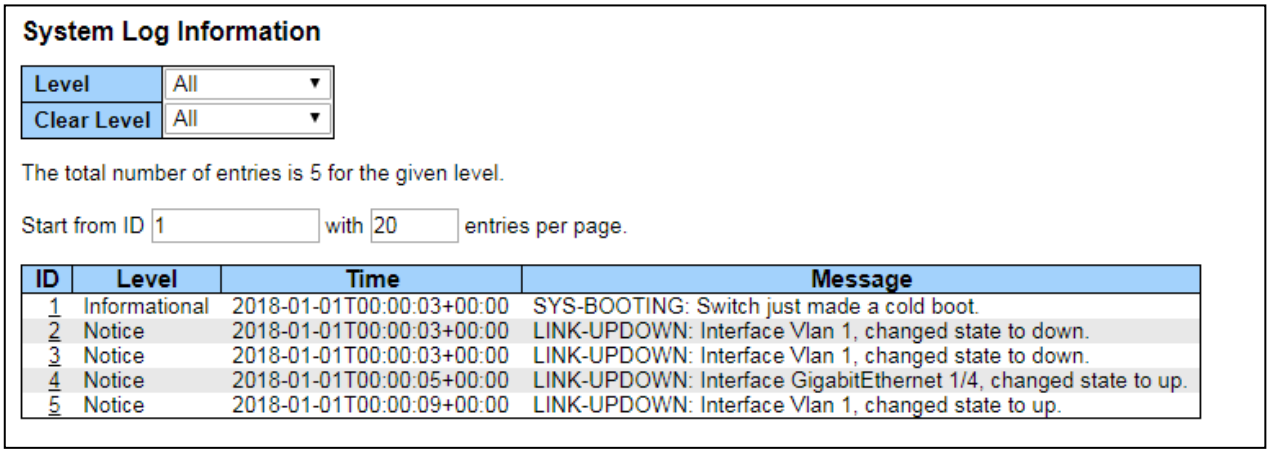
|<<: Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled

<<: Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

>>: Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>>|: Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

LOG



The switch system log information is provided here.

Navigating the System Log Information Table

Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table.

The "Level" input field is used to filter the display system log entries.
The "Clear Level" input field is used to specify which system log entries will be cleared.
To clear specific system log entries, select the clear level first then click the Clear button.

The "Start from ID" input field allow the user to change the starting point in this table. Clicking the Refresh button will update the displayed table starting from that or the closest next entry match.
In addition, these input fields will upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

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

System Log Information Entry Columns

ID

The identification of the system log entry.

Level

The level of the system log entry. **Info**: The system log entry is belonged information level.
Warning: The system log entry is belonged warning level.
Error: The system log entry is belonged error level.

Time

The occurred time of the system log entry.

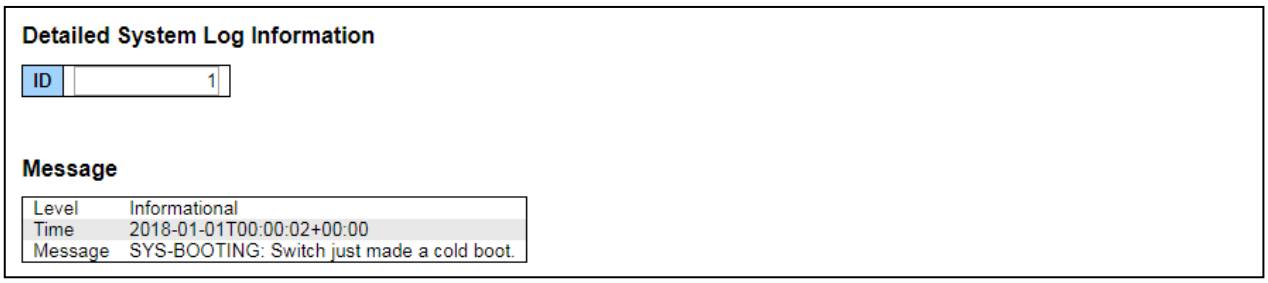
Message

The detail message of the system log entry.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Updates the table entries, starting from the current entry.
Clear: Flushes the selected entries.
|<<: Updates the table entries, starting from the first available entry.
<<: Updates the table entries, ending at the last entry currently displayed.
>>: Updates the table entries, starting from the last entry currently displayed.
>>|: Updates the table entries, ending at the last available entry.

DETAIL SYSTEM LOG INFORMATION



The switch system detailed log information is provided here.

Level

The severity level of the system log entry.

ID

The ID (>= 1) of the system log entry.

Message

The detailed message of the system log entry.

Buttons

Refresh: Updates the system log entry to the current entry ID.

|<<: Updates the system log entry to the first available entry ID.

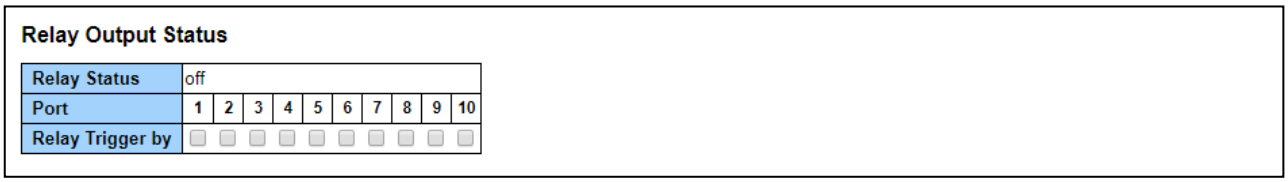
<<: Updates the system log entry to the previous available entry ID.

>>: Updates the system log entry to the next available entry ID.

>>|: Updates the system log entry to the last available entry ID.

RELAY OUTPUT STATUS

This page displays the relay output status the ports of the switch.



Relay status

The switch relay status.

Port

The switch port number of the logical port.

Relay Trigger by

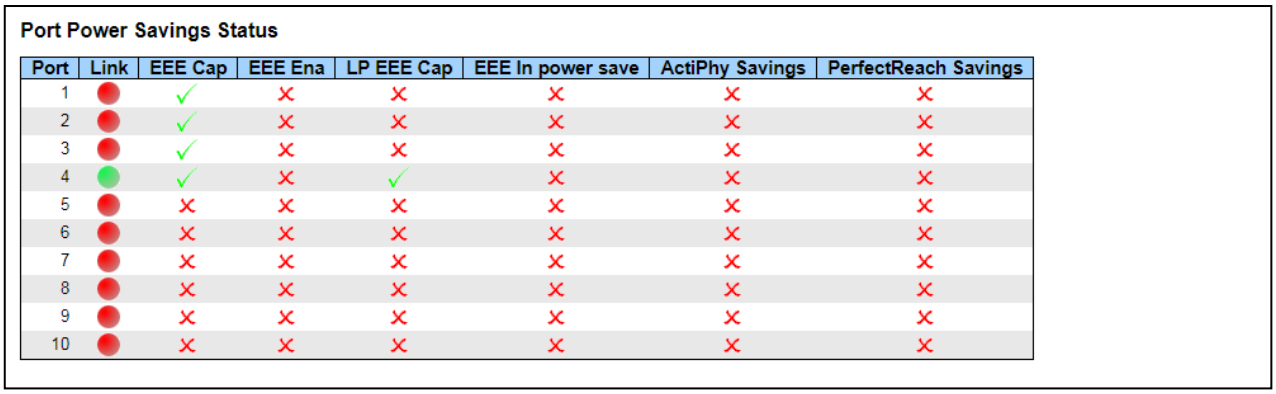
The currently relay status "on" trigger by which ports.

Buttons

Refresh: Click to refresh the page immediately.

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

3.2.2 GREEN ETHERNET



This page provides the current status for EEE.

Local Port

This is the logical port number for this row.

Link

Shows if the link is up for the port (green = link up, red = link down).

EEE cap

Shows if the port is EEE capable.

EEE Enable

Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).

LP EEE cap

Shows if the link partner is EEE capable.

EEE In power save

Shows if the system is currently saving power due to EEE. When EEE is enabled, the system will powered down if no frame has been received or transmitted in 5 uSec.

Actiphy Savings

Shows if the system is currently saving power due to ActiPhy.

PerfectReach Savings

Shows if the system is currently saving power due to PerfectReach.

3.2.3 THERMAL PROTECTION

Thermal Protection Status

Thermal Protection Port Status

Port	Temperature		Port status
1	55	°C	Port link operating normally
2	55	°C	Port link operating normally
3	55	°C	Port link operating normally
4	55	°C	Port link operating normally
5	0	°C	Port link operating normally
6	0	°C	Port link operating normally
7	0	°C	Port link operating normally
8	0	°C	Port link operating normally
9	0	°C	Port link operating normally
10	0	°C	Port link operating normally

This page allows the user to inspect status information related to thermal protection.

Port

The switch port number.

Temperature

Shows the current chip temperature in degrees Celsius.

Port Status

Shows if the port is thermally protected (link is down) or if the port is operating normally.

3.2.4 PORTS

STATE

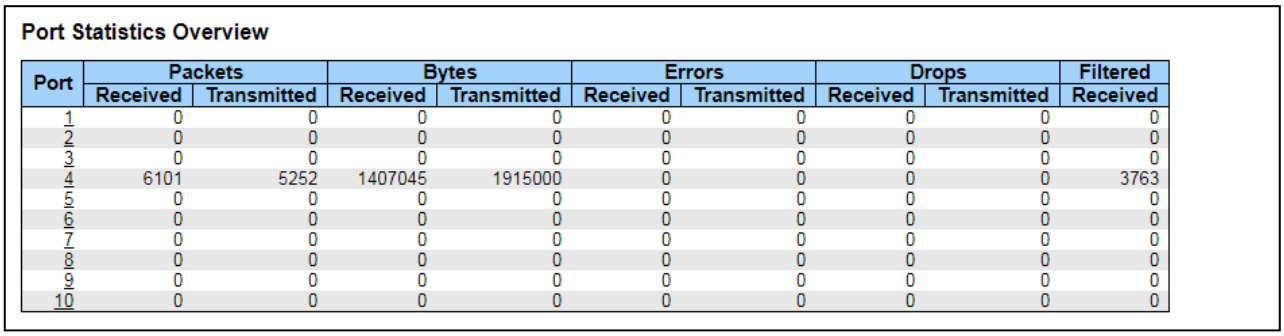


This page provides an overview of the current switch port states.

The port states are illustrated as follows:

RJ45 ports			
SFP ports			
State	Disabled	Down	Link

PORT STATISTICS OVERVIEW



Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	6101	5252	1407045	1915000	0	0	0	0	3763
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0

This page provides an overview of general traffic statistics for all switch ports. The displayed counters are:

Port

The logical port for the settings contained in the same row.

Packets

The number of received and transmitted packets per port.

Bytes

The number of received and transmitted bytes per port.

Errors

The number of frames received in error and the number of incomplete transmissions per port.

Drops

The number of frames discarded due to ingress or egress congestion.

Filtered

The number of received frames filtered by the forwarding process.

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

QoS STATISTICS

Queuing Counters

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	6240	2910	0	0	0	0	0	0	0	0	0	0	0	0	0	2491
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

This page provides statistics for the different queues for all switch ports. The displayed counters are:

Port

The logical port for the settings contained in the same row.

Qn

There are 8 QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx

The number of received and transmitted packets per queue.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

QoS Control List (QCL)

QoS Control List Status

Combined ▾ Auto-refresh ☐ Resolve Conflict

User	QCE	Port	Frame Type	Action						Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	
No entries										

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is **1024** on each switch.

User

Indicates the QCL user.

QCE

Indicates the QCE id.

Port

Indicates the list of ports configured with the QCE.

Frame Type

Indicates the type of frame. Possible values are:

Any: Match any frame type.

Ethernet: Match EtherType frames.

LLC: Match (LLC) frames.

SNAP: Match (SNAP) frames.

IPv4: Match IPv4 frames.

IPv6: Match IPv6 frames.

Action

Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.

Possible actions are:

CoS: Classify Class of Service.

DPL: Classify Drop Precedence Level.

DSCP: Classify DSCP value.

PCP: Classify PCP value.

DEI: Classify DEI value.

Policy: Classify ACL Policy number.

Conflict

Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

Buttons

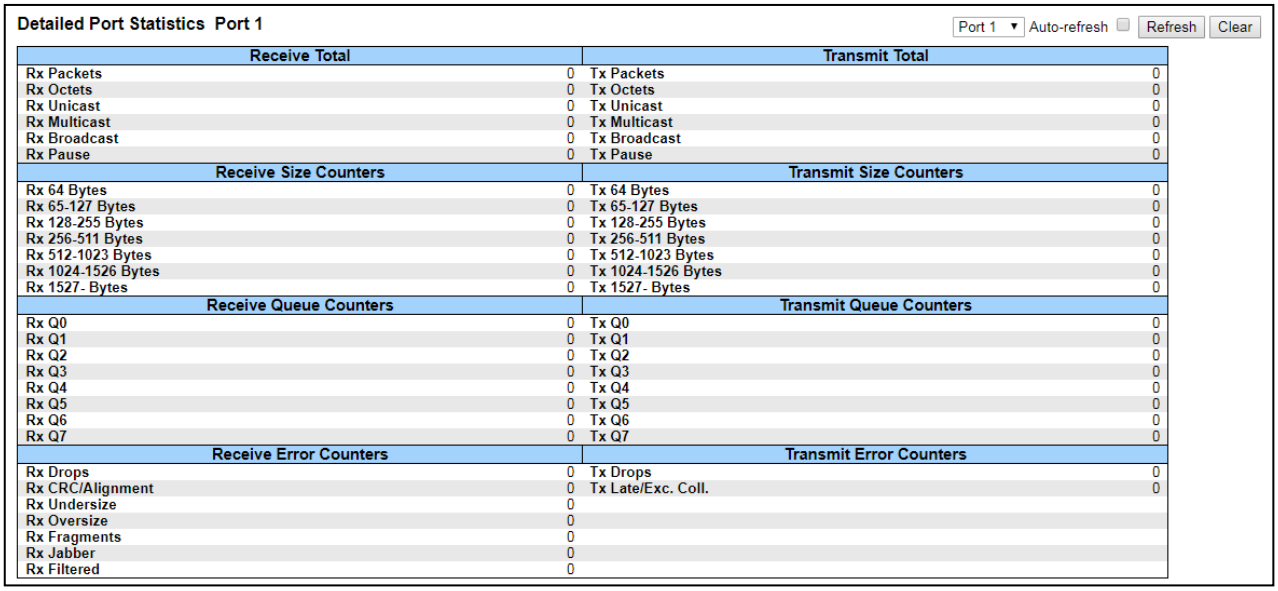
Combined, Static, Voice VLAN, and Conflict: Select the QCL status from this drop down list.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Resolve Conflict: Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.

Refresh: Click to refresh the page.

DETAILED STATISTICS



This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Receive Total and Transmit Total

Rx and Tx Packets

The number of received and transmitted (good and bad) packets.

Rx and Tx Octets

The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

Rx and Tx Unicast

The number of received and transmitted (good and bad) unicast packets.

Rx and Tx Multicast

The number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast

The number of received and transmitted (good and bad) broadcast packets.

Rx and Tx Pause

A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

The number of received and transmitted packets per input and output queue.

Receive Error Counters

Rx Drops

The number of frames dropped due to lack of receive buffers or egress congestion.

Rx CRC/Alignment

The number of frames received with CRC or alignment errors.

Rx Undersize

The number of short [1] frames received with valid CRC.

Rx Oversize

The number of long [2] frames received with valid CRC.

Rx Fragments

The number of short [1] frames received with invalid CRC.

Rx Jabber

The number of long [2] frames received with invalid CRC.

Rx Filtered

The number of received frames filtered by the forwarding process.

[1] Short frames are frames that are smaller than 64 bytes.

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

Transmit Error Counters

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.

Buttons

The port select box determines which port is affected by clicking the buttons.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

3.2.5 SECURITY

ACCESS MANAGEMENT STATISTICS

Access Management Statistics

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0

This page provides statistics for access management.

Interface

The interface type through which the remote host can access the switch.

Received Packets

Number of received packets from the interface when access management mode is enabled.

Allowed Packets

Number of allowed packets from the interface when access management mode is enabled.

Discarded Packets

Number of discarded packets from the interface when access management mode is enabled.

Buttons

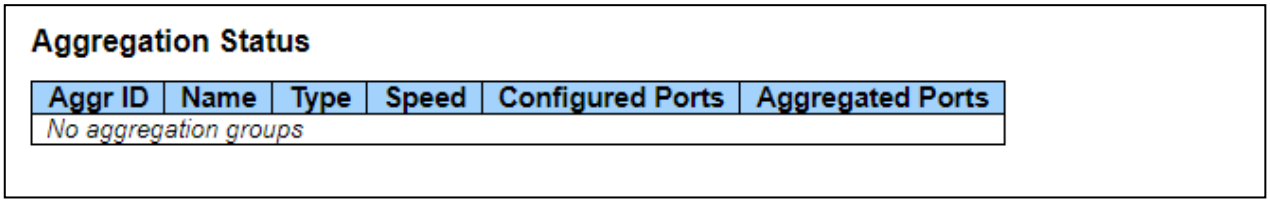
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear All: Clear all statistics.

3.2.6 AGGREGATION

This page is used to see the status of ports in Aggregation group.



Aggregation Group Status

Aggr ID

The Aggregation ID associated with this aggregation instance.

Name

Name of the Aggregation group ID.

Type

Type of the Aggregation group(Static or LACP).

Speed

Speed of the Aggregation group.

Configured ports

Configured member ports of the Aggregation group.

Aggregated ports

Aggregated member ports of the Aggregation group.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Automatic refresh occurs every 3 seconds.

3.2.7 LOOP PROTECTION

Loop Protection Status

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

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

Port

The switch port number of the logical port.

Action

The currently configured port action.

Transmit

The currently configured port transmit mode.

Loops

The number of loops detected on this port.

Status

The current loop protection status of the port.

Loop

Whether a loop is currently detected on the port.

Time of Last Loop

The time of the last loop event detected.

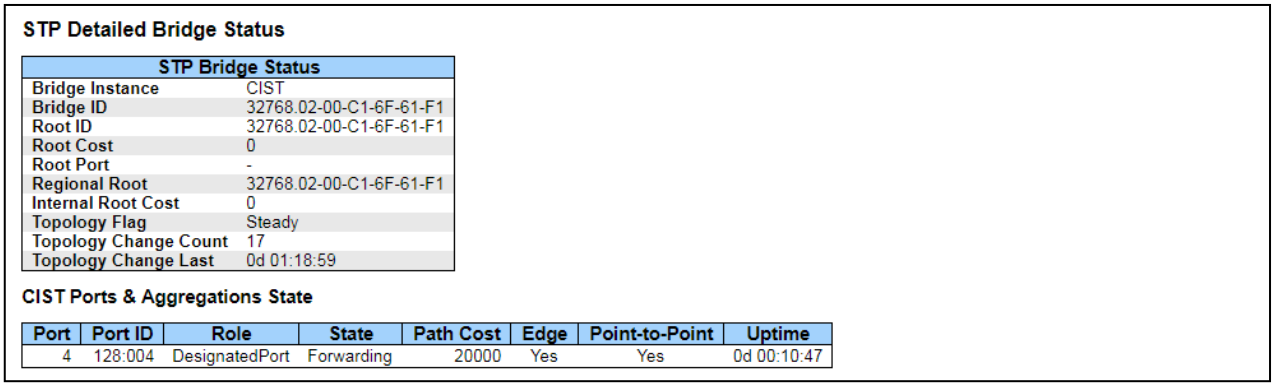
Buttons

Refresh: Click to refresh the page immediately.

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

3.2.8 SPANNING TREE

Bridge Status



STP Detailed Bridge Status

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.02-00-C1-6F-61-F1
Root ID	32768.02-00-C1-6F-61-F1
Root Cost	0
Root Port	-
Regional Root	32768.02-00-C1-6F-61-F1
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	17
Topology Change Last	0d 01:18:59

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
4	128:004	DesignatedPort	Forwarding	20000	Yes	Yes	0d 00:10:47

This page provides detailed information on a single STP bridge instance, along with port state for all active ports associated. The page contains two tables with the following information:

STP Bridge Status

Bridge Instance

The Bridge instance - **CIST**, **MST1**, ...

Bridge ID

The Bridge ID of this Bridge instance.

Root ID

The Bridge ID of the currently elected root bridge.

Root Port

The switch port currently assigned the *root* port role.

Root Cost

Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Regional Root

The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. *(For the CIST instance only)*.

Internal Root Cost

The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. *(For the CIST instance only)*.

Topology Flag

The current state of the Topology Change Flag of this Bridge instance.

Topology Change Count

The number of times where the topology change flag has been set (during a one-second interval).

Topology Change Last

The time passed since the Topology Flag was last set.

CIST Ports & Aggregations State

Port

The switch port number of the logical STP port.

Port ID

The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.

Role

The current STP port role. The port role can be one of the following values: **AlternatePort** **BackupPortRootPort** **DesignatedPort**.

State

The current STP port state. The port state can be one of the following values: **Discarding** **LearningForwarding**.

Path Cost

The current STP port path cost. This will either be a value computed from the **Auto** setting, or any explicitly configured value.

Edge

The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.

Point-to-Point

The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.

Uptime

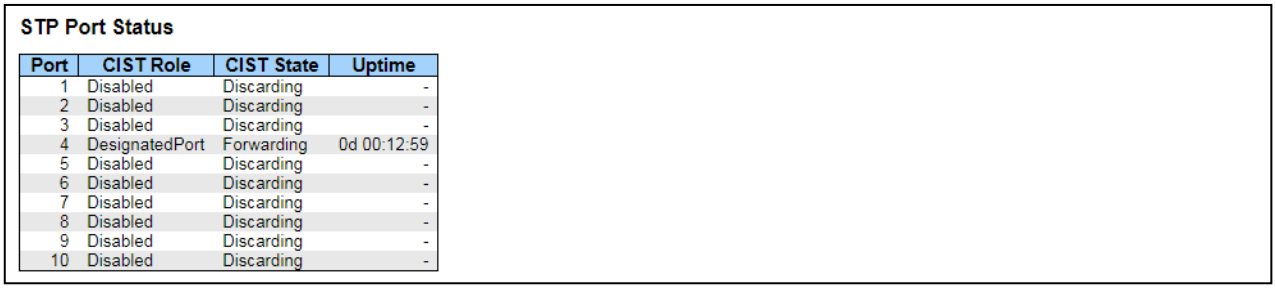
The time since the bridge port was last initialized.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Port Status



STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	DesignatedPort	Forwarding	0d 00:12:59
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	Disabled	Discarding	-

This page displays the STP CIST port status for physical ports of the switch.

Port

The switch port number of the logical STP port.

CIST Role

The current STP port role of the CIST port. The port role can be one of the following values: **AlternatePortBackupPort** **RootPort** **DesignatedPortDisabled**.

CIST State

The current STP port state of the CIST port. The port state can be one of the following values: **DiscardingLearning** **Forwarding**.

Uptime

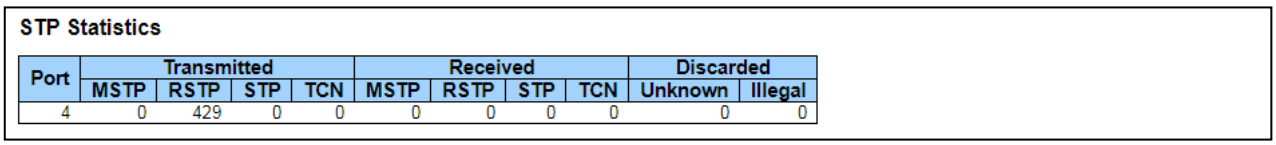
The time since the bridge port was last initialized.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Port Statistics



STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
4	0	429	0	0	0	0	0	0	0	0

This page displays the STP port statistics counters of bridge ports in the switch. The STP port statistics counters are:

Port

The switch port number of the logical STP port.

MSTP

The number of MSTP BPDU's received/transmitted on the port.

RSTP

The number of RSTP BPDU's received/transmitted on the port.

STP

The number of legacy STP Configuration BPDU's received/transmitted on the port.

TCN

The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.

Discarded Unknown

The number of unknown Spanning Tree BPDU's received (and discarded) on the port.

Discarded Illegal

The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Buttons

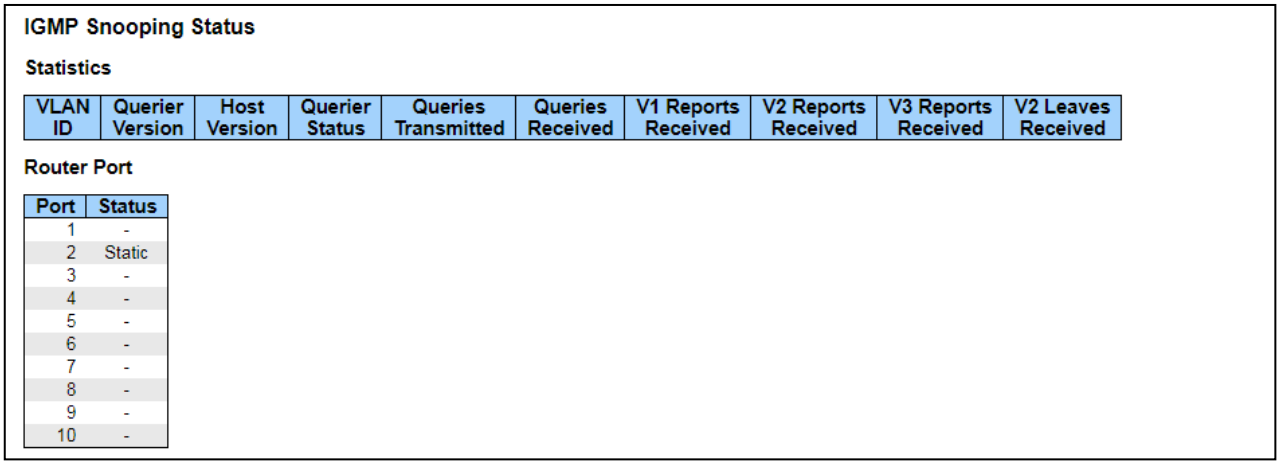
Refresh: Click to refresh the page immediately.

Clear: Click to reset the counters.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

3.2.9 IPMC

IGMP Snooping Status



IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received

Router Port

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

This page provides IGMP Snooping status.

VLAN ID

The VLAN ID of the entry.

Querier Version

Working Querier Version currently.

Host Version

Working Host Version currently.

Querier Status

Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted

The number of Transmitted Queries.

Queries Received

The number of Received Queries.

V1 Reports Received

The number of Received V1 Reports.

V2 Reports Received

The number of Received V2 Reports.

V3 Reports Received

The number of Received V3 Reports.

V2 Leaves Received

The number of Received V2 Leaves.

Router Port

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both denote the specific port is configured or learnt to be a router port.

Port

Switch port number.

Status

Indicate whether specific port is a router port or not.

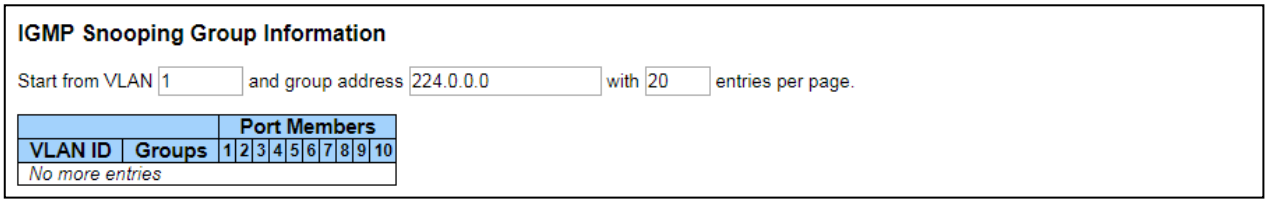
Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears all Statistics counters.

Group Information



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

Navigating the IGMP Group Table

Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

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

The will use the last entry of the currently displayed table 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 Group Table Columns

VLAN ID

VLAN ID of the group.

Groups

Group address of the group displayed.

Port Members

Ports under this group.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the input fields.

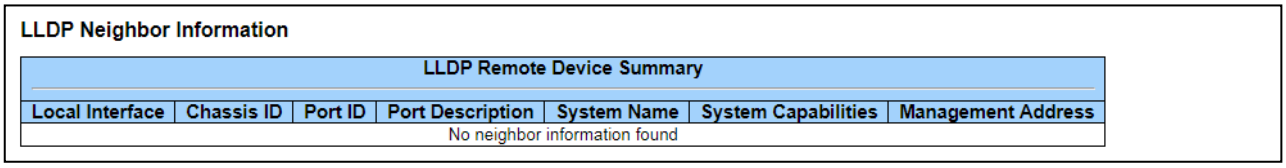
|<<: Updates the table, starting with the first entry in the IGMP Group Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

3.2.10 LLDP

LLDP is an IEEE 802.1ab standard protocol. The **L**ink **L**ayer **D**iscovery **P**rotocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

Neighbors


LLDP Neighbor Information

LLDP Remote Device Summary

Local Interface	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
No neighbor information found						

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

Local Interface

The interface on which the LLDP frame was received.

Chassis ID

The **Chassis ID** is the identification of the neighbor's LLDP frames.

Port ID

The **Port ID** is the identification of the neighbor port.

Port Description

Port Description is the port description advertised by the neighbor unit.

System Name

System Name is the name advertised by the neighbor unit.

System Capabilities

System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:

1. Other
2. Repeater
3. Bridge
4. WLAN Access Point
5. Router
6. Telephone
7. DOCSIS cable device
8. Station only
9. Reserved

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

Management Address

Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

EEE

LLDP Neighbors EEE Information

Local Interface	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
GigabitEthernet 1/4	EEE not enabled for this interface							

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange information about their respective tx

and rx "wakeup time ", as a way to agree upon the minimum wakeup time they need.

This page provides an overview of EEE information exchanged by LLDP.

LLDP Neighbors EEE Information

The displayed table contains a row for each interface.

If the interface does not support EEE, then it displays as "EEE not supported for this interface".

If EEE is not enabled on particular interface, then it displays as "EEE not enabled for this interface".

If the link partner doesn't support EEE, then it displays as "Link partner is not EEE capable.

The columns hold the following information:

Local Interface

The interface at which LLDP frames are received or transmitted.

Tx Tw

The link partner's maximum time that transmit path can hold-off sending data after deassertion of LPI.

Rx Tw

The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.

Fallback Receive Tw

The link partner's fallback receives Tw. A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.

Echo Tx Tw

The link partner's Echo Tx Tw value. The respective echo values shall be defined as the local link partner reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.

Echo Rx Tw

The link partner's Echo Rx Tw value.

Resolved Tx Tw

The resolved Tx Tw for this link. **Note:** NOT the link partner

The resolved value that is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).

Resolved Rx Tw

The resolved Rx Tw for this link. Note: NOT the link partner

The resolved value that is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).

EEE in Sync

Shows whether the switch and the link partner have agreed on wake times.

Red - Switch and link partner have not agreed on wakeup times.

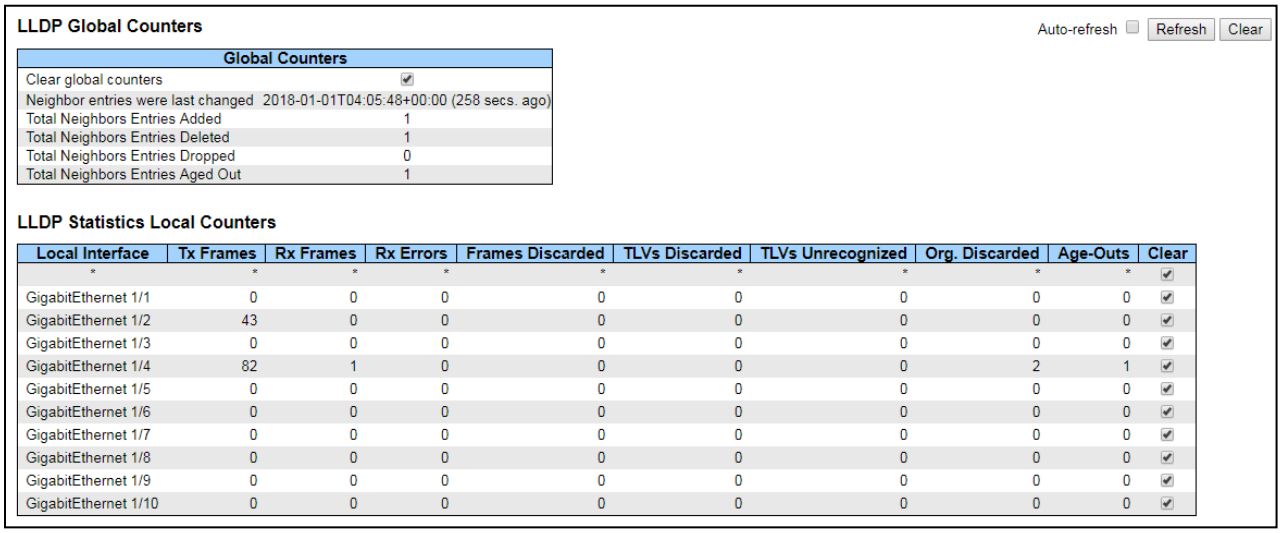
Green - Switch and link partner have agreed on wakeup times.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

Port Statistics



LLDP Global Counters

Auto-refresh Refresh Clear

Global Counters	
Clear global counters	
Neighbor entries were last changed	2018-01-01T04:05:48+00:00 (258 secs. ago)
Total Neighbors Entries Added	1
Total Neighbors Entries Deleted	1
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	1

LLDP Statistics Local Counters

Local Interface	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	Clear
*	*	*	*	*	*	*	*	*	
GigabitEthernet 1/1	0	0	0	0	0	0	0	0	
GigabitEthernet 1/2	43	0	0	0	0	0	0	0	
GigabitEthernet 1/3	0	0	0	0	0	0	0	0	
GigabitEthernet 1/4	82	1	0	0	0	0	2	1	
GigabitEthernet 1/5	0	0	0	0	0	0	0	0	
GigabitEthernet 1/6	0	0	0	0	0	0	0	0	
GigabitEthernet 1/7	0	0	0	0	0	0	0	0	
GigabitEthernet 1/8	0	0	0	0	0	0	0	0	
GigabitEthernet 1/9	0	0	0	0	0	0	0	0	
GigabitEthernet 1/10	0	0	0	0	0	0	0	0	

This page provides an overview of all LLDP traffic.

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

Global Counters

Clear global counters

If checked the global counters are cleared when Clear is pressed.

Neighbor entries were last changed

It shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

Total Neighbors Entries Added

Shows the number of new entries added since switch reboot.

Total Neighbors Entries Deleted

Shows the number of new entries deleted since switch reboot.

Total Neighbors Entries Dropped

Shows the number of LLDP frames dropped due to the entry table being full.

Total Neighbors Entries Aged Out

Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each interface. The columns hold the following information:

Local Interface

The interface on which LLDP frames are received or transmitted.

Tx Frames

The number of LLDP frames transmitted on the interface.

Rx Frames

The number of LLDP frames received on the interface.

Rx Errors

The number of received LLDP frames containing some kind of error.

Frames Discarded

If a LLDP frame is received on a interface, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given interface's link is down, an LLDP shutdown frame is received, or when the entry ages out.

TLVs Discarded

Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized

The number of well-formed TLVs, but with an unknown type value.

Org. Discarded

If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.

Age-Outs

Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the **Age-Out** counter is incremented.

Clear

If checked the counters for the specific interface are cleared when Clear is pressed.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

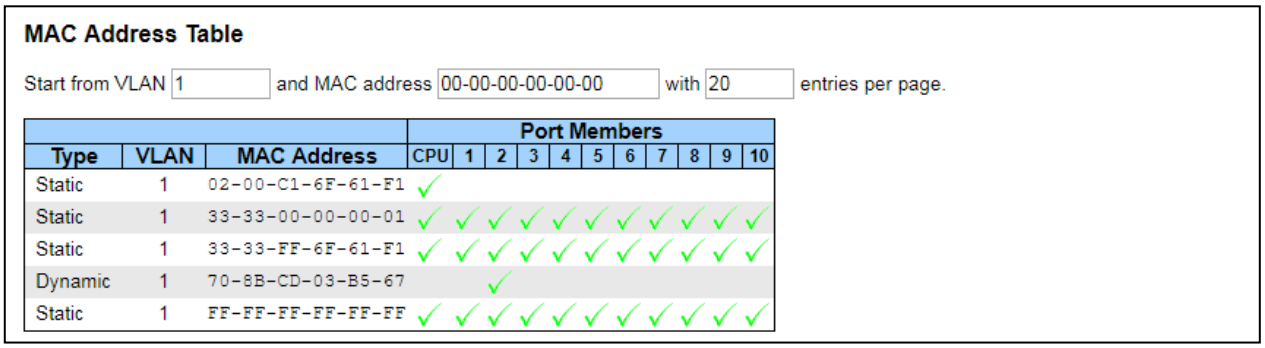
Refresh: Click to refresh the page.

Clear: Clears the counters which have the corresponding checkbox checked.

3.2.11 MAC ADDRESS

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has



been seen after a configurable age time.

Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Navigating the MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.
The "Start from MAC address" and "VLAN" input fields allow the user to select the starting point in the MAC Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will - upon Refresh a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.
The >> will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

MAC Table Columns

Type

Indicates whether the entry is a static or a dynamic entry.

MAC address

The MAC address of the entry.

VLAN

The VLAN ID of the entry.

Port Members

The ports those are members of the entry.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

Clear: Flushes all dynamic entries.

|<<: Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.

>>: Updates the table, starting with the entry after the last entry currently displayed.

3.2.12 VLANS

Membership



This page provides an overview of membership status of VLAN users.

VLAN User

Various internal software modules may use VLAN services to configure VLAN memberships on the fly.

The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

VLAN ID

VLAN ID for which the Port members are displayed.

Port Members

A row of check boxes for each port is displayed for each VLAN ID.

If a port is included in a VLAN, the following image will be displayed: ✓.

If a port is in the forbidden port list, the following image will be displayed: ✗.

If a port is in the forbidden port list and at the same time attempted included in the VLAN, the following image will be displayed: ✗. The port will not be a member of the VLAN in this case.

Navigating the VLAN Membership Status page

Each page shows up to 99 entries from the VLAN table (default being 20), selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input field allows the user to select the starting point in the VLAN Table.

Clicking the Refresh button will update the displayed table starting from that or the closest next VLAN Table match.

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

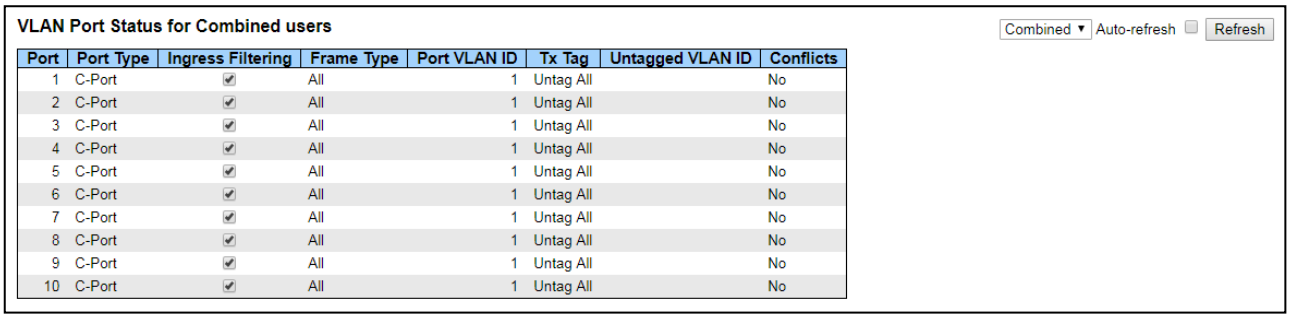
Buttons

Combined, Admin, and Various Internal Software Modules: Select VLAN Users from this drop down list.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Ports



Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag All		No
2	C-Port	☑	All	1	Untag All		No
3	C-Port	☑	All	1	Untag All		No
4	C-Port	☑	All	1	Untag All		No
5	C-Port	☑	All	1	Untag All		No
6	C-Port	☑	All	1	Untag All		No
7	C-Port	☑	All	1	Untag All		No
8	C-Port	☑	All	1	Untag All		No
9	C-Port	☑	All	1	Untag All		No
10	C-Port	☑	All	1	Untag All		No

This page provides VLAN Port Status.

VLAN User

Various internal software modules may use VLAN services to configure VLAN port configuration on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

If a given software modules hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table.

Port

The logical port for the settings contained in the same row.

Port Type

Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the

port. The field is empty if not overridden by the selected user.

Ingress Filtering

Shows whether a given user wants ingress filtering enabled or not.

The field is empty if not overridden by the selected user.

Frame Type

Shows the acceptable frame types (All, Tagged, Untagged) that a given user wants to configure on the port.

The field is empty if not overridden by the selected user.

Port VLAN ID

It shows the Port VLAN ID (PVID) that a given user wants the port to have.

The field is empty if not overridden by the selected user.

Tx Tag

Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port. The field is empty if not overridden by the selected user.

Untagged VLAN ID

If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field will show the VLAN ID the user wants to tag or untag on egress. The field is empty if not overridden by the selected user.

Conflicts

Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress.

Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority. If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module. The "Combined" user reflects what is actually configured in hardware.

Buttons

Combined, Admin, and Various Internal Software Modules: Select VLAN Users from this drop down list.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

3.3 DIAGNOSTICS

WoMaster Switch provides several types of features for User to monitor the status of the switch or diagnostic for User to check the problem when encountering problems related to the switch.

Following commands are included in this group:

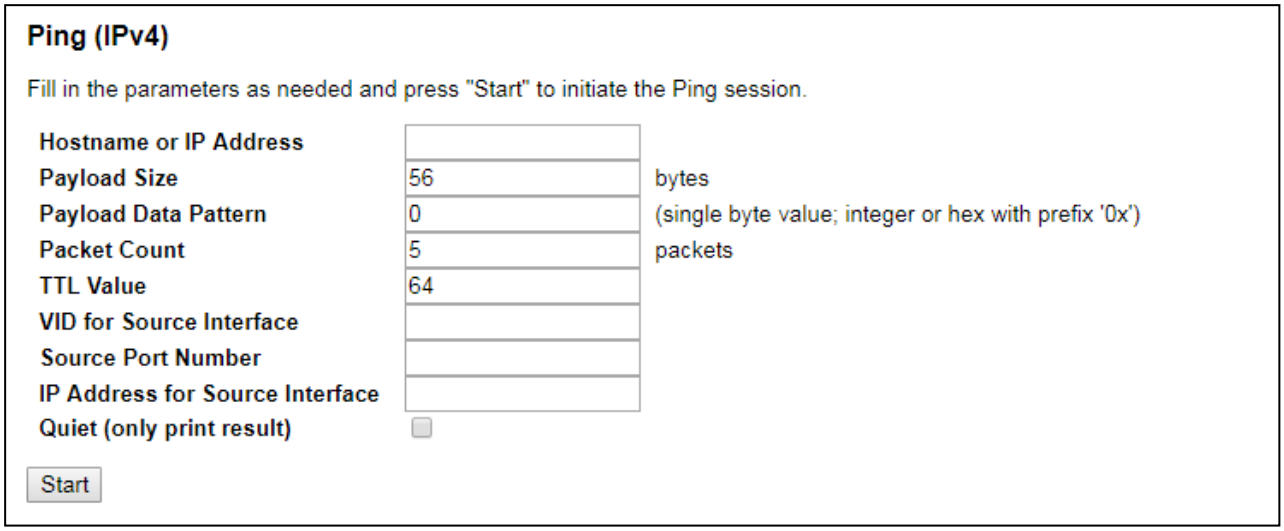
3.3.1 Ping (IPv4)

3.3.2 Traceroute

3.3.3 VeryPHY

3.3.1 PING (IPv4)

Ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected. Ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.



This page allows you to issue ICMP (IPv4) PING packets to troubleshoot IP connectivity issues.

You can configure the following parameters for the test:

Hostname or IP Address

The address of the destination host, either as a symbolic hostname or an IP Address.

Payload Size

Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.

Payload Data Pattern

Determines the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

Packet Count

Determines the number of PING requests sent. The default value is 5. The valid range is 1-60.

TTL Value

Determines the Time-To-Live /TTL) field value in the IPv4 header. The default value is 64. The valid range is 1-255.

VID for Source Interface

This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

Source Port Number

This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the Source Port Number or the IP Address for the source interface.

Address for Source Interface

This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

Quiet (only print result)

Checking this option will not print the result of each ping request but will only show the final result.

After you press, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

The output from the command will look like the following:

PING 172.16.1.1 (172.16.1.1) from 172.16.1.10: 56 data bytes

64 bytes from 172.16.1.1: seq=0 ttl=64 time=2.034 ms

64 bytes from 172.16.1.1: seq=1 ttl=64 time=1.729 ms

64 bytes from 172.16.1.1: seq=2 ttl=64 time=1.954 ms

64 bytes from 172.16.1.1: seq=3 ttl=64 time=1.699 ms

64 bytes from 172.16.1.1: seq=4 ttl=64 time=1.916 ms

--- 172.16.1.1 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

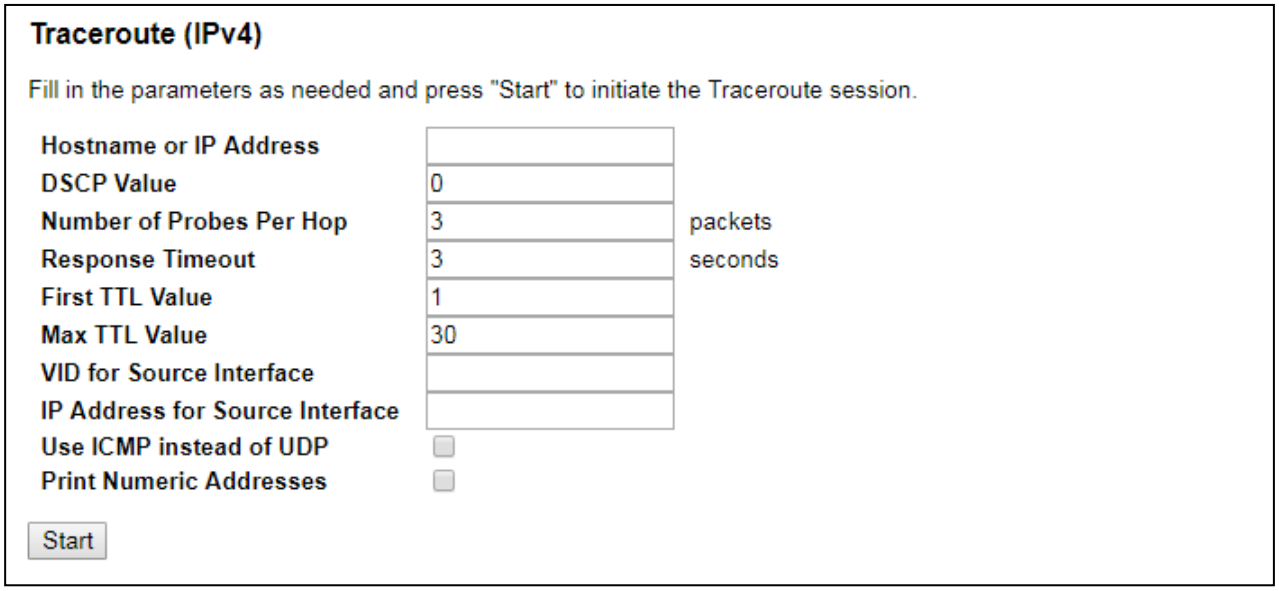
round-trip min/avg/max = 1.699/1.866/2.034 ms

Buttons

Start: Click to start transmitting ICMP packets.

New Ping: Click to re-start diagnostics with PING.

3.3.2 TRACEROUTE (IPv4)



This page allows you to perform a **traceroute** test over IPv4 towards a remote host. **traceroute** is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network.

You can configure the following parameters for the test:

Hostname or IP Address

The destination IP Address.

DSCP Value

This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-63.

Number of Probes Per Hop

Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.

Response Timeout

Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.

First TTL Value

Determines the value of the Time-To-Live (TTL) field in the IPv4 header in the first packet sent. The default number is 1. The valid range is 1-30.

Max TTL Value

Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1-255.

VID for Source Interface

This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

Address for Source Interface

This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for

automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

Use ICMP instead of UDP

By default the **traceroute** command will use UDP datagrams. Selecting this option forces it to use ICMP ECHO packets instead.

Print Numeric Addresses

By default the **traceroute** command will print out hop information using a reverse DNS lookup for the acquired host ip addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the **traceroute** command to print numeric IP addresses instead.

Traceroute (IPv6)

This page allows you to perform a **traceroute** test over IPv6 towards a remote host. **traceroute** is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv6 network.

You can configure the following parameters for the test:

Hostname or IP Address

The destination IP Address.

DSCP Value

This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-255.

Number of Probes Per Hop

Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.

Response Timeout

Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.

Max TTL Value

Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 255. The valid range is 1-255.

VID for Source Interface

This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

Address for Source Interface

This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.

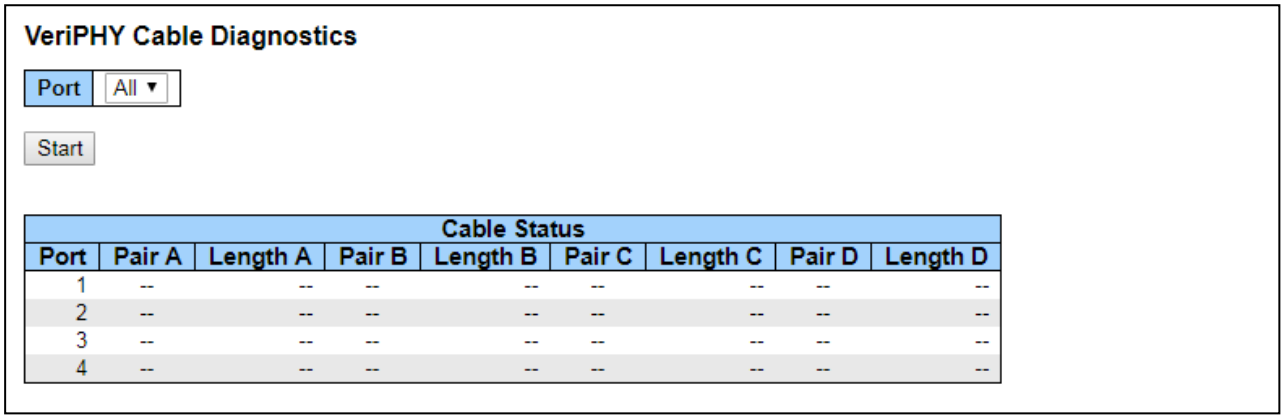
Note: You may only specify either the VID or the IP Address for the source interface.

Print Numeric Addresses

By default the **traceroute** command will print out hop information using a reverse DNS lookup for the acquired host ip addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the **traceroute** command to print numeric IP addresses instead.

3.3.3 VeryPHY

This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.



Press to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters. 10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Port

The port where you are requesting VeriPHY Cable Diagnostics.

Cable Status

Port: Port number.

Pair: The status of the cable pair.

OK - Correctly terminated pair

Open - Open pair

Short - Shorted pair

Short A - Cross-pair short to pair A

Short B - Cross-pair short to pair B

Short C - Cross-pair short to pair C

Short D - Cross-pair short to pair D

Cross A - Abnormal cross-pair coupling with pair A

Cross B - Abnormal cross-pair coupling with pair B

Cross C - Abnormal cross-pair coupling with pair C

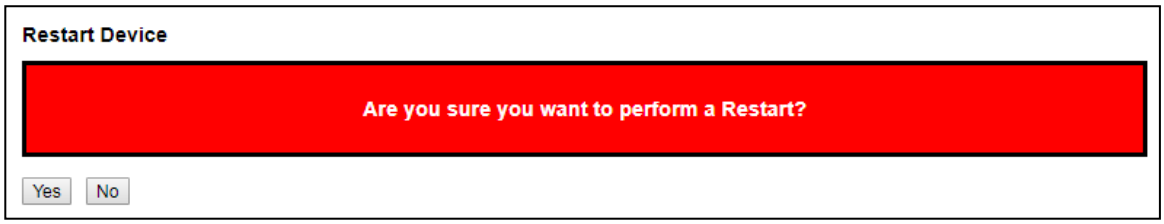
Cross D - Abnormal cross-pair coupling with pair D

Length: The length (in meters) of the cable pair. The resolution is 3 meters

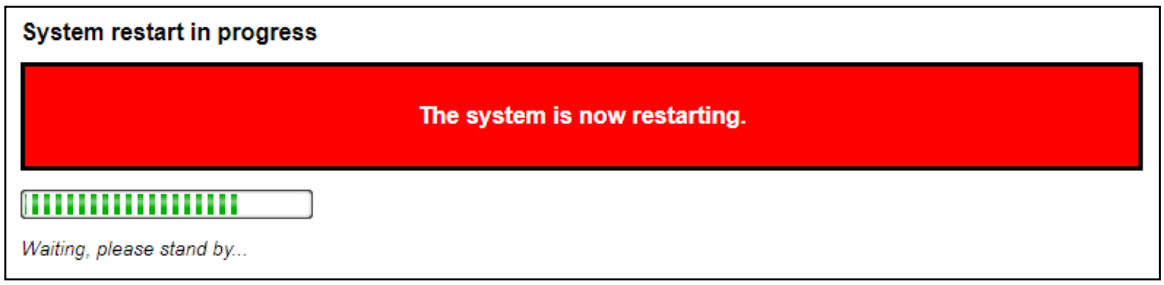
3.4 MAINTANANCE

3.4.1 RESTART

This function allows user to restart the device. Click on **Restart** from the menus. Restart device main screen, to do confirmation request. Click **Yes**, then the switch will restart immediately.



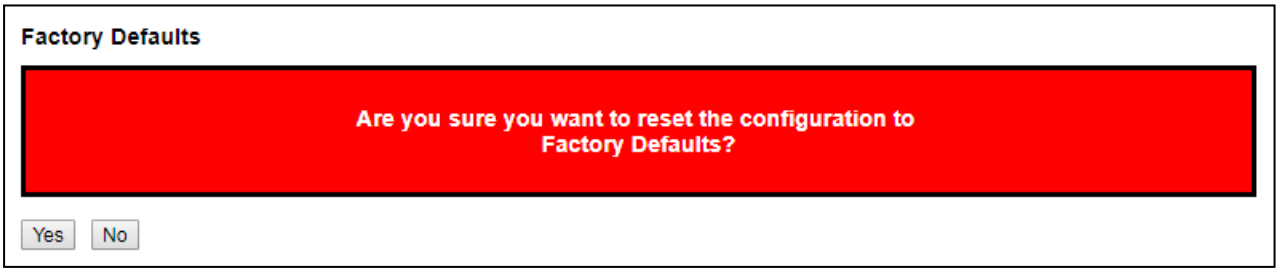
After user clicks Yes then the restart process is executed.



3.4.2 FACTORY DEFAULT

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

The new configuration is available immediately, which means that no restart is necessary.



Yes: Click to reset the configuration to Factory Defaults.

No: Click to return to the Port State page without resetting the configuration.

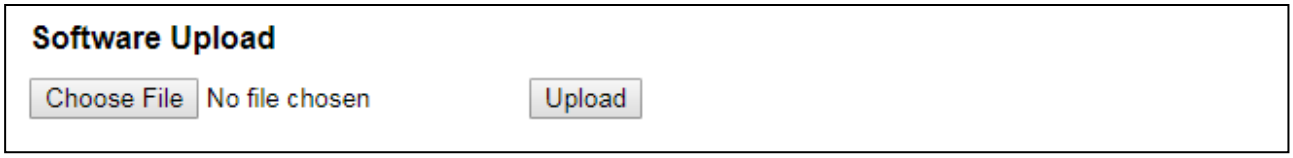
Note: Restoring factory default can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, 'loopback' packets will be transmitted at port 1. If a 'loopback' packet is received at port 2 the switch will do a restore to default

3.4.3 SOFTWARE

Upload

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

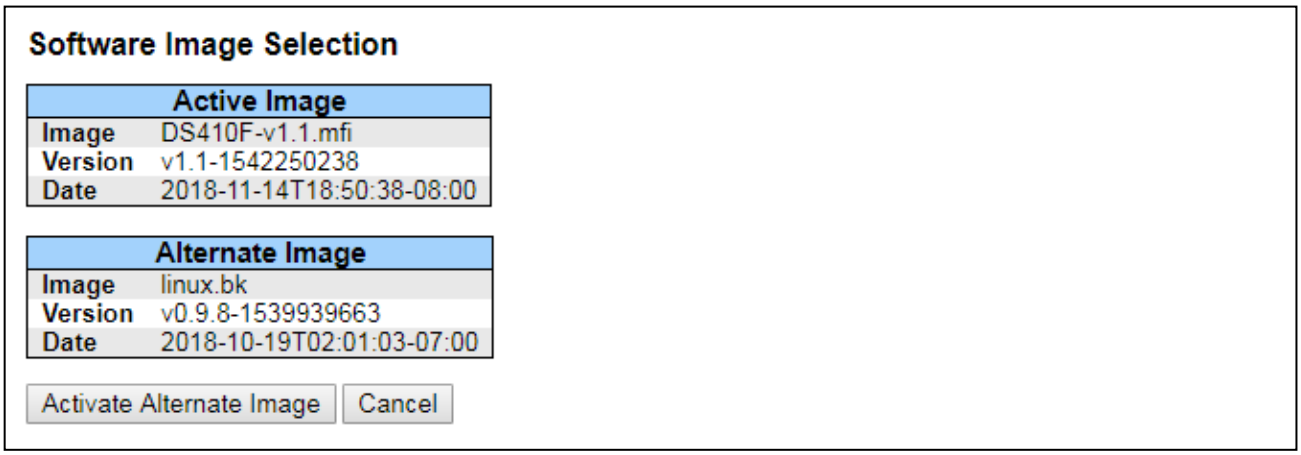
Click Choose File to the location of a software image and click Upload.



After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

***Warning**: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress.* ***Do not restart or power off the device at this time** or the switch may fail to function afterwards.*

Image Select



This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

The web page displays two tables with information about the active and alternate firmware images.

Note:

1. In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the **Activate Alternate Image** button is also disabled.
2. If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

Image Information

Image

The file name of the firmware image, from when the image was last updated.

Version

The version of the firmware image.

Date

The date where the firmware was produced.

Buttons

Activate Alternate Image: Click to use the alternate image. This button may be disabled depending on system state.

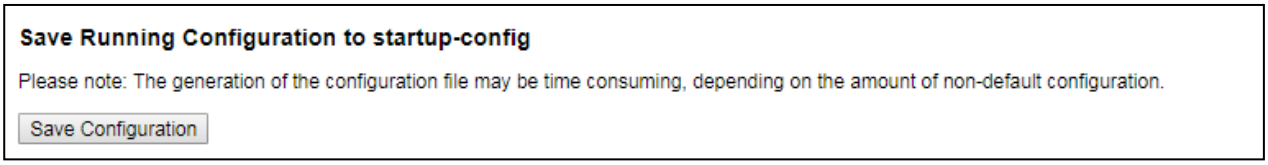
Cancel: Cancel activating the backup image. Navigates away from this page.

3.4.4 CONFIGURATION

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch. The available files are:

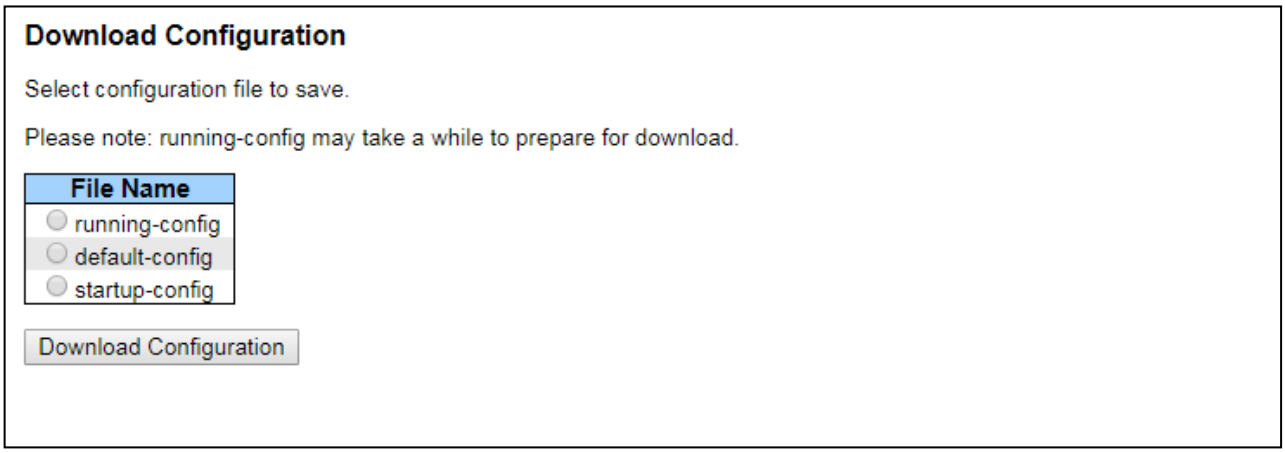
- *running-config*: A virtual file that represents the currently active configuration on the switch. This file is volatile.
- *startup-config*: The startup configuration for the switch, read at boot time. If this file doesn't exist at boot time, the switch will start up in default configuration.
- *default-config*: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.
- Up to 31 other files, typically used for configuration backups or alternative configurations.

Save *startup-config*



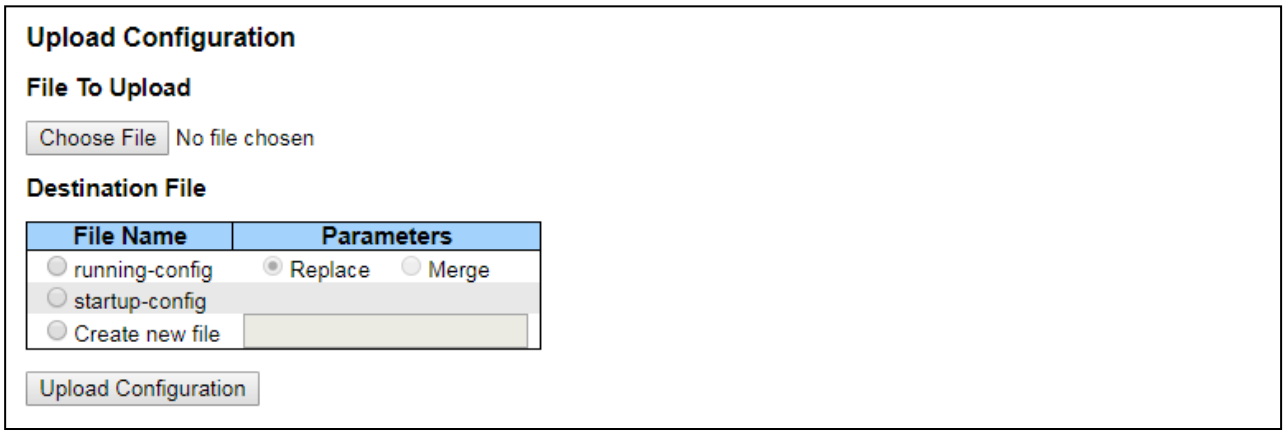
This copies *running-config* to *startup-config*, thereby ensuring that the currently active configuration will be used at the next reboot.

Download



It is possible to download any of the files on the switch to the web browser. Select the file and click Download Configuration. Download of *running-config* may take a little while to complete, as the file must be prepared for download.

Upload

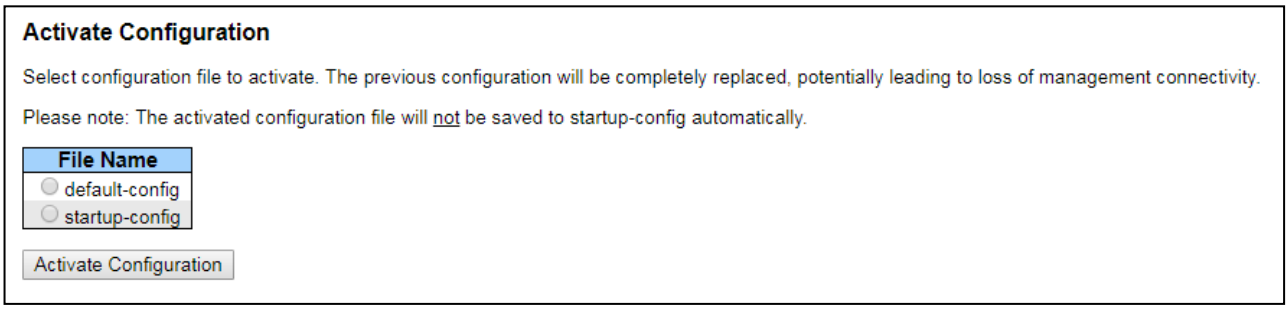


It is possible to upload a file from the web browser to all the files on the switch, except *default-config* which is read-only. Select the file to upload, select the destination file on the target, and then click Upload Configuration. If the destination is *running-config*, the file will be applied to the switch configuration. This can be done in two ways:

- **Replace mode**: The current configuration is fully replaced with the configuration in the uploaded file.
- **Merge mode**: The uploaded file is merged into *running-config*.

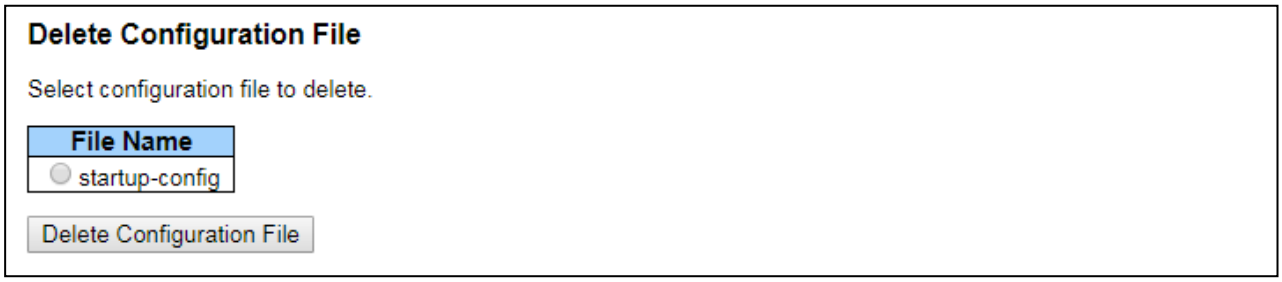
If the flash file system is full (i.e. contains *default-config* and32 other files, usually including *startup-config*), it is not possible to create new files. Instead an existing file must be overwritten or another file must be deleted.

Activate



It is possible to activate any of the configuration files present on the switch, except for *running-config* which represents the currently active configuration. Select the file to activate and click Activate Configuration. This will initiate the process of completely replacing the existing configuration with that of the selected file.

Delete

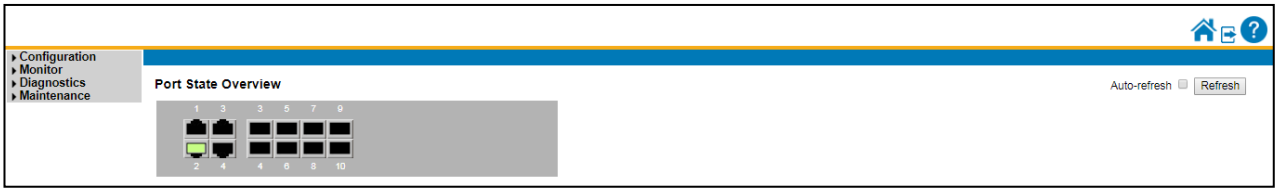


It is possible to delete any of the writable files stored in flash, including *startup-config*. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration.

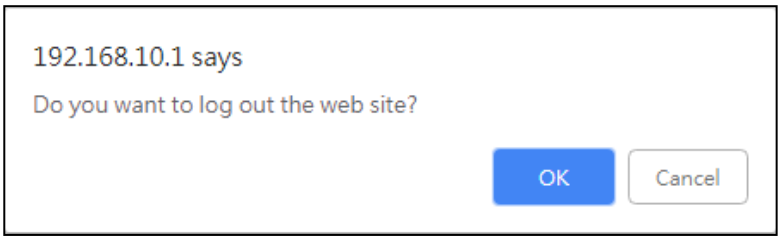
3.5 FRONT PANEL

Front Panel commands allow user to see the port status of the switch. Shown as below. Click Refresh to refresh the Port State, user can check the Auto-refresh to refresh the page automatically.

HOME



LOGOUT



HELP

This help button provide the general information for the configuration page.

