SISGM-CHAS L2/L3
Modular Rackmount Hardened Switch

User Guide

33625 Rev. B

Table of Contents

1. Introduction

1.1 About the SISGM Series Switches

The Transition Networks SISGM family of Modular Rack-mount Hardened Layer 2/3 Switches, Modules and SFPs provide IEC61850 compliant managed Ethernet switch capabilities.

The modular design with three full-size bays accommodates eight-port 100/1000 modules while the half-size bay accommodates either a 2- or 4- port 1000/10Gb SFP module. With complete support of MRP Ethernet Redundancy protocol and MSTP (RSTP/STP compatible) the switch can protect your mission-critical applications from network interruptions with its fast recovery technology. Supporting a wide operating temperature from -40^{0}C to +65^{0}C with 1GB SFP modules, the switch is suitable for use in challenging environments. Centralized management can be done via the Web-based interface and Telnet, with local management available using the Console port CLI.

1.2 Model Numbers

Number	Description
SISGM-CHAS-L2	Layer 2 Chassis
SISGM-CHAS-L3	Layer 3 Chassis (-L2 Chassis plus additional L3 routing functions)
SISGM-PWR-LVC	Power Supply 24 ~ 72VDC
SISGM-PWR-HVC	Power Supply 100~240VAC
SISGM-2P-10G-SFP	2 Port, 10Gb, SFP+
SISGM-4P-10G-SFP	4 Port, 10Gb, SFP+
SISGM-8P-1G-SFP	8 Port, 1Gb, SFP
SISGM-8P-1G-TX	8 Port, 1Gb, RJ45
SFP Modules	Optional. See Transition Networks' SFP and SFP+ landing page.

1.3 Features

- Modular 19-inch rack mountable design
- Redundant power inputs
- Compliant with IEC 61850-3 and IEEE 1613
- Houses three 10/100/1000Base-T(X) RJ-45 modules for up to 24 ports ; or
  houses three 100/1000Base-X SFP modules for up to 24 ports ; or
  houses one 10G SFP+ module for up to 4 ports.
- Hardware routing, RIP and Static Routing (Layer 3 model only)
- IEC 62439-2 MRP (Media Redundancy Protocol)
- MRP (Multiple Registration Protocol)
- IEEE 1588v2 PTP Clock Synchronization
- IPv4/IPv6 internet protocols
- 8K MAC Table
- HTTPS/SSH network security
- SMTP client
- IP-based Bandwidth management
- Application-based QoS management
- DOS/DDOS auto prevention
- IGMP v2/v3 Snooping - 256 Groups/VLAN
- SNMP v1/v2c/v3
- RMON
- VLAN Network Management
- VLAN tagging (4096 VLANs)
- User Authentication for security
- RADIUS/TACACS+
- ACL (Access Control Lists)
- Supports 9.6K Bytes Jumbo Frames
- LLDP (Link Level Discovery Protocol)
- VRRP (Virtual Router Redundancy Protocol)
- MSTP (RSTP/STP compatible)
- TOS/Diffserv supported
- DHCP Server/Client/Relay
- DNS client proxy
- Web-based, Telnet, Console (CLI) configuration

Note: The Static Routing, RIP (Routing Information Protocol) features are available on the Layer 3 Chassis only.

1.4 Specifications

Standards: IEEE 802.1p COS, IEEE 802.1Q VLAN IEEE 802.1D STP, IEEE 802.1w RSTP, IEEE 802.1s MSTP, IEEE 802.1x Authentication, IEEE 802.1AB LLDP, IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX and 100Base-FX, IEEE 802.3ab 1000Base-T, IEEE 802.z, 1000Base-X, IEEE 802.3ae 10Gb, IEEE 802.3x Flow control, IEEE 802.3ad LACP, IEEE 802.3az Energy-Efficient Ethernet (EEE)

Fault Output: Fault Relay 1A@24VDC

Dimensions: Width: 17.32 inches (440 mm)
Depth: 12.8 inches (325 mm)
Height: 1.73 inches (44 mm)
19" Rack Mountable, 1U. (For adequate air circulation for cooling, open space in the rack above and below the chassis is required.)

Power Consumption: 46 watts max.

Environment: Operating with Extended Temperature 1G or 10G SFPs:-40°C to +55°C
Operating with Extended Temperature 1G SFPs only: -40°C to +65°C
Operating Humidity: 5% to 95% (non condensing)

Shipping Weight: 14.52 lbs.

Ingress Protection: P30

Power Input VDC 48(24~72VDC) Dual Inputs
VAC 100~240VAC/100~370VAC Dual Inputs
Current Overload Protection

Port Configurations: (3) Full size 8 Port bays
(1) Half size 2/4 Port Bay
(2) Power Supply Bays
(1) RJ45 Console Serial Port

Network Redundancy: Redundant Rings, Open-Ring, Multiple Ring, MRP (Media Redundancy Protocol), MSTP (RSTP, STP Compatible)

Substation Automation: IEC61850, IEEE1613

EMI Compliance: FCC Part 15, CISPR (EN 55022) Class A, EN55155 (EN50121-3-2, EN50121-4)

Environmental Compliance: EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11

Waranty: 5 Year Limited Warranty

1.5 Package Contents

Contact your sales representative if you did not receive the following:

- One L2 or L3 Switch
- One Power Cord (country-specific)
- One Power Cable Adapter (for SISGM-PWR-HVC only)
- One or more switch modules (shipped separately)
- One Console Cable (see RS-232 Console Port Wiring on page 28)
- 1U and 2U Bracket Kit options
- One printed Quick Start Guide (33624)
- Faceplates

Please save the shipping material for possible future use. **Note**: The product is shipped as separate modules allowing assembly and configuration during installation.

2. Hardware Overview

2.1 Chassis Descriptions

The SISGM is a modular 19" Rack Mountable Chassis with three full size bays to house 8-port 100/1000 modules, one half-size bay to house either a 2- or 4-port 1000/10Gb SFP module, and two power supply bays.

2.2 Power Supply Modules

The SISGM supports one or two power supply modules. The chassis can be powered with a single power supply; using two power supplies provides power supply redundancy protection. The Power Supplies Modules are sold separately from the chassis.

Photo	***Description***
	SISGM-PWR-LVC Power Supply 20~72VDC With Fan

	SISGM-PWR-HVC Power Supply 100~240VAC With Fan

2.3 Port Module Descriptions

Photo	***Description***
	SISGM-2P-10G-SFP 2-Port 10GB SFP+ Module
	SISGM-4P-10G-SFP 4-Port 10GB SFP+ Module

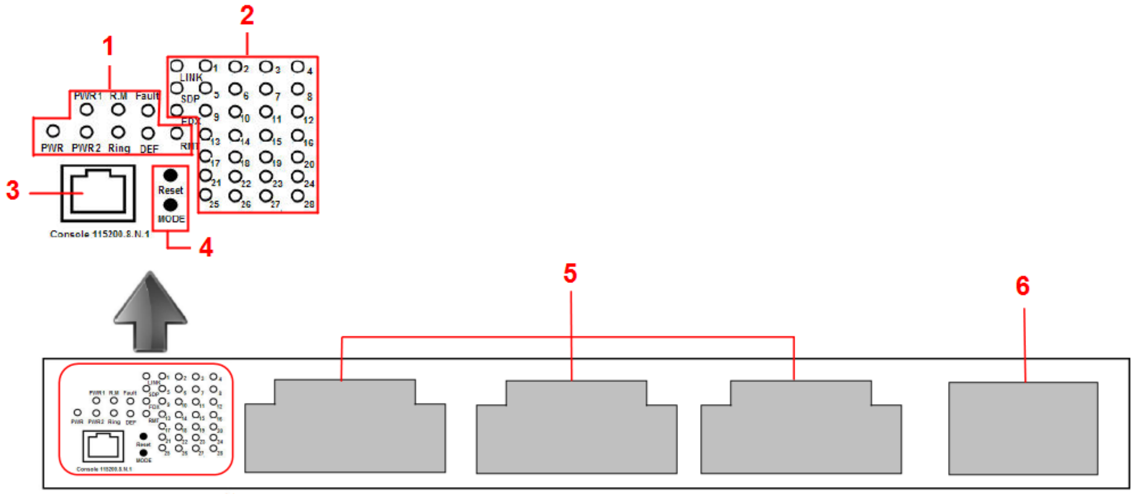
	SISGM-8P-1G-SFP 8-Port 1GB SFP Module
	SISGM-8P-1G-TX 8-Port 1GB TX Module

2.4 Front Panel

2.1.1 Ports and Connectors

The SISGM series switches provide one 10 Gigabit module bay and three 10/100/1000Base-T bays to enable different modular combinations based on your needs. The SISGM has two different 10G modules and two different Gigabit modules that can be used in various combinations to provide the port density and connection types required for your application. For applications requiring long-distance data transmission, the SISGM also provides several fiber transceivers to meet your needs. See Model Numbers above for the list of available modules.

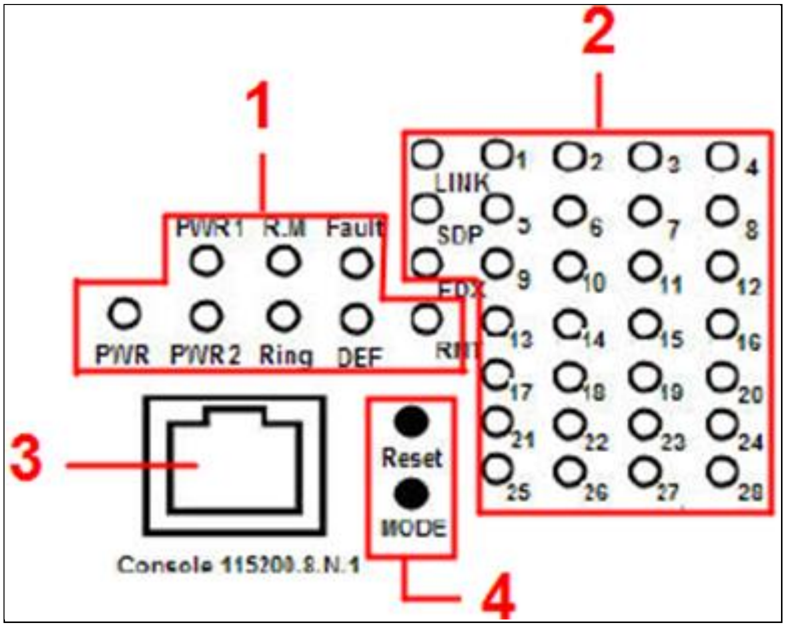
⚠ **Warning**! Network Port modules are not hot-swappable. Be sure to turn off power before changing modules, otherwise the system will not detect newly inserted modules.



1. **System indication LEDs**: PWR/PWR1/PWR2/R.M/Ring/Fault/DEF.
2. **Port status LEDs**: LINK/SPD/FDX/port number.
3. **Console port**
4. **Buttons**: Reset/LED Mode (Press **Reset** for 3 seconds to reset, or press 5 seconds to return to factory defaults. To change the port LED mode, press the **MODE** button.)
5. **RJ-45/SFP module bays**
6. **10G SFP module bay**

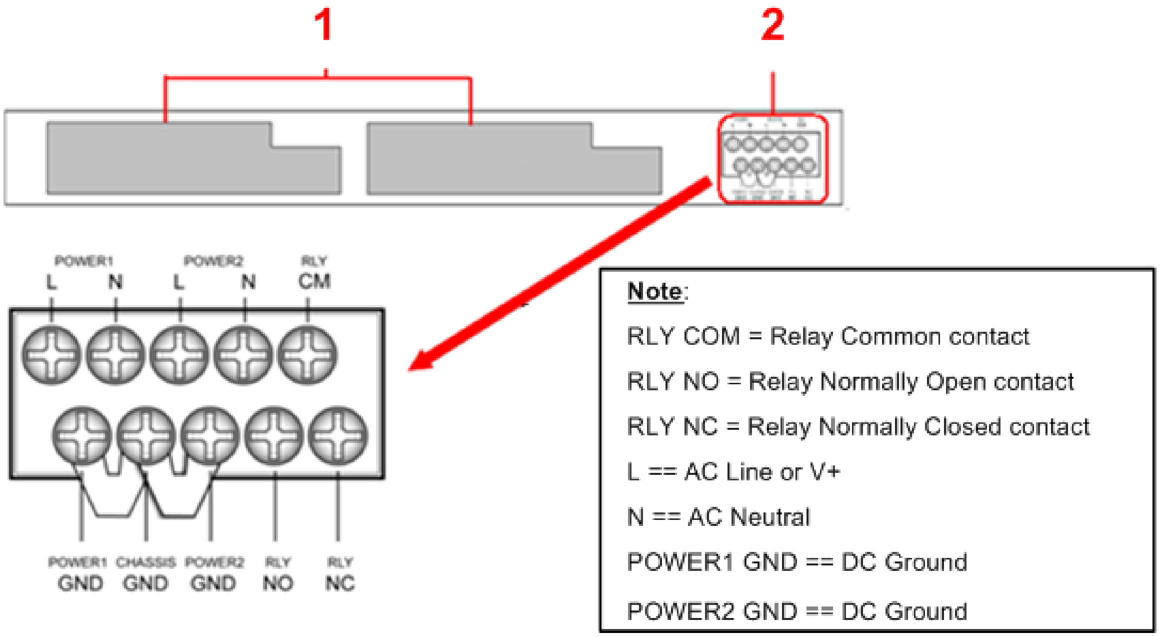
2.1.2 LEDs

LED	Color	Status	Description
PWR	Green	On	System power on
	Green	Blinking	Upgrading firmware
PW1	Green	On	System power module 1 activated
PW2	Green	On	Power module 2 activated
R.M	Green	On	Ring Master
Ring	Green	On	Ring enabled
		Blinking	Ring structure is broken
Fault	Amber	On	Errors (power failure or port malfunctioning)
DEF	Green	On	System reset to default
RMT	Green	On	Accessed remotely
LINK	Green	On	Port link up
SPD	Green	On	Ethernet connection running at 1000Mbps
	Amber	On	Ethernet connection running at 10/100Mbps
FDX	Amber	On	Port works under full duplex.



2.5 Rear Panel

The rear panel of the switch has two panel module bays and one terminal block. The terminal block includes two power pairs for redundant power supply.



Note:

RLY COM = Relay Common contact

RLY NO = Relay Normally Open contact

RLY NC = Relay Normally Closed contact

L == AC Line or V+

N == AC Neutral

POWER1 GND == DC Ground

POWER2 GND == DC Ground

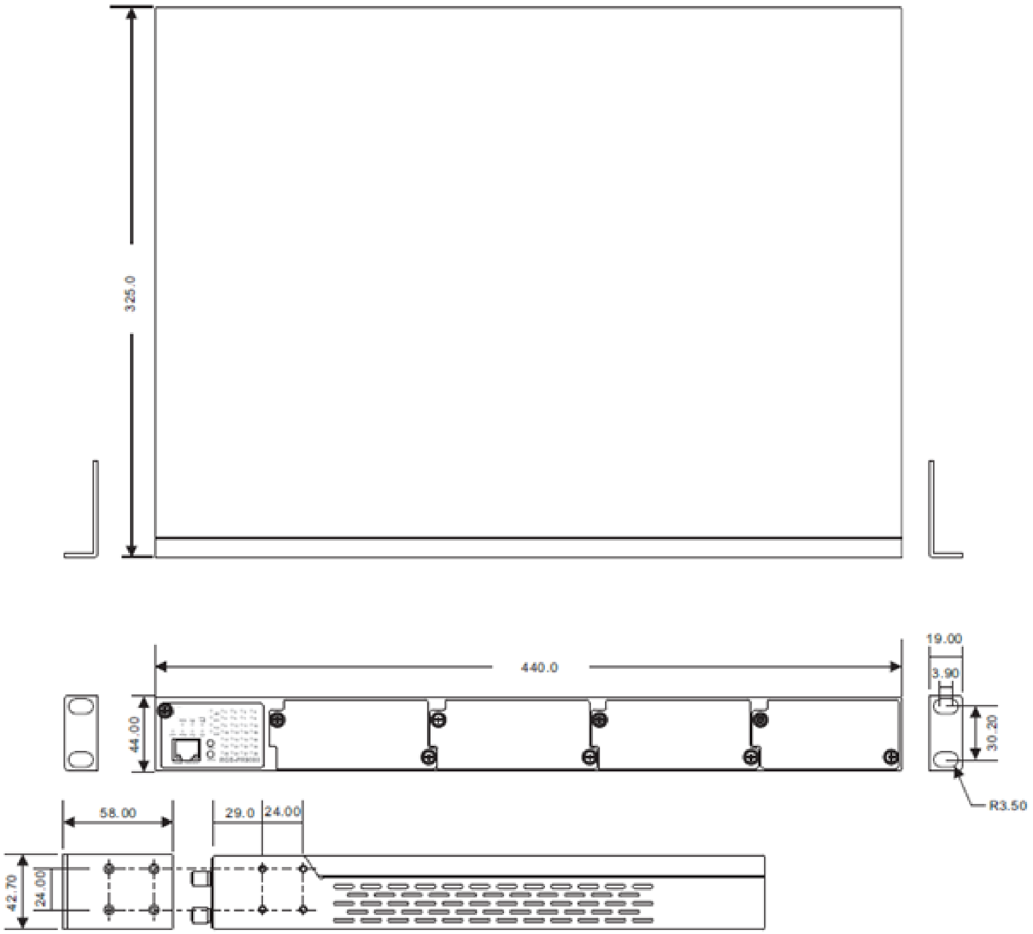
1. Power module bays

2. Terminal block

3. Hardware Installation

2.1 Rack-mount Installation

The switch comes with two rack-mount kits (1U and 2U bracket kits) to fasten the switch to a rack in any environment.



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

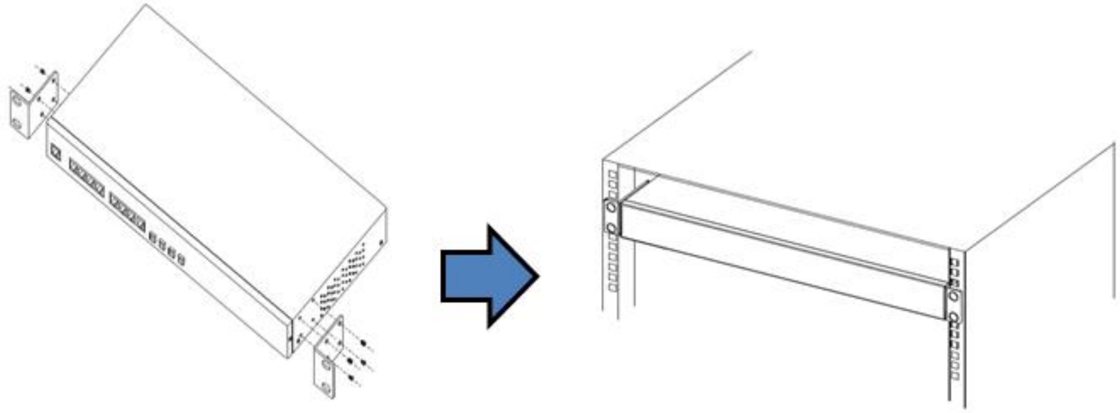
Step 1: Install left and right front mounting brackets to the switch using the four M3 screws on each side provided with switch.

Step 2: With front brackets orientated in front of the rack, nest front and rear brackets together. Fasten together using remaining M4 screws into counter sunk holes.

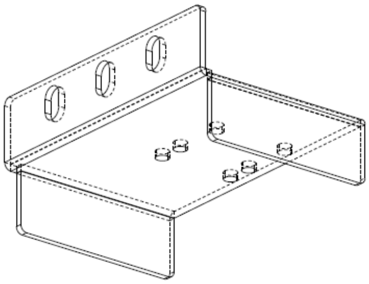
Step 3: Fasten the front mounting bracket to the front of the rack.

Note: You can install the brackets on both sides at back of the device and mount it to the rack with the rear panel facing outward if the space for front panel cabling is limited. Remember:

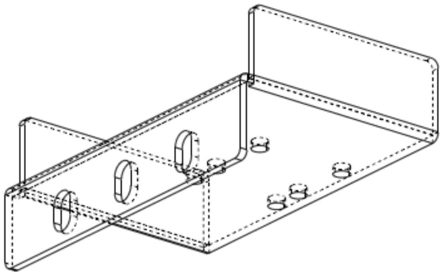
- When installing the brackets on the front sides, use the four screw holes at the top and bottom.
- When installing the brackets on the back sides, use the four screw holes at the top and middle.



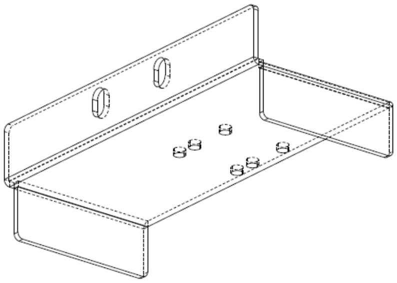
The brackets are designed with 1/2U and 1U space above and below the switch; the total height will be 2U and 3U respectively.



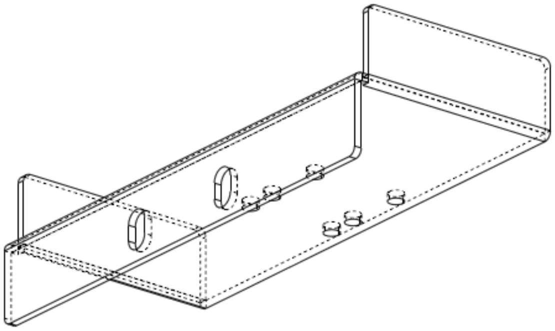
Bracket Ear, Left – 1U



Bracket Ear, Right – 1U



Bracket Ear, Left – 2U

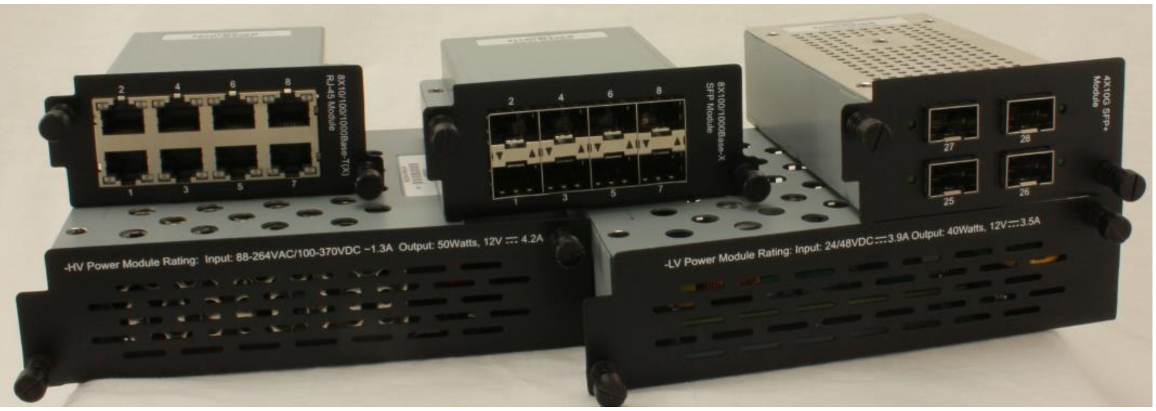


Bracket Ear, Right – 2U

3.2 Module Installation

Removing and installing an Ethernet module can shorten its useful life. Do not remove and insert the modules more often than is absolutely necessary. The network port modules are all shipped with a protective cover over the edge connectors on the back. Carefully remove the protective edge cover before installing the module. Retain the protective edge covers for future use, and replace them when storing or transporting the modules.

⚠ **Warning**! While the power supply modules are hot swappable, replacing network port modules must be done in a power down condition. Be sure to turn off power before changing modules, otherwise the system will not detect newly inserted modules.


8X10/100/1000Base-T(X)
RJ-45 Module
2
4
6
8
1
3
5
7
8X100/1000Base-X
SFP Module
2
4
6
8
1
3
5
7
4X10G SFP+
Module
27
28
25
26
-HV Power Module Rating: Input: 88-264VAC/100-370VDC ~1.3A Output: 50Watts, 12V ⎓ 4.2A
-LV Power Module Rating: Input: 24/48VDC ⎓ 3.9A Output: 40Watts, 12V ⎓ 3.5A

Note: Unoccupied bays should have blank cover installed to ensure proper airflow during operation.

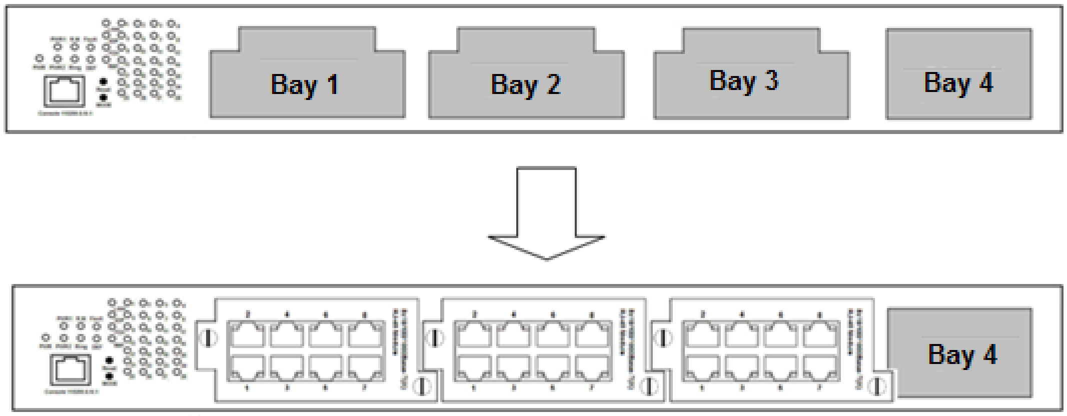
3.2.1 RJ-45 Module

The SISGM switch supports up to three RJ-45 modules, giving you a total of 24 RJ-45 ports. Follow the steps below for installation.

Step 1: Turn the switch power off.

Step 2: Insert the modules in Bays 1, 2, and 3 respectively.

Step 3: Turn the switch power on.



3.2.2 SFP Module

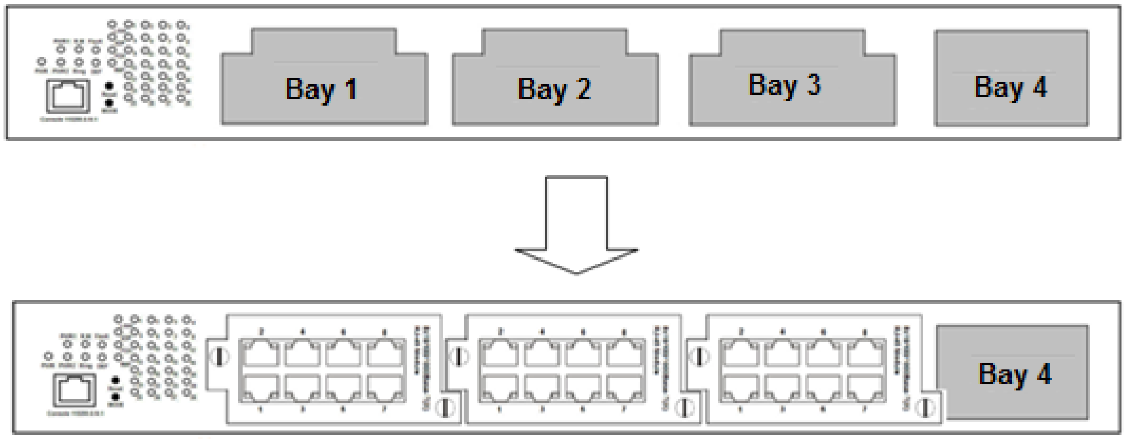
The SISGM series supports maximum three SFP modules, giving you a total of 24 SFP ports.

Follow the steps below for installation.

Step 1: Turn the switch power off.

Step 2: Insert the SFP modules in Bays 1, 2, and 3 respectively.

Step 3: Turn the switch power on.



Transition Networks doesn’t recommend installing any commercial rated SFP (0 – 70°C) in the SFP slot of SISGM Hardened switches.

3.2.3 10G SFP+ Module

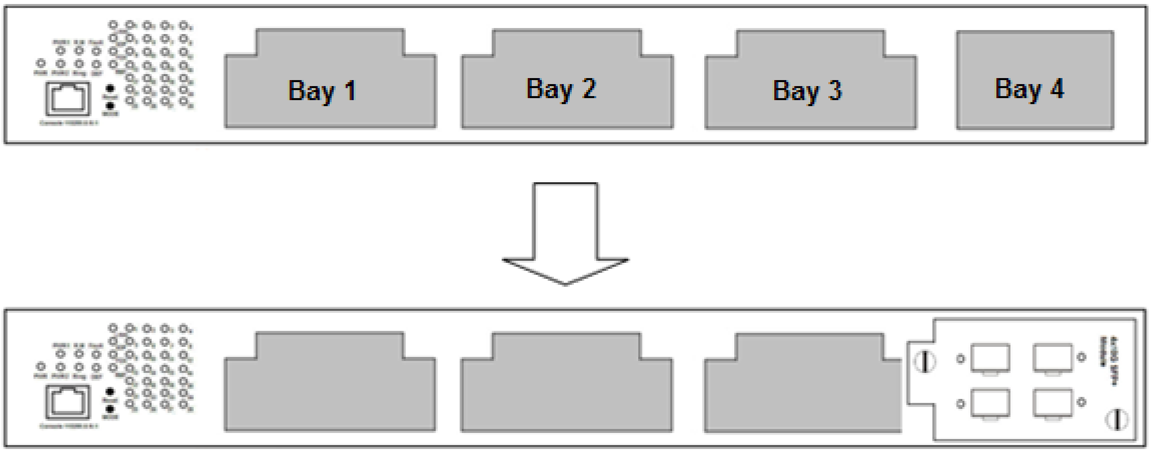
The SISGM series support one 10G SFP+ module, giving you a total of four 10G ports. Follow the steps below for installation. Transition Networks provides two 10G modules, including the SISGM-2P-10G-SFP and the SISGM-4P-10G-SFP. The module can be plugged into the 10-Gigabit Ethernet bay of the switch and connected to fiber-optic networks.

Follow the steps below for installation.

Step 1: Turn the switch power off.

Step 2: Insert the 10G SFP+ module in Bay 4.

Step 3: Turn the switch power on.



1. The 10G Bay can only accommodate a 10G module; therefore, do not insert non-10Gigabit modules in the 10G bay or insert the 10G module in other bays.
2. Removing and installing an Ethernet module can shorten its useful life. Do not remove and insert the modules more often than is absolutely necessary.

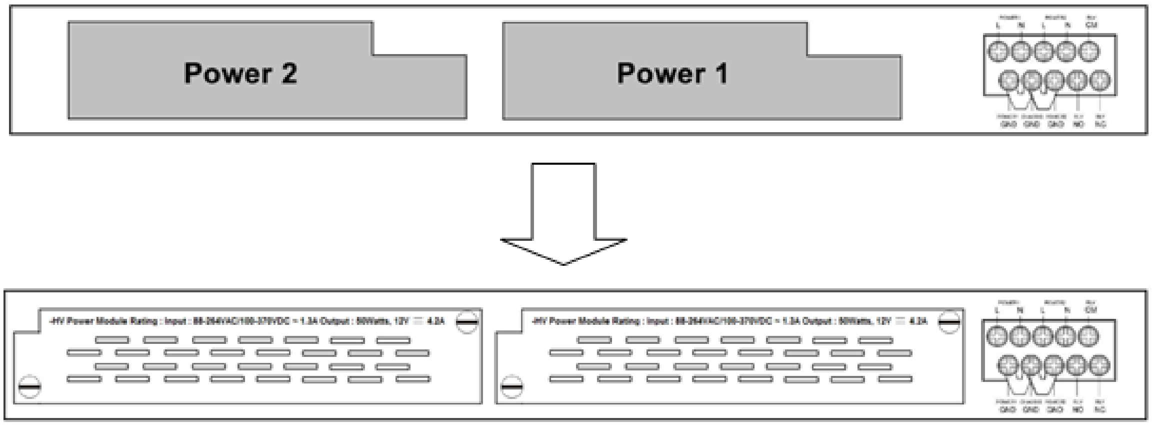
3.2.4 Power Supply Modules

The SISGM series supports one or two power supply modules. Follow the steps below for installation. For fan-less modules, all sheet metal holes should be exposed.

Step 1: Turn the switch power off.

Step 2: Insert the modules in Power 1 and/or Power 2 bays respectively.

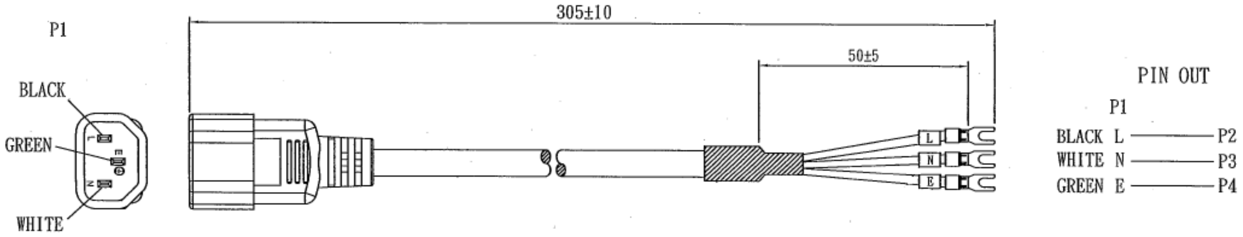
Step 3: Turn the switch power on.


Power 2
Power 1
-HV Power Module Rating : Input : 88-264VAC/100-370VDC ~ 1.3A Output : 50Watts, 12V ⎓ 4.2A
-HV Power Module Rating : Input : 88-264VAC/100-370VDC ~ 1.3A Output : 50Watts, 12V ⎓ 4.2A

Power Cable Adapter (for SISGM-PWR-HVC only)

The SISGM-PWR-HVC ships with a power cable adapter that has a C14 connector that will accept country-specific power cords.

The other end is ROJ (stripped wires). This allows packaged parts that include country-specific Power cords. The drawing below is representative of the cable that is in the box. The cable also has "Y" terminals crimped on the on the three wires that connect to the SISPM-CHAS-L3.



3.3 Wiring

WARNING

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

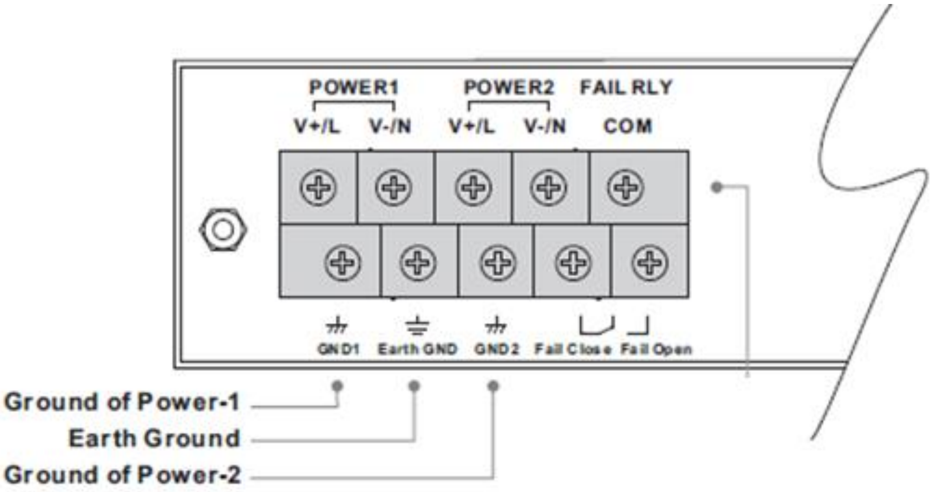
ATTENTION

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

3.3.1 Grounding

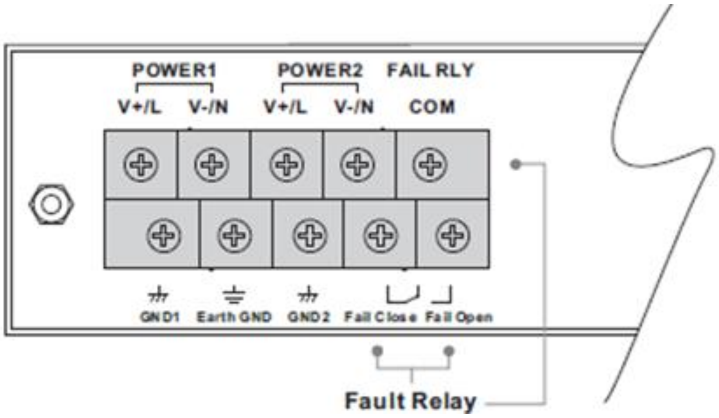
Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI).

Run the ground connection from the ground screws to the grounding surface prior to connecting devices.



3.3.2 Fault Relay (FAIL RLY)

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



3.3.3 Redundant Power Inputs

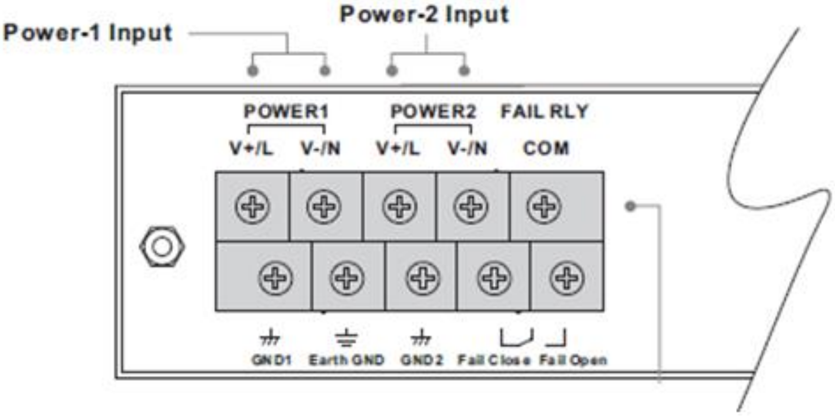
The SISGM series support dual redundant power supplies, Power Supply 1 (POWER1) and Power Supply 2 (POWER2). The connections for POWER1 and POWER2 are located on the terminal block.

Step 1: Remove the transparent protective cover from the terminal block.

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

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

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



3.4 Connection

3.4.1 Cables

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

The SISGM series come with standard Ethernet ports. According to the link type, the switch uses CAT 3, 4, 5,5e UTP cables to connect to any other network devices (PCs, servers, switches, routers, or hubs). Refer to the following table for cable specifications.

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45
1000BASE-T	Cat. 5/Cat. 5e 100-ohm UTP	UTP 100 m (328ft)	RJ-45

With 10/100/1000BASE-T(X) cables, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

10/100 Base-T(X) RJ-45 Pin Assignments:

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

1000 Base-T RJ-45 Pin Assignments:

Pin Number	Assignment
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-

7	BI_DD+
8	BI_DD-

The SISGM series support auto MDI/MDI-X operation. You can use a cable to connect the switch to a PC. The table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

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

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

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

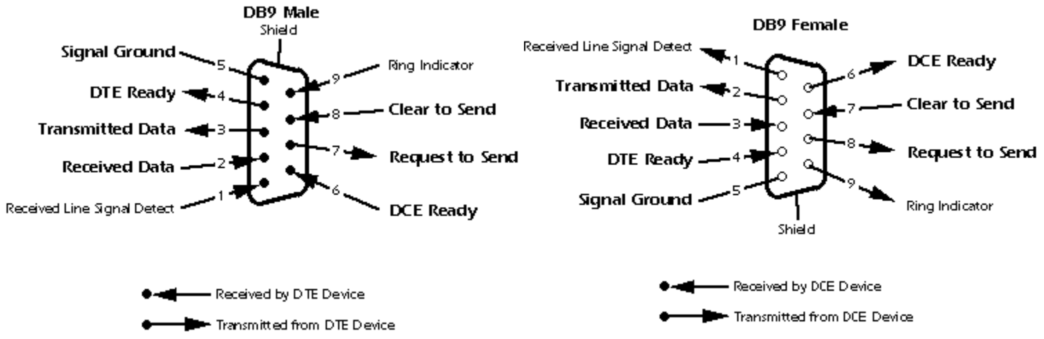
Pin Number	MDI port	MDI-X port
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

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

RS-232 Console Port Wiring

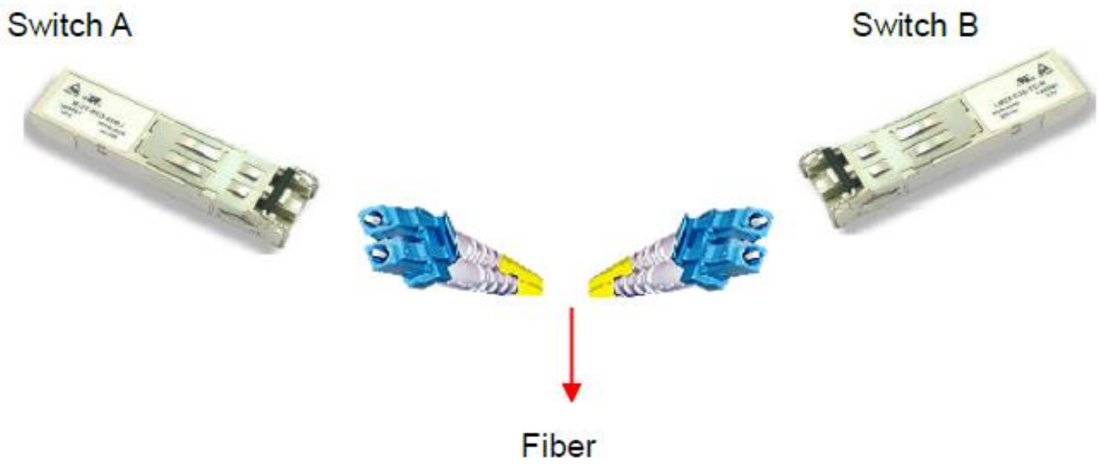
The SISGM series can be managed via the Console port using an RS-232 cable which can be found in the package. You can connect the port to a PC via the RS-232 cable with a DB-9 female connector. The DB-9 female connector of the RS-232 cable should be connected the PC while the other end of the cable (RJ-45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

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



3.4.2 SFPs

The switch comes with fiber optical ports that can connect to other devices using SFP modules. The fiber optical ports are in multi-mode or single-mode with LC connectors. **Note**: the TX port of Switch A should be connected to the RX port of Switch B.



3.4.3 Redundant Rings / Multiple Ring

Redundant Rings

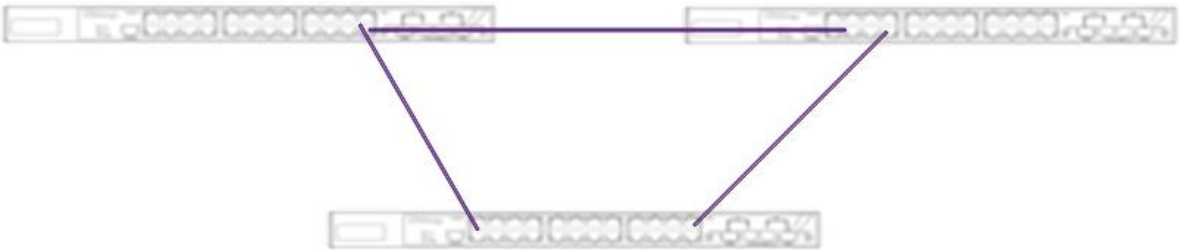
You can connect three or more switches to form a ring topology to gain network redundancy capabilities via these steps :

1. Connect each switch to form a daisy chain using an Ethernet cable.

2. Set one of the connected switches to be the master and make sure the port setting of each connected switch on the management page corresponds to the physical ports connected.

For information about the port setting, refer to section 4.1.2 Configurations.

3. Connect the last switch to the first switch to form a ring topology.

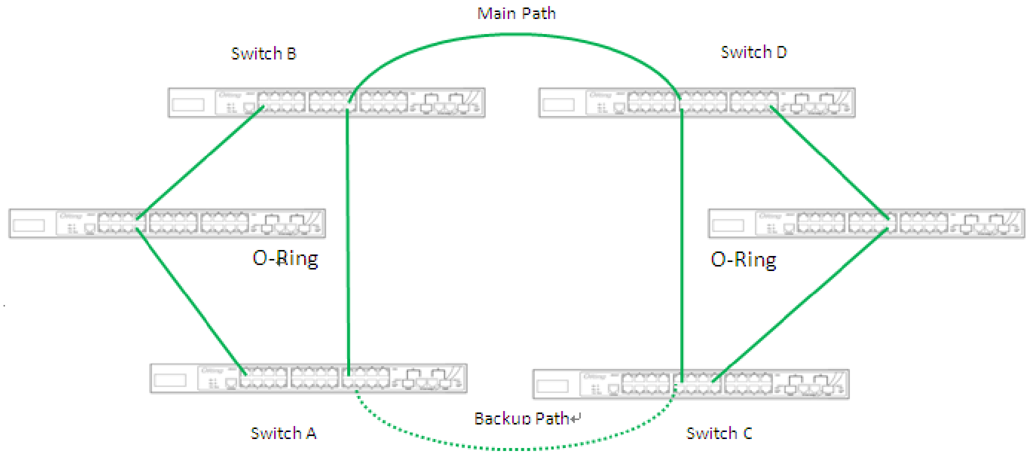


Coupling Ring

If you already have two Redundant Rings topologies and would like to connect the rings, you can form them into a coupling ring. Just select two switches from each ring to be connected ; for example, switch A and B from Ring 1 and switch C and D from Ring 2.

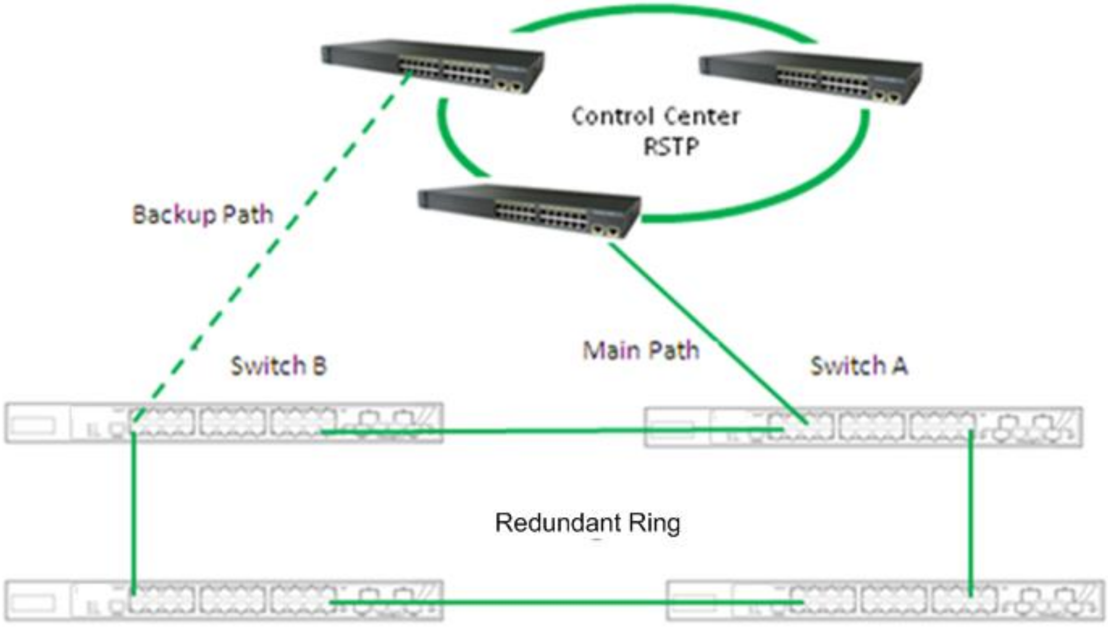
Decide which port on each switch to be used as the coupling port and then link them together (e.g., port 1 of switch A to port 2 of switch C and port 1 of switch B to port 2 of switch D).

Then, enable Coupling Ring on the management page and select the coupling ring in correspondance to the connected port. For more information on port setting, please refer to [4.1.2 Configurations](). Once the setting is completed, one of the connections will act as the main path while the other will act as the backup path.



Dual Homing

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



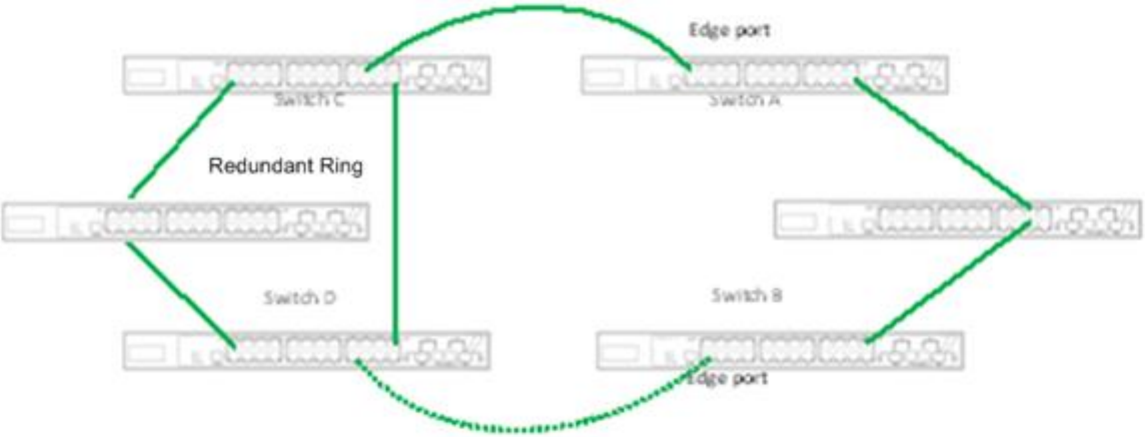
Multiple Ring (SISGM-CHAS-L3 and SISGM-L3-C Only)

When connecting multiple Redundant Rings to meet your expansion demand, you can create a Multiple Ring topology by following these steps.

1. Select two switches from the chain (Switch A & B) that you want to connect to the Redundant Rings and connect them to the switches in the ring (Switch C & D).

2. In correspondence to the ports connected to the ring, configure an edge port for both of the connected switches in the chain by checking the box in the management page (see 4.1.2 Configurations).

3. Once the setting is completed, one of the connections will act as the main path, and the other as the back up path.



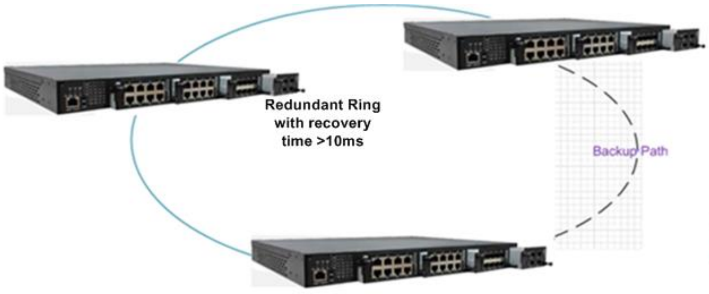
4. Redundancy

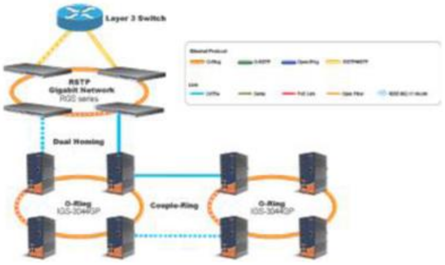
Redundancy for minimized system downtime is one of the most important concerns for industrial networking devices. Hence, Transition Networks has developed redundancy technologies including Redundant-Ring and Open-Ring featuring faster recovery time than existing redundancy technologies widely used in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

4.1 Redundant Ring Technology

4.1.1 Introduction

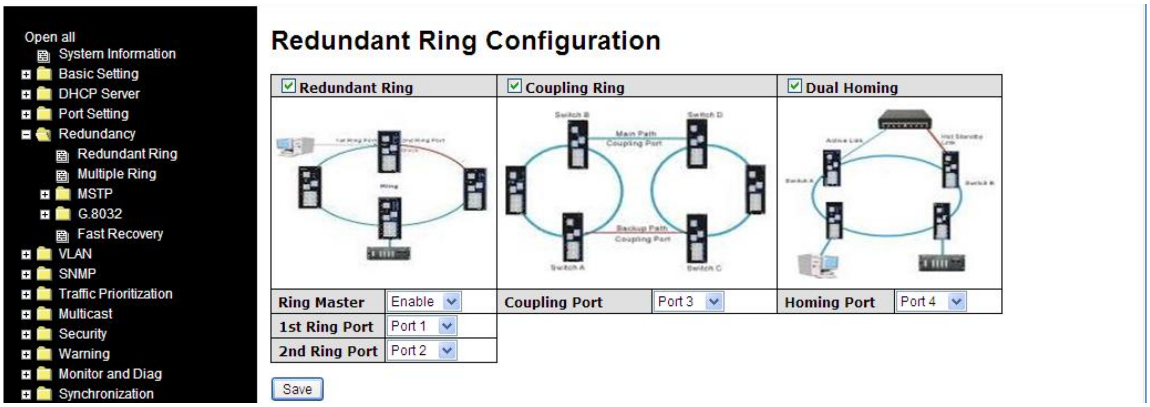
The switch provides redundant ring technology with recovery time of less than 30 milliseconds (in full-duplex Gigabit operation) or 10 milliseconds (in full-duplex Fast Ethernet operation) and up to 250 nodes. The ring protocols identify one switch as the master of the network, and then automatically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





4.1.2 Redundant Ring Configuration

The SISGM supports three ring topologies: **Ring Master**, **Coupling Ring**, and **Dual Homing**.



Redundant Ring Configuration

☑ Redundant Ring | ☑ Coupling Ring | ☑ Dual Homing

Ring Master	Enable	Coupling Port	Port 3	Homing Port	Port 4
1st Ring Port	Port 1				
2nd Ring Port	Port 2				

Label	Description
Redundant Ring	Check to enable Redundant Rings topology.
Ring Master	Only one ring master is allowed in a ring. However, if more than one switch is set to enable **Ring Master**, the switch with the lowest MAC address will be the active ring master and the others will be backup masters.
1st Ring Port	The primary ring port.
2nd Ring Port	The backup ring port.
Coupling Ring	Check to enable **Coupling Ring**. **Coupling Ring** can divide a big ring into two smaller rings to avoid network topology changes affecting all switches. It is a good method for connecting two rings.
Coupling Port	Ports for connecting multiple rings (Layer 3 Chassis only). A coupling ring needs four switches to build an active and a backup link. Links formed by the coupling ports will run in active/backup mode.
Dual Homing	Check to enable **Dual Homing**. When **Dual Homing** is enabled, the ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work in active/backup mode, and connect each ring to the normal switches in RSTP mode.
Apply	Click to apply the configurations.

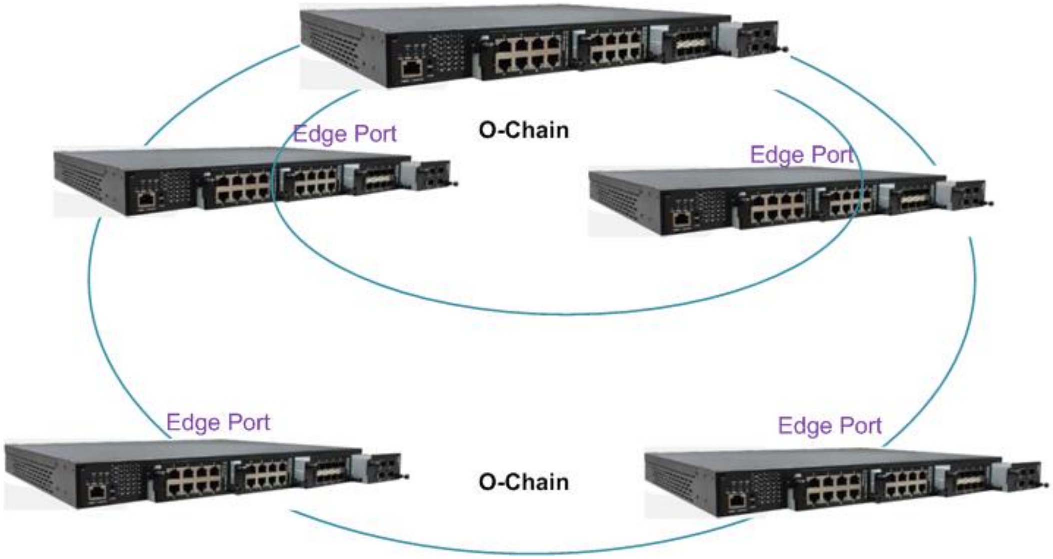
⚠ Due to heavy computing loading, setting one switch as both Ring Master and Coupling Ring at the same time is not recommended.

4.2 Multiple Ring

4.2.1 Introduction

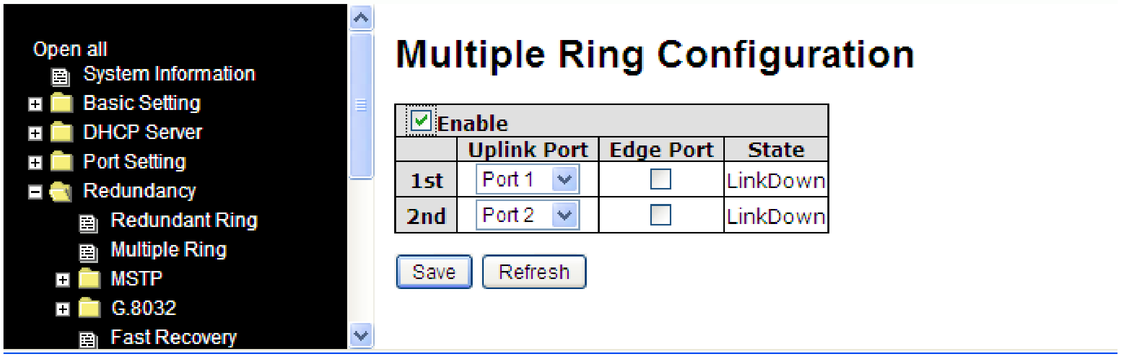
Multiple Ring is the revolutionary network redundancy technology which enhances network redundancy for any backbone networks, providing ease-of-use and maximum fault-recovery swiftness, flexibility, compatibility, and cost-effectiveness in a set of network redundancy topologies. The self-healing Ethernet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

Multiple Ring allows multiple redundant rings of different redundancy protocols to join and function together as a large robust network topology. It can create multiple redundant networks beyond the limitations of current redundant ring technologies.



4.2.2 Multiple Ring Configuration

Multiple Ring is very easy to configure and manage. Only one edge port of the edge switch needs to be defined. Switches other than the edge switch just need to have Multiple Ring enabled.



Multiple Ring Configuration

☑ Enable

	Uplink Port	Edge Port	State
1st	Port 1	□	LinkDown
2nd	Port 2	□	LinkDown

Label	Description
Enable	Check to enable the Multiple Ring function.
1st Ring Port	The first port connecting to the ring.
2nd Ring Port	The second port connecting to the ring.
Edge Port	A Multiple Ring topology must begin with edge ports. The ports with a smaller switch MAC address will serve as the backup link and RM LED will light up.
State	The port state (Link Up, Link Down, Forwarding).

***Messages**: Ring Error*

Another redundancy protocol is running. Only one protocol is acitve at the same time.

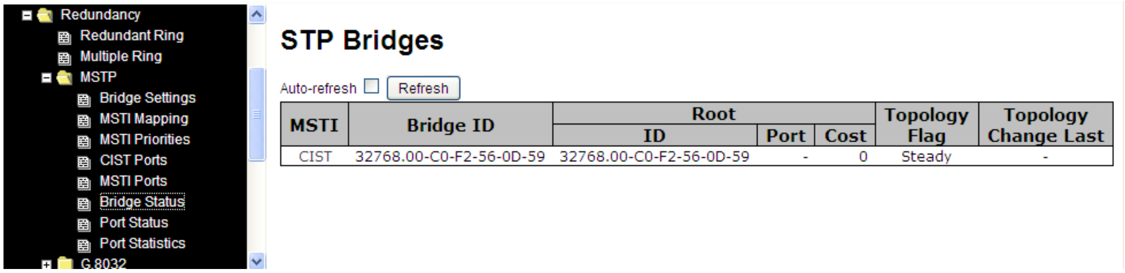
4.4 STP/RSTP/MSTP

4.4.1 STP/RSTP

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

STP Bridge Status

This page shows the status for all STP bridge instances.



STP Bridges

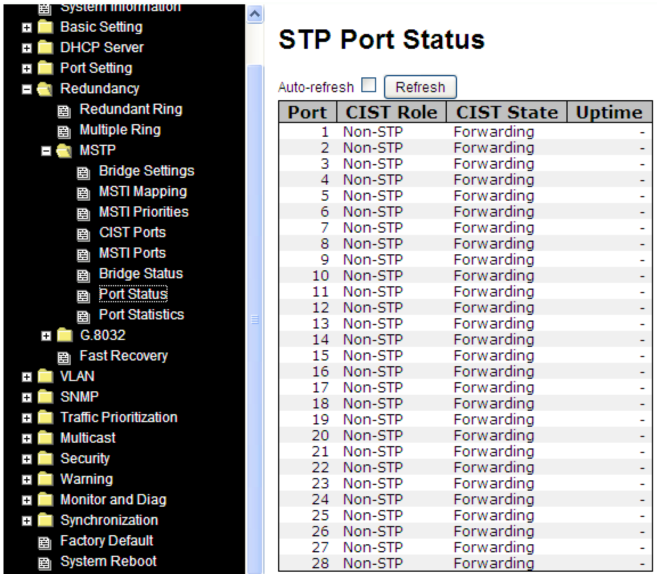
MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-C0-F2-56-0D-59	32768.00-C0-F2-56-0D-59	-	0	Steady	-

The STP Bridges parameters are described below.

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

STP Port Status

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



STP Port Status

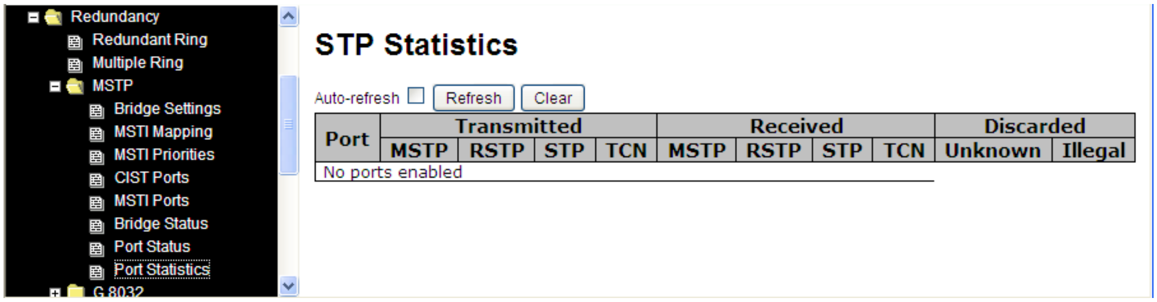
Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding	-
13	Non-STP	Forwarding	-
14	Non-STP	Forwarding	-
15	Non-STP	Forwarding	-
16	Non-STP	Forwarding	-
17	Non-STP	Forwarding	-
18	Non-STP	Forwarding	-
19	Non-STP	Forwarding	-
20	Non-STP	Forwarding	-
21	Non-STP	Forwarding	-
22	Non-STP	Forwarding	-
23	Non-STP	Forwarding	-
24	Non-STP	Forwarding	-
25	Non-STP	Forwarding	-
26	Non-STP	Forwarding	-
27	Non-STP	Forwarding	-
28	Non-STP	Forwarding	-

The STP Port Status parameters are described below.

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

STP Statistics

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



STP Statistics

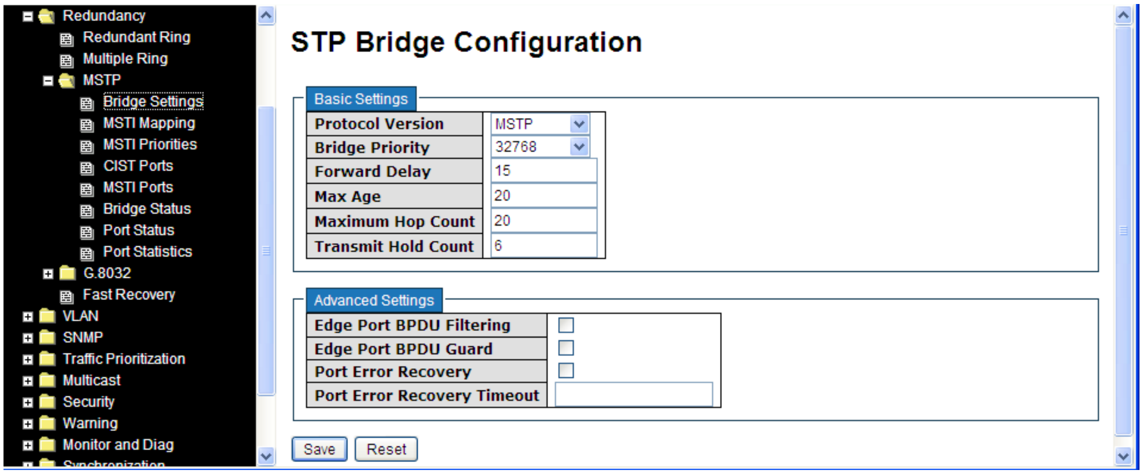
Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
No ports enabled										

The STP Statistics for a port are described below.

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

STP Bridge Configuration

This page lets you configure STP system settings used by all STP Bridge instances.



STP Bridge Configuration

Basic Settings

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

Advanced Settings

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

The STP Bridge Configuration parameters are described below.

Label	Description
Protocol Version	The version of the STP protocol. Valid values include STP, RSTP and MSTP.
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. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
Forward Delay	The delay used by STP bridges to transit root and designated ports to forwarding (used in STP compatible mode). The range of valid values is 4 - 30 seconds.
Max Age	The maximum time the information transmitted by the root bridge is considered valid. The range of valid values is 6 to 40 seconds, and **Max Age** must be <= (FwdDelay-1)*2.
Maximum Hop Count	This defines the initial value of remaining hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. The range of valid values is 4 to 30 seconds, and MaxAge must be <= (FwdDelay-1)*2.

Transmit Hold Count	The number of BPDUs a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. The range of valid values is 1 to 10 BPDUs per second.
Edge Port BPDU Filtering	Controls whether a port explicitly configured as Edge will transmit and receive BPDUs (Bridge Protocol Data Units).
Edge Port BPDU Guard	Controls 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	Controls whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports must 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 30 - 86400 seconds (24 hours).
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

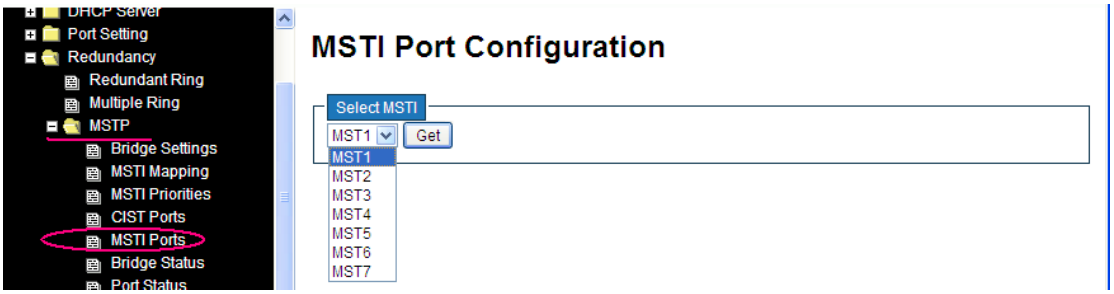
4.4.2 MSTP

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

Port Settings

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

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

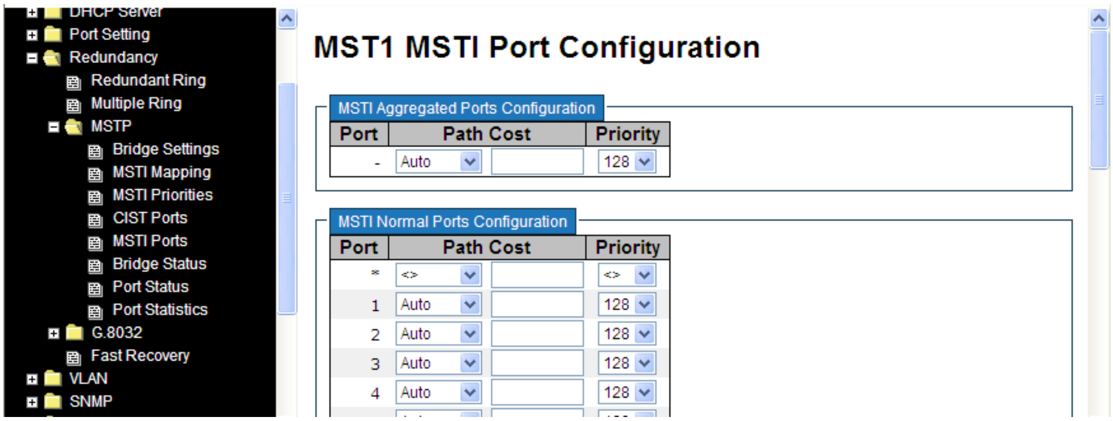


MSTI Port Configuration

Select MSTI

MST1

Select a MSTI instance from the dropdown and click the **Get** button.



MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost		Priority
-	Auto		128

MSTI Normal Ports Configuration

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

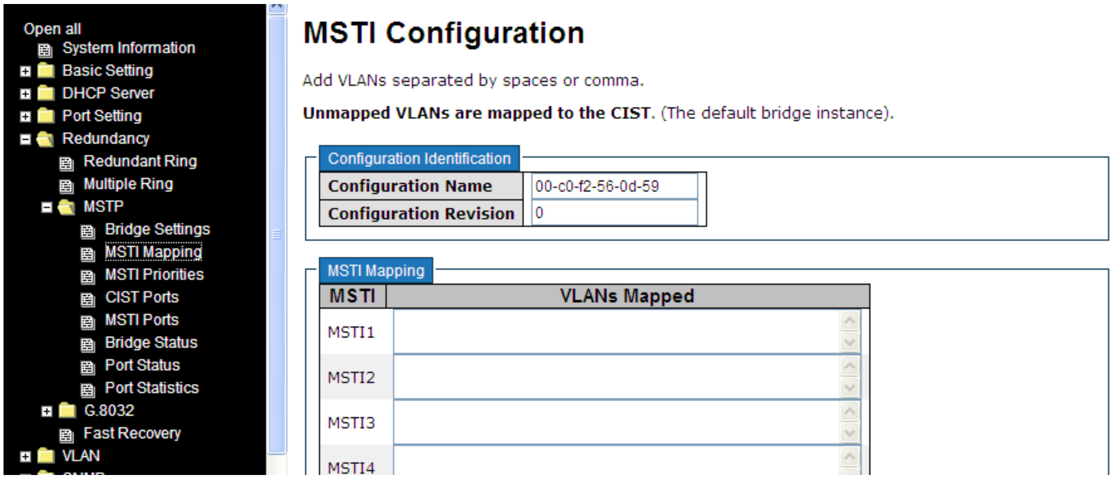
The MSTI Port Configuration parameters are described below.

MSTI Port Configuration Parameters

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

Mapping

This page lets you examine and configure the current STP MSTI bridge instance.



MSTI Configuration

Add VLANs separated by spaces or comma.

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

Configuration Identification

Configuration Name	00-c0-f2-56-0d-59
Configuration Revision	0

MSTI Mapping

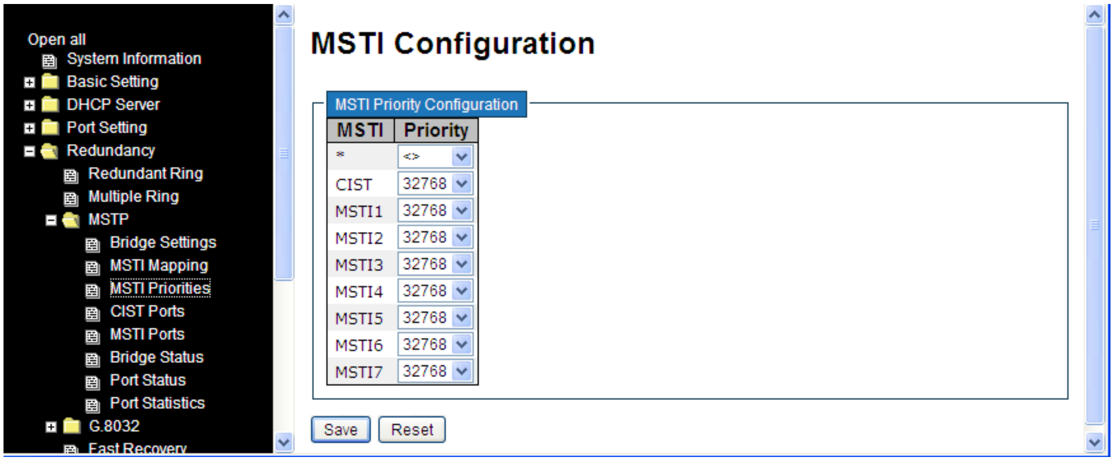
MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	

The MSTI Configuration Identification and MSTI Mapping parameters are described below.

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

Priority

The MSTI Priorities page lets you examine and change the configurations of current STP MSTI bridge instance priority.



MSTI Configuration

MSTI Priority Configuration

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

The MSTI Priority Configuration parameters are described below.

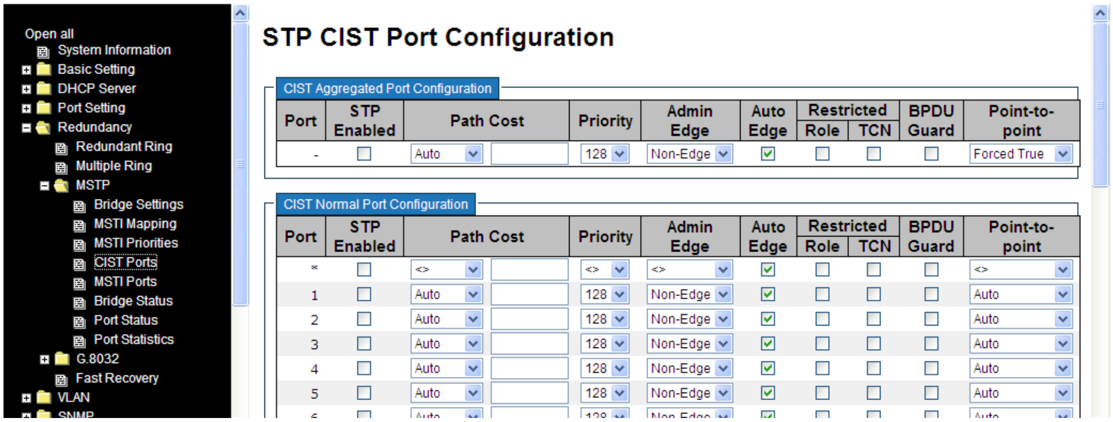
Label	Description
MSTI	The bridge instance. CIST is the default instance, which is always active.
Priority	Indicates bridge priority. The lower the value, the higher the priority. The bridge priority, MSTI instance number, and the 6-byte MAC address of the switch forms a bridge identifier.
Save	Click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

4.4.3 CIST

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

Port Settings

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well. This page contains settings for physical and aggregated ports. The aggregation settings are stack global.



STP CIST Port Configuration

CIST Aggregated Port Configuration

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

CIST Normal Port Configuration

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

The STP CIST Port Configuration parameters are described below.

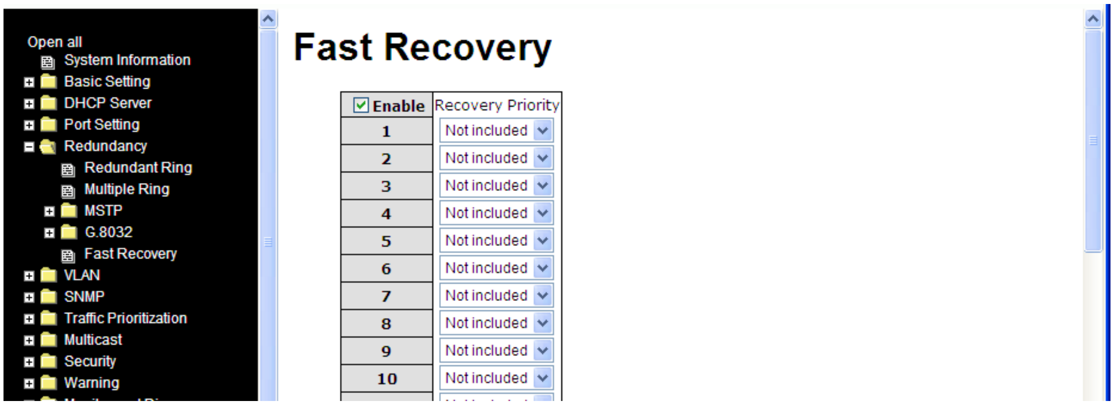
Label	Description
Port	The switch port number to which the following settings will be applied.
STP Enabled	Check to enable STP for the port.
Path Cost	Configures the path cost incurred by the port. **Auto** will set the path cost according to the physical link speed by using the 802.1D-recommended values. **Specific** allows you to enter a user-defined value. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are 1 - 200000000.
Priority	Configures the priority for ports having identical port costs (see above).

AdminEdge	Configures the operEdge flag to start as set or cleared.(the initial operEdge state when a port is initialized).
AutoEdge	Check to enable the bridge to detect edges at the bridge port automatically. This allows **operEdge** to be derived from whether BPDUs are received on the port or not.
Restricted Role	When enabled, the port will not be selected as root port for CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an alternate port after the root port has been selected. If set, spanning trees will lose connectivity. It can be set by a network administrator to prevent bridges outside a core region of the network from influencing the active spanning tree topology because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
Restricted TCN	When enabled, the port will not propagate received topology change notifications and topology changes to other ports. If set, it will cause temporary disconnection after changes in an active spanning trees topology as a result of persistent incorrectly learned station location information. It is set by a network admin to prevent bridges outside a core region of the network from causing address flushing in that region because those bridges are not under the full control of the administrator or is the physical link state for the attached LANs transitions frequently.
BPDU Guard	If checked, causes the port to disable itself upon receiving valid BPDUs. Contrary to the similar bridge setting, the port Edge status does not affect this setting. The default is unchecked. A port entering error-disabled state due to this setting is subject to the bridge 'Port Error Recovery' setting as well.
Point-to-Point	Configures whether the port connects to a point-to-point LAN rather than a shared medium. This can be configured automatically or set to true or false manually. Transiting to forwarding state is faster for point-to-point LANs than for shared media.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

4.5 Fast Recovery

Fast recovery mode can be set to connect multiple ports to one or more switches. The SISGM series with fast recovery mode will provide redundant links. Fast recovery mode supports 28 priorities. Only the first priority will be the active port, and the other ports with different priorities will be backup ports.

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



Fast Recovery

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

The Fast Recovery parameters are described below.

Label	Description
Enable	Check to enable the Fast Recovery function.
Recovery Priority	The port has the highest recovery priority (the lowest number) will be the active port; others will be blocked (if included).
Save	Click to save the configurations.

5. Management

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

Preparing for Web Management

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

IP Address: **192.168.1.77**

Subnet Mask: **255.255.255.0**

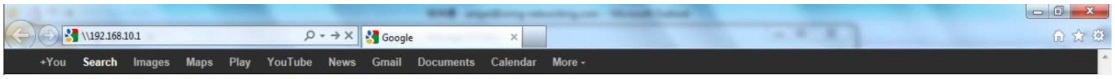
Default Gateway: **192.168.1.254**

User Name: **root**

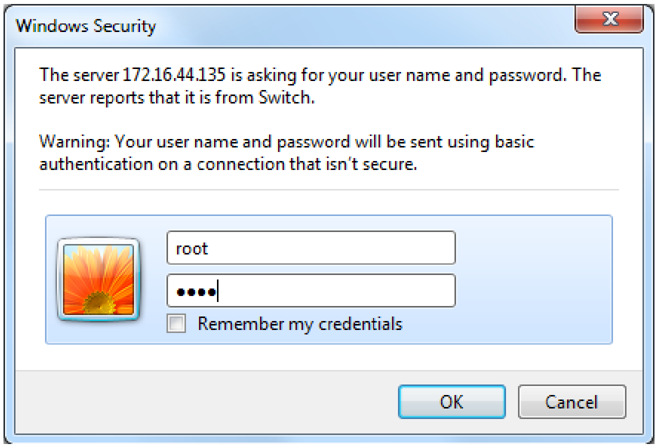
Password: **root**

System Login

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



3. A login screen displays.
4. Type the username and password. The default username and password is **root**.



Windows Security

The server 172.16.44.135 is asking for your user name and password. The server reports that it is from Switch.

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

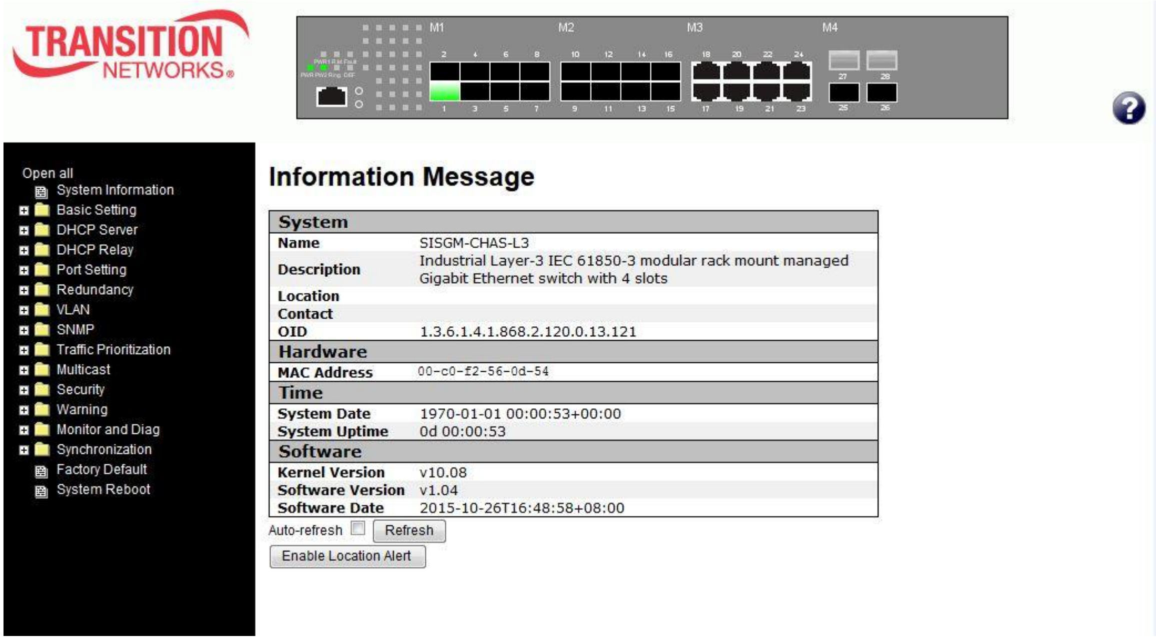
root

••••

□ Remember my credentials

5. Click **Enter** or **OK** button, the management Web page displays.

After logging in, the Information Message page displays as shown below.



Information Message

System	
Name	SISGM-CHAS-L3
Description	Industrial Layer-3 IEC 61850-3 modular rack mount managed Gigabit Ethernet switch with 4 slots
Location	
Contact	
OID	1.3.6.1.4.1.868.2.120.0.13.121
Hardware	
MAC Address	00-c0-f2-56-0d-54
Time	
System Date	1970-01-01 00:00:53+00:00
System Uptime	0d 00:00:53
Software	
Kernel Version	v10.08
Software Version	v1.04
Software Date	2015-10-26T16:48:58+08:00

Auto-refresh ☐ Refresh

Enable Location Alert

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

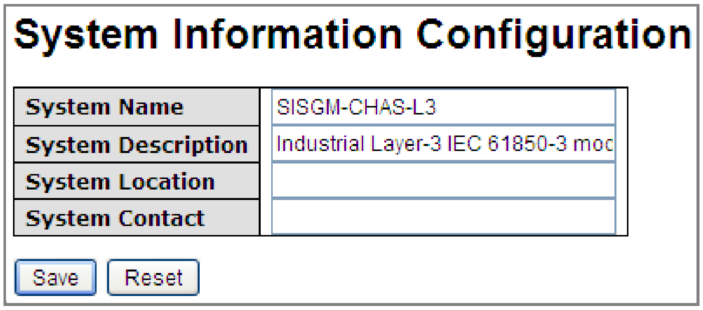
The **Enable Location Alert** button is reserved for future use.

5.1 Basic Settings

Basic Settings let you configure basic switch functions.

5.1.1 System Information

This page shows general switch information.



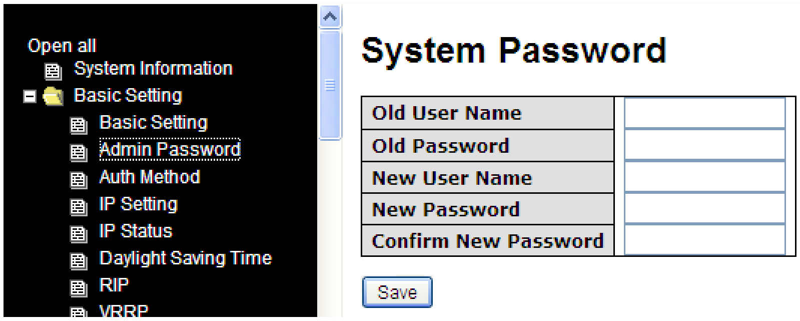
System Information Configuration

System Name	SISGM-CHAS-L3
System Description	Industrial Layer-3 IEC 61850-3 moc
System Location	
System Contact	

.Label	Description
System Name	An administratively assigned name for the managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string consisting of alphabets (A-Z, a-z), digits (0-9), and minus sign (-). Space is not allowed to be part of the name. The first character must be an alpha character, and the first or last character must not be a minus sign. The allowed string length is 0 to 255 characters.
System Description	A description of the device.
System Location	The physical location of the node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and only ASCII characters from 32 to 126 are allowed.
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and only ASCII characters from 32 to 126 are allowed.

5.1.2 System Password

The **Basic Setting** > **Admin Password** page lets you configure the system password required to access the web pages or log in from CLI.



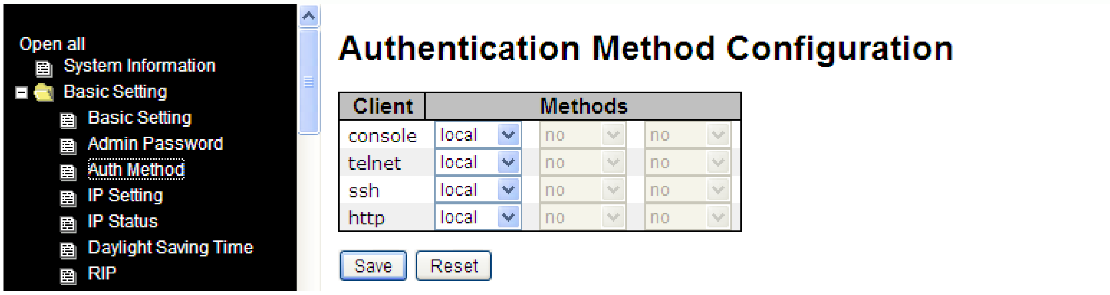
System Password

Old User Name	
Old Password	
New User Name	
New Password	
Confirm New Password	

Label	Description
Old User Name	The existing User Name. If this is incorrect, you can set the new password.
Old Password	The existing password. If this is incorrect, you cannot set the new password.
New User Name	The new User Name.
New Password	The new system password. The allowed string length is 0 to 31, and only ASCII characters from 32 to 126 are allowed.
Confirm New Password	Re-type the new password.
Save	Click to save changes.

5.1.3 Authentication

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



Authentication Method Configuration

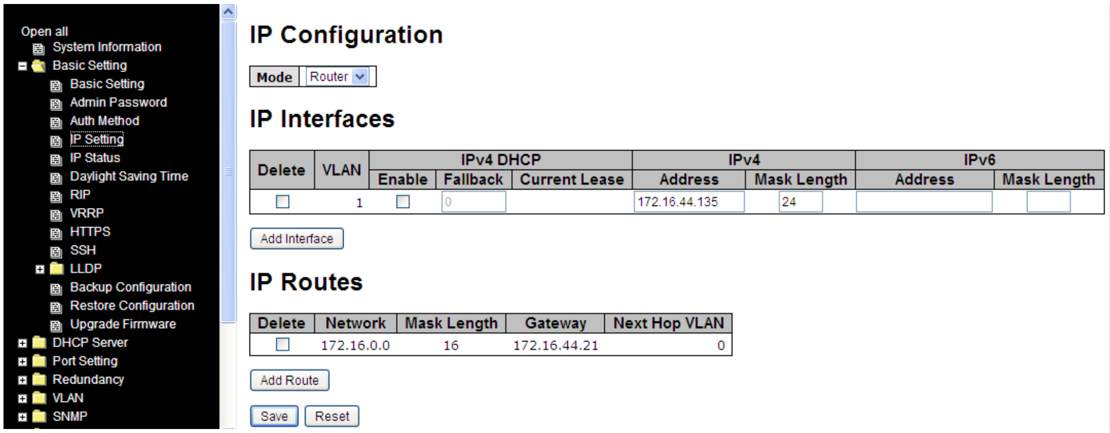
Client	Methods		
console	local	no	no
telnet	local	no	no
ssh	local	no	no
http	local	no	no

The table has one row for each client type and these columns:

Label	Description
Client	The management client for which the configuration below applies (console, telnet, ssh, http).
Authentication Methods	The Authentication 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 stack for authentication. **radius**: Use remote RADIUS server(s) for authentication. **tacacs+**: Use *remote* TACACS+ server(s) for authentication. Methods that involve 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.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values

5.1.4 IP Setting

You can configure IP information of the switch on this page. The maximum number of interfaces supported is 128 and the maximum number of routes is 1024.



IP Configuration

Mode: Router

IP Interfaces

Delete	VLAN	IPv4 DHCP			IPv4		IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Address	Mask Length
□	1	□	0		172.16.44.135	24		

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
□	172.16.0.0	16	172.16.44.21	0

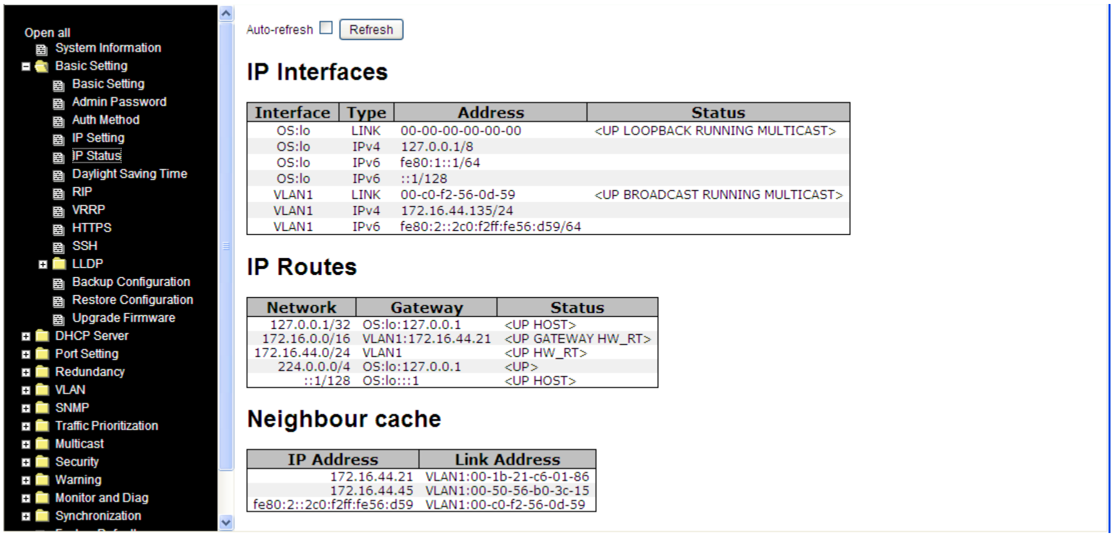
Label	Description
IP Configuration Mode	Configure whether the IP stack should act as a **Host** or a **Router**. In **Host** mode, IP traffic between interfaces will not be routed. In **Router** mode traffic is routed between all interfaces.
IP Interfaces	
Delete	Select this option to delete an existing 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 an new interface.
IPv4 DHCP Enable	Enable the DHCP client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
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 is not used. The field may also be left blank if IPv4 operation on the interface is not desired.
IPv4 Mask Length	The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address. If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.
IPv6 Address	The IPv6 address of the interface. A IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, ::192.1.2.34. The field may be left blank if IPv6 operation on the interface is not desired.
IPv6 Mask Length	The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for a IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.
IP Routes	
Delete	Select this option to delete an existing route.
Network	The IP route network IP. The destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0 or IPv6 :: notation.
Mask Length	The IP route network mask. 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 0 - 32 bits for IPv4 routes or 0 - 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).
Gateway	The IP address of the IP gateway. Valid format is dotted decimal notation or a valid IPv6 notation. The Gateway and Network must be of the same type.

	It may be necessary to add a static route if a default gateway is required or if the device does not reside within the same network. Routing can then be enabled at **System** > **IP** > **IP Configuration**. A default route (AKA, *gateway of last resort*) is the network route used by a router when no other known route exists for an IP packet's destination address (**Network** = **0.0.0.0**, **Mask Length** = **0**, **Gateway 10.0.1.1** as shown above).
Next Hop VLAN	The VLAN ID (VID) of the next hop VLAN.
Add Route	Click to add a row to the table to configure another route.
Add Interface	Click to add a row to the table to configure another interface.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.5 IP Status

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



IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80:1::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	00-c0-f2-56-0d-59	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	172.16.44.135/24	
VLAN1	IPv6	fe80:2::2c0:f2ff:fe56:d59/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	OS:lo:127.0.0.1	<UP HOST>
172.16.0.0/16	VLAN1:172.16.44.21	<UP GATEWAY HW_RT>
172.16.44.0/24	VLAN1	<UP HW_RT>
224.0.0.0/4	OS:lo:127.0.0.1	<UP>
::1/128	OS:lo:::1	<UP HOST>

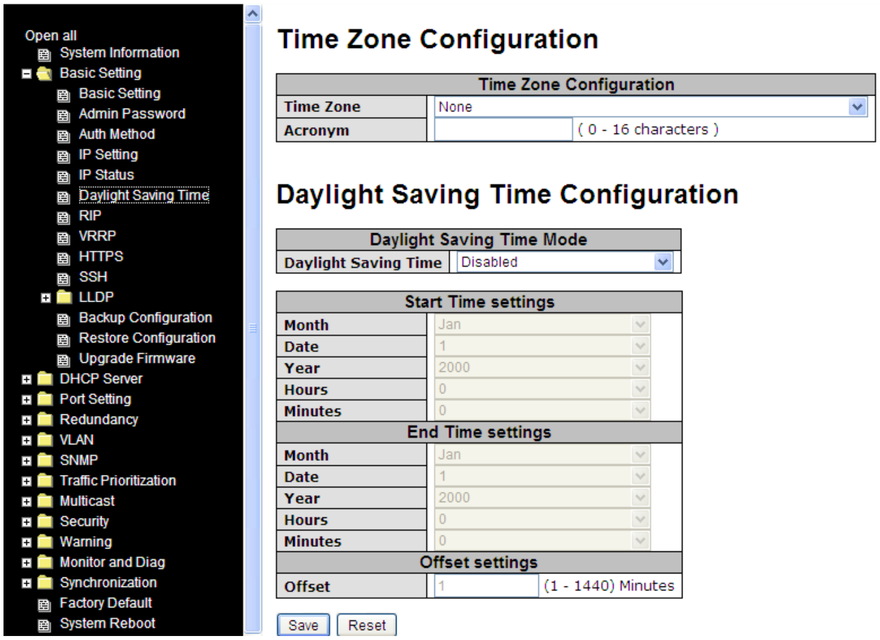
Neighbour cache

IP Address	Link Address
172.16.44.21	VLAN1:00-1b-21-c6-01-86
172.16.44.45	VLAN1:00-50-56-b0-3c-15
fe80:2::2c0:f2ff:fe56:d59	VLAN1:00-c0-f2-56-0d-59

Label	Description
IP Interfaces	
Interface	The name of the IP 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).
IP Routes	
Network	The destination IP 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.
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.6 Daylight Saving Time

This page is used to setup Time zones and Daylight Saving Time configuration.



Time Zone Configuration

Time Zone Configuration	
Time Zone	None
Acronym	(0 - 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled

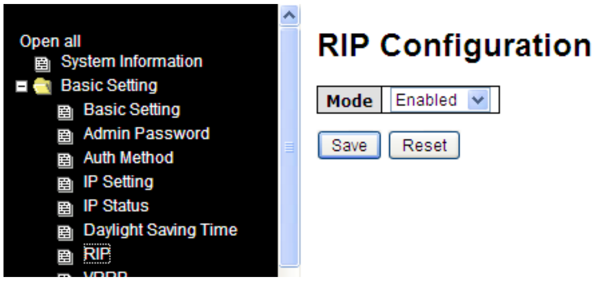
Start Time settings	
Month	Jan
Date	1
Year	2000
Hours	0
Minutes	0
End Time settings	
Month	Jan
Date	1
Year	2000
Hours	0
Minutes	0
Offset settings	
Offset	1 (1 - 1440) Minutes

Label	Description
Time Zone Configuration	
Time Zone	Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Save to set.
Acronym	Set the acronym of the time zone. This is a user configurable acronym to identify the time zone. (Range: up to 16 characters.)
Daylight Saving Time Configuration	This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default : Disabled)
Start time settings	• Week - Select the starting week number. • Day - Select the starting day. • Month - Select the starting month.

	• Hours - Select the starting hour. • Minutes - Select the starting minute.
End time settings	• Week - Select the ending week number. • Day - Select the ending day. • Month - Select the ending month. • Hours - Select the ending hour. • Minutes - Select the ending minute.
Offset	Enter the number of minutes to add during Daylight Saving Time. (Range: 1 - 1440 minutes.)
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.7 RIP

Layer 3 Chassis only. This page is used to configure RIP (Routing Information Protocol).



RIP Configuration

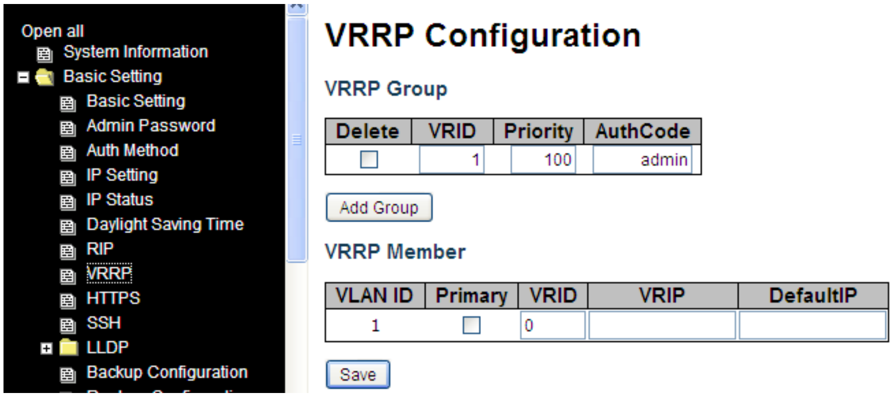
Mode: Enabled

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

5.1.8 VRRP

This page is used to configure Virtual Router Redundancy Protocol.

VRRP provides for automatic assignment of available IP routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork. The protocol does this by creation of virtual routers, which are an abstract representation of multiple routers (i.e., master and backup routers, acting as a group). The default gateway of a participating host is assigned to the virtual router instead of a physical router. If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected to automatically replace it. See IETF RFC 5798.



VRRP Configuration

VRRP Group

Delete	VRID	Priority	AuthCode
□	1	100	admin

VRRP Member

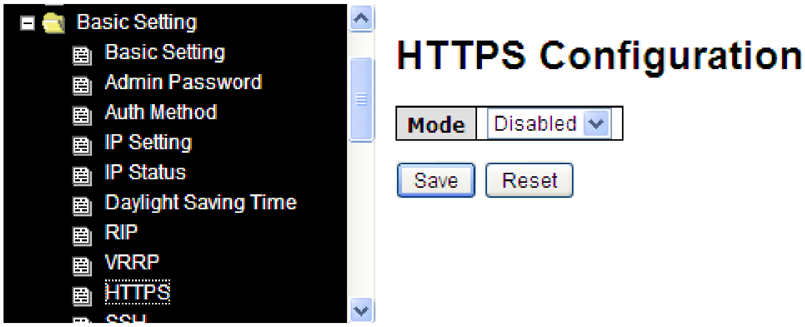
VLAN ID	Primary	VRID	VRIP	DefaultIP
1	□	0		

There are several options for each VRRP Group and each VLAN:

Label	Description
VRID	Virtual Router ID, from 1 to 254.
Priority	Priority, from 1 to 254.
AuthCode	Password, 8 characters.
Primary	Check if Primary interface for a VRRP Group.
VRID	Belongs to the VRRP Group with this ID. (Zero means no group.)
VRIP	Virtual Router IP.
DefaultIP	If this vlan get into backup state from master state, this interface would recover by this IP.
Save	Click to save changes.

5.1.9 HTTPS

You can configure HTTPS settings on the following page.



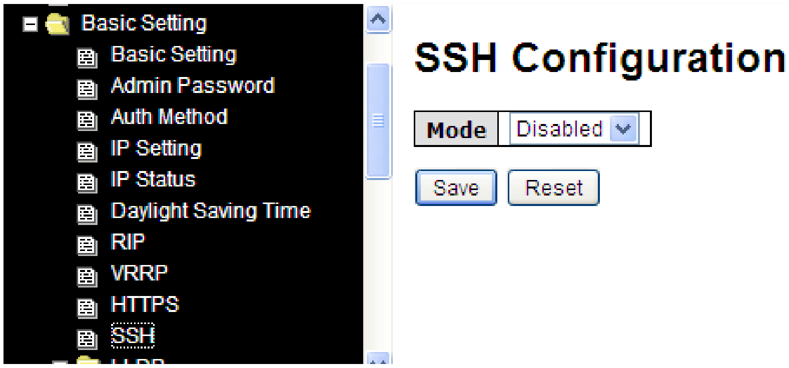
HTTPS Configuration

Mode: Disabled

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

5.1.10 SSH

You can configure SSH settings on the following page.



SSH Configuration

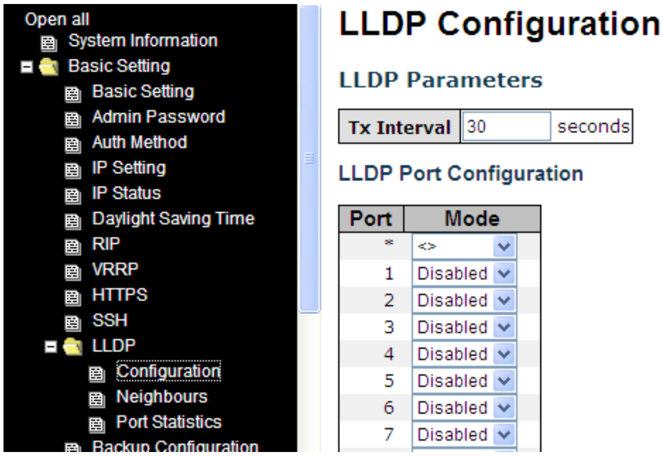
Mode: Disabled

Label	Description
Mode	Indicates the selected SSH mode; either: **Enabled**: enable SSH. **Disabled**: disable SSH.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.11 LLDP

LLDP Configuration

This page lets you examine and configure LLDP port settings.



LLDP Configuration

LLDP Parameters

Tx Interval 30 seconds

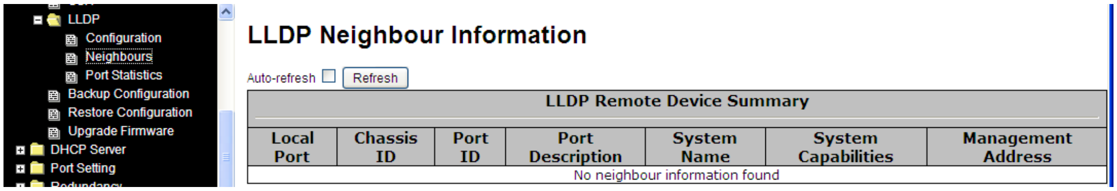
LLDP Port Configuration

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled

Label	Description
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 5 - 32768 seconds.
Port	The switch port number to which the following settings will be applied.
Mode	Indicates the selected LLDP mode **Rx only**: the switch will not send out LLDP information, but LLDP information from its neighbors will be analyzed. **Tx only**: the switch will drop LLDP information received from its neighbors, but will send out LLDP information. **Disabled**: the switch will not send out LLDP information, and will drop LLDP information received from its neighbors. **Enabled**: the switch will send out LLDP information, and will analyze LLDP information received from its neighbors.

LLDP Neighbor Information

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



LLDP Neighbour Information

Auto-refresh □ Refresh

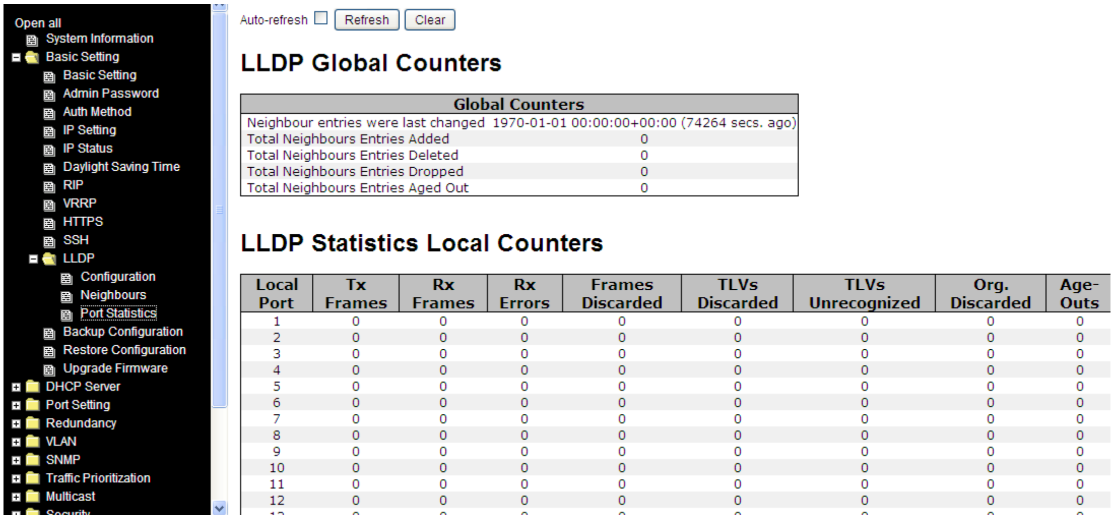
LLDP Remote Device Summary

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
No neighbour information found						

Label	Description
Local Port	The port that you use to transmits and receives LLDP frames.
Chassis ID	The identification number of the neighbor sending out the LLDP frames.
Remote Port ID	The identification of the neighbor port
System Name	The name advertised by the neighbor.
Port Description	The description of the port advertised by the neighbor.
System Capabilities	Description of the neighbor's capabilities. The capabilities include: 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, a (+) will be displayed. If the capability is disabled, a (-) will be displayed.
Management Address	The neighbor's address which can be used to help network management. This may contain the neighbor's IP address.
Refresh	Click to refresh the page immediately
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals

Port Statistics

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



Auto-refresh □ Refresh Clear

LLDP Global Counters

Global Counters	
Neighbour entries were last changed	1970-01-01 00:00:00+00:00 (74264 secs. ago)
Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

LLDP Statistics Local Counters

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

Global Counters

Label	Description
Neighbor entries were last changed at	Shows the time when the last entry was deleted or added.
Total Neighbors Entries Added	Shows the number of new entries added since switch reboot.
Total Neighbors Entries Deleted	Shows the number of new entries deleted since switch reboot.
Total Neighbors Entries Dropped	Shows the number of LLDP frames dropped due to full entry table
Total Neighbors Entries Aged Out	Shows the number of entries deleted due to expired time-to-live.

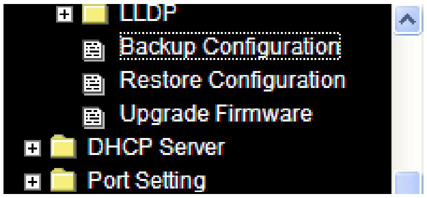
Local Counters

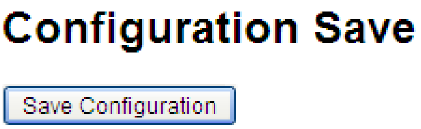
Label	**Description**
Local Port	The port that receives or transmits LLDP frames.
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.

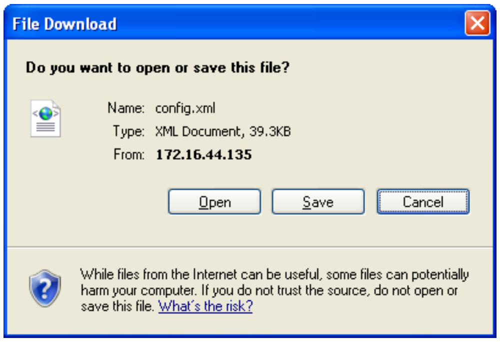
Rx Errors	The number of received LLDP frames containing errors.
Frames Discarded	If a port receives an LLDP frame, and the switch's internal table is full, the LLDP frame will be counted and discarded. This situation is known as "too many neighbors" in the LLDP standard. LLDP frames require a new entry in the table if Chassis ID or Remote Port ID is not included in the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (Type Length Value). If a TLV is malformed, it will be counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value
Org. Discarded	The number of organizationally TLVs received
Age-Outs	Each LLDP frame contains information about how long the LLDP information is valid (age-out time). If no new LLDP frame is received during the age-out time, the LLDP information is removed and the value of the age-out counter is incremented.
Refresh	Click to refresh the page immediately.
Clear	Click to clear the local counters. All counters (including global counters) are cleared upon reboot.
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals.

5.1.12 Backup (Save) Configurations

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



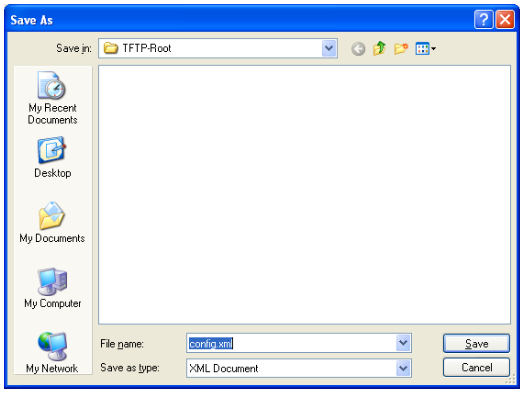




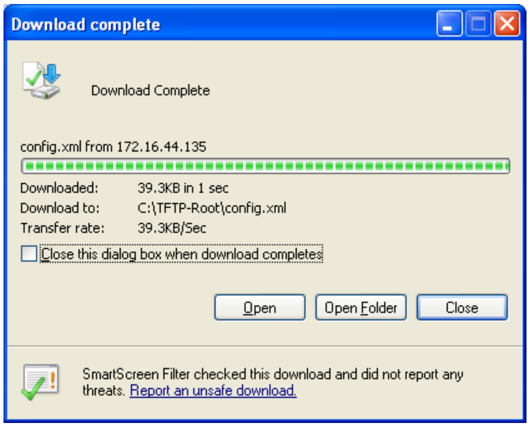
Do you want to open or save this file?

Name: config.xml
Type: XML Document, 39.3KB
From: **172.16.44.135**

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?



Save in: TFTP-Root
File name: config.xml
Save as type: XML Document



Download Complete

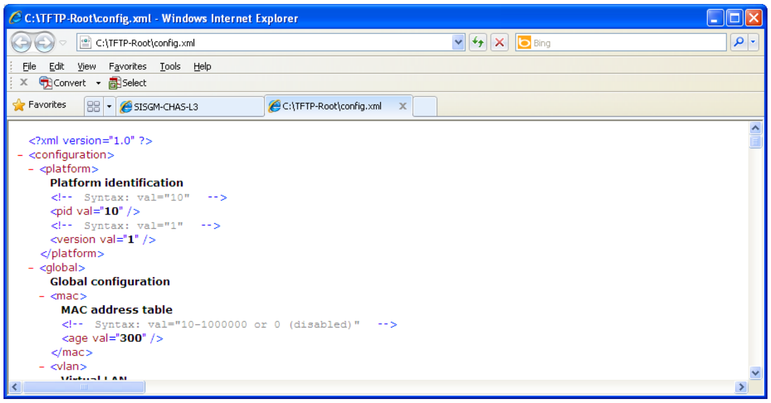
config.xml from 172.16.44.135

Downloaded: 39.3KB in 1 sec
Download to: C:\TFTP-Root\config.xml
Transfer rate: 39.3KB/Sec

□ Close this dialog box when download completes

SmartScreen Filter checked this download and did not report any threats. Report an unsafe download.

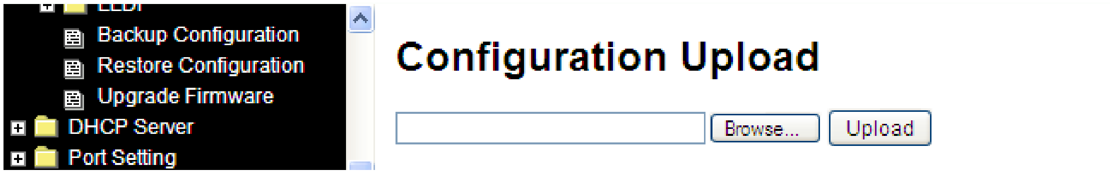
An example of a saved config.xml file is shown below:



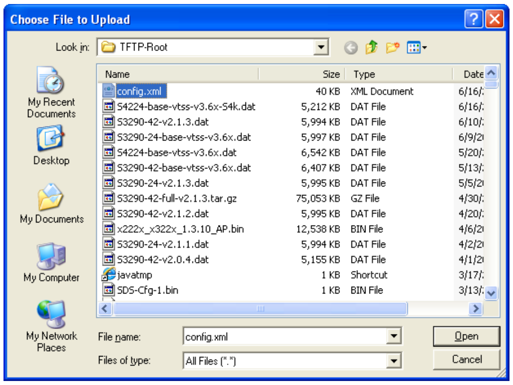
```
  <?xml version="1.0" ?>
- <configuration>
  - <platform>
      Platform identification
      <!--  Syntax: val="10"   -->
      <pid val="10" />
      <!--  Syntax: val="1"   -->
      <version val="1" />
    </platform>
  - <global>
      Global configuration
    - <mac>
        MAC address table
        <!--  Syntax: val="10-1000000 or 0 (disabled)"   -->
        <age val="300" />
      </mac>
    - <vlan>
        Virtual LAN
```

5.1.13 Restore Configuration

You can load the switch configuration. The configuration file is in XML format with a hierarchy of tags



Configuration Upload



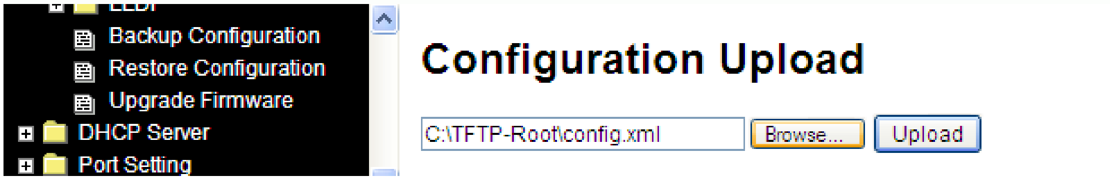
Choose File to Upload

Look in: TFTP-Root

Name	Size	Type	Date
config.xml	40 KB	XML Document	6/16/
S4224-base-vtss-v3.6x-S4k.dat	5,212 KB	DAT File	6/16/
S3290-42-v2.1.3.dat	5,994 KB	DAT File	6/10/
S3290-24-base-vtss-v3.6x.dat	5,997 KB	DAT File	6/9/2
S4224-base-vtss-v3.6x.dat	6,542 KB	DAT File	5/20/
S3290-42-base-vtss-v3.6x.dat	6,407 KB	DAT File	5/13/
S3290-24-v2.1.3.dat	5,995 KB	DAT File	5/5/2
S3290-42-full-v2.1.3.tar.gz	75,053 KB	GZ File	4/30/
S3290-42-v2.1.2.dat	5,995 KB	DAT File	4/20/
x222x_x322x_1.3.10_AP.bin	12,538 KB	BIN File	4/6/2
S3290-24-v2.1.1.dat	5,994 KB	DAT File	4/2/2
S3290-42-v2.0.4.dat	5,155 KB	DAT File	4/1/2
javatmp	1 KB	Shortcut	3/17/
SDS-Cfg-1.bin	1 KB	BIN File	3/13/

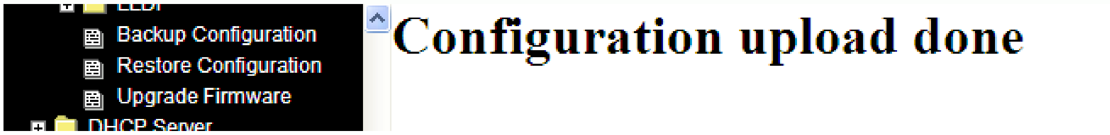
File name: config.xml

Files of type: All Files (*.*)



Configuration Upload

C:\TFTP-Root\config.xml



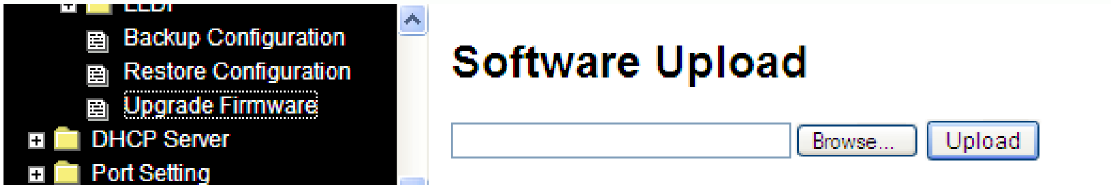
Configuration upload done

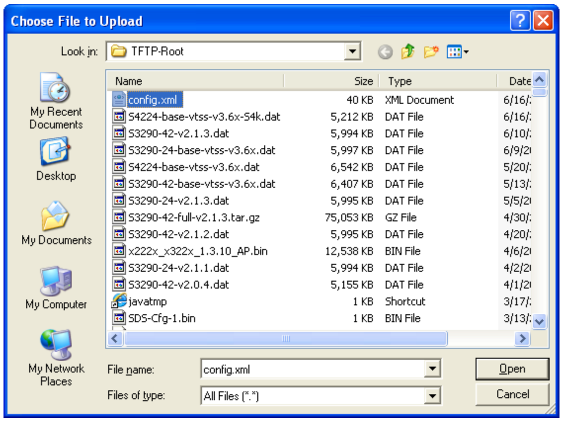
5.1.14 Upgrade Firmware

This page lets you update the switch firmware. 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. **Note**: The Layer 2 switch is NOT upgradeable to Layer 3.

Warning: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green at 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.

Browse to the location of a software image and click the **Upload** button.

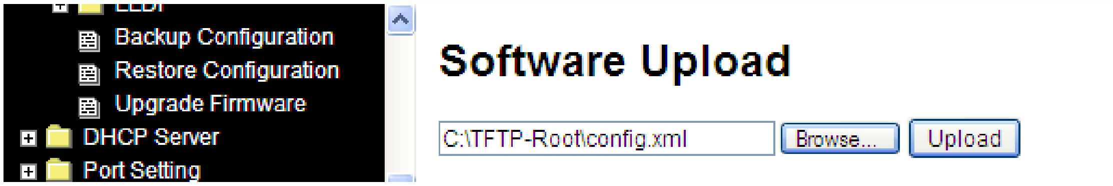




Name	Size	Type	Date
config.xml	40 KB	XML Document	6/16/
S4224-base-vtss-v3.6x-S4k.dat	5,212 KB	DAT File	6/16/
S3290-42-v2.1.3.dat	5,994 KB	DAT File	6/10/
S3290-24-base-vtss-v3.6x.dat	5,997 KB	DAT File	6/9/2
S4224-base-vtss-v3.6x.dat	6,542 KB	DAT File	5/20/
S3290-42-base-vtss-v3.6x.dat	6,407 KB	DAT File	5/13/
S3290-24-v2.1.3.dat	5,995 KB	DAT File	5/5/2
S3290-42-full-v2.1.3.tar.gz	75,053 KB	GZ File	4/30/
S3290-42-v2.1.2.dat	5,995 KB	DAT File	4/20/
x222x_x322x_1.3.10_AP.bin	12,538 KB	BIN File	4/6/2
S3290-24-v2.1.1.dat	5,994 KB	DAT File	4/2/2
S3290-42-v2.0.4.dat	5,155 KB	DAT File	4/1/2
javatmp	1 KB	Shortcut	3/17/
SDS-Cfg-1.bin	1 KB	BIN File	3/13/

File name: config.xml

Files of type: All Files (*.*)



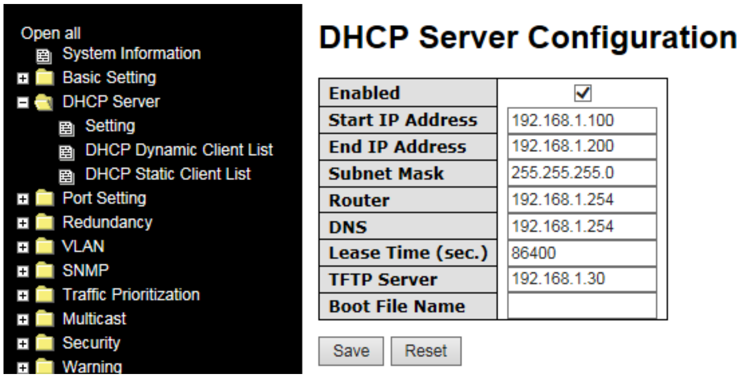
C:\TFTP-Root\config.xml

5.2 DHCP Server

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

5.2.1 Basic Settings

This page lets you set up DHCP settings for the switch. You can check the **Enabled** checkbox to activate the function. Once the box is checked, you can enter information in each field.



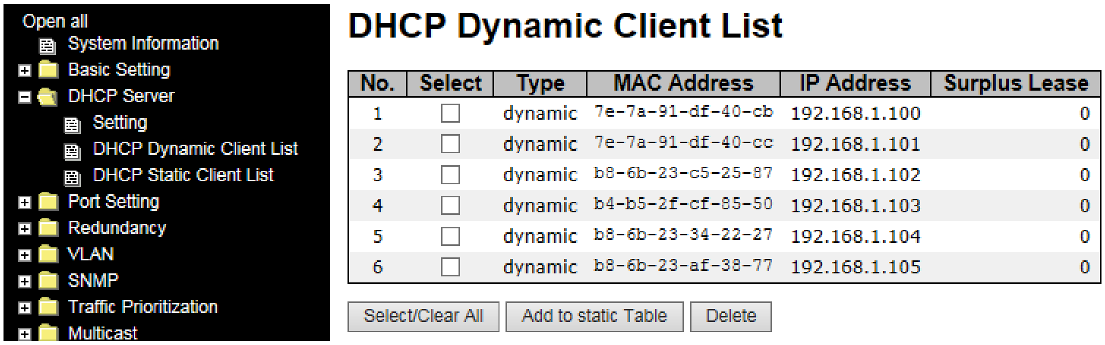
DHCP Server Configuration

Enabled	☑
Start IP Address	192.168.1.100
End IP Address	192.168.1.200
Subnet Mask	255.255.255.0
Router	192.168.1.254
DNS	192.168.1.254
Lease Time (sec.)	86400
TFTP Server	192.168.1.30
Boot File Name	

Label	Description
Enabled	Enable/Disable DHCP server.
Start IP Address	The start IP address of IP pool.
End IP Address	The end IP address of IP pool.
Subnet Mask	The subnet mask.
Router	The IP address of gateway.
DNS	The IP address of Domain Name Server.
Lease Time	Lease timer counted in seconds.
TFTP Server	The IP address of TFTP Sever (Option 66).
Boot File Name	The name of Boot File (Option 67).

5.2.2 DHCP Dynamic Client List

When DHCP server functions are activated, the switch will collect DHCP client information and display it in the following table. A DHCP server can automatically assign an IP address to a DHCP client.



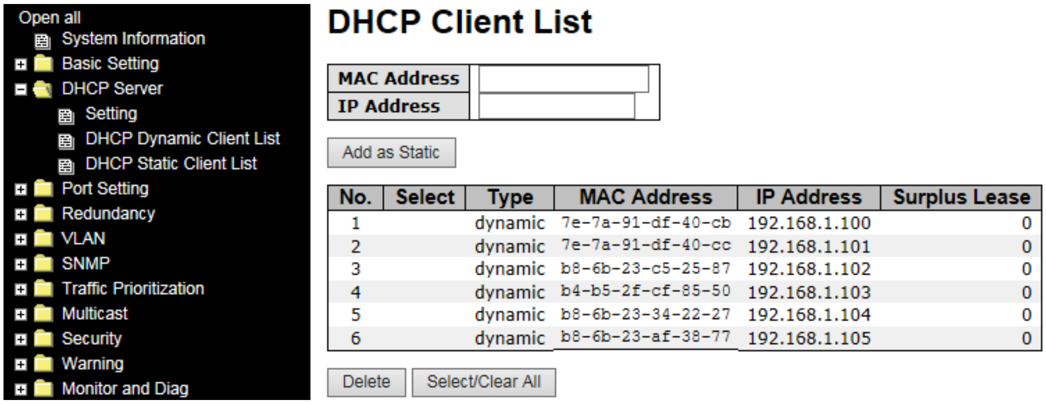
DHCP Dynamic Client List

No.	Select	Type	MAC Address	IP Address	Surplus Lease
1	□	dynamic	7e-7a-91-df-40-cb	192.168.1.100	0
2	□	dynamic	7e-7a-91-df-40-cc	192.168.1.101	0
3	□	dynamic	b8-6b-23-c5-25-87	192.168.1.102	0
4	□	dynamic	b4-b5-2f-cf-85-50	192.168.1.103	0
5	□	dynamic	b8-6b-23-34-22-27	192.168.1.104	0
6	□	dynamic	b8-6b-23-af-38-77	192.168.1.105	0

Label	Description
No.	Client list number.
Select	Check to select device.
Type	The type of client (Dynamic or Static).
MAC Address	The MAC Address of client.
IP Address	The IP address of client.
Surplus Lease	The surplus Lease time.
Select/Clear All	Select all or Clear all check boxes.
Add to static Table	Add selected device(s) to static table.
Delete	Delete selected device(s) from table.

5.2.3 DHCP Static Client List

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



DHCP Client List

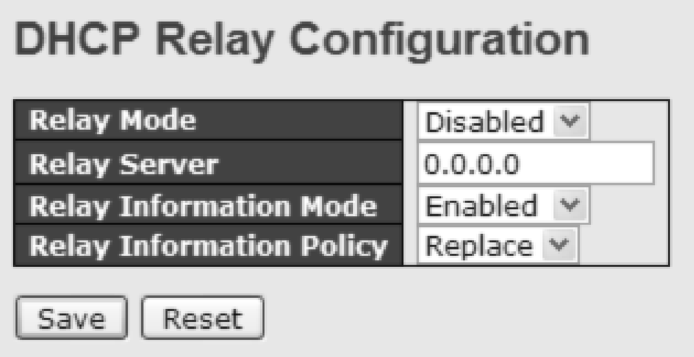
MAC Address	
IP Address	

No.	Select	Type	MAC Address	IP Address	Surplus Lease
1		dynamic	7e-7a-91-df-40-cb	192.168.1.100	0
2		dynamic	7e-7a-91-df-40-cc	192.168.1.101	0
3		dynamic	b8-6b-23-c5-25-87	192.168.1.102	0
4		dynamic	b4-b5-2f-cf-85-50	192.168.1.103	0
5		dynamic	b8-6b-23-34-22-27	192.168.1.104	0
6		dynamic	b8-6b-23-af-38-77	192.168.1.105	0

Label	Description
MAC Address	Enter the MAC Address of client.
IP Address	Enter the IP address of client.
No.	The instance number for this line.
Select	Select device.
Type	The type of client (**dynamic** or **static**).
MAC Address	Enter the MAC Address of client (12 characters).
IP Address	Displays the IP address of client.
Surplus Lease	Displays the surplus Lease time.
Select/Clear All	Click to Select or Clear all check boxes.
Delete	Delete the selected entry.
Add as Static	Click to add a Static entry to the static table.

5.2.4 DHCP Relay

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



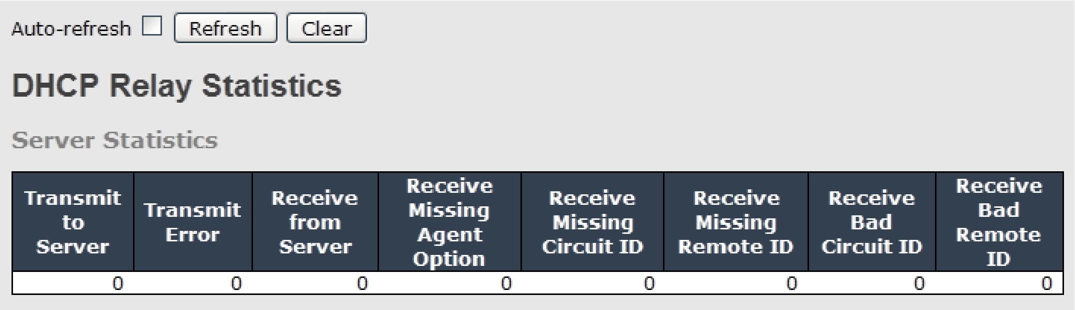
DHCP Relay Configuration

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

Label	Description
Relay Mode	Indicates the existing DHCP relay mode. The modes include: **Enabled**: activate DHCP relay. When DHCP relay is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain to prevent the DHCP broadcast message from flooding for security considerations. **Disabled**: disable DHCP relay
Relay Server	Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and transfer DHCP messages between the clients and the server when they are not in the same subnet domain.
Relay Information Mode	Indicates the existing DHCP relay information mode. The format of DHCP option 82 circuit ID format is "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, and the fifth and sixth characters are the module ID. In stand-alone devices, the module ID always equals to 0; in stacked devices, it means switch ID. The last two characters are the port number. For example, "00030108" means the DHCP message received form VLAN ID 3, switch ID 1, and port No. 8. The option 82 remote ID value equals to the switch MAC address.

	The modes include: **Enabled**: activate DHCP relay information. When DHCP relay information is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to a DHCP server and removes it from a DHCP message when transferring to a DHCP client. It only works when DHCP relay mode is enabled. **Disabled**: disable DHCP relay information
Relay Information Policy	Indicates the policies to be enforced when receiving DHCP relay information. When DHCP relay information mode is enabled, if the agent receives a DHCP message that already contains relay agent information, it will enforce the policy. The Replace option is invalid when relay information mode is disabled. The policies includes: **Replace**: replace the original relay information when a DHCP message containing the information is received. **Keep**: keep the original relay information when a DHCP message containing the information is received. **Drop**: drop the package when a DHCP message containing the information is received.

DHCP Relay Statistics shows the information of relayed packet of the switch.



DHCP Relay Statistics

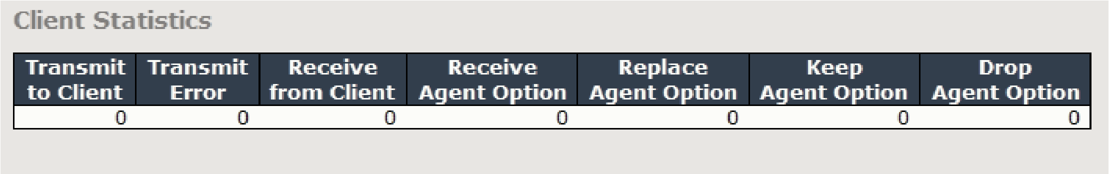
Server Statistics

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

Label	Description
Transmit to Sever	The number of packets relayed from the client to the server
Transmit Error	The number of packets with errors when being sent to clients
Receive from Server	The number of packets received from the server
Receive Missing Agent	The number of packets received without agent information

Option	
Receive Missing Circuit ID	The number of packets received with Circuit ID
Receive Missing Remote ID	The number of packets received with the Remote ID option missing.
Receive Bad Circuit ID	The number of packets whose Circuit ID do not match the known circuit ID
Receive Bad Remote ID	The number of packets whose Remote ID do not match the known Remote ID

DHCP Client Statistics



Client Statistics

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

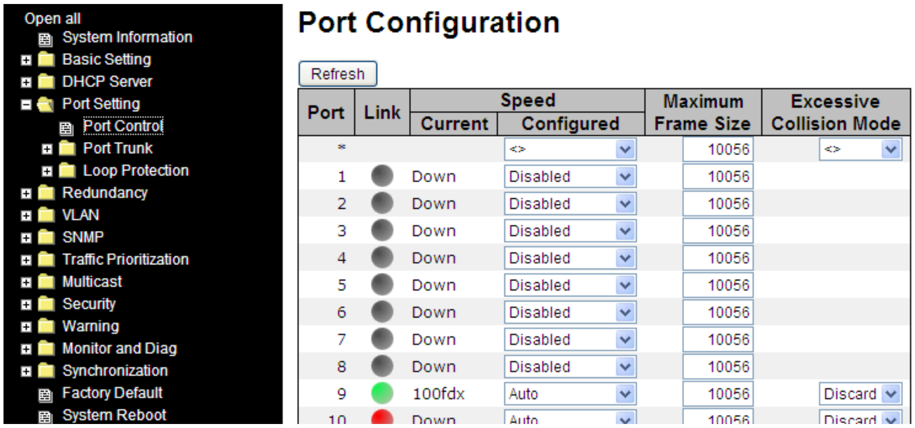
Label	**Description**
Transmit to Client	The number of packets relayed from the server to the client
Transmit Error	The number of packets with errors when being sent to servers
Receive from Client	The number of packets received from the server
Receive Agent Option	The number of received packets containing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

5.3 Port Setting

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

5.3.1 Port Control

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



Port Configuration

Port	Link	Speed		Maximum Frame Size	Excessive Collision Mode
		Current	Configured		
*			<>	10056	<>
1	●	Down	Disabled	10056	
2	●	Down	Disabled	10056	
3	●	Down	Disabled	10056	
4	●	Down	Disabled	10056	
5	●	Down	Disabled	10056	
6	●	Down	Disabled	10056	
7	●	Down	Disabled	10056	
8	●	Down	Disabled	10056	
9	🟢	100fdx	Auto	10056	Discard
10	🔴	Down	Auto	10056	Discard

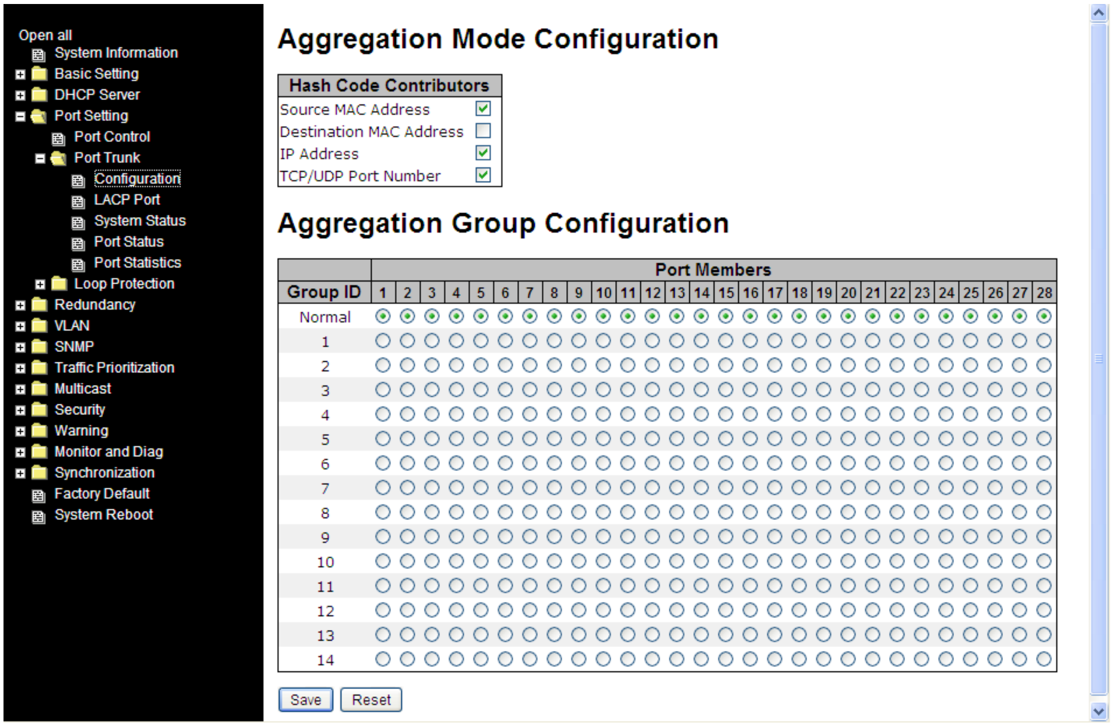
The Port Configuration table parameters are described below.

Label	Description
Port	The switch port number to which the following settings will be applied.
Link	The current link state is shown by different colors. Green indicates the link is up and red means the link is down.
Current Link Speed	Indicates the current link speed of the port.
Configured Link Speed	Select an available link speed for the switch port. Only speeds supported by the specific port are shown. Selections 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 **2.5Gbps FDX** - Forces the Serdes port in 2.5Gbps full duplex mode.
Maximum Frame Size	Enter the maximum frame size allowed for the switch port, including FCS. The default is 10056.

Excessive Collision Mode	Select **Discard** or **Reset** on too many collisions.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Refresh	Click to refresh the page. Any changes made locally will be undone.

5.3.2 Port Trunk

This page lets you configure the aggregation hash mode and the aggregation group.



Aggregation Mode Configuration

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

Aggregation Group Configuration

	Port Members																											
Group ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Normal	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
5	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
6	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
7	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
9	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
10	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
11	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
12	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
13	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
14	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Aggregation Mode Configuration

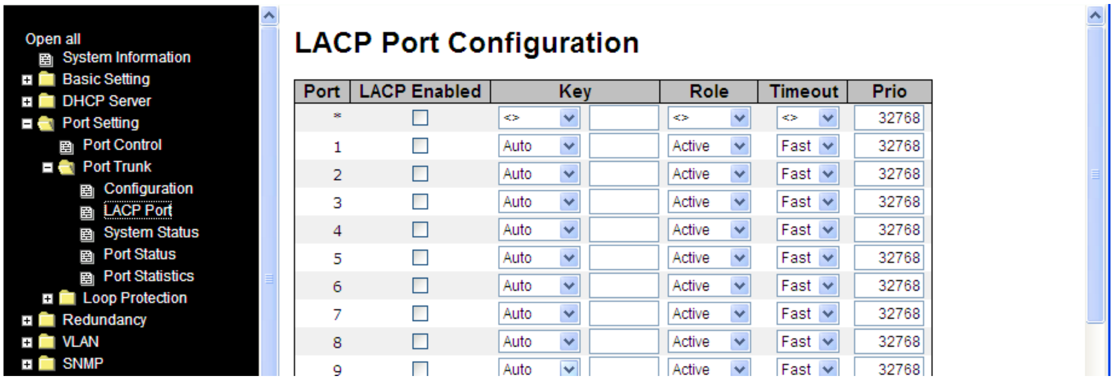
Label	Description
Source MAC Address	Calculates the destination port of the frame. You can check this box to enable the source MAC address, or uncheck to disable. By default, **Source MAC Address** is enabled.
Destination MAC Address	Calculates the destination port of the frame. You can check this box to enable the destination MAC address, or uncheck to disable. By default, **Destination MAC Address** is disabled.
IP Address	Calculates the destination port of the frame. You can check this box to enable the IP address, or uncheck to disable. By default, **IP Address** is enabled.
TCP/UDP Port Number	Calculates the destination port of the frame. You can check this box to enable the TCP/UDP port number, or uncheck to disable. By default, **TCP/UDP Port Number** is enabled.

Aggregation Group Configuration

Label	Description
Group ID	Indicates the ID of each aggregation group. **Normal** means no aggregation. Only one group ID is valid per port.
Port Members	Lists each switch port for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and the ports must be in the same speed in each group.

5.3.3 LACP

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



LACP Port Configuration

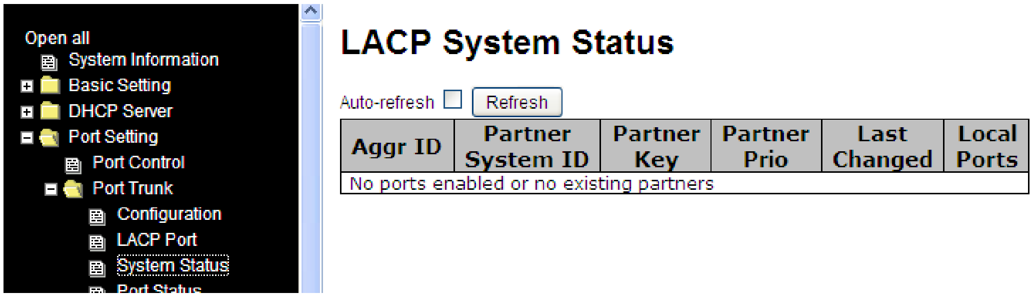
Port	LACP Enabled	Key		Role	Timeout	Prio
*	□	<>		<>	<>	32768
1	□	Auto		Active	Fast	32768
2	□	Auto		Active	Fast	32768
3	□	Auto		Active	Fast	32768
4	□	Auto		Active	Fast	32768
5	□	Auto		Active	Fast	32768
6	□	Auto		Active	Fast	32768
7	□	Auto		Active	Fast	32768
8	□	Auto		Active	Fast	32768
9	□	Auto		Active	Fast	32768

Label	Description
Port	Indicates the ID of each aggregation group. **Normal** indicates there is no aggregation. Only one group ID is valid per port.
LACP Enabled	Lists each switch port for each group ID. Check to include a port in an aggregation, or clear the box to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and the ports must be in the same speed in each group.
Key	The **Key** value varies with the port, ranging from 1 to 65535. **Auto** will set the key according to the physical link speed (10Mb = 1, 100Mb = 2, 1Gb = 3). **Specific** allows you to enter a user-defined value. Ports with the same key value can join in the same aggregation group, while ports with different keys cannot.
Role	Indicates LACP activity status. **Active** will transmit LACP packets every second, while **Passive** will wait for a LACP packet from a partner (*speak if spoken to*).
Timeout	The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait

	for 30 seconds before sending a LACP packet.
Prio	The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values.

LACP System Status

This page provides a status overview for all LACP instances.



LACP System Status

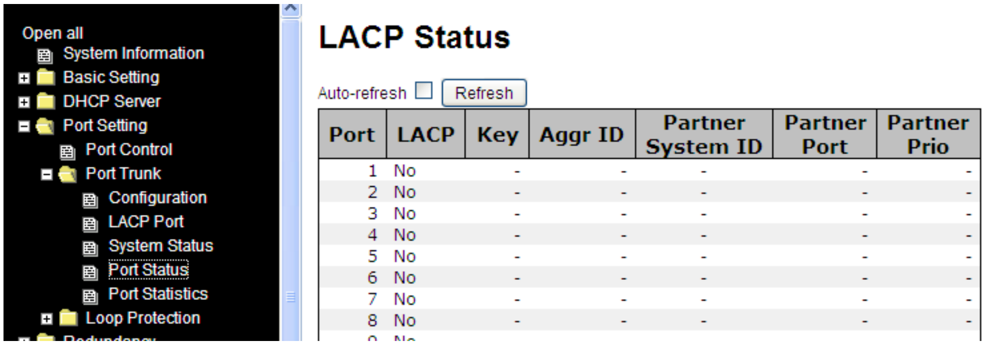
Auto-refresh □ Refresh

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

Label	**Description**
Aggr ID	The aggregation ID is associated with the aggregation instance. For LLAG, the ID is shown as '**isid:aggr-id**' and for GLAGs as '**aggr-id**'.
Partner System ID	System ID (MAC address) of the aggregation partner.
Partner Key	The key assigned by the partner to the aggregation ID.
Partner Prio	The priority number assigned by the partner.
Last Changed	The time since this aggregation changed.
Local Ports	Indicates which ports belong to the aggregation of the switch. The format is: "**Switch ID:Port**".
Refresh	Click to refresh the page immediately.
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals.

LACP Status

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



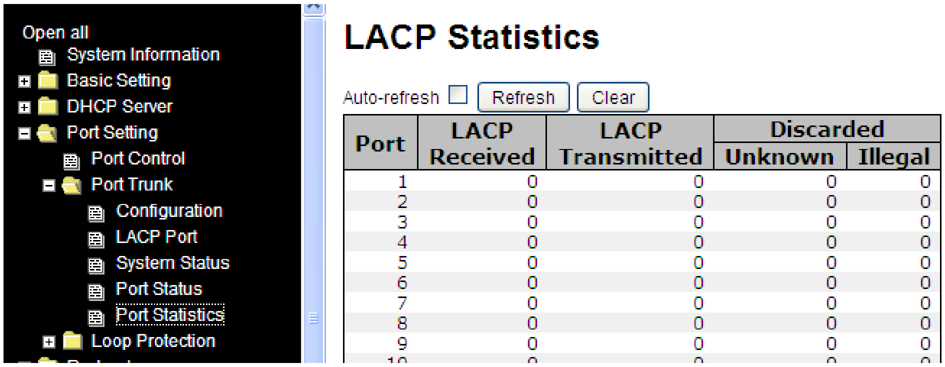
LACP Status

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-

Label	Description
Port	Switch port number.
LACP	**Yes** means LACP is enabled and the port link is up. **No** means LACP is not enabled or the port link is down. **Backup** means the port cannot join in the aggregation group unless other ports are removed. The LACP status is disabled.
Key	The key assigned to the port. Only ports with the same key can be aggregated.
Aggr ID	The aggregation ID assigned to the aggregation group
Partner System ID	The partner's system ID (MAC address)
Partner Port	The partner's port number associated with the port
Partner Prio	The priority number assigned by the partner.
Refresh	Click to refresh the page immediately
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals

LACP Statistics

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



LACP Statistics

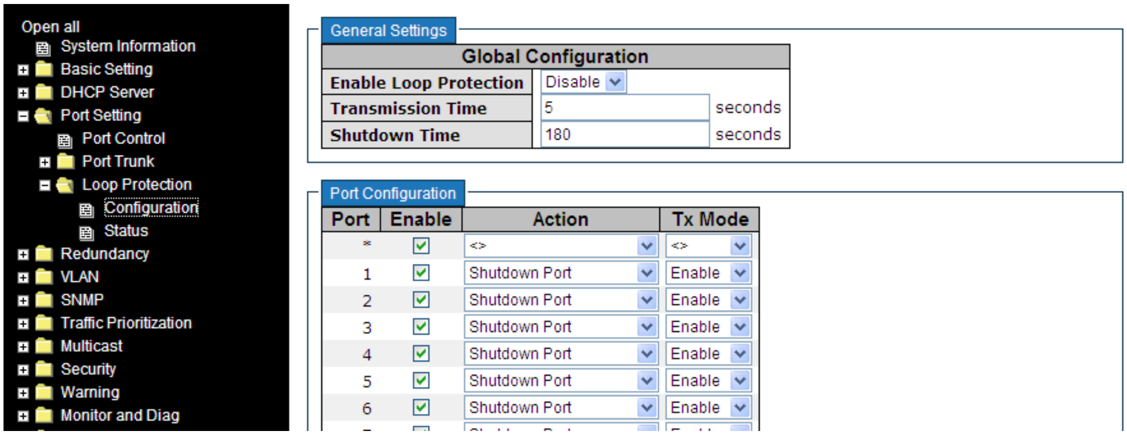
Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0

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

5.3.4 Loop Protection

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

Loop Protection Configuration



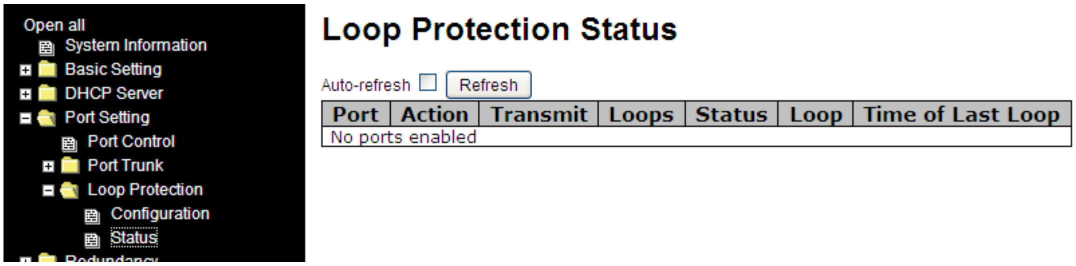
Global Configuration		
Enable Loop Protection	Disable	
Transmission Time	5	seconds
Shutdown Time	180	seconds

Port	Enable	Action	Tx Mode
*	☑	<>	<>
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port	Enable
3	☑	Shutdown Port	Enable
4	☑	Shutdown Port	Enable
5	☑	Shutdown Port	Enable
6	☑	Shutdown Port	Enable

Label	Description
Enable Loop Protection	Activate loop protection functions (as a whole).
Transmission Time	The interval between each loop protection PDU sent on each port. The valid value is 1 to 10 seconds.
Shutdown Time	The period (in seconds) for which a port will be kept disabled when a loop is detected (shutting down the port). The valid value is 0 to 604800 seconds (7 days). A value of **0** will keep a port disabled permanently (until the device is restarted).
Port	Switch port number.
Enable	Activate loop protection functions (as a whole).
Action	Configures the action to take when a loop is detected. Valid values include **Shutdown Port**, **Shutdown Port**, and **Log or Log Only**.
Tx Mode	Controls whether the port is actively generating loop protection PDUs or only passively look for looped PDUs.

Loop Protection Status

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



Loop Protection Status

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
No ports enabled						

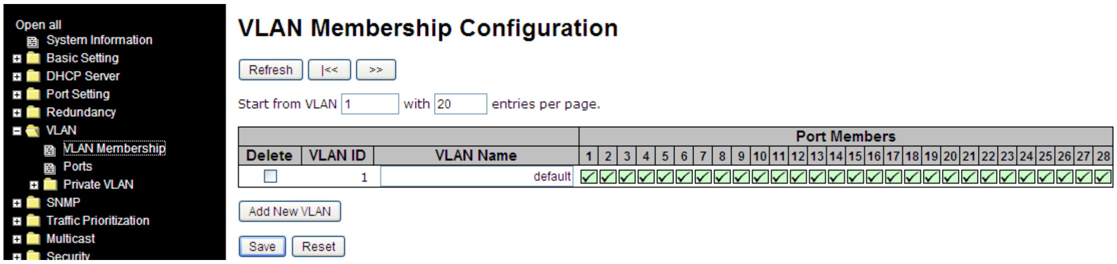
The loop protection port parameters are described below:

Label	Description
Port	The switch port number of the logical port.
Action	The currently configured port action.
Transmit	The currently configured port transmit mode.
Loops	The number of loops detected on this port.
Status	The current loop protection status of the port.
Loop	Whether a loop is currently detected on the port.
Time of Last Loop	The time of the last loop event detected.

5.4 VLAN

5.4.1 VLAN Membership

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



VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page.

			Port Members																											
Delete	VLAN ID	VLAN Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
□	1	default	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Navigating the VLAN Membership Table

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 let you 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 **>>** button 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 more entries" is shown in the displayed table. Use the **|<<** button to start over.

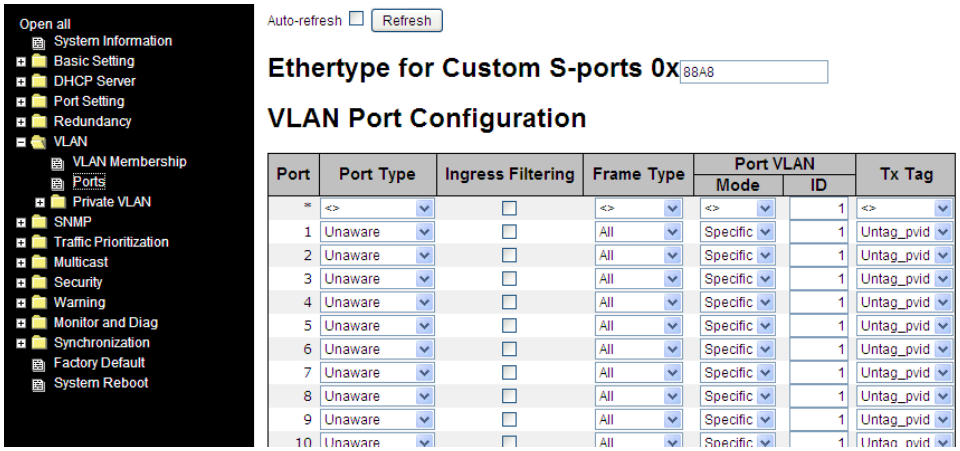
The VLAN Membership Configuration parameters are described below:

Label	**Description**
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID of this particular VLAN.
VLAN Name	Indicates the name of the VLAN. Maximum length of the VLAN Name String is 32. VLAN Name can be null. If it is not null, it must contain alphabets or numbers. At least one alphabet must be present in a non-null VLAN name. VLAN name can be edited for the existing VLAN entries or it can be added to the new entries.

Port Members	A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the green box (☑). To include a port in a forbidden port list, check the red x box (☒). To remove or exclude the port from the VLAN, make sure the unchecked checkbox is shown (□). By default, no ports are members, and for every new VLAN entry all boxes are unchecked.
Add New VLAN	Click to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Valid VLAN ID values are 1 - 4095. After clicking **Save**, the new VLAN will be enabled on the selected switch stack but contains no port members. A VLAN without any port members will be deleted when you click Save. Click **Delete** to undo the addition of new VLANs.

5.4.2 VLAN Port Configurations

This page is used for configuring the switch port VLAN.



Auto-refresh □ Refresh

Ethertype for Custom S-ports 0x 88A8

VLAN Port Configuration

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

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

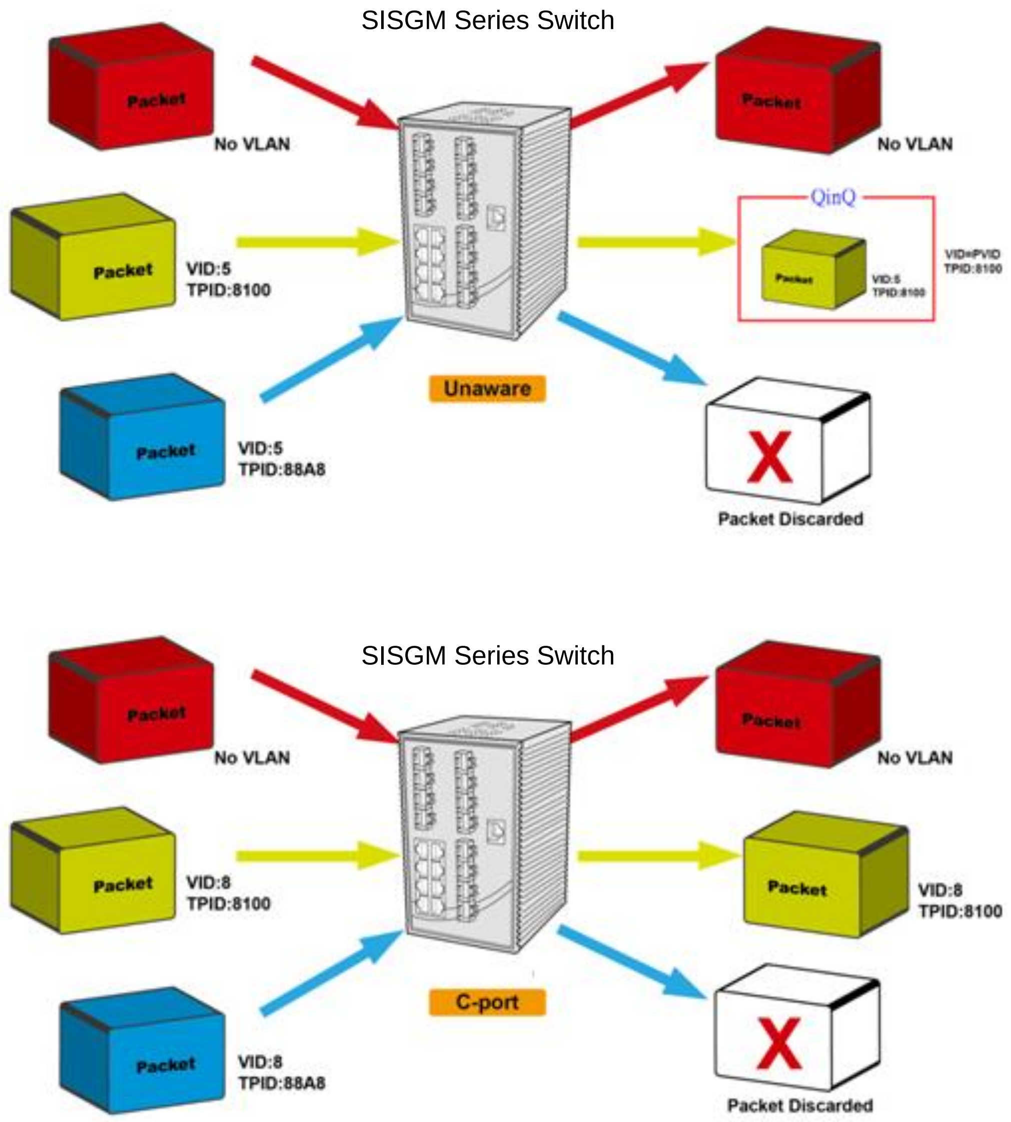
	to VLAN-aware switches. Tx tag should be set to Untag_pvid when this mode is used. If **Specific** (the default value) is selected, a port VLAN ID can be configured (see below). Untagged frames received on the port are classified to the port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the port VLAN ID, a VLAN tag with the classified VLAN ID will be inserted in the frame.
Port VLAN ID	Configures the VLAN identifier for the port. The allowed range of the values is 1 through 4095. The default value is 1. **Note**: The port must be a member of the same VLAN as the port VLAN ID.
Tx Tag	Determines egress tagging of a port. **Untag_pvid**: all VLANs except the configured PVID will be tagged. **Tag_all**: all VLANs are tagged. **Untag_all**: all VLANs are untagged.

Introduction to Port Types

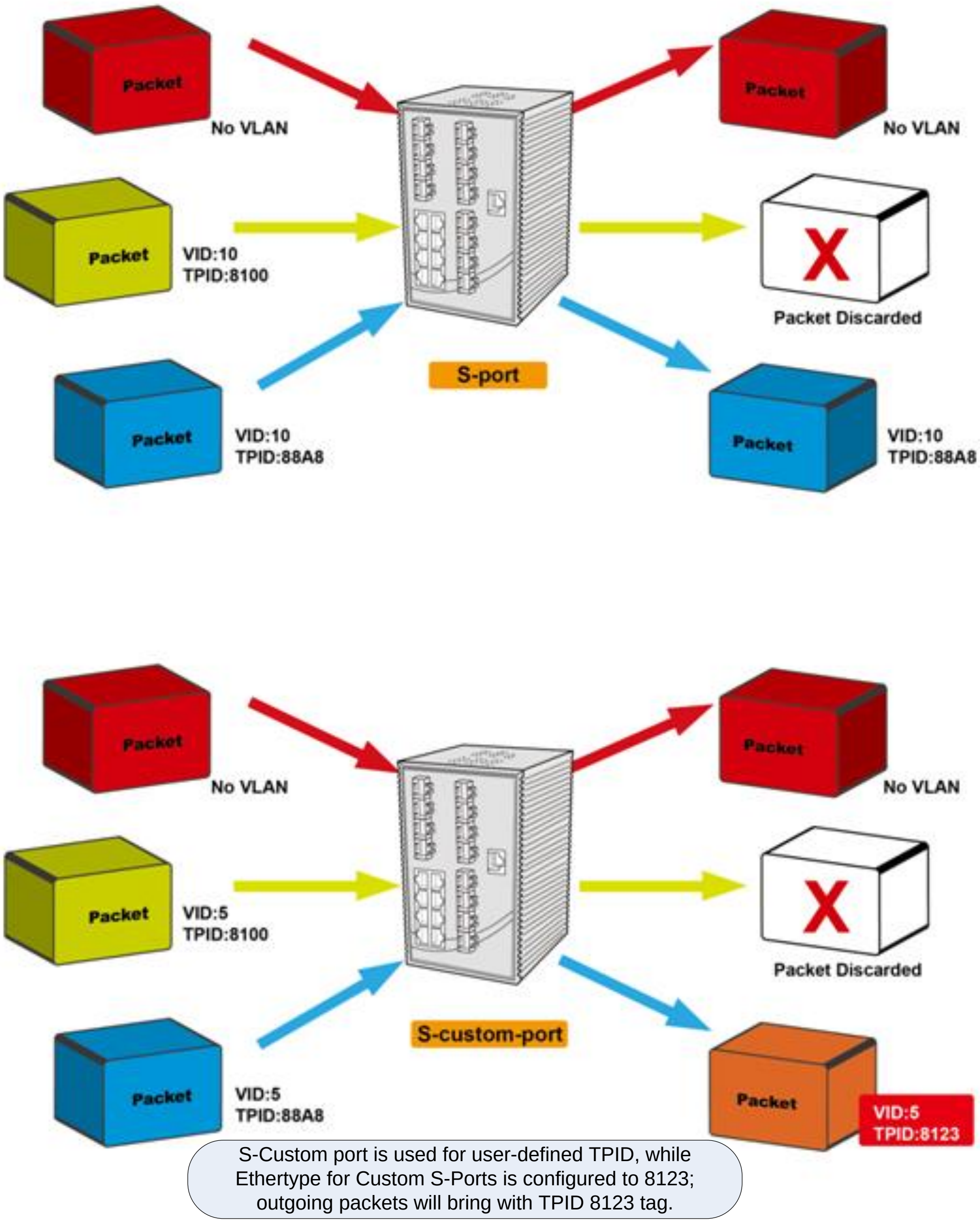
Each port type (Unaware, C-port, S-port, and S-custom-port) is described below.

Type	Ingress action	Egress action
Unaware The function of Unaware can be used for 802.1QinQ (double tag).	When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded. When the port receives tagged frames: 1. If the tagged frame contains a TPID of 0x8100, it will become a double-tag frame and will be forwarded. 2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of a frame transmitted by Unaware port will be set to 0x8100. The final status of the frame after egressing will also be affected by the Egress Rule.
C-port	When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded. When the port receives tagged frames: 1. If the tagged frame contains a TPID of 0x8100, it will be forwarded.	The TPID of a frame transmitted by C-port will be set to 0x8100.

	2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	
S-port	When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded. When the port receives tagged frames: 1. If the tagged frame contains a TPID of 0x8100, it will be forwarded. 2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8100), it will be discarded.	The TPID of a frame transmitted by S-port will be set to 0x88A8.
S-custom-port	When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded. When the port receives tagged frames: 1. If the tagged frame contains a TPID of 0x8100, it will be forwarded. 2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8100), it will be discarded.	The TPID of a frame transmitted by S-custom-port will be set to a self-customized value, which can be set by the user via **Ethertype for Custom S-ports.**



Unaware (top) C-Port (bottom)

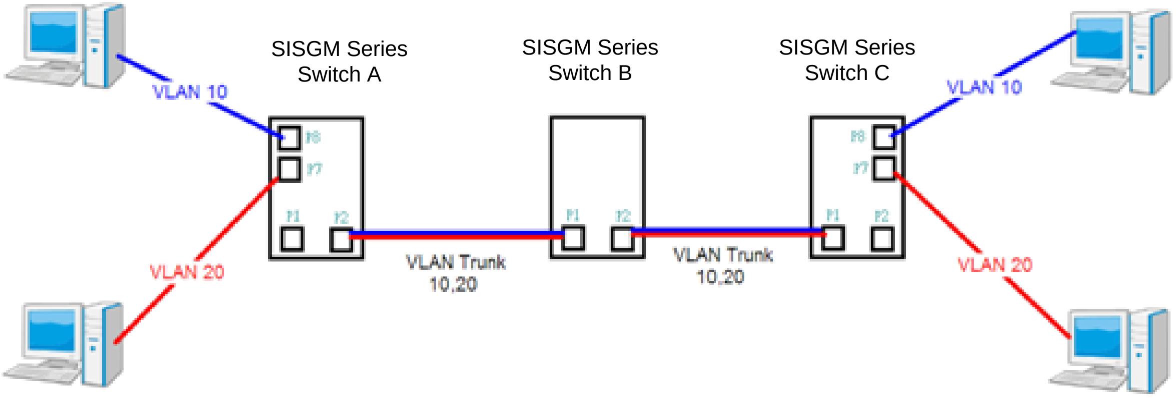


S-Custom port is used for user-defined TPID, while Ethertype for Custom S-Ports is configured to 8123; outgoing packets will bring with TPID 8123 tag.

S-Port (top) S-Custom Port (bottom)

Examples of VLAN Settings

VLAN Access Mode:

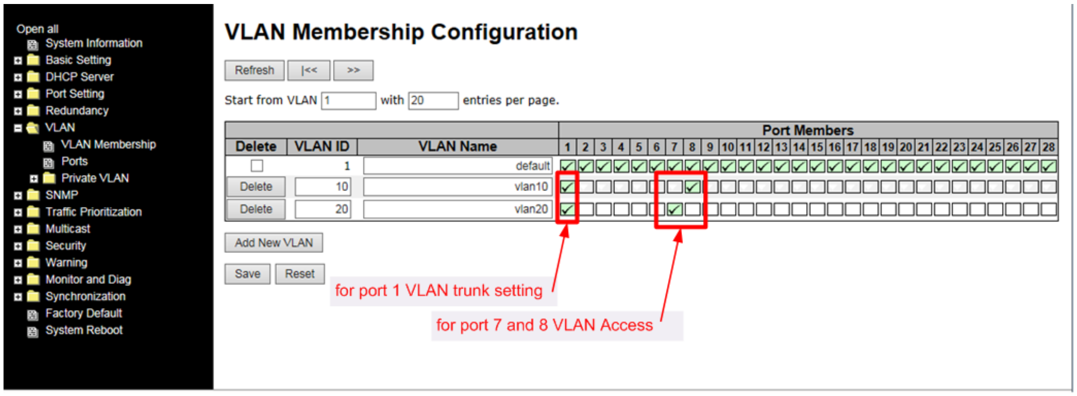


Switch A,

Port 7 is VLAN Access mode = Untagged 20

Port 8 is VLAN Access mode = Untagged 10

Below are the switch settings.



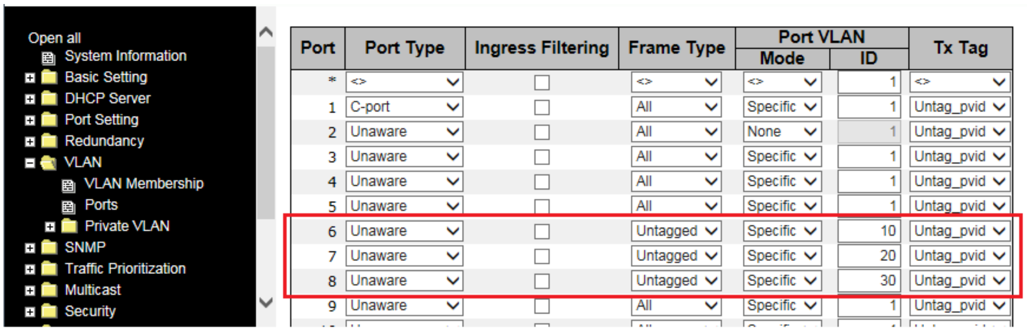
VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page.

			Port Members																											
Delete	VLAN ID	VLAN Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
□	1	default	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Delete	10	vlan10	✓	□	□	□	□	□	□	✓	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Delete	20	vlan20	✓	□	□	□	□	□	✓	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

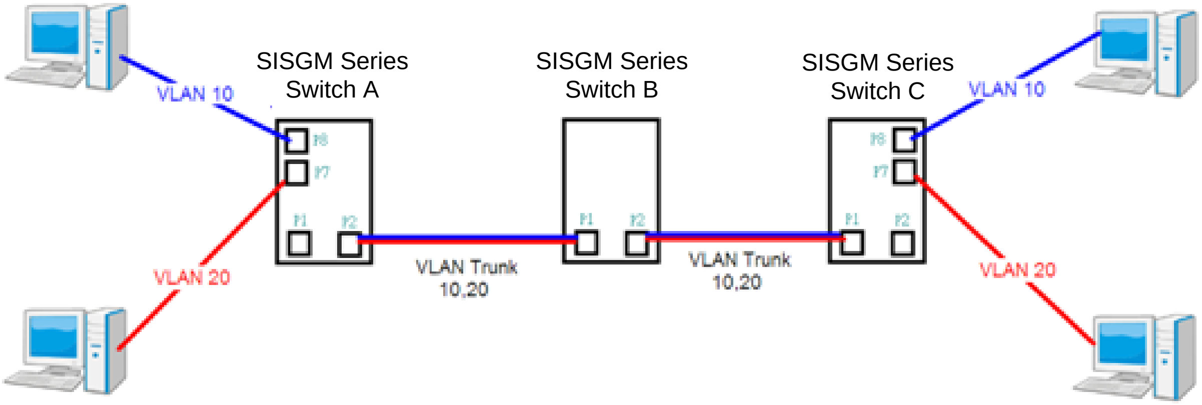
for port 1 VLAN trunk setting

for port 7 and 8 VLAN Access



Port	Port Type	Ingress Filtering	Frame Type	Port VLAN		Tx Tag
				Mode	ID	
*	<>	□	<>	<>	1	<>
1	C-port	□	All	Specific	1	Untag_pvid
2	Unaware	□	All	None	1	Untag_pvid
3	Unaware	□	All	Specific	1	Untag_pvid
4	Unaware	□	All	Specific	1	Untag_pvid
5	Unaware	□	All	Specific	1	Untag_pvid
6	Unaware	□	Untagged	Specific	10	Untag_pvid
7	Unaware	□	Untagged	Specific	20	Untag_pvid
8	Unaware	□	Untagged	Specific	30	Untag_pvid
9	Unaware	□	All	Specific	1	Untag_pvid

VLAN 1Q Trunk Mode:

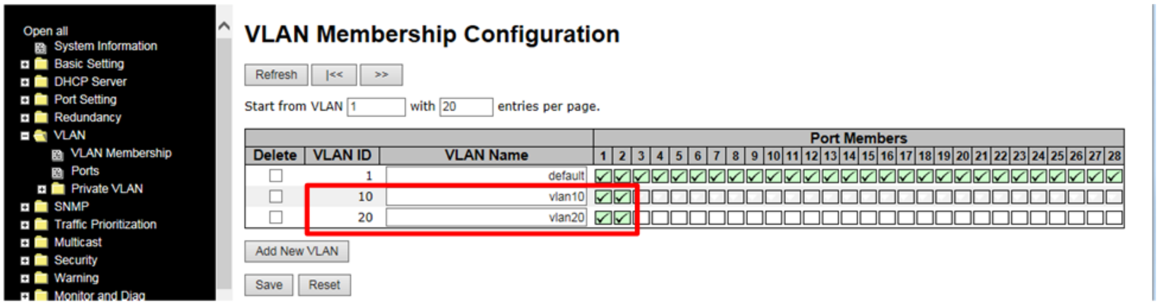


Switch B,

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

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

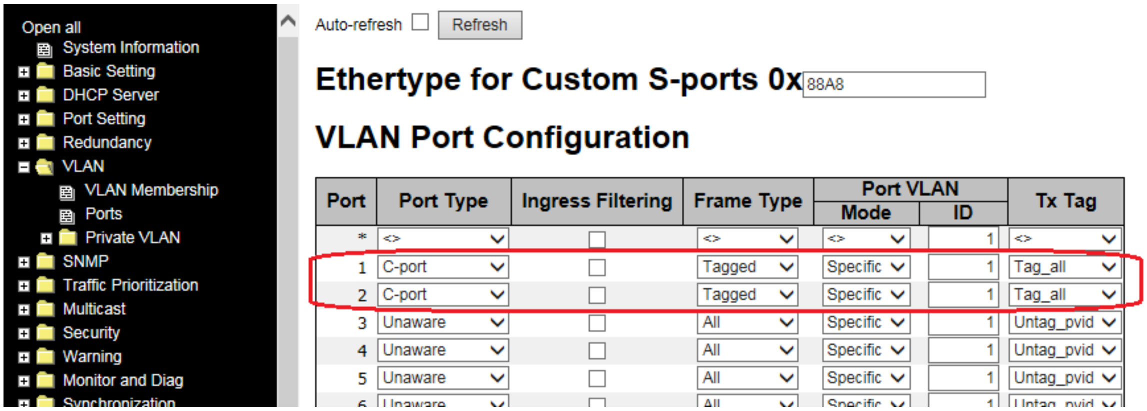
Below are the switch settings.



VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page.

			Port Members																											
Delete	VLAN ID	VLAN Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
□	1	default	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
□	10	vlan10	✓	✓	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
□	20	vlan20	✓	✓	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□



Auto-refresh □

Ethertype for Custom S-ports 0x 88A8

VLAN Port Configuration

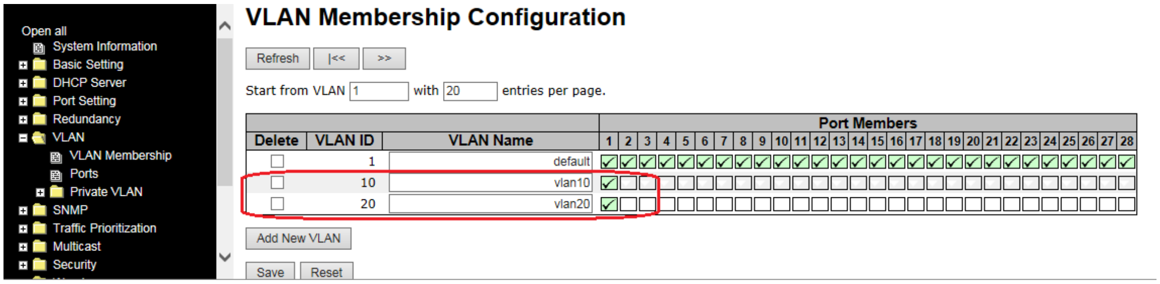
Port	Port Type	Ingress Filtering	Frame Type	Port VLAN Mode	Port VLAN ID	Tx Tag
*	<>	□	<>	<>	1	<>
1	C-port	□	Tagged	Specific	1	Tag_all
2	C-port	□	Tagged	Specific	1	Tag_all
3	Unaware	□	All	Specific	1	Untag_pvid
4	Unaware	□	All	Specific	1	Untag_pvid
5	Unaware	□	All	Specific	1	Untag_pvid
6	Unaware	□	All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

VLAN Hybrid Mode:

Port 1 VLAN Hybrid mode = untagged 10

Tagged 10, 20

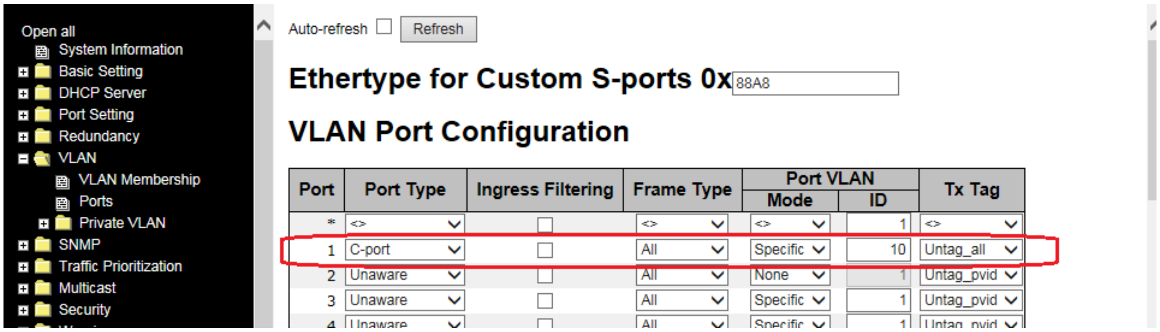
Below are the switch settings.



VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	VLAN Name	Port Members																											
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
□	1	default	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
□	10	vlan10	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
□	20	vlan20	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□



Auto-refresh □

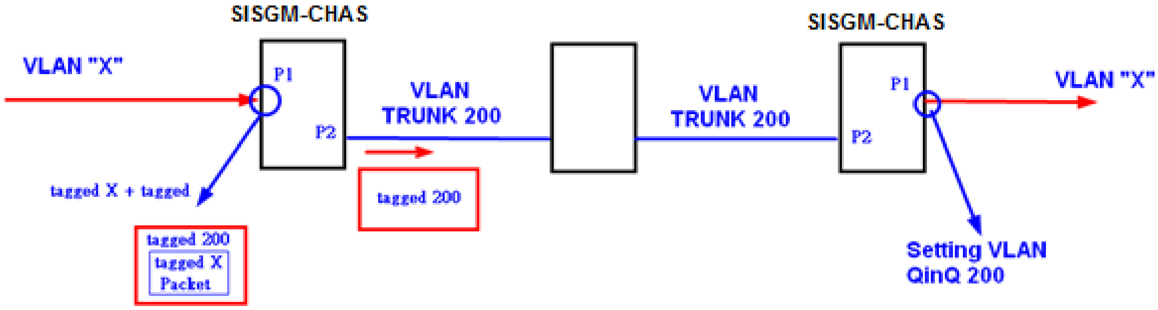
Ethertype for Custom S-ports 0x 88A8

VLAN Port Configuration

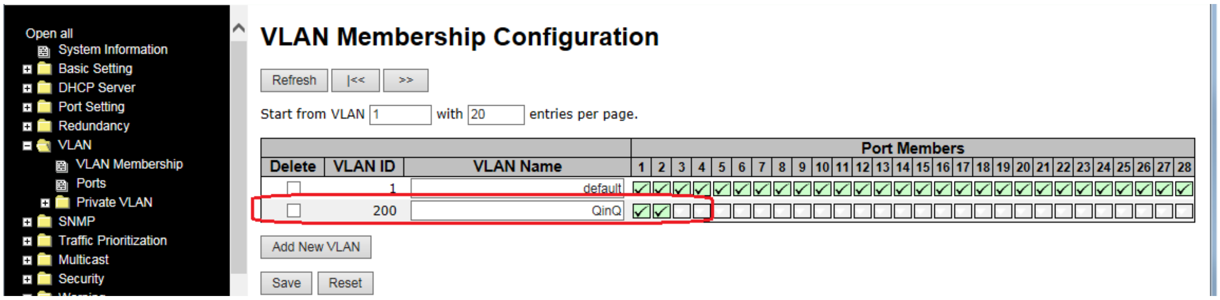
Port	Port Type	Ingress Filtering	Frame Type	Port VLAN		Tx Tag
				Mode	ID	
*	<>	□	<>	<>	1	<>
1	C-port	□	All	Specific	10	Untag_all
2	Unaware	□	All	None	1	Untag_pvid
3	Unaware	□	All	Specific	1	Untag_pvid
4	Unaware	□	All	Specific	1	Untag_pvid

VLAN QinQ Mode:

VLAN QinQ mode is usually used when there are unknown VLANs, as shown in the figure below, where **VLAN “X”** = Unknown VLAN (not configured locally by the SISGM-CHAS).



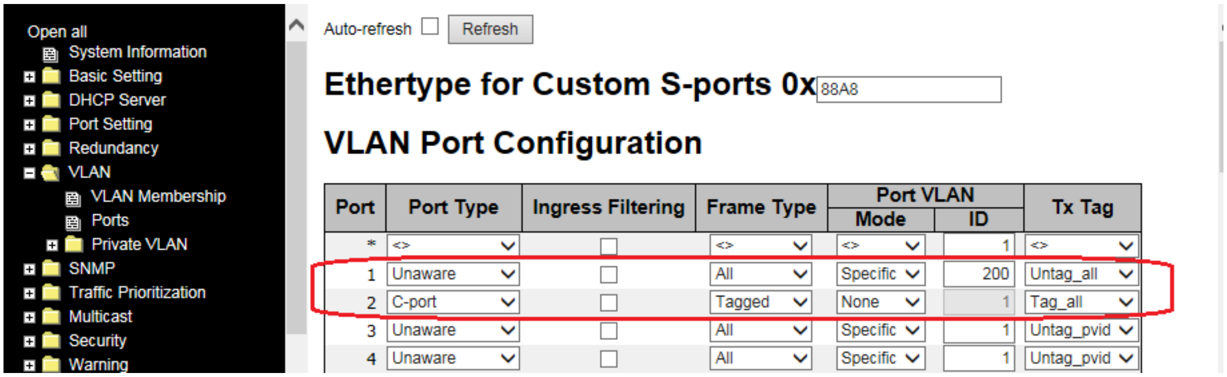
SISGM Series Port 1 VLAN Settings:



VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page.

			Port Members																											
Delete	VLAN ID	VLAN Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
□	1	default	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
□	200	QinQ	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□



Auto-refresh □

Ethertype for Custom S-ports 0x 88A8

VLAN Port Configuration

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

VLAN ID Settings

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

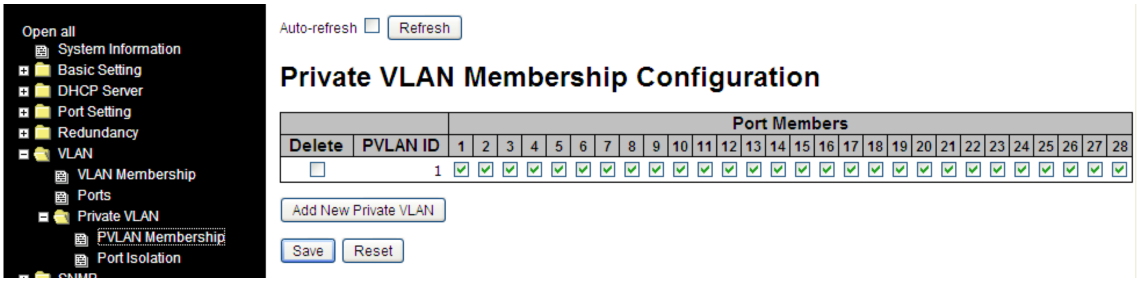
5.4.3 Private VLAN

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

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

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

Private VLAN Membership Configuration



Private VLAN Membership Configuration

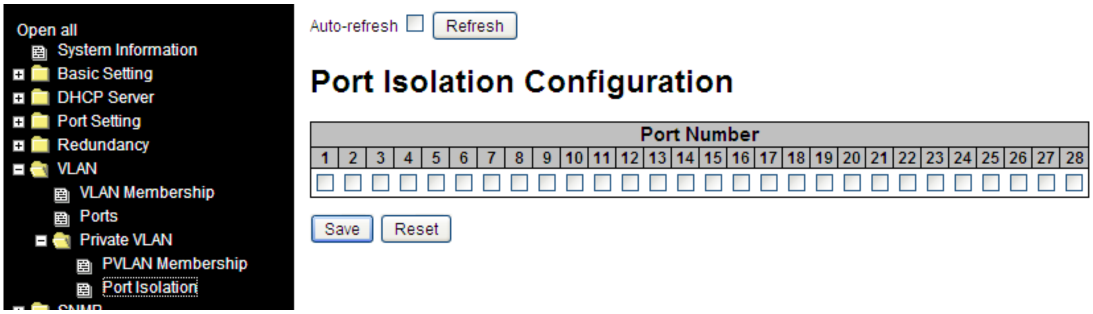
Delete	PVLAN ID	Port Members																											
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
PVLAN ID	Indicates the ID of this particular private VLAN.
MAC Address	The MAC address for the entry.
Port Members	A row of check boxes for each port is displayed for each private VLAN ID. You can check the box to include a port in a private VLAN. To remove or exclude the port from the private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Adding a New Static Entry	Click **Add New Private LAN** to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click **OK** to discard the incorrect entry, or click Cancel to return to the editing and make a correction. The private VLAN is enabled when you click Save. The **Delete** button can be used to undo the addition of new private VLANs.

Port Isolation Configuration

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.



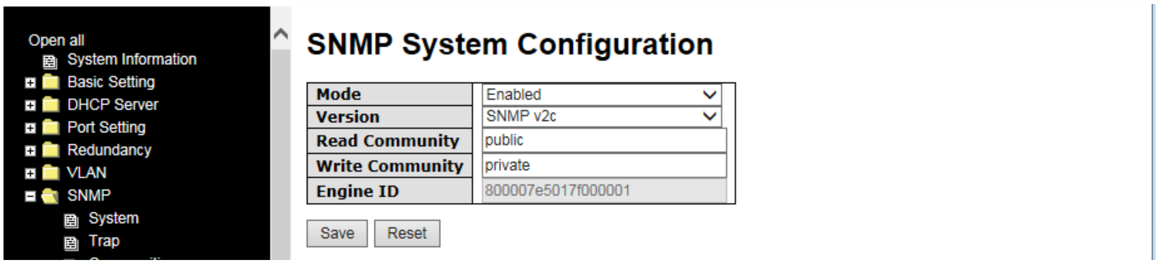
Port Isolation Configuration

Port Number																											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Label	Description
Port Members	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled for that port. When unchecked, port isolation is disabled for that port. By default, port isolation is disabled for all ports.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page immediately.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.5 SNMP

5.5.1 SNMP System Configuration

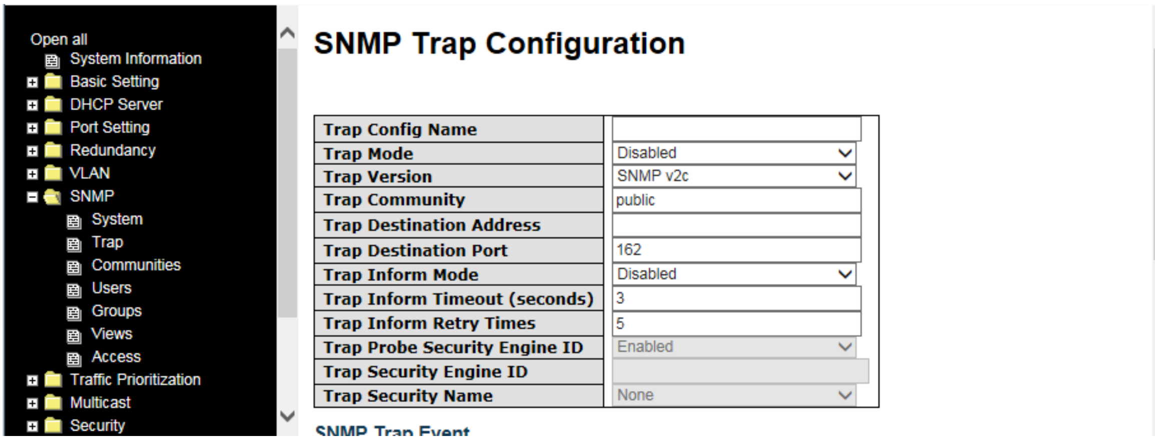


SNMP System Configuration

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

Label	Description
Mode	Indicates existing SNMP mode. Possible modes include: **Enabled**: enable SNMP mode. **Disabled**: disable SNMP mode.
Version	Indicates the supported SNMP version. Possible versions include: **SNMP v1**: supports SNMP version 1. **SNMP v2c**: supports SNMP version 2c. **SNMP v3**: supports SNMP version 3.
Read Community	Indicates the read community string to permit access to SNMP agent. The allowed string length is 0 to 255 characters, and only ASCII characters 33 - 126 are allowed. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 uses USM for authentication and privacy and the community string will be associated with SNMPv3 community table.
Write Community	Indicates the write community string to permit access to SNMP agent. The allowed string length is 0 to 255 characters, and only ASCII characters 33 - 126 are allowed. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 uses USM for authentication and privacy and the community string will be associated with SNMPv3 community table.
Engine ID	Indicates the SNMPv3 engine ID. The string must contain an even number of 10 - 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

5.5.2 SNMP System Configuration



SNMP Trap Configuration

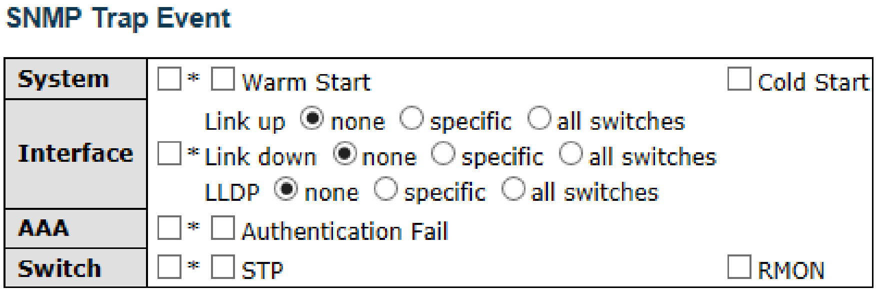
Trap Config Name	
Trap Mode	Disabled
Trap Version	SNMP v2c
Trap Community	public
Trap Destination Address	
Trap Destination Port	162
Trap Inform Mode	Disabled
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Probe Security Engine ID	Enabled
Trap Security Engine ID	
Trap Security Name	None

SNMP Trap Event

Label	Description
Trap Mode	Indicates existing SNMP trap mode. Possible modes include: **Enabled**: enable SNMP trap mode. **Disabled**: disable SNMP trap mode.
Trap Version	Indicates the supported SNMP trap version, including: **SNMP v1**: supports SNMP trap version 1. **SNMP v2c**: supports SNMP trap version 2c. **SNMP v3**: supports SNMP trap version 3.
Trap Community	Indicates the community access string when sending SNMP trap packets. The allowed string length is 0 – 255 characters, and only ASCII characters 33 - 126 are allowed.
Trap Destination Address	Indicates the SNMP trap destination address.
Trap Destination Port	Indicates the SNMP trap destination port. SNMP Agent will send SNMP messages via this port; the port range is 1~65535.
Trap Inform Mode	Indicates the SNMP trap inform mode. Possible modes include: **Enabled**: enable SNMP trap inform mode **Disabled**: disable SNMP trap inform mode
Trap Inform Timeout (seconds)	Configures the SNMP trap inform timeout. The allowed range is 0 to 2147.
Trap Inform Retry Times	Configures the retry times for SNMP trap inform. The allowed range is 0 to 255.

Trap Probe Security Engine ID	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: **Enabled**: Enable SNMP trap probe security engine ID mode of operation. **Disabled**: Disable SNMP trap probe security engine ID mode of operation.
Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.
Trap Security Name	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

SNMP Trap Event Configuration



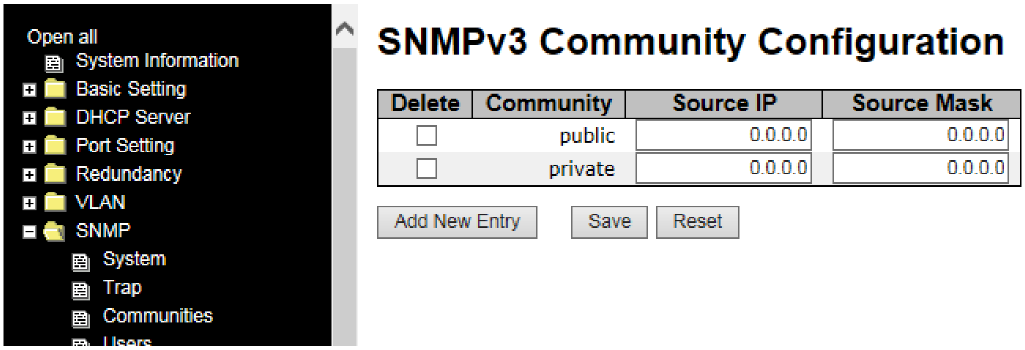
SNMP Trap Event

System	□ * □ Warm Start □ Cold Start
Interface	Link up ● none ○ specific ○ all switches □ * Link down ● none ○ specific ○ all switches LLDP ● none ○ specific ○ all switches
AAA	□ * □ Authentication Fail
Switch	□ * □ STP □ RMON

Label	Description
System	Enable/disable that the Interface group's traps. Possible traps are: **Warm Start**: Enable/disable Warm Start trap. **Cold Start**: Enable/disable Cold Start trap.
Interface	Indicates that the Interface group's traps. Possible traps are: Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are: **Warm Start**: Enable SNMP trap authentication failure. **Link Up**: Enable/disable Link up trap. **Link Down**: Enable/disable Link down trap. **LLDP**: Enable/disable LLDP trap.
AAA	Indicates that the AAA group's traps. Possible traps are: **Authentication Fail** : Enable/disable SNMP trap authentication failure trap.
Switch	Indicates that the Switch group's traps. Possible traps are: **STP**: Enable/disable STP trap. **RMON**: Enable/disable RMON trap.

5.5.3 SNMP Community Configurations

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



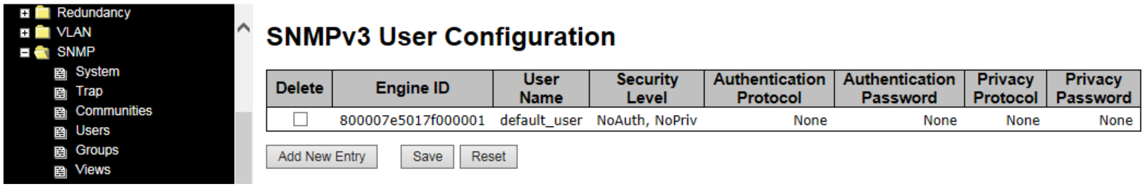
SNMPv3 Community Configuration

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

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

5.5.4 SNMP User Configurations

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



SNMPv3 User Configuration

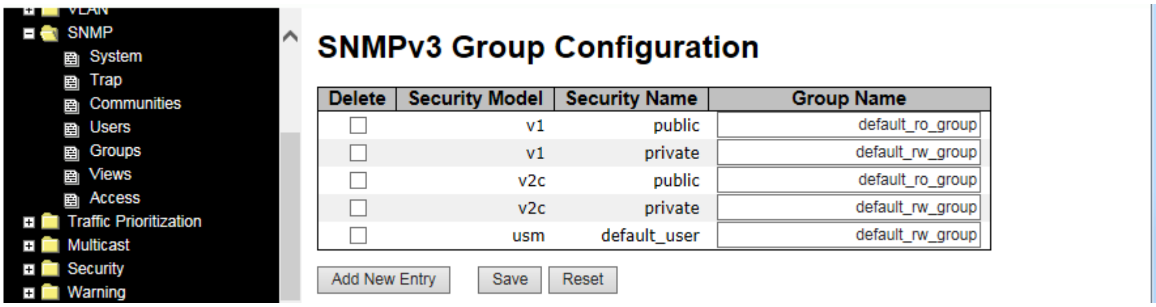
Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☐	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number of 10 - 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses User-based Security Model (USM) for message security and View-based Access Control Model (VACM) for access control. For the USM entry, the **usmUserEngineID** and **usmUserName** are the entry keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID is the same as system engine ID, then it is local user; otherwise it's remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters 33 - 126 are allowed.
Security Level	Indicates the security model that this entry should belong to. Possible security models include: **NoAuth, NoPriv**: no authentication and none privacy. **Auth, NoPriv**: Authentication and no privacy. **Auth, Priv**: Authentication and privacy. The value of security level cannot be modified if the entry already exists, which means the value must be set correctly at the time of entry creation.

Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols include: **None**: no authentication protocol. **MD5**: an optional flag to indicate that this user is using MD5 authentication protocol. **SHA**: an optional flag to indicate that this user is using SHA authentication protocol. The value of security level cannot be modified if the entry already exists, which means the value must be set correctly at the time of entry creation.
Authentication Password	A string identifying the authentication pass phrase. For **MD5** authentication protocol, the allowed string length is 8 – 32 chars. For **SHA** authentication protocol, the allowed string length is 8 – 40 chars. Only ASCII characters 33 - 126 are allowed.
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols include: **None**: no privacy protocol; **DES**: an optional flag to indicate that this user is using DES authentication protocol;
Privacy Password	A string identifying the privacy pass phrase. The allowed string length is 8 – 32 characters, and only ASCII characters 33 - 126 are allowed.

5.5.5 SNMP Group Configurations

This page allows you to configure SNMPv3 group table. The entry index keys are **Security Model** and **Security Name**.



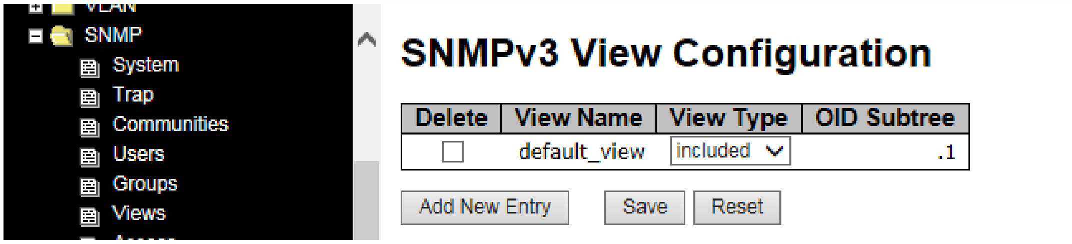
SNMPv3 Group Configuration

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

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

5.5.6 SNMP View Configurations

This page allows you to configure SNMPv3 view table. The entry index keys are **View Name** and **OID Subtree**.



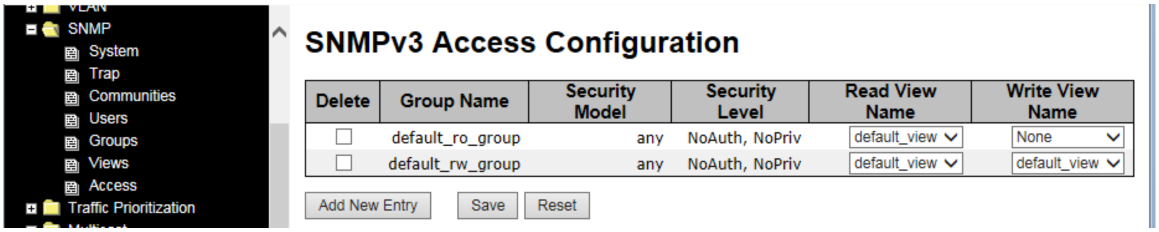
SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
□	default_view	included	.1

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 – 32 characters, and only ASCII characters 33 - 126 are allowed.
View Type	Indicates the view type that this entry should belong to. Possible view types include: **Included**: an optional flag to indicate that this view subtree should be included. **Excluded**: An optional flag to indicate that this view subtree should be excluded. Generally, if an entry's view type is **Excluded**, it should exist another entry whose view type is **Included, and** its OID subtree oversteps the **Excluded** entry.
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128 characters. The allowed string content is a digital number or asterisk (*).

5.5.7 SNMP Access Configurations

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



SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	default_ro_group	any	NoAuth, NoPriv	default_view	None
□	default_rw_group	any	NoAuth, NoPriv	default_view	default_view

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 – 32 characters, and only ASCII characters 33 - 126 are allowed.
Security Model	Indicates the security model that this entry should belong to. Possible security models include: **any**: Accepted any security model (v1|v2c|usm). **v1**: Reserved for SNMPv1. **v2c**: Reserved for SNMPv2c. **usm**: User-based Security Model (USM).
Security Level	Indicates the security model that this entry should belong to. Possible security models include: **NoAuth, NoPriv**: no authentication and no privacy **Auth, NoPriv**: Authentication and no privacy **Auth, Priv**: Authentication and privacy
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 – 32 characters, and only ASCII characters 33 - 126 are allowed.
Write View Name	The name of the MIB view defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 – 32 characters, and only ASCII characters 33 - 126 are allowed.

5.6 Traffic Prioritization

5.6.1 Storm Control

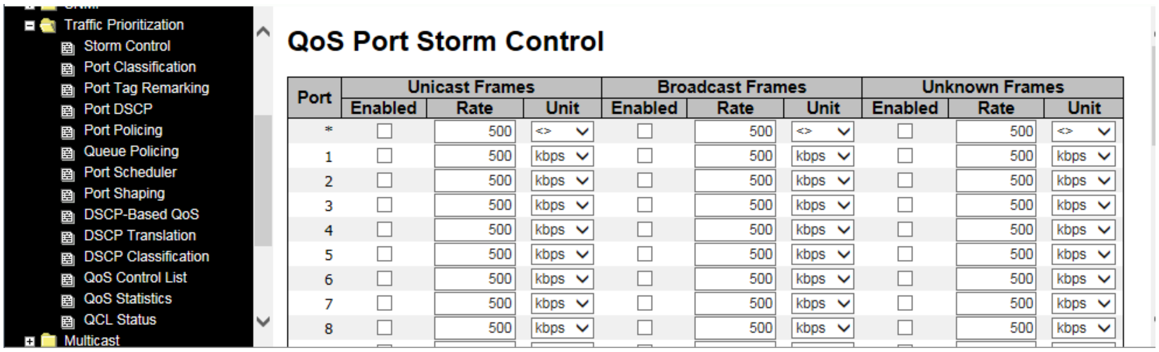
This page allows you to configure the storm control settings for all switch ports.

There is a storm rate control for **Unicast** frames, **Broadcast** frames and **Unknown** (flooded) frames.

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

Note: frames sent to the CPU of the switch are always limited to approximately 4 kpps.

For example, broadcasts in the Management VLAN are limited to this rate. The management VLAN is configured on the IP setup page.



QoS Port Storm Control

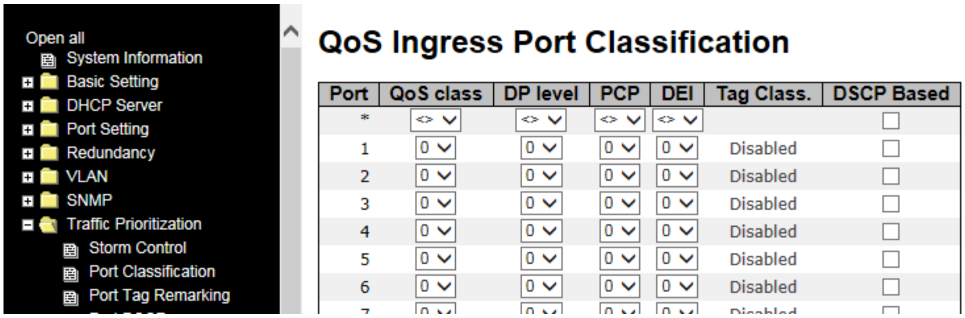
Port	Unicast Frames			Broadcast Frames			Unknown Frames		
	Enabled	Rate	Unit	Enabled	Rate	Unit	Enabled	Rate	Unit
*	□	500	<>	□	500	<>	□	500	<>
1	□	500	kbps	□	500	kbps	□	500	kbps
2	□	500	kbps	□	500	kbps	□	500	kbps
3	□	500	kbps	□	500	kbps	□	500	kbps
4	□	500	kbps	□	500	kbps	□	500	kbps
5	□	500	kbps	□	500	kbps	□	500	kbps
6	□	500	kbps	□	500	kbps	□	500	kbps
7	□	500	kbps	□	500	kbps	□	500	kbps
8	□	500	kbps	□	500	kbps	□	500	kbps

The QoS Port Storm Control parameters are described below.

Label	Description
Port	The port number for which the configuration applies.
Enabled	Controls whether the storm control is enabled on this switch port.
Rate	Controls the rate for the storm control. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-13200 when the "Unit" is "Mbps" or "kfps".
Unit	Controls the unit of measure for the storm control rate as kbps, Mbps, fps or kfps . The default value is "kbps".

5.6.2 Port Classification

QoS (Quality of Service) is a method to achieve efficient bandwidth utilization between individual applications or protocols.



QoS Ingress Port Classification

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

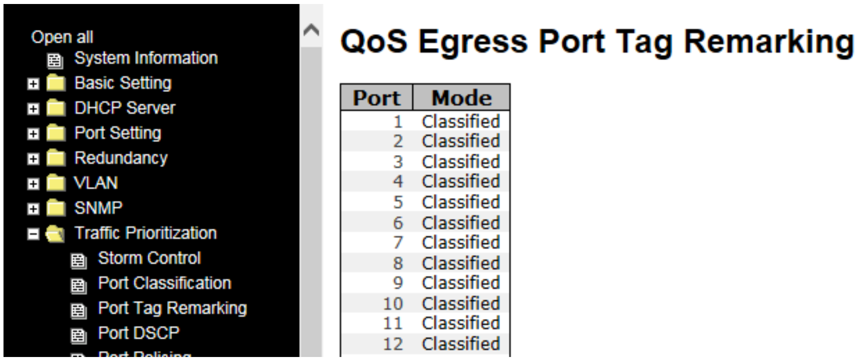
The QoS Ingress Port Classification parameters are described below.

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

DP level	Controls the default Drop Precedence Level. All frames are classified to a DP level. If the port is VLAN aware and the frame is tagged, then the frame is classified to a DP level that is equal to the DEI value in the tag. Otherwise the frame is classified to the default DP level. If the port is VLAN aware, the frame is tagged, and Tag Class is enabled, then the frame is classified to a DP level that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DP level. The classified DP level can be overruled by a QCL entry.
PCP	Controls the default PCP value All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.
DEI	Controls the default DEI value All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.
Tag Class.	Shows the classification mode for tagged frames on this port **Disabled**: Use default QoS class and DP level for tagged frames **Enabled**: Use mapped versions of PCP and DEI for tagged frames Click on the mode to configure the mode and/or mapping Note: this setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN-unaware ports are always classified to the default QoS class and DP level.
DSCP Based	Click to enable DSCP Based QoS Ingress Port Classification

5.6.3 Port Tag Remaking

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



QoS Egress Port Tag Remarking

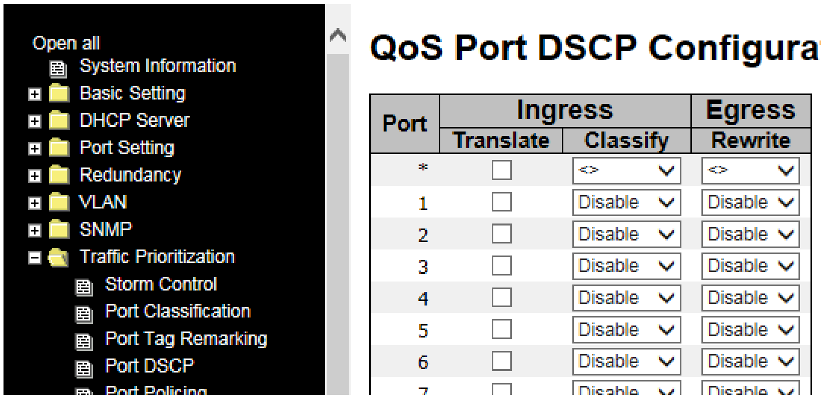
Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified

The QoS Egress Port Tag Remarking parameters are described below.

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

5.6.4 Port DSCP

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



QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	□	<>	<>
1	□	Disable	Disable
2	□	Disable	Disable
3	□	Disable	Disable
4	□	Disable	Disable
5	□	Disable	Disable
6	□	Disable	Disable
7	□	Disable	Disable

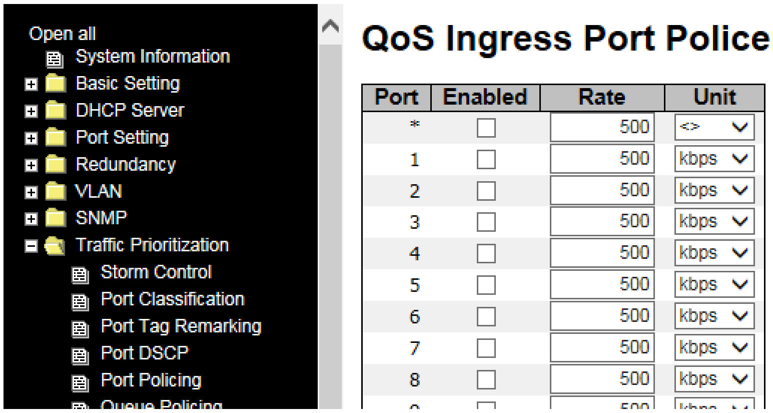
The QoS Port DSCP Configuration parameters are described below.

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

	remarked with a remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the '**DSCP Translation->Egress Remap DP0**' table or from the '**DSCP Translation->Egress Remap DP1**' table.

5.6.5 Port Policing

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



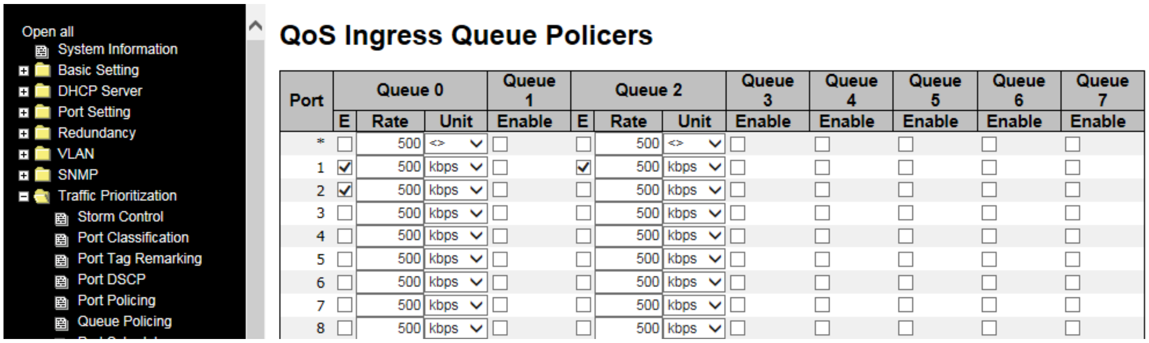
QoS Ingress Port Policers

Port	Enabled	Rate	Unit
*	□	500	<>
1	□	500	kbps
2	□	500	kbps
3	□	500	kbps
4	□	500	kbps
5	□	500	kbps
6	□	500	kbps
7	□	500	kbps
8	□	500	kbps
9	□	500	kbps

Label	Description
Port	The port number for which the configuration below applies
Enabled	Check to enable the policer for individual switch ports
Rate	Configures the rate of each policer. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps** or **fps**, and is restricted to 1 to 3300 when the **Unit** is **Mbps** or **kfps**.
Unit	Configures the unit of measurement for each policer rate as **kbps**, **Mbps**, **fps**, or **kfps**. The default value is **kbps**.

5.6.6 Queue Policing

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



QoS Ingress Queue Policers

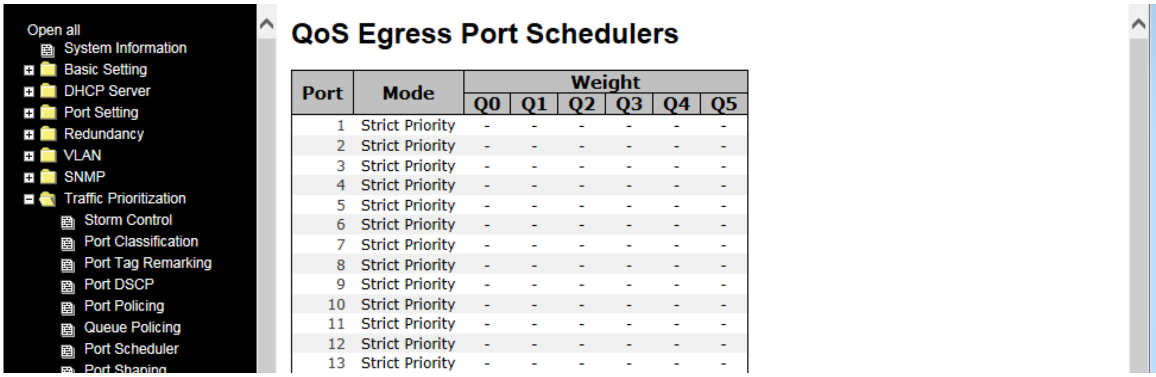
Port	Queue 0			Queue 1	Queue 2			Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	E	Rate	Unit	Enable	E	Rate	Unit	Enable	Enable	Enable	Enable	Enable
*	□	500	<>	□	□	500	<>	□	□	□	□	□
1	☑	500	kbps	□	☑	500	kbps	□	□	□	□	□
2	☑	500	kbps	□	□	500	kbps	□	□	□	□	□
3	□	500	kbps	□	□	500	kbps	□	□	□	□	□
4	□	500	kbps	□	□	500	kbps	□	□	□	□	□
5	□	500	kbps	□	□	500	kbps	□	□	□	□	□
6	□	500	kbps	□	□	500	kbps	□	□	□	□	□
7	□	500	kbps	□	□	500	kbps	□	□	□	□	□
8	□	500	kbps	□	□	500	kbps	□	□	□	□	□

The QoS Ingress Queue Policers parameters are described below.

Label	Description
Port	The port number for which the configuration below applies.
E (Enabled)	Check to enable queue policer for individual switch ports
Rate	Configures the rate of each queue policer. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps**, and is restricted to 1-13200 when the **Unit** is **Mbps**. This field only displays if at least one of the queue policers is enabled.
Unit	Configures the unit of measurement for each queue policer rate as **kbps** or **Mbps**. The default value is **kbps**. This field only displays if at least one of the queue policers is enabled.

5.6.7 QoS Egress Port Scheduler and Shapers

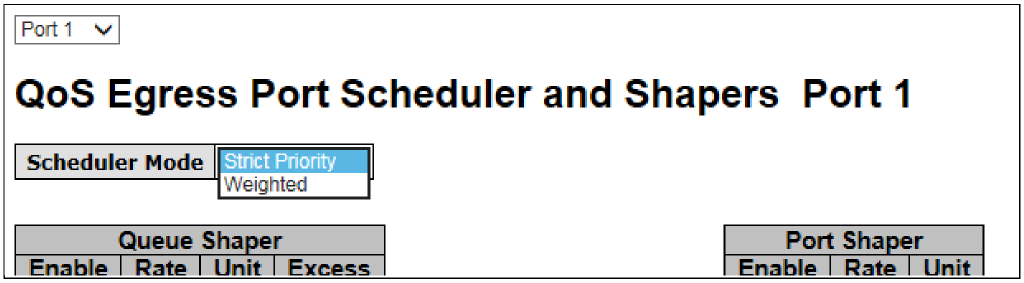
This page provides links that let you configure Scheduler and Shapers for a specific port.



QoS Egress Port Schedulers

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

From the default QoS Egress Port Schedulers page (see above), click a linked number in the Port column to display the default QoS Egress Port Scheduler and Shapers for the selected port (e.g., Port 1 shown below) with the default **Scheduler Mode** set to **Strict Priority**.



QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority

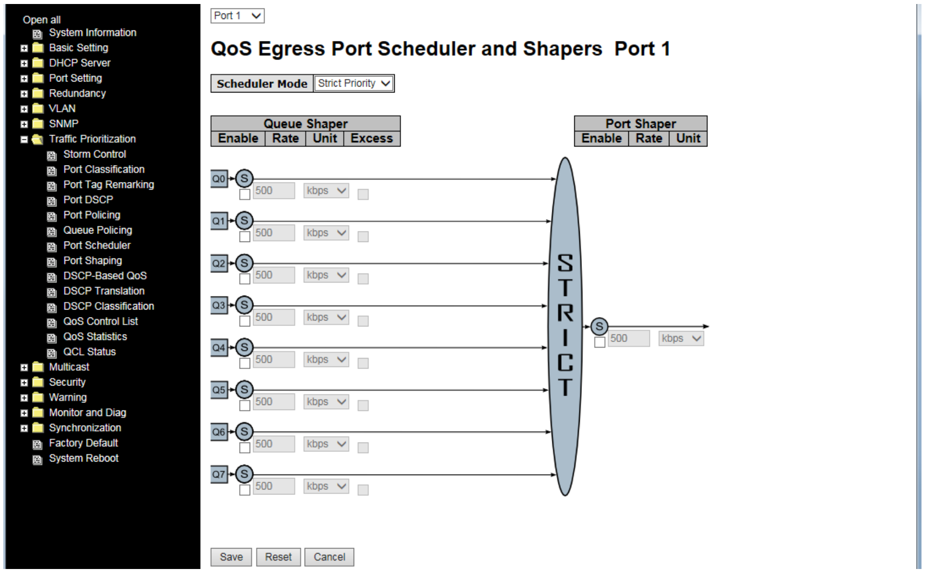
Queue Shaper			
Enable	Rate	Unit	Excess

Port Shaper		
Enable	Rate	Unit

The other **Scheduler Mode** selection is **Weighted**.

Both modes are described in the following sections.

The default QoS Egress Port Scheduler and Shapers page is shown below.



QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority

	Queue Shaper Enable	Rate	Unit	Excess
Q0	□	500	kbps	□
Q1	□	500	kbps	□
Q2	□	500	kbps	□
Q3	□	500	kbps	□
Q4	□	500	kbps	□
Q5	□	500	kbps	□
Q6	□	500	kbps	□
Q7	□	500	kbps	□

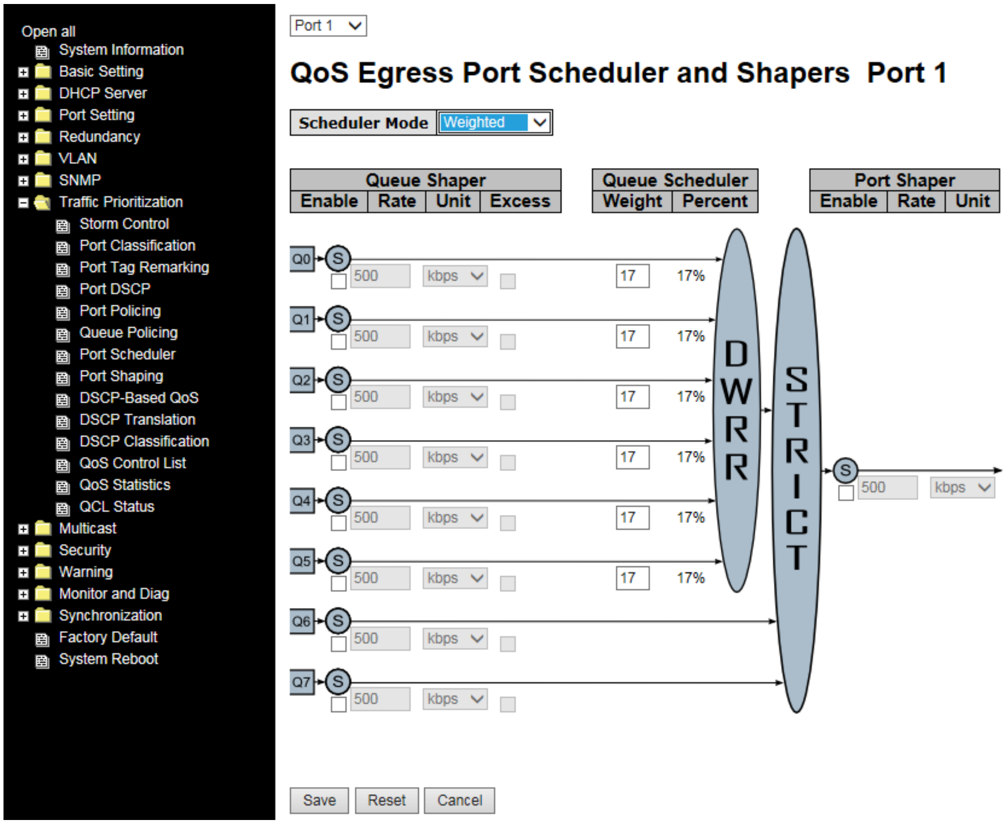
Port Shaper Enable	Rate	Unit
□	500	kbps

Strict Priority

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

Weighted

The QoS Egress Port Scheduler and Shapers page is shown below with **Weighted** selected in the **Scheduler Mode** dropdown.



QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Weighted

Queue	Queue Shaper Enable	Queue Shaper Rate	Queue Shaper Unit	Queue Shaper Excess	Queue Scheduler Weight	Queue Scheduler Percent
Q0	□	500	kbps	□	17	17%
Q1	□	500	kbps	□	17	17%
Q2	□	500	kbps	□	17	17%
Q3	□	500	kbps	□	17	17%
Q4	□	500	kbps	□	17	17%
Q5	□	500	kbps	□	17	17%
Q6	□	500	kbps	□		
Q7	□	500	kbps	□		

Port Shaper Enable	Port Shaper Rate	Port Shaper Unit
□	500	kbps

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

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

5.6.8 Port Scheduler

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

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

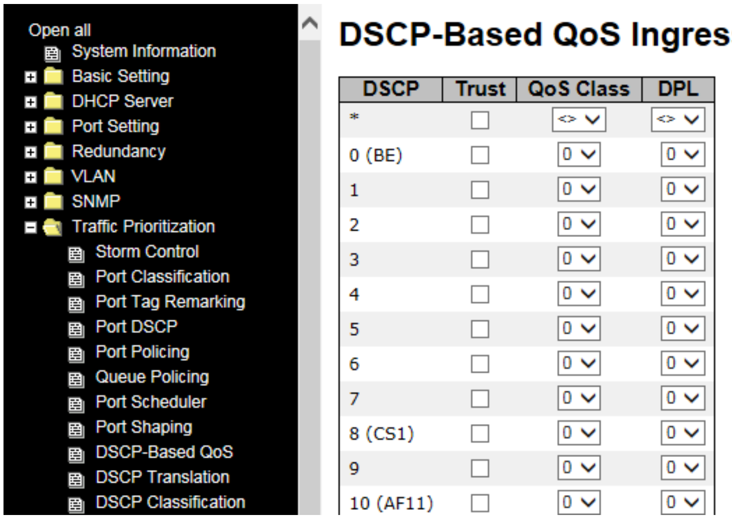
5.6.9 Port Shaping

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

Label	Description
Port	The switch port number to which the following settings will be applied. Click on the port number to configure the shapers.
Mode	Shows **disabled** or actual queue shaper rate - e.g. "800 Mbps".
Qi	Shows **disabled** or actual port shaper rate - e.g. "800 Mbps".

5.6.10 DSCP Based QoS

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



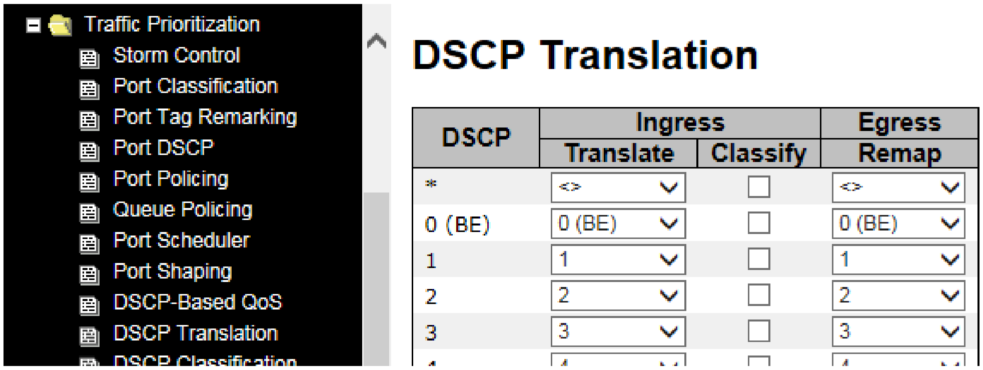
DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*	□	<>	<>
0 (BE)	□	0	0
1	□	0	0
2	□	0	0
3	□	0	0
4	□	0	0
5	□	0	0
6	□	0	0
7	□	0	0
8 (CS1)	□	0	0
9	□	0	0
10 (AF11)	□	0	0

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

5.6.11 DSCP Translation

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



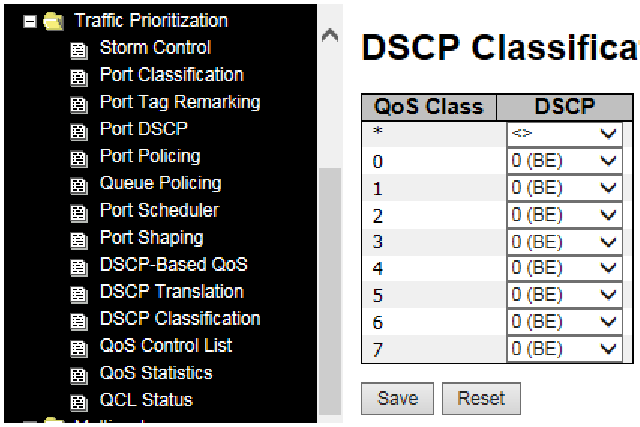
DSCP Translation

DSCP	Ingress		Egress
	Translate	Classify	Remap
*	<>	□	<>
0 (BE)	0 (BE)	□	0 (BE)
1	1	□	1
2	2	□	2
3	3	□	3

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

5.6.12 DSCP Classification

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



DSCP Classification

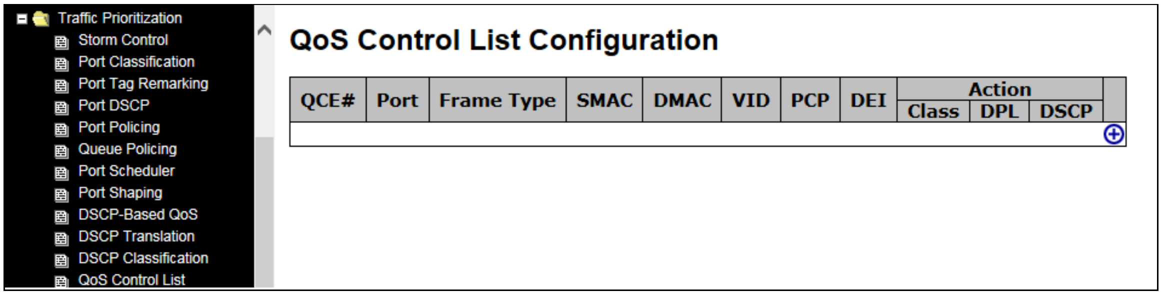
QoS Class	DSCP
*	<>
0	0 (BE)
1	0 (BE)
2	0 (BE)
3	0 (BE)
4	0 (BE)
5	0 (BE)
6	0 (BE)
7	0 (BE)

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

5.6.13 QoS Control List

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

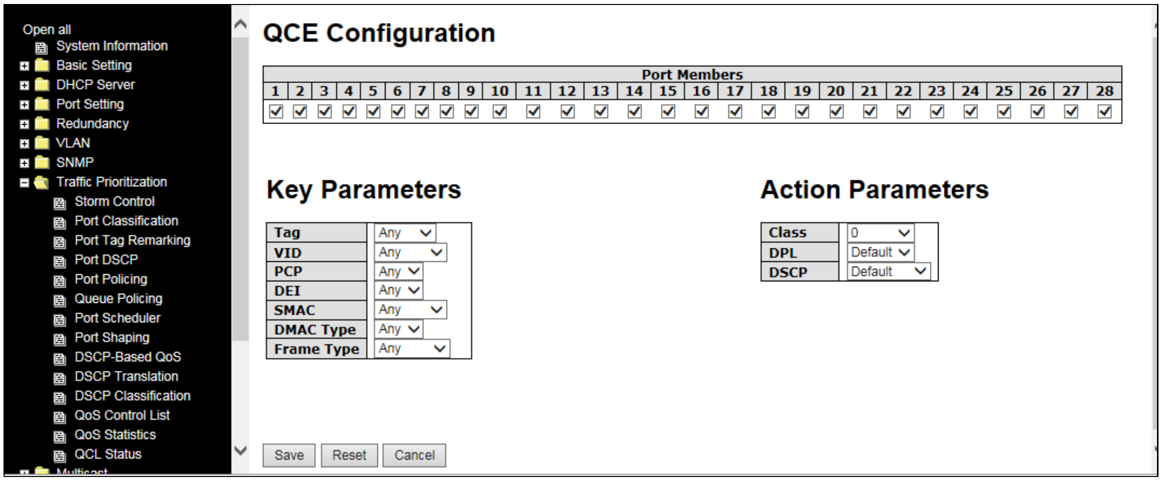
From the default QoS Control List Configuration page click the Add icon (⊕) in the lower right corner.



QoS Control List Configuration

QCE#	Port	Frame Type	SMAC	DMAC	VID	PCP	DEI	Action		
								Class	DPL	DSCP
										⊕

The default QCE Configuration page displays:



QCE Configuration

Port Members																											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Key Parameters

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

Action Parameters

Class	0
DPL	Default
DSCP	Default

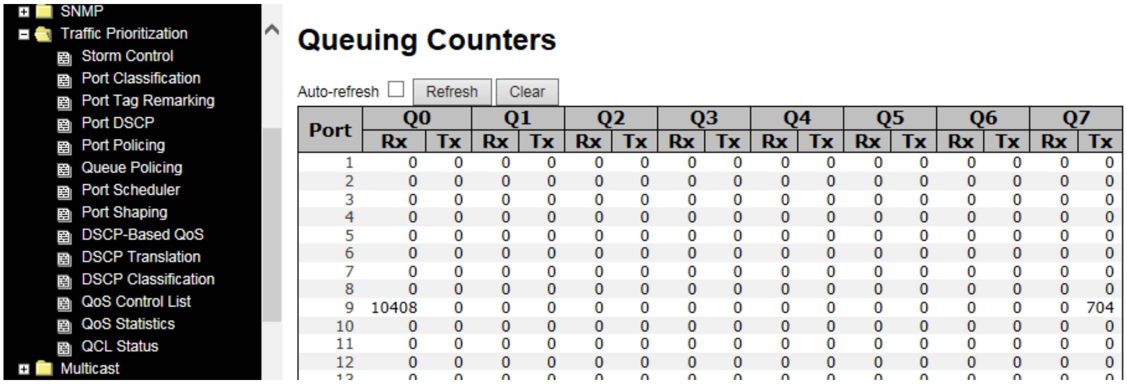
Label	Description
Port Members	Check to include the port in the QCL entry. By default, all ports are included.
Key Parameters	Key configurations include: **Tag**: value of tag, can be Any, Untag or Tag. **VID**: valid value of VLAN ID, can be any value from 1 to 4095 Any: user can enter either a specific value or a range of VIDs. **PCP**: Priority Code Point, can be specific numbers (0, 1, 2, 3, 4, 5, 6, 7), a range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or Any. **DEI**: Drop Eligible Indicator, can be 0, 1, or Any. **SMAC**: Source MAC Address, can be 24 MS bits (OUI) or Any. **DMAC Type**: Destination MAC type, can be unicast (UC), multicast (MC),

	broadcast (BC) or Any. Frame Type can be the following values: Any, Ethernet, LLC, SNAP, IPv4, or IPv6. Note: all frame types are explained below.
Any	Allow all types of frames.
Ethernet	Valid Ethernet values can range from 0x600 to 0xFFFF or Any' but excluding 0x800(IPv4) and 0x86DD(IPv6). The default value is Any.
LLC	SSAP Address: valid SSAP (Source Service Access Point) values can range from 0x00 to 0xFF or Any. The default value is Any. DSAP Address: valid DSAP (Destination Service Access Point) values can range from 0x00 to 0xFF or Any. The default value is Any. Control Valid Control: valid values are 0x00 to 0xFF or Any. The default value is Any.
SNAP	PID: valid PID (Ethernet type) values can range from 0x00 to 0xFFFF or Any. The default value is Any.
IPv4	Protocol IP Protocol Number: (0-255, TCP or UDP) or Any Source IP: specific Source IP address in value/mask format or Any. IP and mask are in the format of x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When the mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero. DSCP (Differentiated Services Code Point): can be a specific value, a range, or Any. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43. IP Fragment: Ipv4 frame fragmented options include 'yes', 'no', and 'any'. Sport Source TCP/UDP Port: (0-65535) or Any, specific value or port range applicable for IP protocol UDP/TCP. Dport Destination TCP/UDP Port: (0-65535) or Any, specific value or port range applicable for IP protocol UDP/TCP.
IPv6	Protocol IP protocol number: (0-255, TCP or UDP) or Any. Source IP IPv6 source address: (a.b.c.d) or Any, 32 LS bits. DSCP (Differentiated Services Code Point): can be a specific value, a range, or Any. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43. Sport Source TCP/UDP port: (0-65535) or Any, specific value or port range applicable for IP protocol UDP/TCP.

	Dport Destination TCP/UDP port: (0-65535) or Any, specific value or port range applicable for IP protocol UDP/TCP.
Action Parameters	Class QoS class: (0-7) or Default. Valid Drop Precedence Level value can be (0-1) or Default. Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or Default. Default means that the default classified value is not modified by this QCE.

5.6.14 QoS Statistics (Queuing Counters)

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



Queuing Counters

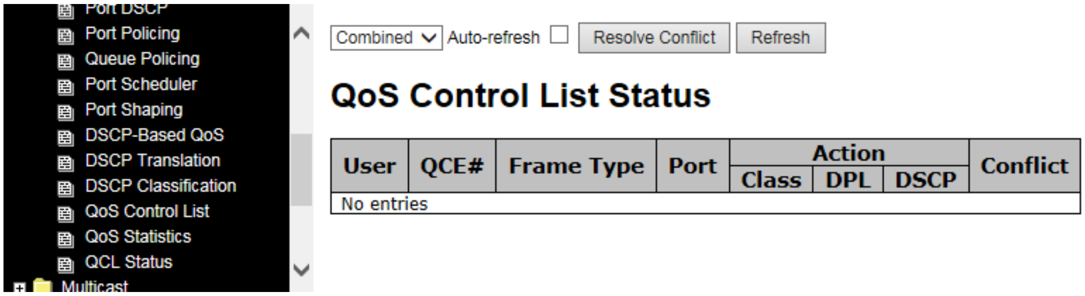
Auto-refresh □

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	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	10408	0	0	0	0	0	0	0	0	0	0	0	0	0	0	704
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

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

5.6.15 QCL Status

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



QoS Control List Status

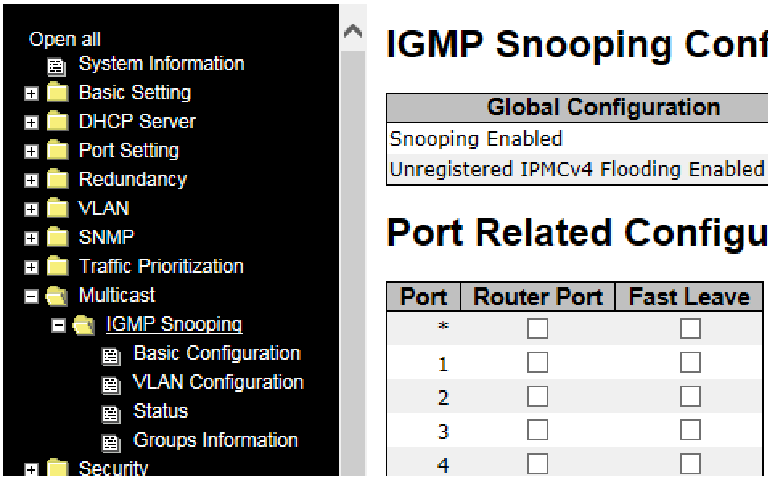
User	QCE#	Frame Type	Port	Action			Conflict
				Class	DPL	DSCP	
No entries							

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

5.7 Multicast

5.7.1 IGMP Snooping

This page provides IGMP Snooping related configurations. The **Basic Configuration** page is shown below.



IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	□
Unregistered IPMCv4 Flooding Enabled	☑

Port Related Configuration

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

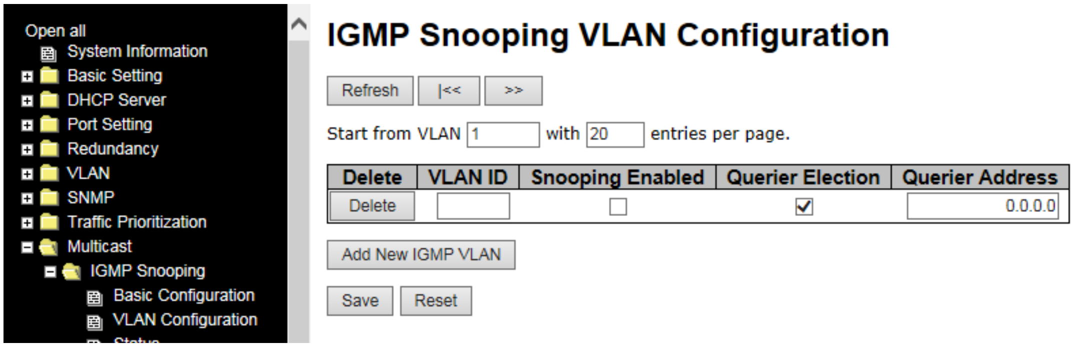
Label	Description
Snooping Enabled	Check to enable global IGMP snooping
Unregistered IPMCv4Flooding Enabled	Check to enable unregistered IPMC traffic flooding.
Port	The port number being configured on this line.
Router Port	Specifies which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Check to enable fast leave on the port.

5.7.2 VLAN Configurations of IGMP Snooping

Each page shows up to 99 entries from the VLAN table, with a default value of 20, selected by the **Entries Per Page** input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

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

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



IGMP Snooping VLAN Configuration

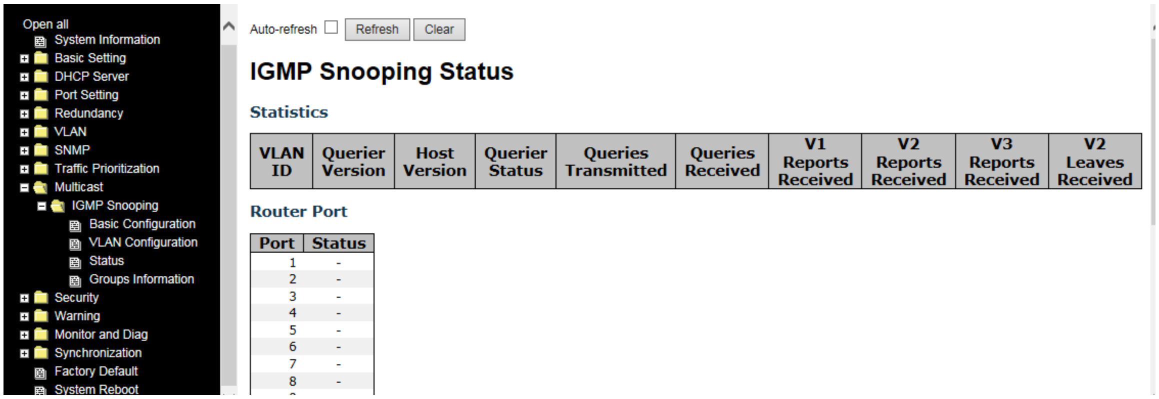
Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address
Delete		☐	☑	0.0.0.0

Label	Description
Delete	Check to delete the entry. The designated entry is deleted at the next save.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enable	Check to enable IGMP snooping for individual VLAN. Up to 32 VLANs can be selected.
IGMP Querier	Check to enable the IGMP Querier in the VLAN. Uncheck (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, the system uses the IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, the system uses the first available IPv4 management address. Otherwise, the system uses a pre-defined value. By default, this value will be 192.0.2.1.

5.7.3 IGMP Snooping Status

This page provides IGMP snooping status.



IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

Label	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	Active Querier version.
Host Version	Active Host version.
Querier Status	Shows the Querier status as **ACTIVE** or **IDLE** or **DISABLE.**
Querier Received	The number of transmitted Querier.
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 Leave Received	The number of received V2 leave packets.
Router Port	Displays 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	Indicates whether a specific port is a router port or not.

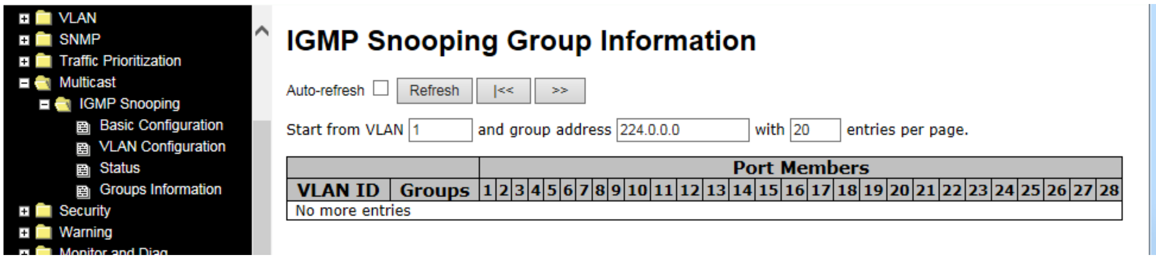
5.7.4 Groups Information of IGMP Snooping

Entries in the **IGMP Snooping Group** table are shown on this page. The **t**able entries are sorted first by VLAN ID, and then by group.

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 **Refresh** 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 **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The **>>** button 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 Snooping Group Information

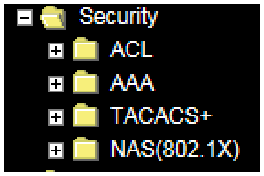
Auto-refresh □ Refresh |<< >>

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

		Port Members																											
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
No more entries																													

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

5.8 Security

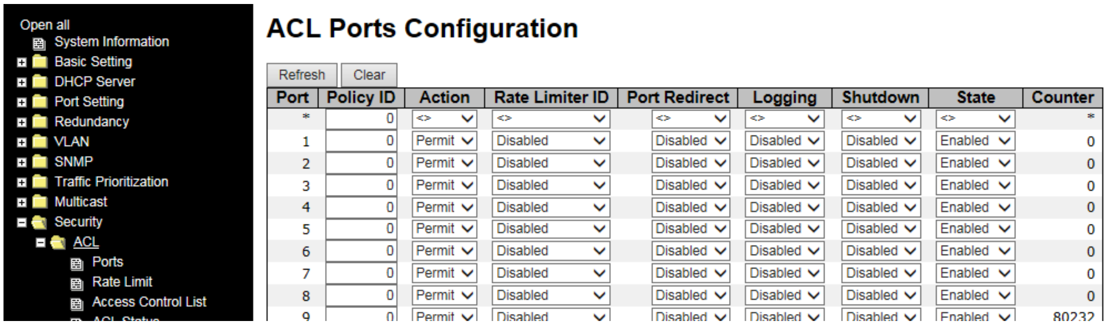


The Security main functions include ACL, AAA, TACACS+, and NAS(802.1X) as described in the following sections.

5.8.1 ACL

Ports

This page lets you configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.



ACL Ports Configuration

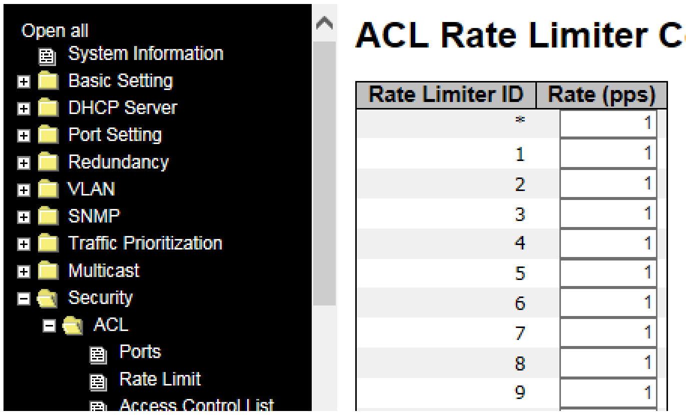
Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Logging	Shutdown	State	Counter
*	0	<>	<>	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	80232

Label	Description
Port	The switch port number to which the following settings will be applied
Policy ID	Select to apply a policy to the port. The allowed values are **1** - **8**. The default value is **1**.
Action	Select to **Permit** to permit or **Deny** to deny forwarding. The default value is **Permit**.
Rate Limiter ID	Select a rate limiter for the port. The allowed values are **Disabled** or numbers from **1** - **15**. The default value is **Disabled**.
Port Redirect	Select which port frames are copied to. The allowed values are **Disabled** or a specific port number. The default value is **Disabled**.
Logging	Specifies the logging operation of the port. The allowed values are: **Enabled**: frames received on the port are stored in the system log **Disabled**: frames received on the port are not logged. The default value is **Disabled**. Please note that system log memory capacity and logging rate is limited.

Shutdown	Specifies the shutdown operation of this port. Valid 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**.
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.

Rate Limit

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



ACL Rate Limiter Configuration

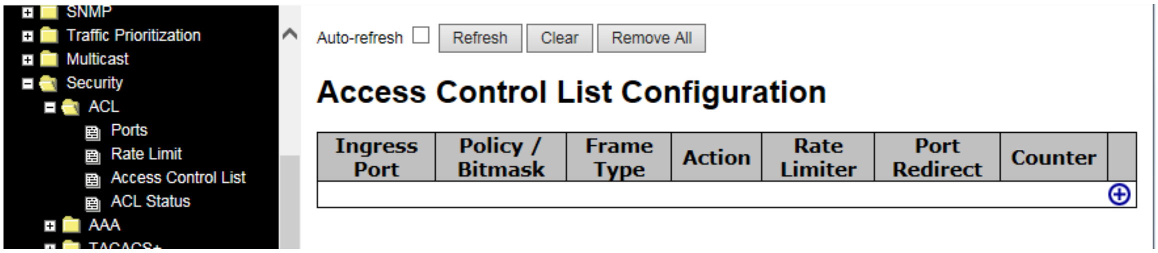
Rate Limiter ID	Rate (pps)
*	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1

Label	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate (pps)	The rate can be configured as 0-131071 pps (packets per second).

ACL Control List

This page lets you configure ACE (Access Control Entry). An ACE consists of several parameters. These parameters vary with the frame type you have selected. First select the ingress port for the ACE, and then the frame type. Different parameter options are displayed according to the frame type you selected. A frame matching the ACE can be configured here.

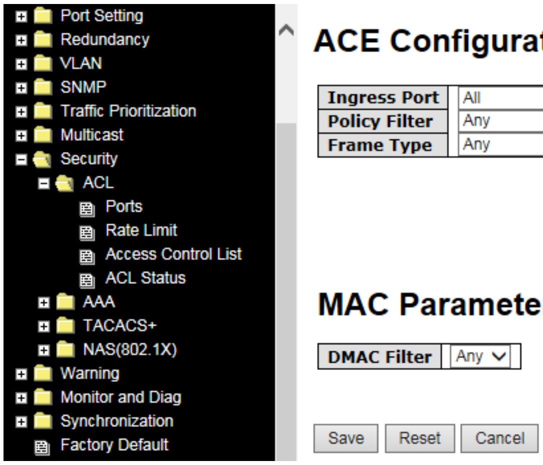
The default Access Control List Configuration page is shown below.



Access Control List Configuration

Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Counter

From the default page click the Add icon (⊕) in the lower right corner to display the default ACE Configuration page.



ACE Configuration

Ingress Port	All
Policy Filter	Any
Frame Type	Any

Action	Permit
Rate Limiter	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

MAC Parameters

DMAC Filter	Any

VLAN Parameters

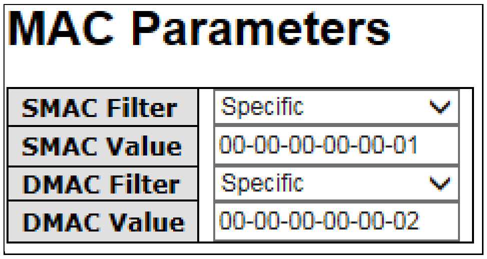
VLAN ID Filter	Any
Tag Priority	Any

The ACE Configuration parameters are described below.

Label	Description
Ingress Port	Indicates the ingress port to which the ACE will apply. **Any**: the ACE applies to any port. **Port n**: the ACE applies to this port number, where ***n*** is the number of the switch port. **Policy n**: the ACE applies to this policy number, where ***n*** can range from 1 - 8.

Frame Type	Indicates the frame type of the ACE. These frame types are mutually exclusive. **Any**: any frame can match the ACE. **Ethernet Type**: only Ethernet type frames can match the ACE. The IEEE 802.3 descripts the value of length/types should be greater than or equal to 1536 decimal (equal to 0600 hexadecimal). **ARP**: only ARP frames can match the ACE. Notice the ARP frames will not match the ACE with Ethernet type. **IPv4**: only IPv4 frames can match the ACE. Notice the IPv4 frames will not match the ACE with Ethernet type.
Action	Specifies the action to take when a frame matches the ACE. **Permit**: takes action when the frame matches the ACE. **Deny**: drops the frame matching the ACE.
Rate Limiter	Specifies the rate limiter in number of base units. The allowed range is 1 to 15. **Disabled** means the rate limiter operation is disabled.
Port 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.
Logging	Specifies the logging operation of the ACE. The allowed values are: **Enabled**: frames matching the ACE are stored in the system log. **Disabled**: frames matching the ACE are not logged. Please note that system log memory capacity and logging rate is limited.
Shutdown	Specifies the shutdown operation of the ACE. The allowed values are: **Enabled**: if a frame matches the ACE, the ingress port will be disabled. **Disabled**: port shutdown is disabled for the ACE.
Counter	Indicates the number of times the ACE matched by a frame.

MAC Parameters

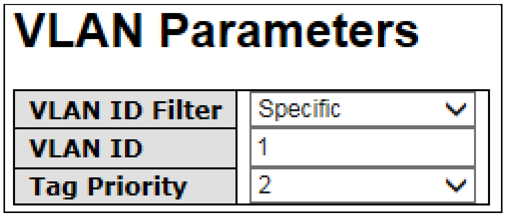


MAC Parameters

SMAC Filter	Specific
SMAC Value	00-00-00-00-00-01
DMAC Filter	Specific
DMAC Value	00-00-00-00-00-02

Label	Description
SMAC Filter	(Only displayed when the frame type is Ethernet Type or ARP.) Specifies the source MAC filter for the 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 the ACE, choose this value. A field for entering an SMAC value appears.
SMAC Value	When **Specific** is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". Frames matching the ACE will use this SMAC value.
DMAC Filter	Specifies the destination MAC filter for this ACE **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 the ACE, choose this value. A field for entering a DMAC value appears.
DMAC Value	When **Specific** is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". Frames matching the ACE will use this DMAC value.

VLAN Parameters

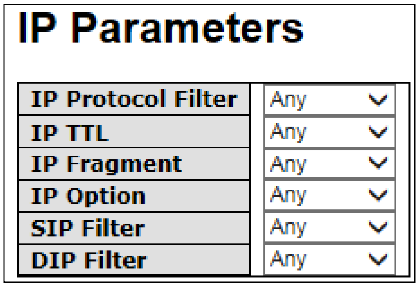


VLAN Parameters

VLAN ID Filter	Specific
VLAN ID	1
Tag Priority	2

Label	Description
VLAN ID Filter	Specifies the VLAN ID filter for the 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 the ACE, choose this value. A field for entering a VLAN ID number appears.
VLAN ID	When **Specific** is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. Frames matching the ACE will use this VLAN ID value.
Tag Priority	Specifies the tag priority for the ACE. A frame matching the ACE will use this tag priority. The allowed number range is 0 to 7. **Any** means that no tag priority is specified (tag priority is "**don't-care**").

IP Parameters



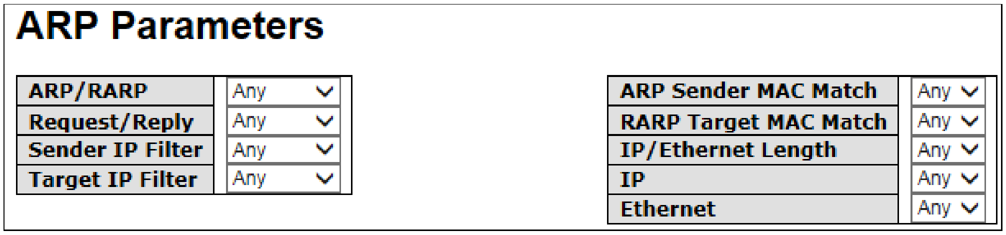
IP Parameters

IP Protocol Filter	Any
IP TTL	Any
IP Fragment	Any
IP Option	Any
SIP Filter	Any
DIP Filter	Any

Label	Description
IP Protocol Filter	Specifies the IP protocol filter for the ACE **Any**: no IP protocol filter is specified ("**don't-care**"). **Specific**: if you want to filter a specific IP protocol filter with the ACE, choose this value. A field for entering an IP protocol filter appears. ICMP: selects ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. For more details of these fields, please refer to the help file. **UDP**: selects UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. For more details of these fields, please refer to the help file. **TCP**: selects TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. For more details of these fields, please refer to the help file.
IP Protocol Value	**Specific** allows you to enter a specific value. The allowed range is 0 to 255. Frames matching the ACE will use this IP protocol value.
IP TTL	Specifies the time-to-live settings for the ACE **Zero**: IPv4 frames with a time-to-live value greater than zero must not be able to match this entry. **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	Specifies the fragment offset settings for the ACE. This includes settings of More Fragments (MF) bit and Fragment Offset (FRAG OFFSET) for an IPv4 frame. **No**: IPv4 frames whose MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.

	Yes: IPv4 frames whose 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	Specifies the options flag settings for the ACE **No**: IPv4 frames whose options flag is set must not be able to match this entry. **Yes**: IPv4 frames whose options flag is set must be able to match this entry. **Any**: any value is allowed ("**don't-care**").
SIP Filter	Specifies 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.
SIP Mask	When **Network** is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
DIP Filter	Specifies the destination IP filter for the ACE **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.
DIP Mask	When **Network** is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

ARP Parameters



ARP Parameters

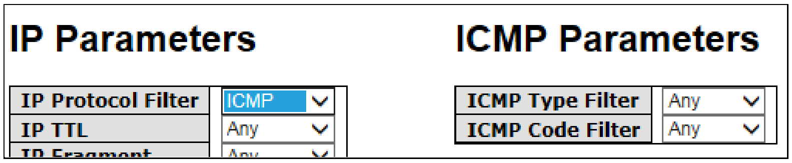
ARP/RARP	Any
Request/Reply	Any
Sender IP Filter	Any
Target IP Filter	Any

ARP Sender MAC Match	Any
RARP Target MAC Match	Any
IP/Ethernet Length	Any
IP	Any
Ethernet	Any

Label	Description
ARP/RARP	Specifies the available ARP/RARP opcode (OP) flag for the ACE **Any**: no ARP/RARP OP flag is specified (OP is "**don't-care**"). **ARP**: frame must have ARP/RARP opcode set to ARP **RARP**: frame must have ARP/RARP opcode set to RARP. **Other**: frame has unknown ARP/RARP Opcode flag.
Request/Reply	Specifies the available ARP/RARP opcode (OP) flag for the ACE **Any**: no ARP/RARP 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	Specifies the sender IP filter for the 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 display.
Sender IP Address	When Host or Network is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.
Sender IP Mask	When Network is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.
Target IP Filter	Specifies the target IP filter for the specific ACE **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 displays. **Network**: target IP filter is set to **Network**. Specify the target IP address and target IP mask in the **Target IP Address** and **Target IP Mask** fields that appear.
Target IP Address	When **Host** or **Network** is selected for the target IP filter, you can enter a

	specific target IP address in dotted decimal notation.
Target IP Mask	When **Network** is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.
ARP SMAC Match	Specifies whether frames will meet the action according to their sender hardware address field (SHA) settings. **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 SMAC Match	Specifies whether frames will meet the action according to their target hardware address field (THA) settings. **0**: RARP frames where THA is not equal to the SMAC address **1**: RARP frames where THA is equal to the SMAC address **Any**: any value is allowed ("**don't-care**")
IP/Ethernet Length	Specifies whether frames will meet the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings. **0**: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must not match this entry. **1**: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must match this entry. **Any**: any value is allowed ("**don't-care**").
IP	Specifies whether frames will meet the action according to their ARP/RARP hardware address space (HRD) settings. **0**: ARP/RARP frames where the HLD is equal to Ethernet (1) must not match this entry. **1**: ARP/RARP frames where the HLD is equal to Ethernet (1) must match this entry. **Any**: any value is allowed ("**don't-care**").
Ethernet	Specifies whether frames will meet the action according to their ARP/RARP protocol address space (PRO) settings. **0**: ARP/RARP frames where the PRO is equal to IP (0x800) must not match this entry. **1**: ARP/RARP frames where the PRO is equal to IP (0x800) must match this entry. **Any**: any value is allowed ("**don't-care**").

ICMP Parameters



IP Parameters

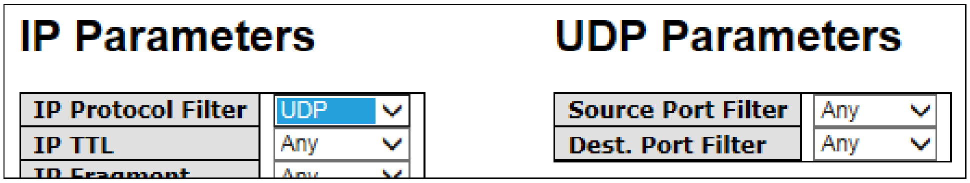
IP Protocol Filter	ICMP
IP TTL	Any
IP Fragment	Any

ICMP Parameters

ICMP Type Filter	Any
ICMP Code Filter	Any

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

TCP / UDP Parameters

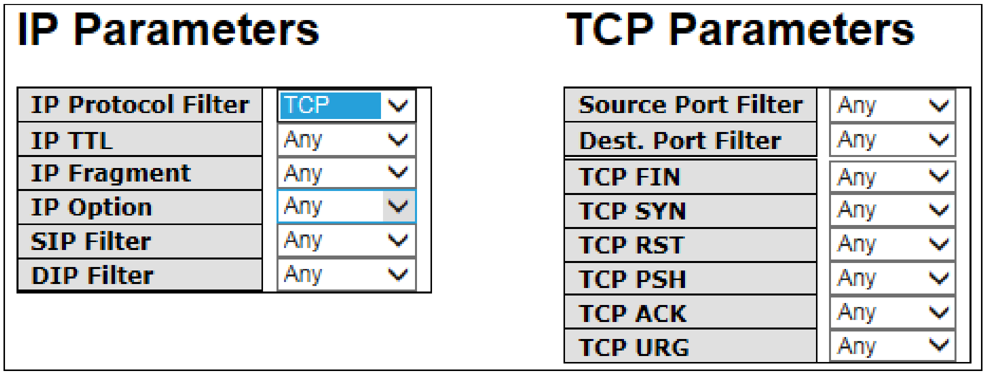


IP Parameters

IP Protocol Filter	UDP
IP TTL	Any
IP Fragment	Any

UDP Parameters

Source Port Filter	Any
Dest. Port Filter	Any



IP Parameters

IP Protocol Filter	TCP
IP TTL	Any
IP Fragment	Any
IP Option	Any
SIP Filter	Any
DIP Filter	Any

TCP Parameters

Source Port Filter	Any
Dest. Port Filter	Any
TCP FIN	Any
TCP SYN	Any
TCP RST	Any
TCP PSH	Any
TCP ACK	Any
TCP URG	Any

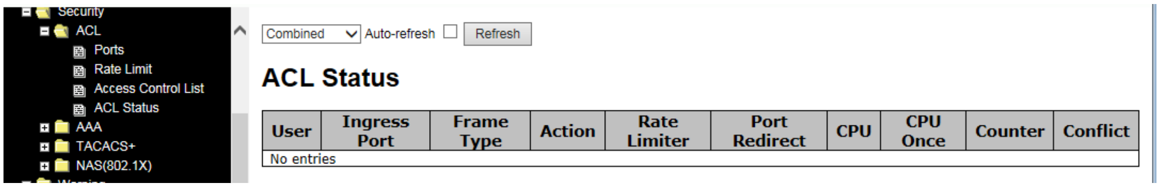
Label	Description
TCP/UDP Source Filter	Specifies the TCP/UDP source filter for the ACE **Any**: no TCP/UDP source filter is specified (TCP/UDP source filter status is "**don't-care**"). **Specific**: if you want to filter a specific TCP/UDP source filter with the ACE, you can enter a specific TCP/UDP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

TCP/UDP Destination Filter	Specifies the TCP/UDP destination filter for the ACE **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 the 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 the ACE, you can enter a specific TCP/UDP destination range. A field for entering a TCP/UDP destination value appears.
TCP/UDP Destination Number	When **Specific** is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame matching the ACE will use this TCP/UDP destination value.
TCP/UDP Destination Range	When **Range** is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame matching the ACE will use this TCP/UDP destination value.
TCP FIN	Specifies the TCP FIN ("no more data from sender") value for the ACE. **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	Specifies the TCP SYN ("synchronize sequence numbers") value for the 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 PSH	Specifies the TCP PSH ("push function") value for the 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	Specifies the TCP ACK ("acknowledgment field significant") value for the ACE **0**: TCP frames where the ACK field is set must not be able to match this entry. **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	Specifies the TCP URG ("urgent pointer field significant") value for the 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**").

ACL Status

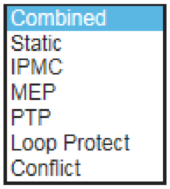
This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 on each switch.



Combined Auto-refresh □ Refresh

ACL Status

User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	CPU	CPU Once	Counter	Conflict
No entries									

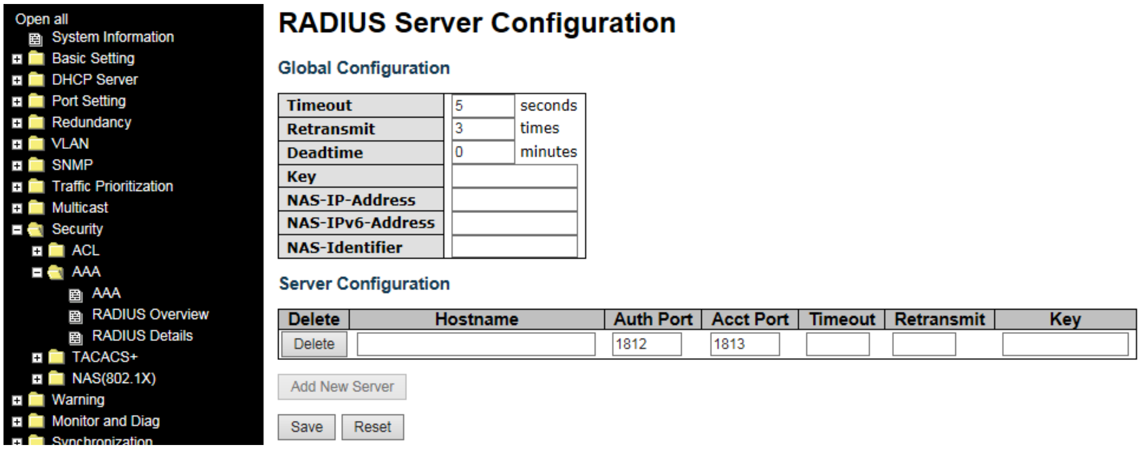
Label	Description
Selection box  Combined Static IPMC MEP PTP Loop Protect Conflict	Allows selection of Combined, Static, MEP, PTP, Loop Protect, Conflict.
User	Indicates the ACL user.
Ingress Port	Indicates the ingress port of the ACE. Possible values are: **All**: The ACE will match all ingress port. **Port**: The ACE will match a specific ingress port
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.

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.
CPU	Forward packet that matched the specific ACE to CPU.
CPU Once	Forward first packet that matched the specific ACE to CPU.
Counter	The counter indicates the number of times the ACE was hit by a frame.
Conflict	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

5.8.2 AAA

RADIUS Server Configuration

This page allows you to configure the RADIUS servers.



RADIUS Server Configuration

Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key		
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
Delete		1812	1813			

Global Configuration

These setting are common for all of the RADIUS servers.

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

Retransmit: 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 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. Deadtime can be set to a number between 0 to 1440 minutes. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

Key: The secret key - up to 63 characters long - shared between the 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-IPv6-Address (Attribute 95): The IPv6 address to be used as attribute 95 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 255 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 IP address of the RADIUS server.

Auth Port: The UDP port to use on the RADIUS server for authentication.

Acct Port: The UDP port to use on the RADIUS server for 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.

Key: This optional setting overrides the global key. Leaving it blank will use the global key.

Adding a New Server

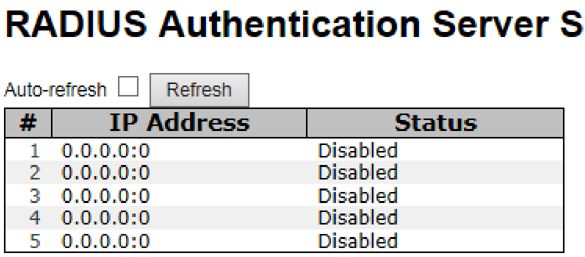
Click the **Add New Server** button to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported.

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

5.8.3 RADIUS

Authentication and Accounting Server Configurations

The table has one row for each RADIUS authentication server and a number of columns:



RADIUS Authentication Server Status Overview

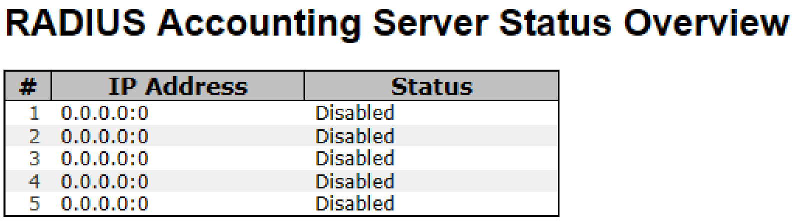
Auto-refresh □ Refresh

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

Label	Description
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
Status	The current status of the server. This field takes one of the following values: **Disabled**: The server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Accounting Server Status Overview

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



RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

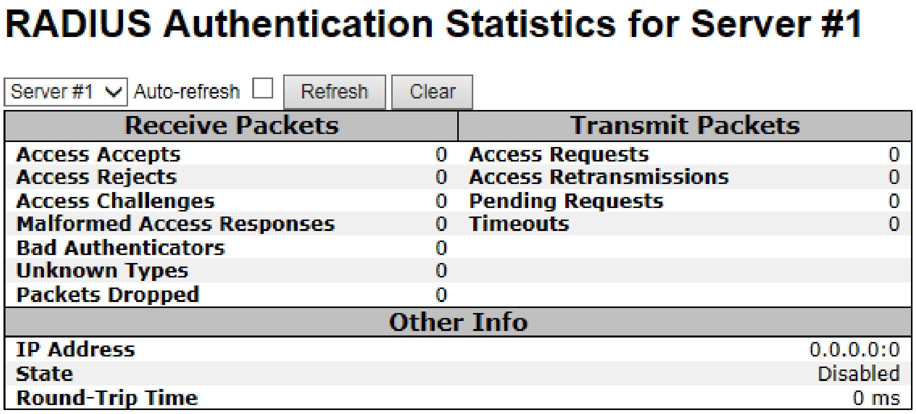
Label	Description
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
Status	The current status of the server. This field takes one of the following values: **Disabled**: The server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Authentication and Accounting Server Statistics

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

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

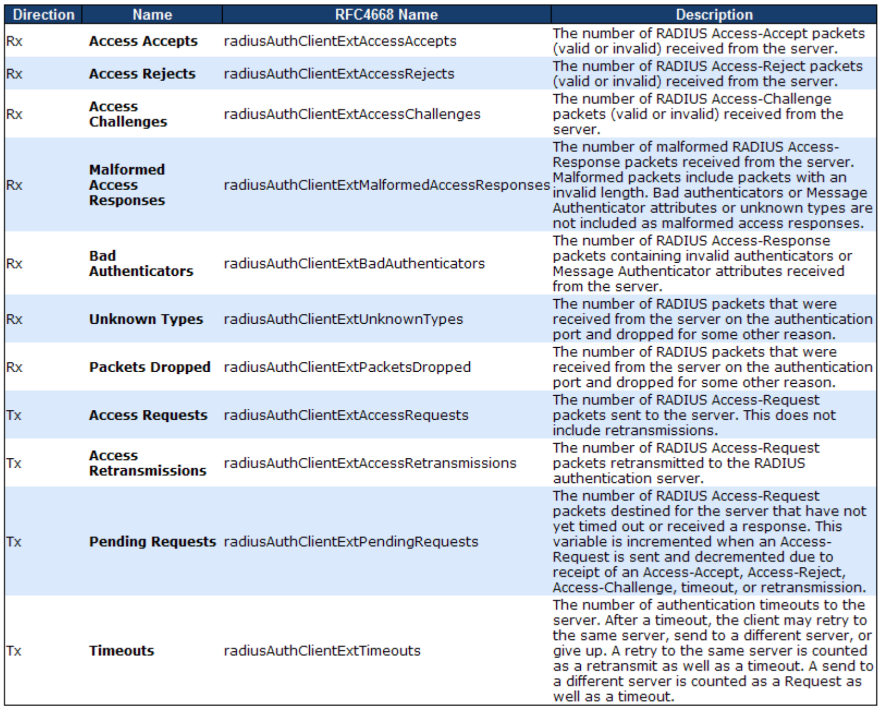
RADIUS Authentication Statistics for Server #x

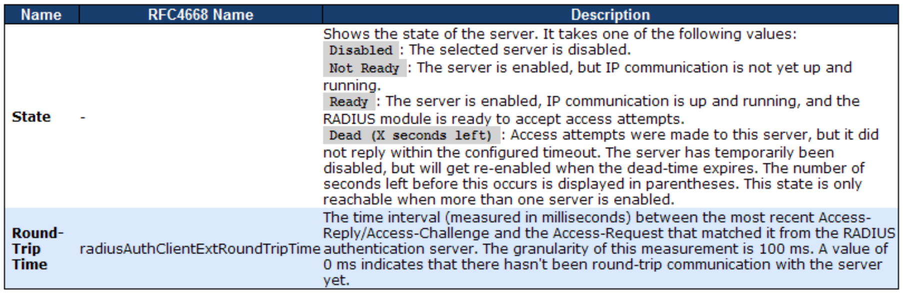


RADIUS Authentication Statistics for Server #1

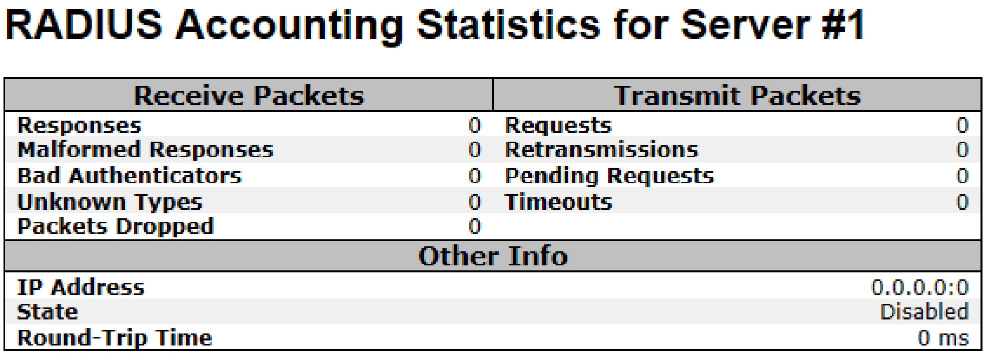
Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		

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

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

<table>
<tr><th>Direction</th><th>Name</th><th>RFC4668 Name</th><th>Description</th></tr>
<tr><td>Rx</td><td><b>Access Accepts</b></td><td>radiusAuthClientExtAccessAccepts</td><td>The number of RADIUS Access-Accept packets (valid or invalid) received from the server.</td></tr>
<tr><td>Rx</td><td><b>Access Rejects</b></td><td>radiusAuthClientExtAccessRejects</td><td>The number of RADIUS Access-Reject packets (valid or invalid) received from the server.</td></tr>
<tr><td>Rx</td><td><b>Access Challenges</b></td><td>radiusAuthClientExtAccessChallenges</td><td>The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.</td></tr>
<tr><td>Rx</td><td><b>Malformed Access Responses</b></td><td>radiusAuthClientExtMalformedAccessResponses</td><td>The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.</td></tr>
<tr><td>Rx</td><td><b>Bad Authenticators</b></td><td>radiusAuthClientExtBadAuthenticators</td><td>The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.</td></tr>
<tr><td>Rx</td><td><b>Unknown Types</b></td><td>radiusAuthClientExtUnknownTypes</td><td>The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.</td></tr>
<tr><td>Rx</td><td><b>Packets Dropped</b></td><td>radiusAuthClientExtPacketsDropped</td><td>The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.</td></tr>
<tr><td>Tx</td><td><b>Access Requests</b></td><td>radiusAuthClientExtAccessRequests</td><td>The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.</td></tr>
<tr><td>Tx</td><td><b>Access Retransmissions</b></td><td>radiusAuthClientExtAccessRetransmissions</td><td>The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.</td></tr>
<tr><td>Tx</td><td><b>Pending Requests</b></td><td>radiusAuthClientExtPendingRequests</td><td>The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.</td></tr>
<tr><td>Tx</td><td><b>Timeouts</b></td><td>radiusAuthClientExtTimeouts</td><td>The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr>
<td><b>Other Info</b></td>
<td>This section contains information about the state of the server and the latest round-trip time.

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

RADIUS Accounting Statistics for Server #x

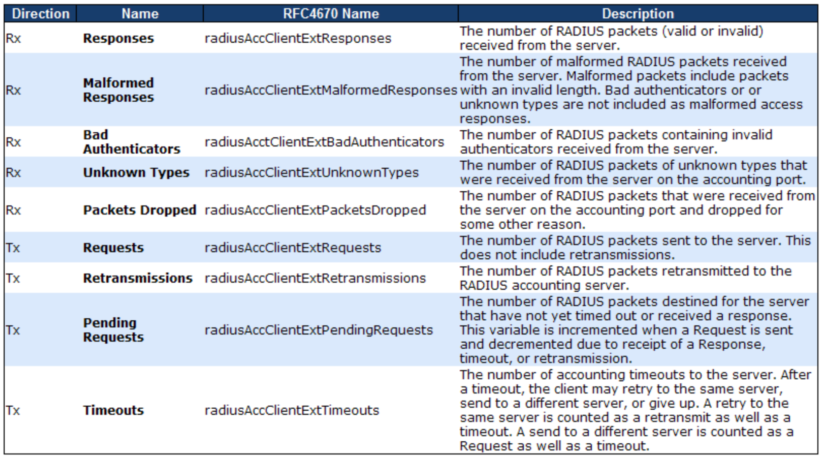


RADIUS Accounting Statistics for Server #1

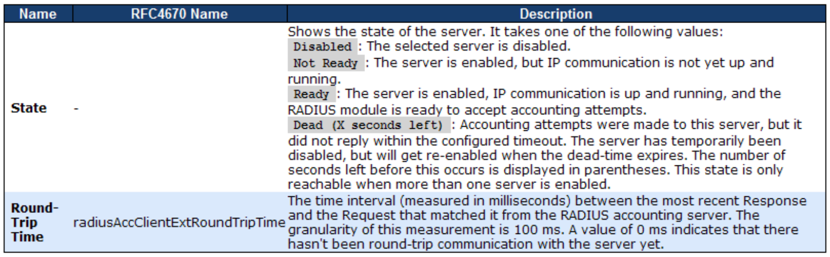
Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		

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

<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td><b>Packet Counters</b></td><td>
RADIUS accounting server packet counters. There are five ‘receive’ and four ‘transmit’ counters.



<table>
<tr><th>Direction</th><th>Name</th><th>RFC4670 Name</th><th>Description</th></tr>
<tr><td>Rx</td><td><b>Responses</b></td><td>radiusAccClientExtResponses</td><td>The number of RADIUS packets (valid or invalid) received from the server.</td></tr>
<tr><td>Rx</td><td><b>Malformed Responses</b></td><td>radiusAccClientExtMalformedResponses</td><td>The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or or unknown types are not included as malformed access responses.</td></tr>
<tr><td>Rx</td><td><b>Bad Authenticators</b></td><td>radiusAcctClientExtBadAuthenticators</td><td>The number of RADIUS packets containing invalid authenticators received from the server.</td></tr>
<tr><td>Rx</td><td><b>Unknown Types</b></td><td>radiusAccClientExtUnknownTypes</td><td>The number of RADIUS packets of unknown types that were received from the server on the accounting port.</td></tr>
<tr><td>Rx</td><td><b>Packets Dropped</b></td><td>radiusAccClientExtPacketsDropped</td><td>The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.</td></tr>
<tr><td>Tx</td><td><b>Requests</b></td><td>radiusAccClientExtRequests</td><td>The number of RADIUS packets sent to the server. This does not include retransmissions.</td></tr>
<tr><td>Tx</td><td><b>Retransmissions</b></td><td>radiusAccClientExtRetransmissions</td><td>The number of RADIUS packets retransmitted to the RADIUS accounting server.</td></tr>
<tr><td>Tx</td><td><b>Pending Requests</b></td><td>radiusAccClientExtPendingRequests</td><td>The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.</td></tr>
<tr><td>Tx</td><td><b>Timeouts</b></td><td>radiusAccClientExtTimeouts</td><td>The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.</td></tr>
</table>
</td></tr>
<tr><td><b>Other Info</b></td><td>
This section contains information about the state of the server and the latest round-trip time.

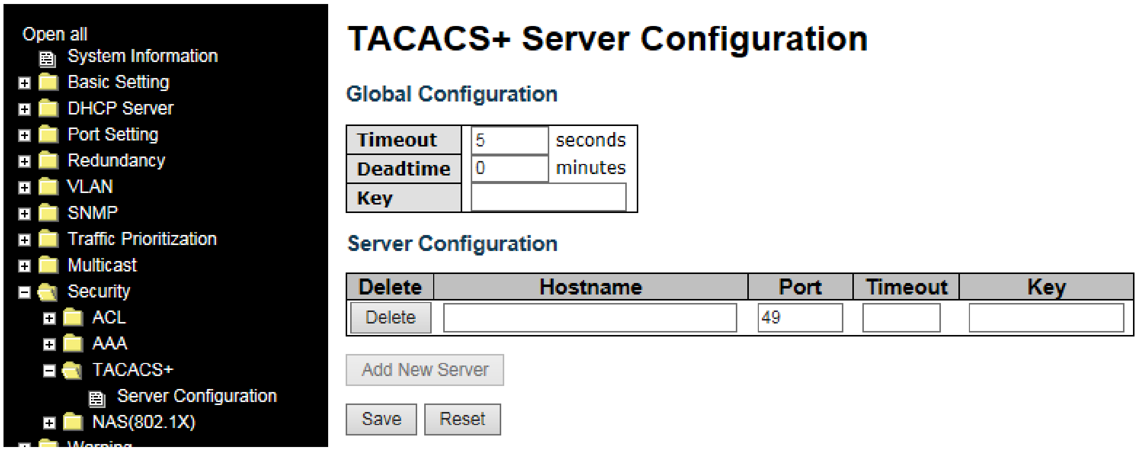


<table>
<tr><th>Name</th><th>RFC4670 Name</th><th>Description</th></tr>
<tr><td><b>State</b></td><td>-</td><td>Shows the state of the server. It takes one of the following values:
`Disabled` : The selected server is disabled.
`Not Ready` : The server is enabled, but IP communication is not yet up and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

5.8.4 TACACS+

TACACS+ Server Configuration

This page allows you to configure the TACACS+ servers.



TACACS+ Server Configuration

Global Configuration

Timeout	5	seconds
Deadtime	0	minutes
Key		

Server Configuration

Delete	Hostname	Port	Timeout	Key
Delete		49		

Global Configuration

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

Label	Description
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead
Deadtime	Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
Key	The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Configuration

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

Label	Description
Delete	To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.
Hostname	The IP address of the TACACS+ server.
Port	The TCP port to use on the TACACS+ server for authentication.
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
Key	This optional setting overrides the global key. Leaving it blank will use the global key.
Adding a New Server	Click the Add New Server button to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported. The Delete button can be used to undo the addition of the new server.

5.8.5 NAS (802.1x)

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers (the backend servers) determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the **Configuration** > **Security** > **AAA** page.

MAC-based authentication allows for authentication of more than one user on the same port, and does not require the users to have special 802.1X software installed on their system. The switch uses the users' MAC addresses to authenticate against the backend server. As intruders can create counterfeit MAC addresses, MAC-based authentication is less secure than 802.1X authentication.

Overview of 802.1X (Port-Based) Authentication

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

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding the result to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

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

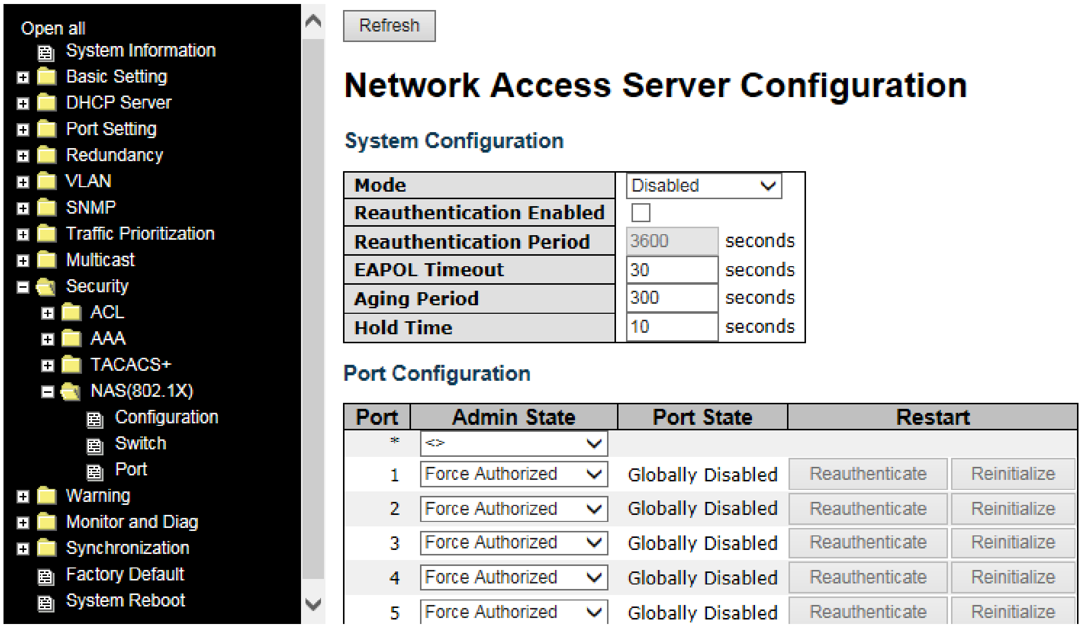
Overview of MAC-Based Authentication

Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string in the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using static entries into the MAC Table. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients do not need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users, equipment whose MAC address is a valid RADIUS user can be used by anyone, and only the MD5-Challenge method is supported.

Network Access Server Configuration

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



Network Access Server Configuration

System Configuration

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

Port Configuration

Port	Admin State	Port State	Restart	
*	<>			
1	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize

Label	Description
Mode	Indicates if 802.1X and MAC-based authentication is globally enabled or disabled on the switch. If globally disabled, all ports are allowed to forward frames.
Reauthentication Enabled	If checked, clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore does not imply that a client is still present on a port (see Age Period below).
Reauthentication Period	Determines the period, in seconds, after which a connected client must be re-authenticated. This is only active if the **Reauthentication Enabled** checkbox is checked. Valid range of the value is 1 to 3600 seconds.
EAPOL Timeout	Determines the time for retransmission of Request Identity EAPOL frames. Valid range of the value is 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 does not cause direct communications between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.
Hold Time	This setting applies to the following modes, i.e. modes using the **Port Security** functionality to secure MAC addresses: **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 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 10 - 1000000 seconds.
Port	The port number for which the configuration below applies.
Admin State	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available: **Force Authorized:** In this mode, the switch will send one EAPOL Success frame when the port link is 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 is up, and any client on the port will be disallowed network access. **Port-based 802.1X:** In an 802.1X network environment, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames which encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server is RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the

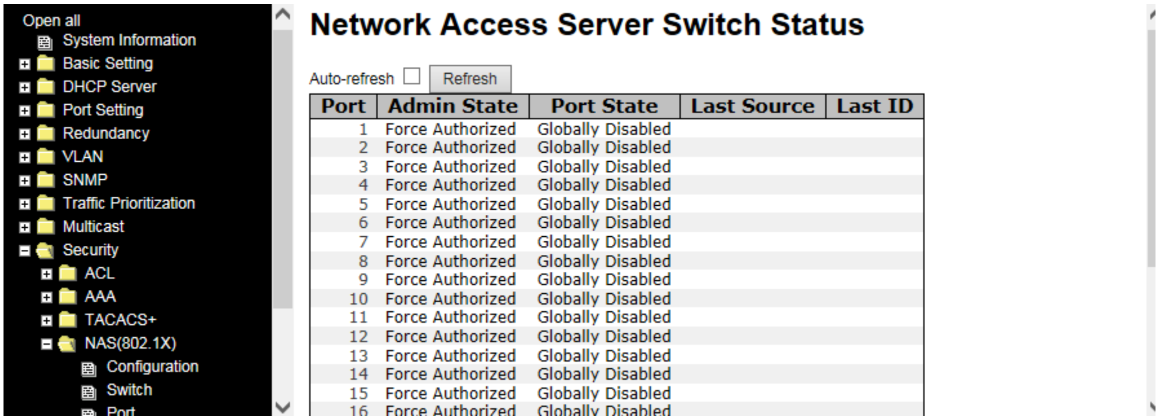
	supplicant's port number on the switch. EAP is very flexible as it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) does not need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it. When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding the result to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant. Note: in an environment where two backend servers are enabled, the server timeout is configured to X seconds (using the authentication configuration page), and the first server in the list is currently down (but not considered dead), if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, it will never be authenticated because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. Since the server has not failed (because the X seconds have not expired), the same server will be contacted when the next backend authentication server request from the switch This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate. **a. Single 802.1X** In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they are not authenticated individually. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is not yet an IEEE standard, but features many of the same characteristics as port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communications between the supplicant and the switch. If more than one supplicant are connected to a port, the one that comes first when the port's link is connected will be the first one considered. If that supplicant does not provide valid credentials within a certain amount of time, the chance will be given to another supplicant. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to

	secure a supplicant's MAC address once successfully authenticated. **b. Multi 802.1X** In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they are not authenticated individually. To overcome this security breach, use the Multi 802.1X variant. Multi 802.1X is not yet an IEEE standard, but features many of the same characteristics as port-based 802.1X. In Multi 802.1X, one or more supplicants can be authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module. In Multi 802.1X it is not possible to use the multicast BPDU MAC address as the destination MAC address for EAPOL frames sent from the switch to the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality. **MAC-based Auth.** Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string in the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be

	forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based authentication has nothing to do with the 802.1X standard. The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients do not need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.
Port State	The current state of the port. It can undertake one of the following values: **Globally Disabled**: NAS is globally disabled. **Link Down**: NAS is globally enabled, but there is no link on the port. **Authorized**: the port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. **Unauthorized:** the port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. **X Auth/Y Unauth**: the port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.
Restart	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect. **Reauthenticate**: schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect on successfully authenticated clients on the port and will not cause the clients to be temporarily unauthorized. **Reinitialize**: forces a reinitialization of the clients on the port and hence a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

NAS Switch Status

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



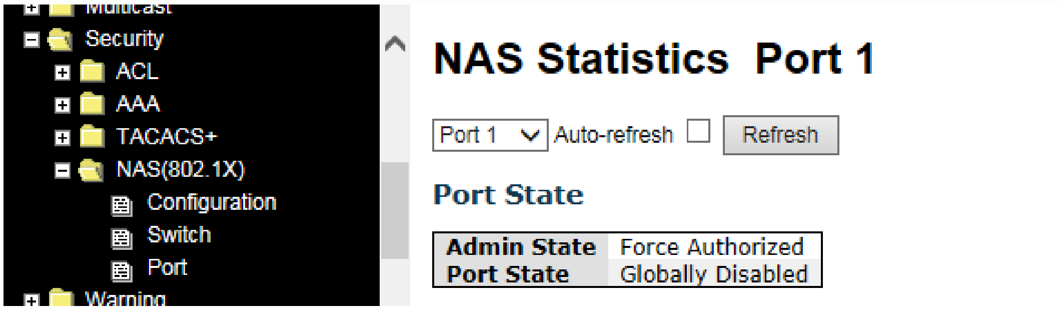
Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID
1	Force Authorized	Globally Disabled		
2	Force Authorized	Globally Disabled		
3	Force Authorized	Globally Disabled		
4	Force Authorized	Globally Disabled		
5	Force Authorized	Globally Disabled		
6	Force Authorized	Globally Disabled		
7	Force Authorized	Globally Disabled		
8	Force Authorized	Globally Disabled		
9	Force Authorized	Globally Disabled		
10	Force Authorized	Globally Disabled		
11	Force Authorized	Globally Disabled		
12	Force Authorized	Globally Disabled		
13	Force Authorized	Globally Disabled		
14	Force Authorized	Globally Disabled		
15	Force Authorized	Globally Disabled		
16	Force Authorized	Globally Disabled		

Label	Description
Port	The switch port number. Click to navigate to detailed 802.1X statistics of each port.
Admin State	The port's current administrative state. Refer to **NAS Admin State** for more details regarding each value.
Port State	The current state of the port. Refer to **NAS Port State** for more details regarding each value.
Last Source	The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.
Last ID	The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

NAS Port Statistics

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

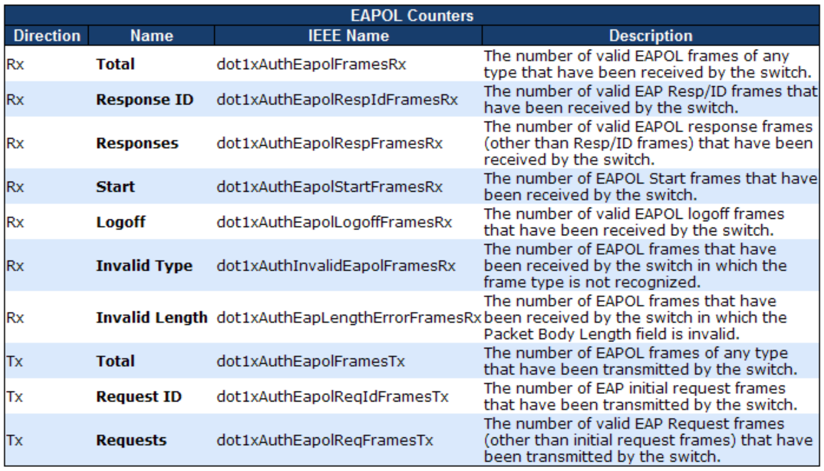


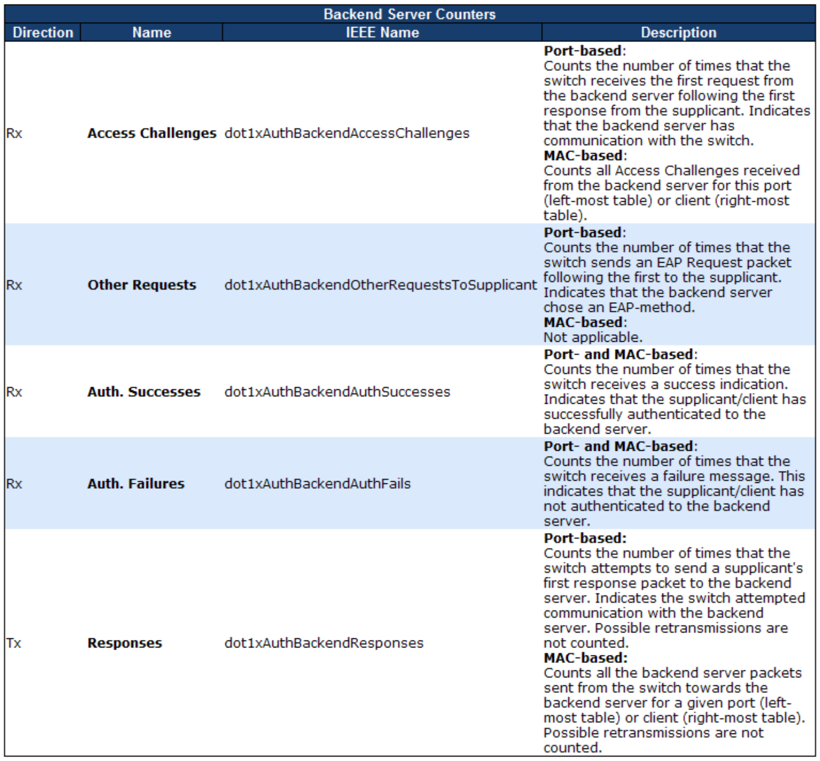
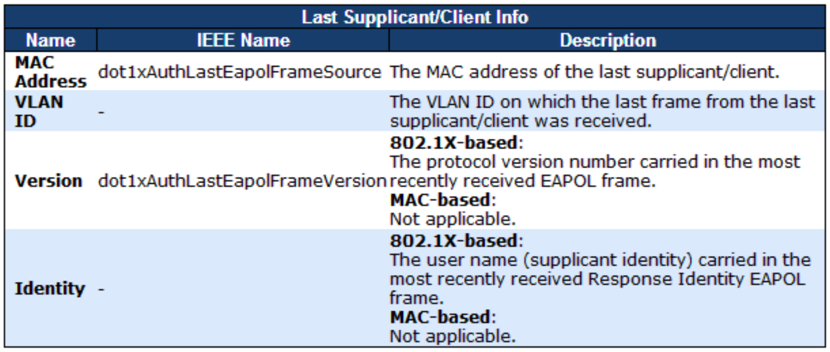
NAS Statistics Port 1

Port 1 Auto-refresh □ Refresh

Port State

Admin State	Force Authorized
Port State	Globally Disabled

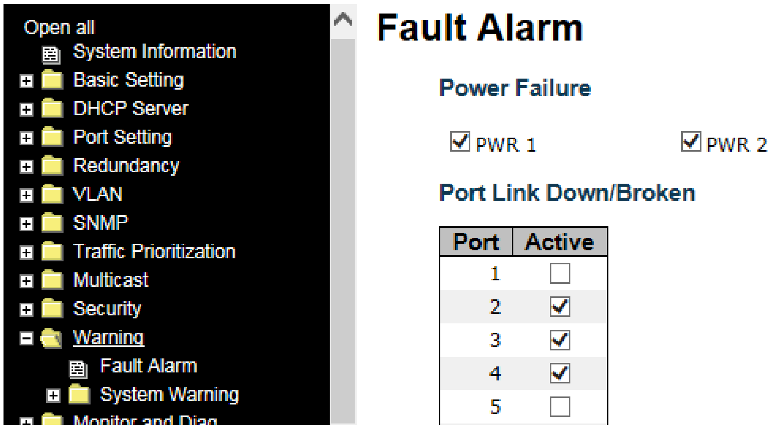
<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td><b>Admin State</b></td><td>The port's current administrative state. Refer to <b>NAS Admin State</b> for more details regarding each value.</td></tr>
<tr><td><b>Port State</b></td><td>The current state of the port. Refer to <b>NAS Port State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

<table>
<tr><th colspan="4">EAPOL Counters</th></tr>
<tr><th>Direction</th><th>Name</th><th>IEEE Name</th><th>Description</th></tr>
<tr><td>Rx</td><td><b>Total</b></td><td>dot1xAuthEapolFramesRx</td><td>The number of valid EAPOL frames of any type that have been received by the switch.</td></tr>
<tr><td>Rx</td><td><b>Response ID</b></td><td>dot1xAuthEapolRespIdFramesRx</td><td>The number of valid EAP Resp/ID frames that have been received by the switch.</td></tr>
<tr><td>Rx</td><td><b>Responses</b></td><td>dot1xAuthEapolRespFramesRx</td><td>The number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch.</td></tr>
<tr><td>Rx</td><td><b>Start</b></td><td>dot1xAuthEapolStartFramesRx</td><td>The number of EAPOL Start frames that have been received by the switch.</td></tr>
<tr><td>Rx</td><td><b>Logoff</b></td><td>dot1xAuthEapolLogoffFramesRx</td><td>The number of valid EAPOL logoff frames that have been received by the switch.</td></tr>
<tr><td>Rx</td><td><b>Invalid Type</b></td><td>dot1xAuthInvalidEapolFramesRx</td><td>The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.</td></tr>
<tr><td>Rx</td><td><b>Invalid Length</b></td><td>dot1xAuthEapLengthErrorFramesRx</td><td>The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.</td></tr>
<tr><td>Tx</td><td><b>Total</b></td><td>dot1xAuthEapolFramesTx</td><td>The number of EAPOL frames of any type that have been transmitted by the switch.</td></tr>
<tr><td>Tx</td><td><b>Request ID</b></td><td>dot1xAuthEapolReqIdFramesTx</td><td>The number of EAP initial request frames that have been transmitted by the switch.</td></tr>
<tr><td>Tx</td><td><b>Requests</b></td><td>dot1xAuthEapolReqFramesTx</td><td>The number of valid EAP Request frames (other than initial request frames) that have been transmitted by the switch.</td></tr>
</table></td></tr>
</table>

<table>
<tr><td><b>Backend Server Counters</b></td><td>
These backend (RADIUS) frame counters are available for the following administrative states:
• <b>802.1X</b>
• <b>MAC-based Auth.</b>

<table>
<tr><th colspan="4">Backend Server Counters</th></tr>
<tr><th>Direction</th><th>Name</th><th>IEEE Name</th><th>Description</th></tr>
<tr><td>Rx</td><td><b>Access Challenges</b></td><td>dot1xAuthBackendAccessChallenges</td><td><b>Port-based</b>:
Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch.
<b>MAC-based</b>:
Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).</td></tr>
<tr><td>Rx</td><td><b>Other Requests</b></td><td>dot1xAuthBackendOtherRequestsToSupplicant</td><td><b>Port-based</b>:
Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method.
<b>MAC-based</b>:
Not applicable.</td></tr>
<tr><td>Rx</td><td><b>Auth. Successes</b></td><td>dot1xAuthBackendAuthSuccesses</td><td><b>Port- and MAC-based</b>:
Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.</td></tr>
<tr><td>Rx</td><td><b>Auth. Failures</b></td><td>dot1xAuthBackendAuthFails</td><td><b>Port- and MAC-based</b>:
Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.</td></tr>
<tr><td>Tx</td><td><b>Responses</b></td><td>dot1xAuthBackendResponses</td><td><b>Port-based</b>:
Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted.
<b>MAC-based</b>:
Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.</td></tr>
</table>
</td></tr>
<tr><td><b>Last Supplicant/Client Info</b></td><td>
Information about the last supplicant/client that attempts to authenticate. This information is available for the following administrative states:
• <b>802.1X</b>
• <b>MAC-based Auth.</b>

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

5.9 Warning (Alerts)

5.9.1 Fault Alarm

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



Fault Alarm

Power Failure

☑ PWR 1 ☑ PWR 2

Port Link Down/Broken

Port	Active
1	□
2	☑
3	☑
4	☑
5	□

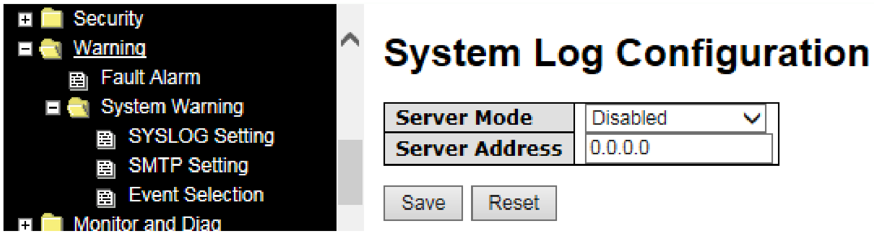
When any selected fault event occurs, the Fault LED in switch panel will be illuminated and the electric relay will be energized at the same time.

Label	Description
Power Failure	Fault alarm when any power source fails. This switch supports dual power sources.
Port Link Down/Broken	Fault alarm when any selected port link is down/broken.

System Warning

SYSLOG Setting

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



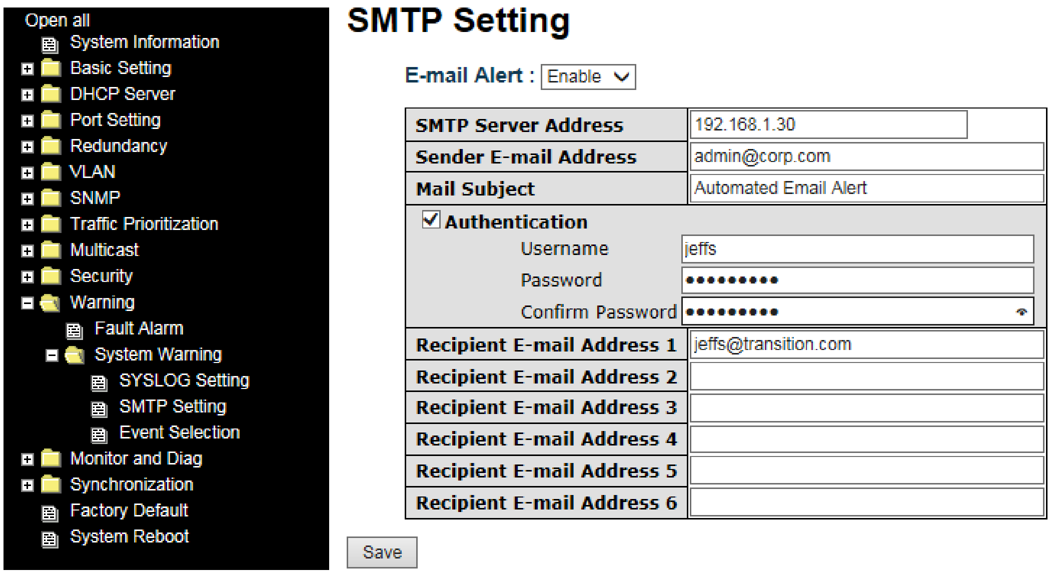
System Log Configuration

Server Mode	Disabled
Server Address	0.0.0.0

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

SMTP Setting

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



SMTP Setting

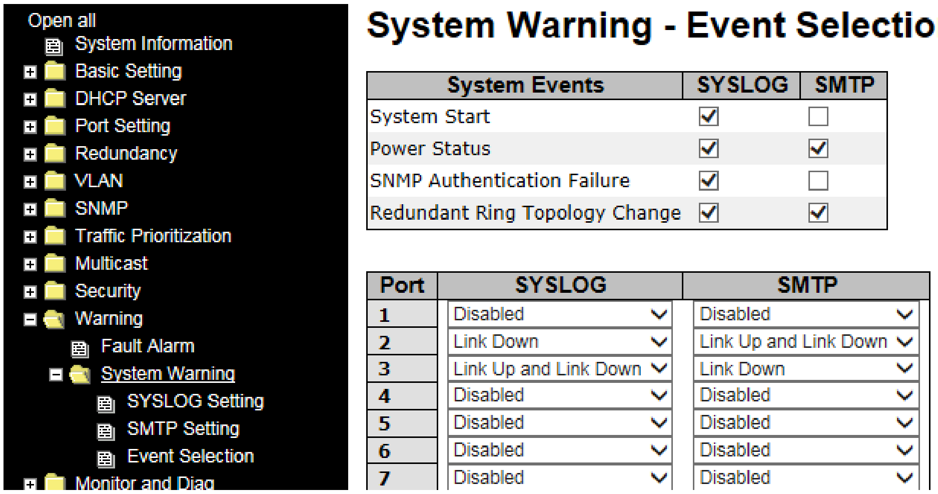
E-mail Alert : Enable

SMTP Server Address	192.168.1.30
Sender E-mail Address	admin@corp.com
Mail Subject	Automated Email Alert
☑ Authentication	
Username	jeffs
Password	●●●●●●●●●
Confirm Password	●●●●●●●●●
Recipient E-mail Address 1	jeffs@transition.com
Recipient E-mail Address 2	
Recipient E-mail Address 3	
Recipient E-mail Address 4	
Recipient E-mail Address 5	
Recipient E-mail Address 6	

Label	Description
E-mail Alert	Enable or Disable transmission of system warnings by e-mail.
Sender E-mail Address	The SMTP server IP address.
Mail Subject	Subject of the email.
Authentication	■ **Username:** the authentication username. ■ **Password:** the authentication password. ■ **Confirm Password:** re-enter password.
Recipient E-mail Address	The recipient's e-mail address. A mail allows for 6 recipients.
Save	Click to activate the configurations.

Event Selection

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



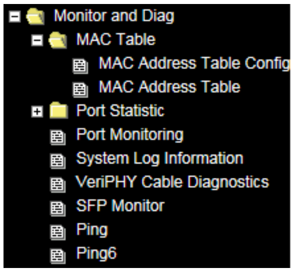
System Warning - Event Selection

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

Port	SYSLOG	SMTP
1	Disabled	Disabled
2	Link Down	Link Up and Link Down
3	Link Up and Link Down	Link Down
4	Disabled	Disabled
5	Disabled	Disabled
6	Disabled	Disabled
7	Disabled	Disabled

Label	Description
System Start	Sends out alerts when the system is restarted.
Power Status	Sends out alerts when power is up or down.
SNMP Authentication Failure	Sends out alert when SNMP authentication fails.
Redundant Ring Topology Change	Sends out alerts when the Redundant Ring topology changes.
Port Event **SYSLOG / SMTP event**	At the dropdown select: • Disabled • Link Up • Link Down • Link Up and Link Down
Save	Click to activate the configurations.
Help	Shows the online help file.

5.10 Monitor and Diag

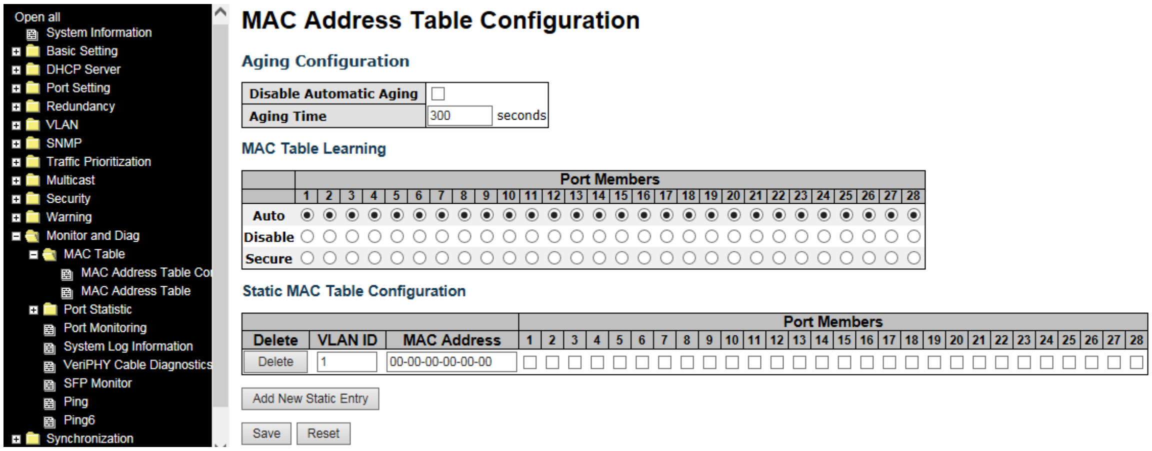


The **Monitor and Diag** sub-menu selections are **MAC Table** and **Port Statistic**.

5.10.1 MAC Table

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

MAC Address Table Configuration



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

MAC Table Learning

	Port Members																											
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Auto	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Static MAC Table Configuration

			Port Members																											
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Delete	1	00-00-00-00-00-00	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

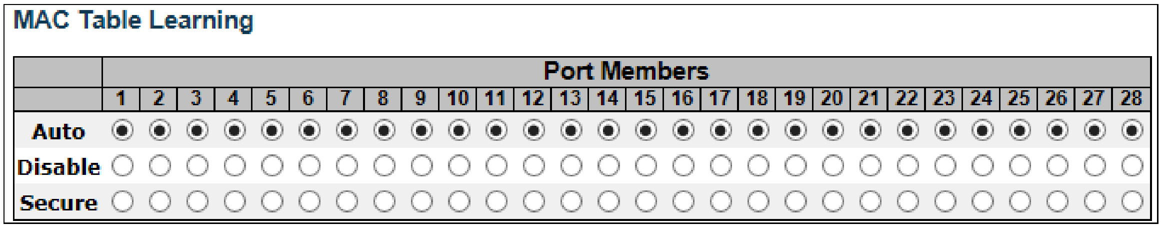
Aging Configuration

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

MAC Table Learning

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

You can configure the port to dynamically learn the MAC address based on these settings:



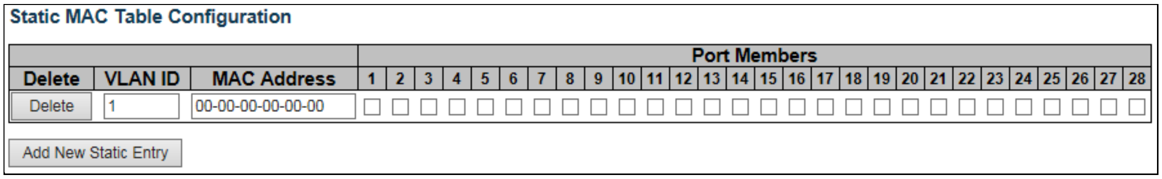
MAC Table Learning

	Port Members																											
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Auto	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Label	Description
Auto	Learning is done automatically as soon as a frame with an unknown SMAC is received.
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped. **Note**: make sure the link used for managing the switch is added to the static Mac table before changing to secure learning mode, otherwise the management link will be lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

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



Static MAC Table Configuration

			Port Members																											
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Delete	1	00-00-00-00-00-00	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

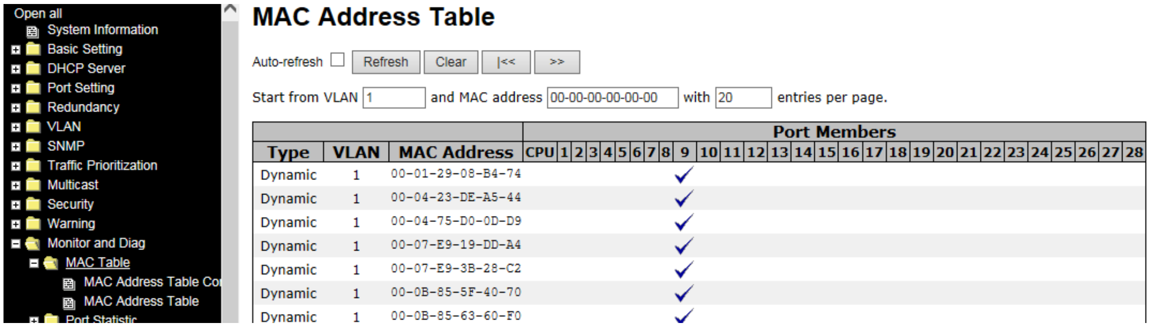
Label	Description
Delete	Check to delete an entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck to modify the entry.
Adding New Static Entry	Click the **Add New Static Entry** button to add a new entry to the static MAC table. You can specify the VLAN ID, MAC address, and port members for the new entry. Click **Save** to save the changes.

MAC Address Table

Each page shows up to 999 entries from the MAC table, with a default value of 20, selected by the **Entries Per Page** input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The **Start from MAC address** and **VLAN** fields allow the user to select the starting point in the MAC table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MAC table match. In addition, the two input fields will – upon clicking **Refresh** - assume the value of the first displayed entry, allows for continuous refresh with the same start address.

The **>>** button will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When it reaches the end, the text "**no more entries**" is shown in the displayed table. Use the **|<<** button to start over.



MAC Address Table

Auto-refresh □ Refresh Clear |<< >>

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

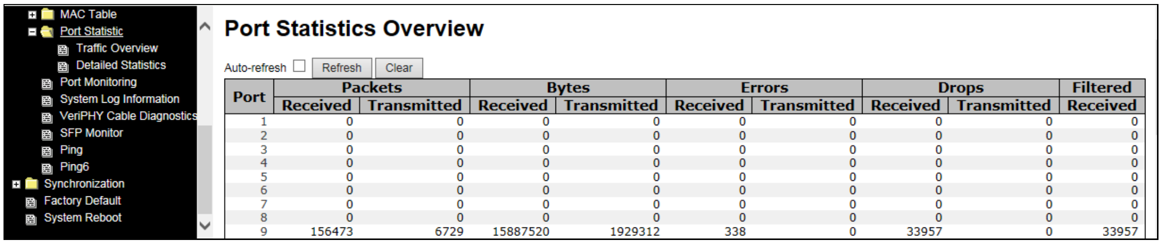
			Port Members																											
Type	**VLAN**	**MAC Address**	**CPU**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**
Dynamic	1	00-01-29-08-B4-74										✓																			
Dynamic	1	00-04-23-DE-A5-44										✓																			
Dynamic	1	00-04-75-D0-0D-D9										✓																			
Dynamic	1	00-07-E9-19-DD-A4										✓																			
Dynamic	1	00-07-E9-3B-28-C2										✓																			
Dynamic	1	00-0B-85-5F-40-70										✓																			
Dynamic	1	00-0B-85-63-60-F0										✓																			

Label	Description
Type	Indicates whether the entry is a Static or Dynamic entry.
VLAN	The VLAN ID of the entry.
MAC address	The MAC address of the entry.
Port Members	The ports that are members of the entry are checked (✓).

5.10.2 Port Statistic

Traffic Overview

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



Port Statistics Overview

Auto-refresh ☐ Refresh Clear

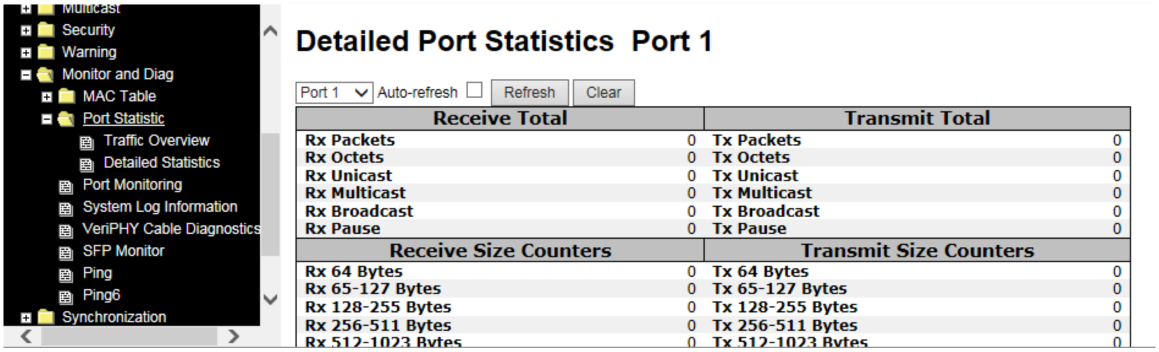
Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	156473	6729	15887520	1929312	338	0	33957	0	33957

Label	Description
Port	The switch port number to which the following settings will be applied.
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions per port.
Drops	The number of frames discarded due to ingress or egress congestion.
Filtered	The number of received frames filtered by the forwarding process.
Auto-refresh	Check to enable an automatic refresh of the page at 3 second intervals.
Refresh	Updates the counter entries, starting from the current entry ID.
Clear	Flushes all counters entries.

Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port drop-down list to decide the details of which switch port to be displayed. The displayed counters include the total number for, the size for, and the errors for receive and transmit.

Detailed Statistics – Total Receive & Transmit



Detailed Port Statistics Port 1

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0

Label	Description
Rx and Tx Packets	The number of received and transmitted (good and bad) packets.
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes, including FCS, except framing bits.
Rx and Tx Unicast	The number of received and transmitted (good and bad) unicast packets.
Rx and Tx Multicast	The number of received and transmitted (good and bad) multicast packets.
Rx and Tx Broadcast	The number of received and transmitted (good and bad) broadcast packets.
Rx and Tx Pause	The number of MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
Rx Drops	The number of frames dropped due to insufficient receive buffer or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short[1] frames received with a valid CRC.
Rx Oversize	The number of long[2] frames received with a valid CRC.
Rx Fragments	The number of short[1] frames received with an invalid CRC.
Rx Jabber	The number of long[2] frames received with an invalid CRC.

Rx Filtered	The number of received frames filtered by the forwarding process
Tx Drops	The number of frames dropped due to output buffer congestion
Tx Late / Exc.Coll.	The number of frames dropped due to excessive or late collisions

1. Short frames are frames smaller than 64 bytes.

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

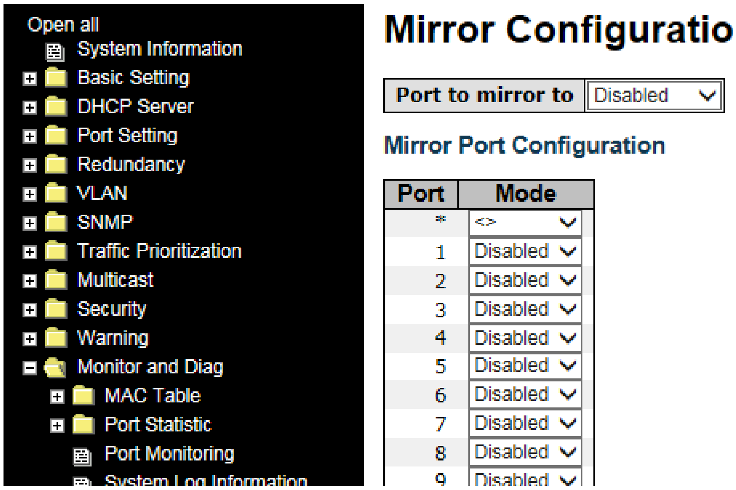
5.10.3 Port Monitor – Mirror Configuration

You can configure port mirroring on this page. To solve network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow. The traffic to be copied to the mirror port is selected as follows:

All frames received on a given port (also known as ingress or source mirroring).

All frames transmitted on a given port (also known as egress or destination mirroring).

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



Mirror Configuration

Port to mirror to: Disabled

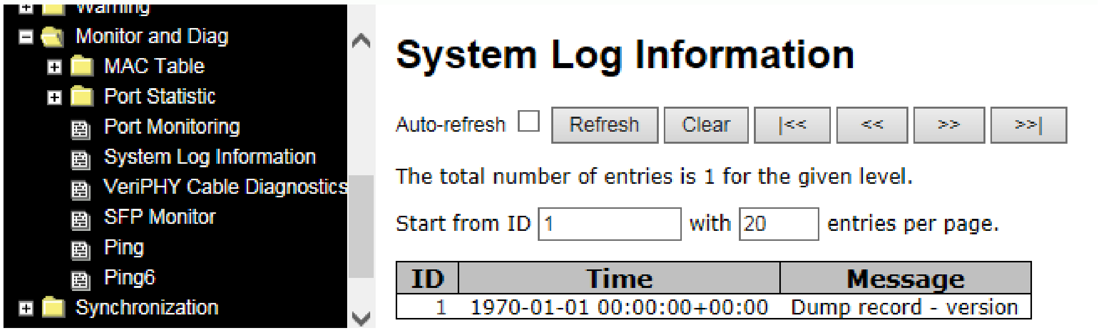
Mirror Port Configuration

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

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

5.10.4 System Log Information

This page provides switch system log information.



System Log Information

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

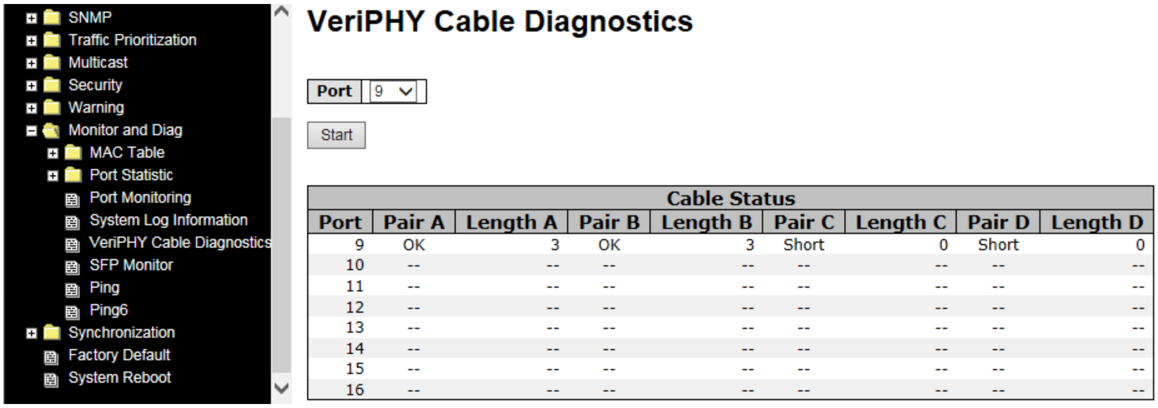
Start from ID 1 with 20 entries per page.

ID	Time	Message
1	1970-01-01 00:00:00+00:00	Dump record - version

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

5.10.5 Cable Diagnostics

This page allows you to perform VeriPHY cable diagnostics.



VeriPHY Cable Diagnostics

Port 9

Cable Status

Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
9	OK	3	OK	3	Short	0	Short	0
10	--	--	--	--	--	--	--	--
11	--	--	--	--	--	--	--	--
12	--	--	--	--	--	--	--	--
13	--	--	--	--	--	--	--	--
14	--	--	--	--	--	--	--	--
15	--	--	--	--	--	--	--	--
16	--	--	--	--	--	--	--	--

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

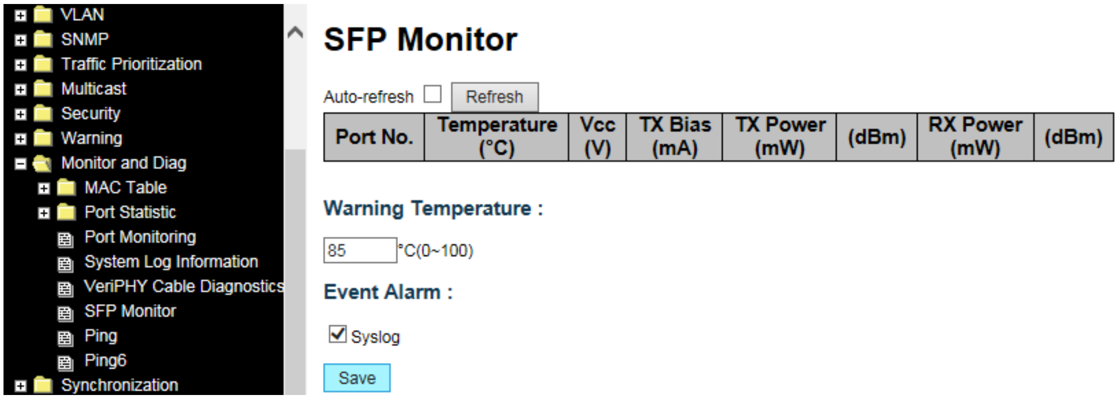
The 10 and 100 Mbps ports will be disconnected while running VeriPHY diagnostics. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Label	Description
Port	The port for which VeriPHY Cable Diagnostics is requested.
Cable Status	**Port**: port number. **Pair**: the status of the cable pair (**OK**, **Open**, **Short**, **Cross**). **Length**: the length (in meters) of the cable pair.

5.10.6 SFP Monitor

SFP modules with DDM (Digital Diagnostic Monitoring) function can measure the temperature of the apparatus, helping you monitor the status of connection and detect errors immediately.

You can manage and set up event alarms through DDM Web interface.



SFP Monitor

Auto-refresh □ Refresh

Port No.	Temperature (°C)	Vcc (V)	TX Bias (mA)	TX Power (mW)	(dBm)	RX Power (mW)	(dBm)

Warning Temperature :

85 °C(0~100)

Event Alarm :

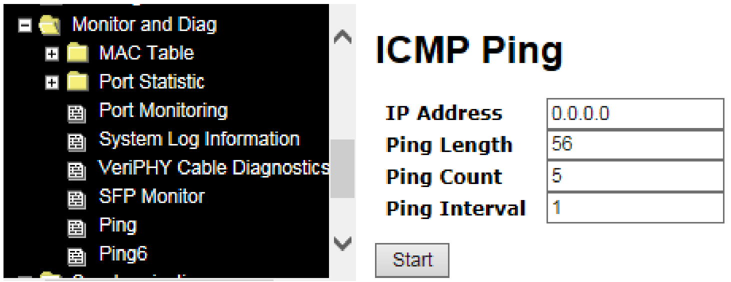
☑ Syslog

Save

Label	Description
Port No.	The port number that this line monitors/ reports.
Temperature (°C)	The SFP temperature in degrees Celsius.
Vcc (V)	The SFP voltage measured in Volts.
TX Bias (mA)	The SFP transmit Bias measured in mA (milliAmps).
TX Power (mW)	The SFP transmit Power measured in mA (milleWatts).
(dBm)	The SFP transmit Power measured in dBm.
RX Power (mW)	The SFP receive Power measured in mA (milleWatts).
(dBm)	The SFP receive Power measured in dBm Decibel-milliwatts.
Warning Temperature : °C (0~100)	Enter the threshold for Temperature warning in Degrees (°) Celsius. The default is 85 °C.
Event Alarm : Syslog	Check the checkbox to report information in the System Log.

5.10.7 Ping

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



ICMP Ping

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

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

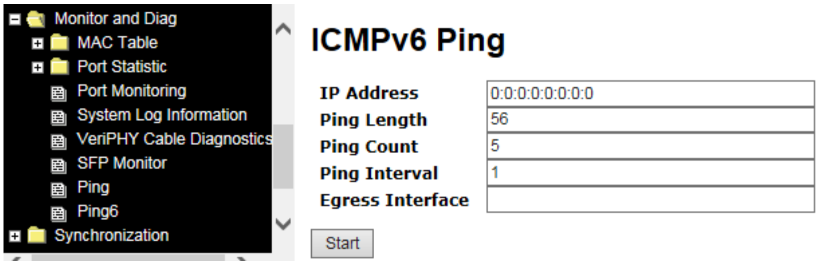
```
PING server 10.10.132.20, 56 bytes of data.
64 bytes from 10.10.132.20: icmp_seq=0, time=0ms
64 bytes from 10.10.132.20: icmp_seq=1, time=0ms
64 bytes from 10.10.132.20: icmp_seq=2, time=0ms
64 bytes from 10.10.132.20: icmp_seq=3, time=0ms
64 bytes from 10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

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

Label	**Description**
IP Address	The destination IP Address.
Ping Length	The payload size of the ICMP packet. Values range from 2 - 1452 bytes.
Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.

5.10.8 IPv6 Ping

This page lets you issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.



ICMPv6 Ping

IP Address	0:0:0:0:0:0:0:0
Ping Length	56
Ping Count	5
Ping Interval	1
Egress Interface	

After you press the **Start** button, ICMPv6 packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING6 server ff02::2, 56 bytes of data.

64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=0, time=10ms

64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=0, time=10ms

64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=1, time=0ms

64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=1, time=0ms

64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=2, time=0ms

64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=2, time=0ms

64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=3, time=0ms

64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=3, time=0ms

64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=4, time=0ms

64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=4, time=0ms

Sent 5 packets, received 10 OK, 0 bad
```

You can configure the following properties of the issued ICMPv6 packets:

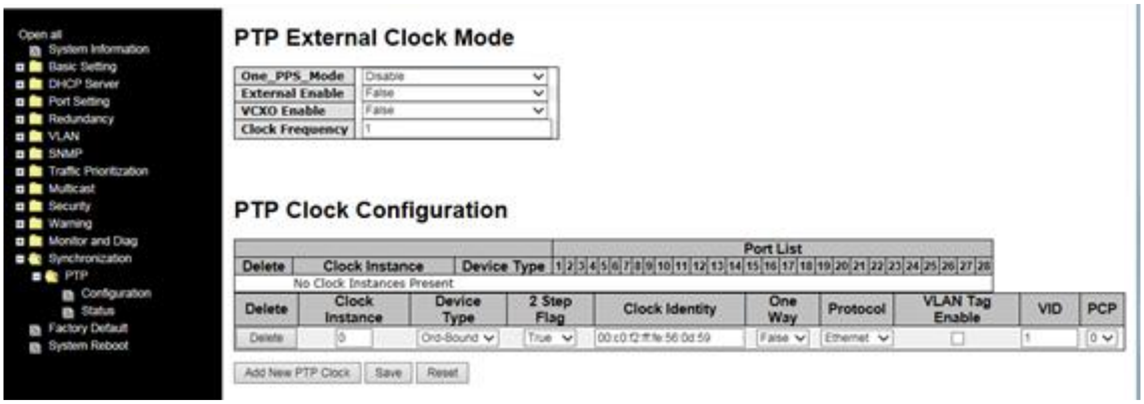
Label	Description
IP Address	The destination IP Address.
Ping Length	The payload size of the ICMP packet. Values range from 2 - 1452 bytes.
Ping Count	Number of PINGs to execute. Values range from 1 to 60.
Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.
Egress Interface	The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet uses. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not given, IPv6 Ping finds the best match interface for destination.

	Do not specify egress interface for loopback address. Do specify egress interface for link-local or multicast address.

5.11 Synchronization

PTP Configuration

This page lets you configure and inspect the current PTP clock settings. This feature is available on the Layer 3 Chassis only.



PTP External Clock Mode

One_PPS_Mode	Disable
External Enable	False
VCXO Enable	False
Clock Frequency	1

PTP Clock Configuration

			Port List																											
Delete	Clock Instance	Device Type	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
	No Clock Instances Present																													

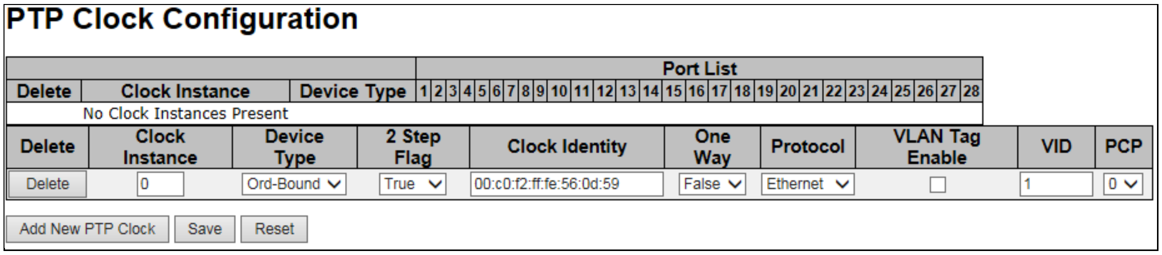
Delete	Clock Instance	Device Type	2 Step Flag	Clock Identity	One Way	Protocol	VLAN Tag Enable	VID	PCP
Delete	0	Ord-Bound	True	00:c0:f2:ff:fe:56:0d:59	False	Ethernet	□	1	0

PTP External Clock Mode

This table lets you configure and examine current PTP clock settings.

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

PTP Clock Configuration



PTP Clock Configuration

Delete	Clock Instance	Device Type	Port List																											
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
	No Clock Instances Present																													

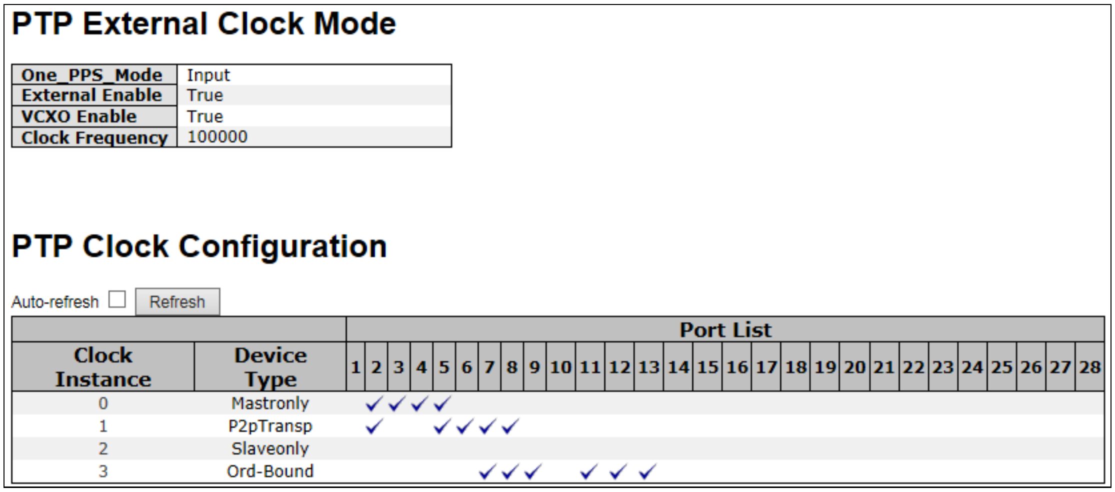
Delete	Clock Instance	Device Type	2 Step Flag	Clock Identity	One Way	Protocol	VLAN Tag Enable	VID	PCP
Delete	0	Ord-Bound	True	00:c0:f2:ff:fe:56:0d:59	False	Ethernet	☐	1	0

Label	Description
Delete	Check this box and click **Save** to delete the clock instance
Clock Instance	Indicates the instance of a particular clock instance (**0**-**3**). Click on the clock instance number to edit the clock details.
Device Type	Indicates the type of the clock instance. The five device types are: **Ord-Bound**: ordinary/boundary clock. **P2p Transp**: peer-to-peer transparent clock. **E2e Transp**: end-to-end transparent clock. **Master Only**: master only. **Slave Only**: slave only.
Port List	Set check mark for each port configured for this Clock Instance.
2 Step Flag	Static member defined by the system; **true** if two-step Sync events and Pdelay_Resp events are used.
Clock Identity	Shows a unique clock identifier.
One Way	If **true**, one-way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.
Protocol	The Transport protocol used by the PTP protocol engine: **Ethernet** PTP over Ethernet multicast. **IP4Multi** PTP over IPv4 multicast. **IP4UNI** PTP over IPv4 unicast. **Note**: IPv4 unicast protocol only works in Master Only and Slave Only clocks. For more information, please refer to **Device Type**. In a unicast Slave Only clock, you must also configure which master clocks to request Announce and Sync messages from. Refer to "Unicast Slave Configuration".

VLAN Tag Enable	Enables VLAN tagging for PTP frames. **Note**: Packets are only tagged if the port is configured for vlan tagging (i.e., Port Type = Unaware and Port VLAN Mode = None, and the port is a member of the VLAN).
VID	VLAN identifiers used for tagging the PTP frames.
PCP	Priority code point values used for PTP frames.

PTP Status

This page lets you monitor (view) the current PTP clock settings.



PTP External Clock Mode

One_PPS_Mode	Input
External Enable	True
VCXO Enable	True
Clock Frequency	100000

PTP Clock Configuration

Auto-refresh ☐ Refresh

		Port List																											
Clock Instance	**Device Type**	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
0	Mastronly		✓	✓	✓	✓																							
1	P2pTransp		✓			✓	✓	✓	✓																				
2	Slaveonly																												
3	Ord-Bound							✓	✓	✓		✓	✓	✓															

PTP External Clock Parameters

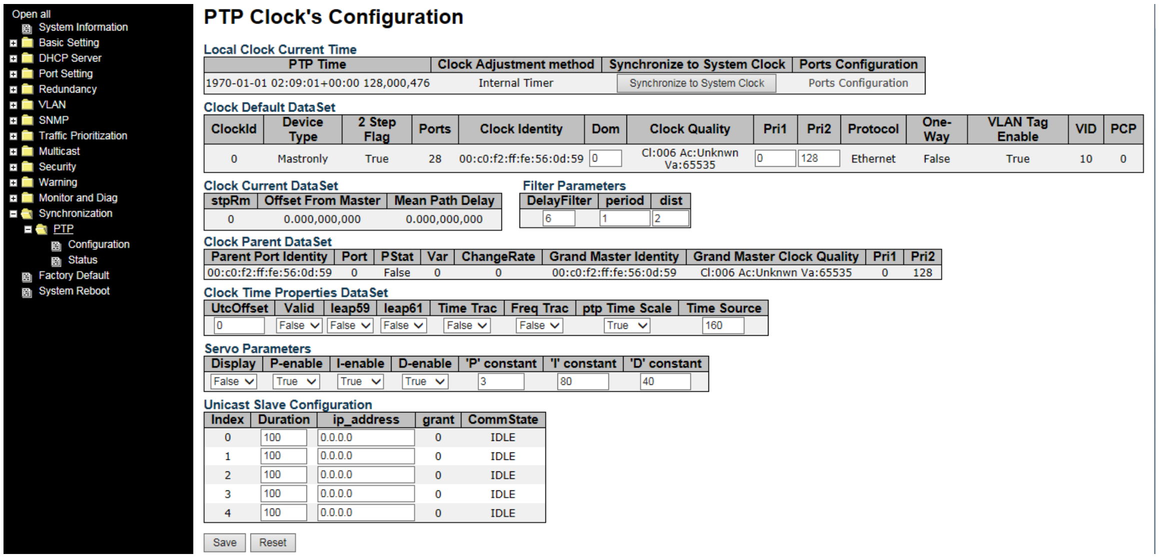
Label	Description
One_pps_mode	The box displays One_pps_mode configurations. The values are: **Output**: enable the 1 pps clock output. **Input**: enable the 1 pps clock input. **Disable**: disable the 1 pps clock in/out-put.
External Enable	The box displays the external clock output. These values are possible: **True**: enable external clock output. **False**: disable external clock output.
VCXO_Enable	The box displays the external VCXO rate. The values are: **True**: enable external VCXO rate adjustment. **False**: disable external VCXO rate adjustment.
Clock Frequency	Displays the current clock frequency of 1 – 25000000 Hz (1 - 25MHz).

PTP Clock Configuration Parameters

Label	Description
Clock Instance	Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to monitor the Clock details.
Device Type	Indicates the Type of the Clock Instance. There are five Device Types. **Ord-Bound** - Clock's Device Type is Ordinary-Boundary Clock. **P2p Transp** - Clock's Device Type is Peer to Peer Transparent Clock. **E2e Transp** - Clock's Device Type is End to End Transparent Clock. **Master Only** - Clock's Device Type is Master Only. **Slave Only** - Clock's Device Type is Slave Only.
Port List	Shows the ports configured for that Clock Instance.

PTP Clock's Configuration

Click on a linked Clock Instance (0-3) to display its PTP Clock's Configuration:



PTP Clock's Configuration

Local Clock Current Time

PTP Time	Clock Adjustment method	Synchronize to System Clock	Ports Configuration
1970-01-01 02:09:01+00:00 128,000,476	Internal Timer	Synchronize to System Clock	Ports Configuration

Clock Default DataSet

ClockId	Device Type	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality	Pri1	Pri2	Protocol	One-Way	VLAN Tag Enable	VID	PCP
0	Mastronly	True	28	00:c0:f2:ff:fe:56:0d:59	0	Cl:006 Ac:Unknwn Va:65535	0	128	Ethernet	False	True	10	0

Clock Current DataSet

stpRm	Offset From Master	Mean Path Delay
0	0.000,000,000	0.000,000,000

Filter Parameters

DelayFilter	period	dist
6	1	2

Clock Parent DataSet

Parent Port Identity	Port	PStat	Var	ChangeRate	Grand Master Identity	Grand Master Clock Quality	Pri1	Pri2
00:c0:f2:ff:fe:56:0d:59	0	False	0	0	00:c0:f2:ff:fe:56:0d:59	Cl:006 Ac:Unknwn Va:65535	0	128

Clock Time Properties DataSet

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	ptp Time Scale	Time Source
0	False	False	False	False	False	True	160

Servo Parameters

Display	P-enable	I-enable	D-enable	'P' constant	'I' constant	'D' constant
False	True	True	True	3	80	40

Unicast Slave Configuration

Index	Duration	ip_address	grant	CommState
0	100	0.0.0.0	0	IDLE
1	100	0.0.0.0	0	IDLE
2	100	0.0.0.0	0	IDLE
3	100	0.0.0.0	0	IDLE
4	100	0.0.0.0	0	IDLE

Here you can view (monitor) and configure the current PTP clock settings:

Label	Description
Local Clock Current Time	Show/update local clock data.
PTP Time	Shows the actual PTP time with nanosecond resolution.
Clock Adjustment	Shows the actual clock adjustment method. The method depends on the available hardware.

Method	
Synchronize to System Clock	Click this button to synchronize the System Clock to PTP Time.
Ports Configuration	Click to edit the port data set for the ports assigned to this clock instance.
Clock Default Dataset	The clock default data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members defined at clock creation time, the Dynamic members defined by the system, and the configurable members which can be set here.
ClockId	An existing internal Clock instance ID (0-3).
Device Type	Indicates the Type of the Clock Instance. There are five Device Types. **1**. Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock. **2**. P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock. **3**. E2e Transp - Clock's Device Type is End to End Transparent Clock. **4**. Master Only - Clock's Device Type is Master Only. **5**. Slave Only - Clock's Device Type is Slave Only.
2 Step Flag	Static member: defined by the system, true if two-step Sync events and Pdelay_Resp events are used.
Ports	The total number of physical ports in the node.
Clock Identity	Shows the unique clock identifier.
Dom	Clock domain [0..127].
Clock Quality	The clock quality is determined by the system, and holds 3 parts: Clock Class, Clock Accuracy and OffsetScaledLog Variance as defined in IEEE1588.The Clock Accuracy values are defined in IEEE1588 table 6 (Currently the clock Accuracy is set to 'Unknown' as default).
Pri1	Clock priority 1 [0..255] used by the BMC master select algorithm..
Pri2	Clock priority 2 [0..255] used by the BMC master select algorithm..
Protocol	Transport protocol used by the PTP protocol engine Ethernet PTP over Ethernet multicast ip4multi PTP over IPv4 multicast ip4uni PTP over IPv4 unicast
One-Way	If **true**, one way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

VLAN Tag Enable	Enables the VLAN tagging for the PTP frames.
VID	VLAN Identifier used for tagging the VLAN packets.
PCP	Priority Code Point value used for PTP frames.
Clock current Data Set	The clock current data set is defined in the IEEE 1588 Standard. The current data set is dynamic.
stpRm	Steps Removed : It is the number of PTP clocks traversed from the grandmaster to the local slave clock.
Offset from master	Time difference between the master clock and the local slave clock, measured in ns.
mean Path Delay	The mean propagation time for the link between the master and the local slave.
Clock Parent Data Set	The clock parent data set is defined in the IEEE 1588 standard. The parent data set is dynamic.
Parent Port Identity	Clock identity for the parent clock, if the local clock is not a slave, the value is the clock’s own ID.
Port	Port Id for the parent master port.
PStat	Parents Stats (always false).
Var	It is observed parent offset scaled log variance.
Change Rate	Observed Parent Clock Phase Change Rate. i.e. the slave clocks rate offset compared to the master. (unit = ns per s).
Grand Master Identity	Clock identity for the grand master clock, if the local clock is not a slave, the value is the clock’s own ID.
Grand Master Clock Quality	The clock quality announced by the grand master (See description of Clock Default DataSet :Clock Quality).
Pri1	Clock priority 1 announced by the grand master,
Pri2	Clock priority 2 announced by the grand master.
Clock Time Properties Data Set	The clock time properties data set is defined in the IEEE 1588 Standard. The data set is both configurable and dynamic, i.e. the parameters can be configured for a grandmaster. In a slave clock the parameters are overwritten by the grandmasters timing properties. The parameters are not used in the current PTP implementation. The valid Time Source values are: **16** (0x10) ATOMIC_CLOCK **32** (0x20) GPS

	48 (0x30) TERRESTRIAL_RADIO **64** (0x40) PTP **80** (0x50) NTP **96** (0x60) HAND_SET **144** (0x90) OTHER **160** (0xA0) INTERNAL_OSCILLATOR
Servo Parameters	The default clock servo uses a PID regulator to calculate the current clock rate. i.e. *clockAdjustment = OffsetFromMaster/ P constant +* *Integral(OffsetFromMaster)/ I constant +* *Differential OffsetFromMaster)/ D constant*
Display	If true then Offset From Master, MeanPathDelay and clockAdjustment are logged on the debug terminal.
P-enable	If true the P part of the algorithm is included.
I-Enable	If true the I part of the algorithm is included.
D-enable	If true the D part of the algorithm is included.
'P' constant	[1..1000] see above
'I' constant	[1..10000] see above
'D' constant	[1..10000] see above
Filter Parameters	The default delay filter is a low pass filter, with a time constant of **2****DelayFilter*DelayRequestRate**.The default offset filter uses a minimum delay filter method i.e. The minimum measured offset during Period samples is used in the calculation. The distance between two calculations is Dist periods. **Note**: In configurations with Timestamp enabled PHYs, the period is automatically increased, if (*period*dist* < *SyncPackets pr sec/4*), i.e. maximum of 4 adjustments are made per second. If **Dist** is 1 the offset is averaged over the Period; If **Dist** is >1 the offset is calculated using 'min' offset.
DelayFilter	See above.
Period	See above.
dist	See above.
Unicast Slave Configuration	When operating in IPv4 Unicast mode, the slave is configured up to 5 master IP addresses. The slave then requests Announce messages from all the configured masters. The slave uses the BMC algorithm to select one as

	master clock, the slave then request Sync messages from the selected master.
Duration	The number of seconds a master is requested to send Announce/Sync messages. The request is repeated from the slave each Duration/4 seconds.
ip_address	The IPv4 Address of the Master clock.
Grant	The granted repetition period for the sync message.
CommState	The state of the communication with the master, possible values are: **IDLE** : The entry is not in use. **INIT** : Announce is sent to the master (Waiting for a response). **CONN** : The master has responded. **SELL** : The assigned master is selected as current master. **SYNC** : The master is sending Sync messages.

PTP Configuration Example

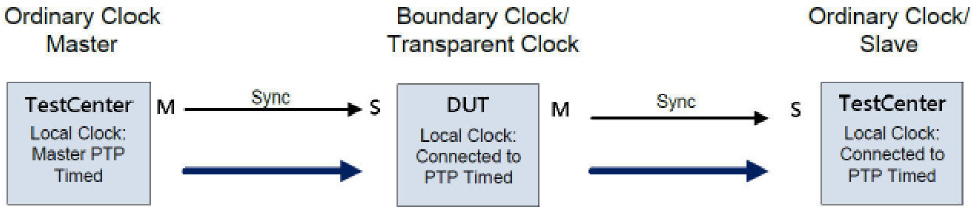
This example describes how to configure the switch as an Ordinary “master” clock and ordinary “slave” clock.

IEEE 1588v2 is a packet based timing protocol. Ethernet packets are sent with timestamps, and the received packets have the timestamps read so the timing (and thus frequency) can be derived. Network timing is hierarchical in nature, such that there is one master that transmits to a large (or infinite) number of slaves. The master source clock can be an SISGM switch, or it can be another device. If it is another device the SISGM switch has two methods to get the master clock timing. If it is another device, it can get the master timing input from either a packet or a 1 pulse per second hardware input pin (1PPS).

If the switch is to give timing information to other devices, the switch can provide it as a packet, or as an output hardware pin as a 1PPS.

The initial release of the SISGM switch does not have the input/output pins available for the 1PPS use for external devices, either master clocks or handoff to slave’s device. However, the 1588v2 for packet is still available to be used, and is fully functional.

Typically, the SISGM switch is a used as a device that passes through the packets and adjusts the timestamps per the protocol. As such the I/O 1PPS pins would not be used for these environments.



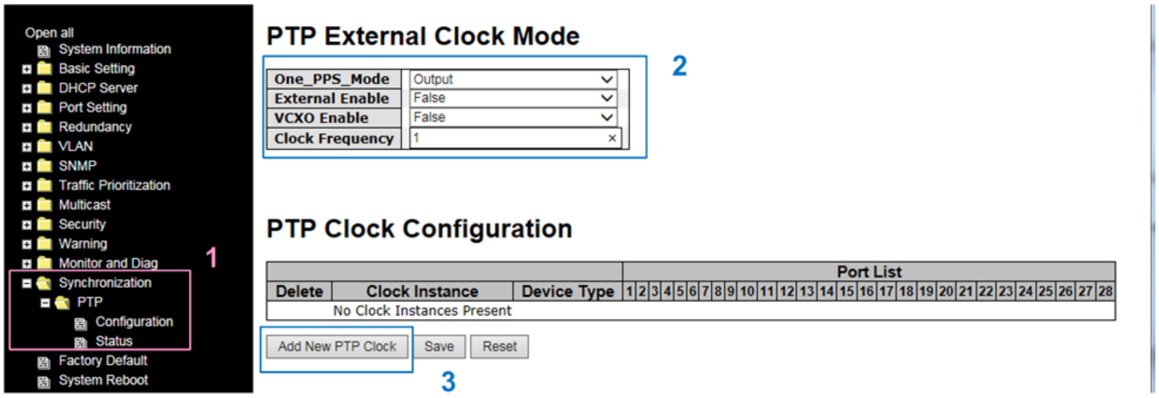
I. System Configuration:

Step 1:

a) Select PTP in the configuration menu and set (1) PPS mode to “output”.

b) Generate 1 PPS (one pulse per second) to measure the 1588 time.

c) First, a PTP Clock instance must be created. Select PTP in the Configuration menu and click the “**Add New PTP Clock**” button.



PTP External Clock Mode

One_PPS_Mode	Output
External Enable	False
VCXO Enable	False
Clock Frequency	1

PTP Clock Configuration

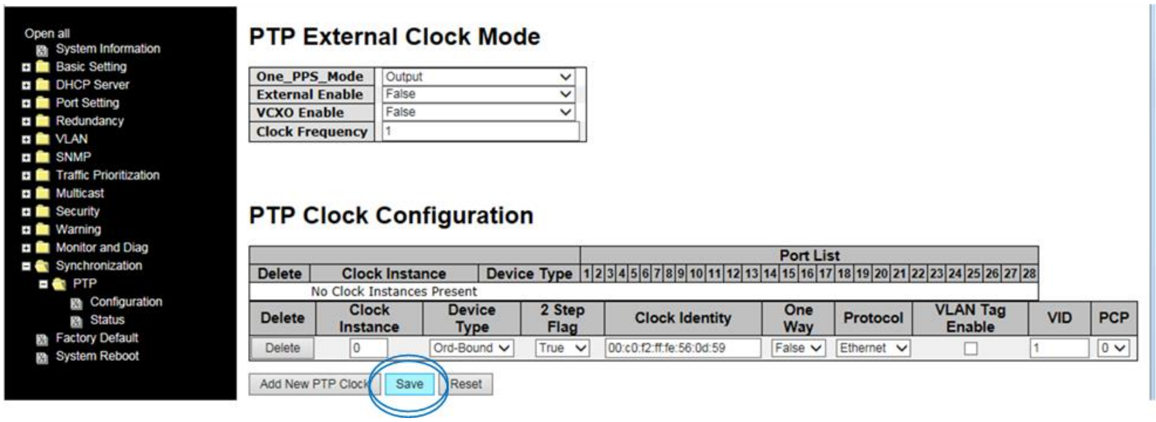
			Port List																											
Delete	Clock Instance	Device Type	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
No Clock Instances Present																														

Step 2:

a) Configure the clock as:

- Device type = Ord-Bound.
- 2 Step Flag = True or False (for single step mode).
- One way = false (for both Sync and delay messages).

b) Click the “**Save**” button to create the clock instance.



PTP External Clock Mode

One_PPS_Mode	Output
External Enable	False
VCXO Enable	False
Clock Frequency	1

PTP Clock Configuration

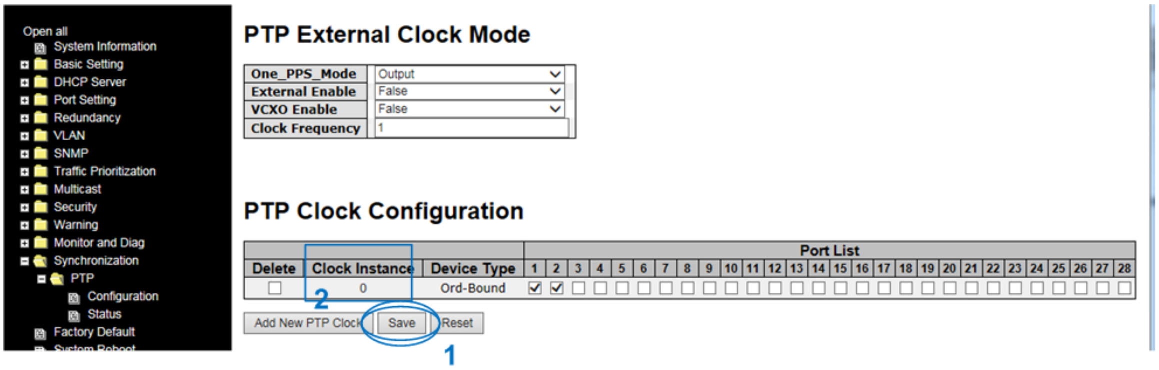
			Port List																											
Delete	**Clock Instance**	**Device Type**	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
No Clock Instances Present																														

Delete	Clock Instance	Device Type	2 Step Flag	Clock Identity	One Way	Protocol	VLAN Tag Enable	VID	PCP
Delete	0	Ord-Bound	True	00:c0:f2:ff:fe:56:0d:59	False	Ethernet	□	1	0

Step 3:

a) Enable/check the port and click the “**Save**” button.

b) Click the linked “0” in the Clock Instance column to display the Clock instance Configuration page.



PTP External Clock Mode

One_PPS_Mode	Output
External Enable	False
VCXO Enable	False
Clock Frequency	1

PTP Clock Configuration

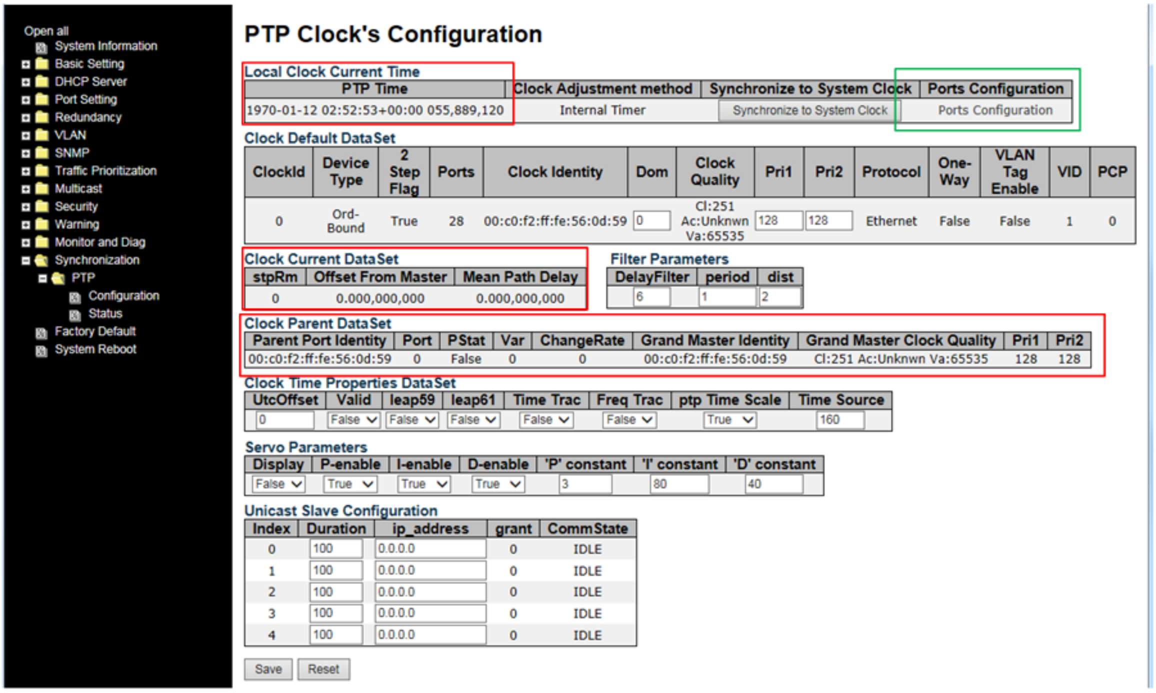
			Port List																											
Delete	**Clock Instance**	**Device Type**	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
□	0	Ord-Bound	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Step 4:

a) Configure Clock parameters. **Note**: Only parameters different from default are listed below:

- Clock Default Dataset:Prio1 = 128 (If want the node the “Master”, set it to 100 or small).
- Servo parameters: P = 3, I=80.
- The local Clock Current Time show the default switch Time.(not get the PTP time).

b) Click the “Save” button then click the linked “Port Configuration” to enter port-specific parameters.



PTP Clock's Configuration

Local Clock Current Time

PTP Time	Clock Adjustment method	Synchronize to System Clock	Ports Configuration
1970-01-12 02:52:53+00:00 055,889,120	Internal Timer	Synchronize to System Clock	Ports Configuration

Clock Default DataSet

ClockId	Device Type	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality	Pri1	Pri2	Protocol	One-Way	VLAN Tag Enable	VID	PCP
0	Ord-Bound	True	28	00:c0:f2:ff:fe:56:0d:59	0	Cl:251 Ac:Unknwn Va:65535	128	128	Ethernet	False	False	1	0

Clock Current DataSet

stpRm	Offset From Master	Mean Path Delay
0	0.000,000,000	0.000,000,000

Filter Parameters

DelayFilter	period	dist
6	1	2

Clock Parent DataSet

Parent Port Identity	Port	PStat	Var	ChangeRate	Grand Master Identity	Grand Master Clock Quality	Pri1	Pri2
00:c0:f2:ff:fe:56:0d:59	0	False	0	0	00:c0:f2:ff:fe:56:0d:59	Cl:251 Ac:Unknwn Va:65535	128	128

Clock Time Properties DataSet

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	ptp Time Scale	Time Source
0	False	False	False	False	False	True	160

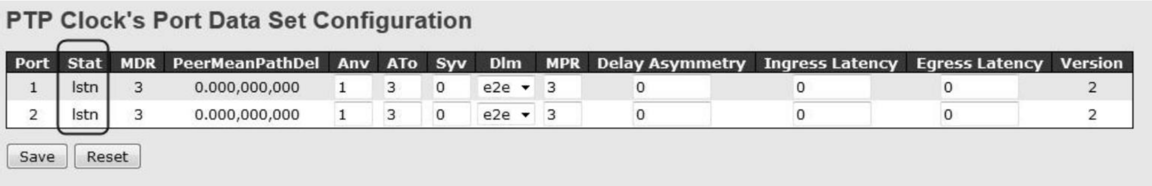
Servo Parameters

Display	P-enable	I-enable	D-enable	'P' constant	'I' constant	'D' constant
False	True	True	True	3	80	40

Unicast Slave Configuration

Index	Duration	ip_address	grant	CommState
0	100	0.0.0.0	0	IDLE
1	100	0.0.0.0	0	IDLE
2	100	0.0.0.0	0	IDLE
3	100	0.0.0.0	0	IDLE
4	100	0.0.0.0	0	IDLE

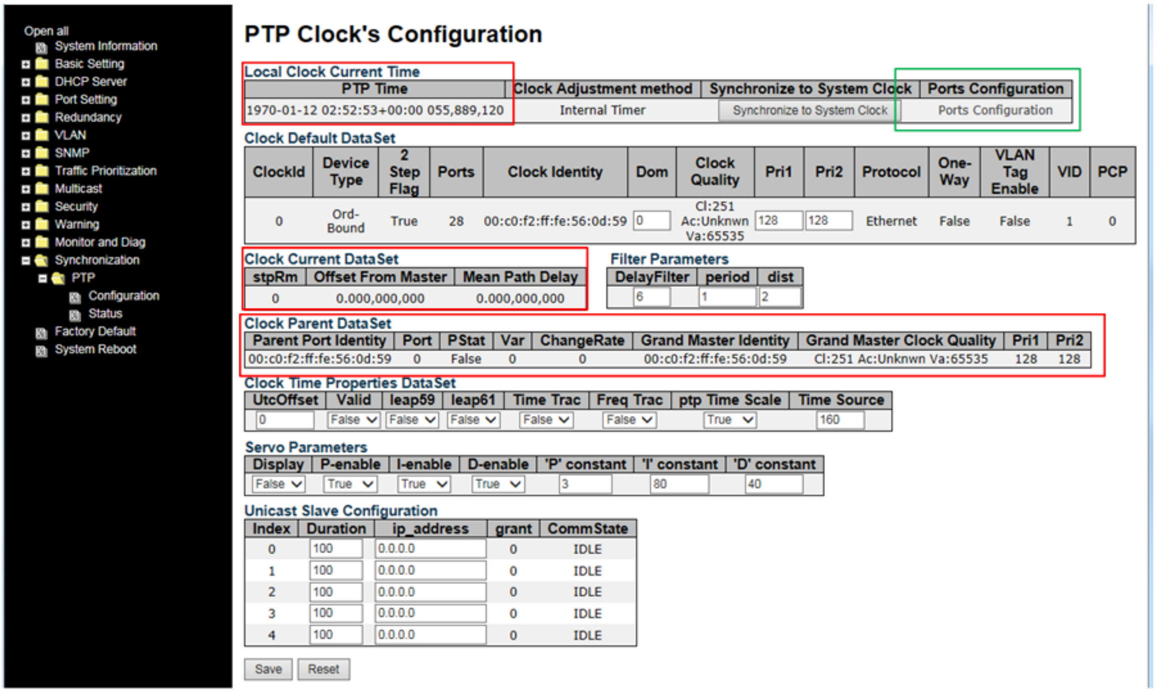
Step 5: Check the ports “Stat=lstn” (Status=listening) before get the PTP time.



PTP Clock's Port Data Set Configuration

Port	Stat	MDR	PeerMeanPathDel	Anv	ATo	Syv	Dlm	MPR	Delay Asymmetry	Ingress Latency	Egress Latency	Version
1	lstn	3	0.000,000,000	1	3	0	e2e	3	0	0	0	2
2	lstn	3	0.000,000,000	1	3	0	e2e	3	0	0	0	2

II. Resulting Configuration:



PTP Clock's Configuration

Local Clock Current Time

PTP Time	Clock Adjustment method	Synchronize to System Clock	Ports Configuration
1970-01-12 02:52:53+00:00 055,889,120	Internal Timer	Synchronize to System Clock	Ports Configuration

Clock Default DataSet

ClockId	Device Type	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality	Pri1	Pri2	Protocol	One-Way	VLAN Tag Enable	VID	PCP
0	Ord-Bound	True	28	00:c0:f2:ff:fe:56:0d:59	0	Cl:251 Ac:Unknwn Va:65535	128	128	Ethernet	False	False	1	0

Clock Current DataSet

stpRm	Offset From Master	Mean Path Delay
0	0.000,000,000	0.000,000,000

Filter Parameters

DelayFilter	period	dist
6	1	2

Clock Parent DataSet

Parent Port Identity	Port	PStat	Var	ChangeRate	Grand Master Identity	Grand Master Clock Quality	Pri1	Pri2
00:c0:f2:ff:fe:56:0d:59	0	False	0	0	00:c0:f2:ff:fe:56:0d:59	Cl:251 Ac:Unknwn Va:65535	128	128

Clock Time Properties DataSet

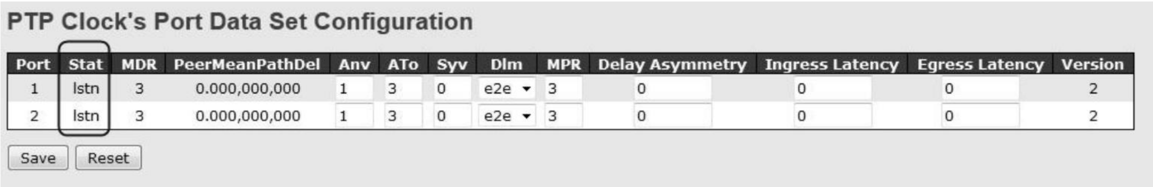
UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	ptp Time Scale	Time Source
0	False	False	False	False	False	True	160

Servo Parameters

Display	P-enable	I-enable	D-enable	'P' constant	'I' constant	'D' constant
False	True	True	True	3	80	40

Unicast Slave Configuration

Index	Duration	ip_address	grant	CommState
0	100	0.0.0.0	0	IDLE
1	100	0.0.0.0	0	IDLE
2	100	0.0.0.0	0	IDLE
3	100	0.0.0.0	0	IDLE
4	100	0.0.0.0	0	IDLE



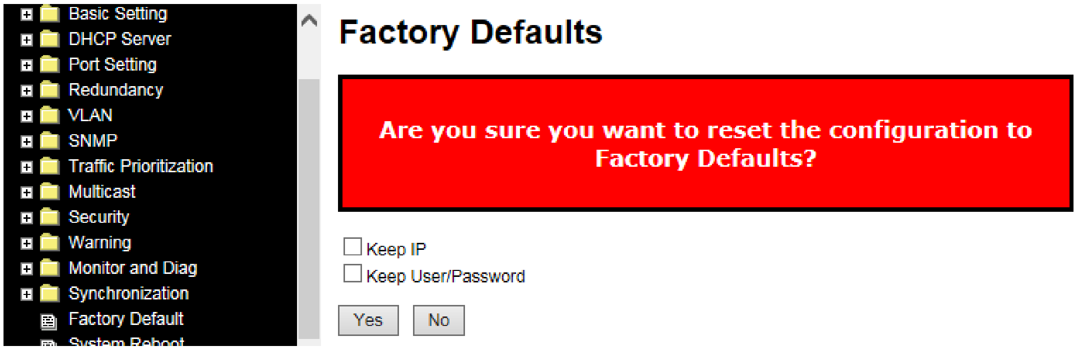
PTP Clock's Port Data Set Configuration

Port	Stat	MDR	PeerMeanPathDel	Anv	ATo	Syv	Dlm	MPR	Delay Asymmetry	Ingress Latency	Egress Latency	Version
1	lstn	3	0.000,000,000	1	3	0	e2e	3	0	0	0	2
2	lstn	3	0.000,000,000	1	3	0	e2e	3	0	0	0	2

5.12 Troubleshooting

5.12.1 Factory Defaults

You can reset the configuration of the switch on this page. Only the IP configuration is retained. The new configuration is available immediately (no restart is necessary). **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



Factory Defaults

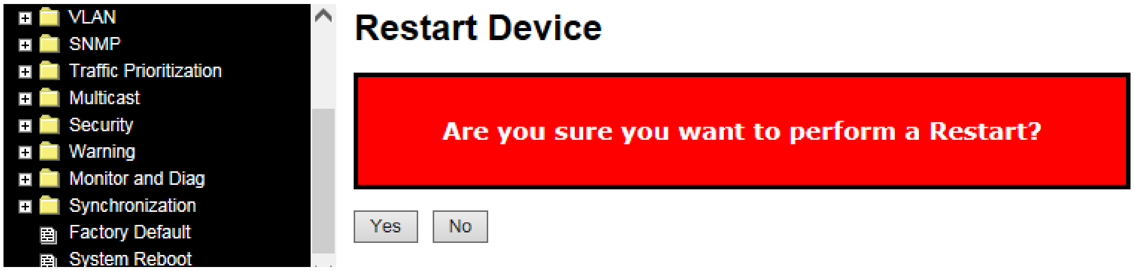
Are you sure you want to reset the configuration to Factory Defaults?

□ Keep IP
□ Keep User/Password

Label	Description
Keep IP	Check to reset to defaults and keep the current IP address.
Keep User/Password	Check to reset to defaults and keep the current User name and Password.
Yes	Click to reset the configuration to factory defaults.
No	Click to return to the Port State page without resetting.

5.12.2 System Reboot (Restart Device)

You can restart the switch on this page. After restart, the switch will boot normally.



Restart Device

Are you sure you want to perform a Restart?

Label	Description
Yes	Click to restart the device.
No	Click to return to the **Port State** page without restarting.

6. Command Line Interface (CLI)

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

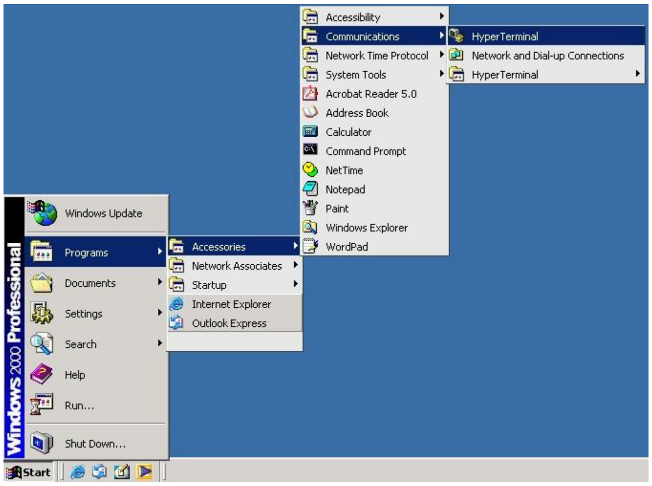
CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

Before configuring RS-232 serial console, connect the RS-232 port of the switch to your PC Com port using a RJ45 to DB9-F cable. See RS-232 Console Port Wiring on page 28.

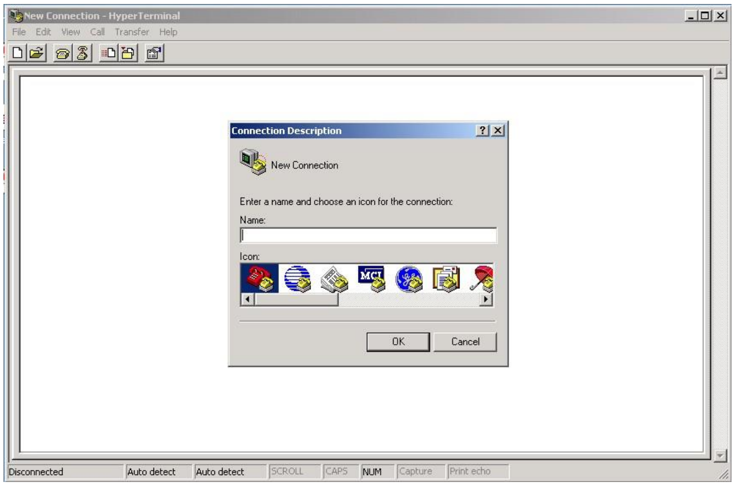
Access the CLI

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

Step 1: On Windows desktop, click Start -> Programs -> Accessories -> Communications -> HyperTerminal.

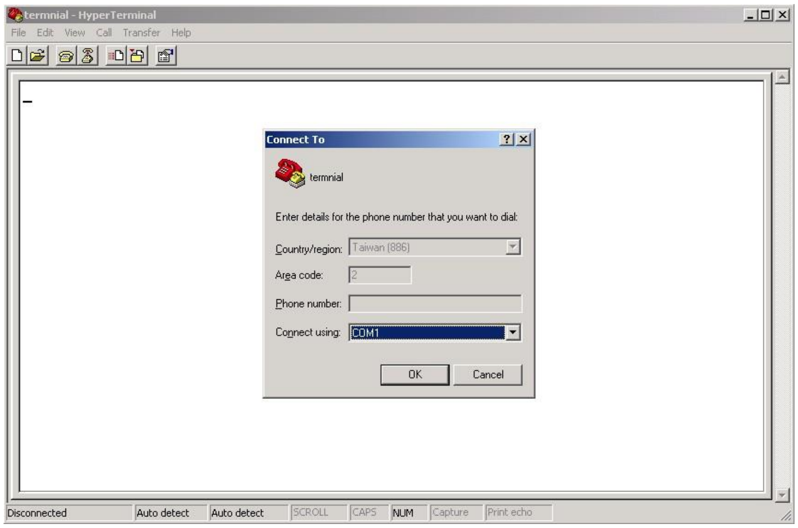


Step 2: Input a name for the new connection.



Enter a name and choose an icon for the connection:

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



termnial - HyperTerminal

Connect To

termnial

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

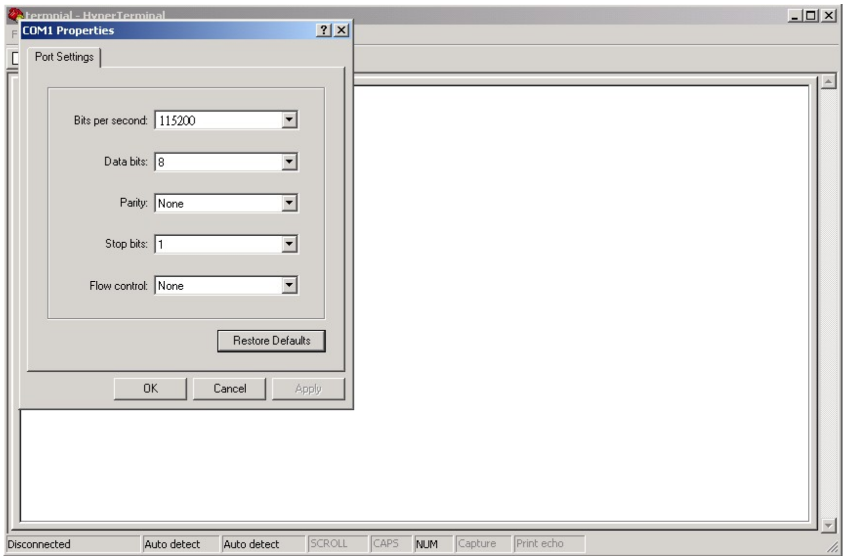
Country/region: Taiwan (886)

Area code: 2

Phone number:

Connect using: COM1

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



termnial - HyperTerminal

COM1 Properties

Port Settings

Bits per second: 115200

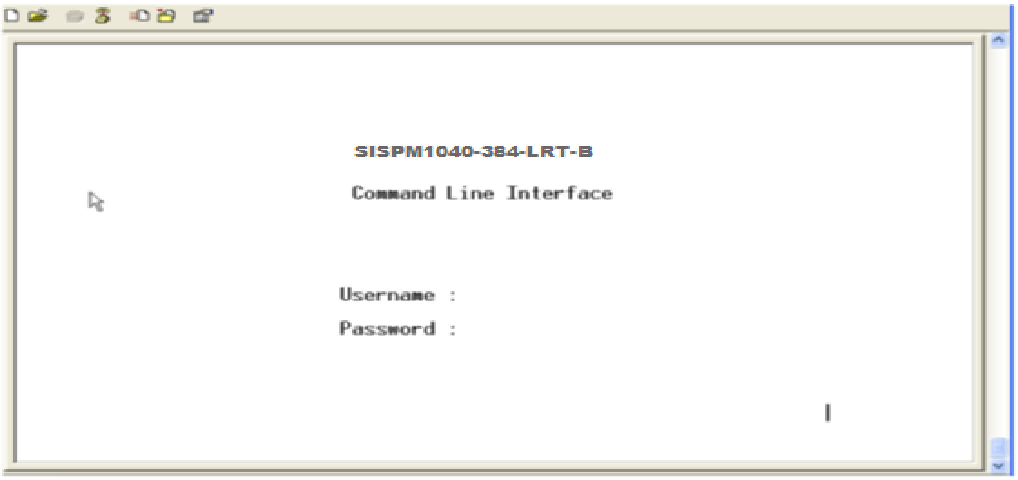
Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

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



```
SISPM1040-384-LRT-B
Command Line Interface

Username :
Password :
```

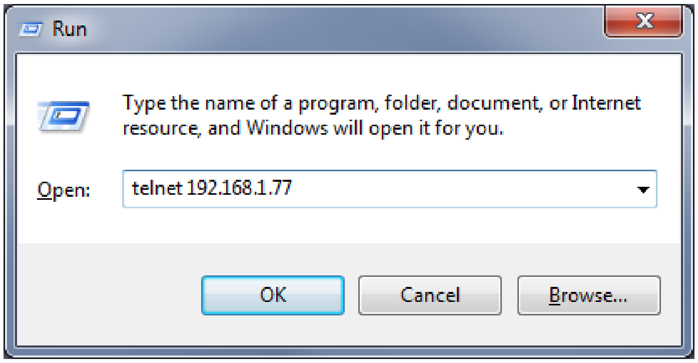
CLI Management via Telnet

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

IP Address:	**192.168.1.77**
Subnet Mask:	**255.255.255.0**
Default Gateway:	**192.168.1.254**
User Name:	**root**
Password:	**root**

Follow the steps below to access console via Telnet.

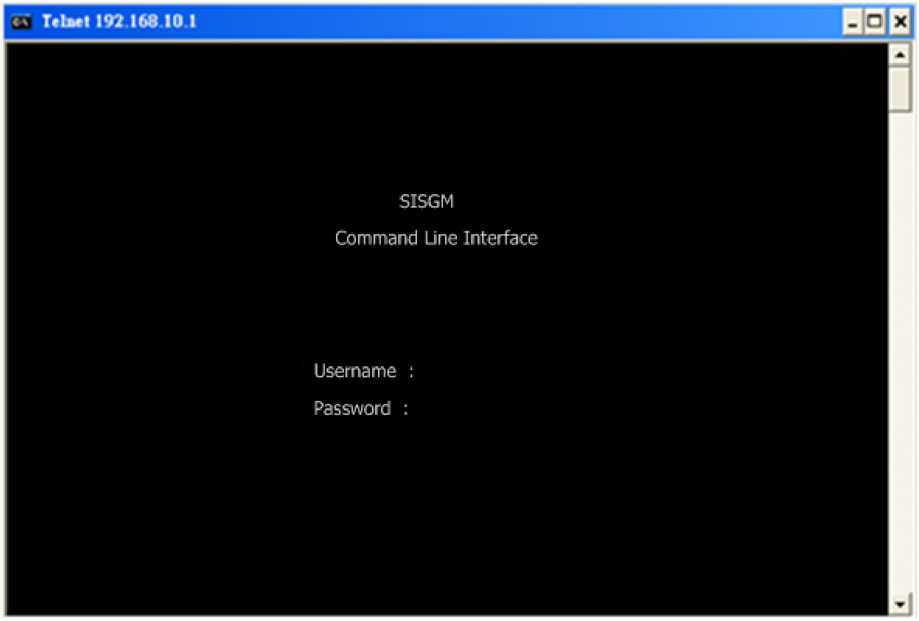
Step 1: Telnet to the IP address of the switch from the **Run** window by entering commands (or from the MS-DOS prompt) as below.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: telnet 192.168.1.77

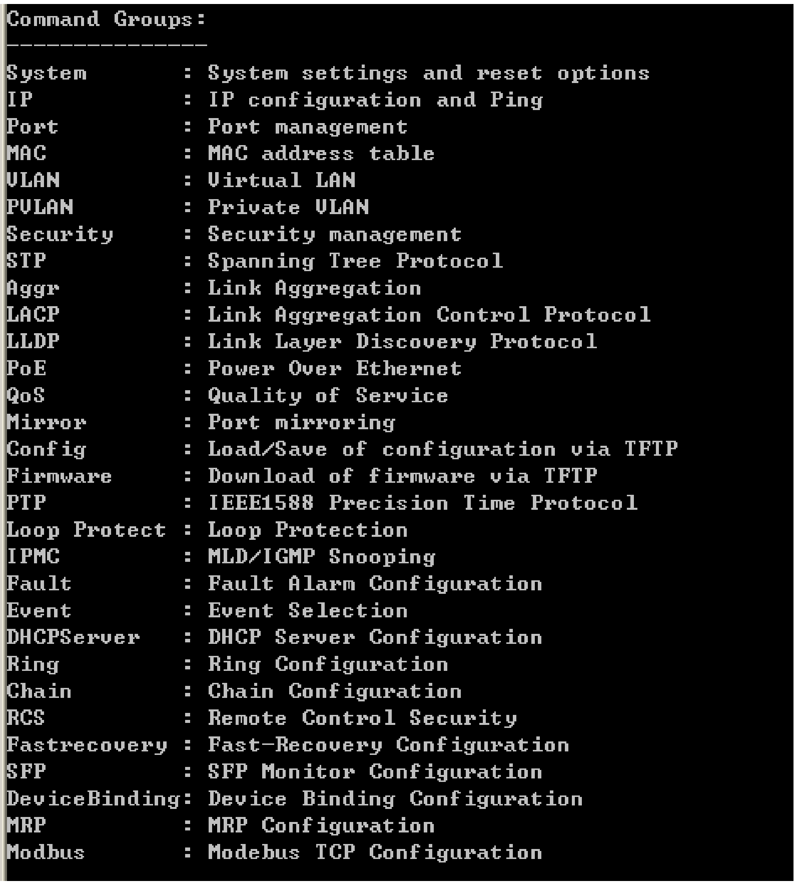
Step 2: The Login screen will appear. Use the keyboard to enter the Username and Password (same as the password for Web browser), and then press **Enter.**



```
SISGM
Command Line Interface


Username  :
Password  :
```

Command Groups



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

System Commands

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

IP Commands

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

Port Commands

port>	Configuration [<port_list>] [up|down]
	Mode [<port_list>] [auto|10hdx|10fdx|100hdx|100fdx|1000fdx|sfp_auto_ams]
	Flow Control [<port_list>] [enable|disable]
	State [<port_list>] [enable|disable]
	MaxFrame [<port_list>] [<max_frame>]
	Power [<port_list>] [enable|disable|actiphy|dynamic]
	Excessive [<port_list>] [discard|restart]
	Statistics [<port_list>] [<command>] [up|down]
	VeriPHY [<port_list>]
	SFP [<port_list>]

MAC Commands

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

VLAN Commands

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

Private VLAN Commands

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

Security Commands

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

Security Switch Commands

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

Security Switch Authentication Commands

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

Security Switch SSH Commands

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

Security Switch HTTPS Commands

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

Security Switch RMON Commands

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

Security Network Commands

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

Security Network Psec Commands

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

Security Network NAS Commands

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

Security Network ACL Commands

Security/Network/ACL>	Configuration [<port_list>]
	Action [<port_list>] [permit|deny] [<rate_limiter>][<port_redirect>] [<mirror>] [<logging>] [<shutdown>]
	Policy [<port_list>] [<policy>]
	Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]
	Add [<ace_id>] [<ace_id_next>][(port <port_list>)] [(policy <policy> <policy_bitmask>)][<tagged>] [<vid>] [<tag_prio>] [<dmac_type>][(etype [<etype>] [<smac>] [<dmac>]) | (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) |

	(ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) | (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) | (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])] [permit|deny] [<rate_limiter>] [<port_redirect>] [<mirror>] [<logging>][<shutdown>]
	Delete <ace_id>
	Lookup [<ace_id>]
	Clear
	Status [combined|static|loop_protect|dhcp|ptp|ipmc|conflicts]
	Port State [<port_list>] [enable|disable]

Security Network DHCP Commands

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

Security Network AAA Commands

Security/Network/AAA>	Configuration
	Timeout [<timeout>]
	Deadtime [<dead_time>]
	RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
	ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
	Statistics [<server_index>]

STP Commands

STP>	Configuration
	Version [<stp_version>] Non-certified release, v
	Txhold [<holdcount>]lt 15:15:15, Dec 6 2007
	MaxAge [<max_age>]
	FwdDelay [<delay>]
	bpduFilter [enable|disable]
	bpduGuard [enable|disable]
	recovery [<timeout>]
	CName [<config-name>] [<integer>]
	Status [<msti>] [<port_list>]
	Msti Priority [<msti>] [<priority>]
	Msti Map [<msti>] [clear]
	Msti Add <msti> <vid>
	Port Configuration [<port_list>]
	Port Mode [<port_list>] [enable|disable]
	Port Edge [<port_list>] [enable|disable]
	Port AutoEdge [<port_list>] [enable|disable]
	Port P2P [<port_list>] [enable|disable|auto]
	Port RestrictedRole [<port_list>] [enable|disable]
	Port RestrictedTcn [<port_list>] [enable|disable]
	Port bpduGuard [<port_list>] [enable|disable]
	Port Statistics [<port_list>]
	Port Mcheck [<port_list>]
	Msti Port Configuration [<msti>] [<port_list>]
	Msti Port Cost [<msti>] [<port_list>] [<path_cost>]
	Msti Port Priority [<msti>] [<port_list>] [<priority>]

Aggregation Commands

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

LACP Commands

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

LLDP Commands

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

QoS Commands

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

Mirror Commands

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

Dot1x Commands

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

IGMP Commands

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

ACL Commands

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

Mirror Commands

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

Config Commands

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

Firmware Commands

Firmware>	Load <ip_addr_string> <file_name>

SNMP Commands

SNMP>	Trap Inform Retry Times [<retries>]
	Trap Probe Security Engine ID [enable|disable]
	Trap Security Engine ID [<engineid>]
	Trap Security Name [<security_name>]
	Engine ID [<engineid>]
	Community Add <community> [<ip_addr>] [<ip_mask>]
	Community Delete <index>
	Community Lookup [<index>]
	User Add <engineid> <user_name> [MD5|SHA] [<auth_password>] [DES] [<priv_password>]
	User Delete <index>
	User Changekey <engineid> <user_name> <auth_password> [<priv_password>]
	User Lookup [<index>]
	Group Add <security_model> <security_name> <group_name>
	Group Delete <index>
	Group Lookup [<index>]
	View Add <view_name> [included|excluded] <oid_subtree>
	View Delete <index>
	View Lookup [<index>]
	Access Add <group_name> <security_model> <security_level> [<read_view_name>] [<write_view_name>] Access Delete <index>
	Access Lookup [<index>]

PTP Commands

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

	Wireless mode <clockinst> [<port_list>] [enable|disable]
	Wireless pre notification <clockinst> <port_list>
	Wireless delay <clockinst> [<port_list>] [<base_delay>] [<incr_delay>]

Loop Protect Commands

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

IPMC Commands

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

Fault Commands

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

Event Commands

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

DHCPServer Commands

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

Ring Commands

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

Chain Commands

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

RCS Commands

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

Fast Recovery Commands

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

SFP Commands

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

MRP Commands

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

7. Technical Specifications

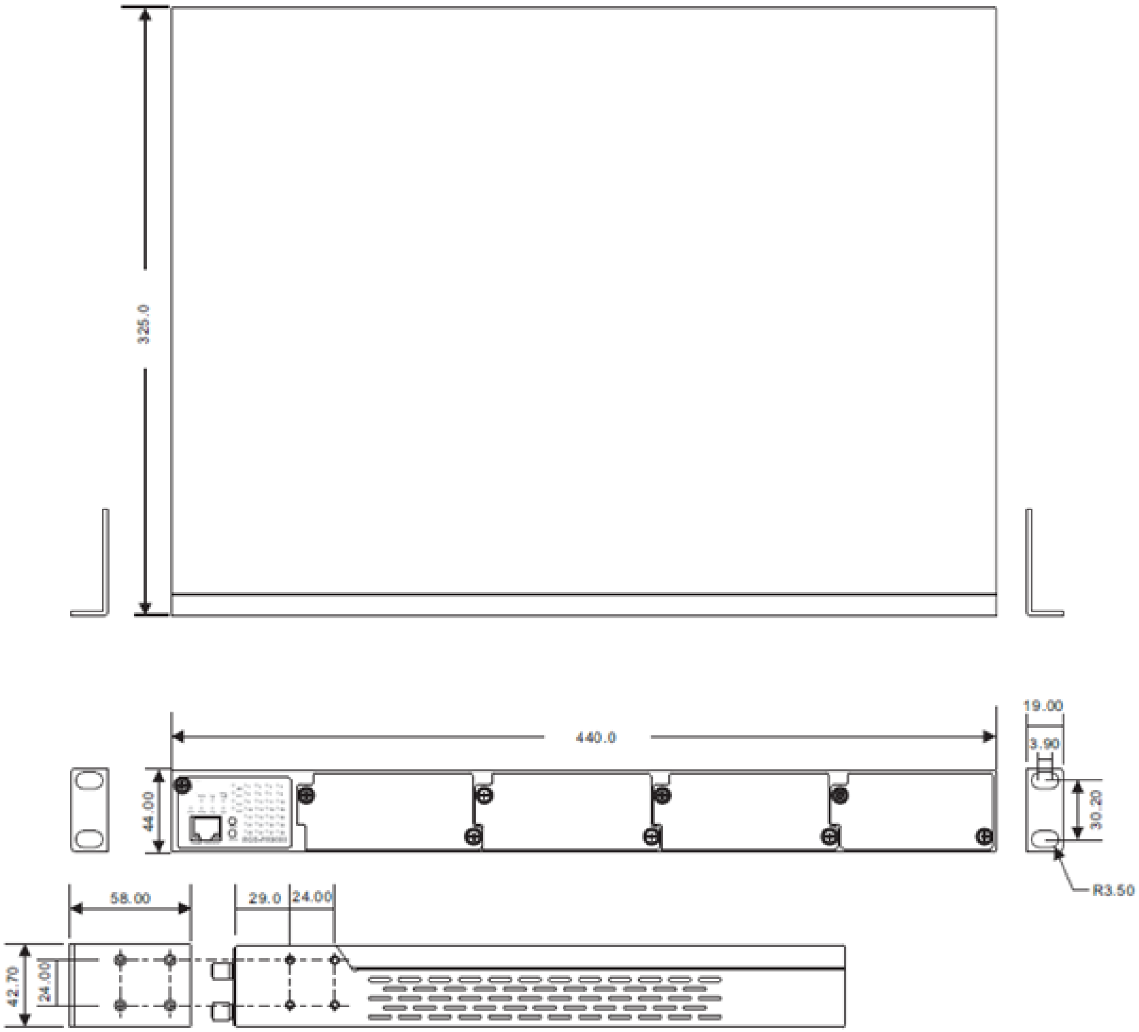
Physical Ports	
Number of bays	**4 (up to 3 bays for 8x1G ports and 1 bay for 4x10G ports)**
Technology	
Ethernet Standards	IEEE 802.3 for 10Base-T IEEE 802.3u for 100Base-TX and 100Base-FX IEEE 802.3ab for 1000Base-T IEEE 802.z for 1000Base-X IEEE 802.3ae for 10Gigabit Ethernet IEEE 802.3x for Flow control IEEE 802.3ad for LACP (Link Aggregation Control Protocol) IEEE 802.1p for COS (Class of Service) IEEE 802.1Q for VLAN Tagging IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol) IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol) IEEE 802.1x for Authentication IEEE 802.1AB for LLDP (Link Layer Discovery Protocol)
MAC Table	8k
Priority Queues	8
Processing	Store-and-Forward
Switch Properties	Switching latency: 7 us Switching bandwidth: 128Gbps Max. Number of Available VLANs: 256 IGMP multicast groups: 128 for each VLAN Port rate limiting: User Defined
Jumbo frame	Up to 10K Bytes
Security Features	Device Binding security feature Enable/disable ports, MAC based port security Port based network access control (802.1x) Single 802.1x and Multiple 802.1x MAC-based authentication QoS assignment Guest VLAN MAC address limit TACACS+ VLAN (802.1Q) to segregate and secure network traffic Radius centralized password management SNMPv3 encrypted authentication and access security

	Https / SSH enhance network security Web and CLI authentication and authorization Authorization (15 levels) IP source guard
Software Features	Hardware routing, RIP and static routing (SISGM Layer 3 only) Hardware IEEE 1588v2 clock synchronization IEEE 802.1D Bridge, auto MAC address learning/aging and MAC address (static) Multiple Registration Protocol (MRP) MSTP (RSTP/STP compatible) Redundant Ring with recovery time less than 30ms over 250 units TOS/Diffserv supported Quality of Service (802.1p) for real-time traffic VLAN (802.1Q) with VLAN tagging IGMP v2/v3 Snooping IP-based bandwidth management Application-based QoS management DOS/DDOS auto prevention Port configuration, status, statistics, monitoring, security DHCP Server/Client DHCP Relay Modbus TCP DNS client proxy SMTP Client
Network Redundancy	Redundant Rings Open-Ring Multiple Ring MRP MSTP (RSTP/STP compatible)
RS-232 Serial Console Port	RS-232 in RJ-45 connector with console cable. 115200bps, 8, N, 1
LED indicators	
System Ready Indicator (PWR)	Green: Indicates that the system ready. The LED is blinking when the system is upgrading firmware
Power Indicator (PWR1 / PWR2)	Green: Power LED x 2
Ring Master Indicator (R.M.)	Green: Indicates that the system is operating in Redundant Rings Master mode
Redundant Rings Indicator (Ring)	Green: Indicates that the system operating in Redundant Rings mode Green Blinking: Indicates that the Ring is broken.
Fault Indicator (Fault)	Amber: Indicate unexpected event occurred
Reset To Default Running Indicator (DEF)	Green: System resets to default configuration

Supervisor Login Indicator (RMT)	Green: System is accessed remotely	
Smart LED Display system	Link/Act(LK/ACT) / Speed(SPD) / Duplex(FDX) / Remote (RMT) green LED indicator x 4 Mode select Button (MODE): Link/Act(LK/ACT) / Speed(SPD) / Duplex(FDX) / Remote (RMT) mode select button Port 1 ~ 28 Link/Act(LK/ACT) LED show: Green x 28	
Fault contact		
Relay	Relay output to carry capacity of 1A at 24VDC	
Power		
Redundant power input modular	Dual 24/48VDC (20~72VDC) power inputs at terminal block	Dual 88~264VAC / 100~370VDC power inputs at terminal block
Power consumption (Typ.)	46 Watts max. (SISGM-LV)	43.5 Watts max. (SISGM-HV)
Overload current protection	Present	
Physical Characteristics		
Enclosure	19 inches rack mountable	
Weight (g)	6450g (SISGM-LV)	6600g (SISGM-HV)
MTBF *	SISGM-4P-10G-SFP: 1882120.6278 hours	SISGM-8P-1G-SFP: MTBF: 3712062.3901 hours
	SISGM-CHAS-L2/L3 Chassis with SISGM-PWR-HVC Power Supply: MTBF: 316958.5417 hours	SISGM-CHAS-L2/L3 Chassis with SISGM-PWR-LVC Power Supply: MTBF: 246537.4576 hours
	SISGM-8P-1G-TX (8 Port, 1Gb, RJ45 Module) : 1303990.4158 hours	**Note *** : All MTBF at Operating Temp: 25° C; Category: Telcordia SR332 Issue 2.
Dimension (W x D x H)	440 (W) x 325 (D) x 44 (H) mm (17.32x12.8x1.73 inches)	
Environmental		
Storage Temperature	-40 to 85°C (-40 to 185°F)	
Operating Temperature	-40 to +40°C (-40 to 104°F)	
Operating Humidity	5% to 95% Non-condensing	
Regulatory approvals		
Power Automation	IEC 61850-3, IEEE 1613 (pending)	
EMI	FCC Part 15, CISPR (EN55022) class A, EN50155 (EN50121-3-2, EN55011, EN50121-4)	
EMS	EN61000-4-2 (ESD); EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11	
Safety	UL Listed I.T.E. E147132	

Warranty	
Chassis and Port Modules	5 Year Limited Warranty

Dimensions



8. Troubleshooting

1. Is one of the Green Power LEDs (**PWR1**, **PWR2**, or **PWR3**) lit?

NO

- Is the power source live and to spec?
- Is the power adapter properly installed?
- Are the power supply modules completely inserted and the thumb screws tight?
- Are the power cables properly installed? See the *SISGM Quick Start Guide* for details.
- Record the model and system information and contact TN Technical Support. Refer to the sections below..

YES

- Proceed to step 2.

2. Check the port LEDs. Is the Green port Link/Act LED or the Amber Link LED lit?

NO

- Verify that the copper and fiber cable requirements are met. See the Connection section on page 26.

YES

- Verify that the feature you are configuring is supported by your particular SISGM-CHAS model; for instance, the SISGM-CHAS-L2 model does not support Static Routing, RIP, Multiple Rings, or PTP features. See the Features section on page 8.
- If you are configuring a feature via the web GUI, try using the CLI, and vice versa.
- Run the device Diagnostics; see MONITOR AND DIAG on page 173.
- Try resetting to factory defaults (FACTORY DEFAULTS on page 199) and/or a system reboot (SYSTEM REBOOT (RESTART DEVICE) on page 200) .

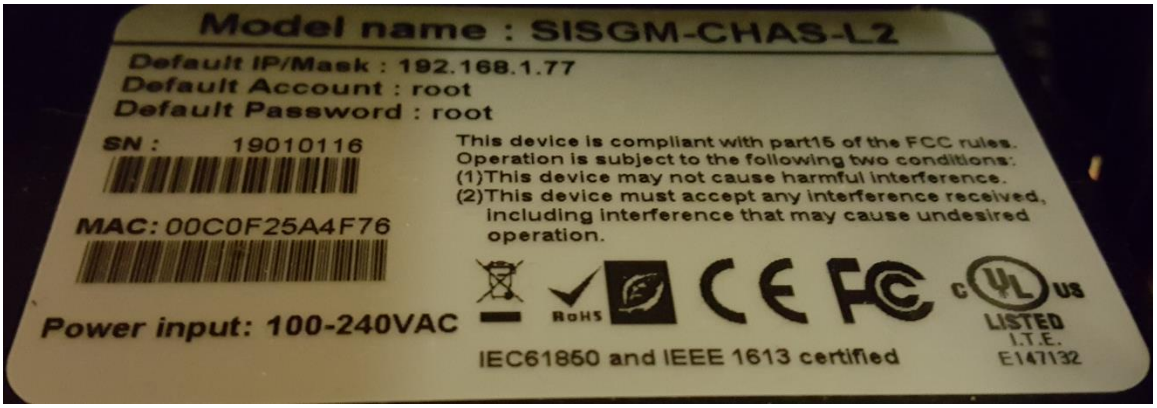
3. Record the model and system information and contact TN Technical Support. Refer to the sections below.

Recording Model and System Information

After performing the troubleshooting procedures, and before contacting Technical Support, please record as much information as possible in order to help the TN Tech Support Specialist.

1. Select the SISGM **System Information** menu path. (From the CLI, use the **show** commands to gather the information below or as requested by the TN Support Specialist).
2. Record SISGM **Model Information**: Name: ____________________________________
   Description: _______________________ OID: _____________________________________
   MAC Address: ____________________ System Date: ____________________________
   System Uptime: ______________________ Software Version: _______________________
3. Record the **Monitor and Diag** menu information:
   System Log Information: ____
   Port Statistics: ____
   LED Status: ____
4. Provide additional troubleshooting information to your Technical Support Specialist.
   See "Troubleshooting" above. ____
   Your Transition Networks service contract number: _________________________________
   A description of the failure: ____
   ____
   ____
   Describe any action(s) already taken to resolve the problem (e.g., change mode, reboot, etc.):
   ____
   ____
   The serial and revision numbers of all involved TN products in the network:
   ____
   ____
   A description of your network environment (layout, cable type, etc.): ___________________
   ____
   ____
   Network load and frame size at the time of trouble (if known): _________________________
   The device history (i.e., have you returned the device before, is this a recurring problem, etc.):
   ____
   ____
   Any previous Return Material Authorization (RMA) numbers: ___________________________

Serial Label on SISGM Bottom



Model name : SISGM-CHAS-L2

Default IP/Mask : 192.168.1.77
Default Account : root
Default Password : root

SN : 19010116

MAC: 00C0F25A4F76

Power input: 100-240VAC

This device is compliant with part15 of the FCC rules.
Operation is subject to the following two conditions:
(1)This device may not cause harmful interference.
(2)This device must accept any interference received,
including interference that may cause undesired
operation.

IEC61850 and IEEE 1613 certified

9. Service, Warranty and Tech Support

Warranty

Hardware Support Products

All Transition Networks products have a hardware warranty that is included in the price of the product. The hardware warranty provides repair or replacement of defective hardware within 20 business days. The length of the included warranty varies depending on the product classification.

5 Year Warranty Classification

Products in this classification include our intelligent network interface devices (S3280 series, S4140 series, S4212, and S4224), the PacketBand, MediaBand, DataBand, and Liberator Series products.

Five-Year Limited Hardware Warranty

Transition Networks warrants to the original consumer or purchaser that each of its Liberator, PacketBand, DataBand, MILAN brand switch and media converters, S3280 series, S4140, S4212, S4224 products and all components thereof, will be free from defects in material and/or workmanship for a period of five years from the original factory shipment date. Any warranty hereunder is extended to the original consumer or purchaser and is not assignable. Transition Networks makes no express or implied warranties including, but not limited to, any implied warranty of merchantability or fitness for a particular purpose, except as expressly set forth in this warranty. In no event shall Transition Networks be liable for incidental or consequential damages, costs, or expenses arising out of or in connection with the performance of the product delivered hereunder. Transition Networks will in no case cover damages arising out of the product being used in a negligent fashion or manner. For more information see:

http://www.transition.com/TransitionNetworks/TechSupport/Warranty.aspx

http://www.transition.com/TransitionNetworks/Uploads/Literature/TN-Care.pdf

Return Authorization

To return a defective product for warranty coverage, contact Transition Networks's technical support department for a return authorization number. Transition's technical support department can be reached through any of the following means:

Contact Us

tel: +1.952.941.7600 | toll free: 1.800.526.9267 | fax: 952.941.2322

sales@transition.com | techsupport@transition.com | customerservice@transition.com

Return Instructions

Send the defective product postage and insurance prepaid to the following address:

Transition Networks, Inc.
10900 Red Circle Drive
Minnetonka, MN 55343 USA
Attn: RETURNS DEPT: CRA/RMA # ___________

Failure to properly protect the product during shipping may void this warranty. The return authorization number must be written on the outside of the carton to ensure its acceptance. We cannot accept delivery of any equipment that is sent to us without a CRA or RMA number.

CRA's are valid for 60 days from the date of issuance. An invoice will be generated for payment on any unit(s) not returned within 60 days.

Upon completion of a demo/ evaluation test period, units must be returned or purchased within 30 days. An invoice will be generated for payment on any unit(s) not returned within 30 days after the demo/ evaluation period has expired.

The customer must pay for the non-compliant product(s) return transportation costs to Transition Networks for evaluation of said product(s) for repair or replacement. Transition Networks will pay for the shipping of the repaired or replaced in-warranty product(s) back to the customer (any and all customs charges, tariffs, or/and taxes are the customer's responsibility).

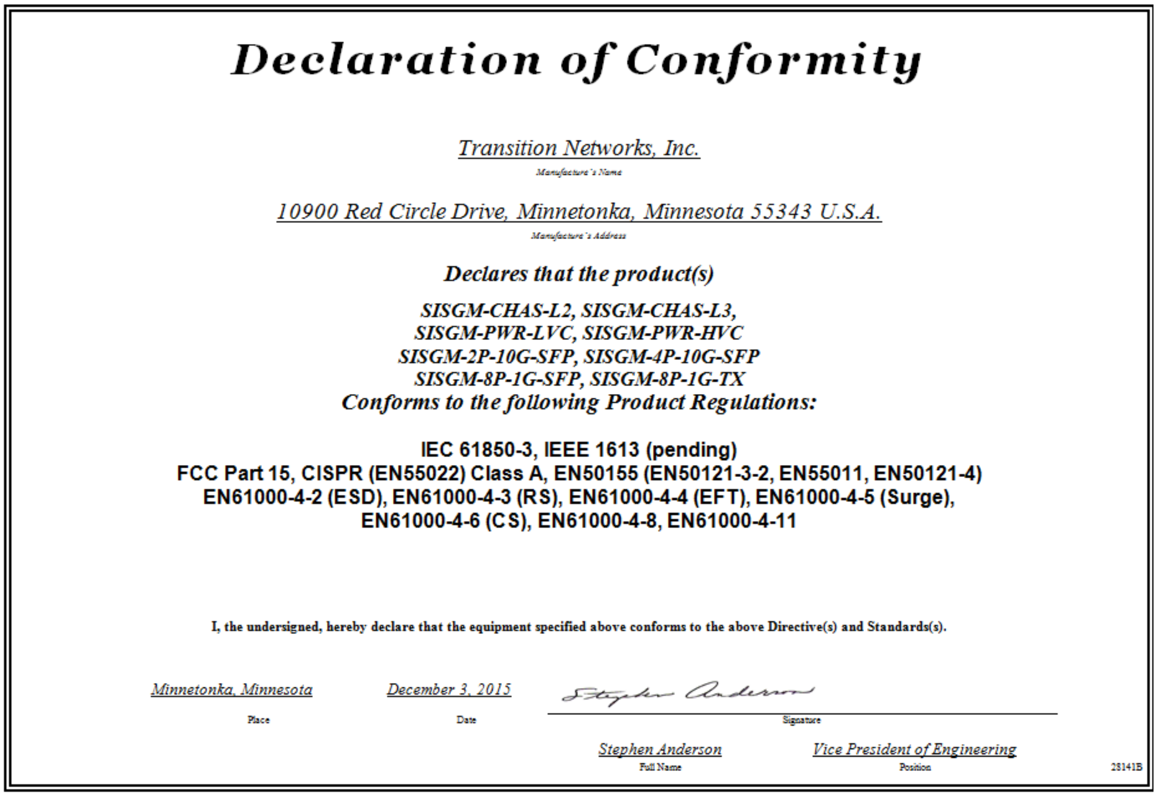
Before making any non-warranty repair, Transition Networks requires a $200.00 charge plus actual shipping costs to and from the customer. If the repair is greater than $200.00, an estimate is issued to the customer for authorization of repair. If no authorization is obtained, or the product is deemed "not repairable", Transition Networks will retain the $200.00 service charge and return the product to the customer not repaired. Non-warranted products that are repaired by Transition Networks for a fee will carry a 180-day limited warranty. All warranty claims are subject to the restrictions and conventions set forth by this document.

Transition Networks reserves the right to charge for all testing and shipping incurred, if after testing, a return is classified as "No Problem Found."

THIS WARRANTY IS YOUR ONLY REMEDY. NO OTHER WARRANTIES, SUCH AS FITNESS FOR A PARTICULAR PURPOSE, ARE EXPRESSED OR IMPLIED. TRANSITION NETWORKS IS NOT LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOSSES, INCLUDING LOSS OF DATA, ARISING FROM ANY CAUSE OR THEORY. AUTHORIZED RESELLERS ARE NOT AUTHORIZED TO EXTEND ANY DIFFERENT WARRANTY ON TRANSITION NETWORKS'S BEHALF.

10. Compliance Information

Declaration of Conformity



Declaration of Conformity

Transition Networks, Inc.

Manufacture´s Name

10900 Red Circle Drive, Minnetonka, Minnesota 55343 U.S.A.

Manufacture´s Address

Declares that the product(s)

SISGM-CHAS-L2, SISGM-CHAS-L3,
SISGM-PWR-LVC, SISGM-PWR-HVC
SISGM-2P-10G-SFP, SISGM-4P-10G-SFP
SISGM-8P-1G-SFP, SISGM-8P-1G-TX
Conforms to the following Product Regulations:

IEC 61850-3, IEEE 1613 (pending)
FCC Part 15, CISPR (EN55022) Class A, EN50155 (EN50121-3-2, EN55011, EN50121-4)
EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge),
EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directive(s) and Standards(s).

Minnetonka, Minnesota *December 3, 2015* Stephen Anderson
Place Date Signature

Stephen Anderson *Vice President of Engineering*
Full Name Position

28141B

European Regulations

WARNING: This is a Class A product. In a domestic environment, this product could cause radio interference in which case the user may be required to take adequate measures.

Achtung ! Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten. In diesem Fäll ist der Benutzer für Gegenmaßnahmen verantwortlich.

Attention ! Ceci est un produit de Classe A. Dans un environment domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilsateur de prende les measures spécifiques appropriées.

In accordance with European Union Directive 2002/96/EC of the European Parliament and of the Council of 27 January 2003, Transition Networks will accept post usage returns of this product for proper disposal. The contact information for this activity can be found in the 'Contact Us' portion of this document.

CAUTION: RJ connectors are NOT INTENDED FOR CONNECTION TO THE PUBLIC TELEPHONE NETWORK. Failure to observe this caution could result in damage to the public telephone network.

Der Anschluss dieses Gerätes an ein öffentlickes Telekommunikationsnetz in den EG-Mitgliedstaaten verstösst gegen die jeweligen einzelstaatlichen Gesetze zur Anwendung der Richtlinie 91/263/EWG zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über Telekommunikationsendeinrichtungen einschliesslich der gegenseitigen Anerkennung ihrer Konformität.

Safety Warnings and Cautions

These products are not intended for use in life support products where failure of a product could reasonably be expected to result in death or personal injury. Anyone using this product in such an application without express written consent of an officer of Transition Networks does so at their own risk, and agrees to fully indemnify Transition Networks for any damages that may result from such use or sale.

⚠ **Attention**: this product, like all electronic products, uses semiconductors that can be damaged by ESD (electrostatic discarge). Always observe appropriate precuations when handling.

⚠ **Warning**: Potential for damage to equipment or personal injury.

⚡ **Warning**: Risk of Electrical Shock

⏚ Functional grounding point

⏚ Protective grounding point

Electrical Safety Warnings

Electrical Safety

IMPORTANT: This equipment must be installed in accordance with safety precautions.

Elektrische Sicherheit

WICHTIG: Für die Installation dieses Gerätes ist die Einhaltung von Sicherheitsvorkehrungen erforderlich.

Elektrisk sikkerhed

VIGTIGT: Dette udstyr skal 232nstallers I overensstemmelse med sikkerhedsadvarslerne.

Elektrische veiligheid

BELANGRIJK: Dit apparaat moet in overeenstemming met de veiligheidsvoorschriften worden geïnstalleerd.

Sécurité électrique

IMPORTANT : Cet équipement doit être utilisé conformément aux instructions de sécurité.

Sähköturvallisuus

TÄRKEÄÄ : Tämä laite on asennettava turvaohjeiden mukaisesti.

Sicurezza elettrica

IMPORTANTE: questa apparecchiatura deve essere installata rispettando le norme di sicurezza.

Elektrisk sikkerhet

VIKTIG: Dette utstyret skal 232nstallers I samsvar med sikkerhetsregler.

Segurança eléctrica

IMPORTANTE: Este equipamento tem que ser instalado segundo as medidas de precaução de segurança.

Seguridad eléctrica

IMPORTANTE: La instalación de este equipo deberá llevarse a cabo cumpliendo con las precauciones de seguridad.

Elsäkerhet

OBS! Alla nödvändiga försiktighetsåtgärder måste vidtas när denna utrustning används.

Record of Revisions

Rev	Date	Description of Changes
A	12/31/15	Initial release for SISGM-CHAS-L3 Firmware v1.04.
B	10/19/17	Remove java applet information, update operating temperature information, add 1U and 2U bracket kit options, revise the SISGM-PWR-LVC range of power input, and update regulatory agency and contact information.

Trademark notice

All trademarks and registered trademarks are the property of their respective owners. All other products or service names used in this publication are for identification purposes only, and may be trademarks or registered trademarks of their respective companies. All other trademarks or registered trademarks mentioned herein are the property of their respective holders.

Copyright restrictions

Address comments on this product or manual to:

Transition Networks Inc.
10900 Red Circle Drive
Telephone: +1-952-941-7600 / Toll Free: 800-526-9267 / Fax: 952-941-2322
E-Mail: customerservice@transition.com or techsupport@transition.com or sales@transition.com or info@transition.com

Transition Networks

10900 Red Circle Drive

Minnetonka, MN 55343 USA

Tel: 952- 941-7600 or 1-800-526-9267

Fax: 952-941-2322

SISGM-CHAS Series Modular Rack Mount Hardened Switch User Guide 33625 Rev. B