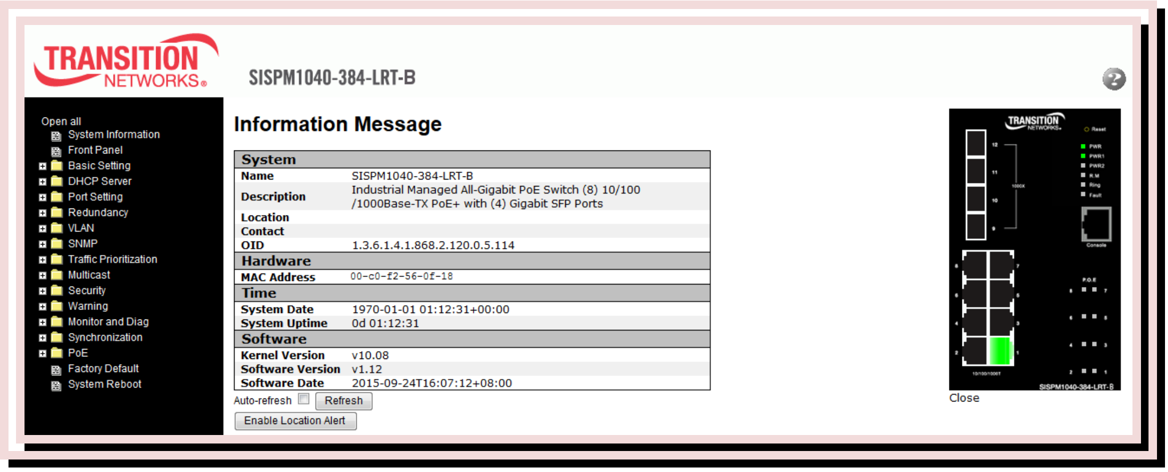
SISPM1040-384-LRT-B

Industrial Managed Ethernet Switch



Information Message

System	
Name	SISPM1040-384-LRT-B
Description	Industrial Managed All-Gigabit PoE Switch (8) 10/100 /1000Base-TX PoE+ with (4) Gigabit SFP Ports
Location	
Contact	
OID	1.3.6.1.4.1.868.2.120.0.5.114
Hardware	
MAC Address	00-c0-f2-56-0f-18
Time	
System Date	1970-01-01 01:12:31+00:00
System Uptime	0d 01:12:31
Software	
Kernel Version	v10.08
Software Version	v1.12
Software Date	2015-09-24T16:07:12+08:00

Auto-refresh □ Refresh

Enable Location Alert

User Guide

33667 Rev. C

v1.12 Jan. 2016

Trademarks

All trademarks and registered trademarks are the property of their respective owners.

Copyright Notice/Restrictions

Contact Information

Transition Networks
10900 Red Circle Drive
Minnetonka, MN 55343 USA
Tel: 952- 941-7600 or 1-800-526-9267
Fax: 952-941-2322

Revision History

Rev	Date	Description
A	11/9/15	Initial release for v1.12.
B	12/3/15	Update power supply, wiring, and Regulatory Agency information.
C	1/11/16	Add power connection information.

Table of Contents

1. Getting Started

1.1 About the SISPM1040-384-LRT-B

The SISPM1040-384-LRT-B is managed redundant ring Ethernet PoE switch with eight 10/100/1000Base-T(X) ports and four 100/1000Base-X SFP ports. The switch supports Ethernet Redundancy protocol, Redundant Ring (recovery time < 30ms over 250 units of connection) and MSTP (RSTP/STP compatible) that can protect your mission-critical applications from network interruptions or temporary malfunctions with its fast recovery technology. The switch also supports Power over Ethernet, a system to transmit electrical power up to 30 watts, along with data, to remote devices over standard twisted-pair cable in an Ethernet network. The switch has eight 10/100/1000Base-T(X) PSE (Power Sourcing Equipment) ports. PSE devices, such as a switch or hub provide power in a PoE connection. The switch supports wide operating temperatures (-40° C to 70° C).

Package Contents

Contact your point of purchase if you have not received these items:

- One SISPM1040-384-LRT-B switch
- One Console cable
- One Wall Mount Kit
- One DIN Rail Mount Kit
- Flat Screws (M3 X5)
- One six-pin Terminal Block

1.2 Hardware Specifications

- Eight 10/100/1000Base-T(X) Ethernet POE Ports
- Four 100/1000Base-X SFP ports
- One Console port
- Redundant DC power inputs (50-57Vdc)
- Rigid IP-30 housing design
- DIN-Rail and wall mounting supported
- Operating temperature: -40 to 70^{o}C; Storage temperature: -40 to 85^{o}C
- Operating humidity: 5% to 95%, non-condensing
- Dimensions: 96.4 (W) x 105.5 (D) x 154 (H) mm (3.8 x 4.15 x 6.06 inches)
- IEEE 802.3az Energy-Efficient Ethernet technology
- Eight port PoE+ compliant with IEEE802.3at standard, provides up to 30 Watts per port (25.5 W at load). Compliant with 802.3at in Environment A when using an isolated power supply. For 802.3at Environment B applications: 1) use an isolated AC/DC power source, e.g. TN 25080, and/or 2) use mid-span injector (s), e.g. MIL-L100i, L1000i-at, between this switch’s PSE port and link partner PD port.

1.3 Software Features

- Redundant Ring (recovery time < 30ms over 250 units of connection) and MSTP (RSTP/STP compatible) for Ethernet Redundancy
- Redundant Ring supports other vendor’s ring technology in open architecture
- Multiple Ring allows multiple redundant network rings
- Standard IEC 62439-2 MRP (Media Redundancy Protocol) function
- PoE scheduled configuration and PoE auto-ping check function
- IEEE 1588v2 clock synchronization
- IPV6 new internet protocol version
- Modbus TCP protocol
- Provides HTTPS/SSH protocol to enhance network security
- Support sSMTP client
- IP-based bandwidth management
- Supports application-based QoS management
- IGMP v2/v3 (IGMP snooping support) for filtering multicast traffic
- SNMP v1/v2c/v3 & RMON & 802.1Q VLAN Network Management
- ACL, TACACS+ and 802.1x User Authentication for security
- 9.6K Bytes Jumbo Frames
- Multiple notifications for warning of unexpected events
- Web-based ,Telnet, Console (CLI), and Windows utility configuration
- LLDP (Link Level Discovery Protocol)Protocol

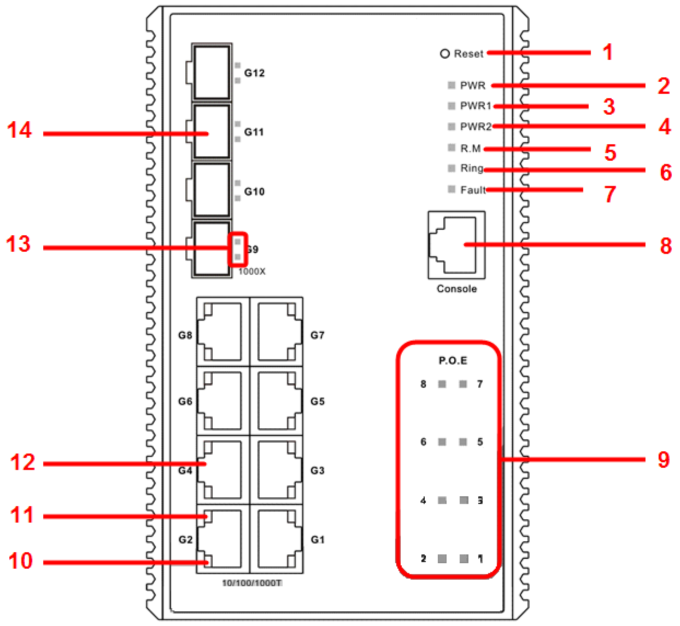
2. Hardware Overview

2.1 Front Panel

2.1.1 Ports and Connectors

The switch front panel is shown and described below.

Port	Description
SFP ports	Four 100 /1000Base-X ports.
Copper ports	Eight 10/100/1000Base-T(X) ports.
Console port	One Console port.



1. Reset Button
2. Power system LED
3. Power 1 LED
4. Power 2 LED
5. R.M (Ring Master) LED
6. Ring status LED
7. Fault indicator
8. Console port
9. POE Status LED
10. Link/action LED for Gigabit Ethernet ports
11. Duplex LED for Gigabit Ethernet ports
12. Gigabit Ethernet ports
13. Link/Act LED for SFP port
14. SFP Port

2.1.2 LEDs

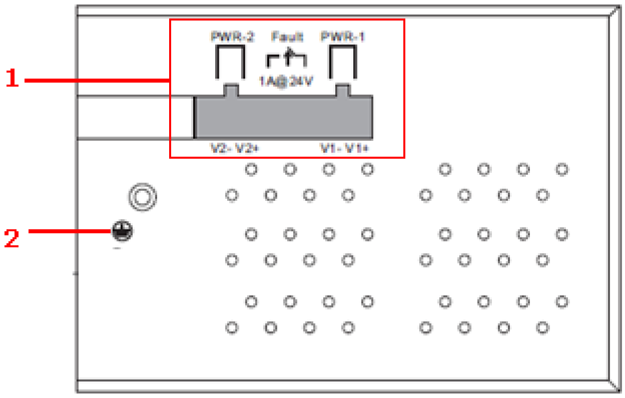
LED	Color	Status	Description
PWR	Green	On	System power on
PW1	Green	On	Power module 1 activated
PW2	Green	On	Power module 2 activated
R.M	Green	On	System operated in Redundant Ring Master mode
Ring	Green	On	System operated in Redundant Ring mode
		Slowly blinking	Ring structure is broken
Fault	Amber	On	Errors occur (power failure or ports disconnected)
10/100/1000Base-T(X) Fast Ethernet ports			
LNK/ACT	Green	On	Port is Linked
		Blinking	Transmitting data
Duplex	Amber	On	Port in full duplex mode
SFP ports			
LNK/ACT	Green	On	Port is linked
		Blinking	Transmitting data

2.2 Top Panel

Below are the SISPM1040-384-LRT-B top panel components:

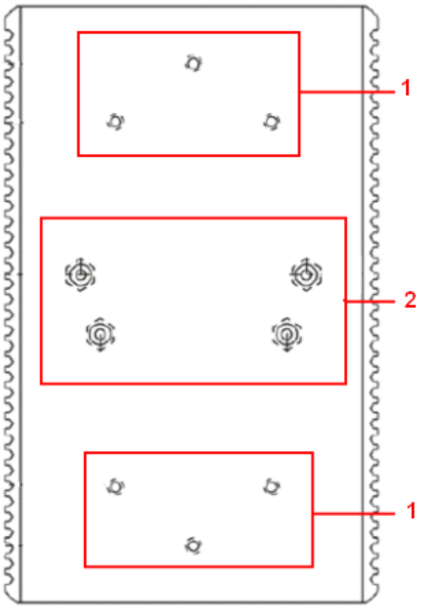
1. Terminal blocks: PWR1, PWR2 (52-57 VDC)

2. Chassis/Frame



2.2 Rear Panel

The rear panel contains three sets of screw holes. The two sets placed in triangular patterns on both ends of the rear panel are used for wall-mounting, and the set of four holes in the middle are used for Din-rail installation. For more information on installation, please refer to 3.1 Din-rail Installation.

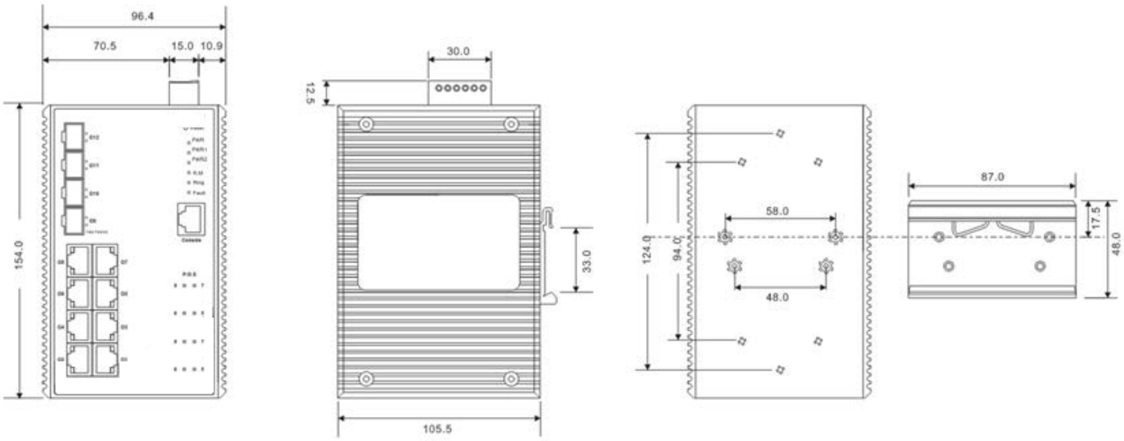


1. Wall-mount screw holes
2. Din-rail screw holes

3. Hardware Installation

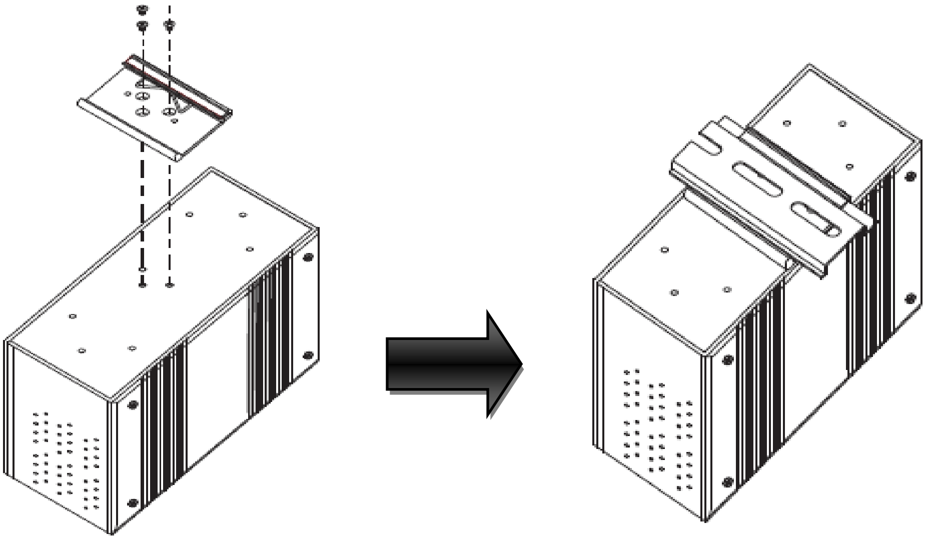
3.1 DIN-Rail Installation

The device comes with a DIN-rail kit to allow you to fasten the switch to a DIN-rail in any environment.



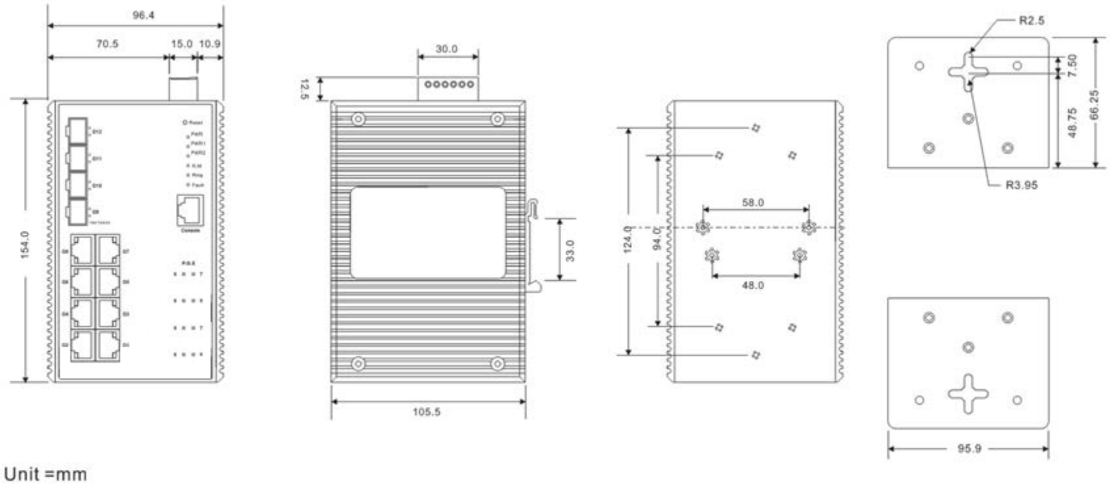
DIN-Rail Measurement

Installing the switch on the DIN-rail is easy. First, screw the Din-rail kit onto the back of the switch, right in the middle of the back panel. Then slide the switch onto a DIN-rail from the Din-rail kit and make sure the switch clicks into the rail firmly.



3.2 Wall Mounting

The switch can also be fixed to the wall via a wall mount panel (included in the package).

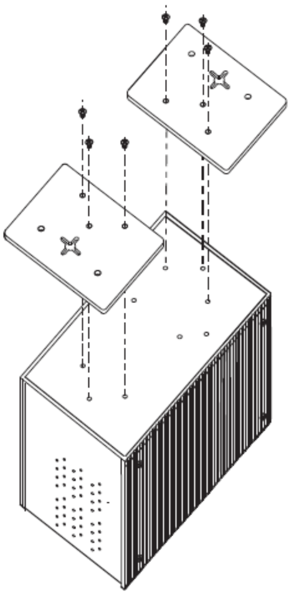


Wall-Mounting Measurement

To mount the switch onto the wall, follow these steps:

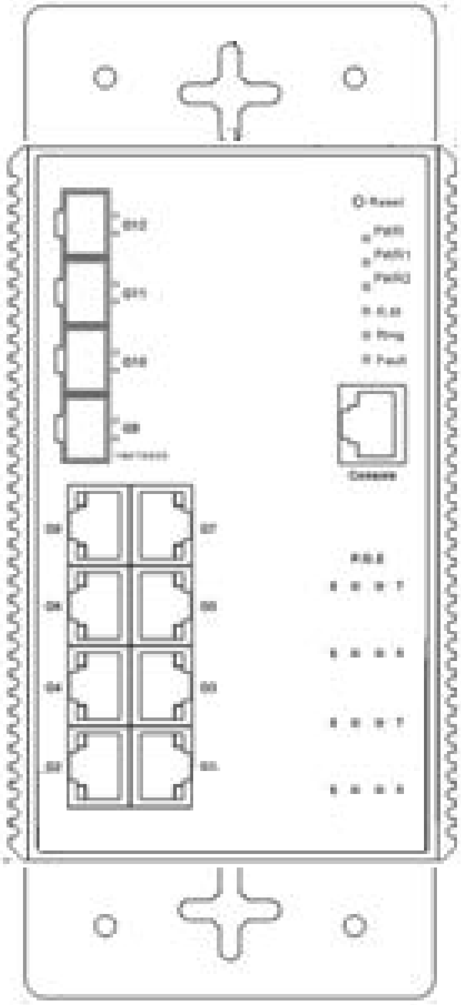
1. Screw the two pieces of wall-mount kits onto both ends of the rear panel of the switch.

A total of six screws are required, as shown below.



2. Use the switch, with wall mount plates attached, as a guide to mark the correct locations of the four screws.

3. Insert four screw heads through the large parts of the keyhole-shaped apertures, and then slide the switch downwards. Tighten the four screws for added stability.



Switch with Wall Mount Plates Attached

3.3 Warning

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

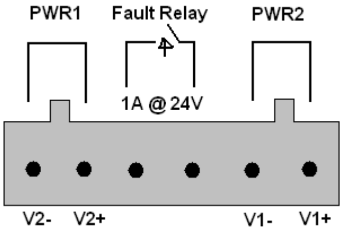
Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screw to the grounding surface prior to connecting devices. When used with an isolated AC/DC input power supply, earth ground the power supply but leave the switch frame/chassis ground float.

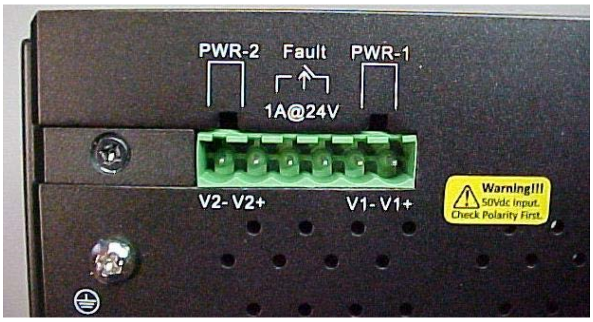
3.3.2 Fault Relay

The two sets of relay contacts of the 6-pin terminal block connector are used to detect user-configured events. The two wires attached to the fault contacts form an open circuit when a user-configured when an event is triggered. If a user-configured event does not occur, the fault circuit remains closed.

3.3.3 Redundant Power Inputs

The switch has two sets of power inputs, power input 1 and power input 2. The top two contacts and the bottom two contacts of the 6-pin terminal block connector on the switch's top panel are used for the two digital inputs.





Follow the steps below to wire redundant power inputs. **Caution**: before applying power, insert screw terminal connectors into the SISPM1040-384-LRT-B switch and verify all connections.

Step 1: insert the negative/positive wires into the V-/V+ terminals, respectively.
Step 2: to keep the DC wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.

3.4 Connection

3.4.1 Cables

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

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

Cable Types and Specifications:

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

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 series also supports auto MDI/MDI-X operation. You can use a cable to connect the switch to a PC. The tables below show the 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

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

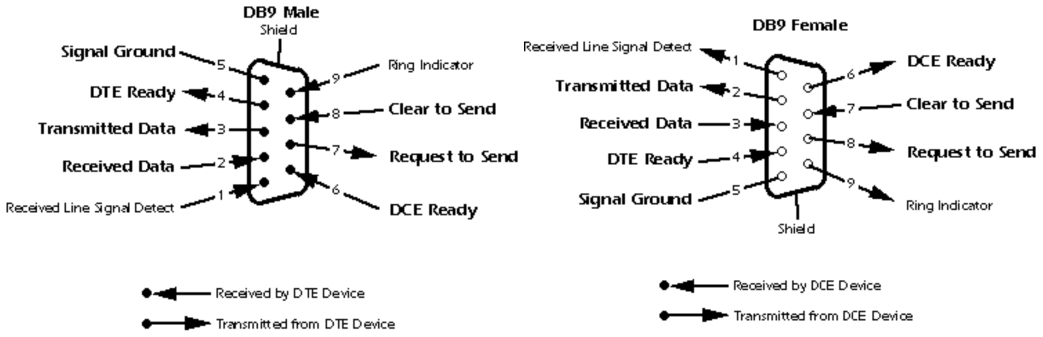
Pin Number	MDI port	MDI-X port
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

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

RS-232 console port wiring

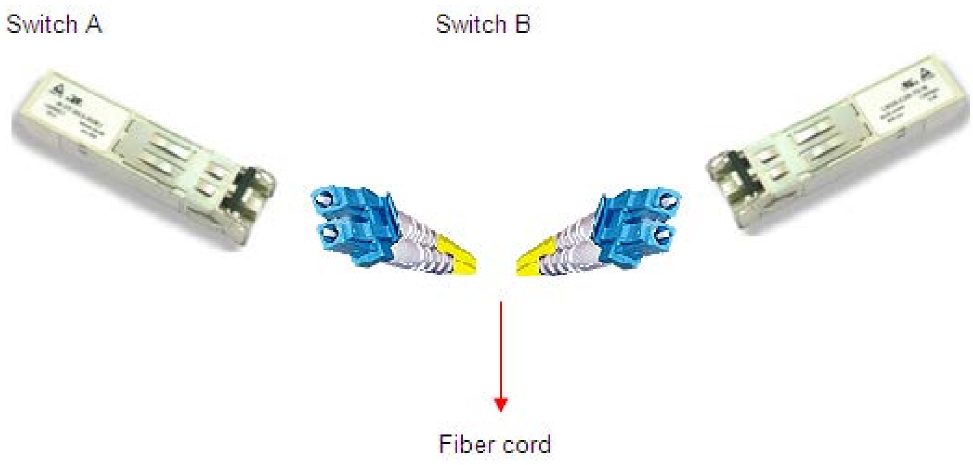
The SISPM1040-384-LRT-B can be managed via console ports using a RS-232 cable which can be found in the package. You can connect the port to a PC via the RS-232 cable with a DB-9 female connector. The DB-9 female connector of the RS-232 cable should be connected the PC while the other end of the cable (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



SFPs

The switch comes with fiber optical ports that utilize SFP connectors. The fiber optical ports are in multi-mode (0 to 550M, 850 nm with 50/125 µm, 62.5/125 µm fiber) and single-mode with LC connectors. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.



3.4.2 Redundant Ring and Multiple Ring

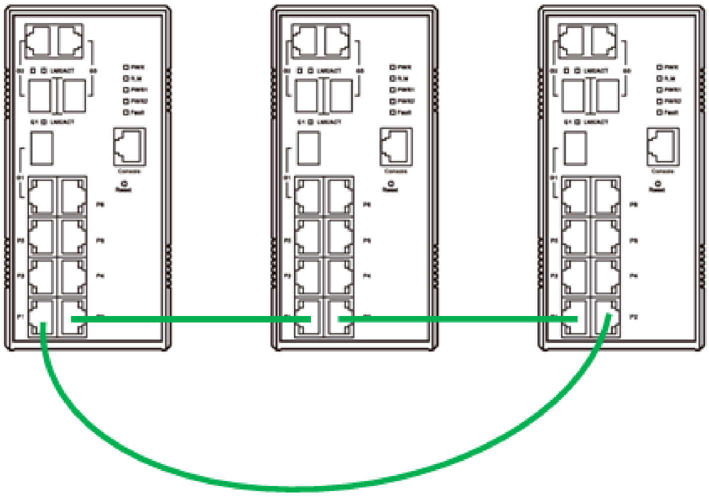
Redundant Ring

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

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

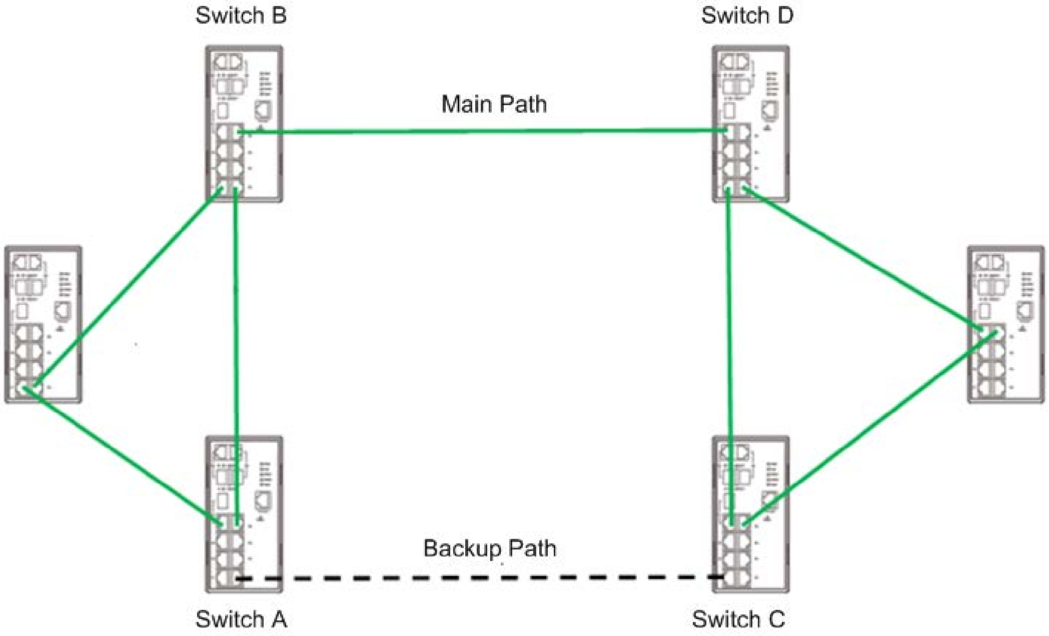
2. Set one of the connected switches to be the master and make sure the port setting of each connected switch on the management page corresponds to the physical ports connected. For information about the port setting, please refer to section 4.1.2 Configurations.

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



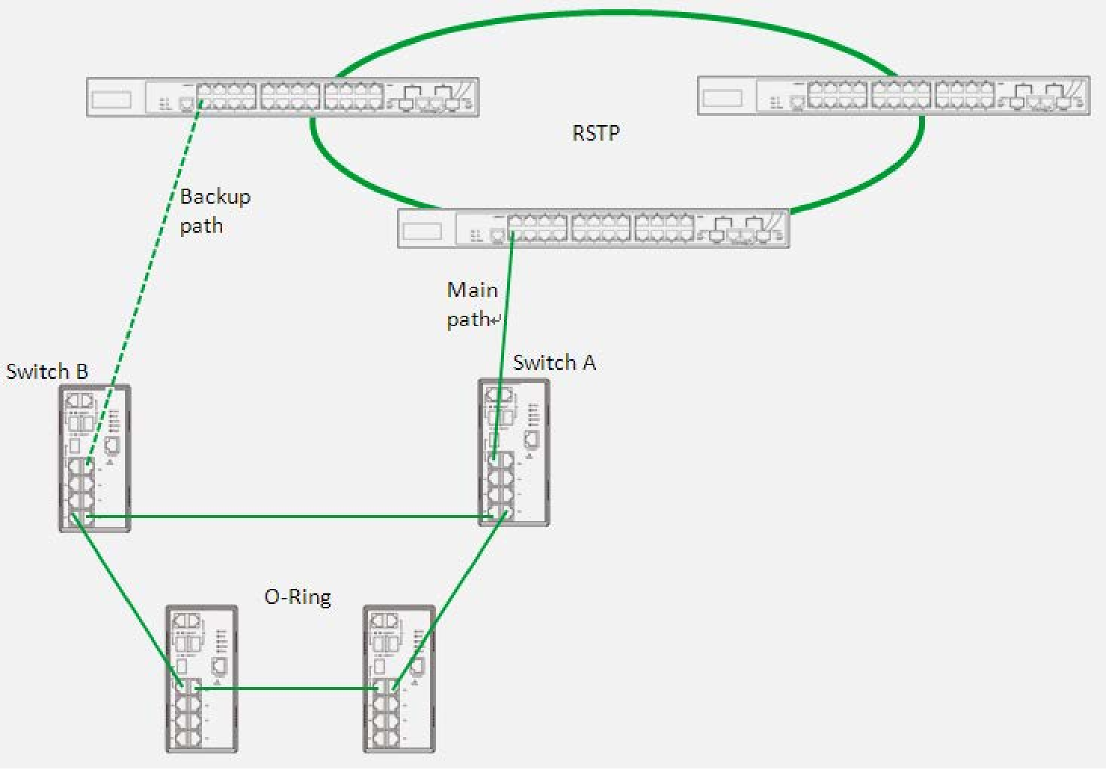
Coupling Ring

If you already have two Redundant Ring topologies and would like to connect the rings, you can form them into a coupling ring. All you need to do is select two switches from each ring to be connected, for example, switch A and B from Ring 1 and switch C and D from ring 2. Decide which port on each switch to be used as the coupling port and then link them together, for example, port 1 of switch A to port 2 of switch C and port 1 of switch B to port 2 of switch D. Then, enable Coupling Ring option by checking the checkbox on the management page and select the coupling ring in correspond dance 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 (Switches A and B) from the ring for connecting to the switches in the RSTP network (core 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.



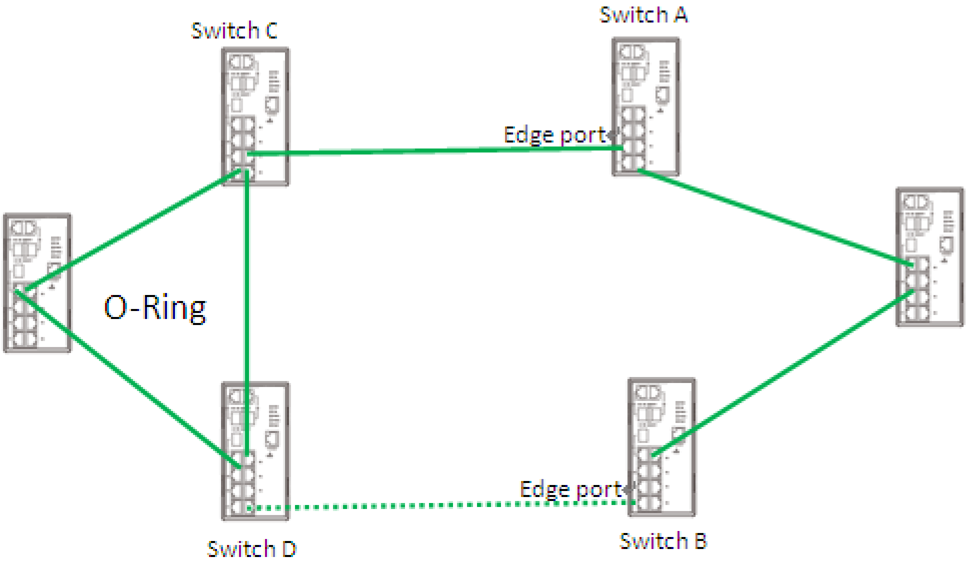
Multiple Rings

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

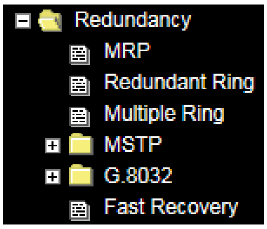
1. Select two switches from the chain (Switch A & B) that you want to connect to the Redundant Ring and connect them to the switches in the ring (Switch C & D).

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

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



4. Redundancy



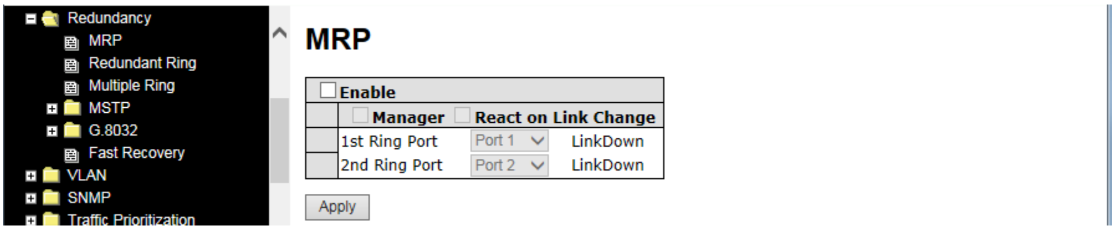
Redundancy for minimized system downtime is one of the most important concerns for industrial networking devices. Supported redundancy technologies include MRP, Redundant Ring, Multiple Ring, MSTP, G.8032, and Fast Recovery featuring faster recovery time than existing redundancy technologies widely used in commercial applications, such as STP, RSTP, etc. These redundancy technologies not only support different networking topologies, but also assure the reliability of the network.

4.3 MRP

4.3.1 Introduction

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

4.3.2 Configurations



MRP

☐ Enable

	☐ Manager	☐ React on Link Change
1st Ring Port	Port 1	LinkDown
2nd Ring Port	Port 2	LinkDown

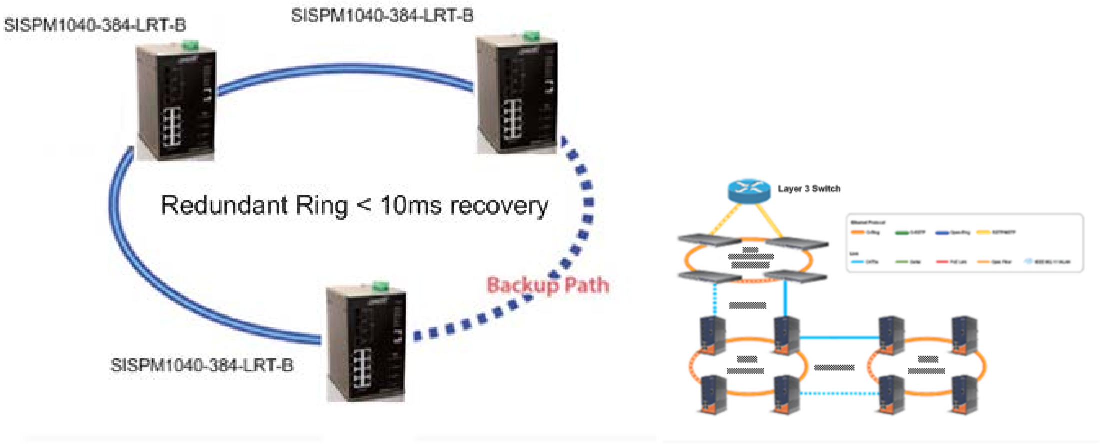
Apply

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

4.1 Redundant Ring

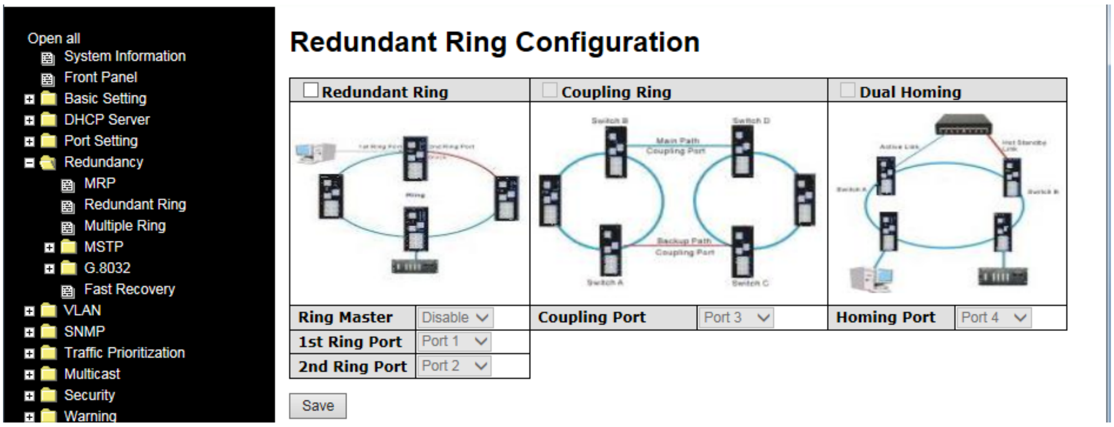
4.1.1 Introduction

Redundant Ring technology can provide recovery time of less than 10 milliseconds on 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 recover technology.



4.1.2 Redundant Ring Configuration

Redundant Ring Protocol is a very fast network redundancy protocol that provides link fail-over protection with very fast self-healing recovery. Redundant Ring supports two ring topologies: **Coupling Ring**, and **Dual Homing**. You can configure the settings as shown below.



Redundant Ring Configuration

☐ Redundant Ring		☐ Coupling Ring		☐ Dual Homing	
Ring Master	Disable	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 Ring 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 port when the switch is ring master
2nd Ring Port	The backup port when the switch is ring master
Coupling Ring	Check to enable **Coupling Ring**. **Coupling Ring** can divide a big ring into two smaller rings to avoid network topology changes affecting all switches. It is a good method for connecting two rings.
Coupling Port	Ports for connecting multiple rings. A coupling ring needs four switches to build an active and a backup link. Links formed by the coupling ports will run in active/backup mode.
Dual Homing	Check to enable **Dual Homing**. When **Dual Homing** is enabled, the ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work in active/backup mode, and connect each ring to the normal switches in RSTP mode.
Apply	Click to apply the configurations.

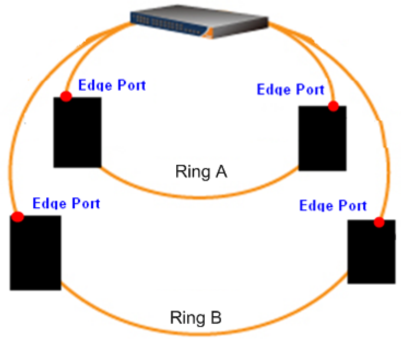
Note: due to heavy loading, setting one switch as ring master and coupling ring at the same time is not recommended. Note: all switchesin a ring should have Redundant Ring enabled.

4.2 Multiple Ring Configuration

4.2.1 Introduction

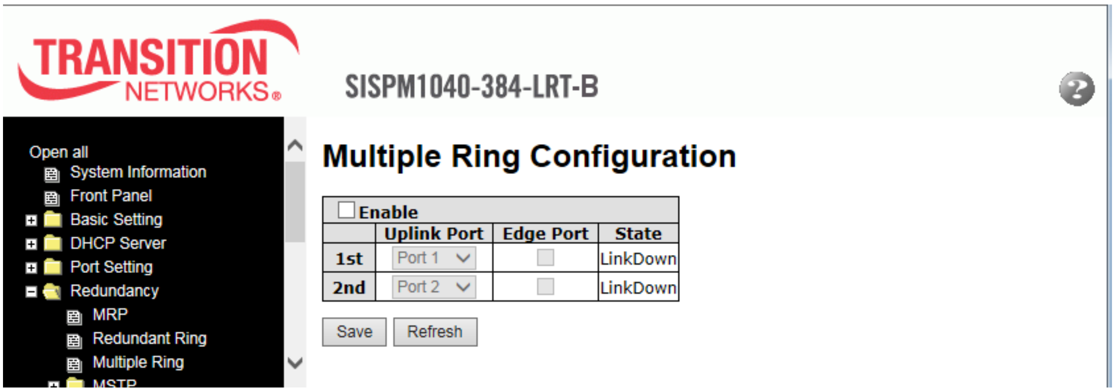
Multiple Ring is an easy to use and powerful network redundancy protocol. The recovery speed of Multiple Ring is very quick. It provides the add-on network redundancy topology for any backbone network; the upper LAN could be Redundant Ring, Multiple Ring, RSTP, Single Switch, or any backbone.

Multiple redundant rings of different redundancy protocols



4.2.2 Multiple Ring Configuration

Multiple Rings are easy to configure and manage. Only one edge port of the edge switch needs to be defined. Other switches beside them just need to have Multiple Ring enabled.



Multiple Ring Configuration

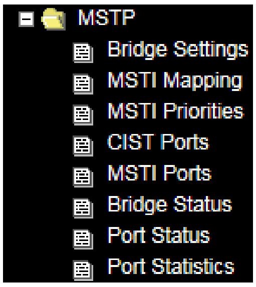
☐ Enable

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

Label	Description
Enable	Check to enable Multiple Ring function
Uplink Port	There are two uplink ports for each device in the chain. You must specify the ports according to topology of network.
Edge Port	Only the edge (head or tail) device needs to specify edge port. The user must specify the edge port according to topology of network.
Edge Port	A Multiple Ring topology must begin with edge ports. Ports with a smaller MAC address will serve as the backup link and the RM LED will light.
State	There three states for uplink port: Link Down, Blocking, and Forwarding.

***Messages**: MRP Error*

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



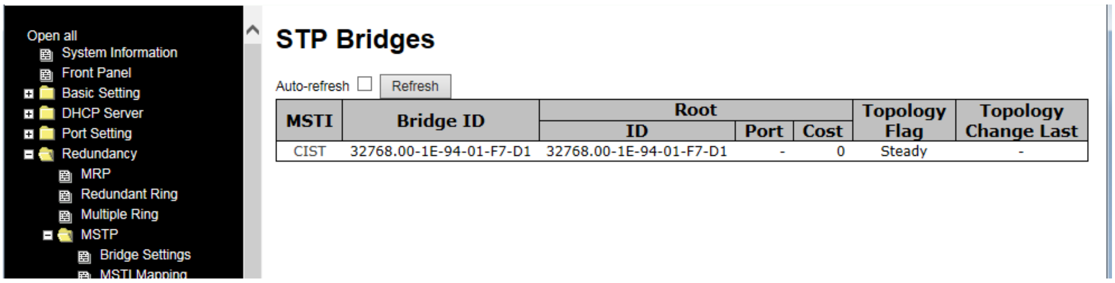
4.4 STP/RSTP/MSTP

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 instance.



STP Bridges

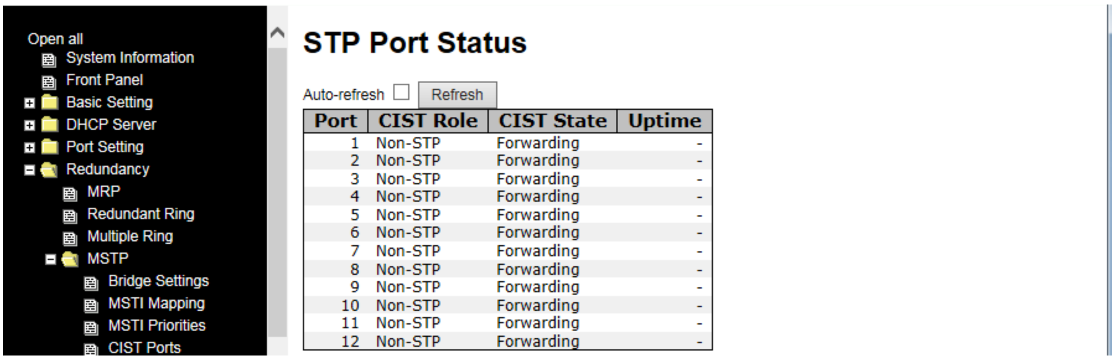
Auto-refresh □ Refresh

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-1E-94-01-F7-D1	32768.00-1E-94-01-F7-D1	-	0	Steady	-

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

STP Port Status

This page displays the STP CIST port status for physical ports of the switch.



STP Port Status

Auto-refresh □ Refresh

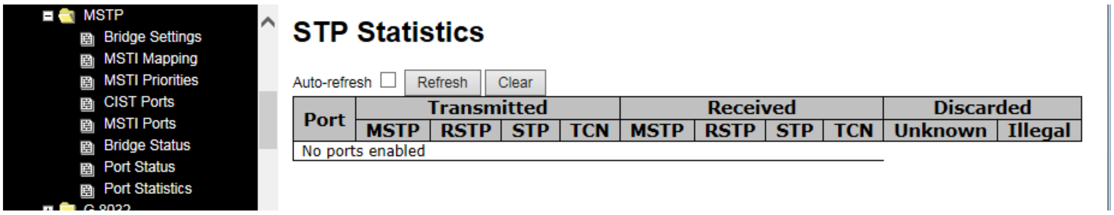
Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding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

STP port status displayed includes:

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.



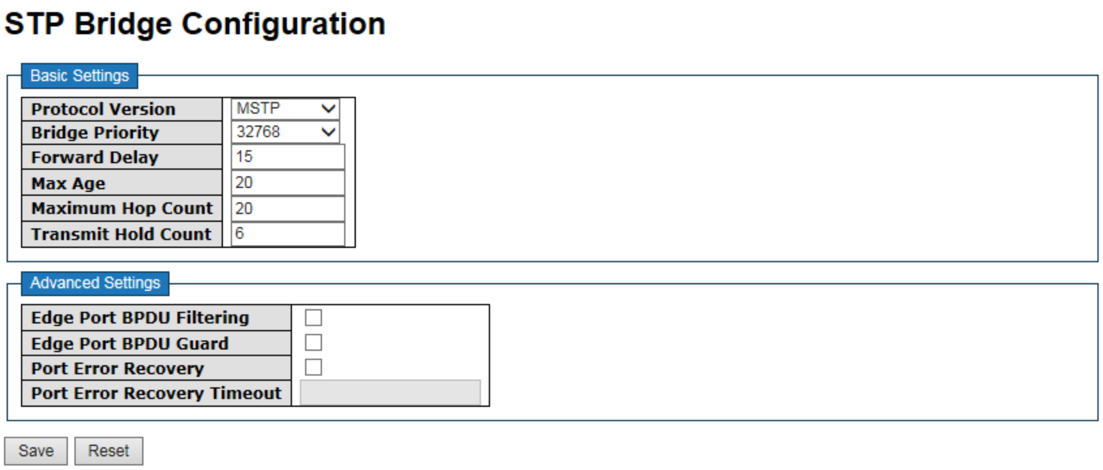
STP Statistics

Auto-refresh □ Refresh Clear

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

Label	Description
Port	The switch port number to which the following settings apply.
MSTP	The number of MSTP BPDU's 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.
Clear	: Click to reset the counters.
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals.

STP Bridge Configuration



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	

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** to **30** seconds.
Max Age	The maximum time the information transmitted by the root bridge is considered valid. The range of valid values is 6 to 40 seconds, and **Max Age** must be <= (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	Control whether a port explicitly configured as **Edge** will transmit and receive BPDUs.

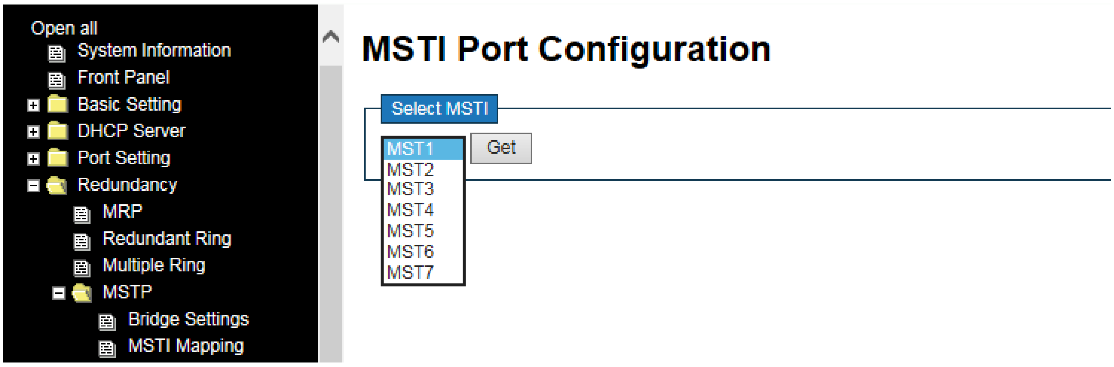
Edge Port BPDU Guard	Control whether a port explicitly configured as **Edge** will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
Port Error Recovery	Control whether a port in the error-disabled state automatically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

4.4.2 MSTP

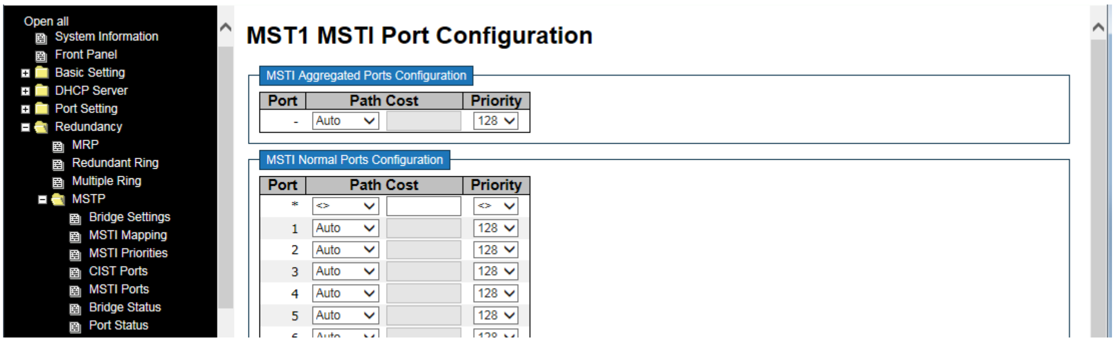
Since the recovery time of STP and RSTP takes seconds, which is unacceptable in some industrial applications, MSTP was developed. The technology supports multiple spanning trees within a network by grouping and mapping multiple VLANs into different spanning-tree instances, known as MSTIs, to form individual 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.

MSTI Port Settings

This page allows you to examine and change the configurations of current MSTI ports.
An 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. Select a MSTI instance to be able to configure MSTI port settings.



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



MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost		Priority
-	Auto		128

MSTI Normal Ports Configuration

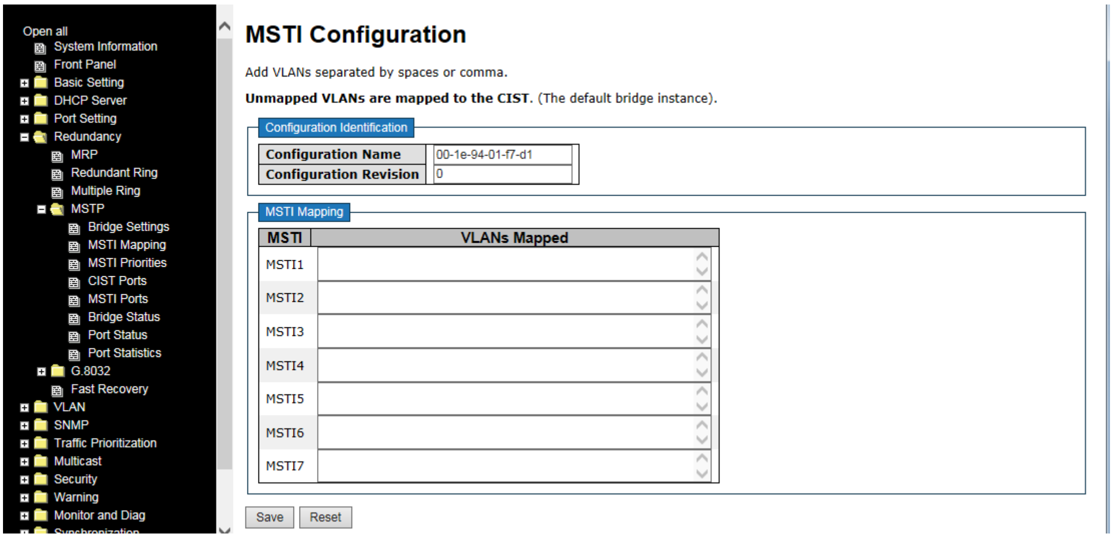
Port	Path Cost		Priority
*	<>		<>
1	Auto		128
2	Auto		128
3	Auto		128
4	Auto		128
5	Auto		128
6	Auto		128

The MSTI port settings are described below.

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).
Get	Click to retrieve settings for a specific MSTI.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Mapping

This page lets you view and change the current STP MSTI bridge instance configuration.



MSTI Configuration

Add VLANs separated by spaces or comma.

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

Configuration Identification

Configuration Name	00-1e-94-01-f7-d1
Configuration Revision	0

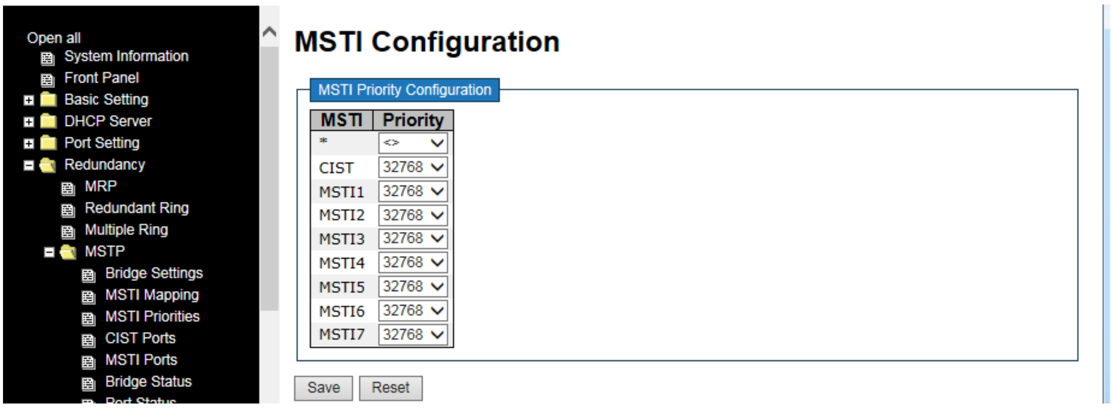
MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

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

Priority

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



MSTI Configuration

MSTI Priority Configuration

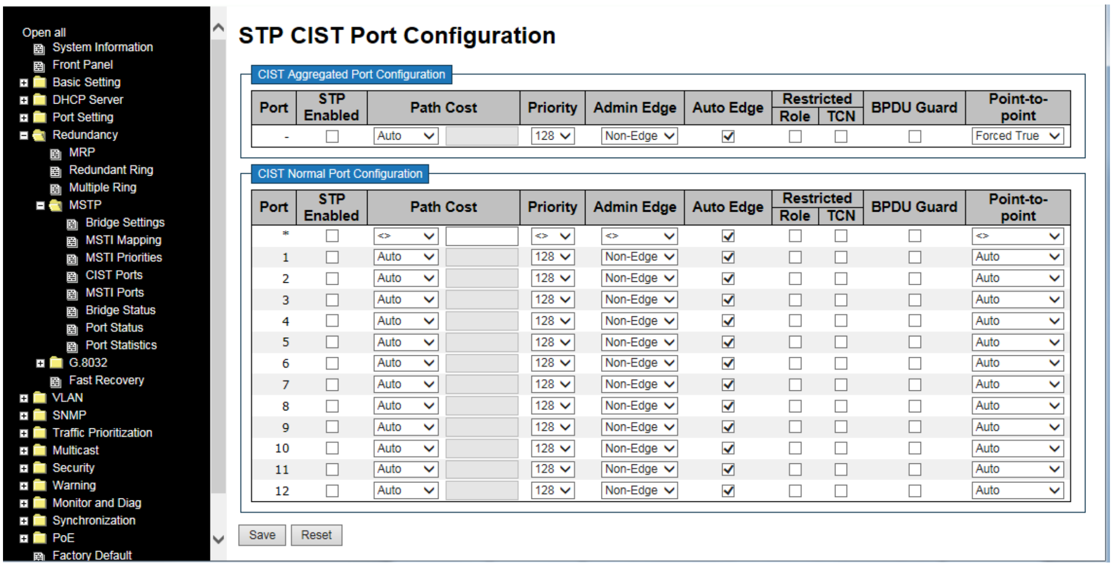
MSTI	Priority
*	<>
CIST	32768
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

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

4.4.3 CIST

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

Port Settings



STP CIST 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
7	□	Auto		128	Non-Edge	☑	□	□	□	Auto
8	□	Auto		128	Non-Edge	☑	□	□	□	Auto
9	□	Auto		128	Non-Edge	☑	□	□	□	Auto
10	□	Auto		128	Non-Edge	☑	□	□	□	Auto
11	□	Auto		128	Non-Edge	☑	□	□	□	Auto
12	□	Auto		128	Non-Edge	☑	□	□	□	Auto

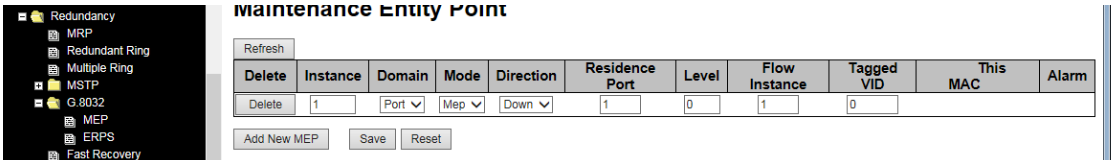
Label	Description
Port	The switch port number to which the following settings will be applied.
STP Enabled	Check to enable STP for the port
Path Cost	Configures the path cost incurred by the port. **Auto** will set the path cost according to the physical link speed by using the 802.1D-recommended values. **Specific** allows you to enter a user-defined value. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range of valid values is 1 to 200000000.
Priority	Configures the priority for ports having identical port costs. (See above).
AdminEdge	Configures the operEdge flag to start as set or cleared (the initial operEdge state when a port is initialized).
AutoEdge	Check to enable the bridge to detect edges at the bridge port automatically. This allows **operEdge** to be derived from whether BPDUs are received on the port or not.
Restricted Role	When enabled, the port will not be selected as root port for CIST or any

	MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an alternate port after the root port has been selected. If set, spanning trees will lose connectivity. It can be set by a network administrator to prevent bridges outside a core region of the network from influencing the active spanning tree topology because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
Restricted TCN	When enabled, the port will not propagate received topology change notifications and topology changes to other ports. If set, it will cause temporary disconnection after changes in an active spanning trees topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges outside a core region of the network from causing address flushing in that region because those bridges are not under the full control of the administrator or is the physical link state for the attached LANs transitions frequently.
BPDU Guard	If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.
Point-to-Point	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.

4.4 G.8032 Ethernet Ring Protection Switching

The **Redundancy** > **G.8032** menu path lets you configure G.8032 ERPS in terms of MEP and ERPS parameters.

MEP Configuration



Maintenance Entity Point

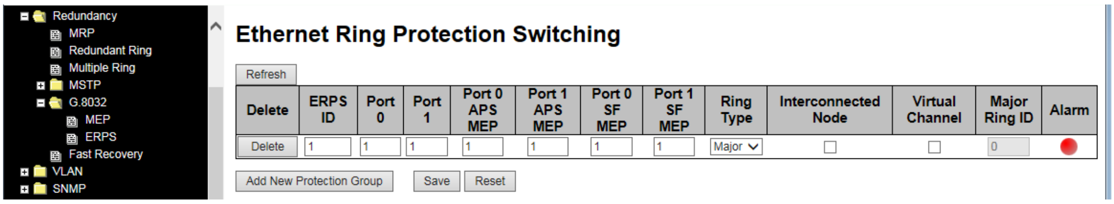
Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
Delete	1	Port	Mep	Down	1	0	1	0		

The Maintenance Entity end Point instances are configured here as described below.

Label	Description
Delete	This box is used to mark a MEP for deletion in next Save operation.
Instance	The ID of the MEP. Click on the MEP ID to enter the configuration page.
Domain	The Domain type, either: **Port**: This is a MEP in the Port Domain. 'Flow Instance' is a Port. **Evc**: This is a MEP in the EVC Domain. 'Flow Instance' is an EVC.
Mode	The Mode of operation, either: **MEP**: This is a Maintenance Entity End Point. **MIP**: This is a Maintenance Entity Intermediate Point.
Direction	**Up**: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'. **Down**: This is an Up MEP - monitoring egress OAM and traffic on 'Residence Port'.
Residence Port	The port where MEP is monitoring - see 'Direction'.
Level	The MEG level of this MEP.
Flow Instance	The MEP is related to this flow - See 'Domain'.
Tagged VID	**Port MEP**: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added. **EVC MIP**: On Serval, this is the Subscriber VID that identifies the subscriber flow in this EVC where the MIP is active.
This MAC	The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).
Alarm	There is an active alarm on the MEP.
Add New MEP	Click to add a new MEP entry.
Refresh	Click to refresh the page immediately.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to saved values.

ERPS Configuration

The Ethernet Ring Protection Switch instances are configured here.



Ethernet Ring Protection Switching

Refresh

Delete	ERPS ID	Port 0	Port 1	Port 0 APS MEP	Port 1 APS MEP	Port 0 SF MEP	Port 1 SF MEP	Ring Type	Interconnected Node	Virtual Channel	Major Ring ID	Alarm
Delete	1	1	1	1	1	1	1	Major	□	□	0	●

Add New Protection Group   Save   Reset

The ERPS parameters are described below.

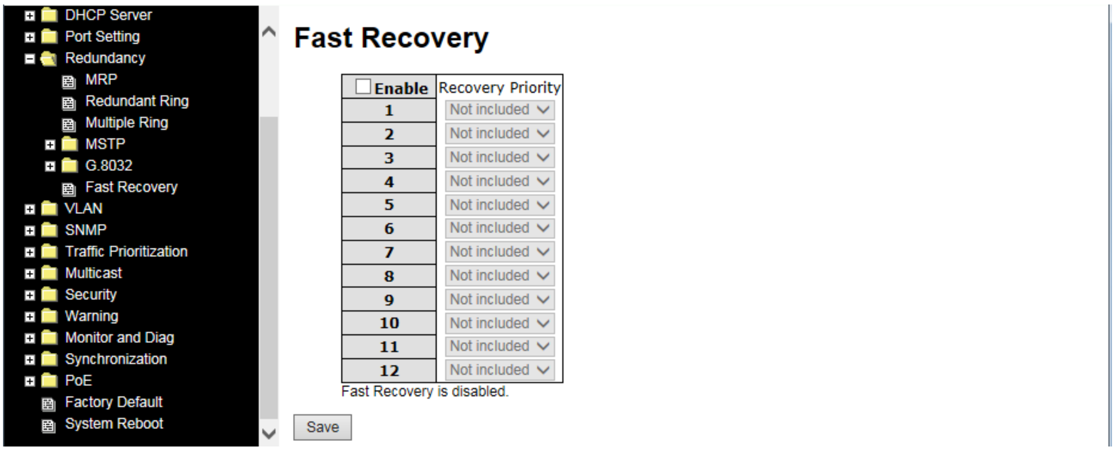
Label	Description
Delete	This box is used to mark an ERPS for deletion in next Save operation.
ERPS ID	Protection group ID: The ID of the created Protection group. Click on the ID of a Protection group to enter its configuration page.
Port 0	This will create a Port 0 of the switch in the ring.
Port 1	This will create "Port 1" of the switch in the Ring. An interconnected sub-ring will have only one ring port; "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance.
Port 0 APS MEP	The Port 0 APS PDU handling MEP. Port 1 APS MEPThe Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.
Port 1 APS MEP	
Port 0 SF MEP	The Port 0 Signal Fail reporting MEP.
Port 1 SF MEP	The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.
Ring Type	The type of Protecting ring. It can be either major ring or sub-ring.
Interconnected Node	Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.
Virtual Channel	Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring

	doesn't have virtual channel.
Major Ring ID	Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.
Alarm	There is an active alarm on the ERPS.
Add New Protection Group	Click to add a new Protection group entry.
Refres	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.

4.5 Fast Recovery

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

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



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
11	Not included
12	Not included

Fast Recovery is disabled.

Save

Label	Description
Enable	Check to enable Fast Recovery function globally.
Recovery Priority	The port that has the highest recovery priority (the lowest number) will be the active port; others will be blocked (if included). Select **0-12** or **Not Included**.
Save	Click to save changes.

5. Management

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

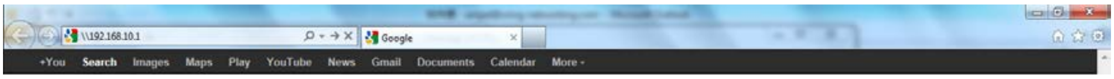
Note: By default, IE5.0 or later version do not allow Java applets to open sockets. You must modify the browser setting separately in order to enable Java applets for network ports.

Management via Web Browser

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

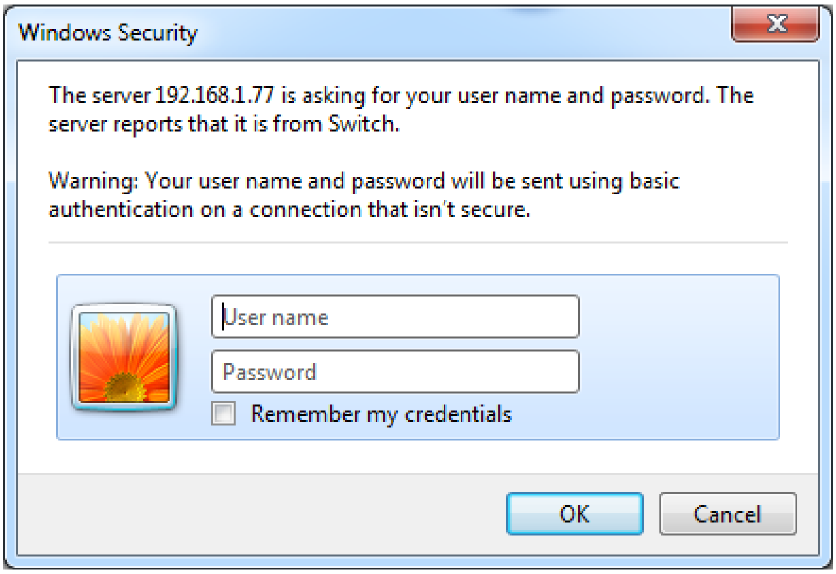
System Login

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



\\192.168.10.1

3. The login screen displays.
4. Type in the username and password. The default username and password is **root**.
5. Click **Enter** or **OK** button and the main interface of the management page displays.



Windows Security

The server 192.168.1.77 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.

Default Values

IP Address: **192.168.1.77 /24**

Subnet Mask: **255.255.255.0**

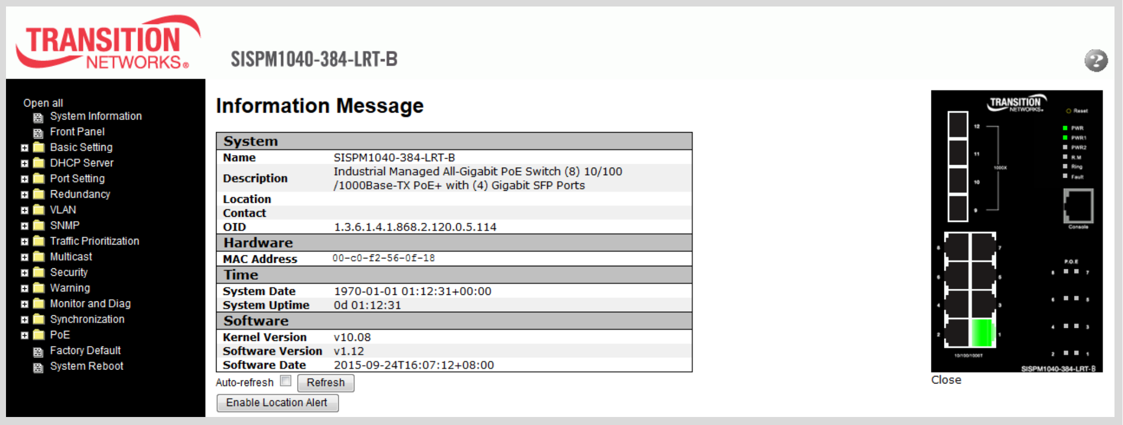
Default Gateway: **192.168.1.254**

User Name: **root**

Password: **root**

System Information

After logging in, the switch System Information displays as shown below.



Information Message

System	
Name	SISPM1040-384-LRT-B
Description	Industrial Managed All-Gigabit PoE Switch (8) 10/100 /1000Base-TX PoE+ with (4) Gigabit SFP Ports
Location	
Contact	
OID	1.3.6.1.4.1.868.2.120.0.5.114
Hardware	
MAC Address	00-c0-f2-56-0f-18
Time	
System Date	1970-01-01 01:12:31+00:00
System Uptime	0d 01:12:31
Software	
Kernel Version	v10.08
Software Version	v1.12
Software Date	2015-09-24T16:07:12+08:00

Auto-refresh □ Refresh

Enable Location Alert

Left panel menu system: The left side of the management interface provides links to device and port settings. Clicking on the links will bring you to individual configuration pages.

Open all / **Close all**: expands and contracts the menu panel, alternately showing / hiding all of the sub-menu items.

Front Panel: Displays a graphic of the front panel. When displayed, click the **Close** button to hide the front panel graphic again. Check the **Auto Refresh** checkbox to ensure the on-screen interface LEDs update properly.

Name: The system name configured in **Configuration** > **System** > **Information** > **System Name**.

Description: e.g., *Industrial Managed All-Gigabit PoE Switch (8) 10/100/1000Base-TX PoE+ with (4) Gigabit SFP Ports*.

Location: System location configured at **Configuration** > **System** > **Information** > **System** > **Location**.

Contact: System contact configured at **Configuration** > **System** > **Information** > **System** > **Contact**.

OID: The object identifier (OID) identification mechanism jointly developed by ITU-T and ISO/IEC for naming any type of object, concept or "thing" with a globaly unambiguous name which requires a persistent name (long life-time). e.g., *1.3.6.1.4.1.868.2.120.0.5.114*.

MAC Address: The MAC Address of this switch.

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

System Uptime: The period of time the device has been operational (e.g., *0d 01:17:59*).

Software Version: The software version of this switch (e.g., *v1.09*).

Software Date: The date the switch software was produced "*2015-08-25T17:46:03+08:00*".

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds. Check the **Auto Refresh** checkbox should to ensure the on-screen interface LEDs on the front panel display update properly.

Refresh: Click to refresh the page immediately. Click to ensure the on-screen interface LEDs on the front panel display update properly.

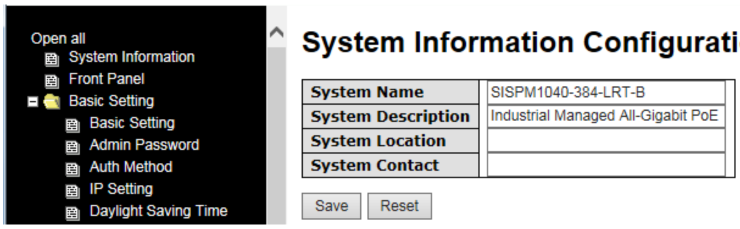
Enable Location Alert / **Disable Location Alert**: reserved for future use.

5.1 Basic Settings

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

5.1.1 System Information Configuration

This page shows the general information of the switch.



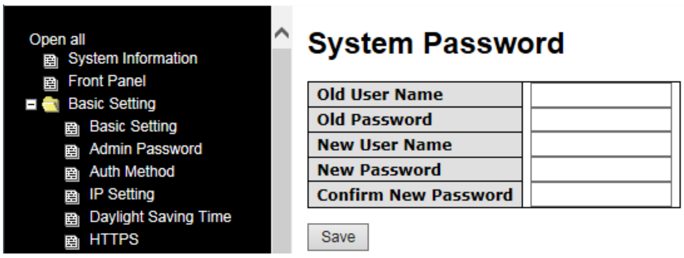
System Information Configuration

System Name	SISPM1040-384-LRT-B
System Description	Industrial Managed All-Gigabit PoE
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. The default is “SISPM1040-384-LRT-B”.
System Description	Description of the device. The default is “Industrial Managed All-Gigabit PoE Switch (8) 10/100/1000Base-TX PoE+ with (4) Gigabit SFP Ports”.
System Location	The physical location of the node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and only ASCII characters from 32 to 126 are allowed.
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and only ASCII characters from 32 to 126 are allowed.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.2 Admin & Password

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



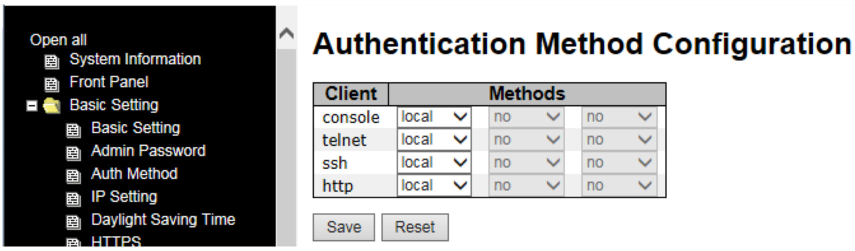
System Password

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

Label	Description
Old User Name	The existing username.
Old Password	The existing password. If this is incorrect, you cannot set the new password.
New User Name	The new username.
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 Method

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



Authentication Method Configuration

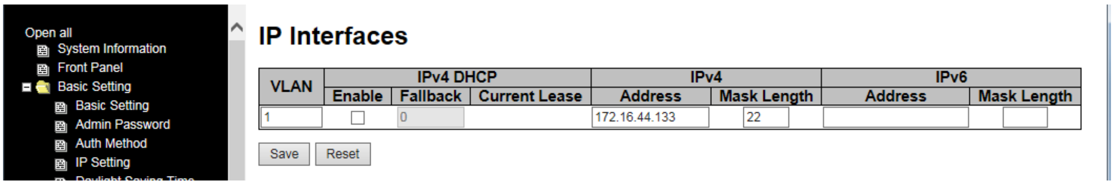
Client	Methods		
console	local	no	no
telnet	local	no	no
ssh	local	no	no
http	local	no	no

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

Label	Description
Client	The management client for which the configuration below applies.
Authentication Method	The Auth Method can be set to one of the following values: **no**: Authentication is disabled and login is not possible. **local**: Use the local user database on the switch for authentication. **radius**: Use remote RADIUS server(s) for authentication. **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.
Fallback	Check to enable fallback to local authentication. If none of the configured authentication servers are active, the local user database is used for authentication. This is only possible if **Authentication Method** is set to a value other than **none** or **local**.
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values

5.1.4 IP Setting

This page lets you configure IPv4 or IPv6 information for the switch.



IP Interfaces

VLAN	IPv4 DHCP			IPv4		IPv6	
	Enable	Fallback	Current Lease	Address	Mask Length	Address	Mask Length
1	□	0		172.16.44.133	22		

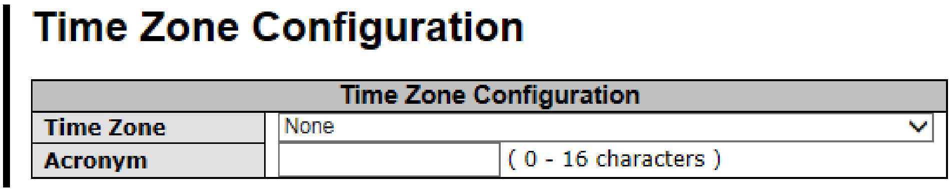
IPv6 is the next-generation IP that uses a 128-bit address standard. It is developed to supplement, and eventually replace the IPv4 protocol. You can configure IPv6 information of the switch on the following page.

Label	Description
Delete	Select this option to delete an existing IP interface.
VLAN	The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface. IPv4 DHCP 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 an 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. An 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 an IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.5 Daylight Saving Time

Time Zone Configuration

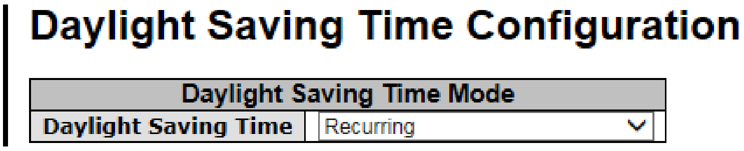


Time Zone Configuration

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

Label	Description
Time Zone	Lists various Time Zones world wide. Select the appropriate Time Zone from the drop down and click Save to set.
Acronym	User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range: Up to 16 alpha-numeric characters and can contain '-', '_' or '.')

Daylight Saving Time Configuration

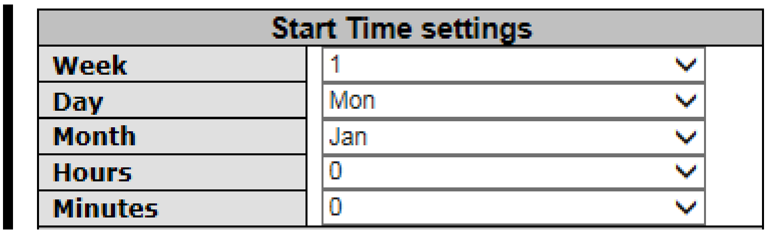


Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Recurring

Label	Description
Daylight Saving Time	This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the 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)

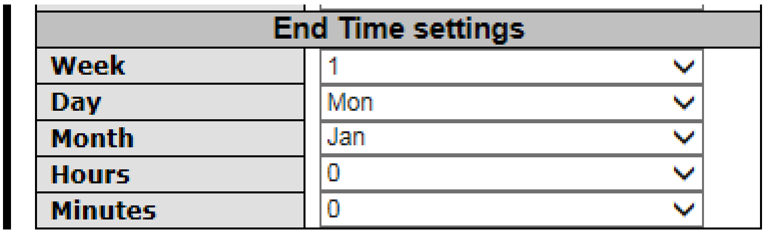
Start Time Settings



Start Time settings	
Week	1
Day	Mon
Month	Jan
Hours	0
Minutes	0

Label	Description
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.

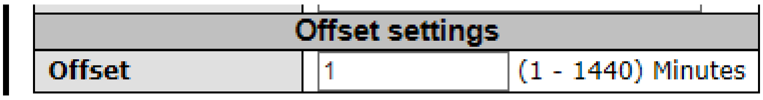
End Time Settings



End Time settings	
Week	1
Day	Mon
Month	Jan
Hours	0
Minutes	0

Label	Description
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 Settings

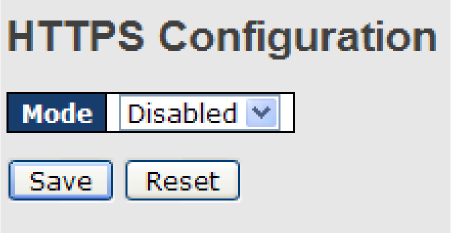


Offset settings		
Offset	1	(1 - 1440) Minutes

Label	Description
Week	Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

5.1.6 HTTPS

You can configure the HTTPS mode in the following page.



HTTPS Configuration

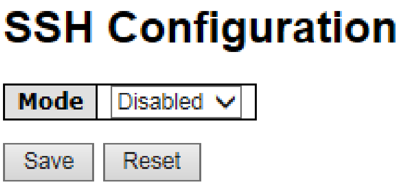
Mode: Disabled

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 include: **Enabled**: enable HTTPS. **Disabled**: disable HTTPS.
Save	Click to save changes

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

5.1.7 SSH

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



SSH Configuration

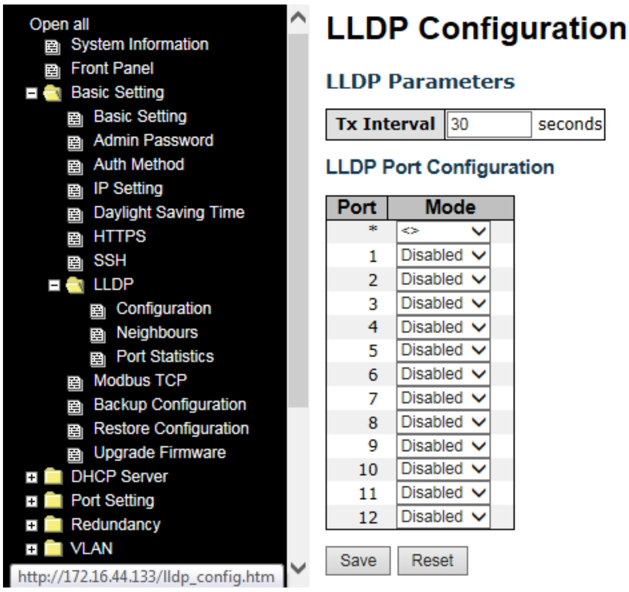
Mode: Disabled

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

5.1.8 LLDP

LLDP Configuration

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



LLDP Configuration

LLDP Parameters

Tx Interval 30 seconds

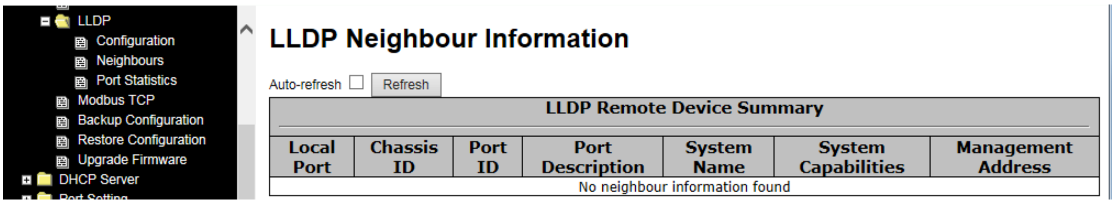
LLDP Port Configuration

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

Label	Description
Tx Interval	The time between LLDP transmits in seconds. The switch periodically transmits LLDP frames to its neighbours for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds. The default is 30 seconds.
Port	The switch port number to which the following settings will be applied.
Mode	Indicates the selected LLDP mode: **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 displayed table contains a row for each port on which an LLDP neighbour is detected.



LLDP Neighbour Information

Auto-refresh □ Refresh

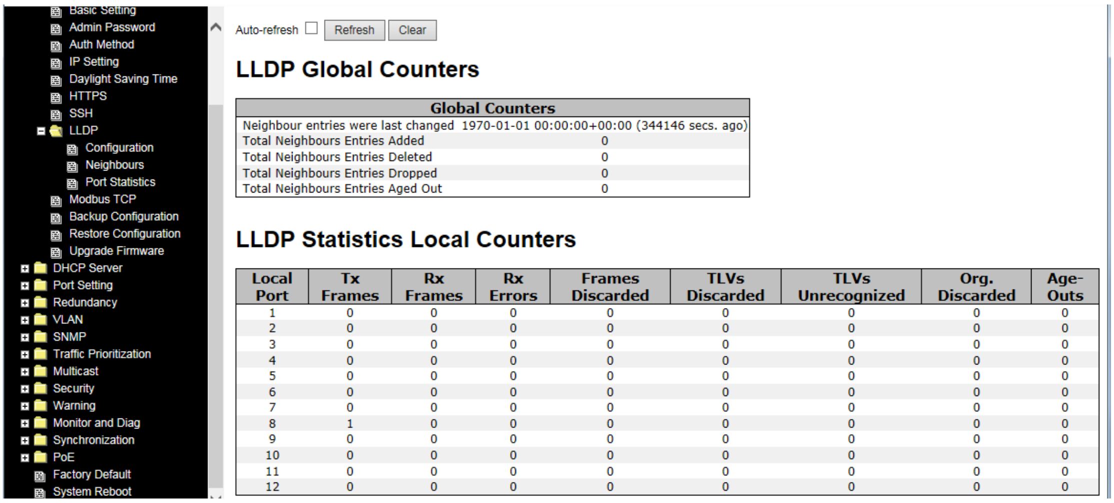
LLDP Remote Device Summary						
Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
No neighbour information found						

The columns include the following information:

Label	Description
Local Port	The port that you use to transmits and receives LLDP frames.
Chassis ID	The identification number of the neighbor sending out the LLDP frames.
Remote Port ID	The identification of the neighbor port.
System Name	The name advertised by the neighbor.
Port Description	The description of the port advertised by the neighbor.
System Capabilities	Description of the neighbor's capabilities. The capabilities include: 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

LLDP Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refer to per port counters for the currently selected switch.



LLDP Global Counters

Global Counters	
Neighbour entries were last changed	1970-01-01 00:00:00+00:00 (344146 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	1	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

LLDP 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

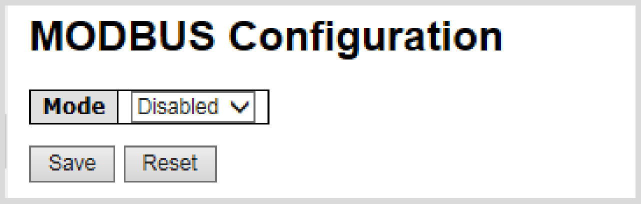
LLDP Local Counters

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 LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" in the LLDP

	standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (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	If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.
Age-Outs	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.
Refresh	Click to refresh the page immediately
Clear	Click to clear the local counters. All counters (including global counters) are cleared upon reboot.
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals

5.1.9 Modbus TCP

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



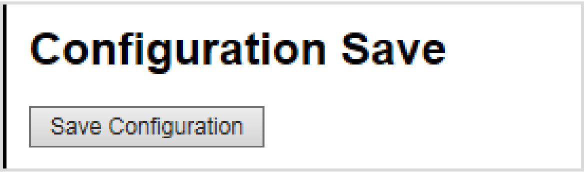
MODBUS Configuration

Mode: Disabled

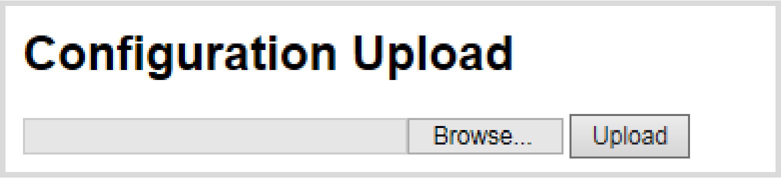
Label	Description
Mode	Disable or enable Modbus function. (Disabled by default.)

5.1.10 Backup/Restore Configurations

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



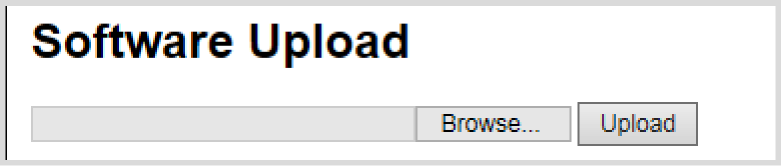
Configuration Save



Configuration Upload

5.1.11 Upgrade Firmware

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



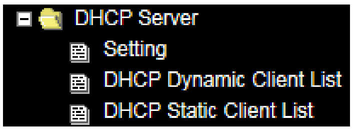
Software Upload

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

After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

Warning: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress.
Do not restart or power off the device at this time or the switch may fail to function afterwards.

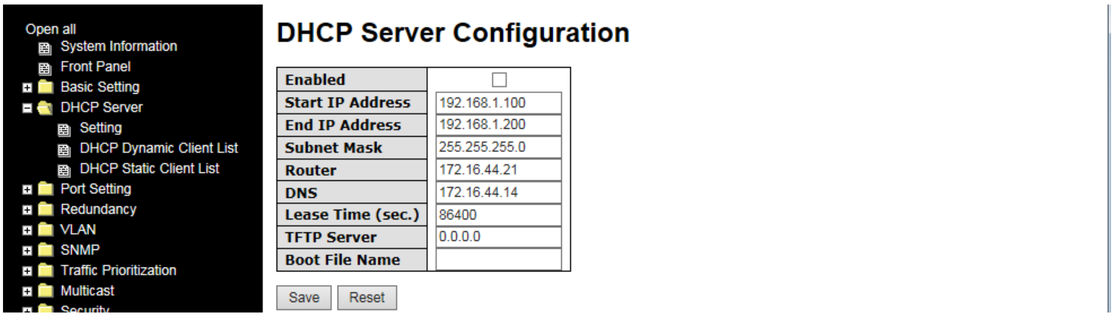
5.2 DHCP Server



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

5.2.1 Basic Settings

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

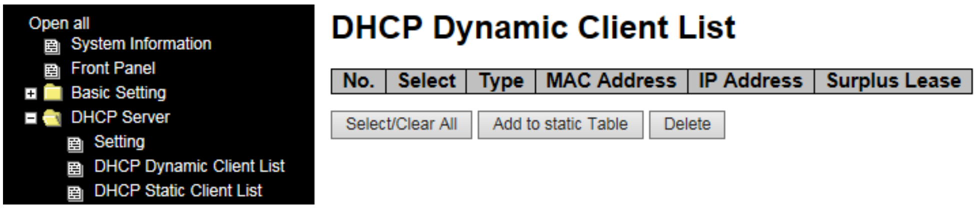


DHCP Server Configuration

Enabled	□
Start IP Address	192.168.1.100
End IP Address	192.168.1.200
Subnet Mask	255.255.255.0
Router	172.16.44.21
DNS	172.16.44.14
Lease Time (sec.)	86400
TFTP Server	0.0.0.0
Boot File Name	

5.2.2 Dynamic Client List

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

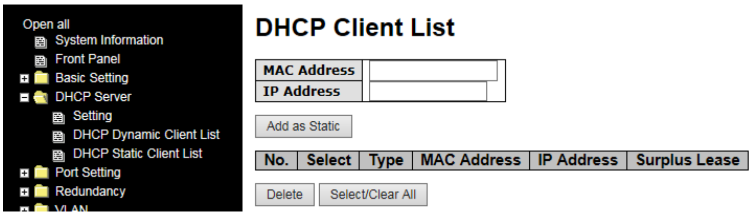


DHCP Dynamic Client List

No.	Select	Type	MAC Address	IP Address	Surplus Lease

5.2.3 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	

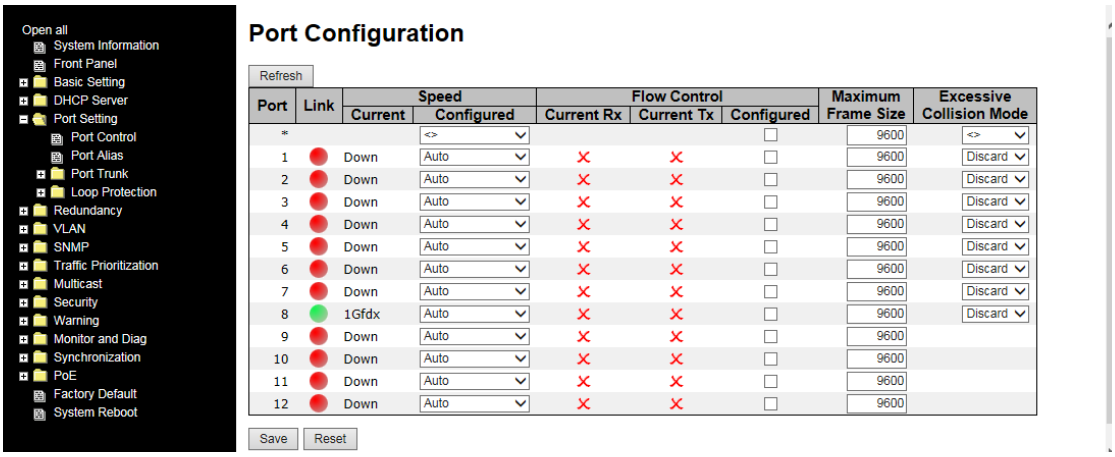
No.	Select	Type	MAC Address	IP Address	Surplus Lease

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

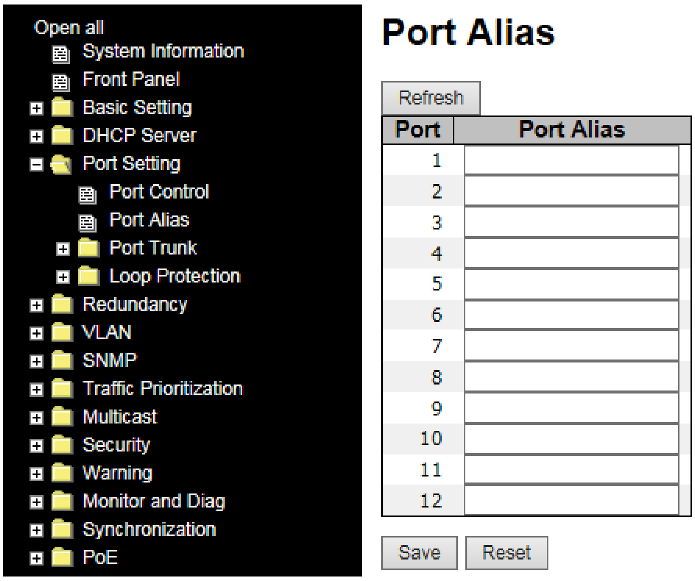
Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode
		Current	Configured	Current Rx	Current Tx	Configured		
*			<>			□	9600	<>
1	🔴	Down	Auto	✕	✕	□	9600	Discard
2	🔴	Down	Auto	✕	✕	□	9600	Discard
3	🔴	Down	Auto	✕	✕	□	9600	Discard
4	🔴	Down	Auto	✕	✕	□	9600	Discard
5	🔴	Down	Auto	✕	✕	□	9600	Discard
6	🔴	Down	Auto	✕	✕	□	9600	Discard
7	🔴	Down	Auto	✕	✕	□	9600	Discard
8	🟢	1Gfdx	Auto	✕	✕	□	9600	Discard
9	🔴	Down	Auto	✕	✕	□	9600	
10	🔴	Down	Auto	✕	✕	□	9600	
11	🔴	Down	Auto	✕	✕	□	9600	
12	🔴	Down	Auto	✕	✕	□	9600	

Label	Description
Port	This is the logical port number for this row.
Link	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
Current Link Speed	Indicates the current link speed of the port.
Configured Link Speed	The drop-down list provides available link speed options for a given switch port. Selects any available link speed for the given switch port. Only speeds supported by the specific port are shown. Possible speeds are: **`Disabled`** - Disables the switch port operation. **`Auto`** - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner. **`10Mbps HDX`** - Forces the cu port in 10Mbps half duplex mode. **`10Mbps FDX`** - Forces the cu port in 10Mbps full duplex mode. **`100Mbps HDX`** - Forces the cu (Copper) port to 100Mbps half duplex mode. **`100Mbps FDX`** - Forces the cu port in 100Mbps full duplex mode. **`1Gbps FDX`** - Forces the port in 1Gbps full duplex

	<> configures all ports
Flow Control	When **Auto** is selected for the speed, the flow control will be negotiated to the capacity advertised by the link partner. When a fixed-speed setting is selected, that is what is used. **Current Rx** indicates whether pause frames on the port are obeyed, and **Current Tx** indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last auto-negotiation. You can check the Configured column to use flow control. This setting is related to the setting of **Configured Link Speed**.
Maximum Frame	You can enter the maximum frame size allowed for the switch port in this column, including FCS. The allowed range is 1518 bytes to 9600 bytes.
Power Control	Shows the current power consumption of each port in percentage. The **Configured** column allows you to change power saving parameters for each port. **Disabled**: all power savings functions are disabled. **ActiPHY**: link down and power savings enabled. **PerfectReach**: link up and power savings enabled. **Enabled**: both link up and link down power savings enabled.
Excessive Collision Mode	Configure port transmit collision behavior. **Discard**: Discard frame after 16 collisions (default). **Restart**: Restart backoff algorithm after 16 collisions.
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values
Refresh	Click to refresh the page. Any changes made locally will be undone.

5.3.2 Port Alias

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

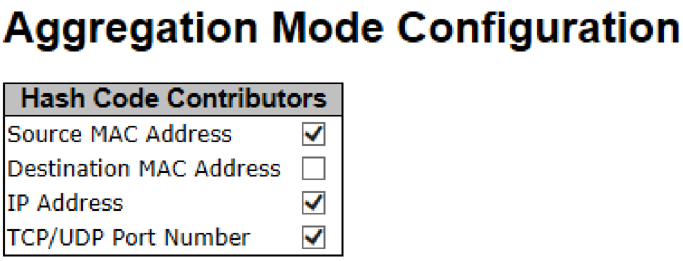


Port Alias

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

5.3.3 Port Trunk

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

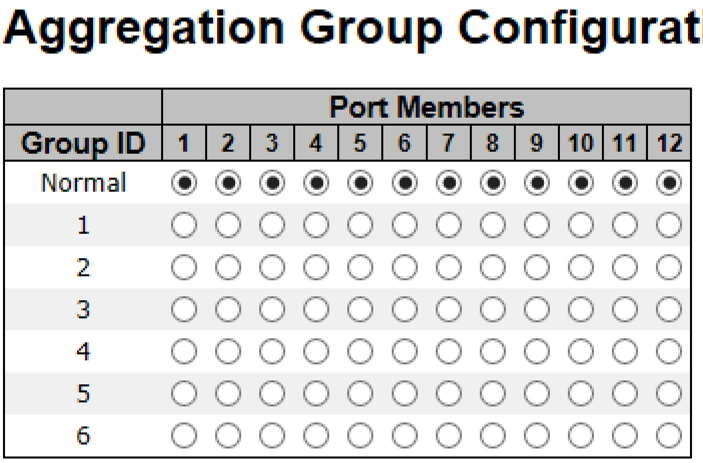


Aggregation Mode Configuration

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

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.



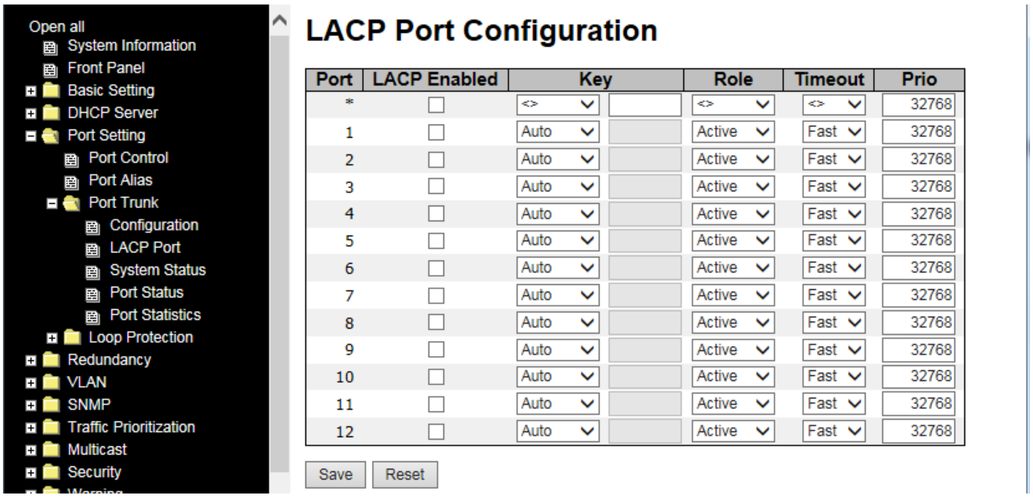
Aggregation Group Configuration

	Port Members											
Group ID	1	2	3	4	5	6	7	8	9	10	11	12
Normal	●	●	●	●	●	●	●	●	●	●	●	●
1	○	○	○	○	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○	○	○	○	○
5	○	○	○	○	○	○	○	○	○	○	○	○
6	○	○	○	○	○	○	○	○	○	○	○	○

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.

5.3.4 LACP

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



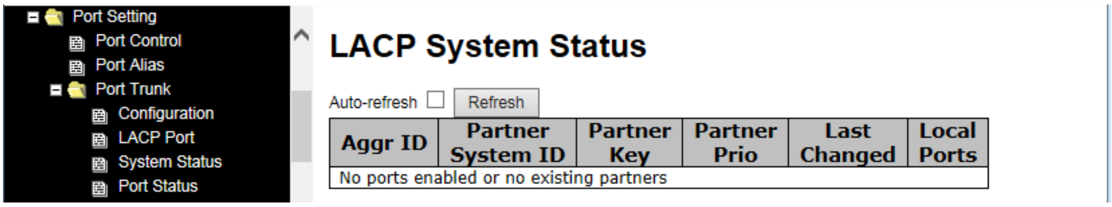
LACP Port Configuration

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
10	□	Auto		Active	Fast	32768
11	□	Auto		Active	Fast	32768
12	□	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*).
Save	Click to save changes.
Reset	Click to undo changes made locally and revert to previous values

LACP System Status

This page provides a status overview for all LACP instances.



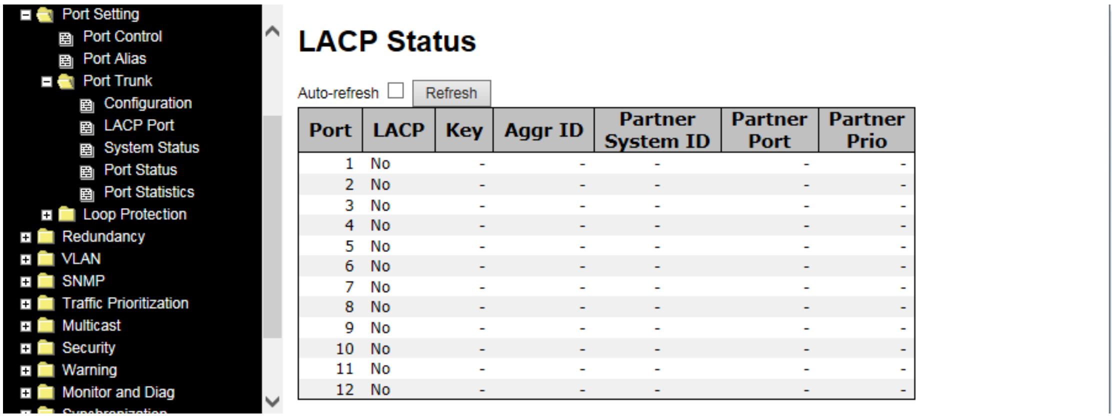
LACP System Status

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.
Last Changed	The time since this aggregation changed.
Local Ports	Indicates which ports belong to the aggregation of the switch/stack. The format is: "**Switch ID:Port**".
Refresh	Click to refresh the page immediately
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals.

LACP Status

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



LACP Status

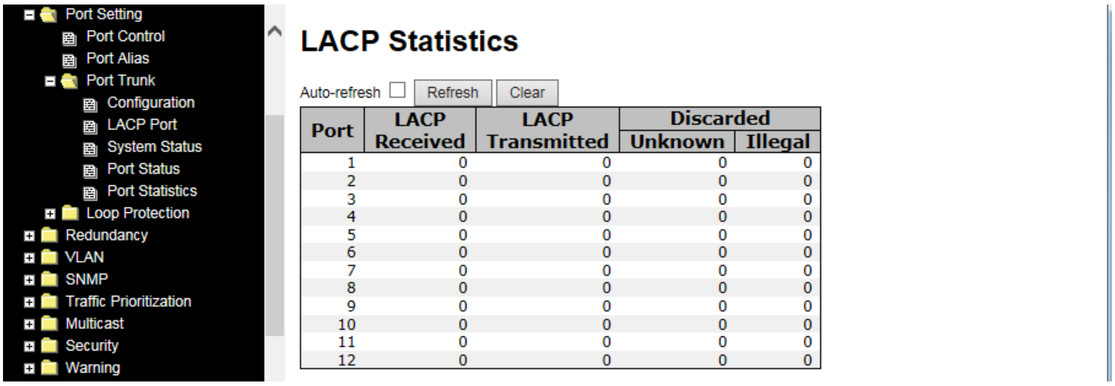
Auto-refresh □

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	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-
11	No	-	-	-	-	-
12	No	-	-	-	-	-

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

LACP Statistics

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



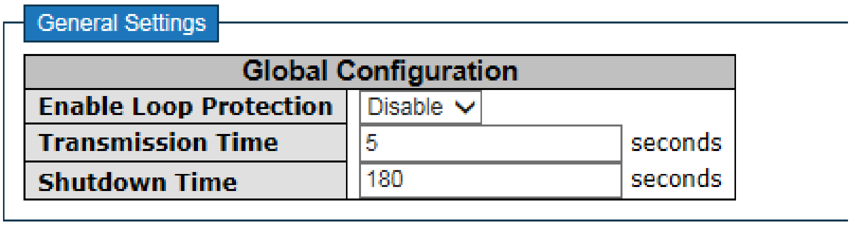
LACP Statistics

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
10	0	0	0	0
11	0	0	0	0
12	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.

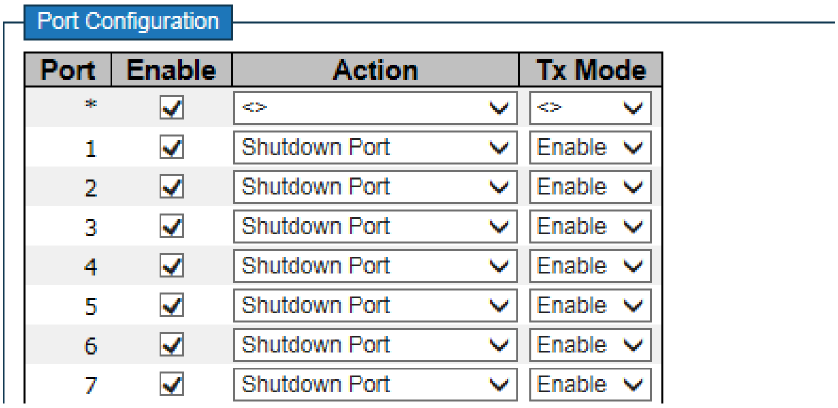
5.3.5 Loop Protection Configuration

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


General Settings

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

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

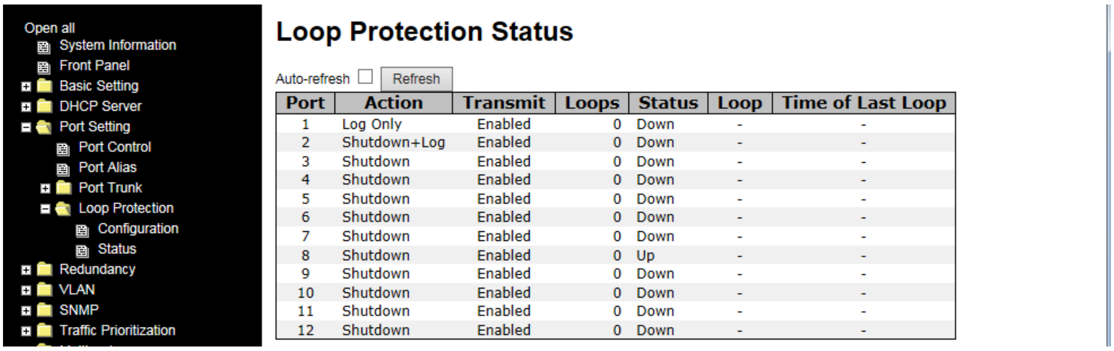

Port Configuration

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

Label	Description
Port	Switch port number.
Enable	Activate loop protection functions (as a whole).
Action	Configures the action to take when a loop is detected. Valid values include **Shutdown Port**, **Shutdown Port** and **Log, or Log Only**.
Tx Mode	Controls whether the port is actively generating loop protection PDUs or only passively look for looped PDUs.

5.3.6 Loop Protection Status

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



Loop Protection Status

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Log Only	Enabled	0	Down	-	-
2	Shutdown+Log	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Up	-	-
9	Shutdown	Enabled	0	Down	-	-
10	Shutdown	Enabled	0	Down	-	-
11	Shutdown	Enabled	0	Down	-	-
12	Shutdown	Enabled	0	Down	-	-

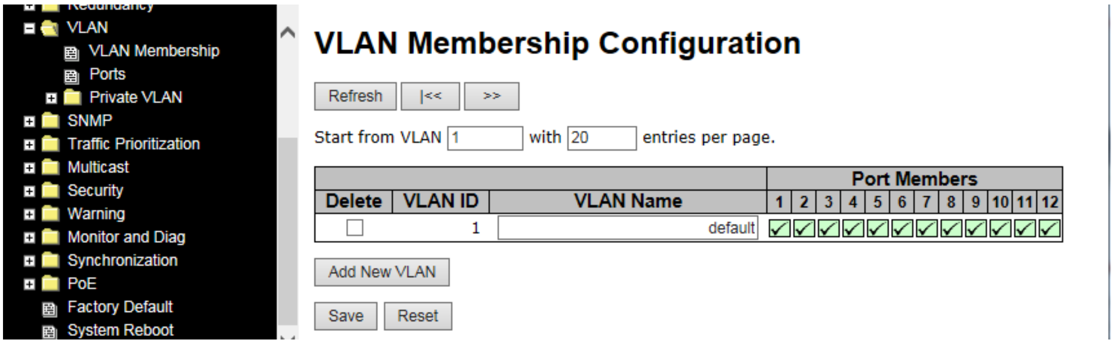
Loop protection port status is described below.

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

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



VLAN Membership Configuration

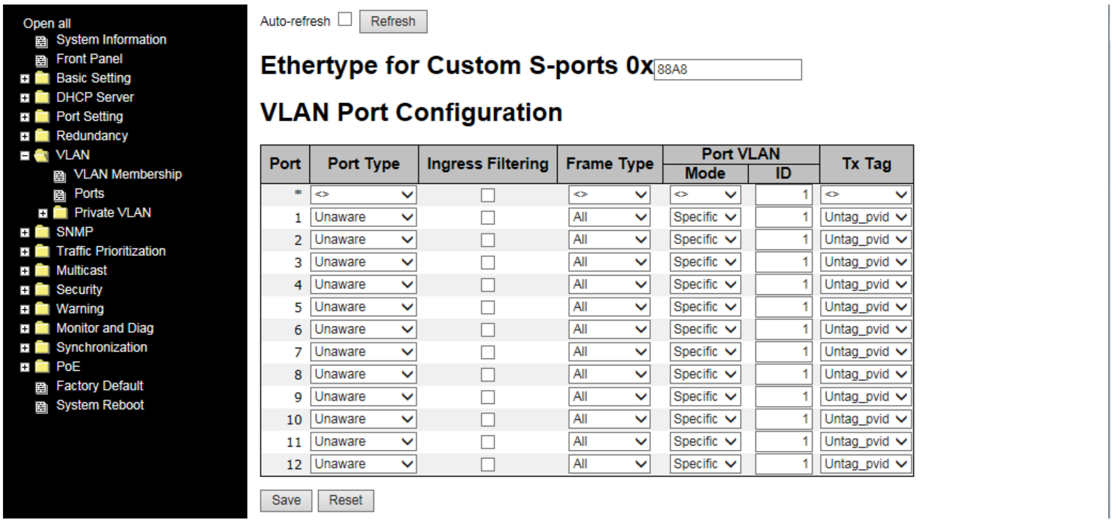
Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	VLAN Name	Port Members											
			1	2	3	4	5	6	7	8	9	10	11	12
□	1	default	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry
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 alpha or numeric characters. At least one alpha character 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	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Add New VLAN	Click to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Valid values for a VLAN ID are **1** through **4095**. 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 on any stack will be deleted when you click Save. Click **Delete** to undo the addition of new VLANs.

5.4.2 Port Configurations

This page is used for configuring the switch port VLAN.



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
11	Unaware	□	All	Specific	1	Untag_pvid
12	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	The switch port number to which the following settings will be applied.
Port type	Port can be one of the following types: **Unaware**, **Customer** (**C-port**), **Service** (**S-port**), **Custom Service** (**S-custom-port**). If port type is **Unaware**, all frames are classified to the port VLAN ID and tags are not removed.
Ingress Filtering	Enable ingress filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame will be discarded. By default, ingress filtering is disabled (no check mark).
Frame Type	Determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port will be discarded. By default, the field is set to All.
Port VLAN Mode	Configures the Port VLAN Mode. The allowed values are **None** or **Specific**. This parameter affects VLAN ingress and egress processing.

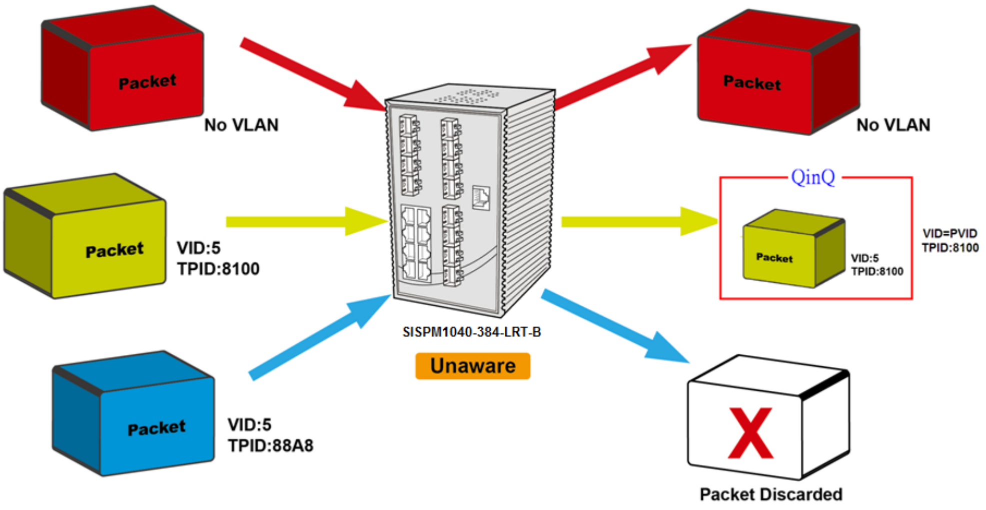
	If **None** is selected, a VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN-aware switches. Tx tag should be set to Untag_pvid when this mode is used. If **Specific** (the default value) is selected, a port VLAN ID can be configured (see below). Untagged frames received on the port are classified to the port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the port VLAN ID, a VLAN tag with the classified VLAN ID 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.

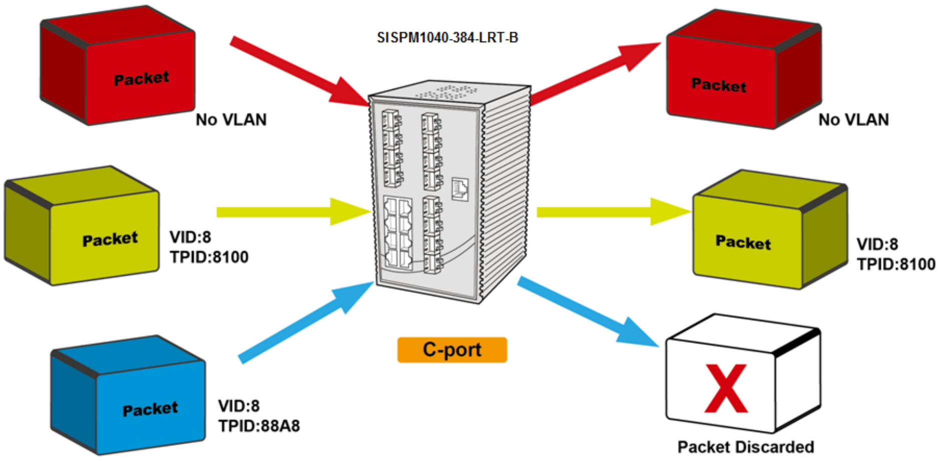
Introduction of Port Types

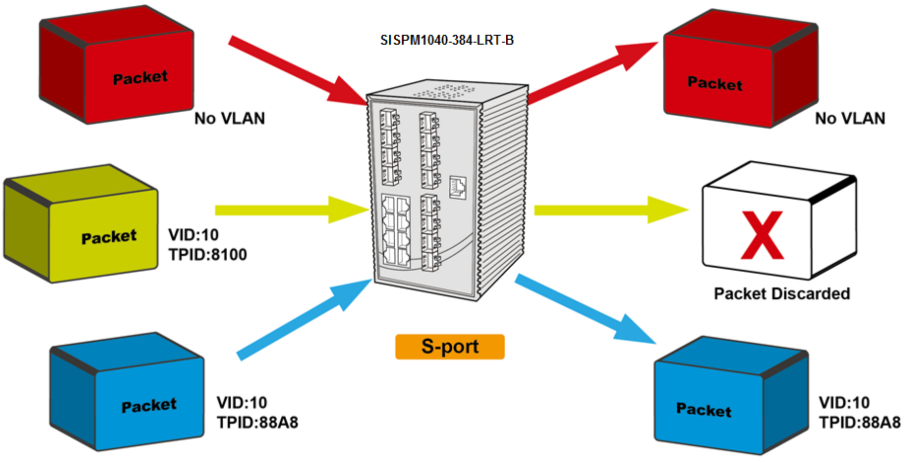
Below is a description of each port type (Unaware, C-port, S-port, and S-custom-port).

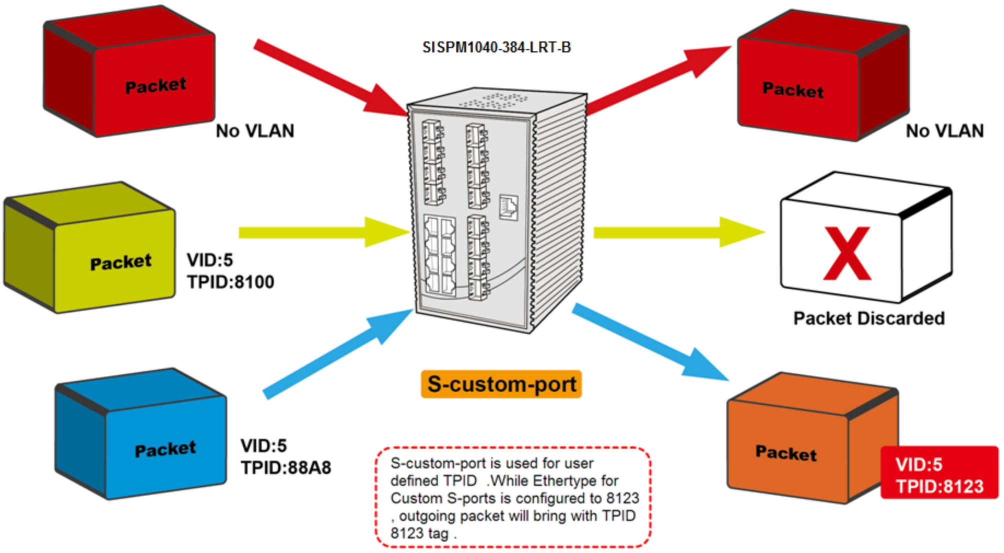
Type	Ingress action	Egress action
Unaware The function of Unaware can be used for 802.1QinQ (*double tag*)	When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded. When the port receives tagged frames: 1. If the tagged frame contains a TPID of 0x8100, 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. 2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of a frame transmitted by C-port will be set to 0x8100.
S-port	When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded. 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 users can set via **Ethertype for Custom S-ports.**

Below are illustrations of the port types:





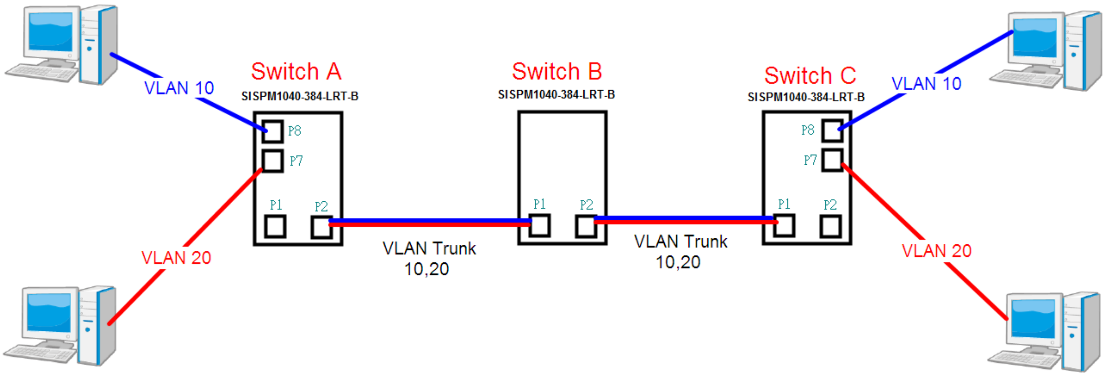




S-custom-port is used for user defined TPID .While Ethertype for Custom S-ports is configured to 8123 , outgoing packet will bring with TPID 8123 tag .

Examples of VLAN Settings

VLAN Access Mode:

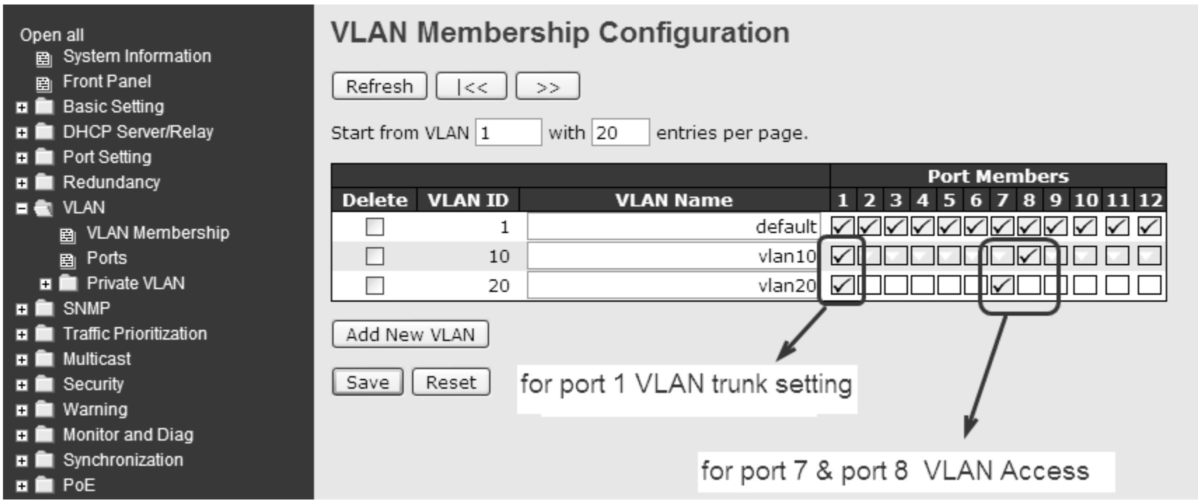


Switch A,

Port 7 is VLAN Access mode = Untagged 20

Port 8 is VLAN Access mode = Untagged 10

Below are the switch settings.



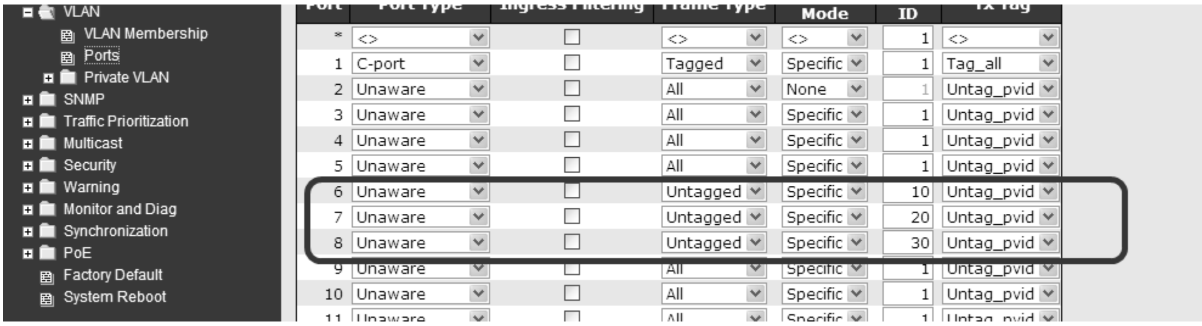
VLAN Membership Configuration

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
□	1	default	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
□	10	vlan10	☑	□	□	□	□	□	□	☑	□	□	□	□
□	20	vlan20	☑	□	□	□	□	□	☑	□	□	□	□	□

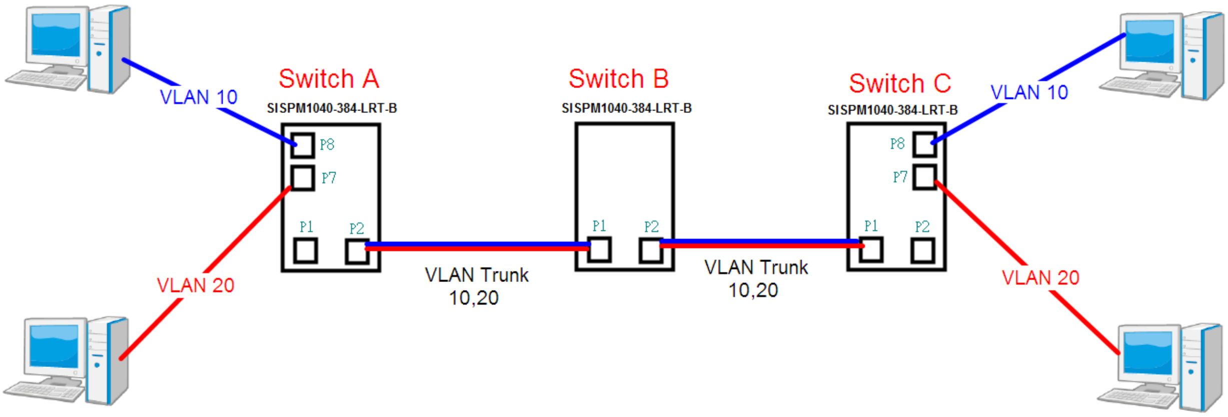
for port 1 VLAN trunk setting

for port 7 & port 8 VLAN Access



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

VLAN 1Q Trunk Mode:

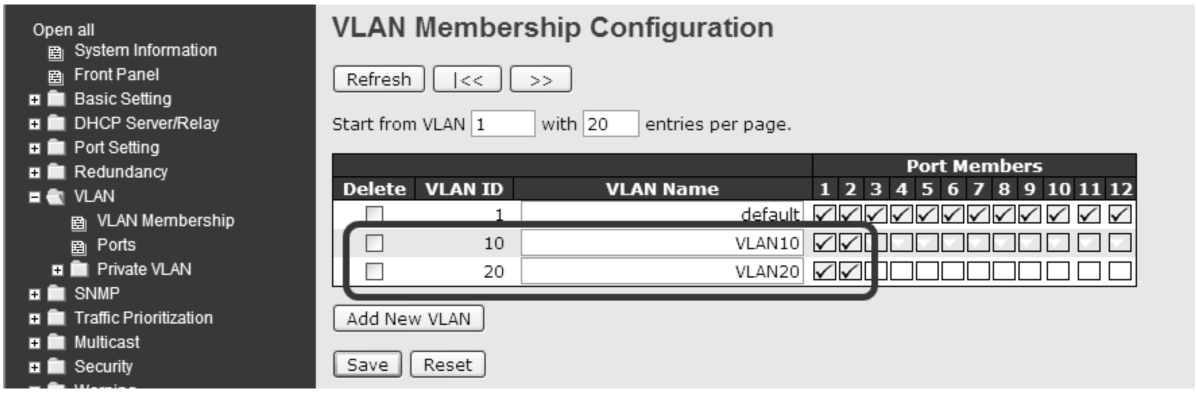


Switch B,

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

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

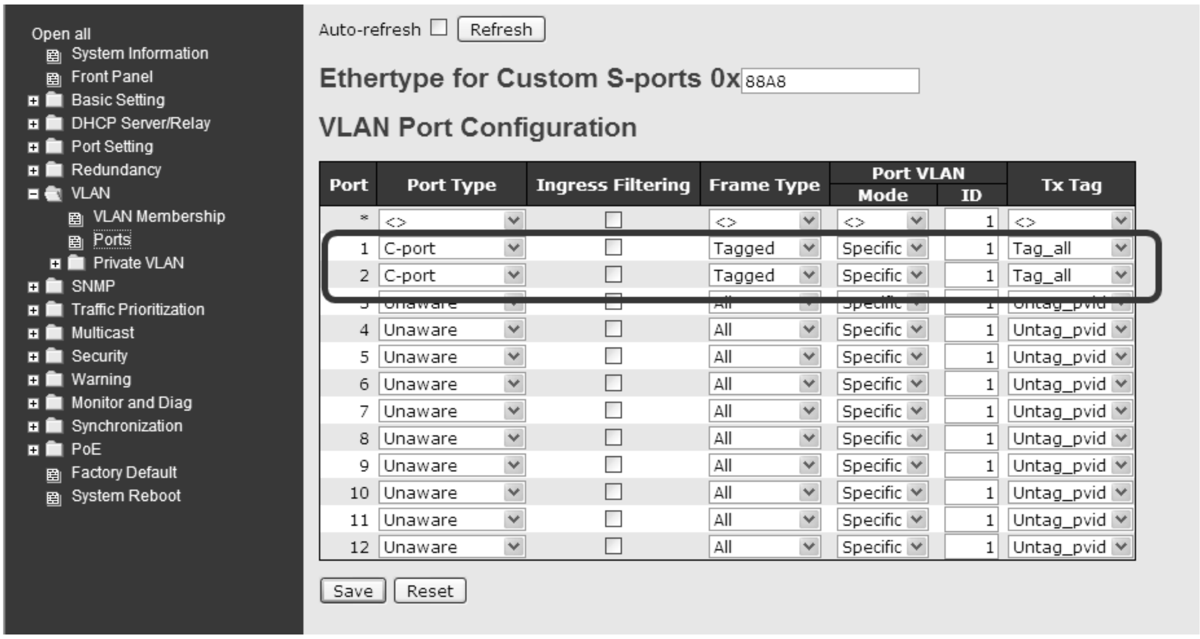
Below are the switch settings.



VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	VLAN Name	Port Members 1	2	3	4	5	6	7	8	9	10	11	12
□	1	default	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
□	10	VLAN10	☑	☑	□	□	□	□	□	□	□	□	□	□
□	20	VLAN20	☑	☑	□	□	□	□	□	□	□	□	□	□



Auto-refresh □

Ethertype for Custom S-ports 0x 88A8

VLAN Port Configuration

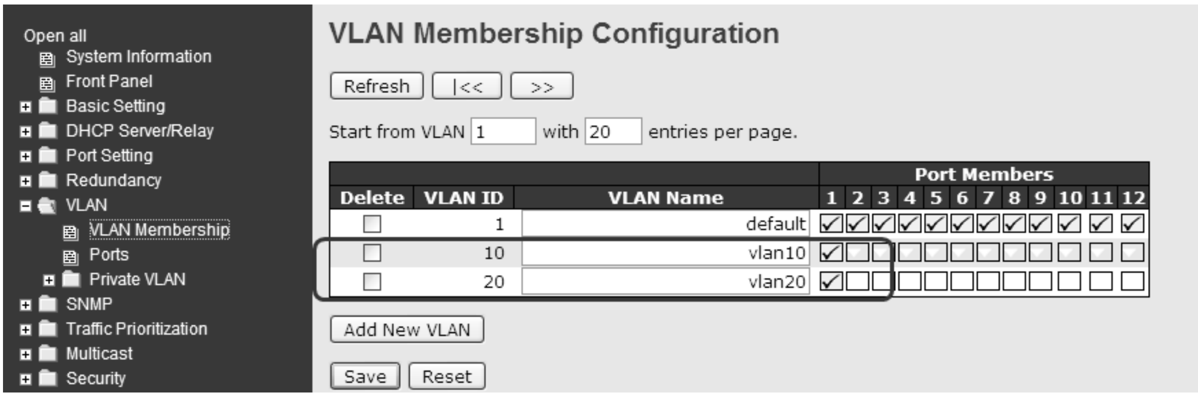
Port	Port Type	Ingress Filtering	Frame Type	Port VLAN Mode	Port VLAN ID	Tx Tag
*	<>	□	<>	<>	1	<>
1	C-port	□	Tagged	Specific	1	Tag_all
2	C-port	□	Tagged	Specific	1	Tag_all
3	Unaware	□	All	Specific	1	Untag_pvid
4	Unaware	□	All	Specific	1	Untag_pvid
5	Unaware	□	All	Specific	1	Untag_pvid
6	Unaware	□	All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

VLAN Hybrid Mode:

Port 1 VLAN Hybrid mode = untagged 10

Tagged 10, 20

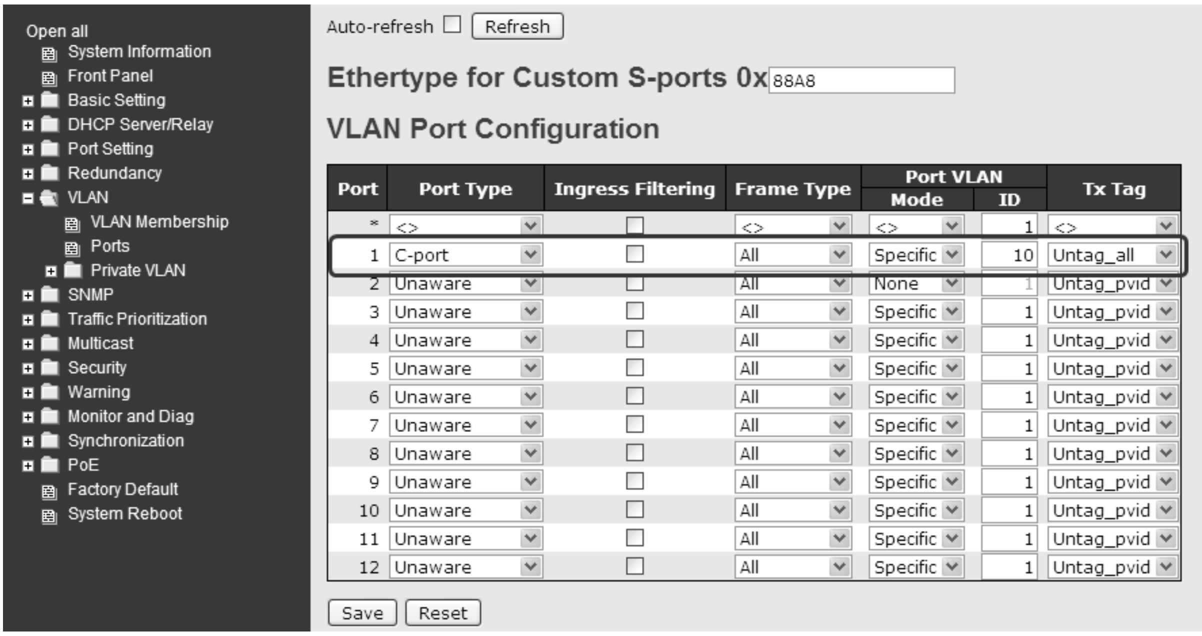
Below are the switch settings.



VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page.

			Port Members											
Delete	VLAN ID	VLAN Name	1	2	3	4	5	6	7	8	9	10	11	12
□	1	default	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
□	10	vlan10	☑	□	□	□	□	□	□	□	□	□	□	□
□	20	vlan20	☑	□	□	□	□	□	□	□	□	□	□	□



Auto-refresh □

Ethertype for Custom S-ports 0x 88A8

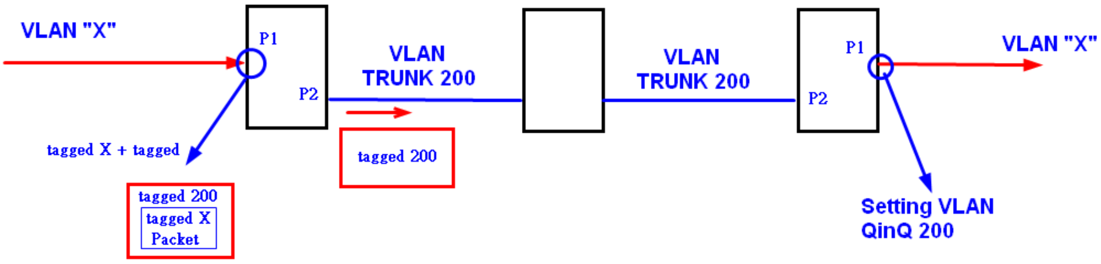
VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN Mode	Port VLAN ID	Tx Tag
*	<>	□	<>	<>	1	<>
1	C-port	□	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
5	Unaware	□	All	Specific	1	Untag_pvid
6	Unaware	□	All	Specific	1	Untag_pvid
7	Unaware	□	All	Specific	1	Untag_pvid
8	Unaware	□	All	Specific	1	Untag_pvid
9	Unaware	□	All	Specific	1	Untag_pvid
10	Unaware	□	All	Specific	1	Untag_pvid
11	Unaware	□	All	Specific	1	Untag_pvid
12	Unaware	□	All	Specific	1	Untag_pvid

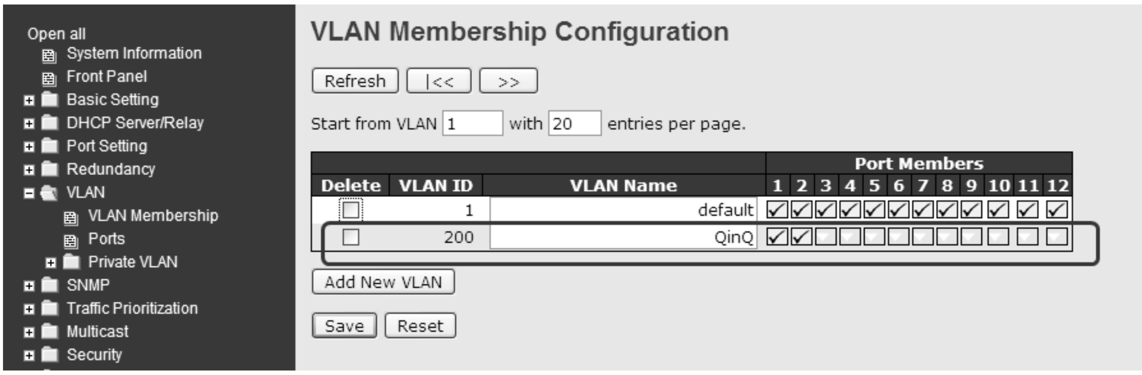
VLAN QinQ Mode:

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

VLAN “X” = Unknown VLAN



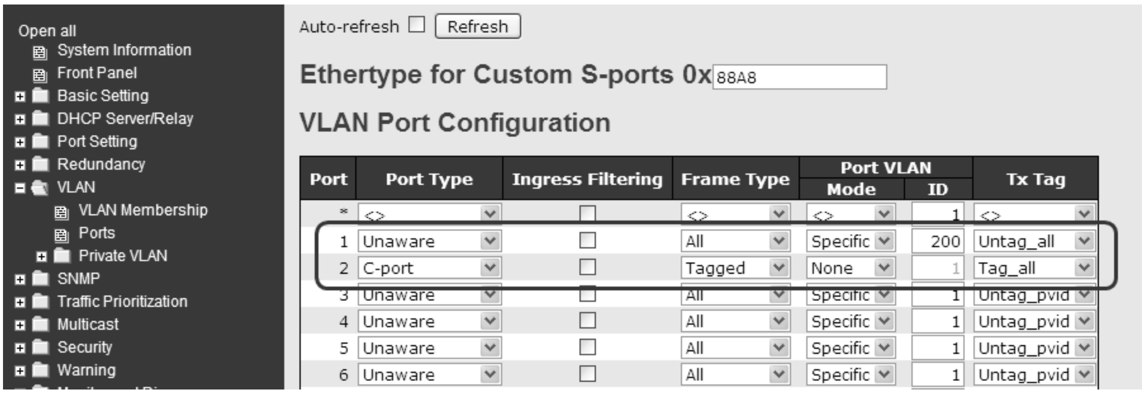
Port 1 VLAN Settings:



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
□	1	default	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
□	200	QinQ	☑	☑	□	□	□	□	□	□	□	□	□	□



Auto-refresh □

Ethertype for Custom S-ports 0x 88A8

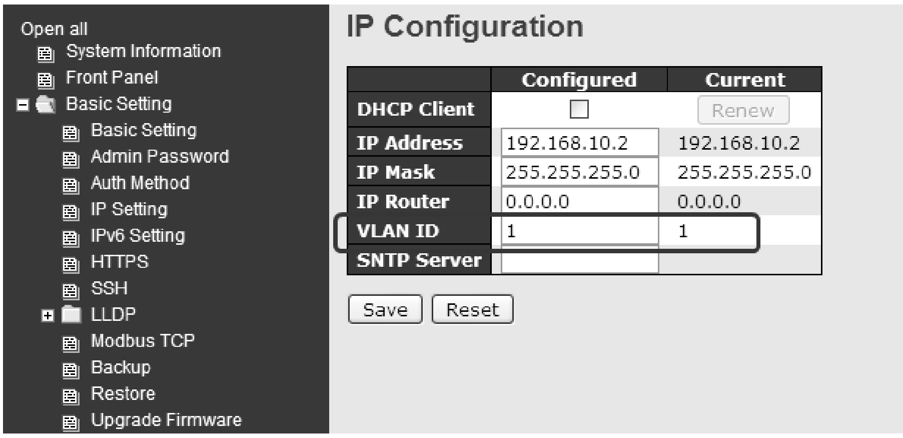
VLAN Port Configuration

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
5	Unaware	□	All	Specific	1	Untag_pvid
6	Unaware	□	All	Specific	1	Untag_pvid

VLAN ID Settings

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

VLAN Settings:

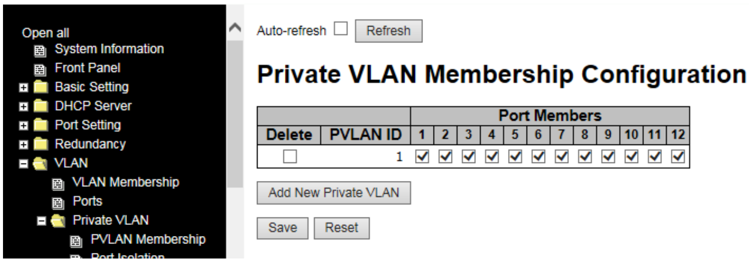


IP Configuration

	Configured	Current
DHCP Client	☐	Renew
IP Address	192.168.10.2	192.168.10.2
IP Mask	255.255.255.0	255.255.255.0
IP Router	0.0.0.0	0.0.0.0
VLAN ID	1	1
SNTP Server		

5.4.3 Private VLAN Membership

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



Private VLAN Membership Configuration

Delete	PVLAN ID	Port Members											
		1	2	3	4	5	6	7	8	9	10	11	12
☐	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

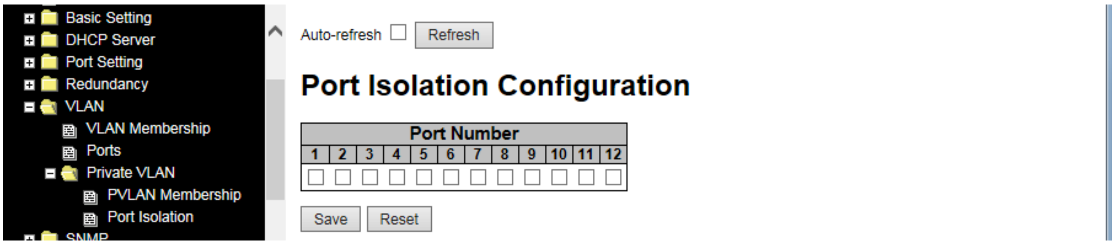
Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Private VLAN ID	Indicates the ID of this particular private VLAN.
MAC Address	The MAC address for the entry.
Port Members	A row of check boxes for each port is displayed for each private VLAN ID. You can check the box to include a port in a private VLAN. To remove or exclude the port from the private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Adding a New Static	Click **Add new Private VLAN** to add a new private VLAN ID. An

Entry	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.

5.4.4 Port Isolation

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

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



Port Isolation Configuration

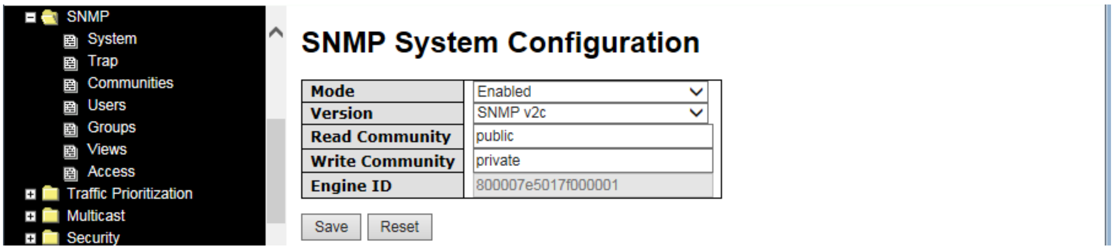
Port Number											
1	2	3	4	5	6	7	8	9	10	11	12
□	□	□	□	□	□	□	□	□	□	□	□

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

5.5 SNMP

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

5.5.1 SNMP System Configuration



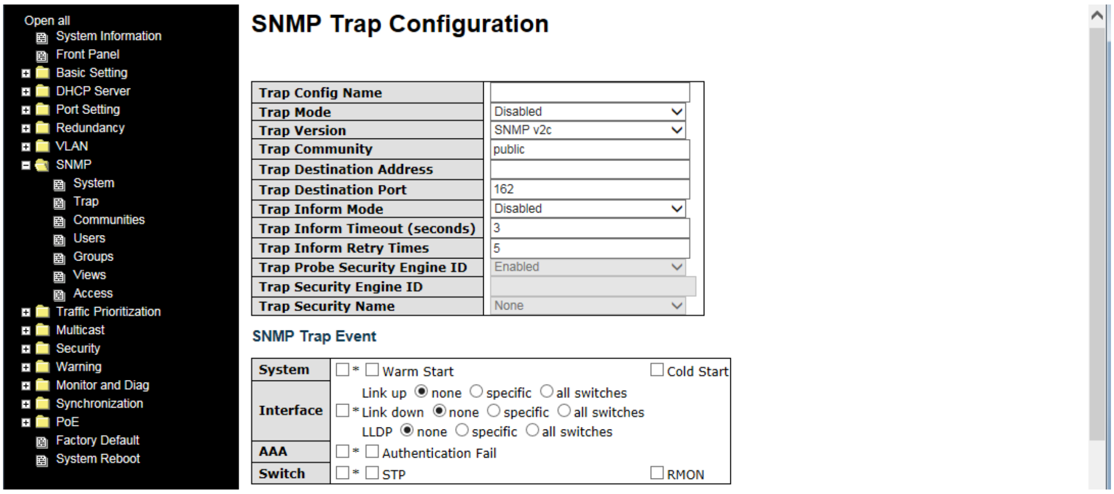
SNMP System Configuration

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, and only ASCII characters from 33 to 126 are allowed. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 uses USM for authentication and privacy and the community string will be associated with SNMPv3 community table.
Write Community	Indicates the write community string to permit access to SNMP agent. The allowed string length is 0 to 255, and only ASCII characters from 33 to 126 are allowed. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 uses USM for authentication and privacy and the community string will be associated with SNMPv3 community table.
Engine ID	Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

5.5.2 SNMP Trap Configuration

Click the Add New Entry button to display the configurable parameters.



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

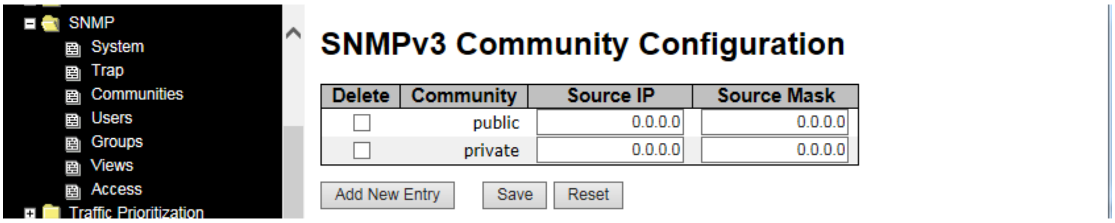
System	□ * □ Warm Start □ Cold Start
Interface	□ * Link up ● none ○ specific ○ all switches Link down ● none ○ specific ○ all switches LLDP ● none ○ specific ○ all switches
AAA	□ * □ Authentication Fail
Switch	□ * □ STP □ RMON

Label	Description
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. Versions can include: **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 to 255, and only ASCII characters from 33 to 126 are allowed.
Trap Destination Address	Indicates the SNMP trap destination address
Trap Destination IPv6 Address	Provides the trap destination IPv6 address of this switch. IPv6 address consists of 128 bits represented as eight groups of four hexadecimal digits with a colon separating each field (:). For example, in 'fe80::215:c5ff:fe03:4dc7', the symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also uses a following legally IPv4 address. For example, '::192.1.2.34'.
Trap Authentication Failure	Indicates the SNMP entity is permitted to generate authentication failure traps. Possible modes include: **Enabled**: enable SNMP trap authentication failure. **Disabled**: disable SNMP trap authentication failure

Trap Link-up and Link-down	Indicates the SNMP trap link-up and link-down mode. Possible modes include: **Enabled**: enable SNMP trap link-up and link-down mode **Disabled**: disable SNMP trap link-up and link-down mode
Trap Inform Mode	Indicates the SNMP trap inform mode. Possible modes include: **Enabled**: enable SNMP trap inform mode. **Disabled**: disable SNMP trap inform mode.
Trap Inform Timeout(seconds)	Configures the SNMP trap inform timeout. The allowed range is **0** to **2147**.
Trap Inform Retry Times	Configures the retry times for SNMP trap inform. The allowed range is **0** to **255**.

5.5.2 SNMP Community Configurations

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



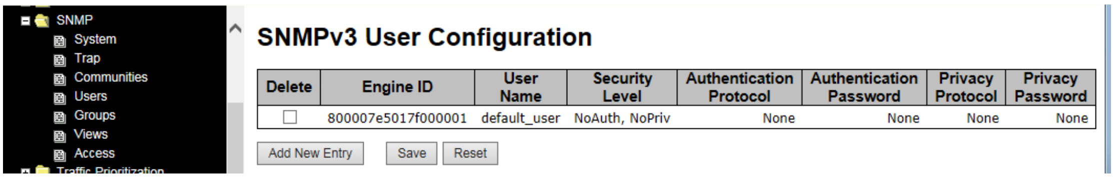
SNMPv3 Community Configuration

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.

5.5.3 SNMP User Configurations

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



SNMPv3 User Configuration

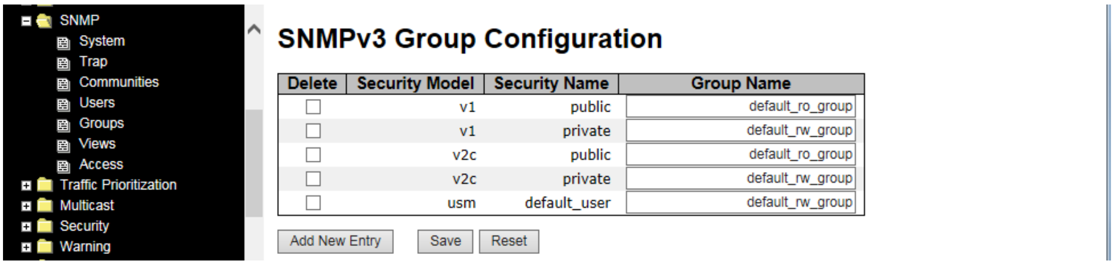
Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
□	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

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 between **10** and **64** hexadecimal digits, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses User-based Security Model (USM) for message security and View-based Access Control Model (VACM) for access control. For the USM entry, the **usmUserEngineID** and **usmUserName** are the entry keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID is the same as system engine ID, then it is local user; otherwise it's remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is **1** to **32**, and only ASCII characters from 33 to 126 are allowed.
Security Level	Indicates the security model that this entry should belong to. Possible security models include: **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 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. Only ASCII characters from 33 to 126 are allowed.
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols include: **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 to 32, and only ASCII characters from 33 to 126 are allowed.

5.5.4 SNMP Group Configurations

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



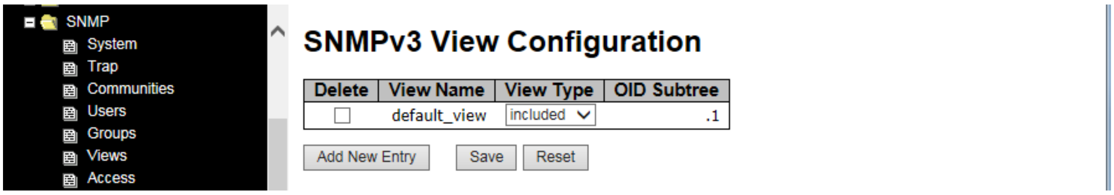
SNMPv3 Group Configuration

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. Security models can include: **v1**: Reserved for SNMPv1. **v2c**: Reserved for SNMPv2c. **usm**: User-based Security Model (USM).
Security Name	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.

5.5.5 SNMP View Configurations

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



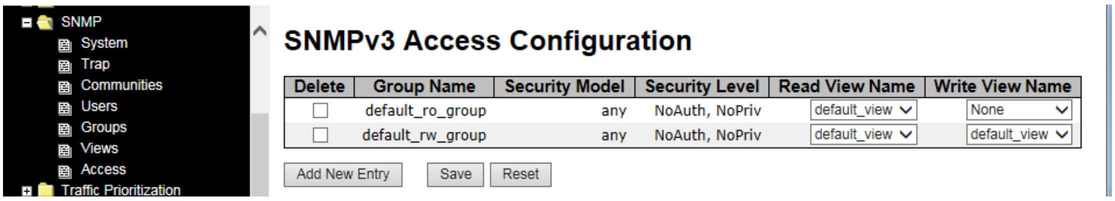
SNMPv3 View Configuration

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 to 32, and only ASCII characters from 33 to 126 are allowed.
View Type	Indicates the view type that this entry should belong to. View Types can 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 with another entry whose view type is **Included, and** its OID subtree oversteps the **Excluded** entry.
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk (*).

5.5.6 SNMP Access Configurations

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



SNMPv3 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

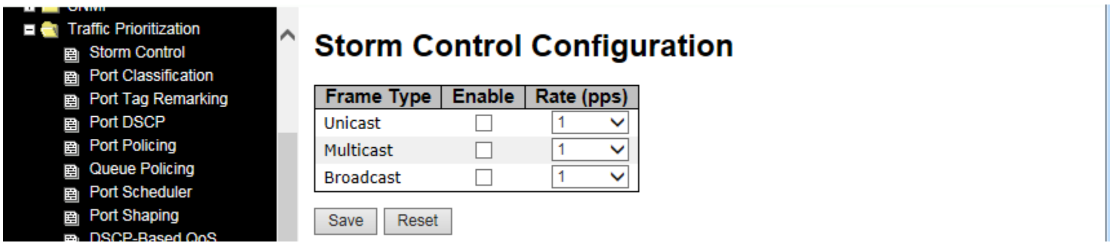
Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
Security Model	Indicates the security model that this entry should belong to. Security Models can 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. Security models can include: **NoAuth, NoPriv**: no authentication and no privacy **Auth, NoPriv**: Authentication and no privacy **Auth, Priv**: Authentication and privacy
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
Write View Name	The name of the MIB view defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.

5.6 Traffic Prioritization

5.6.1 Storm Control

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

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



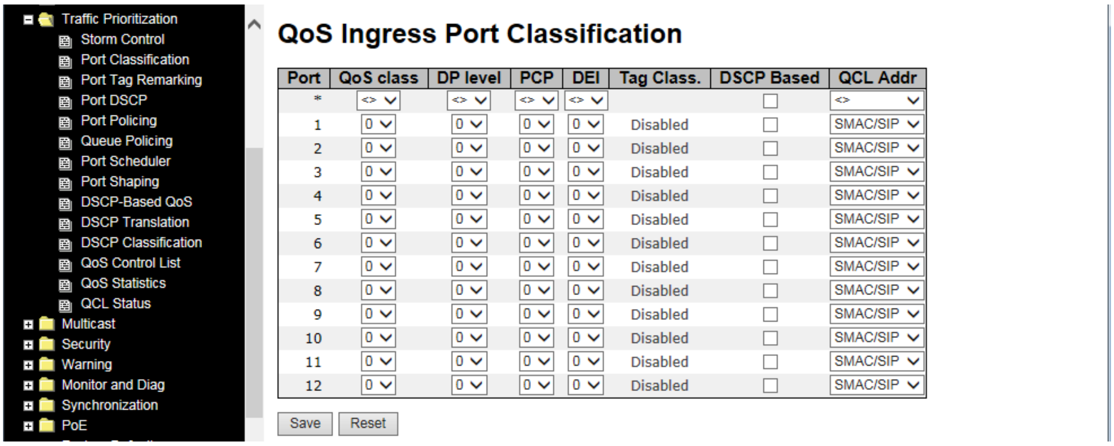
Storm Control Configuration

Frame Type	Enable	Rate (pps)
Unicast	□	1
Multicast	□	1
Broadcast	□	1

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

5.6.2 Port Classification

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



QoS Ingress Port Classification

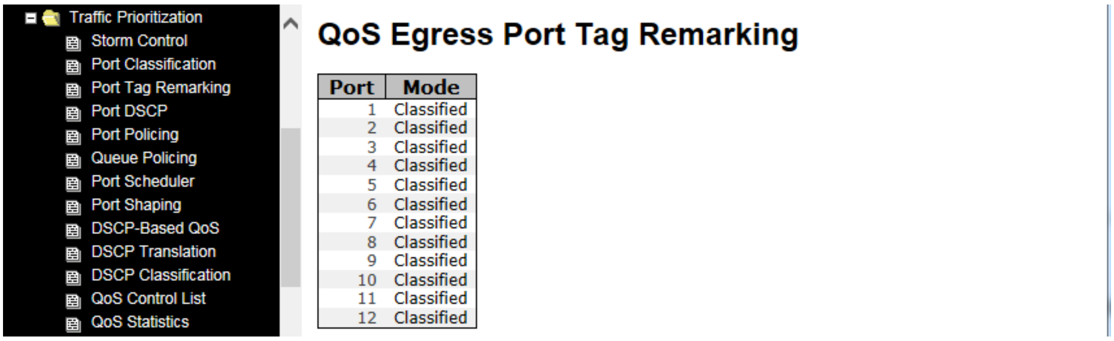
Port	QoS class	DP level	PCP	DEI	Tag Class.	DSCP Based	QCL Addr
*	<>	<>	<>	<>		□	<>
1	0	0	0	0	Disabled	□	SMAC/SIP
2	0	0	0	0	Disabled	□	SMAC/SIP
3	0	0	0	0	Disabled	□	SMAC/SIP
4	0	0	0	0	Disabled	□	SMAC/SIP
5	0	0	0	0	Disabled	□	SMAC/SIP
6	0	0	0	0	Disabled	□	SMAC/SIP
7	0	0	0	0	Disabled	□	SMAC/SIP
8	0	0	0	0	Disabled	□	SMAC/SIP
9	0	0	0	0	Disabled	□	SMAC/SIP
10	0	0	0	0	Disabled	□	SMAC/SIP
11	0	0	0	0	Disabled	□	SMAC/SIP
12	0	0	0	0	Disabled	□	SMAC/SIP

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 affect if the port is VLAN unaware. Tagged frames received on VLAN-unaware ports are always classified to the default QoS class and DP level.
DSCP Based	Click to enable DSCP-based QoS Ingress Port Classification.

5.6.3 Port Tag Remaking

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



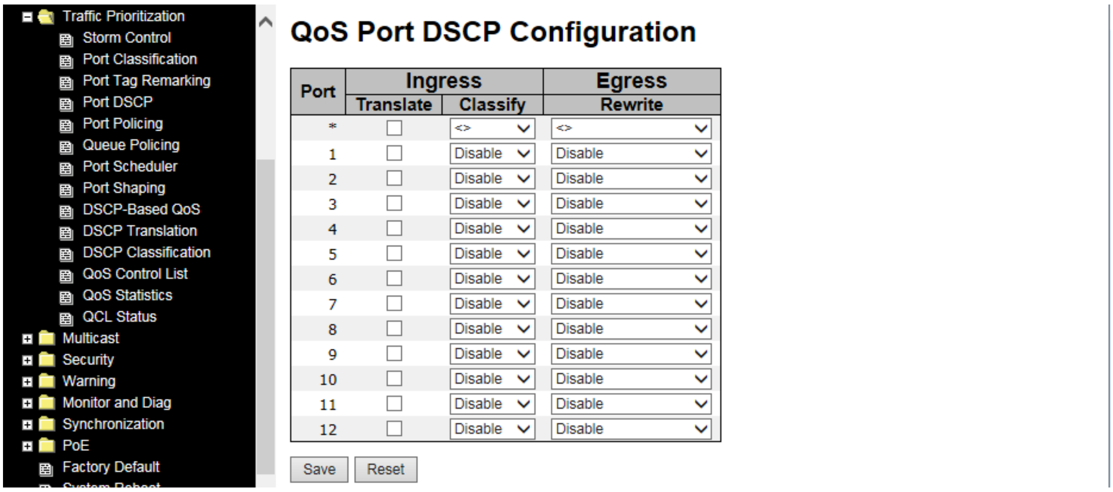
QoS Egress Port Tag Remarking

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

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

5.6.4 Port DSCP

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



QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	☐	<>	<>
1	☐	Disable	Disable
2	☐	Disable	Disable
3	☐	Disable	Disable
4	☐	Disable	Disable
5	☐	Disable	Disable
6	☐	Disable	Disable
7	☐	Disable	Disable
8	☐	Disable	Disable
9	☐	Disable	Disable
10	☐	Disable	Disable
11	☐	Disable	Disable
12	☐	Disable	Disable

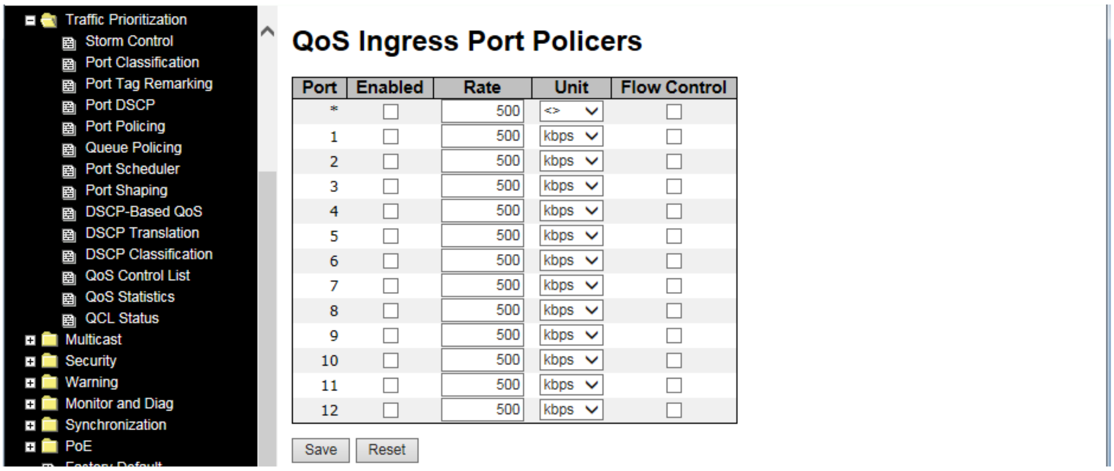
Label	Description
Port	Shows the list of ports for which you can configure DSCP Ingress and Egress settings.
Ingress	In **Ingress** settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: **Translate:** check to enable the function. **Classify:** includes 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	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 Policing

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

Port Policing

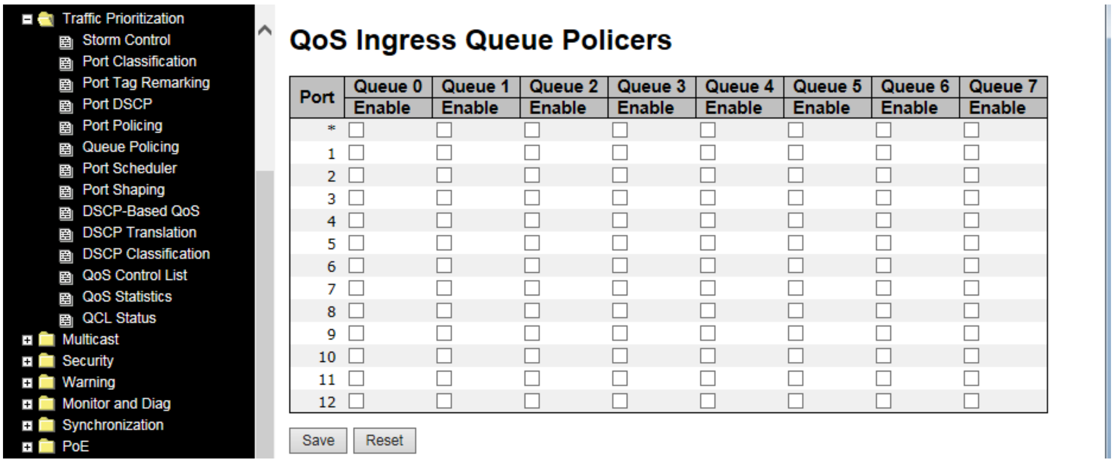


QoS Ingress Port Policers

Port	Enabled	Rate	Unit	Flow Control
*	□	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	□
10	□	500	kbps	□
11	□	500	kbps	□
12	□	500	kbps	□

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

Queue Policing



QoS Ingress Queue Policers

Port	Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable
*	□	□	□	□	□	□	□	□
1	□	□	□	□	□	□	□	□
2	□	□	□	□	□	□	□	□
3	□	□	□	□	□	□	□	□
4	□	□	□	□	□	□	□	□
5	□	□	□	□	□	□	□	□
6	□	□	□	□	□	□	□	□
7	□	□	□	□	□	□	□	□
8	□	□	□	□	□	□	□	□
9	□	□	□	□	□	□	□	□
10	□	□	□	□	□	□	□	□
11	□	□	□	□	□	□	□	□
12	□	□	□	□	□	□	□	□

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

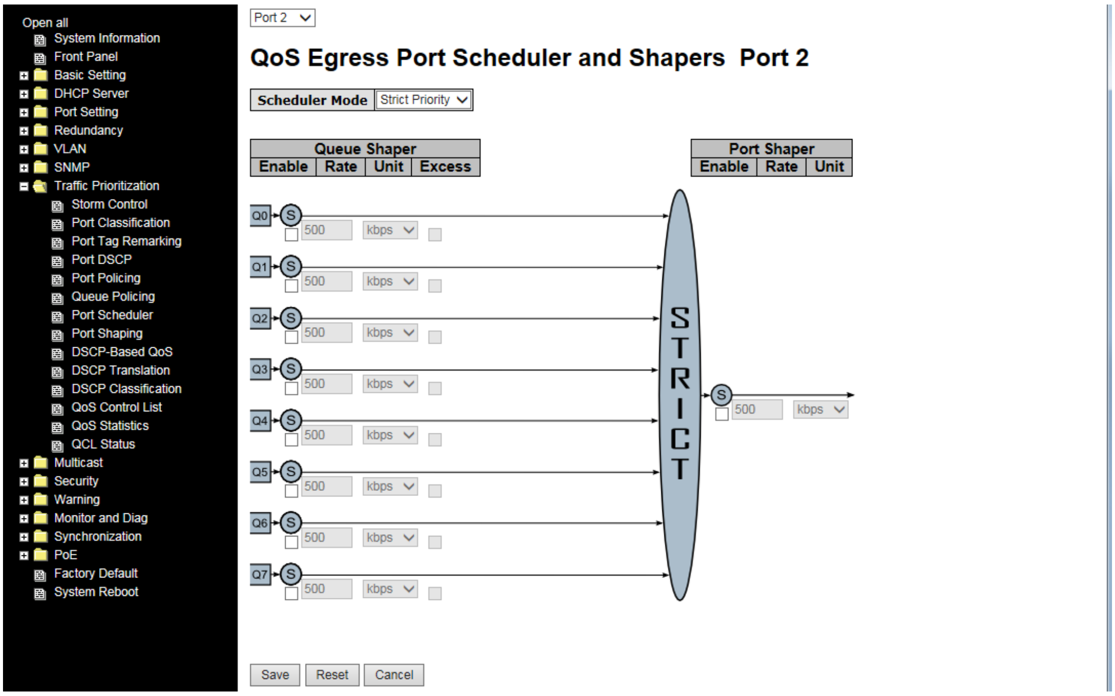
5.6.6 Scheduling and Shaping

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

QoS Egress Port Scheduler and Shaper

Strict Priority

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



QoS Egress Port Scheduler and Shapers Port 2

Scheduler Mode: Strict Priority

Q0–Q7: □ 500 kbps □

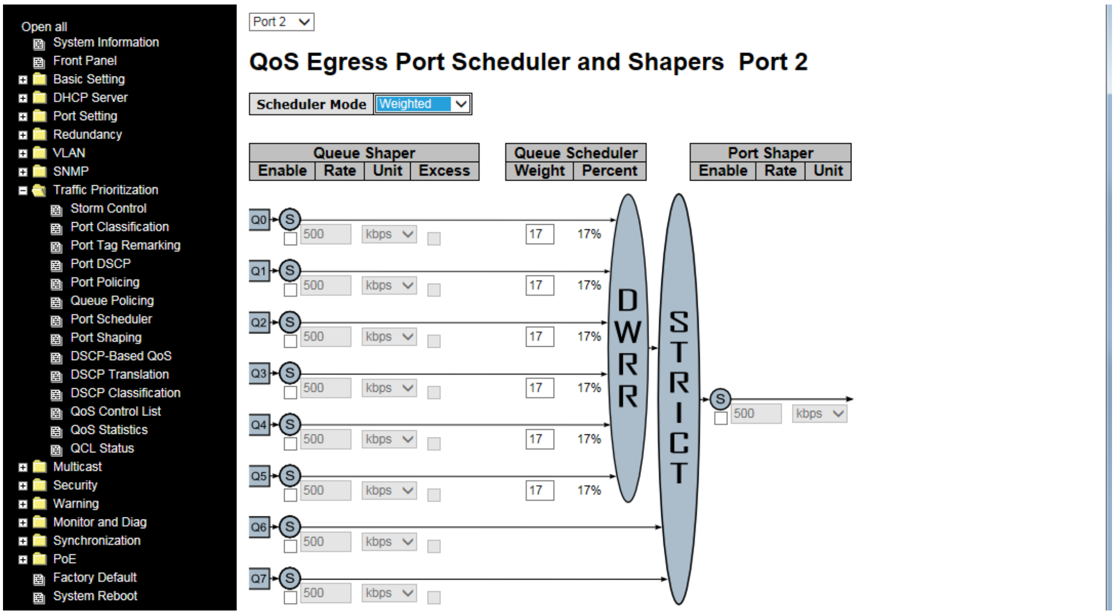
Port Shaper: □ 500 kbps

Label	Description
Scheduler Mode	Two scheduling modes are available: **Strict Priority** or **Weighted**.
Queue Shaper Enable	Check to enable queue shaper for individual switch ports
Queue Shaper Rate	Configures the rate of each queue shaper. The default value is **500**. This value is restricted to 100 to 1000000 whn the **Unit** is **kbps**", and it is restricted to 1 to 3300 when the **Unit** is **Mbps**.
Queues Shaper Unit	Configures the rate for each queue shaper. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps**, and it is restricted to 1 to 3300 when the **Unit** is **Mbps**.
Queue Shaper Excess	Allows the queue to use excess bandwidth
Port Shaper Enable	Check to enable port shaper for individual switch ports
Port Shaper Rate	Configures the rate of each port shaper. The default value is **500** This value is restricted to 100 to 1000000 when the **Unit** is **kbps**,

	and it is restricted to 1 to 3300 when the **Unit** is **Mbps**.
Port Shaper Unit	Configures the unit of measurement for each port shaper rate as **kbps** or **Mbps**. The default value is **kbps**.

Weighted

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



Port 2

QoS Egress Port Scheduler and Shapers Port 2

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	□		

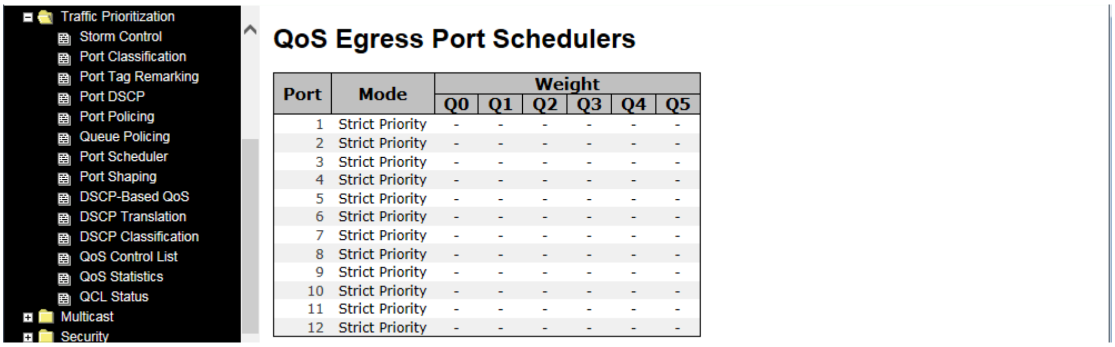
Port Shaper: Enable □ Rate 500 Unit kbps

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

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

5.6.7 Port Scheduler

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



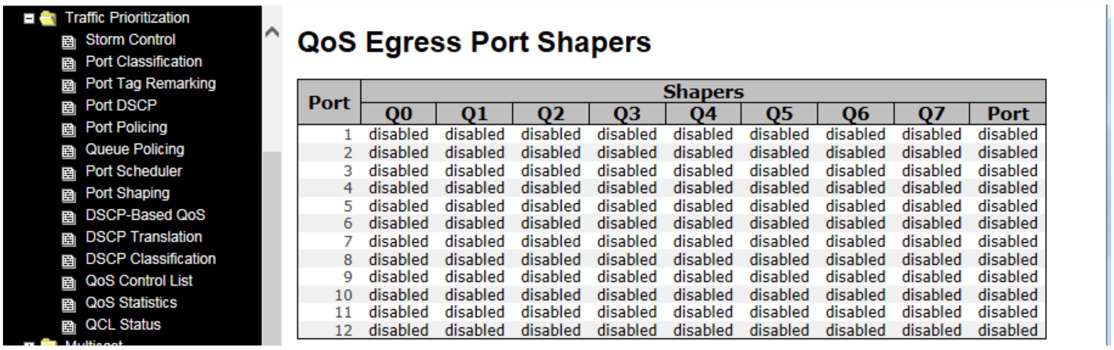
QoS Egress Port Schedulers

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

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

5.6.8 Port Shaping

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



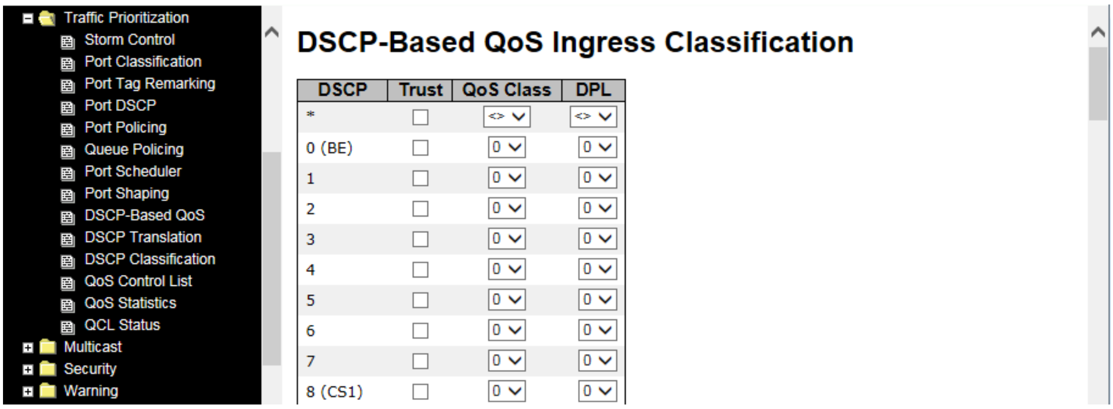
QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
11	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
12	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

Label	Description
Port	The switch port number to which the following settings will be applied. Click on the port number to configure the shapers.
Mode	Shows **disabled** or actual queue shaper rate - e.g. "800 Mbps".
Q0~Q7	Shows **disabled** or actual port shaper rate - e.g. "800 Mbps".

5.6.9 DSCP-based QoS

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



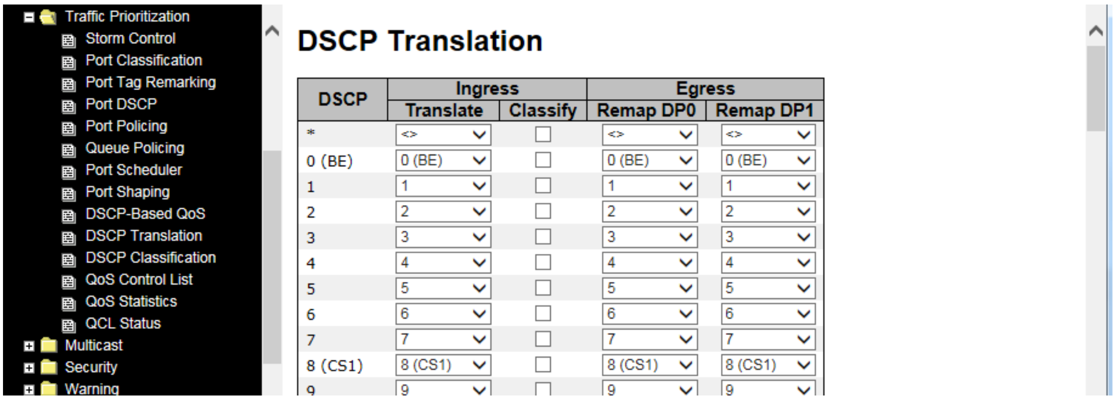
DSCP-Based QoS Ingress Classification

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

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	The QoS Class value can be any number from 0-7.
DPL	Drop Precedence Level (0-1).

5.6.10 DSCP Translation

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



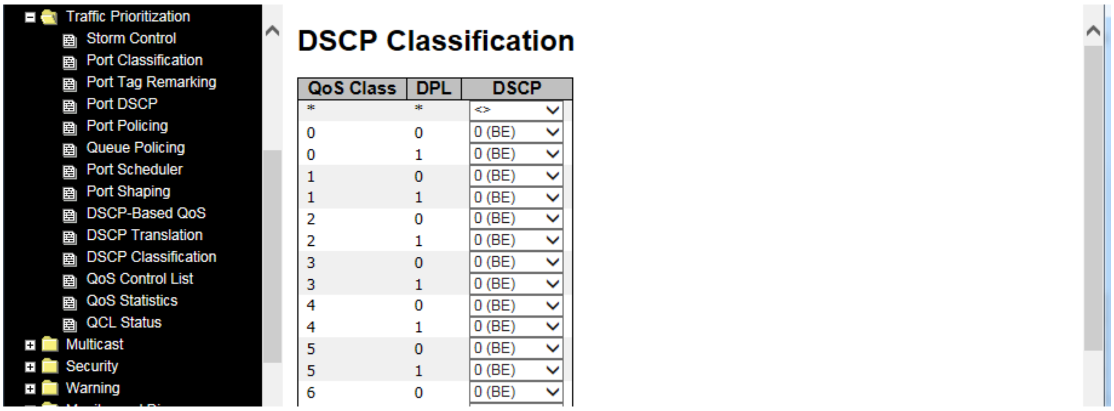
DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	□	<>	<>
0 (BE)	0 (BE)	□	0 (BE)	0 (BE)
1	1	□	1	1
2	2	□	2	2
3	3	□	3	3
4	4	□	4	4
5	5	□	5	5
6	6	□	6	6
7	7	□	7	7
8 (CS1)	8 (CS1)	□	8 (CS1)	8 (CS1)
9	9	□	9	9

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:** Enables ingress translation of DSCP values based on the specified classification method. DSCP can be translated to any of (0-63) DSCP values. 2. **Classify:** Enable Classification at ingress side as defined in the QoS Port DSCP Configuration table.
Egress	Configurable engress parameters include; **Remap DP0**: Re-maps DP0 field to selected DSCP value. DP0 indicates a drop precedence with a low priority. You can select the DSCP value from a selected menu to which you want to remap. DSCP value ranges form 0 to 63. **Remap DP1**: Re-maps DP1 field to selected DSCP value. DP1 indicates a drop precedence with a high priority. You can select the DSCP value from a selected menu to which you want to remap. DSCP value ranges form 0 to 63.

5.6.11 DSCP Classification

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



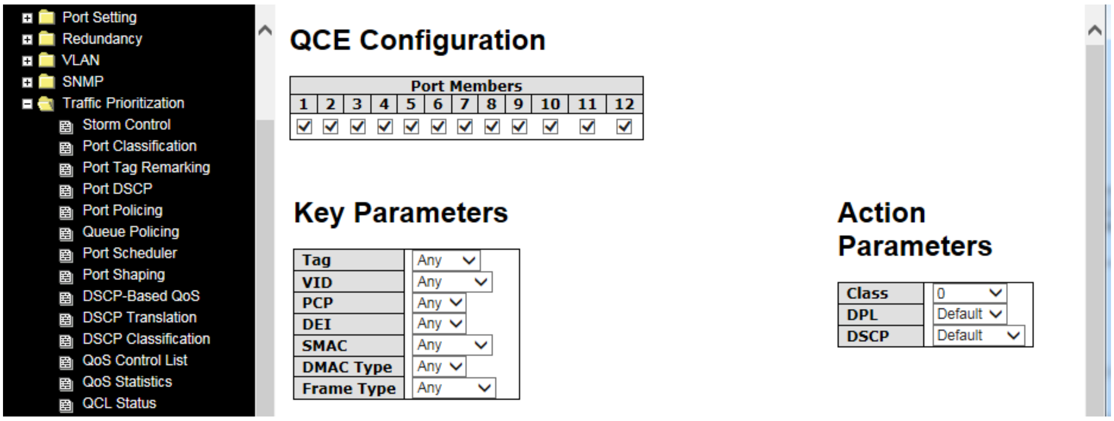
DSCP Classification

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

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

5.6.12 QoS Control List

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



QCE Configuration

Port Members											
1	2	3	4	5	6	7	8	9	10	11	12
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Key Parameters

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

Action Parameters

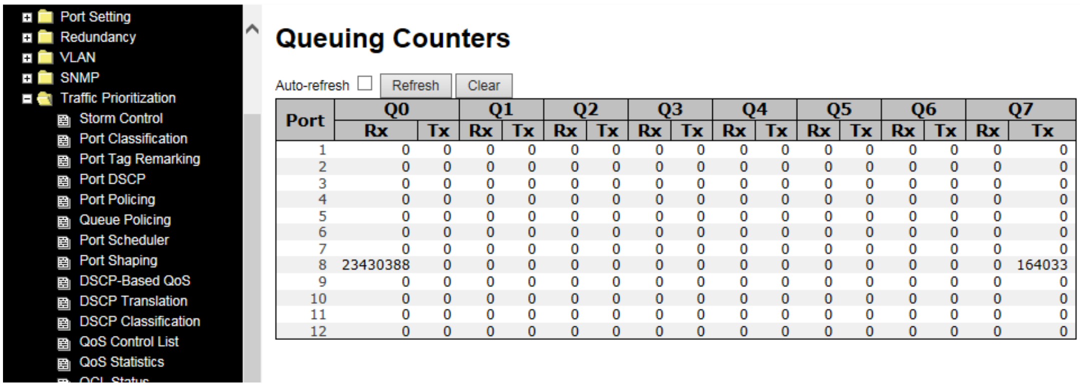
Class	0
DPL	Default
DSCP	Default

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 from 1 to 4095 **Any**: can be a specific value or a range of VIDs. **PCP**: Priority Code Point, can be specific numbers (0, 1, 2, 3, 4, 5, 6, 7), a range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or **Any** **DEI**: Drop Eligible Indicator, can be any of values between 0 and 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**, and **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 can range from 0x00 to 0xFF or **Any**. The default value is **Any**.
SNAP	PID: valid PID (a.k.a ethernet type) values can range from 0x00 to 0xFFFF or Any. The default value is Any.
IPv4	Protocol IP Protocol Number: (0-255, TCP or UDP) or **Any** 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 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 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.

5.6.13 QoS Counters

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



Queuing Counters

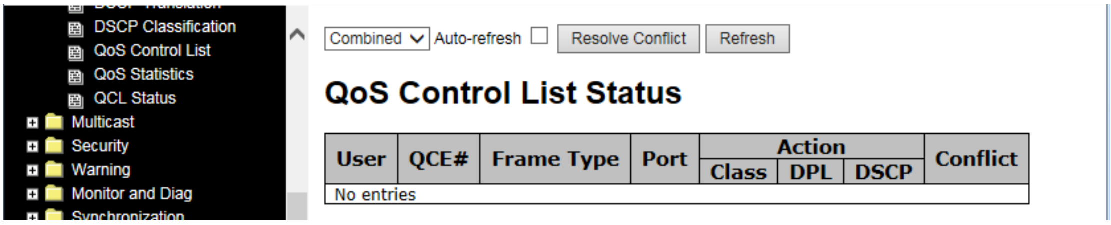
Auto-refresh □

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	23430388	0	0	0	0	0	0	0	0	0	0	0	0	0	0	164033
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

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

5.6.14 QCL Status

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



QoS Control List Status

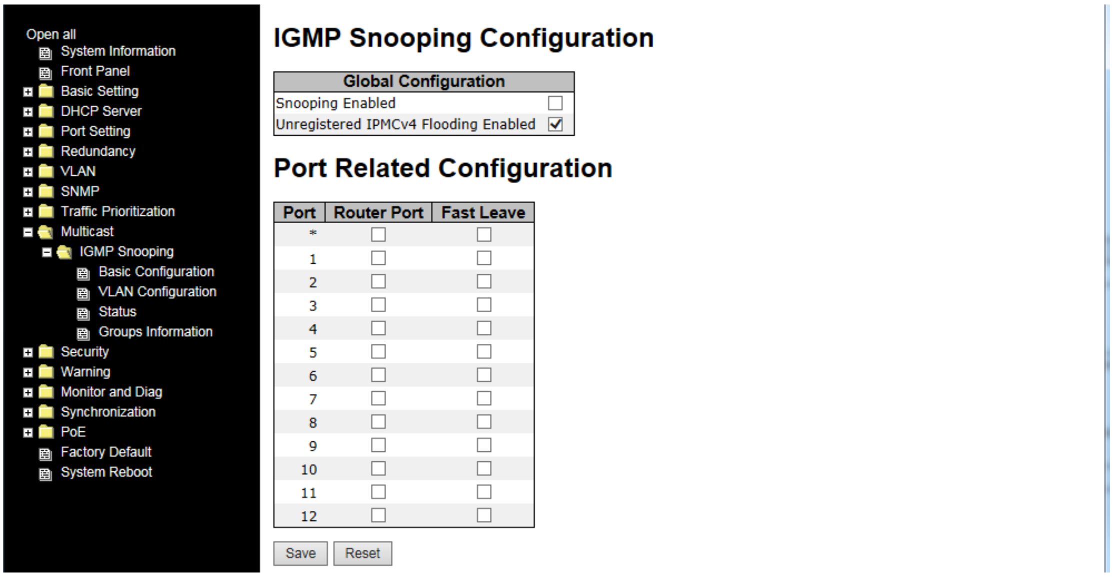
User	QCE#	Frame Type	Port	Action			Conflict
				Class	DPL	DSCP	
No entries							

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. Frame types are: **Any**: the QCE will match all frame type. **Ethernet**: Only Ethernet frames with Ether Type 0x600-0xFFFF are allowed. **LLC**: Only (LLC) frames are allowed. **SNAP**: Only (SNAP) frames are allowed. **IPv4**: the QCE will match only IPV4 frames. **IPv6**: the QCE will match only IPV6 frames.
Port	Indicates the list of ports configured with the QCE.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: **Class**, **DPL**, and **DSCP**. **Class**: Classified QoS; 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 QCL entries conflict status. 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**. Note that conflict can be resolved by releasing the hardware resources required to add the QCL entry by pressing Resolve Conflict button.

5.7 Multicast

5.7.1 IGMP Snooping

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



IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	□
Unregistered IPMCv4 Flooding Enabled	☑

Port Related Configuration

Port	Router Port	Fast Leave
*	□	□
1	□	□
2	□	□
3	□	□
4	□	□
5	□	□
6	□	□
7	□	□
8	□	□
9	□	□
10	□	□
11	□	□
12	□	□

Label	Description
Snooping Enabled	Check to enable global IGMP snooping.
Unregistered IPMCv4Flooding enabled	Check to enable unregistered IPMC traffic flooding.
Router Port	Specifies which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. 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.

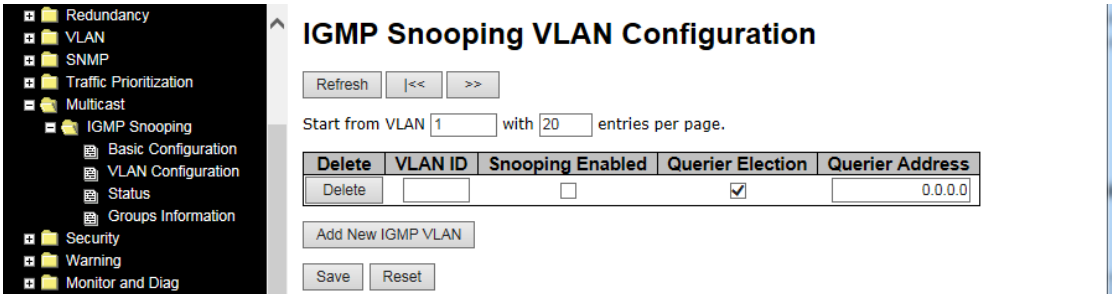
5.7.2 IGMP Snooping VLAN Configuration

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

Each page shows up to 99 entries from the VLAN table, depending on the value in the Entries Per Page field. By default, the page will show the first 20 entries from the beginning of the VLAN table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

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

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



IGMP Snooping VLAN Configuration

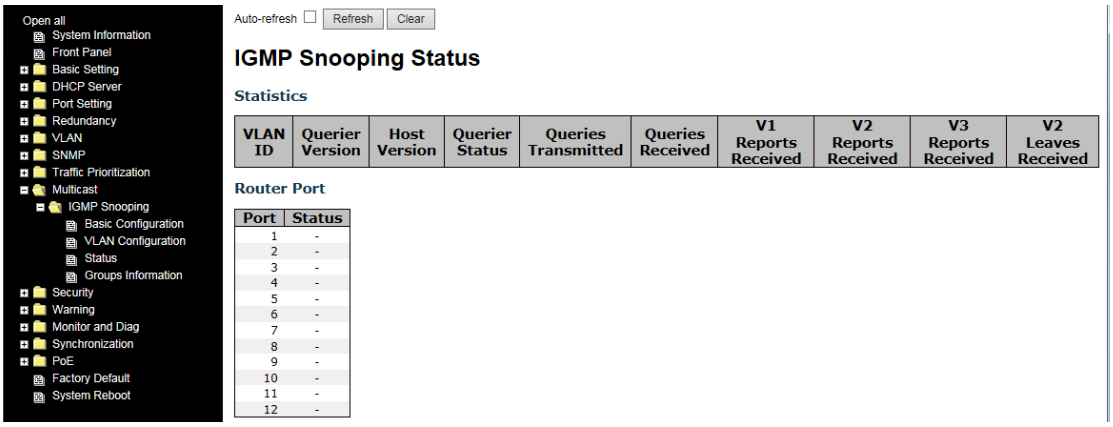
Start from VLAN 1 with 20 entries per page.

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 will be deleted during the next save.
VLAN ID	The VLAN ID of the entry
IGMP Snooping Enable	Check to enable IGMP snooping for individual VLAN. Up to 32 VLANs can be selected.
IGMP Querier	Check to enable the IGMP Querier in the VLAN

5.7.3 IGMP Snooping Status

This page provides IGMP snooping status.



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

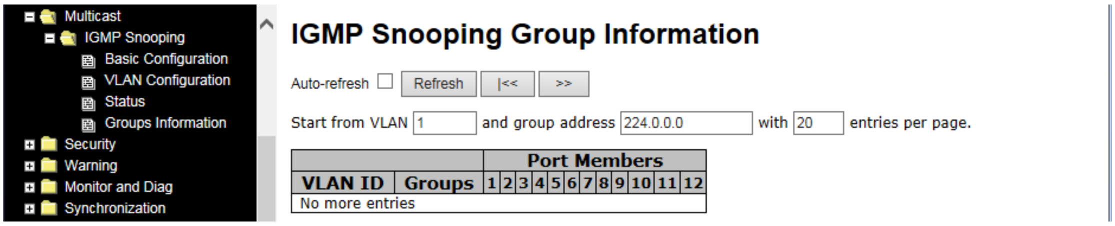
Router Port

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

Label	Description
VLAN ID	The VLAN ID of the entry
Querier Version	Active Querier version
Host Version	Active Host version
Querier Status	Shows the Querier status as **ACTIVE** or **IDLE**
Querier Receive	The number of transmitted Querier
V1 Reports Receive	The number of received V1 reports
V2 Reports Receive	The number of received V2 reports
V3 Reports Receive	The number of received V3 reports
V2 Leave Receive	The number of received V2 leave packets
Refresh	Click to refresh the page immediately
Clear	Clear all statistics counters
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals
Port	Switch port number
Status	Indicates whether a specific port is a router port or not

5.7.4 Groups Information of IGMP Snooping

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



IGMP Snooping Group Information

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

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

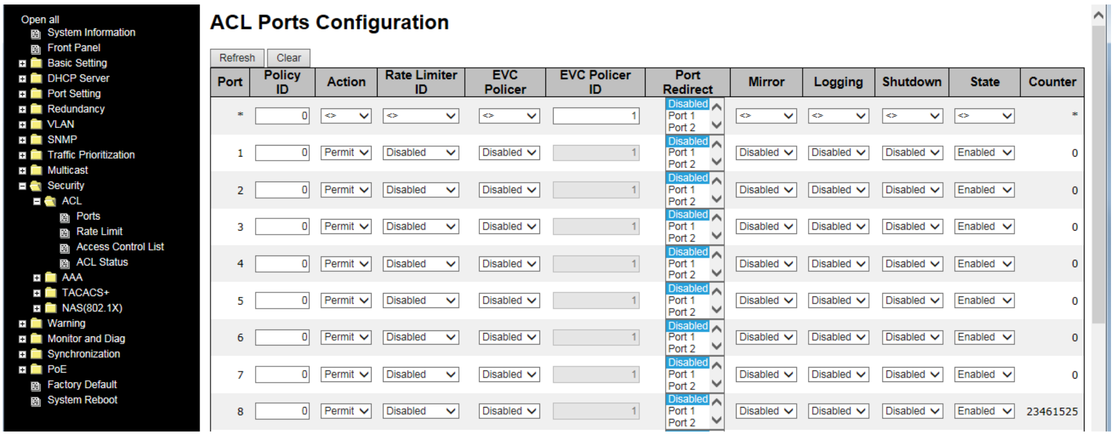
Label	Description
VLAN ID	The VLAN ID of the group.
Groups	The group address of the group displayed.
Port Members	Ports under this group.

5.8 Security

5.8.1 ACL

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

Port Configuration



ACL Ports Configuration

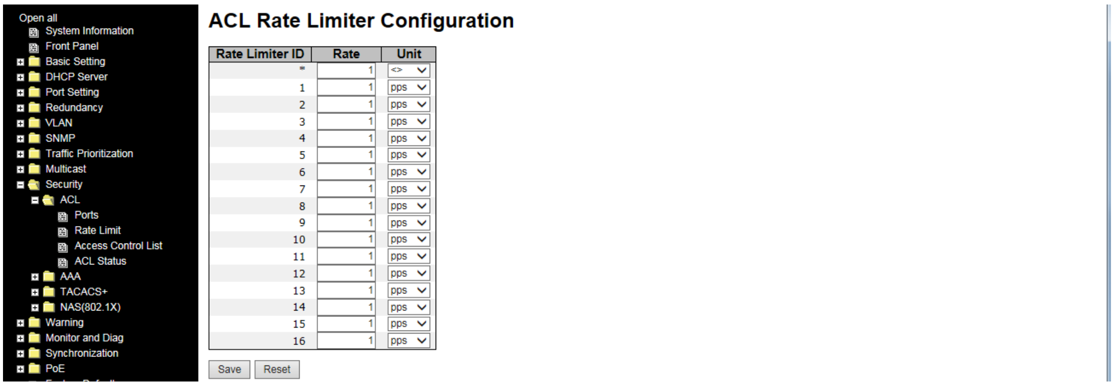
Port	Policy ID	Action	Rate Limiter ID	EVC Policer	EVC Policer ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	<>	1	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	23461525

Label	Description
Port	The switch port number to which the following settings will be applied
Policy ID	Select to apply a policy to the port. The allowed values are **1** to **8**. The default value is **1**.
Action	Select to **Permit** to permit or **Deny** to deny forwarding. The default value is **Permit**.

Rate Limiter ID	Select a rate limiter for the port. The allowed values are **Disabled** or numbers from **1** to **15**. The default value is **Disabled**.
Port Copy	Select which port frames are copied to. The allowed values are **Disabled** or a specific port number. The default value is **Disabled**.
Logging	Specifies the logging operation of the port. The allowed values are: **Enabled**: frames received on the port are stored in the system log **Disabled**: frames received on the port are not logged The default value is **Disabled**. Please note that system log memory capacity and logging rate is limited.
Shutdown	Specifies the shutdown operation of this port. The allowed values are: **Enabled**: if a frame is received on the port, the port will be disabled. **Disabled**: port shut down is disabled. The default value is **Disabled**.
Counter	Counts the number of frames that match this ACE.

Rate Limiters

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



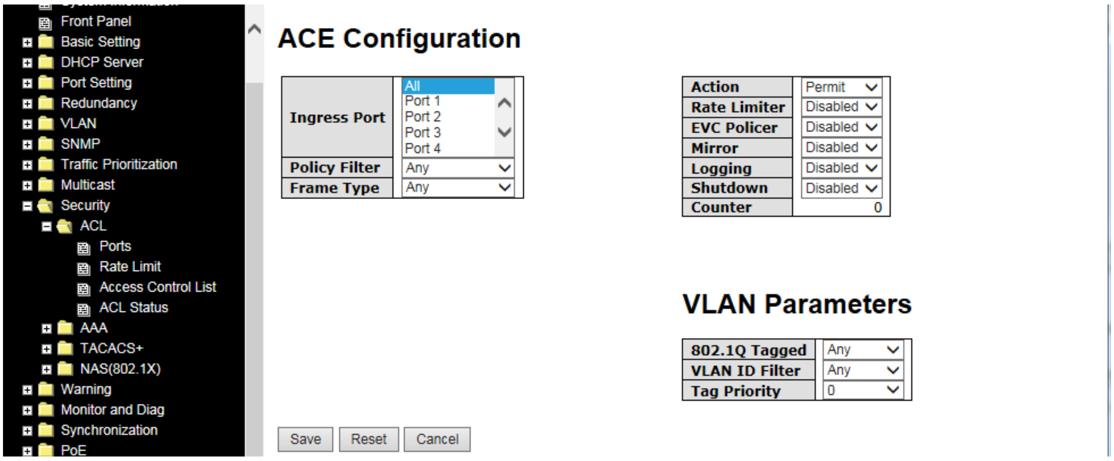
ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	1	<>
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

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

ACL Control List

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



ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Any
Frame Type	Any

Action	Permit
Rate Limiter	Disabled
EVC Policer	Disabled
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

VLAN Parameters

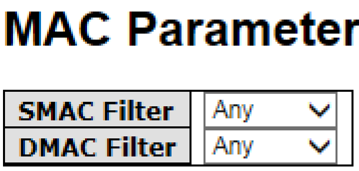
802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	0

Label	Description
Ingress Port	Indicates the ingress port to which the ACE will apply. **Any**: the ACE applies to any port.

	Port n: the ACE applies to this port number, where n is the number of the switch port. **Policy n**: the ACE applies to this policy number, where n can range from **1** to **8**.
Frame Type	Indicates the frame type of the ACE. These frame types are mutually exclusive. **Any**: any frame can match the ACE. **Ethernet Type**: only Ethernet type frames can match the ACE. The IEEE 802.3 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 Copy	Frames matching the ACE are copied to the port number specified here. The allowed range is the same as the switch port number range. Disabled means the port copy operation is disabled.
Logging	Specifies the logging operation of the ACE. The allowed values are: **Enabled**: frames matching the ACE are stored in the system log. **Disabled**: frames matching the ACE are not logged. Please note that system log memory capacity and logging rate is limited.
Shutdown	Specifies the shutdown operation of the ACE, either: **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.

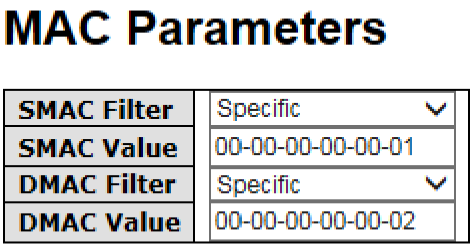
MAC Parameters

Source MAC and Destination MAC parameters for an ACE are configured here.



MAC Parameters

SMAC Filter	Any
DMAC Filter	Any



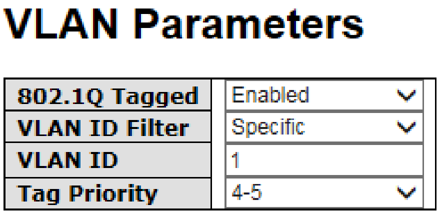
MAC Parameters

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 for an ACE are configured here.



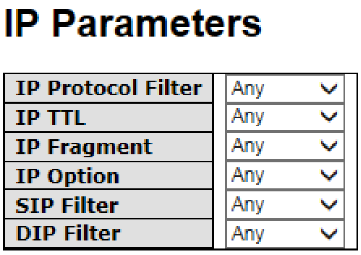
VLAN Parameters

802.1Q Tagged	Enabled
VLAN ID Filter	Specific
VLAN ID	1
Tag Priority	4-5

Label	Description
802.1Q Tagged	At the dropdown select IEEE 802.1Q tagging **Enabled** or **Disabled**. The default is **Enabled**.
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**").

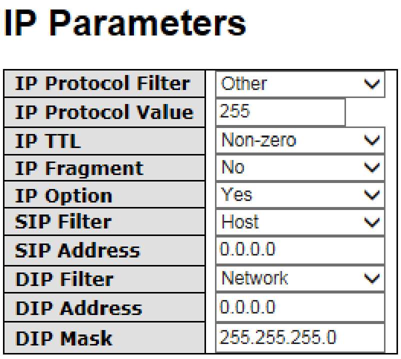
IP Parameters

IP parameters for an ACE are configured here.



IP Parameters

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



IP Parameters

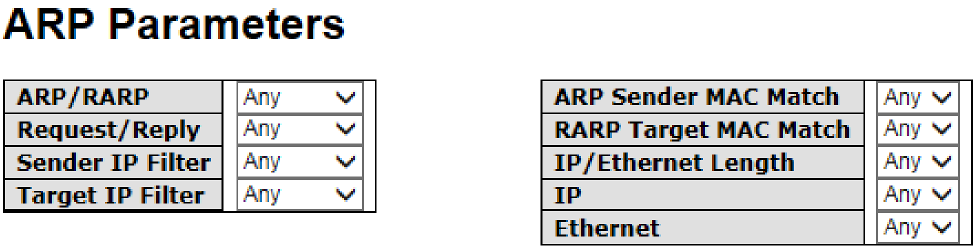
IP Protocol Filter	Other
IP Protocol Value	255
IP TTL	Non-zero
IP Fragment	No
IP Option	Yes
SIP Filter	Host
SIP Address	0.0.0.0
DIP Filter	Network
DIP Address	0.0.0.0
DIP Mask	255.255.255.0

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 for an ACE are configured here.



ARP Parameters

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

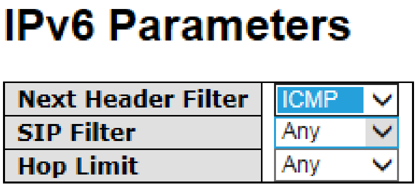
ARP Sender MAC Match	Any
RARP Target MAC Match	Any
IP/Ethernet Length	Any
IP	Any
Ethernet	Any

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 appear.
Sender IP Address	When Host or Network is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.
Sender IP Mask	When Network is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.
Target IP Filter	Specifies the target IP filter for the specific ACE **Any**: no target IP filter is specified (target IP filter is "**don't-care**"). **Host**: target IP filter is set to **Host**. Specify the target IP address in the **Target IP Address** field that appears. **Network**: target IP filter is set to **Network**. Specify the target IP address and target IP mask in the **Target IP Address** and **Target IP**

	Mask fields that appear.
Target IP Address	When **Host** or **Network** is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.
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**").

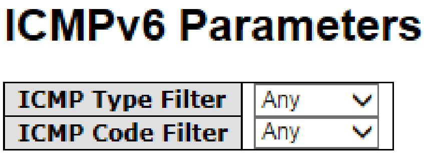
ICMP Parameters

ICMP parameters for an ACE are configured here.



IPv6 Parameters

Next Header Filter	ICMP
SIP Filter	Any
Hop Limit	Any



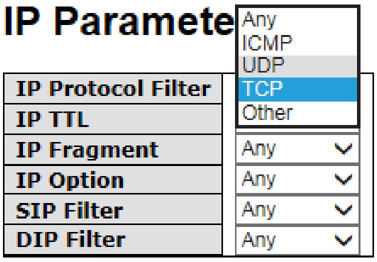
ICMPv6 Parameters

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

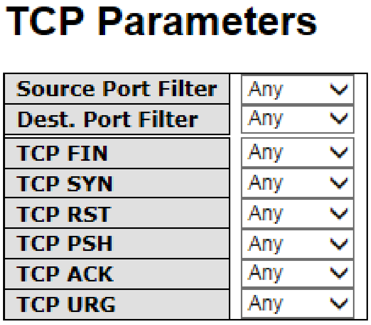
TCP and UDP Parameters

TCP and UDP parameters for an ACE are configured here.



IP Parameters

IP Protocol Filter	TCP
IP TTL	
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

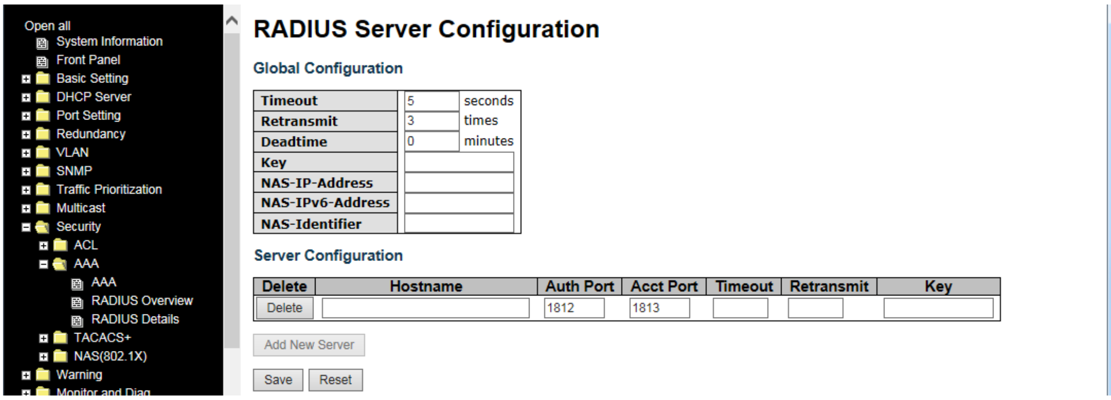
Label	Description
TCP/UDP Source Filter	Specifies the TCP/UDP source filter for the ACE **Any**: no TCP/UDP source filter is specified (TCP/UDP source filter status is "**don't-care**"). **Specific**: if you want to filter a specific TCP/UDP source filter with the ACE, you can enter a specific TCP/UDP 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**").

5.8.2 Authentication, Authorization, and Accounting (AAA)

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



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			

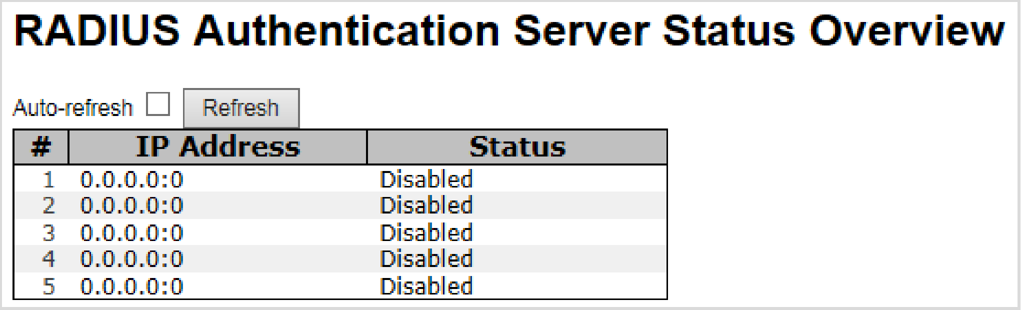
Label	Description
Timeout	The timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this time frame, we will consider it to be dead and continue with the next enabled server (if any). RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.
Dead Time	The dead time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the dead time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

5.8.3 RADIUS

Authentication and Accounting Server

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

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

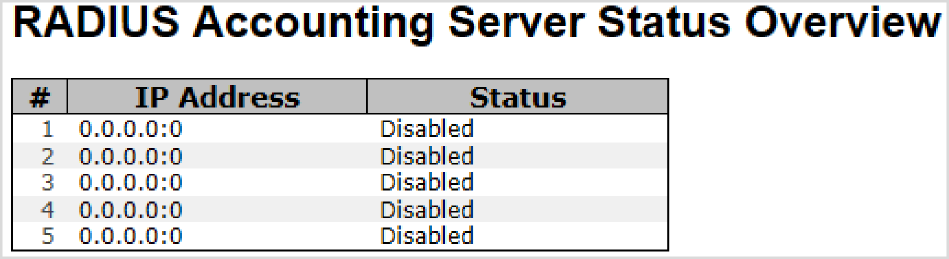


RADIUS Authentication Server Status Overview

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 authentication server number for which the configuration below applies.
Enabled	Check to enable the RADIUS authentication server.
IP Address	The IP address or hostname of the RADIUS authentication server. IP address is expressed in dotted decimal notation.
Port	The UDP port to use on the RADIUS authentication server. If the port is set to **0** (zero), the default port (1812) is used on the RADIUS authentication server.
Secret	The secret is a text string used by RADIUS to encrypt the client and server authenticator field during exchanges between the router and a RADIUS authentication server. The router encrypts PPP PAP passwords using this text string. The secret - up to 29 characters long - shared between the RADIUS authentication server and the switch stack.



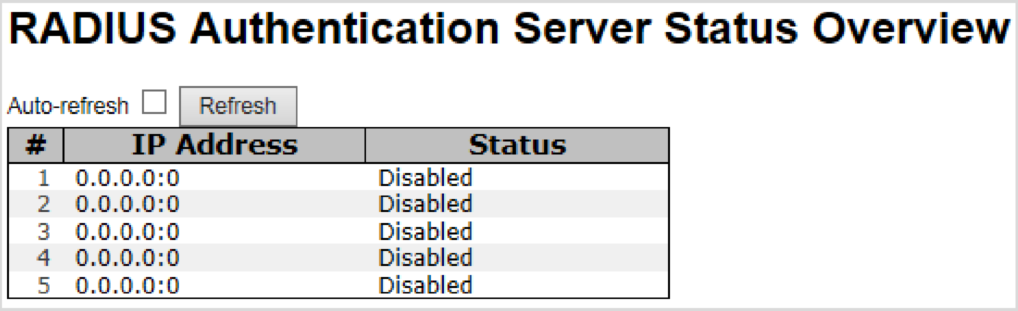
RADIUS Accounting Server Status Overview

#	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 accounting server number for which the configuration below applies.
Enabled	Check to enable the RADIUS accounting server
IP Address	The IP address or hostname of the RADIUS accounting server. IP address is expressed in dotted decimal notation.
Port	The UDP port to use on the RADIUS accounting server. If the port is set to **0** (zero), the default port (1813) is used on the RADIUS accounting server.
Secret	The secret is a text string used by RADIUS to encrypt the client and server authenticator field during exchanges between the router and a RADIUS authentication server. The router encrypts PPP PAP passwords using this text string. The secret - up to 29 characters long - shared between the RADIUS authentication server and the switch stack.

Authentication and Accounting Server Status

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

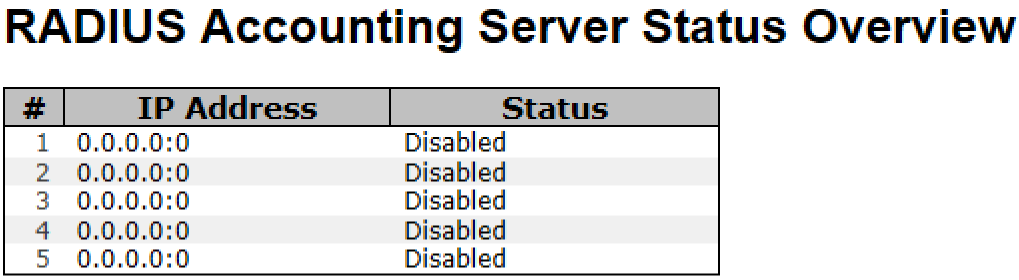


RADIUS Authentication Server Status Overview

Auto-refresh □ 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 of the server
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of the server
Status	The current status of the server. This field has one of the following values: **Disabled**: the server is disabled. **Not Ready**: the server is enabled, but IP communication is not yet up and running. **Ready**: the server is enabled, IP communications are built, and the RADIUS module is ready to accept access attempts. **Dead** (X seconds left): access attempts are made to this server, but it does not reply within the configured timeout. The server has temporarily been disabled, but will be re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.



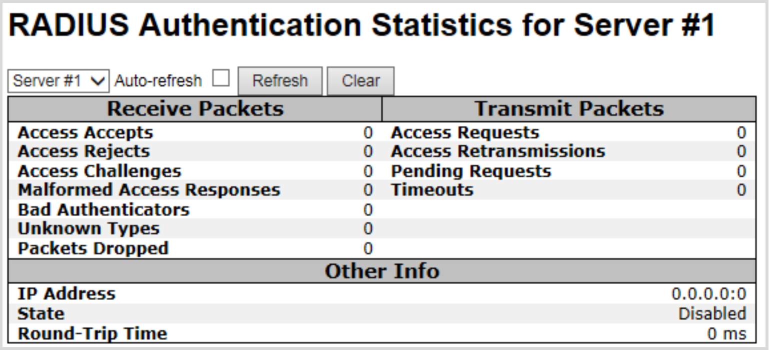
RADIUS Accounting Server Status Overview

#	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 of the server
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of the server
Status	The current status of the server. This field has one of the following values: Disabled: the server is disabled. **Not Ready**: the server is enabled, but IP communication is not yet up 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 are made to this server, but it does not reply within the configured timeout. The server has temporarily been disabled, but will be re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Authentication and Accounting Server Statistics

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

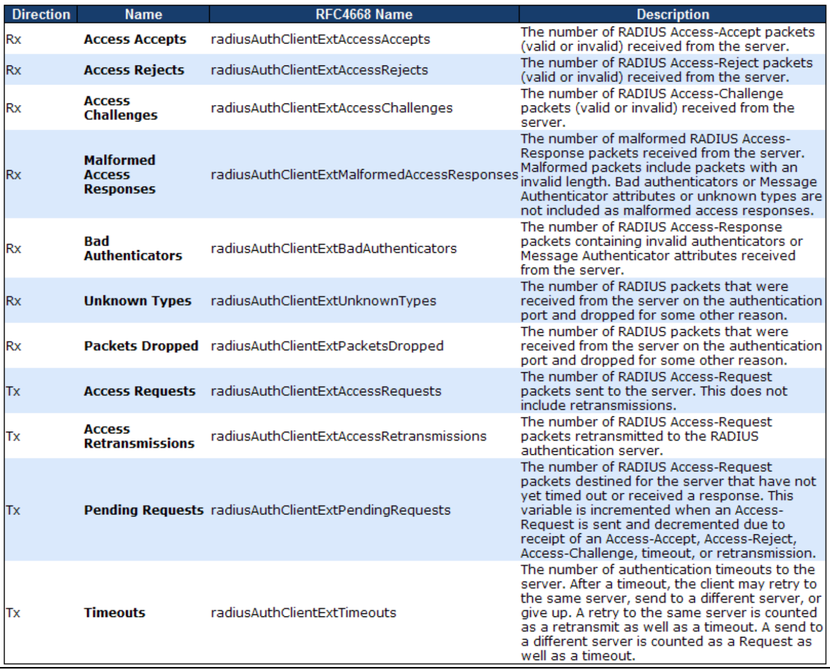
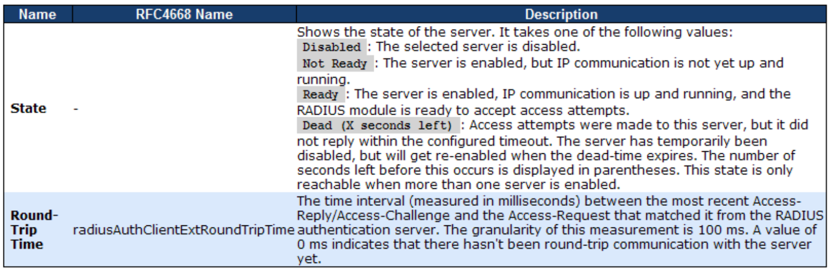


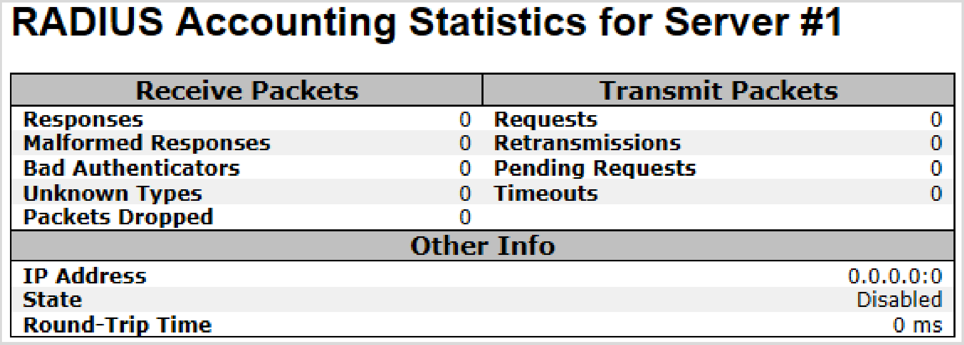
RADIUS Authentication Statistics for Server #1

Server #1 Auto-refresh □ Refresh Clear

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

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

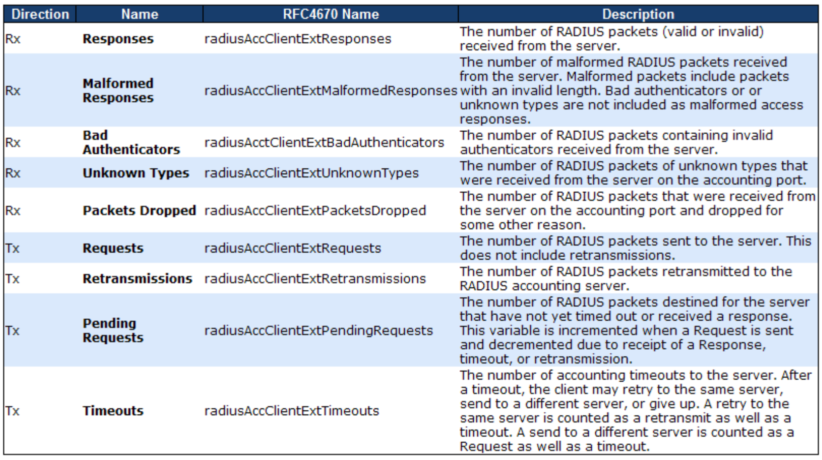
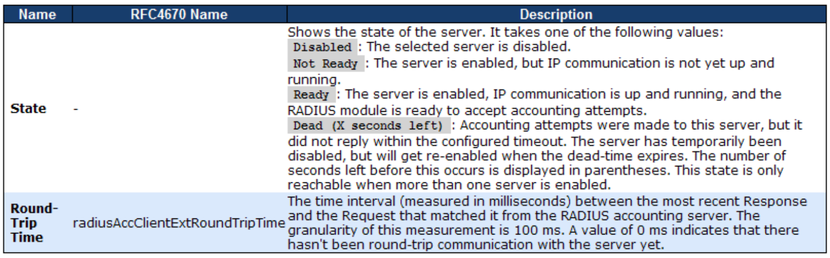
<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td>Packet Counters</td><td>RADIUS authentication server packet counters. There are seven ‘receive’ and four ‘transmit’ counters.

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

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



RADIUS Accounting Statistics for Server #1

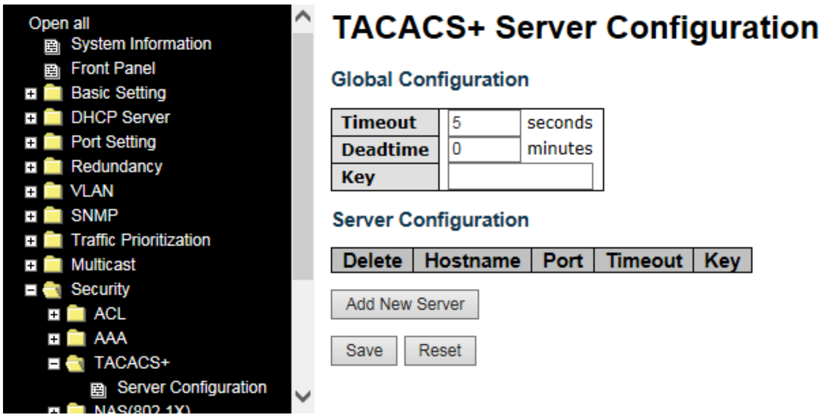
Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		

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>Packet Counters</td><td>RADIUS accounting server packet counters. There are five ‘receive’ and four ‘transmit’ counters.

<table>
<tr><th>Direction</th><th>Name</th><th>RFC4670 Name</th><th>Description</th></tr>
<tr><td>Rx</td><td><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>Other Info</td><td>This section contains information about the state of the server and the latest round-trip time.

<table>
<tr><th>Name</th><th>RFC4670 Name</th><th>Description</th></tr>
<tr><td><b>State</b></td><td>-</td><td>Shows the state of the server. It takes one of the following values:
<code>Disabled</code>: The selected server is disabled.
<code>Not Ready</code>: The server is enabled, but IP communication is not yet up and running.
<code>Ready</code>: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.
<code>Dead (X seconds left)</code>: Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.</td></tr>
<tr><td><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+ Server Configuration

TACACS+ (Terminal Acess Controller Access Control System Plus) is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.



TACACS+ Server Configuration

Global Configuration

Timeout	5	seconds
Deadtime	0	minutes
Key		

Server Configuration

Delete	Hostname	Port	Timeout	Key

Global Configuration

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

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:

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 **Add New Server** 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 **Reset** button can be used to undo the addition of the new server.

5.8.5 NAS (802.1x)

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

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more backend servers (RADIUS) determine whether the user is allowed access to the network.

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

Overview of 802.1X (Port-Based) Authentication

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

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

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

Overview of MAC-Based Authentication

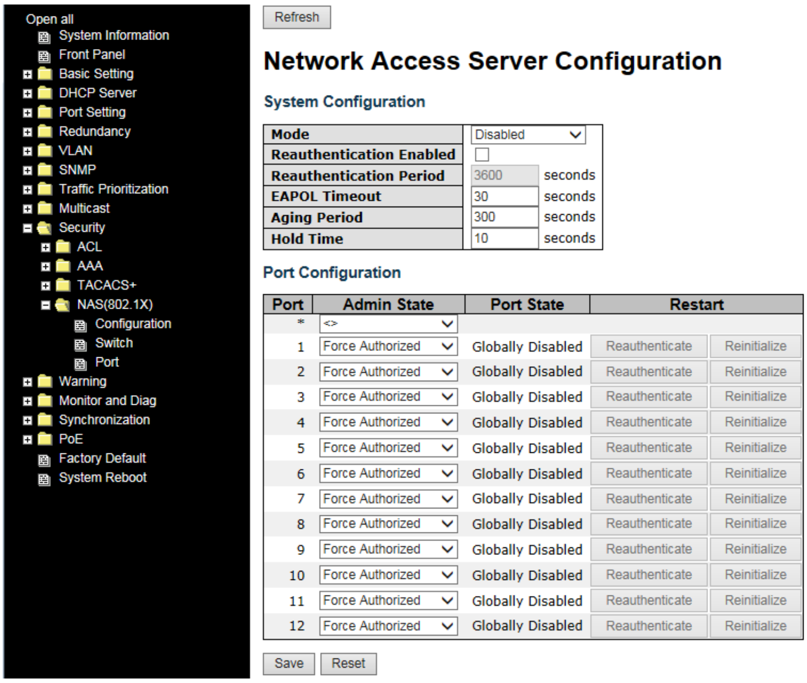
Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by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

The advantage of MAC-based authentication over 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients do npt need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users, equipment whose MAC address is a valid RADIUS user can be used by anyone, and only the MD5-Challenge method is supported.

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

Network Access Server Configuration

NAS system and port configuration is done here.



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
6	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
9	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
10	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
11	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
12	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize

The NAS system and port configuration parameters are described below.

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.

Age Period	This setting applies to the following modes, i.e. modes using the **Port Security** functionality to secure MAC addresses: **MAC-Based Auth.**: When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. For ports in **MAC-based Auth.** mode, reauthentication 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 a number between 10 and 1000000 seconds.
Port	The port number for which the configuration below applies
Admin State	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available: **Force Authorized**: In this mode, the switch will send one EAPOL Success frame when the port link 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

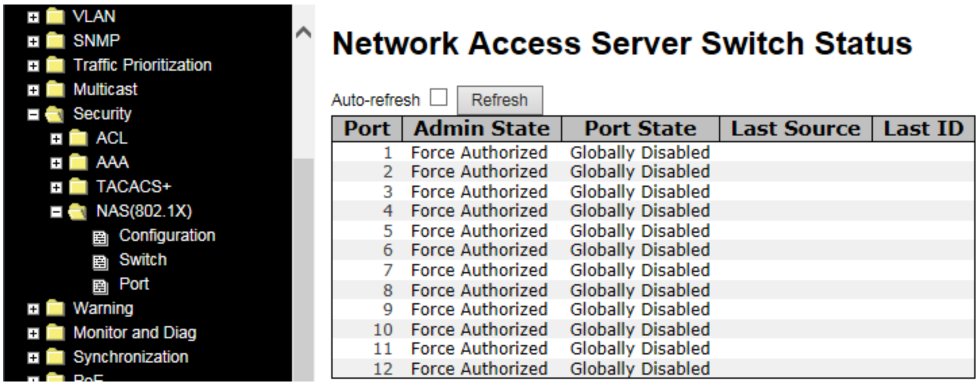
	not authenticated individually. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is not yet an IEEE standard, but features many of the same characteristics as port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal 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 shows the information on current NAS switch status.



Network Access Server Switch Status

Auto-refresh □ Refresh

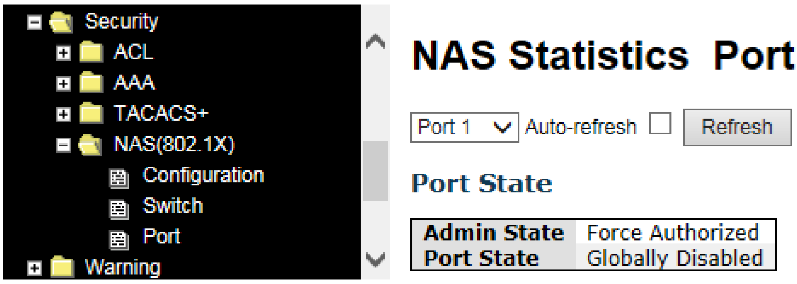
Port	Admin State	Port State	Last Source	Last ID
1	Force Authorized	Globally Disabled		
2	Force Authorized	Globally Disabled		
3	Force Authorized	Globally Disabled		
4	Force Authorized	Globally Disabled		
5	Force Authorized	Globally Disabled		
6	Force Authorized	Globally Disabled		
7	Force Authorized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

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 Status

This page shows the information on current NAS ports status.

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

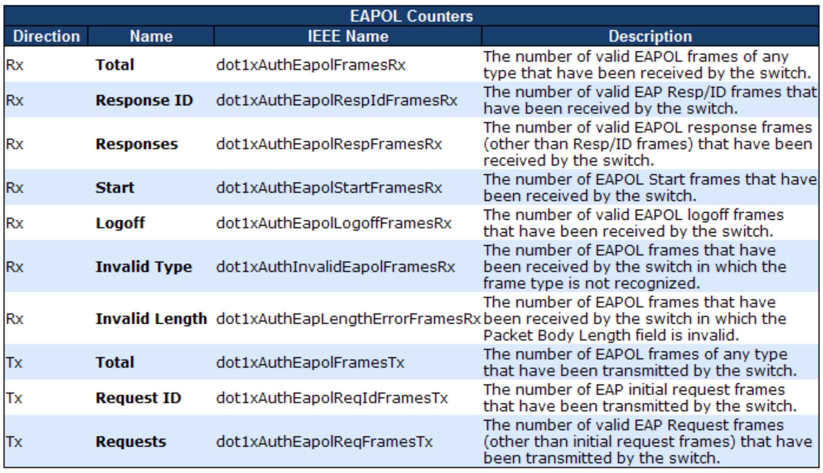


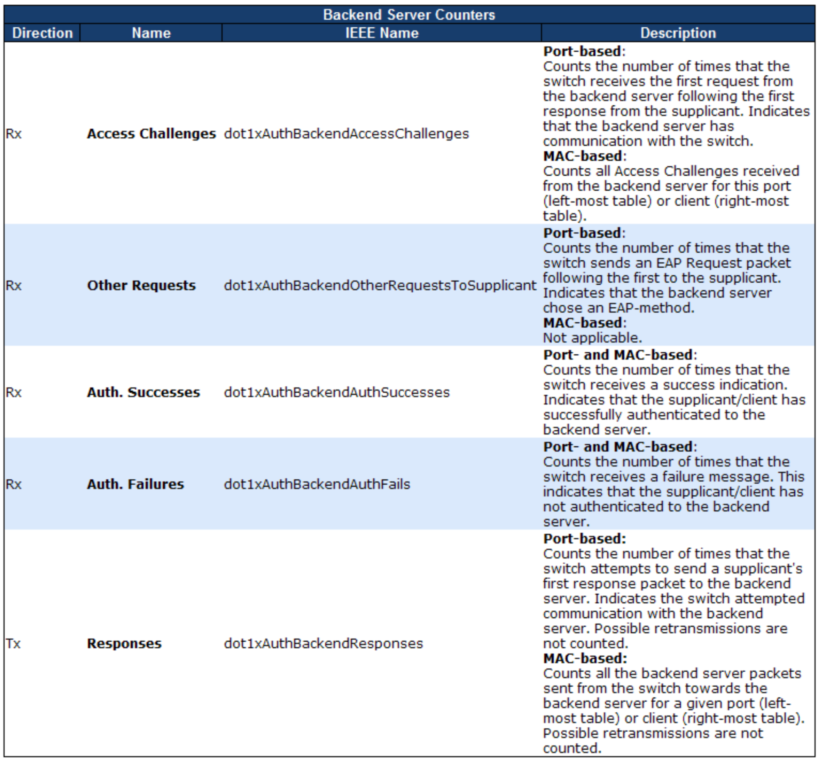
NAS Statistics Port 1

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>
<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></td></tr>
</table>

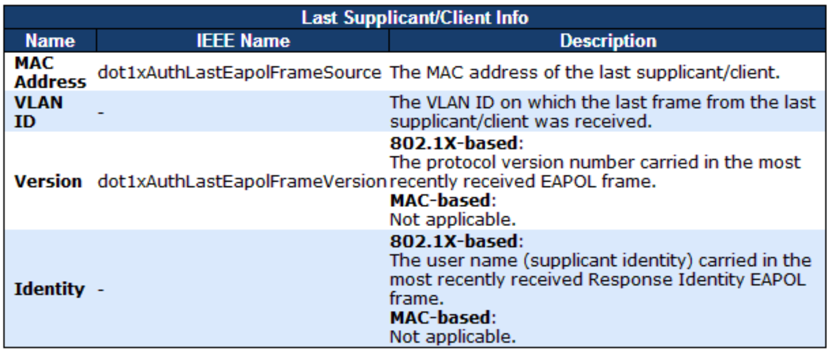


Backend Server Counters			
Direction	**Name**	**IEEE Name**	**Description**
Rx	**Access Challenges**	dot1xAuthBackendAccessChallenges	**Port-based**: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. **MAC-based**: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).
Rx	**Other Requests**	dot1xAuthBackendOtherRequestsToSupplicant	**Port-based**: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. **MAC-based**: Not applicable.
Rx	**Auth. Successes**	dot1xAuthBackendAuthSuccesses	**Port- and MAC-based**: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.
Rx	**Auth. Failures**	dot1xAuthBackendAuthFails	**Port- and MAC-based**: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
Tx	**Responses**	dot1xAuthBackendResponses	**Port-based:** Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. **MAC-based:** Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

Last Supplicant/Client Info

Information about the last supplicant/client that attempts to authenticate. This information is available for the following administrative states:

- **802.1X**
- **MAC-based Auth.**

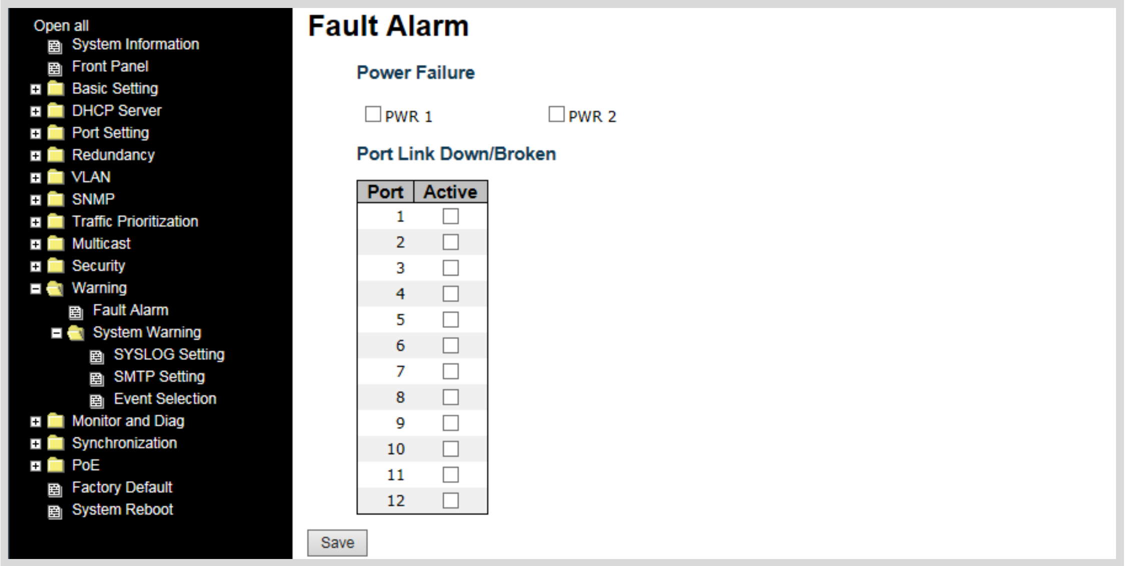


Last Supplicant/Client Info		
Name	**IEEE Name**	**Description**
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
VLAN ID	-	The VLAN ID on which the last frame from the last supplicant/client was received.
Version	dot1xAuthLastEapolFrameVersion	**802.1X-based**: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

5.9 Warning

5.9.1 Fault Alarm

When any selected fault event happens, the Fault LED on the switch panel will light up and the electric relay will signal at the same time. The following pages you set up alert conditions based on your needs for individual switch ports, including actions to be taken during disconnection and power failure.



Fault Alarm

Power Failure

□ PWR 1 □ PWR 2

Port Link Down/Broken

Port	Active
1	□
2	□
3	□
4	□
5	□
6	□
7	□
8	□
9	□
10	□
11	□
12	□

When any selected fault event happens, the Fault LED in the switch front panel will light and the electric relay will be signaled at the same time.

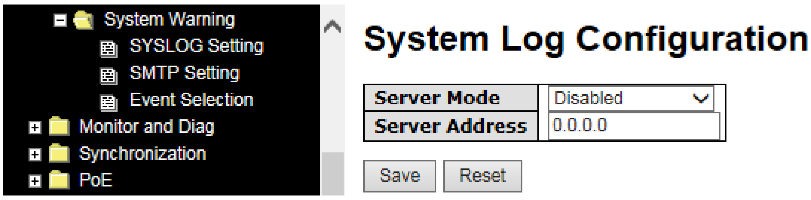
Power Failure: Fault alarm when any selected power failure. This switch supports dual power sources (PWR 1 and PWR 2).

Port Link Down/Broken: Fault alarm when any selected port link is down or broken.

5.9.2 System Warning

SYSLOG Setting

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



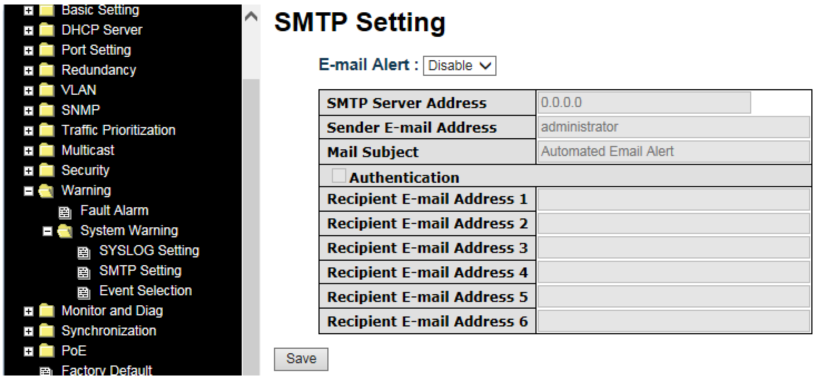
System Log Configuration

Server Mode	Disabled
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
Server Address	Indicates the IPv4 host address of syslog server. If the switch provides DNS functions, it also can be a host name.

SMTP Setting

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



SMTP Setting

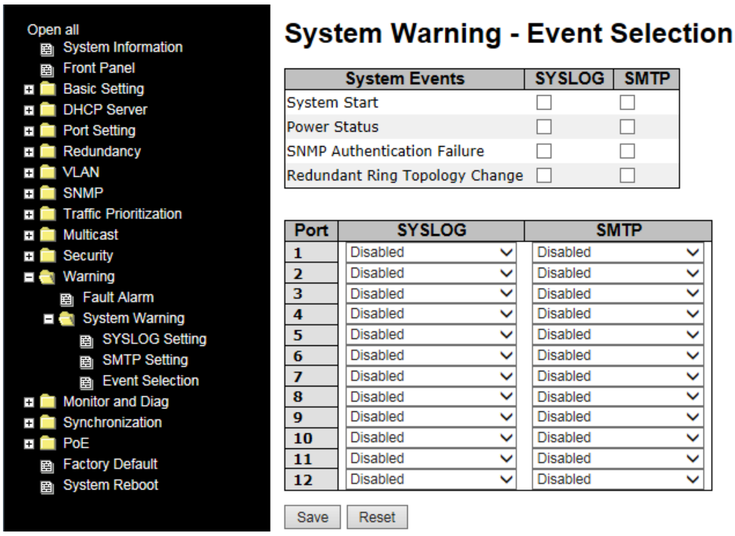
E-mail Alert : Disable

SMTP Server Address	0.0.0.0
Sender E-mail Address	administrator
Mail Subject	Automated Email Alert
□ Authentication	
Recipient E-mail Address 1	
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	Enables or disables transmission of system warnings by e-mail.
Sender E-mail Address	The SMTP server IP address.
Mail Subject	The Subject of the e-mail.
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.
Apply	Click to activate the configurations.
Help	Shows help file.

Event Selection

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



System Warning - Event Selection

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

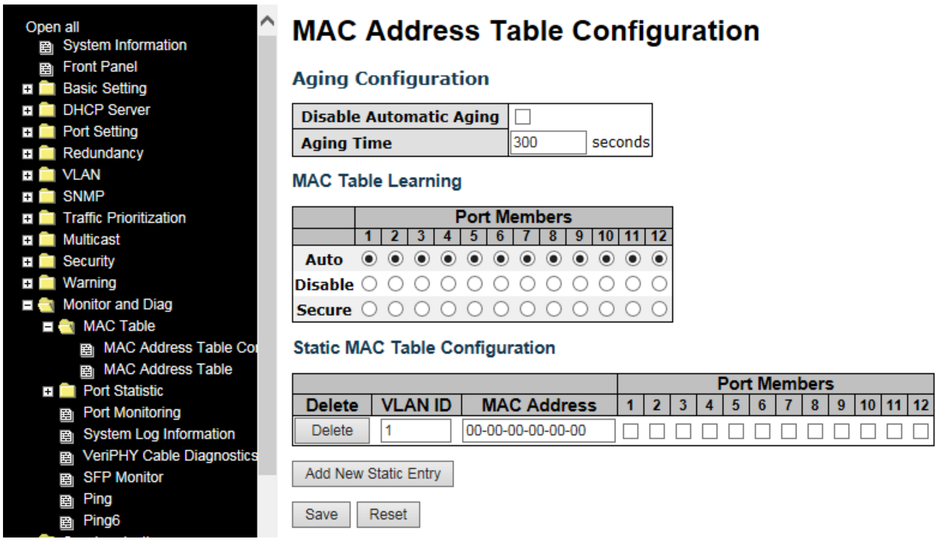
Port	SYSLOG	SMTP
1	Disabled	Disabled
2	Disabled	Disabled
3	Disabled	Disabled
4	Disabled	Disabled
5	Disabled	Disabled
6	Disabled	Disabled
7	Disabled	Disabled
8	Disabled	Disabled
9	Disabled	Disabled
10	Disabled	Disabled
11	Disabled	Disabled
12	Disabled	Disabled

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 Redundant Ring topology changes .
Port Event SYSLOG / SMTP event	■ **Disable** ■ **Link Up** ■ **Link Down** ■ **Link Up & Link Down**
Apply	Click to activate the configurations.
Help	Shows help file.

5.10Monitor and Diag

5.10.1 MAC Table

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



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

MAC Table Learning

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

Static MAC Table Configuration

			Port Members											
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12
Delete	1	00-00-00-00-00-00	□	□	□	□	□	□	□	□	□	□	□	□

Aging Configuration

Aging enables the switch to track only active MAC addresses on the network and flush out MAC addresses that are no longer used, thereby keeping the table current. By default, aged entries are removed after 300 seconds. You can configure aging time by entering a value in the **Age Time** box in seconds. The allowed range is 10 to 1000000 seconds. You can also disable the automatic aging of dynamic entries by checking **Disable Automatic Aging**.

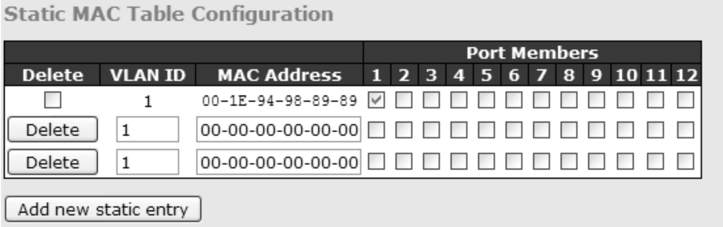
MAC Table Learning

The switch can add the address and port on which the packet was received to the MAC table if the address does not exist in the table by examining the source address of each packet received on a port. This is called learning. It allows the MAC table to expand dynamically. If the learning mode for a given port is grayed out, it means another module is in control of the mode, and thus the user cannot change the configurations. An example of such a module is MAC-Based authentication under 802.1X.

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

Static MAC Table Configurations

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



Static MAC Table Configuration

			Port Members											
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12
□	1	00-1E-94-98-89-89	☑	□	□	□	□	□	□	□	□	□	□	□
Delete	1	00-00-00-00-00-00	□	□	□	□	□	□	□	□	□	□	□	□
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 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.

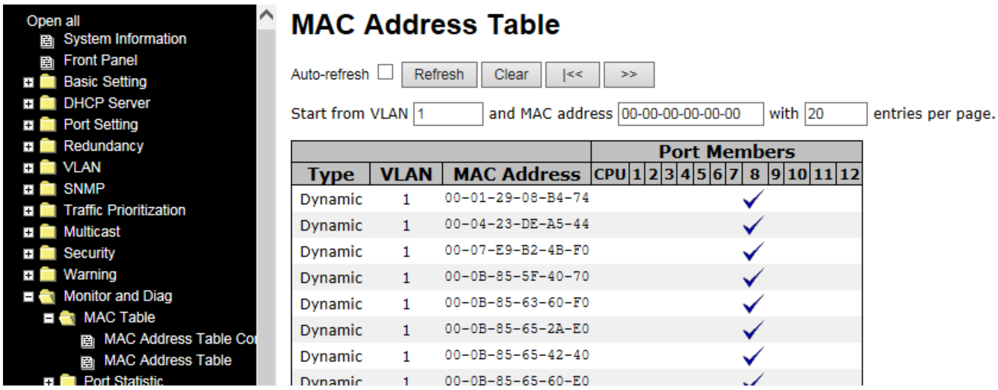
MAC Table

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

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

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

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

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

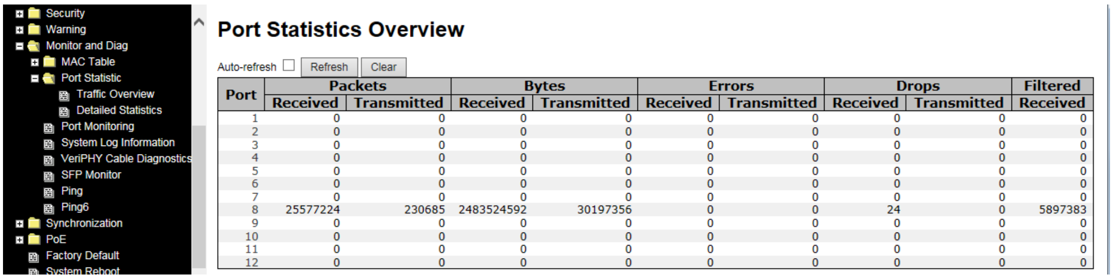
			Port Members												
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12
Dynamic	1	00-01-29-08-B4-74									✓				
Dynamic	1	00-04-23-DE-A5-44									✓				
Dynamic	1	00-07-E9-B2-4B-F0									✓				
Dynamic	1	00-0B-85-5F-40-70									✓				
Dynamic	1	00-0B-85-63-60-F0									✓				
Dynamic	1	00-0B-85-65-2A-E0									✓				
Dynamic	1	00-0B-85-65-42-40									✓				
Dynamic	1	00-0B-85-65-60-E0									✓				

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

5.10.2 Port Statistics

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	25577224	230685	2483524592	30197356	0	0	24	0	5897383
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0

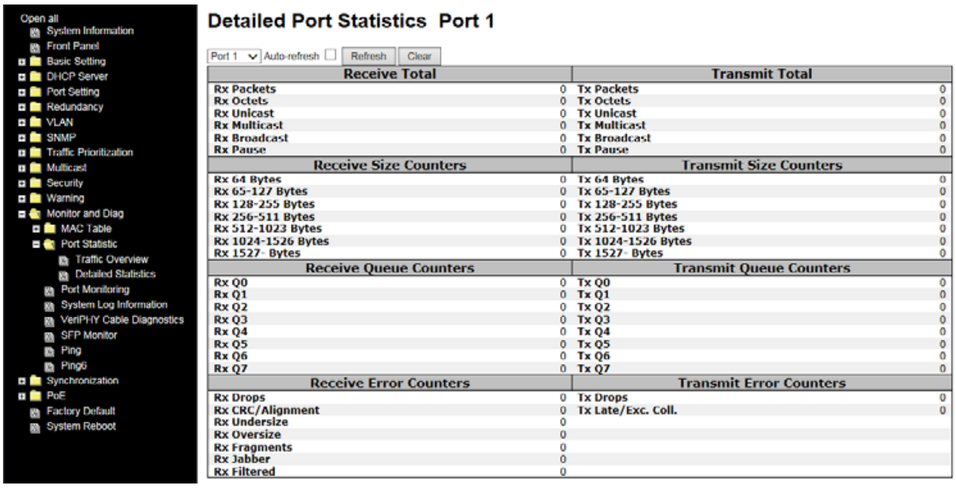
Label	Description
Port	The switch port number to which the following settings will be applied.
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions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

Detailed Statistics

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

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

Detailed Statistics – Total Receive & Transmit



Detailed Port Statistics Port 1

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

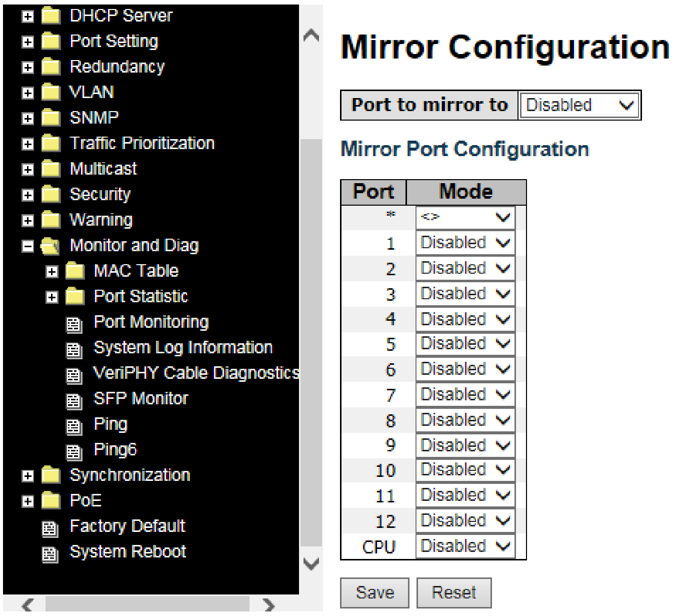
Label	Description
Rx and Tx Packets	The number of received and transmitted (good and bad) packets.
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes, including FCS, except framing bits.
Rx and Tx Unicast	The number of received and transmitted (good and bad) unicast packets.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

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

5.10.3 Port Mirroring

Port mirroring function will copy the traffic of one port to another port on the same switch to allow the network analyzer attached to the mirror port to monitor and analyze packets. The function is useful for troubleshooting. To solve network problems, selected traffic can be copied or mirrored to a mirror port where a frame analyzer can be attached to analyze the frame flow.

The traffic to be copied to the mirror port can be all frames received on a given port (also known as ingress or source mirroring) or all frames transmitted on a given port (also known as egress or destination mirroring). The port to which the monitored traffic is copied is called mirror port.



Mirror Configuration

Port to mirror to: Disabled

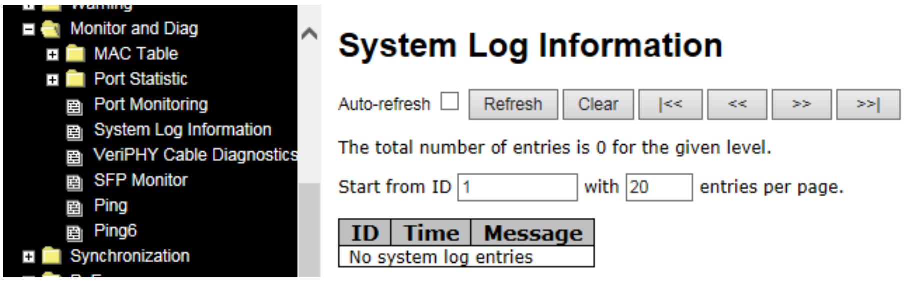
Mirror Port Configuration

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
CPU	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 recived 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 nly**.

5.10.4 System Log Information

This page provides switch system log information.



The total number of entries is 0 for the given level.

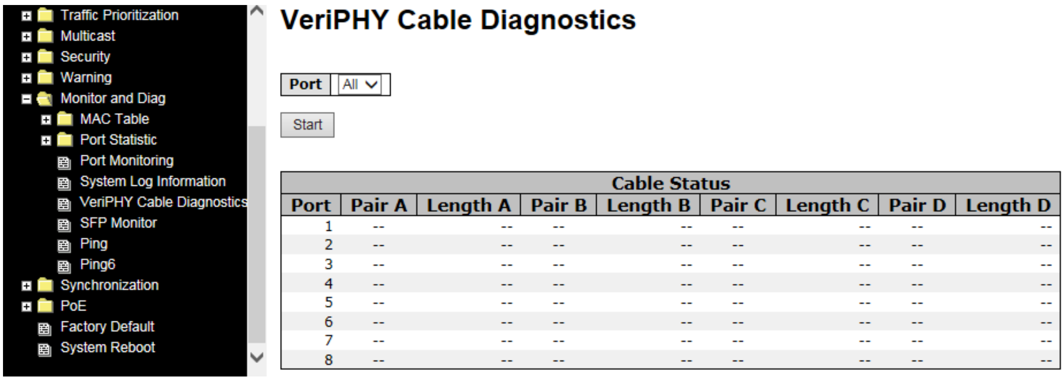
Start from ID 1 with 20 entries per page.

ID	Time	Message
No system log entries		

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 logging. **Warning**: provides warning for abnormal operation. **Error**: provides error message logging. **All**: enables all levels of logging.
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 VeriPHY Cable Diagnostics

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



VeriPHY Cable Diagnostics

Port: All

Start

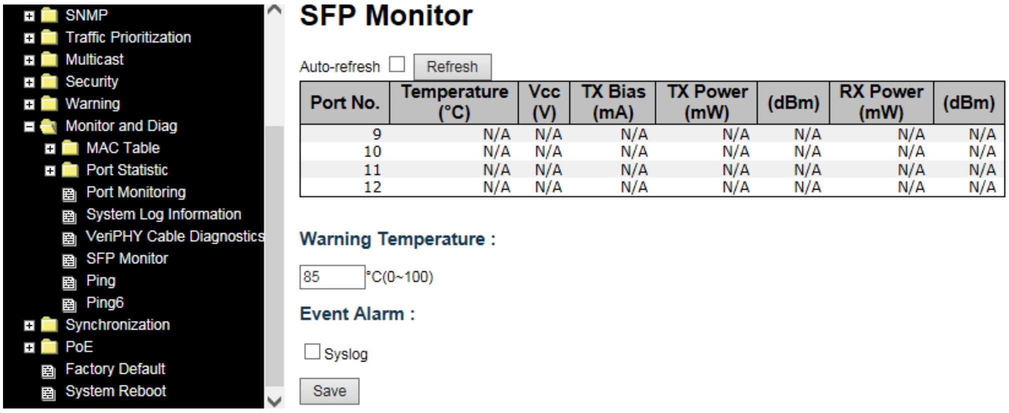
Cable Status

Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--
7	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--

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

5.10.6 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)
9	N/A	N/A	N/A	N/A	N/A	N/A	N/A
10	N/A	N/A	N/A	N/A	N/A	N/A	N/A
11	N/A	N/A	N/A	N/A	N/A	N/A	N/A
12	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Warning Temperature :

85 °C(0~100)

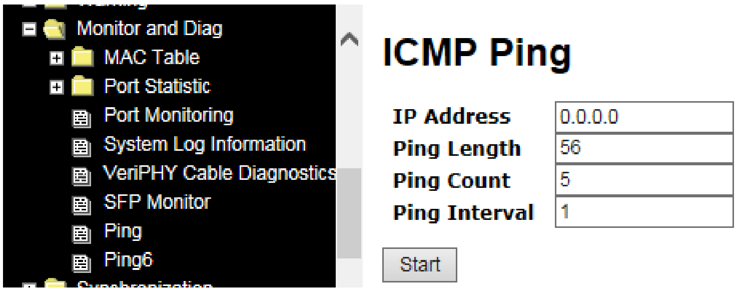
Event Alarm :

□ Syslog

Save

5.10.7 ICMP Ping

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



ICMP Ping

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

Start

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

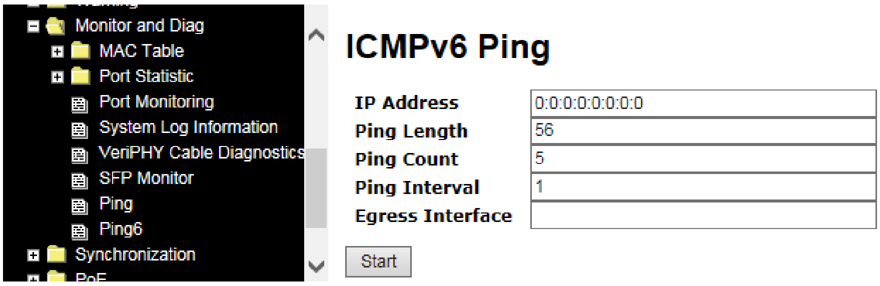
```
PING6 server ::10.10.132.20
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

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

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

5.10.8 ICMPv6 Ping

This page allows you to issue ICMP PING packets to troubleshoot IP 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	

Start

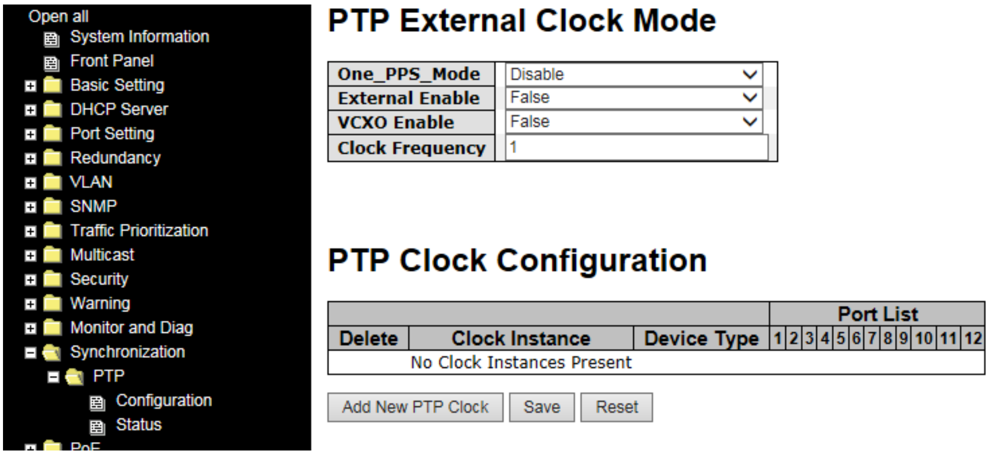
After you press **Start**, ICMPv6 packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING6 server ::192.168.10.1
sendto
sendto
sendto
sendto
sendto
Sent 5 packets, received 0 OK, 0 bad
```

5.11Synchronization

PTP External Clock Mode

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



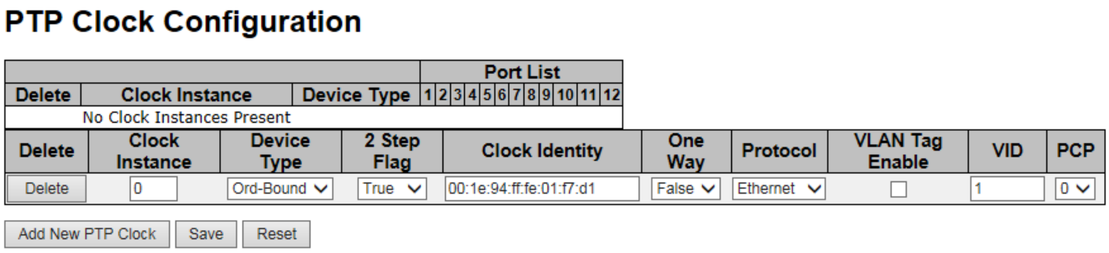
PTP External Clock Mode

One_PPS_Mode	Disable
External Enable	False
VCXO Enable	False
Clock Frequency	1

PTP Clock Configuration

			Port List											
Delete	Clock Instance	Device Type	1	2	3	4	5	6	7	8	9	10	11	12
	No Clock Instances Present													

Label	Description
One_pps_mode	The box allows you to select One_pps_mode configurations. The following values are possible: **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 allows you to configure the external VCXO rate adjustment. The following values are possible: **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 (1 - 25MHz).



PTP Clock Configuration

			Port List											
Delete	Clock Instance	Device Type	1	2	3	4	5	6	7	8	9	10	11	12
	No Clock Instances Present													

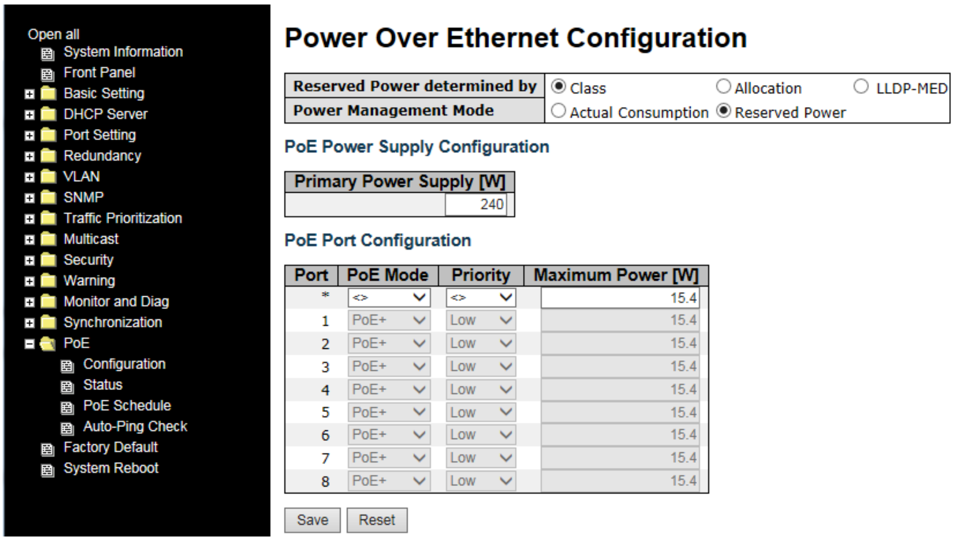
Delete	Clock Instance	Device Type	2 Step Flag	Clock Identity	One Way	Protocol	VLAN Tag Enable	VID	PCP
Delete	0	Ord-Bound	True	00:1e:94:ff:fe:01:f7:d1	False	Ethernet	□	1	0

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	Transport protocol used by the PTP protocol engine: **Ethernet** PTP over Ethernet multicast. **ip4multi** PTP over IPv4 multicast. **ip4uni** PTP over IPv4 unicast. Note: IPv4 unicast protocol only works in Master Only and Slave Only clocks. See also **Device Type**. In a unicast Slave Only clock, you also must configure the master clocks to request Announce and Sync messages from. See also **Unicast Slave Configuration**.
VLAN Tag Enable	Enables VLAN tagging for PTP frames. Note: Packets are only tagged if the port is configured for VLAN tagging (i.e: Port Type != Unaware and PortVLAN mode == None, and the port is member of the VLAN).
VID	VLAN identifiers used for tagging the PTP frames.
PCP	Priority code point values used for PTP frames.

5.12 POE

5.12.1 Power Over Ethernet Configuration

PoE (Power Over Ethernet) is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.



Power Over Ethernet Configuration

Reserved Power determined by	● Class ○ Allocation ○ LLDP-MED
Power Management Mode	○ Actual Consumption ● Reserved Power

PoE Power Supply Configuration

Primary Power Supply [W]
240

PoE Port Configuration

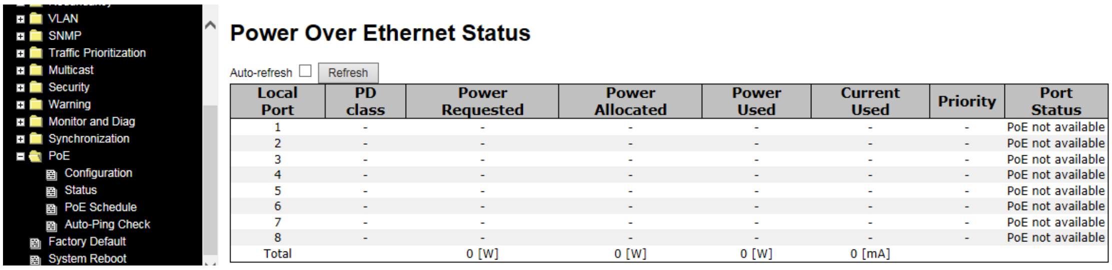
Port	PoE Mode	Priority	Maximum Power [W]
*	<>	<>	15.4
1	PoE+	Low	15.4
2	PoE+	Low	15.4
3	PoE+	Low	15.4
4	PoE+	Low	15.4
5	PoE+	Low	15.4
6	PoE+	Low	15.4
7	PoE+	Low	15.4
8	PoE+	Low	15.4

Label	Description
Reserved Power determined by	There are three modes for configuring how the ports/PDs may reserve power. **Allocation** mode: In this mode you allocate the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields. **Class** mode: In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode the Maximum Power fields have no effect. **LLDP-MED** mode: This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode In this mode the Maximum Power fields have no effect **For all modes**: If a port uses more power than the reserved

	power for the port, the port is shut down.
Power Management Mode	There are 2 modes for configuring when to shut down the ports: **Actual Consumption**: In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down. **Reserved Power**: In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.
Primary and Backup Power Source	Some switches support having two PoE power supplies. One is used as primary power source, and one as backup power source. If the switch doesn't support backup power supply only the primary power supply settings will be shown. In case that the primary power source fails the backup power source will take over. For being able to determine the amount of power the PD may use, it must be defined what amount of power the primary and backup power sources can deliver. Valid values are in the range 0 to 2000 Watts.
Port	This is the logical port number for this row. Ports that are not PoE-capable are grayed out and can not be configured for PoE.
PoE Mode	The PoE Mode represents the PoE operating mode for the port. **Disabled**: PoE disabled for the port. **PoE** : Enables PoE IEEE 802.3af (Class 4 PDs limited to 15.4W) **PoE+** : Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 30W)
Priority	The Priority represents the ports priority. The three levels of power priority are **Low**, **High** and **Critical**. The priority is used when the remote device requires more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.
Maximum Power (W)	The Maximum Power value indicates the maximum power in watts that can be delivered to a remote device. (The maximum allowed value is 30 W.)

5.12.2 PoE Status

This page displays the current status for all PoE ports.



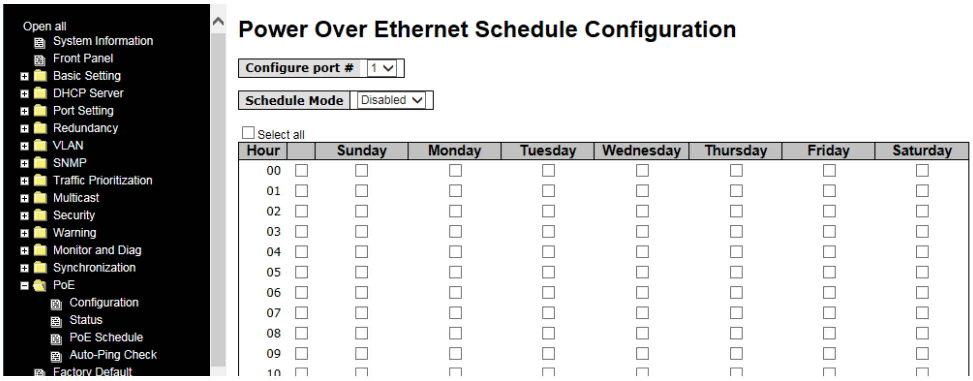
Power Over Ethernet Status

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	-	-	-	-	-	PoE not available
2	-	-	-	-	-	-	PoE not available
3	-	-	-	-	-	-	PoE not available
4	-	-	-	-	-	-	PoE not available
5	-	-	-	-	-	-	PoE not available
6	-	-	-	-	-	-	PoE not available
7	-	-	-	-	-	-	PoE not available
8	-	-	-	-	-	-	PoE not available
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

Label	Description
Local Port	This is the logical port number for this row.
PD Class	Each PD is classified according to a class that defines the maximum power the PD will use. The five PD Classes defined are: Class 0: Max. power 15.4 W. Class 1: Max. power 4.0 W. Class 2: Max. power 7.0 W. Class 3: Max. power 15.4 W Class 4: Max. power 30.0 W
Power Requested	The Power Requested shows the requested amount of power the PD wants to be reserved.
Power Allocated	The Power Allocated shows the amount of power the switch has allocated for the PD.
Power Used	The Power Used shows how much power the PD is using.
Current Used	The Power Used shows how much current the PD is using.
Priority	The Priority shows the port's priority configured by the user.
Port Status	The Port Status shows the port's status. The status can be: **PoE not available - No PoE chip found:** PoE not supported for the port. **PoE turned OFF - PoE disabled**: PoE is disabled by user. **PoE turned OFF - Power budget exceeded**- The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down. **No PD detected**: No PD detected for the port. **PoE turned OFF - PD overload**: The PD has requested or used more power than the port can deliver, and is powered down. **PoE turned OFF**: PD is off. **Invalid PD**: PD detected, but is not working correctly.

5.12.3 POE Schedule Configuration

PoE (Power Over Ethernet) Schedule configuration is performed here.



Power Over Ethernet Schedule Configuration

Configure port # 1

Schedule Mode Disabled

□ Select all

Hour		Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00	□	□	□	□	□	□	□	□
01	□	□	□	□	□	□	□	□
02	□	□	□	□	□	□	□	□
03	□	□	□	□	□	□	□	□
04	□	□	□	□	□	□	□	□
05	□	□	□	□	□	□	□	□
06	□	□	□	□	□	□	□	□
07	□	□	□	□	□	□	□	□
08	□	□	□	□	□	□	□	□
09	□	□	□	□	□	□	□	□
10	□	□	□	□	□	□	□	□

Configure port #: At the dropdown, select port number (e.g., **1-8**) for PoE scheduling configuration.

Schedule Mode: at the dropdown select **Enabled** or **Disabled** (default).

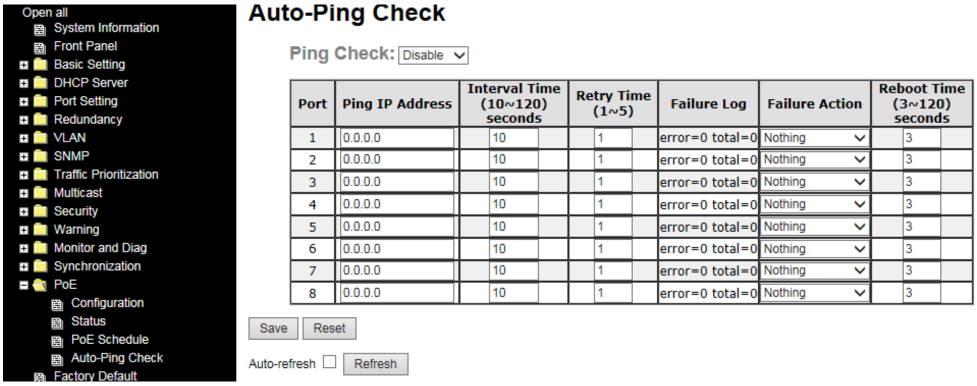
Select all: Check to select all available scheduling.

Hour: Check the checkbox for hourly scheduling.

Sunday – Saturday: Check the checkbox for daily scheduling.

5.12.4 Auto-Ping Check

PoE (Power Over Ethernet) automatic Ping checking is configured here.



Auto-Ping Check

Ping Check: Disable

Port	Ping IP Address	Interval Time (10~120) seconds	Retry Time (1~5)	Failure Log	Failure Action	Reboot Time (3~120) seconds
1	0.0.0.0	10	1	error=0 total=0	Nothing	3
2	0.0.0.0	10	1	error=0 total=0	Nothing	3
3	0.0.0.0	10	1	error=0 total=0	Nothing	3
4	0.0.0.0	10	1	error=0 total=0	Nothing	3
5	0.0.0.0	10	1	error=0 total=0	Nothing	3
6	0.0.0.0	10	1	error=0 total=0	Nothing	3
7	0.0.0.0	10	1	error=0 total=0	Nothing	3
8	0.0.0.0	10	1	error=0 total=0	Nothing	3

Port: the port being configured.

Ping IP Address: the address to ping.

Interval Time (10~120) seconds: the time in seconds between pings.

Retry Time (1~5): the number of times to retry before quitting retry attempts.

Failure Log: e.g., error=0 total=0.

Failure Action: the action to take upon ping failure (Nothing, Restart Forever, Restart Once, Power On, Power Down).

Reboot Time (3~120) seconds:

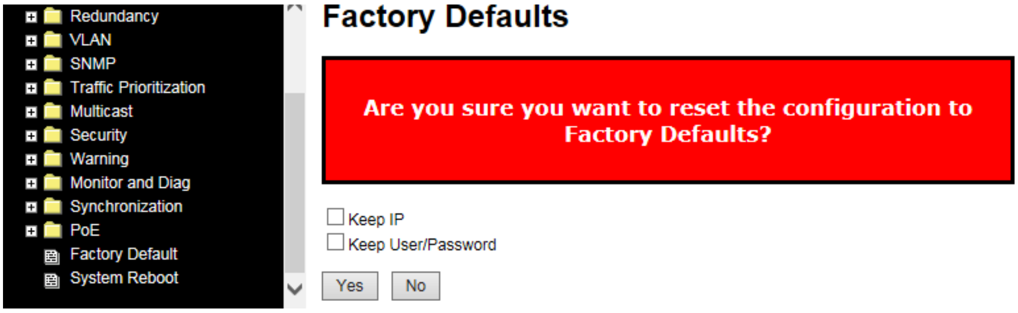
5.13 TROUBLESHOOTING

5.13.1 Factory Defaults

This function is to force the switch back to the original factory settings.

To reset the switch, select **Reset to Factory Defaults** from the drop-down list and click **Yes**. Use the checkboxes to retain the IP configuration and/or the Username / Password currently configured.

Click **No** to return to the Port State page without rebooting.



Factory Defaults

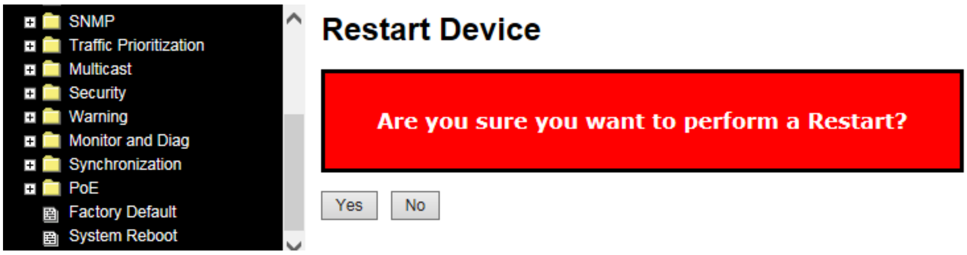
Are you sure you want to reset the configuration to Factory Defaults?

□ Keep IP

□ Keep User/Password

5.13.2 System Reboot

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



Restart Device

Are you sure you want to perform a Restart?

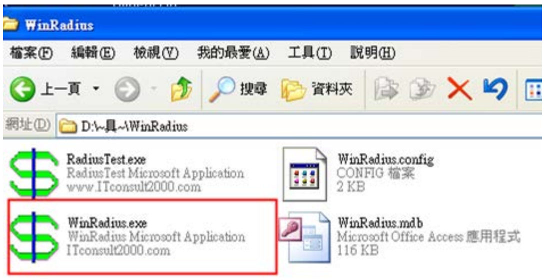
Label	Description
Yes	Click to reboot device.
No	Click to return to the **Port State** page without rebooting.

6. Radius Server and Switch Settings

This section provides MS WinRadius and Windows / PC settings. See section 5.1.8.6 - “802.1x 802.1x - Radius Server” for the switch’s RADIUS parameter descriptions.

Radius Server and Switch Setting

1. Enable the WinRadius tool.



D:\~具~\WinRadius

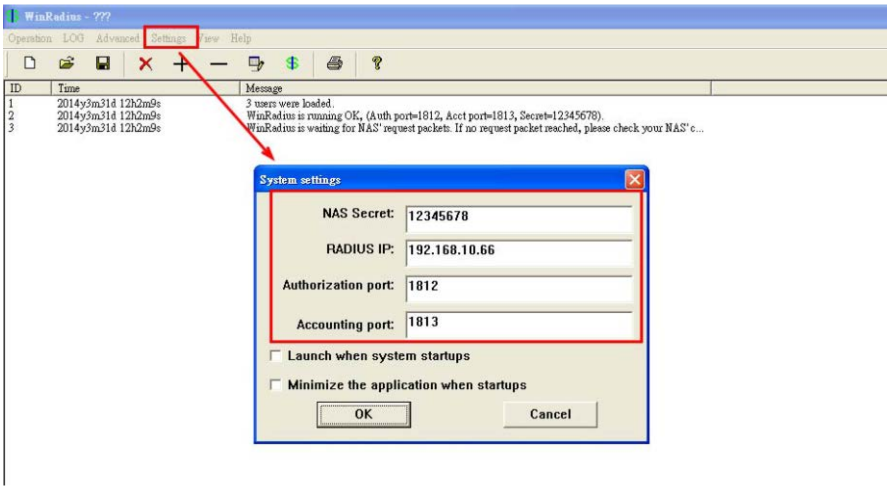
RadiusTest.exe
RadiusTest Microsoft Application
www.ITconsult2000.com

WinRadius.config
CONFIG 檔案
2 KB

WinRadius.exe
WinRadius Microsoft Application
ITconsult2000.com

WinRadius.mdb
Microsoft Office Access 應用程式
116 KB

2. Set the Radius Server IP、NSA and Port.



ID	Time	Message
1	2014y3m31d 12h2m9s	3 users were loaded.
2	2014y3m31d 12h2m9s	WinRadius is running OK, (Auth port=1812, Acct port=1813, Secret=12345678).
3	2014y3m31d 12h2m9s	WinRadius is waiting for NAS' request packets. If no request packet reached, please check your NAS' c...

NAS Secret: 12345678

RADIUS IP: 192.168.10.66

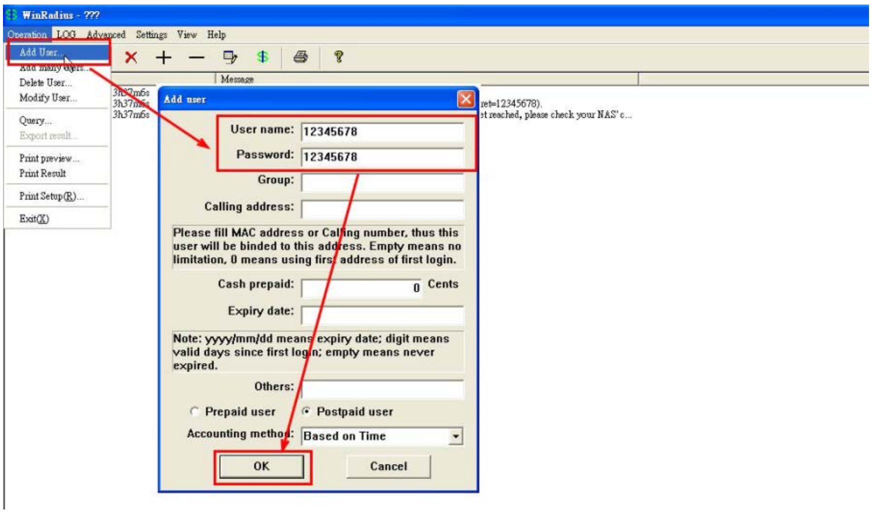
Authorization port: 1812

Accounting port: 1813

☐ Launch when system startups

☐ Minimize the application when startups

3. Create a new User.



User name: 12345678

Password: 12345678

Group:

Calling address:

Please fill MAC address or Calling number, thus this user will be binded to this address. Empty means no limitation, 0 means using first address of first login.

Cash prepaid: 0 Cents

Expiry date:

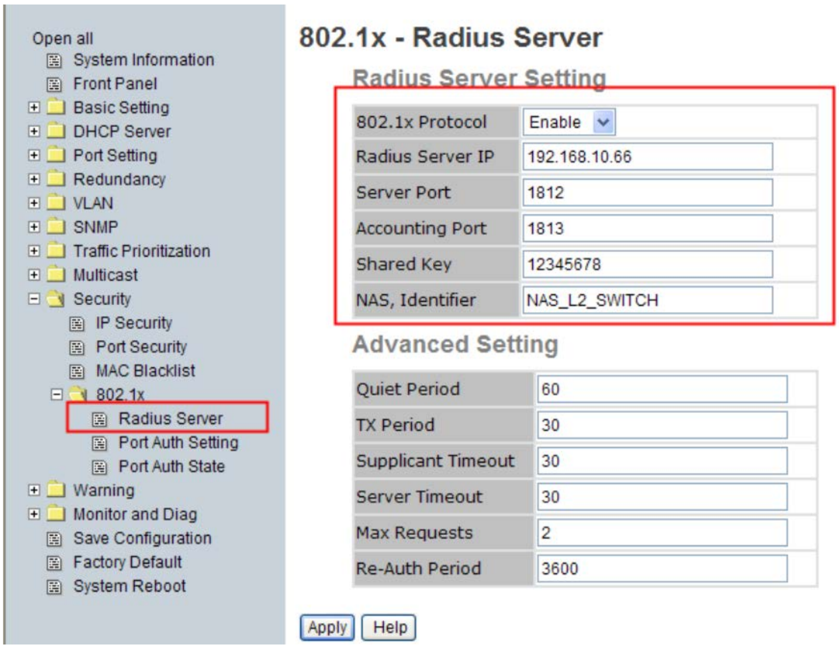
Note: yyyy/mm/dd means expiry date; digit means valid days since first login; empty means never expired.

Others:

○ Prepaid user ● Postpaid user

Accounting method: Based on Time

4. Enter the Switch Radius Server settings. Note: all settings need the same Radius Server settings.



802.1x - Radius Server

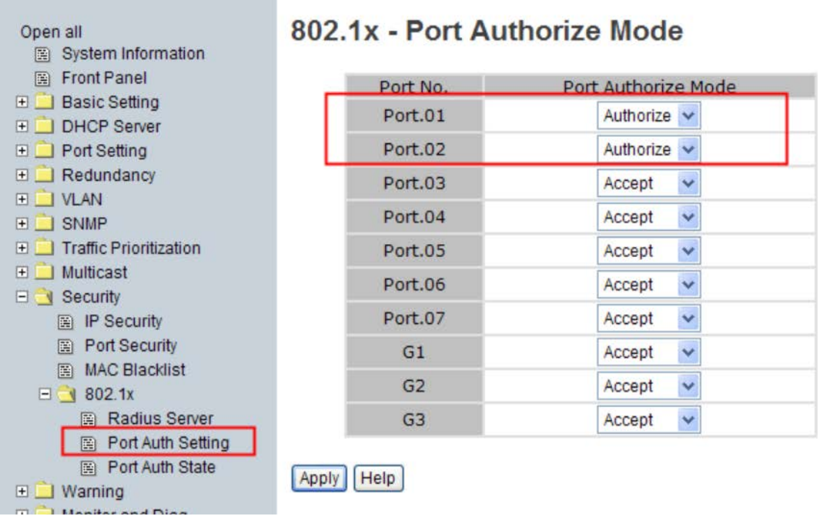
Radius Server Setting

802.1x Protocol	Enable
Radius Server IP	192.168.10.66
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

Advanced Setting

Quiet Period	60
TX Period	30
Supplicant Timeout	30
Server Timeout	30
Max Requests	2
Re-Auth Period	3600

5. Select 802.1x Authorize Port (e.g., select Port 1 and Port 2 = Authorize).



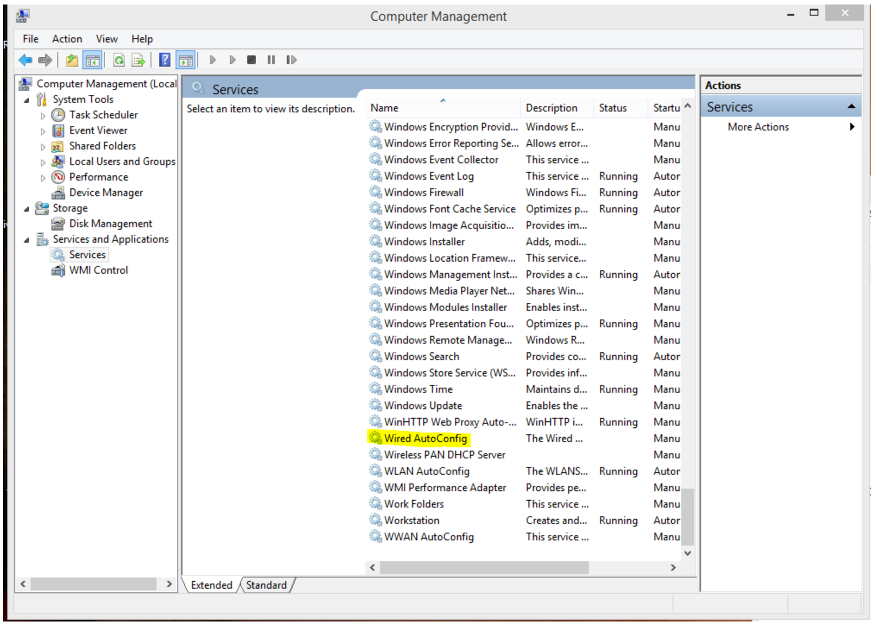
802.1x - Port Authorize Mode

Port No.	Port Authorize Mode
Port.01	Authorize
Port.02	Authorize
Port.03	Accept
Port.04	Accept
Port.05	Accept
Port.06	Accept
Port.07	Accept
G1	Accept
G2	Accept
G3	Accept

6. Continue with the User PC Setting section below.

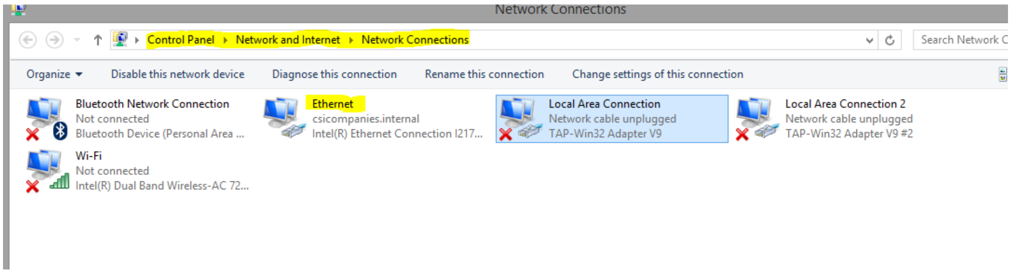
User PC Settings

1. Enable Windows 802.1x Services: To complete this procedure, you must first enable the Wired AutoConfig service, which is turned off by default.
   a. Click the **Start** button. In the search box, type **services.msc**, and then press Enter. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
   b. In the Services dialog box, click the **Standard** tab at the bottom of main pane, right-click **Wired AutoConfig**, and then click **Start**.



Name	Description	Status	Startu
Windows Encryption Provid...	Windows E...		Manu
Windows Error Reporting Se...	Allows error...		Manu
Windows Event Collector	This service ...		Manu
Windows Event Log	This service ...	Running	Autor
Windows Firewall	Windows Fi...	Running	Autor
Windows Font Cache Service	Optimizes p...	Running	Autor
Windows Image Acquisitio...	Provides im...		Manu
Windows Installer	Adds, modi...		Manu
Windows Location Framew...	This service...		Manu
Windows Management Inst...	Provides a c...	Running	Autor
Windows Media Player Net...	Shares Win...		Manu
Windows Modules Installer	Enables inst...		Manu
Windows Presentation Fou...	Optimizes p...	Running	Manu
Windows Remote Manage...	Windows R...		Manu
Windows Search	Provides co...	Running	Autor
Windows Store Service (WS...	Provides inf...		Manu
Windows Time	Maintains d...	Running	Manu
Windows Update	Enables the ...		Manu
WinHTTP Web Proxy Auto-...	WinHTTP i...	Running	Manu
Wired AutoConfig	The Wired ...		Manu
Wireless PAN DHCP Server			Manu
WLAN AutoConfig	The WLANS...	Running	Autor
WMI Performance Adapter	Provides pe...		Manu
Work Folders	This service ...		Manu
Workstation	Creates and...	Running	Autor
WWAN AutoConfig	This service ...		Manu

   c. Open Network Connections by clicking the **Start** button, and then clicking **Control Panel**. In the search box, type **adapter**, and then, under Network and Sharing Center, click **View network connections**.
   d. Right-click the connection that you want to enable 802.1X authentication for, and then click **Properties**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.



Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...

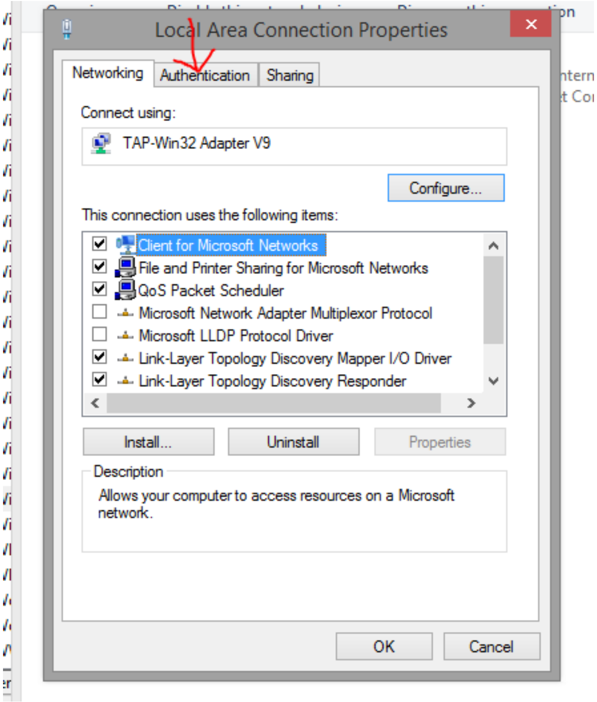
Ethernet
csicompanies.internal
Intel(R) Ethernet Connection I217...

Local Area Connection
Network cable unplugged
TAP-Win32 Adapter V9

Local Area Connection 2
Network cable unplugged
TAP-Win32 Adapter V9 #2

Wi-Fi
Not connected
Intel(R) Dual Band Wireless-AC 72...

a. Click the **Authentication** tab, and then select the **Enable IEEE 802.1X authentication** check box.



Local Area Connection Properties

Connect using:

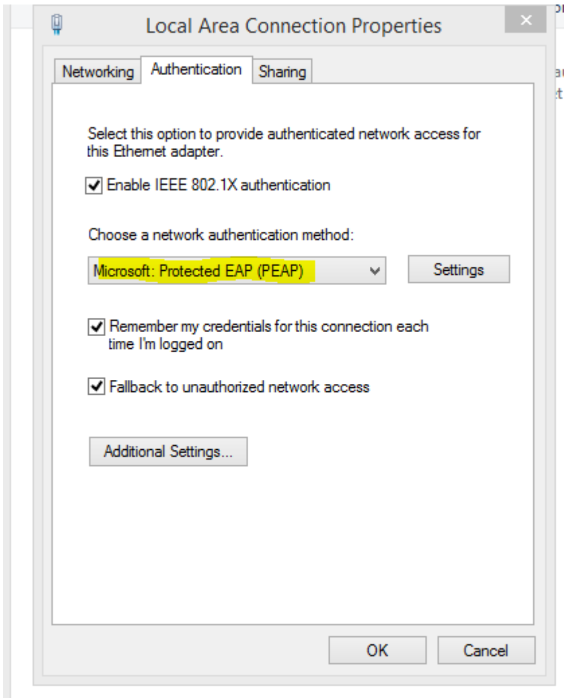
TAP-Win32 Adapter V9

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☐ Microsoft LLDP Protocol Driver
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Allows your computer to access resources on a Microsoft network.



Local Area Connection Properties

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

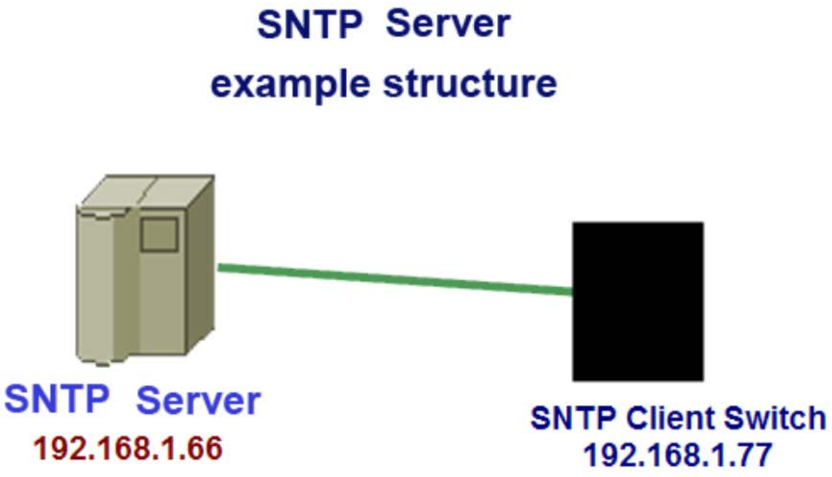
☑ Fallback to unauthorized network access

b. In the **Choose a network authentication method** list, click the method you want to use.

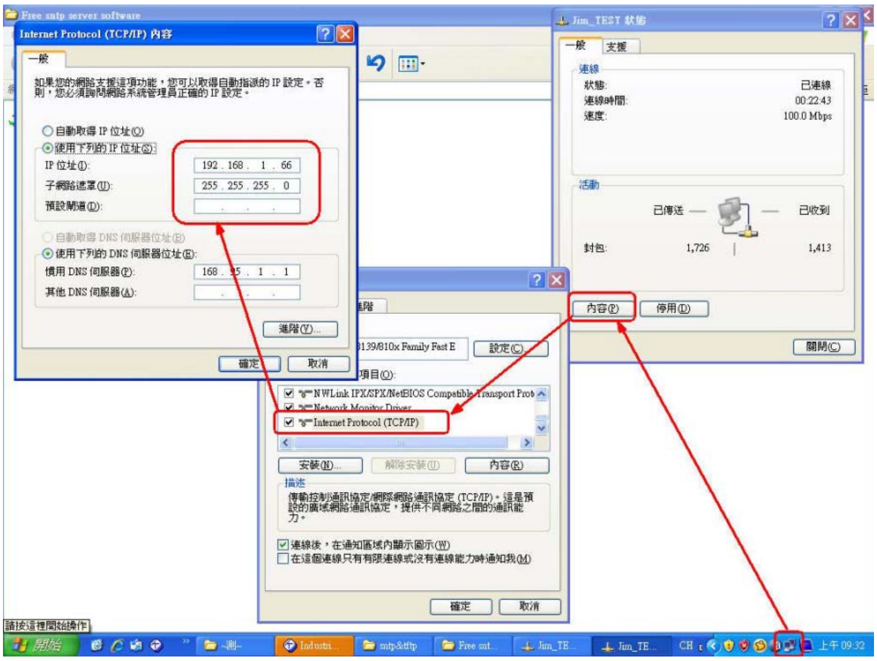
To configure additional settings, click **Settings**.

7. SNTP Server Setup

This section provides a sample setup procedure for the following SNTP server/client configuration.



1. Set up IP of PC (e.g., 192.168.1.66 / 24).



Internet Protocol (TCP/IP) 內容

如果您的網路支援這項功能，您可以取得自動指派的 IP 設定。否則，您必須詢問網路系統管理員正確的 IP 設定。

○ 自動取得 IP 位址(O)
● 使用下列的 IP 位址(S):
IP 位址(I): 192 . 168 . 1 . 66
子網路遮罩(U): 255 . 255 . 255 . 0
預設閘道(D): . . .

○ 自動取得 DNS 伺服器位址(B)
● 使用下列的 DNS 伺服器位址(E):
慣用 DNS 伺服器(P): 168 . 95 . 1 . 1
其他 DNS 伺服器(A): . . .

☑ NWLink IPX/SPX/NetBIOS Compatible Transport Prot
☑ Network Monitor Driver
☑ Internet Protocol (TCP/IP)

描述
傳輸控制通訊協定/網際網路通訊協定 (TCP/IP)。這是預設的廣域網路通訊協定，提供不同網路之間的通訊能力。

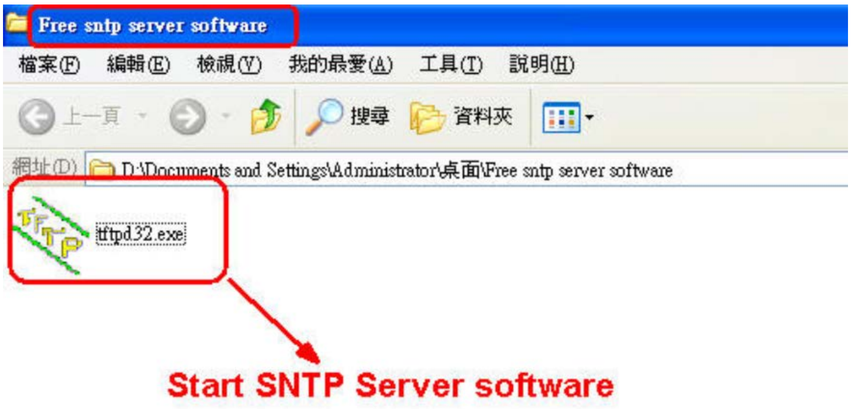
☑ 連線後，在通知區域內顯示圖示(W)
□ 在這個連線只有有限連線或沒有連線能力時通知我(M)

Jim_TEST 狀態

連線
狀態: 已連線
連線時間: 00:22:43
速度: 100.0 Mbps

活動
已傳送 — 已收到
封包: 1,726 | 1,413

2. Start the SNTP Server software, making the PC into an SNTPand Syslog Server (this example uses the free tool tftpd32).



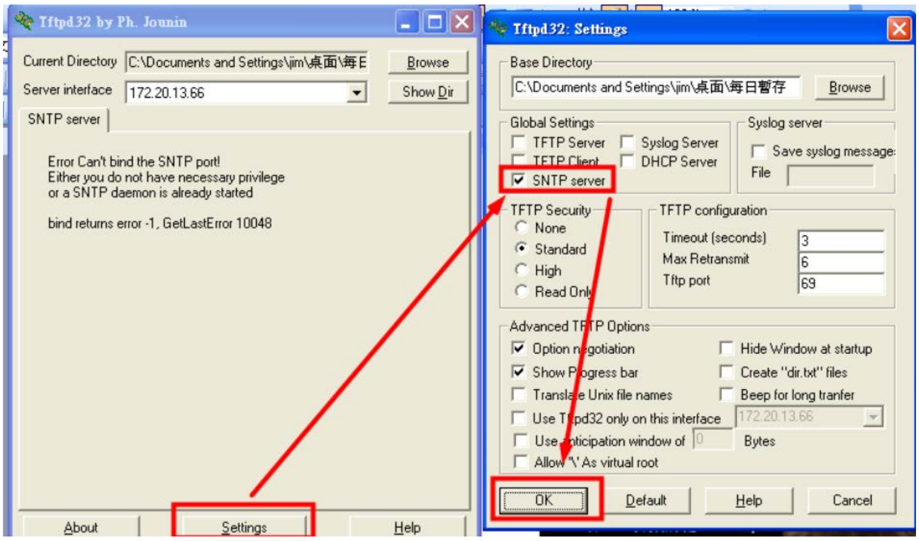
Free sntp server software

網址(D) D:\Documents and Settings\Administrator\桌面\Free sntp server software

tftpd32.exe

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
資料夾
Start SNTP Server software

3. Confirm whether to open the SNTP function.



Tftpd32 by Ph. Jounin

Current Directory: C:\Documents and Settings\jim\桌面\每E

Server interface: 172.20.13.66

SNTP server

Error Can't bind the SNTP port!
Either you do not have necessary privilege
or a SNTP daemon is already started

bind returns error -1, GetLastError 10048

Tftpd32: Settings

Base Directory: C:\Documents and Settings\jim\桌面\每日暫存

Global Settings: □ TFTP Server □ Syslog Server □ TFTP Client □ DHCP Server ☑ SNTP server

Syslog server: □ Save syslog message File

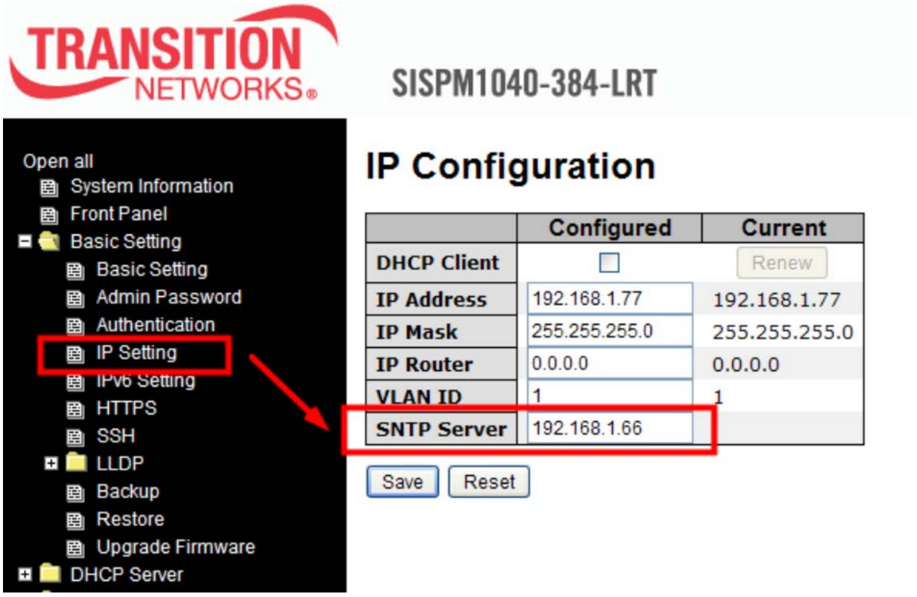
TFTP Security: ○ None ● Standard ○ High ○ Read Only

TFTP configuration: Timeout (seconds) 3; Max Retransmit 6; Tftp port 69

Advanced TFTP Options:
☑ Option negotiation □ Hide Window at startup
☑ Show Progress bar □ Create "dir.txt" files
□ Translate Unix file names □ Beep for long tranfer
□ Use Tftpd32 only on this interface 172.20.13.66
□ Use anticipation window of 0 Bytes
□ Allow '\' As virtual root

4. Set up and finish, then restart the software.

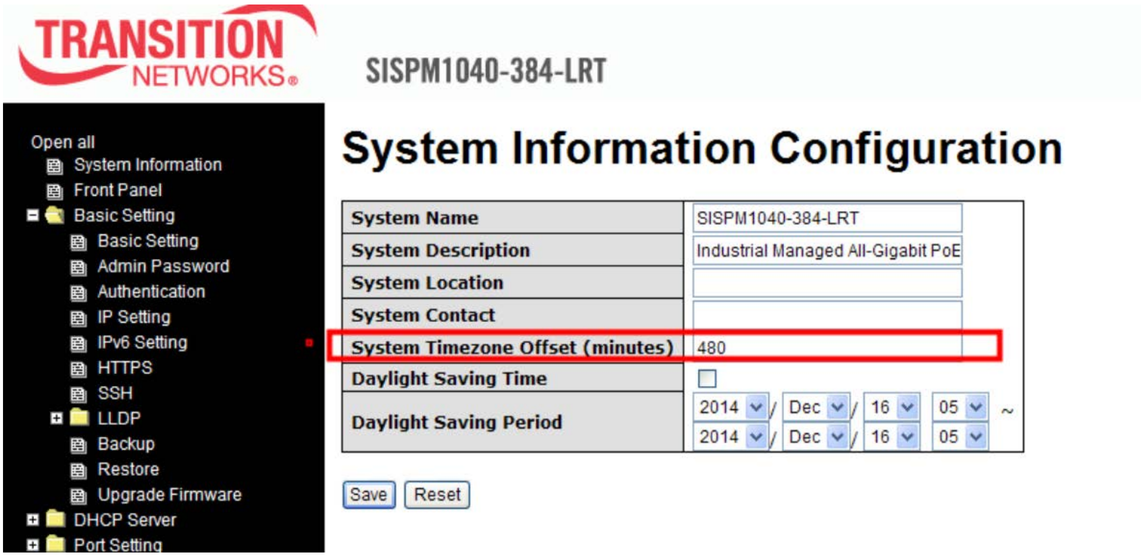
5. At the **Basic Setting** > **IP Setting** menu path, set the SNTP Server IP Address and clcik the **Save** button.



IP Configuration

	Configured	Current
DHCP Client	□	Renew
IP Address	192.168.1.77	192.168.1.77
IP Mask	255.255.255.0	255.255.255.0
IP Router	0.0.0.0	0.0.0.0
VLAN ID	1	1
SNTP Server	192.168.1.66	

6. At the **Basic Setting** > **Basic Setting** menu path, set the SNTP Timezone.



System Information Configuration

System Name	SISPM1040-384-LRT
System Description	Industrial Managed All-Gigabit PoE
System Location	
System Contact	
System Timezone Offset (minutes)	480
Daylight Saving Time	□
Daylight Saving Period	2014 / Dec / 16 05 ~ 2014 / Dec / 16 05

7. Observe the system time at the **System Information** page in the System Timezone Offset field.

8. Command Line Interface

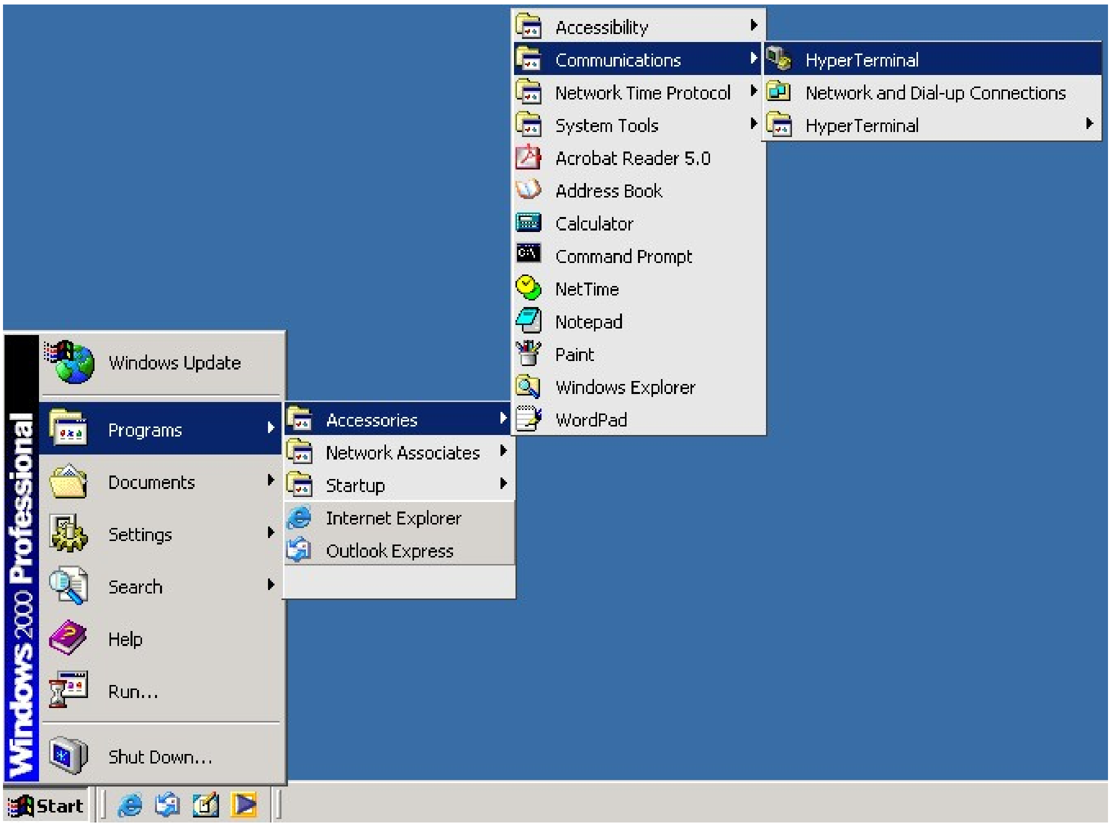
Besides Web-based management, the switch also supports CLI management. You can use console or telnet to manage the switch by CLI.

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

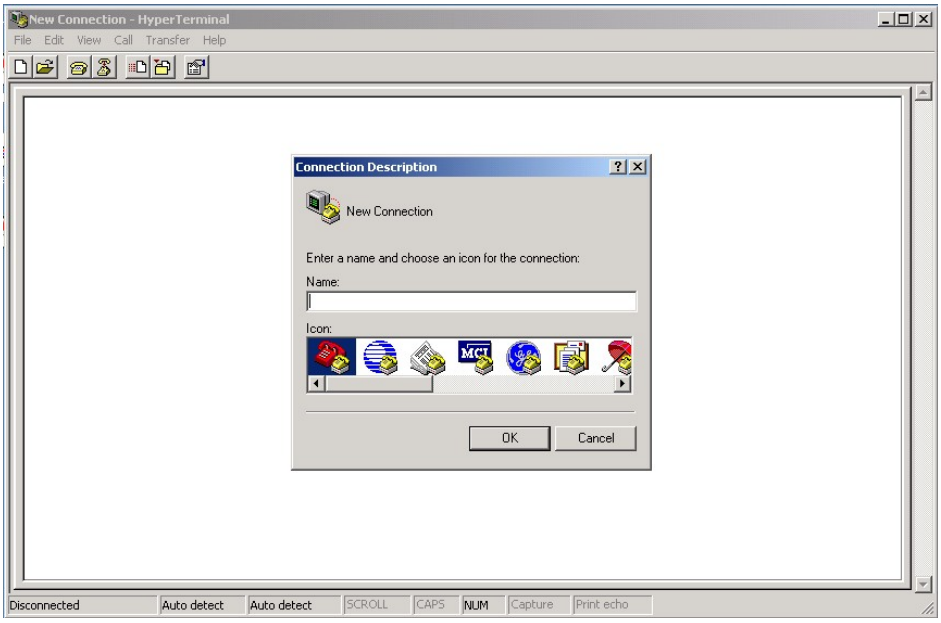
Before configuring RS-232 serial console, connect the RS-232 port of the switch to your PC Com port using a RJ45 to DB9-F cable.

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

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



Step 2. Input a name for the new connection.



Connection Description

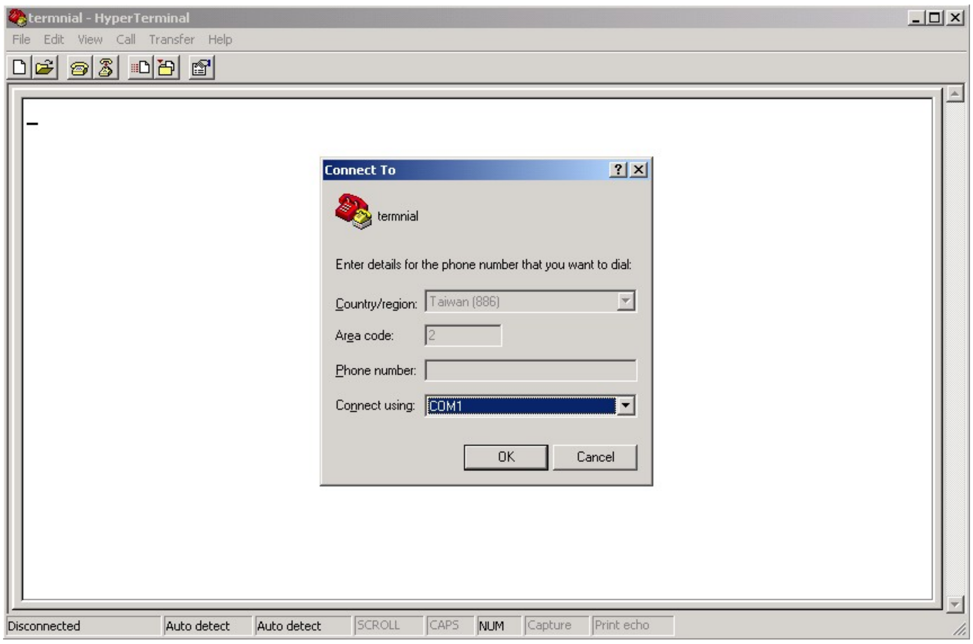
New Connection

Enter a name and choose an icon for the connection:

Name:

Icon:

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



Connect To

termnial

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

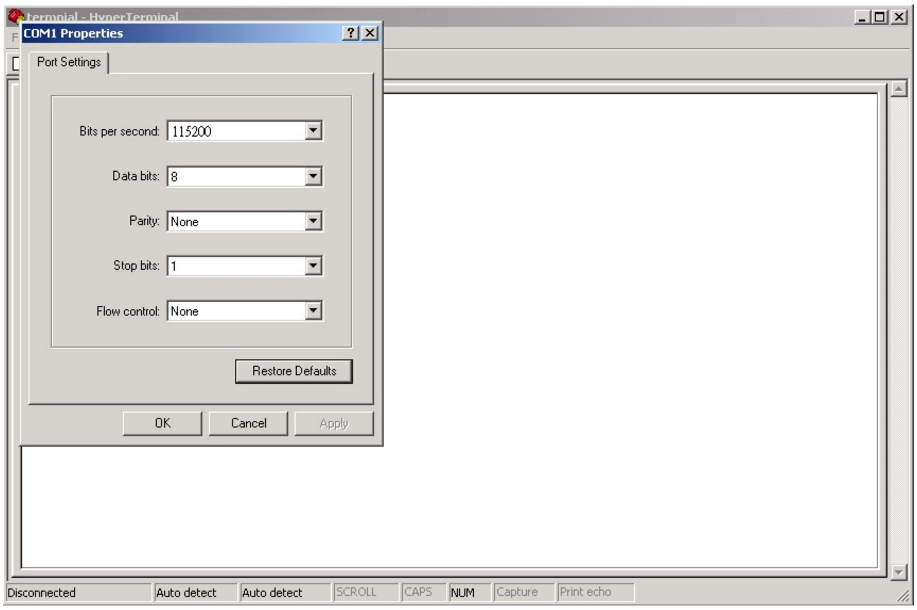
Country/region: Taiwan (886)

Area code: 2

Phone number:

Connect using: COM1

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



COM1 Properties

Port Settings

Bits per second: 115200

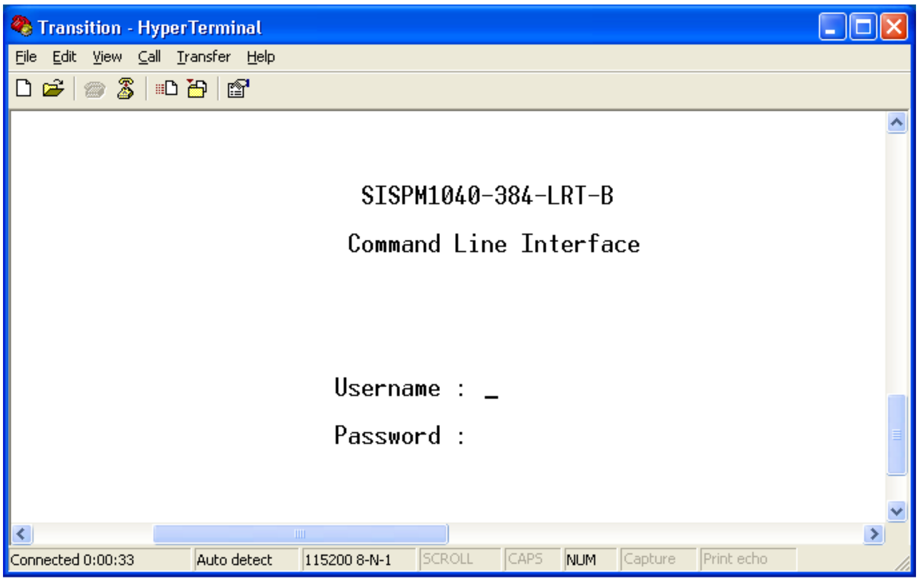
Data bits: 8

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 by Telnet

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

IP Address: **192.168.1.77/24**

Subnet Mask: **255.255.255.0**

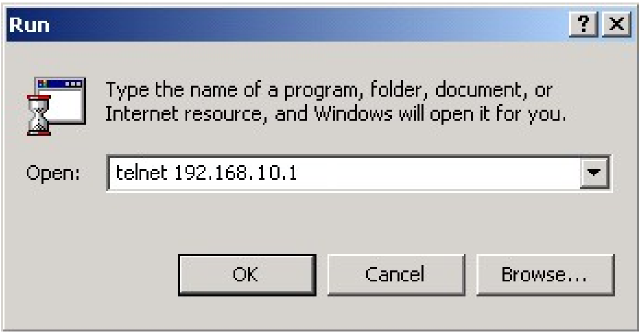
Default Gateway: **192.168.1.254**

User Name: **root**

Password: **root**

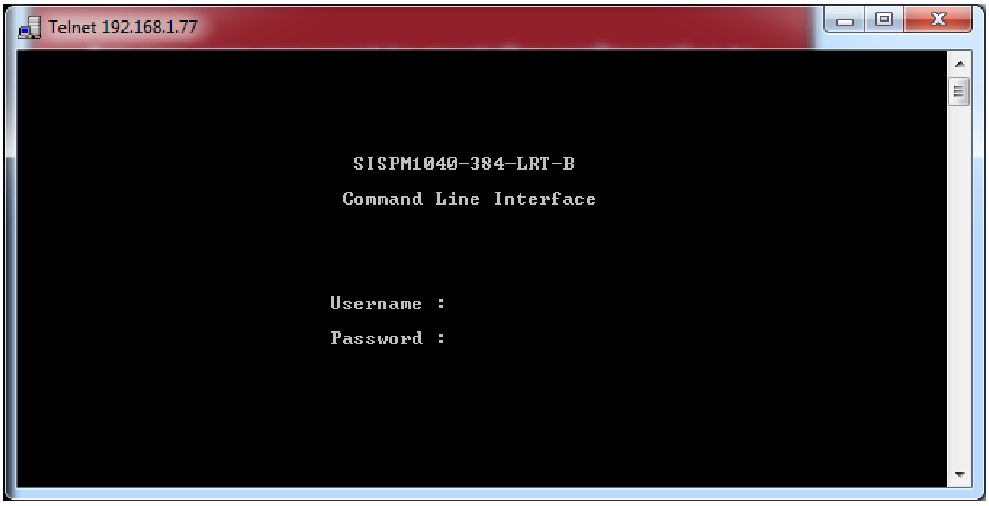
Follow the steps below to access console via Telnet.

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


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

Open: telnet 192.168.10.1

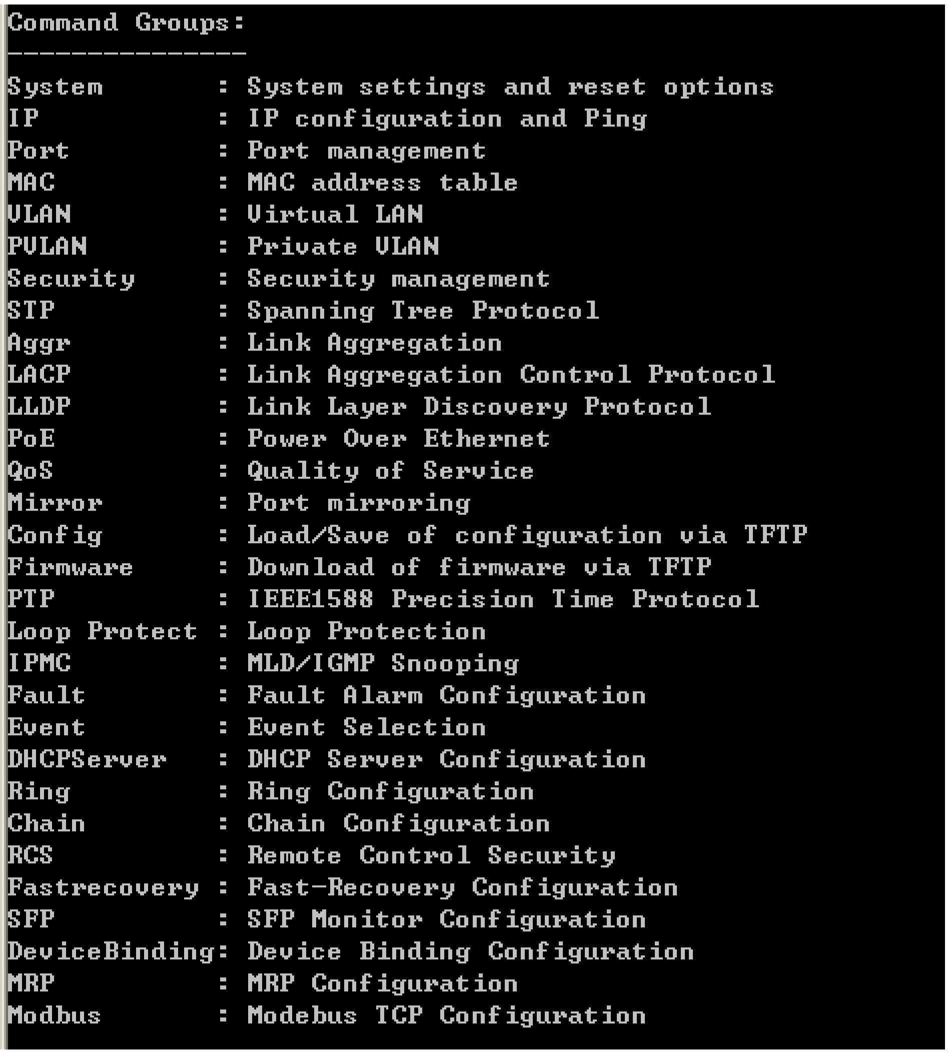
Step 2. The Login screen will appear. Use the keyboard to enter the Username and Password (same as the password for Web browser), and then press **Enter.**



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


Username :
Password :
```

CLI 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

<table>
<tr><td rowspan="10">Security/Network/NAS></td><td>Configuration [<port_list>]</td></tr>
<tr><td>Mode [enable|disable]</td></tr>
<tr><td>State [<port_list>] [auto|authorized|unauthorized|macbased]</td></tr>
<tr><td>Reauthentication [enable|disable]</td></tr>
<tr><td>ReauthPeriod [<reauth_period>]</td></tr>
<tr><td>EapolTimeout [<eapol_timeout>]</td></tr>
<tr><td>Agetime [<age_time>]</td></tr>
<tr><td>Holdtime [<hold_time>]</td></tr>
<tr><td>Authenticate [<port_list>] [now]</td></tr>
<tr><td>Statistics [<port_list>] [clear|eapol|radius]</td></tr>
</table>

Security Network ACL Commands

<table>
<tr><td rowspan="9">Security/Network/ACL></td><td>Configuration [<port_list>]</td></tr>
<tr><td>Action [<port_list>] [permit|deny] [<rate_limiter>][<port_redirect>] [<mirror>] [<logging>] [<shutdown>]</td></tr>
<tr><td>Policy [<port_list>] [<policy>]</td></tr>
<tr><td>Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]</td></tr>
<tr><td>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>]</td></tr>
<tr><td>Delete <ace_id></td></tr>
<tr><td>Lookup [<ace_id>]</td></tr>
<tr><td>Clear</td></tr>
<tr><td>Status [combined|static|loop_protect|dhcp|ptp|ipmc|conflicts]</td></tr>
</table>

	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>]

Aggr 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>]

PoE Commands

<table>
<tr><td rowspan="7">PoE></td><td>Configuration [<port_list>]</td></tr>
<tr><td>Mode [<port_list>] [disabled|poe|poe+]</td></tr>
<tr><td>Priority [<port_list>] [low|high|critical]</td></tr>
<tr><td>Mgmt_mode [class_con|class_res|al_con|al_res|lldp_res|lldp_con]</td></tr>
<tr><td>Maximum_Power [<port_list>] [<port_power>]</td></tr>
<tr><td>Status</td></tr>
<tr><td>Primary_Supply [<supply_power>]</td></tr>
</table>

QoS Commands

<table>
<tr><td rowspan="15">QoS></td><td>DSCP Map [<dscp_list>] [<class>] [<dpl>]</td></tr>
<tr><td>DSCP Translation [<dscp_list>] [<trans_dscp>]</td></tr>
<tr><td>DSCP Trust [<dscp_list>] [enable|disable]</td></tr>
<tr><td>DSCP Classification Mode [<dscp_list>] [enable|disable]</td></tr>
<tr><td>DSCP Classification Map [<class_list>] [<dpl_list>] [<dscp>]</td></tr>
<tr><td>DSCP EgressRemap [<dscp_list>] [<dpl_list>] [<dscp>]</td></tr>
<tr><td>Storm Unicast [enable|disable] [<packet_rate>]</td></tr>
<tr><td>Storm Multicast [enable|disable] [<packet_rate>]</td></tr>
<tr><td>Storm Broadcast [enable|disable] [<packet_rate>]</td></tr>
<tr><td>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>]</td></tr>
<tr><td>QCL Delete <qce_id></td></tr>
<tr><td>QCL Lookup [<qce_id>]</td></tr>
<tr><td>QCL Status [combined|static|conflicts]</td></tr>
<tr><td>QCL Refresh</td></tr>
</table>

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>]

Firmware Commands

Firmware>	Load <ip_addr_string> <file_name>

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

FastRecovery Commands

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

SFP Commands

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

DeviceBinding Commands

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

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

MRP 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>]

Modbus Commands

Modbus>	Status
	Mode [enable|disable]

9. Technical Specifications

Switch Model	**SISPM1040-384-LRT-B**
Physical Ports	
10/100/1000Base-T(X) with P.S.E. Ports in RJ45 Auto MDI/MDIX	**8**
100/1000Base-X with SFP port	**4**
Technology	
Ethernet Standards	IEEE 802.3 for 10/100/1000Base-T, and PoE+ IEEE 802.3u for 100Base-TX and 100Base-FX IEEE 802.3ab for 1000Base-T IEEE 802.z for 1000Base-X 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) IEEE 802.3at PoE specification (up to 25.5W delivered to load 30W out of PSE port)
MAC Table	8k
Priority Queues	8
Processing	Store-and-Forward
Buffer Size	4Mbit
Switch Properties	Switching latency: 7 us Switching bandwidth: 24Gbps Max. Number of Available VLANs: 256 IGMP multicast groups: 128 for each VLAN Port rate limiting: User defined
Jumbo frame	Up to 9.6K Bytes
Security Features	Device Binding security feature Enable/disable ports, MAC based port security Port based network access control (802.1x) VLAN (802.1Q) to segregate and secure network traffic Radius centralized password management SNMPv3 encrypted authentication and access security HTTPS / SSH enhance network security

Software Features	STP/RSTP/MSTP (IEEE 802.1D/w/s) Redundant Ring (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 Snooping IP-based bandwidth management Application-based QoS management DOS/DDOS auto prevention Port configuration, status, statistics, monitoring, security DHCP Server/Client/Relay SMTP Client Modbus TCP NTP server STP/RSTP/MSTP (IEEE 802.1D/w/s) Redundant Ring with recovery time less than 30ms over 250 units
Network Redundancy	Redundant Ring / Multiple Rings / Fast Recovery MRP MSTP (RSTP/STP compatible) Modbus TCP NTP server
RS-232 Serial Console Port	RS-232 in RJ45 connector with console cable. 115200bps, 8, N, 1
LED indicators	
Power Indicator (PWR)	Green : Power LED x 2
Ring Master Indicator (R.M.)	Green : Indicates that the system is operating in Redundant Ring Master mode
Redundant Ring Indicator (Ring)	Green : Indicates that the system operating in Redundant Ring mode Green Blinking: Indicates that the Ring is broken.
Fault Indicator (Fault)	Amber : Indicate unexpected event occurred
10/100/1000Base-T(X) RJ45 Port Indicator	Dual color LED: Green for 1000Mbps Link/Act indicator. Amber for 10/100Mbps Link/Act indicator.
100/1000Base-X SFP Port Indicator	Green for port Link/Act.
PoE Indicator	Green : PoE enabled LED x 8
Fault contact	
Relay	Relay output to carry capacity of 1A at 24VDC
Power	
Redundant Input power	Dual DC inputs. 52~57VDC on 6-pin terminal block
Power consumption (Typ.)	13.2 Watts
Overload current protection	Present
Reverse Polarity Protection	Present
Physical Characteristic	
Enclosure	IP-30
Dimension (W x D x H)	96.4 (W) x 105.5 (D) x 154 (H) mm (3.8 x 4.15 x 6.06 inches)

Weight	1205 g (2.65 pounds)
Environmental	
Storage Temperature	-40° to 85°C (-40 to 185°F)
Operating Temperature	-40° to 70°C (-40 to 158°F) 70° C with industrial temperature SFPs
Operating Humidity	5% to 95% Non-condensing
Regulatory approvals	
EMI	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD) EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11
Shock	IEC60068-2-27
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6
Safety	EN60950-1, UL 60950-1
MTBF	188,236 Hours (MIL-HDBK-217F2, GB, GC, 25°C)

10. Service, Warranty & Compliance Information

Service

Direct Contact Numbers:

Domestic:	+ 1 800-260-1312
International:	+ 1 952-358-3601
Fax	+1 952-941-2322
Email:	techsupport@transition.com

Service Hours:

USA:7 AM until 8 PM CST Monday to Friday.

Out of Hours the calls will be answered by an on-call engineer.

Live Help Online Support: Chat live with a Transition Networks representative at http://transition.com/TransitionNetworks/TechSupport/ContactUs.aspx.

Warranty

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' behalf.

Limited Lifetime Warranty

Effective for Products Shipped May 1, 1999 and After. Every Transition Networks labeled product purchased after May 1, 1999, and not covered by a fixed-duration warranty will be free from defects in material and workmanship for its lifetime. This warranty covers the original user only and is not transferable.

This warranty does not cover damage from accident, acts of God, neglect, contamination, misuse or abnormal conditions of operation or handling, including over-voltage failures caused by use outside of the product's specified rating, or normal wear and tear of mechanical components. If the user is unsure about the proper means of installing or using the equipment, contact Transition Networks's free technical support services.

Transition Networks will, at its option:

- Repair the defective product to functional specification at no charge
- Replace the product with an equivalent functional product
- Refund a portion of purchase price based on a depreciated value

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:

Service Hours

USA: 8:00 PM Sunday through 8:00 PM Friday CST
After Hours: Calls will be answered by an on call engineer.

Direct Contact Numbers

Domestic: + 1 800-260-1312
International: + 1 952-358-3601
Fax: +1 952-941-2322
Email: techsupport@transition.com   Online Support
Live Help: Chat live with a Transition Networks representative.

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.

11. Regulatory Agency Information

Regulatory approvals

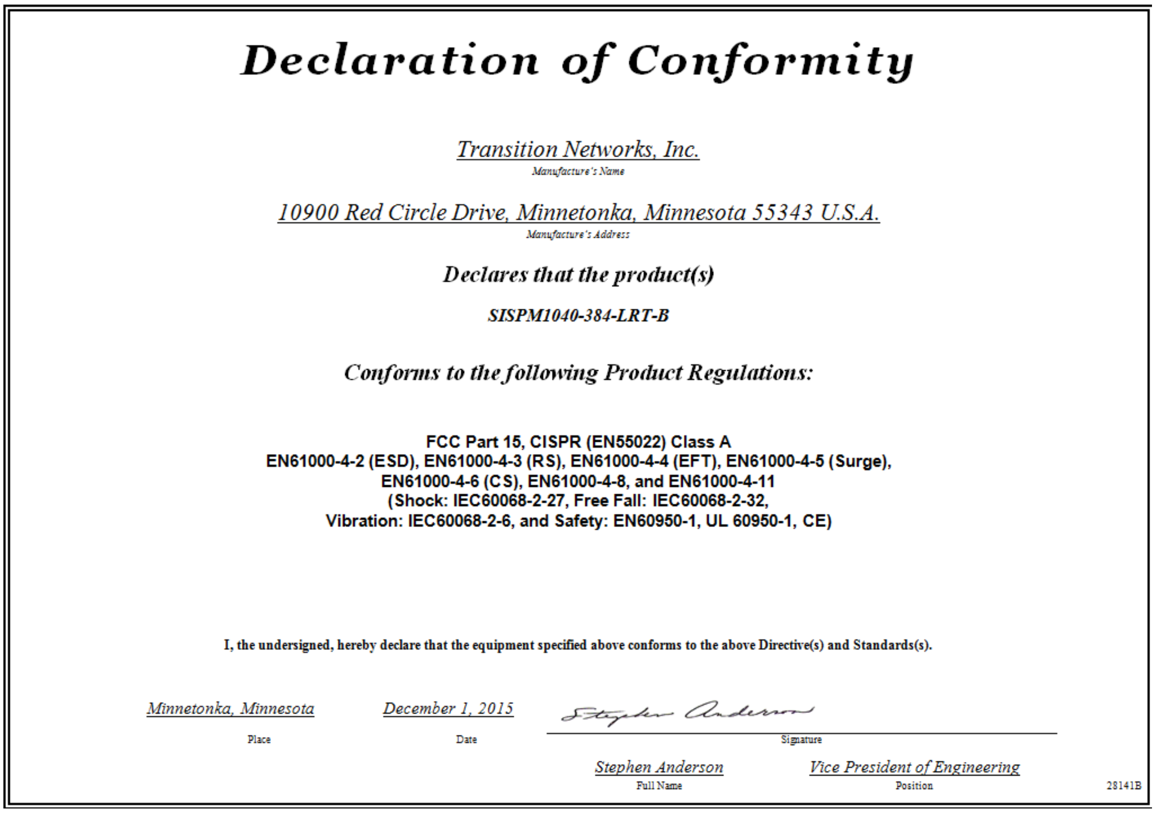
EMI FCC Part 15, CISPR (EN55022) Class A

EMS EN61000-4-2 (ESD)

EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11

Shock	IEC60068-2-27
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6
Safety	EN60950-1, UL 60950-1, CE

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)

SISPM1040-384-LRT-B

Conforms to the following Product Regulations:

FCC Part 15, CISPR (EN55022) Class A
EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge),
EN61000-4-6 (CS), EN61000-4-8, and EN61000-4-11
(Shock: IEC60068-2-27, Free Fall: IEC60068-2-32,
Vibration: IEC60068-2-6, and Safety: EN60950-1, UL 60950-1, CE)

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

Minnetonka, Minnesota — Place
December 1, 2015 — Date
Signature

Stephen Anderson — Full Name
Vice President of Engineering — Position

28141B

12. Power Supply Information

Several power supply models are available from Transition Networks. **Warning**: You must use an isolated power supply in order for Transition Networks to honor the warranty. The power supply that Transition Networks makes available is 25104; Industrial Power Supply 48-55VDC 240W.

Industrial Power Supply 25104 (Mean Well SDR-240-48)

INPUT: 100-240VAC 2.6A 50/60 Hz

OUTPUT: 48V - 5A

“Use copper wire only”

“Maximum surrounding air temperature: 60°C”

“Instructions for installation in a pollution degree 2 environment”

Terminal Torque: 7 Lb-in (DC connections at top of PS).

Terminal Torque: 4.4 Lb-in (AC connections at bottom of PS).

+V ADJ: access to small Phillips screw; turn clockwise to increase voltage. Adjustable, 48-55V. Recommend adjusting output to a minimum 52V out for PoE+ applications.

DC OK LED: lights to indicate a DC OK condition.

See the *SISPM1040-384-LRT-B Quick Start Guide* (PN 33616) for Power Requirements, Isolation, Redundant Power Inputs, Power Connection, and Chassis Ground information. To access the manuals, firmware, datasheet or other documentation for your product, enter your model number: SISPM1040-384-LRT-B in the “Search” box at our website at www.transition.com.

Voltage Isolation

Warning: To meet isolation requirements you must use an isolated power supply.

IEEE 802.3at defines power isolation of 1500 VAC and 2250 VAC.

- port-to-case
- port-to-port; to achieve port to port isolation, use a mid-span injector (see Software Features on page 9).
- port-to-power.

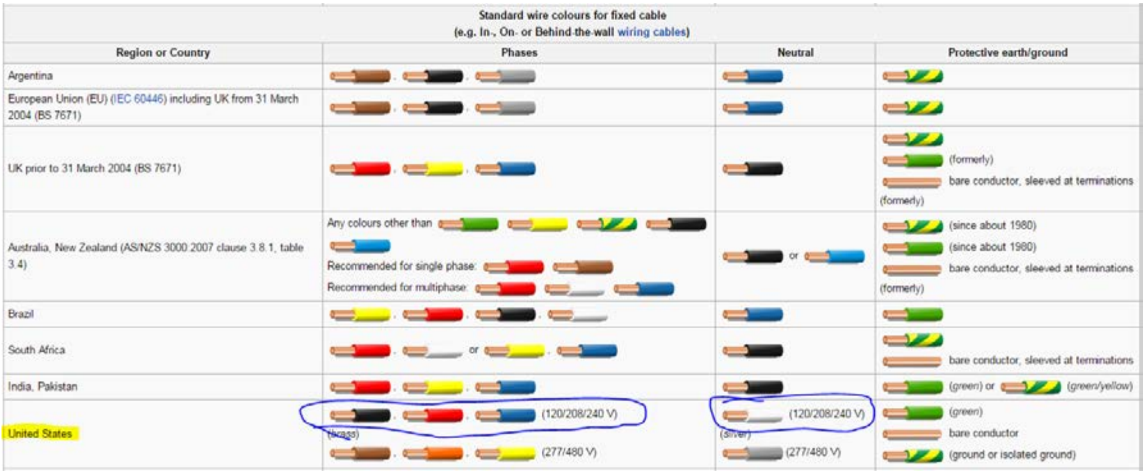
Power Budget Behavior

See the POE STATUS section on page 163.

PoE Behavior

See the POEsection on page 161.

Standard Wire Colors



Standard wire colours for fixed cable (e.g. In-, On- or Behind-the-wall wiring cables)			
Region or Country	Phases	Neutral	Protective earth/ground
Argentina	🟫 , ⬛ , ⬜	🟦	🟩🟨
European Union (EU) (IEC 60446) including UK from 31 March 2004 (BS 7671)	🟫 , ⬛ , ⬜	🟦	🟩🟨
UK prior to 31 March 2004 (BS 7671)	🟥 , 🟨 , 🟦	⬛	🟩🟨 🟩 (formerly) ▭ bare conductor, sleeved at terminations (formerly)
Australia, New Zealand (AS/NZS 3000:2007 clause 3.8.1, table 3.4)	Any colours other than 🟩 🟨 🟩🟨 ⬛ 🟦 Recommended for single phase: 🟥 🟫 Recommended for multiphase: 🟥 ⬜ 🟦	⬛ or 🟦	🟩🟨 (since about 1980) 🟩 (since about 1980) ▭ bare conductor, sleeved at terminations (formerly)
Brazil	🟨 , 🟥 , ⬛ , ⬜	🟦	🟩
South Africa	🟥 , ⬜ or 🟨 , 🟦	⬛	🟩🟨 ▭ bare conductor, sleeved at terminations
India, Pakistan	🟥 , 🟨 , 🟦	⬛	🟩 (green) or 🟩🟨 (green/yellow)
United States	⬛ , 🟥 , 🟦 (120/208/240 V) (brass) 🟫 , 🟧 , 🟨 (277/480 V)	⬜ (120/208/240 V) (silver) ⬜ (277/480 V)	🟩 (green) ▭ bare conductor 🟩🟨 (ground or isolated ground)

Transition Networks

10900 Red Circle Drive

Minnetonka, MN 55343 USA

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

Fax: 952-941-2322

Printed in the U.S.A.

SISPM1040-384-LRT-B Industrial Managed Ethernet Switch User Guide, 33667 Rev. C