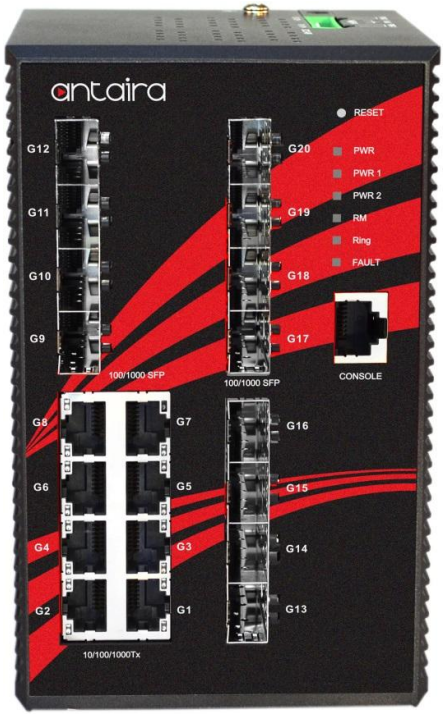
LNX-2012GN-SFP Series

20-Port Industrial Gigabit Managed Ethernet Switches with 8*10/100/1000Tx + 12*100/1000 SFP Slots



User Manual

Version 1.2

www.antaira.com

Disclaimer

Antaira Technologies, LLC provides this manual without warranty of any kind, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Antaira Technologies, LLC may make improvements and/or changes to the product and/or specifications of the product described in this manual, without prior notice. Antaira Technologies, LLC will not be liable for any technical inaccuracies or typographical errors found in this guide. Changes are periodically made to the information contained herein and will be incorporated into later versions of the manual. The information contained is subject to change without prior notice.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

CE Mark Warning

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

Industrial Ethernet Switches

Industrial Grade Gigabit Managed Ethernet Switches

User Manual
Version 1.2 (February 2018)

This manual supports the following models:

- LNX-2012GN-SFP
- LNX-2012GN-SFP-T

This document is the current official release manual. Please check our website (www.antaira.com) for any updated manual or contact us by e-mail (support@antaira.com).

Table of Contents

1. Introduction

All Antaira industrial managed switches come with a pre-installed “user friendly” web console interface, which allows users to easily configure and manage the units, whether one is using a serial console and command line interface(CLI) commands like Telnet, SSH, HTTP (Web GUI) or simple network management protocols (SNMP).

1.1 Product Overview

Antaira’s LNX-2012GN-SFP series is a 20-port industrial gigabit managed Ethernet switch that is embedded with eight gigabit Ethernet ports and twelve dual rate (100/1000) SFP slots for fiber connection. It supports jumbo frames up to 9.6K for huge Ethernet data packet transmissions. It is a fully manageable Layer 2 Ethernet switch that is pre-loaded with a user-friendly web management console design. It supports the Super Ring network redundancy system to prevent any single failure causing extended downtime. The advanced network filtering and security functions, such as, IGMP, VLAN, QoS, SNMP, port lock, RMON, Modbus TCP, and 802.1X/HTTPS/SSH/SSL increase determinism and improve network management for remote SCADA systems or control networks.

The LNX-2012GN-SFP series is compact, IP30 rated, and DIN-rail or wall mountable. There are also two wide operating temperature models for either a standard temperature range (STD: -10°C to 70°C) or an extended temperature range (EOT: -40°C to 75°C). It also provides high EFT and ESD protection for industrial networking applications, such as, power/utility, water wastewater, oil/gas/mining, factory automation, security surveillance, ITS and any other outdoor or harsh environment.

1.2 Product Software Features

- Network Redundancy
  - STP, RSTP, MSTP network redundancy
- Network Management
  - Web UI based management, SNMP v1/v2/v3, serial console
  - Qos, traffic classification QoS, Cos, bandwidth control for Ingress and Egress, broadcast storm control, Diffserv
  - SMTP (Simple Mail Transport Protocol) client
  - IEEE 1588v2 clock synchronization
  - 9.6K Bytes jumbo frame support
  - IEEE802.1q VLAN tagging, port-based VLAN support

- IGMP snooping v2/v3, IGMP filtering / throttling, IGMP query up to 256 group
- Supports IPv4/IPv6, RMON, MIB II, port mirroring, event syslog, DNS, NTP/SNTP, HTTPS, SSH/SSL, TFTP
- IEEE 802.3az energy-efficient Ethernet
- MODBUS TCP for SCADA system integration

- Port Configuration
  - Status, statistics, mirroring, rate limiting, event syslog
- Event Handling
  - Event Notification by Email: cold/warm start, power failure, authentication, SNMP trap and fault alarm relay output
- Software Upgrade via TFTP and HTTP

1.3 Product Hardware Features

- System Interface and Performance
  - All RJ-45 ports support auto MDI/MDI-X function
  - Embedded 8*10/100/1000Tx fast Ethernet RJ45 ports, and 12*100/1000 SFP slot
  - Console port
  - Store-and-forward switching architecture
  - 8K MAC address table
  - Power line EFT protection: 2,000VDC; Ethernet ESD protection: 6,000VDC
- Power Input
  - DC 12~48V redundant with a 6-pin removal terminal block
  - One user programmable alarm relay contact
- Operating Temperature
  - Standard operating temperature models: -10°C to 70°C
  - Extended operating temperature models: -40°C to 75°C
- Case/Installation
  - IP-30 protection metal housing
  - DIN-Rail and wall mount design

1.4 Package Contents

- 1– LNX-2012GN-SFP series: 20-port industrial gigabit managed Ethernet switch, with 8*10/100/1000Tx and 12*100/1000 SFP slots
- 1-Product CD
- 2-Wall mounting brackets and screws
- 1-RJ45 to DB9 Serial Console cable
- 1-DC cable –18 AWG & DC jack 5.5x2.1mm

1.5 Safety Precaution

Attention: If the DC voltage is supplied by an external circuit, please use a protection device on the power supply input. The industrial Ethernet switch's hardware specs, ports, cabling information, and wiring installation will be described within this user manual.

2. Hardware Description

2.1 Physical Dimensions

Figure 2.1, below, shows the physical dimensions of Antaira's LNX-2012GN-SFP series: 20-port industrial gigabit managed Ethernet switches with 8*10/100/1000Tx and 12*100/1000 SFP slots.

(W x D x H) is **96.4mm x 105.5mm x 154mm**

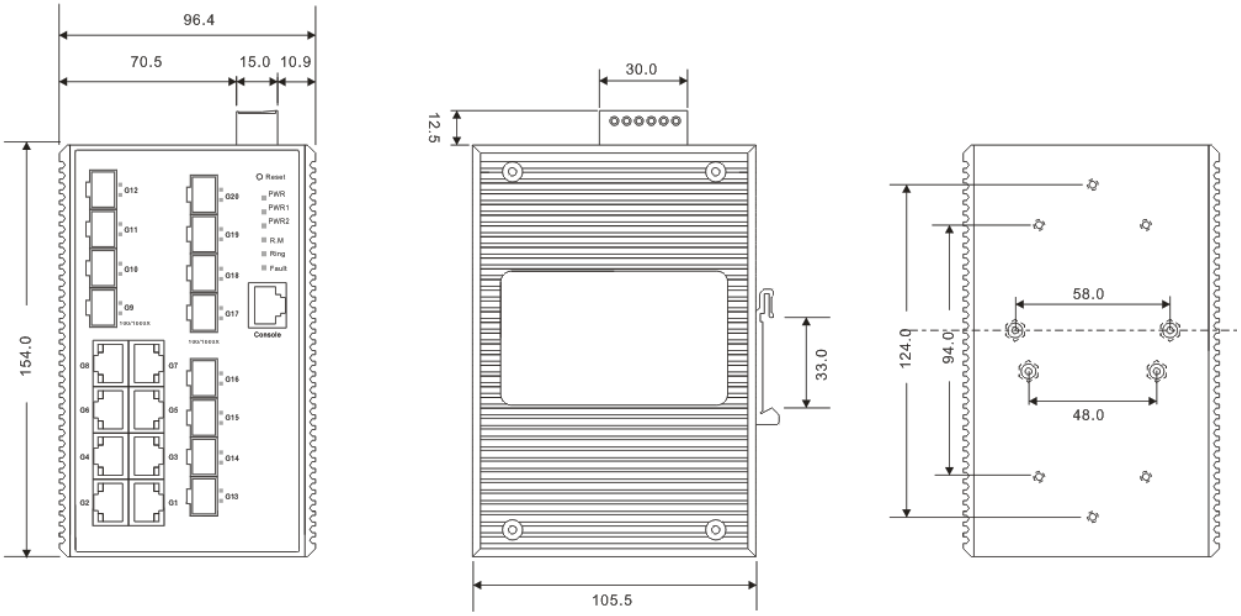


Figure2.1

LNX-2012GN-SFP Series Physical Dimensions

2.2 Front Panel

The front panel of the LNX-2012GN-SFP series industrial gigabit managed Ethernet switch is shown below in *Figure 2.2*.

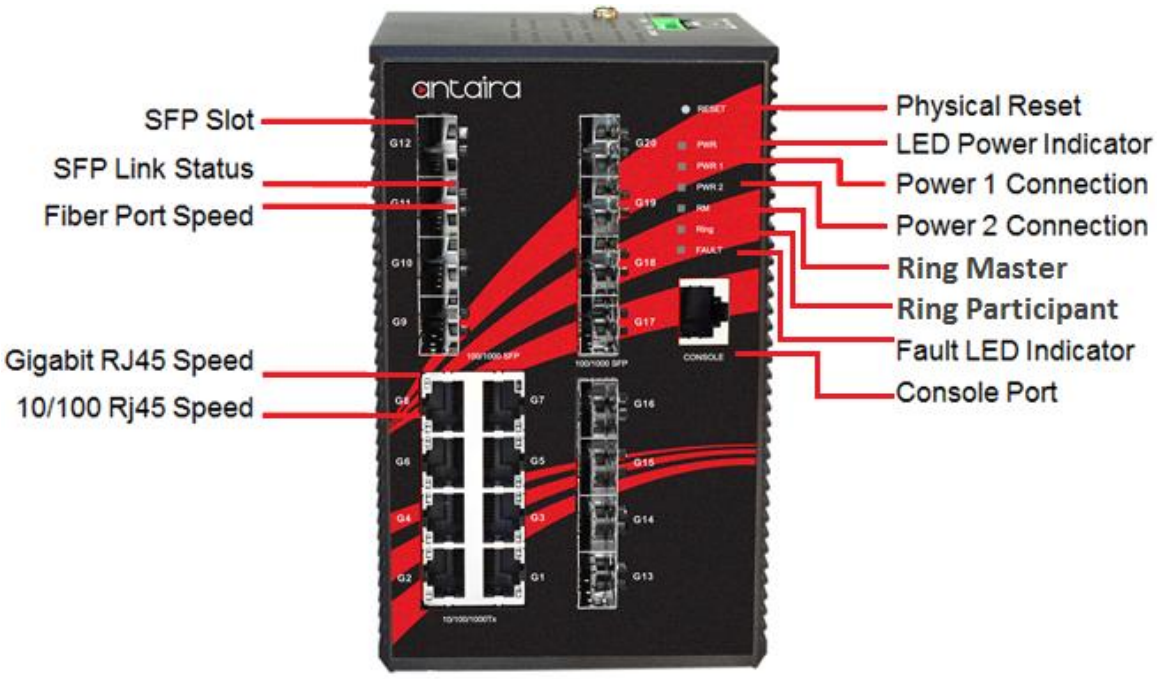


Figure2.2
The Front Panel of LNX-2012GN-SFP Series

2.3 Top View

Figure 2.3, below, shows the top panel of the LNX-2012GN-SFP series switch that is equipped with one 6-pin removal terminal block connector for dual DC power inputs 12~48VDC.

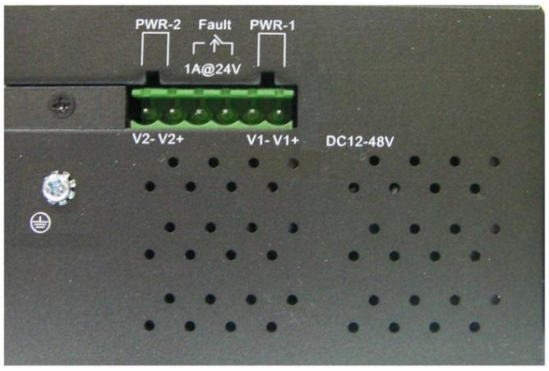


Figure2.3
Top Panel View of LNX-2012GN-SFP *Series*

2.4 LED Indicators

There are LED light indicators located on the front panel of the industrial Ethernet switch that display the power status and network status. Each LED indicator has a different color and has its own specific meaning, see below in *Table 2.1*.

LED	Color	Description	
P1	Green	On	Power input 1 is active
		Off	Power input 1 is inactive
P2	Green	On	Power input 2 is active
		Off	Power input 2 is inactive
R.M	Green	On	Power input 2 is active
		Off	Power input 2 is inactive
Ring	Green	On	Power input 2 is active
		Off	Power input 2 is inactive
Fault	Amber	On	Power failure or Port failure/inactive
		Off	Power input 1 and 2 are both functional, or no power, inputs/ports link is active/port alarm is disabled
LAN Port 1 ~ 8 (Left LED)	Green 	On	Connected to network, 1000Mbps
		Flashing	Networking is active
		Off	Not connected to network
LAN Port 1~ 8 (Right LED)	Green 	On	Networking is active, 100/10Mbps
		Flashing	Networking is active
		Off	Not connected to network
Fiber Port #9~20 SFP LNK/ACT	ACT	On	Connected to network
		Flashing	Networking is active
	LNK	On	Port link is up

Table 2.1 - LED Indicators for LNX-2012GN-SFP Series

2.5 Reset Button

There is a Reset button located on the front panel of the industrial Ethernet switch that helps users to reboot, restore default, or save running configurations by pressing the button for different seconds. Please refer to *Table 2.2* for the timing and function.

Seconds	Function
3	Reboot the switch
6 or more	Restore factory default

Table 2.2 – Reset Button Functions

2.6 Ethernet Ports

- **RJ-45 Ports**

RJ-45 Ports (Auto MDI/MDIX): The RJ-45 ports are auto-sensing for 10Base-T, 100Base-TX, or 1000Base-T connections. Auto MDI/MDIX means that the switch can connect to another switch or workstation without changing the straight-through or crossover cabling. See the figures below for straight-through and crossover cabling schematics.

- **RJ-45 Pin Assignments**

Pin Number	Assignment
1	DA+ (Receive)
2	DA- (Receive)
3	DB+ (Transmit)
4	DC+(Receive)
5	DC-(Receive)
6	DB-(Transmit)
7	DD+(Transmit)
8	DD-(Transmit)

Table 2.3 - RJ45 Pin Assignments

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

All ports on this industrial Ethernet switch support automatic MDI/MDI-X operations. Users can use straight-through cables (see figure below) for all network connections to PCs, servers, and other switches or hubs. With straight-through cabling, pins 1, 2, 3, and 6 are at one end of the cable and are connected straight through to pins 1, 2, 3 and 6 at the other end of the cable. The table below (*Table 2.3*) shows the 10BASE-T/100BASE-TX/1000BASE-T MDI and MDI-X port pin outs.

Pin MDI-X	Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)

Table 2.4 - Ethernet Signal Pin

The following figures show the cabling schematics for straight-through and crossover.

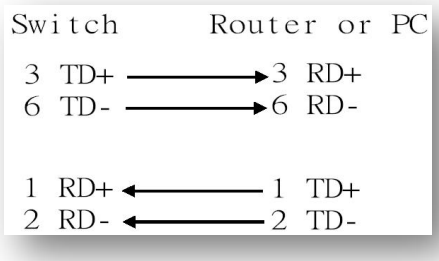


Figure 2.4
Straight-Through Cable Schematic

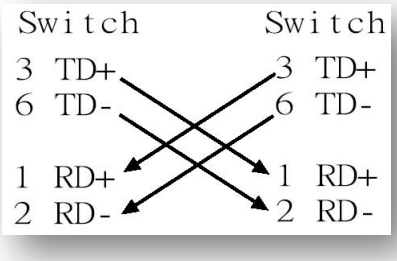


Figure 2.5
Crossover Cable Schematic

2.7 Cabling

Use the four twisted-pair, category 5e, or the above cabling for the RJ-45 port connections. The cable between the switch and the link partner (switch, hub, workstation, etc.) must be less than 100 meters (328 ft.) in length.

The small form-factor pluggable (SFP) is a compact optical transceiver used in optical communications for both telecommunication and data communication applications. To connect the transceiver and LC cable, please follow the steps below:

First, insert the SFP transceiver module into the SFP slot as shown below in *Figure 2.6*. Notice that the triangle mark is at the bottom of the SFP slot. *Figure 2.7* shows that the SFP transceiver module has been inserted.

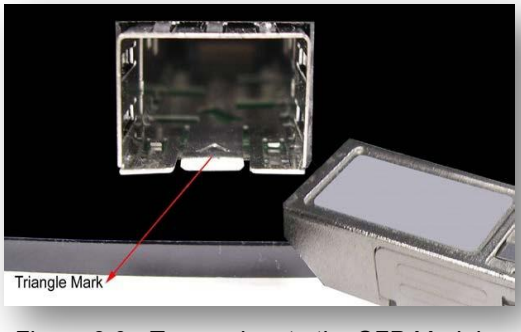


Figure 2.6 - Transceiver to the SFP Module

Figure 2.7 - Transceiver Inserted

Second, insert the fiber cable of the LC connector into the transceiver as shown in *Figure 2.8.*

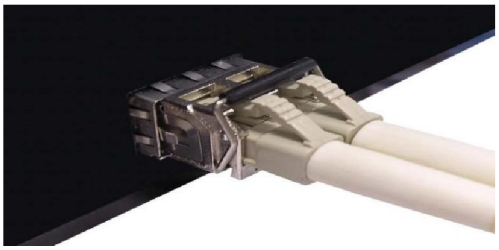


Figure 2.8 - LC Connector to the Transceiver

To remove the LC connector from the transceiver, please follow the steps shown below:

1. Press the upper side of the LC connector from the transceiver and pull it out to release as shown below in *Figure 2.9*.

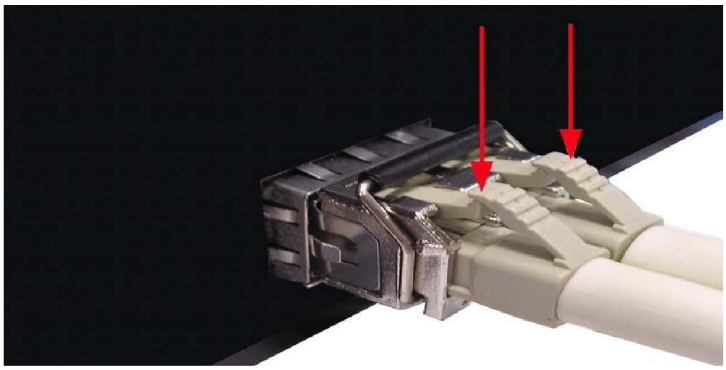


Figure 2.9
Remove LC Connector

2. Push down the metal clasp and pull the transceiver out by the plastic part as shown below in *Figure 2.10*.

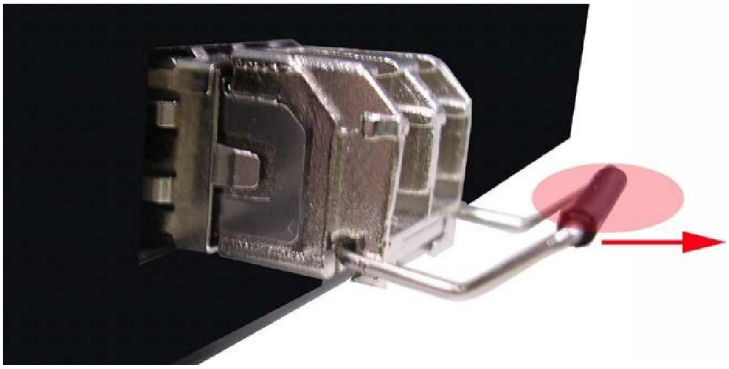


Figure 2.10
Pull Out from the SFP Module

2.8 Wiring the Power Inputs

Please follow the steps below when inserting the power wire.

1. Insert the positive and negative wires into the PWR1 (V1+, V1-) and PWR2 (V2+, V2-) contacts on the terminal block connector as shown below in *Figure 2.11*.

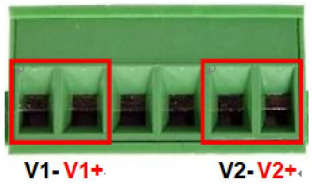


Figure 2.11 - Power Terminal Block

2. Tighten the wire-clamp screws to prevent the wires from loosening, as shown below in *Figure 2.12*.

Figure 2.12 - Power Terminal Block

***Note**	• *Only use copper conductors, **60/75°C**, tighten to **5lbs.***
	• *The wire gauge for the terminal block should range between **18~20 AWG**.*

2.9 Wiring the Fault Alarm Contact

The fault alarm contact is in the middle of the terminal block connector as the picture shows below in *Figure 2.13*. By inserting the wires, it will detect the fault status including power failure or port link failure (managed industrial switch only) and form a normally open circuit. An application example for the fault alarm contact is shown below in *Figure 2.13*.

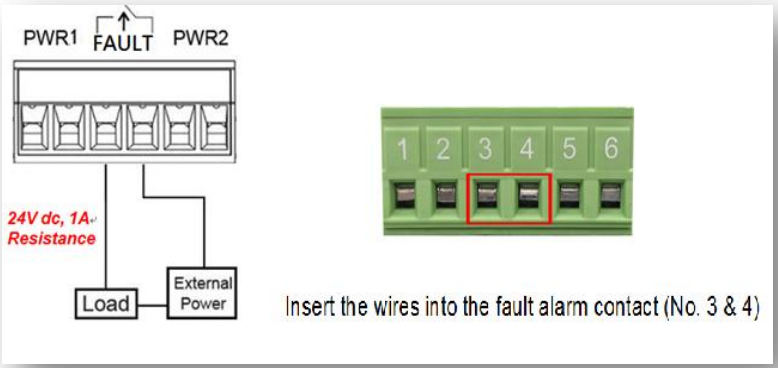


Figure 2.13 - Wiring the Fault Alarm Contact

***Note**	• *The wire gauge for the terminal block should range between **12 ~ 24AWG***

3. Mounting Installation

3.1 DIN-Rail Mounting

The DIN-Rail is pre-installed on the industrial Ethernet switch from the factory. If the DIN-Rail is not on the industrial Ethernet switch, please attach the DIN-Rail mount that has a metal spring on it to securely fasten the unit to standard DIN-Rail.

Figure 3.1
The Rear Side of the Switch and DIN-Rail Bracket

Follow the steps below to learn how to hang the industrial Ethernet switch.

1. Use the screws to install the DIN-Rail bracket on the rear side of the industrial Ethernet switch.
2. To remove the DIN-Rail bracket, do the opposite from step 1.
3. After the DIN-Rail bracket is installed on the rear side of the switch, insert the top of the DIN-Rail on to the track as shown below in *Figure 3.2*.
4. Lightly pull down the bracket on to the rail as shown below in *Figure 3.3*.
5. Check if the bracket is mounted tightly on the rail.
6. To remove the industrial Ethernet switch from the rail, do the opposite from the above steps.

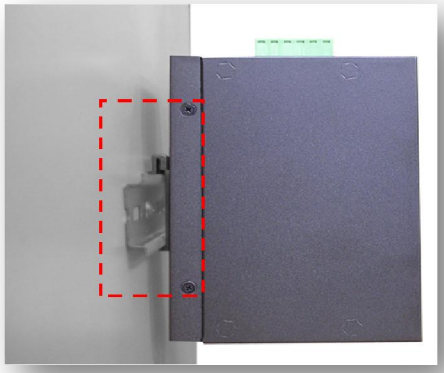


Figure 3.2
Insert the Switch on the DIN-Rail

Figure 3.3
Stable the Switch on DIN-Rail

3.2 Wall Mounting

Follow the steps below to mount the industrial Ethernet switch using the wall mounting bracket as shown below in *Figure 3.4*.

1. Remove the DIN-Rail bracket from the industrial Ethernet switch by loosening the screws.
2. Place the wall mounting brackets on the top and bottom of the industrial Ethernet switch.
3. Use the screws to screw the wall mounting bracket on the industrial Ethernet switch.
4. Use the hook holes at the corners of the wall mounting bracket to hang the industrial Ethernet switch on the wall.
5. To remove the wall mount bracket, do the opposite from the steps above.

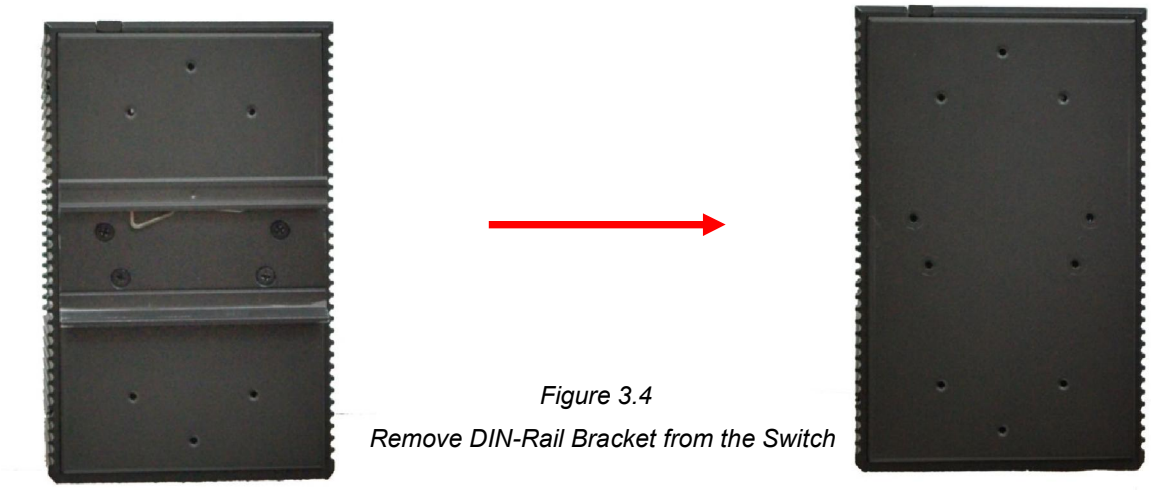


Figure 3.4
Remove DIN-Rail Bracket from the Switch

Below, in *Figure 3.5* are the dimensions of the wall mounting bracket.

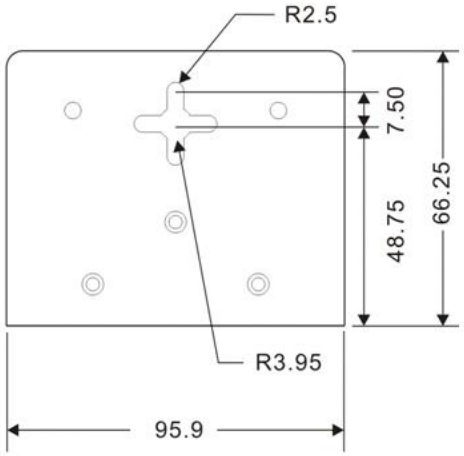


Figure 3.5
Wall Mounting Bracket Dimensions

4. Hardware Installation

4.1 Installation Steps

This section will explain how to install Antaira's LNX-2012GN-SFP series: 20-port industrial gigabit managed Ethernet switches with 8*10/100/1000Tx and 12*100/1000 SFP slots for fiber.

Installation Steps

1. Unpack the industrial Ethernet switch from the original packing box.
2. Check if the DIN-Rail bracket is screwed on the industrial Ethernet switch.
    - If the DIN-Rail is not screwed on the industrial Ethernet switch, please refer to the **DIN-Rail Mounting** section for DIN-Rail installation.
    - If you want to wall mount the industrial Ethernet switch, please refer to the **Wall Mounting** section for wall mounting installation.
3. To hang the industrial Ethernet switch on a DIN-Rail or wall, please refer to the **Mounting Installation** section.
4. Power on the industrial Ethernet switch and then the power LED light will turn on.
    - If you need help on how to wire power, please refer to the **Wiring the Power Inputs** section.
    - Please refer to the **LED Indicators** section for LED light indication.
5. Prepare the twisted-pair, straight-through category 5 cable for Ethernet connection.
6. Insert one side of the RJ-45 cable into switch's Ethernet port and on the other side into the networking device's Ethernet port, e.g. switch PC or server. The Ethernet port's (RJ-45) LED on the industrial Ethernet switch will turn on when the cable is connected to the networking device.
    - Please refer to the **LED Indicators** section for LED light indication.
7. When all connections are set and the LED lights all show normal, the installation is complete.

5. Web Management

5.1 Web Console Configuration

This section introduces the configuration by web browser.

5.1.1 About Web-Based Management

All of Antaira's industrial managed switches are embedded with HTML web console interfaces that have a flash memory on the CPU board. It is a "user-friendly" design with advanced management features that allow users to manage the switch from anywhere on the network through any Internet browser, such as Internet Explorer (version 9.0 or above is recommended), Firefox, Chrome and many others.

Preparing for Web Console Configuration

Antaira's industrial managed switches come with a factory default value as below:

- Default IP Address: **192.168.10.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.10.254**
- Default User Name: **admin**
- Default Password: **admin**

System Login

1. Launch any Internet browser
2. Type in factory default IP address: http://192.168.10.1 of the switch. Press "**Enter**".

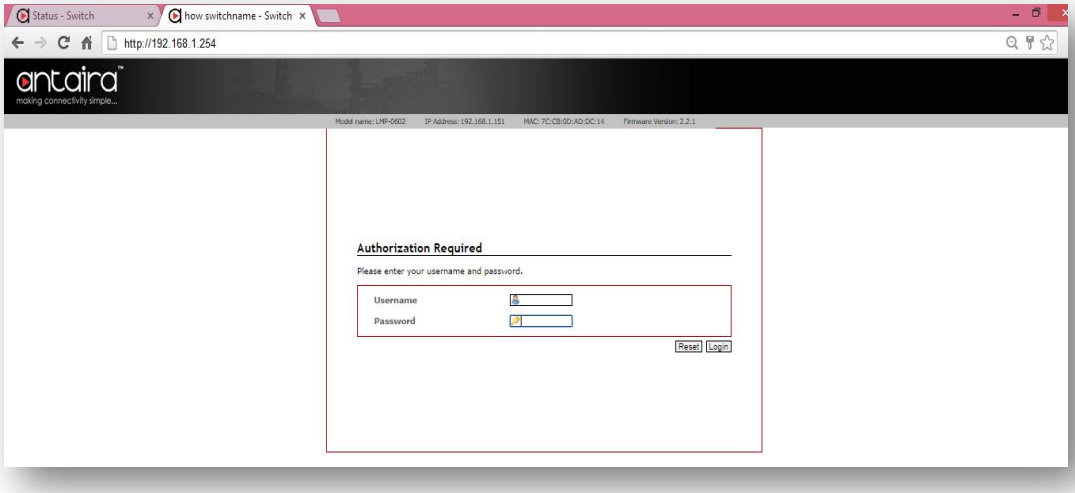


Figure 5.1 - Web Console "Login"

3. The login screen appears.

4. Key in the default username: **admin** and password **admin**.

5. Click the “Login” button, then the main (status) page of the Web Console will appear as shown below in *Figure 5.1.1*. The online image of the switch will display the real-time ports connection status.

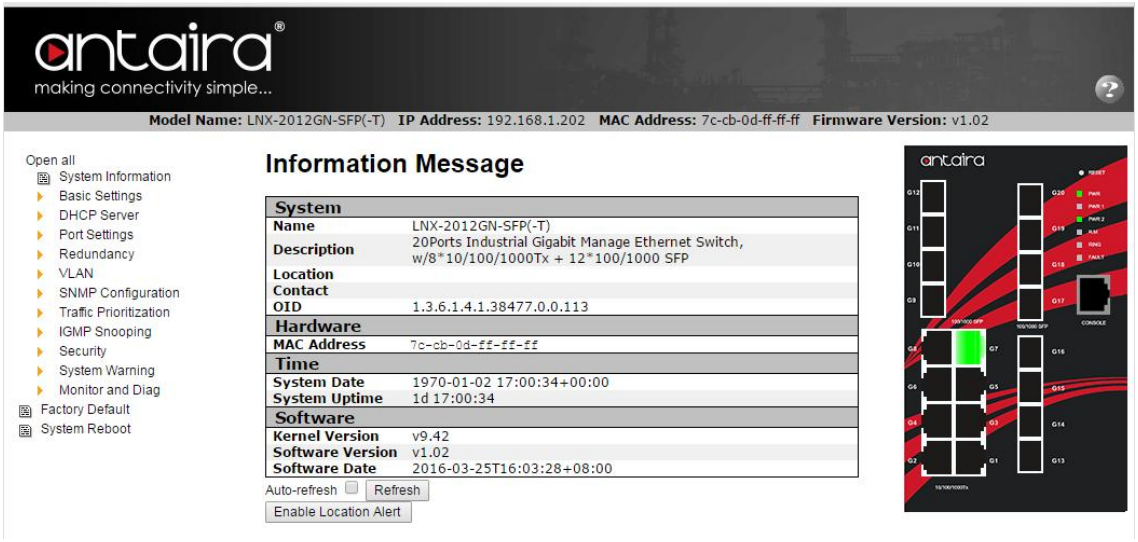


Figure 5.1.1 - Web Console Main (Status) Page

5.2 Basic Setting

5.2.1 System Information

Below, *Figure 5.2*, shows the switch system setting information.

Figure 5.2 – Switch Settings (Status) Page

Label	Description
System Name	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z, a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
System Description	The device description.
System Location	The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
System Timezone offset(minutes)	Provide the time-zone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Table 5.2 – Switch Settings Description

5.2.2 Admin & Password

Below, describes how to configure the system user name and password for the web console login.

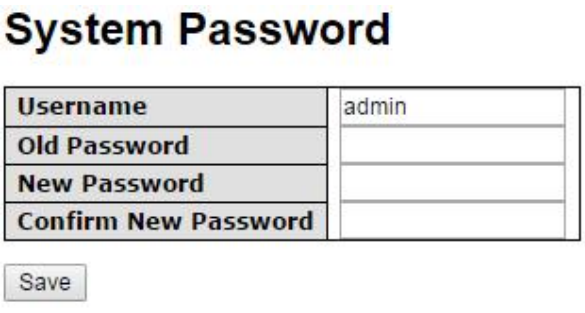


Figure 5.2.2 – Administrative Account

Label	Description
Old Password	Enter the current system password. If this is incorrect, the new password will not be set.
New Password	The system password. The allowed string length is 0 to 31, and the allowed content is the ASCII characters from 32 to 126.
Confirm password	Re-type the new password.
Save	Click to save changes.

Table 5.2.2 – Admin & Password Description

5.2.3 IP Setting

Configure the managed switch's IP setting information.

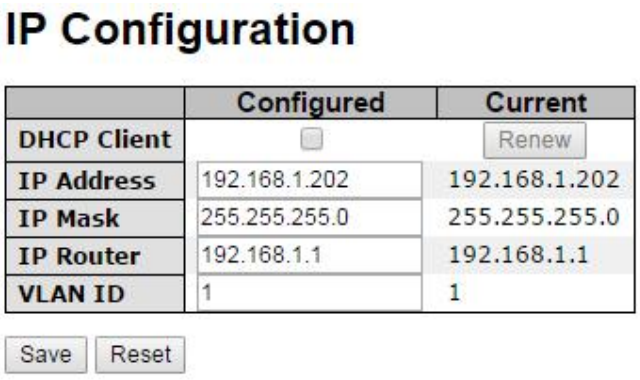


Figure 5.2.3 – IP Setting Information

Label	Description
DHCP Client	Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
IP Address	Assign the IP address that the network is using. If DHCP client function is enabling, you do not need to assign the IP address. The network DHCP server will assign the IP address for the switch and it will be display in this column. The default IP is 192.168.10.1

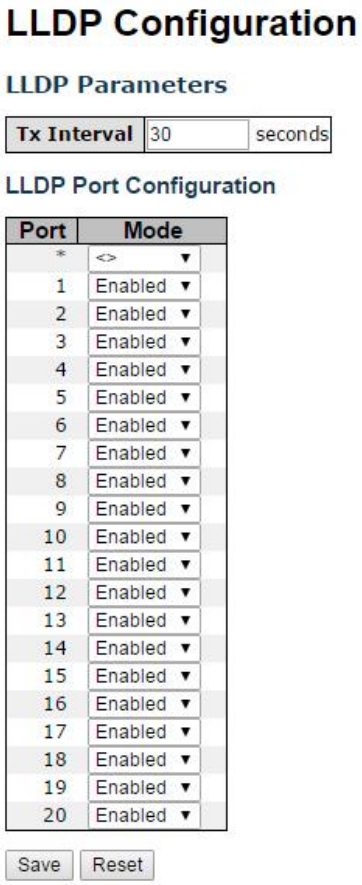
IP Mask	Assign the subnet mask of the IP address. If DHCP client function is enabling, you do not need to assign the subnet mask
IP Router	Assign the network gateway for the switch. The default gateway is 192.168.10.254
VLAN ID	Provide the managed VLAN ID. The allowed range is 1 through 4095.
DNS Server	Provide the IP address of the DNS Server in dotted decimal notation.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Table 5.2.3 – IP Setting Information Description

5.2.4 SSH

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

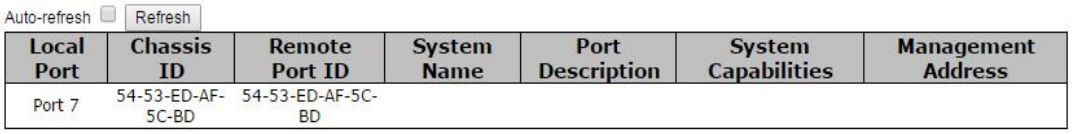
5.2.5 LLDP



Label	Description
Port	The switch port number of the logical LLDP port.
Mode	Select LLDP mode. Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed. Tx only The switch will drop LLDP information received from neighbors, but will send out LLDP information. Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors. Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

5.2.5.1 LLDP Neighbors

The LLDP neighbor page provides a status overview for all LLDP neighbors. The table displayed below contains a row for each port LLDP neighbor that is associated to the ports.



Label	Description
Local Port	The port on which the LLDP frame was received.
Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.
Remote Port ID	The Remote Port ID is the identification of the neighbor port.
System Name	System Name is the name advertised by the neighbor unit.
Port Description	Port Description is the port description advertised by the neighbor unit.
System Capabilities	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
Management Address	Management Address is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address.
Refresh	Click to refresh the page immediately.
Auto-refresh ☐	Check this box to enable an automatic refresh of the page at regular intervals.

5.2.5.2 LLDP Port Statistics

The LLDP Port Statistics page provides and overview of all LLDP traffic. There are global counters that monitor the whole stack of LLDP traffic on the network segment, whereas the LLDP statistical local counters reference only the counter on the selected switch.

LLDP Global Counters

Global Counters	
Neighbour entries were last changed	1970-01-03 04:20:54+00:00 (45055 secs. ago)
Total Neighbours Entries Added	8
Total Neighbours Entries Deleted	7
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	359	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	7785	240	0	0	0	0	466	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	82	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0

Global Counter Table

Label	Description
Neighbor entries were last changed at	Shows the time for when the last entry was last 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 that the entry table was full.
Total Neighbors Entries Aged Out	Shows the number of entries deleted due to Time-To-Live expiring.

Local Counter Table

Label	Description
Local Port	The port on which LLDP frames are received or transmitted.
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 some kind of error.
Frames Discarded	If an 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 Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.
Org. Discarded	The number of organizationally TLVs received.
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	Clears the local counters. All counters (including global counters) are cleared upon reboot.
Auto-refresh ☐	Check this box to enable an automatic refresh of the page at regular intervals.

5.2.6 Backup

The Backup function will save the configuration files of the switch.

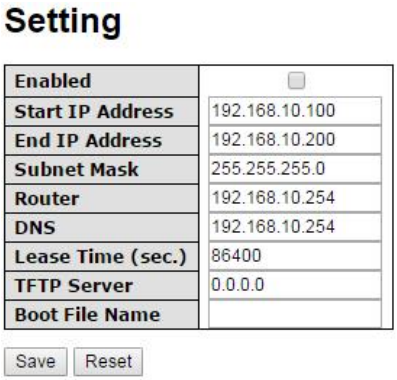
The Restore function will load previously saved configuration files to the switch.

The Firmware Upgrade will upload new firmware to the switch.

5.3 DHCP Server

5.3.1 Settings

Below displays the DHCP server settings that are active when the DHCP server has been enabled.

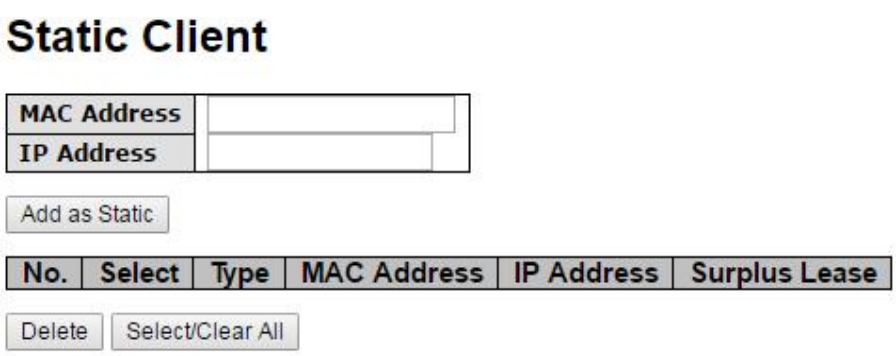


5.3.2 Dynamic Client

When the DHCP server has been enabled the unit will collect the DHCP client information and display it within the Dynamic Client list.

5.3.3 Static Client

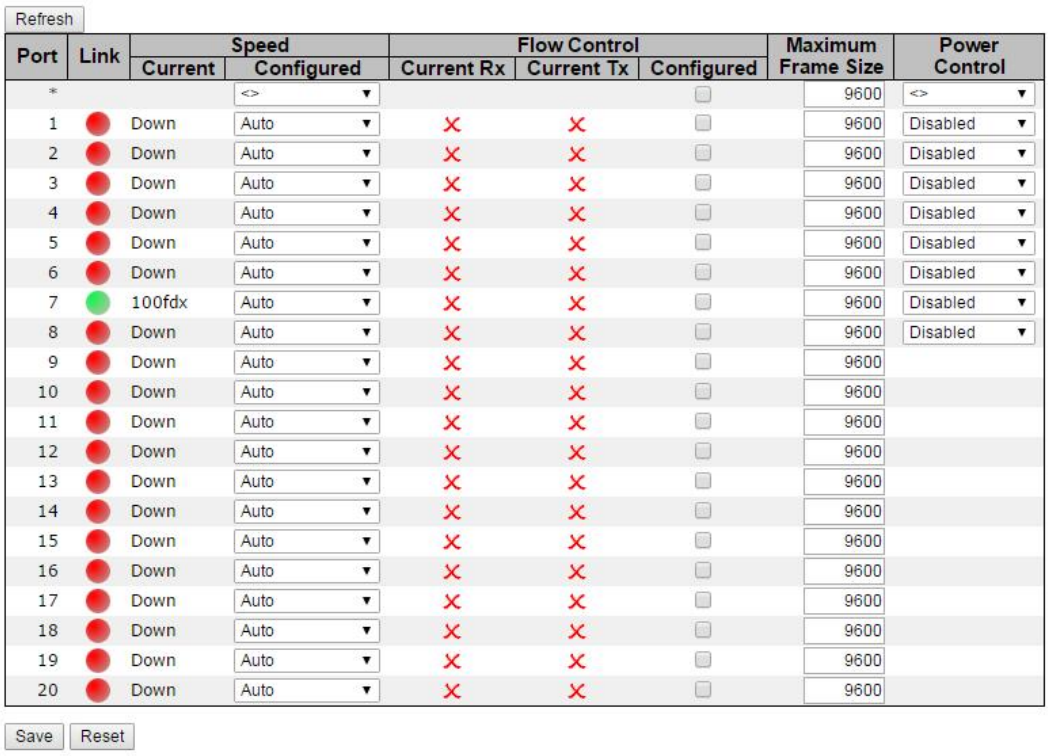
A specific IP address which is in the assigned dynamic IP range to the specific port can be assigned. When the device is connecting to the port and asks for dynamic IP assigning, the system will assign the IP address that has been assigned before in the connected device.



5.4 Port Settings

5.4.1 Port Configuration

The Port Configuration page shows the current port settings.

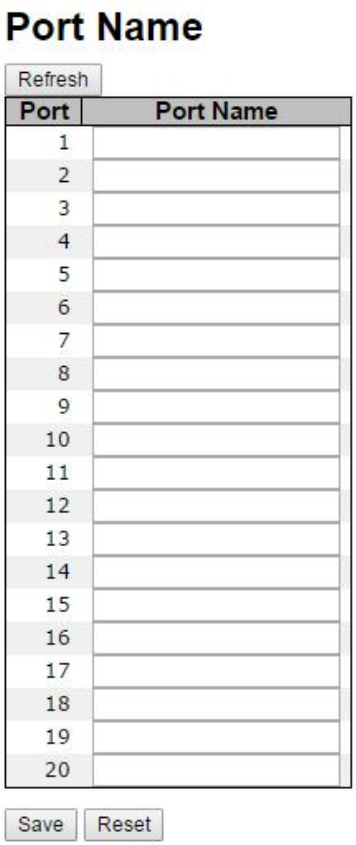


Port Configuration Table

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	Provides the current link speed of the port.
Configured Link Speed	Select any available link speed for the given switch port. *Auto Speed* selects the highest speed that is compatible with a link partner. *Disabled* disables the switch port operation. <> : configuration all port .
Flow Control	When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
Maximum Frame	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 9600 bytes.
Power Control	The Usage column shows the current percentage of the power consumption per port. The Configured column allows for changing the power savings mode parameters per port. Disabled: All power savings mechanisms disabled. ActiPHY: Link down power savings enabled. PerfectReach: Link up power savings enabled. Enabled: Both link up and link down power savings enabled.
Total Power Usage	Total power usage in board, measured in percent.
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.

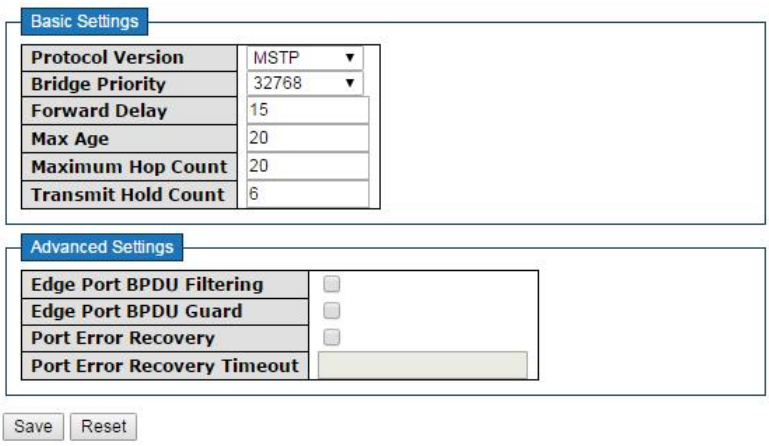
5.4.2 Port Name

The user is able to name each individual port.



5.5 Redundancy

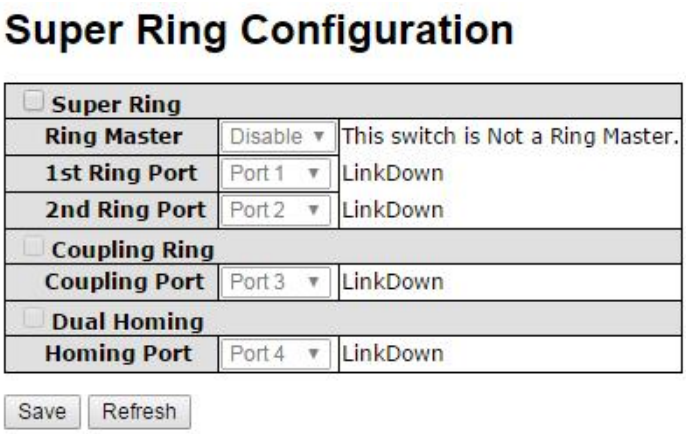
5.5.1 STP Bridge Configuration



Label	Description
Protocol Version	The STP protocol version setting. Valid values are STP, RSTP and MSTP.
Forward Delay	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.
Maximum Hop Count	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range 4 to 30 seconds, and MaxAge must be <= (FwdDelay-1)*2.
Transmit Hold Count	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.5.2 Super Ring

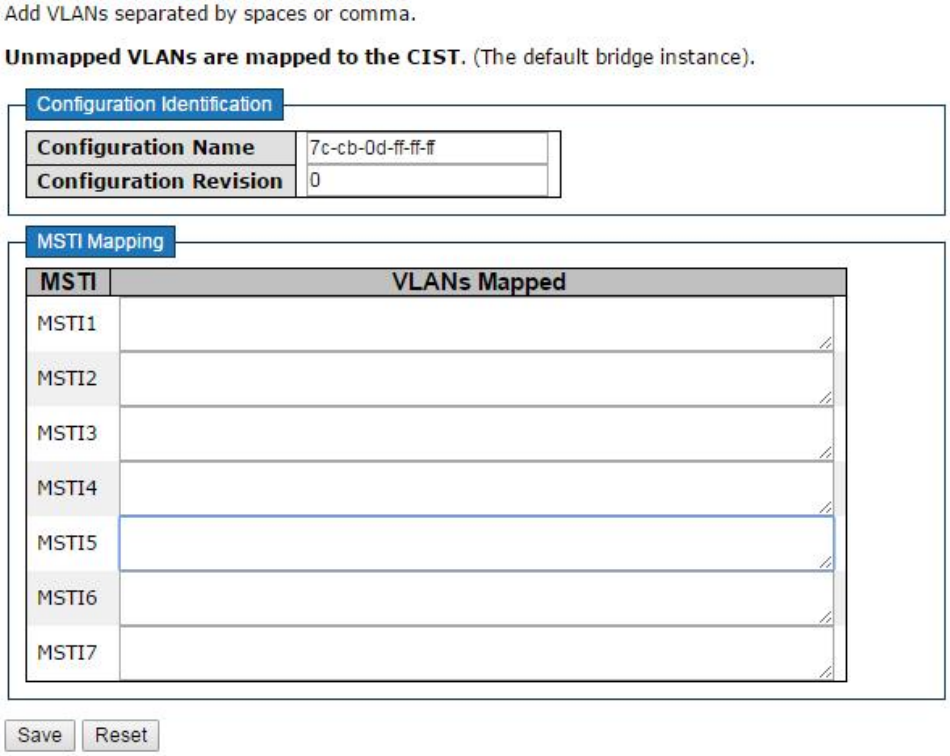
The super ring redundancy protocol allows for extremely fast recovery times in the event of a network connection failure. The Super Ring is able to perform and reroute traffic in less than 10 ms to regaining network communication that was interrupted by an unexpected failure to the network topology.



Super Ring Configuration Descriptions

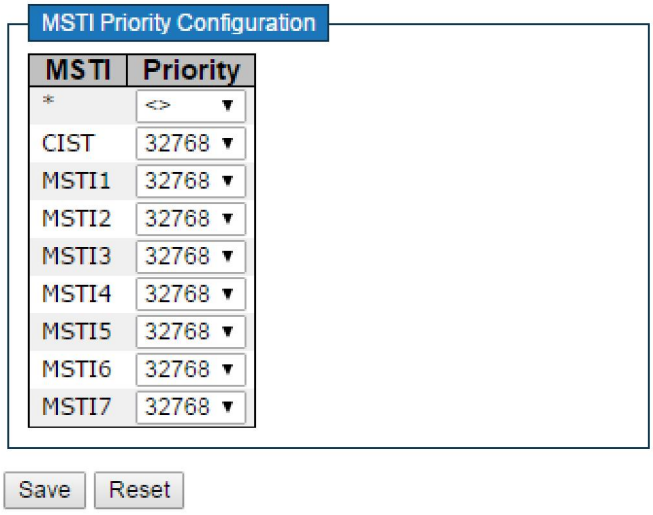
Label	Description
Redundant Ring	Mark to enable Ring.
Ring Master	There should be one and only one Ring Master in a ring. However if there are two or more switches which set the Ring Master to enable, the switch with the lowest MAC address will be the actual Ring Master and others will be Backup Masters.
1st Ring Port	The primary port, when this switch is Ring Master.
2nd Ring Port	The backup port, when this switch is Ring Master.
Coupling Ring	Mark to enable Coupling Ring. Coupling Ring can be used to divide a big ring into two smaller rings to avoid effecting all switches when network topology change. It is a good application for connecting two Rings.
Coupling Port	Link to a Coupling Port of the switch in another ring. Coupling Rings need four switches to build an active backup link. Set a port as a coupling port. The coupled four ports of four switches will be run at in an active/backup mode.
Dual Homing	Mark to enable Dual Homing. By selecting Dual Homing mode, the Ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work as an active/backup mode, and connect each Ring to the normal switches in RSTP mode.
Apply	Click "**Apply**" to set the configurations.

5.5.3 MSTI Configuration



Label	Description
Configuration Name	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is at most 32 characters.
Configuration Revision	The 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 VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

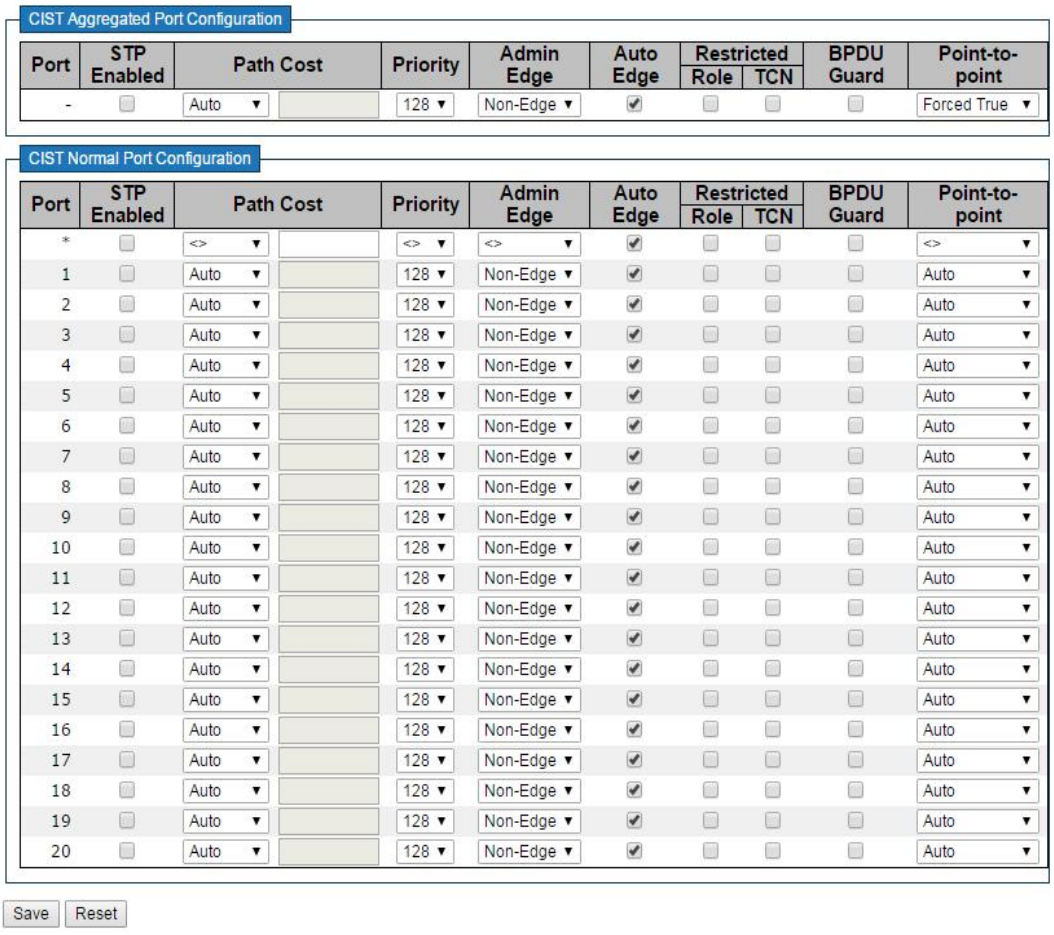
5.5.4 MSTI Priority Configuration



Label	Description
MSTI	The bridge instance. The CIST is the default instance, which is always active.
Priority	Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, linked with 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.

5.5.5 CIST Port Configuration

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



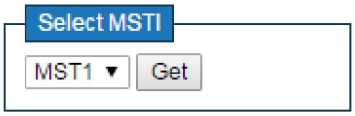
CIST Port Configuration

Label	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to

	200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
Open Edge (setate flag)	Operational flag describing whether the port is connecting directly to the edge devices. (No Bridges attached). Transitioning to the forwarding state is faster for edge ports (having operEdge true) than for other ports.
Admin Edge	Controls whether the operEdge flag should start as being set or cleared. (The initial operEdge state when a port is initialized).
Auto Edge	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.
Restricted Role	If enabled, causes the port not to be selected as Root Port for the CIST 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, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
Restricted TCN	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning trees active 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, causing address flushing in that region, possibly because those bridges are not under full control of the administrator or is the physical link state for the attached LANs transitions frequently.

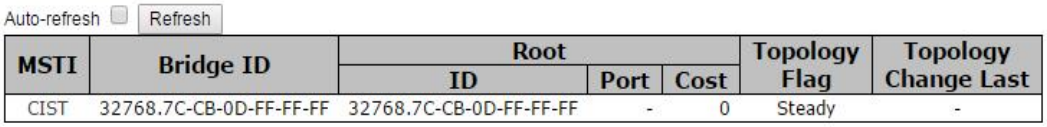
Point2Point	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either as true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

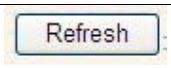
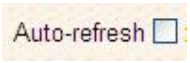
5.5.6 MSTI Port Configuration



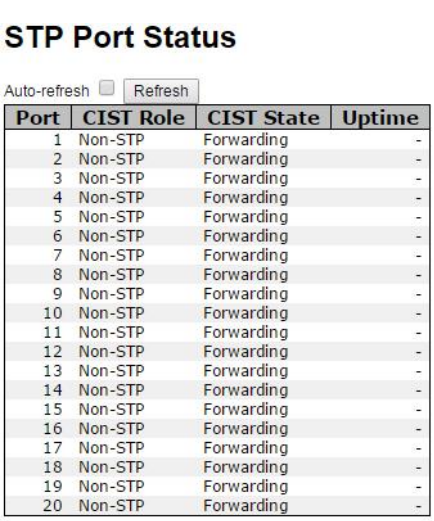
Label	Description
Port	The switch port number of the corresponding STP CIST (and MSTI) port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.5.7 Bridge Status



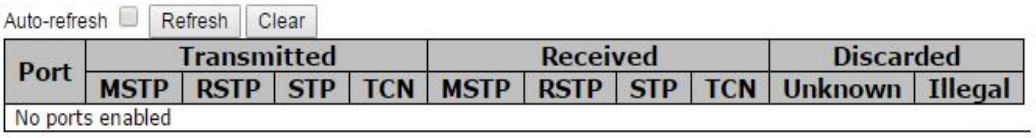
Label	Description
MSTI	The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
Bridge ID	The Bridge ID of this Bridge instance.
Root ID	The Bridge ID of the currently elected root bridge.
Root Port	The switch port currently assigned the root port role.
Root Cost	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Topology Flag	The current state of the Topology Change Flag for this Bridge instance.
Topology Change Last	The time since last Topology Change occurred.
	Click to refresh the page immediately.
	Check this box to enable an automatic refresh of the page at regular intervals.

5.5.8 Port Status



Label	Description
Port	The switch port number of the logical STP port.
CIST Role	The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort.
State	The current STP port state of the CIST port. The port state can be one of the following values: Blocking Learning Forwarding.
Uptime	The time since the bridge port was 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.

5.5.9 STP Port Statistics

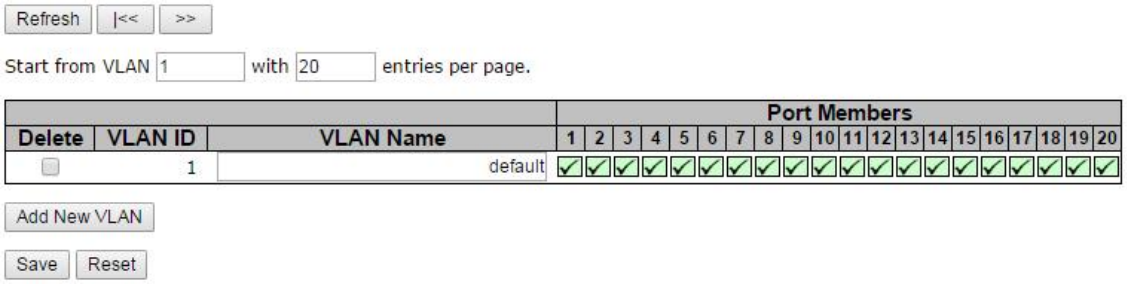


Label	Description
Port	The switch port number of the logical RSTP port.
RSTP	The number of RSTP Configuration BPDU's received/transmitted on the port.
STP	The number of legacy STP Configuration BPDU's received/transmitted on the port.
TCN	The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
Discarded Unknown	The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
Discarded Illegal	The number of illegal Spanning Tree BPDU's received (and discarded) on the port.
Refresh	Click to refresh the page immediately.
Auto-refresh ☐	Check this box to enable an automatic refresh of the page at regular intervals.

5.6 VLAN

5.6.1 Membership Configuration

The VLAN membership configuration for the selected switch can be monitored and modified here. Up to 64 VLANs are supported. This page allows for adding and deleting of VLANs as well as adding and deleting port members of each VLAN.



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Adding a New Static Entry	Click Add New VLAN to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The VLAN is enabled on the selected stack switch unit when you click on "Save". The VLAN is thereafter present on the other stack switch units, but with no port members. A VLAN without any port members on any stack unit will be deleted when you click "Save". The Delete button can be used to undo the addition of new VLANs.

5.6.2 VLAN Port Configuration

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	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
13	Unaware	☐	All	Specific	1	Untag_pvid
14	Unaware	☐	All	Specific	1	Untag_pvid
15	Unaware	☐	All	Specific	1	Untag_pvid
16	Unaware	☐	All	Specific	1	Untag_pvid
17	Unaware	☐	All	Specific	1	Untag_pvid
18	Unaware	☐	All	Specific	1	Untag_pvid
19	Unaware	☐	All	Specific	1	Untag_pvid
20	Unaware	☐	All	Specific	1	Untag_pvid

Save Reset

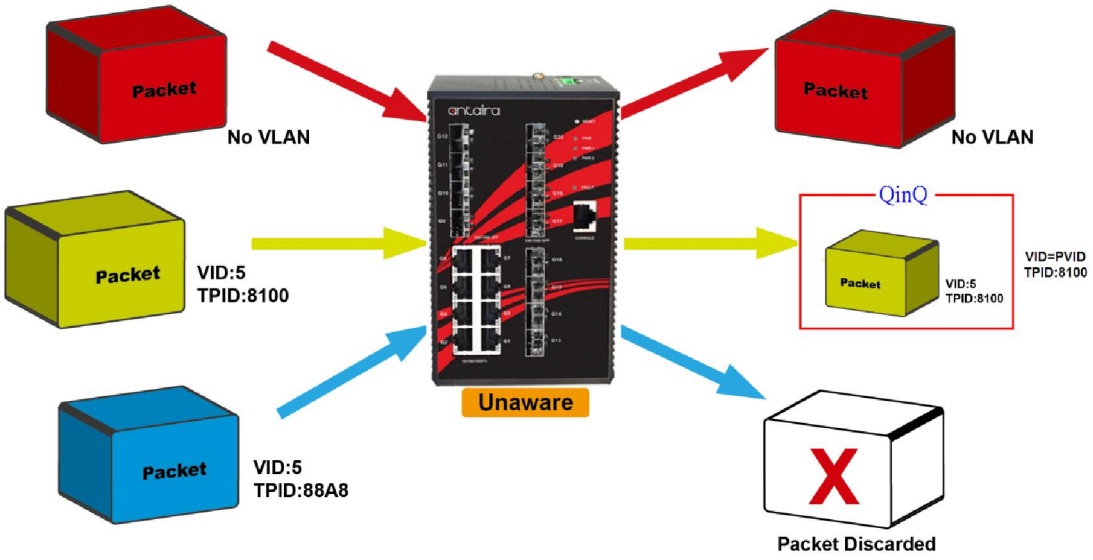
Port Configuration Table

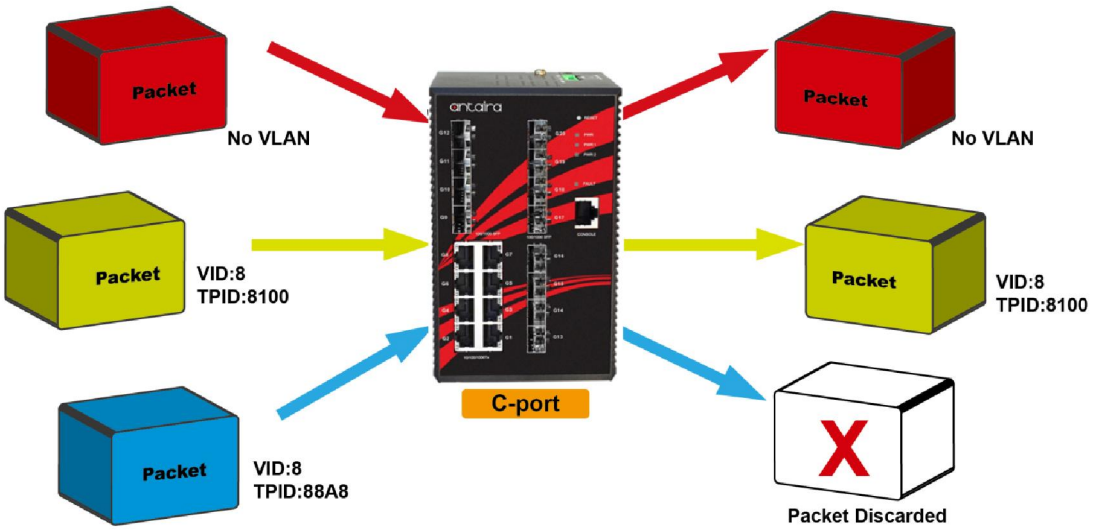
Label	Description
Ethertype for Customer S-Ports	This field specifies the Ether type used for Custom S-ports. This is a global setting for all the Custom S-ports.
Port	This is the logical port number of this row.
Port Type	Ports can be one of the following types: Unaware, Customer port(C-port), Service port(S-port), Custom Service port(S-custom-port) If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed.

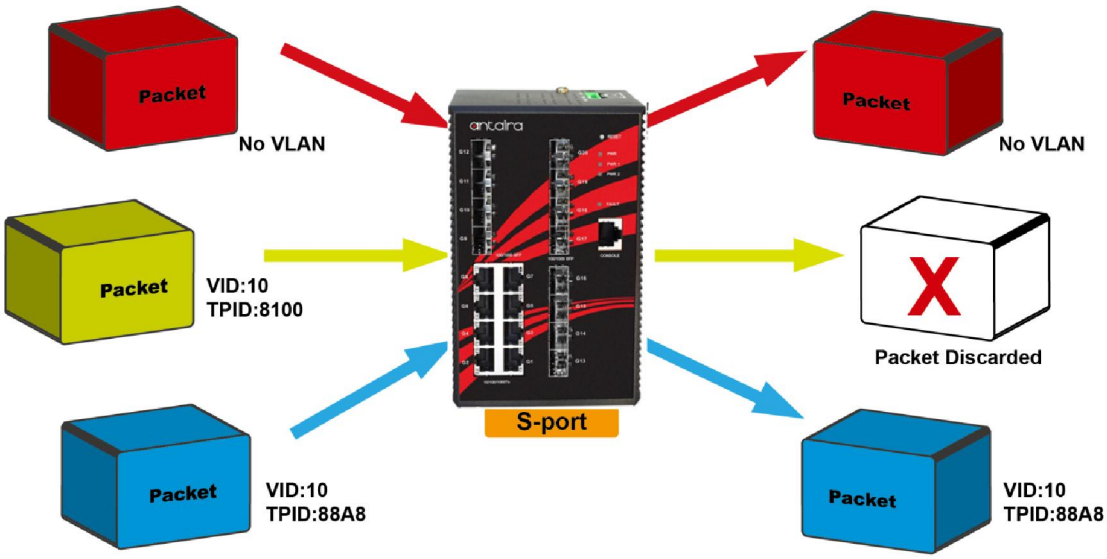
Ingress Filtering	Enable ingress filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no checkmark).
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 are 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 a specific 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 is inserted in the frame.
Port VLAN ID	Configures the VLAN identifier for the port. The allowed values are from 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.

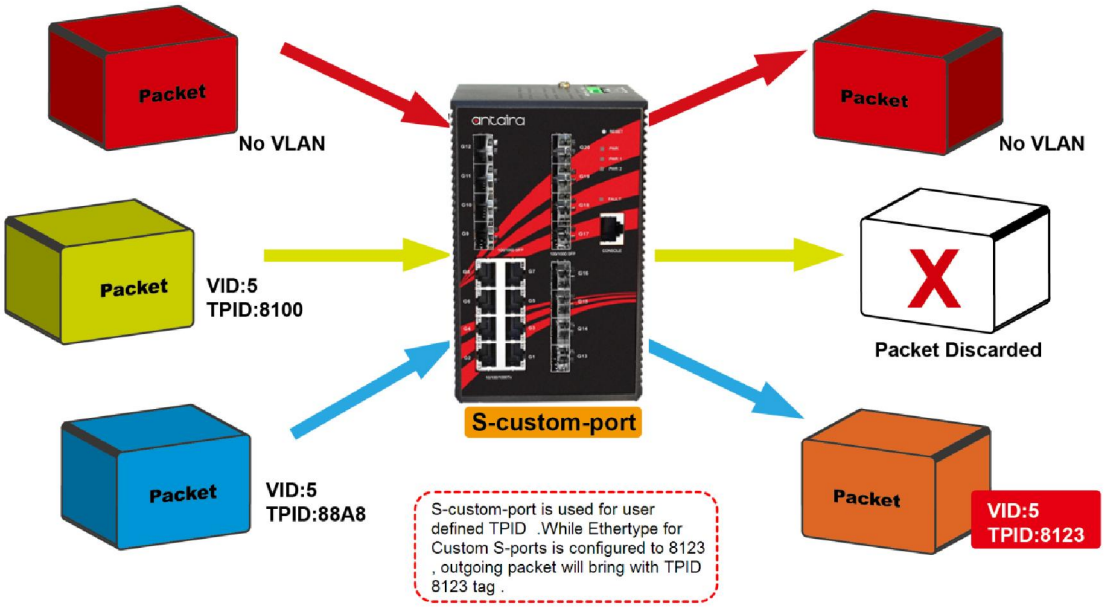
C-Port, S-Port and S-Custom Port Configuration

	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 obtaining a tag (based on PVID) is forwarded. When the port receives tagged frames, 1. If the tagged frame with TPID=0x8100 becomes a double-tagged frame, and is forwarded. 2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of the frame is transmitted by an unaware port that will be set to 0x8100. The final status of the frame after egressing is also effected by the Egress Rule.
C-Port	When the port receives untagged frames, an untagged frame obtaining a tag (based on PVID) is forwarded. When the port received tagged frames, 1. If there is a tagged frame with TPID=0x8100, it is forwarded. 2. If the TPID of a tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of the frame is transmitted by C-port and will be set to 0x8100.
S-Port	When the port receives untagged frames, an untagged frame obtaining a tag (based on PVID) is forwarded. When the port received tagged frames, 1. If there is a tagged frame with TPID=0x88A8, it is forwarded. 2. If the TPID of a tagged frame is not 0x88A8 (ex. 0x8100), it will be discarded.	The TPID of the frame transmitted by S-port will be set to 0x88A8.
S-Custom-Port	When the port receives untagged frames, an untagged frame obtaining a tag (based on PVID) is forwarded. When the port received tagged frames, 1. If there is a tagged frame with TPID=0x88A8, it is forwarded. 2. If the TPID of a tagged frame is not 0x88A8 (ex. 0x8100), it will be discarded.	The TPID of the frame transmitted by S-custom-port will be set to a self-customized value, which can be set by the user using the column of **Ethertype for Custom S-ports.**


Packet
No VLAN
Packet
VID:5
TPID:8100
Packet
VID:5
TPID:88A8
Unaware
Packet
No VLAN
QinQ
Packet
VID:5
TPID:8100
VID=PVID
TPID:8100
X
Packet Discarded

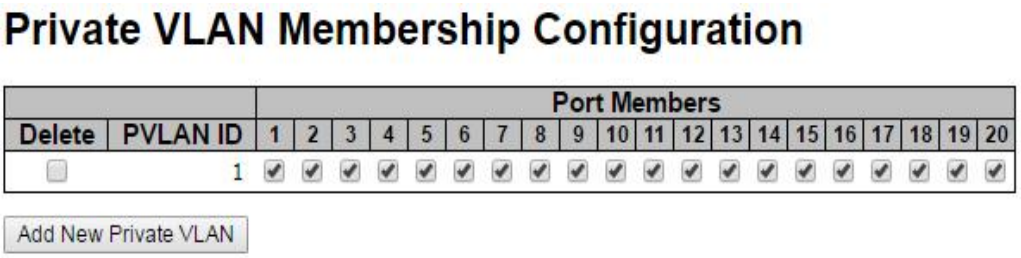

Packet
No VLAN
Packet
VID:8
TPID:8100
Packet
VID:8
TPID:88A8
C-port
Packet
No VLAN
Packet
VID:8
TPID:8100
X
Packet Discarded


Packet
No VLAN
Packet
VID:10
TPID:8100
Packet
VID:10
TPID:88A8
S-port
Packet
No VLAN
X
Packet Discarded
Packet
VID:10
TPID:88A8


Packet
No VLAN
Packet
VID:5
TPID:8100
Packet
VID:5
TPID:88A8
S-custom-port
Packet
No VLAN
X
Packet Discarded
Packet
VID:5
TPID:8123
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 .

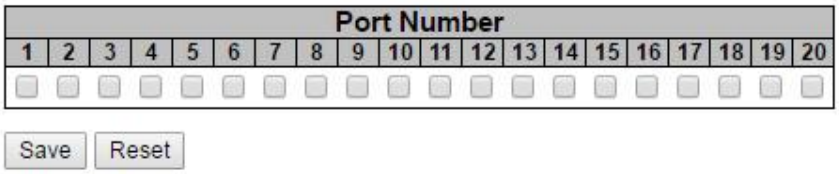
5.6.2.1 Private VLAN

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical. A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.
A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.



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. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Adding a New Static Entry	Click Add New Private VLAN to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction. The Private VLAN is enabled when you click "Save". The Delete button can be used to undo the addition of new Private VLANs.

5.6.2.2 Port Isolation Configuration

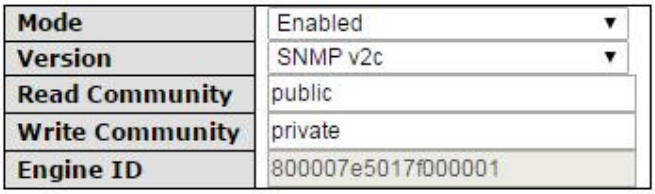


Label	Description
Port Members	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled for that port. When unchecked, port isolation is disabled for that port. By default, port isolation is disabled for all ports.

5.7 SNMP

The Simple Network Management Protocol is used on IP based networks for the collection and organization of data from end devices by managed networking equipment.

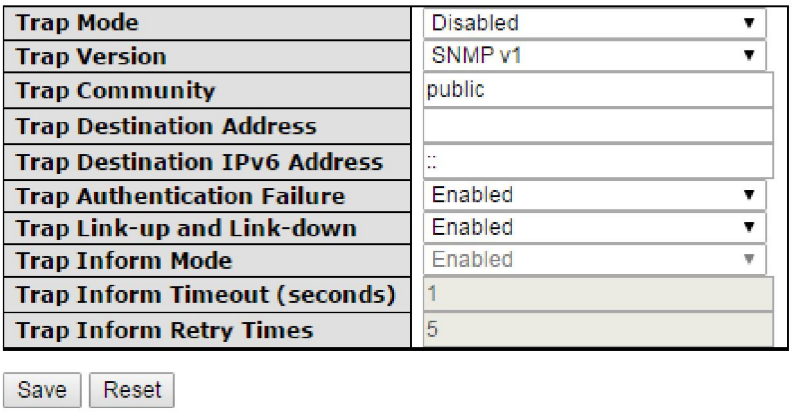
5.7.1 SNMP System Configuration



Label	Description
Mode	Indicates the SNMP mode operation. Possible modes are: Enabled: Enable SNMP mode operation. Disabled: Disable SNMP mode operation.
Version	Indicates the SNMP supported version. Possible versions are: SNMP v1: Set SNMP supported version 1. SNMP v2c: Set SNMP supported version 2c. SNMP v3: Set SNMP supported version 3.
Read Community	Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using USM for authentication and privacy and the community string will associated with SNMPv3 communities table

Write Community	Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using USM for authentication and privacy and the community string will associated with SNMPv3 communities 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.

5.7.2 SNMP Trap Configuration

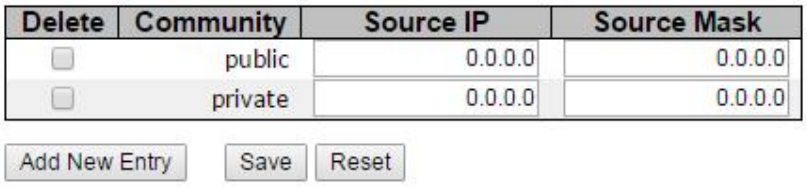


Label	Description
Trap Mode	Indicates the SNMP trap mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.
Trap Version	Indicates the SNMP trap supported version. Possible versions are: SNMP v1: Set SNMP trap supported version 1. SNMP v2c: Set SNMP trap supported version 2c. SNMP v3: Set SNMP trap supported version 3.
Trap Community	Indicates the community access string when sending an SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.
Trap Destination Address	Indicates the SNMP trap destination address. Trap Destination IPv6 Address

Trap Destination IPv6 Address	Provide the trap destination IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates 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 only appear once. It also used 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 are: 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 operation. Possible modes are: Enabled: Enable SNMP trap link-up and link-down mode operation. Disabled: Disable SNMP trap link-up and link-down mode operation.
Trap Inform Mode	Indicates the SNMP trap inform mode operation. Possible modes are: Enabled: Enable SNMP trap inform mode operation. Disabled: Disable SNMP trap inform mode operation.
Trap Inform Timeout(seconds)	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.
Trap Inform Retry Times	Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.
Trap Probe Security Engine ID	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: Enabled: Enable SNMP trap probe security engine ID mode of operation. Disabled: Disable SNMP trap probe security engine ID mode of operation.
Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is

	used. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed.
Trap Security Name	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

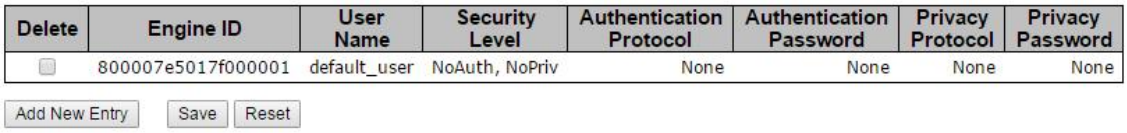
5.7.3 SNMP-Communities



SNMP Communities Table

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 the allowed content is the ASCII characters from 33 to 126.
Source IP	Indicates the SNMP access source address.
Source Mask	Indicates the SNMP access source address mask.

5.7.4 SNMP Users



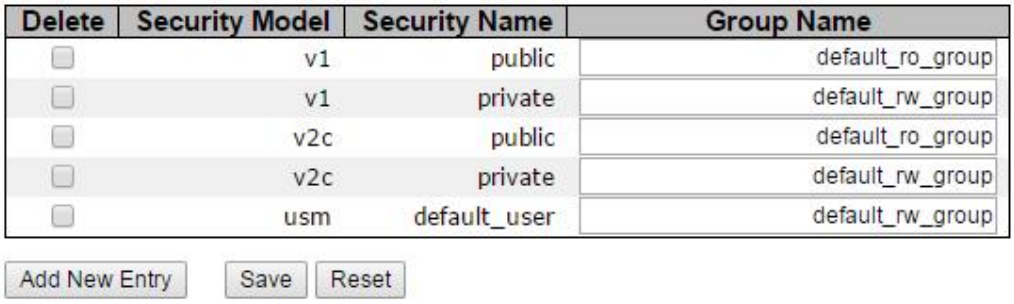
SNMPv3 Table

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 the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM

	entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In othe words, if user engine ID equal system engine ID then it is local user; otherwize it's remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: None authentication and none privacy. Auth, NoPriv: Authentication and none privacy. Auth, Priv: Authentication and privacy. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: None: None authentication protocol. MD5: An optional flag to indicate that this user using MD5 authentication protocol. SHA: An optional flag to indicate that this user using SHA authentication protocol. The value of security level cannot be modified if an entry already exists. That means you must first ensure that the value is set correctly.
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. The allowed content is the ASCII characters from 33 to 126.
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are: None: None privacy protocol. DES: An optional flag to indicate that this user using DES authentication protocol.
Privacy	A string identifying the privacy pass phrase. The allowed string

Password	length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126.

5.7.5 SNMPv3 Group Configuration



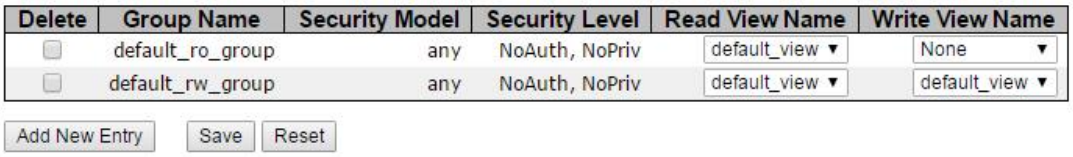
Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: v1: Reserved for SNMPv1. v2c: Reserved for SNMPv2c. usm: User-based Security Model (USM).
Security Name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

5.7.6 SNMPv3 View Configuration

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 the allowed content is the ASCII characters from 33 to 126.
View Type	Indicates the view type that this entry should belong to. Possible view types are: Included: An optional flag to indicate that this view subtree should be included. Excluded: An optional flag to indicate that this view subtree should be excluded. Generally, if a view entry's view type is 'excluded', it should be another view entry in which the view type is 'included' and it's OID subtree oversteps the 'excluded' view entry.
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

5.7.7 SNMPv3 Access Configuration



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 the allowed content is the ASCII characters from 33 to 126.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: Any: Accepted any security model (v1|v2c|usm). V1: Reserved for SNMPv1.

	V2c: Reserved for SNMPv2c. Usm: User-based Security Model (USM).
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: None authentication and none privacy. Auth, NoPriv: Authentication and none privacy. Auth, Priv: Authentication and privacy.
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Write View Name	The name of the MIB view defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

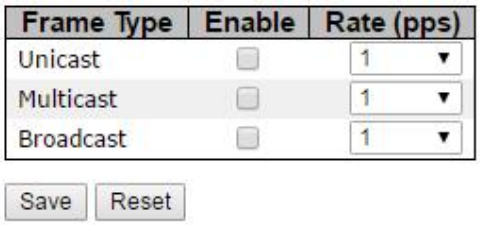
5.8 Traffic Prioritization

The practice of implementing a process that when under heavy traffic pressure the network will begin giving higher preference to traffic that has been assigned higher priority levels then other traffic or non-assigned traffic.

5.8.1 Storm Control Configuration

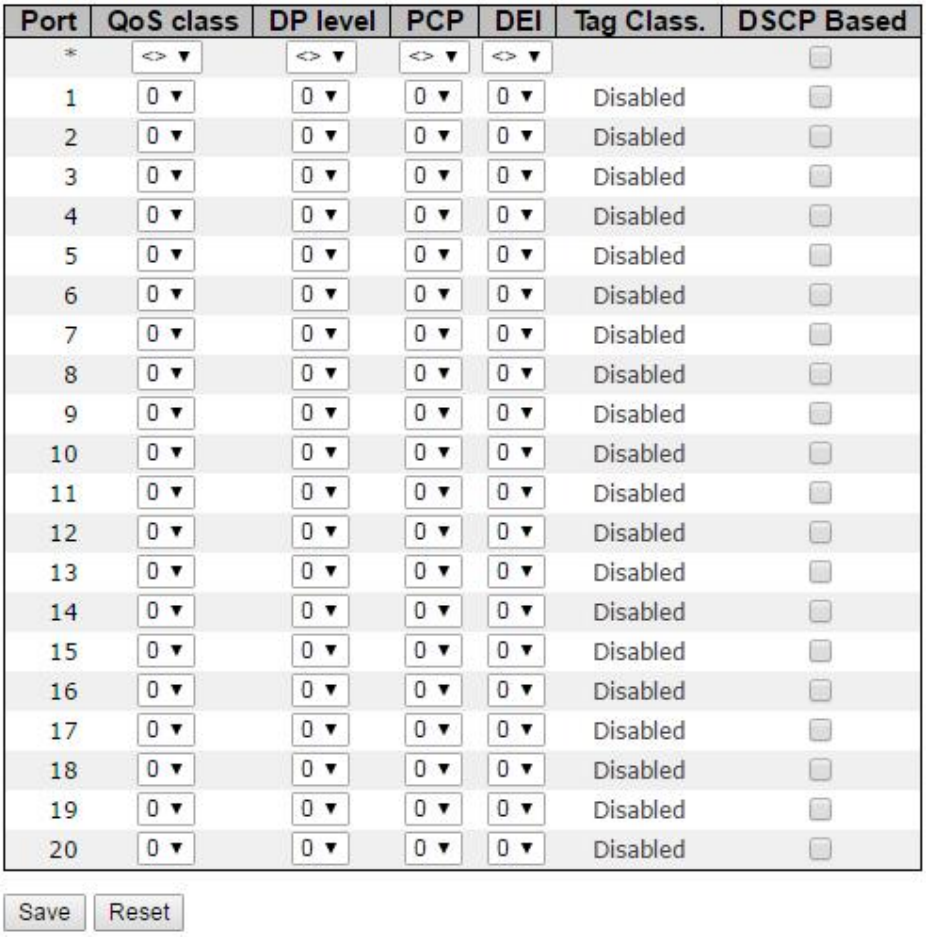
There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.
The rate is 2^n, where n is equal to or less than 15, or "No Limit". The unit of the rate can be either pps (packets per second) or kpps (kilopackets per second). The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

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



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

5.8.2 Port QoS (Quality of Service)



Port	QoS class	DP level	PCP	DEI	Tag Class.	DSCP Based
*	<>	<>	<>	<>		
1	0	0	0	0	Disabled	
2	0	0	0	0	Disabled	
3	0	0	0	0	Disabled	
4	0	0	0	0	Disabled	
5	0	0	0	0	Disabled	
6	0	0	0	0	Disabled	
7	0	0	0	0	Disabled	
8	0	0	0	0	Disabled	
9	0	0	0	0	Disabled	
10	0	0	0	0	Disabled	
11	0	0	0	0	Disabled	
12	0	0	0	0	Disabled	
13	0	0	0	0	Disabled	
14	0	0	0	0	Disabled	
15	0	0	0	0	Disabled	
16	0	0	0	0	Disabled	
17	0	0	0	0	Disabled	
18	0	0	0	0	Disabled	
19	0	0	0	0	Disabled	
20	0	0	0	0	Disabled	

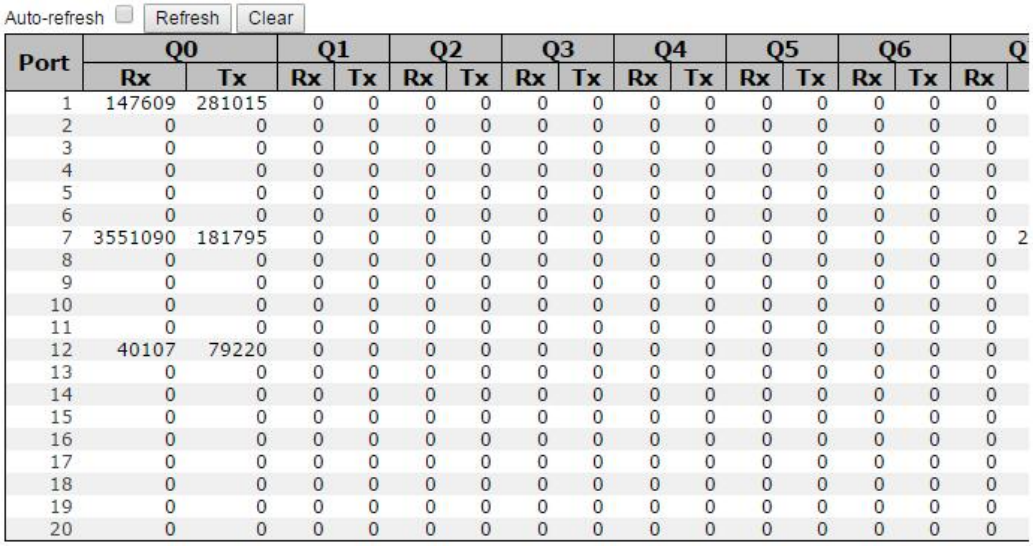
Save Reset

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 has a Tag Class. If 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 has aTag Class. If 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 in order to configure the mode and/or mapping. **Note:** This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default QoS class and DP level.
DSCP Based	Click to Enable DSCP Based QoS Ingress Port Classification.

5.8.3 QoS Statistics


Auto-refresh Refresh Clear

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx
1	147609	281015	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
3	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
5	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
7	3551090	181795	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	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
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	40107	79220	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Label	Description
Port	The logical port for the settings contained in the same row.
Qn	There are 8 QoS queues per port. Q0 is the lowest priority queue.
Rx / Tx	The number of received and transmitted packets per queue.

5.9 IGMP Snooping

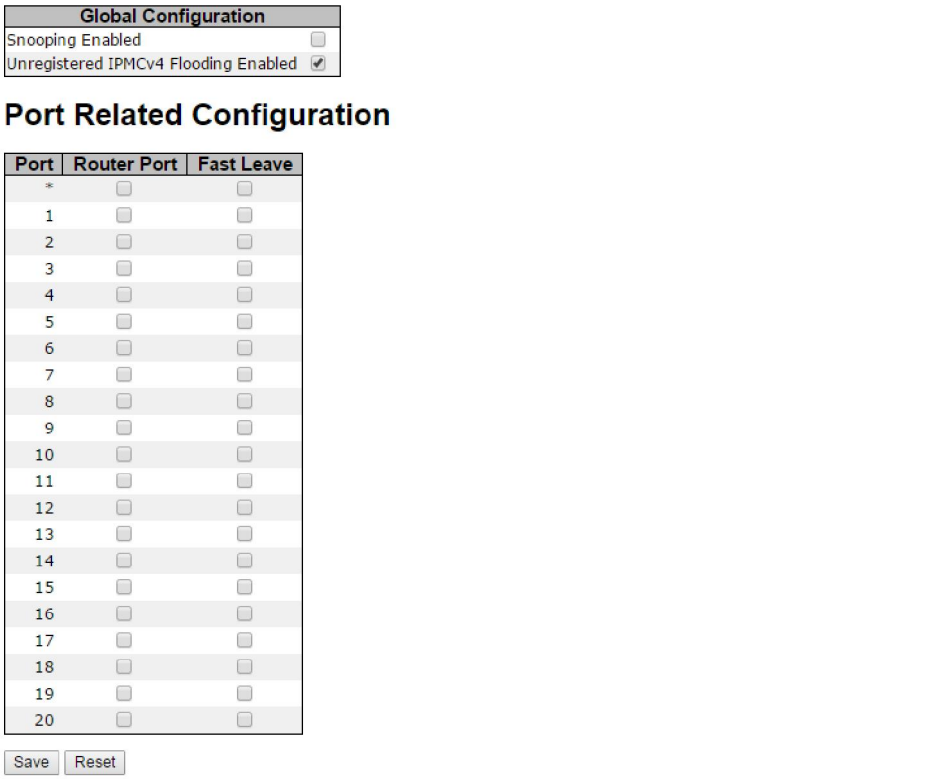
The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships.

When IGMP snooping is enabled in a switch, it analyzes all the IGMP packets between hosts connected to the switch and multicast routers in the network. When a switch receives an IGMP report for a given multicast group from a host, the switch adds the host's port number to the multicast list for that group. When the switch hears an IGMP leave, it removes the host's port from the table entry.

IGMP snooping can reduce multicast traffic from streaming and other bandwidth intensive IP applications more effectively. A switch using IGMP snooping will only forward multicast traffic to the hosts in that traffic. This reduction of multicast traffic reduces the packet processing at the switch (at the cost of needing additional memory to handle the multicast tables) and also decreases the workload at the end hosts since their network cards (or operating system) will not receive and filter all the multicast traffic generated in the network.

IGMP has 3 versions, IGMP v1, v2, and v3, and support query group up to 256 groups.

5.9.1 IGMP Snooping Configuration



Label	Description
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMCv4 Flooding Enabled	Enable unregistered IPMC traffic flooding.
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port.

5.9.2 IGMP Snooping Status

Statistics

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

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-
17	-
18	-
19	-
20	-

IGMP Snooping Table

Label	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	Working Querier Version currently.
Host Version	Working Host Version currently.
Querier Status	Show the Querier status is "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.
Refresh	Click to refresh the page immediately.
Clear	Clears all Statistics counters.
Auto-refresh ☐	Check this box to enable an automatic refresh of the page at regular intervals.
Port	Switch Port number
Status	Indicate whether specific port is a router port or not .

5.10 Security

5.10.1 ACL

Refresh Clear

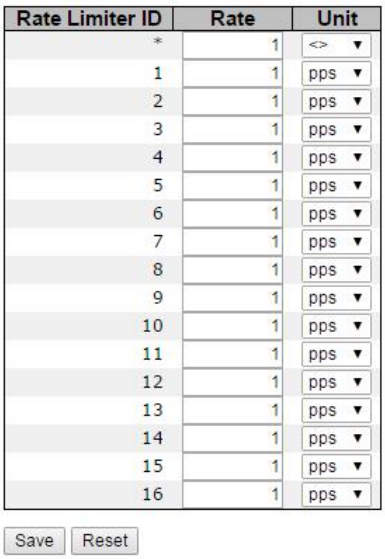
Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	147609
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	3593447

Label	Description
Port	The logical port for the settings contained in the same row.
Policy ID	Select the policy to apply to this port. The allowed values are 1 through 8. The default value is 1.
Action	Select whether forwarding is permitted ("Permit") or denied

	("Deny"). The default value is "Permit".
Rate Limiter ID	Select which rate limiter to apply to this port. The allowed values are Disabled or the values 1 through 15. The default value is "Disabled".
Port Copy	Select which port frames are copied. The allowed values are Disabled for a specific port number. The default value is "Disabled".
Logging	Specify the logging operation of this 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 the System Log memory size and logging rate is limited.
Shutdown	Specify the port shut down operation of this port. The allowed values are: Enabled: If a frame is received on the port, the port will be disabled. Disabled: Port shut down is disabled. The default value is "Disabled".
Counter	Counts the number of frames that match this ACE.

5.10.1.1 Rate Limit

Configuration of the rate limiting the access control list of the switch.



Label	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate	The rate unit is packets per second (pps), configure the rate 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.

5.10.1.2 Access Control List

Configure an ACE (Access Control Entry) on this page.

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type that you selected.

Access Control List Configuration

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

Label	Description
Ingress Port	Select the ingress port for which this ACE applies. 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 through 8.
Frame Type	Select the frame type for this ACE. These frame types are mutually exclusive. Any: Any frame can match this ACE. Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 descripts the value of Length/Type Field specifications should be greater than or equal to 1536 decimal (equal to 0600 hexadecimal). ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with Ethernet type. IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with Ethernet type.

Action	Specify the action to take with a frame that hits this ACE. Permit: The frame that hits this ACE is granted permission for the ACE operation. Deny: The frame that hits this ACE is dropped.
Rate Limiter	Specify the rate limiter in number of base units. The allowed range is 1 to 15. Disabled indicates that the rate limiter operation is disabled.
Port Copy	Frames that hit the ACE are copied to the port number specified here. The allowed range is the same as the switch port number range. Disabled indicates that the port copy operation is disabled.
Logging	Specify 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 the System Log memory size and logging rate is limited.
Shutdown	Specify the port shut down operation of the ACE. The allowed values are: Enabled: If a frame matches the ACE, the ingress port will be disabled. Disabled: Port shut down is disabled for the ACE.
Counter	The counter indicates the number of times the ACE was hit by a frame.

5.10.2 802.1x

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

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

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

Overview of 802.1X (Port-Based) Authentication

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The 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 is special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames 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, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

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

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

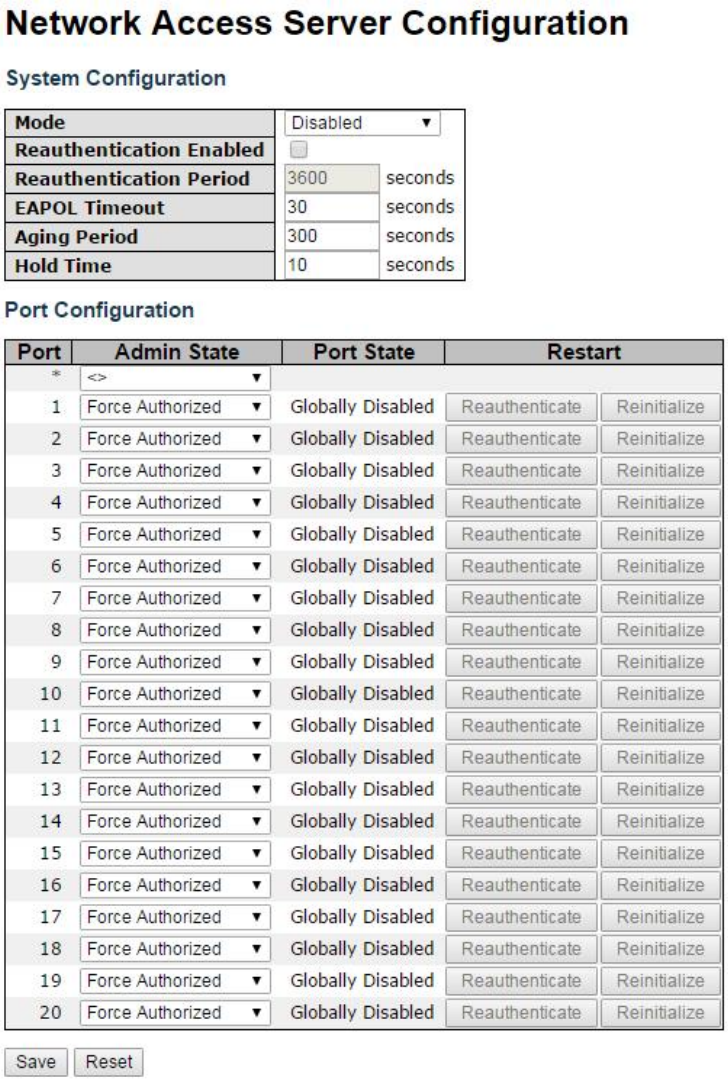
Overview of MAC-Based Authentication

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 on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using 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 don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users, equipment whose MAC address is a valid RADIUS user can be used by anyone, and only the MD5-Challenge method is supported.

The 802.1X and MAC-Based Authentication configuration consists of two sections, a system- and a port-wide

5.10.2.1 Configuration



802.1x Configuration Definition Table

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 forwarding of 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 doesn't 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 reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
EAPOL Timeout	Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.
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 doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.
Hold Time	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: • MAC-Based Auth. If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified

	on the "Configuration→Security→AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. The switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.
Port	The port number for which the configuration below applies.
Admin State	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available: **Force Authorized** In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication. **Force Unauthorized** In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access. **Port-based 802.1X** In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch is special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames 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, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or

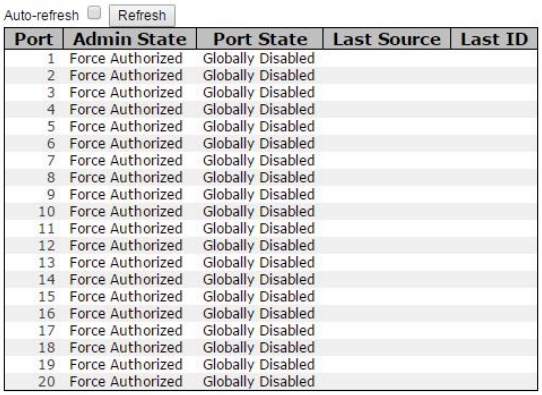
	how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it. When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant. Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate. 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 really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does 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 communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. 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. 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 really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant. Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get 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 destination MAC address for EAPOL frames sent from the switch towards 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 on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard. The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is

	that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.
Port State	The current state of the port. It can undertake one of the following values: **Globally Disabled**: NAS is globally disabled. **Link Down**: NAS is globally enabled, but there is no link on the port. **Authorized**: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. **Unauthorized:** The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. **X Auth/Y Unauth**: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.
Restart	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-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 for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized. **Reinitialize**: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

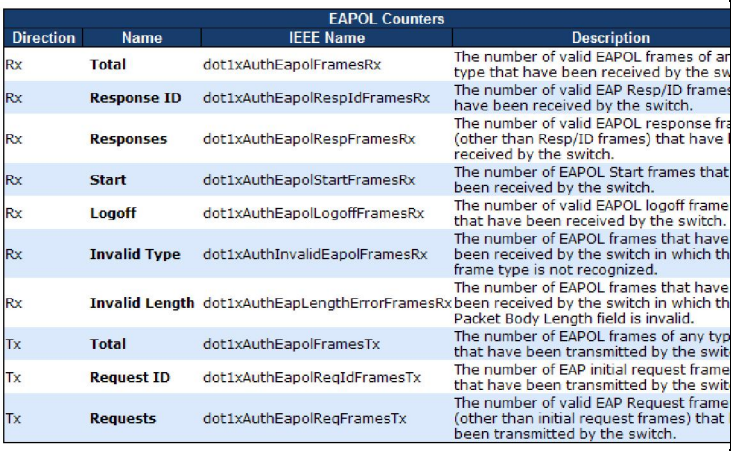
5.10.2.2 802.1x Switch Status



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

5.10.2.3 802.1x Port Statistics

This page provides detailed IEEE 802.1X statistics for a specific switch port running port-based authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only. Use the port select box to select which port details to be displayed.

<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td>Admin State</td><td>The port's current administrative state. Refer to NAS Admin State for a description of possible values.</td></tr>
<tr><td>Port State</td><td>The current state of the port. Refer to NAS Port State for a description of the individual states.</td></tr>
<tr><td>EAPOL Counters</td><td>These supplicant frame counters are available for the following administrative states:
• Force Authorized
• Force Unauthorized
• 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>Total</td><td>dot1xAuthEapolFramesRx</td><td>The number of valid EAPOL frames of ar type that have been received by the sw</td></tr>
<tr><td>Rx</td><td>Response ID</td><td>dot1xAuthEapolRespIdFramesRx</td><td>The number of valid EAP Resp/ID frames have been received by the switch.</td></tr>
<tr><td>Rx</td><td>Responses</td><td>dot1xAuthEapolRespFramesRx</td><td>The number of valid EAPOL response fra (other than Resp/ID frames) that have received by the switch.</td></tr>
<tr><td>Rx</td><td>Start</td><td>dot1xAuthEapolStartFramesRx</td><td>The number of EAPOL Start frames that been received by the switch.</td></tr>
<tr><td>Rx</td><td>Logoff</td><td>dot1xAuthEapolLogoffFramesRx</td><td>The number of valid EAPOL logoff frame that have been received by the switch.</td></tr>
<tr><td>Rx</td><td>Invalid Type</td><td>dot1xAuthInvalidEapolFramesRx</td><td>The number of EAPOL frames that have been received by the switch in which th frame type is not recognized.</td></tr>
<tr><td>Rx</td><td>Invalid Length</td><td>dot1xAuthEapLengthErrorFramesRx</td><td>The number of EAPOL frames that have been received by the switch in which th Packet Body Length field is invalid.</td></tr>
<tr><td>Tx</td><td>Total</td><td>dot1xAuthEapolFramesTx</td><td>The number of EAPOL frames of any typ that have been transmitted by the swit</td></tr>
<tr><td>Tx</td><td>Request ID</td><td>dot1xAuthEapolReqIdFramesTx</td><td>The number of EAP initial request frame that have been transmitted by the swit</td></tr>
<tr><td>Tx</td><td>Requests</td><td>dot1xAuthEapolReqFramesTx</td><td>The number of valid EAP Request frame (other than initial request frames) that been transmitted by the switch.</td></tr>
</table></td></tr>
<tr><td>Backend Server Counters</td><td>These backend (RADIUS) frame counters are available for the following administrative states:
• 802.1X
• MAC-based Auth.</td></tr>
</table>

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

802.1X
MAC-based Auth.

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

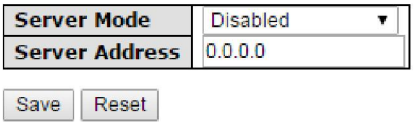
5.11 System Warnings

5.11.1 Fault Alarm

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

5.11.2 System Log Configuration

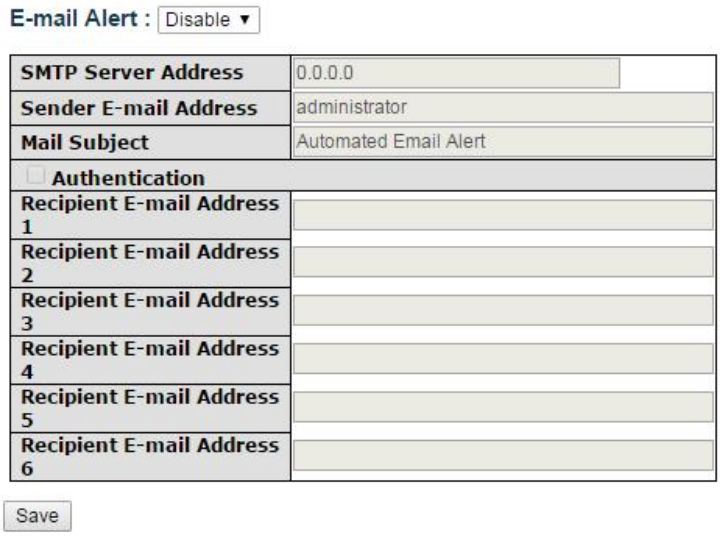
The SYSLOG is a protocol that transmits event notification messages across networks. Please refer to RFC 3164 - The BSD SYSLOG Protocol



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

5.11.3 SMTP Settings

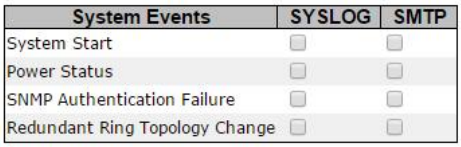
The SMTP is short for Simple Mail Transfer Protocol. It is a protocol for e-mail transmission across the Internet. Please refer to RFC 821 - Simple Mail Transfer Protocol.



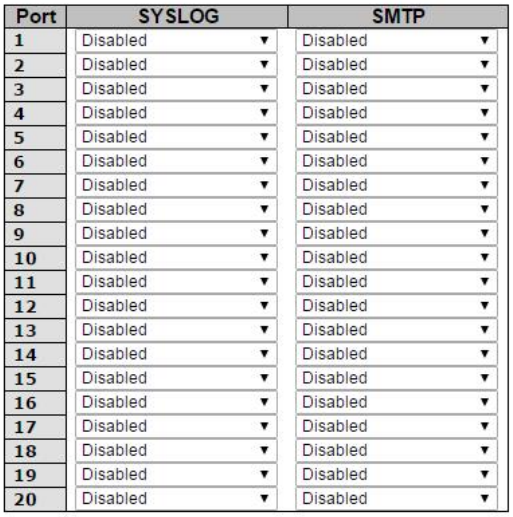
Label	Description
E-mail Alarm	Enable/Disable transmission system warning events by e-mail.
Sender E-mail Address	The SMTP server IP address
Mail Subject	The Subject of the mail
Authentication	■ **Username:** the authentication username. ■ **Password:** the authentication password. ■ **Confirm Password:** re-enter password.
Recipient E-mail Address	The recipient's E-mail address. It supports 6 recipients for a mail.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.11.4 Event Selection

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



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
13	Disabled	Disabled
14	Disabled	Disabled
15	Disabled	Disabled
16	Disabled	Disabled
17	Disabled	Disabled
18	Disabled	Disabled
19	Disabled	Disabled
20	Disabled	Disabled

Label	Description
System Cold Start	Alert when system restarts
Power Status	Alert when a power up or down occurs
SNMP Authentication Failure	Alert when SNMP authentication fails
Super Ring Topology Change	Alert when Super Ring topology changes
Port Event SYSLOG / SMTP event	■ **Disable** ■ **Link Up** ■ **Link Down** ■ **Link Up & Link Down**
Apply	Click "**Apply**" to activate the configurations
Help	Show help file

5.12 Monitor and Diagnose

5.12.1 MAC Table

5.12.1.1 MAC Address Table Configuration

The configuration for the MAC addresses is set by the following options. The user will need to set timeouts for the dynamic MAC table here.

Aging Configuration

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

Configure aging time by entering a value here in seconds; for example, **Age time** seconds.

The allowed range is 10 to 1000000 seconds.

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

Aging Configuration

Disable Automatic Aging	☐
Aging Time	300 seconds

MAC Table Learning

If the learning mode for a given port is grayed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

Each port can do learning based upon the following settings:

MAC Table Learning

	Port Members																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Auto	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

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.

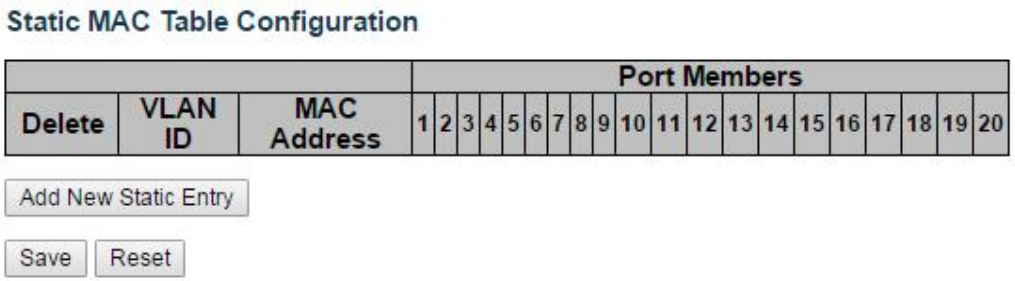
	Note: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The maximum of 64 entries is for the whole stack, and not per switch.

The MAC table is sorted first by VLAN ID and then by MAC address.



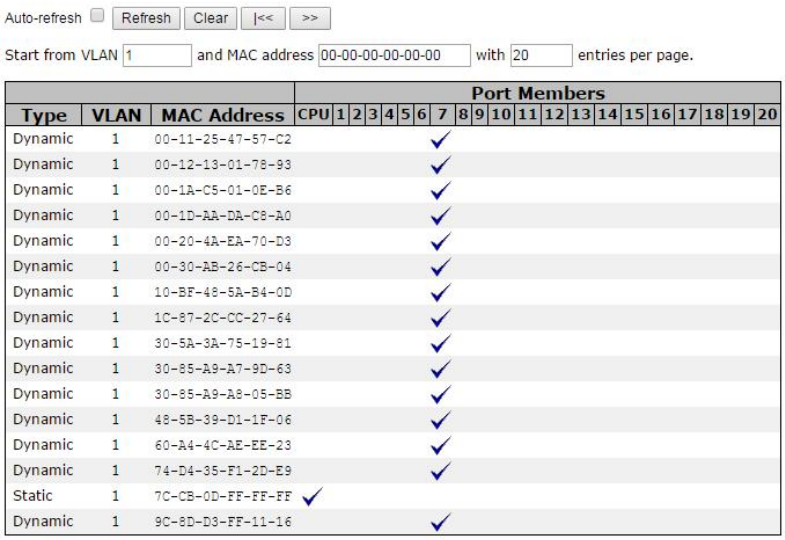
Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Adding a New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

5.12.1.2 MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

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

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



MAC Table Description

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.

5.12.2 Port Statistics for Monitoring and Diagnostics

5.12.2.1 Traffic Overview

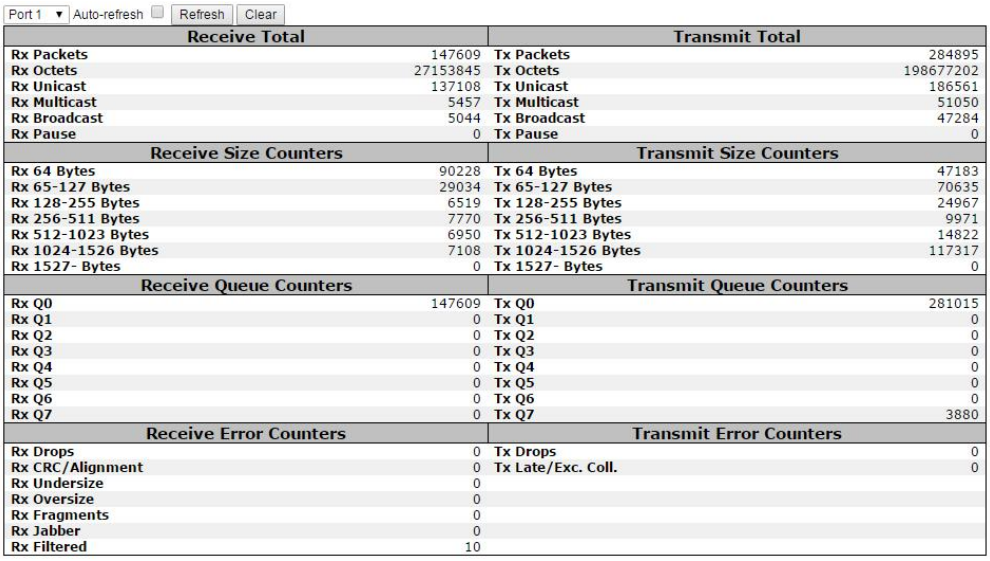
Auto-refresh ☐ Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	147609	284895	27153845	198677202	0	0	0	0	10
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	3662679	472342	721281569	173456288	0	0	34	0	914539
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	40107	79302	5139579	70780802	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0

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

5.12.2.2 Detailed Port Statistics

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.



Receive Total		Transmit Total	
Rx Packets	147609	Tx Packets	284895
Rx Octets	27153845	Tx Octets	198677202
Rx Unicast	137108	Tx Unicast	186561
Rx Multicast	5457	Tx Multicast	51050
Rx Broadcast	5044	Tx Broadcast	47284
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	90228	Tx 64 Bytes	47183
Rx 65-127 Bytes	29034	Tx 65-127 Bytes	70635
Rx 128-255 Bytes	6519	Tx 128-255 Bytes	24967
Rx 256-511 Bytes	7770	Tx 256-511 Bytes	9971
Rx 512-1023 Bytes	6950	Tx 512-1023 Bytes	14822
Rx 1024-1526 Bytes	7108	Tx 1024-1526 Bytes	117317
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	147609	Tx Q0	281015
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	3880
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	10		

Detailed Port Statistics Description

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. Includes FCS, but excludes framing bits.
Rx and Tx Unicast	The number of received and transmitted (good and bad) unicast packets.
Rx and Tx Multicast	The number of received and transmitted (good and bad) multicast packets.
Rx and Tx Broadcast	The number of received and transmitted (good and bad) broadcast packets.
Rx and Tx Pause	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
Rx Drops	The number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short 1 frames received with valid CRC.
Rx Oversize	The number of long 2 frames received with valid CRC.

Rx Fragments	The number of short 1 frames received with invalid CRC.
Rx Jabber	The number of long 2 frames received with invalid CRC.
Rx Filtered	The number of received frames filtered by the forwarding process.
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.

5.12.3 Port Monitoring

Configure port Mirroring on this page.

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

The traffic to be copied to the mirror port is selected as follows:
-All frames received on a given port (also known as ingress or source mirroring).
-All frames transmitted on a given port (also known as egress or destination mirroring).
Port to mirror is also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this port. The Disabled setting disables mirroring.

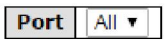
Label	Description
Port	The logical port for the settings contained in the same row.
Mode	Select mirror mode. Rx Only: Frames received at this port are mirrored to the mirror port. Frames transmitted are not mirrored. Tx Only: Frames transmitted from this port are mirrored to the mirror port. Frames received are not mirrored. Disabled: Neither frames transmitted nor frames received are mirrored. Enabled: Frames received and frames transmitted are mirrored to the mirror port.

	***Note:** For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames for the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

5.12.4 System Log Information

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: Information level of the system log. Warning: Warning level of the system log. Error: Error level of the system log. All: All levels.
Time	The time of the system log entry.
Message	The MAC Address of this switch.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Updates the system log entries, starting from the current entry ID.
Clear	Flushes all system log entries.
|<<	Updates the system log entries, starting from the first available entry ID.
<<	Updates the system log entries, ending at the last entry currently displayed.
>>	Updates the system log entries, starting from the last entry currently displayed.
>>|	Updates the system log entries, ending at the last available entry ID.

5.12.5 VeriPHY Cable Diagnostics



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	--	--	--	--	--	--	--	--

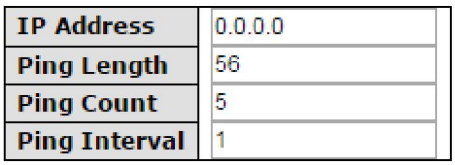
Press “Start” to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate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

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

Label	Description
Port	The port where you are requesting VeriPHY Cable Diagnostics.
Cable Status	Port: Port number. Pair: The status of the cable pair. Length: The length (in meters) of the cable pair.

5.12.6 ICMP Ping

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



Start

After you press “Start”, 5 ICMP packets are transmitted, and the sequence number and roundtrip 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 ::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

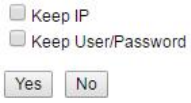
Sent 5 packets, received 5 OK, 0 bad

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 bytes to 1400 bytes.

5.13 Factory Default

The switch can be returned to the original factory settings. Options are available to keep the current in use IP address or to keep the current in use User/Password information.

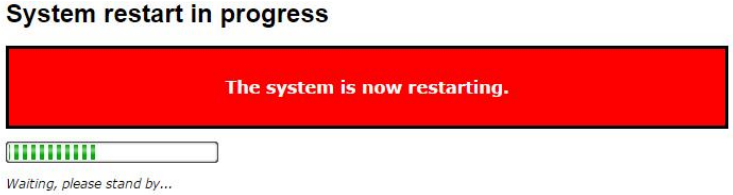


Label	Description
Yes	Click to reset the configuration to Factory Defaults.
No	Click to return to the Port State page without resetting the configuration.

5.14 System Reboot

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

After restarting the switch a progress bar will appear.



6. Command Line Interface Management

6.1 About CLI Management

Besides WEB-based management, LNX-2012GN-SFP series also supports CLI management. Users can use console or telnet to management switch by CLI.

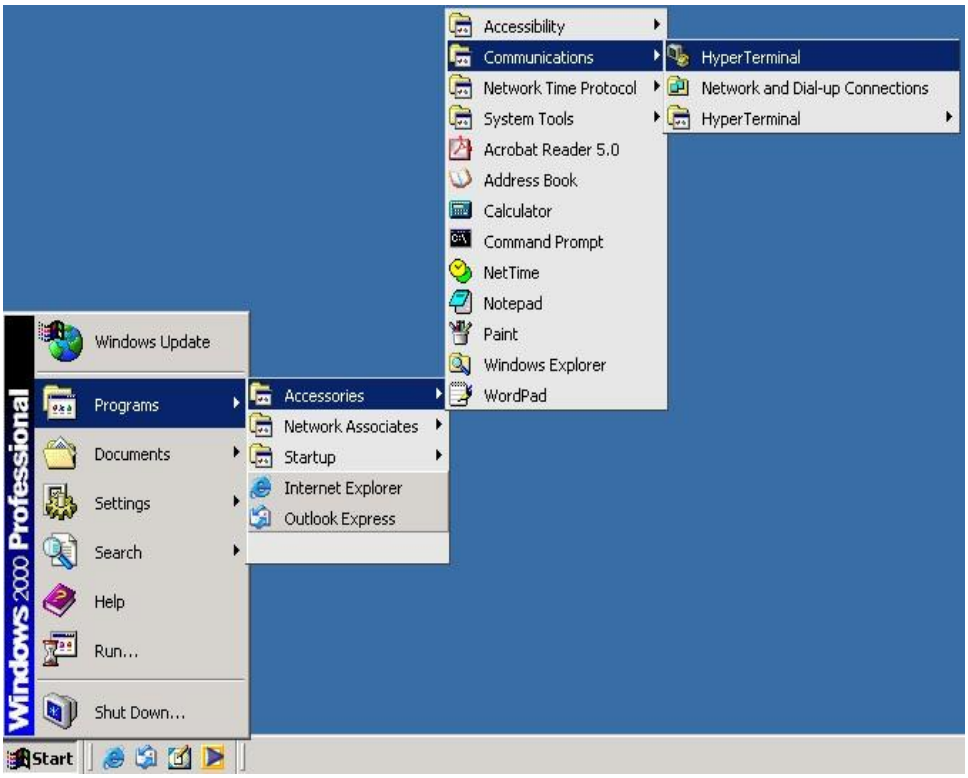
CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

Before configuring by an RS-232 serial console, use an RJ45 to DB9-F cable to connect the switches' RS-232 Console port to the PC's COM port.

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

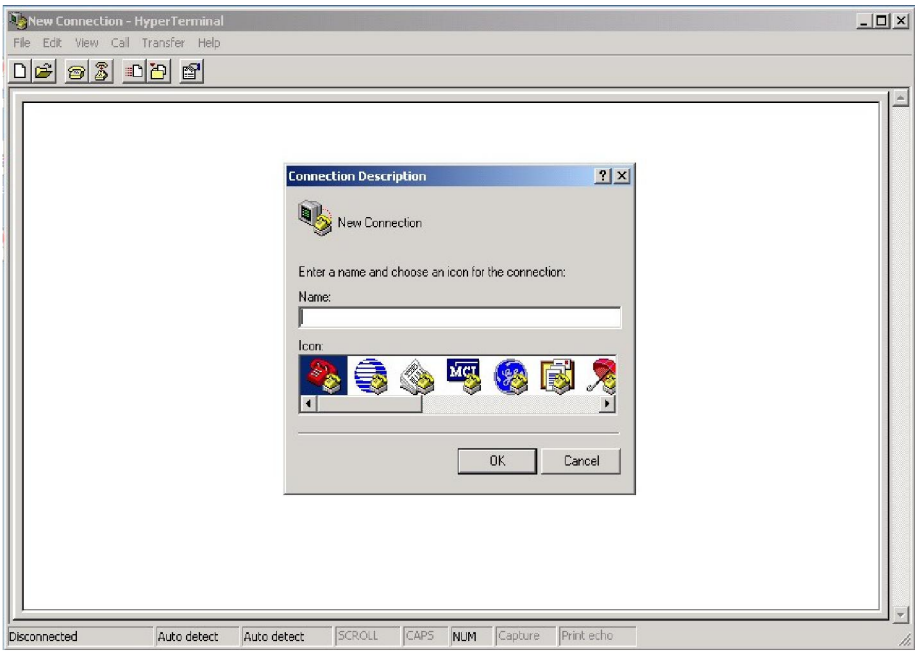
Step 1:

From the Windows desktop, click on Start -> Programs -> Accessories -> Communications -> Hyper Terminal.



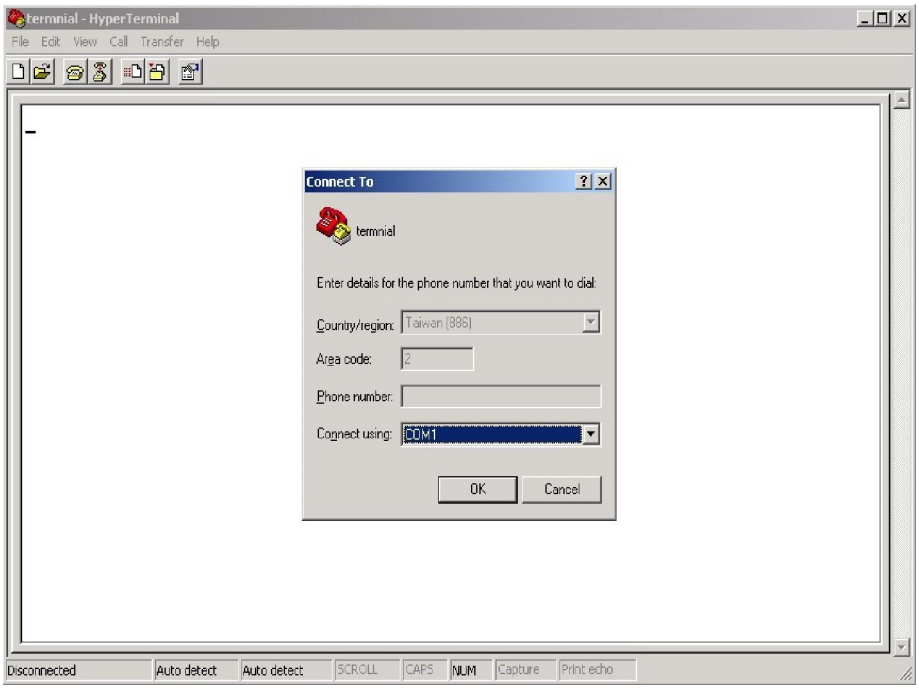
Step 2:

Input a name for the new connection.



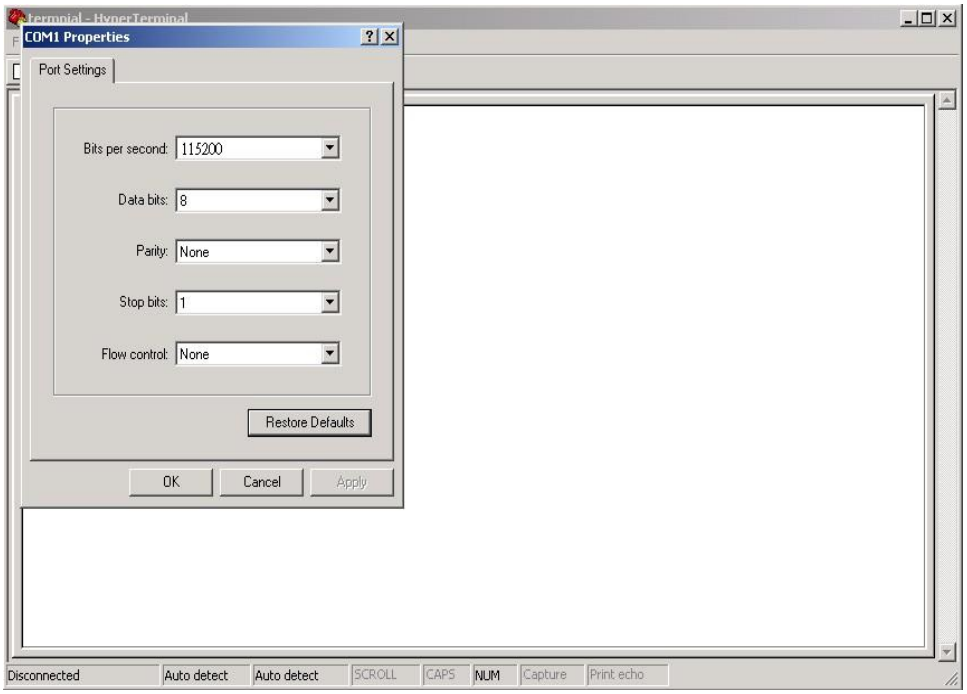
Step 3:

Select to use a specific COM port number.



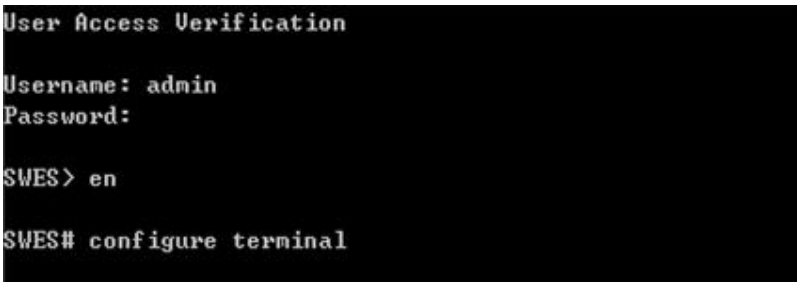
Step 4:

The COM port property settings are as follows: 115200 for “Bits per second”, 8 for “Data bits”, None for Parity, 1 for “Stop bits” and none for “Flow control”.



Step 5:

The Console login screen will appear. Use the keyboard to enter the Username and Password, and then press “**Enter**”.



CLI Management by Telnet

Users can use "**TELNET**" to configure the switches.

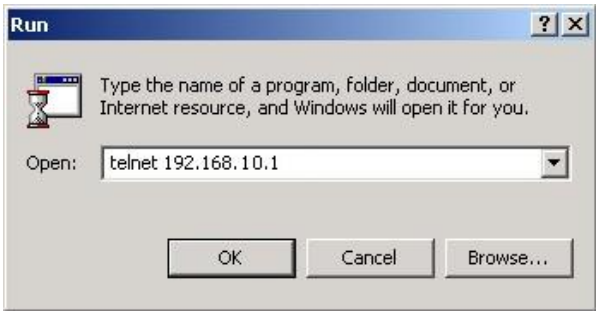
The default value is as below:

- IP Address: **192.168.1.254**
- Subnet Mask: **255.255.255.0**
- Default Gateway: none
- User Name: **admin**
- Password: **admin**

Follow the steps below to access the console via Telnet.

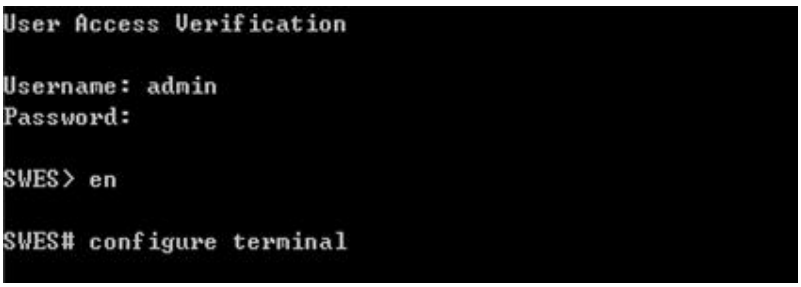
Step 1:

Telnet to the IP address of the switch from the Windows "**Run**" command as below.



Step 2:

The Login screen will appear. Use the keyboard to enter the Username and Password, and then press "**Enter**"



Commander Groups

Group	Command	Mode
System	Configuration [all] [<port_list>]	configure
	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	Configuration	configure
	DHCP [enable|disable]	
	Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]	
	Ping <ip_addr_string> [<ping_length>]	
	SNTP [<ip_addr_string>]	
MAC	Configuration [<port_list>]	configure
	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	
Security	Switch **Switch security setting**	configure
	Network **Network security setting**	
	AAA **Authentication, Authorization and Accounting setting**	
Security Switch	Password <password>	configure
	Auth **Authentication**	
	SSH **Secure Shell**	
	HTTPS **Hypertext Transfer Protocol over Secure Socket Layer**	

	RMON **Remote Network Monitoring**	
Security Switch Authentication	Configuration	configure
	Method [console|telnet|ssh|web] [none|local|radius] [enable|disable]	
Security Switch SSH	Configuration	configure
	Mode [enable|disable]	
Security Switch HTTPS	Configuration	configure
	Mode [enable|disable]	
Security Switch RMON	Statistics Add <stats_id> <data_source>	configure
	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	Psec **Port Security Status**	configure
	NAS **Network Access Server (IEEE 802.1X)**	
	ACL **Access Control List**	
	DHCP **Dynamic Host Configuration Protocol**	
Security Network Psec	Switch [<port_list>]	configure
	Port [<port_list>]	
Security Network ACL	Configuration [<port_list>]	configure
	Action [<port_list>] [permit|deny] [<rate_limiter>][<port_redirect>] [<mirror>] [<logging>] [<shutdown>]	
	Policy [<port_list>] [<policy>]	
	Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]	
	Add [<ace_id>] [<ace_id_next>][(port <port_list>)] [(policy <policy> <policy_bitmask>)][<tagged>] [<vid>] [<tag_prio>] [<dmac_type>][(etype [<etype>] [<smac>] [<dmac>]) |	

	(arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) | (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) | (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) | (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])] [permit|deny] [<rate_limiter>] [<port_redirect>] [<mirror>] [<logging>][<shutdown>]	
	Delete <ace_id>	
	Lookup [<ace_id>]	
	Clear	
	Status [combined|static|loop_protect|dhcp|ptp|ipmc|conflicts]	
	Port State [<port_list>] [enable|disable]	
Security Network DHCP	Configuration	configure
	Mode [enable|disable]	
	Server [<ip_addr>]	
	Information Mode [enable|disable]	
	Information Policy [replace|keep|drop]	
	Statistics [clear]	
STP	Configuration	
	Version [<stp_version>] Non-certified release, v	configure
	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>]	configure
	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>]	
STP	Msti Port Configuration [<msti>] [<port_list>]	
	Msti Port Cost [<msti>] [<port_list>] [<path_cost>]	
	Msti Port Priority [<msti>] [<port_list>] [<priority>]	
LACP	Configuration [<port_list>]	configure
	Mode [<port_list>] [enable|disable]	
	Key [<port_list>] [<key>]	
	Role [<port_list>] [active|passive]	
	Status [<port_list>]	
	Statistics [<port_list>] [clear]	
LLDP	Configuration [<port_list>]	configure
	Mode [<port_list>] [enable|disable]	
	Statistics [<port_list>] [clear]	
	Info [<port_list>]	
QoS	DSCP Map [<dscp_list>] [<class>] [<dpl>]	configure
	DSCP Translation [<dscp_list>] [<trans_dscp>]	
	DSCP Trust [<dscp_list>] [enable|disable]	
	DSCP Classification Mode [<dscp_list>] [enable|disable]	
	DSCP Classification Map [<class_list>] [<dpl_list>] [<dscp>]	
	DSCP EgressRemap [<dscp_list>] [<dpl_list>] [<dscp>]	
	Storm Unicast [enable|disable] [<packet_rate>]	
	Storm Multicast [enable|disable] [<packet_rate>]	
	Storm Broadcast [enable|disable] [<packet_rate>]	
	QCL Add [<qce_id>] [<qce_id_next>] [<port_list>]	

	[<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type>] [(etype [<etype>]) | (LLC [<DSAP>] [<SSAP>] [<control>]) | (SNAP [<PID>]) | (ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) | (ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])] [<class>] [<dp>] [<classified_dscp>]	
	QCL Delete <qce_id>	
	QCL Lookup [<qce_id>]	
	QCL Status [combined|static|conflicts]	
	QCL Refresh	
Mirror	Configuration [<port_list>]	configure
	Port [<port>|disable]	
	Mode [<port_list>] [enable|disable|rx|tx]	
IGMP	Configuration [<port_list>]	Configure
	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	Configuration [<port_list>]	configure
	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	Configuration [<port_list>]	configure
	Port [<port>|disable]	
	Mode [<port_list>] [enable|disable|rx|tx]	
Config	Save <ip_server> <file_name>	configure
	Load <ip_server> <file_name> [check]	
Firmware	Load <ip_addr_string> <file_name>	configure
SNMP	Trap Inform Retry Times [<retries>]	configure
	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	Load <ip_addr_string> <file_name>	configure
Loop Protect	Configuration	configure
	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	Configuration [igmp]	configure
	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	Alarm PortLinkDown [<port_list>] [enable|disable]	configure
	Alarm PowerFailure [pwr1|pwr2|pwr3] [enable|disable]	
Event	Configuration	configure
	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	Mode [enable|disable]	configure
	Setup [<ip_start>] [<ip_end>] [<ip_mask>] [<ip_router>] [<ip_dns>] [<ip_tftp>] [<lease>] [<bootfile>]	
Fast Recovery	Mode [enable|disable]	configure
	Port [<port_list>] [<fr_priority>]	
SFP	syslog [enable|disable]	configure
	temp [<temperature>]	
	Info	
Modbus	Status	configure
	Mode [enable|disable]	

7. Technical Specifications

Table 7.1 has the technical specifications for Antaira's LNX-2012GN-SFP series: 20-port industrial gigabit managed Ethernet switches with 8*10/100/1000Tx and 12*100/1000 SFP slots for fiber.

Standards	IEEE 802.3	10Base-T 10Mbit/s Ethernet
	IEEE 802.3u	100Base-Tx, 100Base-Fx, Fast Ethernet
	IEEE 802.3ab	1000Base-Tx Gigabit Ethernet
	IEEE 802.3z	Gigabit Fiber
	IEEE 802.3x	Flow Control for Full Duplex
	IEEE 802.3ad	Port Trunking with LACP
	IEEE 802.1w	RSTP (Rapid Spanning Tree Protocol)
	IEEE 802.1s	MTP (Multiple Spanning Tree Protocol)
	IEEE 802.1q	Virtual LANs (VLAN)
	IEEE 802.1x	Port based Network Control, Authentication
	IEEE 802.1AB	LLDP
	IEEE 802.1p	QoS/CoS Protocol for Traffic Prioritization
Switch	Protocol	IGMPv1/v2, SNMPv1/v2c/v3, TFTP, SNTP, SMTP, RMON, HTTP, HTTPS, Telnet, Syslog, DHCP Option 82, SSH/SSL, Modbus/TCP, LLDP, IPv4/IPv6
	Data Process	Store and Forward
	Transfer Rate	14,880 pps for 10Base-Tx Ethernet port 148,800 pps for 100Base-TX Fast Ethernet port 1,488,000pps for 1000Base-TxGigabit Ethernet port
	Switch Bandwidth	40Gbps
	Packet Buffer	4 Mbits
	MAC Table	8K
	Jumbo Frame	9.6k
	Flow Control	IEEE 802.3x for full duplex mode, back pressure for half duplex mode
	VLAN Groups	1 ~ 4094
	IGMP Groups	Up to 256
Port Interface	Ethernet (RJ45) Port	8*10/100/1000BaseTx auto negotiation speed, Full/Half duplex mode, and auto MDI/MDI-X connection
	Fiber Port	12*100/1000 dual rate SFP Slots for fiber
	Wavelength	Refer to SFP Key Module
	Serial Console Port	1*RS232 in RJ45 connector with console cable, 115.2Kbps, 8,N,1
Protection	Overload Current	Present
	Power Reverse polarity	Present

	Network Cable	10Base-T: 2-pair UTP/STP Cat. 3, 4, 5 cable; 100Base-TX: 2-pair UTP/STP Cat. 5 cable. EIA/TIA-568 100-ohm (100m) 1000BaseTX: UTP/STP Cat.5/5E cable; EIA/TIA-568 100-ohm (100m)
Mechanical Characteristics	LED Indicator	Power Unit: P1 (Green), P2 (Green),fault(Amber) Ethernet port: Link/active(Green), 1000Mbps SFP: Link/active(Green)
	Housing	Metal IP30 protection
	Dimension	96.4 x 154 x 105.5 mm
	Weight	Unit Weight: 2.8 lbs. Shipping Weight: 3.6 lbs
	Mounting	DIN-Rail Mounting, wall-mounting (optional)
Power Requirement	Input Voltage	12~48VDC Redundant Input
	Power Connection	1 removable 6-contact terminal block
	Power Consumption	10 Watts
Environmental Limits	Operating Temperature	STD: -10° to 70° C (14° to 158° F); EOT: -40° to 75° C (-40° to 167° F)
	Storage Temperature	-40°C ~ 85°C (-40°F ~ 185°F)
	Ambient Relative Humidity	5 to 95%, (non-condensing)
Regulatory Approvals	EMI	FCC Class A
	EMS	IEC61000-4-2/3/4/5/6/8; IEC61000-6-2; IEC6100-6-4
	Stability Testing	IEC60068-2-32 (Free fall) IEC60068-2-27 (Shock) IEC60068-2-6 (Vibration)
	Safety	UL 508

Table 7.1 - LNX-2012GN-SFP Series Technical Specifications

Antaira Customer Service and Support

(Antaira US Headquarter) + 844-268-2472

(Antaira Europe Office) + 48-22-862-88-81

(Antaira Asia Office) + 886-2-2218-9733

Please report any problems to Antaira:

www.antaira.com / support@antaira.com

www.antaira.eu / info@antaira.eu

www.antaira.com.tw / info@antaira.com.tw

Any changes to this material will be announced on the Antaira website.