LMP-0600 Series

6-Port Industrial PoE+ Managed Ethernet Switch, with 4*10/100Tx (30W/Port) and 2*10/100Tx; 48~55VDC Power Input

User Manual

Version 1.2

www.antaira.com

© Copyright 2018 Antaira Technologies, LLC

All Rights Reserved
This document contains information, which is protected by copyright. Reproduction, adaptation or translation without prior permission is prohibited, except as allowed under the copyright laws.

Trademark Information

Antaira is a registered trademark of Antaira Technologies, LLC, Microsoft Windows and the Windows logo are the trademarks of Microsoft Corp. NetWare is the registered trademark of Novell Inc. WMM and WPA are the registered trademarks of Wi-Fi Alliance. All other brand and product names are trademarks or registered trademarks of their respective owners.

Notice: Copyrights © 2018 by Antaira Technologies, LLC. All rights reserved. Reproduction, adaptation, or translation without prior permission of Antaira Technologies, LLC is prohibited, except as allowed under the copyright laws.

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 Unmanaged Ethernet Switches

User Manual
Version 1.2 (March 2018)

This manual supports the following models:

- LMP-0600, LMP-0600-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 1
1.1 Product Overview 1
1.2 Product Software Features 1
1.3 Product Hardware Features 2
1.4 Package Contents 2
1.5 Safety Precaution 3
2. Hardware Description 4
2.1 Physical Dimensions 4
2.2 Front Panel 5
2.3 Top View 5
2.4 LED Indicators 6
2.5 Ethernet Ports 6
2.6 Cabling 7
2.7 Wiring the Power Inputs 8
2.8 Wiring the Fault Alarm Contact 8
3. Mounting Installation 9
3.1 DIN-Rail Mounting 9
3.2 Wall Mounting 10
4. Hardware Installation 11
4.1 Installation Steps 11
5. Web Management 12
5.1 Web Console Configuration 12
5.1.1 About Web-Based Management 12

5.2 Basic Setting 13
5.2.1 System Information 13
5.2.2 Admin &Password 14
5.2.3 IP Setting 15
5.2.4 System Time 16
5.3Port Management 17
5.3.1 Port Status 17
5.3.2 Port Configuration 17
5.4PoE (Power-over-Ethernet) 18
5.4.1 PoE Configuration 18
5.4.2 Ping Alarm 19
5.4.3 PoE Schedule 20
5.5 ERPS 21
5.5.1 ERPS Status 22
5.5.2 ERPS Configuration 22
5.5.3 Before Configuring ERPS 24
5.6 Spanning Tree 31
5.6.1 RSTP Status 32
5.6.2 RSTP Configuration 32

5.6.3 MSTI Status 34
5.6.4 MSTI Configuration 35
5.7. 802.1Q VLAN 37
5.7.1 802.1Q VLAN settings 37
5.7.2 802.1Q VLAN Settings 38
5.8. IGMP Snooping 38
5.8.1 IGMP Settings 39
5.8.2 IGMP Snooping Status Table 40
5.9 QoS (Traffic Prioritization) 40
5.9.1 QoS Classification 41
5.9.2 CoS Mapping 42
5.9.3 ToS Mapping 43
5.10 Port Mirroring 44
5.11 SNMP… 45
5.11.1 SNMP Agent 45
5.11.2 SNMP Trap setting 46
5.12 System Warning 47
5.12.1 Syslog Setting 47
5.12.2 System Event Log 48

5.12.3 SMTP Setting 49
5.12.4 Event Selection 50
5.12.5 Fault Alarm 50
5.13 MAC Table 51
5.13.1 MAC Address Table 51
5.13.2 MAC Table Configuration 51
5.14 Maintenance 52
5.14.1 Upgrade 52
5.14.2 Reboot 53
5.14.3 Default 53
5.15 Configuration 53
5.15.1 Save…. 54
5.15.2 Backup & Store 54
5.15.3 Auto Load & Backup 55
5.16 Logout.. 55
6. Command Line Interface Management 56
6.1 About CLI Management 56
7. Technical Specification 74

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 LMP-0600 series is a 6-Port Industrial PoE+ Managed Ethernet Switch with IEEE 802.3at complaint (Power-over-Ethernet Plus), which embedded with four 10/100Tx Ethernet ports that support either IEEE802.3af or IEEE802.3at for maximum 30 watts per port, and two 10/100Tx Fast Ethernet ports. It is a fully manageable Industrial Ethernet Switch and supporting standard Layer 2 Ethernet configurable settings. This product series is IP30 rated and DIN-rail mountable designed and provides standard operating temperature range models in -10°C to 70°C, and extended operating temperature range models in -40°C to 75°C. It also designed with high EFT and ESD protection to prevent any unregulated voltage for any industrial networking application in Process Control automation, Intelligent Transportation Systems (ITS), Power/Utility, Water Wastewater Treatment plants, any outdoor or harsh environment.

1.2 Product Software Features

- Network Redundancy
  - STP, RSTP, MSTP, ITU-T G.8032 Ethernet Ring Protection Switch (ERPS) for network redundancy
- Network Management
  - Web UI based management, SNMP v1/v2, Serial Console
  - Qos, traffic classification QoS, Cos, bandwidth control for Ingress and Egress, broadcast storm control, Diffserv
  - IEEE802.1q VLAN, port-based VLAN support
  - IGMP snooping v1/v2, IGMP filtering / throttling, IGMP query up to 256 group
  - Supports RMON, MIB II, port mirroring, event syslog, DNS, NTP/SNTP, SSH/SSL, TFTP.
- Advanced PoE Ports Management (auto ping check)
  - Auto powered device (PD) detection
  - Auto reset (cycle power to unresponsive PD)
  - PoE ports weekly power scheduling

- 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
- Configuration Backup – USB Port

1.3 Product Hardware Features

- System Interface and Performance
  - All RJ-45 ports support Auto MDI/MDI-X Function
  - Embedded 4*10/100Tx (PSE 30W/Port) RJ45 Ports, and 2*10/100Tx Fast Ethernet
  - Store-and-forward switching architecture
  - 8K MAC address table
  - Power line EFT protection: 2,000VDC; Ethernet ESD protection: 6,000VDC
- Power Input
  - DC 48~55V 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
  - Installation in pollution degree to environment
  - DIN-Rail and wall mount design

1.4 Package Contents

- 1– LMP-0600 series: 6-port industrial PoE+ managed Ethernet switch, with 4*10/100Tx (30W/Port) RJ45 ports, and 2*10/100Tx Fast Ethernet.
- 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 LMP-0600 series: 6-port industrial PoE+ managed Ethernet switch with 4*10/100Tx (30W/Port), and 2*10/100Tx Fast Ethernet ports.

(W x D x H) is **46mm x 99mm x 142mm**

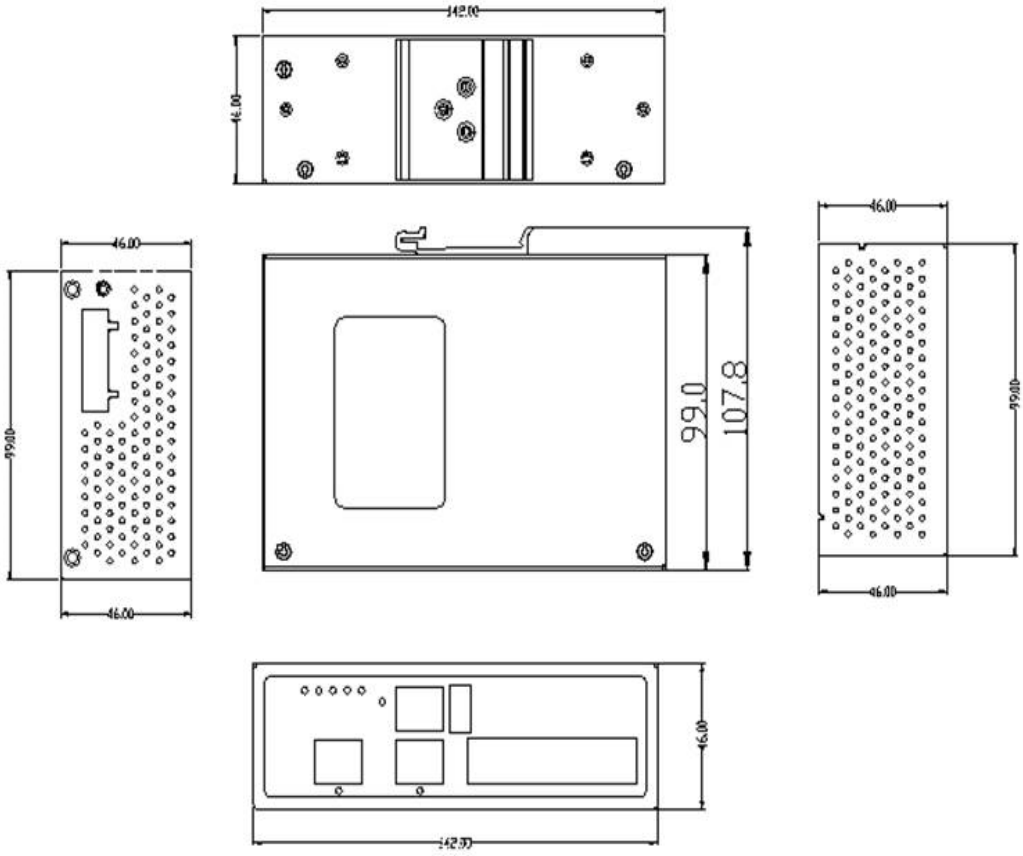


Figure2.1

LMP-0600 Series Physical Dimensions

2.2 Front Panel

The front panel of the LMP-0600 series industrial PoE+ managed Ethernet switches is shown below in *Figure 2.2*.

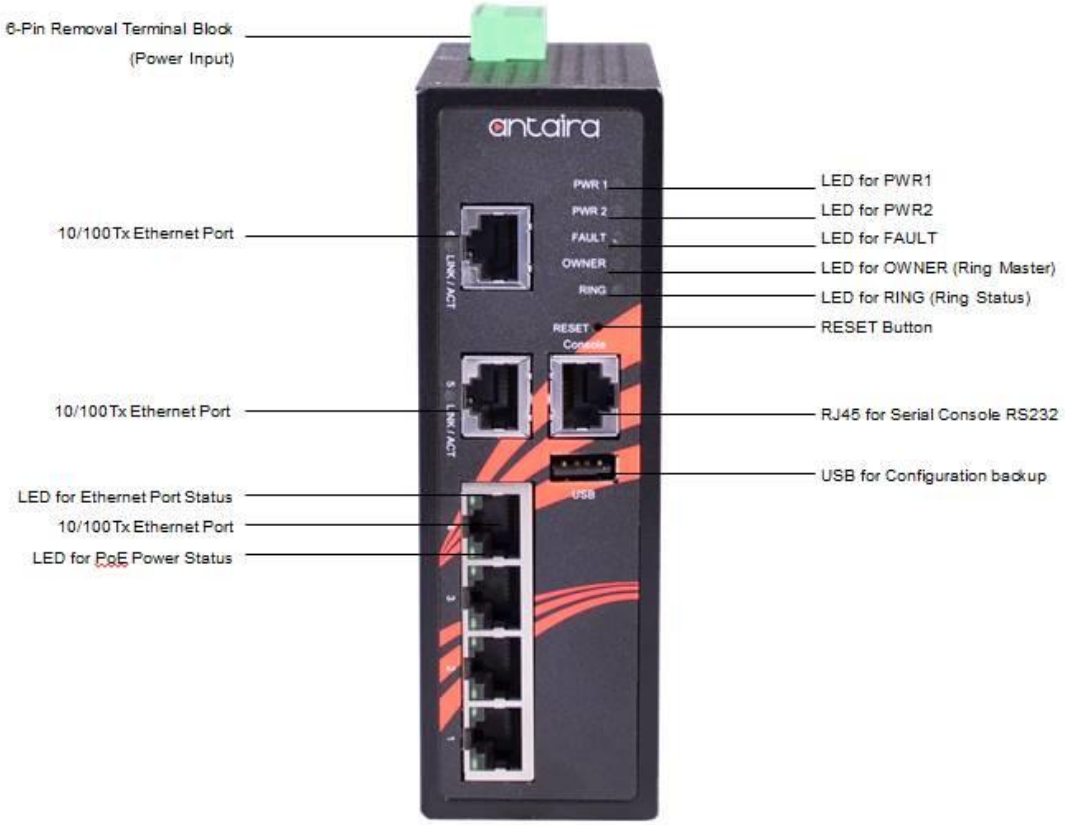


Figure2.2
The Front Panel of LMP-0600 Series

2.3 Top View

Figure 2.3, below, shows the top panel of the LMP-0600 series switch that is equipped with one 6-pin removal terminal block connector for dual DC power inputs (48~55VDC).

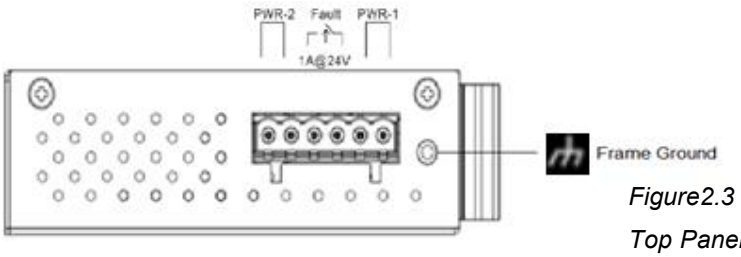


Figure2.3
Top Panel View of LMP-0600 Series

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	Powerinput1is active
		Off	Powerinput1isinactive
P2	Green	On	Powerinput2is active
		Off	Powerinput2isinactive
Fault	Green	On	System is ready
		Off	System is booting
	Red	On	Fault Alarm
		Off	System is in normal state
LAN Port 1~ 6 (Left LED)	Green 	On	Connected to network, 10/100Mbps
		Flashing	Networking is active
		Off	Not connected to network
LAN Port 1~ 4 (Right LED) PoE Indicators	Green 	On	The port is supplying power to the powered-device
		Off	No powered-device attached or power supplying fails

Table 2.1- LED Indicators for LMP-0600 Series

2.5 Ethernet Ports

- **RJ-45 Ports**

RJ-45 Ports (Auto MDI/MDIX): The RJ-45 ports are auto-sensing for 10Base-T, 100Base-TX 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 as below for straight-through and crossover cabling schematics.

- **RJ-45 Pin Assignments** (Table 2.2)

Pin Number	Assignment
1	Rx+
2	Rx-
3	Tx+
6	Tx-

Table 2.2 - RJ45 Pin Assignments

Note *"+" 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 operation. Users can use straight-through cables (see figure below) for all network connections to PCs, servers, other switches or hubs. With straight-through cable pins 1, 2, 3, and 6, at one end of the cable 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 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 2.3 - Ethernet Signal Pin Outs

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

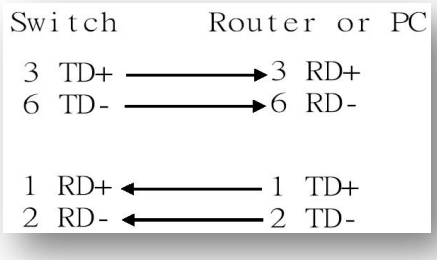


Figure 2.4
Straight-Through Cable Schematic

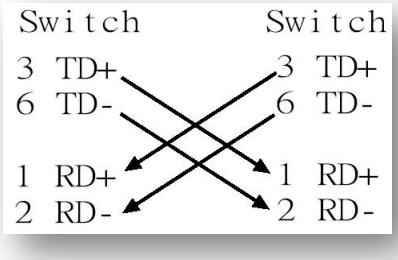


Figure 2.5
Crossover Cable Schematic

2.6 Cabling

- Twisted-pair segments can be connected with an unshielded twisted pair (UTP) or shielded twisted pair (STP) cable. The cable must comply with the IEEE 802.3u 100Base TX standard (e.g. Category 5, 5e, or 6). The cable between the equipment and the link partner (switch, hub, workstation, etc.) must be less than 100 meters (328 ft.) long.
- Fiber segment using **single-mode** connector type must use 9/125μm single-mode fiber cable.
- Fiber segment using **multi-mode** connector type must use 50 or 62.5/125 μm multi-mode fiber cable.

2.7 Wiring the Power Inputs

Please follow below steps to insert 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 2.7*.

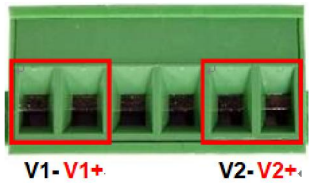


Figure 2.7
Power Terminal Block

2. Tighten the wire-clamp screws to prevent the wires from loosening, as shown below in *Figure 2.8*.



Figure 2.8
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**.*

2.8 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 2.16*. By inserting the wires, it will detect the fault status including power failure or port link failure (managed industrial switch only) and forma normally open circuit. An application example for the fault alarm contact is shown below in *Figure 2.9*.

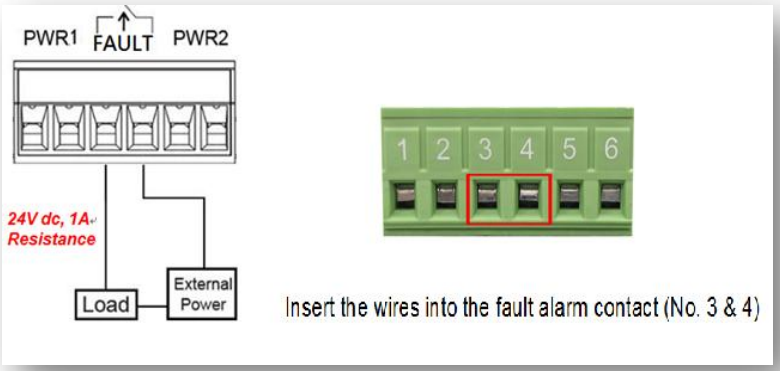


Figure 2.9
Wiring the Fault Alarm Contact

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 see Figure 3.1 to learn how to install the DIN-Rail on the switch.

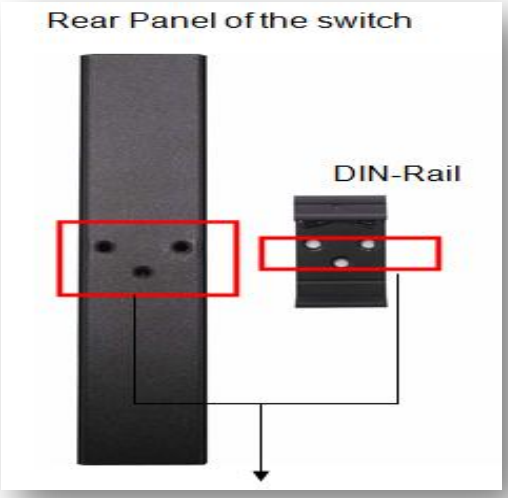


Figure 3.1
The Rear Side of the Switch and DIN-Rail Bracket

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.

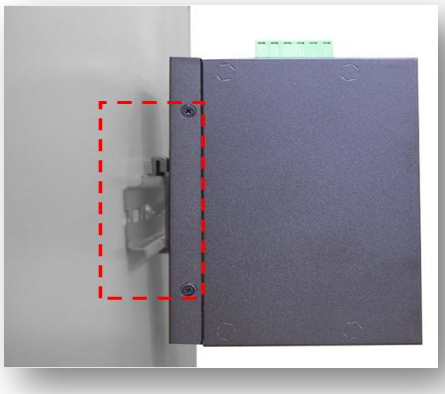


Figure 3.2
Insert the Switch on the DIN-Rail



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.

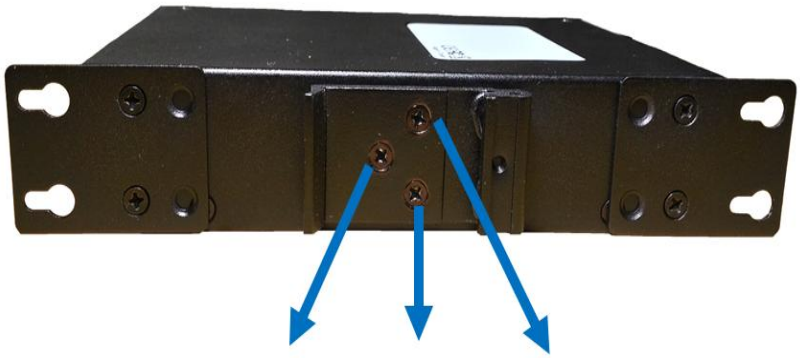


Figure 3.4
Remove DIN-Rail Bracket from the Switch

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

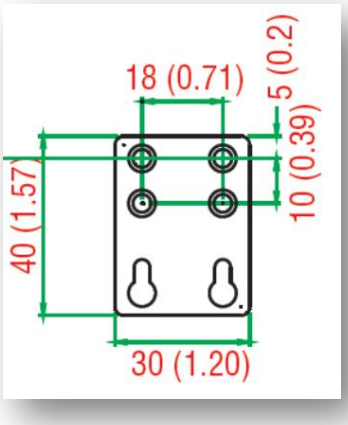


Figure 3.5
Wall Mounting Bracket Dimensions

4. Hardware Installation

4.1 Installation Steps

This section will explain how to install Antaira's LMP-0600 series: 6-port industrial PoE+ managed Ethernet switch with 4*10/100Tx (30W/Port) RJ45 ports and 2*10/100Tx Fast Ethernet ports.

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: **192.168.1.254**
- Default User Name: **admin**
- Default Password: **admin**

System Login

1. Launch any Internet browser
2. Type in factory default IP address: http://192.168.1.254 of the switch. Press "**Enter**".

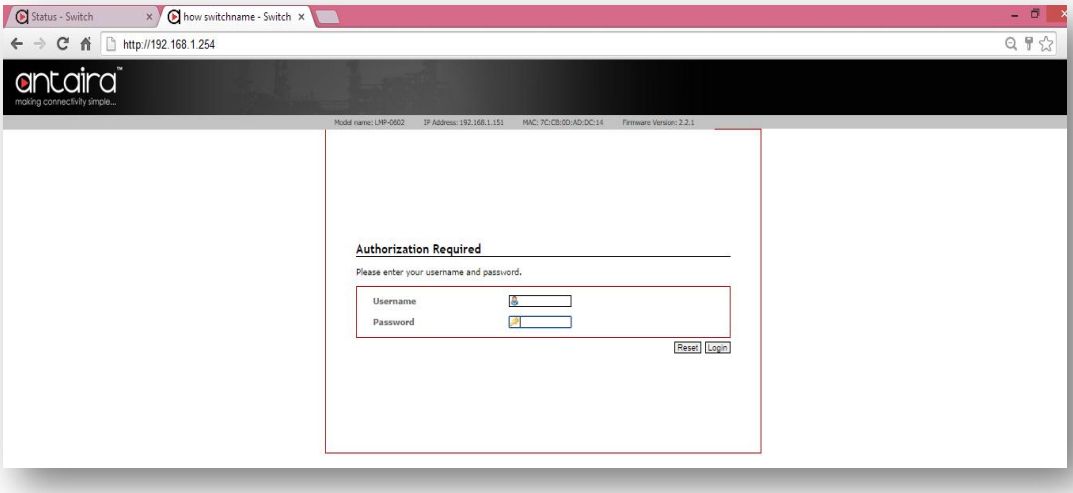


Figure 5.1 - Web Console "Login"

3. The login screen appears.
4. Key in the default username: **admin** and password **admin**.
5. Click “Login” button, then the main (status) page of the Web Console will appear as below *Figure 5.2*. The online image of the switch will display the real-time ports connection status.

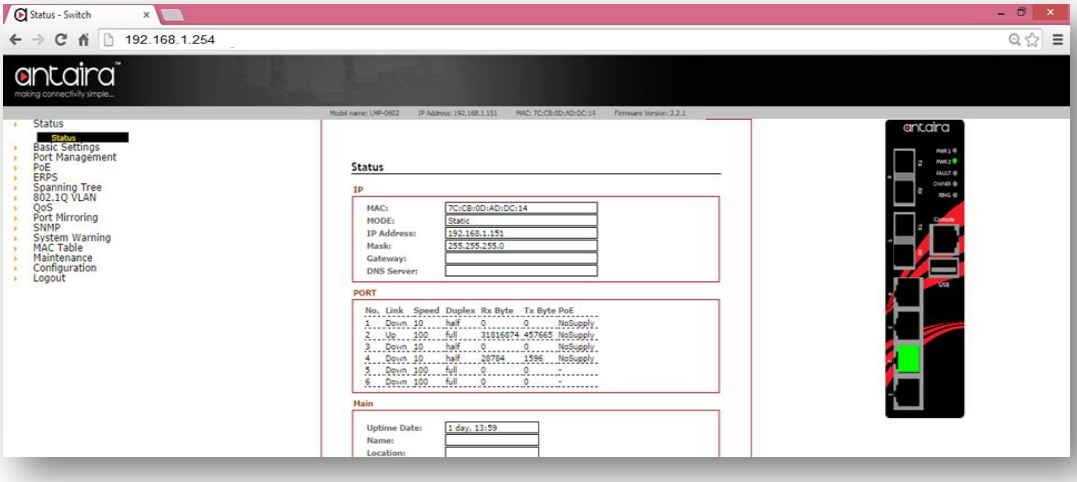


Figure 5.2 - Web Console Main (Status) Page

5.2 Basic Setting

5.2.1 System Information

Below, *Figure 5.3*, shows the switch system setting information.

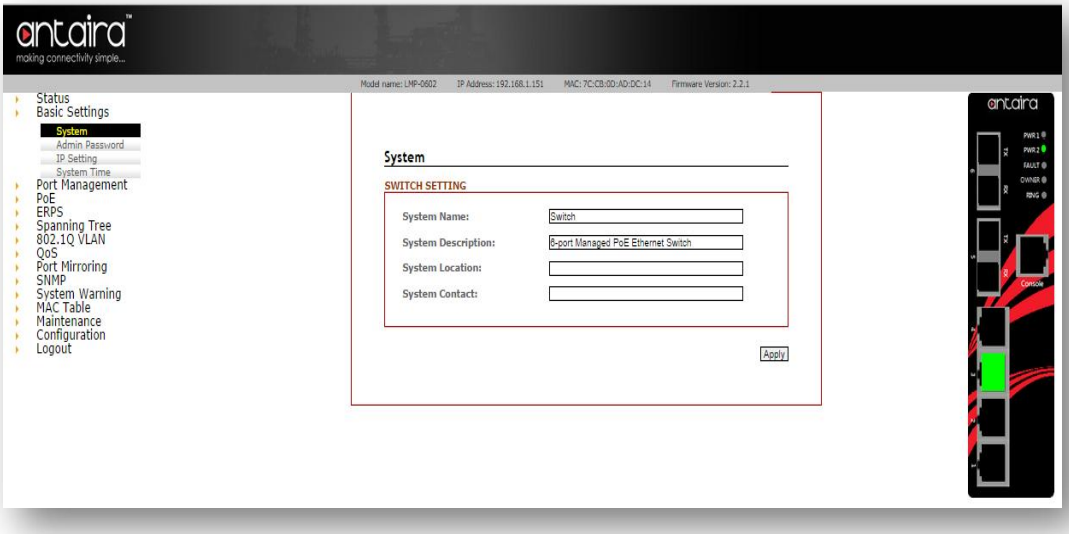


Figure 5.3 – Switch Settings (Status) Page

Terms	Value Description
System Name	Factory Default: Switch *Users can assign any name label to identify this managed node. By convention, 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	Factory Default: 6-port Managed PoE Ethernet Switch * Users can assign any new name label to describe this PoE Managed Switch.
System Location	Factory Default: blank *Users can use this field to insert The physical location of this switch (e.g., telephone closet, 3rd floor). The maximum allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
System Contact	Factory Default: blank *Users can insert this field with the administrator of this switch together with information on how to contact this person. The maximum allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
Apply	Click “Apply” button to save changes.

Figure 5.4 – Switch Settings Description

5.2.2 Admin &Password

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

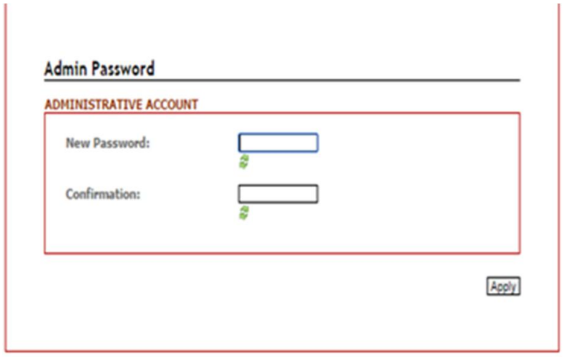


Figure 5.5 – Administrative Account

Terms	Value Description
New Password	Users can assign a New Password, and the maximum allow string length is 0 to 31 characters.
Confirmation	Re-type the new password.
Apply	Click “Apply” to save changes.

Figure 5.6 – Admin & Password Description

5.2.3 IP Setting

Configure the managed switch’s IP setting information.

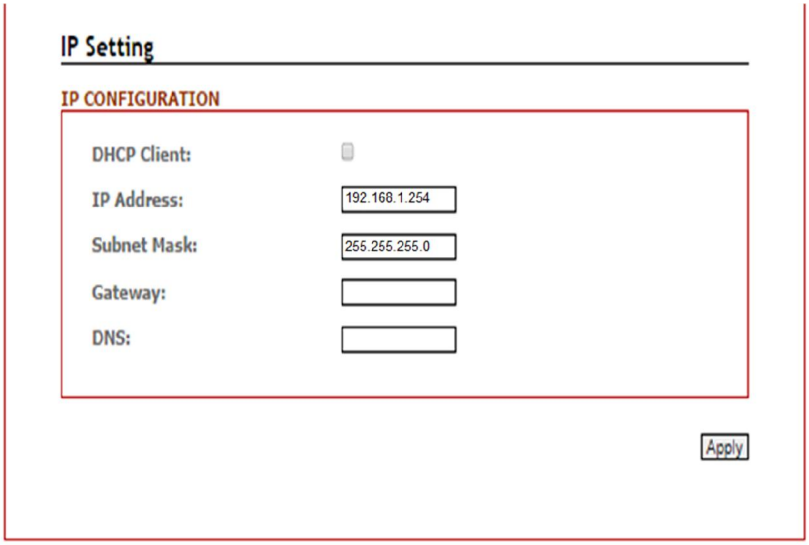


Figure 5.7 – IP Setting information

Terms	Value 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	The unit default IP is 192.168.1.254. Assign the IP address that the network is using. If DHCP client function is enabling, user does not require assigning the IP address. The network DHCP server will assign the IP address for the switch and it will be display in this column.

Subnet Mask	Assign the subnet mask of the IP address. If DHCP client function is enabling, user does not require to assign the subnet mask
Gateway	Assign the network gateway for the switch. If DHCP client function is enabling, user does not require to assign the Gateway.
DNS	Assign the DNS IP address
Apply	Click “Apply” button to save changes.

Figure 5.8 – IP Setting Information Description

5.2.4 System Time

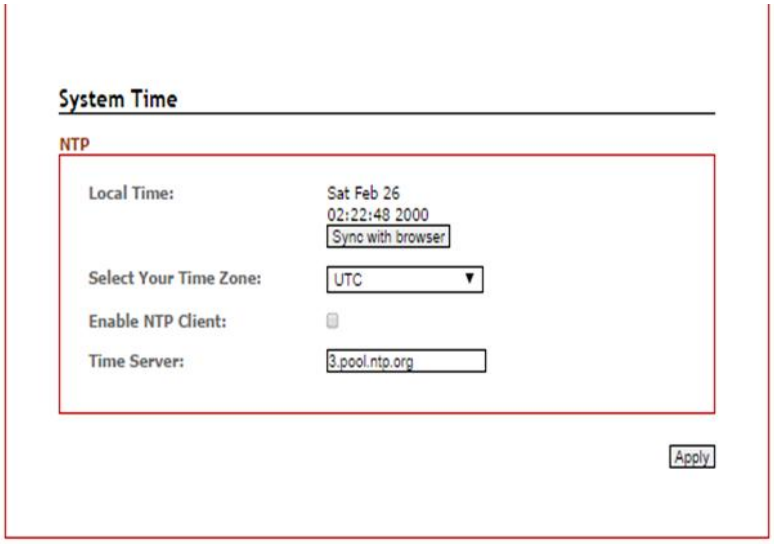


Figure 5.9 – System Time Settings

Terms	Value Description
Local Time	Users can define the switch’s local time, or click “Sync with browser” button to have local time setup automatically.
Select Your Time Zone	Users can use dropdown box to setup the switch location time zone
Enable NTP Client	Enable or disable NTP function to get the time from the SNTP server.
Time Server	User can define the Time Server info
Apply	Click “Apply” button to save changes.

Figure 5.10 – System Time Settings Description

5.3Port Management

5.3.1 Port Status

The following information provides the current port status.

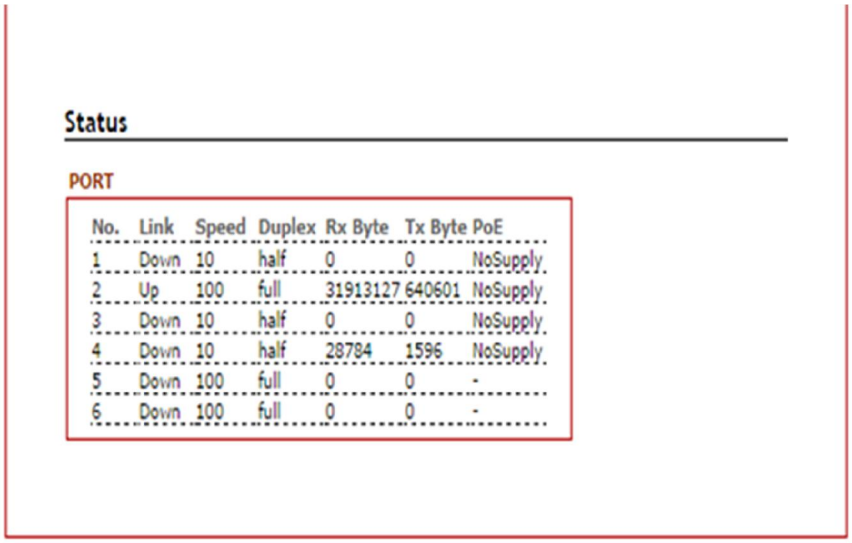


Figure 5.11 – Port Status Interface

5.3.2 Port Configuration

Users can assign or insert a “value/label” for each port under each “Port Name” box; enable or disable each port function; state the speed/duplex of each port; and enable or disable the flow control of the port.

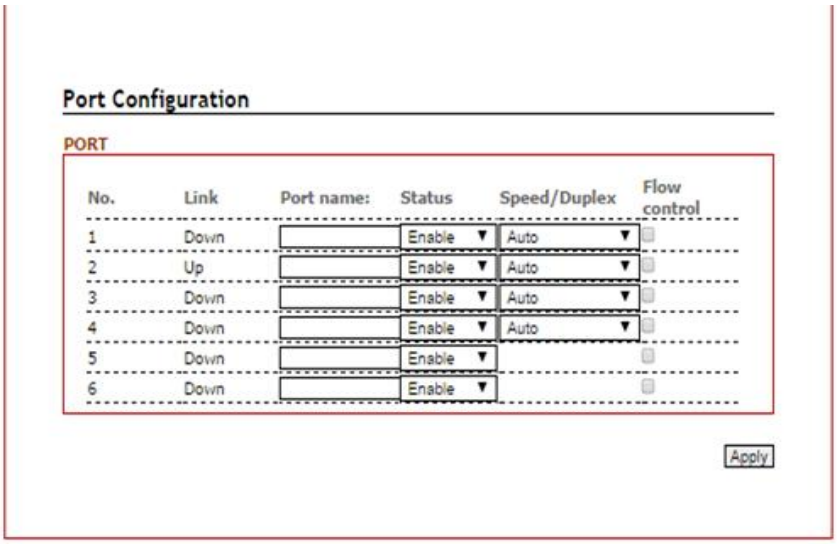


Figure 5.12 – Port Configuration Interface

Terms	Value Description
Port No.	It shows each port status: Up for link active, and Down for link inactive.
Port Name	User can create or insert a value or label for each port's identification
Status	Enable or disable a port
Speed/Duplex	User can set the bandwidth of each port as Auto-negotiation, 100 full,100 half,10 full,10 half mode.
Flow Control	Support symmetric and asymmetric mode to avoid packet loss when congestion occurred.
Apply	Click "Apply" button to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Figure 5.13 – Port Configuration Description

5.4PoE (Power-over-Ethernet)

LMP-0602 series is one of Antaira's industrial PoE+ managed switches that has four built-in IEEE802.3at complaint ports, and each PoE port would support PoE output power up to a maximum of 30W per port. It is also backward compatible with IEEE 802.af to support any standard PoE powered devices (PD).

5.4.1 PoE Configuration

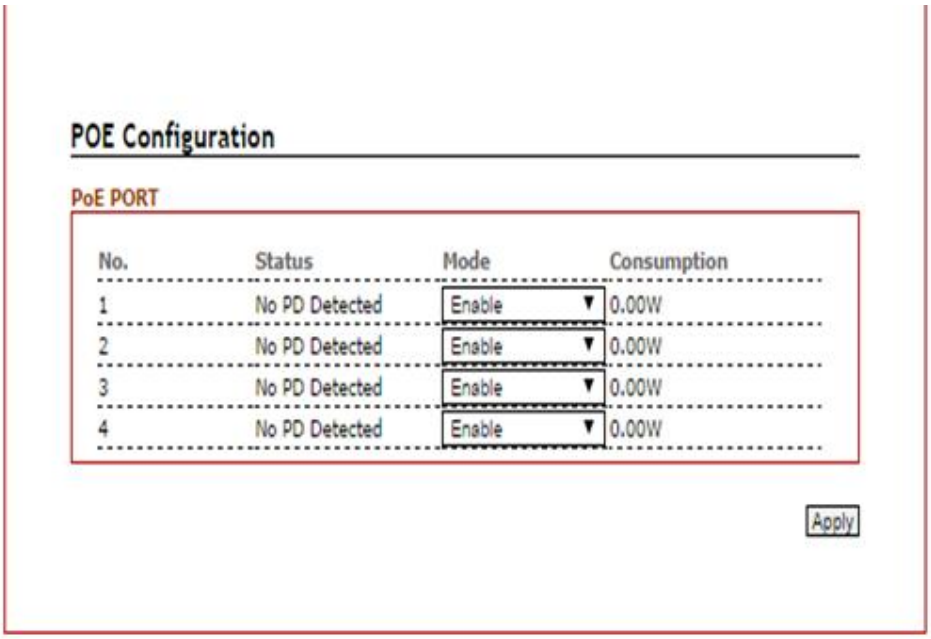


Figure 5.14 – PoE Port Configuration Interface

Terms	Value Description
Port No.	PoE Port Number
Status	Any PoE port will automatically detect any PD (Powered Device) is connected and display the situation.
Mode	Users can use the dropdown box to enable or disable any PoE port function
Consumption	Set the PoE power output limit value. The maximum value must less than 30.0W
Apply	Click “Apply” button to save changes.

Figure 5.15 – PoE Port Configuration Description

5.4.2 Ping Alarm

The PoE ping alarm function is using the ping command to turn on or off any PoE power output port. Users can insert any particular powered device’s IP address and set the interval time for a power recycle, timing the particular PoE port.

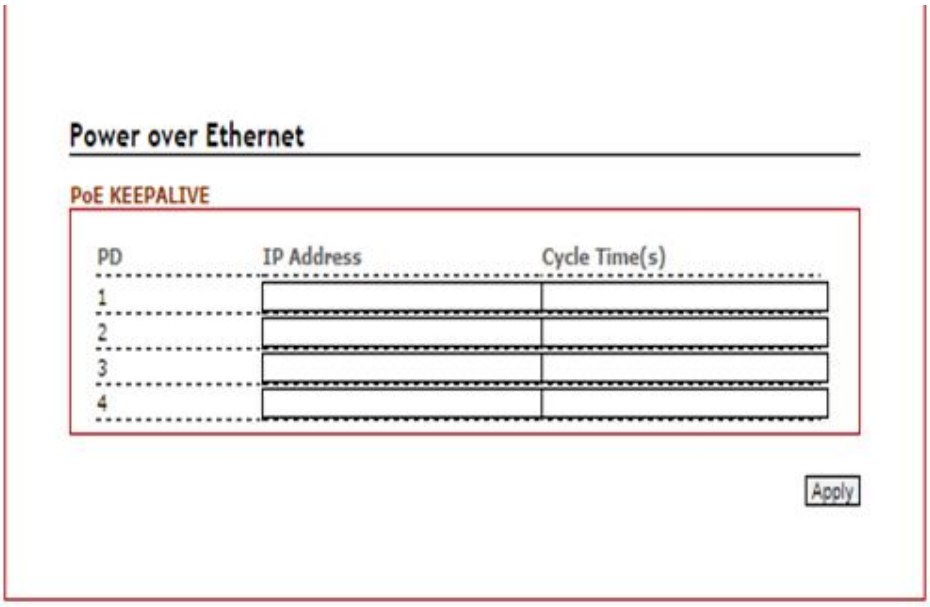


Figure 5.16 – PoE Ping Alarm Interface

5.4.3 PoE Schedule

For energy saving or power recycle powered devices, the PoE managed switch's PoE schedule interface allows users to appoint any date and time to enable or disable PoE functions for each PoE port.

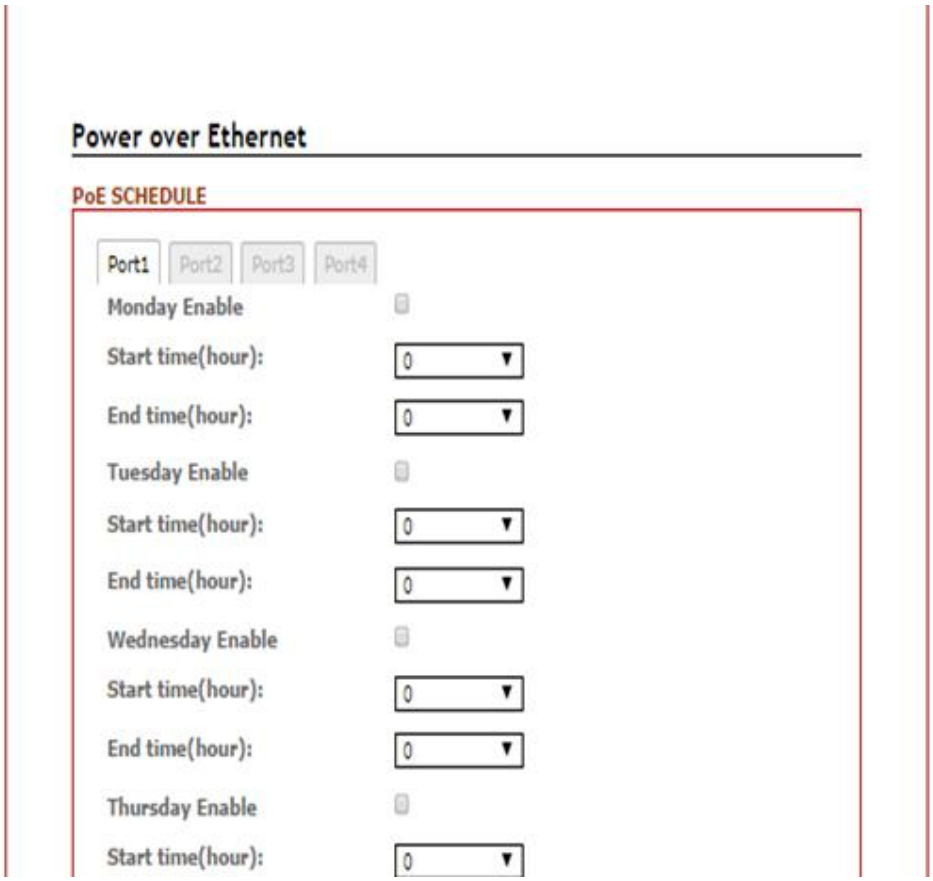


Figure 5.17 – PoE Schedule Interface

5.5 ERPS

In any industrial automation application, designing the redundant ring network paths can protect networks from unexpected failovers is extremely important in mission-critical networks that need to provide uninterrupted services. In practice, several loop protection methods are implemented to ensure that network functions normally without loops and recovers as soon as possible when a point of failure occurs. The most popular ones are RSTP (802.1w) and MSTP (802.1s). For industrial applications, the ERPS (G.8032) are highly recommended since they can achieve faster recovery time than any STP protocol.

Due to different manufacturers who provide their own proprietary redundant ring protocol, and users facing inconvenient situations with compatible issues when they are planning to design or upgrade their ring network for future proof, Antaira is proud to introduce and implement Ethernet Ring Protection Switching (ERPS) protocol as a standard ring solution for network redundancy with all new industrial managed Ethernet switches. In order to provide users with the flexibility and compatibility when there are any existing switches that contains the standard ERPS protocol.

Ethernet Ring Protection Switching (ERPS), defined in ITU-T G8032, implements a protection switching mechanism for Ethernet traffic in a ring topology. By performing the ERPS function, potential loops in a network can be avoided by blocking traffic to flow to the ring protection link (RPL) to protect the entire Ethernet ring.

In a network with ring topology that runs ERPS, only one switch is assigned as an “owner” that is responsible for blocking traffic in RPL so as to avoid loops. The switch adjacent to the RPL owner is called the RPL “neighbor” node that is responsible for blocking its end of the RPL under normal condition. Other participating switches adjacent to the RPL owner or neighbor in a ring are members or RPL next-neighbor nodes to this topology and normally forward receive traffic. ERPS, like STP, provides a loop-free network by using polling packets to detect faults. When a fault occurs, ERPS heals itself by sending traffic over a protected reverse path less than 50ms and recover quickly to forward traffic. Because of this fault detection mechanism, the network broadcast storm problem could be avoided as well.

5.5.1 ERPS Status

Below, *Figure 5.18,* shows the network redundancy ring status with the Ethernet Ring Protection Switch (ERPS) protocol.



Figure 5.18 – Redundant Ring Network – ERPS Status

5.5.2 ERPS Configuration

Figure 5.19, shows the ERPS configuration interface.

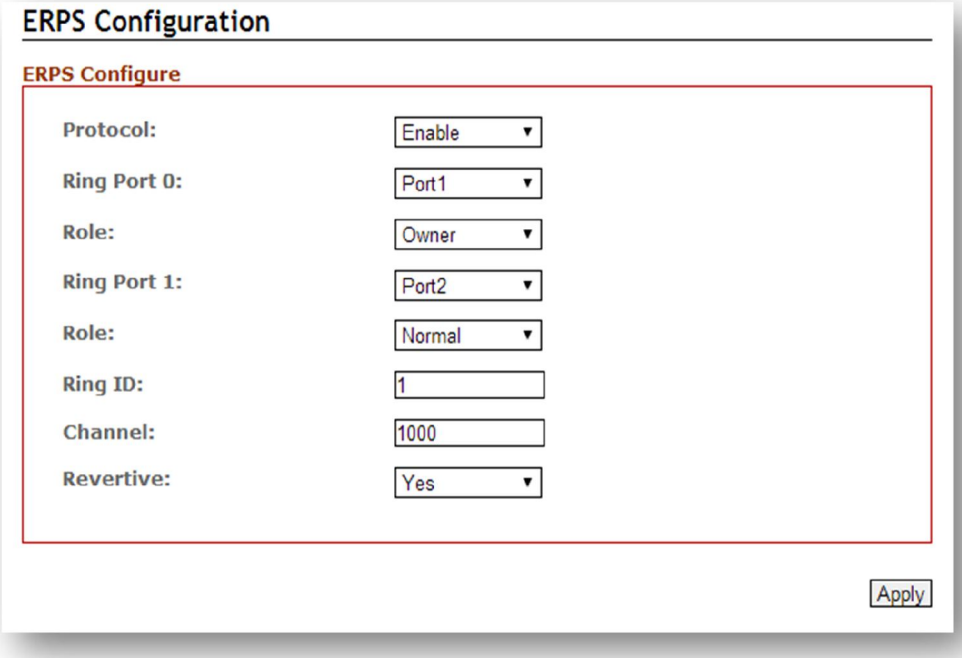


Figure 5.19 – ERPS Configuration Interface

Terms	Value Description
Protocol	"Enable" or "Disable" ERPS protocol
Ring Port 0	ERPS ring port 0, it could be map to real switch port 1 – port 6. Do not set the same as Ring port 1.
Ring Port 1	ERPS ring port 1, it could be map to real switch port 1 – port 6. Do not set the same as Ring port 0.
Role	Set the ERPS role as Owner, Neighbor or Normal. ***[Owner]*** *In charge of blocking one side of RPL link. It will prevent the packet flow from its blocked port.* ***[Neighbor]*** *In charge of blocking one side of RPL link. It will prevent the packet flow from its blocked port.* ***[Normal]*** *Besides Owner and Neighbor node, the rest of nodes are defined as Normal node.* *All node roles have the ability to block the port if the link attach to the port is failed and disconnected.*
Ring ID	ERPS ring ID, ranges from 1 to 239. Ring ID distinguishes different Ring topology.
Channel	ERPS Channel ID, ranges from 1 to 4094. It's a channel to send PDUs of ERPS.
Revertive	Set to Revertive (yes) or Non-revertive (no). The revertive mode works only under the scenario A at the RPL Owner node. ***[Revertive]*** *While the revertive mode is set, the RPL link will be blocked in 5 minutes after recovery form link failure situation. Otherwise, it will remain unchanged of the blocking state. That is, the failed link port will block permanently until the next event happen.* ***[Non-Revertive]*** *The failed ring link the port attached to it will remain blocked even the situation is eliminated.*
Apply	Click "Apply" button to save changes.

Figure 5.20 – ERPS Configuration Terms & Description

5.5.3 Before Configuring ERPS

Before configuring ERPS, the rapid spanning tree protocol (RSTP), or multiple spanning tree protocol is required to disabled, due to only one protocol is exclusive running within a switch. Below are the steps to disable RSTP, or MSTP.

Step 1: Login the switch with a web browser.

Step 2: Open the "RSTP Configuration" page under the "Spanning Tree" manual as below figure 5.21.

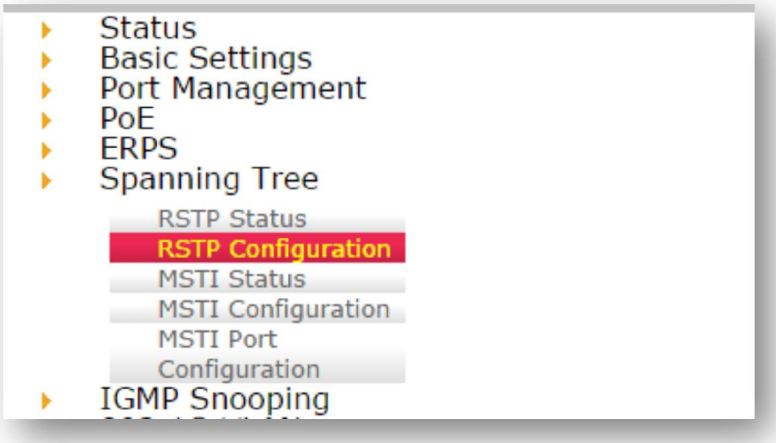


Figure 5.21 – Spanning Tree Manual

Step 3: When the RSTP/CIST Configuration page shows up, set "Mode" to "Disable" as the figure 5.22.

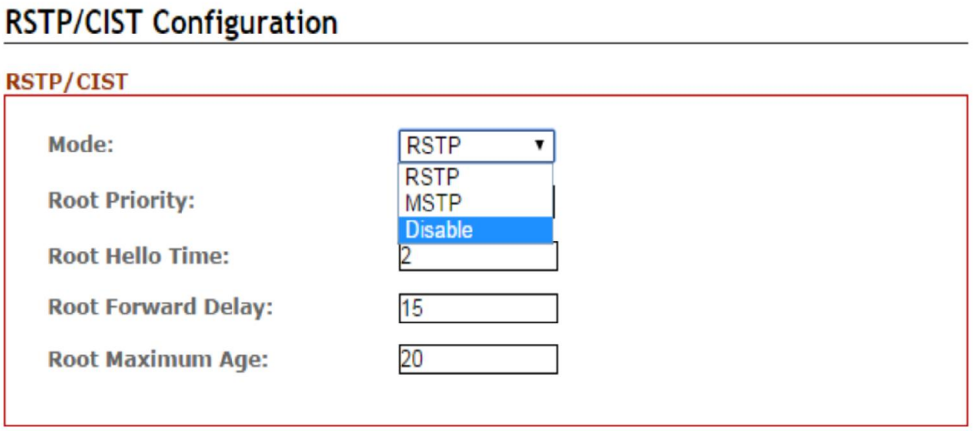


Figure 5.22 – RSTP/CIST Configuration interface

Step 4: Press the Apply button in the lower right corner as below figure 5.23.

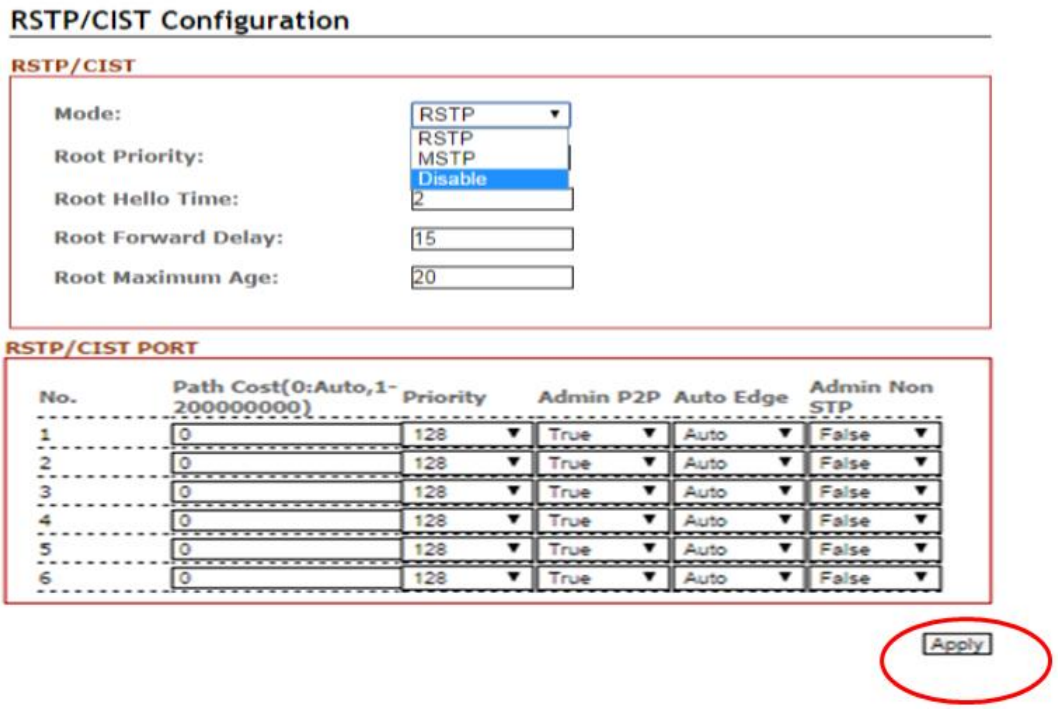


Figure 5.23 – RSTP/CIST Configuration interface

Ethernet Ring Protection Switch (ERPS) is an Ethernet ring protection protocol which is used to prevent forming the loop in LAN, thus, the Broadcast Storm problem could be avoided. The loop avoidance mechanism ensures the traffic flows on all but the RPL ring link. In order to achieve the loop-avoidance mechanism, ITU-T G.8032 defines three roles in ERPS, which are “RPL Owner Node”, “RPL Neighbor Node”, and “Normal Node”.

Below are two scenarios describing how to configure the ERPS in Antaira Industrial Managed Ethernet Switches. Users can reference it to configure the managed switch as RPL-configured architecture as figure 5.24 or Non-configure architecture as figure 5.25.

5.5.3.1 Scenario A – RPL configured Architecture

Under this scenario A, there are three major roles are required to be configured within the ERPS configuration.

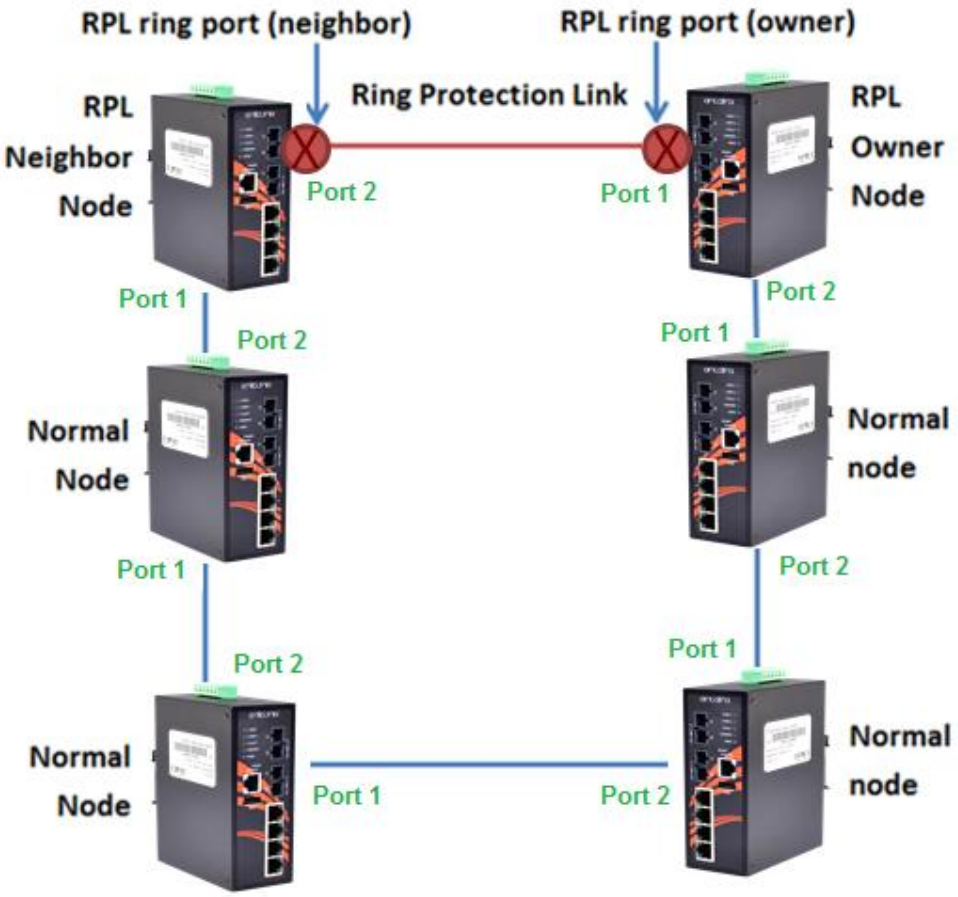


Figure 5.24 – RPL-configured Architecture

Caution:	***Before enabling any ERPS protocols on any of the Ring Nodes, please DO NOT connect all switches to form a loop (ring) network yet. There should have at least one ring port leave unplugged until all nodes in the topology are ready.***

[RPL Owner Node]

There is only one RPL Owner Node could be set in a ring network. In order to set up the RPL Owner Node, choose a switch and enable "Protocol" under the ERPS Configuration interface, and follow below steps and use below figure 5.25 as example:

Step 1: Choose a specific port from the dropdown box next to "ring port 0", and set it as "Owner" node by clicking the dropdown box next to "Role" below "ring port 0". At this point, "**Port 1**" was chosen as example.

Step 2: Choose a specific port from the dropdown box next to "ring port 1", then set it as "**Normal**" from the dropdown box next to "Role" (which locates below "ring port 1"). At this point, "**Port 2**" was chosen as example.

Note: The port number of "Ring Port 0" and "Ring Port 1" cannot be duplicated.

After the configurations, press the "Apply" button on the right bottom corner to save the setting.

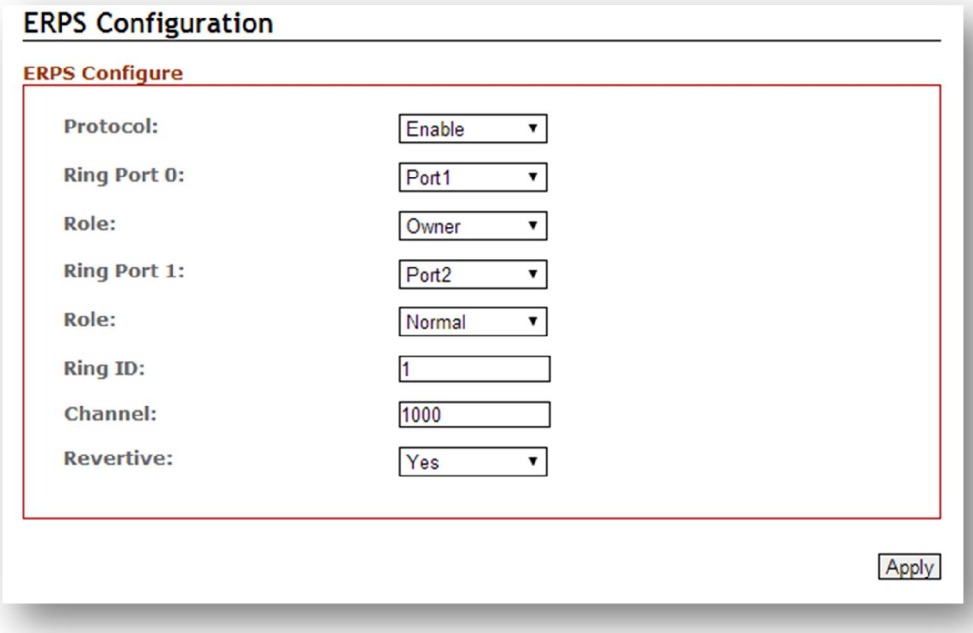


Figure 5.25 – RPL Owner Node Setup Example

Please be aware, when the revertive mode is set to "**Yes**", the ring will recover same as above figure 5.24 after the ring state form ABNORMAL to NORMAL in 5 minutes. Otherwise, the blocked port will remain blocked permanently unless users reconfigure it.

[RPL Neighbor Node]

Users should choose a second managed switch that is adjacent to the first managed switch and set it up as the RPL neighbor node. For configuration, users should login to the second managed switch's ERPS configuration interface and choose a specific port number under "Ring Port 0" and set it as the "Normal" node by clicking the dropdown box of "Role"; then, set another specific port number under "Ring Port 1" as the "Neighbor" node as shown below in *Figure 5.26*. So the link between neighbor port and owner port forms the ring protection link (RPL). After the configurations, press the "Apply" button on the bottom right corner to save the settings.

Note: The port number of "Ring Port 0" and "Ring Port 1" cannot be duplicated.

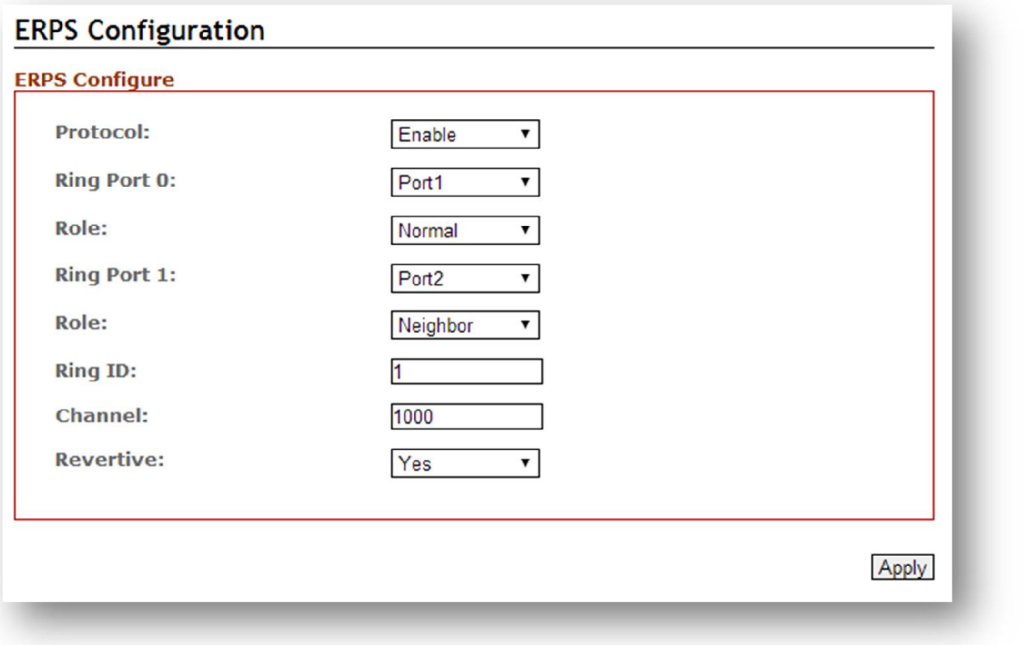


Figure 5.26 – RPL Neighbor Node Setup Example

[Normal Node]

Then user should setup the rest of the managed switches' "Role" of both "Ring Port 0 and 1" as "Normal Node" as shown above in *Figure 5.27*. Please be sure no duplicate port number has been chosen within a managed switch's ERPS ring setting, the incorrect configurations may lead to unexpected errors.

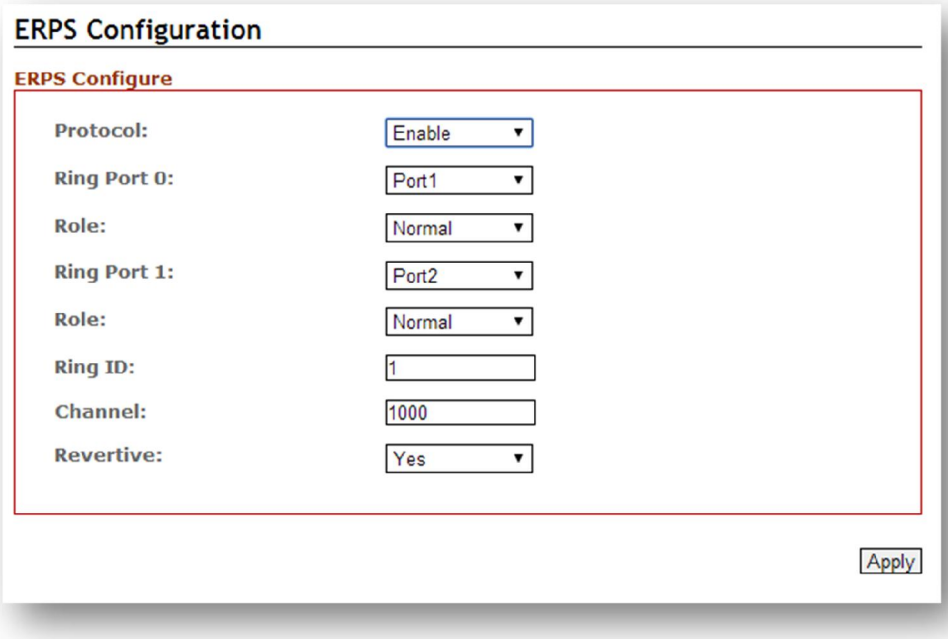


Figure 5.27 – RPL Normal Node Setup Example

5.5.3.2 Scenario B – Non-configured Architecture

In some situations, users can choose not to configure the RPL owner and neighbor node; the ERPS could still work well under the mechanism by blocking one of the ring ports in the ERPS ring topology.

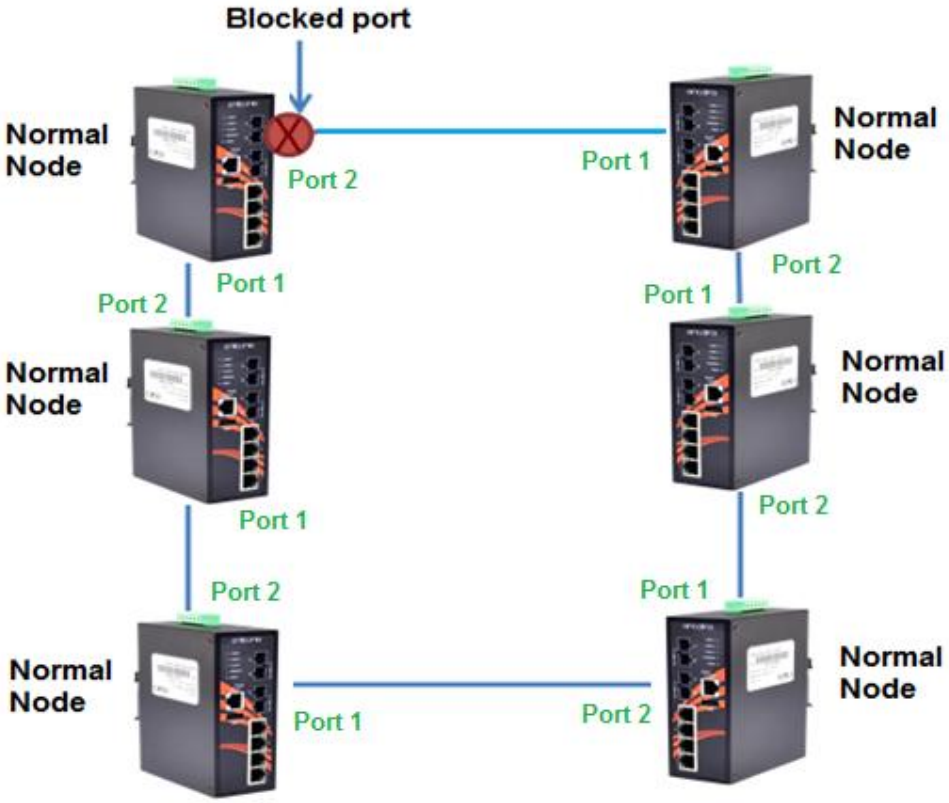


Figure 5.28 – Non-Configured Architecture

> ***Caution***: ***Before enabling any ERPS protocols on any of the Ring Nodes, please DO NOT connect all switches to form a loop (ring) network yet. There should have at least one ring port leave unplugged until all nodes in the topology are ready.***

As above *Figure 5.28*, the ERPS is blocked at one of the ring node ports. The blocked port is chosen by an election mechanism that is decided by the MAC address. Due to the MAC address is unique; the ERPS will just choose the biggest MAC as the blocking node.

However, the user is still required to enable the RRPS protocol, and assign a dedicated port number for each uplink port under “Ring Port 0 and 1” but there is no requirement to setting the role. *Figure 5.29*, below, shows the configurations as a reference.

After the configurations, press the “Apply” button on the bottom right corner to save the settings.

Note: The port number of “Ring Port 0” and “Ring Port 1” cannot be duplicated.

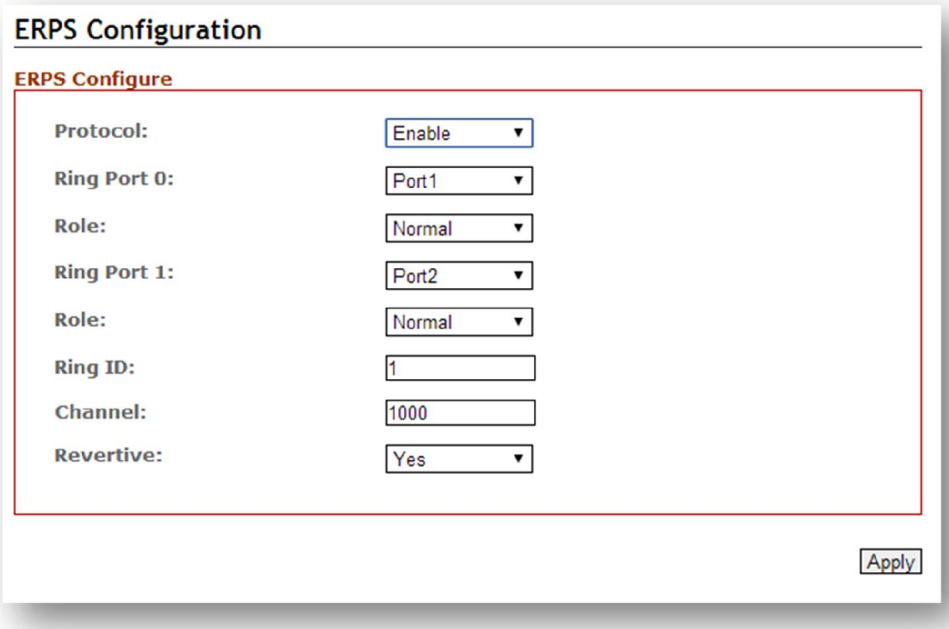


Figure 5.29 – Non-configured Architecture setup

5.6 Spanning Tree

The Spanning Tree Protocol (STP), defined in the IEEE Standard 802.1d, can be created within a mesh network of connected layer-2 switches.

The Rapid Spanning Tree Protocol (RSTP), defined in the IEEE 802.1w. RSTP is an enhanced solution of STP. It shares most of its basic operation characteristics, and essentially creates a cascading effect away from the root bridge where each designated bridge proposes to its neighbors to determine if it can make a rapid transition.

Another extension of RSTP is the Multiple Spanning Tree protocol (MSTP), defined in the IEEE802.1s. It allows different VLANs to travel along separate instances of spanning tree. Unlike STP and RSTP, MSTP eliminates the needs for having different STP for each VLAN. Therefore, in a large networking environment that employs many VLANs, MSTP can be more useful than legacy STP.

5.6.1 RSTP Status

Below *Figure 5.30* shows the RSTP algorithm results.

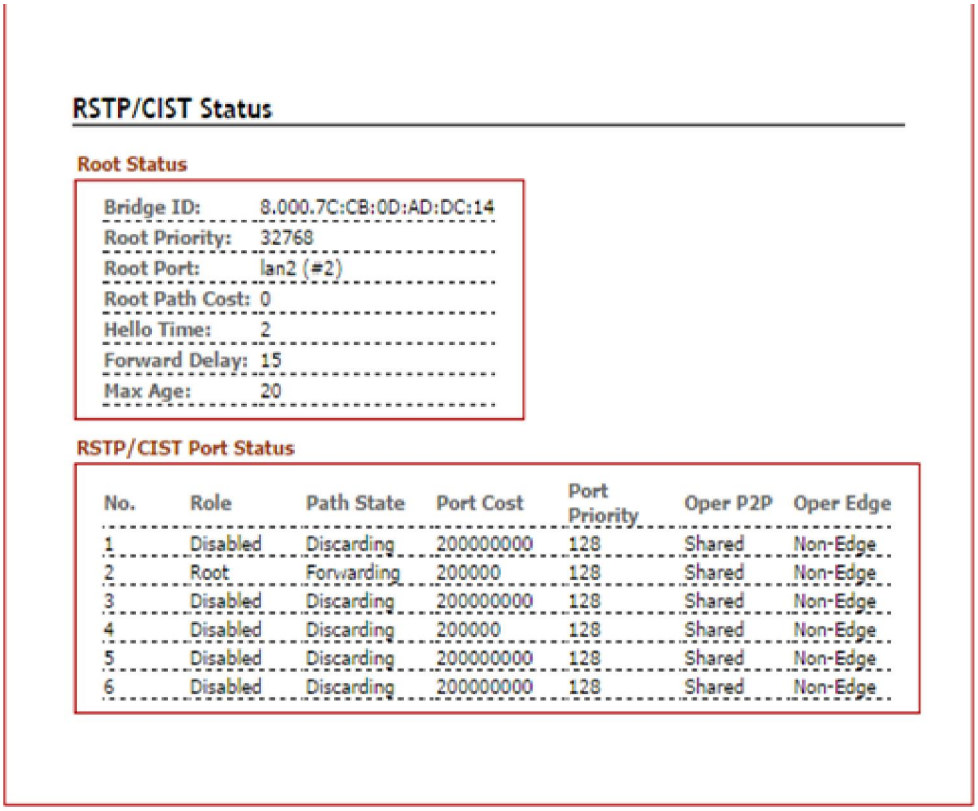


Figure 5307 – RSTP Information Interface

5.6.2 RSTP Configuration

Users can enable/disable the RSTP function, and set the parameters for each port.

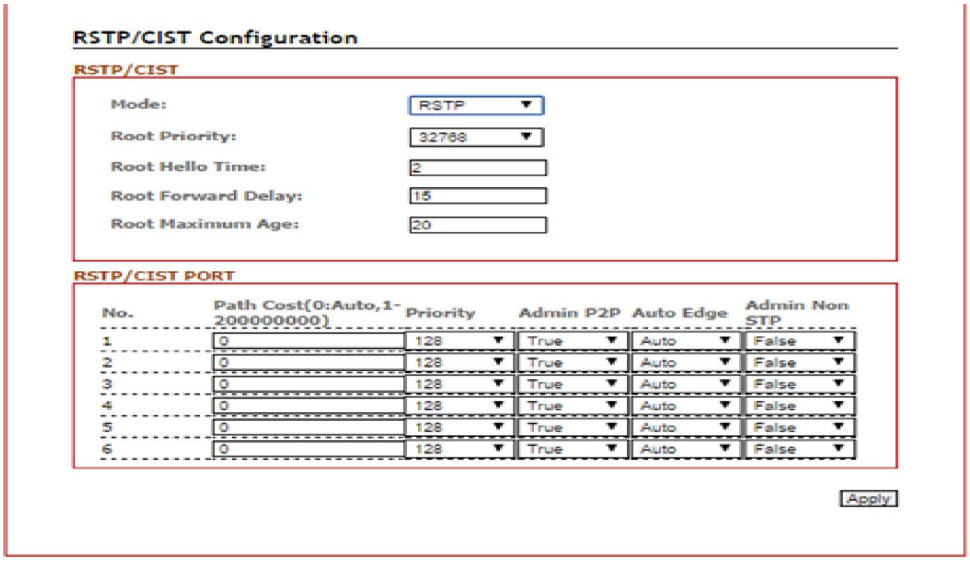


Figure 5.31 – RSTP Configuration Interface

Terms	Value Description
Mode	Users can select RSTP or MSTP function to be enabled or disabled before configuring the related parameters.
Root Priority (0~61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If any change of the value, the switch is required to be reboot. The value must be multiple of 4096 according to the protocol standard rule.
Root Hello Time (1~10)	Enter a value between 1 through 10 for the time to control the switch to send out the BPDU packet for RSTP current status checking.
Root Forward Delay (4~30)	Enter a value between 4 through 30 asthe number of seconds for a port to wait before changing from its RSTP learning and listening states to the forwarding state.
Root Maximum Age (6~40)	Enter a value between 6 through 40 as the number of seconds a bridge waits without receiving STP configuration messages before attempting a reconfiguration.
Path Cost (0~200000000)	Enter a value from 1 through 200000000 to define the path cost for the other switch from this transmitting switch at the specified port. When path cost insert in 0, the switches will be setup as automatic data transmitting.
Priority (0~240)	Enter a number 0 through 240 to decide which port should be blocked by priority in LAN. The value of priority must be the multiple of 16
Admin P2P	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other switch (i.e. It is served by a point-to-point LAN segment), or it can be connected to two or more switches (i.e. It is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True means P2P enabling. False means P2P disabling.
Auto Edge	The port is directly connected to end stations, and it cannot create bridging loop in the network.To configure the port as an edge port, set the port to "**True**".

Admin Non STP	The port includes the STP mathematic calculation. **True** is not including STP mathematic calculation. **False** is including the STP mathematic calculation.
Apply	Click “Apply” button to save changes.

Figure 5.32 – RSTP Configuration Terms & Value Description

MSTP (Multiple Spanning Tree Protocol)

It is defined in IEEE 802.1s, it can map a group of VLAN’s into a single Multiple Spanning Tree instance (MSTI). In fact, the Spanning Tree Protocol is applied separately for a set of VLAN’s instead of the whole network. Different root switches and different STP parameters can be individually configured for each MSTI. So, one link can be active for one MSTI and the other link active for the second MSTI. This enables some degree of load-balancing and generally two MSTI’s are used in the network for easier implementation.

5.6.3 MSTI Status

Users can display the MSTI root status and port status by selecting the instance ID number from 1 to 15 by clicking on the dropdown box from the “MSTI Status” interface.

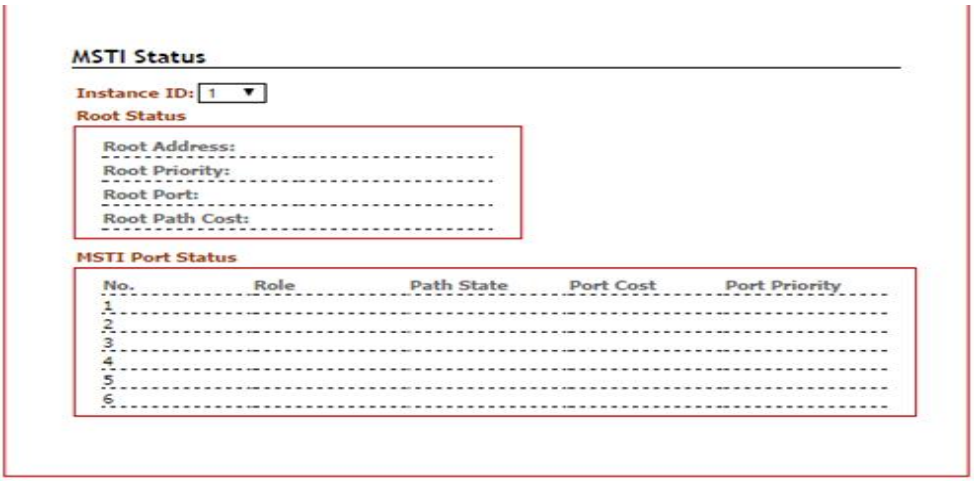


Figure 5.33 – MSTI Status Interface

5.6.4 MSTI Configuration

Users can display the MSTI root status and port status by selecting the “Instance ID” number from 1 to 15 by clicking on the dropdown box from the “MSTI Status” interface.

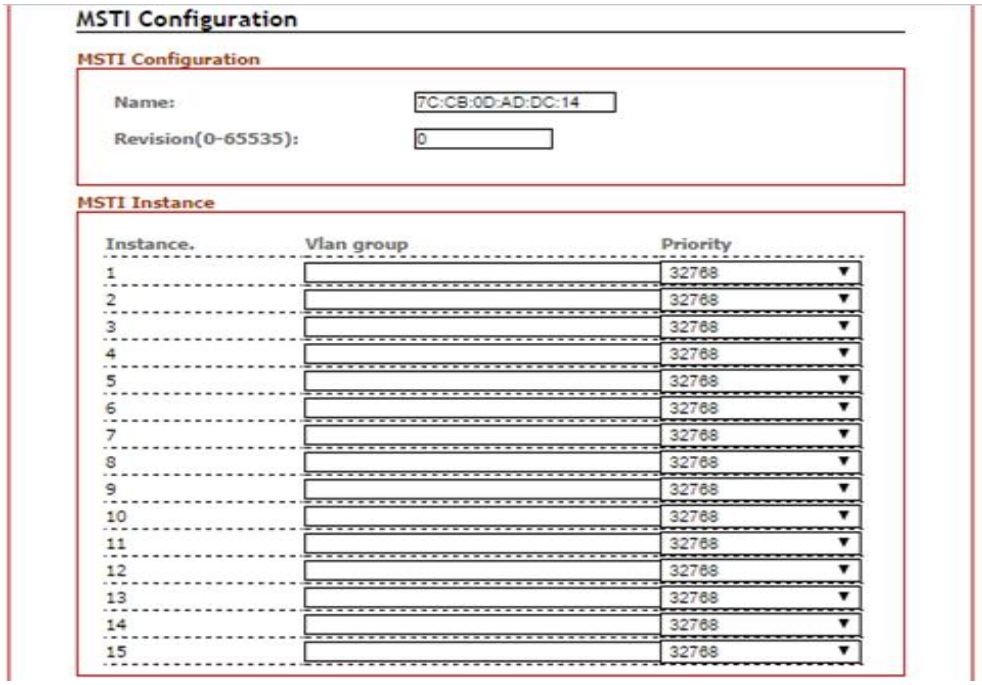


Figure 5.34 – MSTI Configuration Interface

Terms	Value Description
MTSI Configuration	
Name	Users can insert the unique MAC address of the bridge switch.
Revision	User can insert the value from 0~65535
MTSI Instance	
Instance No. & VLAN Group	There are 1~15 instance number, user can insert which VLAN Group info into the belonging Instance number
Priority (0~61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. The switch is required to reboot when there’s any value change. The value must be multiple of 4096 according to the protocol standard rule.

Apply	Click “Apply” button to save changes.

Figure 5.35 – MSTI Configuration –Terms & Value Description

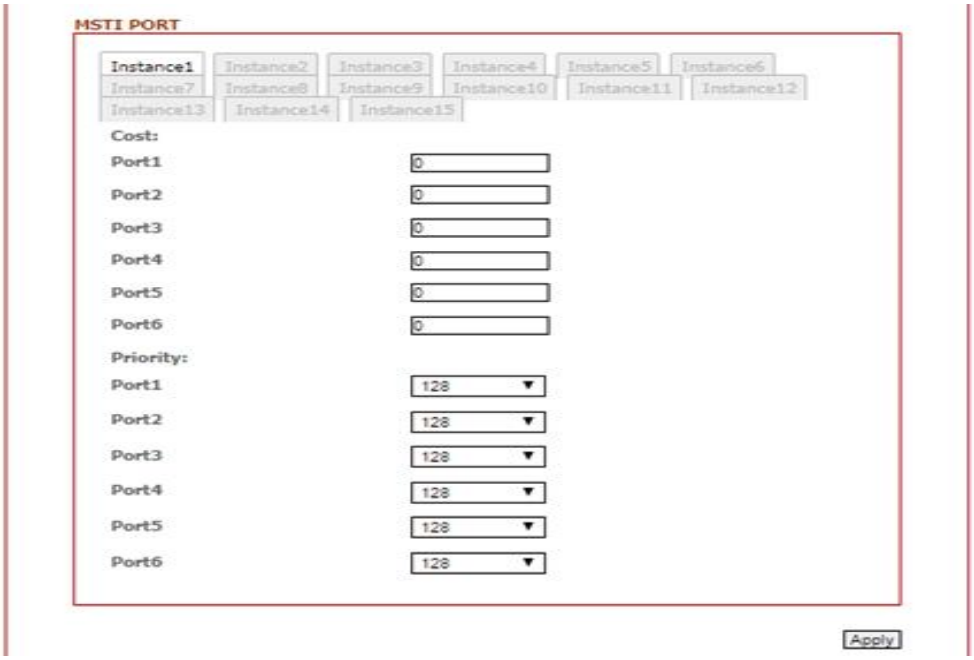


Figure 5.36 – MSTI Port Configuration Interface

Terms	Value Description
Instance Tabs	User can select Instance Tab #1~#15 to configure each MSTI port “Cost” & “Priority” value.
Cost	User can define the path cost value from 1 through 200000000 to the other bridge from this transmitting bridge at the specified port.
Priority	User can decide which port should be blocked by priority in LAN by select the value from 0 to 240 from the dropdown box.
Apply	Click “Apply” button to save changes.

Figure 5.37 – MSTI Port Configuration Terms & Value Description

5.7. 802.1Q VLAN

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which allows user to isolate network traffic. Only the members of the VLAN will receive traffic from the same members of VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

The switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration of VLAN operation mode is at "**802.1Q**".

5.7.1 802.1Q VLAN settings

Tagged-based VLAN is an IEEE 802.1Q specification standard, and it is possible to create a VLAN across devices from different switch venders. IEEE 802.1Q VLAN uses a technique to insert a "tag" into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

Ports in a port-based VLAN are referred to as untagged ports and the frames received on the ports as untagged frames. The names derive from the fact that the frames received on a port do not contain any information that indicates VLAN membership, and that VLAN membership is determined solely by a port's PVID.

All of Antaira's industrial managed switches' have a default VLAN setting set to "none" for each port, so the users can login to the VLAN setting interface to create a VLAN Group name and choose "Tag" or "Untag" for each port.



Figure 5.38 – 802.1Q VLAN Settings Interface

5.7.2 802.1Q VLAN Settings

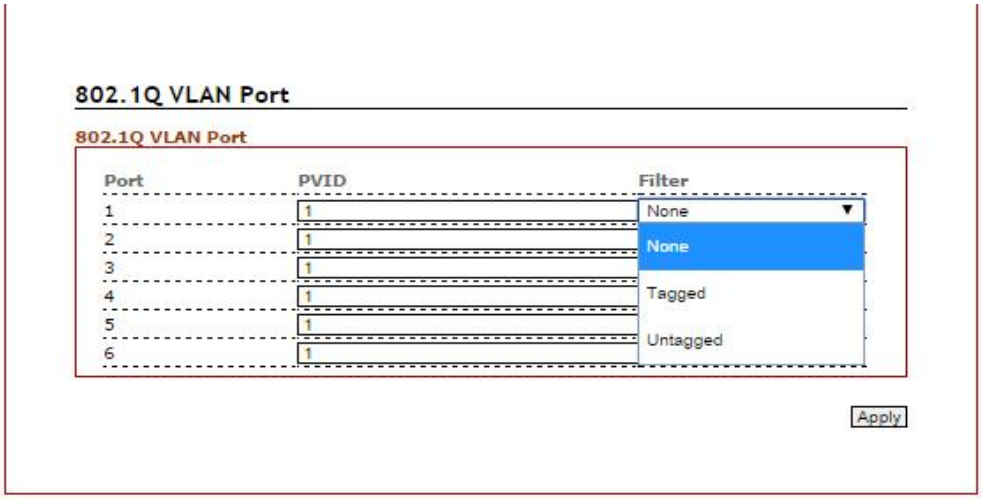


Figure 5.39 – 802.1Q VLAN Settings Interface

Terms	Value Description
PVID	User can assign a Port VLAN ID for each port
Filter	User can choose any port be “Tagged” or “Untagged”. Tagged VLAN: set the tagged PVIDs to carry different VLAN frames to other switch. Untagged VLAN: set the port PVID for untagged devices that connect to the port. The range of PVID is 1 to 4094.
Apply	Click “Apply” button to save changes.

Figure 5.40 – 802.1Q VLAN settings Terms & Value Description

5.8. 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.

5.8.1 IGMP Settings

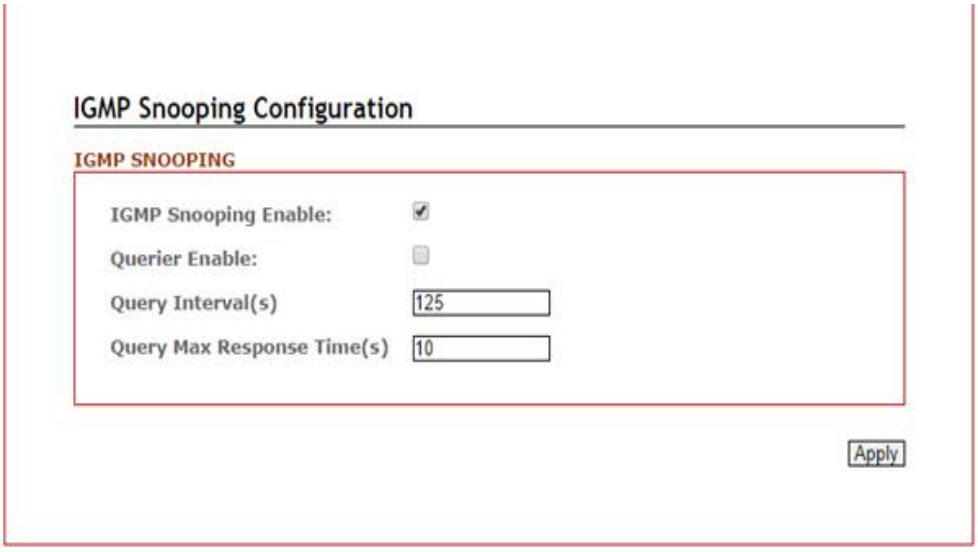


Figure 5.41 – IGMP Snooping Settings Interface

Terms	Value Description
IGMP Protocol	Check the box to enable or disable IGMP Snooping
Querier	Switch will be IGMP querier or not. There should have the existing one and only one IGMP querier in an IGMP application – up to 256 Groups
Query Interval	The frequency at which the querier sends query messages
Query Max Response Time	The maximum response time advertised.
Apply	Click “Apply” button to save changes.

Figure 5.42 – IGMP Snooping Settings Terms & Value Description

5.8.2 IGMP Snooping Status Table

Multicast filtering is the system by which end stations only receive multicast traffic if they register to join specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end stations.

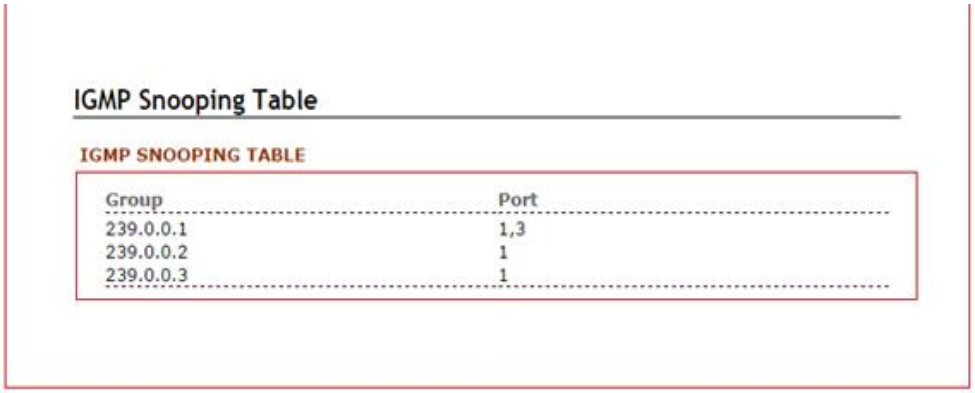


Figure 5.43 – IGMP Snooping Status Table

5.9 QoS (Traffic Prioritization)

Network traffic is always unpredictable and the only basic assurance that can be offered is the best effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria and receives preferential treatments.

Traffic Prioritization includes three modes: port base, 802.1p/COS, and TOS/DSCP. By traffic prioritization function, users can classify the traffic into four classes for differential network application. All of Antaira's industrial managed switches support four priority queues.

5.9.1 QoS Classification

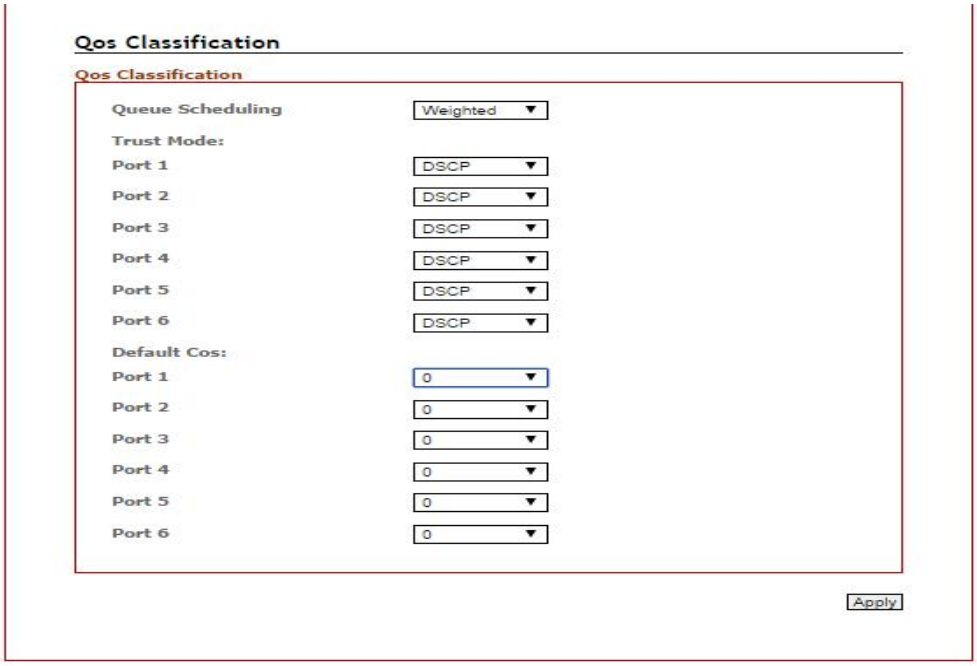


Figure 5.44 – QoS Classification Interface

Terms	Value Description
Queue Scheduling	User can set it as “Weighted” or “Strict” Weighted mode: An 8, 4, 2, 1 weighting is applied to each round robin priority queue. Strict mode: It gives egress queues with higher priority to be transmitted first before lower priority queues are serviced. ”
Trust mode	User can select the trust mode with either DSCP or Cos. When select DSCP, only trusted DSCP (Differentiated Services Code Point) values are mapped to a specific QoS class and drop precedence level (DPL). Frames with untrusted DSCP values are treated as non-IP frames. CoS: (Class Of Service) is well known as 802.1p. It describes that the output priority of a packet is determined by user priority field in 802.1Q VLAN tag. The priority value is supported 0to7COS value map to 4 priority queues: Highest, SecHigh, SecLow, and Lowest
Default Cost	User can set each port’s priority queue from 0 to 7 by clicking from dropdown box; of which 0 is the Highest, and

	7 is the Lowest
Apply	Click “Apply” button to save changes.

Figure 5.45 – QoS Classification Terms & Value Description

5.9.2 CoS Mapping

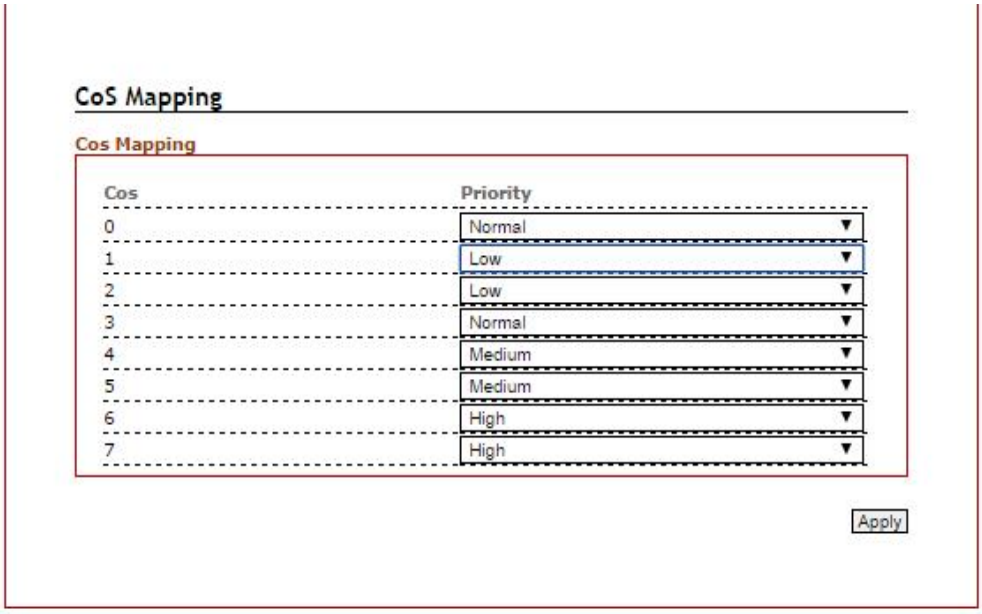


Figure 5.46 – CoS Mapping Interface

Terms	Value Description
Cos Value (0~7)	User can assign each port a CoS value from 0 to 7. According to the IEEE 802.1p, user can define each CoS value in 4 priority queues: from Low to Normal, Medium, and High.
Apply	Click “Apply” button to save changes.

Figure 5.47 – QoS Mapping Terms & Value Description

5.9.3 ToS Mapping

ToS is an acronym for Type of Service. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

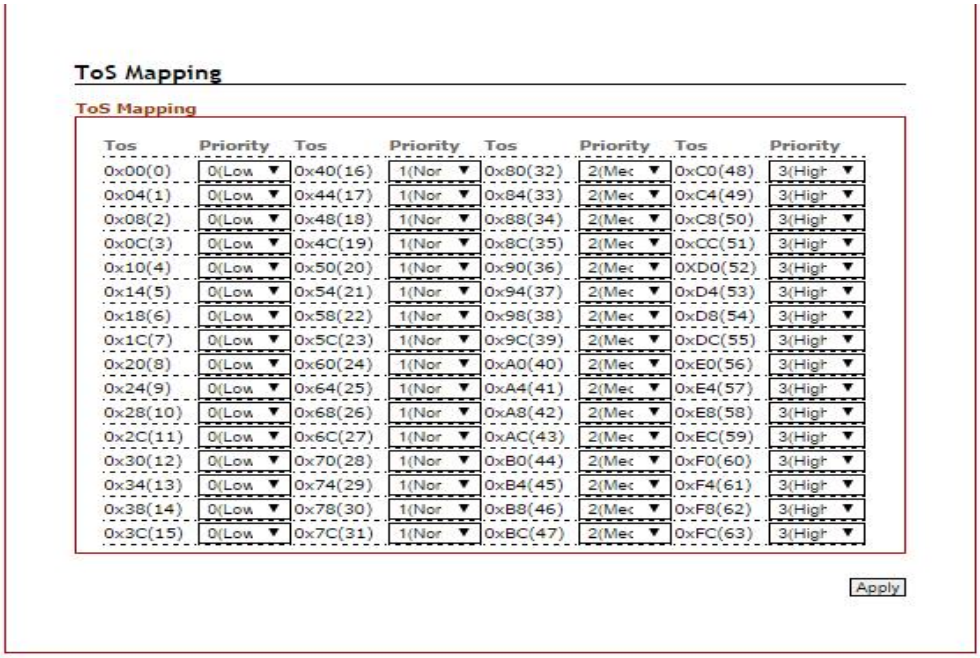


Figure 5.48 – ToS Mapping Interface

Terms	Value Description
ToS	User can assign each ToS value with 4 priority queues form 0 (Low) to 1 (Normal), 2 (Medium), and 3 (High).
Apply	Click “Apply” button to save changes.

Figure 5.49 – ToS Mapping Terms & Value Description

5.10 Port Mirroring

Enable or disable mirroring feature. When enabled, a copy of matched frames will be mirrored to the destination port specified in the port mirroring interface.

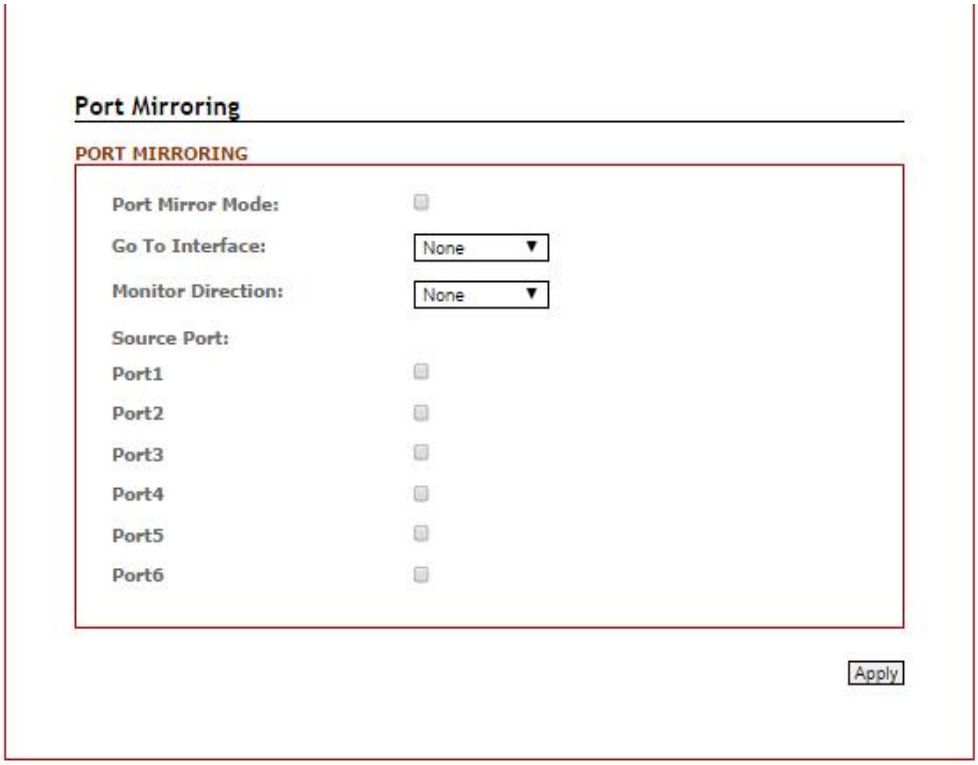


Figure 5.50 – Port Mirroring Configuration Interface

Terms	Value Description
Port Mirror Mode	Enable Port Mirroring function by check the box
Go To Interface	User can use the dropdown box to choose the destination port as “Port to mirror on” feature
Monitor Direction	User can select the monitor direction from the dropdown box by “Tx”, “Rx”, or “Tx/Rx”.
Source Port	User can decide any particular port as the source port(s) will require port mirroring.
Apply	Click “Apply” button to save changes.

Figure 5.51 – Port Mirroring Terms & Value Description

5.11 SNMP

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

5.11.1 SNMP Agent



Figure 5.52 – SNMP Agent Setup Interface

Terms	Value Description
Enable SNMP	Enable SNMP function by check the box
Read-only Community	User can release the SNMP to public for “read-only”
Apply	Click “Apply” button to save changes.

Figure 5.53 – SNMP Agent Interface Terms & Value Description

5.11.2 SNMP Trap setting



Figure 5.54 – SNMP Trap Setting

Terms	Value Description
Enable SNMP Trap	Enable SNMP Trap function by check the box
Trap Destination IP	User could insert the Server IP address as Trap Destination IP info
Community	User can release the SNMP to public for “read-only”
Apply	Click “Apply” button to save changes.

Figure 5.55 – SNMP Trap Settings Terms & Value Description

5.12 System Warning

System warning function is very important for managing a switch. Users can manage the switch by “Syslog”, “System Event Log”, and “Email Server” setup for Advanced Notice in any event type, “Event Type Selection”, and “Fault Alarm” setting. By setting up all these system warning features, users will receive the in advanced warning message through email, whenever any event occurs. It definitely increases the flexibility and capability for the user to monitor the remote site network and device statuses.

5.12.1 Syslog Setting

The SYSLOG is a protocol to transmit event notification messages across networks.

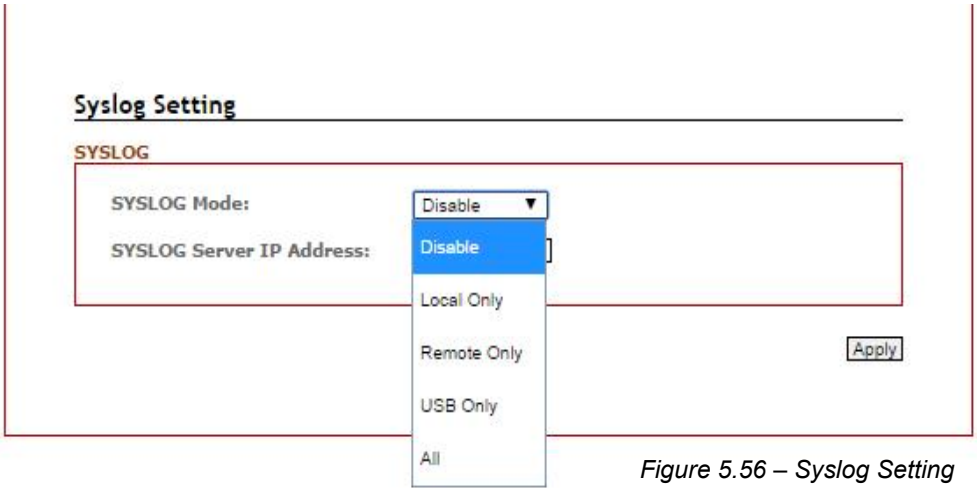


Figure 5.56 – Syslog Setting

Terms	Value Description
SYSLOG Mode	**Disable:** disable SYSLOG. **Local Only:** log to local system. **Remote Only:** log to a remote SYSLOG server. **USB Only:** log and store SYSLOG data and warning file to USB storage device through built-in USB Port; and the file name is “message” **All:** log to all local server / USB port, and remote SYSLOG server at the same time. Notice that there is one log in local server or USB port. If USB presented, it will log to USB storage. Otherwise it logs to local server.
SYSLOG Server IP Address	Insert remote SYSLOG server IP address

Apply	Click “Apply” button to save changes.

Figure 5.57 – SYSLOG Setting Terms & Value Description

5.12.2System Event Log

Users can view and display the system event log by clicking the “Apply” button on the right bottom corner of the interface. Then, the system event logs will display within the SYSLOG LIST window. The SYSLOG LIST will contain up to 5 pages of system event log information. Users also can click the “Refresh” button to have the most updated system event logs information to display.

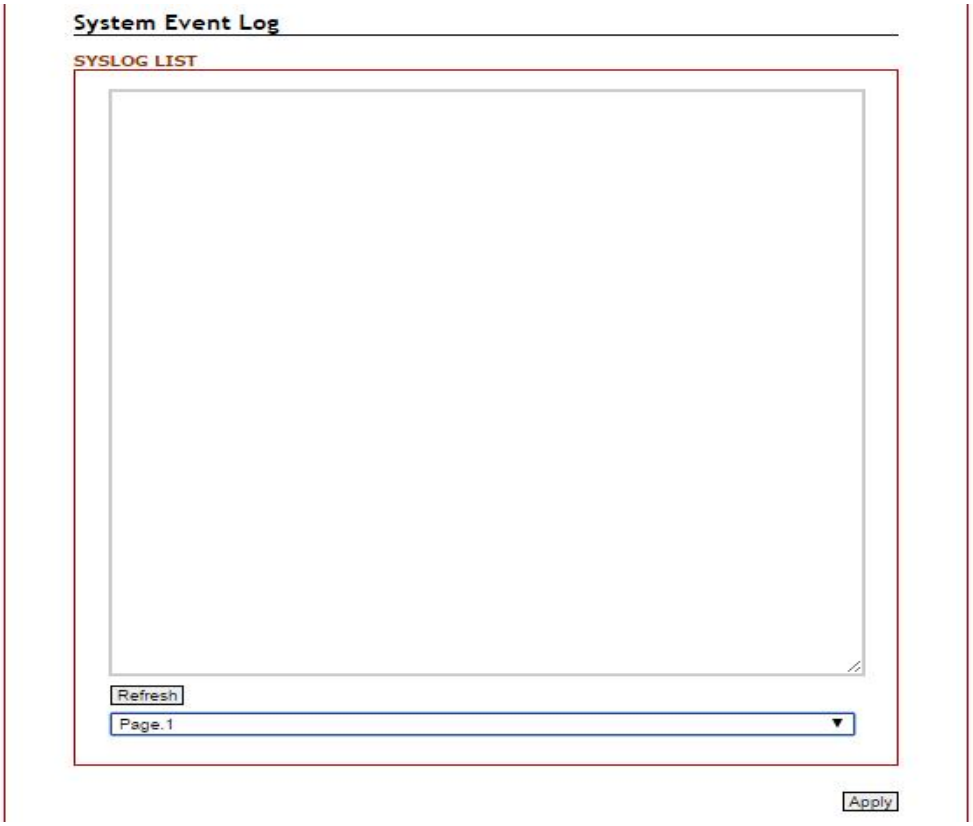


Figure 5.58 – System Event Logs Interface

5.12.3 SMTP Setting

The Simple Mail Transfer Protocol (SMTP) is for e-mail transmission across the Internet.

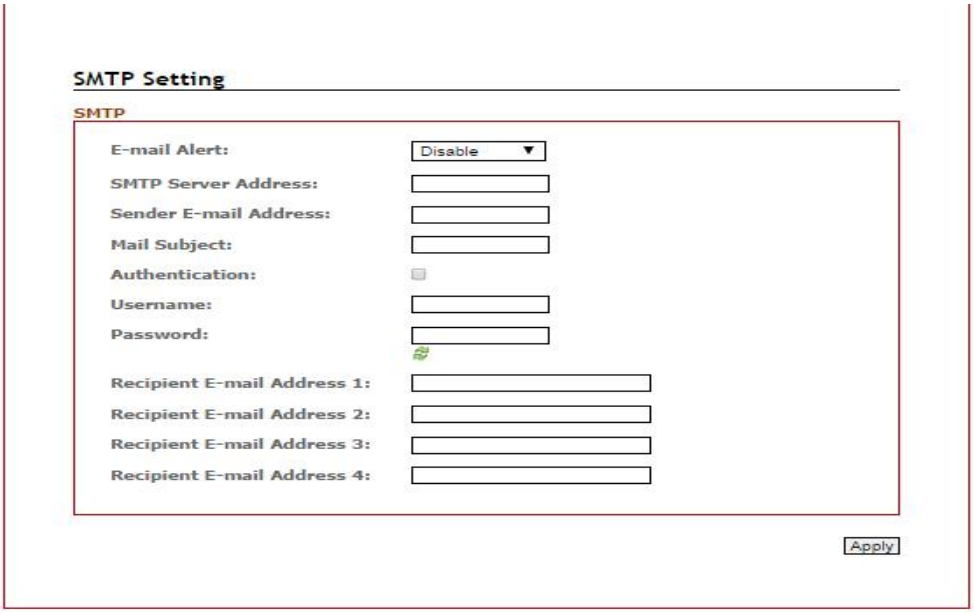


Figure 5.59 – SMTP Setting Interface

Terms	Value Description
E-mail Alert	Enable/Disable transmission system warning events by e-mail.
SMTP Server Address	Setting up the mail server IP address
Sender E-mail Address	Set up the email account to send the alert.
Mail Subject	The subject of the mail
Authentication	Check the box to enable the Authentication function **Username:** the authentication username. **Password:** the authentication password.
Recipient E-mail Address(es)	User can setup up to 4 recipient E-mail addresses to receive any system warning message.
Apply	Click “Apply” button to save changes.

Figure 5.60 – SMTP Setting Terms & Value Description

5.12.4 Event Selection

Users can select any event type through the “Event Selection” interface, such as “System Cold Start”, any ports’ “Link Up”, “Link Down”, “Link Up & Link Down” and send the system warning massage to either SYSLOG or SMTP, or both at the same time. After the event selection, users can click the “Apply” button to save changes.

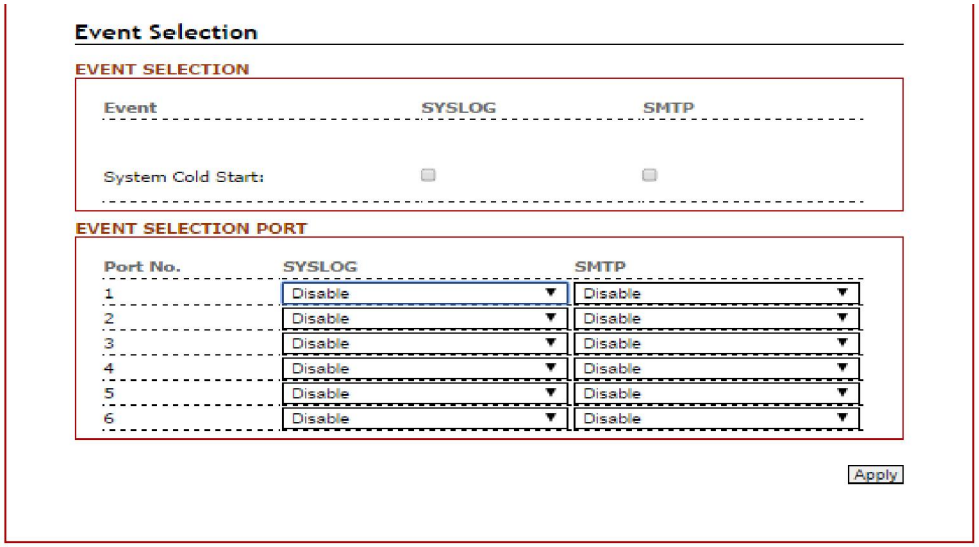


Figure 5.61 – Event Selection Setting Interface

5.12.5 Fault Alarm

When any selected fault event has occurred, the fault LED of the switch’s front panel will light up and the electric relay will signal at the same time. Users can check the checkbox of any “Fault Alarm” type, such as power failure, port link down or broken through the “Fault Alarm” setting interface to trigger this function.

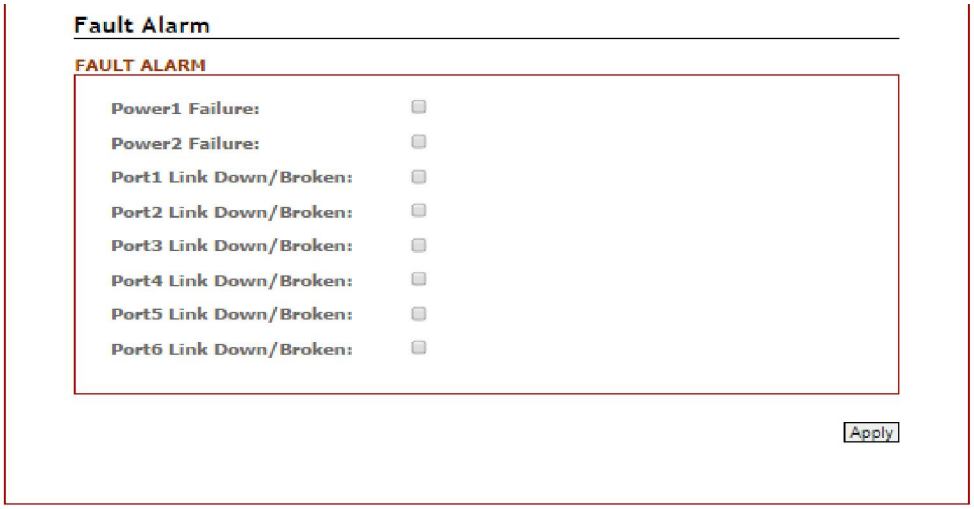


Figure 5.62 – Event Selection Setting Interface

5.13 MAC Table

The MAC address table is the filtering database that supports queries by the forwarding process, as to whether a frame received by a given port with a given destination MAC address is to be forwarded through a given potential transmission port.

5.13.1 MAC Address Table

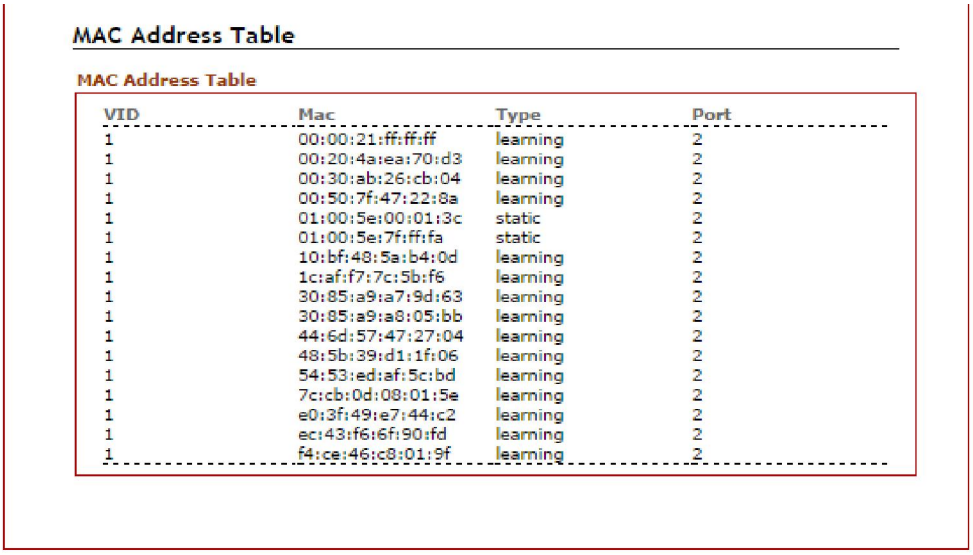


Figure 5.63 – MAC Address Table Interface

5.13.2 MAC Table Configuration

Users can check the checked box of each port and insert the port's VID and MAC address of the device that is connected to that port, then click the "Add" button to continue adding other ports' information. Click the "Apply" button to save all the settings.

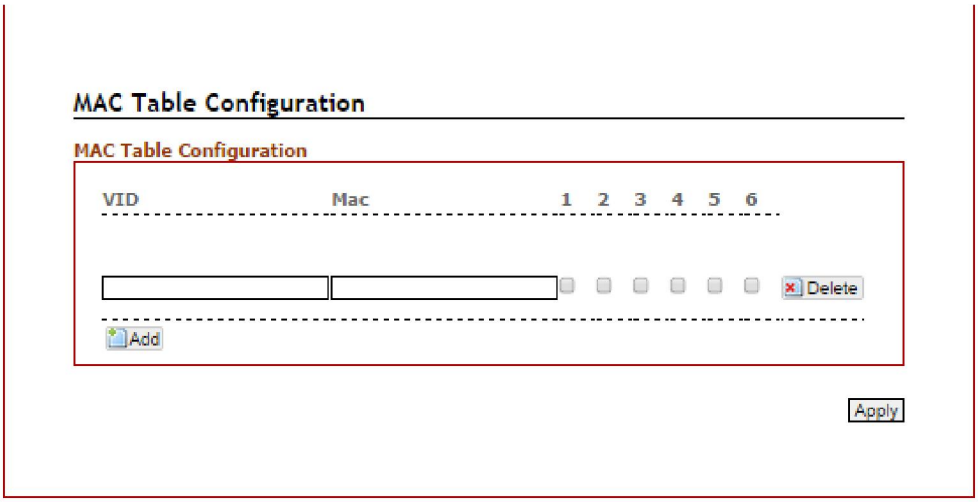


Figure 5.64 – MAC Table Setting Interface

5.14 Maintenance

Under the mnaintenance section, users can execute updated firmware upgrade, system reboot, and reset the system to factory default.

5.14.1 Upgrade

Antaira is continuously developing new functions and features for specific application requirements for the industrial managed switches. Users can download the latest firmware from Antaira's website and store it within their local PC, server, or USB drive.



Figure 5.65 – Firmware Upgrade Interface

Terms	Value Description
FIRMWARE UPGRADE	User can click the "Choose File" button to select the latest firmware from the local PC, or Server; then click the "Upgrade" button to have the switch be updated.
USB FIRMWARE UPGRADE	Fill in the folder and filename and click the button of Upgrade. If the folder or filename does not exist, system will return error. If it succeeds, system will reboot. Ex: file1, / folder /file2.

Figure 5.66 – Firmware Upgrade setting Terms & Value Description

5.14.2 Reboot

Users can click the “Apply” button under the “Reboot” interface to reboot the switch.

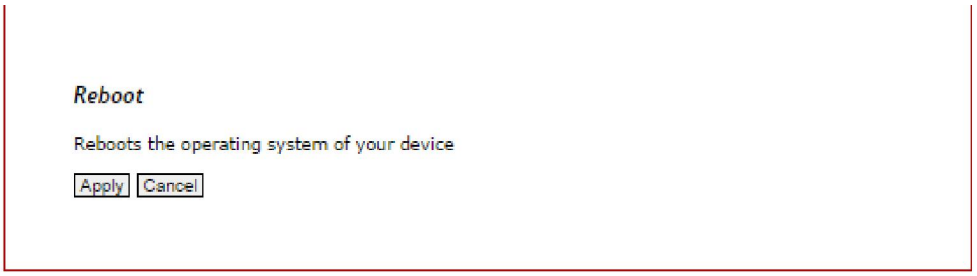


Figure 5.67 – Switch Reboot Interface

5.14.3 Default

Users can reset the switch to “Factory Default” by click the “Apply” button under the default interface.

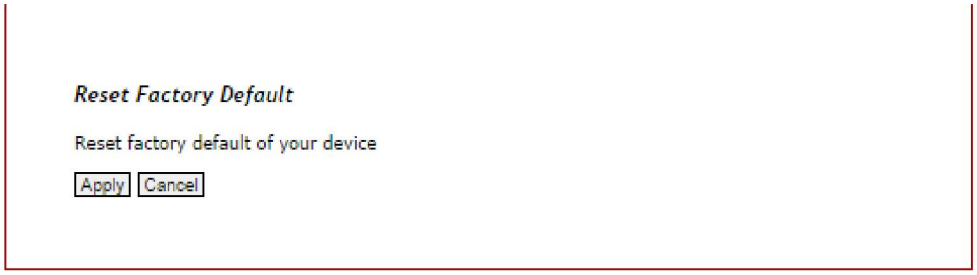


Figure 5.68 – Reset Factory Default Interface

5.15 Configuration

Under the “Configuration” section, users can save all the settings that have been configured, backed up and stored to a local PC, Server, or a USB storage device through the built-in USB port.

Users can use the USB port feature to execute the “Auto Load” function to boot the switch’s configuration that has been saved within the USB storage device, or users can utilize this function to “Auto Load” the configuration to other switches, and those switches would require the same configuration settings.

Users can keep the USB storage device plugged in with the switch to enable the USB “Auto Backup” function to allow the switch’s configuration settings to backup to the USB storage device whenever users makes and save configuration settings.

5.15.1 Save

Users can click the “Save” button under the “SAVE CONFIGURATION” interface, once all the settings had been configured.

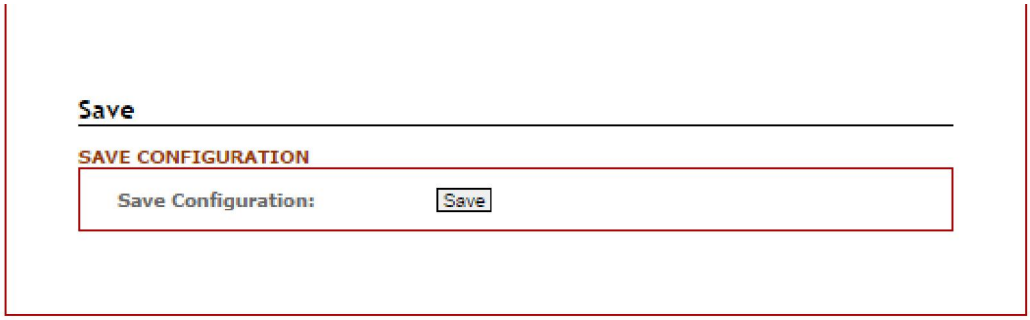


Figure 5.69 – Save Setting Interface

5.15.2 Backup & Store

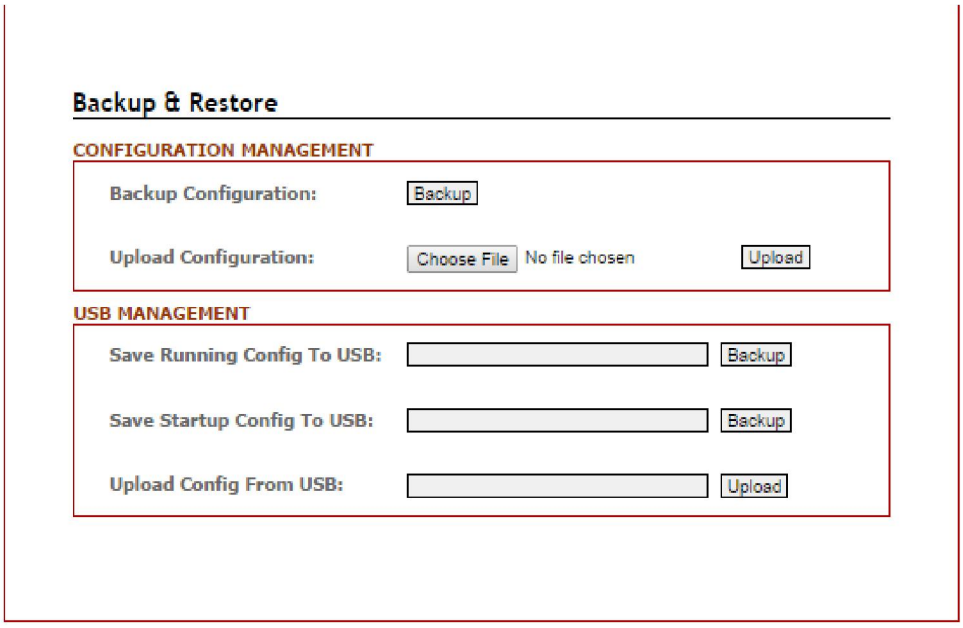


Figure 5.70 – Backup & Restore Setting Interface

Terms	Value Description
CONFIGURATION MANAGEMNET	
Backup Configuration	By click the “Backup” button, it allows user to backup the switch configuration setting to local PC, or server.
Upload Configuration	User can click the “Choose File” button to select the saved configuration file from local PC, or server, then click the “Upload” the settings to the switch.

USB Management	
Save Running Config to USB	Fill in the folder and filename and click the button of Backup. If the folder or filename does not exist, system will generate it automatically. Ex: file1, / folder /file2.
Save Startup Config to USB	Fill in the folder and filename and click the button of Backup. Because startup file didn't exist in default, it will be error to save in default. If the folder or filename does not exist, system will generate it automatically. Ex: file1, / folder /file2.
Upload Config from USB	Fill in the folder and filename and click the button of Upload. If the folder or filename does not exist, system will return error. If it succeeds, system will reboot. Ex: file1, / folder /file2.

Figure 5.71 – Backup & Restore Setting Terms & Value Description

5.15.3 Auto Load & Backup



Figure 5.72 – USB Auto Load and Backup Setting Interface

Terms	**Value Description**
USB Auto Load	Select USB Auto Load, it can auto load startup file from USB to Switch. And the file name is "switch-[MAC ADDRESS].cfg", if the file didn't exist, it will find "switch-config.cfg". If all of them didn't exist, it does not work.
USB Auto Backup	Select USB Auto Backup, it can auto Backup running-config file from Switch to USB. And the file name is "startup-config".

Figure 5.73 – USB Auto Load and Backup Setting Terms & Value Description

5.16 Logout

Users can logout of the web console interface by pointing at and clicking 'logout' from the menu.

6. Command Line Interface Management

6.1 About CLI Management

Besides WEB-based management, LMP-0602 series also supports CLI management. Users can use console or telnet to management switch by CLI.

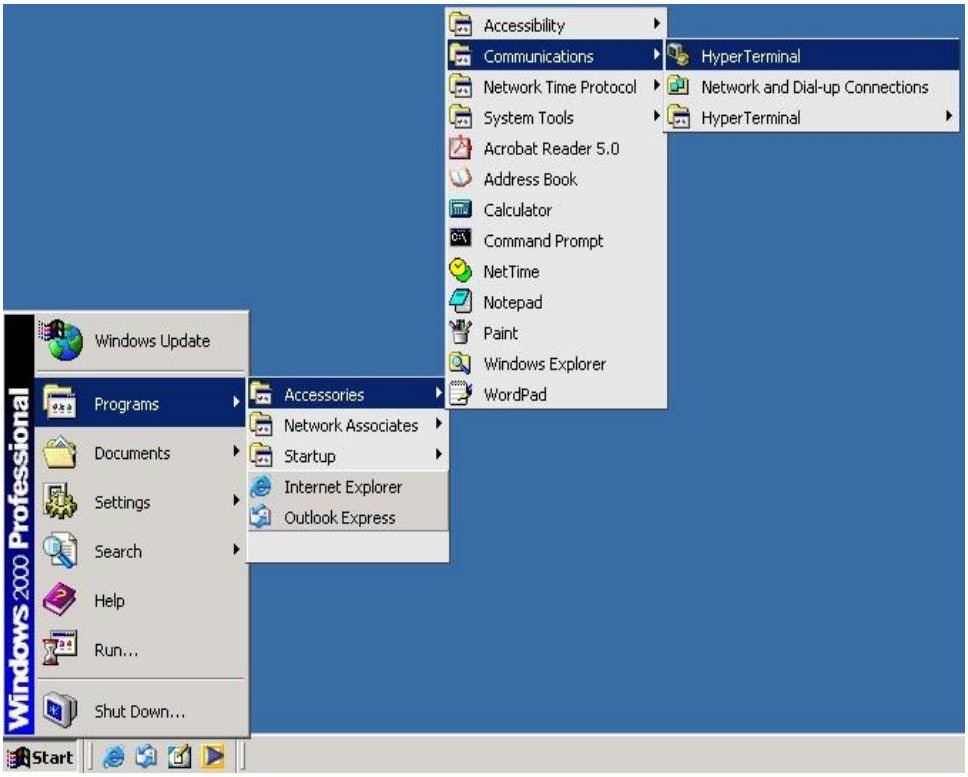
CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

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.

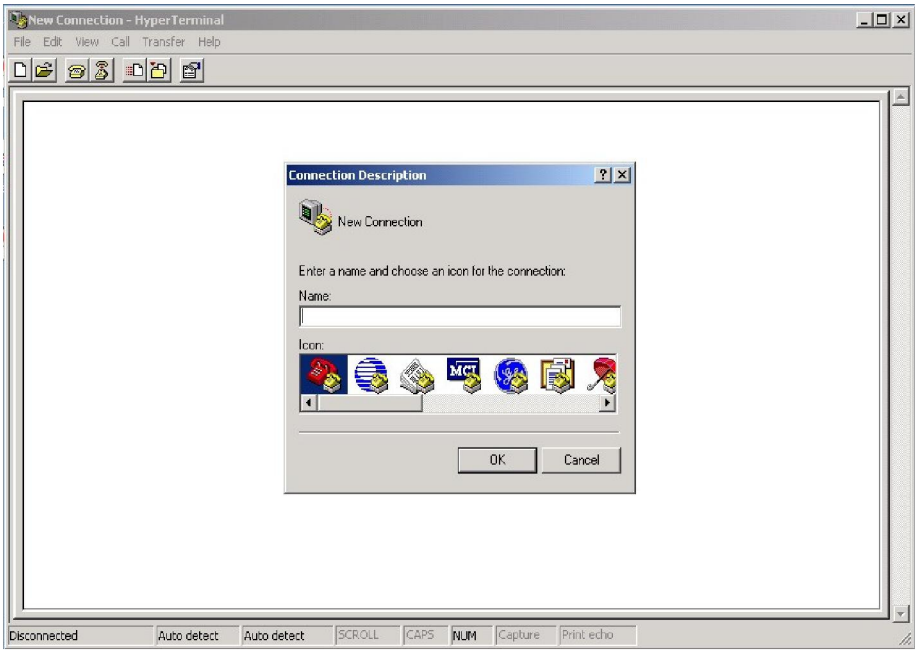
Step 1:

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



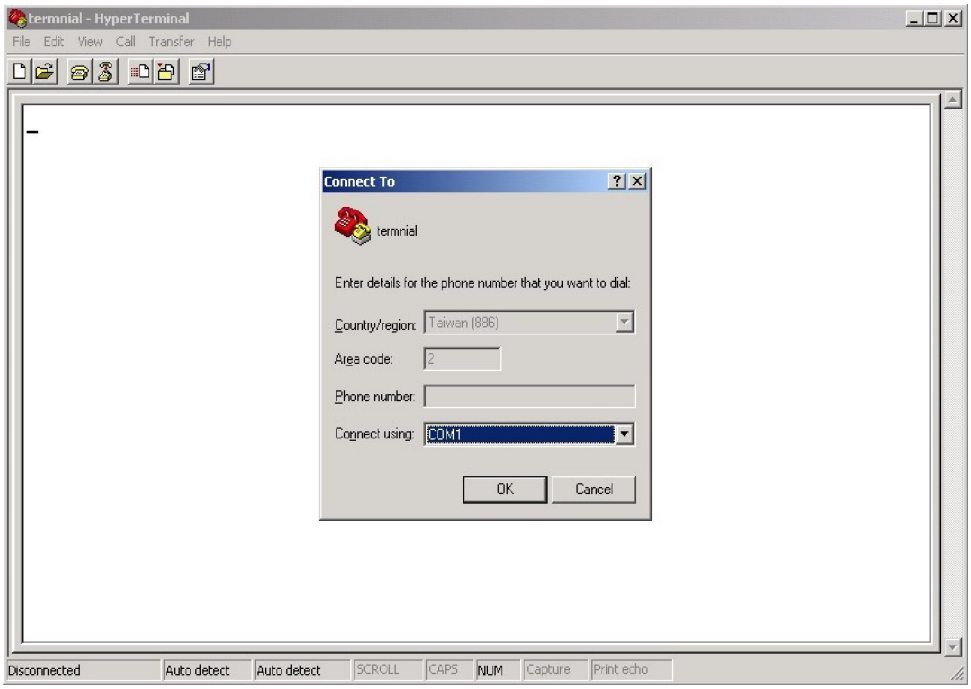
Step 2:

Input a name for the new connection.



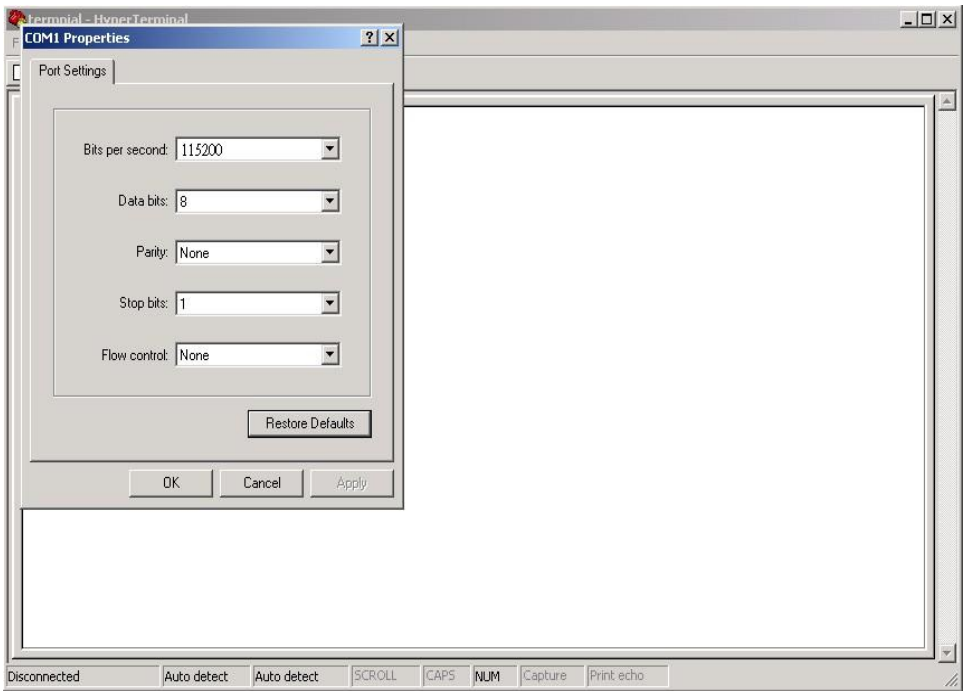
Step 3:

Select to use COM port number



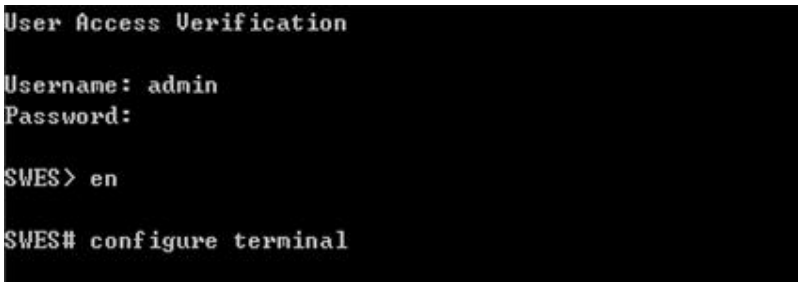
Step 4:

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, then press “**Enter**”.



CLI Management by Telnet

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

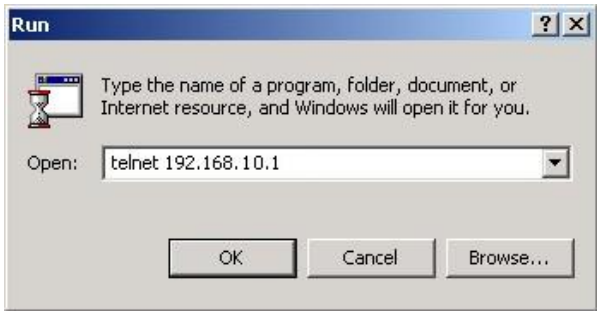
The default value is as below:

- 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.

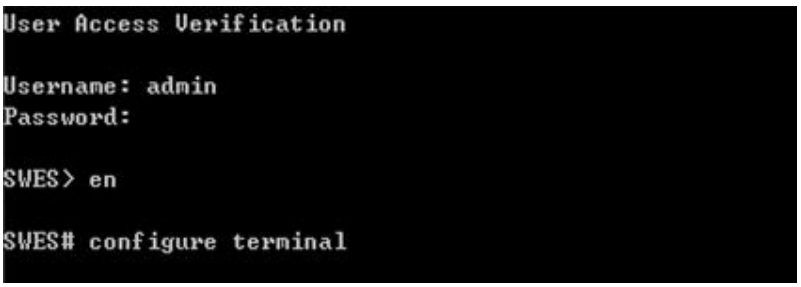
Step 1:

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	hostname [Switch]	configure
	system location [none]	configure
	system contact [none]	configure
	no system location	configure
	no system contact	configure
	show system uptime	configure
	show system mac	configure
	show system version firmware	configure
	show system version loader	configure
	show environment power 1	configure
	show environment power 2	configure
	show environment temperature	configure
	admin username admin	configure
	admin password admin	configure
IP	boot host dhcp	configure
	ip address [ip_addr] [ip_mask]	configure
	ip default-gateway [ip_router]	configure
	ip name-server [ip_addr_string]	configure
	no boot host dhcp	configure
	no ip default-gateway	configure
	no ip name-server	configure
	show boot host dhcp	configure
	show ip address	configure
	show ip default-gateway	configure
	show ip name-server	configure
	show ip mode	configure
Time	ntp time update	configure
	ntp client enable	
	ntp client timeserver [ip_addr_string]	configure
	clock set [hh:mm:ss] [day] [month] [year]	configure
	clock timezone [area] [city]	configure
	ntp sync schedule enable	configure
	ntp sync minute [time]	configure

	ntp sync hour [time]	configure
	ntp sync day [time]	configure
	ntp sync month [time]	configure
	ntp sync weekly [time]	configure
	no ntp client enable	Configure
	no ntp client timeserver	configure
	no clock timezone	configure
	no ntp sync schedule enable	configure
	no ntp sync minute	configure
	no ntp sync hour	configure
	no ntp sync day	configure
	no ntp sync month	configure
	no ntp sync weekly	configure
	show ntp client enable	configure
	show ntp client timeserver	configure
	show clock timezone	configure
	show ntp sync schedule enable	configure
	show ntp sync minute	configure
	show ntp sync hour	configure
	show ntp sync day	configure
	show ntp sync month	configure
	show ntp sync weekly	configure
Port	speed [auto | 10 | 100 | 1000]	interface
	duplex [auto | full | half]	interface
	flowcontrol <receive> [on | off | desired]	interface
	name [string]	interface
	shutdown	interface
	no speed	interface
	no duplex	interface
	no flowcontrol	interface
	no name	interface
	no shutdown	interface
	show speed	interface
	show duplex	interface
	show flowcontrol	interface

	show administrate	interface
	show name	interface
	show link status	interface
	show link state	interface
	show link speed	interface
	show duplex	interface
	show link rx	interface
	show link tx	interface
	show link summary	interface
	show interface transceiver	interface
VLAN	name [vlan_name]	vlan
	member [member_portlist] [<untag_portlist>]	vlan
	vlan-mode [port | tag | qinq]	configure
	vlan-group [group_num] [group_portlist]	configure
	switchport pvid [vlan_id]	interface
	switchport filter [tagged | untagged]	interface
	switchport provider	interface
	switchport ethertype [ether_type]	interface
	no name	vlan
	no member	vlan
	no vlan-mode	configure
	no vlan-group	configure
	no switchport pvid	interface
	no switchport filter	interface
	no switchport provider	interface
	no switchport ethertype	interface
	show name	vlan
	show member	vlan
	show vlan-mode	configure
	show vlan-group	configure
	show switchport pvid	interface
	show switchport filter	interface
	show switchport provider	interface
	show switchport ethertype	interface
	enable	g8032

ERPS	disable	g8032
	rpl [port0 | port1] [owner | neighbor]	g8032
	aps-channel [channel ID]	g8032
	revertive	g8032
	clear	g8032
	port0 interface [interface name]	g8032
	port1 interface [interface name]	g8032
	fs	g8032
	ms	g8032
	ring-id [erps ring ID]	g8032
	timer hold-off [time]	g8032
	timer guard [time]	g8032
	timer wtr [time]	g8032
	no rpl [port0 | port1]	g8032
	no aps-channel	g8032
	no revertive	g8032
	no port0	g8032
	no port1	g8032
	no ring-id	g8032
	no timer hold-off	g8032
	no timer guard	g8032
	no timer wtr	g8032
	show ethernet ring g8032 status	g8032
	show ethernet ring g8032 brief	g8032
	show ethernet ring g8032 port status	g8032
	power inline auto	interface
	power inline never	interface
	power inline delay	interface
	power inline apply	interface
	power inline priority [priority_value]	interface
	power inline max [watts]	interface
	power inline status	interface
	power inline power-supply [watts]	configure
	power inline threshold [theshold_value]	configure
	no power inline	interface

PoE	no power inline priority	interface
	no power inline max	interface
	show power inline	interface
	show power inline priority	interface
	show power inline max	interface
	show power inline status	interface
	show power inline power-supply	configure
	show power inline total-consumption	configure
	show power inline threshold	configure
STP	spanning-tree enable	configure
	spanning-tree mode [rstp | mst]	configure
	spanning-tree priority [priority_value]	configure
	spanning-tree forward-time [forward time]	configure
	spanning-tree hello-time [hello_time]	configure
	spanning-tree max-age [max_age]	configure
	spanning-tree cost [link_cost_value]	interface
	spanning-tree port-priority [port_priority]	interface
	spanning-tree link-type [point-to-point | point-to-multiple]	interface
	spanning-tree auto-edge off	interface
	spanning-tree admin-edge on	interface
	spanning-tree stp disable	interface
	no spanning-tree enable	configure
	no spanning-tree mode	configure
	no spanning-tree priority	configure
	no spanning-tree forward-time	configure
	no spanning-tree hello-time	configure
	no spanning-tree max-age	configure
STP	no spanning-tree mst [instance_ID] priority	configure
	no spanning-tree cost	interface
	no spanning-tree port-priority	interface
	no spanning-tree link-type	interface
	no spanning-tree auto-edge	interface
	no spanning-tree admin-edge	interface
	no spanning-tree admin-edge	interface
	no spanning-tree stp	interface

STP	show spanning-tree mode	configure
	show spanning-tree priority	configure
	show spanning-tree forward-time	configure
	show spanning-tree hello-time	configure
	show spanning-tree max-age	configure
	show spanning-tree cost	interface
	show spanning-tree port-priority	interface
	show spanning-tree link-type	interface
	show spanning-tree auto-edge	interface
	show spanning-tree admin-edge	interface
	show spanning-tree stp	interface
	spanning-tree mst [instance_ID] priority [priority]	configure
	spanning-tree mst name [NAME]	configure
	spanning-tree mst revision [REVISION]	configure
	spanning-tree mst instance [instance_ID] vlan [vlan_grp]	configure
	spanning-tree mst [instance_ID] priority [priority_number]	configure
	spanning-tree mst [instance_ID] cost [cost_value]	interface
	spanning-tree mst [instance_ID] port-priority [priority]	interface
	no spanning-tree mst name	configure
	no spanning-tree mst revision	configure
	no spanning-tree mst instance [instance_ID] vlan	configure
	no spanning-tree mst [instance_ID] cost	interface
	no spanning-tree mst [instance_ID] port-priority	interface
	show spanning-tree mst name	configure
	show spanning-tree mst revision	configure
	show spanning-tree mst instance [instance_ID] vlan	configure
	show spanning-tree mst [instance_ID] priority	configure
	show spanning-tree mst [instance_ID] cost	interface
	show spanning-tree mst [instance_ID] port-priority	interface
	event smtp power1 enable	configure
	event smtp power2 enable	configure
	event smtp cold-start enable	configure
	event smtp warm-start enable	configure
	event smtp authentication-failure enable	configure
	event smtp erps-change enable	configure

Event	event smtp interface [INTERFACE_NAME] [up | down]	configure
	no event smtp power1	configure
	no event smtp power2	configure
	no event smtp cold-start	configure
	no event smtp warm-start	configure
	no event smtp authentication-failure	configure
	no event smtp erps-change	configure
	no event smtp interface [INTERFACE_NAME] [up | down]	configure
	show event smtp power1	configure
	show event smtp power2	configure
	show event smtp cold-start	configure
	show event smtp warm-start	configure
	show event smtp authentication-failure	configure
	show event smtp erps-change	configure
	show event smtp interface [INTERFACE_NAME] [up | down]	configure
	event syslog power1 enable	configure
	event syslog power2 enable	configure
	event syslog cold-start enable	configure
	event syslog warm-start enable	configure
	event syslog authentication-failure enable	configure
	event syslog erps-change enable	configure
	event syslog interface [INTERFACE_NAME] [up | down]	configure
	no event syslog power1	configure
	no event syslog power2	configure
	no event syslog cold-start	configure
	no event syslog warm-start	configure
	no event syslog authentication-failure	configure
	no event syslog erps-change	configure
	no event syslog interface [INTERFACE_NAME] [up | down]	configure
Event	show event syslog power1	configure
	show event syslog power2	configure
	show event syslog cold-start	configure
	show event syslog warm-start	configure
	show event syslog authentication-failure	configure
	show event syslog erps-change	configure

	show event syslog interface [INTERFACE_NAME] [up | down]	configure
	event alarm power1 enable	configure
	event alarm power2 enable	configure
	event alarm interface [INTERFACE_NAME] [up | down]	configure
	no event alarm power1	configure
	no event alarm power2	configure
	no event alarm interface [INTERFACE_NAME] [up | down]	configure
	show event alarm power1	configure
	show event alarm power2	configure
	show event alarm interface [INTERFACE_NAME] [up | down]	configure
	event apply	configure
SYSLOG	syslog server [IP_address]	configure
	syslog mode [both | remote | local]	configure
	no syslog server	configure
	no syslog mode	configure
	show syslog server	configure
	show syslog mode	configure
	show syslog log	configure
SMTP	smtp enable	configure
	smtp sender [E-MAIL_ADDR]	configure
	smtp subject [subject_text]	configure
	smtp server address [GMAIL_SMPT_SERVER]	configure
	smtp server port [GMAIL_SMPT_SERVER]	configure
	smtp authentication enable	configure
	smtp authentication username [GMAIL_ACCOUNT]	configure
	smtp authentication password [GMAIL_PASS]	configure
	smtp receive [1 | 2 | 3 | 4] [e-mail_address]	configure
	no smtp enable	configure
	no smtp sender	configure
	no smtp subject	configure
	no smtp server address	configure
	no smtp server port	configure
	no smtp authentication enable	configure
	no smtp authentication username	configure
	no smtp authentication password	configure

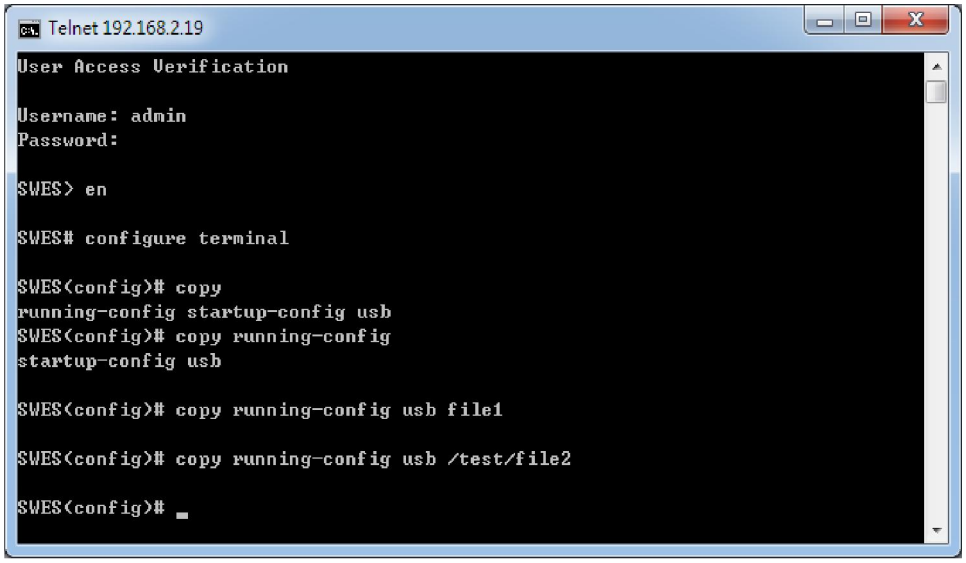
	no smtp receive [1 | 2 | 3 | 4]	configure
	show smtp state	configure
	show smtp sender	configure
	show smtp subject	configure
	show smtp server address	configure
	show smtp server port	configure
	show smtp authentication enable	configure
	show smtp authentication username	configure
	show smtp receive [1 | 2 | 3 | 4]	configure
SNMP	snmp server enable [<v1-v2c-only | v3-only>]	configure
	snmp server community [ro | rw] [community_name]	configure
	snmp server v3 level [admin| user] [auth | noauth | priv]	configure
	snmp server v3 auth [admin | user] [md5 | sha] [PWD]	configure
	snmp server v3 encryption [admin | user] [des | aes] [PWD]	configure
	no snmp server enable	configure
	no snmp server community [ro | rw]	configure
	no snmp server v3 level [admin| user]	configure
	no snmp server v3 auth [admin | user]	configure
	no snmp server v3 encryption [admin | user]	configure
	show snmp server enable	configure
	show snmp server community [ro | rw]	configure
	show snmp server v3 level [admin| user]	configure
	show snmp server v3 auth [admin | user]	configure
	show snmp server v3 encryption [admin | user]	configure
	snmp trap enable	configure
	snmp trap host [DESTINATION_IP]	configure
	snmp trap version [1 | 2c | 3] [traps | inform]	configure
	snmp trap community [trap_community_name]	configure
	snmp trap inform retry [retry_time]	configure
	snmp trap inform timeout [retry_interval]	configure
	snmp trap v3 user [user_ID]	configure
	snmp trap v3 level [auth | noauth | priv]	configure
	snmp trap v3 engine-ID [engineID]	configure
SNMP	snmp trap v3 auth [md5 | sha] [PASSWORD]	configure
	snmp trap v3 encryption [des | aes] [PASSWORD]	configure

SNMP	no snmp trap enable	configure
	no snmp trap host	configure
	no snmp trap version	configure
	no snmp trap community	configure
	no snmp trap inform retry	configure
	no snmp trap inform timeout	configure
	no snmp trap v3 user	configure
	no snmp trap v3 level	configure
	no snmp trap v3 engine-ID	configure
	no snmp trap v3 auth	configure
	no snmp trap v3 encryption	configure
	show snmp trap enable	configure
	show snmp trap host	configure
	show snmp trap version	configure
	show snmp trap community	configure
	show snmp trap inform retry	configure
	show snmp trap inform timeout	configure
	show snmp trap v3 user	configure
	show snmp trap v3 level	configure
	show snmp trap v3 engine-ID	configure
	show snmp trap v3 auth	configure
	show snmp trap v3 encryption	configure
FILE	copy running-config startup-config	configure
	copy startup-config running-config	configure
PORT MIRROR	monitor enable	configure
	monitor source [rx | tx | both] [port_list]	configure
	monitor destination [dest_port_number]	configure
	no monitor enable	configure
	no monitor source	configure
	no monitor destination	configure
	show monitor enable	configure
	show monitor source	configure
	show monitor destination	configure
	qos queue-schedule [strict | wrr]	configure
	qos map cos [priority_type] to tx-queue [queue]	configure

QoS	qos map dscp [[priority_type] to tx-queue [[queue]	configure
	qos trust [cos | dscp]	interface
	qos default cos [cos_default_value]	interface
	no qos queue-schedule	configure
	no qos map cos [priority_type]	configure
	no qos map dscp [priority_type]	configure
	no qos trust	interface
	no qos default cos	interface
	show qos queue-schedule	configure
	show qos map cos [priority_type]	configure
	show qos map dscp [priority_type]	configure
	show qos trust	interface
	show qos default cos	interface
IGMP	igmp snooping enable	configure
	igmp snooping query max-respond-time [second]	configure
	igmp snooping query interval [second]	configure
	igmp snooping last-member count [time]	configure
	igmp snooping last-member interval [second]	configure
	igmp snooping querier enable	configure
	igmp snooping fast-leave enable	interface
	no igmp snooping enable	configure
	no igmp snooping query max-respond-time	configure
	no igmp snooping query interval	configure
	no igmp snooping last-member count	configure
	no igmp snooping last-member interval	configure
	no igmp snooping querier	configure
	no igmp snooping fast-leave	interface
	show igmp snooping mdb	configure
	show igmp snooping all	configure
	show igmp snooping fast-leave	interface

Save and Load Configuration File to/from USB

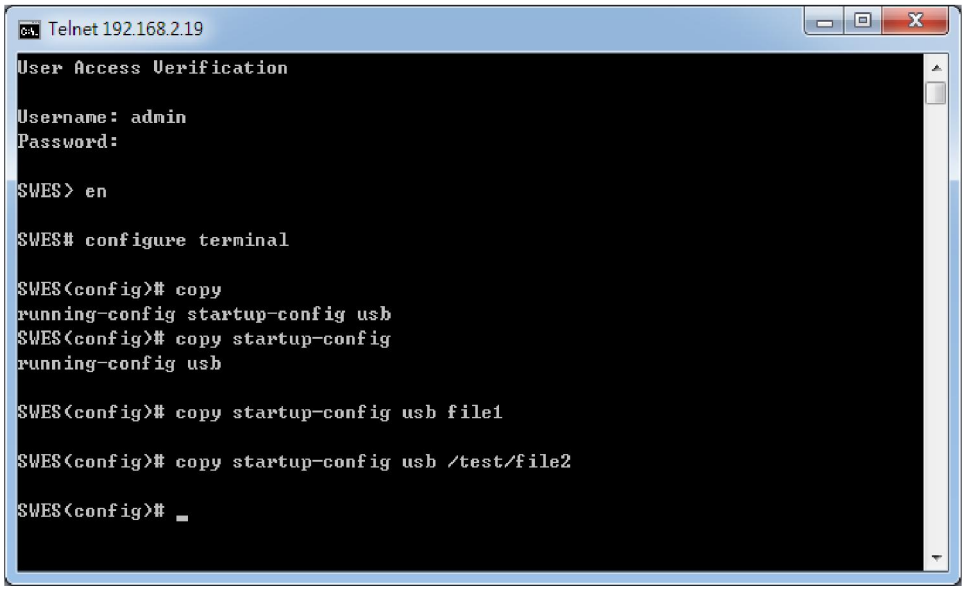
1. CLI: enable -> configure terminal ->copy running-config usb (path)



Fill in the folder and filename behind the “copy running-config usb” command.

Ex: file1, / folder /file2.

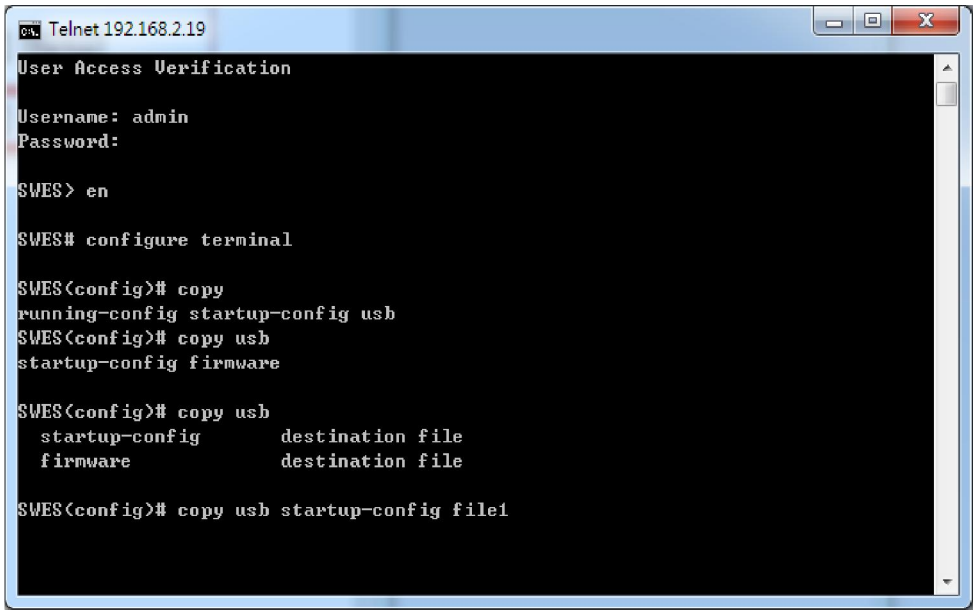
2. CLI : enable -> configure terminal ->copy startup-config usb (path)



Fill in the folder and filename behind the “copy startup-config usb” command.

Ex: file1, / folder /file2.

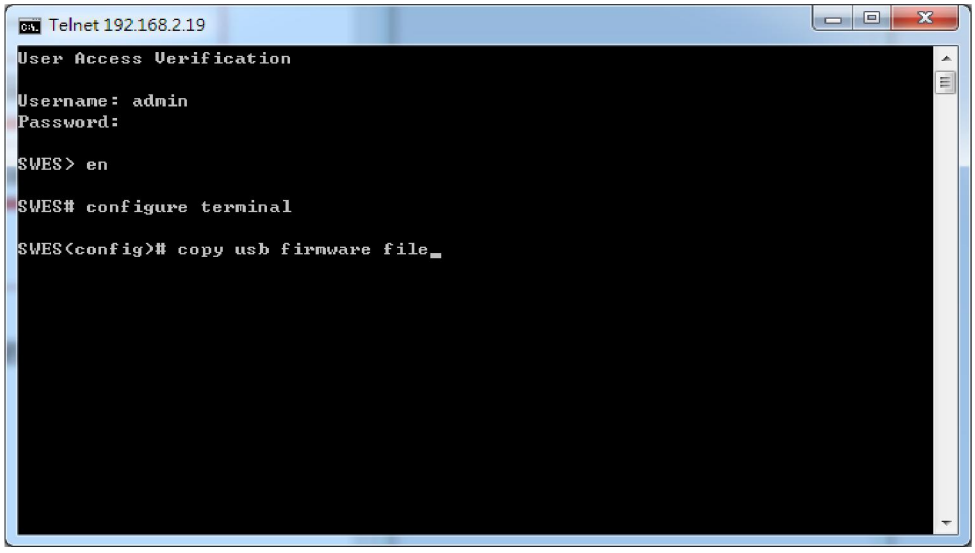
3. CLI :enable -> configure terminal ->copy usb startup-config (path)



Fill in the folder and filename behind the “copy usb startup-config” command.

Ex: file1, / folder /file2.

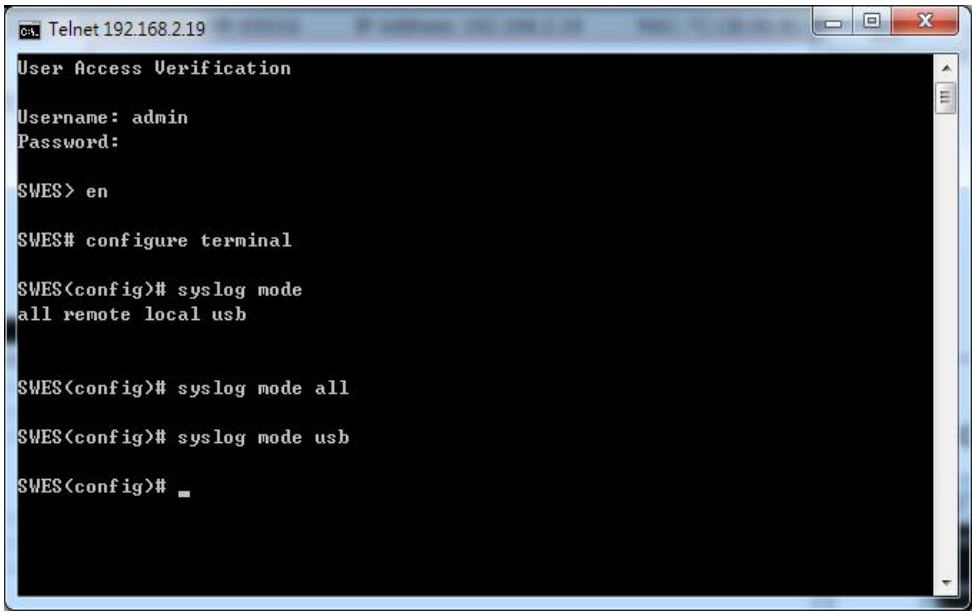
4. CLI : enable -> configure terminal ->copy usb firmware (path)



Fill in the folder and filename behind the “copy usb startup-config” command.

Ex: file1, / folder /file2.

5. CLI : enable -> configure terminal -> Syslog mode (usb or all)



Select USB or ALL, it can auto save waning file to USB. And the file name is “message”.

6. CLI : enable -> configure terminal ->usb auto load enable
7. CLI : enable -> configure terminal ->usb auto load enable

7. Technical Specification

Table 7.1 has the technical specifications for Antaira's LMP-0600 series: 6-port industrial PoE+ managed Ethernet switch with 4*10/100Tx (30W/Port), and 2*10/100Tx; 48~55VDC power input.

Standards	IEEE 802.3	10Base-T 10Mbit/s Ethernet
	IEEE 802.3u	100Base-Tx, 100Base-Fx, Fast Ethernet
	IEEE 802.3x	Flow Control for Full Duplex
	IEEE 8023.af	Power-over-Ethernet
	IEEE 802.3at	Power-over-Ethernet Plus (Enhanced)
	IEEE 802.1d	STP (Spanning Tree Protocol)
	IEEE 802.1w	RSTP (Rapid Spanning Tree Protocol)
	IEEE 802.1s	MTP (Multiple Spanning Tree Protocol)
	ITU-TG.8032 / Y.1344	ERPS (Ethernet Ring Protection Switch)
	IEEE 802.1q	Virtual LANs (VLAN)
	IEEE 802.1x	Port based Network Control, Authentication
	IEEE 802.1ad	Stacked VLAN, Q-in-Q
	IEEE 802.1p	QoS/CoS Protocol for Traffic Prioritization
Switch	Protocol	CSMA/CD,IGMPv1/v2,SNMPv1/v2,TFTP,SNTP,SMTP,RARP, Syslog
	Data Process	Store and Forward
	Transfer Rate	14,880 pps for 10Base-T Ethernet port 148,800 pps for 100Base-TX Fast Ethernet port
	Packet Buffer	1Mbits
	MAC Table	8K
	Jumbo Frame	-
	Flow Control	IEEE 802.3x for full duplex mode, back pressure for half duplex mode
	VLAN Groups	0 ~ 4094
	IGMP Groups	Up to 256
Port Interface	Ethernet (RJ45) Port	4*10/100BaseTx (PSE: 30W/Port), and 2*10/100Tx Fast Ethernet ports, auto negotiation speed, Full/Half duplex mode, and auto MDI/MDI-X connection
	PoE Pin Assignment	V+, V+, V-, V-, for pin 1, 2, 3, 6 (Endspan, MDI-X Alternative A)
	RS232 Serial Console	1*RS232 in RJ45 connector with console cable, 115.2Kbps, 8,N,1
	Configuration Backup	1*USB 2.0
Protection	Overload Current	Present
	Power Reverse polarity	Present

	CPU Watch Dog	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)
Mechanical Characteristics	LED Indicator	Per Unit: Power 1 (Green), Power 2 (Green), Fault (Red); Per Port: Link/Activity (Green); PoE: Feeding Power (Green)
	Housing	Metal IP30 protection
	Dimension	46 x 142 x 99 mm (1.81 x 5.59 x 3.90 in.)
	Weight	Unit Weight: 1.3 lbs. Shipping Weight: 2.2 lbs
	Mounting	DIN-Rail Mounting, wall-mounting (optional)
Power Requirement	Input Voltage	48~55VDC Redundant Input
	Power Connection	1 removable 6-contact terminal block
	PoE Power Output	25W @ 48VDC (per PoE port); 30W @ 51~55VDC (per PoE port)
	Power Consumption	10 Watts (no PD included); 130 Watts (Fully loaded)
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	CE EN6100-4-2/3/4/5/6/8; CE EN6100-6-2; EN6100-6-4
	Stability Testing	IEC60068-2-32 (Free fall) IEC60068-2-27 (Shock) IEC60068-2-6 (Vibration)
	Safety	UL 61010-1, UL 61010-2-201

Table 7.1

LMP-0600 Series Technical Specification

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