



## LMP-0600-24 Series

**6-Port Industrial PoE+ Managed Ethernet Switch,  
with 6\*10/100Tx (w/4\*PoE Ports: 30W/Port);  
12~36VDC Power Input (w/Voltage Booster)**



Version 1.1

## User Manual



## **© 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 PoE Managed Ethernet Switches

User Manual

Version 1.1 (March 2018)

This manual supports the following models:

- LMP-0600-24
- LMP-0600-24-T

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

# Table of Contents

<b>1. Introduction .....</b>	<b>1</b>
1.1 Product Overview .....	1
1.2 Product Software Features .....	1
1.3 Product Hardware Features .....	2
1.4 Package Contents .....	3
1.5 Safety Precaution .....	3
<b>2. Hardware Description .....</b>	<b>4</b>
2.1 Physical Dimensions .....	4
2.2 Front Panel .....	5
2.3 Top View .....	5
2.4 LED Indicators .....	6
2.5 Reset Button .....	6
2.6 Ethernet Ports .....	7
2.7 Cabling .....	8
2.8 Wiring the Power Inputs .....	10
2.9 Wiring the Fault Alarm Contact .....	10
<b>3. Mounting Installation .....</b>	<b>11</b>
3.1 DIN-Rail Mounting .....	11
3.2 Wall Mounting .....	12
<b>4. Hardware Installation .....</b>	<b>13</b>
4.1 Installation Steps .....	13
<b>5. Web Management .....</b>	<b>14</b>
5.1 Web Console Configuration .....	14
5.1.1 About Web-Based Management .....	14
5.2 Basic Setting .....	15

5.2.1 System Information .....	15
5.2.2 Admin & Password .....	16
5.2.3 IP Setting.....	17
5.2.4 IPv6 Neighbor Cache .....	18
5.2.5 IPv6 Settings .....	18
5.2.6 System Time .....	19
5.3 Port Management .....	20
5.3.1 Port Status.....	20
5.3.2 Port Configuration .....	20
5.4 PoE (Power-over-Ethernet) .....	21
5.4.1 PoE Configuration .....	21
5.4.2 Ping Alarm.....	22
5.4.3 PoE Schedule.....	23
5.5 ERPS .....	24
5.5.1 ERPS Status .....	25
5.5.2 ERPS Configuration .....	25
5.5.3 Before Configuring ERPS.....	27
5.6 Spanning Tree .....	35
5.6.1 RSTP Status.....	35
5.6.2 RSTP Configuration .....	36
5.6.3 MSTI Status.....	38

5.6.4 MSTI Configuration .....	38
5.7 IGMP Snooping .....	40
5.7.1 IGMP Settings .....	41
5.7.2 IGMP Snooping Status Table .....	41
5.8 802.1Q VLAN .....	42
5.8.1 802.1Q VLAN Settings .....	42
5.8.2 802.1Q VLAN Port Settings .....	43
5.9 QoS (Traffic Prioritization) .....	44
5.9.1 QoS Classification .....	45
5.9.2 CoS Mapping .....	46
5.9.3 ToS Mapping .....	47
5.10 Port Trunk .....	48
5.10.1 Trunk Status .....	48
5.10.2 Trunk Configuration .....	49
5.11 Port Mirroring .....	50
5.12 SNMP .....	51
5.12.1 SNMP Agent .....	51
5.12.2 SNMP Trap Setting .....	53
5.13 DHCP Server / Rely .....	54
5.13.1 DHCP Client .....	55
5.13.2 DHCP Server .....	56
5.13.3 DHCP Server Binding .....	57

5.13.4 DHCP Relay .....	58
5.14 802.1X .....	59
5.14.1 802.1X Settings .....	59
5.14.2 Local Database .....	60
5.14.3 RADIUS Server.....	61
5.15 UPnP .....	62
5.15.1 UPnP .....	62
5.16 Modbus TCP .....	63
5.16.1 Enable Modbus TCP .....	63
5.16.2 MODBUS Data Map and Information .....	63
5.17 System Warning .....	69
5.17.1 Syslog Setting .....	69
5.17.2 System Event Log .....	70
5.17.3 SMTP Setting.....	71
5.17.4 Event Selection.....	72
5.17.5 Fault Alarm .....	73
5.18 MAC Table .....	73
5.18.1 MAC Address Table .....	73
5.18.2 MAC Table Configuration .....	74
5.19 Maintenance .....	74
5.19.1 Upgrade.....	74
5.19.2 Reboot.....	75

5.19.3 Default.....	75
5.20 Configuration	76
5.20.1 Save .....	76
5.20.2 Backup & Restore .....	76
5.20.3 Auto Load & Backup.....	77
5.21 Logout	78
<b>6. Command Line Interface Management .....</b>	<b>79</b>
6.1 About CLI Management.....	79
<b>7. Technical Specifications .....</b>	<b>100</b>



# 1. Introduction

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

## 1.1 Product Overview

**Antaira's LMP-0600-24 series** is a 6-port industrial PoE+ managed Ethernet switch embedded with 6\*10/100Tx Ethernet ports that support 4\*PoE+ ports that are IEEE802.3at/af compliant with a maximum of 30W/port. The LMP-0600-24 series is a fully manageable Layer 2 Ethernet switch that is pre-loaded with a user-friendly web management console design. It supports the ring network redundancy function using the market's open standard ITU-T G.8032 ERPS (Ethernet Ring Protection Switch) protocol that has a <50ms network recovery time. The advanced network filtering and security functions, such as, IGMP, VLAN, QoS, SNMP, port lock, RMON, Modbus TCP, and 802.1X/HTTPS/SSH/SSL increase determinism and improve network management for remote SCADA systems or control networks.

The LMP-0600-24 series is IP30 rated and DIN-rail mountable. There are also two wide operating temperature models for either a standard temperature range (STD: -10°C to 70°C) or an extended temperature range (EOT: -40°C to 75°C). This series supports a dual power input having a low voltage range (12~36VDC) and a built-in voltage booster allowing the unit to give a full 48VDC PoE power for any mobile PoE application or any low voltage power sourcing environment. It also provides high EFT and ESD protection for industrial networking applications, such as, power/utility, water wastewater, oil/gas/mining, factory automation, security surveillance within transportation, ITS and any other 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/v3, Serial Console
  - Qos, traffic classification QoS, Cos, bandwidth control for Ingress and Egress, broadcast storm control, Diffserv

- IEEE802.1q VLAN tagging, port-based VLAN support
- IGMP snooping v1/v2, IGMP filtering / throttling, IGMP query up to 256 group
- Supports IPv4/IPv6, RMON, MIB II, port mirroring, event syslog, DNS, NTP/SNTP, HTTPS, SSH/SSL, TFTP
- MODBUS TCP for SCADA system integration
- Port Configuration
  - Status, statistics, mirroring, rate limiting, event syslog
- Event Handling
  - Event notification by Email: Cold/Warm Start, Power Failure, Authentication, SNMP trap and Fault Alarm Relay Output
- Software Upgrade via TFTP and HTTP
- Configuration Backup – USB Port

## 1.3 Product Hardware Features

- System Interface and Performance
  - All RJ-45 ports support Auto MDI Function
  - Embedded 6\*10/100Tx (w/4\*PoE Ports: 30W/Port) RJ45 Ports
  - Store-and-forward switching architecture
  - 8K MAC address table
  - Power line EFT protection: 2,000VDC; Ethernet ESD protection: 6,000VDC
- Power Input
  - DC 12~36V redundant with a 6-pin removal terminal block
  - One user programmable alarm relay contact
- Operating Temperature
  - Standard operating temperature models: -10°C to 70°C
  - Extended operating temperature models: -40°C to 75°C
- Case/Installation
  - IP-30 protection metal housing
  - DIN-Rail and wall mount design

## 1.4 Package Contents

- 1– LMP-0600-24 series: 6-port industrial PoE+ managed Ethernet switch, with 6\*10/100Tx (w/4\*PoE Ports: 30W/Port); 12~36VDC power input
- 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-0600-24 series: 6-port industrial PoE+ managed Ethernet switches with 6\*10/100Tx (w/4\*PoE Ports: 30W/Port); 12~36VDC input (w/voltage booster).

(W x D x H) is **54mm x 99mm x 142mm**

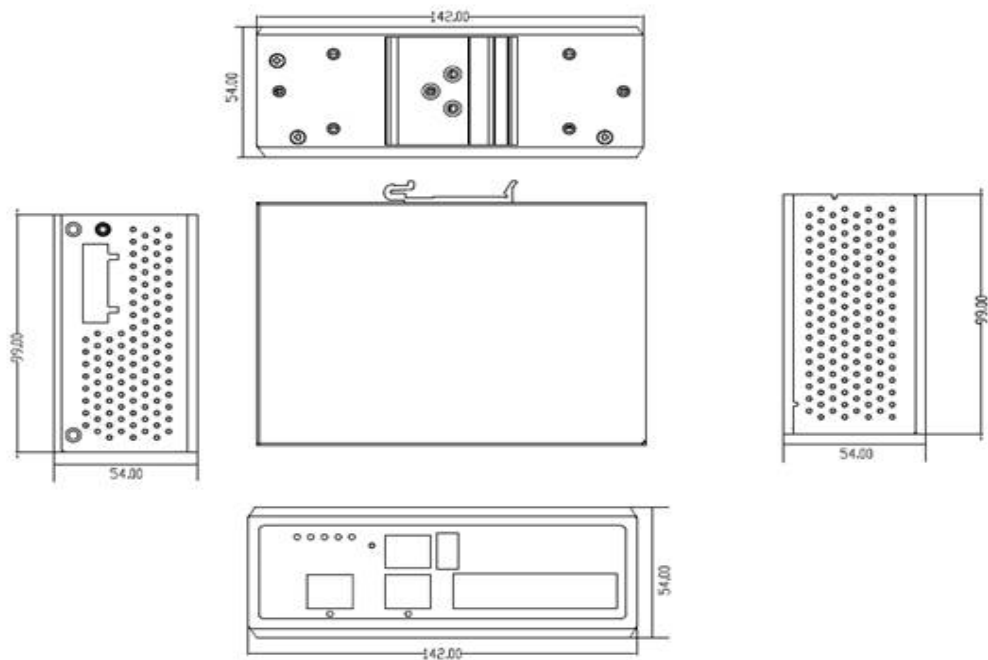


Figure2.1

LMP-0600-24 Series Physical Dimensions

## 2.2 Front Panel

The front panel of the LMP-0600-24 series industrial PoE+ managed Ethernet switch is shown below in *Figure 2.2*.

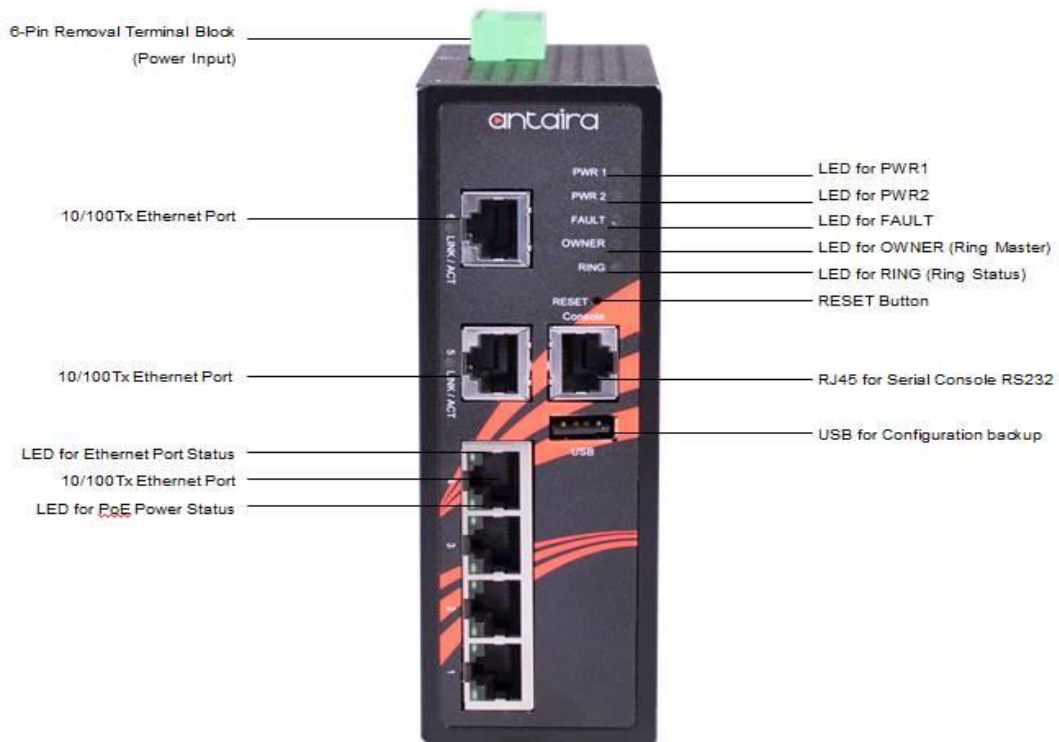


Figure2.2 - The Front Panel of LMP-0600-24 Series

## 2.3 Top View

*Figure 2.3*, below, shows the top panel of the LMP-0600-24 series switch that is equipped with one 6-pin removal terminal block connector for dual DC power inputs 12~36VDC.

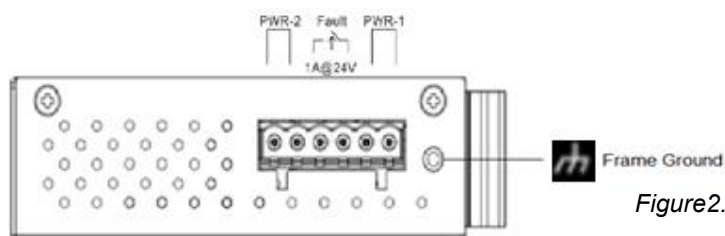




Figure2.3

Top Panel View of LMP-0600-24 Series

## 2.4 LED Indicators

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

LED	Color	Description	
P1	Green	On	Power input 1 is active
		Off	Power input 1 is inactive
P2	Green	On	Power input 2 is active
		Off	Power input 2 is inactive
Fault	Red	On	Power input 1 or 2 is inactive
		Off	Power input 1 and 2 are both functional, or no power, inputs/ports link is active/port alarm is disabled
Owner	Green	On	ERPS Owner Mode (Ring Master) is ready
		Off	ERPS Owner Mode is not active
Ring	Green	On	Ring Network is active
		Off	Ring Network is not active
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~ 6 (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-0600-24 Series*

## 2.5 Reset Button

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

Seconds	Function
1	Save running configuration to USB
4-6	Reboot the switch
7 or more	Restore factory default

*Table 2.2 – Reset Button Functions*

## 2.6 Ethernet Ports

### ■ RJ-45 Ports

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

### ■ RJ-45 Pin Assignments

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

Table 2.3 - RJ45 Pin Assignments

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

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

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

Table 2.4 - Ethernet Signal Pin

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

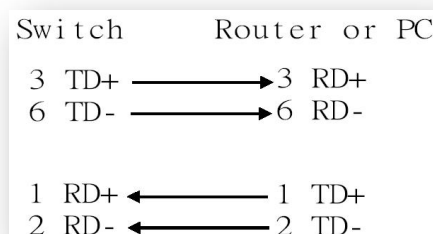


Figure 2.4  
Straight-Through Cable Schematic

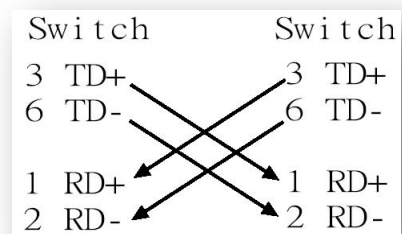


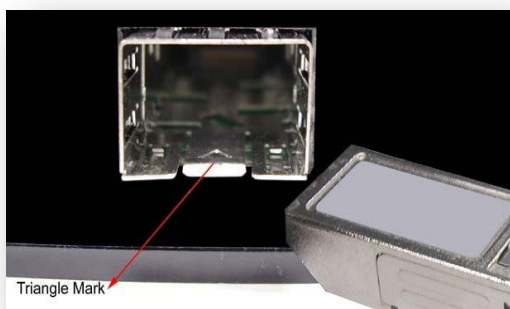
Figure 2.5  
Crossover Cable Schematic

## 2.7 Cabling

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

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

First, insert the SFP transceiver module into the SFP slot as shown below in *Figure 2.7*. Notice that the triangle mark is at the bottom of the SFP slot. *Figure 2.8* shows that the SFP transceiver module has been inserted.

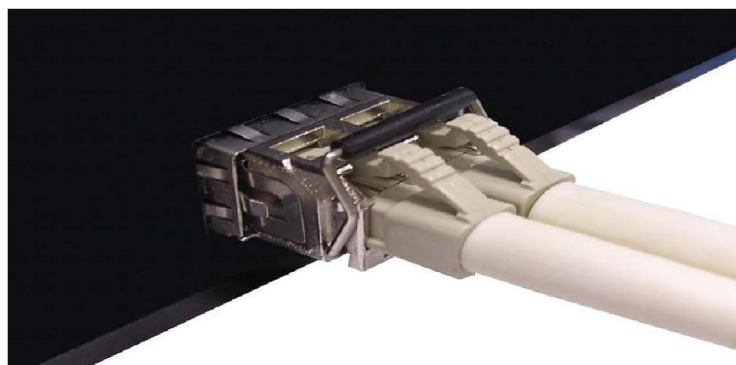


*Figure 2.6 - Transceiver to the SFP Module*



*Figure 2.7 - Transceiver Inserted*

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

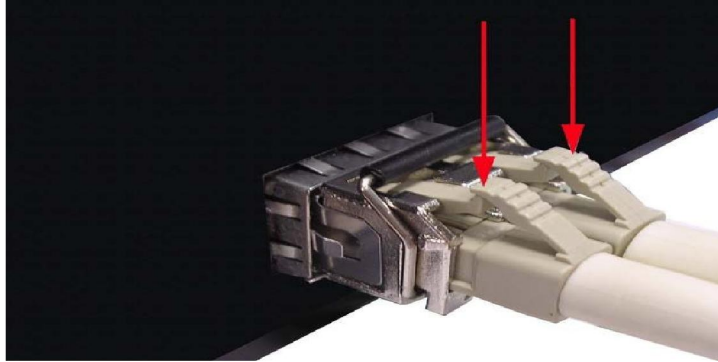


*Figure 2.8 - LC Connector to the Transceiver*



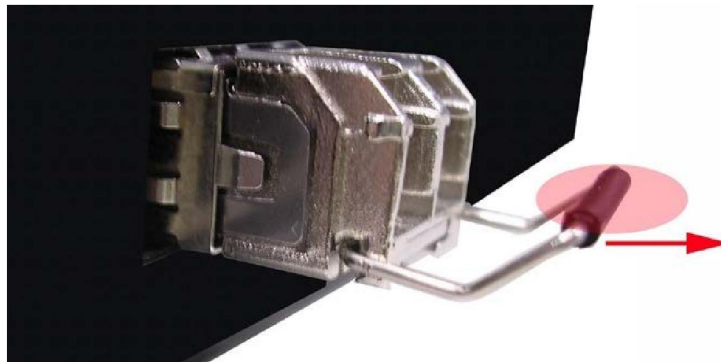
To remove the LC connector from the transceiver, please follow the steps shown below:

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



*Figure 2.9*  
*Remove LC Connector*

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



*Figure 2.10*  
*Pull Out from the SFP Module*

## 2.8 Wiring the Power Inputs

Please follow the steps below when inserting the power wire.

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

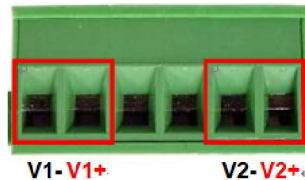


Figure 2.11 - Power Terminal Block

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

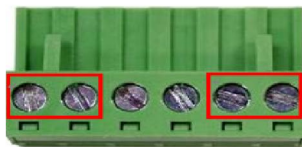


Figure 2.12 - Power Terminal Block

### Note

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

## 2.9 Wiring the Fault Alarm Contact

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

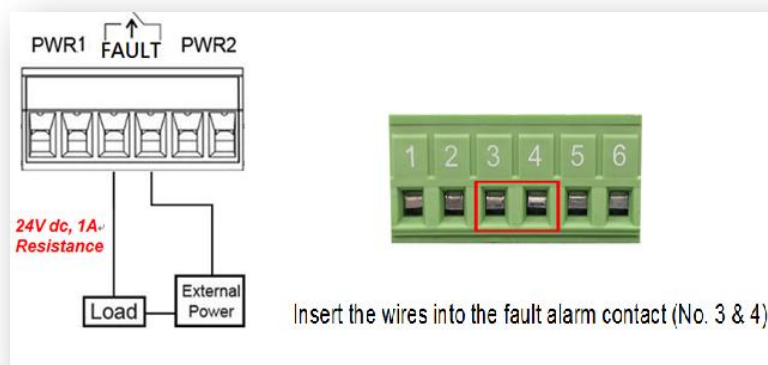


Figure 2.13 - Wiring the Fault Alarm Contact

### Note

- The wire gauge for the terminal block should range between 12 ~ 24AWG

## 3. Mounting Installation

### 3.1 DIN-Rail Mounting

The DIN-Rail is pre-installed on the industrial Ethernet switch from the factory. If the DIN-Rail is not on the industrial Ethernet switch, please see Figure 3.1 to learn how to install the DIN-Rail on the switch.

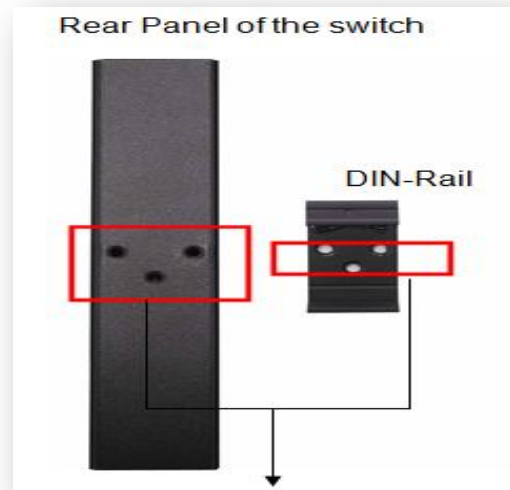


Figure 3.1

*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.

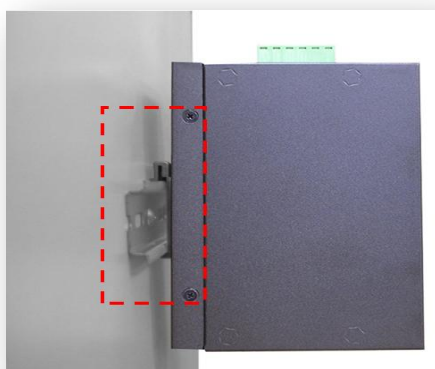


Figure 3.2

*Insert the Switch on the DIN-Rail*



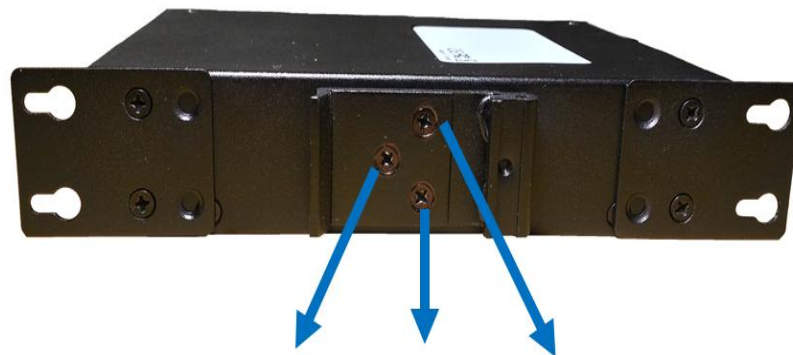
Figure 3.3

*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*.

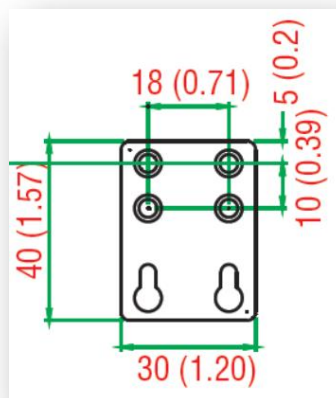
1. Remove the DIN-Rail bracket from the industrial Ethernet switch by loosening the screws.
2. Place the wall mounting brackets on the top and bottom of the industrial Ethernet switch.
3. Use the screws to screw the wall mounting bracket on the industrial Ethernet switch.
4. Use the hook holes at the 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-0600-24 series: 6-Ports industrial PoE+ managed Ethernet switches with 6\*10/100Tx (w/4\*PoE Ports: 30W/Port); 12~36VDC input (w/Voltage Booster).

#### 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".

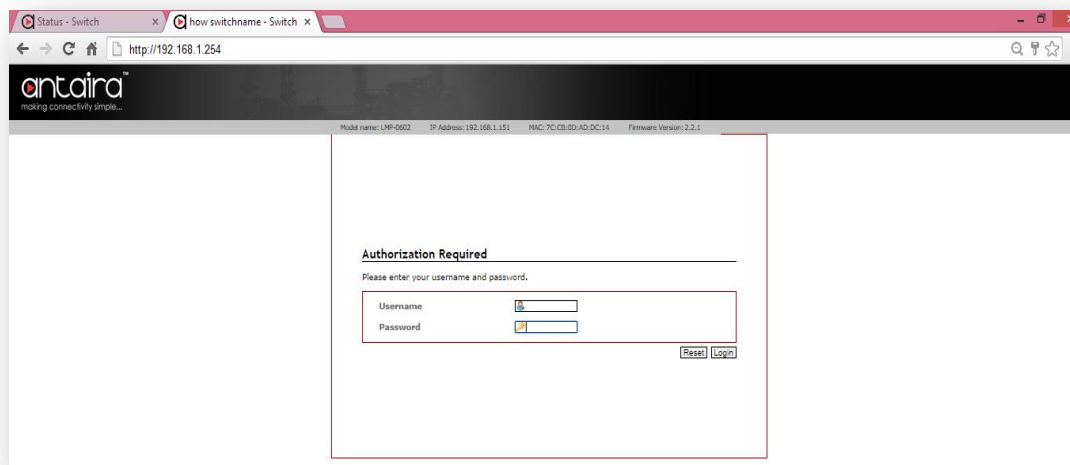


Figure 5.1 - Web Console "Login"

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.

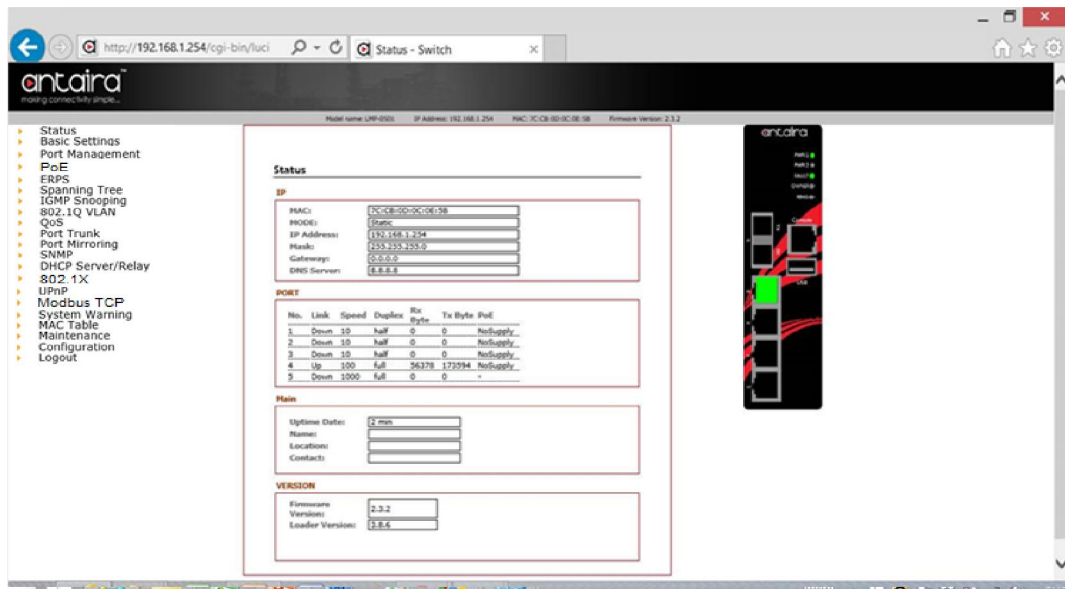


Figure 5.2 - Web Console Main (Status) Page

## 5.2 Basic Setting

### 5.2.1 System Information

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

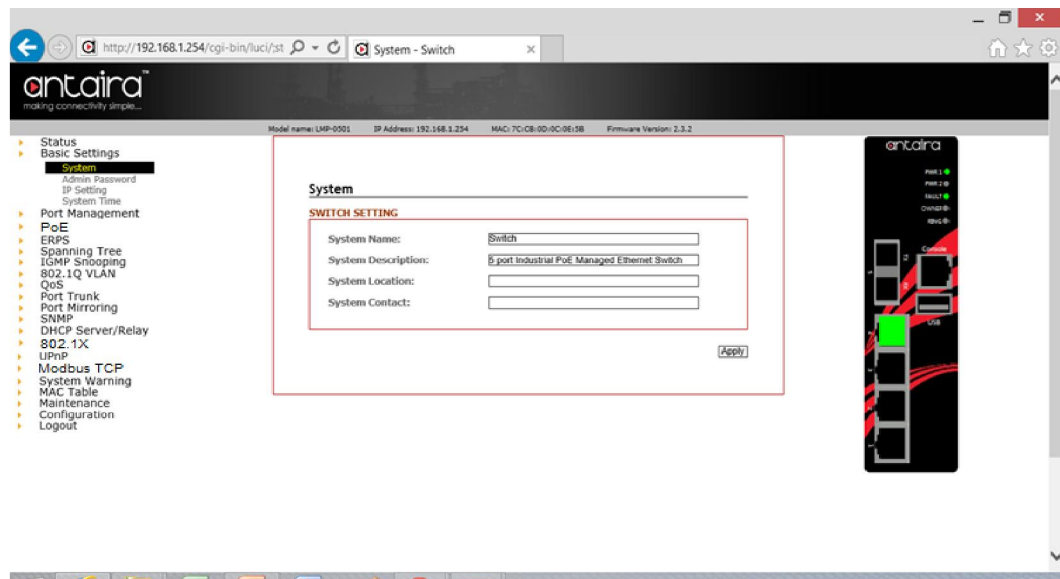


Figure 5.3 – Switch Settings (Status) Page


Terms	Value Description
<b>System Name</b>	<p>Factory Default: Switch</p> <p>*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.</p>
<b>System Description</b>	<p>Factory Default: 6-port Managed PoE Ethernet Switch</p> <p>* Users can assign any new name label to describe this PoE Managed Switch.</p>
<b>System Location</b>	<p>Factory Default: blank</p> <p>*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.</p>
<b>System Contact</b>	<p>Factory Default: blank</p> <p>*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.</p>
	Click the “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.

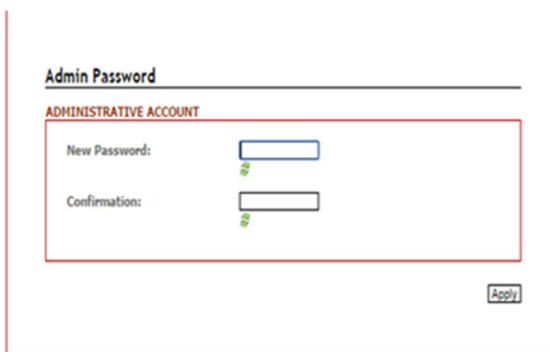


Figure 5.5 – Administrative Account




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

Figure 5.6 – Admin &amp; Password Description

### 5.2.3 IP Setting

Configure the managed switch’s IP setting information.

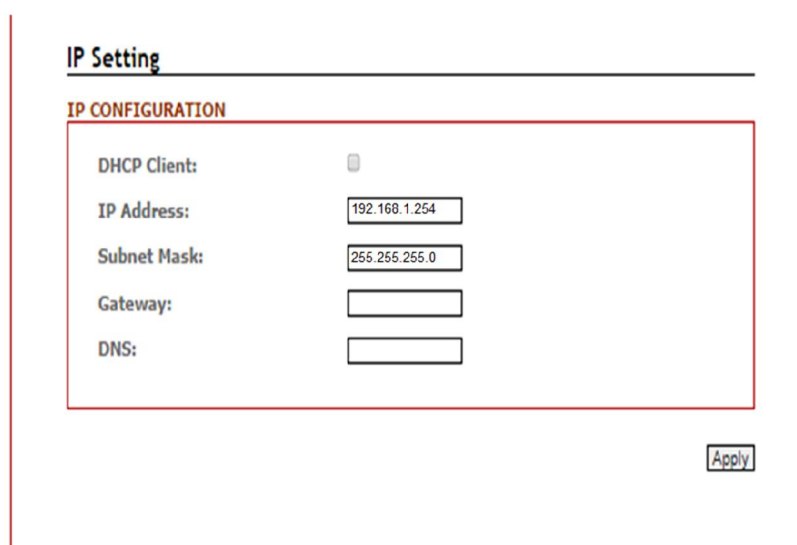


Figure 5.7 – IP Setting Information

Terms	Value Description
<b>DHCP Client</b>	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.
<b>IP Address</b>	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.


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

Figure 5.8 – IP Setting Information Description

## 5.2.4 IPv6 Neighbor Cache

The following information provides the current IPv6 neighbors and their states.

### IPv6 Neighbor Cache

#### IPv6 NEIGHBOR CACHE

IPv6 Address	Link Layer(MAC)	Address State
fe80::7941:e3ea:d701:a7cd	c4:6e:1f:03:1e:5a	REACHABLE

Figure 5.9 – IPv6 Neighbor Cache Status

## 5.2.5 IPv6 Settings

### IPv6 Address

#### IPv6 ENABLE

IPv6 Enable:



#### IPv6 CONFIGURATION

IPv6 Address

IPv6 Length Prefix

 Delete Add

Figure 5.10 – IPv6 Settings


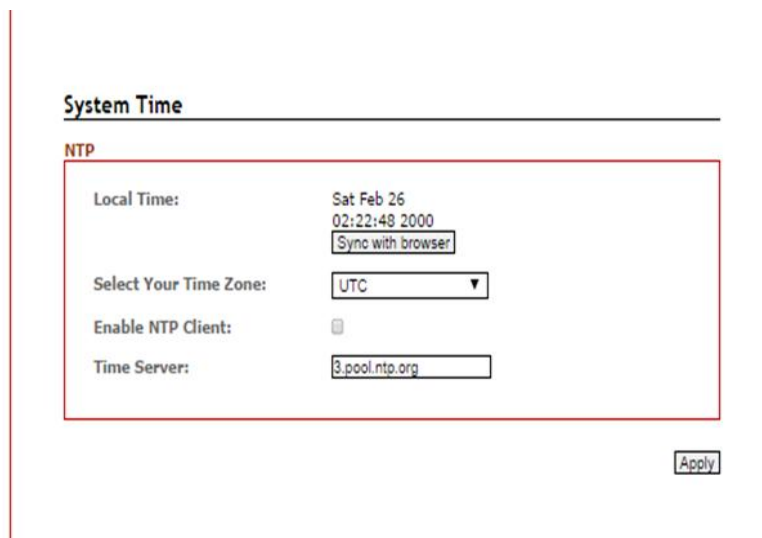
Terms	Value Description
<b>IPv6 Enable/Disable</b>	Check or uncheck the box to enable or disable IPv6 settings
<b>IPv6 Address</b>	The unit default IPv6 address is depended on MAC address. Assign the IPv6 address that the network is using. Users can add more than one IPv6 addresses.
<b>IPv6 Length Prefix</b>	The prefix length of this IPv6 address
	Click the “Apply” to save changes.

Figure 5.11 – IPv6 Terms and Value Description

## 5.2.6 System Time



**System Time**

**NTP**

Local Time: Sat Feb 26 02:22:48 2000

Select Your Time Zone: UTC ▼

Enable NTP Client: ☐

Time Server: 3.pool.ntp.org

Figure 5.12 – System Time Settings


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

Figure 5.13 – System Time Settings Description

## 5.3 Port Management

### 5.3.1 Port Status

The following information provides the current port status.

Status						
PORT						
No.	Link	Speed	Duplex	Rx Byte	Tx Byte	PoE
1	Down	10	half	0	0	NoSupply
2	Up	100	full	31913127	640601	NoSupply
3	Down	10	half	0	0	NoSupply
4	Down	10	half	28784	1596	NoSupply
5	Down	100	full	0	0	-
6	Down	100	full	0	0	-

Figure 5.14 – 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.

Port Configuration					
PORT					
No.	Link	Port name:	Status	Speed/Duplex	Flow control
1	Down	<input type="text"/>	Enable ▼	Auto ▼	<input type="checkbox"/>
2	Up	<input type="text"/>	Enable ▼	Auto ▼	<input type="checkbox"/>
3	Down	<input type="text"/>	Enable ▼	Auto ▼	<input type="checkbox"/>
4	Down	<input type="text"/>	Enable ▼	Auto ▼	<input type="checkbox"/>
5	Down	<input type="text"/>	Enable ▼		<input type="checkbox"/>
6	Down	<input type="text"/>	Enable ▼		<input type="checkbox"/>

Figure 5.15 – Port Configuration Interface



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

Figure 5.16 – Port Configuration Description

## 5.4 PoE (Power-over-Ethernet)

LMP-0600-24 series is one of Antaira's industrial PoE+ gigabit managed switches that has four built-in IEEE802.3at complaint ports, and each PoE port can 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

#### POE Configuration

**PoE PORT**

No.	Status	Mode	Consumption
1	No PD Detected	Enable ▼	0.00W
2	No PD Detected	Enable ▼	0.00W
3	No PD Detected	Enable ▼	0.00W
4	No PD Detected	Enable ▼	0.00W

Apply

Figure 5.17 – PoE Port Configuration Interface

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

Figure 5.18 – 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.

The screenshot displays the 'Power over Ethernet' configuration page. Under the 'PoE KEEPALIVE' section, there is a table with three columns: 'PD', 'IP Address', and 'Cycle Time(s)'. The table has four rows, numbered 1 to 4. Each row contains input fields for the IP address and cycle time. Below the table, there is an 'Apply' button.

PD	IP Address	Cycle Time(s)
1		
2		
3		
4		

Apply

Figure 5.19 – 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.

The screenshot displays the 'Power over Ethernet' configuration page, specifically the 'PoE SCHEDULE' section. At the top, there are four tabs labeled 'Port1', 'Port2', 'Port3', and 'Port4'. Below the tabs, the interface is organized into sections for each day of the week, starting with 'Monday Enable'. Each day section contains a checkbox to enable PoE for that day, followed by 'Start time(hour):' and 'End time(hour):' dropdown menus. The 'Monday Enable' section shows the start time set to 0. The 'Tuesday Enable' section shows the start time set to 0. The 'Wednesday Enable' section shows the start time set to 0. The 'Thursday Enable' section shows the start time set to 0. The interface is designed to allow users to configure PoE scheduling for each of the four ports.

Figure 5.20 – PoE Schedule Interface

## 5.5 ERPS

In any industrial automation application, designing redundant ring network paths to protect networks from unexpected failovers is extremely important in mission-critical networks because they 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) is 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 compatibility issues when 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 5.21*, shows the network redundancy ring status with the Ethernet Ring Protection Switch (ERPS) protocol.

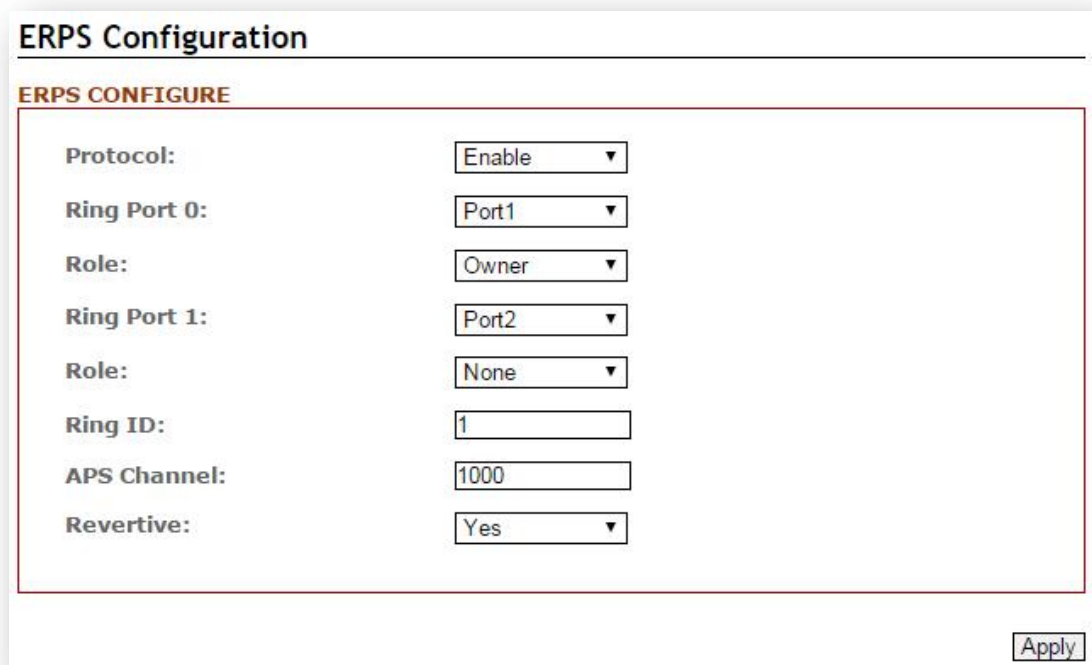


ERPS Status	
Protocol:	Disable
Ring ID:	1
Ring State:	Normal
Node State:	INITIAL STATE
Channel:	1000
Revertive:	Enable

*Figure 5.21 – Redundant Ring Network – ERPS Status*

### 5.5.2 ERPS Configuration

Below, *Figure 5.22* shows the ERPS configuration interface.



ERPS CONFIGURE	
Protocol:	Enable ▼
Ring Port 0:	Port1 ▼
Role:	Owner ▼
Ring Port 1:	Port2 ▼
Role:	None ▼
Ring ID:	1
APS Channel:	1000
Revertive:	Yes ▼

Apply

*Figure 5.22 – ERPS Configuration Interface*


Terms	Value Description
<b>Protocol</b>	“Enable” or “Disable” ERPS protocol
<b>Ring Port 0</b>	ERPS ring port 0, it could be map to real switch port 1 – port 6. Do not set the same as Ring port 1.
<b>Ring Port 1</b>	ERPS ring port 1, it could be map to real switch port 1 – port 6. Do not set the same as Ring port 0.
<b>Role</b>	Set the ERPS role as Owner, Neighbor or None. <b>[Owner]</b> In charge of blocking one side of RPL link. It will prevent the packet flow from its blocked port. <b>[Neighbor]</b> In charge of blocking one side of RPL link. It will prevent the packet flow from its blocked port. <b>[None]</b> Besides Owner and Neighbor node, the rest of nodes are defined as None node. All node roles have the ability to block the port if the link attach to the port is failed and disconnected.
<b>Ring ID</b>	ERPS ring ID, ranges from 1 to 239. Ring ID distinguishes different Ring topology.
<b>Channel</b>	ERPS Channel ID, ranges from 1 to 4094. It's a channel to send PDUs of ERPS.
<b>Revertive</b>	Set to Revertive (yes) or Non-revertive (no). The revertive mode works only under the scenario A at the RPL Owner node. <b>[Revertive]</b> 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. <b>[Non-Revertive]</b> The failed ring link the port attached to it will remain blocked even the situation is eliminated.
	Click the “Apply” button to save changes.

Figure 5.23 – ERPS Configuration Terms &amp; Description

### 5.5.3 Before Configuring ERPS

Before configuring ERPS, the rapid spanning tree protocol (RSTP), or multiple spanning tree protocol is required to be 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 shown below in *Figure 5.24*.

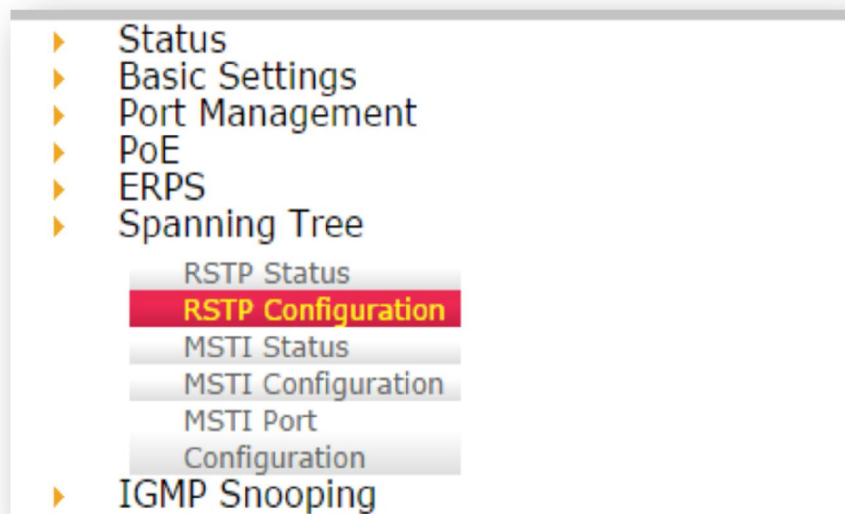


Figure 5.24 – Spanning Tree Manual

- Step 3:** When the RSTP/CIST Configuration page shows up, set “Mode” to “Disable” as shown in *Figure 5.25*.

A screenshot of the 'RSTP/CIST Configuration' web page. The page has a title bar at the top. Below the title, there is a section labeled 'RSTP/CIST'. Inside this section, there are several configuration fields. The first field is 'Mode:', which has a dropdown menu. The dropdown menu is open, showing three options: 'RSTP', 'MSTP', and 'Disable'. The 'Disable' option is currently selected and highlighted in blue. Below the 'Mode' field are four other fields: 'Root Priority:', 'Root Hello Time:', 'Root Forward Delay:', and 'Root Maximum Age:'. Each of these fields has a corresponding input box with numerical values: 2, 15, and 20 respectively. The 'Root Priority' field is currently empty.

Figure 5.25 – RSTP/CIST Configuration Interface

**Step 4:** Press the Apply button in the lower right corner as shown below in *Figure 5.26*.

**RSTP/CIST Configuration**

**RSTP/CIST**

Mode: RSTP ▼  
 Root Priority: RSTP ▼  
 Root Hello Time: MSTP ▼  
 Root Forward Delay: Disable ▼  
 Root Maximum Age: 2 ▼

**RSTP/CIST PORT**

No.	Path Cost(0:Auto,1-200000000)	Priority	Admin P2P	Auto Edge	Admin Non STP
1	0	128 ▼	True ▼	Auto ▼	False ▼
2	0	128 ▼	True ▼	Auto ▼	False ▼
3	0	128 ▼	True ▼	Auto ▼	False ▼
4	0	128 ▼	True ▼	Auto ▼	False ▼
5	0	128 ▼	True ▼	Auto ▼	False ▼
6	0	128 ▼	True ▼	Auto ▼	False ▼

**Apply**

*Figure 5.26 – 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 “None Node”.

Below are two scenarios describing how to configure the ERPS in Antaira’s industrial managed Ethernet switches. Users can reference it to configure the managed switch as RPL-configured architecture as shown in *Figure 5.27* or Non-configure architecture shown in *Figure 5.31*.

### 5.5.3.1 Scenario A – RPL Configured Architecture

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

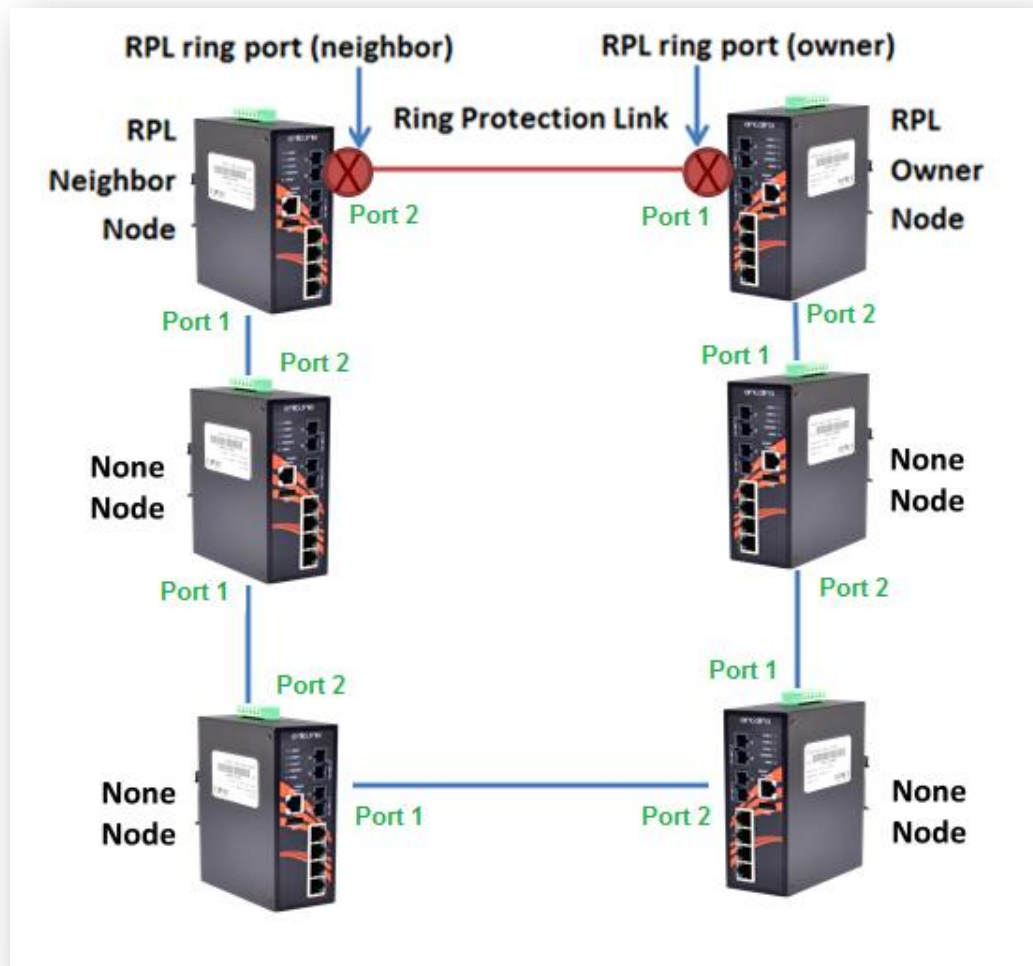


Figure 5.27 – RPL-Configured Architecture

**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]**

Only one RPL Owner Node can be set in a ring network. In order to set up the RPL Owner Node, one must choose a switch and enable the “Protocol” under the ERPS Configuration interface. Follow the steps below and use *Figure 5.28* as an example:

- Step 1:** Choose a specific port from the dropdown menu, next to “ring port 0”, and set it as the “Owner” node by clicking the dropdown menu next to “Role”. At this point, “**Port 1**” has been chosen as an example.
- Step 2:** Choose a specific port from the dropdown menu, next to “ring port 1”, then set it as “None” from the dropdown menu next to “Role” (which locates below “ring port 1”). At this point, “**Port 2**” has been chosen as an 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 settings.

The screenshot displays the 'ERPS Configuration' window. At the top, it says 'ERPS CONFIGURE'. Below this, there are several configuration fields:

Protocol:	Enable
Ring Port 0:	Port1
Role:	Owner
Ring Port 1:	Port2
Role:	None
Ring ID:	1
APS Channel:	1000
Revertive:	Yes

An 'Apply' button is located at the bottom right corner of the configuration area.

*Figure 5.28 – RPL Owner Node Setup Example*

Please be aware, when the revertive mode is set to “**Yes**”, the ring will recover the same way as explained in *Figure 5.27*, after the ring state form goes from 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 "None" 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 5.29*. 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.

The screenshot displays the 'ERPS Configuration' window. At the top, it says 'ERPS CONFIGURE'. Below this, there are several configuration fields:

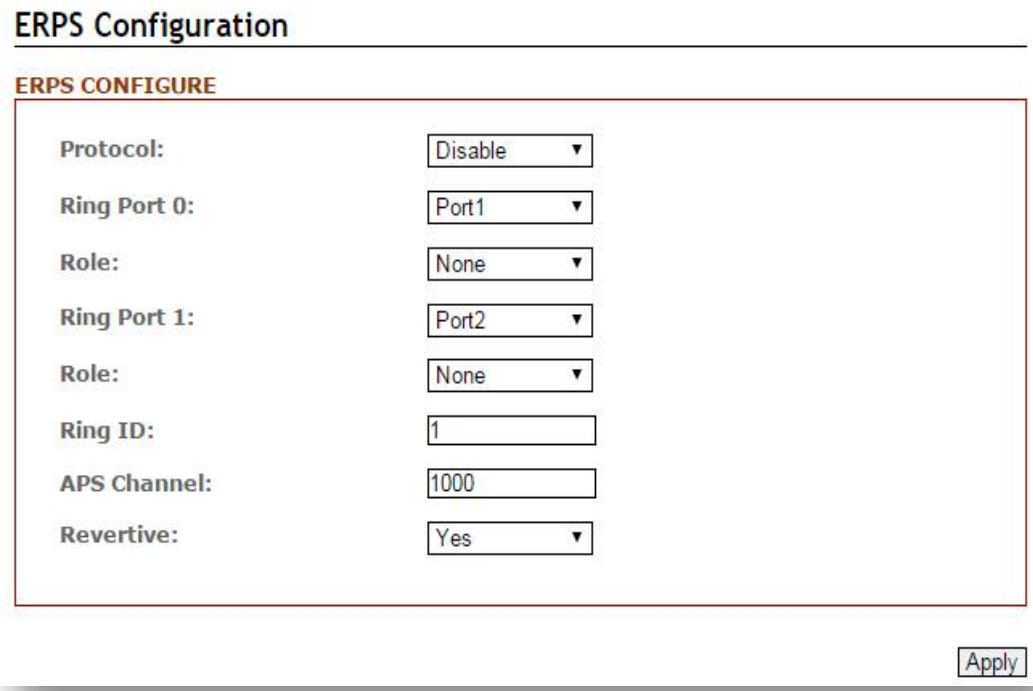
Protocol:	Enable ▼
Ring Port 0:	Port1 ▼
Role:	None ▼
Ring Port 1:	Port2 ▼
Role:	Neighbor ▼
Ring ID:	1
APS Channel:	1000
Revertive:	Yes ▼

An 'Apply' button is located at the bottom right corner of the configuration area.

*Figure 5.29 – RPL Neighbor Node Setup Example*

**[None Node]**

Then users should setup the rest of the managed switches' "Role" of both "Ring Port 0 and 1" as "None 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.



The screenshot shows a web-based configuration interface for ERPS. The main title is "ERPS Configuration". Below it, there is a section titled "ERPS CONFIGURE" in red. This section contains several configuration fields:

Field	Value
Protocol:	Disable
Ring Port 0:	Port1
Role:	None
Ring Port 1:	Port2
Role:	None
Ring ID:	1
APS Channel:	1000
Revertive:	Yes

An "Apply" button is located at the bottom right of the configuration area.

*Figure 5.30 – RPL None 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 can still work well under the mechanism by blocking one of the ring ports in the ERPS ring topology.

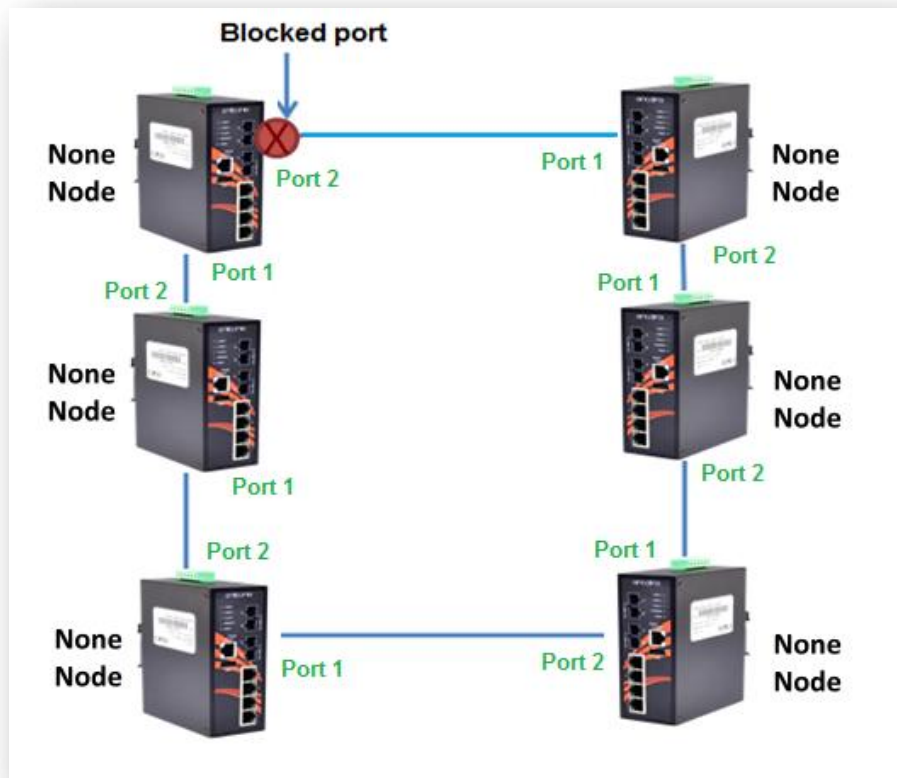


Figure 5.31 – Non-Configured Architecture

**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.

Shown above in Figure 5.31, 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 5.32, below, shows the configurations as a reference.

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

### ERPS Configuration

---

#### ERPS CONFIGURE

Protocol:	Disable ▼
Ring Port 0:	Port1 ▼
Role:	None ▼
Ring Port 1:	Port2 ▼
Role:	None ▼
Ring ID:	1
APS Channel:	1000
Revertive:	Yes ▼

Apply

Figure 5.32 – 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

Figure 5.33 shows the RSTP algorithm results.

## RSTP/CIST Status

---

### Root Status

Bridge ID:	8.000.7C:CB:0D:AD:DC:14
Root Priority:	32768
Root Port:	lan2 (#2)
Root Path Cost:	0
Hello Time:	2
Forward Delay:	15
Max Age:	20

### RSTP/CIST Port Status

No.	Role	Path State	Port Cost	Port Priority	Oper P2P	Oper Edge
1	Disabled	Discarding	200000000	128	Shared	Non-Edge
2	Root	Forwarding	200000	128	Shared	Non-Edge
3	Disabled	Discarding	200000000	128	Shared	Non-Edge
4	Disabled	Discarding	200000	128	Shared	Non-Edge
5	Disabled	Discarding	200000000	128	Shared	Non-Edge
6	Disabled	Discarding	200000000	128	Shared	Non-Edge

Figure 5.33 – RSTP Information Interface

## 5.6.2 RSTP Configuration

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

**RSTP/CIST Configuration**

**RSTP/CIST**

Mode:

Root Priority:

Root Hello Time:

Root Forward Delay:

Root Maximum Age:

**RSTP/CIST PORT**

No.	Path Cost(0:Auto,1-200000000)	Priority	Admin P2P	Auto Edge	Admin Non STP
1	0	128	True	Auto	False
2	0	128	True	Auto	False
3	0	128	True	Auto	False
4	0	128	True	Auto	False
5	0	128	True	Auto	False
6	0	128	True	Auto	False

Apply

Figure 5.34 – RSTP Configuration Interface

Terms	Value Description
<b>Mode</b>	Users can select RSTP or MSTP function to be enabled or disabled before configuring the related parameters.
<b>Root Priority (0~61440)</b>	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.
<b>Root Hello Time (1~10)</b>	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.
<b>Root Forward Delay (4~30)</b>	Enter a value between 4 through 30 as the number of seconds for a port to wait before changing from its RSTP learning and listening states to the forwarding state.
<b>Root Maximum Age (6~40)</b>	Enter a value between 6 through 40 as the number of seconds a bridge waits without receiving STP configuration messages before attempting a


	reconfiguration.
<b>Path Cost (0~200000000)</b>	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.
<b>Priority (0~240)</b>	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
<b>Admin P2P</b>	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.
<b>Auto Edge</b>	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 " <b>True</b> ".
<b>Admin Non STP</b>	The port includes the STP mathematic calculation. <b>True</b> is not including STP mathematic calculation. <b>False</b> is including the STP mathematic calculation.
	Click the "Apply" button to save changes.

Figure 5.35 – RSTP Configuration Terms &amp; 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.

**MSTI Status**

Instance ID: 1 ▼

**Root Status**

Root Address: .....  
 Root Priority: .....  
 Root Port: .....  
 Root Path Cost: .....

**MSTI Port Status**

No.	Role	Path State	Port Cost	Port Priority
1	.....	.....	.....	.....
2	.....	.....	.....	.....
3	.....	.....	.....	.....
4	.....	.....	.....	.....
5	.....	.....	.....	.....
6	.....	.....	.....	.....

Figure 5.36 – 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.

**MSTI Configuration**

**MSTI Configuration**

Name: 7C:CB:0D:AD:DC:14  
 Revision(0-65535): 0

**MSTI Instance**

Instance.	Vlan group	Priority
1	.....	32768 ▼
2	.....	32768 ▼
3	.....	32768 ▼
4	.....	32768 ▼
5	.....	32768 ▼
6	.....	32768 ▼
7	.....	32768 ▼
8	.....	32768 ▼
9	.....	32768 ▼
10	.....	32768 ▼
11	.....	32768 ▼
12	.....	32768 ▼
13	.....	32768 ▼
14	.....	32768 ▼
15	.....	32768 ▼

Figure 5.37 – MSTI Configuration Interface

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

Figure 5.38 – MTSI Configuration –Terms &amp; Value Description

**MTSI PORT**

Instance1 Instance2 Instance3 Instance4 Instance5 Instance6  
Instance7 Instance8 Instance9 Instance10 Instance11 Instance12  
Instance13 Instance14 Instance15

**Cost:**

Port1 0  
Port2 0  
Port3 0  
Port4 0  
Port5 0  
Port6 0

**Priority:**

Port1 128 ▼  
Port2 128 ▼  
Port3 128 ▼  
Port4 128 ▼  
Port5 128 ▼  
Port6 128 ▼

Apply

Figure 5.39 – MTSI Port Configuration Interface


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

Figure 5.40 – MSTI Port Configuration Terms & Value Description

## 5.7 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.



## 5.7.1 IGMP Settings

**IGMP Snooping Configuration**

**IGMP SNOOPING**

IGMP Snooping Enable: ☒

Querier Enable: ☐

Query Interval(s):

Query Max Response Time(s):

Figure 5.41 – IGMP Snooping Settings Interface

Terms	Value Description
<b>IGMP Protocol</b>	Check the box to enable or disable IGMP Snooping
<b>Querier</b>	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
<b>Query Interval</b>	The frequency at which the querier sends query messages
<b>Query Max Response Time</b>	The maximum response time advertised.
<input type="button" value="Apply"/>	Click the “Apply” button to save changes.

Figure 5.42 – IGMP Snooping Settings Terms & Value Description

## 5.7.2 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.

**IGMP Snooping Table**

**IGMP SNOOPING TABLE**

Group	Port
239.0.0.1	1,3
239.0.0.2	1
239.0.0.3	1

Figure 5.43 – IGMP Snooping Status Table

## 5.8 802.1Q VLAN

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which allows users to isolate network traffic. Only the members of the VLAN will receive traffic from the same members on that 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 physically plugged into the same switch.

All Antaira's industrial managed switches support 802.1Q VLAN. Tagged-based VLAN is an IEEE 802.1Q specification standard, and it is possible to create a VLAN across devices from different switch vendors. 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.

The managed switches also provide users with a defined management VLAN, so that users can connect an Antaira switch to other "commercial" switches that have existed and set a non VLAN 1 management VLAN.

### 5.8.1 802.1Q VLAN Settings

All of Antaira's industrial managed switches' have a default VLAN 1 setting set to "Untag" 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.

ID	name	1	2	3	4	5	6	
1		Untag	Untag	Untag	Untag	Untag	Untag	Delete
100		none	Untag	none	Tag	none	none	Delete

[Add](#) [Apply](#)

Figure 5.44 – 802.1Q VLAN Settings Interface

Terms	Value Description
<b>Management VLAN ID</b>	Set the VLAN ID of management VLAN. Users have to configure other settings done, and configure this field finally.
<b>802.1Q VLAN ID</b>	The ID of this VLAN. VLANs that have the same ID will consider being the same group.
<b>802.1Q VLAN Name</b>	The name of this VLAN. The same VLAN in the different switches can have different name.
<b>Apply</b>	Click the “Apply” button to save changes.

Figure 5.45 – 802.1Q VLAN Settings Terms

## 5.8.2 802.1Q VLAN Port Settings

**802.1Q VLAN Port**

**802.1Q VLAN PVID**

Port	PVID
1	1
2	1
3	1
4	1
5	1
6	1

**802.1Q VLAN FILTER**

Port	Filter
1	None
2	None
3	None
4	None
5	None
6	None

Apply

Figure 5.46 – 802.1Q VLAN Port Settings Interface


Terms	Value Description
<b>PVID</b>	When a frame comes into the port, it will be tagged with the PVID if the frame is without VLAN tag.
<b>Filter</b>	An incoming frame will be dropped or kept forwarding according to the filter. <ul style="list-style-type: none"><li>• None: All frames can keep forwarding.</li><li>• Tagged: Only the frames with 802.1Q tag can keep forwarding, untagged frames will be dropped.</li><li>• Untagged: Only the frames without 802.1Q tag can keep forwarding, tagged frames will be dropped.</li></ul>
	Click the “Apply” button to save changes.

Figure 5.47 – 802.1Q VLAN Settings Terms & Value Description

## 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

**Qos Classification**

**Qos Classification**

Queue Scheduling: Weighted ▼

Trust Mode: DSCP ▼

Port 1: DSCP ▼

Port 2: DSCP ▼

Port 3: DSCP ▼

Port 4: DSCP ▼

Port 5: DSCP ▼

Port 6: DSCP ▼

Default Cos: 0 ▼

Port 1: 0 ▼

Port 2: 0 ▼

Port 3: 0 ▼

Port 4: 0 ▼

Port 5: 0 ▼

Port 6: 0 ▼

Apply

Figure 5.48 – QoS Classification Interface

Terms	Value Description
<b>Queue Scheduling</b>	<p>Users can set it as “Weighted” or “Strict”</p> <p><b>Weighted Mode:</b> An 8, 4, 2, 1 weighting is applied to each round robin priority queue.</p> <p><b>Strict Mode:</b> It gives egress queues with higher priority to be transmitted first before lower priority queues are serviced.</p>
<b>Trust Mode</b>	<p>Users can select the trust mode with either DSCP or Cos.</p> <p>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.</p> <p><b>CoS:</b> (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</p> <p><b>Queues:</b> Highest, SecHigh, SecLow, and Lowest.</p>
<b>Default Cost</b>	<p>Users can set each port's priority queue from 0 to 7 by clicking from dropdown box; of which 0 is the Highest, and</p>

	7 is the Lowest
<b>Apply</b>	Click "Apply" button to save changes.

Figure 5.49 – QoS Classification Terms &amp; Value Description

## 5.9.2 CoS Mapping

**CoS Mapping**

**CoS Mapping**

CoS	Priority
0	Normal
1	Low
2	Low
3	Normal
4	Medium
5	Medium
6	High
7	High

**Apply**

Figure 5.50 – CoS Mapping Interface

Terms	Value Description
<b>CoS Value (0~7)</b>	Users 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.
<b>Apply</b>	Click the "Apply" button to save changes.

Figure 5.51 – QoS Mapping Terms &amp; 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).

**ToS Mapping**

**ToS Mapping**

ToS	Priority	ToS	Priority	ToS	Priority	ToS	Priority
0x00(0)	0(Low ▼)	0x40(16)	1(Nor ▼)	0x80(32)	2(Mec ▼)	0xC0(48)	3(High ▼)
0x04(1)	0(Low ▼)	0x44(17)	1(Nor ▼)	0x84(33)	2(Mec ▼)	0xC4(49)	3(High ▼)
0x08(2)	0(Low ▼)	0x48(18)	1(Nor ▼)	0x88(34)	2(Mec ▼)	0xC8(50)	3(High ▼)
0x0C(3)	0(Low ▼)	0x4C(19)	1(Nor ▼)	0x8C(35)	2(Mec ▼)	0xCC(51)	3(High ▼)
0x10(4)	0(Low ▼)	0x50(20)	1(Nor ▼)	0x90(36)	2(Mec ▼)	0xD0(52)	3(High ▼)
0x14(5)	0(Low ▼)	0x54(21)	1(Nor ▼)	0x94(37)	2(Mec ▼)	0xD4(53)	3(High ▼)
0x18(6)	0(Low ▼)	0x58(22)	1(Nor ▼)	0x98(38)	2(Mec ▼)	0xD8(54)	3(High ▼)
0x1C(7)	0(Low ▼)	0x5C(23)	1(Nor ▼)	0x9C(39)	2(Mec ▼)	0xDC(55)	3(High ▼)
0x20(8)	0(Low ▼)	0x60(24)	1(Nor ▼)	0xA0(40)	2(Mec ▼)	0xE0(56)	3(High ▼)
0x24(9)	0(Low ▼)	0x64(25)	1(Nor ▼)	0xA4(41)	2(Mec ▼)	0xE4(57)	3(High ▼)
0x28(10)	0(Low ▼)	0x68(26)	1(Nor ▼)	0xA8(42)	2(Mec ▼)	0xE8(58)	3(High ▼)
0x2C(11)	0(Low ▼)	0x6C(27)	1(Nor ▼)	0xAC(43)	2(Mec ▼)	0xEC(59)	3(High ▼)
0x30(12)	0(Low ▼)	0x70(28)	1(Nor ▼)	0xB0(44)	2(Mec ▼)	0xF0(60)	3(High ▼)
0x34(13)	0(Low ▼)	0x74(29)	1(Nor ▼)	0xB4(45)	2(Mec ▼)	0xF4(61)	3(High ▼)
0x38(14)	0(Low ▼)	0x78(30)	1(Nor ▼)	0xB8(46)	2(Mec ▼)	0xF8(62)	3(High ▼)
0x3C(15)	0(Low ▼)	0x7C(31)	1(Nor ▼)	0xBC(47)	2(Mec ▼)	0xFC(63)	3(High ▼)

Apply

Figure 5.52 – ToS Mapping Interface

Terms	Value Description
ToS	Users can assign each ToS value with 4 priority queues form 0 (Low) to 1 (Normal), 2 (Medium), and 3 (High).
<span style="border: 1px solid black; padding: 2px 5px;">Apply</span>	Click the “Apply” button to save changes.

Figure 5.53 – ToS Mapping Terms & Value Description

## 5.10 Port Trunk

Port Trunk, also called “Link Aggregation”, is a method of combining multiple network connections in parallel. It is to increase throughput beyond what a single connection could sustain. For example, if the application requires a 5-Gigabit link, and each port supports only 1-Gigabit link, the “Port Trunk” allows users to link 5 of 1-Gigabit ports to obtain a 5-Gigabit trunk feature. All Antaira’s industrial managed switches support 2 types of Port Trunk. One is LACP (dynamic) and the other is Static.

- LACP mode is more flexible, and it can change modes, either trunk or single port.
- Dynamic Port Trunk also provides a redundancy function, in case one of the links fail. If one of the trunk members has failed, it will still work well in LACP mode, but it will link down if using static mode. Static mode is still necessary, because some devices only support static trunk.

### 5.10.1 Trunk Status

The below graph is the Port Trunk Status.

Trunk Status		
AGGREGATION		
Group	Type	Port
1	lacp	1,2
2	-	-
3	-	-
4	lacp	3,5,6
5	-	-
6	-	-
7	-	-
8	-	-

Figure 5.54 – Port Trunk Status

The below table describes the term and value description of “Port Trunk”.

Terms	Value Description
Aggregation	Show the status of Port Trunk. List all Trunks and show their type and members.

Figure 5.55 – Port Trunk Terms and Value Description



## 5.10.2 Trunk Configuration

The below graph is the “Port Trunk” configuration interface.

**Trunk Configuration**

**AGGREGATION GROUP TYPE**

Group ID	Trunk Type
Trunk1	LACP
Trunk2	LACP
Trunk3	LACP
Trunk4	LACP
Trunk5	LACP
Trunk6	LACP
Trunk7	LACP
Trunk8	LACP

**AGGREGATION GROUP MEMBER**

PORT NO.	Group ID
Port1	Trunk 1
Port2	Trunk 1
Port3	None
Port4	None
Port5	None
Port6	None

Figure 5.56 – Port Trunk Configuration Interface

The below table describes the field of the terms and value descriptions of “Port Trunk”.

Terms	Value Description
Aggregation Group Type	Type “LACP” for dynamic trunking, and type “Static” for static trunking.
Aggregation Group Member	Map ports to Trunk1 ~ Trunk 8.

Figure 5.57 – Port Trunk Terms and Value Description

## 5.11 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.

**Port Mirroring**

**PORT MIRRORING**

Port Mirror Mode: ☐

Go To Interface: None ▼

Monitor Direction: None ▼

Source Port:

Port1 ☐

Port2 ☐

Port3 ☐

Port4 ☐

Port5 ☐

Port6 ☐

Apply

Figure 5.58 – Port Mirroring Configuration Interface

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

Figure 5.59 – Port Mirroring Terms & Value Description

## 5.12 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.

### 5.12.1 SNMP Agent

#### SNMP Agent

---

##### SNMP GENERAL

SNMP Version:	v1 , v2c , v3 ▼
Read-Only Community	public
Read and Write Community	private


##### SNMP v3

Admin Auth level:	Auth-only ▼
Admin Auth Type:	SHA ▼
Auth Passphrase	..... 
Admin Data Encrypt Type:	AES ▼
Encrypt Passphrase	..... 
User Auth level:	Auth-only ▼
User Auth Type:	SHA ▼
Auth Passphrase	..... 
User Data Encrypt Type:	AES ▼
Encrypt Passphrase	..... 

[Apply](#)

Figure 5.60 – SNMP Agent Setup Interface

**SNMP General**

Terms	Value Description
<b>SNMP Version</b>	All Antaira Managed Switches support SNMP v1, v2c, and v3 server. Users can enable all SNMP server v1, v2c and v3, or enable only v1 and v2c, or enable only enable v3. Default SNMP server is enabled, set version to "None" to disable it.
<b>Read-Only Community</b>	Using "Read-Only Community" on the SNMP MIB walk utility can only read information.
<b>Read and Write Community</b>	Using "Read and write Community" on the SNMP MIB walk utility not only can read information, but can write/edit part of information.
	Click the "Apply" button to save changes.

**SNMP V3**

There are 2 accounts when using SNMP v3 authentication. These 2 accounts are "admin" and "user". In this section, it introduces the authentication settings and encryption information.


Terms	Value Description
<b>Admin Auth level</b>	"Auth-only" means only do authentication but not encrypt data. "Both" means both do authentication and encrypt data. "None" means not do authentication and not encrypt data.
<b>Admin Auth Type</b>	The method used to encrypt the passphrase
<b>Auth Passphrase</b>	"Auth Passphrase" is a string used to authenticate (Admin).
<b>Admin Data Encrypt Type</b>	The method used to encrypt the data.
<b>Encrypt Passphrase</b>	"Encrypt Passphrase" is a string used to encrypt data (Admin).
<b>User Auth level</b>	"Auth-only" means only do authentication but not encrypt data. "Both" means both do authentication and encrypt data. "None" means not do authentication and not encrypt data.
<b>User Auth Type</b>	The method used to encrypt the passphrase
<b>Auth Passphrase</b>	"Auth Passphrase" is a string used to authenticate (User).
<b>User Data Encrypt Type</b>	The method used to encrypt the data.
<b>Encrypt Passphrase</b>	"Encrypt Passphrase" is a string used to encrypt data (User).
	Click the "Apply" button to save changes.

Figure 5.61 – SNMP Agent Interface Terms &amp; Value Description

## 5.12.2 SNMP Trap Setting

### Trap Setting

**SNMP**

Trap Mode:	None ▼
Inform Retry:	10
Inform Timeout:	30
Trap Destination IP:	
Community:	public

Figure 5.62 – SNMP Trap Setting

Terms	Value Description
<b>Trap Mode</b>	SNMP Trap is disabled (set to “None”) by default. Users can set it to “Trap v1”, “Trap v2c”, or “Inform (v2c)”. If users set it to “Trap”, the trap message will only send once, but if set the mode to “Inform”, the trap message will send “Inform Retry” times.
<b>Inform Retry</b>	The trap message will be sent “Inform Retry” times. This field works only when “Trap Mode” is set to “Inform”.
<b>Inform Timeout</b>	The trap message will be sent after “Inform Timeout” expired. This field works only when “Trap Mode” is set to “Inform”.
<b>Trap Destination IP</b>	The Destination IP that trap message will be sent to.
<input type="button" value="Apply"/>	Click “Apply” button to save changes.

Figure 5.63 – SNMP Trap Settings Terms &amp; Value Description

## 5.13 DHCP Server / Rely

### DHCP Client & Server

Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol. It is used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters. For example, devices can request IP addresses for interfaces from a DHCP server. Using DHCP can also reduce the need for a network administrator or a user to configure these settings manually.

The protocol operates based on the client-server model. When DHCP Clients connect to a network, they will send a broadcast query to request necessary information from a DHCP server. DHCP Servers manage a pool of IP address and network configuration information. If they get queries from DHCP Clients, they will automatically distribute IP address and network parameters to them.

### DHCP Relay Agent

DHCP Relay Agents help DHCP Clients forwarding request to DHCP Servers. With DHCP Relay Agents, DHCP Servers and Clients will not know each other. A Relay Agent can connect to more than 1 DHCP Server, so that DHCP Clients will have more resources.

### DHCP Relay Option 82

Users can also use the information of DHCP Relay Option 82 to distribute IP address. Antaira's industrial managed switches provides "Cisco-like" Option 82 format. It contains Circuit ID and Remote ID. The packets format of Circuit ID and Remote ID are shown below in Figure 5.64 and Figure 5.66; and the detail of packet fields are in Figure 5.65 and Figure 5.67. The IP addresses will get more controllable with DHCP Relay Option 82 function.

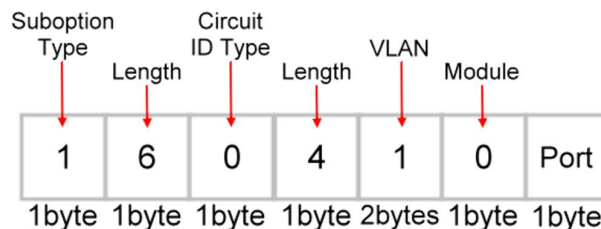


Figure 5.64 – DHCP Relay Option 82 Circuit ID

Field	Description
VLAN	The management VLAN ID. Always VLAN 1.
Module	The stack number. Always 0 here.
Port	It is the incoming port number from DHCP Client, and the port number is started by 1.

Figure 5.65 – DHCP Relay Option 82 Circuit ID Details

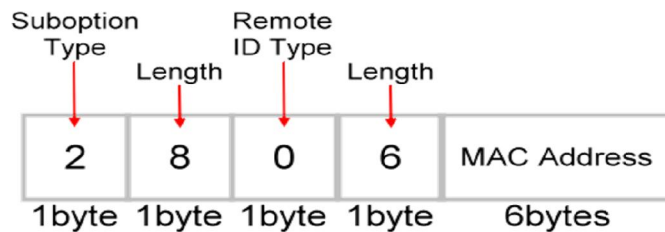


Figure 5.66 – DHCP Relay Option 82 Remote ID

Field	Description
MAC Address	The MAC address of the Relay Agent. The MAC address is all hex format and without ":" or "-", for example, "7CCB0AC49B2D".

Figure 5.67 – DHCP Relay Option 82 Remote ID Details

### 5.13.1 DHCP Client

The below figure is the IP Setting of DHCP Client.

The screenshot shows the 'IP Setting' configuration page. Under the 'IP CONFIGURATION' section, the following settings are visible:

- DHCP Client:** A checkbox that is currently unchecked.
- IP Address:** A text box containing '192.168.10.20'.
- Subnet Mask:** A text box containing '255.255.255.0'.
- Gateway:** An empty text box.
- DNS:** An empty text box.

An 'Apply' button is located at the bottom right of the configuration area.

Figure 5.68 – DHCP Client IP Configuration

The below table describes the field of the DHCP Client terms and value descriptions.

Terms	Value Description
DHCP Client	"Enable" or "Disable" DHCP Client.
IP Address	Static IP address setting. Assign the IP address that the network is using.
Subnet Mask	Assign the subnet mask of the IP address.
Gateway	The IP address that connects the LAN to the Internet.
DNS	The IP address of DNS.

Figure 5.69 – DHCP Client Terms and Value Description

### 5.13.2 DHCP Server

The below figure is the DHCP Server web interface.

The screenshot shows the 'DHCP Server' configuration page. At the top, the title 'DHCP Server' is displayed. Below it, the section 'DHCP SERVER' is highlighted. The configuration fields are as follows:

- Server Status:** Down
- Enable:** ☐
- Included Start Address:**
- Included End Address:**
- Default Gateway:**
- Name Server:**
- Lease Time:**

An 'Apply' button is located at the bottom right of the configuration area.

Figure 5.70 – DHCP Server Configuration

The below table describes the field of the DHCP Server terms and value description.

Terms	Value Description
Server Status	DHCP Server Status, It shows "Down" when "Disable", and it shows "Up" when "Enable".
Enable	"Enable" or "Disable" DHCP Server.
Included Start	The start address of the pool that DHCP Server managed.



Address	
Included End Address	The end address of the pool that DHCP Server managed.
Default Gateway	The IP address that connects the LAN to the Internet.
Name Server	The IP address of DNS.
Lease Time	A controllable time period that DHCP server will reclaim IP addresses.

Figure 5.71 – DHCP Server Terms and Value Description

### 5.13.3 DHCP Server Binding

The below figure is the web interface for DHCP Server Binding.

Figure 5.72 – DHCP Server Binding Interface

Terms	Value Description
ID	“Enable” or “Disable” DHCP Client.
Binding Mac	The MAC address of the device that wishes binding.
Binding IP	The IP address that will assign to the device with the Binding MAC address.

Figure 5.73 – DHCP Server Binding Terms and Value Description

### 5.13.4 DHCP Relay

#### DHCP Relay

##### DHCP RELAY

Enable:	<input type="checkbox"/>
Relay option82:	<input type="checkbox"/>
Relay to server1:	<input type="text"/>
Relay to server2:	<input type="text"/>
Relay to server3:	<input type="text"/>
Relay to server4:	<input type="text"/>

##### DHCP RELAY UNTRUST

No.	Relay Untrust
1	Disable ▼
2	Disable ▼
3	Disable ▼
4	Disable ▼
5	Disable ▼
6	Disable ▼

Figure 5.74 – DHCP RELAY Interface

Apply

#### DHCP RELAY

Terms	Value Description
Enable	“Enable” or “Disable” DHCP Relay Agent
Relay Option 82	“Enable” or “Disable” DHCP Relay Option 82
Relay to server1	The IP address of the first DHCP Server that Relay Agent connect to
Relay to server2	The IP address of the second DHCP Server that Relay Agent connect to
Relay to server3	The IP address of the third DHCP Server that Relay Agent connect to
Relay to server4	The IP address of the fourth DHCP Server that Relay Agent connect to

Figure 5.75 – DHCP RELAY – Terms &amp; Value Description

## DHCP RELAY UNTRUST

Terms	Value Description
Relay Untrust	Per-port “Enable” or “Disable” Relay Untrust. DHCP frames can pass that port when it set to “Enable” only.

Figure 5.76 – DHCP RELAY – Terms & Value Description

## 5.14 802.1X

802.1X is an IEEE Standard for Port-based Network Access Control. It provides an authentication mechanism to devices that wish to attach to a LAN or WLAN. This port-based network access control protocol contains 3 parts, supplicant, authenticator, and authentication server. With 802.1X authentication, we can link a username with an IP address, MAC address, and port. This provides greater visibility into the network. 802.1X also provides more security because it only allows traffic transmitting on authenticated ports or MAC addresses. Although the IEEE standard defined it as a “Port-based” control, to provide more robust service, Antaira implements all managed switches with 802.1X to a “MAC-based” access control.

### RADIUS

RADIUS is used in the authentication process. Database of authorized users is maintained on a RADIUS server. There is an authenticator, our switch enabling 802.1X, to forward the authentication requests between authentication (RADIUS) server and client. Allowing or denying the requests decides if the client can connect to a LAN/WAN or not.

### 5.14.1 802.1X Settings

The below figure is the 802.1X configuration interface.

**802.1X**

**802.1X**

802.1X Enable: ☐  
Server Type: Local

**802.1X PORT**

No.	Enable Port	Re-Auth	Re-Auth Period(Sec.)
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600

Apply

Figure 5.77 – 802.1X Configuration Interface

The below table describes 802.1X Terms and Value Description.

#### 802.1X

Terms	Value Description
802.1X Enable	Check the checkbox to enable “802.1X” protocol.
Server Type	“Local” for authenticating with local server setting on the “Local Database” page.

#### 802.1X Port

Terms	Value Description
No.	The number of ports, from 1 to N, N depends on models.
Enable Port	Check the checkbox(es) to enable authentication before connecting to a LAN or WAN.
Re-Auth	“Re-Auth” means re-authenticate, it is enabled by default. Check the checkbox(es) to enable re-authentication after “Re-Auth Period” seconds.
Re-Auth Period(Sec.)	“Re-Auth Period” default value is 3600 seconds (60 minutes). Switch will ask the client for re-authentication every “Re-Auth Period” seconds.
No.	The number of ports, from 1 to N, N depends on models.

Figure 5.78 – 802.1X – Terms & Value Description

### 5.14.2 Local Database

The below figure is the Local Database web interface.

#### Local Database

##### LOCAL DATABASE

User Name	Password	Confirm Password	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Delete"/>
<input type="button" value="Add"/>			

Figure 5.79 – Local Database Web Interface

The below table describes Local Database Terms and Value Description.

Terms	Value Description
User Name	The user name use to authenticate in 802.1X when server set to "Local".
Password	The password use to authenticate in 802.1X when server set to "Local".
Confirm Password	Fill in the password again.

Figure 5.80 – Local Database – Terms & Value Description

### 5.14.3 RADIUS Server

The below figure is the RADIUS Server setting interface.

#### RADIUS Server

##### RADIUS SERVER



1st Server IP	<input type="text"/>
1st Server Port	<input type="text" value="1812"/>
1st Server Shared Key	<input type="text"/>
	
2nd Server IP	<input type="text"/>
2nd Server Port	<input type="text" value="1812"/>
2nd Server Shared Key	<input type="text"/>
	

Figure 5.81 – RADIUS Server Setting Interface

The below table describes RADIUS Server Terms and Value Description.


Terms	Value Description
Server IP	IP Address of RADIUS server
Server Port	"Server Port" default value is 1812. Switch will communicate with RADIUS server via this port.
Server Shared Key	Shared key is used to authenticate authenticator (switch) and authentication (RADIUS) server. Click "  " icon to show the shared key.

Figure 5.82 – RADIUS Server – Terms & Value Description

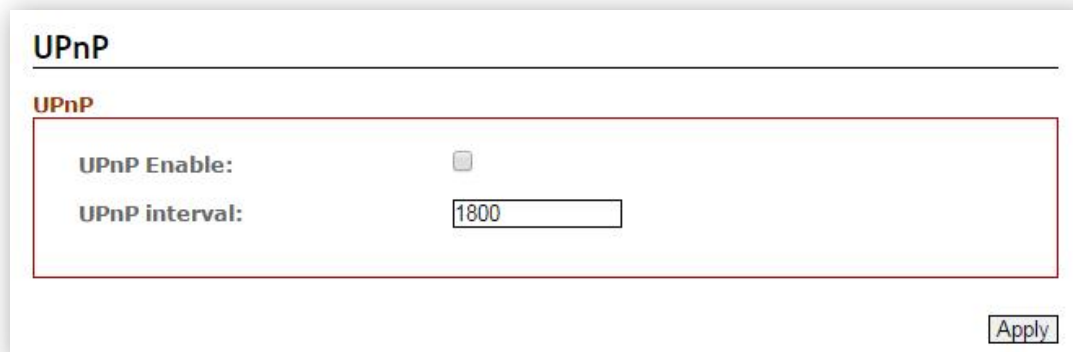
## 5.15 UPnP

Universal Plug and Play (UPnP) is a set of networking protocols that were promoted by the UPnP Forum. UPnP Protocol permits networked devices to discover each other's presence on the network and seamlessly establish functional network services for data sharing, communications, and entertainment.

The concept of UPnP is an extension of plug-and-play, a technology for dynamically attaching devices directly to a computer. But UPnP is not directly related to the earlier plug-and-play technology any more. UPnP devices are "plug-and-play" in that when connected to a network they automatically establish working configurations with other devices.

### 5.15.1 UPnP

Below, *Figure 5.83*, is the UPnP web interface.

The screenshot shows a web interface titled "UPnP". Below the title is a sub-header "UPnP" in orange. The main configuration area is enclosed in a red border and contains two settings: "UPnP Enable:" with a checkbox that is currently unchecked, and "UPnP interval:" with a text input field containing the value "1800". An "Apply" button is located at the bottom right of the configuration area.

*Figure 5.83 – UPnP Configuration Interface*

The below table describes UPnP Terms and Value Description.

Terms	Value Description
UPnP Enable	"Enable" or "Disable" UPnP protocol
UPnP Interval	UPnP Interval is the setting of Advertisement interval. It controls the time of sending advertisement.

*Figure 5.84 – UPnP Terms and Value Description*

## 5.16 Modbus TCP

Modbus is a serial communications protocol that is used with industrial automation equipment, such as programmable logic controllers (PLCs), sensors, and meters. It is a common, simple, and robust method of connecting industrial devices.

MODBUS TCP is a variant of the MODBUS family, vendor-neutral communication protocol commonly used for the integration of a SCADA system; of which, it covers the use of MODBUS messaging in an 'intranet' or 'internet' environment using the TCP/IP protocols.

According to the standard, Modbus encapsulates the message with an Ethernet TCP/IP wrapper.

Antaira's industrial Managed Ethernet switches support Modbus TCP/IP protocol to allow users to integrate it into those industrial control systems for real-time monitoring in a SCADA system.

### 5.16.1 Enable Modbus TCP

Below, *Figure 5.85*, is the ModbusTCP web interface.



*Figure 5.85 – Modbus TCP Web Interface*

The below table describes Modbus Terms and Value Description.

Terms	Value Description
Modbus TCP Enable	Check the checkbox to enable Modbus TCP.

*Figure 5.86 – Modbus TCP – Terms & Value Description*

### 5.16.2 MODBUS Data Map and Information

The data map addresses for Antaira's switches are shown in the table for **Function Code 6**.

Address Offset	Data Type	Interpretation	Description
<b>System Information</b>			
0x0000 to 0x0005	1 word	HEX	Port 1 to 6 Status 0x0000 : Link down 0x0001 : Enable 0x0002 : Disable Port 1 to 6 Status Configuration 0x0001 : Enable

			0x0002 : Disable
--	--	--	------------------

The data map addresses for Antaira's switches are shown in the following table starting from MODBUS for Function Code 4. For example, the address offset 0x0000 (hex) equals MODBUS address 30001, and the address offset 0x0015 (hex) equals MODBUS address 30022. Note that all the information read from Antaira switches are in hex mode. To interpret the information, refer to the ASCII table for the translation (e.g. 0x41 = 'A', 0x6E = 'n').

Address Offset	Data Type	Interpretation	Description
<b>System Information</b>			
0x0000	1 word	HEX	Vendor ID = 0x0000
0x0001	1 word		Unit ID (Ethernet = 1)
0x0002	1 word	HEX	Product Code = 0x0000
0x0010	20 words	ASCII	Vendor Name = "Antaira" Word 0 Hi byte = 'A' Word 0 Lo byte = 'n' Word 1 Hi byte = 't' Word 1 Lo byte = 'a' Word 2 Hi byte = 'i' Word 2 Lo byte = 'r' Word 3 Hi byte = 'a' Word 3 Lo byte = '\0'
0x0030	20 words	ASCII	Product Name = "LMP-0602" Word 0 Hi byte = 'L' Word 0 Lo byte = 'M' Word 1 Hi byte = 'P' Word 1 Lo byte = '-' Word 2 Hi byte = '0' Word 2 Lo byte = '6' Word 3 Hi byte = '0' Word 3 Lo byte = '2' Word 4 Hi byte = '\0' Word 4 Lo byte = '\0'
0x0050	1 word		Product Serial Number
0x0051	2 words	HEX	Firmware Version For example : Word 0 = 0 x 0203 Word 1 = 0 x 0300 Firmware Version was 2.3.3



0x0053	2 words	HEX	Firmware Release Date For example : Word 0 = 0 x 2319 Word 1 = 0 x 1501 Firmware was released on 2015-01-23 at 19:00
0x0055	3 words	HEX	Ethernet MAC Address Ex : MAC = 7C:CB:0D:AD:DC:14 Word 0 Hi byte = 0 x 7C Word 0 Lo byte = 0 x CB Word 1 Hi byte = 0 x 0D Word 1 Lo byte = 0 x AD Word 2 Hi byte = 0 x DC Word 2 Lo byte = 0 x 14
0x0058	1 word	HEX	Power 1 0x0000 : Off 0x0001 : On
0x0059	1 word	HEX	Power 2 0x0000 : Off 0x0001 : On
0x005A	1 word	HEX	Fault LED Status 0x0000 : Boot error 0x0001 : Normal 0x0002 : Fault
0x0082	1 word	HEX	DO1 0x0001 : Normal 0x0002 : Fault
<b>Port Information</b>			
0x1000 to 0x1005	1 word	HEX	Port 1 to 6 Status 0x0000 : Link down 0x0001 : Link up 0x0002 : Disable 0xFFFF : No port
0x1100 to 0x1105	1 word	HEX	Port 1 to 6 Speed 0x0000 : 10M-Half 0x0001 : 10M-Full

			0x0002 : 100M-Half 0x0003 : 100M-Full 0xFFFF : No port
0x1200 to 0x1205	1 word	HEX	Port 1 to 6 Flow Ctrl 0x0000 : Off 0x0001 : On 0xFFFF : No port
0x1300 to 0x1305	1 word	HEX	Port 1 to 6 MDI/MDIX 0x0000: MDI 0x0001: MDIX 0xFFFF: No port
0x1400 to 0x1413 (Port 1) 0x1414 to 0x1427 (Port 2)	20 words	ASCII	Port 1 to 6 Name Port Name = "100FDX,RJ45." Word 0 Hi byte = '1' Word 0 Lo byte = '0' Word 1 Hi byte = '0' Word 1 Lo byte = 'F' ... Word 5 Hi byte = '5' Word 5 Lo byte = ':'
<b>Packets Information</b>			
0x2000 to 0x200B	2 words	HEX	Port 1 to 6 Tx Packets Ex : Port1 Tx Packet Amount = 13244800 Received MODBUS response : 0x13244800 Word 0 = 0 x 1324 Word 1 = 0 x 4800
0x2080 to 0x208B	2 words	HEX	Port 1 to 6 Tx Bytes Ex : Port1 Tx Bytes Amount = 13244800 Received MODBUS response : 0x13244800 Word 0 = 0 x 1324 Word 1 = 0 x 4800
0x2100 to	2 words	HEX	Port 1 to 6 Rx Packets

0x210B			Ex : Port1 Rx Packet Amount = 13244800 Received MODBUS response : 0x13244800 Word 0 = 0 x 1324 Word 1 = 0 x 4800
0x2180 to 0x218B	2 words	HEX	Port 1 to 6 Rx Bytes Ex : Port1 Rx Bytes Amount = 13244800 Received MODBUS response : 0x13244800 Word 0 = 0 x 1324 Word 1 = 0 x 4800
0x2200 to 0x220B	2 words	HEX	Port 1 to 6 Tx Error Packets Ex : Port 1 Tx Error Packet Amount = 13244800 Received MODBUS response : 0x13244800 Word 0 = 0 x 1324 Word 1 = 0 x 4800
0x2300 to 0x230B	2 words	HEX	Port 1 to 6 Rx Error Packets Ex : Port1 Rx Error Packet Amount = 13244800 Received MODBUS response : 0x13244800 Word 0 = 0 x 1324 Word 1 = 0 x 4800
<b>Redundancy Information</b>			
0x3000	1 word	HEX	Redundancy Protocol 0x0000 : None 0x0001 : RSTP 0x0002 : MSTP 0x0003 : ERPS
0x3100	1 word	HEX	RSTP Root 0xFFFF : None

			0x0001 : Root 0x0002 : Not root
0x3200 to 0x3205	1 word	HEX	RSTP Port 1 to 6 Status 0xFFFF : Spanning tree not enable 0x0000 : Disable 0x0001 : Not spanning tree port 0x0002 : Link down 0x0003 : Blocked 0x0004 : Learning 0x0005 : Forwarding
0x3300	1 word	HEX	ERPS Port0 Role 0xFFFF : ERPS not enable 0x0000 : Normal 0x0001 : Neighbor 0x0002 : RPL Owner
0x3301	1 word	HEX	ERPS Port1 Role 0xFFFF : ERPS not enable 0x0000 : Normal 0x0001 : Neighbor 0x0002 : RPL Owner
0x3302	1 word	HEX	ERPS Port0 Status 0x0000 : Disable 0x0001 : ERPS not enable 0x0002 : Link down 0x0003 : Forwarding 0x0004 : Learning 0x0005 : Blocking
0x3303	1 word	HEX	ERPS Port1 Status 0x0000 : Disable 0x0001 : ERPS not enable 0x0002 : Link down 0x0003 : Forwarding 0x0004 : Learning 0x0005 : Blocking
0x3304	1 word	HEX	ERPS Port0 Port Ex : ERPS Port0 is Port1

			Word 0 = 0 x0001
0x3305	1 word	HEX	ERPS Port1 Port Ex : ERPS Port1 is Port2 Word 0 = 0 x0002

Figure 5.87 – Antaira Switches – Modbus Data Map &amp; Information

## 5.17 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.

### 5.17.1 Syslog Setting

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

**Syslog Setting**

**SYSLOG**


SYSLOG Mode: Disable

SYSLOG Server IP Address:

Apply

Disable  
Local Only  
Remote Only  
USB Only  
All

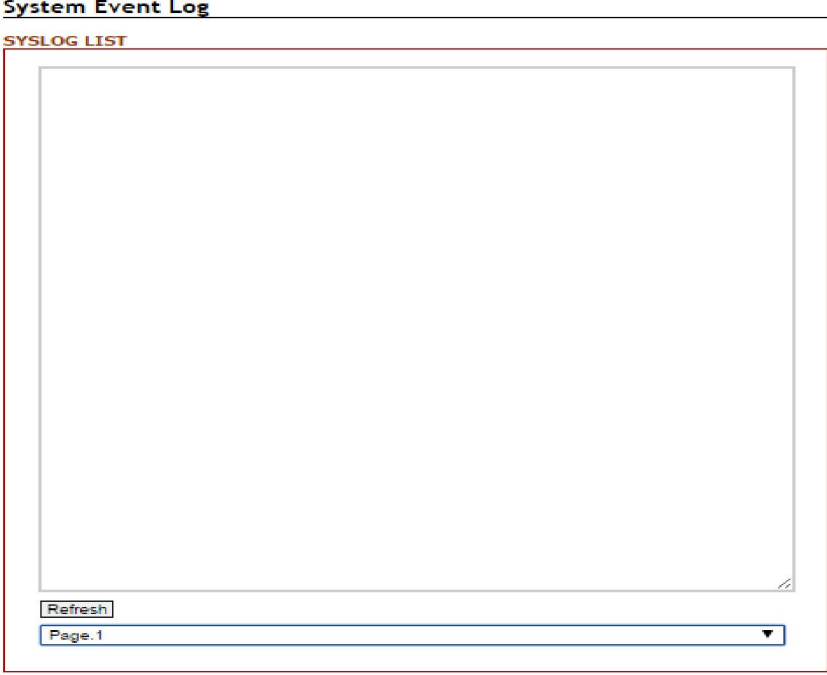
Figure 5.88 – Syslog Setting

Terms	Value Description
<b>SYSLOG Mode</b>	<b>Disable:</b> disable SYSLOG. <b>Local Only:</b> log to local system. <b>Remote Only:</b> log to a remote SYSLOG server. <b>USB Only:</b> log and store SYSLOG data and warning file to USB storage device through built-in USB Port; and the file name is "message" <b>All:</b> 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.
<b>SYSLOG Server IP Address</b>	Insert remote SYSLOG server IP address
	Click the "Apply" button to save changes.

*Figure 5.89 – SYSLOG Setting Terms & Value Description*

### 5.17.2 System 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.

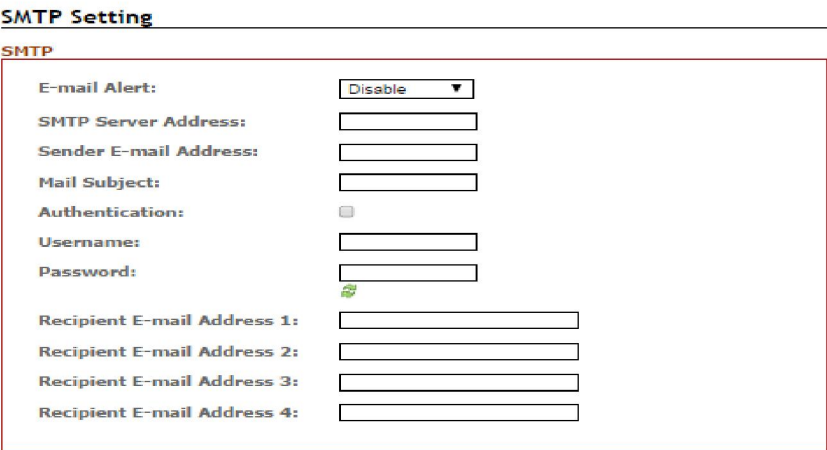


The screenshot shows the 'System Event Log' interface. At the top, the title 'System Event Log' is displayed. Below it, the text 'SYSLOG LIST' is shown. A large, empty rectangular box occupies the center of the interface, intended for displaying log entries. At the bottom left of this box, there is a 'Refresh' button. Below the box, there is a 'Page: 1' label with a dropdown arrow. At the bottom right of the entire interface, there is an 'Apply' button.

Figure 5.90 – System Event Logs Interface

### 5.17.3 SMTP Setting

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



The screenshot shows the 'SMTP Setting' interface. The title 'SMTP Setting' is at the top. Below it, the text 'SMTP' is displayed. The interface contains several configuration fields: 'E-mail Alert:' with a dropdown menu set to 'Disable'; 'SMTP Server Address:', 'Sender E-mail Address:', and 'Mail Subject:' each with a text input field; 'Authentication:' with an unchecked checkbox; 'Username:' and 'Password:' each with a text input field; and four 'Recipient E-mail Address' fields (1 through 4), each with a text input field. A small green icon is visible next to the 'Password' field. At the bottom right of the interface, there is an 'Apply' button.

Figure 5.91 – SMTP Setting Interface

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

Figure 5.92 – SMTP Setting Terms &amp; Value Description

### 5.17.4 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 message to either SYSLOG or SMTP, or both at the same time. After the event selection, users can click the “Apply” button to save changes.

**Event Selection**

**EVENT SELECTION**

Event	SYSLOG	SMTP
System Cold Start:	<input type="checkbox"/>	<input type="checkbox"/>

**EVENT SELECTION PORT**

Port No.	SYSLOG	SMTP
1	Disable	Disable
2	Disable	Disable
3	Disable	Disable
4	Disable	Disable
5	Disable	Disable
6	Disable	Disable

Apply

Figure 5.93 – Event Selection Setting Interface



### 5.17.5 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.

**Fault Alarm**

**FAULT ALARM**

Power1 Failure:	<input type="checkbox"/>
Power2 Failure:	<input type="checkbox"/>
Port1 Link Down/Broken:	<input type="checkbox"/>
Port2 Link Down/Broken:	<input type="checkbox"/>
Port3 Link Down/Broken:	<input type="checkbox"/>
Port4 Link Down/Broken:	<input type="checkbox"/>
Port5 Link Down/Broken:	<input type="checkbox"/>
Port6 Link Down/Broken:	<input type="checkbox"/>

Apply

Figure 5.94 – Event Selection Setting Interface

## 5.18 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.

### 5.18.1 MAC Address Table

**MAC Address Table**

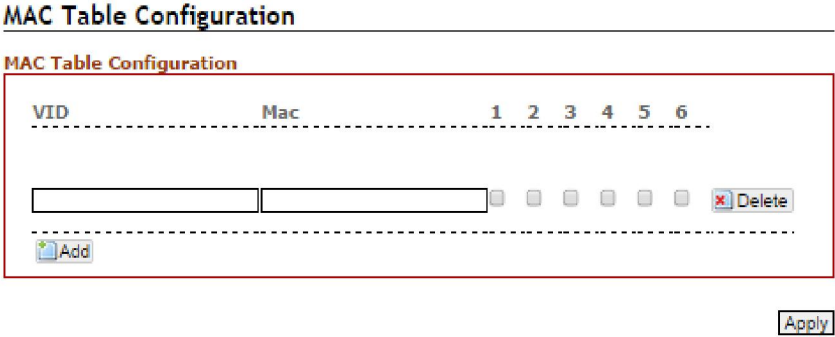
**MAC Address Table**

VID	Mac	Type	Port
1	00:00:21:ff:ff:ff	learning	2
1	00:20:4a:ea:70:d3	learning	2
1	00:30:ab:26:cb:04	learning	2
1	00:50:7f:47:22:8a	learning	2
1	01:00:5e:00:01:3c	static	2
1	01:00:5e:7f:ff:fa	static	2
1	10:bf:48:5a:b4:0d	learning	2
1	1c:af:f7:7c:5b:f6	learning	2
1	30:85:a9:a7:9d:63	learning	2
1	30:85:a9:a8:05:bb	learning	2
1	44:6d:57:47:27:04	learning	2
1	48:5b:39:d1:1f:06	learning	2
1	54:53:ed:af:5c:bd	learning	2
1	7c:cb:0d:08:01:5e	learning	2
1	e0:3f:49:e7:44:c2	learning	2
1	ec:43:f6:6f:90:fd	learning	2
1	f4:ce:46:c8:01:9f	learning	2

Figure 5.95 – MAC Address Table Interface

## 5.18.2 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.



The screenshot shows the 'MAC Table Configuration' web interface. It features a table with columns for 'VID', 'Mac', and six ports labeled '1' through '6'. Each port has a checkbox. Below the table is an 'Add' button with a plus icon. At the bottom right is an 'Apply' button.

VID	Mac	1	2	3	4	5	6
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

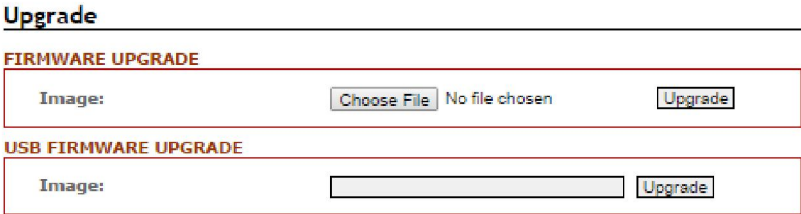
Figure 5.96 – MAC Table Setting Interface

## 5.19 Maintenance

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

### 5.19.1 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, or server.



The screenshot shows the 'Upgrade' web interface. It has two sections: 'FIRMWARE UPGRADE' and 'USB FIRMWARE UPGRADE'. The first section has an 'Image:' label, a 'Choose File' button, a 'No file chosen' status, and an 'Upgrade' button. The second section has an 'Image:' label, a text input field, and an 'Upgrade' button.

**Upgrade**

**FIRMWARE UPGRADE**

Image:  No file chosen

**USB FIRMWARE UPGRADE**

Image:

Figure 5.97 – Firmware Upgrade Interface

Terms	Value Description
<b>FIRMWARE UPGRADE</b>	Users 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.
<b>USB FIRMWARE UPGRADE</b>	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 5.98 – Firmware Upgrade setting Terms & Value Description

### 5.19.2 Reboot

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

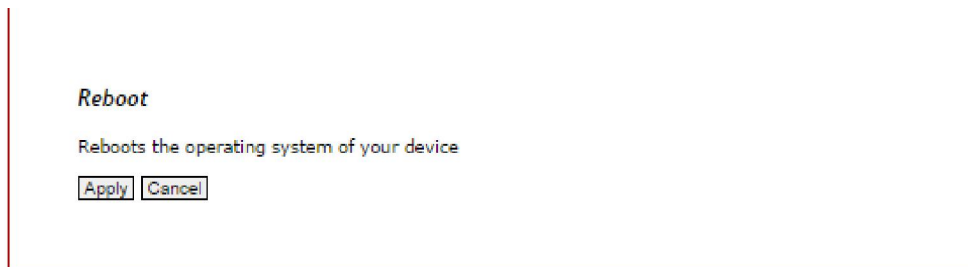


Figure 5.99 – Switch Reboot Interface

### 5.19.3 Default

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

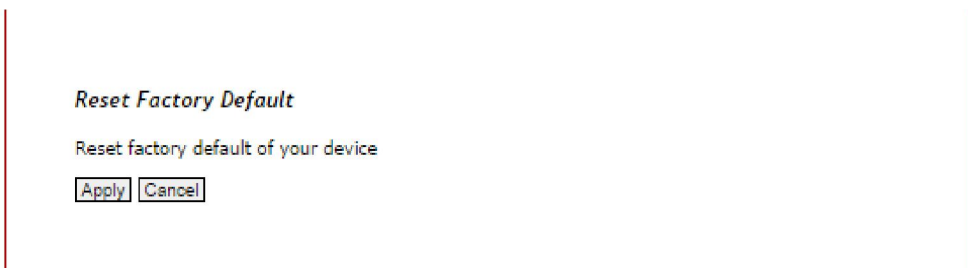


Figure 5.100 – Reset Factory Default Interface

## 5.20 Configuration

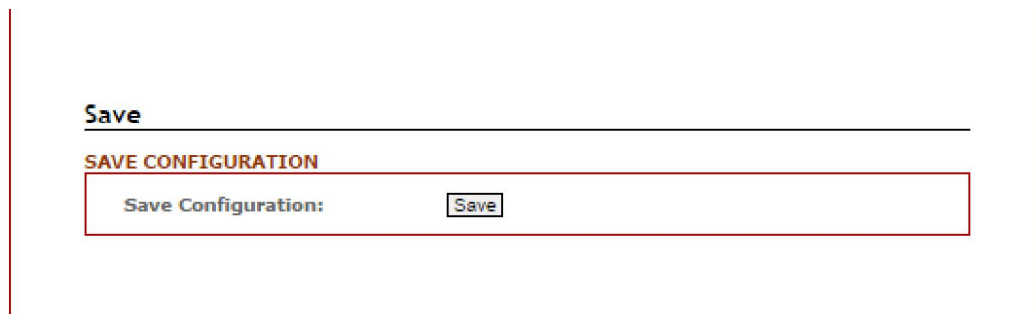
Under the “Configuration” section, users can save all the settings that have been configured, backed up and stored to a local PC, Server, or a USB storage device through the built-in USB port.

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 back up to the USB storage device whenever users makes and save configuration settings.

### 5.20.1 Save

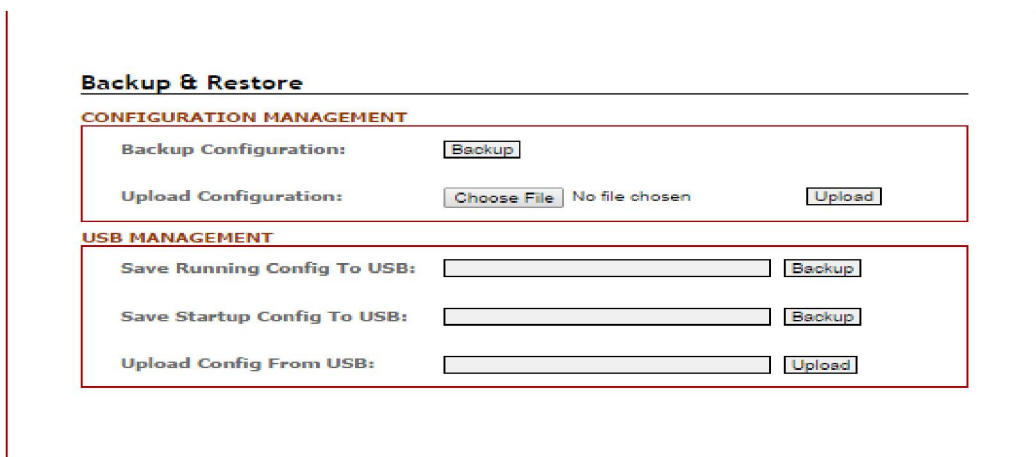
Users can click the “Save” button under the “SAVE CONFIGURATION” interface, once all the settings had been configured.



The screenshot shows a web interface for saving configuration. At the top, there is a header "Save" followed by a horizontal line. Below this is a section titled "SAVE CONFIGURATION" in orange. Underneath, there is a label "Save Configuration:" followed by a button labeled "Save".

Figure 5.101 – Save Setting Interface

### 5.20.2 Backup & Restore



The screenshot shows a web interface for backup and restore operations. At the top, there is a header "Backup & Restore" followed by a horizontal line. Below this is a section titled "CONFIGURATION MANAGEMENT" in orange. Underneath, there are two rows of controls. The first row is for "Backup Configuration:" with a "Backup" button. The second row is for "Upload Configuration:" with a "Choose File" button, the text "No file chosen", and an "Upload" button. Below this is another section titled "USB MANAGEMENT" in orange. Underneath, there are three rows of controls. The first row is for "Save Running Config To USB:" with a text input field and a "Backup" button. The second row is for "Save Startup Config To USB:" with a text input field and a "Backup" button. The third row is for "Upload Config From USB:" with a text input field and an "Upload" button.

Figure 5.102 – Backup & Restore Setting Interface

Terms	Value Description
<b>CONFIGURATION MANAGEMNET</b>	
<b>Backup Configuration</b>	By click the “Backup” button, it allows user to back up the switch configuration setting to local PC, or server.
<b>Upload Configuration</b>	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.
<b>USB Management</b>	
<b>Save Running Config to USB</b>	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.
<b>Save Startup Config to USB</b>	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.
<b>Upload Config from USB</b>	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 5.103 – Backup &amp; Restore Setting Terms &amp; Value Description

### 5.20.3 Auto Load & Backup

**USB Auto Load and Backup**

**Auto Load and Backup**

USB Auto Load: ☒

USB Auto Backup: ☐

Apply

Figure 5.104 – USB Auto Load and Backup Setting Interface

Terms	Value Description
<b>USB Auto Load</b>	Select USB Auto Load (plug USB stick and reboot the switch), it will auto load startup file from USB to Switch. Please make sure the startup 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.
<b>USB Auto Backup</b>	Select USB Auto Backup, it can auto Backup running-config file from Switch to USB. And the file name is "startup-config".

*Figure 5.105 – USB Auto Load and Backup Setting Terms & Value Description*

## 5.21 Logout

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

## 6. Command Line Interface Management

### 6.1 About CLI Management

Besides WEB-based management, LMP-0600-24 series also supports CLI management. Users can use console or telnet to management switch by CLI.

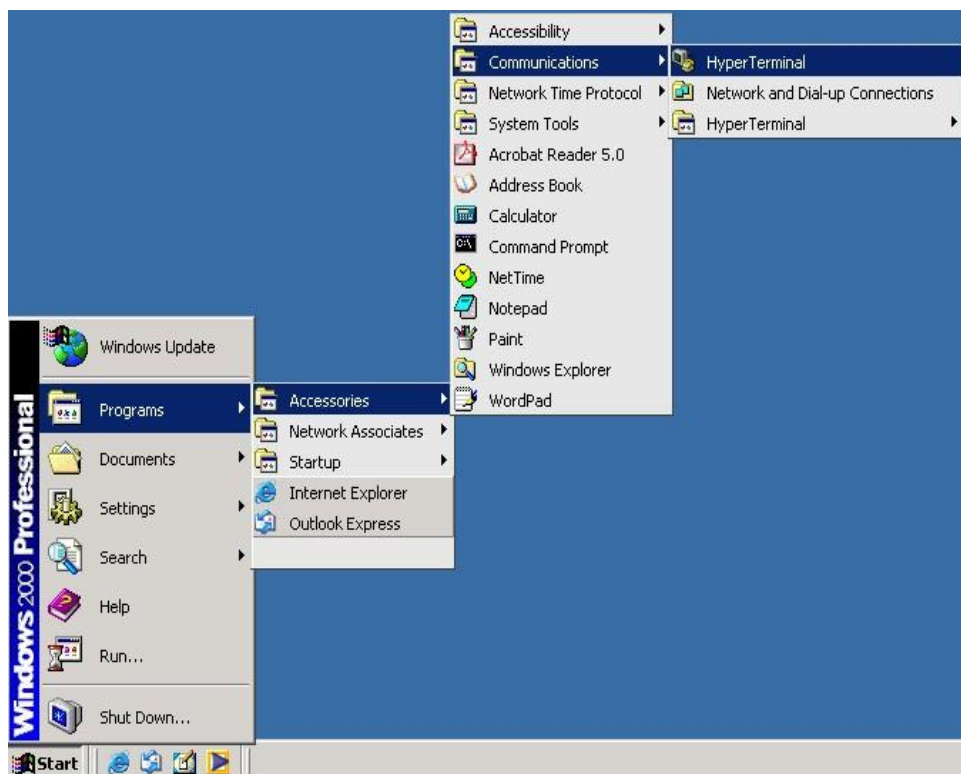
#### CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

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

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

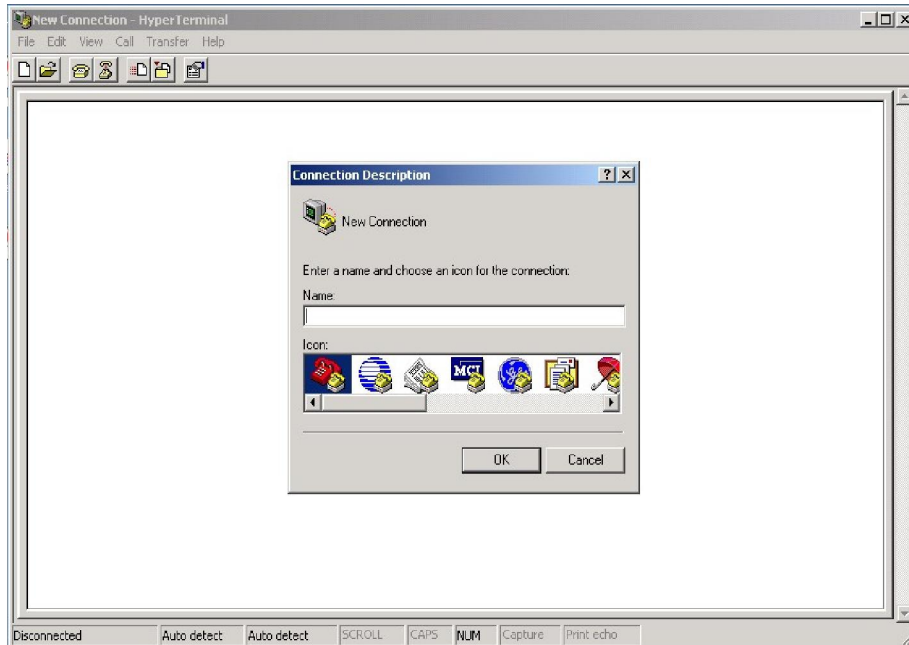
#### Step 1:

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



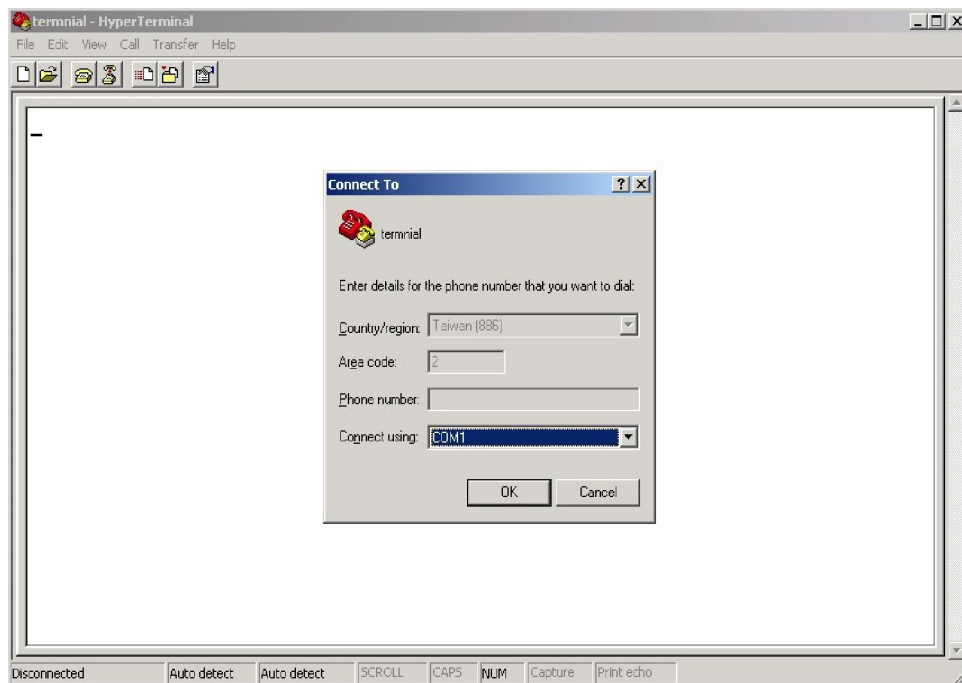
**Step 2:**

Input a name for the new connection.



**Step 3:**

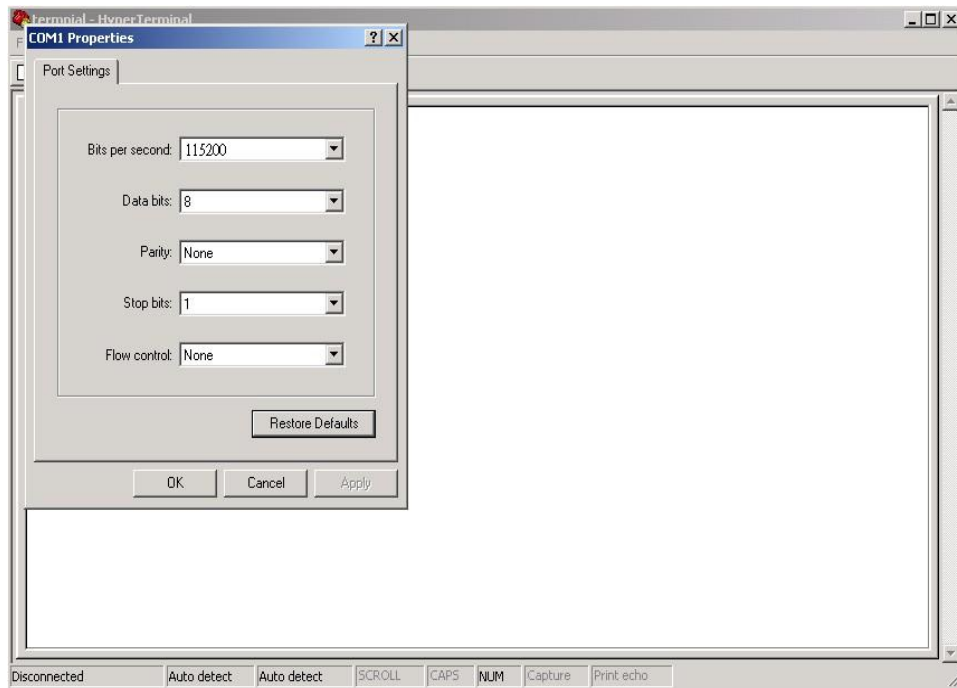
Select to use a specific COM port number.





**Step 4:**

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



**Step 5:**

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

```
User Access Verification
Username: admin
Password:
SWES> en
SWES# configure terminal
```

### CLI Management by Telnet

Users can use “**TELNET**” to configure the switches.

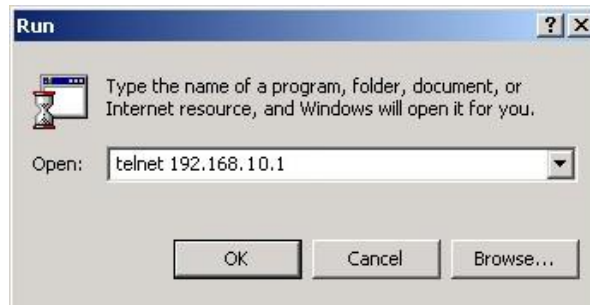
The default value is as below:

- 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**”

```
User Access Verification
Username: admin
Password:
SWES> en
SWES# configure terminal
```

## Commander Groups

Group	Command	Mode
System	hostname [Switch]	configure
	no hostname	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
	username [NAME] password [PASSWD]	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 timeserver [ip_addr_string]	configure
	clock time [hh:mm:ss] [day] [month] [year]	configure
	clock timezone [area] [city]	configure
	ntp client sync schedule enable	configure
	ntp client sync minute [time]	configure
	ntp client sync hour [time]	configure

Time	ntp client sync day [time]	configure
	ntp client sync month [time]	configure
	ntp client sync weekly [time]	configure
	no ntp client timeserver	configure
	no clock timezone	configure
	no ntp client sync schedule	configure
	no ntp client sync minute	configure
	no ntp client sync hour	configure
	no ntp client sync day	configure
	no ntp client sync month	configure
	no ntp client sync weekly	configure
	show ntp client timeserver	configure
	show clock timezone	configure
	show ntp client sync schedule enable	configure
	show ntp client sync minute	configure
	show ntp client sync hour	configure
	show ntp client sync day	configure
	show ntp client sync month	configure
	show ntp client sync weekly	configure
Port	speed_duplex [10   100   1000] [full   half]	interface
	flowcontrol <receive> [on   off   desired]	interface
	name [string]	interface
	shutdown	interface
	no speed_duplex	interface
	no flowcontrol	interface
	no name	interface
	no shutdown	interface
	show speed	interface
	show flowcontrol	interface
	show administrate	interface
	show name	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	configure
VLAN	management vlan [vlan_id]	configure
	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
ERPS	ethernet ring erps major	configure
	enable	erps
	disable	erps
	rpl [port0   port1] [owner   neighbor]	erps
	aps-channel [channel ID]	erps
	revertive	erps
	clear	erps

	port0 interface [interface name]	erps
	port1 interface [interface name]	erps
	fs [port0   port1]	erps
	ms [port0   port1]	erps
	ring-id [erps ring ID]	erps
	timer hold-off [0~1000]	erps
	timer guard [10~2000]	erps
	timer wtr [1~12]	erps
	no rpl [port0   port1]	erps
	no aps-channel	erps
	no revertive	erps
	no port0	erps
	no port1	erps
	no ring-id	erps
	no timer hold-off	erps
	no timer guard	erps
	no timer wtr	erps
	show status	erps
	show brief	erps
	show port status	erps
	show configuration	erps
PoE	power inline never	interface
	keepalive ip [IP_Address]	interface
	keepalive time [Seconds]	interface
	schedule [monday~sunday] enable	interface
	schedule [monday~sunday] starttime [Hour]	interface
	schedule [monday~sunday] endtime [Hour]	interface
	no power inline never	interface
	no keepalive ip	interface
	no keepalive time	interface
	no schedule [monday~sunday] enable	interface
	no schedule [monday~sunday] starttime	interface
	no schedule [monday~sunday] endtime	interface
	show power inline status	interface
	show keepalive ip	interface

<b>PoE</b>	show keepalive time	interface
	show schedule [monday~sunday] enable	interface
	show schedule [monday~sunday] starttime	interface
	show schedule [monday~sunday] endtime	interface
<b>STP</b>	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 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
	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
<b>STP</b>	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
<b>Event</b>	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 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
	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
<b>Event</b>	show event syslog interface [INTERFACE_NAME] [up   down]	configure
	event alarm power1 enable	configure
	event alarm power2 enable	configure
	event alarm interface [INTERFACE_NAME] [-down]	configure
	no event alarm power1	configure
	no event alarm power2	configure

	no event alarm interface [INTERFACE_NAME] [-down]	configure
	show event alarm power1	configure
	show event alarm power2	configure
	show event alarm interface [INTERFACE_NAME] [-down]	configure
	event apply	configure
<b>SYSLOG</b>	syslog server [IP_address]	configure
	syslog mode [both1   both2   remote   local   usb]	configure
	no syslog server	configure
	no syslog mode	configure
	show syslog server	configure
	show syslog mode	configure
	show syslog log	configure
<b>SMTP</b>	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
<b>SNMP</b>	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 trap v3 auth [md5   sha] [PASSWORD]	configure
	snmp trap v3 encryption [des   aes] [PASSWORD]	configure
<b>SNMP</b>	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
<b>FILE</b>	copy running-config startup-config	configure
	copy startup-config running-config	configure
<b>PORT MIRROR</b>	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
<b>QoS</b>	qos queue-schedule [strict   wrr]	configure
	qos map cos [priority_type] to tx-queue [queue]	configure
	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
<b>IGMP</b>	igmp snooping enable	configure
	igmp snooping query max-respond-time [1..12]	configure
	igmp snooping query interval [1..3600]	configure
	igmp snooping last-member count [2..10]	configure
	igmp snooping last-member interval [60..300]	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
<b>Trunk</b>	trunk group [group] [static   lacp] [interface_list]	configure
<b>DHCP Server/Relay</b>	dhcp service server	configure
	dhcp server included-address [IP_START] [IP_END]	configure
	dhcp server default-gateway [router_ip]	configure
	dhcp server name-server [dns_ip]	configure
	dhcp server lease [dhcp_lease_time]	configure
	dhcp server binding [bind_num][MAC] [bind_IP]	configure
	dhcp server port-binding [Port] [bind_IP]	configure
	dhcp service relay	configure
	dhcp relay server [server_number] [IP]	configure
	dhcp relay information option	configure

	dhcp relay information policy [replace   keep   drop]	configure
	dhcp relay untrust	interface
	no dhcp service server	configure
	no dhcp server included-address	configure
	no dhcp server default-gateway	configure
	no dhcp server name-server	configure
	no dhcp server lease	configure
	no dhcp server binding [bind_num]	configure
	no dhcp service relay	configure
	no dhcp relay server [server_number]	configure
	no dhcp relay information option	configure
	no dhcp relay information policy [replace   keep   drop]	configure
	no dhcp relay untrust	configure
	show dhcp service	interface
	show dhcp server status	configure
	show dhcp server included-address	configure
	show dhcp server default-gateway	configure
	show dhcp server name-server	configure
	show dhcp server lease	configure
	show dhcp server binding [bind_num][MAC] [bind_IP]	configure
	show dhcp relay enable	configure
	show dhcp relay server [server_number]	configure
	show dhcp relay information option	configure
	show dhcp relay information policy [replace   keep   drop]	configure
	show dhcp relay untrust	interface
<b>UPnP</b>	<b>upnp enable</b>	configure
	<b>upnp advertisement interval [SEC]</b>	configure
	<b>no upnp enable</b>	configure
	<b>no upnp advertisement interval</b>	configure
	<b>show upnp enable</b>	configure
	<b>show upnp advertisement interval</b>	configure
<b>Modbus</b>	modbus tcp server	configure
	no modbus tcp server	configure
	show modbus tcp server	configure
<b>802.1X</b>	dot1x enable	configure

	dot1x authentication server type [local   radius]	configure
	dot1x authentication server 1 ip [IP]	configure
	dot1x authentication server 1 port [PORT]	configure
	dot1x authentication server 1 share-key [KEY]	configure
	dot1x authentication server 2 ip [IP]	configure
	dot1x authentication server 2 port [PORT]	configure
	dot1x authentication server 2 share-key [KEY]	configure
	dot1x local-db [USER] [PASSWORD]	configure
	dot1x authenticator enable	interface
	dot1x reauthentication enable	interface
	dot1x reauthentication period [SEC]	interface
	no dot1x enable	configure
	no dot1x authentication server type	configure
	no dot1x authentication server 1 ip	configure
	no dot1x authentication server 1 port	configure
	no dot1x authentication server 1 share-key	configure
	no dot1x authentication server 2 ip	configure
	no dot1x authentication server 2 port	configure
	no dot1x authentication server 2 share-key	configure
	no dot1x local-db [USER] [PASSWORD]	configure
	no dot1x authenticator enable	interface
	no dot1x reauthentication enable	interface
	no dot1x reauthentication period	interface
	show dot1x enable	configure
	show dot1x authentication server type	configure
	show dot1x authentication server 1 ip	configure
	show dot1x authentication server 1 port	configure
	show dot1x authentication server 1 share-key	configure
	show dot1x authentication server 2 ip	configure
	show dot1x authentication server 2 port	configure
	show dot1x authentication server 2 share-key	configure
	show dot1x local-db [USER] [PASSWORD]	configure
	show dot1x brief	configure
	show dot1x server brief	configure
	show dot1x brief	interface

	show dot1x server brief	interface
	show dot1x authenticator enable	interface
	show dot1x reauthentication enable	interface
	show dot1x reauthentication period	interface
IPv6	ipv6 enable	configure
	ipv6 address add [IPV6_ADDR</PREFIX_LEN>]	configure
	ipv6 neighbor flush	configure
	ipv6 ping [IPV6_ADDR] [<size PKG_SIZE>   <repeat PKG_CNT> ]	configure
	no ipv6 enable	configure
	no ipv6 address [IPV6_ADDR/PREFIX_LEN]	configure
IPv6	show ipv6 enable	configure
	show ipv6 address	configure
	show ipv6 neighbor	configure
TFTP	tftp upgrade	configure
	tftp server ip [IP_ADDRESS]	configure
	tftp file name [UPGRADE_FILE_NAME]	configure

## Save and Load Configuration File to/from USB

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

```

Telnet 192.168.2.19
User Access Verification
Username: admin
Password:
SWES> en
SWES# configure terminal
SWES(config)# copy
running-config startup-config usb
SWES(config)# copy running-config
startup-config usb
SWES(config)# copy running-config usb file1
SWES(config)# copy running-config usb /test/file2
SWES(config)# _

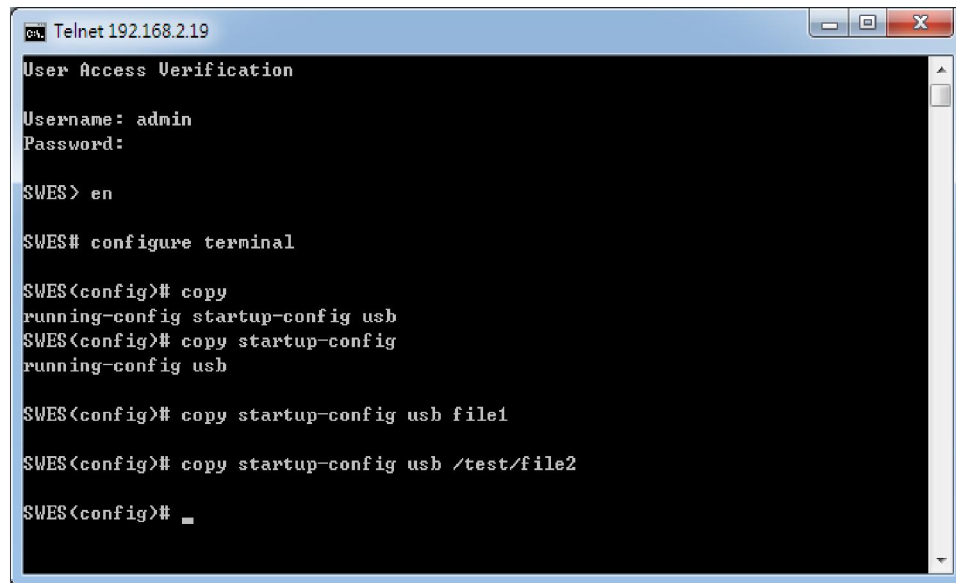
```

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)

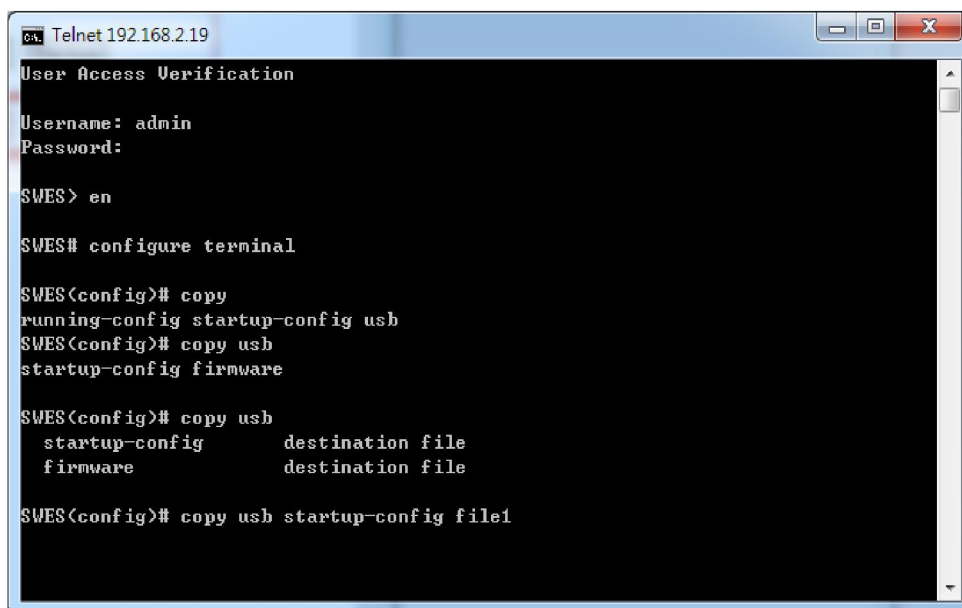


```
Telnet 192.168.2.19
User Access Verification
Username: admin
Password:
SWES> en
SWES# configure terminal
SWES(config)# copy
running-config startup-config usb
SWES(config)# copy startup-config
running-config usb
SWES(config)# copy startup-config usb file1
SWES(config)# copy startup-config usb /test/file2
SWES(config)#
```

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)

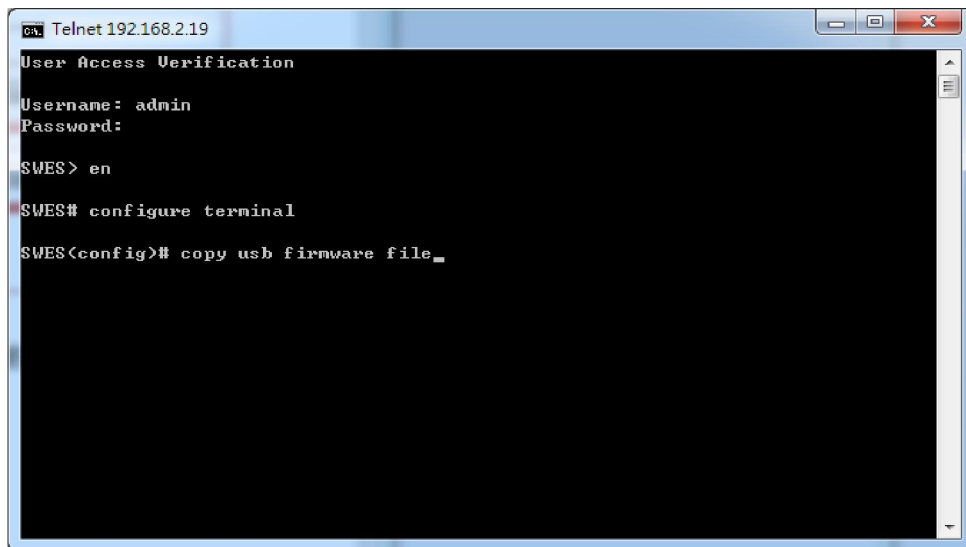


```
Telnet 192.168.2.19
User Access Verification
Username: admin
Password:
SWES> en
SWES# configure terminal
SWES(config)# copy
running-config startup-config usb
SWES(config)# copy usb
startup-config firmware
SWES(config)# copy usb
startup-config      destination file
firmware            destination file
SWES(config)# copy usb startup-config file1
```

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)

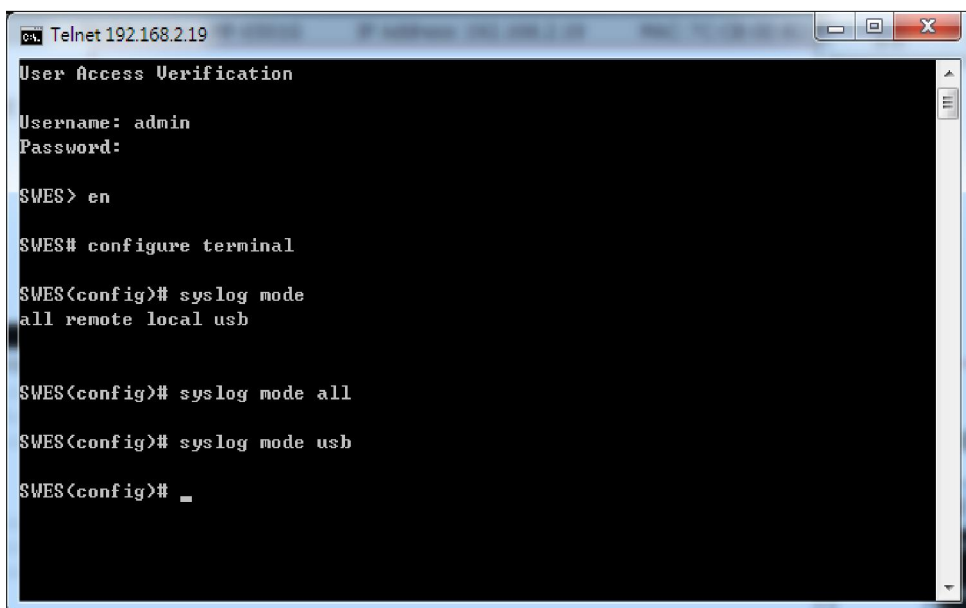


```
cs Telnet 192.168.2.19
User Access Verification
Username: admin
Password:
SWES> en
SWES# configure terminal
SWES(config)# copy usb firmware file_
```

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)



```
cs Telnet 192.168.2.19
User Access Verification
Username: admin
Password:
SWES> en
SWES# configure terminal
SWES(config)# syslog mode
all remote local usb

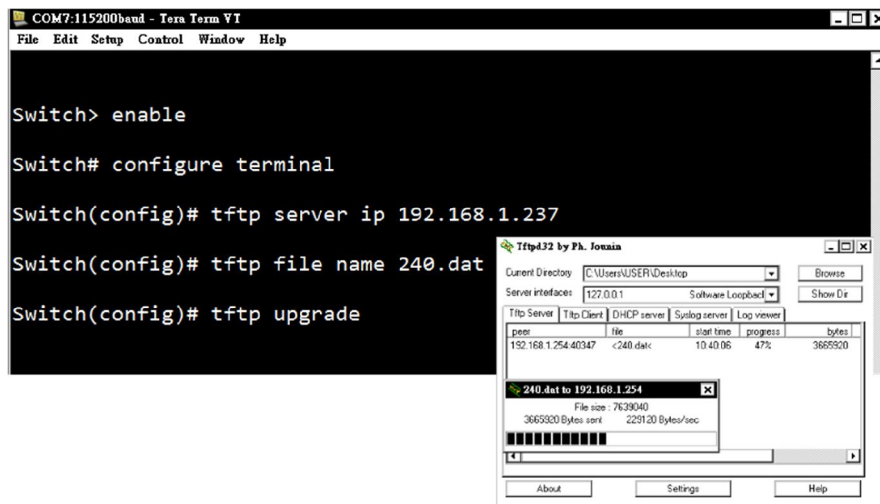
SWES(config)# syslog mode all
SWES(config)# syslog mode usb
SWES(config)# _
```

Select USB or ALL, it can auto save warning 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

## Upgrade via TFTP

CLI : enable -> configure terminal -> tftp server ip [IP\_ADDRESS] -> tftp file name [UPGRADE\_FILE\_NAME] -> tftp upgrade



Fill in the TFTP server IP and upgrade file name behind the "tftp server ip [IP\_ADDRESS]" and "tftp file name [UPGRADE\_FILE\_NAME]"

## 7. Technical Specifications

Table 7.1 has the technical specifications for Antaira's LMP-0600-24 series: 6-port industrial PoE+ managed Ethernet switch with 6\*10/100Tx (w/4\*PoE Ports: 30W/Port); 12~36VDC power input.

<b>Standards</b>	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 802.3af	Power-over-Ethernet
	IEEE 802.3at	Power-over-Ethernet Plus (Enhanced)
	IEEE 802.3ad	Port Trunking with LACP
	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
<b>Switch</b>	Protocol	IGMPv1/v2, SNMPv1/v2c/v3, TFTP, SNTP, SMTP, RMON, HTTP, HTTPS, Telnet, Syslog, DHCP Option 66/67/82, SSH/SSL, Modbus/TCP, LLDP, IPv4/IPv6
	Data Process	Store and Forward
	Transfer Rate	14,880 pps for 10Base-Tx Ethernet port 148,800 pps for 100Base-TX Fast Ethernet port
	Packet Buffer	1 Mbit
	MAC Table	8K
	Jumbo Frame	-
	Flow Control	IEEE 802.3x-full duplex mode, back pressure-half duplex mode
	VLAN Groups	1 ~ 4094
	IGMP Groups	Up to 256
<b>Port Interface</b>	Ethernet (RJ45) Port	6*10/100BaseTx (4*PoE Ports: 30W/Port) auto negotiation speed, Full/Half duplex mode, and auto MDI connection
	PoE Pin Assignment	V+, V+, V-, V-, for pin 1, 2, 3, 6 (Endspan, MDI Alternative A)
	Serial Console Port	1*RS232 in RJ45 connector with console cable, 115.2Kbps, 8,N,1
	Configuration Backup Port	1*USB 2.0
<b>Protection</b>	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)
<b>Mechanical Characteristics</b>	LED Indicator	Power Unit: P1 (Green), P2 (Green), fault (Red) Ethernet port: Link/active (Green), 10/100Mbps PoE: Link/active (Green)
	Housing	Metal IP30 protection
	Dimension	54 x 142 x 99 mm
	Weight	Unit Weight: 2.1 lbs. Shipping Weight: 2.9 lbs
	Mounting	DIN-Rail Mounting, wall-mounting (optional)
<b>Power Requirement</b>	Input Voltage	12~36VDC Redundant Input
	Power Connection	1 removable 6-contact terminal block
	Power Consumption	10 Watts (no PD included); 145 Watts @12~36VDC input
<b>Environmental Limits</b>	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)
<b>Regulatory Approvals</b>	EMI	FCC Class A
	EMS	IEC6100-4-2/3/4/5/6/8; IEC6100-6-2; IEC6100-6-4
	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-0600-24 Series Technical Specifications***Antaira Customer Service and Support**

(Antaira US Headquarter) + 844-268-2472

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

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

**Please report any problems to Antaira:**[www.antaira.com](http://www.antaira.com) / [support@antaira.com](mailto:support@antaira.com)[www.antaira.eu](http://www.antaira.eu) / [info@antaira.eu](mailto:info@antaira.eu)[www.antaira.com.tw](http://www.antaira.com.tw) / [info@antaira.com.tw](mailto:info@antaira.com.tw)**Any changes to this material will be announced on the Antaira website.**