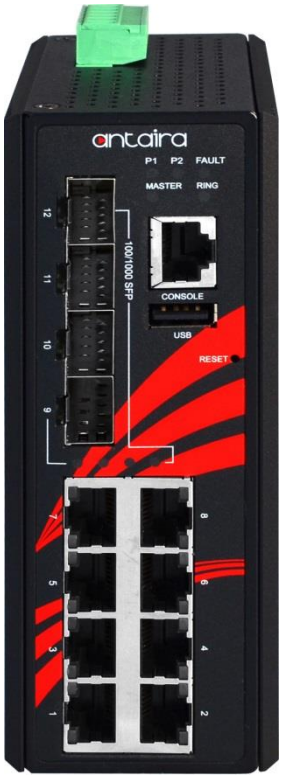
LMX-1204G-SFP Series

12-Port Industrial Gigabit Managed Ethernet Switches

8*10/100/1000Tx, 4*100/1000 SFP Slots



Version 1.0

User Manual

www.antaira.com

© Copyright 2016 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 © 2016 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 Managed Ethernet Switches

User Manual
Version 1.0 (January 2016)

This manual supports the following models:

- LMX-1204G-SFP
- LMX-1204G-SFP-T

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

Table of Contents

1. Introduction 1
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
2. Hardware Description 4
2.1 Physical Dimensions 4
2.2 Front Panel 5
2.3 Top View 5
2.4 LED Indicators 6
2.5 Reset Button 6
2.6 Ethernet Ports 7
2.7 Cabling 8
2.8 Wiring the Power Inputs 8
2.9 Wiring the Fault Alarm Contact 9
3. Mounting Installation 10
3.1 DIN-Rail Mounting 10
3.2 Wall Mounting 11
4. Hardware Installation 12
4.1 Installation Steps 12
5. Web Management 13
5.1 Web Console Configuration 13
5.1.1 About Web-Based Management 13
5.2 Basic Setting 15

5.2.1 System Information 15
5.2.2 Admin & Password 16
5.2.3 IP Setting.....16
5.2.4 IPv6 Neighbor Cache 17
5.2.5 IPv6 Settings 18
5.2.6 System Time 18
5.3 Port Management 19
5.3.1 Port Status.....19
5.3.2 Port Configuration 20
5.4 ERPS 21
5.4.1 ERPS Status 22
5.4.2 ERPS Configuration 23
5.4.3 Before Configuring ERPS.....24
5.5 Spanning Tree 31
5.5.1 RSTP Status.....32
5.5.2 RSTP Configuration 32
5.5.3 MSTI Status.....34
5.5.4 MSTI Configuration 35
5.6 IGMP Snooping 37
5.6.1 IGMP Settings 38
5.6.2 IGMP Snooping Status Table 38

5.7 802.1Q VLAN 39
5.7.1 802.1Q VLAN Settings 39
5.8 QoS (Traffic Prioritization) 41
5.8.1 QoS Classification 42
5.8.2 CoS Mapping.....43
5.8.3 ToS Mapping 44
5.9 Port Trunk 44
5.9.1 Trunk Status 45
5.9.2 Trunk Configuration 46
5.10 Port Mirroring 47
5.11 SNMP 48
5.11.1 SNMP Agent.....48
5.11.2 SNMP Trap Setting 50
5.12 DHCP Server / Rely 51
5.12.1 DHCP Client 53
5.12.2 DHCP Server.....53
5.12.3 DHCP Server Binding.....54
5.12.4 DHCP Relay 55
5.13 802.1X 56
5.13.1 802.1X Settings 57
5.13.2 Local Database 58
5.13.3 RADIUS Server 59

5.14 UPnP 60
5.14.1 UPnP 60
5.15 Modbus TCP 61
5.15.1 Enable Modbus TCP 61
5.15.2 MODBUS Data Map and Information 61
5.16 System Warning 67
5.16.1 Syslog Setting 67
5.16.2 System Event Log 68
5.16.3 SMTP Setting 68
5.16.4 Event Selection 69
5.16.5 Fault Alarm 70
5.17 MAC Table 71
5.17.1 MAC Address Table 71
5.17.2 MAC Table Configuration 72
5.18 Maintenance 72
5.18.1 Upgrade 72
5.18.2 Reboot 73
5.18.3 Default 73
5.19 Configuration 73
5.19.1 Save 74
5.19.2 Backup & Restore 74
5.19.3 Auto Load & Backup 75

5.20 Logout 75

6. Command Line Interface Management 76

6.1 About CLI Management 76

7. Technical Specifications 95

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 Technologies’ LMX-1204G-SFP series is a 12-port industrial Gigabit managed Ethernet switch embedded with 8*10/100/1000Tx Ethernet ports and 4*100/1000 dual rate SFP slots for fiber connections. The LMX-1204G-SFP 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 LMX-1204G-SFP 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). It also provides high EFT and ESD protection for industrial networking applications, such as, power/utility, water wastewater, oil/gas/mining, factory automation, security surveillance, ITS and any other outdoor or harsh environment.

1.2 Product Software Features

- Network Redundancy
  - STP, RSTP, MSTP, 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 8*10/100/1000Tx RJ45 Ports and 4*100/1000 SFP slots for fiber
  - Store-and-forward switching architecture
  - 8K MAC address table
  - Power line EFT protection: 2,000VDC; Ethernet ESD protection: 6,000VDC
- Power Input
  - DC 12~48V redundant with a 6-pin removal terminal block
  - One user programmable alarm relay contact
- Operating Temperature
  - Standard operating temperature models: -10°C to 70°C
  - Extended operating temperature models: -40°C to 75°C
- Case/Installation
  - IP-30 protection metal housing
  - DIN-Rail and wall mount design

1.4 Package Contents

- 1– LMX-1204G-SFP series: 12-port industrial gigabit managed Ethernet switch, with 8*10/100/1000Tx ports and 4*100/1000 SFP slots for fiber connectivity
- 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 LMX-1204G-SFP series: 12-port industrial gigabit managed Ethernet switches with 8*10/100/1000Tx ports and 4*100/1000Fx SFP slots.

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

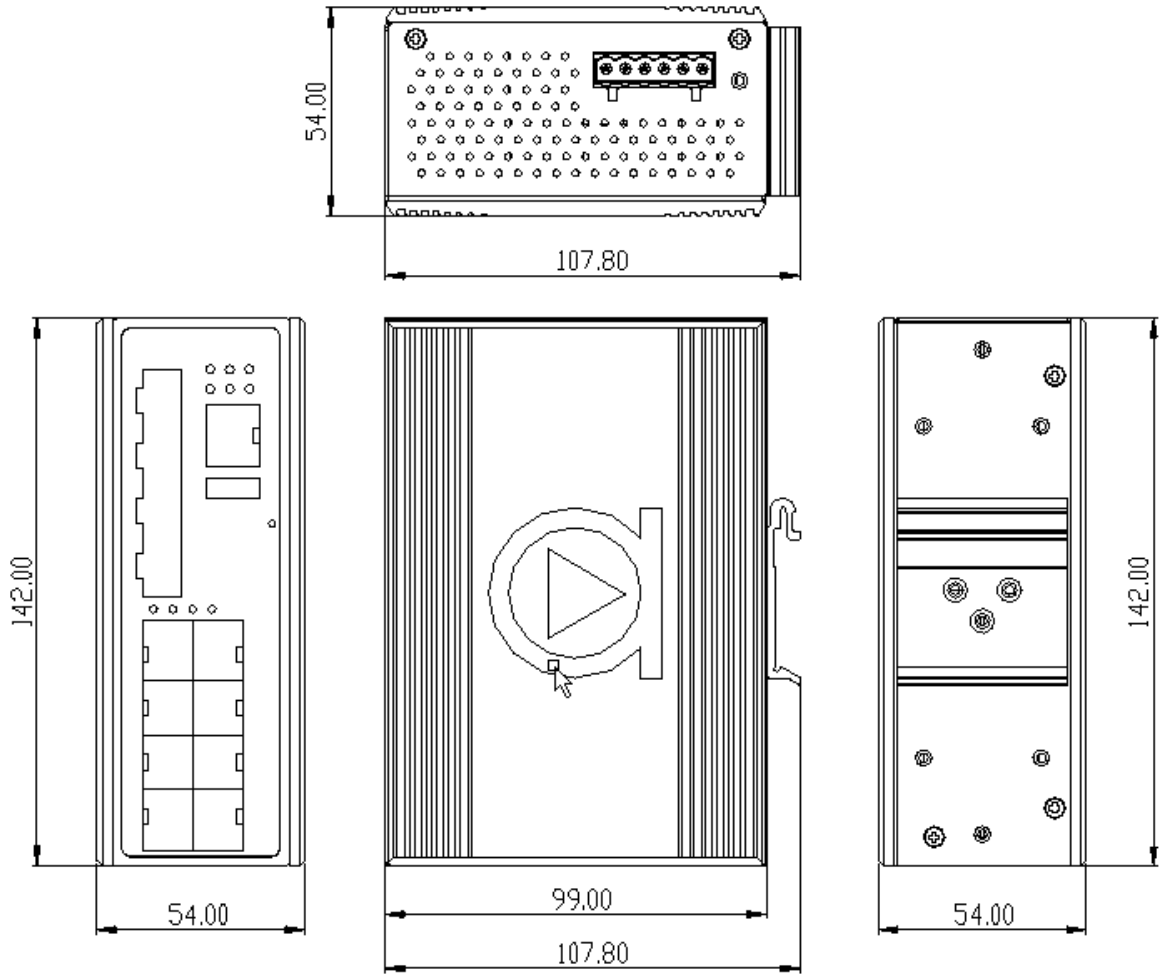


Figure2.1

LMX-1204G-SFP Series Physical Dimensions

2.2 Front Panel

The front panel of the LMX-1204G-SFP series industrial gigabit managed Ethernet switch is shown below in *Figure 2.2*.

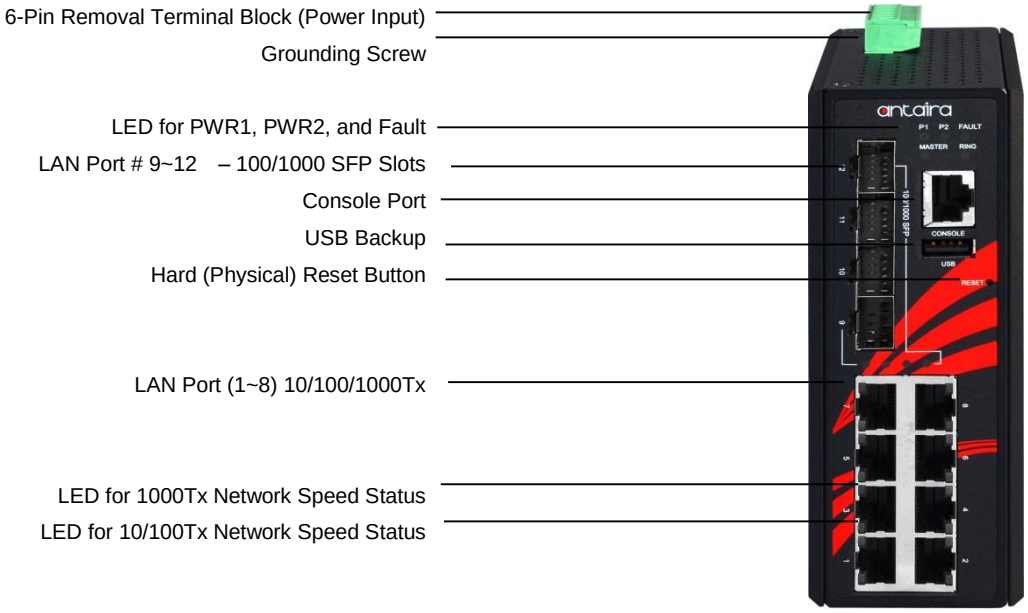


Figure2.2

The Front Panel of LMX-1204G-SFP Series

2.3 Top View

Figure 2.3, below, shows the top panel of the LMX-1204G-SFP series switch that is equipped with one 6-pin removal terminal block connector for dual DC power inputs 12~48VDC.

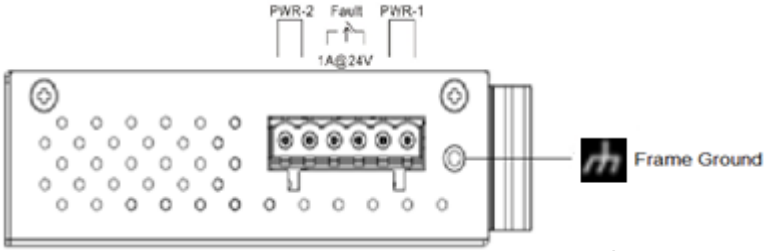


Figure2.3

Top Panel View of LMX-1204G-SFP Series

2.4 LED Indicators

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

LED	Color	Description	
P1	Green	On	Power input 1 is active
		Off	Power input 1 is inactive
P2	Green	On	Power input 2 is active
		Off	Power input 2 is inactive
Fault	Green/ Red	Green	Power input 1 or 2 is active
		Red	An applied alarm (such as port disconnect) has been triggered
		Off	System is booting or down
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 9~12 Link/ACT (SFP Port)	Green	On	Connected to Network
		Flashing	Network is active
		Off	Not Connected to Network
LAN Port 1 ~ 8 (Left LED)	Green 	On	Connected to network, 1000Mbps
		Flashing	Networking is active
		Off	Not connected to network
LAN Port 1~ 8 (Right LED)	Green 	On	Connected to network, 10/100Mbps
		Flashing	Networking is active
		Off	Not connected to network

Table 2.1 - LED Indicators for LMX-1204G-SFP Series

2.5 Reset Button

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

Seconds	Function
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/MDIX): The RJ-45 ports are auto-sensing for 10Base-T, 100Base-TX, or 1000Base-T 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/1000BASE-T 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.

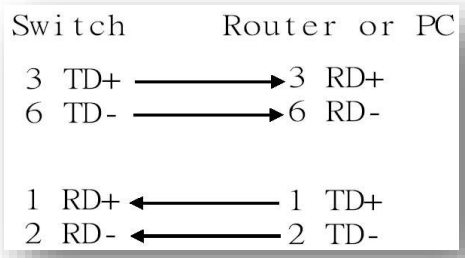


Figure 2.4
Straight-Through Cable Schematic

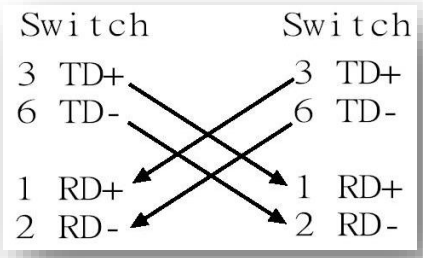


Figure 2.5
Crossover Cable Schematic

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.

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 2.6*.

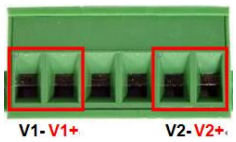


Figure 2.6 - Power Terminal Block

2. Tighten the wire-clamp screws to prevent the wires from loosening, as shown below in *Figure 2.7*.



Figure 2.7 - 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 2.8*. By inserting the wires, it will detect the fault status including power failure or port link failure (managed industrial switch only) and forma normally open circuit. An application example for the fault alarm contact is shown below in *Figure 2.8*.

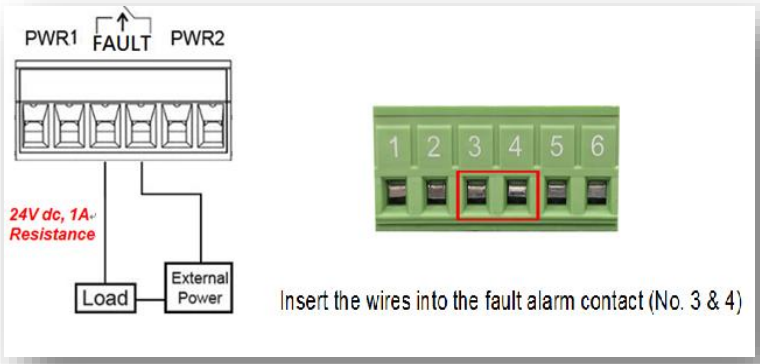


Figure 2.8 - Wiring the Fault Alarm Contact

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.

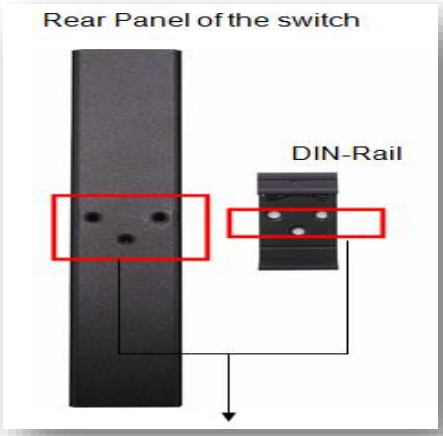


Figure 3.1

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.

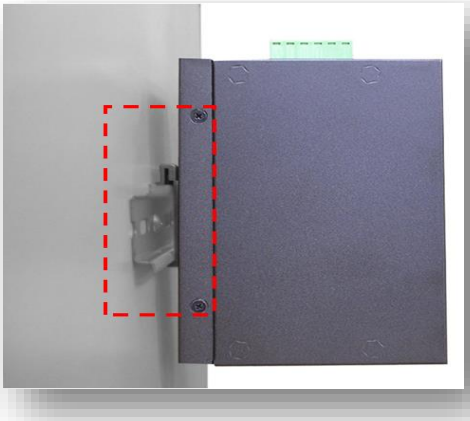


Figure 3.2

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.

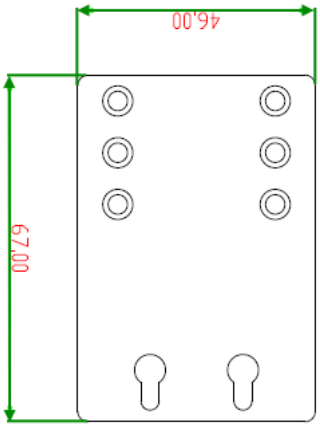


Figure 3.5
Wall Mounting Bracket Dimensions

4. Hardware Installation

4.1 Installation Steps

This section will explain how to install Antaira's LMX-1204G-SFP series: 12-port industrial gigabit managed Ethernet switches with 8*10/100/1000Tx ports and 4*100/1000 dual rate SFP fiber slots.

Installation Steps

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

5. Web Management

5.1 Web Console Configuration

This section introduces the configuration by web browser.

5.1.1 About Web-Based Management

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

Preparing for Web Console Configuration

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

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

System Login

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

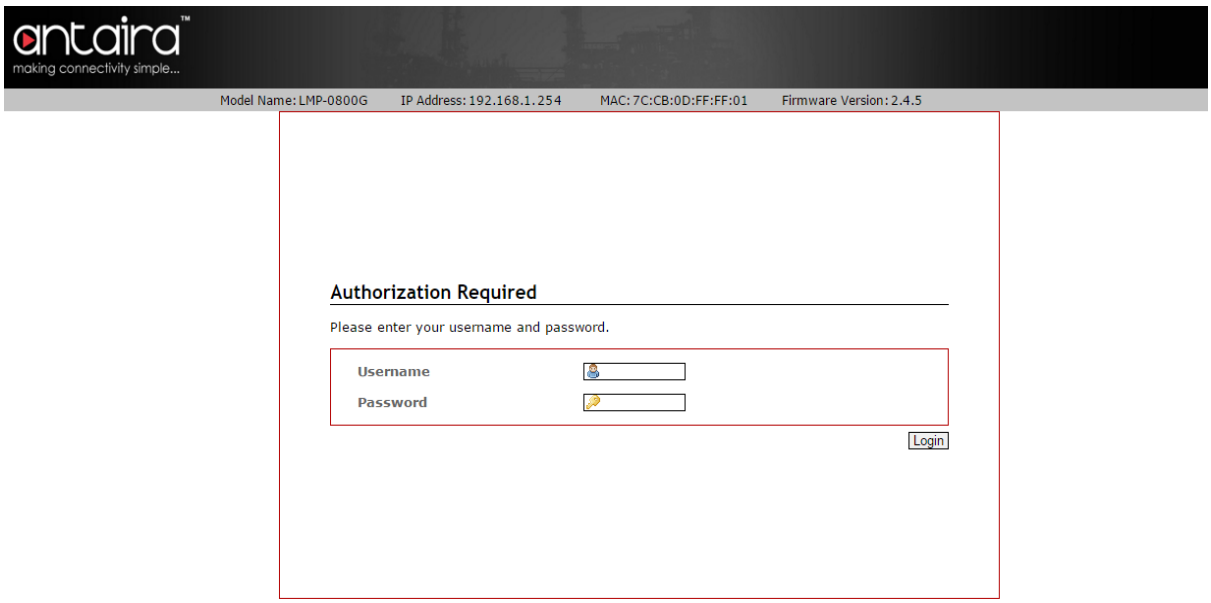


Figure 5.1 - Web Console "Login"

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

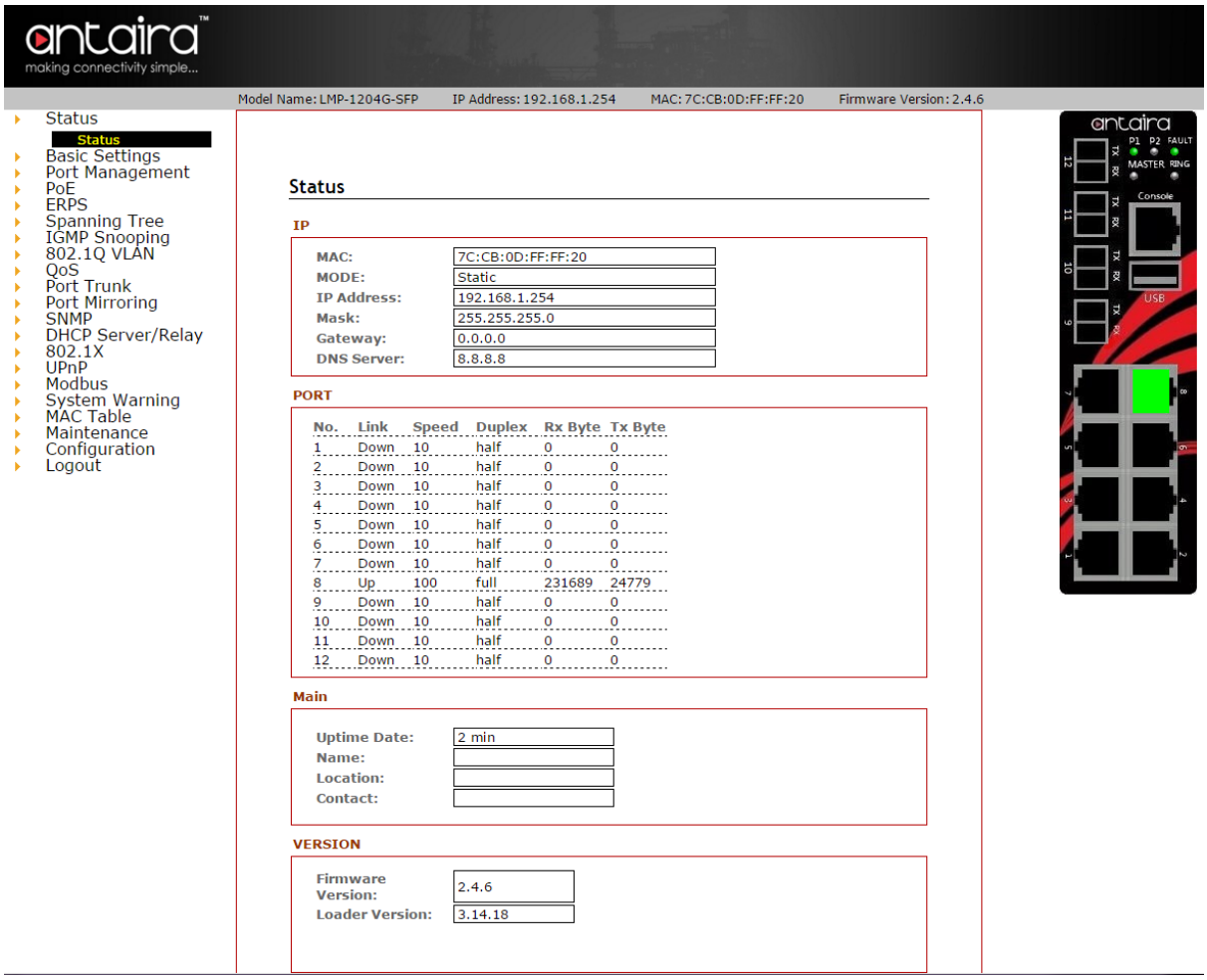


Figure 5.2 - Web Console Main (Status) Page

5.2 Basic Setting

5.2.1 System Information

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

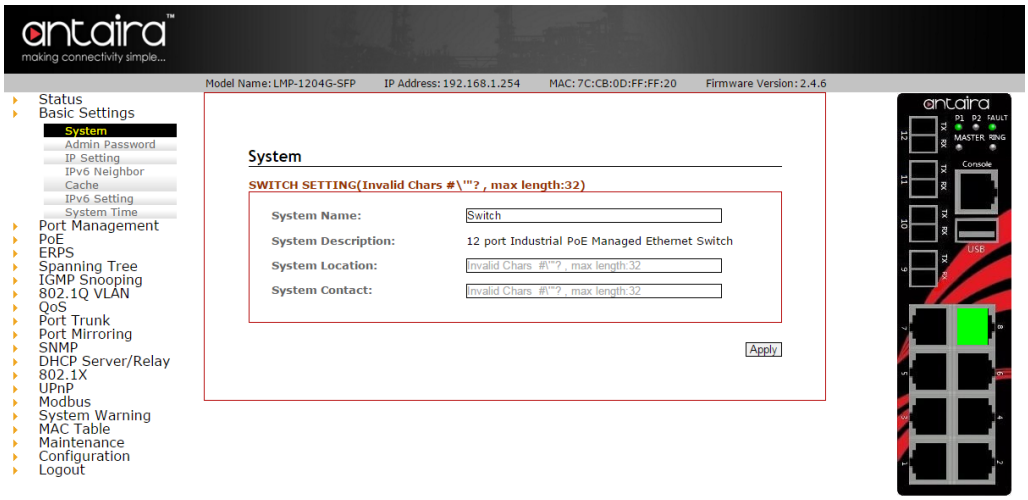


Figure 5.3 – Switch Settings (Status) Page

Terms	Value Description
System Name	Factory Default: Switch *Users can assign any name label to identify this managed node. By convention, the maximum length of the System Name is 32 characters and #, \, ‘, “, ? are invalid characters.
System Description	Factory Default: 12-port Managed Ethernet Switch The fixed system description is “n port Industrial Managed Ethernet Switch”.
System Location	Factory Default: blank *Users can use this field to insert The physical location of this switch (e.g., telephone closet, 3rd floor). The maximum length of System Location is 32 characters and #, \, ‘, “, ? are invalid characters.
System Contact	Factory Default: blank *Users can insert this field with the administrator of this switch together with information on how to contact this person. The maximum length of System Location is 32 characters and #, \, ‘, “, ? are invalid characters.
Apply	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.

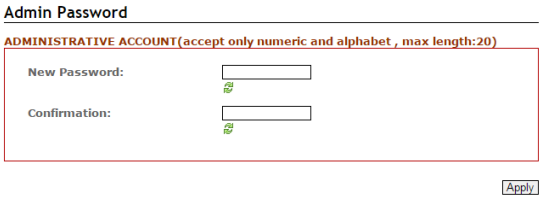


Figure 5.5 – Administrative Account

Terms	Value Description
New Password	Users can assign a New Password and the maximum length of the new password is 20 characters (alphabet and numeric values only)
Confirmation	Re-type the new password.
Apply	Click “Apply” to save changes.

Figure 5.6 – Admin & Password Description

5.2.3 IP Setting

Configure the managed switch’s IP setting information.

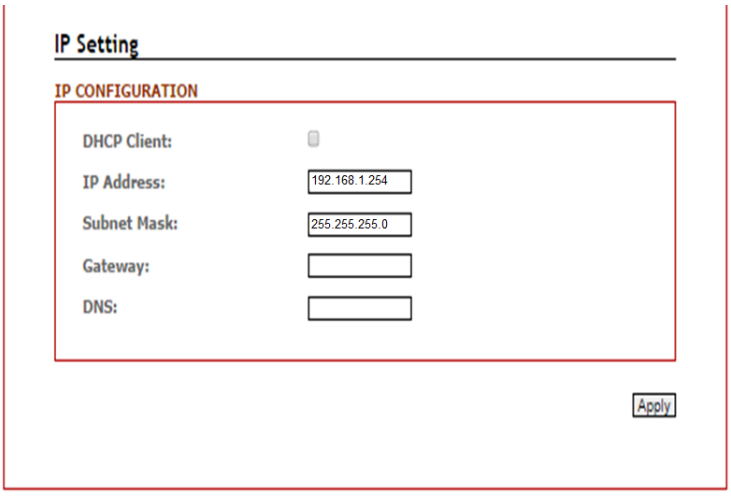


Figure 5.7 – IP Setting Information

Terms	Value Description
DHCP Client	Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
IP Address	The unit default IP is 192.168.1.254. Assign the IP address that the network is using. If DHCP client function is enabling, user does not require assigning the IP address. The network DHCP server will assign the IP address for the switch and it will be display in this column.
Subnet Mask	Assign the subnet mask of the IP address. If DHCP client function is enabling, user does not require to assign the subnet mask
Gateway	Assign the network gateway for the switch. If DHCP client function is enabled, the user is not required to assign the Gateway.
DNS	Assign the DNS IP address
Apply	Click the “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.



Figure 5.9 – IPv6 Neighbor Cache Status

5.2.5 IPv6 Settings

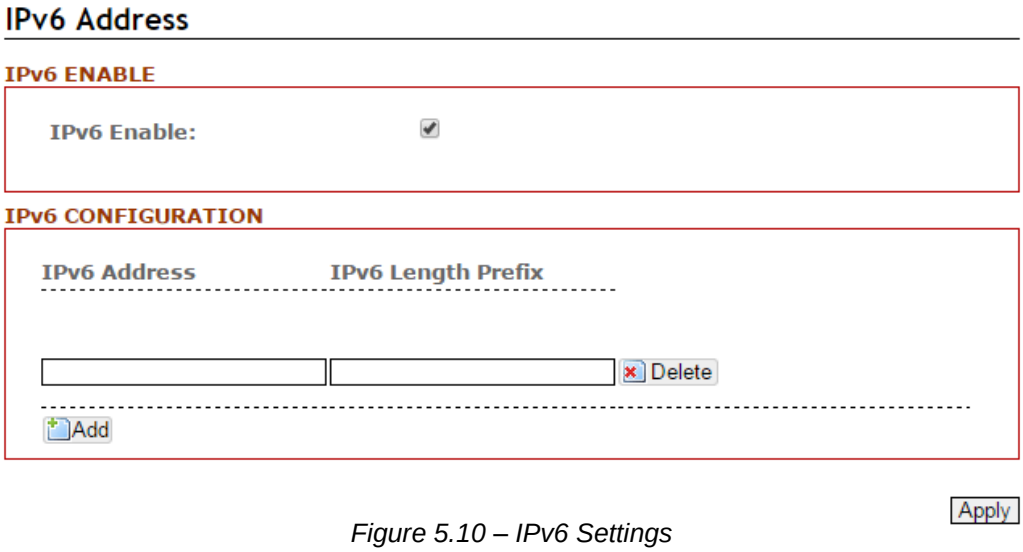


Figure 5.10 – IPv6 Settings

Terms	Value Description
IPv6 Enable/Disable	Check or uncheck the box to enable or disable IPv6 settings
IPv6 Address	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.
IPv6 Length Prefix	The prefix length of this IPv6 address
Apply	Click “Apply” to save changes.

Figure 5.11 – IPv6 Terms and Value Description

5.2.6 System Time

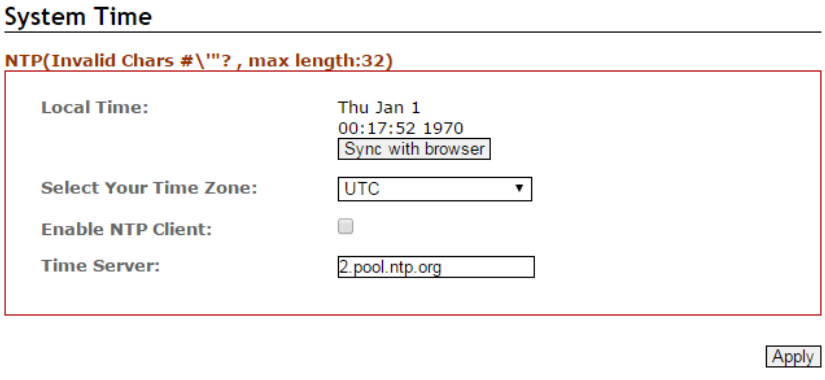


Figure 5.12 – System Time Settings

Terms	Value Description
Local Time	Users can define the switch's local time, or click "Sync with browser" button to have local time setup automatically.
Select Your Time Zone	Users can use dropdown box to setup the switch location time zone
Enable NTP Client	Enable or disable NTP function to get the time from the SNTP server.
Time Server	Users can define the Time Server info The maximum length of Time Server is 32 characters and #, \, ', ", ? are invalid characters.
Apply	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.

PORT

No.	Link	Speed	Duplex	Rx Byte	Tx Byte
1	Down	10	half	0	0
2	Down	10	half	0	0
3	Up	1000	full	34477090	4325515
4	Down	10	half	0	0
5	Down	10	half	0	0
6	Down	10	half	0	0
7	Down	10	half	0	0
8	Up	10	full	3918779	34196586

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.

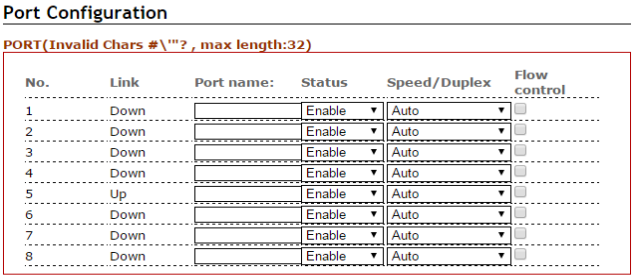


Figure 5.15 – Port Configuration Interface

Terms	Value Description
Port No.	It shows each port status: Up for link active, and Down for link inactive.
Port Name	Users can create or insert a value or label for each port’s identification. The maximum length of Port Name is 32 characters and #, \, ‘, “, ? are invalid.
Status	Enable or disable a port
Speed/Duplex	Users can set the bandwidth of each port as Auto-negotiation, gigabit full, gigabit half, 100 full,100 half,10 full,10 half mode.
Flow Control	Support symmetric and asymmetric mode to avoid packet loss when congestion occurred.
Apply	Click the “Apply” button to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Figure 5.16 – Port Configuration Description

5.4 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 they are planning to design or upgrade their ring network for future proof, Antaira is proud to introduce and implement Ethernet Ring Protection Switching (ERPS) protocol as a standard ring solution for network redundancy with all new industrial managed Ethernet switches. In order to provide users with the flexibility and compatibility when there are any existing switches that contains the standard ERPS protocol. **Ethernet Ring Protection Switching (ERPS)**, defined in ITU-T G8032, implements a protection switching mechanism for Ethernet traffic in a ring topology. By performing the ERPS function, potential loops in a network can be avoided by blocking traffic to flow to the ring protection link (RPL) to protect the entire Ethernet ring.

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

5.4.1 ERPS Status

Below is the REPS LED information on the front Panel

Terms	Value Description
MASTER	**ON(Green):** If one of ERPS ports is set to RPL “Owner”. **OFF(Gray)**: No port is set to RPL “Owner”
RING	**ON(Green)**: ERPS works well. **ON(Flashing)**: The ring is open, one of ERPS node link failed or link down or ERPS is misconfigured. **OFF(Gray)**: ERPS is disabled.

Below, *Figure 5.17,* shows the network redundancy ring status with the Ethernet Ring Protection Switch (ERPS) protocol.

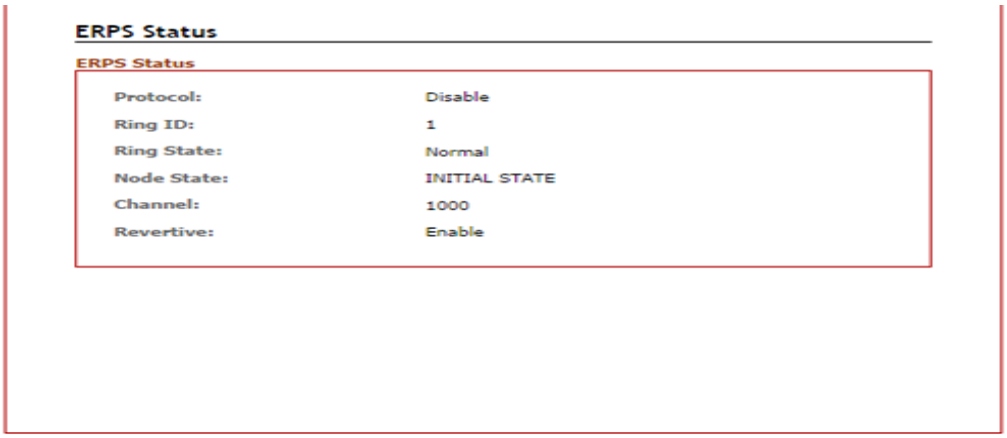


Figure 5.17 – Redundant Ring Network – ERPS Status

Terms	Value Description
Ring State	**Abnormal**: After enabling ERPS, one of ERPS node link failed or link down. **Normal**: ERPS disable or after enabling ERPS, the ring is closed and working well.
Node State	**INITIAL**: ERPS disable **PROTECTION**: One of ERPS node link failed or link down. **PENDING**: The ring is from open to closed and the WTR timer is counting down. **IDLE**: After WTR timer is expired or users issue "Clear" command by CLI, the ring is working well.

5.4.2 ERPS Configuration

Below, *Figure 5.18* shows the ERPS configuration interface.

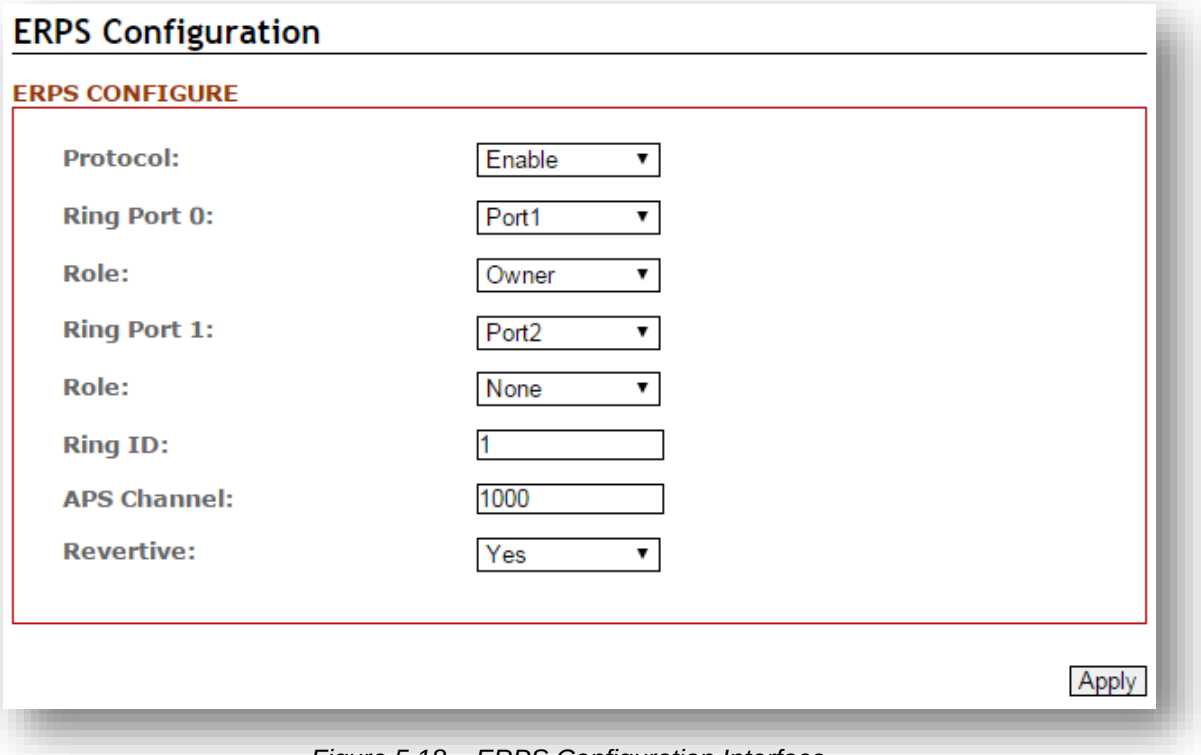


Figure 5.18 – ERPS Configuration Interface

Terms	Value Description
Protocol	"Enable" or "Disable" ERPS protocol
Ring Port 0	ERPS ring port 0, it could be map to real switch port 1 – port 6. Do not set the same as Ring port 1.
Ring Port 1	ERPS ring port 1, it could be map to real switch port 1 – port 6. Do not set the same as Ring port 0.
Role	Set the ERPS role as Owner, Neighbor or None. ***[Owner]*** *In charge of blocking one side of RPL link. It will prevent the packet flow from its blocked port.* ***[Neighbor]*** *In charge of blocking one side of RPL link. It will prevent the packet flow from its blocked port.* ***[None]*** *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.*
Ring ID	ERPS ring ID, ranges from 1 to 239. Ring ID distinguishes different Ring

	topology.
Channel	ERPS Channel ID, ranges from 1 to 4094. It's a channel to send PDUs of ERPS.
Revertive	Set to Revertive (yes) or Non-revertive (no). The revertive mode works only under the scenario A at the RPL Owner node. ***[Revertive]*** *While the revertive mode is set, the RPL link will be blocked in 5 minutes after recovery form link failure situation. Otherwise, it will remain unchanged of the blocking state. That is, the failed link port will block permanently until the next event happen.* ***[Non-Revertive]*** *The failed ring link the port attached to it will remain blocked even the situation is eliminated.*
Apply	Click the "Apply" button to save changes.

Figure 5.19 – ERPS Configuration Terms & Description

5.4.3 Before Configuring ERPS

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

Step 1: Login the switch with a web browser.

Step 2: Open the "RSTP Configuration" page under the "Spanning Tree" manual shown below in *Figure 5.20*.

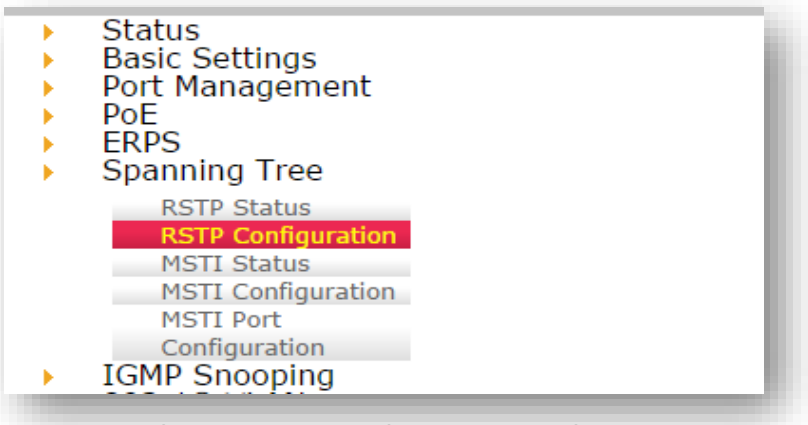


Figure 5.20 – Spanning Tree Manual

Step 3: When the RSTP/CIST Configuration page shows up, set “Mode” to “Disable” as shown in *Figure 5.21*.

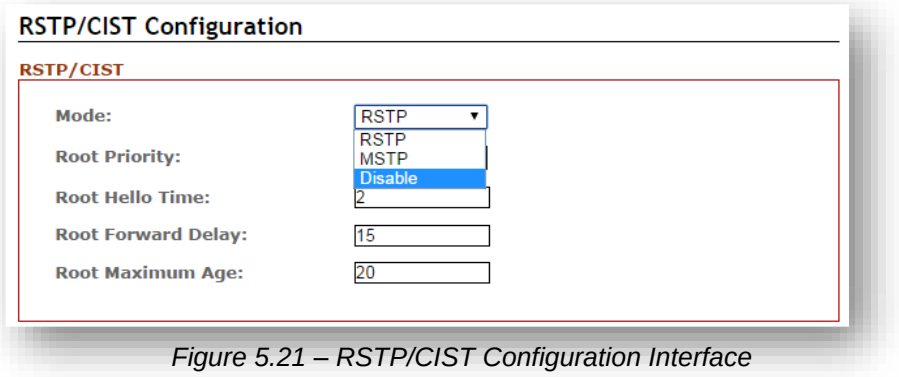


Figure 5.21 – RSTP/CIST Configuration Interface

Step 4: Press the Apply button in the lower right corner as shown below in *Figure 5.22*.

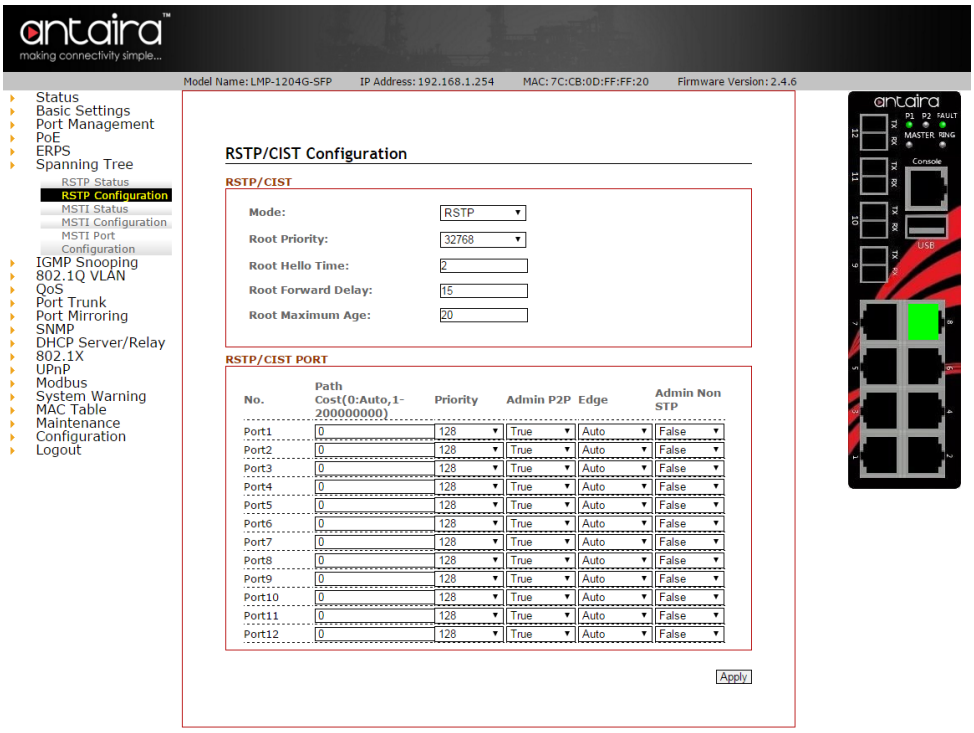


Figure 5.22 – RSTP/CIST Configuration Interface

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 5.23 or the non-configured architecture shown in Figure 5.27.

5.4.3.1 Scenario A – RPL Configured Architecture

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

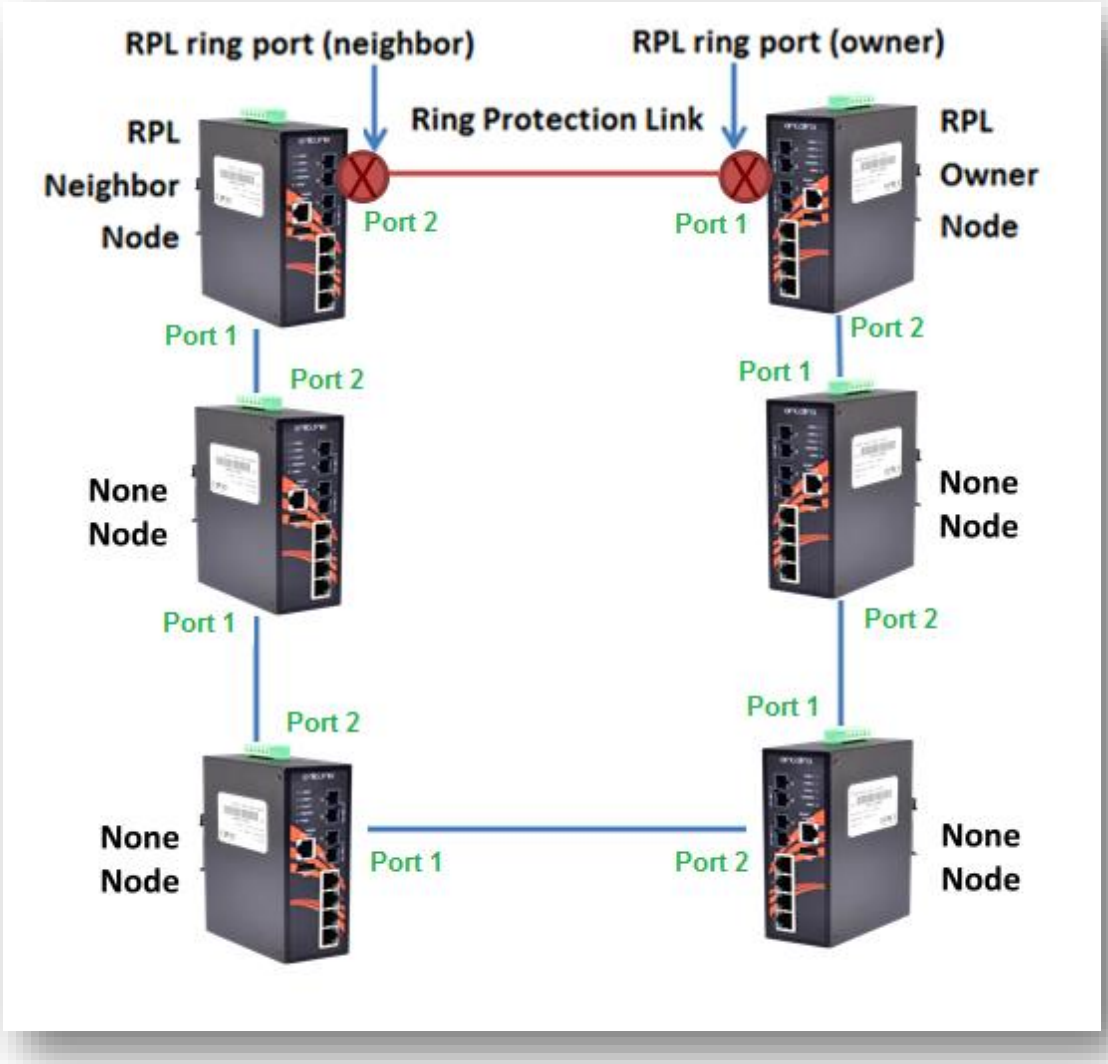


Figure 5.23 – RPL-Configured Architecture

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.***

There is only one RPL Owner Node could be set in a ring network. In order to set up the RPL Owner Node, choose a switch and enable "Protocol" under the ERPS Configuration interface, and follow below steps and use *Figure 5.24*, below, as an example:

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

Step 2: Choose a specific port from the dropdown box next to "ring port 1", then set it as "**None**" from the dropdown box next to "Role" (which locates below "ring port 1"). At this point, "**Port 2**" was chosen as example.

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

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

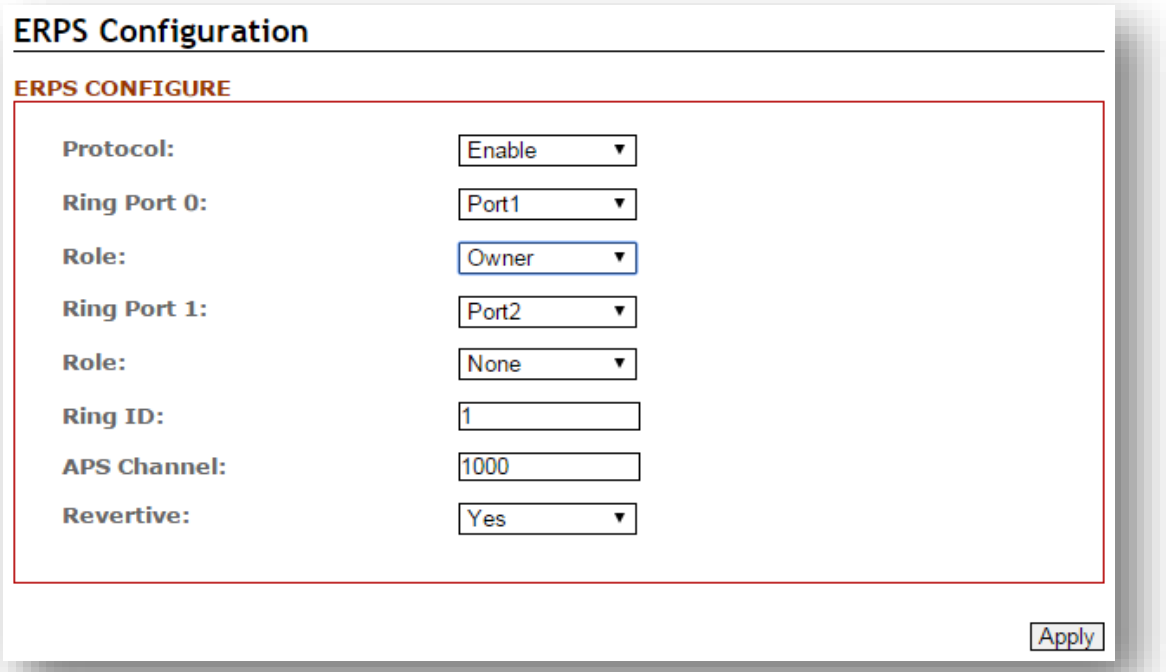


Figure 5.24 – RPL Owner Node Setup Example

Please be aware, when the revertive mode is set to "**Yes**", the ring will recover the same way as explained in *Figure 5.23*, 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 5.25*. So the link between neighbor port and owner port forms the ring protection link (RPL). After the configurations, press the "Apply" button on the bottom right corner to save the settings.

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

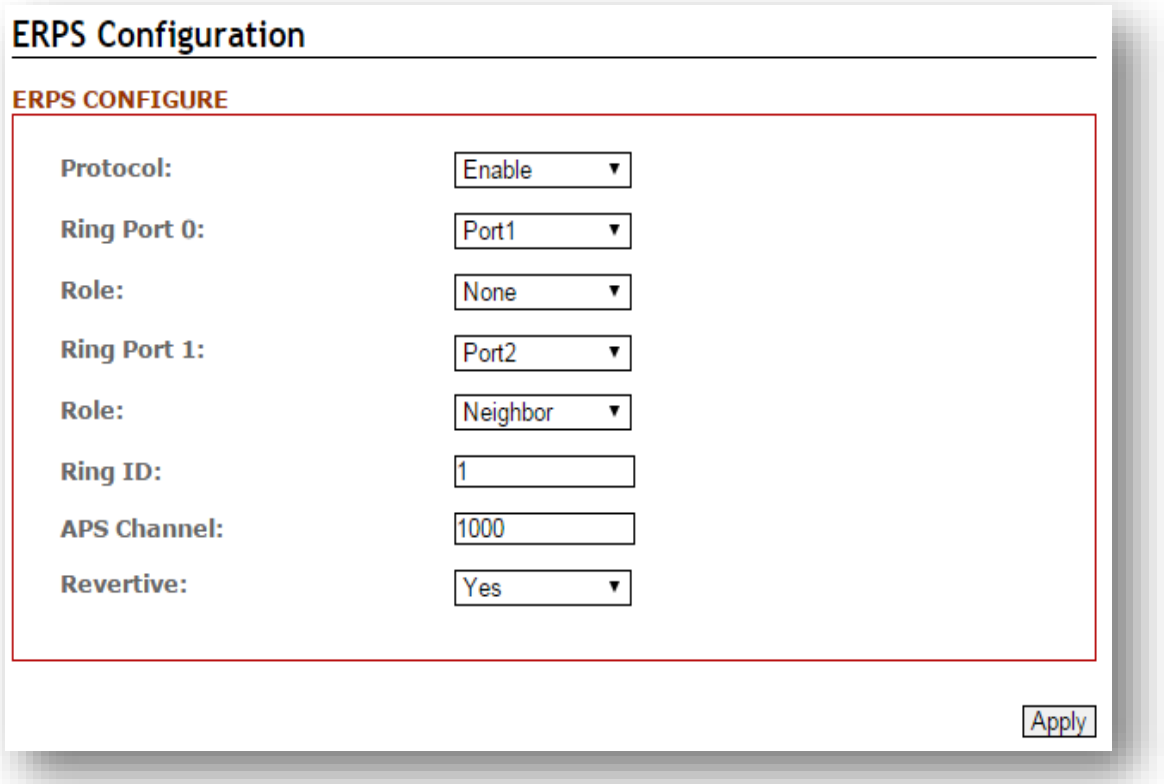


Figure 5.25 – RPL Neighbor Node Setup Example

[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 5.23*. Please be sure no duplicate port number has been chosen within a managed switch's ERPS ring setting, the incorrect configurations may lead to unexpected errors.

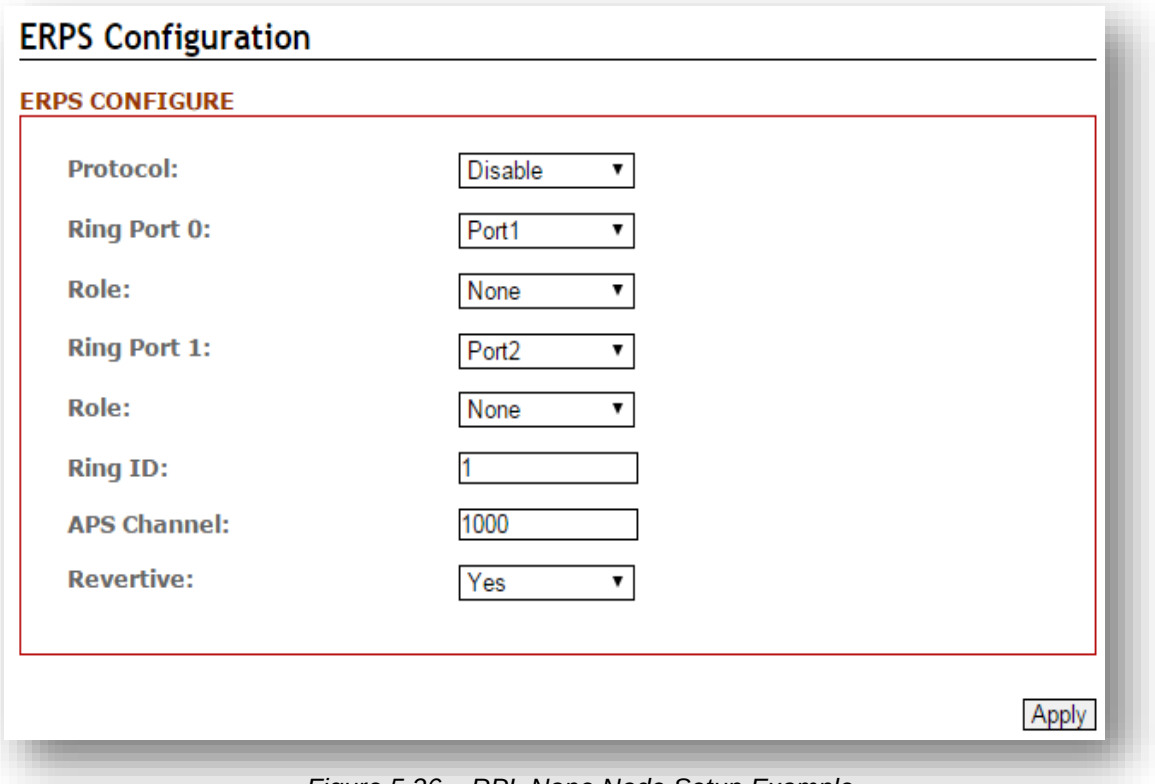


Figure 5.26 – RPL None Node Setup Example

5.4.3.2 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.

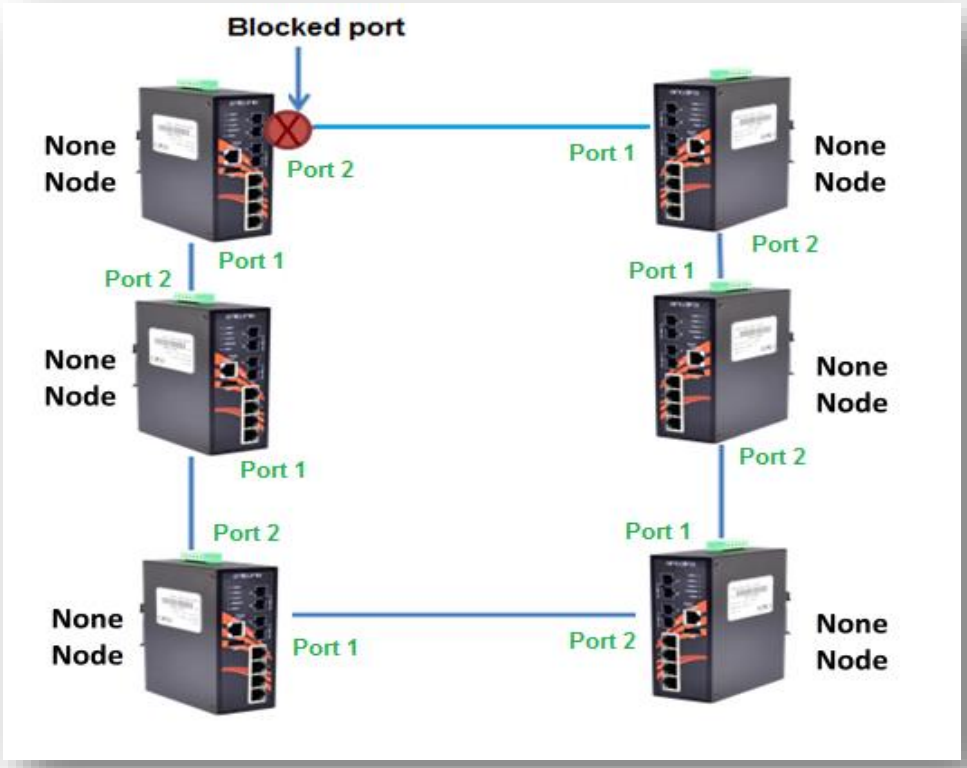


Figure 5.27 – Non-Configured Architecture

> ***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 5.27*, 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 5.28*, below, shows the configurations as a reference.

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

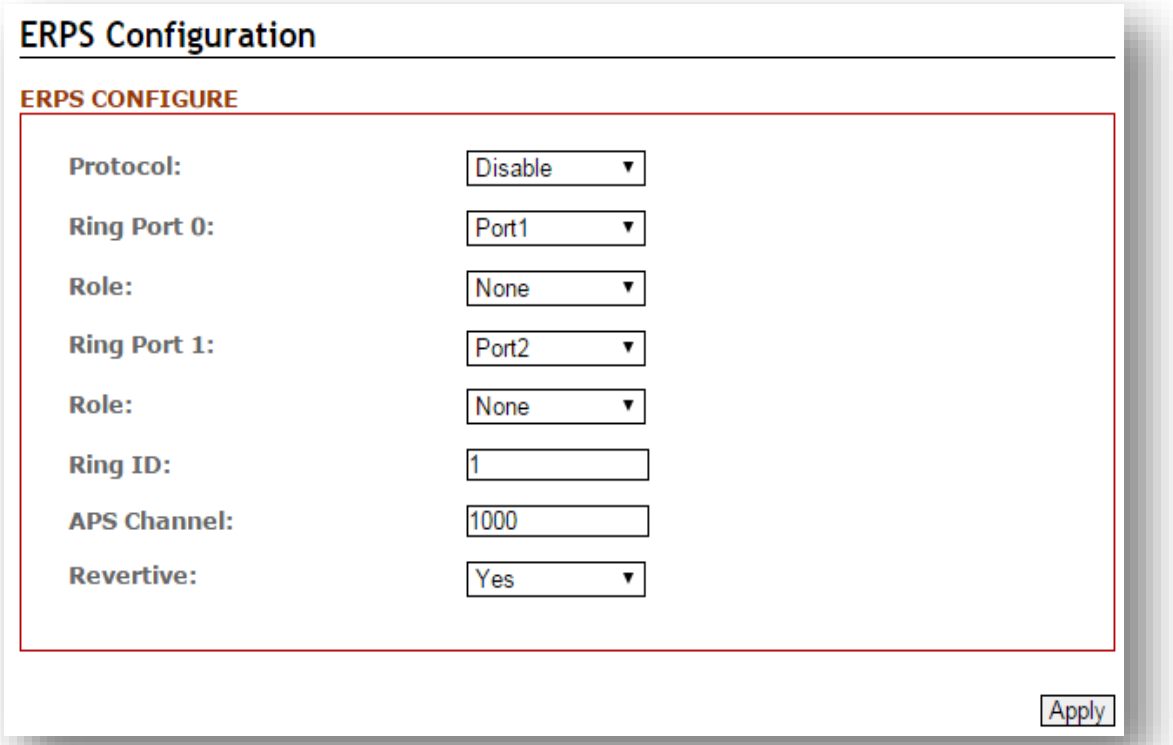


Figure 5.28 – Non-Configured Architecture Setup

.

5.5 Spanning Tree

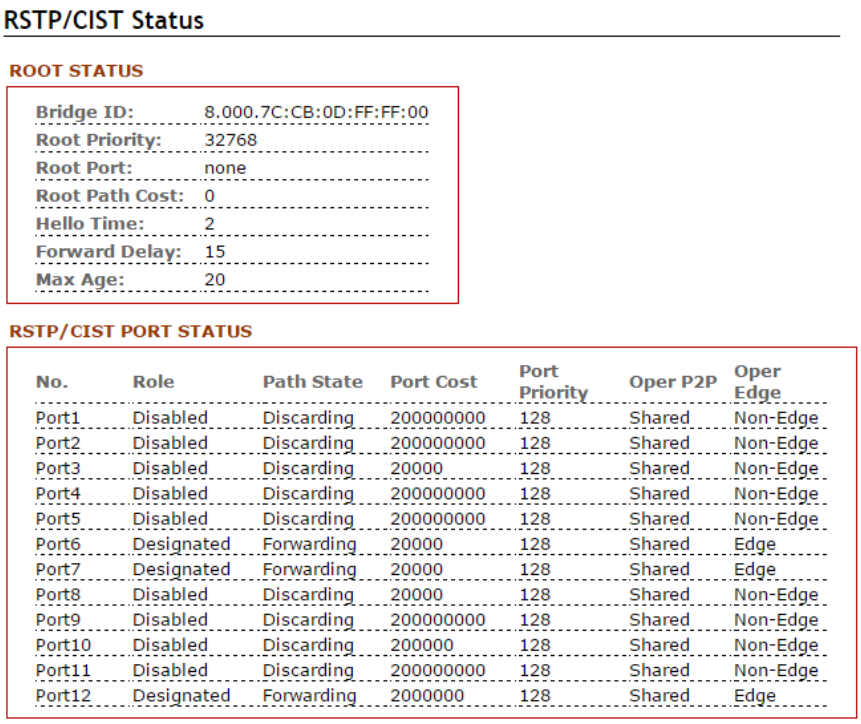
The Spanning Tree Protocol (STP), defined in the IEEE Standard 802.1d, can be created within a mesh network of connected layer-2 switches.

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.

5.5.1 RSTP Status

Figure 5.29 shows the RSTP algorithm results.



RSTP/CIST Status

ROOT STATUS

Bridge ID:	8.000.7C:CB:0D:FF:FF:00
Root Priority:	32768
Root Port:	none
Root Path Cost:	0
Hello Time:	2
Forward Delay:	15
Max Age:	20

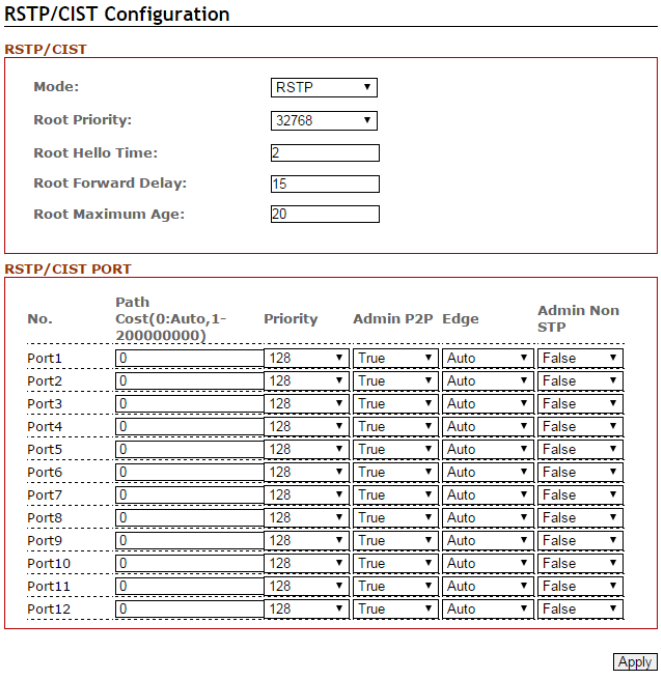
RSTP/CIST PORT STATUS

No.	Role	Path State	Port Cost	Port Priority	Oper P2P	Oper Edge
Port1	Disabled	Discarding	200000000	128	Shared	Non-Edge
Port2	Disabled	Discarding	200000000	128	Shared	Non-Edge
Port3	Disabled	Discarding	20000	128	Shared	Non-Edge
Port4	Disabled	Discarding	200000000	128	Shared	Non-Edge
Port5	Disabled	Discarding	200000000	128	Shared	Non-Edge
Port6	Designated	Forwarding	20000	128	Shared	Edge
Port7	Designated	Forwarding	20000	128	Shared	Edge
Port8	Disabled	Discarding	20000	128	Shared	Non-Edge
Port9	Disabled	Discarding	200000000	128	Shared	Non-Edge
Port10	Disabled	Discarding	200000	128	Shared	Non-Edge
Port11	Disabled	Discarding	200000000	128	Shared	Non-Edge
Port12	Designated	Forwarding	2000000	128	Shared	Edge

Figure 5.29 – RSTP Information Interface

5.5.2 RSTP Configuration

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



RSTP/CIST Configuration

RSTP/CIST

Mode:	RSTP
Root Priority:	32768
Root Hello Time:	2
Root Forward Delay:	15
Root Maximum Age:	20

RSTP/CIST PORT

No.	Path Cost(0:Auto,1-200000000)	Priority	Admin P2P	Edge	Admin Non STP
Port1	0	128	True	Auto	False
Port2	0	128	True	Auto	False
Port3	0	128	True	Auto	False
Port4	0	128	True	Auto	False
Port5	0	128	True	Auto	False
Port6	0	128	True	Auto	False
Port7	0	128	True	Auto	False
Port8	0	128	True	Auto	False
Port9	0	128	True	Auto	False
Port10	0	128	True	Auto	False
Port11	0	128	True	Auto	False
Port12	0	128	True	Auto	False

Apply

Figure 5.30 – RSTP Configuration Interface

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

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

Figure 5.31 – RSTP Configuration Terms & Value Description

MSTP (Multiple Spanning Tree Protocol)

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

5.5.3 MSTI Status

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

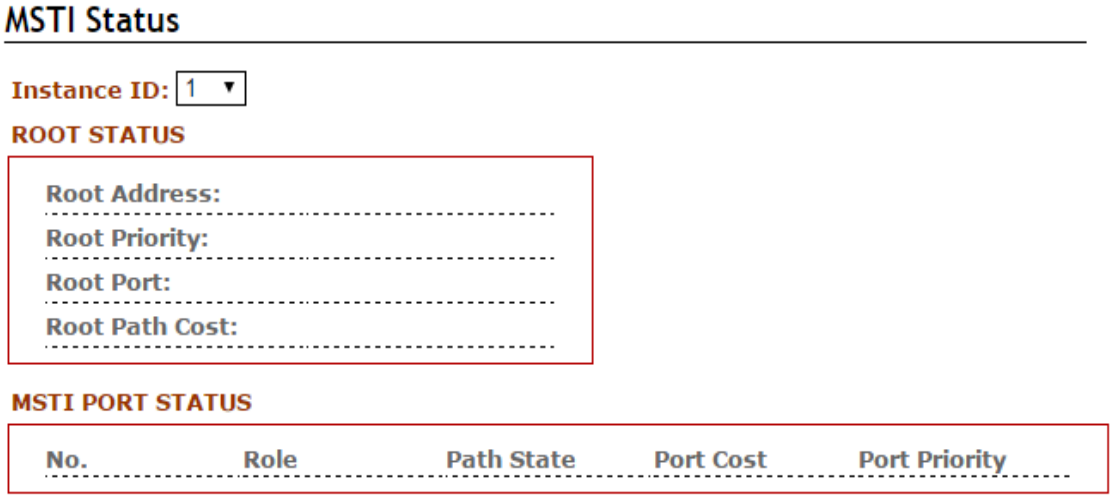


Figure 5.32 – MSTI Status Interface

5.5.4 MSTI Configuration

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

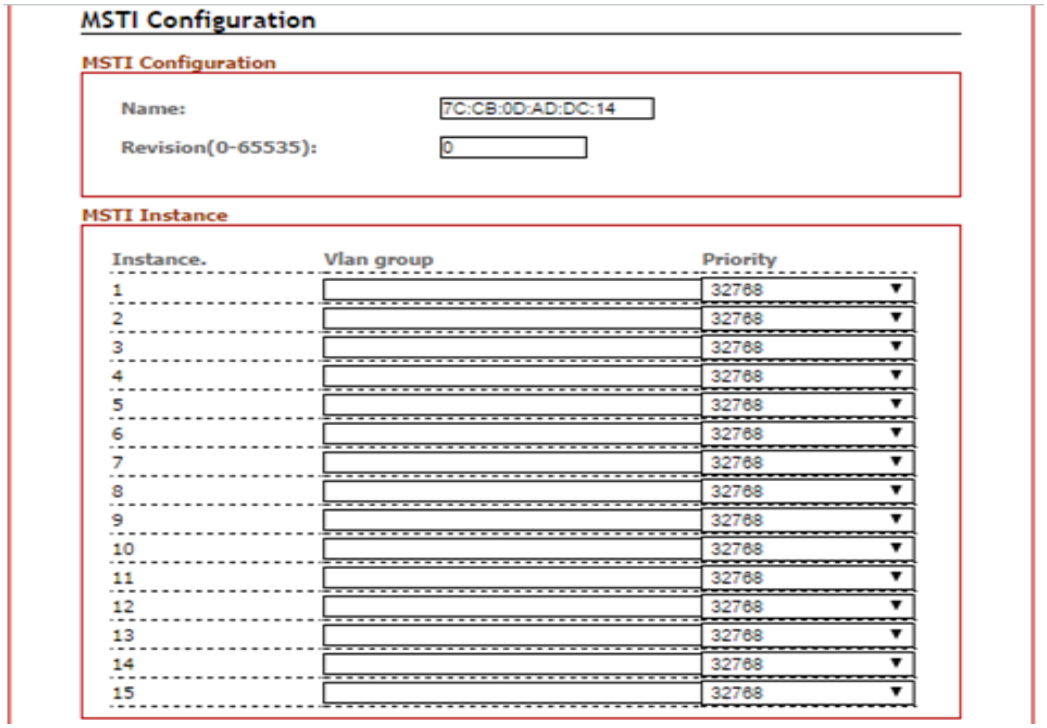


Figure 5.33 – MSTI Configuration Interface

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

Figure 5.34 – MSTI Configuration –Terms & Value Description

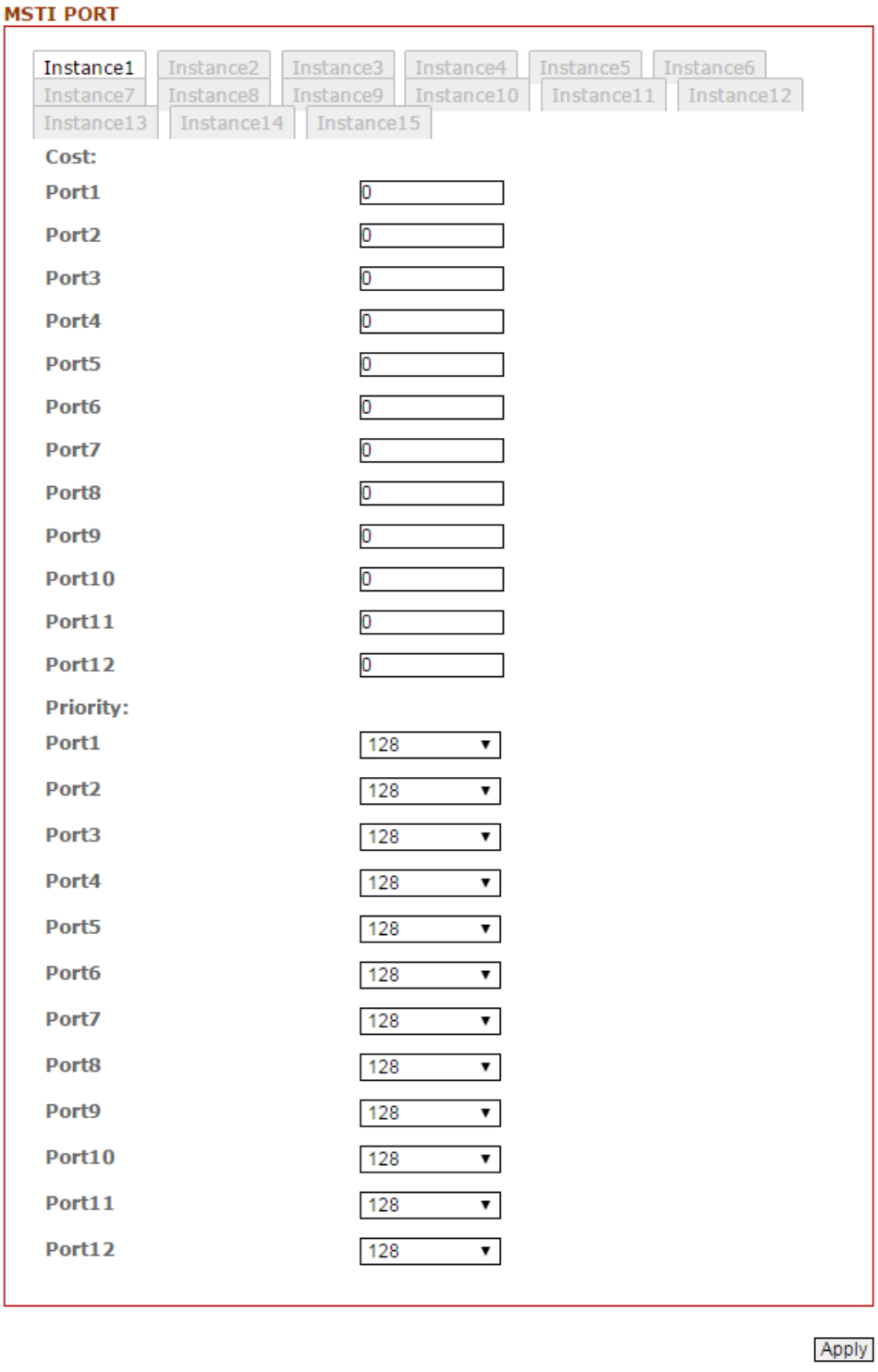


Figure 5.35 – MSTI Port Configuration Interface

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.
Apply	Click the “Apply” button to save changes.

Figure 5.36 – MSTI Port Configuration Terms & Value Description

5.6 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.

5.6.1 IGMP Settings

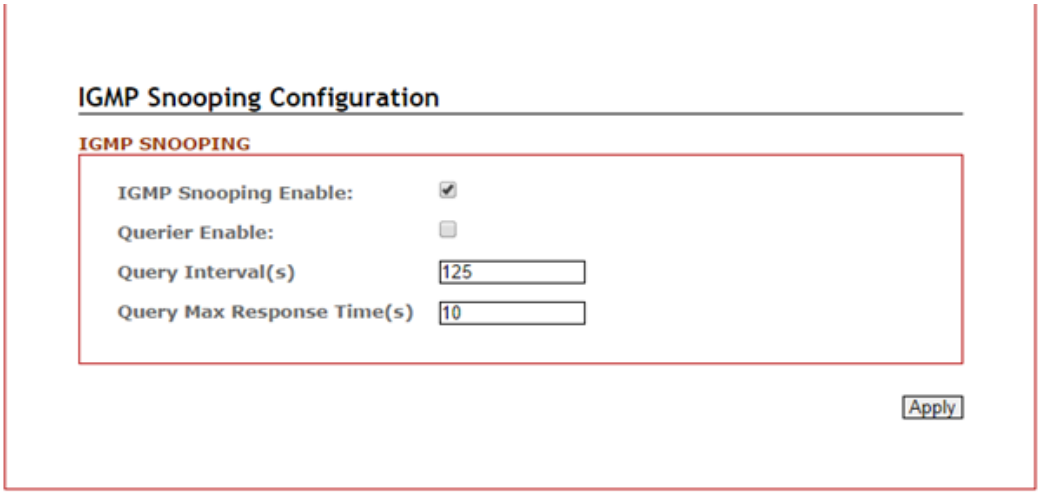


Figure 5.37 – IGMP Snooping Settings Interface

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

Figure 5.38 – IGMP Snooping Settings Terms & Value Description

5.6.2 IGMP Snooping Status Table

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

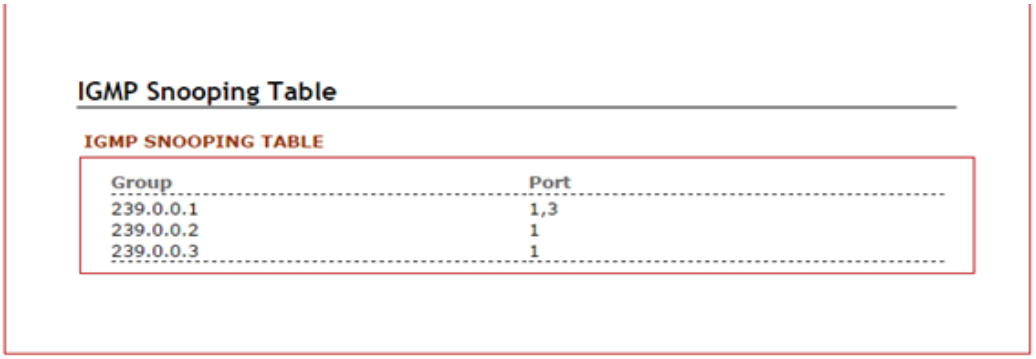


Figure 5.39 – IGMP Snooping Status Table

5.7 802.1Q 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 venders. IEEE 802.1Q VLAN uses a technique to insert a "tag" into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

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.

5.7.1 802.1Q 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.

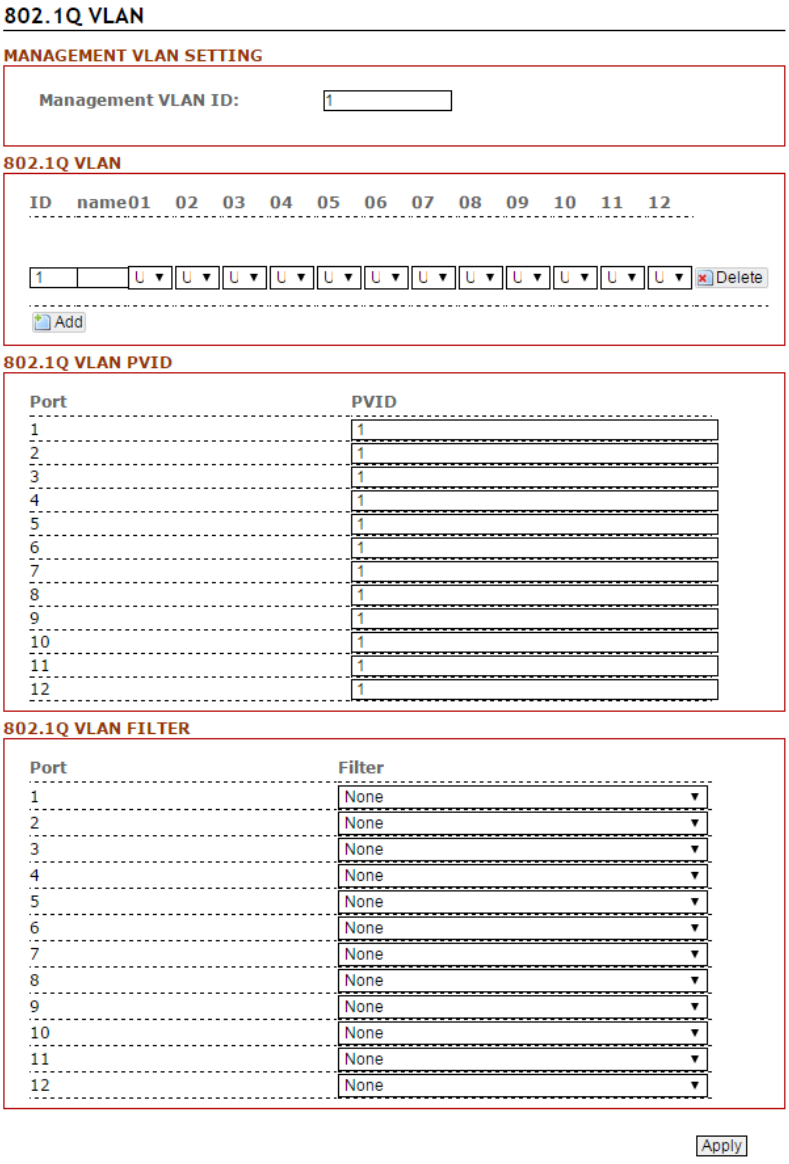


Figure 5.40 – 802.1Q VLAN Settings Interface

Terms	Value Description
Management VLAN ID	Set the VLAN ID of management VLAN. Users have to configure other settings done, and configure this field finally.
802.1Q VLAN ID	The ID of this VLAN. VLANs that have the same ID will consider being the same group.
802.1Q VLAN Name	The name of this VLAN. The same VLAN in the different switches can have different name.
802.1Q VLAN PVID	When a frame comes into the port, it will be tagged with the PVID if the frame is without VLAN tag.

802.1Q VLAN Filter	An incoming frame will be dropped or kept forwarding according to the filter. • None: All frames can keep forwarding. • Tagged: Only the frames with 802.1Q tag can keep forwarding, untagged frames will be dropped. • Untagged: Only the frames without 802.1Q tag can keep forwarding, tagged frames will be droped.
Apply	Click the “Apply” button to save changes.

Figure 5.41 – 802.1Q VLAN Settings Terms

5.8 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.

5.8.1 QoS Classification

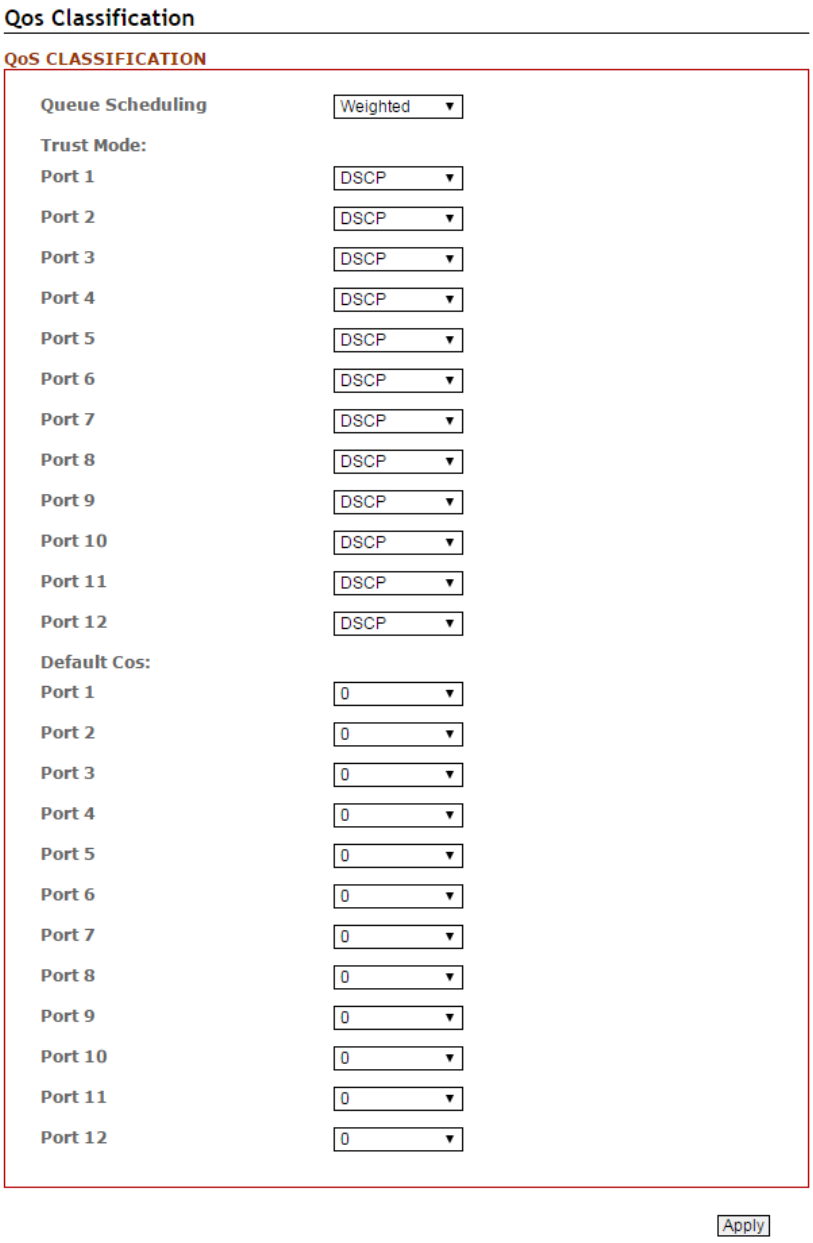


Figure 5.42 – QoS Classification Interface

Terms	Value Description
Queue Scheduling	Users can set it as “Weighted” or “Strict” **Weighted Mode:** An 6, 4, 4, 3, 2, 1 weighting is applied to each round robin priority queue. **Strict Mode:** It gives egress queues with higher priority to be transmitted first before lower priority queues are serviced.

Trust Mode	Users can select the trust mode with either DSCP or Cos. When select DSCP, only trusted DSCP (Differentiated Services Code Point) values are mapped to a specific QoS class and drop precedence level (DPL). Frames with untrusted DSCP values are treated as non-IP frames. **CoS:** (Class Of Service) is well known as 802.1p. It describes that the output priority of a packet is determined by user priority field in 802.1Q VLAN tag. The priority value is supported 0to7COS value map to 4 priority **Queues:** Highest, SecHigh, SecLow, and Lowest.
Default Cost	Users can set each port's priority queue from 0 to 7 by clicking from dropdown box; of which 0 is the Highest, and 7 is the Lowest
Apply	Click the "Apply" button to save changes.

Figure 5.43 – QoS Classification Terms & Value Description

5.8.2 CoS Mapping

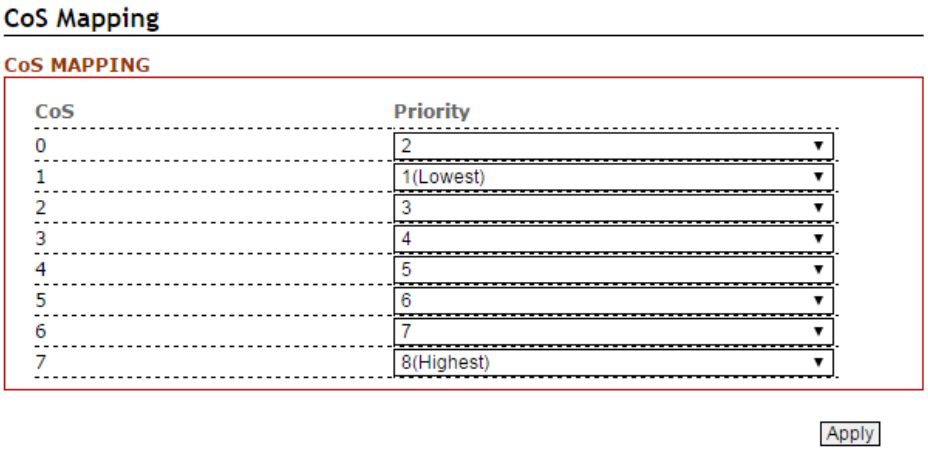


Figure 5.44 – CoS Mapping Interface

Terms	Value Description
Cos Value (0~7)	User can assign each port a CoS value from 0 to 7. According to the IEEE 802.1p, user can define each CoS value in 8 priority queues: from Low to High.
Apply	Click the "Apply" button to save changes.

Figure 5.45 – QoS Mapping Terms & Value Description

5.8.3 ToS Mapping

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

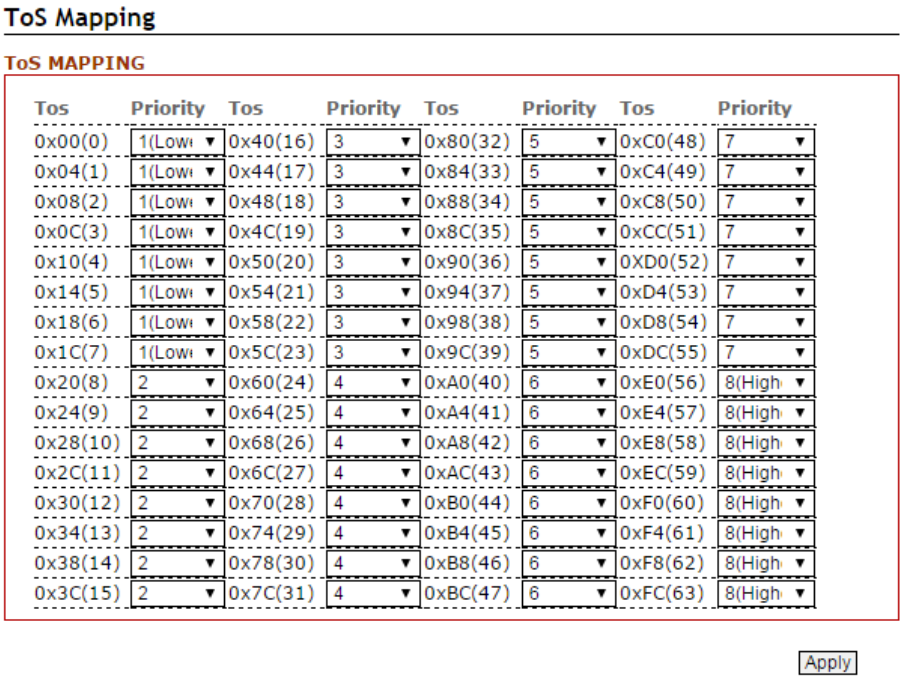


Figure 5.46 – ToS Mapping Interface

Terms	Value Description
ToS	Users can assign each ToS value with 8 priority queues form 1 (Low) to 8 (High).
Apply	Click the “Apply” button to save changes.

Figure 5.47 – ToS Mapping Terms & Value Description

5.9 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.

5.9.1 Trunk Status

The below graph is the Port Trunk Status.

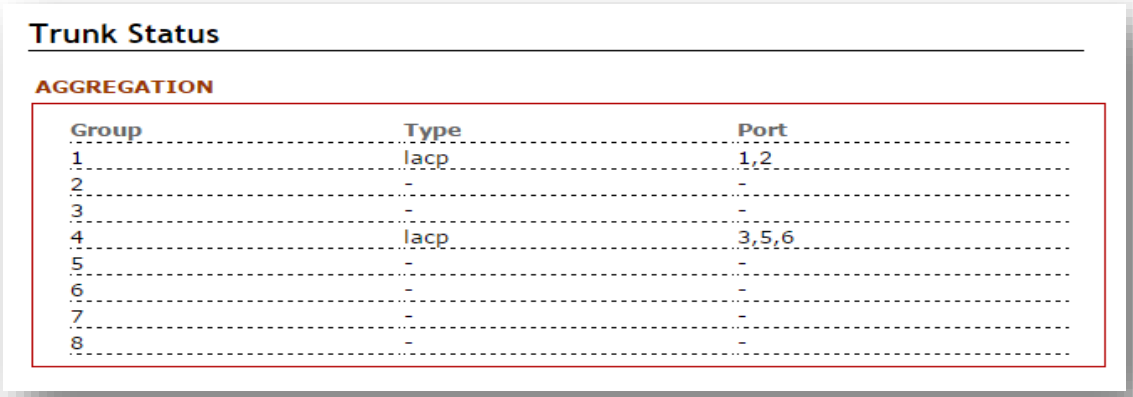


Figure 5.48 – Port Trunk Status

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 5.49 – Port Trunk Terms and Value Description

5.9.2 Trunk Configuration

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

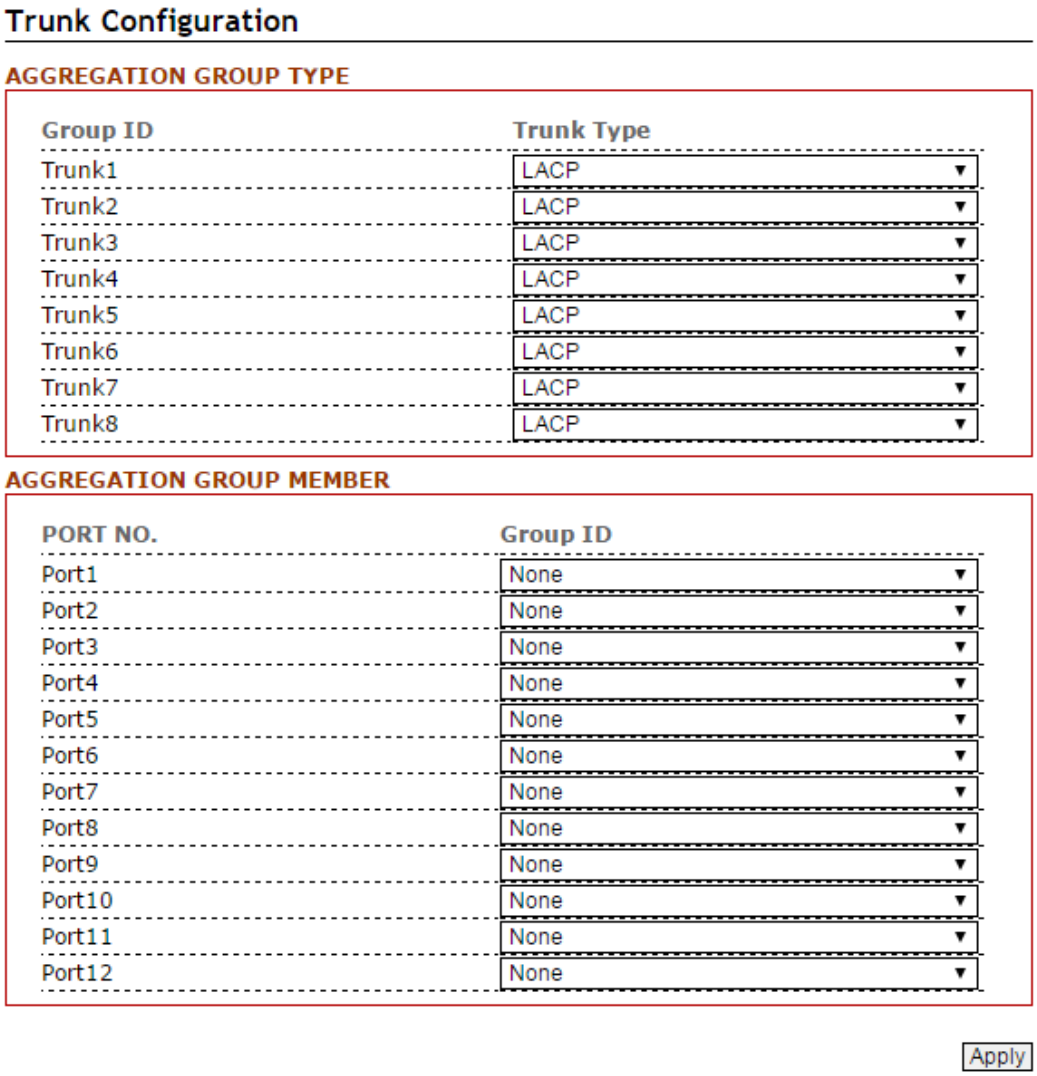


Figure 5.50 – Port Trunk Configuration Interface

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 5.51 – Port Trunk Terms and Value Description

5.10 Port Mirroring

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

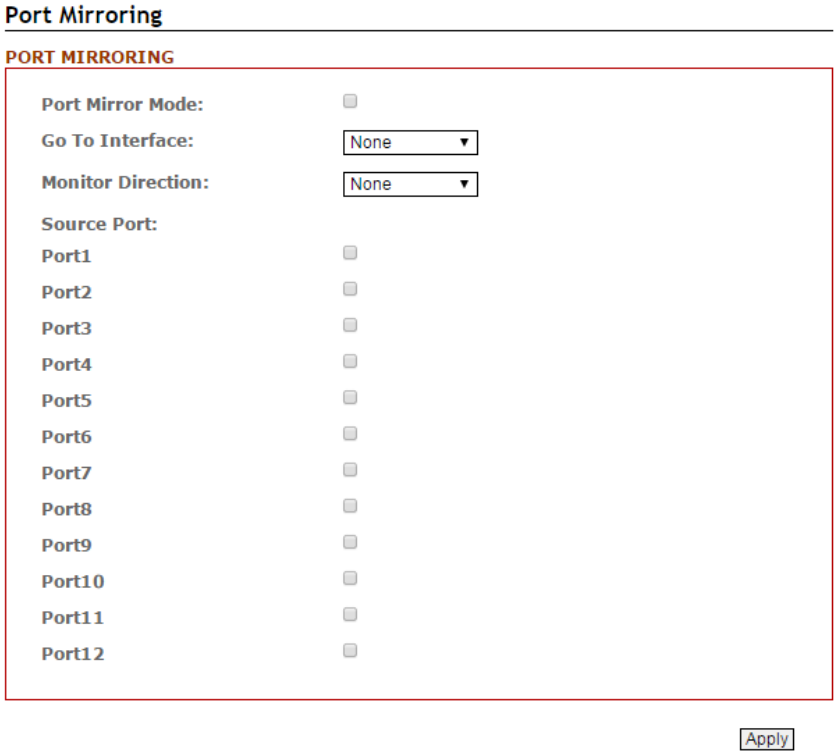


Figure 5.52 – Port Mirroring Configuration Interface

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

Figure 5.53 – Port Mirroring Terms & Value Description

5.11 SNMP

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

5.11.1 SNMP Agent

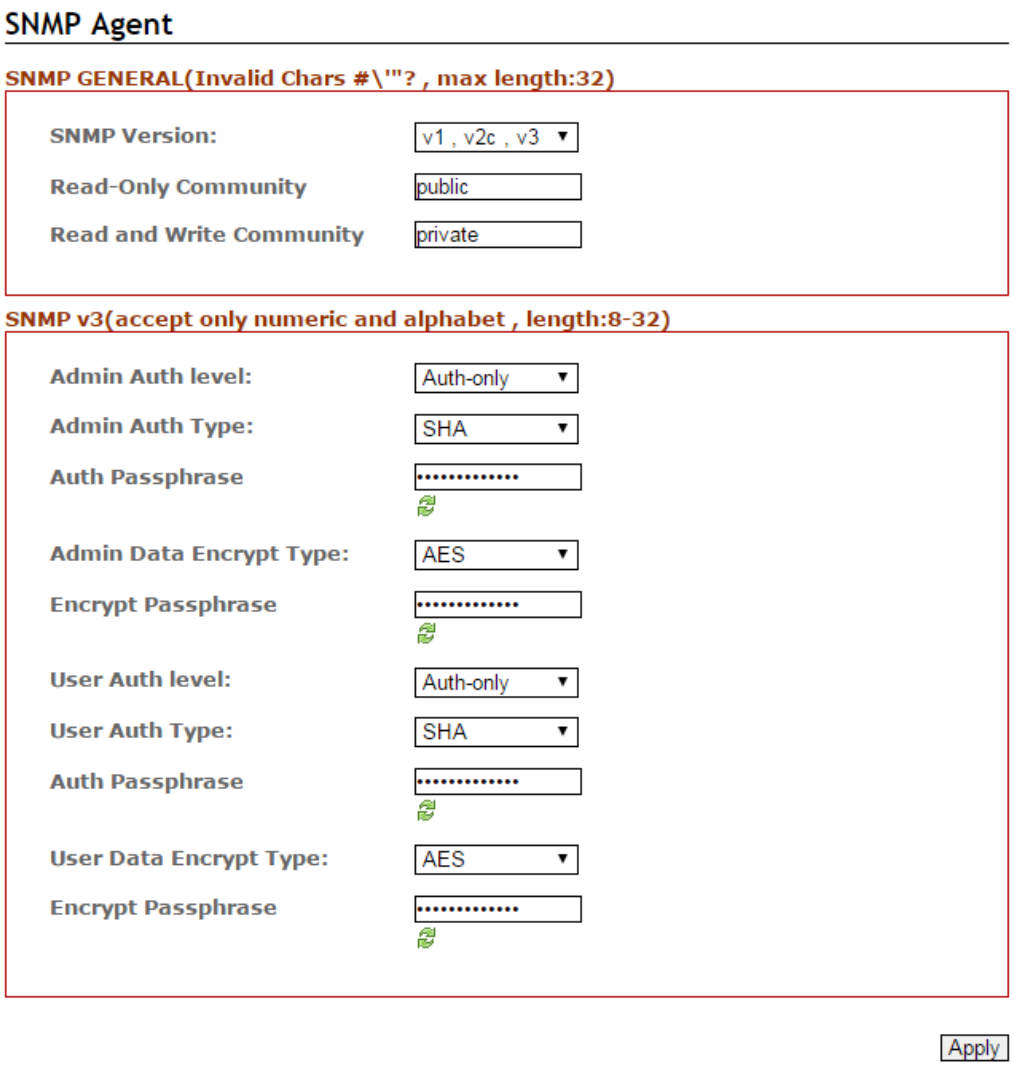


Figure 5.54 – SNMP Agent Setup Interface

SNMP General -

Terms	Value Description
SNMP Version	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.
Read-Only Community	Using “Read-Only Community” on the SNMP MIB walk utility can only read information. The maximum length of Read-Only Community is 32 characters and #, \, ‘, “, ? are invalid characters.
Read and Write Community	Using “Read and write Community” on the SNMP MIB walk utility not only can read information, but can write/edit part of information. The maximum length of Read-Only Community is 32 characters and #, \, ‘, “, ? are invalid characters.
Apply	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
Admin Auth Level	“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.
Admin Auth Type	The method used to encrypt the passphrase
Auth Passphrase	“Auth Passphrase” is a string used to authenticate (Admin). The range of length is from 8 to 32 characters with only numeric and alphabet characters accepted.
Admin Data Encrypt Type	The method used to encrypt the data.
Encrypt Passphrase	“Encrypt Passphrase” is a string used to encrypt data (Admin). The range of length is from 8 to 32 characters with only numeric and alphabet characters accepted.
User Auth Level	“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.

User Auth Type	The method used to encrypt the passphrase
Auth Passphrase	"Auth Passphrase" is a string used to authenticate (User). The range of length is from 8 to 32 characters with only numeric and alphabet characters accepted.
User Data Encrypt Type	The method used to encrypt the data.
Encrypt Passphrase	"Encrypt Passphrase" is a string used to encrypt data (User). The range of length is from 8 to 32 characters with only numeric and alphabet characters accepted.
Apply	Click the "Apply" button to save changes.

Figure 5.55 – SNMP Agent Interface Terms & Value Descriptions

5.11.2 SNMP Trap Setting

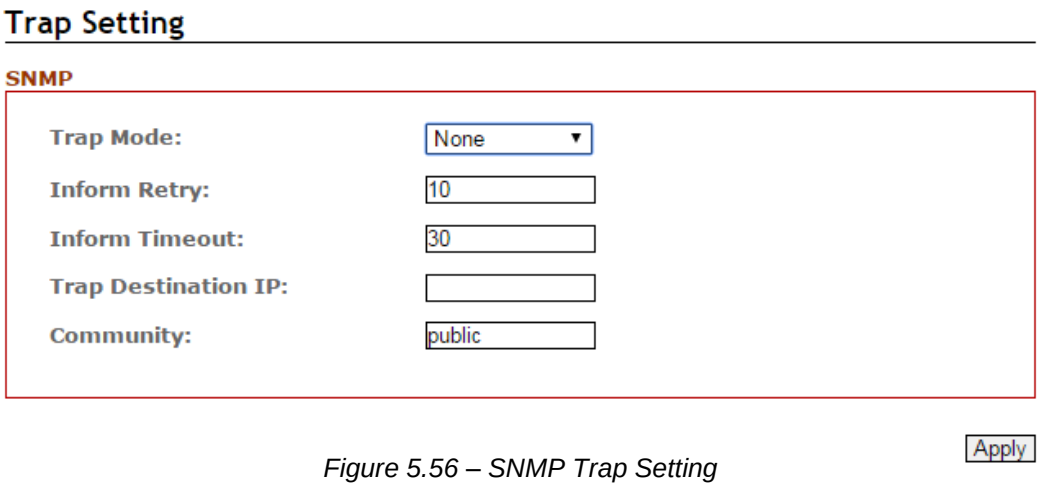


Figure 5.56 – SNMP Trap Setting

Terms	Value Description
Trap Mode	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.
Inform Retry	The trap message will be sent "Inform Retry" times. This field works only when "Trap Mode" is set to "Inform".

Inform Timeout	The trap message will be sent after “Inform Timeout” expired. This field works only when “Trap Mode” is set to “Inform”.
Trap Destination IP	The Destination IP that trap message will be sent to.
Apply	Click the “Apply” button to save changes.

Figure 5.57 – SNMP Trap Settings Terms & Value Description

5.12 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 Rely 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 as below Figure 5.58 and Figure 5.60; and the detail of packet fields are in Figure 5.59 and Figure 5.61. The IP addresses will get more controllable with DCHP Relay Option 82 function.

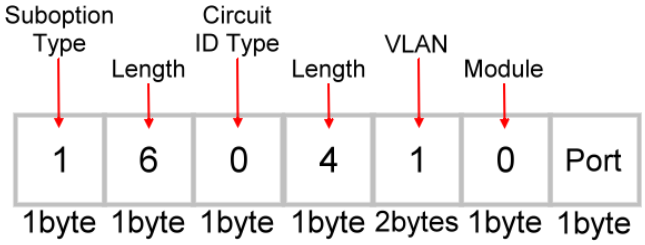


Figure 5.58 – DHCP Relay Option 82 Circuit ID

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 5.59 – DHCP Relay Option 82 Circuit ID Details

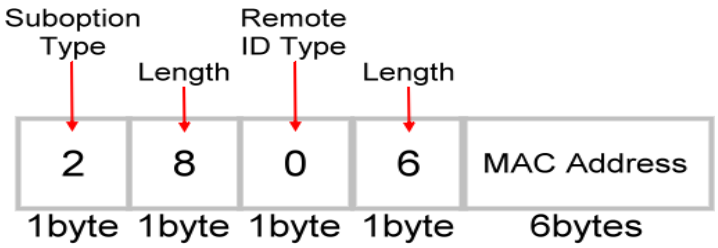


Figure 5.60 – DHCP Relay Option 82 remote ID

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 5.61 – DHCP Relay Option 82 Remote ID Details

5.12.1 DHCP Client

The below figure is the IP Setting of DHCP Client.

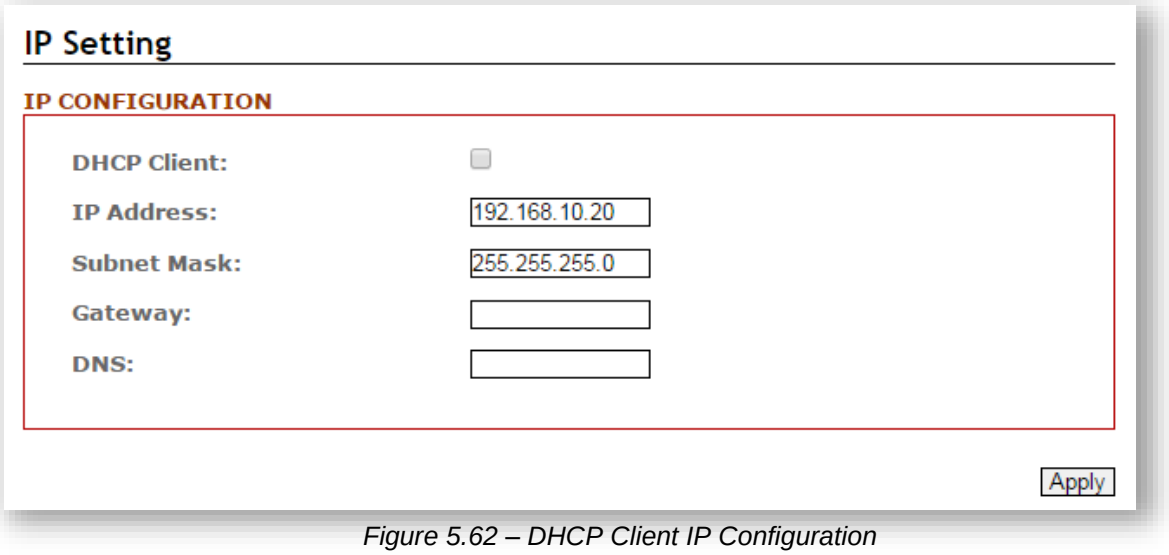


Figure 5.62 – DHCP Client IP Configuration

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 5.63 – DHCP Client Terms and Value Description

5.12.2 DHCP Server

The below figure is the DCHP Server web interface.



Figure 5.64 – 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 Address	The start address of the pool that DHCP Server managed.
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 5.65 – DHCP Server Terms and Value Description

5.12.3 DHCP Server Binding

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

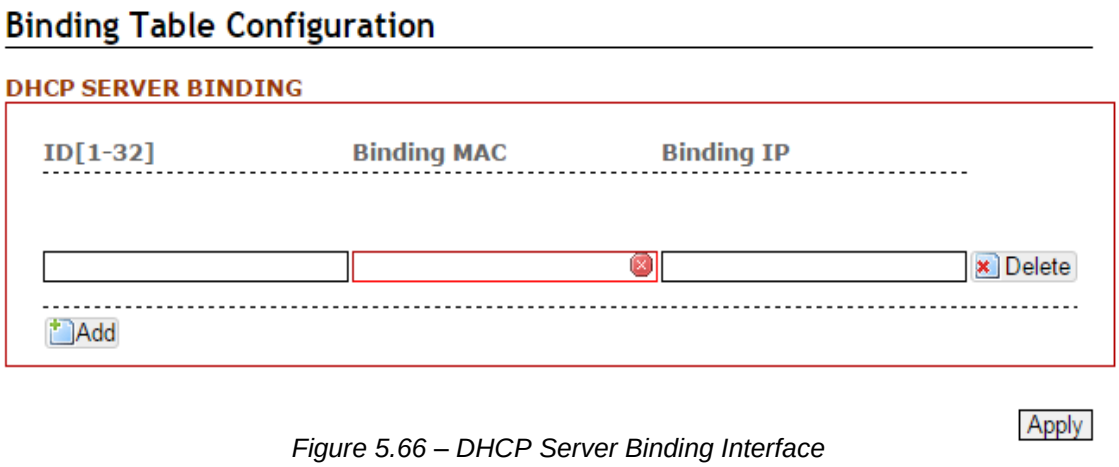


Figure 5.66 – DHCP Server Binding Interface

Terms	Value Description
ID	“Enable” or “Disable” DHCP Client. Users can enter ID’s 1 to 32 binding a MAC and binding IP address
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 5.67 – DHCP Server Binding Terms and Value Description

5.12.4 DHCP Relay

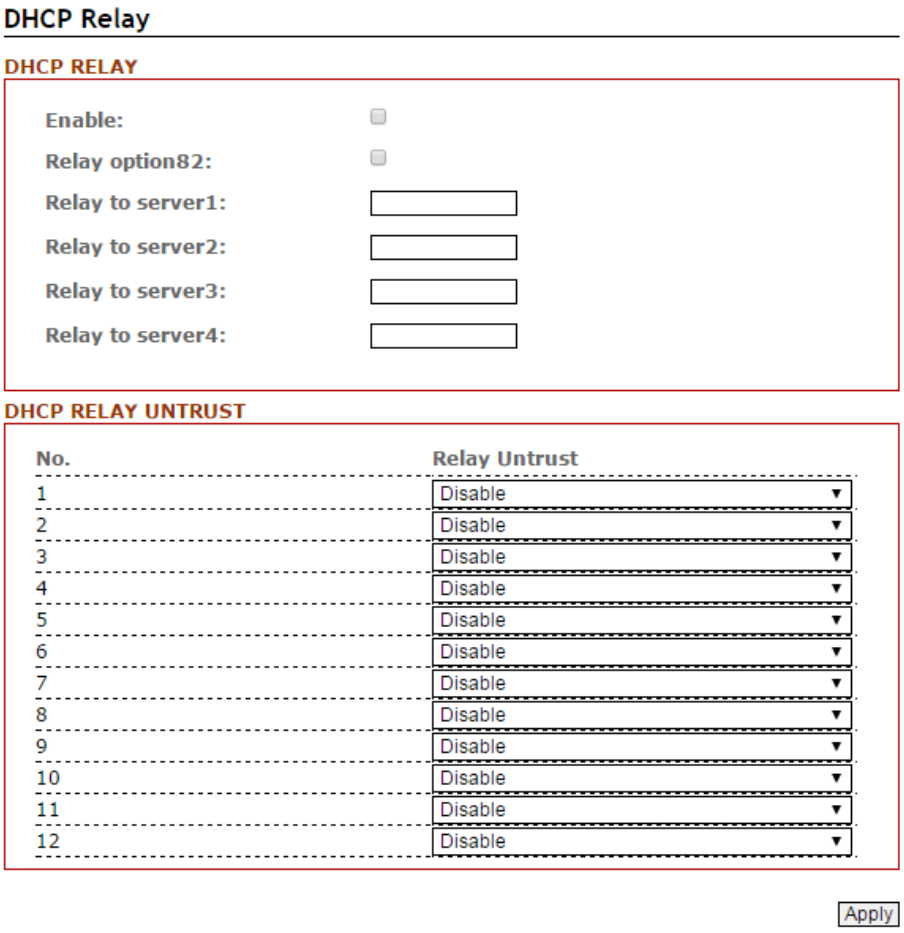


Figure 5.68 – DHCP RELAY Interface

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 5.69 – DHCP RELAY – Terms & 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 5.70 – DHCP RELAY – Terms & Value Description

5.13 802.1X

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.

5.13.1 802.1X Settings

The below figure is the 802.1X configuration interface.

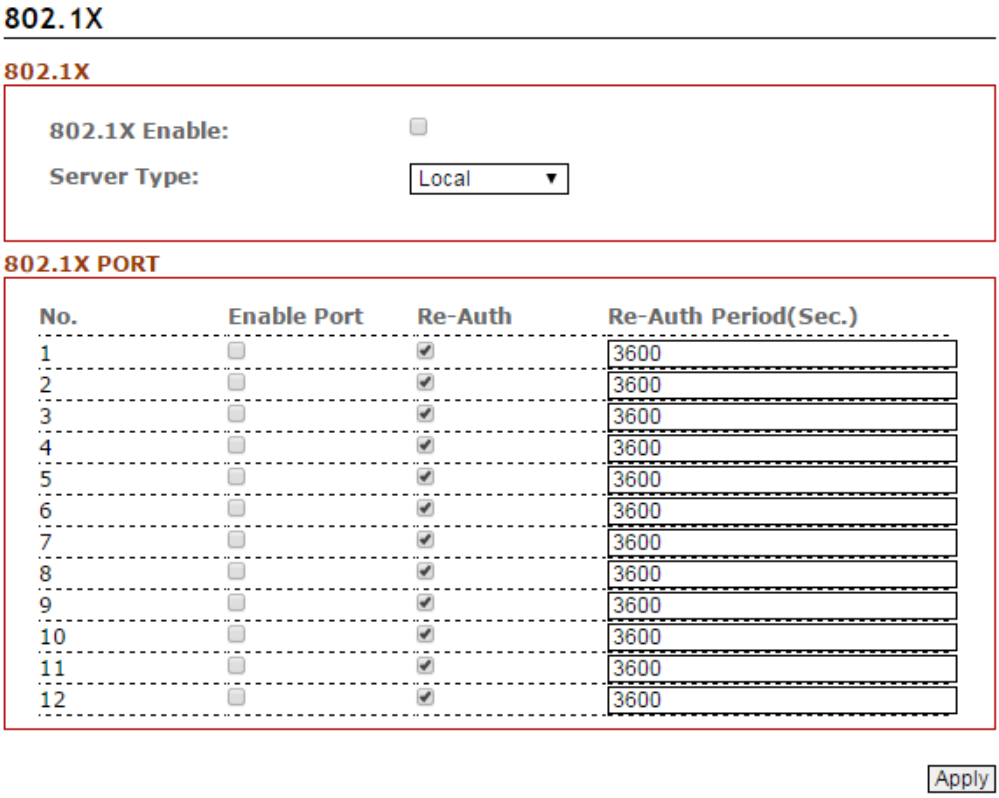


Figure 5.71 – 802.1X Configuration Interface

The below tables 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 5.72 – 802.1X – Terms & Value Description

5.13.2 Local Database

The below figure is the Local Database web interface.

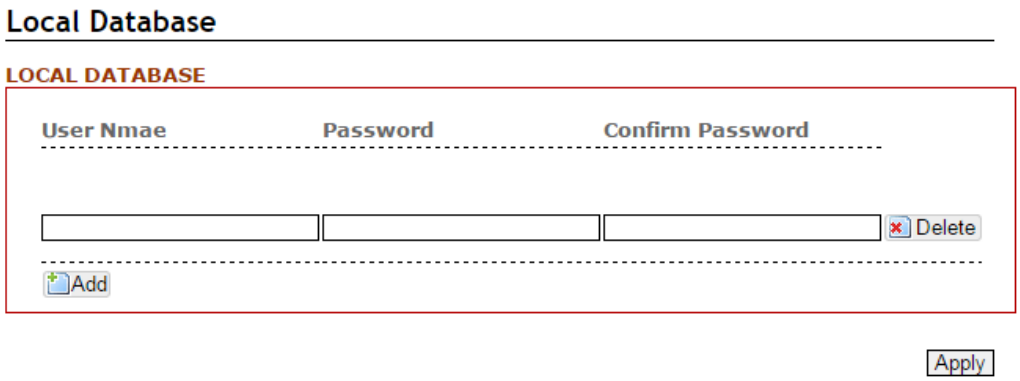


Figure 5.73 – Local Database Web Interface

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 5.74 – Local Database – Terms & Value Description

5.13.3 RADIUS Server

The below figure is the RADIUS Server setting interface.

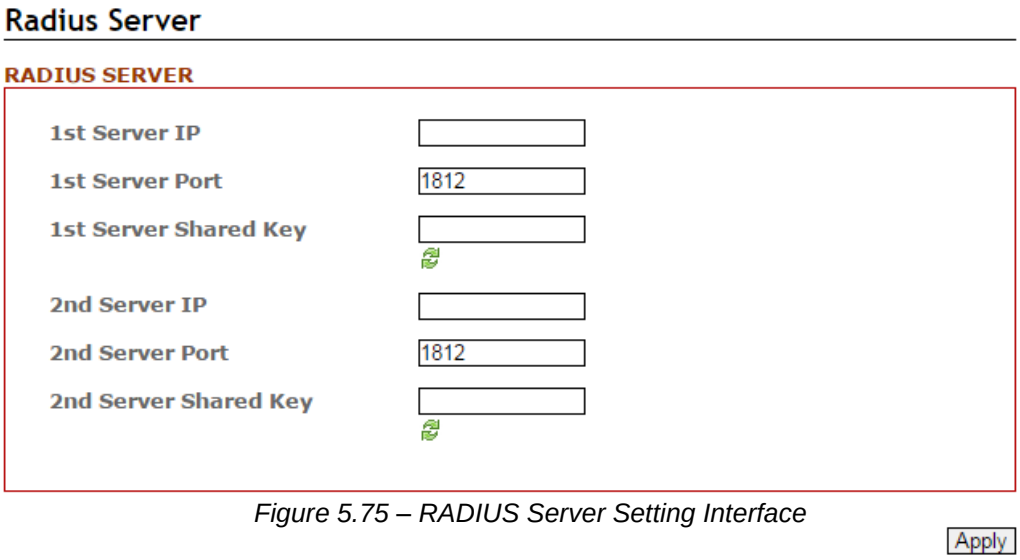


Figure 5.75 – RADIUS Server Setting Interface

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 5.76 – RADIUS Server – Terms & Value Description

5.14 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.

5.14.1 UPnP

Below, *Figure 5.77,* is the UPnP web interface.

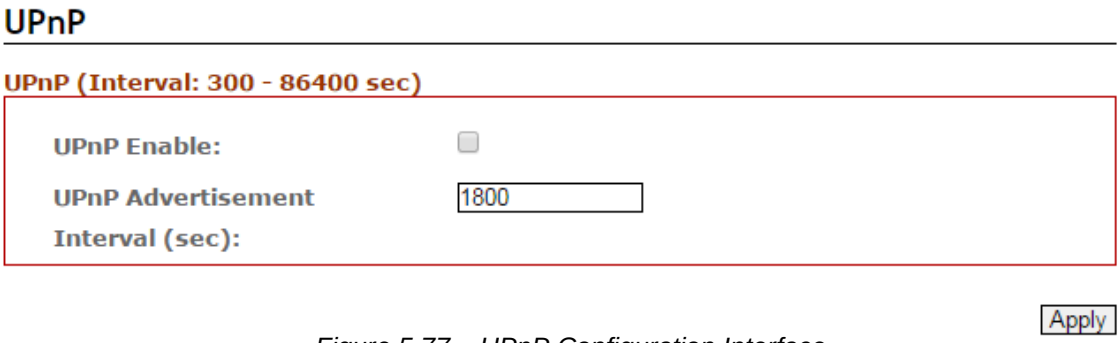


Figure 5.77 – UPnP Configuration Interface

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. The advertisement interval is from 300 to 86400 seconds.

Figure 5.78 – UPnP Terms and Value Description

5.15 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.

5.15.1 Enable Modbus TCP

Below, *Figure 5.79*, is the ModbusTCP web interface.

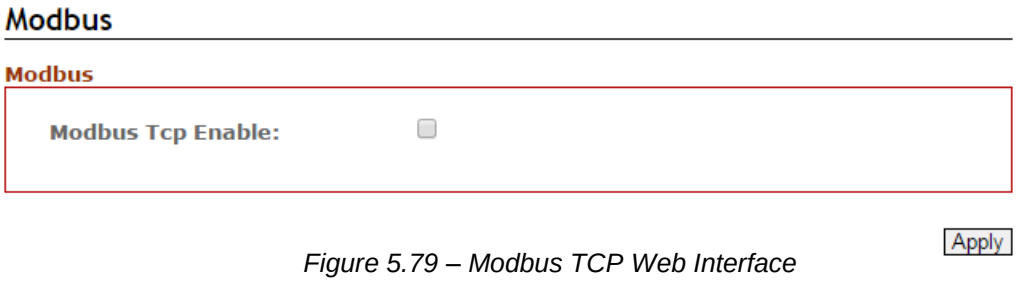


Figure 5.79 – Modbus TCP Web Interface

The below table describes Modbus Terms and Value Description.

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

Figure 5.80 – Modbus TCP – Terms & Value Description

5.15.2 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
System Information			
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
System Information			
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 = "LMX-1204G-SFP" 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
Port Information			
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 = ‘.’
Packets Information			
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 0x210B	2 words	HEX	Port 1 to 6 Rx Packets 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
Redundancy Information			
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 5.81 – Antaira Switches – Modbus Data Map & Information

5.16 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.

5.16.1 Syslog Setting

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

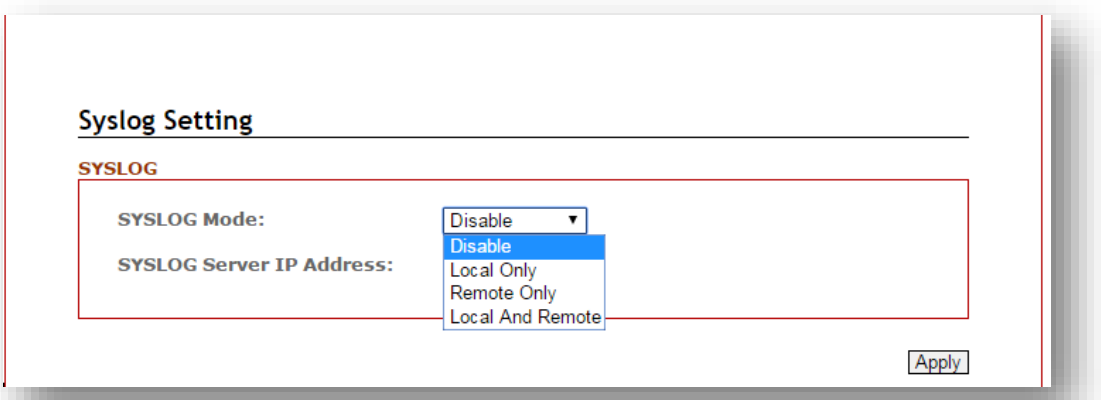


Figure 5.82 – Syslog Setting

Terms	Value Description
SYSLOG Mode	**Disable:** disable SYSLOG. **Local Only:** log to local system. **Remote Only:** log to a remote SYSLOG server.

	Local And Remote: log to local server and remote SYSLOG server at the same time.
SYSLOG Server IP Address	Insert remote SYSLOG server IP address
Apply	Click the “Apply” button to save changes.

Figure 5.83 – SYSLOG Setting Terms & Value Description

5.16.2 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.

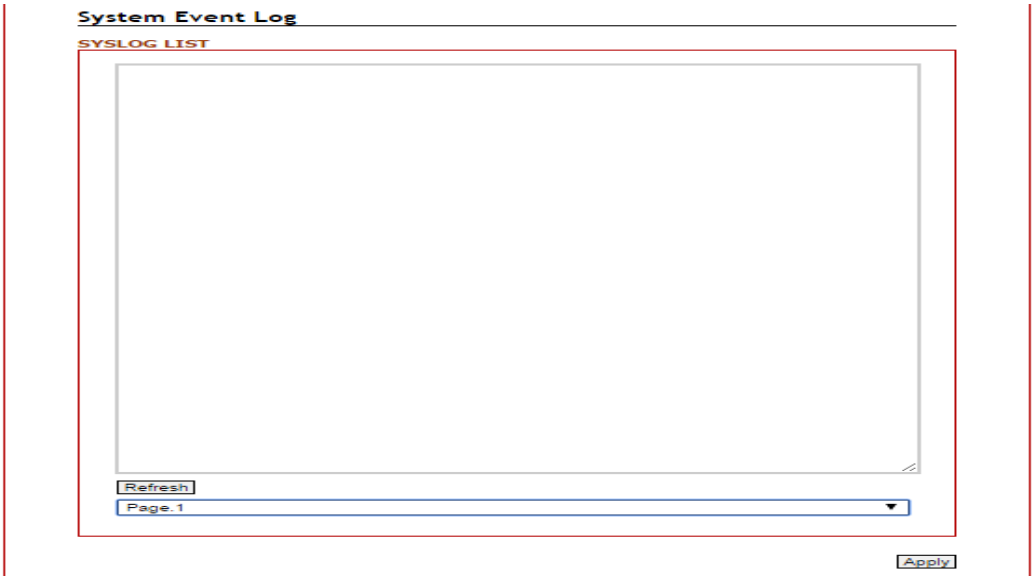


Figure 5.84 – System Event Logs Interface

5.16.3 SMTP Setting

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

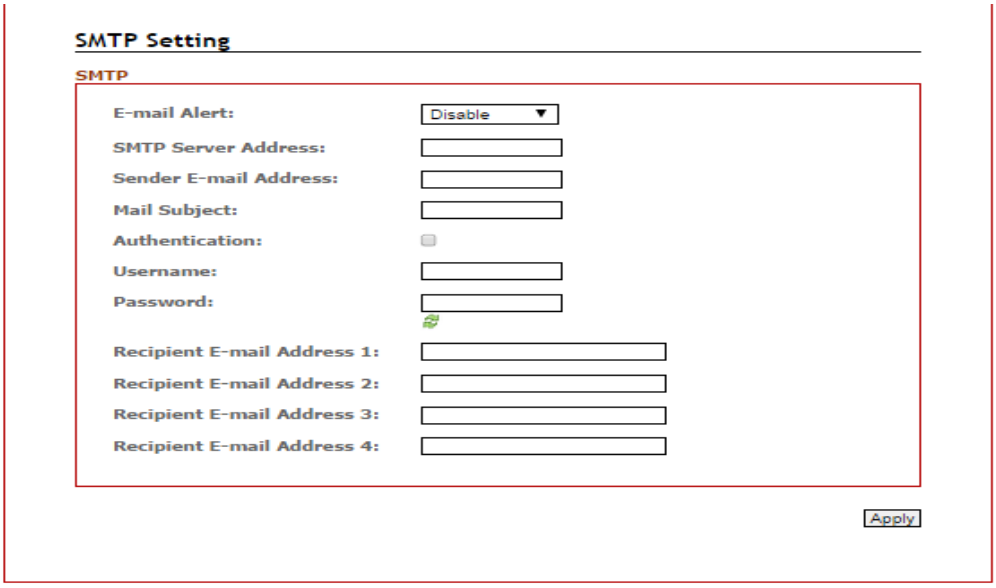


Figure 5.85 – SMTP Setting Interface

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

Figure 5.86 – SMTP Setting Terms & Value Description

5.16.4 Event Selection

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

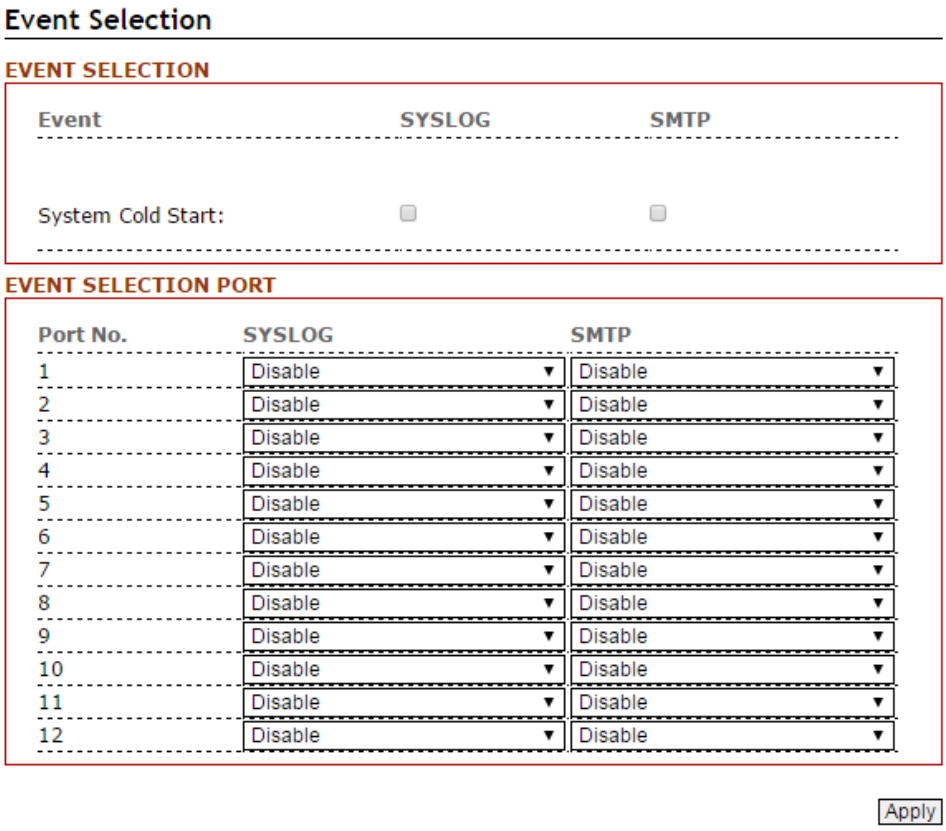


Figure 5.87 – Event Selection Setting Interface

5.16.5 Fault Alarm

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

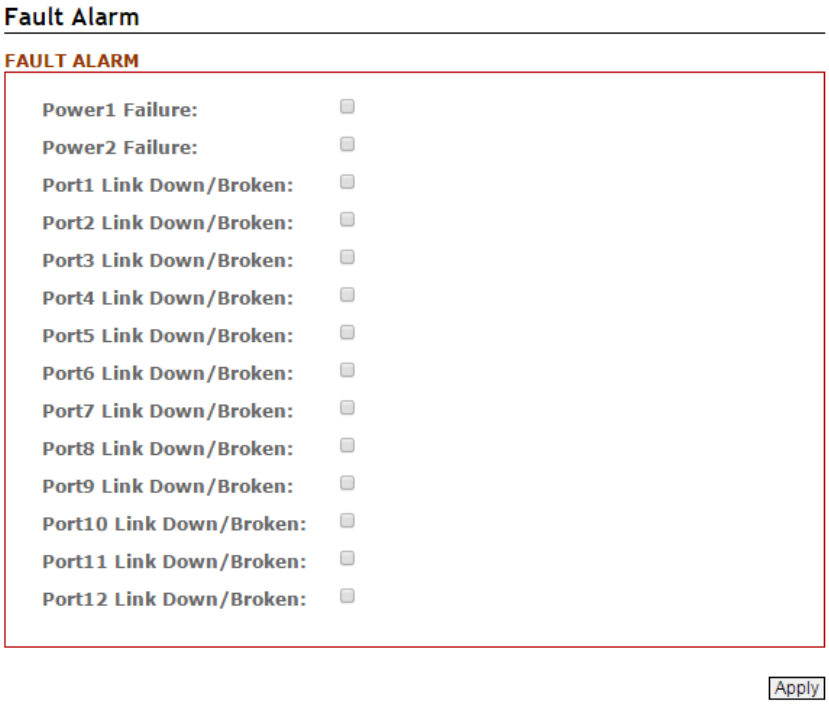


Figure 5.88 – Event Selection Setting Interface

5.17 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.

5.17.1 MAC Address Table

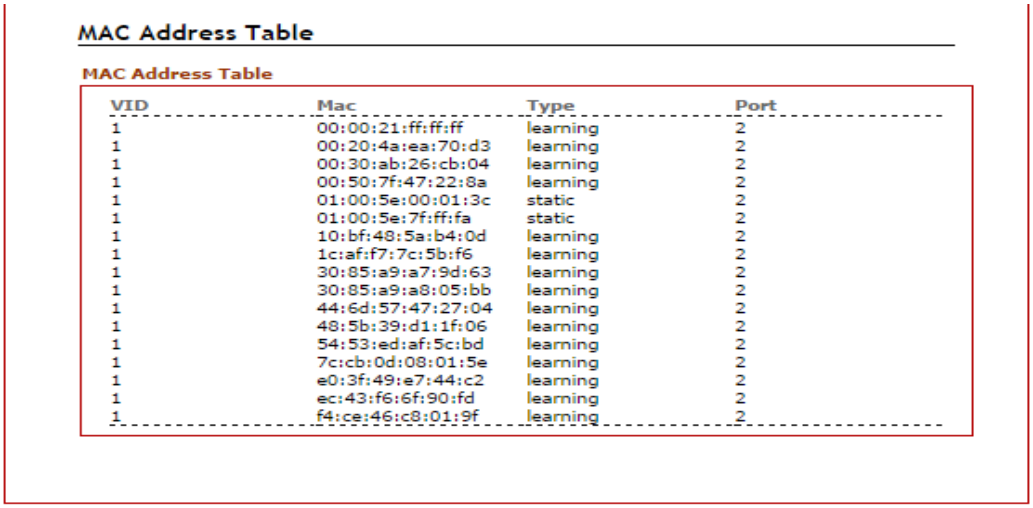


Figure 5.89 – MAC Address Table Interface

5.17.2 MAC Table Configuration

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

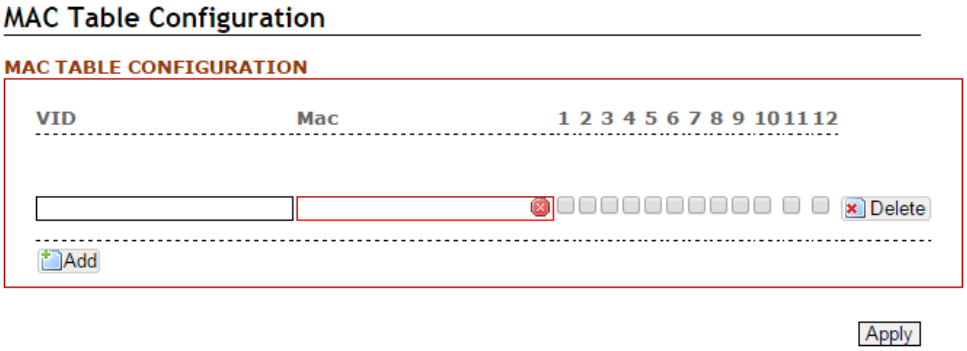


Figure 5.90 – MAC Table Setting Interface

5.18 Maintenance

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

5.18.1 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.

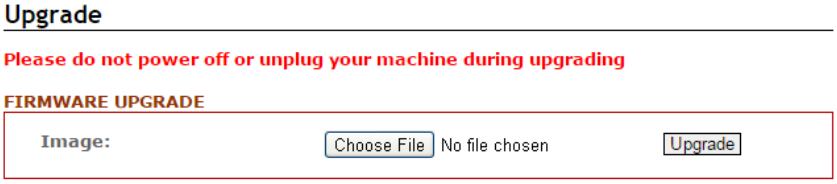


Figure 5.91 – Firmware Upgrade Interface

Terms	Value Description
FIRMWARE UPGRADE	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.

Figure 5.92 – Firmware Upgrade Setting Terms & Value Description

5.18.2 Reboot

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

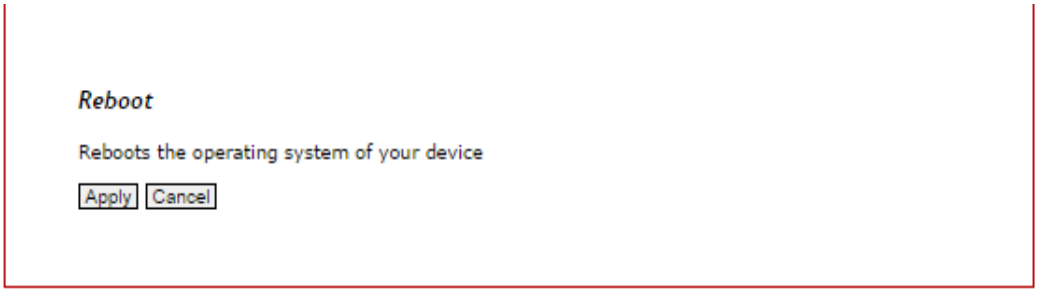


Figure 5.93 – Switch Reboot Interface

5.18.3 Default

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

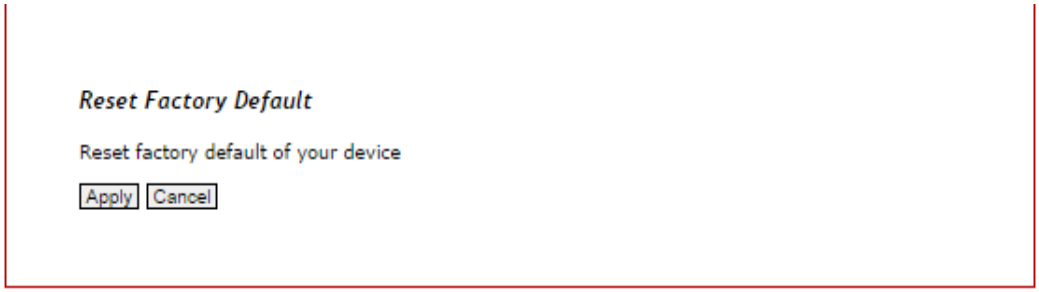


Figure 5.94 – Reset Factory Default Interface

5.19 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.

5.19.1 Save

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

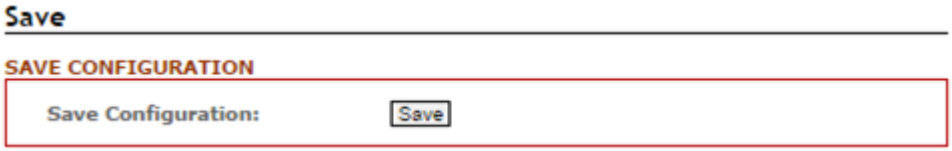


Figure 5.95 – Save Setting Interface

5.19.2 Backup & Restore

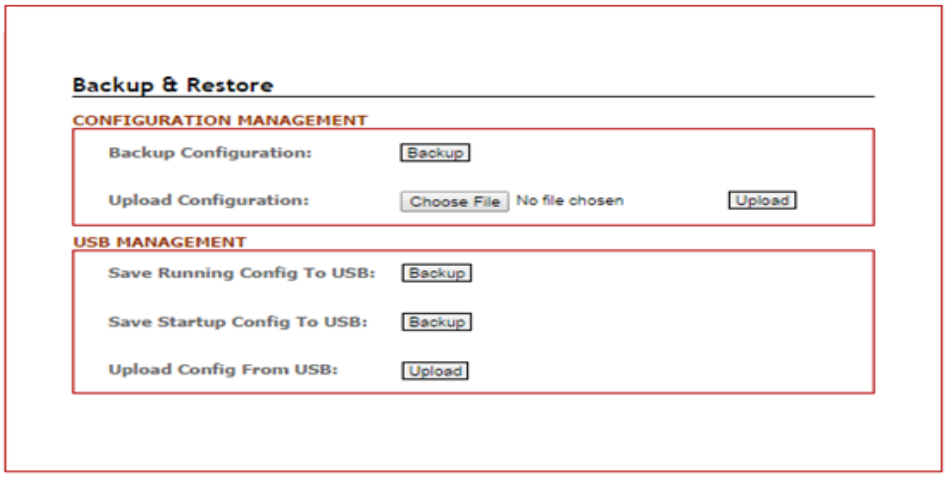


Figure 5.96 – Backup & Restore Setting Interface

Terms	Value Description
CONFIGURATION MANAGEMNET	
Backup Configuration	By clicking the “Backup” button, it allows users to back up the switch configuration setting to their local PC, or server.
Upload Configuration	Users can click the “Choose File” button to select the saved configuration file from local PC, or server, then click the “Upload” the settings to the switch.
USB Management	
Save Running Config to USB	Click the button of Backup to save running-config file to USB.
Save Startup Config to USB	Click the button of Backup to save startup-config file to USB.
Upload Config from USB	Click the button of Upload to load startup-config from USB.

Figure 5.97 – Backup & Restore Setting Terms & Value Description

5.19.3 Auto Load & Backup

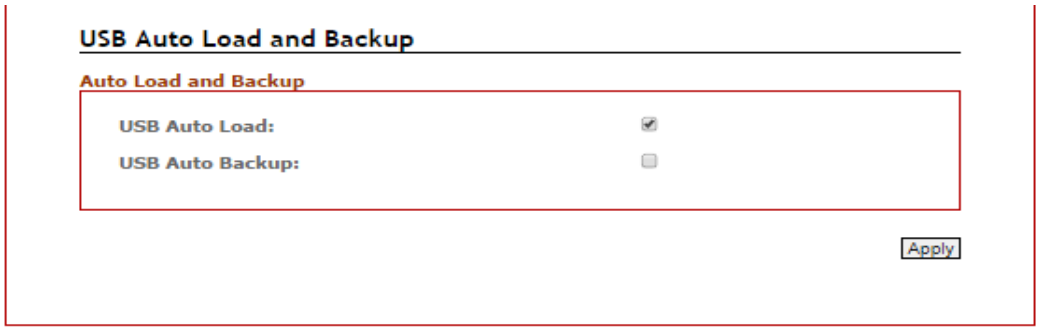


Figure 5.98 – USB Auto Load and Backup Setting Interface

Terms	Value Description
USB Auto Load	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.
USB Auto Backup	Select USB Auto Backup, it can auto Backup running-config file from Switch to USB. And the file name is “startup-config”.

Figure 5.99 – USB Auto Load and Backup Setting Terms & Value Description

5.20 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, LMX-1204G-SFP series also supports CLI management. Users can use console or telnet to management switch by CLI.

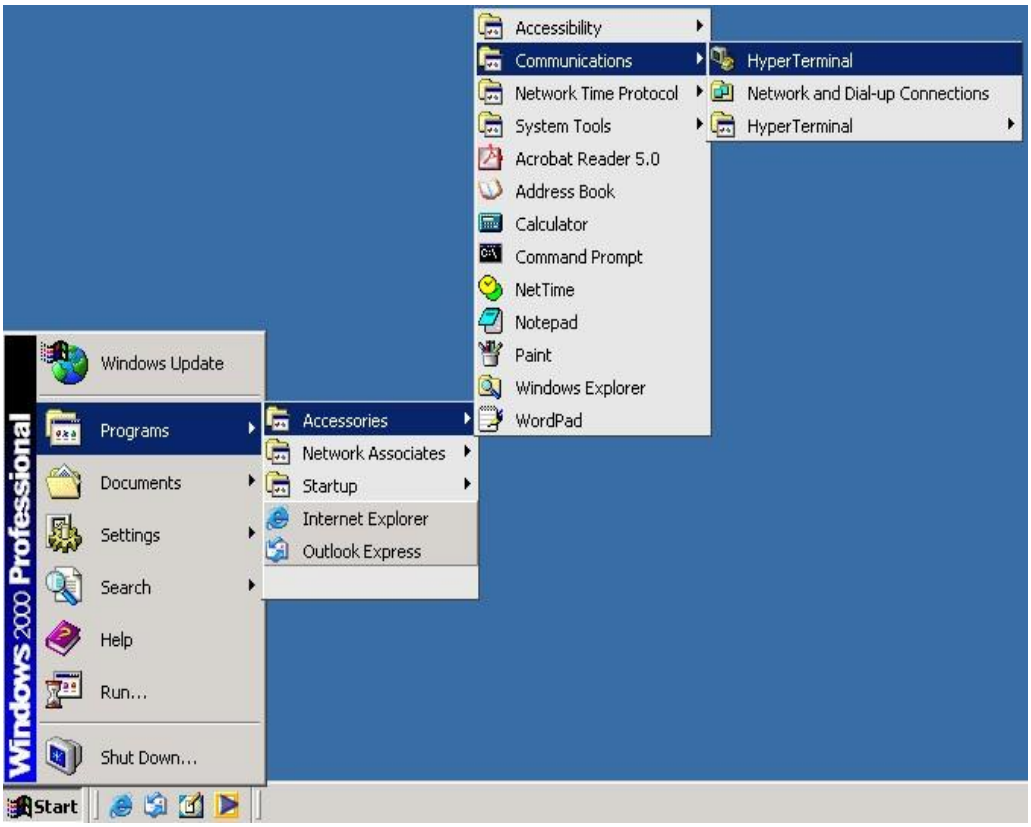
CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

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

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

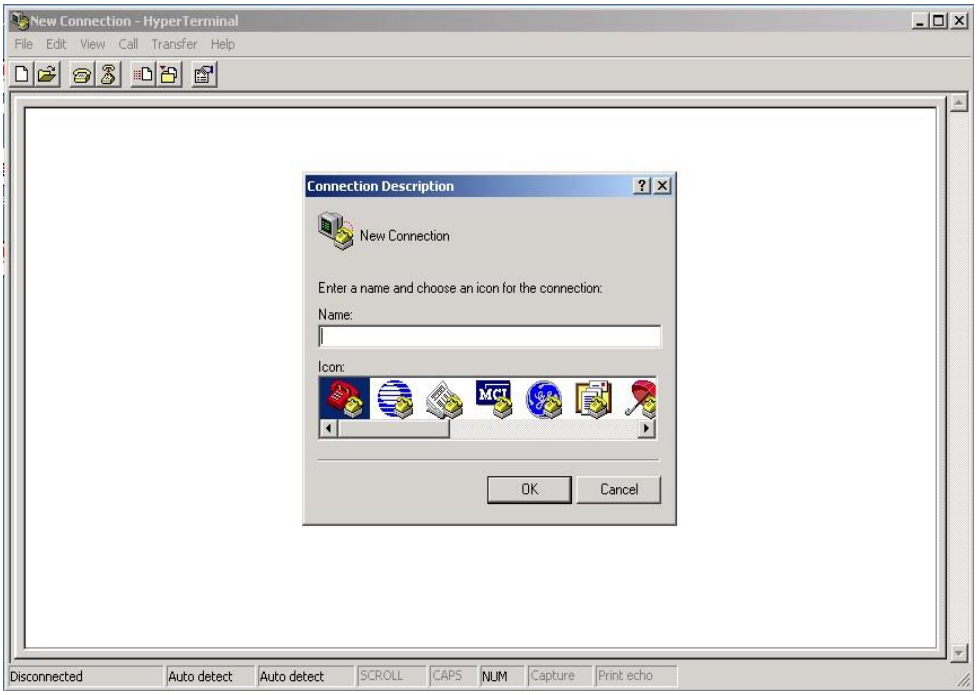
Step 1:

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



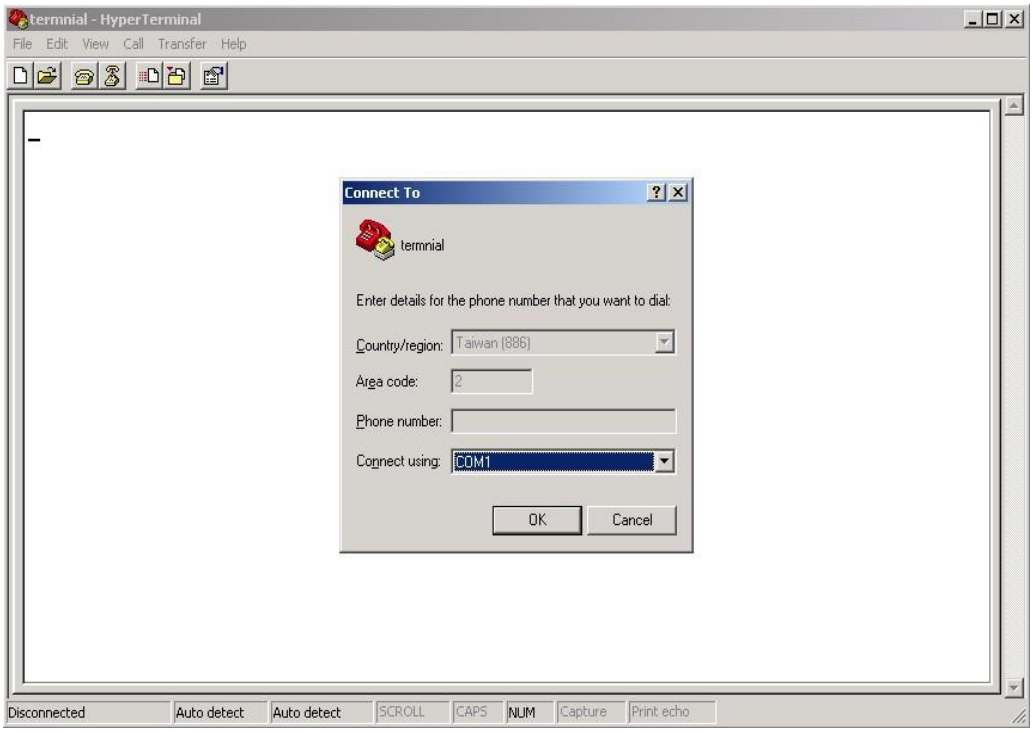
Step 2:

Input a name for the new connection.



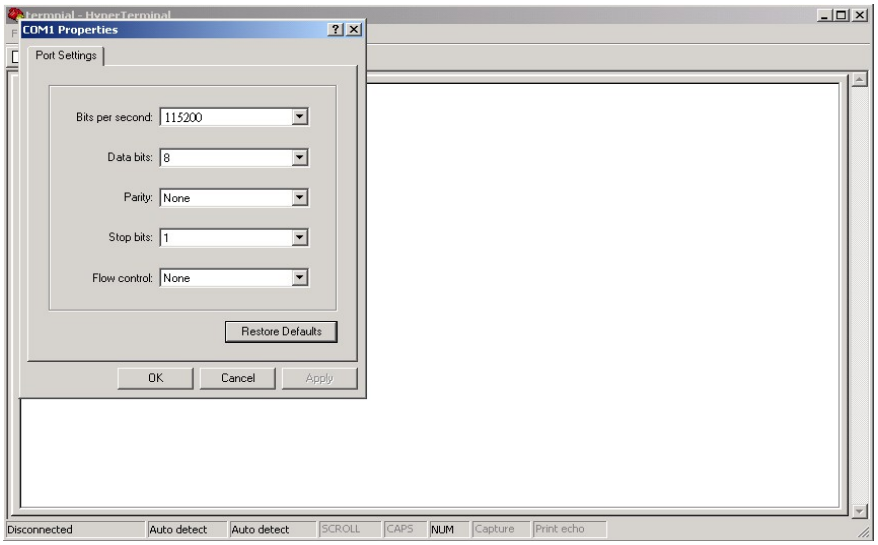
Step 3:

Select to use a specific COM port number.



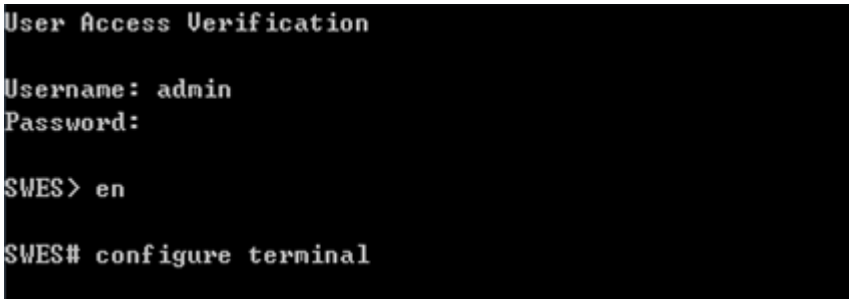
Step 4:

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



Step 5:

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



CLI Management by Telnet

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

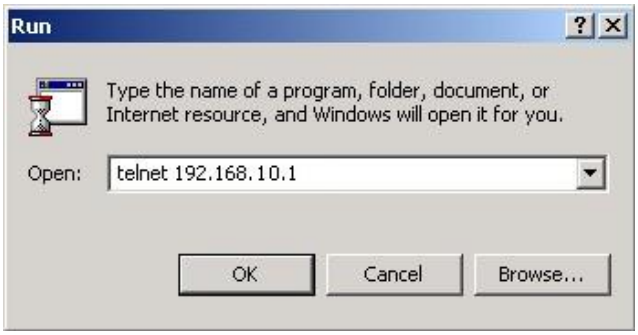
The default value is as below:

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

Follow the steps below to access the console via Telnet.

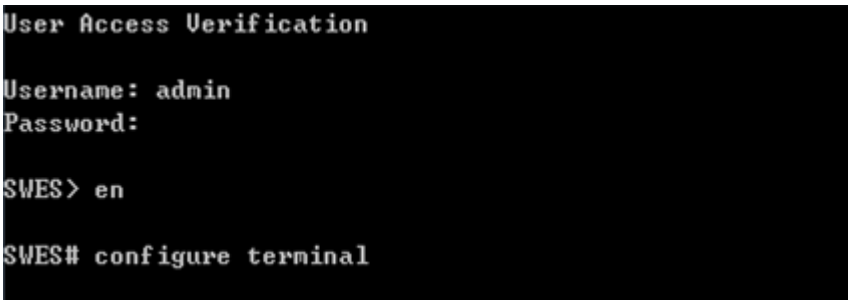
Step 1:

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



Step 2:

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



Commander Groups

Group	Command	Mode
System	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
	admin username admin	configure
	admin password admin	configure
IP	boot host dhcp	configure
	ip address [ip_addr] [ip_mask]	configure
	ip default-gateway [ip_router]	configure
	ip name-server [ip_addr_string]	configure
	no boot host dhcp	configure
	no ip default-gateway	configure
	no ip name-server	configure
	show boot host dhcp	configure
	show ip address	configure
	show ip default-gateway	configure
	show ip name-server	configure
	show ip mode	configure
Time	ntp time update	configure
	ntp client timeserver [ip_addr_string]	configure
	clock set [hh:mm:ss] [day] [month] [year]	configure
	clock timezone [area] [city]	configure
	ntp client sync [minute|hour|day|month|year] [NUMBER]	configure
	no ntp client timeserver	configure
	no clock timezone	configure
Time	no ntp client sync [minute|hour|day|month|year] [NUMBER]	configure
	show ntp client timeserver	configure

	show clock timezone	configure
	show ntp client sync [minute|hour|day|month|year] [NUMBER]	configure
Port	speed [auto | 10 | 100 | 1000] [full | half]	interface
	Duplex [auto | full | half]	interface
	flowcontrol <receive> [on | off | desired]	interface
	name [string]	interface
	shutdown	interface
	no speed	interface
	no duplex	interface
	no flowcontrol	interface
	no name	interface
	no shutdown	interface
	show speed	interface
	show duplex	interface
	show flowcontrol	interface
	show name	interface
	show link rx	interface
	show link tx	interface
	show link summary	interface
VLAN	management vlan [vlan_id]	configure
	name [vlan_name]	vlan
	member [member_portlist] [<untag_portlist>]	vlan
	switchport pvid [vlan_id]	interface
	switchport filter [tagged | untagged]	interface
	no name	vlan
	no member	vlan
	no switchport pvid	interface
	no switchport filter	interface
	show name	vlan
	show member	vlan
	show switchport pvid	interface
	show switchport filter	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 ethernet ring g8032 configuration	erps
STP	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 stp	interface
STP	show spanning-tree mode	configure
	show spanning-tree priority	configure
	show spanning-tree forward-time	configure
	show spanning-tree hello-time	configure
	show spanning-tree max-age	configure
	show spanning-tree cost	interface
	show spanning-tree port-priority	interface
	show spanning-tree link-type	interface
	show spanning-tree auto-edge	interface
	show spanning-tree admin-edge	interface
	show spanning-tree stp	interface
	spanning-tree mst [instance_ID] priority [priority]	configure
	spanning-tree mst name [NAME]	configure
	spanning-tree mst revision [REVISION]	configure
	spanning-tree mst instance [instance_ID] vlan [vlan_grp]	configure
	spanning-tree mst [instance_ID] cost [cost_value]	interface
	spanning-tree mst [instance_ID] port-priority [priority]	interface
	no spanning-tree mst name	configure
	no spanning-tree mst revision	configure
	no spanning-tree mst instance [instance_ID] vlan	configure
	no spanning-tree mst [instance_ID] cost	interface
	no spanning-tree mst [instance_ID] port-priority	interface

	show spanning-tree mst name	configure
	show spanning-tree mst revision	configure
	show spanning-tree mst instance [instance_ID] vlan	configure
	show spanning-tree mst [instance_ID] priority	configure
	show spanning-tree mst [instance_ID] cost	interface
	show spanning-tree mst [instance_ID] port-priority	interface
Event	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	configure
	event smtp interface [INTERFACE_NAME] 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	configure
	no event smtp interface [INTERFACE_NAME] 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	configure
	show event smtp interface [INTERFACE_NAME] 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	configure
	event syslog interface [INTERFACE_NAME] 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	configure
	no event syslog interface [INTERFACE_NAME] 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
	show event syslog interface [INTERFACE_NAME] up	configure
	show event syslog interface [INTERFACE_NAME] 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
SYSLOG	syslog server [IP_address]	configure
	syslog mode [all | remote | local | usb]	configure
	no syslog server	configure
	no syslog mode	configure
	show syslog server	configure
	show syslog mode	configure

	show syslog log	configure
SMTP	smtp enable	configure
	smtp sender [E-MAIL_ADDR]	configure
	smtp subject [subject_text]	configure
	smtp server address [GMAIL_SMPT_SERVER]	configure
	smtp server port [GMAIL_SMPT_SERVER]	configure
	smtp authentication enable	configure
	smtp authentication username [GMAIL_ACCOUNT]	configure
	smtp authentication password [GMAIL_PASS]	configure
	smtp receive [1 | 2 | 3 | 4] [e-mail_address]	configure
	no smtp enable	configure
	no smtp sender	configure
	no smtp subject	configure
	no smtp server address	configure
	no smtp server port	configure
	no smtp authentication enable	configure
	no smtp authentication username	configure
	no smtp authentication password	configure
	no smtp receive [1 | 2 | 3 | 4]	configure
	show smtp state	configure
	show smtp sender	configure
	show smtp subject	configure
	show smtp server address	configure
	show smtp server port	configure
	show smtp authentication enable	configure
	show smtp authentication username	configure
	show smtp receive [1 | 2 | 3 | 4]	configure
SNMP	snmp server enable [<v1-v2c-only | v3-only>]	configure
	snmp server community [ro | rw] [community_name]	configure
	snmp server v3 level [admin| user] [auth | noauth | priv]	configure
	snmp server v3 auth [admin | user] [md5 | sha] [PWD]	configure
	snmp server v3 encryption [admin | user] [des | aes] [PWD]	configure
	no snmp server enable	configure
	no snmp server community [ro | rw]	configure
	no snmp server v3 level [admin| user]	configure

	no snmp server v3 auth [admin | user]	configure
	no snmp server v3 encryption [admin | user]	configure
	show snmp server enable	configure
	show snmp server community [ro | rw]	configure
	show snmp server v3 level [admin| user]	configure
	show snmp server v3 auth [admin | user]	configure
	show snmp server v3 encryption [admin | user]	configure
	snmp trap enable	configure
	snmp trap host [DESTINATION_IP]	configure
	snmp trap version [1 | 2c | 3] [traps | inform]	configure
	snmp trap community [trap_community_name]	configure
	snmp trap inform retry [retry_time]	configure
	snmp trap inform timeout [retry_interval]	configure
	snmp trap v3 user [user_ID]	configure
	snmp trap v3 level [auth | noauth | priv]	configure
	snmp trap v3 engine-ID [engineID]	configure
	snmp trap v3 auth [md5 | sha] [PASSWORD]	configure
	snmp trap v3 encryption [des | aes] [PASSWORD]	configure
SNMP	no snmp trap enable	configure
	no snmp trap host	configure
	no snmp trap version	configure
	no snmp trap community	configure
	no snmp trap inform retry	configure
	no snmp trap inform timeout	configure
	no snmp trap v3 user	configure
	no snmp trap v3 level	configure
	no snmp trap v3 engine-ID	configure
	no snmp trap v3 auth	configure
	no snmp trap v3 encryption	configure
	show snmp trap enable	configure
	show snmp trap host	configure
	show snmp trap version	configure
	show snmp trap community	configure
	show snmp trap inform retry	configure
	show snmp trap inform timeout	configure

	show snmp trap v3 user	configure
	show snmp trap v3 level	configure
	show snmp trap v3 engine-ID	configure
	show snmp trap v3 auth	configure
	show snmp trap v3 encryption	configure
FILE	copy running-config startup-config	configure
	copy startup-config running-config	configure
PORT MIRROR	monitor enable	configure
	monitor source [rx | tx | both] [port_list]	configure
	monitor destination [dest_port_number]	configure
	no monitor enable	configure
	no monitor source	configure
	no monitor destination	configure
	show monitor enable	configure
	show monitor source	configure
	show monitor destination	configure
QoS	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
IGMP	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
Trunk	trunk group [group] [static | lacp] [interface_list]	configure
DHCP Server/Relay	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

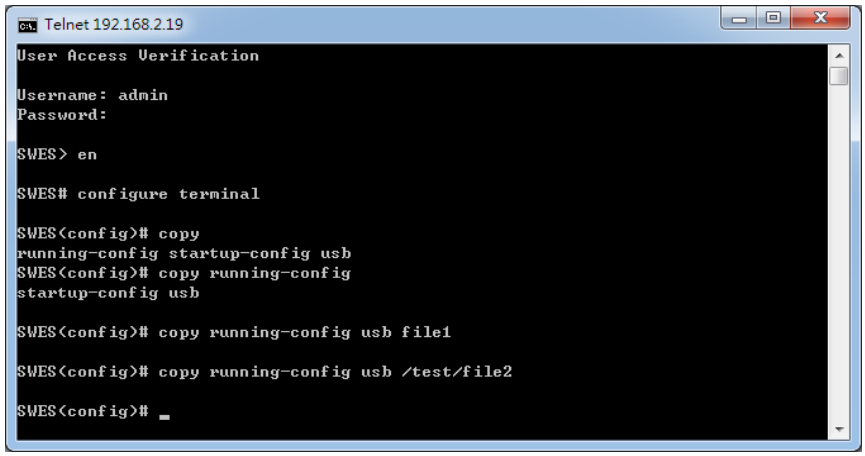
	no dhcp relay information policy [replace | keep | drop]	configure
	no dhcp relay untrust	configure
	show dhcp service	interface
	show dhcp server status	configure
	show dhcp server included-address	configure
	show dhcp server default-gateway	configure
	show dhcp server name-server	configure
	show dhcp 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
UPnP	**upnp enable**	configure
	upnp advertisement interval [SEC]	configure
	no upnp enable	configure
	no upnp advertisement interval	configure
	show upnp enable	configure
	show upnp advertisement interval	configure
Modbus	modbus tcp server	configure
	no modbus tcp server	configure
	show modbus tcp server	configure
802.1X	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_SIZ> | <repeat PKG_CNT>]	configure
	no ipv6 enable	configure
	no ipv6 address [IPV6_ADDR/PREFIX_LEN]	configure
	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

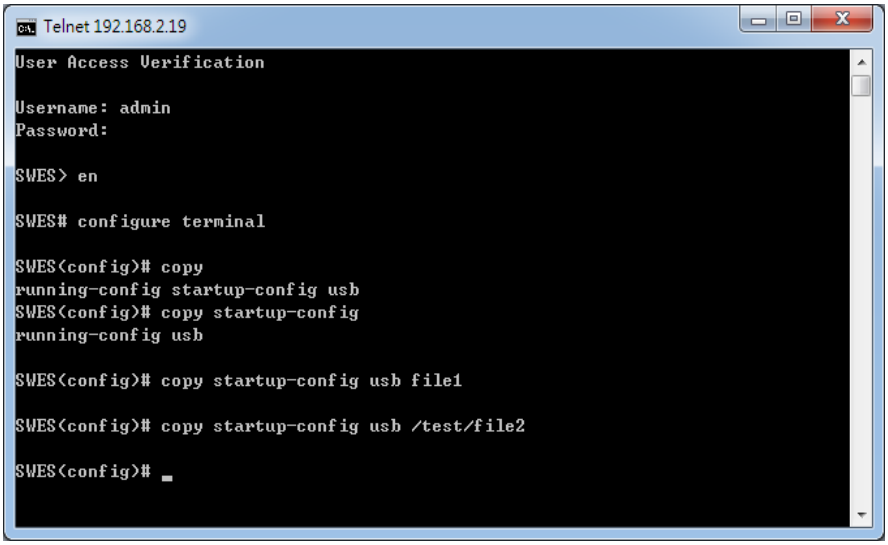
1. CLI: enable -> configure terminal ->copy running-config usb (path)



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

Ex: file1, / folder /file2.

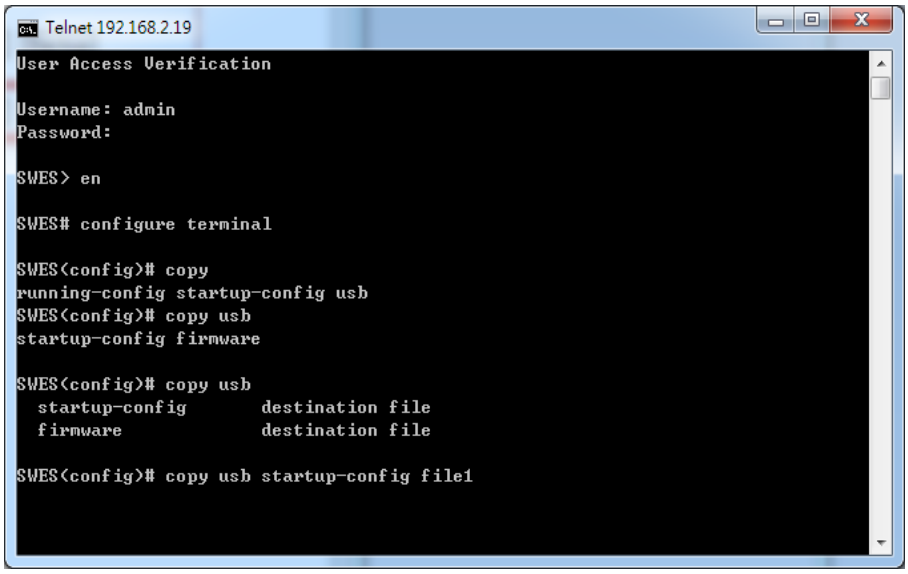
2. CLI : enable -> configure terminal ->copy startup-config usb (path)



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

Ex: file1, / folder /file2.

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

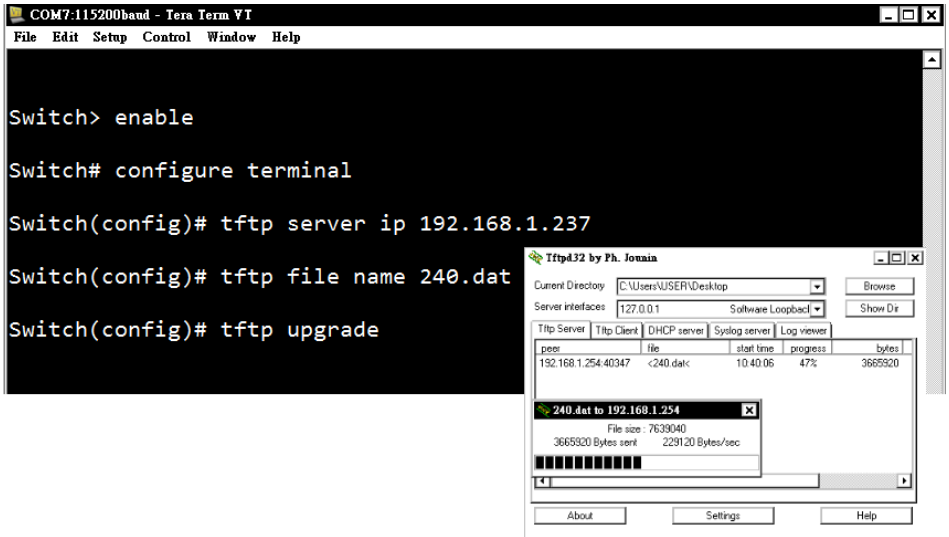


Fill in the folder and filename behind the “copy usb startup-config” command.

Ex: file1, / folder /file2.

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 LMX-1204G-SFP series: 12-port industrial gigabit managed Ethernet switch with 8*10/100/1000Tx and 4*100/1000 SFP slots.

Standards	IEEE 802.3	10Base-T 10Mbit/s Ethernet
	IEEE 802.3u	100Base-Tx, 100Base-Fx, Fast Ethernet
	IEEE 802.3ab	1000Base-Tx Gigabit Ethernet
	IEEE 802.3z	Gigabit Fiber
	IEEE 802.3x	Flow Control for Full Duplex
	IEEE 802.3ad	Port Trunking with LACP
	IEEE 802.1d	STP (Spanning Tree Protocol)
	IEEE 802.1w	RSTP (Rapid Spanning Tree Protocol)
	IEEE 802.1s	MTP (Multiple Spanning Tree Protocol)
	ITU-TG.8032 / Y.1344	ERPS (Ethernet Ring Protection Switch)
	IEEE 802.1q	Virtual LANs (VLAN)
	IEEE 802.1x	Port based Network Control, Authentication
	IEEE 802.1ad	Stacked VLAN, Q-in-Q
	IEEE 802.1p	QoS/CoS Protocol for Traffic Prioritization
Switch	Protocol	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 1,488,000pps for 1000Base-TxGigabit Ethernet port
	Packet Buffer	4 Mbits
	MAC Table	8K
	Jumbo Frame	9.6k
	Flow Control	IEEE 802.3x-full duplex mode, back pressure-half duplex mode
	VLAN Groups	1 ~ 4094
	IGMP Groups	Up to 256
Port Interface	Ethernet (RJ45) Port	8*10/100/1000BaseTx auto negotiation speed, Full/Half duplex mode, and auto MDI connection
	Fiber Connections	4*100/1000 Dual rate SFP fiber slots
	Serial Console Port	1*RS232 in RJ45 connector with console cable, 115.2Kbps, 8,N,1
	Configuration Backup Port	1*USB 2.0
Protection	Overload Current	Present

	Power Reverse polarity	Present
	CPU Watch Dog	Present
	Network Cable	10Base-T: 2-pair UTP/STP Cat. 3, 4, 5 cable; 100Base-TX: 2-pair UTP/STP Cat. 5 cable. EIA/TIA-568 100-ohm (100m) 1000BaseTX: UTP/STP Cat.5/5E cable; EIA/TIA-568 100-ohm (100m)
Mechanical Characteristics	LED Indicator	Power Unit: P1 (Green), P2 (Green),fault(Green/Red) Ethernet port: Link/active(Green), 1000Mbps
	Housing	Metal IP30 protection
	Dimension	54 x 142 x 99 mm
	Weight	Unit Weight: 2.4 lbs. Shipping Weight: 3.2 lbs
	Mounting	DIN-Rail Mounting, wall-mounting (included)
Power Requirements	Input Voltage	12~48VDC Redundant Input
	Power Connection	1 removable 6-contact terminal block
	Power Consumption	15 Watts
Environmental Limits	Operating Temperature	STD: -10° to 70° C (14° to 158° F); EOT: -40° to 75° C (-40° to 167° F)
	Storage Temperature	-40°C ~ 85°C (-40°F ~ 185°F)
	Ambient Relative Humidity	5 to 95%, (non-condensing)
Regulatory Approvals	EMI	FCC Class A
	EMS	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 508 (Pending)

Table 7.1 - LMX-1204G-SFP Series Technical Specifications

Antaira Customer Service and Support

(Antaira US Headquarter) + 844-268-2472

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

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

Please report any problems to Antaira:

www.antaira.com / support@antaira.com

www.antaira.eu / info@antaira.eu

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

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