EH7510
Industrial Managed Ethernet Switch

User Manual

EUROMOBILE
WIRELESS SOLUTIONS

Version 1.0

October, 2011

atop Technologies

TEL: +7 (812) 331-75-76

8 800 555-75-76

http://www.euromobile.ru

info@euroml.ru

Important Announcement

The information contained in this document is the property of Atop Technologies, Inc. and is supplied for the sole purpose of operation and maintenance of Atop Technologies, Inc products. No part of this publication is to be used for any other purposes, and it is not to be reproduced, copied, disclosed, transmitted, stored in a retrieval system, or translated into any human or computer language, in any form, by any means, in whole or in part, without the prior explicit written consent of Atop Technologies, Inc.

Published by

Atop Technologies, Inc.

2F, No. 146, Sec. 1, Tung-Hsing Rd.
Jubei, Hsinchu 30261
Taiwan, R.O.C.
Tel: 886-3-5508137
Fax: 886-3-5508131
www.atop.com.tw

Table of Contents

Preface

This manual contains some advanced network management knowledge, instructions, examples, guidelines, and general theories; designed to help users manage EH7510 and use its software, a background in general theory is a must when reading it. Please refer to the Glossary for technical terms and abbreviations.

Who Should Use This User Manual

This manual is to be used by qualified network personnel or support technicians who are familiar with network operations; it might be useful for system programmers or network planners as well. This manual also provides helpful and handy information for first time users. For any related problems please contact your local distributor, should they be unable to assist you, please redirect your inquiries to www.atop.com.tw.

Supported Platform

This manual is designed specifically for the EH7510 switch series.

Warranty Period

Atop technology provides a limited 5-year warranty for EH7510 switches.

Chapter 1: Introduction

1.1 What is a Managed Industrial Switch

Atop's EH (**E**thernet Switching **H**ub) 7510 is a powerful managed industrial switch; a switch is referred to as an OSI Layer 2* bridging device. Unlike an "**unmanaged**" switch, which is normally found in homes or in SOHO environments and runs in "auto-negotiation" mode, each port on a "**managed switch**" can be configured for its link bandwidth, priority, security, and duplex settings. The managed switches can be managed by web browsers, Telnet, or serial console. Since every single port can be configured to specific settings, network administrators can better control the network and maximize network functionality.

EH7510 is an industrial switch (as opposed to a commercial switch); a commercial switch simply works in a comfortable office environment. However, an industrial switch like EH7510 is designed to perform in harsh industrial environments, i.e., extreme temperature, high humidity, dusty air, potential high impact or the presence of potentially high static charges. EH7510 works fine even in these environments.

Atop EH7510 is designed to provide faster, securer, and more stable networks. One advantage that makes EH7510 a powerful switch is that it supports technologies including ERPS, iA-Ring, Compatible Ring and RSTP. These technologies provide better network reliability, and decreases recovery time down to less than 20 ms.

EH7510 Ethernet Switch supports a wide range of IEEE standard protocols. This switch is excellent for keeping systems running smoothly, reliable for preventing system damage or losses, and friendly to all levels of users. The goal of this innovative product is to bring users a brand new network-management experience.

***Note:**

Throughout the manual, the symbol * indicates that more detailed information of the subject will be provided at the end of this book.

1.2 Software Features

- Atop's iA-Ring ERPS Technologies
  - Improve network redundancy
  - Fast recovery time (<20ms)
  - iA-Ring Provides Ring Coupling and Dual Homing
- Three User Friendly Interfaces Supported
  - Web browser
  - Telnet Console
  - Serial Console
- SNMP v1/v2/v3 Supported (with MD5 Authentication and DES encryption)
- RSTP Support
- QoS Traffic Regulation Supported
- IGMP supported (with IGMP snooping)
- Alarm System Supported (with E-mail Notification)
- IEEE 802.1x (with RADIUS) Supported for Network Access Control
- LACP Supported
- Compatible Ring
- U-Ring
- SNTP
- PTP
- GVRP
- GMRP
- Spanning Tree
- LLDP

1.3 Hardware Features

Device Appearance, Fig. 1.1:

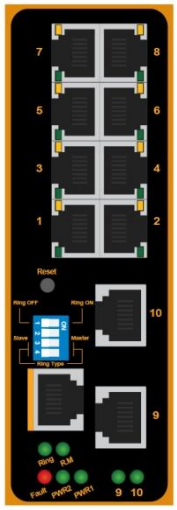


Fig. 1.1

- Dimensions: 53.4 mm (W) x 119.9 mm (D) x 145.7 mm (H)
- Weight: approx 1.1kg
- 8 x 10/100M Ethernet ports (Port # 1~8)
- 2 x Gigabit Ethernet ports or 2 x Fiber ports (Port # 9~10)
- 1 x Serial Console Port
- 1x4 DIP switch
- LED indicators
- 1 x Reset button

Caution

An approved Optical transceiver should be chosen to plug into the slot.


Never install or work on electrical or cabling during periods of lighting activity.

Never connect or disconnect power when hazardous gases are present.


WARNING: Disconnect the power and allow to cool 5 minutes before touching.


Caution: CLASS 1 LASER PRODUCT. Do not stare into the laser!

1.4 Power Requirements

- Dual Inputs: 12~48 Volts DC
- Input Current: 1.2A Max.

1.5 Environmental Limitations

- Operating Temp: -40°C ~ 80°C (or -40°F ~ 176°F)
- Storage Temp: -40°C ~ 85°C (or -40°F ~ 185°F)
- Relative Humidity (non-condensing): 5 to 95 %

Note: for UL policy, the maximum operating temperature is 60°C and the human body can tolerate a maximum of 70°C.

1.6 LED Indicators

- Port LED:

  Green Light: Steady- Link up, Blinking- Data transmitting

  Orange Light: on- full duplex, off- half duplex (refer to section Port)
- PWR 1: Indicates power 1 status
- PWR 2: Indicates power 2 status
- Fault: Indicates Fault status
- R.M: Indicates Atop's Ring Master Status (Refer to section ERPS/Ring)
- Ring: Indicates Atop's Ring Status (Refer to section ERPS/Ring)

Chapter 2: Configuring with a Web Browser

This chapter explains how to access EH7510 for the first time. There are three ways to configure this Ethernet Switch:

1. Web browser
2. Telnet console
3. Serial console

The web browser and telnet console methods allow users to access the switch over the Internet or the Ethernet LAN, while the serial console method requires a serial cable connection between the computer and the switch; there are only a few differences among these three methods.

2.1 Web-based Management Basics

Users can access EH7510 easily by their web browsers (Internet Explorer 7.0 and Mozilla Firefox 3.5.7 or later versions recommended). We will proceed to use a web browser to introduce EH7510's functions; this web console interface is user-friendly.

2.1.1 Default Settings

Below there is a list of default factory settings; this information will be used during the login process..

IP Address: **10.0.50.1**
Subnet Mask: **255.255.0.0**
Default Gateway: **10.0.0.254**
User Name: **admin**
Password: **NULL (leave it blank)**

2.1.2 Login Process and Main Window Interface

Before the user access EH7510 switch's configuration they have to log in; this can be done in 3 simple steps.

1. Launch a web browser.
2. Type the switch's IP address (e.g. https://10.0.50.48), (next page, Fig. 2.1).

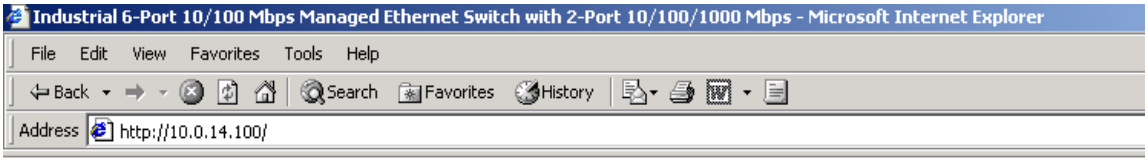


Fig. 2.1

3. Key in the username and password on the login window, and click "**OK**" to login.

＊Note: Please take care on configuring the IP in your PC's Settings when pairing the switch. ＊

After the login process, the main interface will show up, which should look as Fig. 2.2. The main menu (left side of the screen) provides the links at the top level of the menu hierarchy and allows them to be expanded to display lower level links. Note that in this case the port 1 is highlighted in green; this shows that the port is being connected to a LAN cable. Detailed explanations of each sub-section will be addressed later as the need arises.

+ Information
+ Administration
+ Port
+ Trunking
+ Unicast/Multicast MAC
+ GARP/GVRP/GMRP
+ IGMP/IP Multicast
+ SNMP
+ Spanning Tree
+ VLAN
+ Port Security
+ ERPS/Ring
+ LLDP
+ System Warning
+ Diagnosis
+ System Log
+ System

Basic

Description	Managed Switch EH7510
MAC address	00:60:E9:07:98:96
Application Version	1.25
Kernel Version	1.20
Memory	78108K used, 49612K free, 0K shrd, 560K buff, 62532K cached

Fig. 2.2

2.2 Information

To help users be familiar with the device, the **Information** section provides important details of it; this is also the main welcoming screen once the user has logged in. The details make it easier to identify different devices connected to the network; they are divided into four sections.

2.2.1 Basic

An introduction to the equipment and net is done in this section, Fig. 2.3.

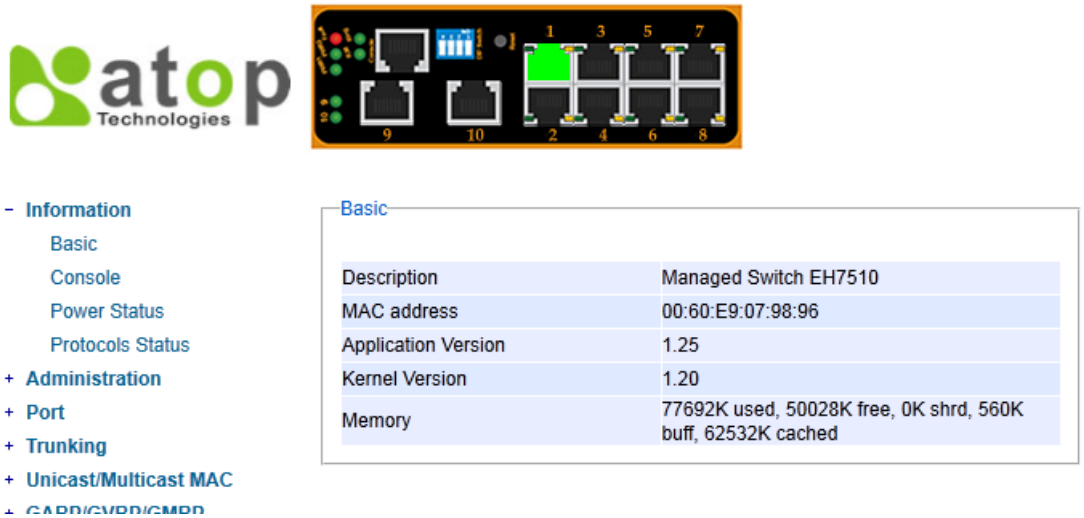


Fig. 2.3

Table 2.1

Label	Description
Description	Describes the model type of current device.
MAC address	Indicates MAC address* (See Appendix A).
Application Version	States current Application version of the device.
Kernel Version	Shows current Kernel Version of the device.
Memory	Shows current RAM's size availability also shows the cached and shared memory.

2.2.2 Console

In this chapter, we use a web browser for configuring the switch. However, there is a specific page for the serial console method. The **Console option** is only for serial console; it indicates the connection parameters related to the method.

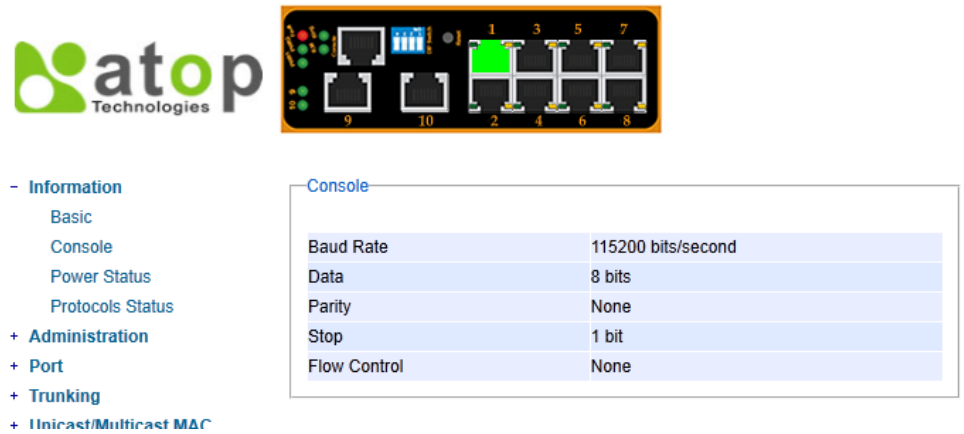


Fig. 2.4

2.2.3 Power Status

EH7510 Managed Switch has dual VDC power inputs; Fig. 2.5 below, shows the status of each power input.

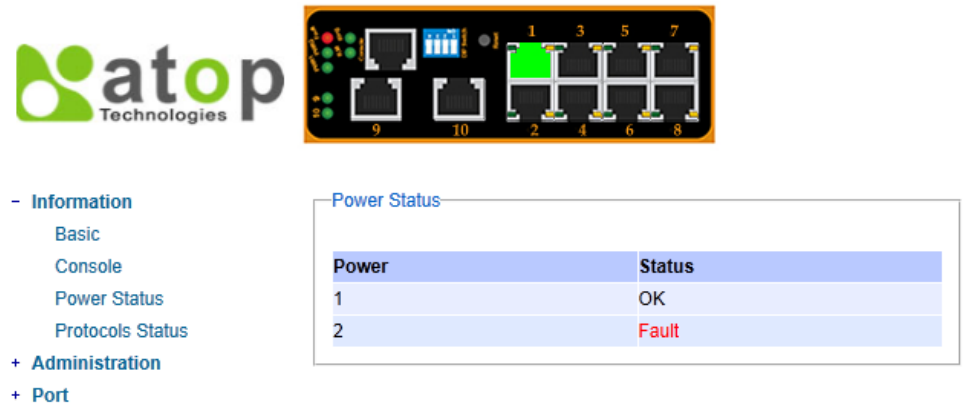


Fig. 2.5

2.2.4 Protocol Status

Reports an overall status of each protocol; while users can view status all at once here, detailed explanations of each protocol and methods will be provided in later sections, Fig. 2.6.

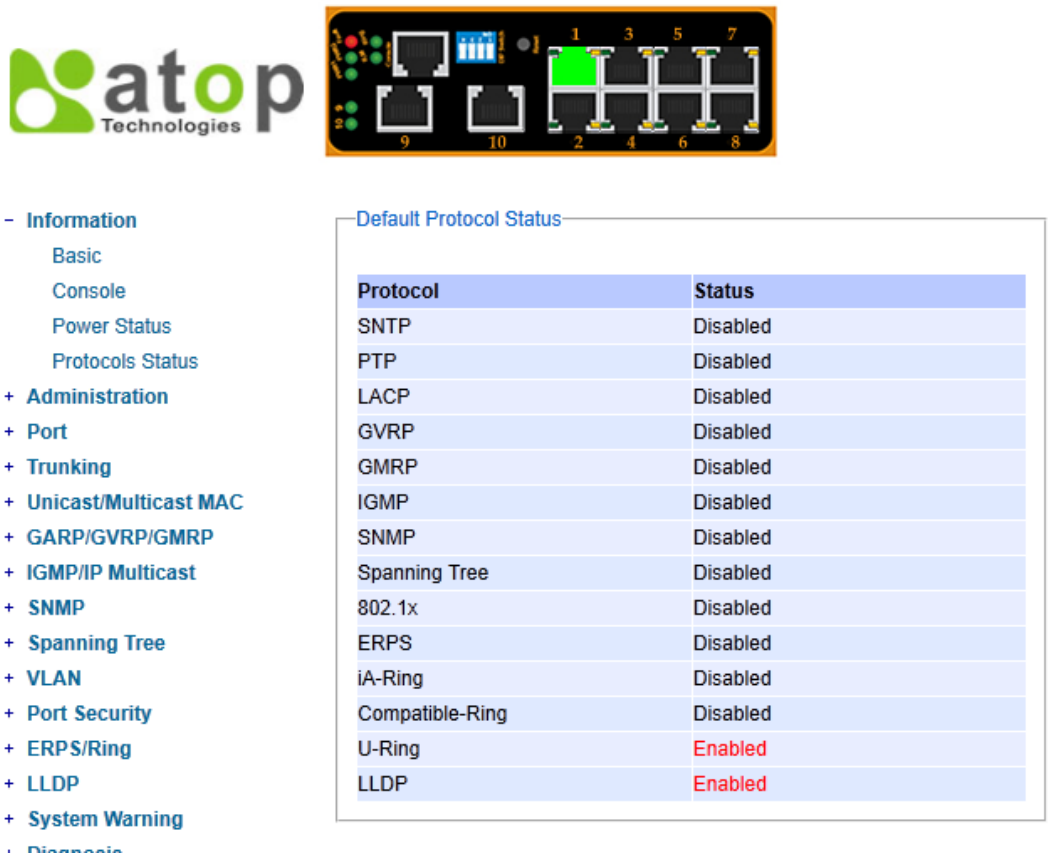


Fig. 2.6

2.3 Administration

Here users will be able to make changes on **System Settings**, **Password**, **IP Settings**, **Forwarding and QoS**, **Mirror Port**, **System Time/SNTP, Modbus Setting** and **PTP setting**.

2.3.1 System Settings

Users can enter system's details here; this information can help identify one specific switch among all the devices in the network, (Fig. 2.7).

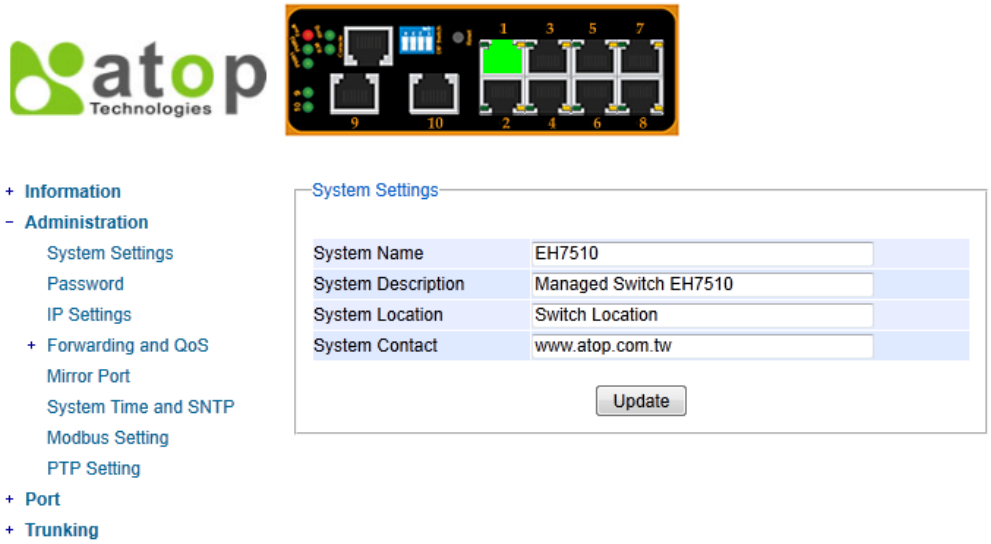


Fig. 2.7

Table 2.2

Label	Description	Factory Default
System Name	Specifies a particular role or application of different switches. The name entered here, will also be shown in Switch View and Device View. Max. 63 Characters.	EH7510
System Description	Detailed description of the unit. Max. 63 Characters.	Managed Switch EH7510
System Location	Locations of different switch units. Max. 63 Characters.	Switch Location
System Contact	Provides contact information for maintenance. Enter the name of whom to contact in case a problem arises. Max. 63 Characters.	www.atop.com.tw

2.3.2 Password

Although no password is set for the device when it is manufactured, users can make changes to assure overall system security, Fig. 2.8.

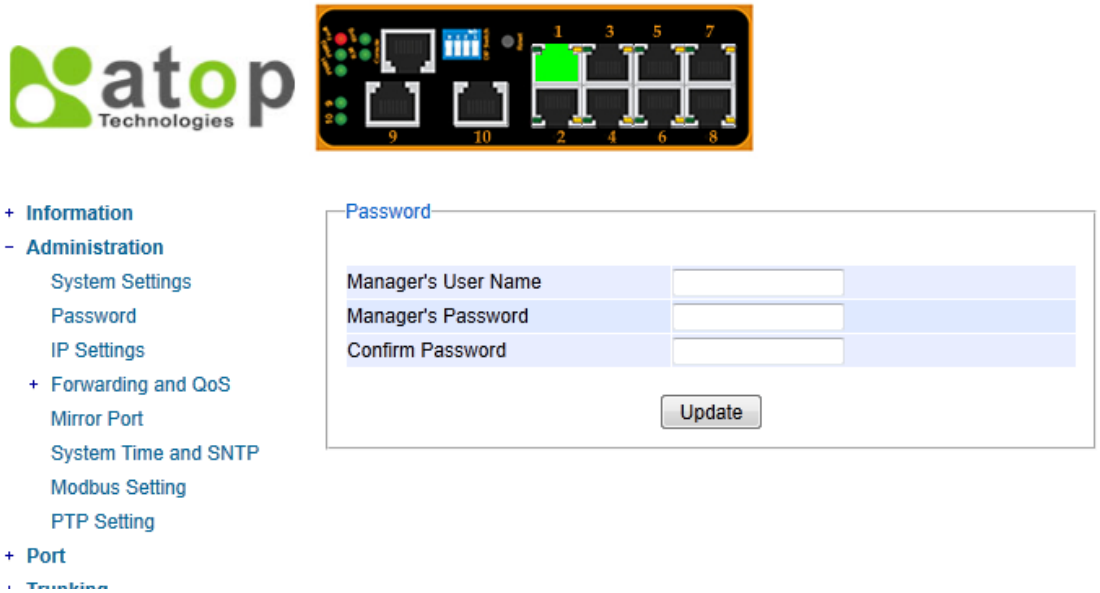


Fig. 2.8

Table 2.3

Label	Description	Factory Default
Manager's User name	User's Name. Max. 15 Characters.	NULL
Manager's Password	Password. Max. 15 Characters.	NULL
Confirmed Password	Re-type the Password. This has to be exactly as the password entered in the above field. Max.15 Characters.	NULL

2.3.3 IP Settings

In this section, users may modify IP address functions to reconfigure the switch's network settings. Users can choose to enable DHCP (Dynamic Host Configuration Protocol)* here. This function can obtain an IP address automatically; it provides automatic configuration and eliminates the need for intervention by the administrator. Users can also opt to set up the IP address and related fields manually; after each update, a reboot will be required before the new settings are effective, Fig. 2.9.a.

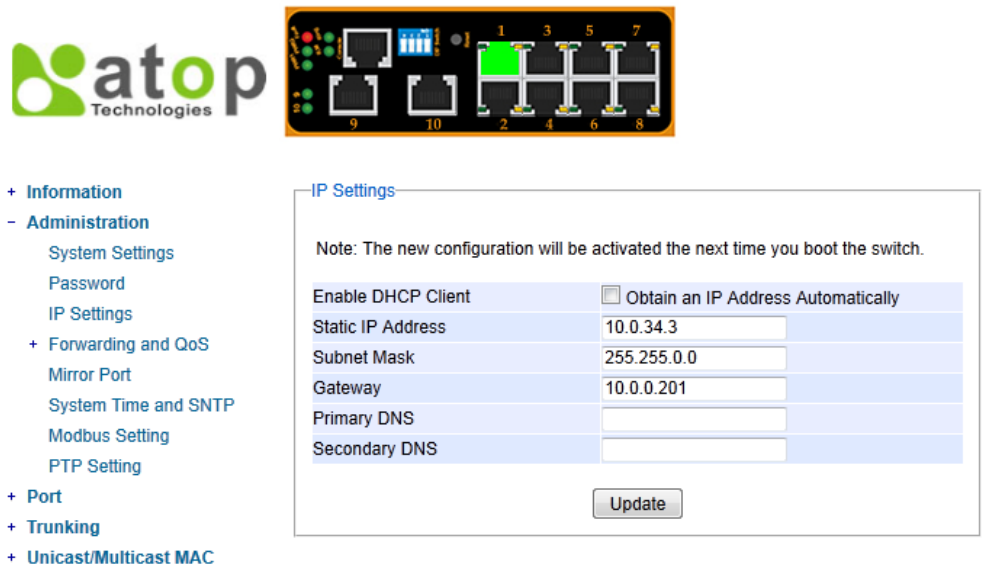


Fig. 2.9.a

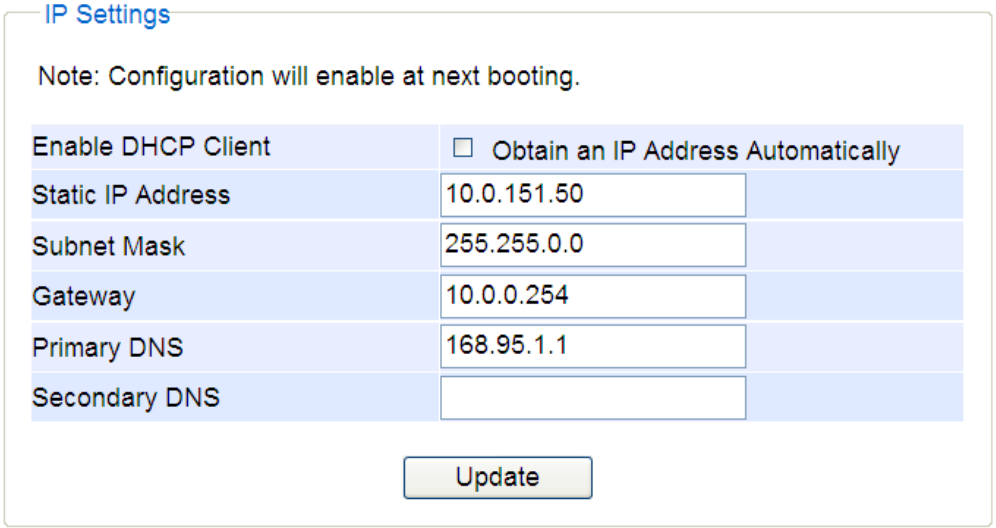


Fig. 2.9.b ＊Example＊

Table 2.4

Label	Description	Factory Default
Enable DHCP Client	By checking this box, an IP address will be automatically assigned. Otherwise users can set up the IP address manually.	Uncheck
Static IP address	Displays current IP address. Users can also set new static IP address for the device.	10.0.50.1
Subnet Mask	Displays current Subnet Mask or set new subnet mask.	255.255.0.0
Gateway	Shows current Gateway or set a new one.	10.0.0.254
Primary DNS	Sets the DNS IP address * used by your network.	NULL
Secondary DNS	Sets the Secondary DNS IP address EH7510 will locate the secondary DNS server if the Primary DNS Server fails to connect.	NULL

2.3.4 Forwarding and QoS

EH7510 provides:

- **Forwarding function**
- **Filter functions**
- **Quality of Service (QoS) functions**

To make data delivery more reliable; for forwarding functions, users can set up an ageing time, to avoid the case that a MAC address cannot be found, Fig. 2.10.

Filter Functions

Storm Filter Function:

For this function, users can select filtering levels,

- DLF Mode: **D**estination **L**ookup **F**ailure. The switch wi**ll** always lo**o**k for a MA**C** desti**n**ation address first. In case that a MAC address cannot be found, which means DLF occurs, the switch will forward the packets to all ports that are in the same VLAN.
- Multicast: This type of transmission sends messages from one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive it; also networks that support multicast send only one copy of the information across the network until the delivery path that reaches group members diverges. At these diverging points, multicast packets will be copied and forwarded; this method can manage high volume of traffic with different destinations while using network bandwidth efficiently.
- Broadcast: Messages sent to all devices.

QoS:

The main objective of Quality of Service is to transfer certain data packets either particularly safe or as immediately as possible. With EH7510, users are able to prioritize traffic on the network to ensure that high priority data can be transmitted as soon as possible. Network traffic is controlled by a set of rules. These rules help classify different types of traffic and define how each of them should be treated as they're being transmitted. EH7510 can also inspect both 802.1p CoS tags and DiffServ tag to provide consistent classification.

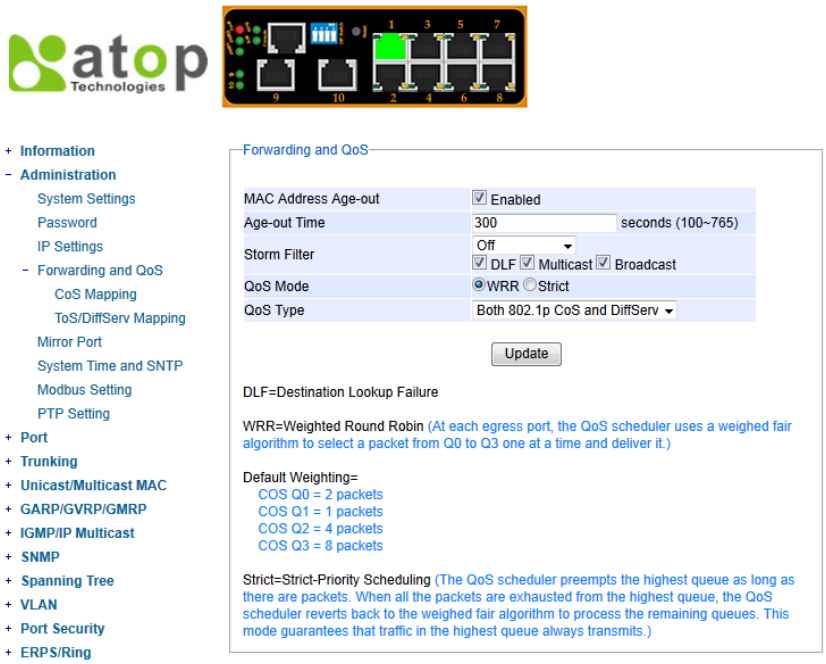


Fig. 2.10

Table 2.5

Label	Description	Factory Default
MAC Address Ageing Time	Choose to enable MAC Address* ageing time function. If enabled, when an entry reaches its aging time, it will be cleared from the switch. Enabling this function can cancel frame forwarding effectively.	Checked
Ageing Time	Specifies the **ageing time**. Range100 ~ 765 seconds.	300
Storm Filter	Select filter level from **Off, 5%, 10%, 15%, 20%, or 25%**.	Off
	Enable **storm filter** function and choose from **DLF, Multicast** and/or **Broadcast traffic.** See notes below for a detailed description.	DLF, Multicast and Broadcast enabled.
QoS Mode	Select the device **QoS mode: WRR** or **Strict**. See notes below for a detailed description and comparison.	WRR
Qos Type	**802.1p CoS only**: Switch only checks L2 802.1p CoS priority bits. **Both 802.1p CoS and DiffServ**: Switch checks both types. See notes below for a detailed description.	Both types are selected.

QoS Mode:

- **WRR**: **W**eighted **R**ound **R**obin. This method services all the traffic queues, but higher priority queues still retain their advantage; this mode guarantees that in the event that high-priority traffic exceeds the link capacity, lower priority traffic will still proceed and not be blocked.
- **Strict** is Strict-Priority Scheduling. The QoS scheduler preempts the highest queue as long as there are packets. When all the packets are exhausted from the highest queue, the QoS scheduler reverts back to the weighed fair algorithm to process the remaining queues. This mode guarantees that traffic in the highest queue always flows first.

QoS Type:

- **802.1p CoS:** IEEE standard of layer 2 marking scheme. It specifies a priority value between 0 and 7 that can be used by QoS to differentiate traffic. When this option is enabled, EH7510 inspects the 802.1p CoS tag in the MAC frame to determine the priority of each frame.
- **DiffServ/ToS**: DiffServ stands for Differentiated Services. It's a networking architecture that specifies a simple but scalable mechanism for classifying network traffic and providing QoS guarantees on networks. It uses the DiffServ Code Point (DSCP, which is the modern redefinition of the ToS). DiffServ/ToS function allows users to use up to 64 values to define service levels and set priority.

  Settings of CoS and ToS can be accessed on the mapping tables in next two options.

2.3.4.1 CoS Mapping

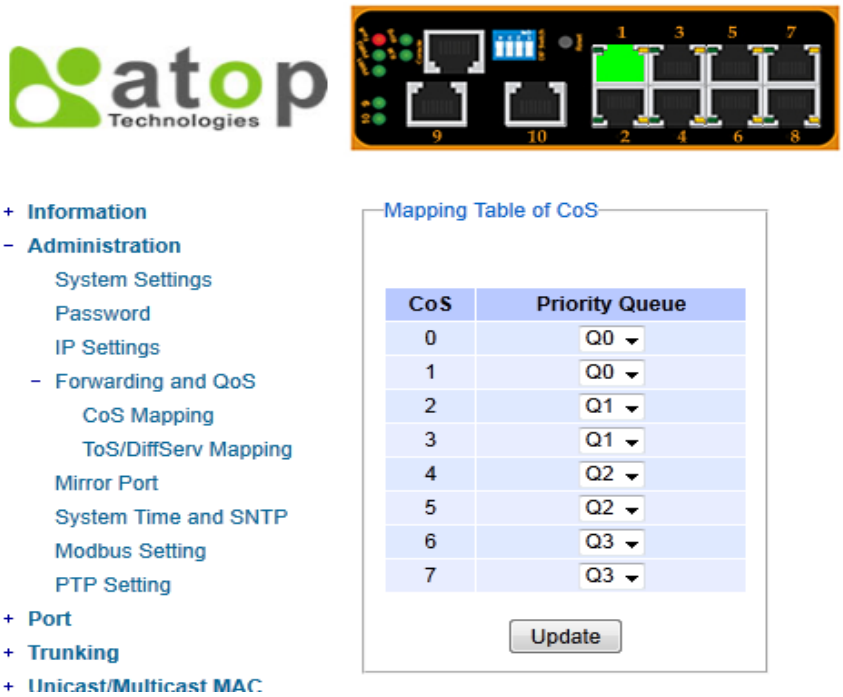


Fig. 2.11

The switch can classify traffic based on a valid 802.1p (CoS) priority tag. These options allow users to map CoS to the different priority queues, Fig. 2.11.

The default queue weighting is assigned as follow:

Q0 = 2 packets (Lowest priority)

Q1 = 1 packets (Low priority)

Q2 = 4 packets (Median priority)

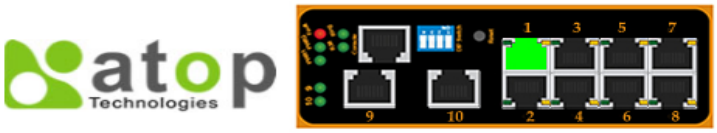
Q3 = 8 packets (High priority)

For example, Q3 has the highest priority, and it carries 8 packets, while Q0 has the lowest priority, and it carries 2 packets. When CoS 6 is assigned to Q3, it has the highest priority. When Co1 is assigned to Q0, it has the lowest priority. For CoS explanations, please refer to page 14.

Table 2.6

Label	Description	Factory Default
Priority Queue	Set the mapping table of different CoS to 4 different level queues.	CoS 0, 1: Q0 CoS 2, 3: Q1 CoS 4, 5: Q2 CoS 6, 7: Q3

2.3.4.2 ToS/DiffServ Mapping



- + Information
- − Administration
  - System Settings
  - Password
  - IP Settings
  - − Forwarding and QoS
    - CoS Mapping
    - ToS/DiffServ Mapping
  - Mirror Port
  - System Time and SNTP
  - Modbus Setting
  - PTP Setting
- + Port
- + Trunking
- + Unicast/Multicast MAC
- + GARP/GVRP/GMRP
- + IGMP/IP Multicast
- + SNMP
- + Spanning Tree
- + VLAN
- + Port Security
- + ERPS/Ring
- + LLDP

Mapping Table of ToS (DSCP)

ToS	Level	ToS	Level	ToS	Level	ToS	Level
0x00(0)	Q1	0x04(1)	Q1	0x08(2)	Q1	0x0C(3)	Q1
0x10(4)	Q1	0x14(5)	Q1	0x18(6)	Q1	0x1C(7)	Q1
0x20(8)	Q1	0x24(9)	Q1	0x28(10)	Q1	0x2C(11)	Q1
0x30(12)	Q1	0x34(13)	Q1	0x38(14)	Q1	0x3C(15)	Q1
0x40(16)	Q0	0x44(17)	Q0	0x48(18)	Q0	0x4C(19)	Q0
0x50(20)	Q0	0x54(21)	Q0	0x58(22)	Q0	0x5C(23)	Q0
0x60(24)	Q0	0x64(25)	Q0	0x68(26)	Q0	0x6C(27)	Q0
0x70(28)	Q0	0x74(29)	Q0	0x78(30)	Q0	0x7C(31)	Q0
0x80(32)	Q2	0x84(33)	Q2	0x88(34)	Q2	0x8C(35)	Q2
0x90(36)	Q2	0x94(37)	Q2	0x98(38)	Q2	0x9C(39)	Q2
0xA0(40)	Q2	0xA4(41)	Q2	0xA8(42)	Q2	0xAC(43)	Q2
0xB0(44)	Q2	0xB4(45)	Q2	0xB8(46)	Q2	0xBC(47)	Q2
0xC0(48)	Q3	0xC4(49)	Q3	0xC8(50)	Q3	0xCC(51)	Q3
0xD0(52)	Q3	0xD4(53)	Q3	0xD8(54)	Q3	0xDC(55)	Q3
0xE0(56)	Q3	0xE4(57)	Q3	0xE8(58)	Q3	0xEC(59)	Q3
0xF0(60)	Q3	0xF4(61)	Q3	0xF8(62)	Q3	0xFC(63)	Q3

Update

Fig. 2.12

The switch can classify traffic based on a valid DiffServ (ToS) priority tag; Fig. 2.12 shows where users can map ToS to the different priority queues.

Table 2.7

Label	Description	Factory Default
Level	Sets the mapping table of different ToS to 4 distinct output queues, which are Q0 (lowest), Q1 (los), Q2 (median), and Q3 (highest).	ToS 0~15: Q1 ToS 16~31: Q0 ToS 32~47: Q2 ToS 48~63: Q3

For example, when ToS 0*F8 (62) is assigned to Q3, it has the highest priority. When ToS 0*40(16) is assigned to Q1, it has the lowest priority. For ToS explanations please refer to page 14.

2.3.5 Mirror Port

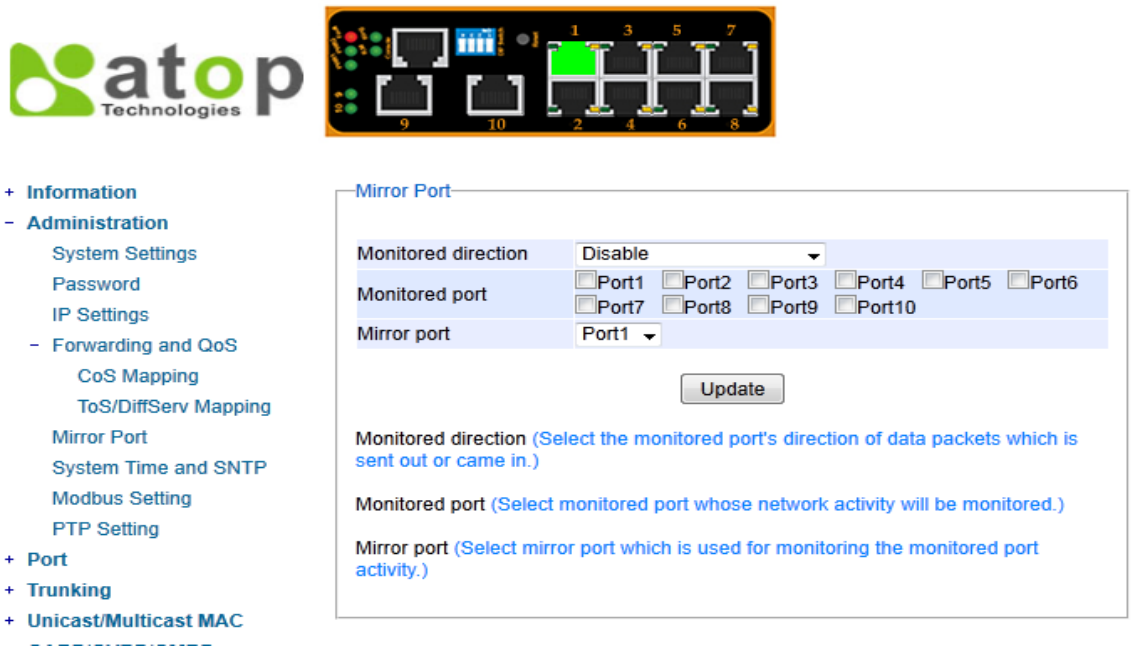


Fig. 2.13

In order to help the network administrator keep tracks of network activities, EH7510 supports port mirroring, which allows incoming and/or exiting traffic to be monitored by a single port that is defined as **mirror port,** (Fig. 2.13). IGMP snooping (Section 2.7) and mirroring functions are mutually exclusive. When IGMP snooping is enabled, the port mirroring function is disabled.

Table 2.8

Label	Description	Factory Default
Monitored direction	Select the monitoring direction. **Disable:** disable port monitoring. **Input data stream:** monitor input data stream of monitored ports only. **Output data stream**: monitor output data stream of monitored ports only. **Input /Output data stream:** monitor both input and output data stream of monitored ports.	Disabled
Monitored Port	Select the ports that will be monitored.	Unchecked all
Mirror port	Select the mirror port that will be used to monitor the activity of the monitored ports.	Port1

2.3.6 System Time and SNTP

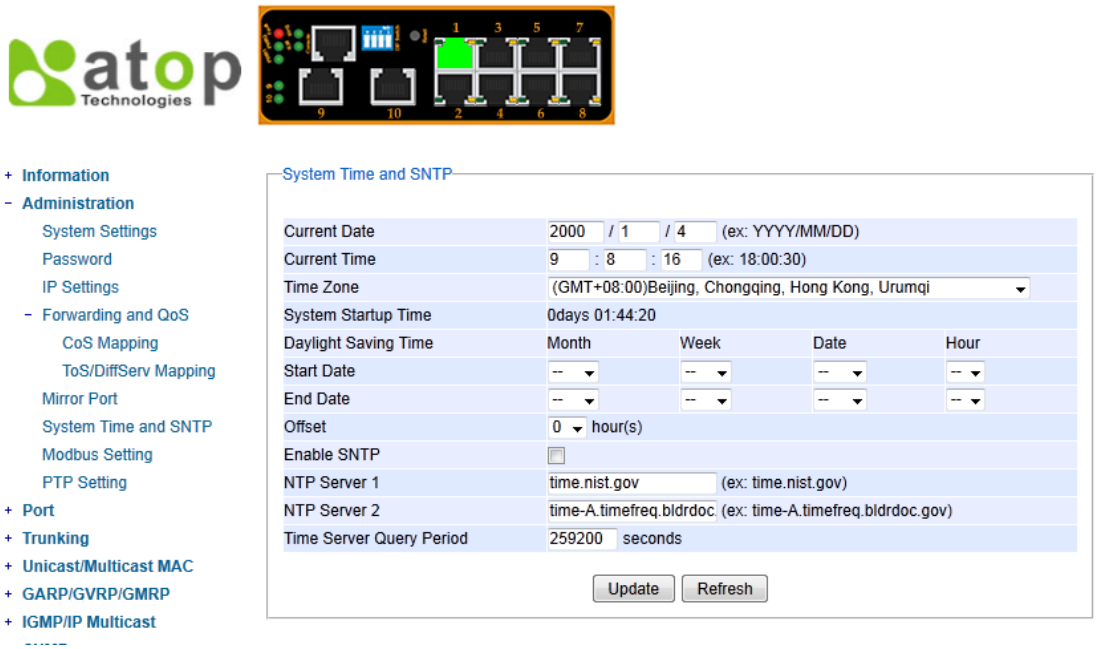


Fig. 2.14

This option, (Fig. 2.14) configures EH7510 time and date; it also supports Daylight Saving Time and SNTP (See notes below for explanation).

Table 2.9

Label	Description	Factory Default
Current Date	Allows local date configuration in yyyy/mm/dd format	None
Current Time	Allows local time configuration in local 24-hour format.	None
System Startup Time	Indicates how long the switch has been working.	Dependant
Daylight Saving Time	Start Date: defines the start date of daylight saving. End Date: defines the end date of daylight saving. Offset: decide how many hours to be shifted forward/backward when daylight saving time begins and ends. See note below.	None
Enable SNTP	**Enables SNTP** function. See note below.	Unchecked
NTP Server 1	Sets the first IP or Domain address of **NTP Server.**	time.nist.gov
NTP Server 2	Sets the second IP or Domain address of **NTP Server.** Switch will locate the 2nd NTP Server if the 1st NTP Server fails to connect.	Time-A.timefreq.bldrdoc.gov
Time Zone	User's current local time.	(GMT+08:00)Beijing, Chongqing, Hong Kong
Time Server Query Period	This parameter determines how frequently the time is updated from the NTP server.	259200 seconds.

Note:

- Daylight Saving Time: In certain regions (e.g. US), local time is adjusted during summer season in order to provide an extra hour of daylight in the afternoon, and the time shifted

forward (or backward) is usually an hour.

- SNTP: **N**etwork **T**ime **P**rotocol. It is used to synchronize the computer systems' clocks. Two of the NTP server examples would be *time.nist.gov* and *clock.stdtime.gov.tw.*

2.3.7 Modbus Setting

Modbus is a serial communication protocol which allows communication between devices to be connected to the same network. It is used to connect a supervising computer to the network, and thus control all the devices behind it.

Fig. 2.15

Fig. 2.15 shows where users can set up the modbus address; in addition to that, users can use **Modbus Poll** for configurations. Setup steps are illustrated as follows:

1. Make sure the **Modbus Poll** is connected to your target EH7510.
2. Click on "**06**" on the top toolbar.

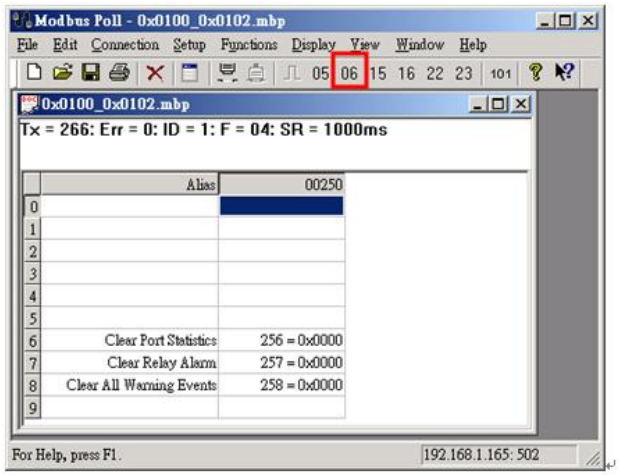


Fig. 2.16

3. Set **Address** to a desired value between 250 and 256.

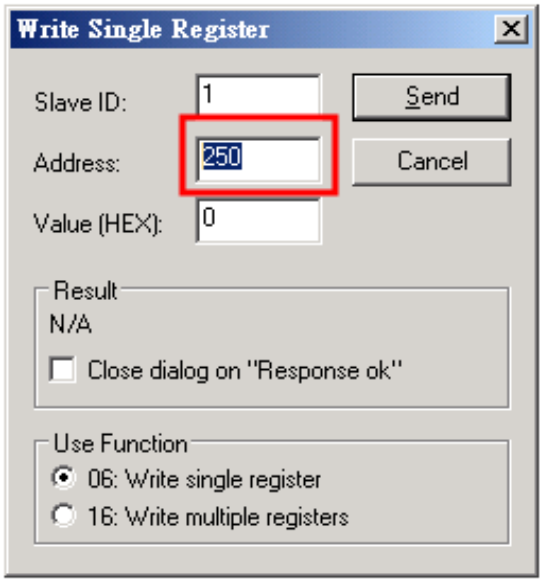


Fig. 2.17

4. Correct **Value (HEX)** has to be selected corresponding to **Address** entered above. As in this example, **Result** shows “Illegal Data Value” since **Address** 256 can only take 1 as **Value (HEX)**.

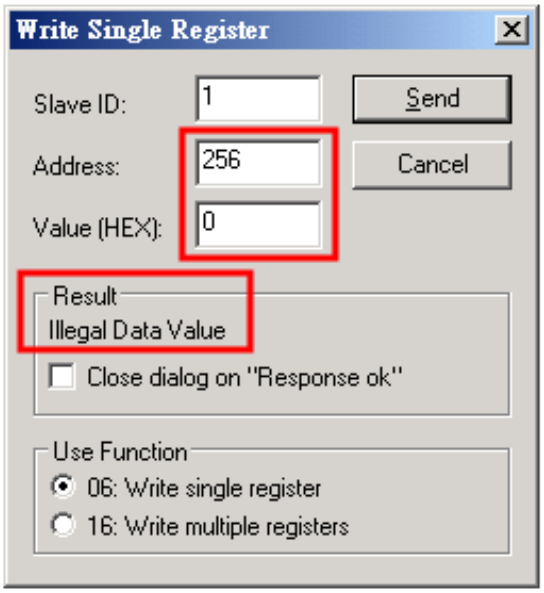


Fig. 2.18

5. If a correct **Value (HEX)** is selected, the process will be completed successfully.

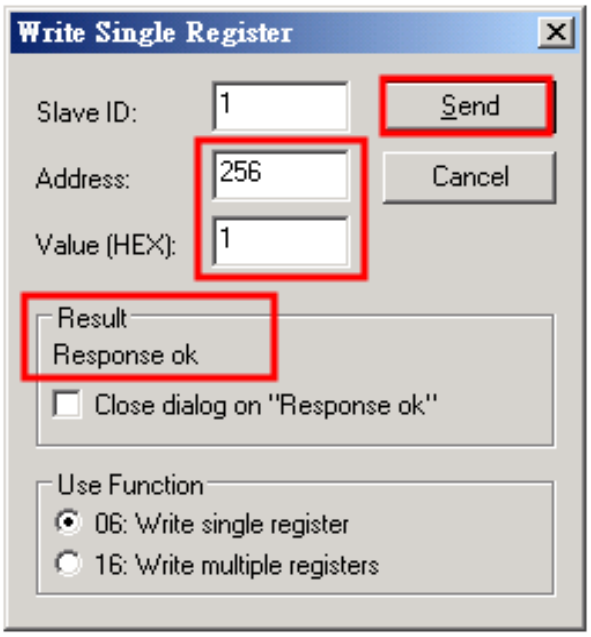


Fig. 2.19

2.3.8 PTP Setting

The Precision Time Protocol (PTP) is a high-precision time protocol. It is for precise synchronization of clocks on a local area network by measurement and control systems. Fig. 2.20 (on the next page), shows where to configure PTP and to see PTP status

+ Information
- Administration
  - System Settings
  - Password
  - IP Settings
  - Forwarding and QoS
    - CoS Mapping
    - ToS/DiffServ Mapping
  - Mirror Port
  - System Time and SNTP
  - Modbus Setting
  - PTP Setting
+ Port
+ Trunking
+ Unicast/Multicast MAC
+ GARP/GVRP/GMRP
+ IGMP/IP Multicast
+ SNMP
+ Spanning Tree
+ VLAN
+ Port Security
+ ERPS/Ring
+ LLDP
+ System Warning
+ Diagnosis
+ System Log
+ System

PTP Configuration

State	Enabled
Version	1
Clock Mode	End-to-End
Transport	Ethernet
Sync Interval	1 seconds
Clock Stratum	3
Clock Class	248
priority 1	128
priority 2	128
UTC Offset	0
Offset To Master	0 ns
Grandmaster UUID	0-60-e9-7-98-96
Parent UUID	0-60-e9-7-98-96
Clock Identifier	DFLT

Update

PTP Port

Port	Enabled	Status
Port1	Enabled	Disabled
Port2	Enabled	Disabled
Port3	Enabled	Disabled
Port4	Enabled	Disabled
Port5	Enabled	Disabled
Port6	Enabled	Disabled
Port7	Enabled	Disabled
Port8	Enabled	Disabled
Port9	Enabled	Disabled
Port10	Enabled	Disabled

Port	Mode
Port1 Port2 Port3 Port4 Port5 Port6	Disabled

Update

Fig. 2.20

Table 2.10

Label	Description	Factory Default
State	Enabled/Disable the PTP function	Unchecked
Version	Set the PTP operation version	1
Clock Mode	PTP (Precision Time Protocol) clock type selection.	End-to-End
Transport	Ethernet (layer 2) multicast transport or layer 3 (UDP/IP) multicast transports for PTP (Precision Time Protocol) messages' selection.	Ethernet
Sync Interval	Set the interval of the sync packet transmitted time	1
Clock Stratum	To set the Clock Stratum. The lower values take precedence to be selected as the master clock in the best master clock algorithm.	3
Clock Class	Clock's accuracy level, it's an attribute of an ordinary or boundary clock; denotes time traceability or frequency distributed by the grandmaster clock. Please refer to IEEE 1588-2008, Table 5 for definitions, allowed values, and interpretation.	248
priority 1	To set the clock priority 1 (PTP version 2). The lower values take precedence to be selected as the master clock in the best master clock algorithm.	128
priority 2	To set the clock priority 2 (PTP version 2). The lower values take precedence to be selected as the master clock in the best master clock algorithm.	128
UTC Offset	UTC offset value	0
Offset To Master	The offset time to the master clock	None
Grandmaster UUID	The grand master UUID for PTP version 1	None
Parent UUID	The parent master UUID for PTP version 1	None
Clock Identifier	The clock identifier for PTP version 1	None

The lower part of Fig. 2.20 shows how to configure PTP and to see its status per port.

Table 2.11

Label	Description	Factory Default
Port	Port number	None
Enabled	The port mode information, it indicates that the PTP port function is enabled or disabled.	None
Status	PTP port operation status	None
Mode	Enabled/Disabled PTP port function	Disabled

2.4 Port

This function contains three options, which are,

- **Port Status**
- **Port statistics**
- **Port control**

2.4.1 Port Status

+ Information
+ Administration
− Port
  - Port Status
  - Port Statistics
  - Port Control
+ Trunking
+ Unicast/Multicast MAC
+ GARP/GVRP/GMRP
+ IGMP/IP Multicast
+ SNMP
+ Spanning Tree
+ VLAN
+ Port Security
+ ERPS/Ring
+ LLDP

Port Status

Port	Mode	Enable	Link	Negotiation		Speed		Duplex		Flow Control		Rate Control		Security
				Config	Actual	Config	Actual	Config	Actual	Config	Actual	Ingress	Egress	
Port1	Copper	On	Up	Auto	Auto	100	100	Full	Full	Off	Off	Off	Off	Off
Port2	Copper	On	Down	Auto	Auto	100	0	Full	Half	Off	Off	Off	Off	Off
Port3	Copper	On	Down	Auto	Auto	100	0	Full	Half	Off	Off	Off	Off	Off
Port4	Copper	On	Down	Auto	Auto	100	0	Full	Half	Off	Off	Off	Off	Off
Port5	Copper	On	Down	Auto	Auto	100	0	Full	Half	Off	Off	Off	Off	Off
Port6	Copper	On	Down	Auto	Auto	100	0	Full	Half	Off	Off	Off	Off	Off
Port7	Copper	On	Down	Auto	Auto	100	0	Full	Half	Off	Off	Off	Off	Off
Port8	Copper	On	Down	Auto	Auto	100	0	Full	Half	Off	Off	Off	Off	Off
Port9	Giga Copper	On	Down	Auto	Auto	1000	0	Full	Half	Off	On	Off	Off	Off
Port10	Giga Copper	On	Down	Auto	Auto	1000	0	Full	Half	Off	On	Off	Off	Off

Fig. 2.21

All ports status are shown,

- **Mode**
- **Enable State**(On or Off)
- **Link** condition(Up or down)
- **Negotiation** type(Auto or Force)
- **Speed** (unit: Mbps)
- **Duplex**
- **Flow Control**
- **Rate Control**
- **Security** (802.1X port status).

***NOTE**

- **Negotiation:** "**Force**" specifies forcing the speed and duplex as configured by users. "**Auto**" specifies using auto negotiation to determine the actual speed and duplex to use.
- **Duplex:** "**Half** duplex" allows one-way communication at a time, while "**Full** duplex" allows both-way communication at the same time.

2.4.2 Port Statistics

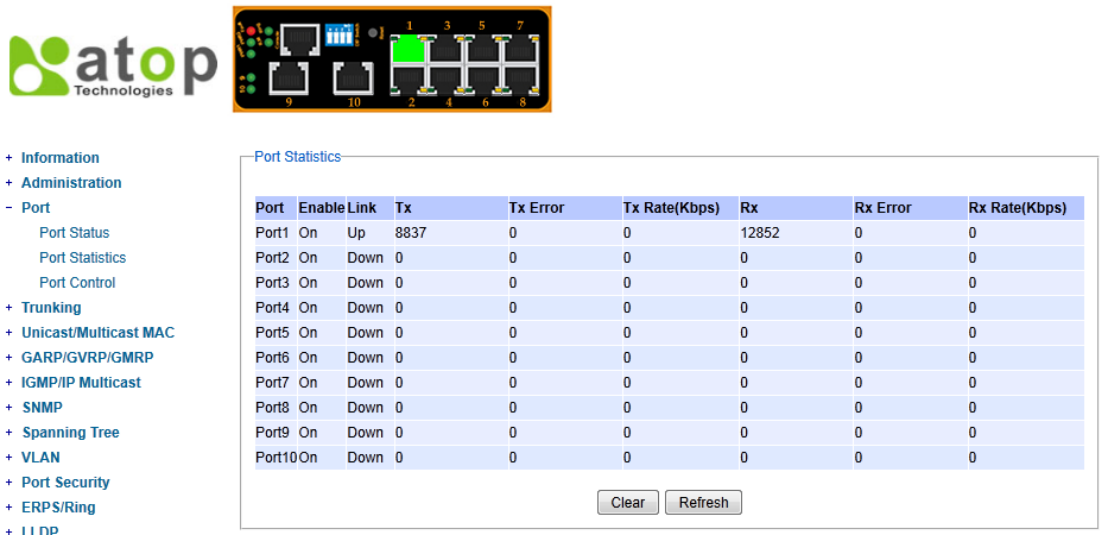


Fig. 2.22

Statistics for all ports showed (Fig. 2.22).

***NOTE**

- Link (Up or down): Actual link status of the port.

- Tx: Total number of unicast and non-unicast packets transmitted**.**

- Tx Error: Number of outbound packets which are chosen to be discarded even though no errors have been detected to prevent them being transmitted.

- Tx Rate (Kbps): Speed of transmission.

- Rx: Total number of packets (not including faulty packets) received.

- Rx Error: Total number of faulty packets (including Oversize, Undersize, FCS, Alignment, Jabbers and Fragments Errors packets) received.

- Rx Rate (Kbps): Receiving speed.

2.4.3 Port Control

Port settings are included to give users control over State (enabled or disabled), Port Transmission Speed, Duplex, Flow Control, Rate Control and Throughput Test.

- + Information
- + Administration
- − Port
  - Port Status
  - Port Statistics
  - Port Control
- + Trunking
- + Unicast/Multicast MAC
- + GARP/GVRP/GMRP
- + IGMP/IP Multicast
- + SNMP
- + Spanning Tree
- + VLAN
- + Port Security
- + ERPS/Ring
- + LLDP
- + System Warning
- + Diagnosis

Port Control

Port	Enable	Negotiation	Speed	Duplex	Flow Control	Rate Control(Kbps)		Throughput Test(Kbps)		
						Ingress	Egress	Ingress	Egress	Action
Port1	☑	Auto	100	Full	Off	0	0	0	0	Test
Port2	☑	Auto	100	Full	Off	0	0	0	0	Test
Port3	☑	Auto	100	Full	Off	0	0	0	0	Test
Port4	☑	Auto	100	Full	Off	0	0	0	0	Test
Port5	☑	Auto	100	Full	Off	0	0	0	0	Test
Port6	☑	Auto	100	Full	Off	0	0	0	0	Test
Port7	☑	Auto	100	Full	Off	0	0	0	0	Test
Port8	☑	Auto	100	Full	Off	0	0	0	0	Test
Port9	☑	Auto	1000	Full	Off	0	0	0	0	Test
Port10	☑	Auto	1000	Full	Off	0	0	0	0	Test

Update

Fig. 2.23

Table 2.12

Label	Description	Factory Default
Port	Port number on the switch.	
Enable	Check the box to allow data to be transmitted and received through this port.	All ports are enabled
Negotiation	Choose from **Force** or **Auto**. See notes below.	All ports Auto- Negotiation is enabled.
Speed	Select either **10**, **100,1000***(Port 9, 10 only)* Mbps	Port1~Port8: 100Mbps. Port9, Port10: 1000Mbps.
Duplex	Select either **Half** or **Full Duplex.** See note below.	All ports are Full-Duplex mode.
Flow Control	Either **on** or **off** "Flow Control" to avoid packet loss when congestion occurs.	All ports flow control is disabled.
Rate Control	Sets limits on its transmission rate for the incoming and outgoing. Unit: kbps	All ports rate control is disabled.
Throughput Test	Click Test button to start test ingress and outgoing rate of this port. Note: The maximum rate test is limited under 98Mbps.	-

***Note:**

- Rate Control: Outgoing and incoming values have to be set between 0 and 102400(for 100M) or 1024000(for 1000M)..

0 is to turn off rate control.

The values have to be integer multiples of 64 when rate is less than 1792Kbps. Ex: 64k, 128k .. 512k…1792Kbps.

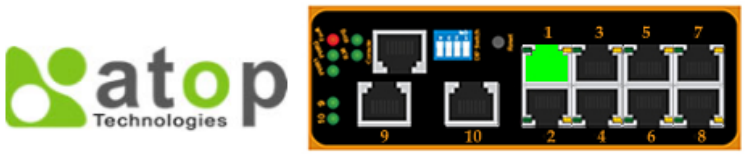
The value has to be an integer multiple of 1024 when rate is between 1792Kbps and 102400Kbps (for 100M) or 106496Kbps (for 1000M).. Ex: 2048K, 3072K… 102400Kbps.
The values have to be integer multiples of 8192 when rate is greater than 106496Kbps.

2.5 Trunking

EH7510 supports Link Trunking; it allows one or more links to be added together to form one single but larger group. The advantage of this function gives the user more flexibility while setting up network connections; the bandwidth of a link can be doubled or tripled. Also, if one link is disconnected, the remaining trunked ports can share the traffic within the trunk group; this function increases the redundancy for higher reliability.

2.5.1 LACP

LACP: IEEE standard, **L**ink **A**ggregation **C**ontrol **P**rotocol.
This option shows the switch's trunking information (Fig. 2.24); users can only specify the system priority here. Other settings including defining a trunk group and specifying LACP functions will be described in the next section.



+ Information
+ Administration
+ Port
− Trunking
  LACP
  Trunking
+ Unicast/Multicast MAC
+ GARP/GVRP/GMRP
+ IGMP/IP Multicast
+ SNMP
+ Spanning Tree
+ VLAN
+ Port Security
+ ERPS/Ring
+ LLDP
+ System Warning
+ Diagnosis
+ System Log

LACP

LACP	Disabled
System Priority	32768 (0~65535)

Port	LACP	Group ID	LACP Partner
Port1	Disable		
Port2	Disable		
Port3	Disable		
Port4	Disable		
Port5	Disable		
Port6	Disable		
Port7	Disable		
Port8	Disable		
Port9	Disable		
Port10	Disable		

Update

Fig. 2.24

Table 2.13

Label	Description	Factory Default
LACP Status	Shows whether LACP is active, passive, or disabled.	Disabled
System Priority	Indicates the system priority, in the range 1 ~ 65535	32768
Group ID	Shows which trunk group this port belongs to.	-
LACP Partner	Indicates whether **LACP Partner** information is received at the corresponding port	-

2.5.2 Trunking

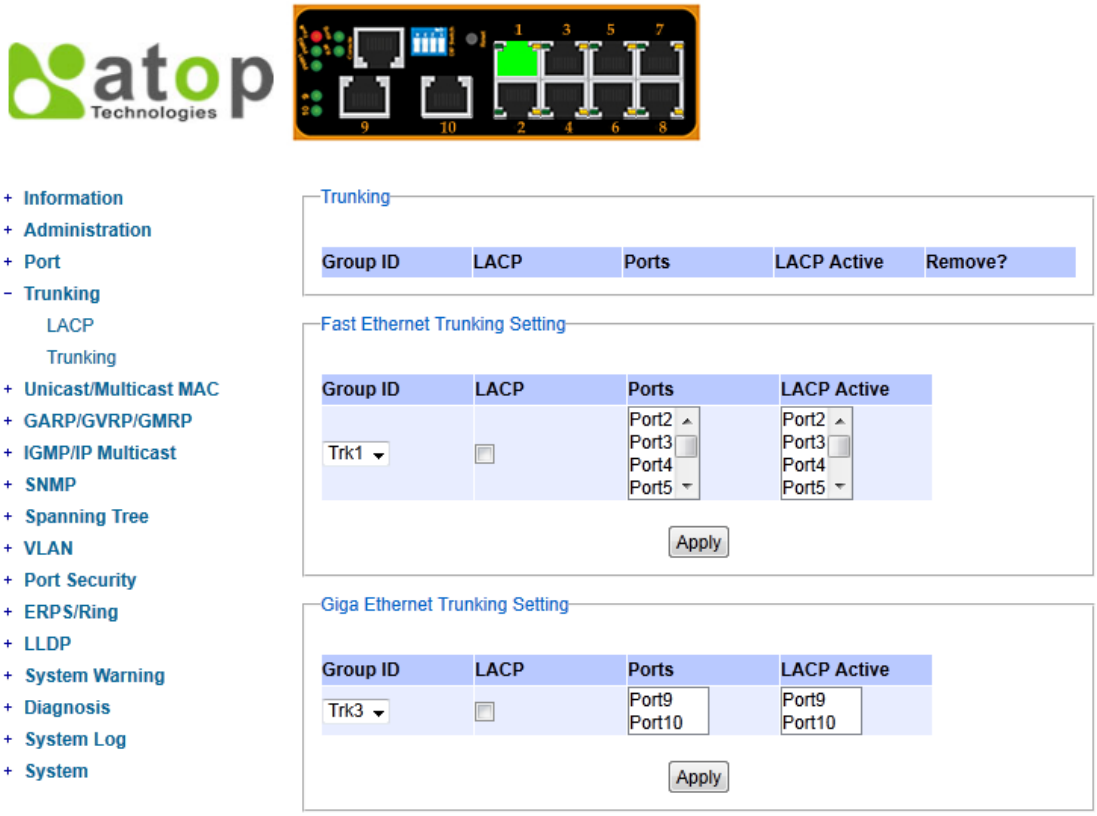


Fig. 2.25

There are four steps to setup a trunking group, Fig. 2.25.

Step 1: Select either Trk1 or Trk2 from Group ID.

Step 2: Choose whether to enable LACP (IEEE standard, Link Aggregation Control Protocol).

Step 3: Select specific ports to be in this trunk group.

Step 4: Select specific ports in this trunk group to be LACP active.

Table 2.14

Label	Description
Group ID	EH7510 can have up to 2 trunk group. Trk1 and Trk2.
LACP (Yes/No)	Enable/Disable LACP.
Ports	Specifies the member ports. Hold **Contro**l to select more than one port at a time.
LACP Active	Specifies which ports within the group are LACP active. Non-selected ports would be LACP passive.
Apply	Click **Apply** to confirm changes.
Remove	Removes any existing trunk group.

2.6 Unicast/Multicast MAC

This function includes three sub-pages

- **MAC Address Table**
- **Add Uni/Multicast MAC**
- **Filter MAC**.

Multicast filtering improves the performance of networks that carry multicast traffic; this section will explain what Multicast and Unicast are as well as their benefits, (Fig. 2.26).

- **Unicast:** This type of transmission sends messages to a single network destination identified by a unique address. This method is simple but not widely used.
- **Multicast:** This type of transmission is more complicated. It sends messages from one host to multiple hosts; only those hosts that belong to a specific multicast group will receive the multicast. Also, networks that support multicast send only one copy of the information across the network until the delivery path that reaches group members diverges. At these diverging points, multicast packets will be copied and forwarded. This method can manage high volume traffic with different destinations while using network bandwidth efficiently.

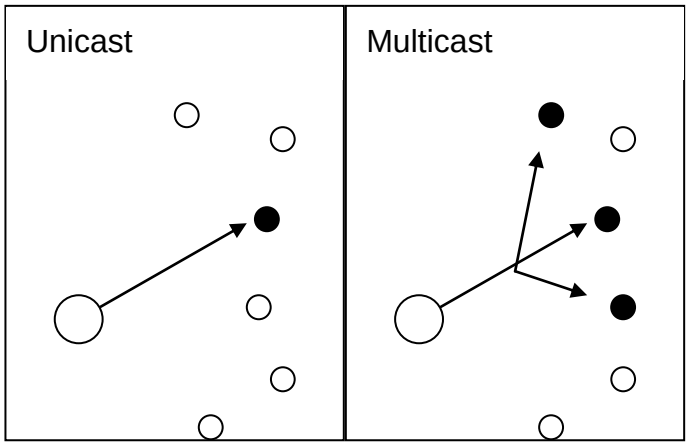


Fig. 2.26

2.6.1 MAC Address Table

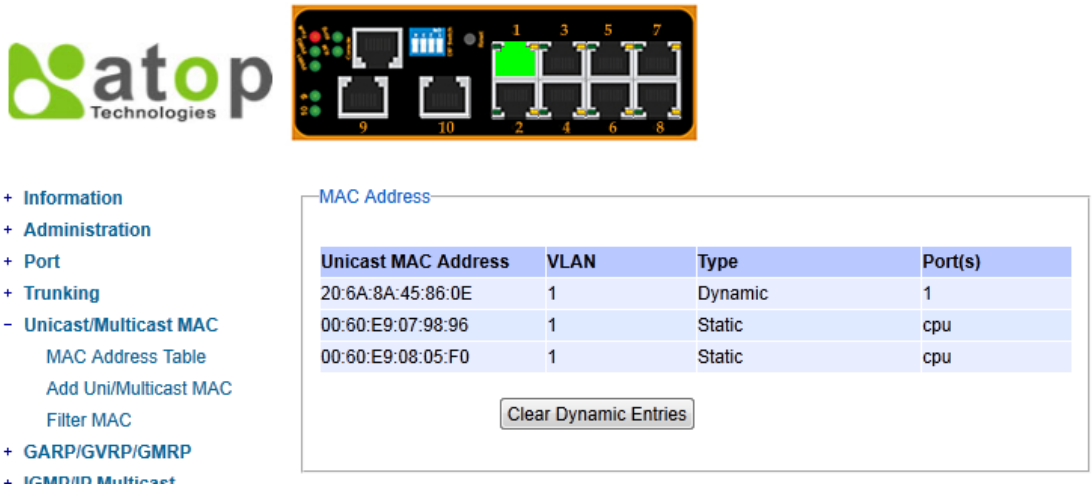


Fig. 2.27

Information of current Unicast and Multicast MAC addresses is displayed as on Fig. 2.27. Unicast would be shown first followed by Multicast MAC address.

Table 2.15

Label	Description
Unicast/Multicast MAC	Displays MAC address.
VLAN	Displays VLAN ID.
Type	Displays whether the MAC address is dynamic or static.
Ports	Displays which port this MAC belongs to.
Clear Dynamic Entries	**Clears** all Dynamic MAC addresses.

2.6.2 Add Uni/Multicast MAC

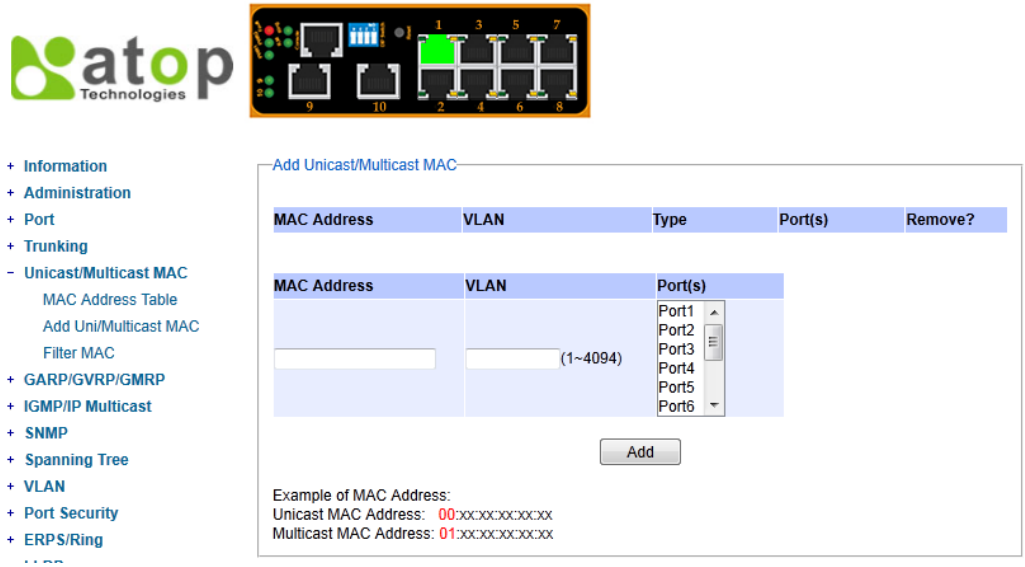


Fig. 2.28

EH7510 also supports adding static MAC address manually (Fig. 2.28); the steps are as follows,

Step 1: Enter MAC Address. Unicast address starts with 00 and Multicast address starts with 01.

Step 2: Specify VLAN ID.

Step 3: Decide which ports belong to its corresponding address; use **Ctrl** to add more than one port.

Table 2.16

Label	Description
MAC address	Enter MAC address manually.
VLAN	Specify VLAN ID that this static MAC belong to
Type	-
Port(s)	Define which ports belong to this address
Add	Confirm and add the MAC address.
Remove	Remove any existing MAC address.

2.6.3 Filter MAC

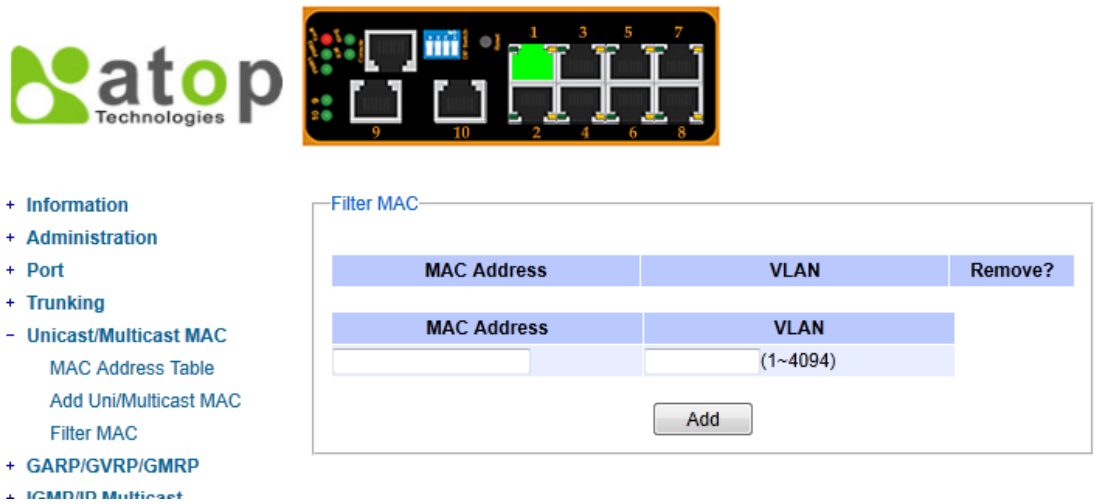


Fig. 2.29.a

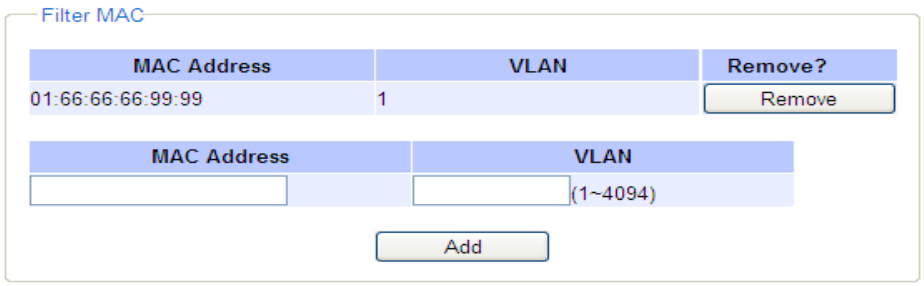


Fig. 2.29.b ∗Example∗

This function allows users to set MAC filter manually, see Fig. 2.29.a, and Fig. 2.29.b for an example.

Table 2.17

Label	Description
MAC address	MAC address entered in this field will be blocked.
VLAN	Assign VLAN ID to this static MAC address
Remove	**Remove** this entry in filter table.
Add	**Add** the MAC addresses to the filter table

2.7 GARP/GVRP/GMRP

This function includes three options, **GARP, GVRP** and **GMRP.**

GARP: Generic **A**ttribute **R**egistration **P**rotocol, also known as Multiple Registration Protocol (MRP). It operates at the data link layer of OSI, and it defines the architecture, rules of operation, state machines and variables for the registration and removing of attribute values. GARP is used by two applications: **GARP VLAN Registration Protocol** (**GVRP**), and **GARP Multicast Registration Protocol** (**GMRP**). GVRP provides a method to share VLAN information dynamically and configure the needed VLANs. GMRP provides a mechanism that allows bridges and switches to register trunking information dynamically. GVRP and GMRP are similar, and the only difference is that GVRP works with VLAN but GMPR works with Multicast MAC address.

2.7.1 Multicast Group Table

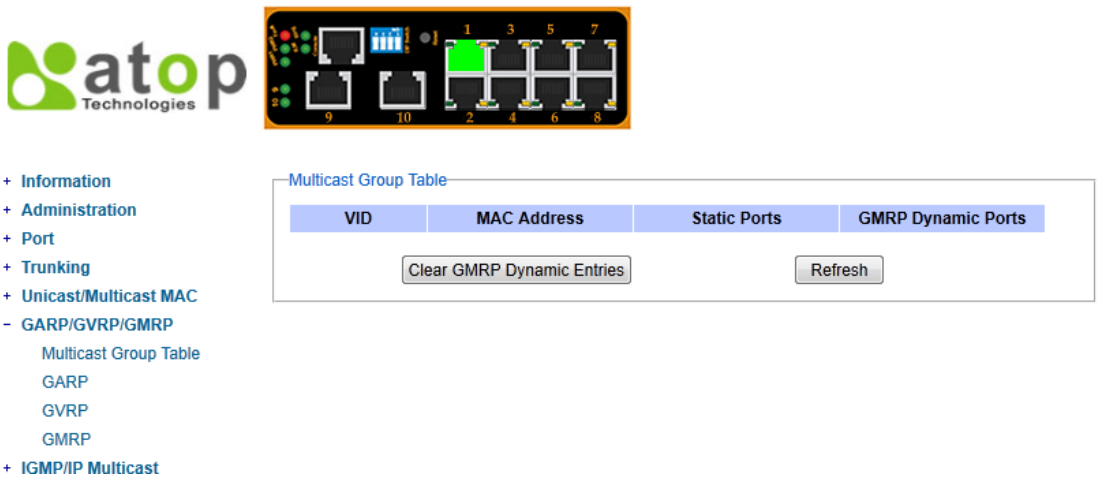


Fig. 2.30

Table 2.18

Label	Description
VID	VLAN identifier.
MAC address	Multicast group's MAC address..
Static Ports	Statically joined ports through in Static MAC Table and to which the multicast group traffic is forwarded.
GMRP Dynamic Ports	Dynamically joined ports through GMRP Application presently on the group and to which the multicast group traffic is forwarded.

2.7.2 GARP

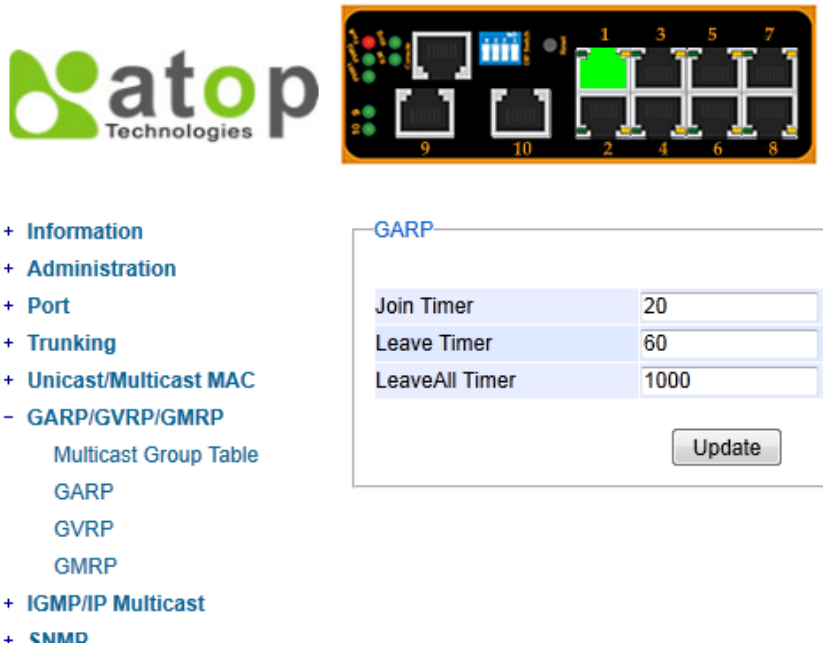


Fig. 2.31

Fig. 2.31 shows how to configure GARP timer:

Table 2.19

Label	Description	Factory Default
Join Timer	Indicate the GARP **Join timer,** in 0 ~ 65535 seconds**.**	20 seconds
Leave Timer	Indicate the GARP **Leave timer,** in 0 ~ 65535 seconds.	60 seconds
LeaveAll Timer	Indicate the GARP **Leave All timer**, in 0 ~ 65535 seconds.	1000 seconds

2.7.3 GVRP

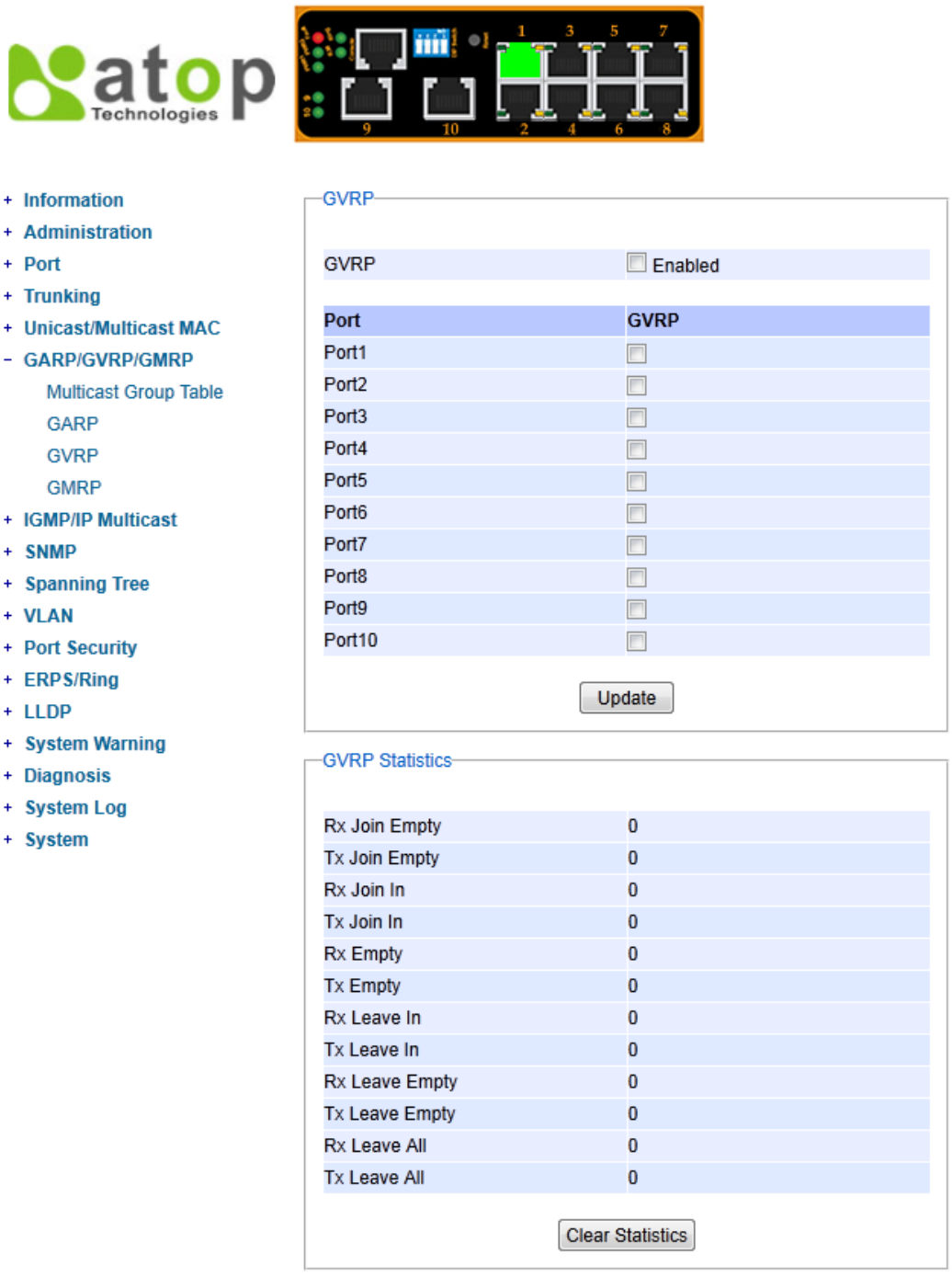


Fig. 2.32

Fig. 2.32 indicates GVRP configurations and functions. When GVRP is enabled, the switch which is an end node of a network needs only to add static VLANs locally. Others switches dynamically learn the rest of the VLANs configured elsewhere in the network via GVRP.

Table 2.20

Label	Description	Factory Default
GVRP	Enables or disables GVRP protocol. Enables GVRP, the switch must be in 802.1q VLAN mode.	Disabled
Port	Enables or disables GVRP on each port. If users have already define trunking group (e.g. Trk1), it can also be selected to be enabled.	All ports are disabled
Clear Statistics	Clears all GVRP statistics counts	Clears the record

2.7.4 GMRP

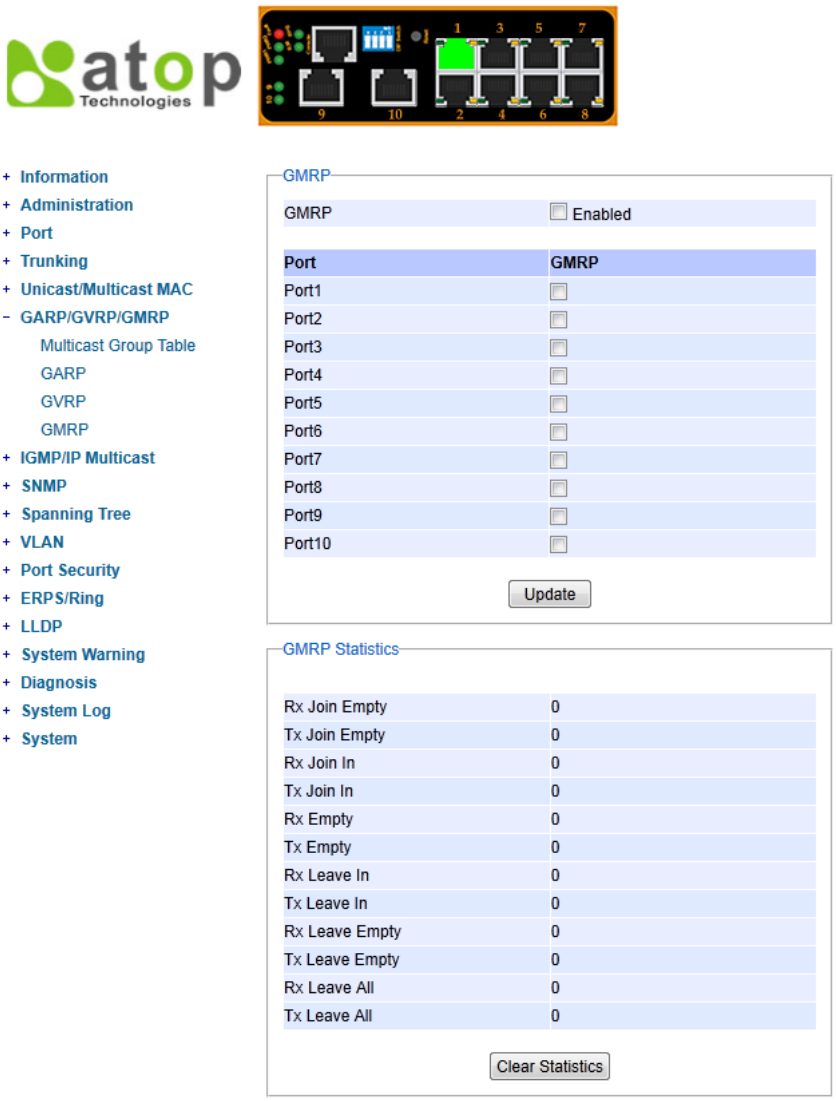


Fig. 2.33

The above figure shows GMRP functions and configurations; when GMRP is enabled, the switch allows to receive the “join” multicast group message from an end station. It then creates dynamic multicast MAC address entry in MAC table and spreads this message to other switches.

Table 2.21

Label	Description	Factory Default
GMRP	Enables or disables GMRP protocol. To enable GMRP, the switch must be in 802.1q VLAN mode and IGMP snooping must be disabled.	Disabled
Port	Choose the ports to be GMRP enabled.	Disabled
Clear Statistics	Clear all GMRP statistics counts	-

2.8 IGMP/IP Multicast

This function contains four options (Fig. 2.34.a), which are:

- **IGMP/IP Multicast Table**
- **Static IP Multicast**
- **IGMP**
- **IGMP Statistics**.

IGMP: Internet **G**roup **M**anagement **P**rotocol is used on IP networks to establish multicast group memberships. It operates above the network layer of OSI. One of the most important features related to this protocol is IGMP snooping, which is supported by EH7510 and greatly strengthens network functionality.

IGMP Snooping: It is the process of "listening" to IGMP network traffic. By listening to conversations between different devices, it maintains a map of which links need which IP multicast streams. This means multicasts may be filtered from the links which do not need them, and IGMP snooping allows a switch to only forward multicast traffic to the links that have requested it.

2.8.1 IGMP/IP Multicast Table

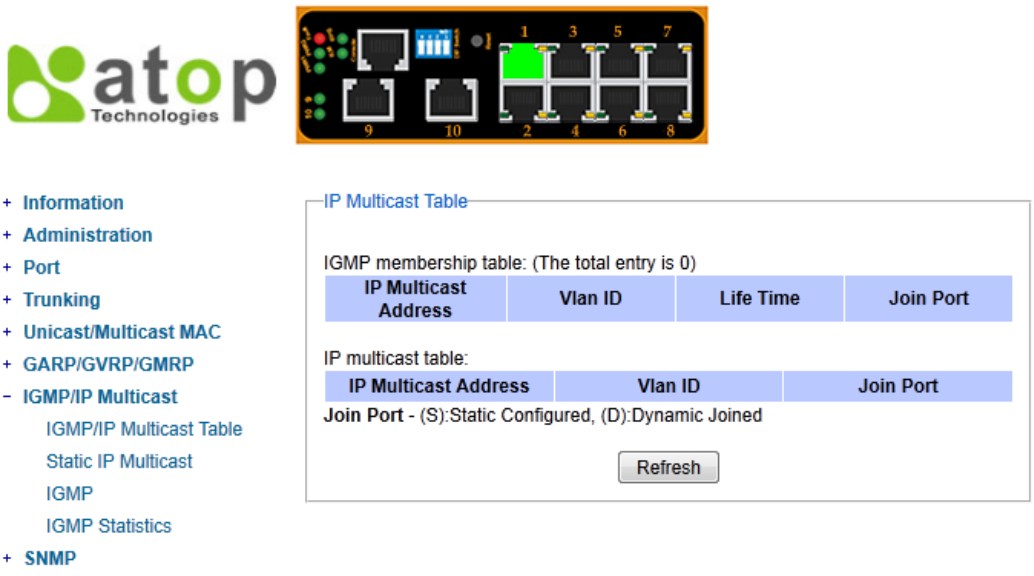


Fig. 2.34.a

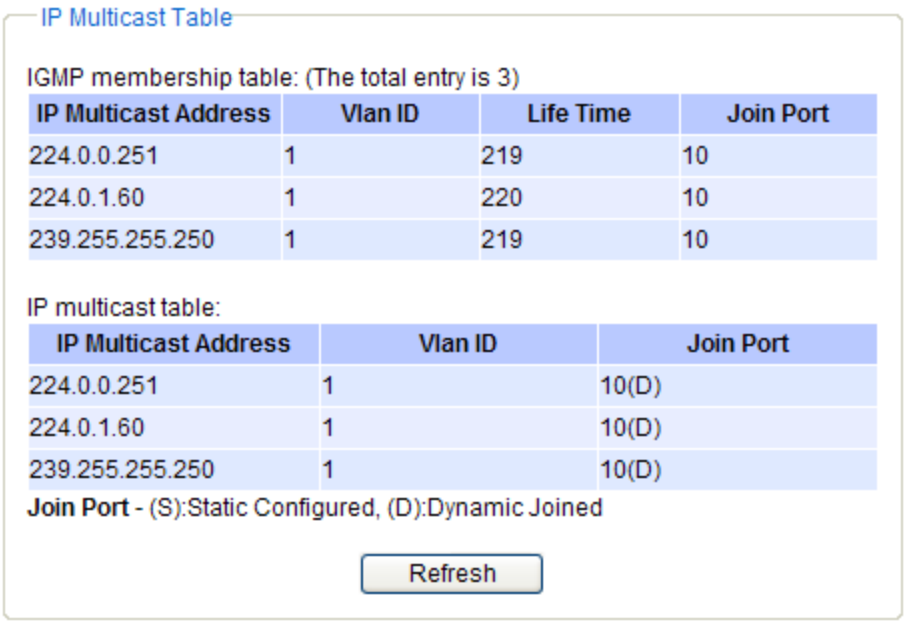


Fig. 2.34.b ∗Example∗

This option shows:

1. The IGMP membership group table.

2. Static and dynamic IP Multicast table. The dynamic join port is added by the switch's IGMP snooping function. The static join port is manually added by the user.

2.8.2 Static IP Multicast

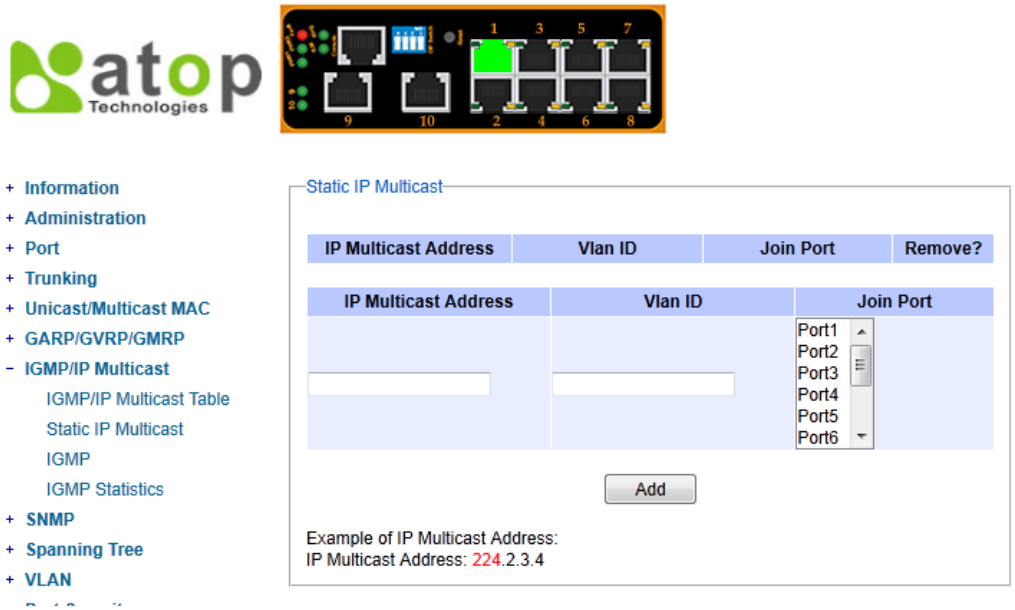


Fig. 2.35.a

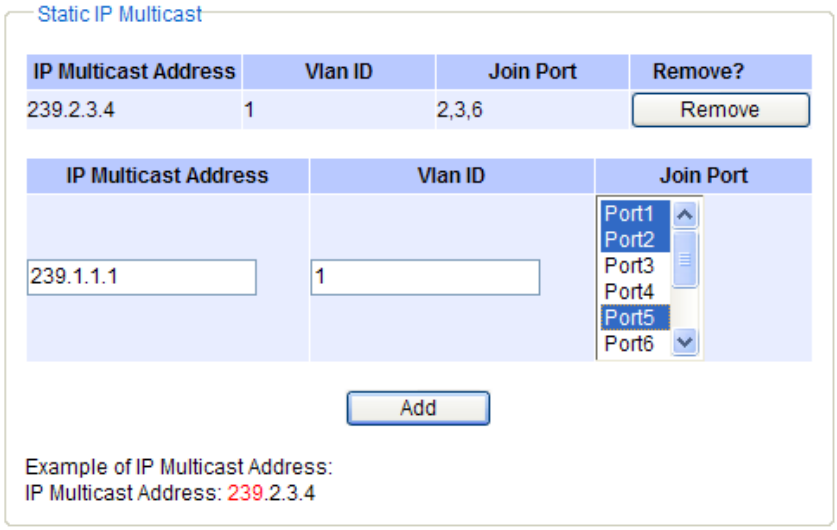


Fig. 2.35.b ＊Example＊

Fig. 2.35.a, 2.35.b display current IP multicast addresses, and it allows users to add more manually.

For example, an IP multicast group address is: 239.1.1.1; joining ports are Port1, Port2 and Port5 with VLAN=1.

Users should key the IP in the **IP Multicast Address** column and click the corresponding port's number in the source column. Click the **"Ctrl"** key on the keyboard to add more ports. Then click on the Add button, the IP address is then added as it can be seen on Fig 2.35.b, above; to remove the static IP multicast address entry setting, click the Remove button. These procedures are similar as when we added Uni/Multicast MAC address previously, the only difference being that the IP multicast address has the form 239.XX.XX.XX.

2.8.3 IGMP

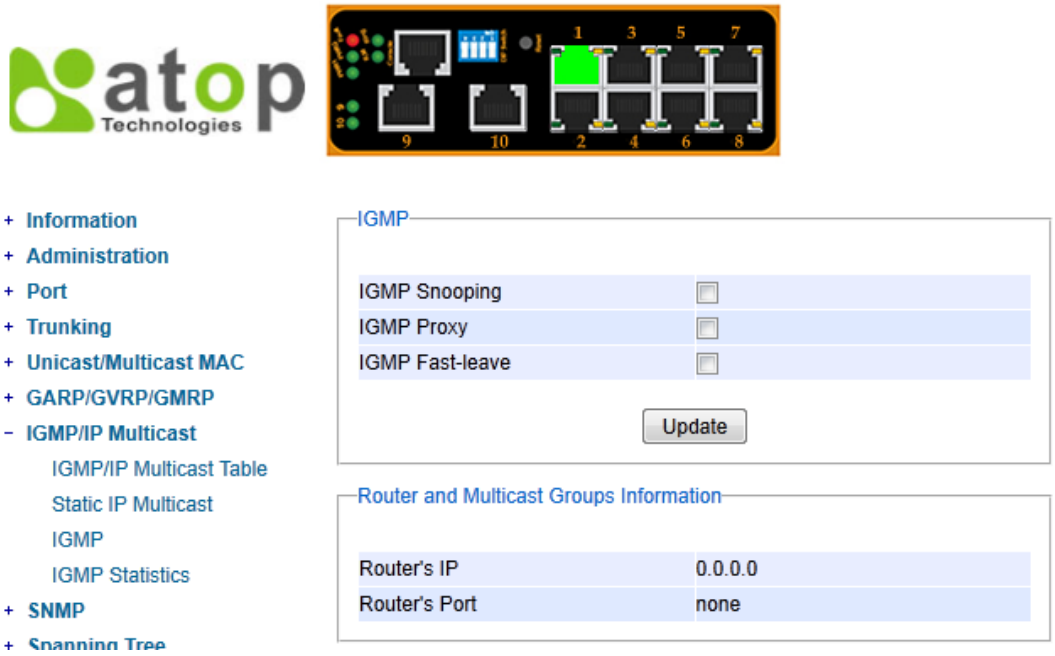


Fig. 2.36

Table 2.22

Label	Description	Factory Default
IGMP Snooping	Choose to enable IGMP snooping. To enable IGMP snooping, GMRP must be disabled	Disabled
IGMP Proxy	Choose to enable IGMP snooping. See note below.	Disabled
IGMP Fast-leave	Choose to enable IGMP Fast-leave. See note below.	Disabled
Router's IP	Display the multicast router's IP address.	-
Router's Port	Display the port that is connected to multicast router.	-

***NOTE:**

IGMP Proxy: works as an intermediate server; when it receives a query message from the router; it sends a report message to the router port. When it receives a report message from a device in a new group, it sends a report message back to the router port. When it receives a leave message from a device which is the only one in the group, it sends a leave message to the router port and removes the device. Proxy is like a middle man that handles information in between routers and computers.

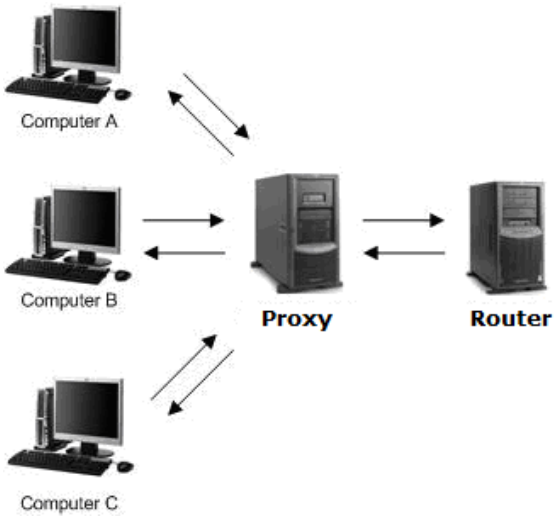


Fig. 2.37

IGMP Fast-leave: When a leave message is received, the ports in the group will be immediately removed from the IP multicast entry.

2.8.4 IGMP Statistics

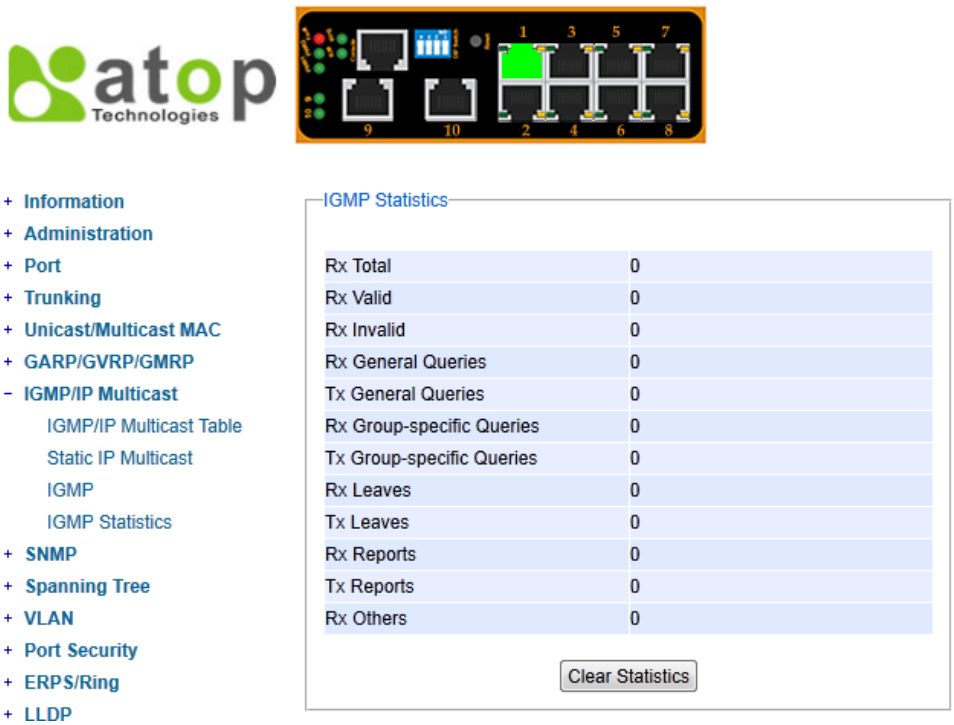


Fig. 2.38.a

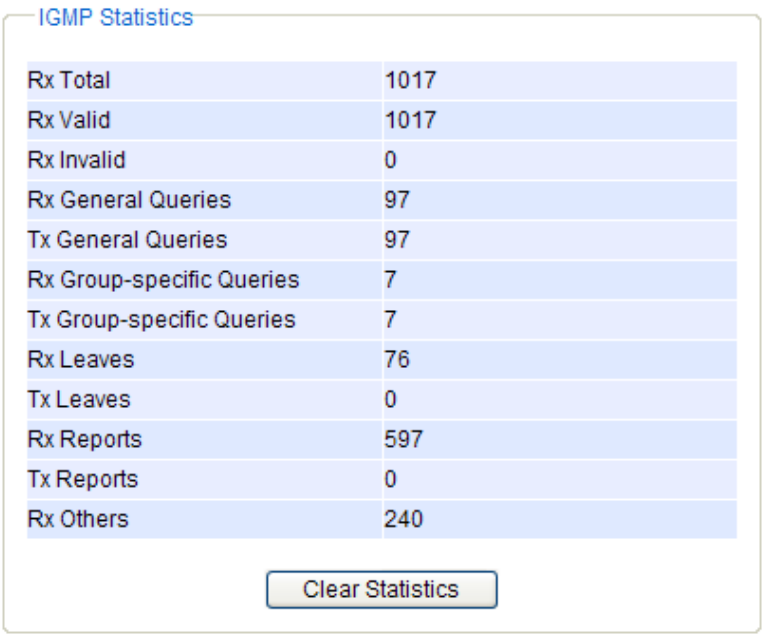


Fig. 2.38.b ∗Example∗

IGMP's statistics are shown in Fig. 2.38.a, and its example on Fig. 2.38.b.

2.9 SNMP

This section has four categories, which are

- **SNMP**
- **Community Strings**
- **Trap Receivers**
- **SNMP V3 Users**.

SNMP: Simple **N**etwork **M**anagement **P**rotocol is a protocol for managing devices on IP networks. It exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried/ defined by users.

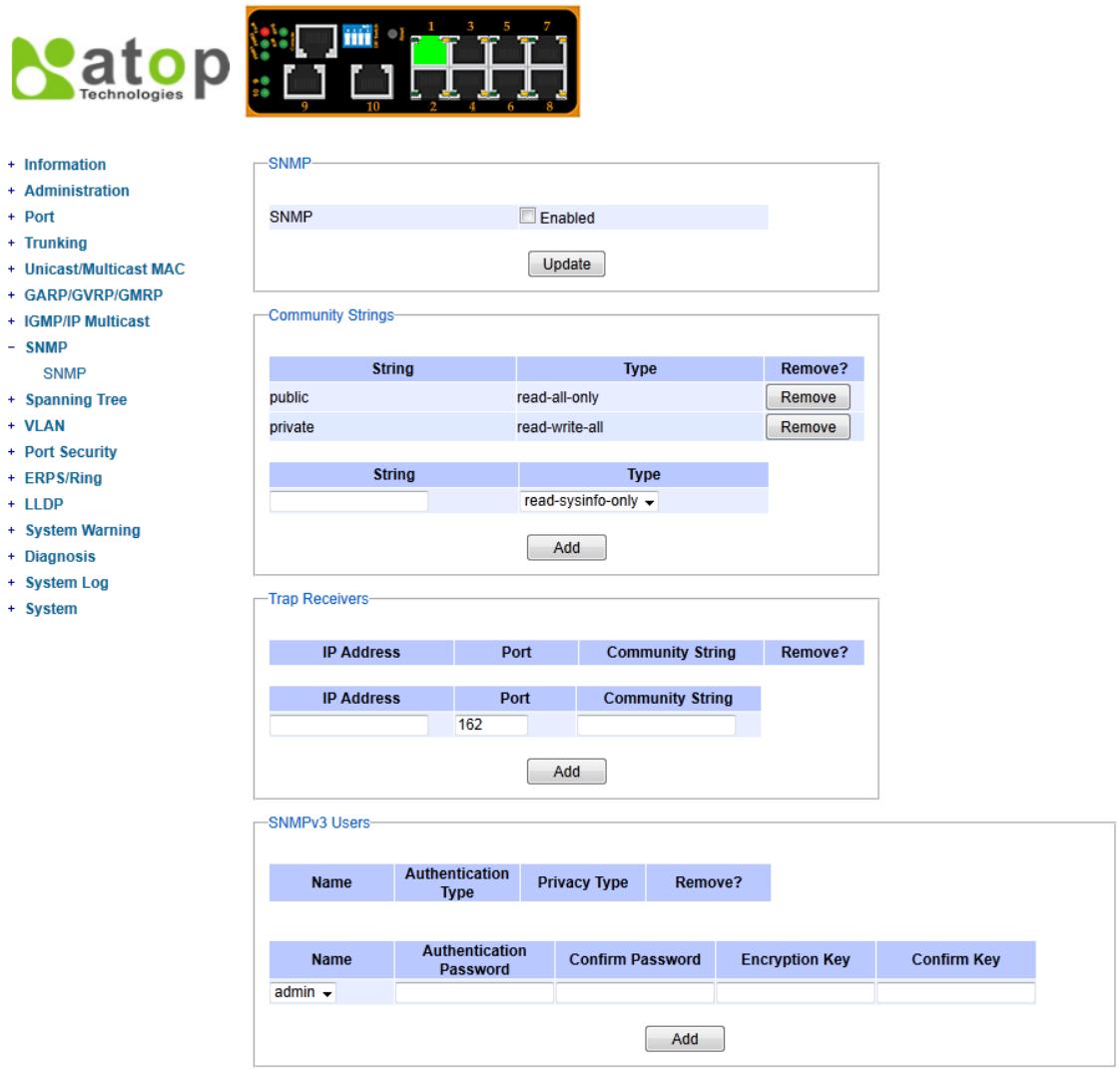


Fig. 2.39.a

Table 2.23

Label	Description	Factory Default
SNMP	Choose to enable SNMP V1/V2c/V3.	Disabled

2.9.1 Community Strings

EH7510 supports SNMP V1, V2c, and V3; V1 and V2c use a community string match for authentication; there are three levels of authentications which are read-sysinfo-only, read-all-only, or read-write-all. For example, in our default setting, the SNMP agent can access all objects with read-all-only permissions using the string *public*. Another example is that the string *private* has permission of read-write-all.

This option allows users to use a community string match for authentication; users can specify the string names and the type of permissions on the **String** field, Fig. 2.39.a.

Table 2.24

Label	Description	Factory Default
Community Strings	Define name of strings. Max. 15 Characters.	**Public**(read-all-ony) **Private**(read-write-all)
Type	Choose from read-sysinfo-only, read-all-only, and read-write-all. See notes below for a detailed explanation.	-

***NOTE:**

Read-sysinfo-only: permission to read OID 1.3.6.1.2.1.1 Sub Tree.

Read-all-only: permission to read OID 1 Sub Tree.

Read-write-all: permission to read/write OID 1 Sub Tree.

2.9.2 Trap Receivers

EH7510 provides a trap function that allows an SNMP agent to notify the network management system in case of a significant event, this allows users to configure SNMP Trap setting, Fig. 2.39.b.

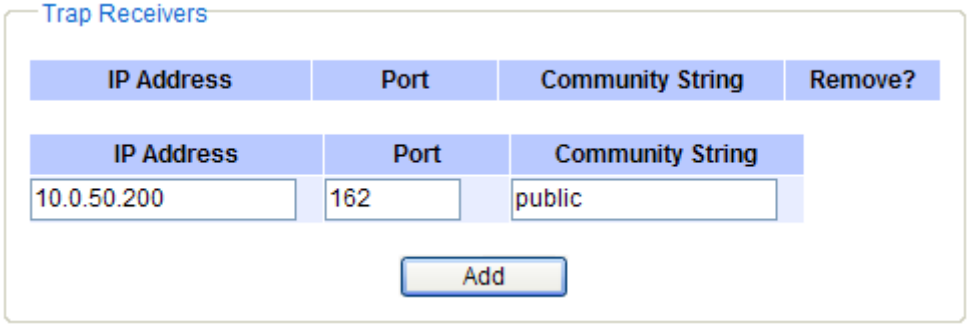


Fig. 2.39.b ∗Trap Receiver Example∗

Table 2.25

Label	Description	Factory Default
IP address	IP address of your Trap Server	NULL
Port	Trap Server service port.	162
Community String	Community string for authentication. Max. 15 characters.	NULL

2.9.3 SNMPv3 Users

SNMP V3 is an even securer protocol; users will be able to set a password and an encryption key to enhance data security.

When choosing this option users can configure SNMP V3. EH7510 use MD5 (Message-Digest algorithm 5) for authentication password, and DES (Data Encryption Standard) for data encryption, Fig. 2.39.a.

Table 2.26

Label	Description	Factory Default
Name	**Admin**: Administration level. **User**: Normal user level.	Admin
Authentication Password	Set password. If the field is left blank, there will be no authentication. Authentication password is based on MD5. Max. 31 characters.	NULL
Confirm Password	Re-type the Authentication Password	NULL
Encryption Key	Set encryption key for securer protection. Encryption is based on DES. Max. 31 characters.	NULL
Confirm Key	Re-type the Encryption Key	NULL

2.10 Spanning Tree

EH7510 provides the IEEE Standard Spanning tree functionality. The **S**panning **T**ree **P**rotocol (**STP**) provides function to prevent switching loops and ensuring broadcast radiation. A switching loop occurs in network when there are multiple connections between two network switches or two ports. The loop creates broadcast radiation, the accumulation of broadcast and multicast traffic on a computer network. As broadcasts and multicasts are forwarded by bridges/switches to every port, the bridges/switches will repeatedly rebroadcast the broadcast messages, and this can floods the network. STP creates a spanning tree and disables those links of the network that are part of the spanning tree, which leaves only a single active path between two nodes. This function avoids flooding and increases network efficiency.

EH7510 also supports **RSTP** (**R**apid **S**panning **T**ree **P**rotocol). It is an evolution of the STP. It has a slightly changed topology, which helps to provide a much faster spanning tree convergence.

2.10.1 Spanning Tree

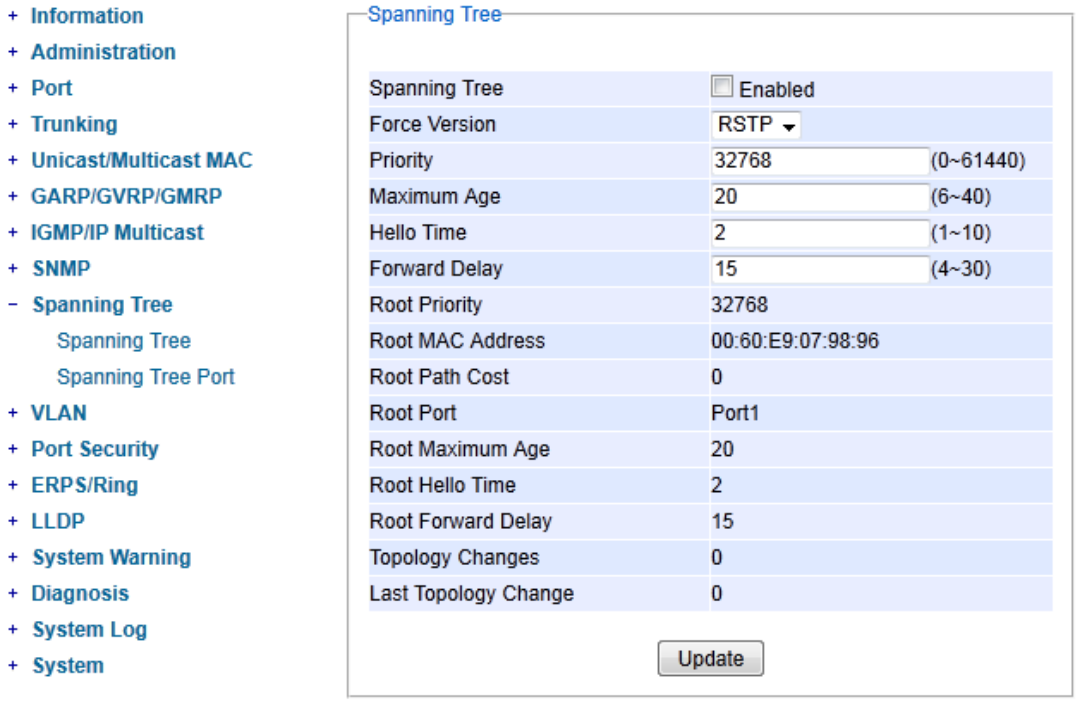


Fig. 2.40

Fig. 2.40 shows how to configure the Spanning Tree and indicates the parameters' status.

Table 2.27

Label	Description	Factory Default
Spanning Tree	Choose to enable or disable Spanning Tree.	Disabled
Force Version	Select **STP** or **RSTP.**	RSTP
Priority	Configures the bridge priority in the range of 0 ~ 61440.The switch with lower bridge priority has more chance to become a root bridge.	32768
Maximum Age	If a device is not the root and it doesn't receive hello message in "Max. Age", it will reconfigure itself as a root. See note below for "hello message". Range from 6 to 40 seconds.	20
Hello Time	Amount of time the root waits between sending hello messages. See note below. Range from 1 to 10 seconds.	2
Forward Delay	Configures the amount of time to wait before checking to see if the device should change from the learning state to the forwarding state. Less delay time means changing state quickly. Range from 4 to 30 seconds.	15
Root Priority	Indicates the current root priority value.	Dependant
Root MAC Address	Indicates the current root MAC address.	Dependant
Root Path Cost	Indication of cost. Higher cost means less suitability for Spanning Tree topology.	Dependant
Root Port	Indicates the port that receives the best BPDU. See note below.	Dependant
Root Maximum Age	Indicates the current root maximum ageing time value.	Dependant
Root Hello Time	Indicates the current hello time value.	Dependant
Root Forward Delay	Indicates the current root forward delay time value.	Dependant
Topology Changes	Indicates the time which topology change is occurred.	Dependant
Last Topology changes	Indicates the working time since last Topology changes occurred.	Dependant

***NOTE**

- **"Hello" Message:** The root of the Spanning Tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy.
- **BPDU:** In STP, to ensure that each bridge has enough information, the bridges use special data frames called **B**ridge **P**rotocol **D**ata **U**nits (BPDU) to exchange information about bridge IDs and root path costs.

2.10.2 Spanning Tree Port

Fig. 2.41 shows how to configure per-port Spanning Tree parameters and indicate each port's status.

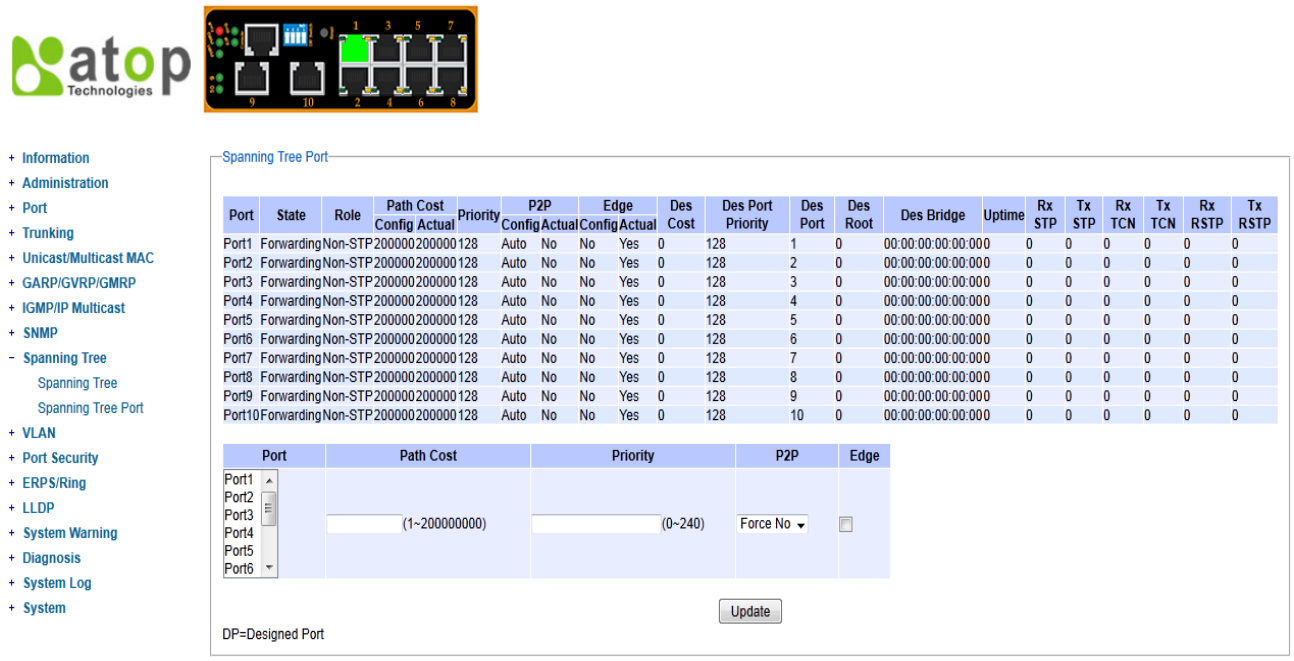
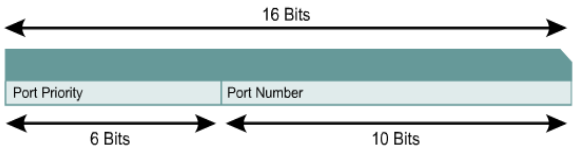


Fig. 2.41

***NOTE:**

- Recall that Tx Packets are those transmitted/sent out from EH7510, and Rx Packets are packets received from connected devices, then
- **Des Cost:** (Designated Root) cost for a packet to travel from a port to the root in the current Spanning Tree.
- **Des Port:** (Designated Port) port designated to send the best BPDU.
- **Des Root:** (Designated Root) device's priority from which the port must communicate to reach the Spanning tree's root.
- **Uptime:** Indicates how long it has been up.
- **Tx/Rx SPT:** sending/receiving STP packet total count.
- **Tx/Rx TCN:** Topology change Notification
- **Tx/Rx RSTP:** sending/receiving RSTP packet total count.

Table 2.28

Label	Description	Factory Default
Port	Selects the ports to be configured.	
Path Cost	Configures the port path cost in the range 1~200000000. This value will affect the combination path cost. The lowest combination path cost will be the best path to the Root Bridge	200000
Priority	Configures the port priority in the range 0~240. The port has the best route to the root bridge with the lowest priority value. This field is consist of : 	128
P2P	Selects P2P Point to point connection type: **Force No:** Force port P2P link to false. **Force Yes:** Force port P2P link to true. **Auto:** Select port P2P link to auto detection.	Force No
Edge	Choose whether it is an edge connection.	Uncheck

2.11 VLAN

A **V**irtual **L**ane **A**rea **N**etwork (**VLAN**) is a group of devices that can be located anywhere on a network, but all devices in the group have connection with others as they're physically connected together. In other words, VLAN allows end stations to be grouped together even if they're not located on the same network switch. With traditional network, users usually spend a lot of time on devices relocations, but a VLAN reconfiguration can be performed entirely through software. Also, VLAN provides extra security because devices within a VLAN group can only communicate with other devices in the same group; for the same reason, VLAN can help to control network traffic. Traditional network broadcasts data to all devices, no matter whether they need it or not. By allowing a member to receive data only from other members in the same VLAN group, VLAN avoids broadcasting and increase traffic efficiency (next page, Fig. 2.42).

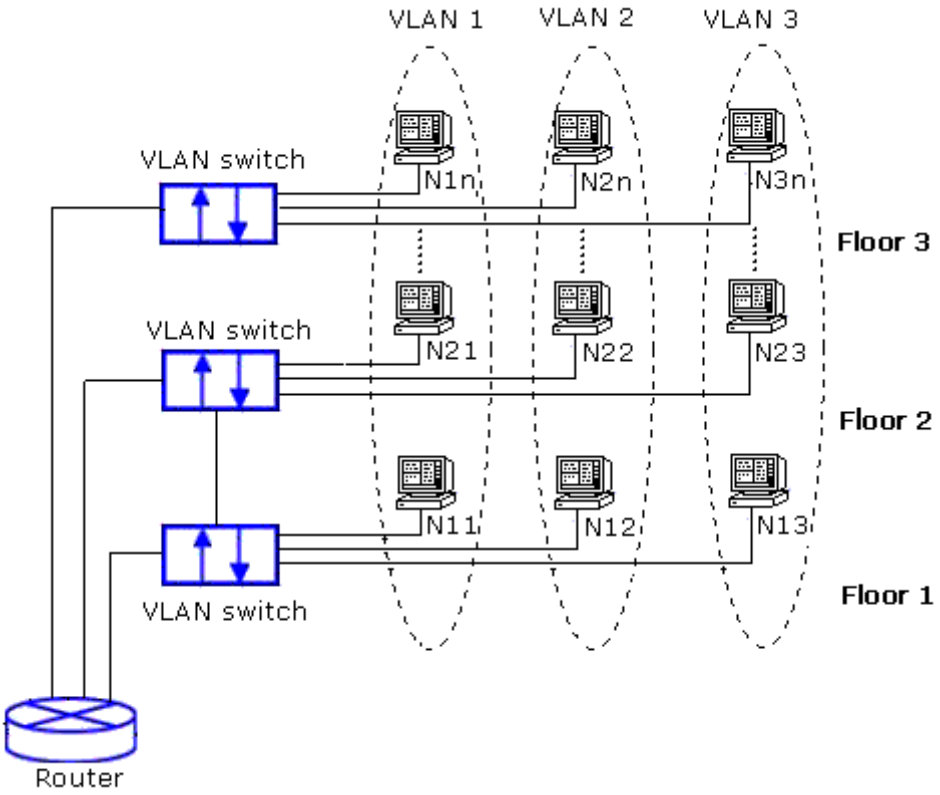


Fig. 2.42

There are two common approaches to assigning VLAN memberships,

- Port-based VLAN
- Tagging-based (802.1q) VLAN

EH7510 supports both of them.

2.11.1 VLAN Mode

Port-Based VLAN (or Static VLAN equivalently) assignments are created by assigning ports to a VLAN. If a device is connected to a certain port, the device will assign a VLAN to that specific port; if users change the port connected, they must manually make a new port-VLAN assignment for this new connection.

Steps to set up Port-Based VLAN:

1. On *VLAN Mode* page, select Port-Based -> Update -> Reset.
2. Select specific ports to be included to certain group.

Fig. 2.43.a ∗Default screen∗

Table 2.29

Label	Description	Factory Default
VLAN Mode	Choose either **Port-Based** or **802.1Q**. The switch will reboot after changing to VLAN mode.	802.1Q

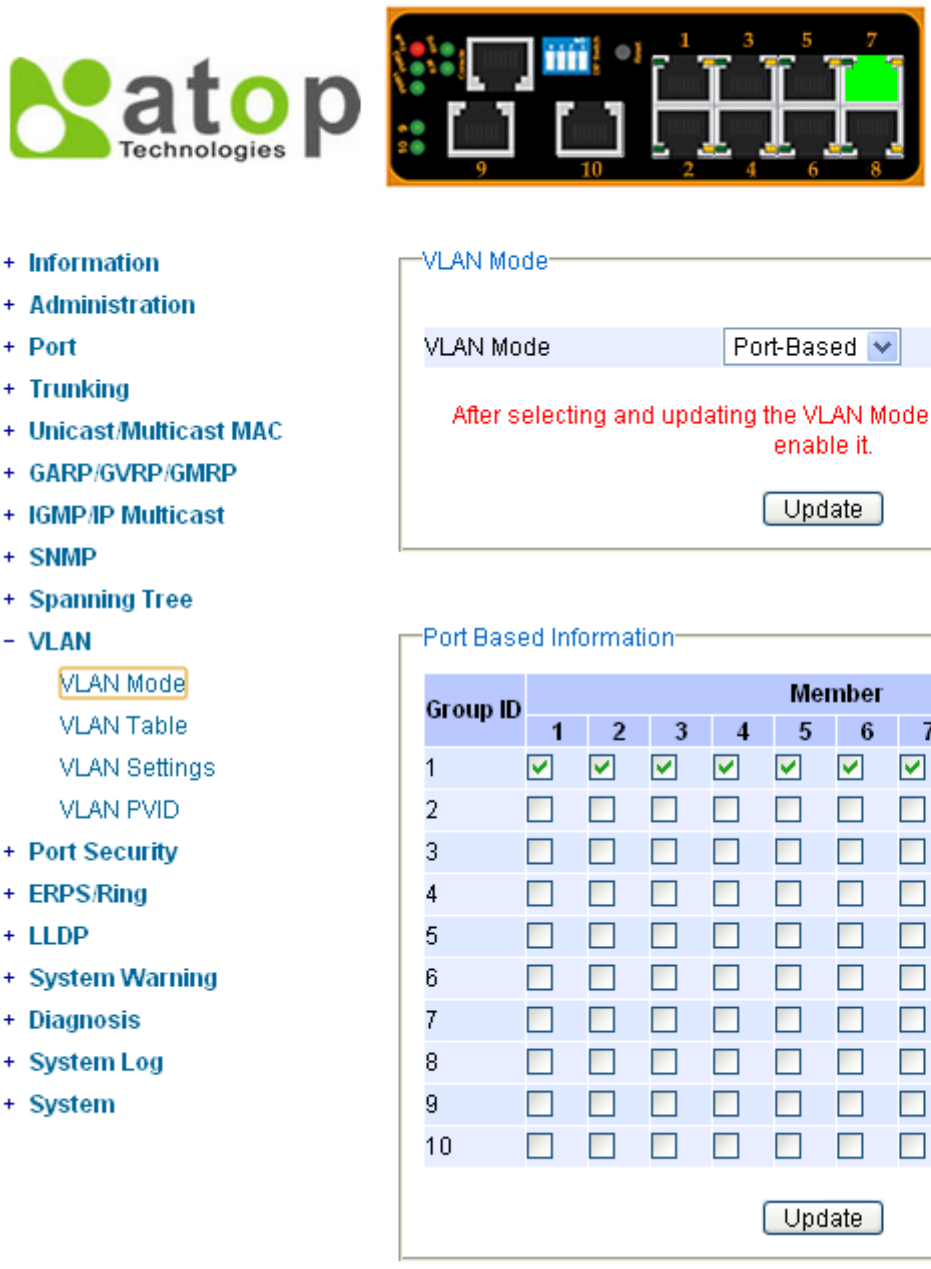


Fig. 2.43.b ∗Screen when on Port Based mode∗

Table 2.30

Label	Description	Factory Default
Group ID	Indicates the VLAN Group ID.	Group ID 1
Member	Adds specific ports to specific group.	Port 1 ~ Port10.

***NOTE:**

- *VLAN Table*, *VLAN Settings*, and *VLAN PVID* (following subsections) are not available for **Port-Based VLAN** but only available for **802.1Q.**

802.1Q (or tagging-based equivalently)

Another VLAN mode that EH7510 supports is **802.1Q**. Tagged frames are frames with 802.1Q (VLAN) tags that specify a valid VLAN identifier (VID). Untagged frames are frames without tags or frames that carry 802.1p (prioritization) tags and only having prioritization information and a VID of 0. When a switch receives a tagged frame, it extracts the VID and forwards the frame to other ports in the same VLAN, Fig. 2.43.a, and Fig. 2.43.b.

Table 2.31

Label	Description	Factory Default
VLAN Mode	Choose **802.1Q**. The switch will reboot after changing VLAN mode.	802.1Q
Management VLAN ID	Configure the management VLAN ID that can be accessed this switch. Range from 1 to 4095.	1

2.11.2 VLAN TABLE

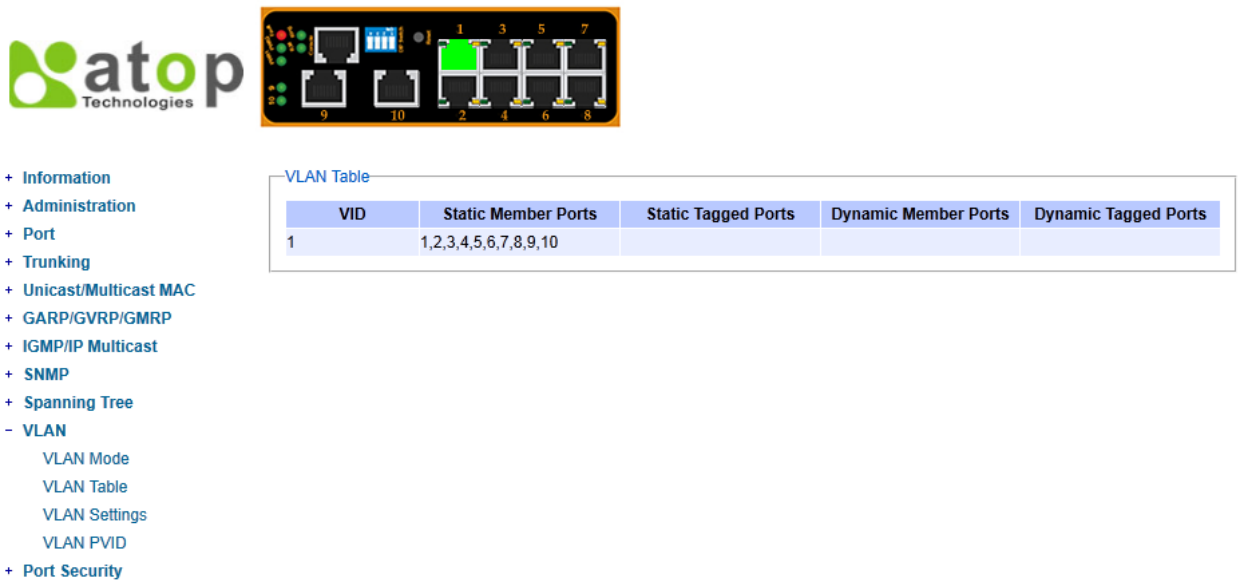


Fig. 2.44.a

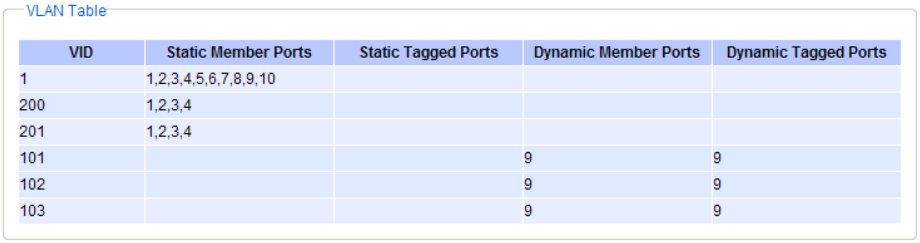


Fig. 2.44.b ＊Example＊

Fig. 2.44.a, 2.44.b (example), displays the static and dynamic VLAN information of each VID.

Table 2.32

Label	Description	Factory Default
VID	Indicates the VLAN ID number.	Dependant
Static Member Ports	Indicates the member ports to this VID. This entry is created by user.	All ports
Static Tagged Ports	Indicates the ports that outgoing packet is tagged or untagged. **Displayed**: The outgoing packet is tagged from this port. **Undisplayed**: The outgoing packet is untagged from this port. This entry is created by user.	Dependant
Dynamic Member Ports	Indicates the member ports to this VID. This entry is created by GVRP.	Dependant
Dynamic Tagged Ports	Indicates the member ports that outgoing packet is tagged or untagged. **Displayed**: The outgoing packet is tagged from this port. **Undisplayed**: The outgoing packet is untagged from this port. This entry is created by GVRP.	Dependant

2.11.3 VLAN Setting

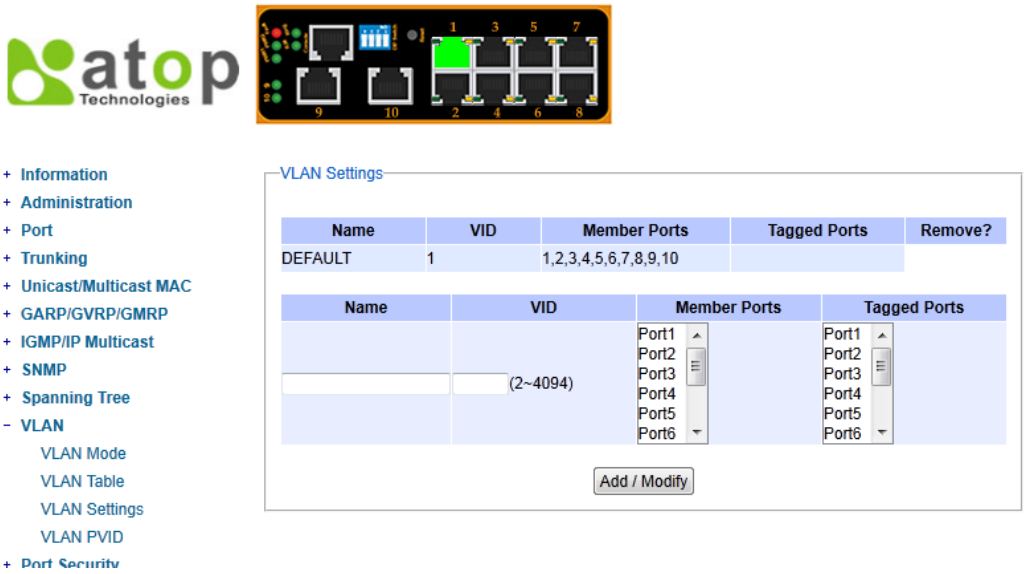


Fig. 2.45.a

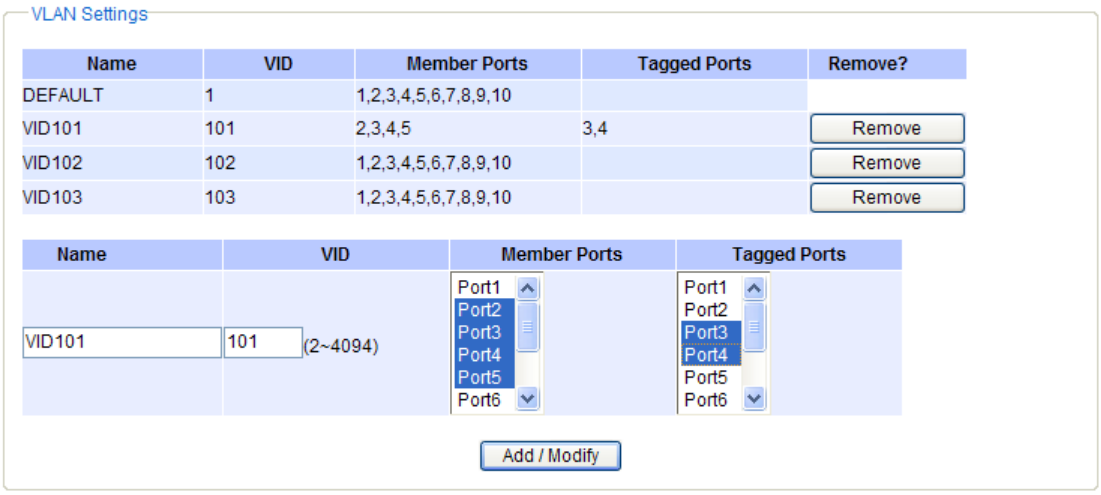


Fig. 2.45.b ∗Example∗

Fig. 2.45 and 2.45.b (example), display the current VLAN entry configuration; note that below there are the corresponding VLAN entries.

Table 2.33

Label	Description	Factory Default
Name	The VLAN ID name that can be assigned by the user.	DEFAULT
VID	Configures the VLAN ID that will be added in static VLAN table in switch. The VLAN ID is in the range 2~4094.	Dependant
Member Ports	Configures the ports to this specific VID.	All Ports
Tagged Ports	Configures the ports that outgoing packet is tagged or untagged. **Selected**: The outgoing packet is tagged from this port. **Unselected**: The outgoing packet is untagged from this port.	Dependant

***NOTE:**

- Default settings only have VLAN ID on 1.To configure settings for VLAN ID other than 1, users will have to assign ports to be in that VLAN group.

1. Go to *VLAN Setting.*
2. Fill in appropriate Name, VID, Member Ports, and Tagged Ports -> click on Add/Modify.
3. Go to *VLAN PVID*.
4. Choose the same ports, and enter PVID (which is the same as VID).

2.11.4 VLAN PVID

Each port is assigned a native VLAN number, the Port VLAN ID (PVID). When an untagged frame goes through a port, it is assigned to the port's PVID.

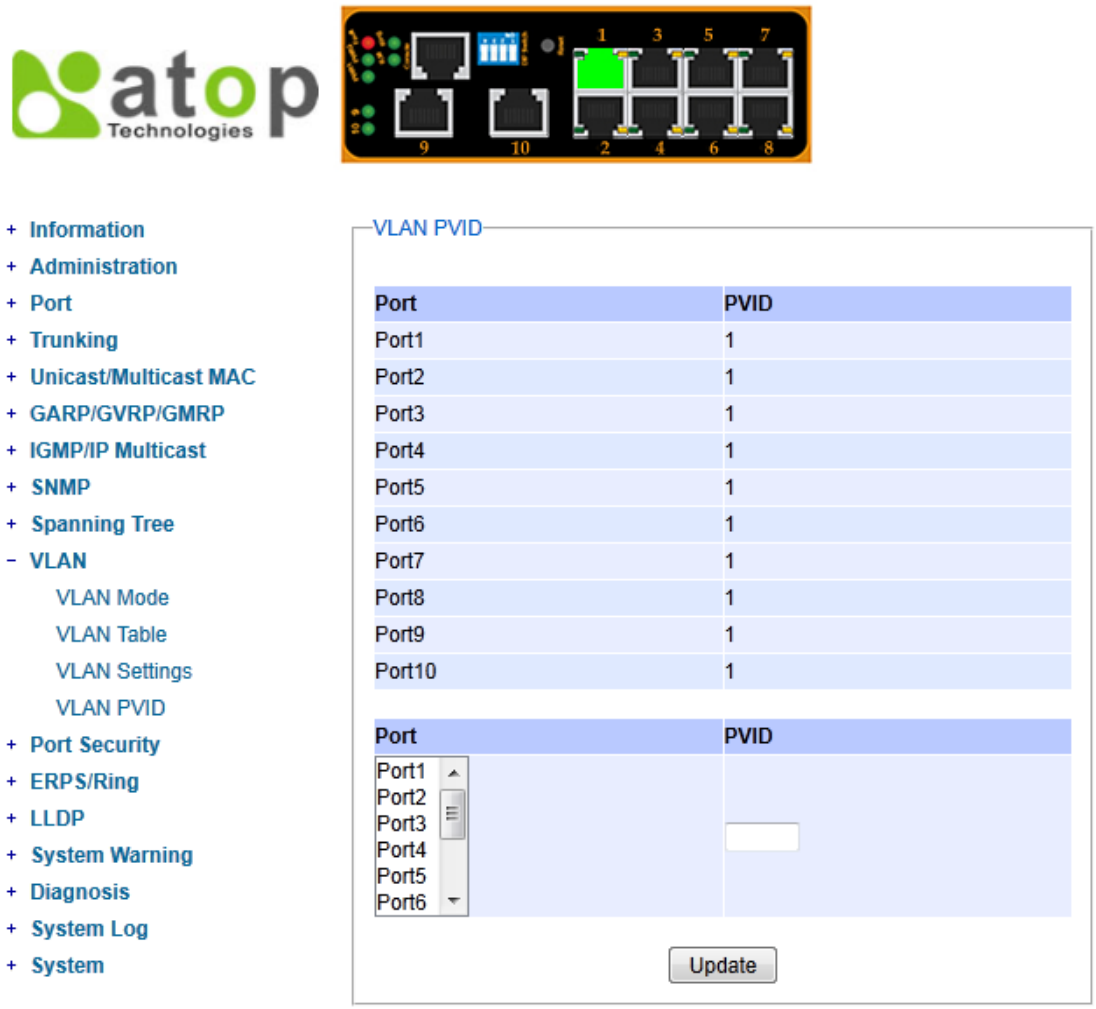


Fig. 2.46

Fig. 2.46 displays the ports' default VLAN ID; the lower portion allows the user to configure the port's PVID.

Table 2.34

Label	Description	Factory Default
Port	Select specific ports to be configured the PVID value.	-
PVID	Configures the default 802.1Q VID tag assigned to specific Port. The VLAN ID is in the range 1~4094.	1

2.11.5 Example of using 802.1Q VLAN

To configure 802.1Q VLAN, use the Static VLAN Setting page. For example, set Port 1, 2 and 3 into a VLAN group name VLAN 2 with VID 2 and Port 3 are tagged, Fig. 2.47.

Users should follow below settings:

Table 2.35

Label	Setting
Name	VLAN 2
VID	2
Member Ports	Choice Port 1, 2 and 3
Tagged Ports	Choice Port 2 and 3
Add/Modify	Click button after done

To select more than one port, user can simply click the "**Ctrl**" Key in keyboard

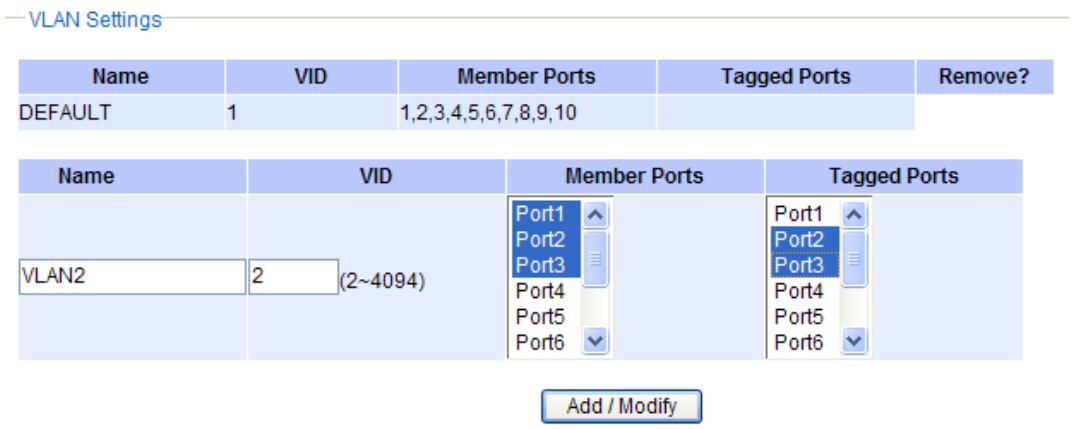


Fig. 2.47

2.12 Port Security

2.12.1 Static Port Security

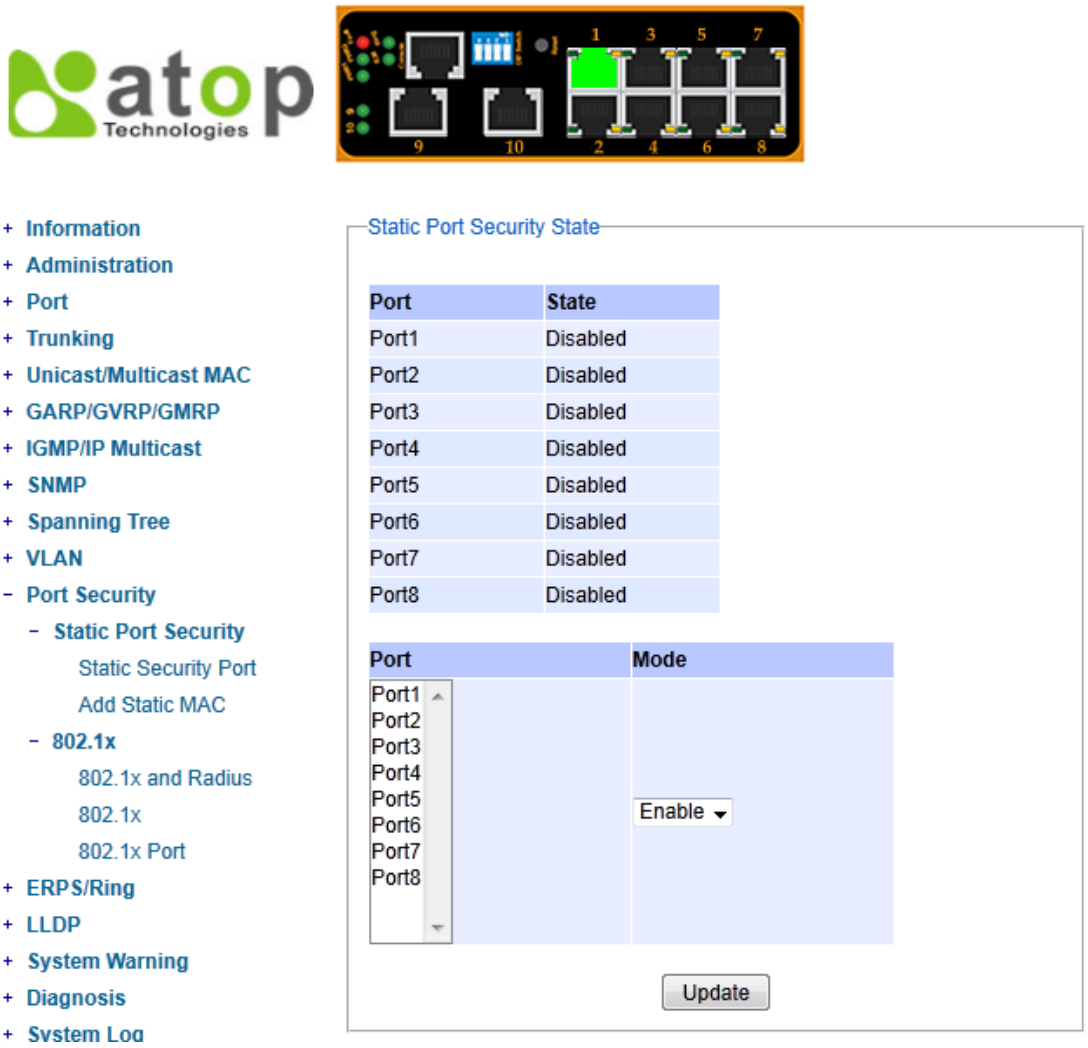


Fig. 2.48

802.1X: is an IEEE standard for port-based Network-Access Control, and it provides an authentication mechanism to devices wishing to attach to a LAN or WLAN. This protocol restricts unauthorized clients from connecting to a LAN through ports that are open to the Internet. The authentication basically involves three parties (Fig. 2.49): a supplicant, an authenticator, and an authentication server.

- Supplicant: The client device that request access to the LAN.

- Authentication Server: The server that performs the actual authentication. We use RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) as the authentication server.

- Authenticator: It is a network device that acts as a proxy between supplicant and authentication server. It passes around information, verifies information with the server, and relays response to the supplicant.

The authenticator acts like a security guard to a protected network. The supplicant is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. With 802.1X authentication, a supplicant and an authenticator exchange **EAP** (**E**xtensible **A**uthentication **P**rotocol, an authentication framework widely used by IEEE). Then the authenticator forwards this information to the authentication server for verification; if the authentication server confirms the request, the supplicant (client device) will be allowed to access resources located on the protected side of the network.

RADIUS: It is a networking protocol that provides authentication, authorization and accounting management for devices to connect and use a network service.

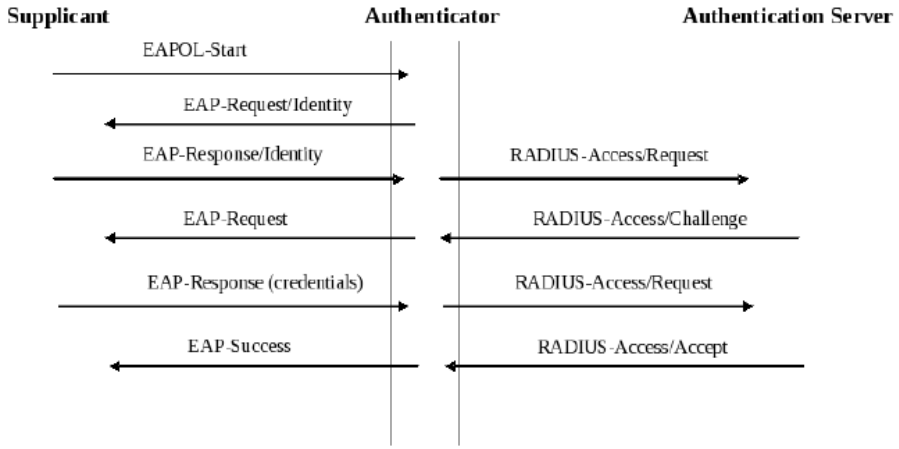


Fig. 2.49

2.12.2 Add Static MAC

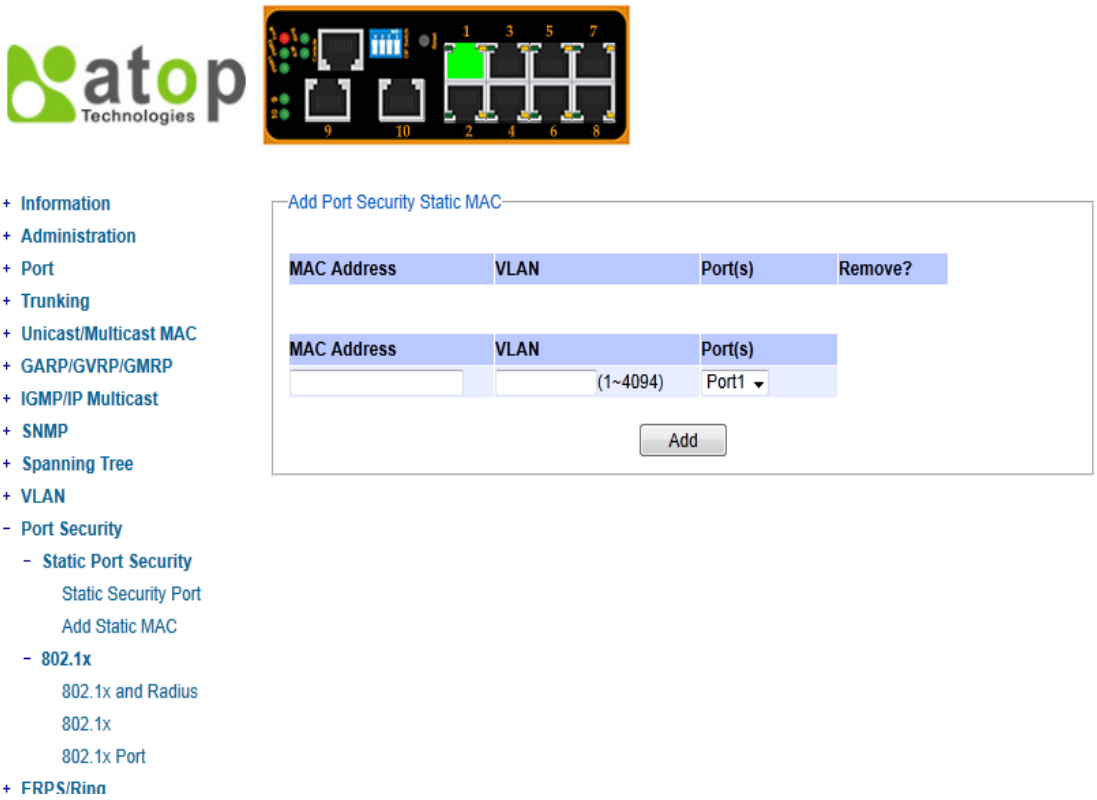


Fig. 2.50

Table 2.36

Label	Description
MAC Address	Type the suitable MAC address.
Ports	Choose between ports.
Remove	Option to remove the corresponding MAC address
Add	Click to add a MAC address
VLAN	Specify the corresponding VLAN address to MAC address.

The procedure for adding a MAC address is simple, just type in it in the corresponding field, choose the VLAN, the Port, and proceed to click on Add. Please remember that a MAC address cannot be assigned to 2 different ports, this will produce an error message.

2.12.3 802.1x and Radius

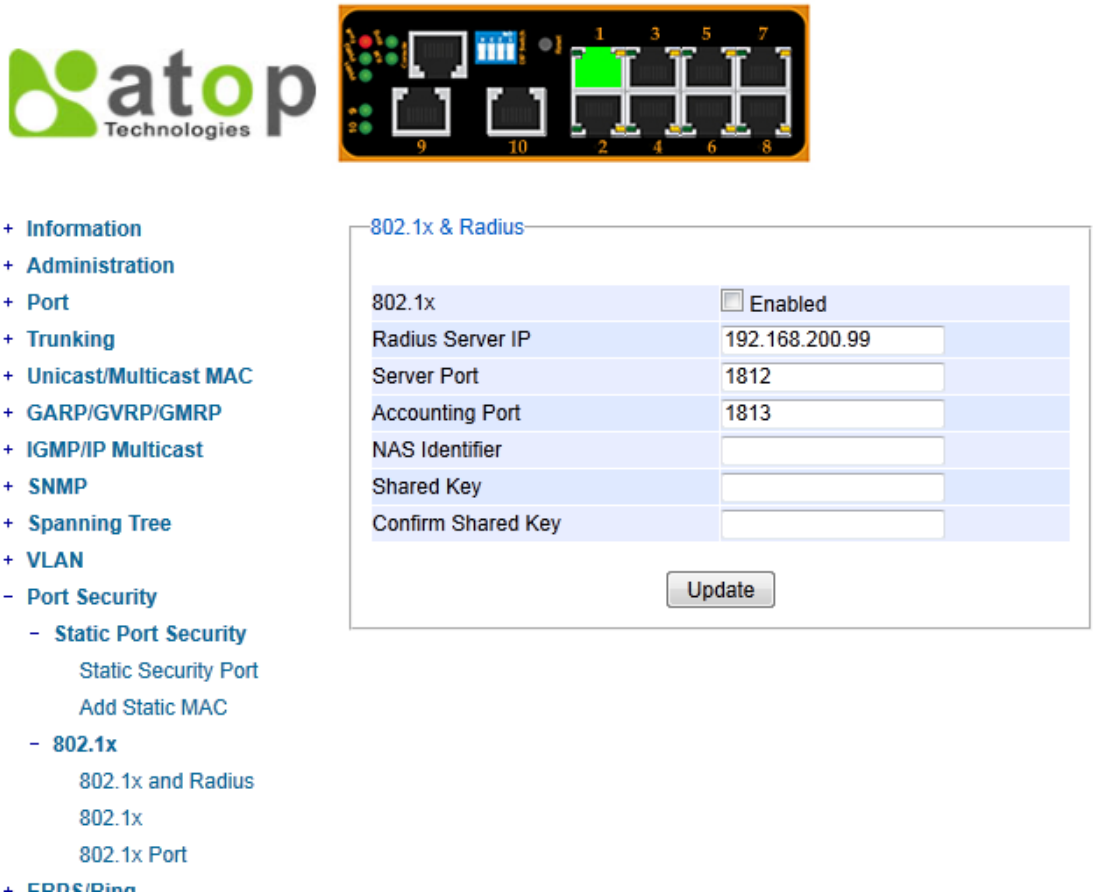


Fig. 2.51

Configuration for 802.1x and Radius server information is shown on Fig. 2.51.

Table 2.37

Label	Description	Factory Default
802.1x	Choose whether to Enable 802.1X for all ports or not.	Disabled
Radius Server IP	Set Radius server IP address.	192.168.200.99
Server Port	Set radius server port number. The range is 1024 ~ 65535.	1812
Accounting Port	Set radius accounting port number. The range is 1024 ~ 65535.	1813
NAS Identifier	Specifies 802.1X Network Access Server (NAS) identifier string. Max. 30 characters.	NULL
Shared Key	A key to be shared by EH7510 and the Radius Server. Both ends must be configured to use the same key. Max. 30 characters.	NULL
Confirm Shared Key	Re-type the Shared Key string.	Dependant

2.12.4 802.1.x

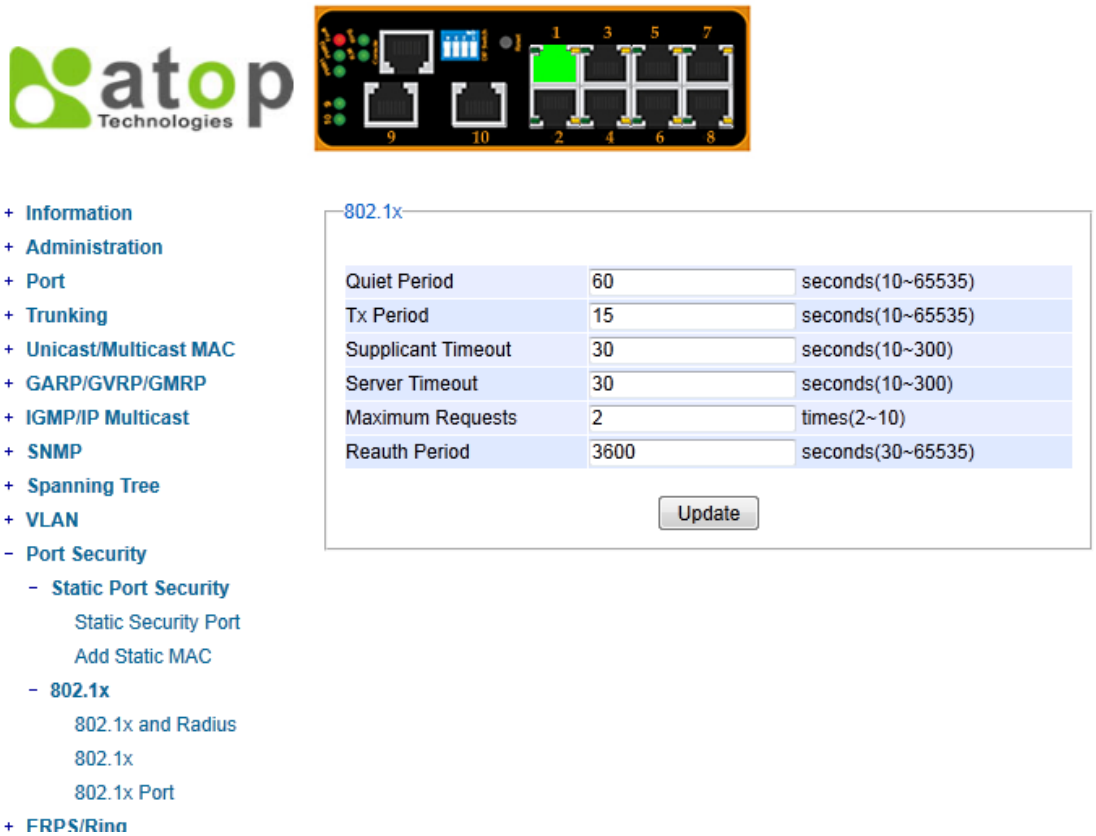


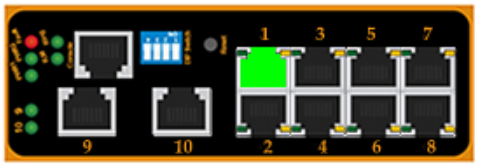
Fig. 2.52

802.1x settings and configurations shown in Fig. 2.52.

Table 2.38

Label	Description	Factory Default
Quiet Period	Waiting time between requests when the authorization has failed. Range from 10 to 65535 seconds.	60
Tx Period	Waiting time for the supplicant's EAP response packet before retransmitting another EAP request packet. Range from 10 to 65535 seconds.	15
Supplicant Timeout	Waiting time for the supplicant response to the authentication server's EAP packet. Range from 10 to 300 seconds.	30
Server Timeout	Waiting time for the authentication server's response to the supplicant's EAP packet. Range from 10 to 300 seconds.	30
Maximum Requests	Maximum number of times to retransmit the authentication server's EAP request packet to the supplicant before the authentication session times out. Range from 2 to 10 seconds.	2
Reauth Period	Time between periodic re-authentication of the supplicant. Range from 30 to 65535 seconds.	3600

2.12.5 802.1x Port



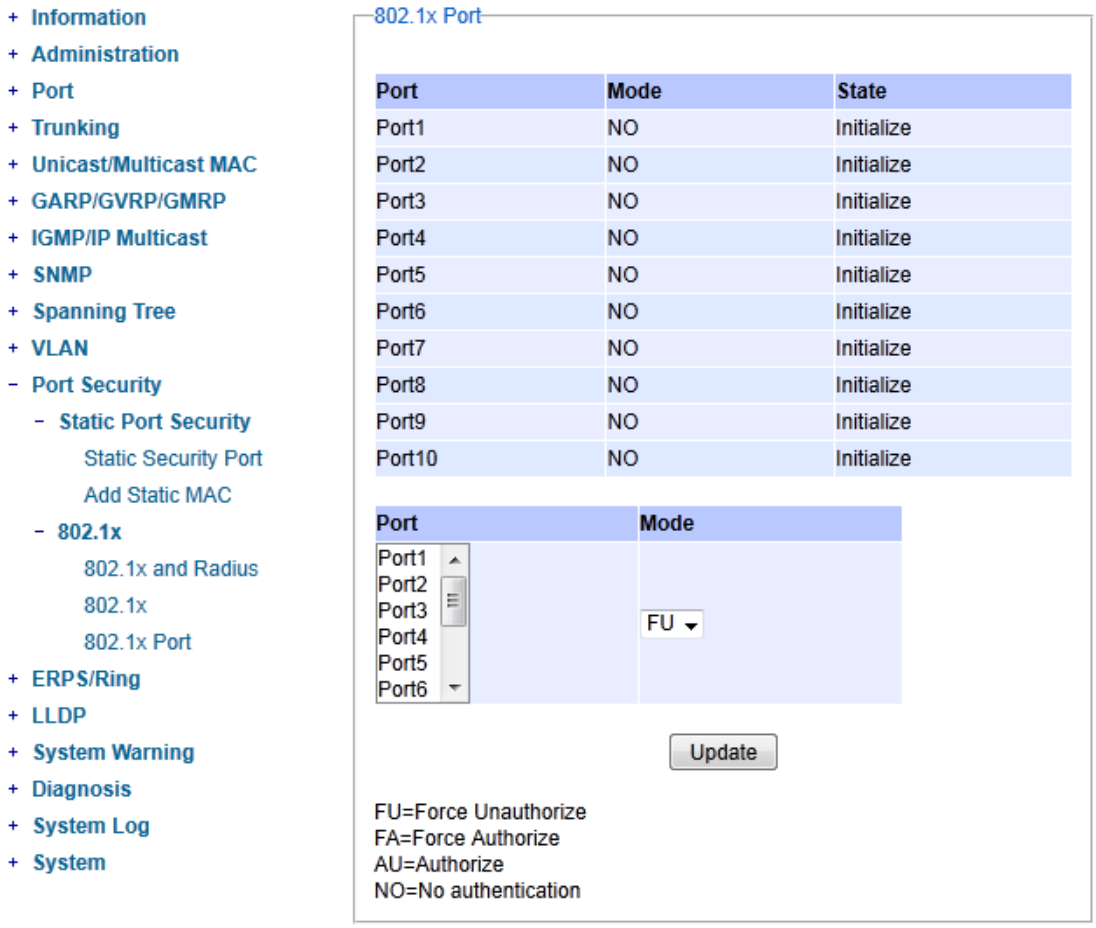


Fig. 2.53

802.1x Port information shown in Fig. 2.53.

Table 2.39

Label	Description	Factory Default
Port	Set specific ports to be configured.	Option
Mode	Choose from: **FU:** specifies forced unauthorized **FA:** specifies forced authorized **AU:** specifies authorization **NO**: specifies disable authorization	FU

2.13 ERPS/Ring

2.13.1 DIP Switch

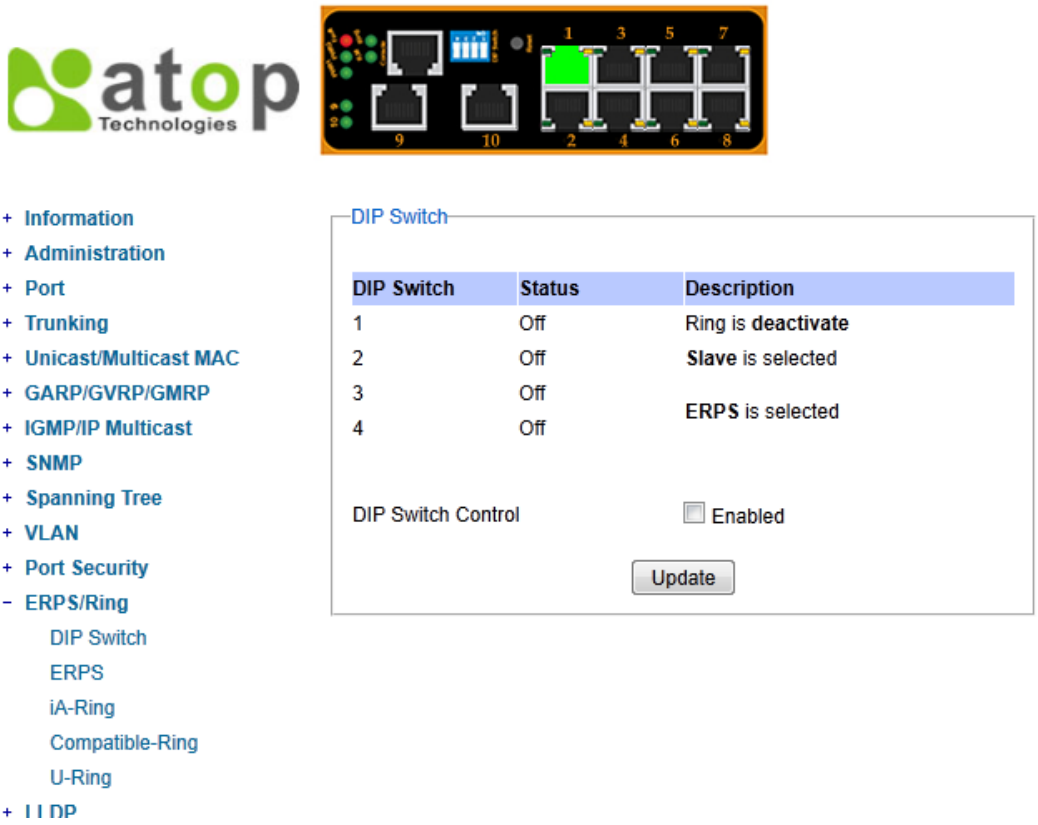


Fig. 2.54

This selection allows users to set the DIP Switch control; the DIP switches are located on EH7510 outer case, so it's another easy and convenient way to configure ERPS or iA-ring or Compatible-Ring via DIP Switches (instead of modifying configuration on web browser). Fig. 2.54 shows the current DIP Switch's status; the bottom portion allows the user to modify settings.

Table 2.40

Label	Description	Factory Default
DIP Switch Control	Enables or disables ERPS/iA-Ring/Compatible-Ring configuration via hardware DIP Switch.	Unchecked

After enabling the DIP Switch Control at DIP Switch page, users can control DIP Switch following the mode selection below.

- DIP 1 and 2 definition:

Table 2.41

DIP Switch	Off	On
1	Ring is deactivated	Ring is activate
2	Slave	Master

- DIP 3 and 4 definition:

Table 2.42

DIP Switch 3	DIP Switch 4	Ring Type
Off	Off	Select ERPS
Off	On	Select iA-Ring
On	Off	Select Compatible-Ring (only slave mode is supported)

- Factory default setting:
  - DIP Switch 1: OFF (Ring is inactive)
  - DIP Switch 2: OFF (Slave is selected)
  - DIP Switch 3/4: OFF/OFF (ERPS is selected)
- DIP switch 1 must be set to the “ON” position to enable DIP switches 2, 3, and 4. If DIP switch 1 is set to the “OFF” position, then DIP switches 2, 3, and 4 will all be disabled.
- When DIP 1 is set to “ON”, the default ring ports are Port9 and Port10 (Port10 is RPL port).
- When the Compatible-Ring is selected, DIP 2 is unused.

For example, if users want to set this device to be a master in an ERPS Ring, DIP switch 1 and 2 should be on, and DIP switch 3 and 4 should be off. These settings define the device to be a master with Port10 being RPL in an ERPS ring.

LED Indicators of DIP Switch are as below,

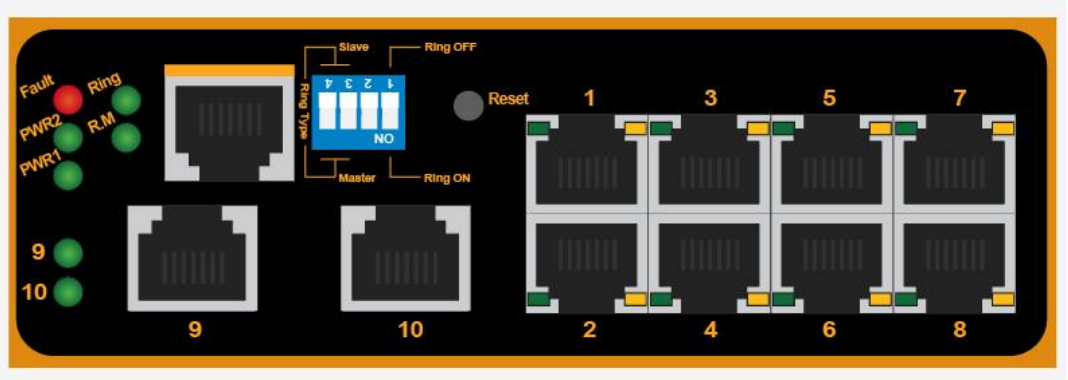


Fig. 2.55

EH7510 is designed with two LEDs on the outer case for indicating current DIP switches' status; these LEDs are for **Ring** and **Ring Master** as shown above (Fig. 2.55). There are four possible outcomes, and each outcome indicates different ring status; these four circumstances are addressed below.

Table 2.43

R.M. LED	Ring LED	R.M. Definition	Ring Definition
Light on	Light on	There's a RPL owner. ERPS enabled.	All rings in normal condition. ERPS enabled.
Off	On	No RPL owner. ERPS disabled.	All rings in normal condition. ERPS enabled.
Off	Off	No RPL owner. ERPS disabled.	ERPS disabled.
Off	Blinking	No RPL owner. ERPS disabled.	Ring in protection state. ERPS enabled.
On	Blinking	There's a RPL owner. ERPS enabled.	Ring in protection state. ERPS enabled.

2.13.2 ERPS

Ethernet **R**ing **P**rotection **S**witching (**ERPS**) is a protocol for Ethernet layer network rings, and it specifies protection mechanism. The ring topology provides multipoint connectivity economically by reducing number of links. ERPS provides highly reliable and stable protection in the ring topology, and it never forms loops, which can affect network operation.

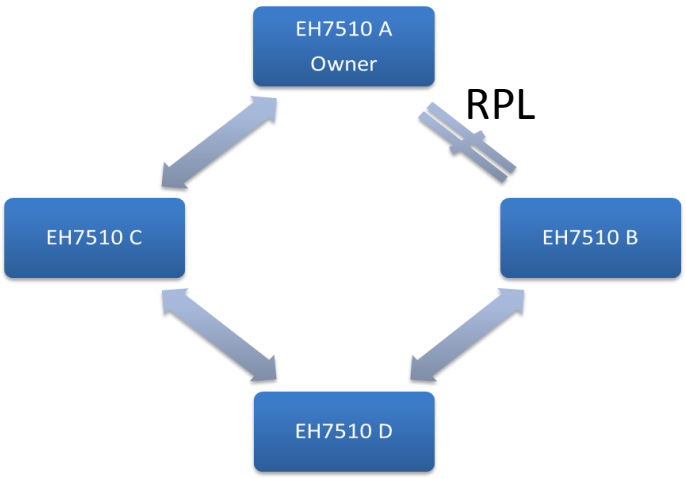


Fig. 2.56

As Fig. 2.56 shows, each Ethernet Ring Node is connected to adjacent Ethernet Ring Nodes participating in the same Ethernet Ring using two independent links (i.e. two ways). In the Ethernet ring, loops can be avoided by guaranteeing that traffic may flow on all but one of the ring links at any time. This particular link is called Ring Protection Link (RPL). A control message called R-APS coordinates the activities of switching on/off the RPL. Under normal conditions, this link is blocked by the Owner Node. Thus loops can be avoided by this mechanism. In case an Ethernet ring failure occurs, the RPL Owner node will be responsible to unblock its end of the RPL to allow RPL to be used for traffic. The RPL is as the backup link when one link failure occurs.

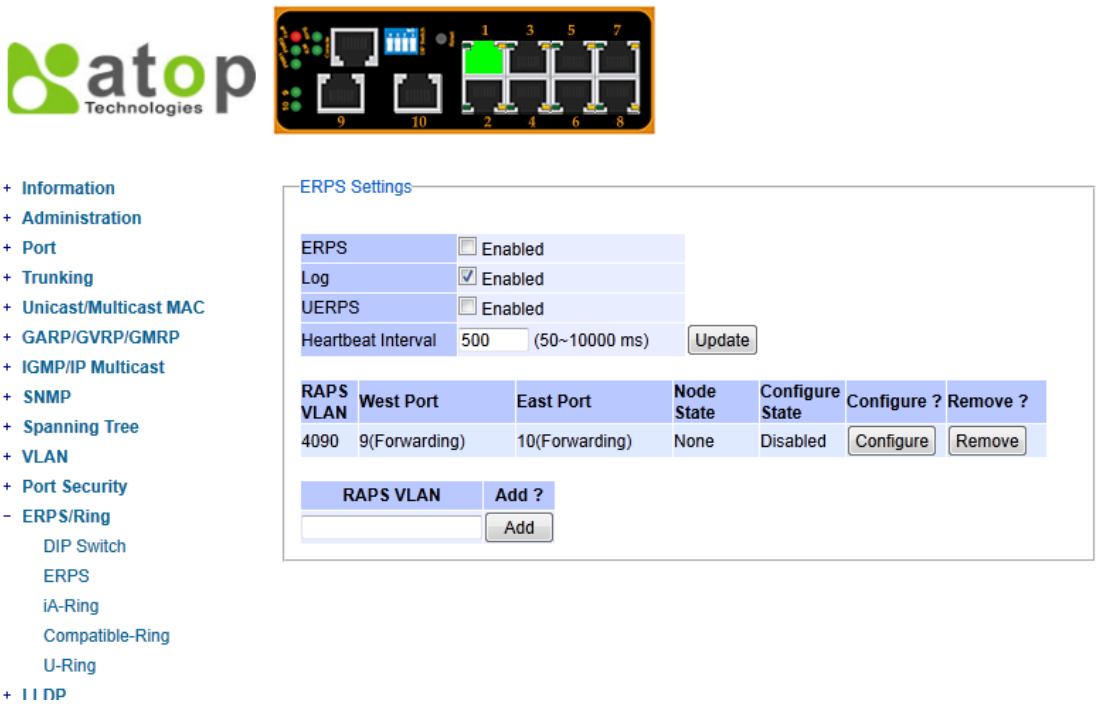


Fig. 2.57

ERPS settings are shown on Fig. 2.57; users should disable the DIP Switch Control first in order to set up ERPS parameters.

Table 2.44

Label	Description	Factory Default
ERPS	Choose whether to enable ERPS or not.	Disabled
Log	Choose to enable log.	Enabled
UERPS	Choose whether to enable UERPS. When UERPS is enabled, ring ports periodically sent a "heartbeat" packet to peer ring ports in order to determine whether the link path (etc. wireless bridge) is failure or alive. If peer ring port cannot receive "heartbeat" packets over 3 packets, the ring port will enter protection state. Note: This function affect the recovery time to more than 20 ms.	Disabled
Heartbeat Interval	Set the Heartbeat Interval. Range from 50 to 10000 milliseconds.	500 ms
RAPS VLAN	Create the ring by specifying the R-APS VLAN ID of the ring. VLAN ID ranges from 1 to 4094.	None

After enabling the ERPS and adding a RAPS VLAN, users can click on Configure for more details and configurations, which are shown on Fig. 2.58.

Fig. 2.58

Table 2.45

Label	Description	Factory Default
ERPS VLAN	Indicate current RAPS VLAN ID.	None
Status	Choose to enable ERPS with this particular VLAN.	Disabled
West Port	Choose the *West Port* of the RPL.	Port9
East Port	Choose the *East Port* of the RPL.	Port10
RPL Owner	Choose to enable Owner Function.	Disabled
RPL Port	Select the *Owner Port*.	None
WTR Timer	Set the wait-to-restore (WTR) time of the ring in minutes. Lower value has lower protection time. Range from 0 to 12 minutes.	0
Holdoff Timer	Set the holdoff time of the ring. Range from 0 to 10000 milliseconds.	0
Guard Timer	Set the guard time of the ring. Range from 0 to 2000 milliseconds.	500
MEL	Set the maintenance entity group level (MEL) of the ring. Range from 0 to 7.	1
Propagate TC	Indicate the topology change propagation of the ring ability.	Enabled

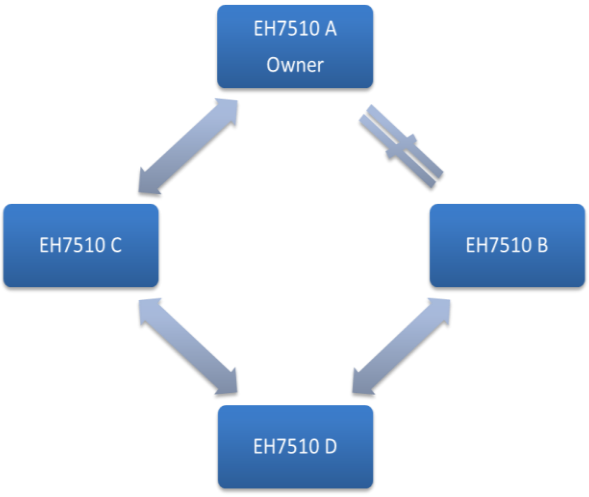


Fig. 2.59

Using the same example as above, configurations of two switches can be set up individually as follows:

Table 2.46

EH7510	A		EH7510	B
RAPS VLAN	8		RAPS VLAN	8
ERPS RAPS	Enabled		ERPS RAPS	Enabled
West Port	1		West Port	1
East Port	2		East Port	2
RPL Owner	Enabled		RPL Owner	Disabled
RPL Port	West		RPL Port	none

Table 2.47

EH7510	C		EH7510	D
RAPS VLAN	8		RAPS VLAN	8
ERPS RAPS	Enabled		ERPS RAPS	Enabled
West Port	1		West Port	1
East Port	2		East Port	2
RPL Owner	Disabled		RPL Owner	Disabled
RPL Port	none		RPL Port	none

2.13.2.1 UERPS Settings (optional)

1. Prepare two EH7510 (EH7510 A and EH7510 B). We will use Port 7 and Port 8 on both EH7510 for redundancy.
2. Connect EH7510 A and EH7510 B to the network or PC so you can access them. For simplicity you can use Port 1 for Web configuration on both switches.
3. Open SwitchView (Management Utility) and change the IP of EH7510 B or both switches, so the IP won't be conflicting.
4. Open EH7510 A and B's WebUI and setup ERPS settings like the following. You just need to enable ERPS, Log, and UERPS. You need to press "Update" for the changes to take effect.

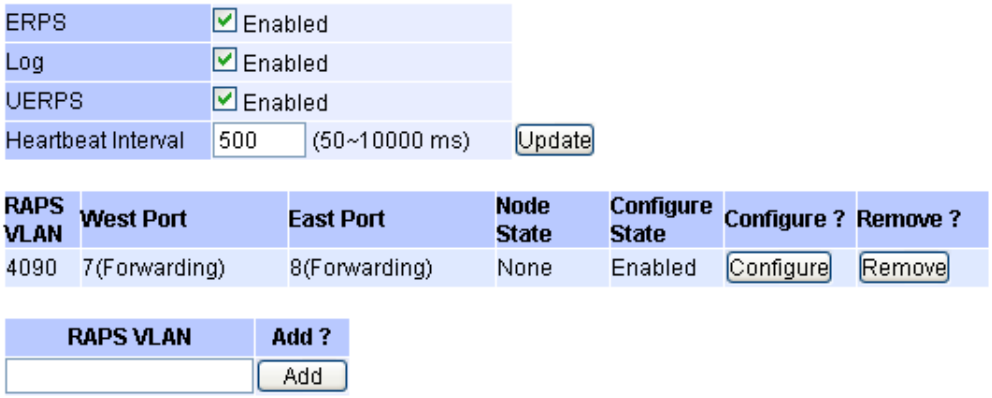


Fig. 2.60

5. On EH7510 A, Click “Configure” on RAPS VLAN and setup as the below figure.

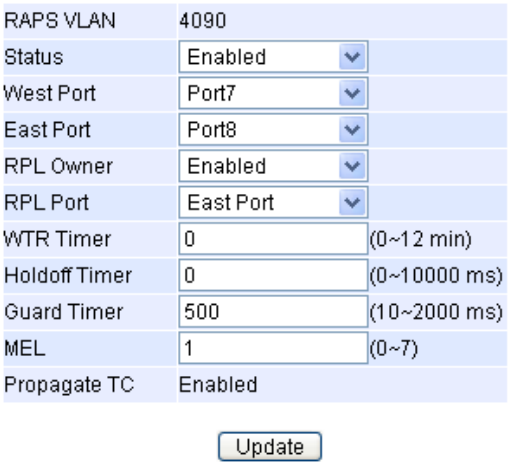


Fig. 2.61

6. Open EH7510 B’s WebUI and setup ERPS settings like the following.

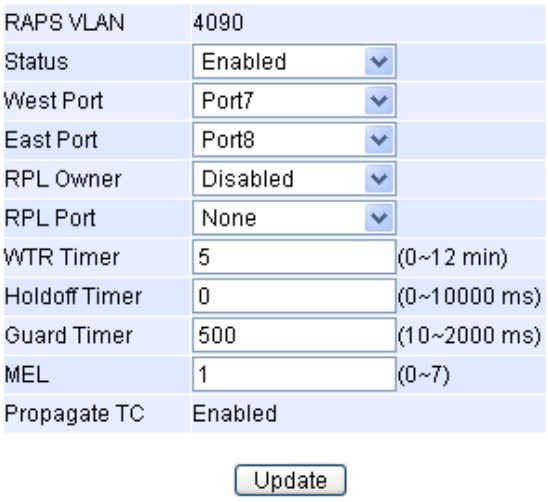


Fig.2.62

7. Connect EH7510 A’s Port 7 to EH7510 B’s Port 8. Connect EH7510 A’s Port 8 to EH7510 B’s Port 7 (like cross-over) for the redundancy port.
8. If everything is setup properly, you will find EH7510 A to have the following ERPS state. It will automatically block Port 8 to prevent network loop.

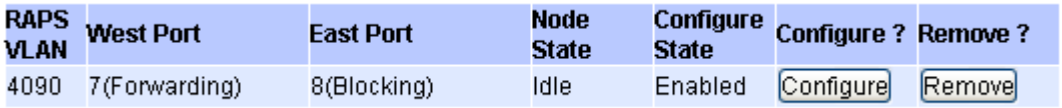


Fig. 2.63

9. Now you can add any other bridge that you want in between the two EH7510s.

Trick: If you want to test the real throughput of your wireless bridge, you can find this function under Port tically block Port 8 to prevent network loop.the changess failure or alive.ing, loops can be avoided by guarant

Port	Enable	Negotiation	Speed	Duplex	Flow Control	Rate Control(Kbps)		Throughput Test(Kbps)		
						Ingress	Egress	Ingress	Egress	Action
Port1	☑	Auto	100	Full	Off	0	0	0	0	Test
Port2	☑	Auto	100	Full	Off	0	0	0	0	Test
Port3	☑	Auto	100	Full	Off	0	0	0	0	Test
Port4	☑	Auto	100	Full	Off	0	0	0	0	Test
Port5	☑	Auto	100	Full	Off	0	0	0	0	Test
Port6	☑	Auto	100	Full	Off	0	0	0	0	Test
Port7	☑	Auto	100	Full	Off	0	0	0	0	Test
Port8	☑	Auto	100	Full	Off	0	0	98782	98782	Test
Port9	☑	Auto	1000	Full	Off	0	0	0	0	Test
Port10	☑	Auto	1000	Full	Off	0	0	0	0	Test

Fig. 2.64

2.13.3 iA-Ring

EH7510 is designed to be compatible with iA-Ring protocol for providing better network reliability and faster recovery time for redundant ring topologies; it is in the same category as R Rings, but with its own protocol. It has been a successful development that reduces recovery time to less than 20 ms. iA-Ring can be used for any single ring, which is shown on the picture below (Fig. 2.65).

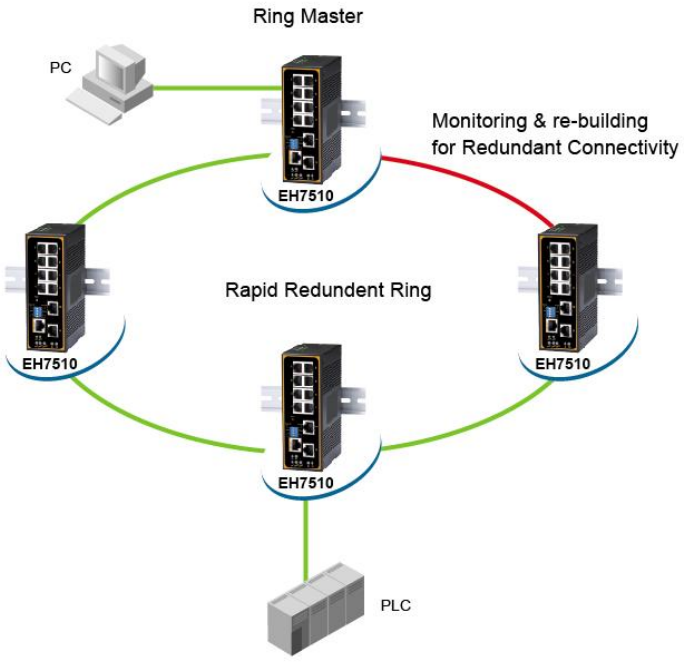


Fig. 2.65

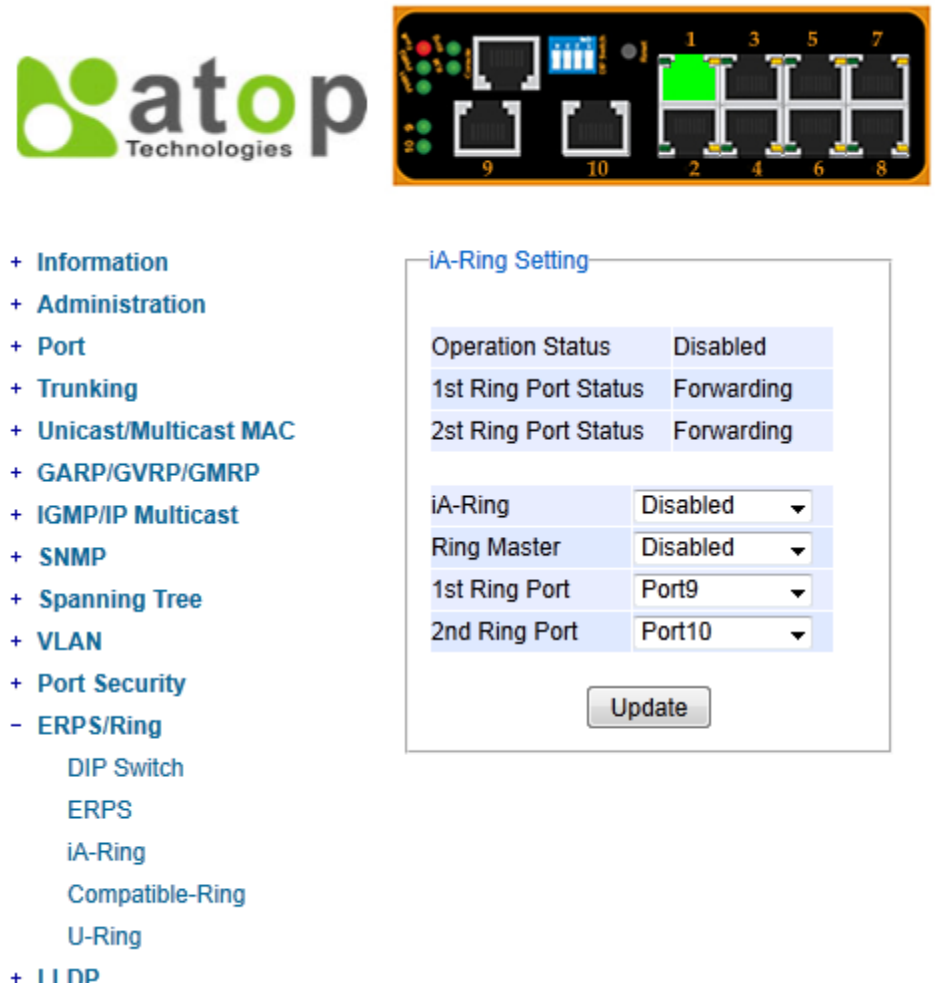


Fig. 2.66

Fig. 2.66 shows iA-Ring redundancy protocol; users should disable DIP Switch Control and ERPS first in order to enable/configure iA-Ring parameters on a web browser.

Table 2.48

Label	Description	Factory Default
iA-Ring	Enable iA-Ring or disable iA-Ring.	Disabled
Ring Master	Enabled: Master Mode. Disabled: Slave Mode.	Disabled
1st Ring Port	Select the primary port for the Ring.	Port9
2nd Ring Port	Select the backup port for the Ring.	Port10

2.13.4 Compatible-Ring

Compatible-Ring is similar as iA-Ring, the only difference being it can be used for MOXA rings as well. To get more details of this redundant ring protocol, please contact Atop.

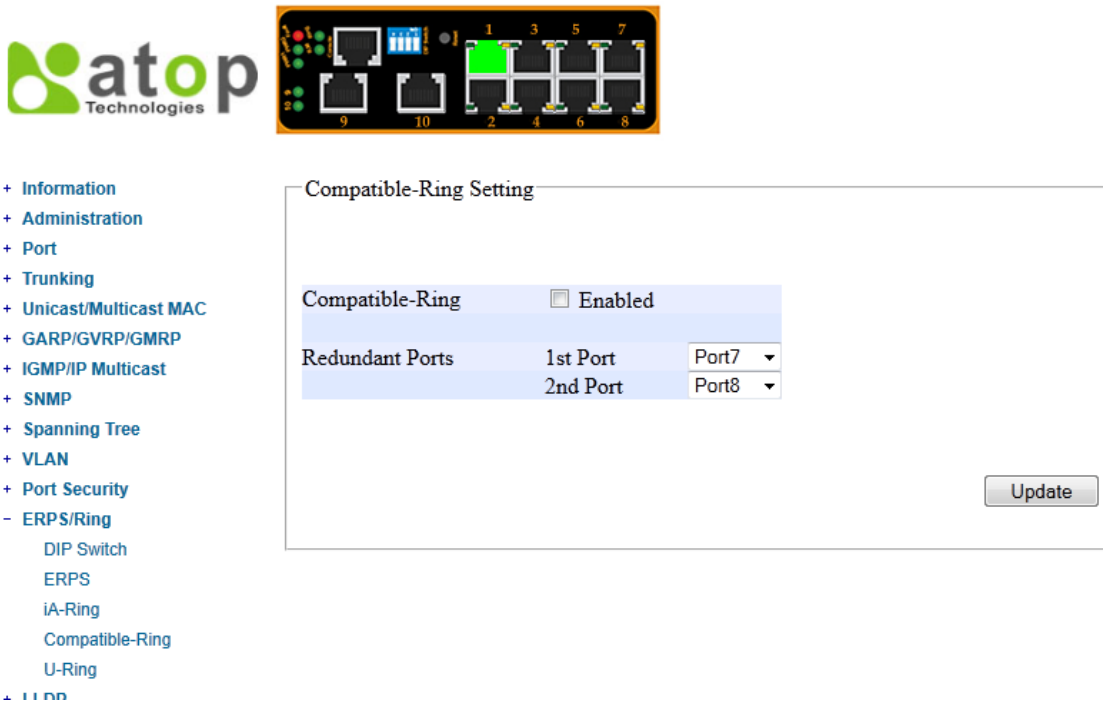


Fig. 2.67

Fig. 2.67 shows how to set the Compatible-Ring redundancy protocol; users should disable DIP Switch Control and ERPS first in order to enable/configure Compatible-Ring parameters on the web browser.

Table 2.49

Label	Description	Factory Default
Compatible-Ring	Enables Compatible-Ring or disable Compatible-Ring.	Disabled
1st Ring Port	Selects the primary port for the Ring.	Port7
2nd Ring Port	Selects the backup port for the Ring.	Port8

2.13.5 U-Ring

U-Ring (Unicast Ring) Setup

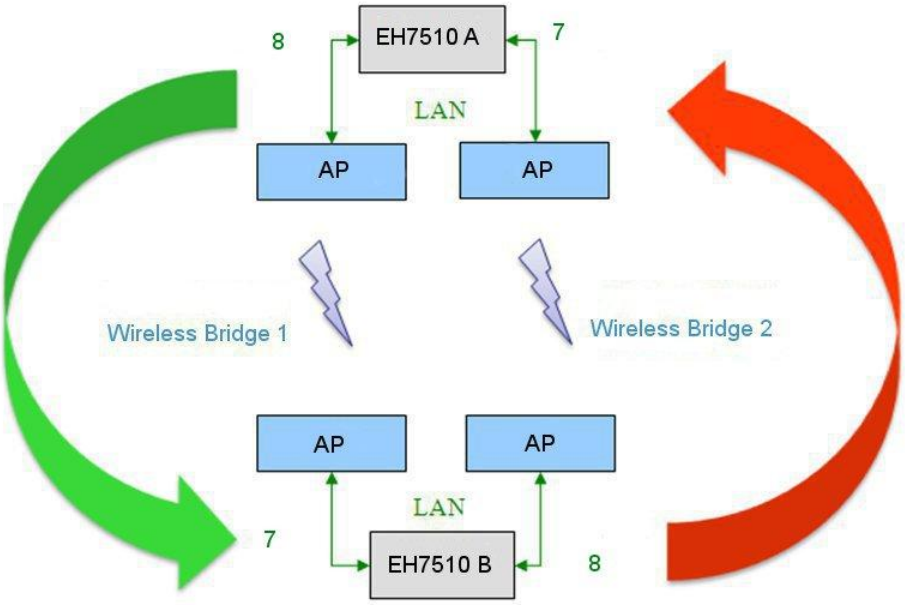


Fig. 2.68.a ＊Example of a 2-bridge U-ring＊

This configuration is for access between 2 points; in this example each point is connected to the Access Points by an Ethernet LAN line and these in turn are connected by Wireless Bridges 1 and 2. In the figure below, the same protocol is used instead of a wireless connection between the Access Points there is a physical line.

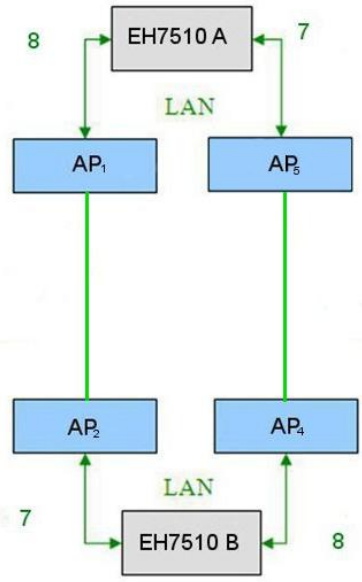


Fig. 2.68.b

U-ring protocol could be used in the above environment, the AP_x could be:

- Dump-switch
- Transceiver
- XDSL bridge

Care should be taken that if a dump-switch is used as an AP (**A**ccess **P**oint) the one in the other side must be a dump-switch as well; again care should be taken when connecting the cables to the ports.

The main screen will look as follows.

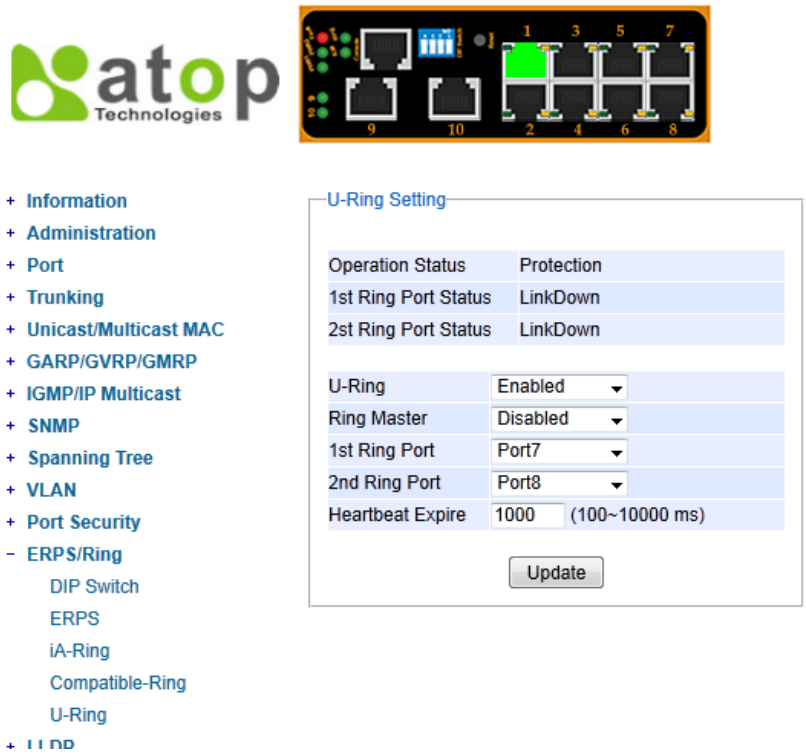


Fig. 2.69

Table 2.50

Label	Description	Factory Default
Operation Status	Shows whether the device's state is normal or protected.	Dependant
1st Ring Port Status	Displays the 1st ring port's status.	Forwarding
2nd Ring Port Status	Displays the 2nd ring port's status.	Forwarding
U-Ring	Shows whether the Unicast ring is working.	Disabled
Ring Master	Shows whether the device is a slave or master on this ring. For Slave option leave it as disabled.	Disabled
1st Ring Port	Displays whether this Ethernet port is being used for the corresponding ring's port.	Port 1
2nd Ring Port	Displays whether this Ethernet port is being used for the corresponding ring's port.	Port 2
Heartbeat Expire	Time interval between checking-packets.	1000

2.14 LLDP

2.14.1 LLDP

Link **L**ayer **D**iscovery **P**rotocol (**LLDP**) is an IEEE standard OSI layer-2 protocol. It's used by network devices for advertising their identity, capabilities, and neighbors' information on a local area network. It allows each network device, e.g. an EH7510 switch, to inform its neighbors about its information and configurations periodically. As a result, all of the networks devices would discover their neighbors across connected network links using this standard mechanism.

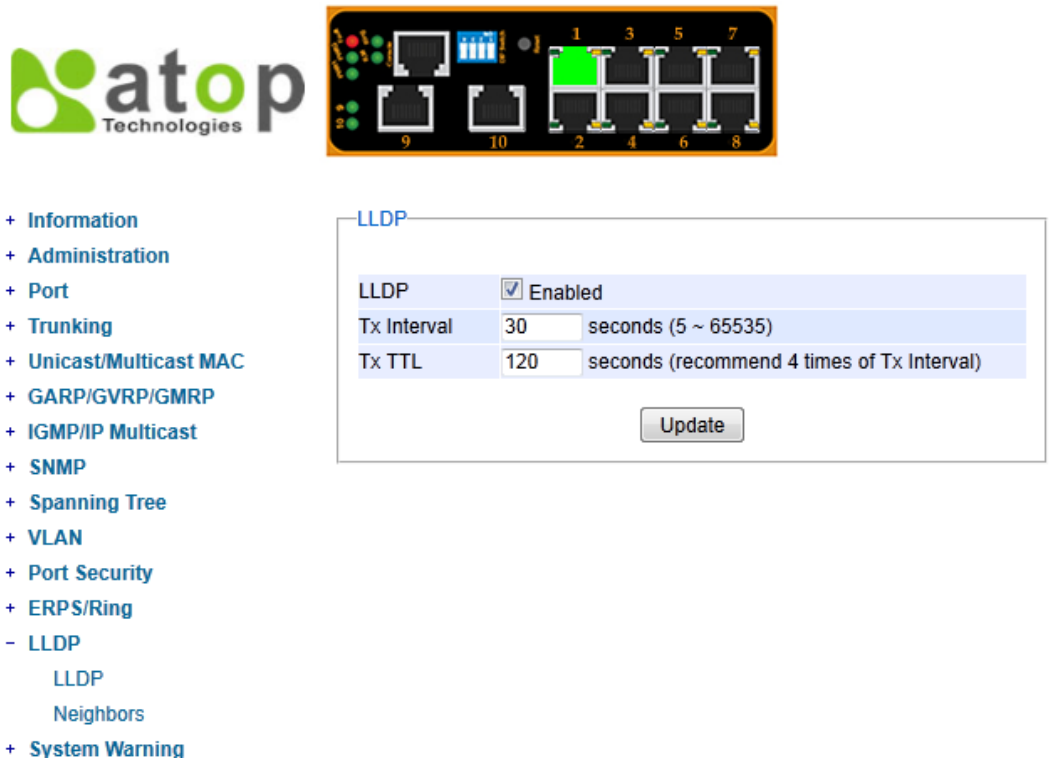


Fig. 2.70

Fig. 2.70 allows users to have options for enabling or disabling the LLDP, as well as setting LLDP transition parameters. This function should be enabled if users want to use Device View to monitor the switches' topology of the whole network. For information of using Device View, please refer to Chapter 4.

Table 2.51

Label	Description	Factory Default
LLDP	Choose to either enable or disable LLDP.	Enabled
Tx Interval	To set the transmit interval of LLDP messages. Range from 5 to 65535 seconds.	30
TxTTL	*Tx Time-To-Live*. Amount of time to keep neighbors' information. The recommend TTL value is 4 times of *Tx Interval*. Range from 5 to 65535 seconds.	120

2.14.2 Neighbors

- + Information
- + Administration
- + Port
- + Trunking
- + Unicast/Multicast MAC
- + GARP/GVRP/GMRP
- + IGMP/IP Multicast
- + SNMP
- + Spanning Tree
- + VLAN
- + Port Security
- + ERPS/Ring
- − LLDP
  - LLDP
  - Neighbors
- + System Warning

Neighbors

Port	Neighbor Information					
	Chassis ID	Port ID	Port Description	System Name	System Description	Management Address
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Fig. 2.71.a

Neighbors

Port	Neighbor Information					
	Chassis ID	Port ID	Port Description	System Name	System Description	Management Address
1						
2						
3						
4	00:60:E9:07:98:9D	3	Port 3	EH7510	Managed Switch EH7510	10.0.7.4
5						
6						
7						
8						
9	00:60:E9:07:98:99	10	Port 10	EH7510 1	Managed Switch EH7510	10.0.7.8
10	00:60:E9:07:98:9B	9	Port 9	EH7510	Managed Switch EH7510	10.0.7.6

Fig. 2.71.b ∗Example∗

Fig. 2.71 allows users to view the information of each neighbor close to this switch, and its example on Fig. 2.71.b.

Table 2.52

Label	Description
Port	Indicates particular port number of the switch.
Chassis ID	Indicates the identity of the neighbor of this particular port.
Port ID	Indicates the port number of this neighbor.
Port Description	Shows a textual description of the neighbor port.
System Name	Indicates the system name/ hostname of the neighbor.
System Description	Shows a more detailed description of the neighbor's system.
Management Address	Indicates neighbor's management IP address.

2.15 System Warning

It is important for network administrators to know what's happening in their networks, and know where the events are happening. However, it is difficult to locate network devices that are at the endpoints of systems. Thus Ethernet switches connected to these devices play an important role of providing first-moment alarm messages to system administrators. This means network administrators can be informed instantaneously when accidents happen.

EH7510 uses email and relay output to provide fast and reliable warn alerts for administrators.

2.15.1 Warning Event Selection

There are three different types of events: Port Events, Power Events, and System Events. Port Events (Fig. 2.72), are related to the activities of a certain port, Power Events, keep track of power status of the switch, and System Events, are related to the overall functionalities of the switch.

Fig. 2.72

Table 2.53

Label	Description	Factory Default
Port	Indicates the port number.	
Port state event	**Disable:** Disables alarm function, i.e. no alarm message will be sent. **Link Up:** Alarm message will be sent when this port/link is up and connection begins. **Link Down:** Alarm message will be sent when this port/link is down and disconnected. **Link Up /Down:** Alarm message will be sent whenever there's a change, i.e. connection begins or connection disrupted.	Disabled

Table 2.54.a

Label	Description	Factory Default
Power	Indicates specific power supply.	
Power status event	**Disable:** Disables alarm function. **Power On:** Sends an alarm when power is turned on. **Power Off:** Sends an alarm when power is turned off.	Disabled

Table 2.54.b

Label	Description	Factory Default
System log event	**Disable:** Disable power status detection. **0: (LOG_EMERG):** Enable log level 0~7 detection. **1: (LOG_ALERT):** Enable log level 1~7 detection. **2: (LOG_CRIT):** Enable log level 2~7 detection. **3: (LOG_ERR):** Enable log level 3~7 detection. **4: (LOG_WARNING):** Enable log level 4~7 detection. **5: (LOG_NOTICE):** Enable log level 5~7 detection. **6: (LOG_INFO):** Enable log level 6~7 detection. **7: (LOG_DEBUG):** Enable log level 7 detection. See note below for specific log level description.	Disabled

***NOTE:**

- **Log levels** are inclusive. In other word, when log level is set to 0, alarm is triggered whenever 0, 1, 2… 6, and/or 7 happen. When log level is set to 5, alarm is triggered whenever 5, 6, and/or 7 happen.

  0: Emergency: system is unstable

  1: Alert: action must be taken immediately

  2: Critical: critical conditions

  3: Error: error conditions

  4: Warning: warning condition

  5: Notice: normal but significant condition

  6: Informational: informational messages

  7: Debug: debug-level messages

2.15.2 Alert Warning Events

EH7510 warns its users in case any event occurs; a table in this section displays the warning events (as shown in Fig. 2.73.b as an example). A short alarm message on the top portion of the web browser interface; users can click the "**Alarms**!" to hyperlink to the "Warning Events" web page. For example, the top of web page now displays "**2 Alarms!**". We can click the "**2 Alarms!**" to see the events. In this example, "**2 Alarms**!" means there two events occurred:

1. port4 is down
2. port5 is up.

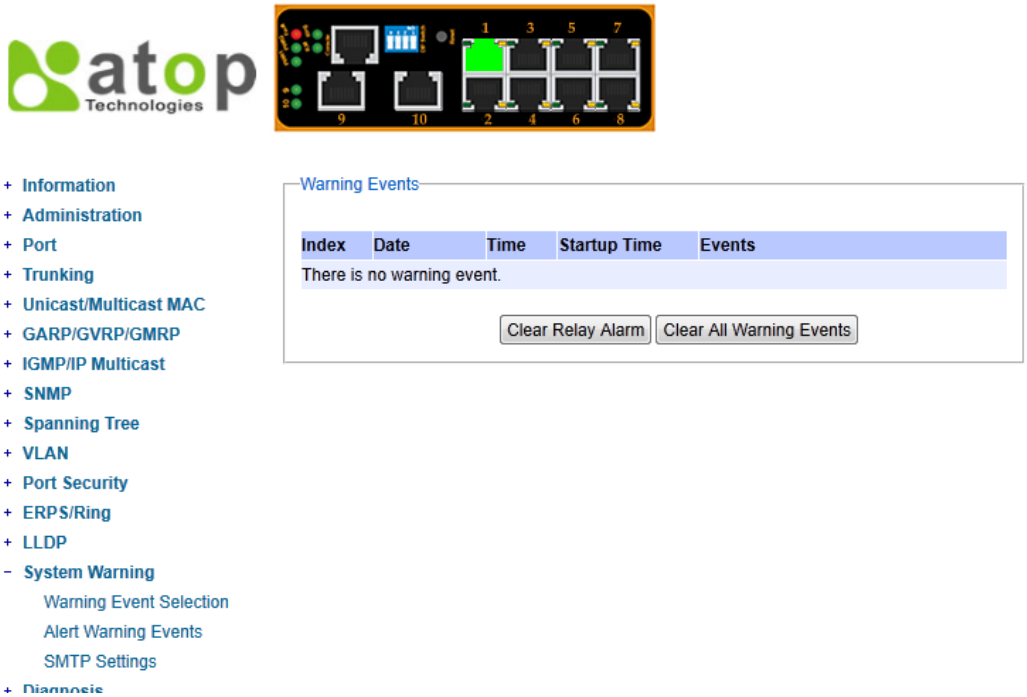


Fig.2.73.a

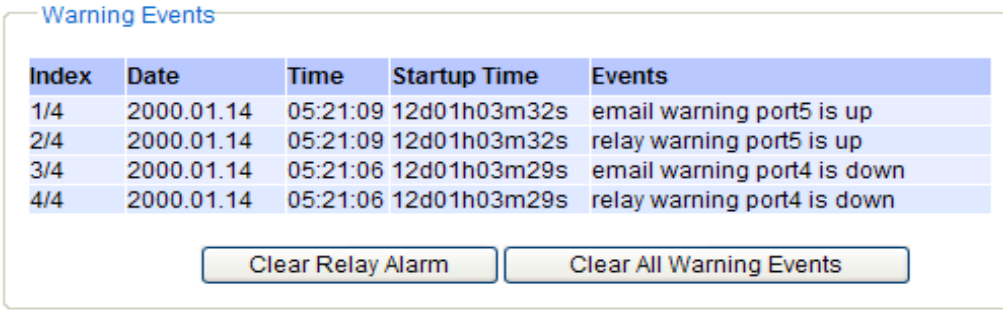


Fig. 2.73.b

Table 2.55

Label	Description	Factory Default
Clear Relay Alarm	Sets Hardware Relay Alarm to off.	Relay is off
Clear All Warning Events	Clears all warning events that are displayed.	

2.15.3 SMTP Settings

Simple **M**ail **T**ransfer **P**rotocol (**SMTP**) is an internet standard for email transmission across IP networks. In case any warning events occur, the system can send an alarm message to users through email. Here, users will be allowed to modify email-related settings for system alarm, (Fig. 2.74.a 2.74.b).

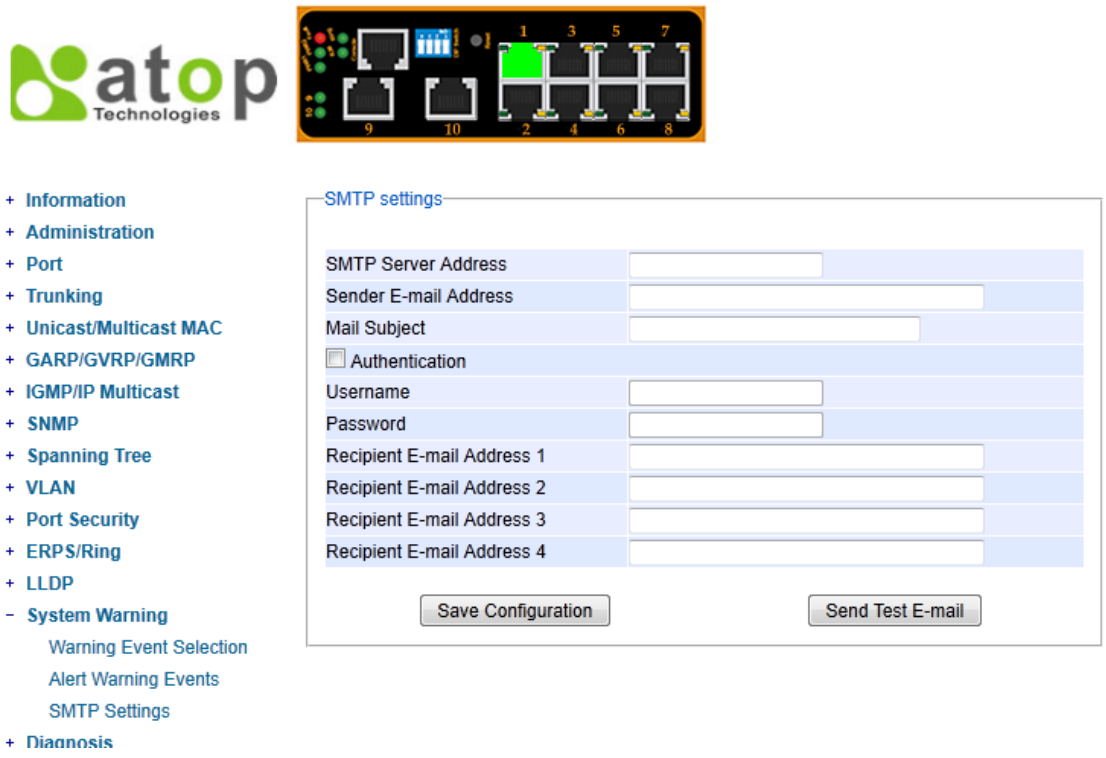


Fig. 2.74.a

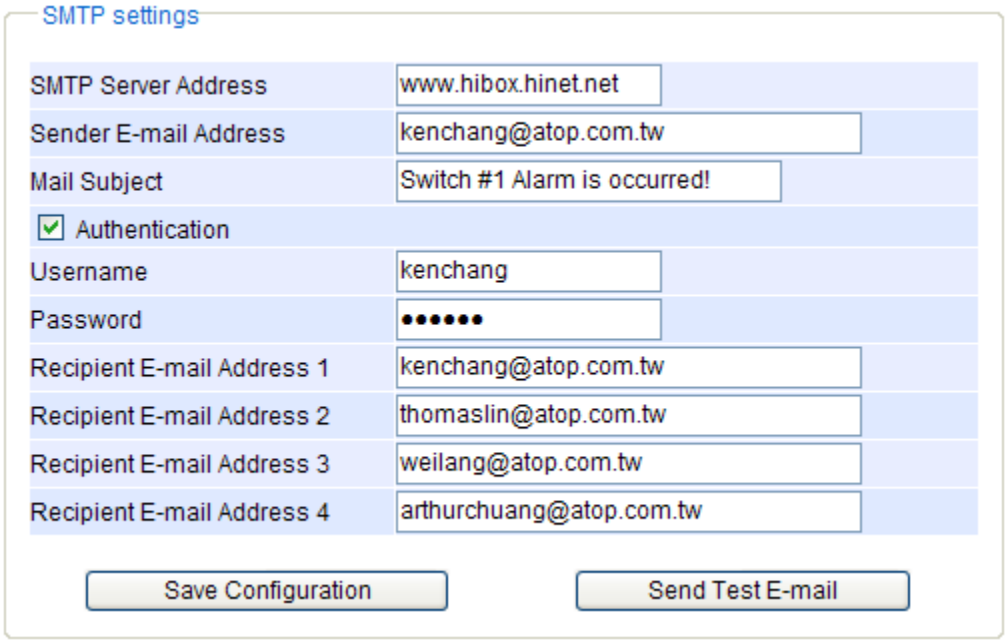


Fig. 2.74.b

Table 2.56

Label	Description	Factory Default
SMTP Server Address	Configure the IP address of email server	NULL
Sender E-mail Address	Configure the sender e-mail address.	NULL
Mail Subject	Type the subject of this warning message. Max. 31 characters.	NULL
Authentication	Enable or disable authentication login. If enabled, server will need authentication to login; users will also need to setup username and password.	Checked
Username	Set the user name (or account name) to login. Max. 31 characters.	NULL
Password	Set the account password for login. Max. 15 characters.	NULL
Recipient E-mail Address 1	Set the first receiver's E-mail address.	NULL
Recipient E-mail Address 2	Set the second receiver's E-mail address.	NULL
Recipient E-mail Address 3	Set the third receiver's E-mail address.	NULL
Recipient E-mail Address 4	Set the fourth receiver's E-mail address.	NULL
Save Configuration	Update these modifications.	
Send Test E-mail	A test email can be sent to recipient to check accuracy.	

2.16 Diagnosis

EH7510 provides a *Ping* function, which is a simple but useful tool, for troubleshooting network problems, (next page Fig.2.75.a, b, c, d).

2.16.1 Ping

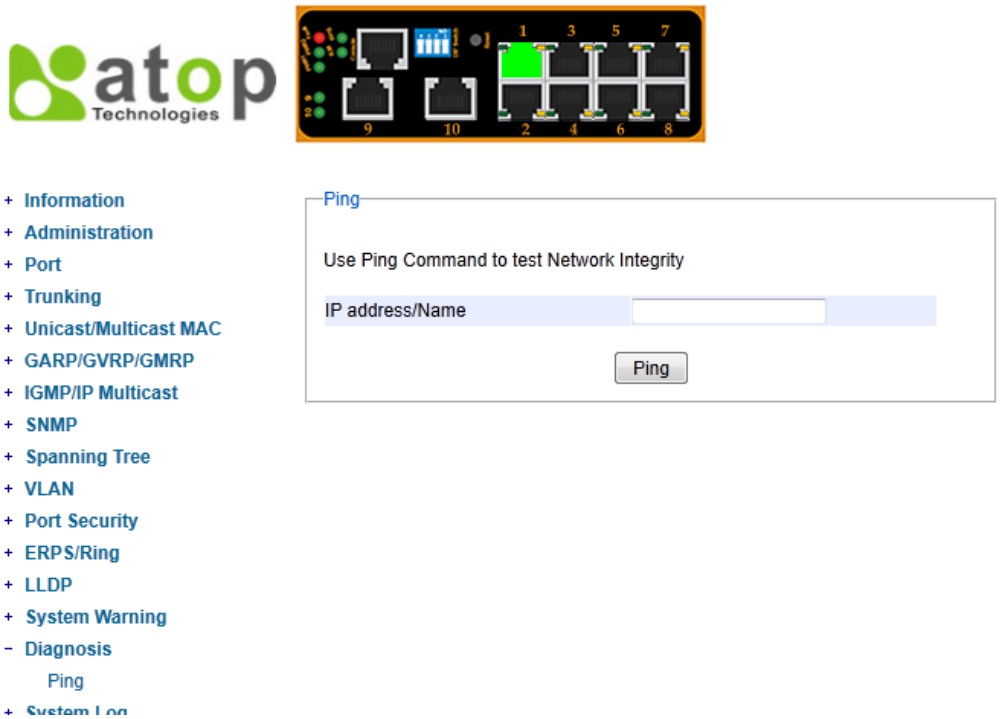


Fig. 2.75.a

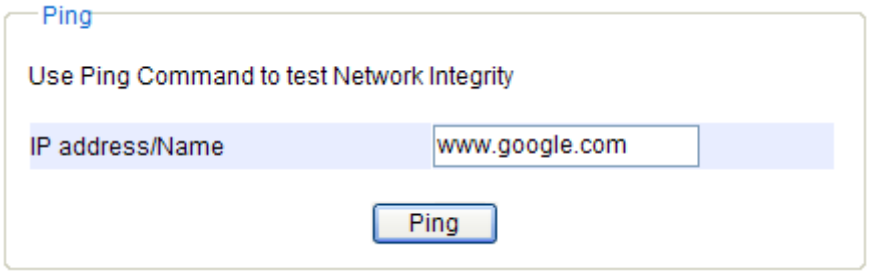


Fig. 2.75.b

Users can assign IP address or domain name to verify the network connectivity. After typing the IP address/name, please click Ping button to start the ping function; an example is shown below.

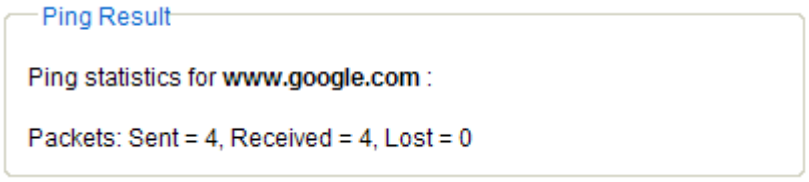


Fig. 2.75.c

Users will have the following result for a failed ping.

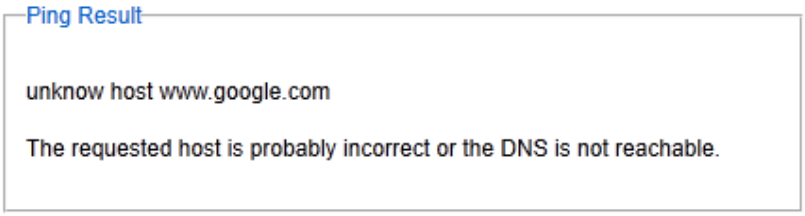


Fig. 2.75.d

***Note:**

If users assign domain name instead of IP address, they should assign DNS* first. This can be done through **Administration** > IP Settings. An example is shown below.

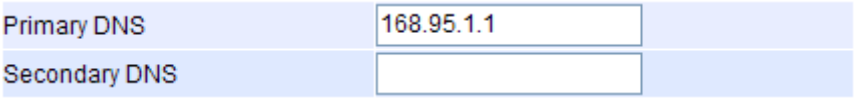


Fig. 2.76

2.17 System Log

This function contains two pages, Syslog and Event Log.

2.17.1 Syslog

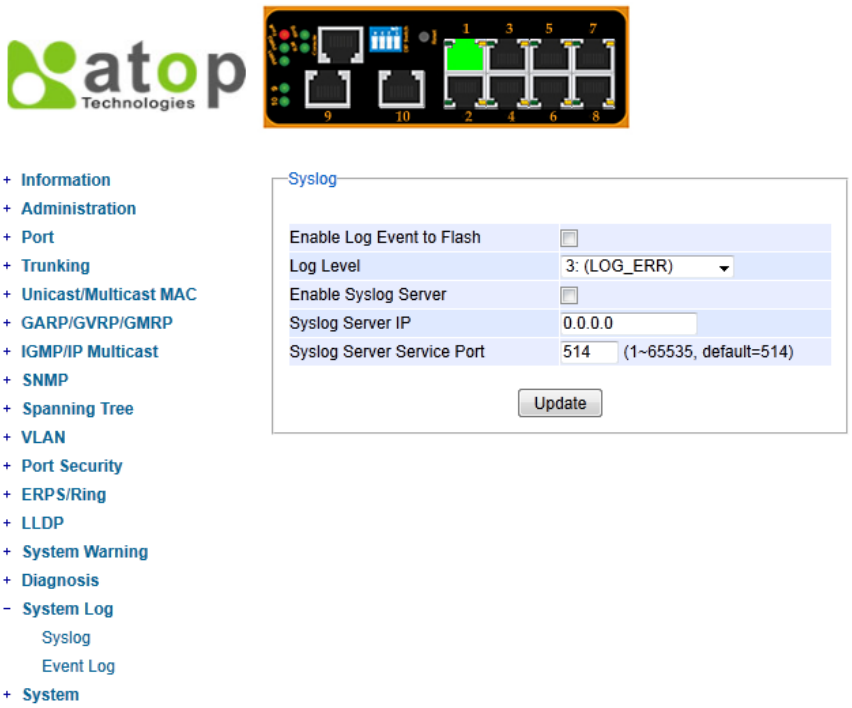


Fig. 2.77

Fig. 2.77 shows Syslog related settings configuration. The actual log event recorded will be showed in **Event Log** on next page.

Table 2.57

Label	Description	Factory Default
Enable Log Event to Flash	**Checked**: Saving log event into flash memory. The flash memory can keep the log event files even if the switch is rebooted. **Unchecked**: Saving log event into RAM memory. The RAM memory cannot keep the log event files after each reboot.	Uncheck
Log Level	Set the log level to determine what events to be displayed on the next page (**Event Log**). Level selected is inclusive. For example, if 3 :(Log_ERR) is selected, all 0, 1 , 2 and 3 levels will be implied.	3: (LOG_ERR)
Enable Syslog Server	**Checked**: Enable Syslog Server. **Uncheck**: Disable Syslog Server. If enabled, all log events recorded will be sent to the remote Syslog server.	Uncheck
Syslog Server IP	Set the IP address of Syslog server	0.0.0.0
Syslog Server Service Port	Set the service port number of Syslog server	514

2.17.2 Event Log

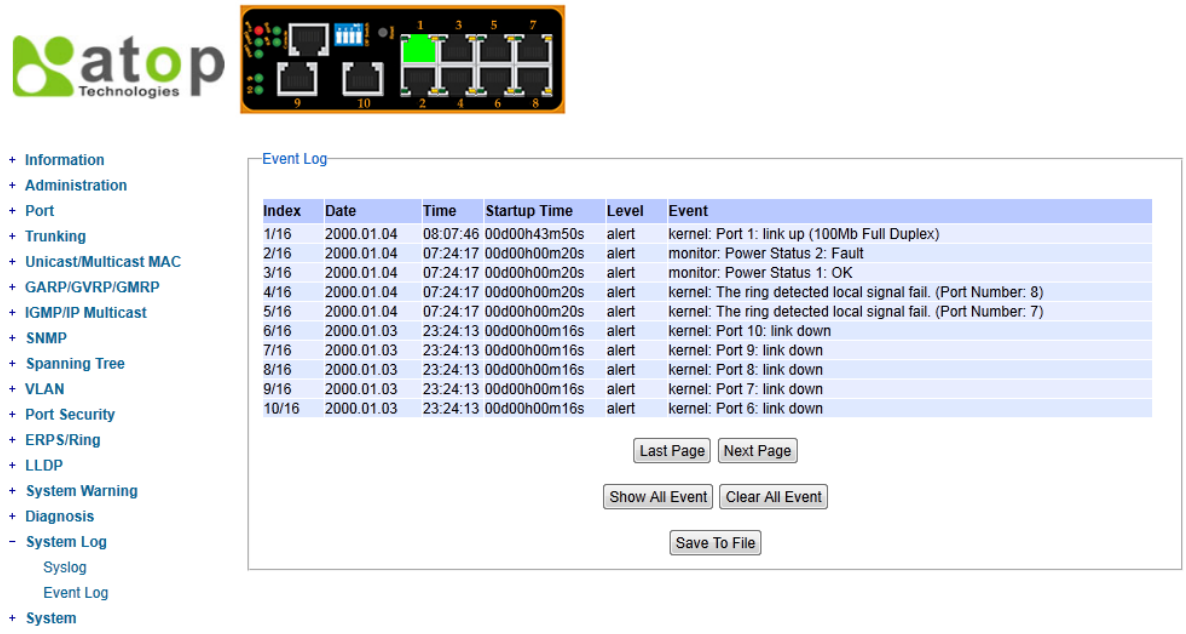


Fig. 2.78

Fig. 2.78 is an example of all of the events logs; they are sorted by date and time.

Table 2.58

Label	Description
Index	Indicates the index of a particular log event.
Date	Indicates the system date of this event has occurred.
Time	Indicates the system time of this event has occurred.
Startup Time	Indicates how long the system has been up since this event occurred.
Level	Indicates the level of this event.
Event	Details description of this event.
Last Page	Displays events on the last page.
Next Page	Next page.
Show All Event	Click to display all events.
Clear All Event	Click to clear all events

2.18 System

This function includes the following:

- **Backup/restore**
- **Firmware upgrade**
- **TFTP**
- **Factory default**
- **Reboot**

2.18.1 Backup/Restore

Backup: Download the current EH7510 configuration to the computer as well as save it.

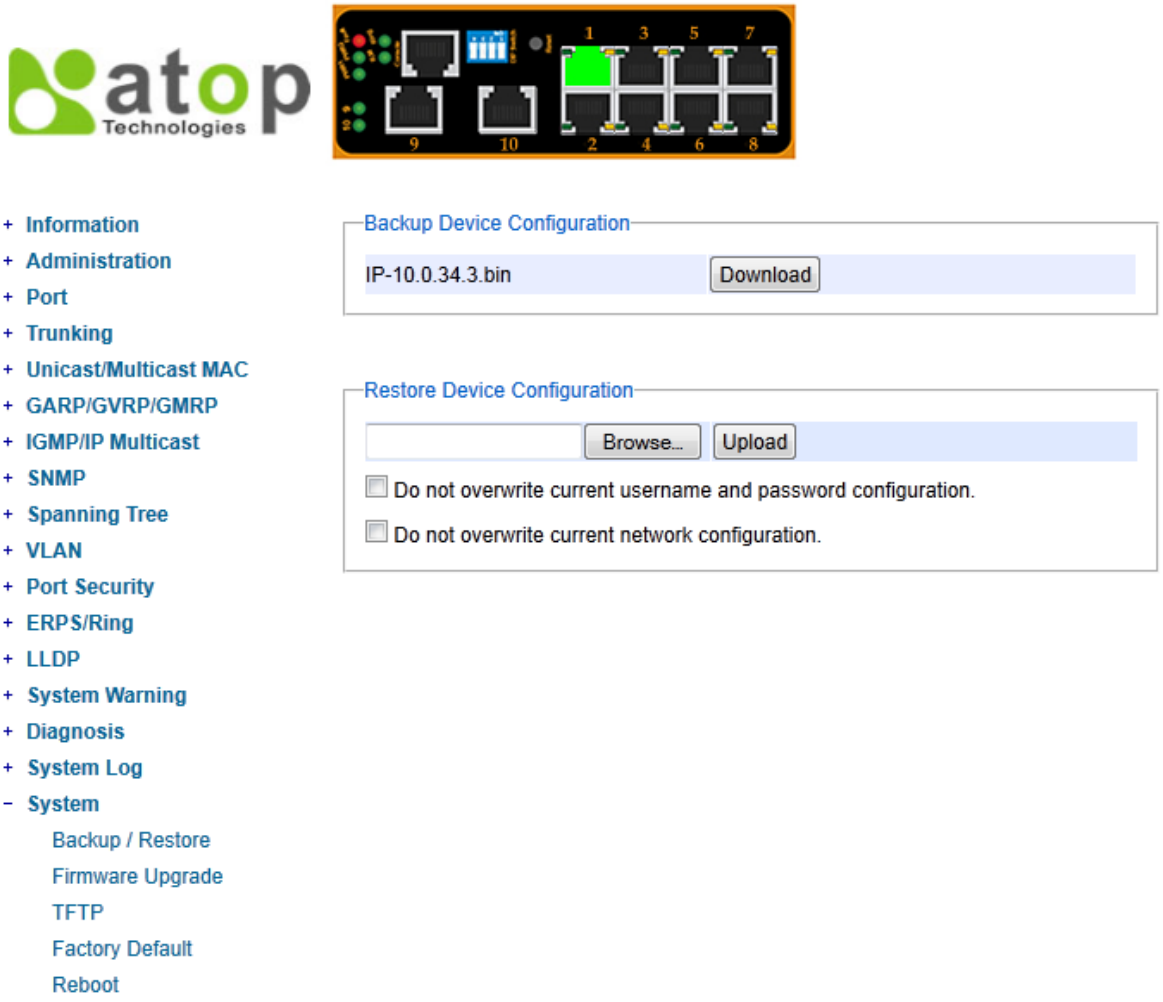


Fig. 2.79

Restore: Upload EH7510 configuration to EH7510 unit from the computer, it will replace the older configuration on EH7510.

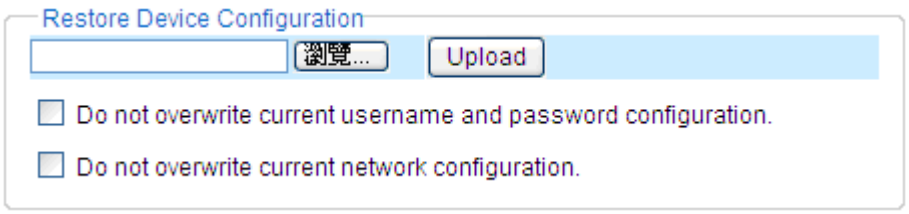


Fig. 2.80

***Notes:**

There're two options which can store the username, password or network configuration, it will prevent the user who can't login due to a different username, password or network configuration after settings are restored!

2.18.2 Firmware Upgrade

Select EH7510 firmware from the computer, and upgrade it via web interface.

Fig. 2.81

2.18.3 TFTP

Trivial **F**ile **T**ransfer **P**rotocol. This protocol is designed to be small and easy to implement. EH7510 allows users to upload configuration settings to a TFTP server, and users can also download these settings when needed from the server.

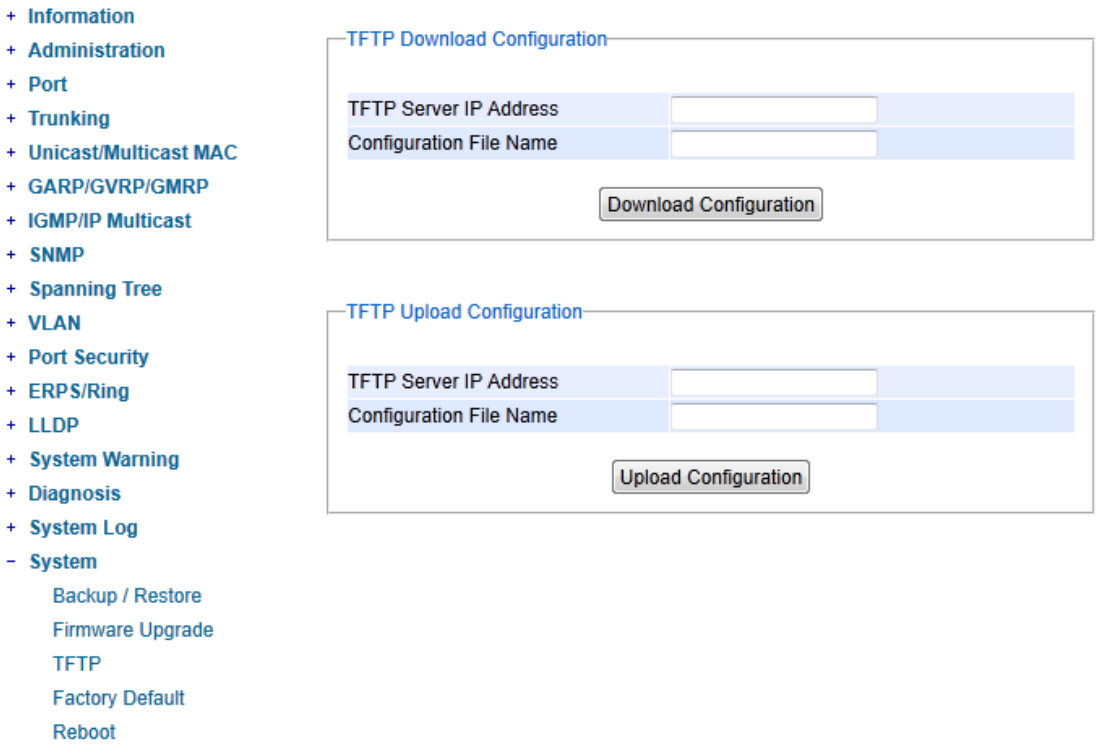


Fig. 2.82.a

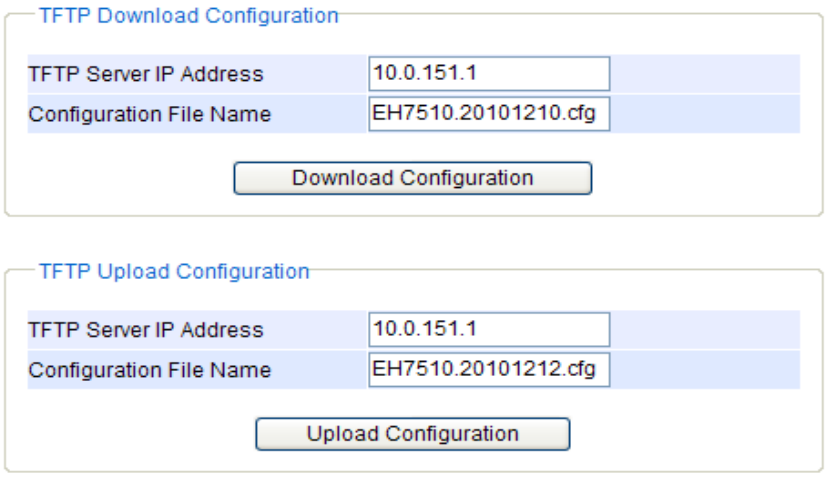


Fig. 2.82.b

This selection allows users to save the current configuration file to a remote TFTP server, or replace download a configuration setting which already exits from a TFTP server.

Table 2.59

Label	Description	Factory Default
TFTP Server IP Address	Sets the IP address or remote TFTP server domain name.	NULL
Configuration File Name	Type in the name of the file to be uploaded or downloaded.	NULL
Download Configuration	Click to start download remote configuration into Switch.	-
Upload Configuration	Click to start upload Switch configuration to remote TFTP server.	-

2.18.4 Factory Default

Users can reset EH7510 to default factory settings by clicking **Reset**.

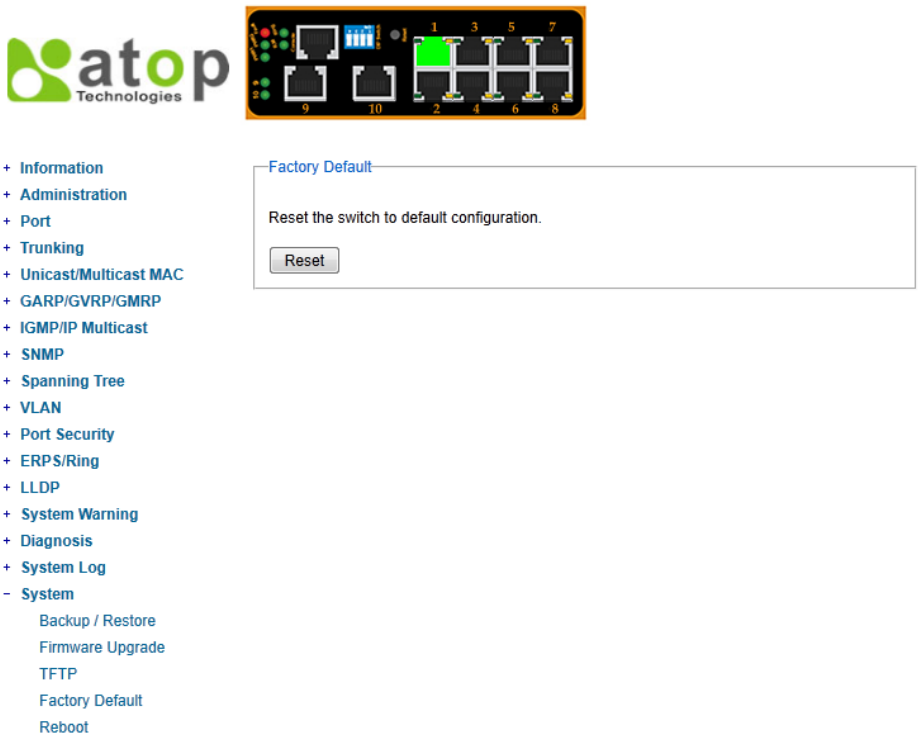


Fig. 2.83

2.18.5 Reboot

EH7510 provides an easy reboot function that only requires one click.

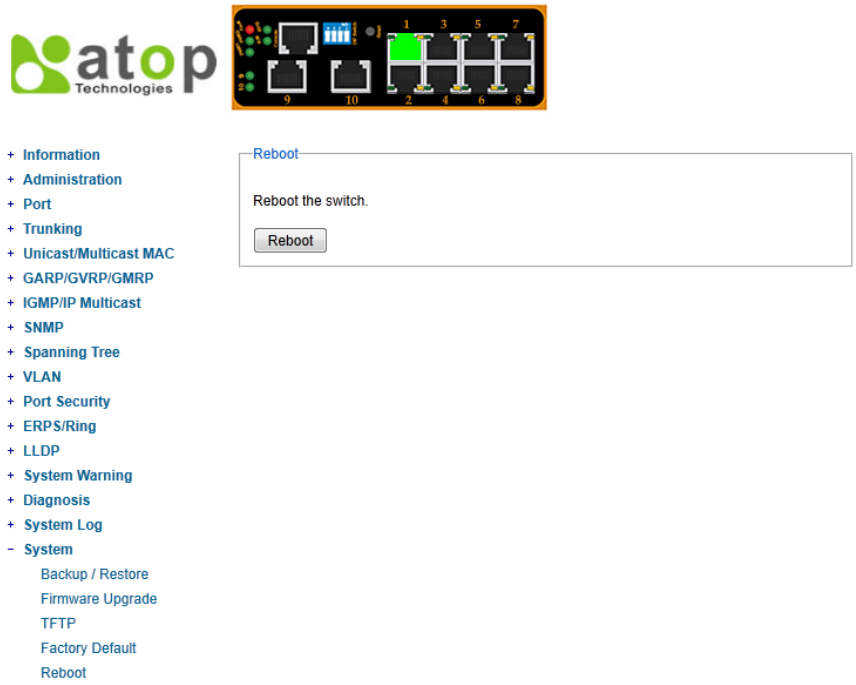


Fig. 2.84

Chapter 3: Configuring with a Serial Console

EH7510 switch can also be configured by using serial console; this method is similar to the web browser one. The options are the same, so users can take the same procedures as those examples in Chapter 2.

3.1 Serial Console Setup

After users install **Tera Term**, perform the following steps to access the serial console utility.

1. Start **Tera Term**. In **New Connection** window, select **serial** and appropriate port.

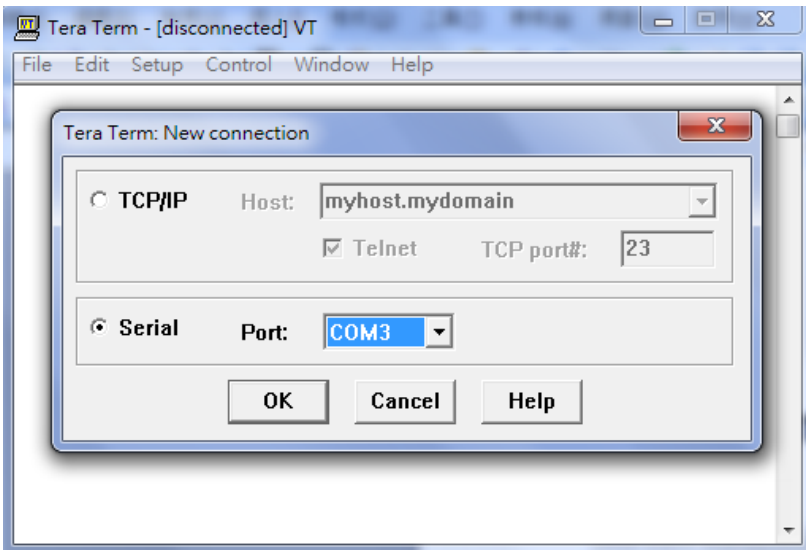


Fig. 3.1

2. Click **Setup** -> **Serial Port**.

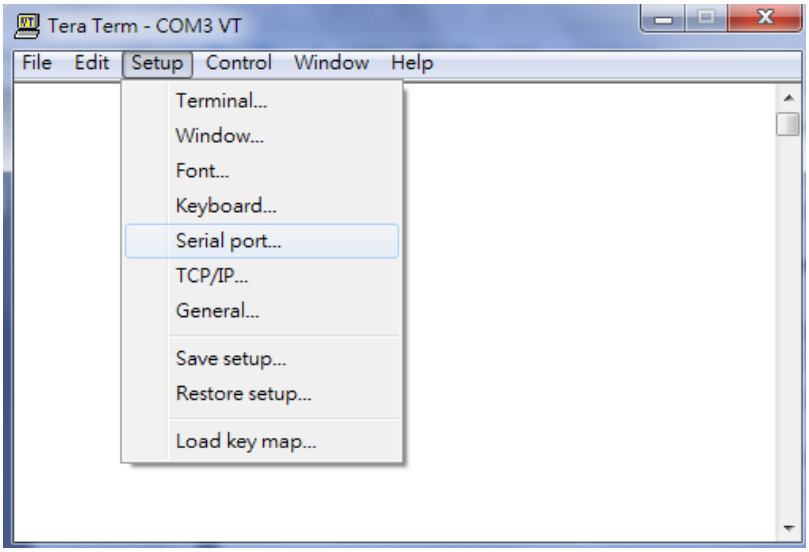


Fig. 3.2

3. The **Serial Port Setup** window pops up. Select appropriate port for **Port**, **115200** for **Baud Rate**, **8 bit** for **Data**, **none** for **Parity**, and **1 bit** for **Stop**.

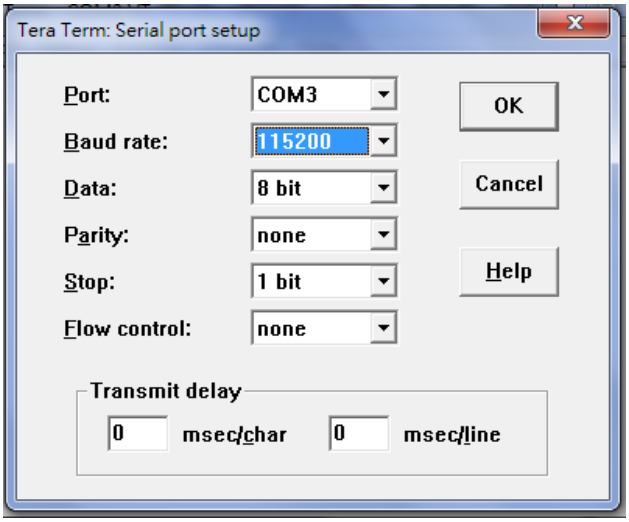


Fig. 3.3

4. After finishing settings and clicking **OK**, a **Command Line Interface** (**CLI**) will be brought up.

3.2 Command Line Interface Introduction

The Command Line Interface supports two types of privileges, which are operator and manager privileges. Users with operator privileges may only view the information; while those with manager privileges are allowed to view information and configure settings. Operator and manager privileges are initially entered without the need of passwords, but a user may assign password to both the operator and manager. If passwords are assigned, then when a user attempts to enter the CLI next time, they will need to enter the correct username and password.

If users enter the password for the operator, then the prompt changes to indicate operator privilege. Users are now in the “user” mode:

Switch>

If users enter the password for the operator, then the prompt changes to indicate manger privilege. Users are now in the “privileged” mode:

Switch#

If users are in the user mode and want to switch to the privileged mode, they may simply type in the command “**enable**” and then enter the correct username and password following the prompt:

Switch> ***enable***

Username: ***(enter username here)***

Password: ***(enter password here)***

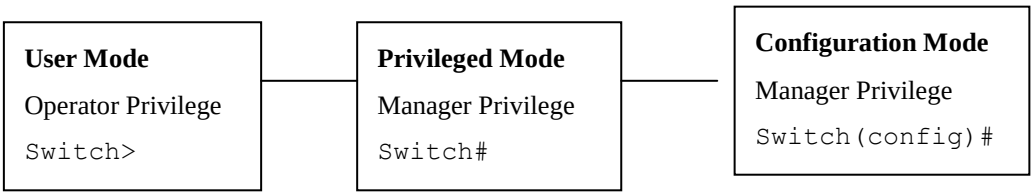
Switch#

To enter the “configuration” mode, you need to be in the privileged mode, and then type in the command “**configure**”:

Switch# ***configure***

Switch(config)#

Below is a graphical view of the modes and its related privileges and screen prompt:



Users may enter “***?***” at any command mode and the CLI will return possible commands at that point, along with some description of the keywords:

Switch(config)# ***ip ?***

address Set IP address and subnet mask

default-gateway Set default gateway IP address

dns Set DNS IP address

Users may use the <Tab> key to do keyword auto completion:

Switch(config)# ***syst*** <***Tab***>

Switch(config)# ***system***

3.3 General Command

The table below shows some useful commands that may be used anytime when using serial console.

Table 3.1

Command	Description
Enable	Turn on privileged mode.
Disable	Turn off privileged mode.
Configure	Enter configuration mode.
?	List all available options.
Exit	Go back to previous menu.
Help	Show any available helpful information.
Logout	Log out of CLI
history <0~256>	Set the number of command to remember as history Ex: *history 5* : memorize 5 previous commends.
No history	Disable command history
Show history	List last history commands
Hostname <string>	Set switch name.
no hostname	Reset the switch name to factory default setting.
[**no**] **password** <**manager** | **operator** | **all**>	Set or remove username and password for manager or operator. The manager username and password are also used by the web user interface (web browser method of configuration).

3.4 Command Example

Serial console method is available to make any configuration just like the web browser method; these two methods have similar functionalities. The picture below shows all the options on CLI. Two examples of making configurations, **Administration** and **Spanning Tree**, are shown in following sub-sections; configurations are the same as explained in Chapter 2 by using web browser, but the only difference is that we're using a serial console this time.

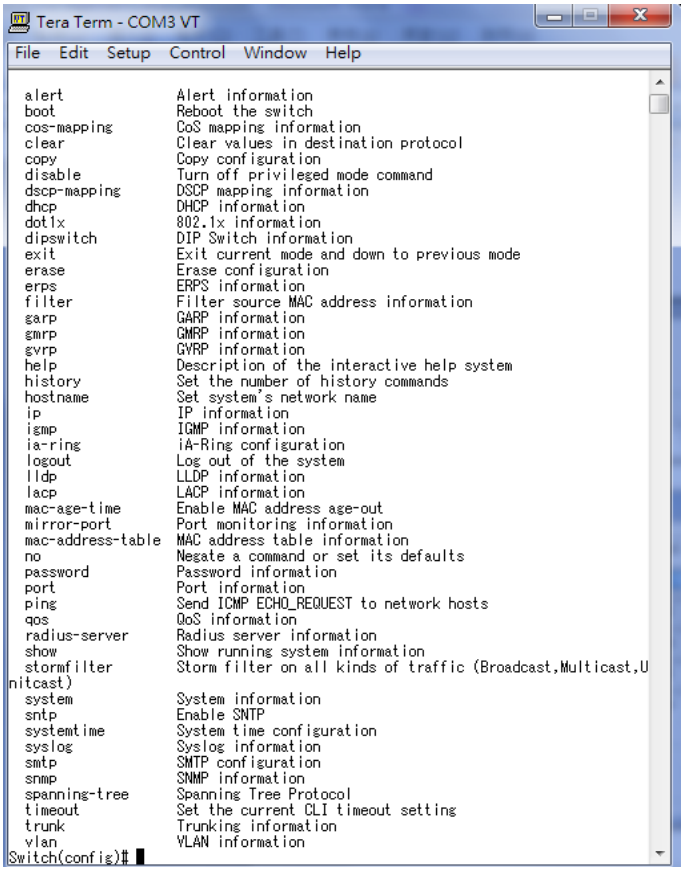


Fig. 3.4

3.4.1 Administration Setup using Serial Console

This section shows how users can see administration information and make changes using command. Detailed explanations of each technical term can be found in Chapter 2 of this manual.

Table 3.2

Command	Description
sntp <IP-add> <before-utc | after-utc> <0 ~ 24 hours>	Starts SNTP service.
[no] dhcp	Enable or disable DHCP.
show dhcp	Shows DHCP status.
ip address<ip-addr> <ip-mask>	Set IP address and subnet mask.
Ip default-gateway <ip-addr>	Set the gateway IP address
show ip	Show IP address, subnet mask, and the default gateway.
Boot	Use this command to reboot the switch.
Show running-config	Display the running configurations of the switch.
copy running-config startup-config	Backup the switch configurations.
erase startup-config	Reset to default factory settings at next boot time.
Show arp	Show the IP ARP translation table.
Ping ip-addr <1~999>	Send ICMP Echo-Request to network host. <1 ~ 999> specifies the number of repetitions.
Exec	Switch to shell mode. Shell mode may do shell command.

3.4.2 Spanning Tree Setup using Serial Console

This section shows how users can see spanning tree information and make changes using command. Detailed explanations of each technical term can be found in Chapter 2 of this manual.

Table 3.3

Command	Description
[no] spanning-tree	Enable/disable spanning-tree.
Spanning-tree forward-dalay<11~30>	Set the amount of forward delay in seconds. Ex: *spanning-tree forward-delay 20*: set forward delay time to be 20 seconds.
Spanning-tree hello-time<1~10>	Set hello time in seconds.
Spanning-tree maximum-age<6~40>	Set spanning tree maximum age in seconds.
Spanning-tree priority<0~61440>	Set spanning tree bridge priority.
Spanning-tree port path-cost <0 ~ 2E8><port #>	Set path cost to specific port.
Spanning-tree port priority <0 ~ 240><port #>	Set priority to specific port.
Show spanning-tree	Show spanning-tree information.
Show spanning-tree port <port #>	Show port information.
[no] spanning-tree debug	Enable or disable spanning tree debugging.
Spanning-tree protocol-version <stp/retp>	Choose protocol version. A detailed description of stp/rstp can be found in section **Spanning Tree** of chapter 2
[no] spanning-tree port mcheck <port#>	Force the port to transmit RST BPDU.
[no] spanning-tree port edge-port <port #>	Set the port to be edge connection.
[no] spanning-tree port non-stp <port#>	Enable or disable spanning tree protocol on this port.
[no] spanning-tree port point-to-point-mac <auto | true | false> <port #>	Set the port to be point to point connection. Auto: specifies point to point link auto detection. True: set the point to point link to true. False: set the link to false.

Chapter 4: SwitchView & Topolog Diagram

SwitchView and Topolog Diagram are interfaces developed by Atop Technology; instead of providing detailed descriptions for a specific device, SwitchView and Topolog Diagram have information for all devices in the network. SwitchView allows users to locate, upgrade, or reboot devices, and Topolog Diagram shows how all managed switches in the network are connected; this chapter illustrates how these two tools can be used effectively.

4.1 SwitchView

SwitchView shows Model name, IP address, MAC address and other information of devices in the network; the window is shown below.

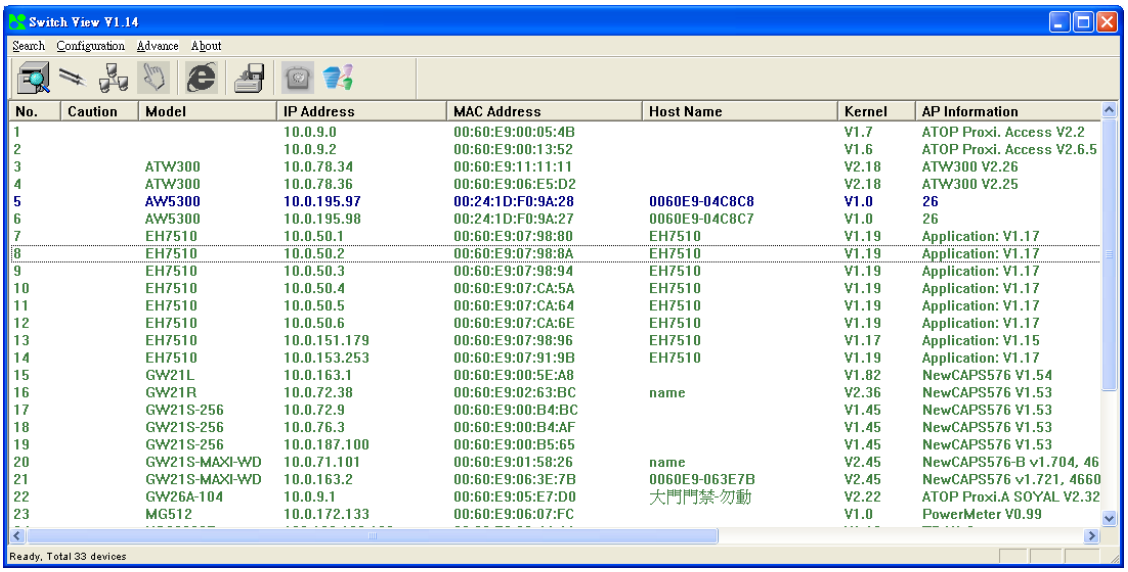


Fig. 4.1

Table 4.1

Label/Icons	Description
	Search devices again with current search condition.
	Ping a device in the network.
	Configure network settings.
	Locate a device. Device beeps if selected.
	Open a web browser for configuration for selected device.
	Upgrade application of kernel firmware version from local disk.
	Open Telnet for configuration for selected device.
	Open “Topology Diagram” utility to see the switches topology.

4.2 Firmware Upgrade

As addressed in 2.14.1, EH7510 can be upgraded by using SwitchView; there are kernel firmwares and application firmwares to be updated; this can be done easily in 3 steps.

1. In SwitchView, click on 

2. Choose either Kernel of AP (application) firmware, and find your upgrade file in your local disk. Then click **Upgrade**.

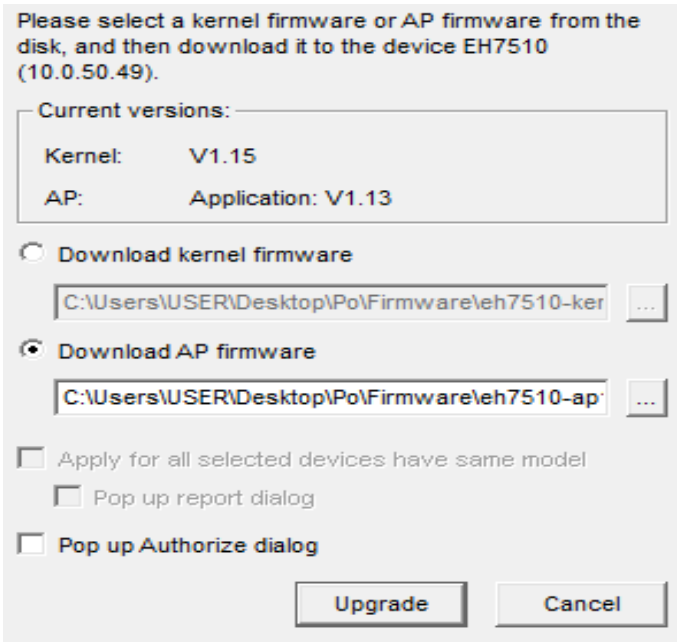


Fig. 4.2

3. After users confirm, SwitchView will start its download process.

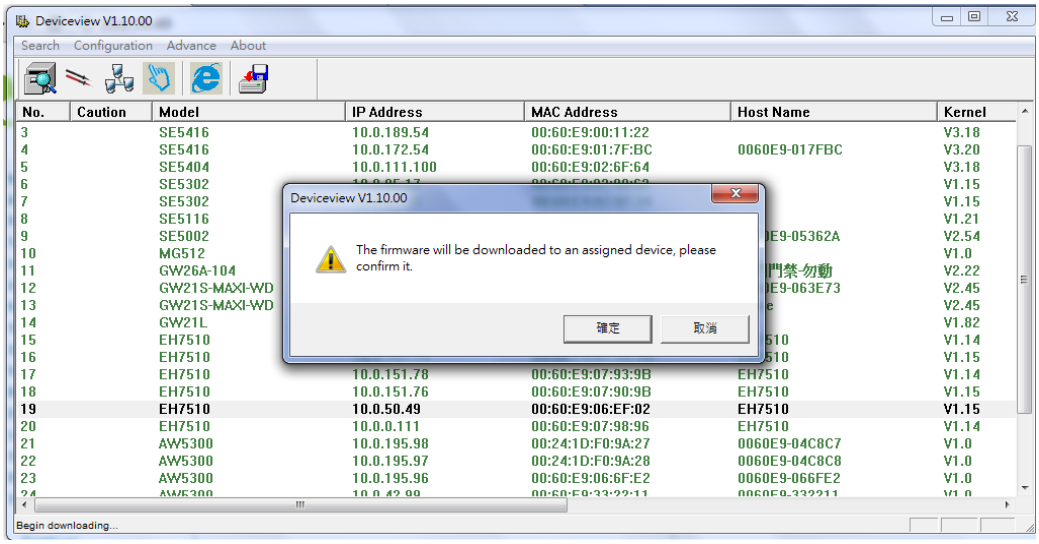


Fig. 4.3

After the application firmware is updated, the web browser interface will be the newest version to show the most updated functionalities.

4.3 Topology Diagram

Topolog Diagram is a software developed by Atop to help users visualize how devices are connected to the network. As of version 1.0.0, Topolog Diagram is mainly designed for managed switches; all other devices will be tagged as unknown. This tool shows the MAC and IP address of a device, and shows which ports of this device are connected to other devices; right click on a specific EH7510 to open and view its configuration.

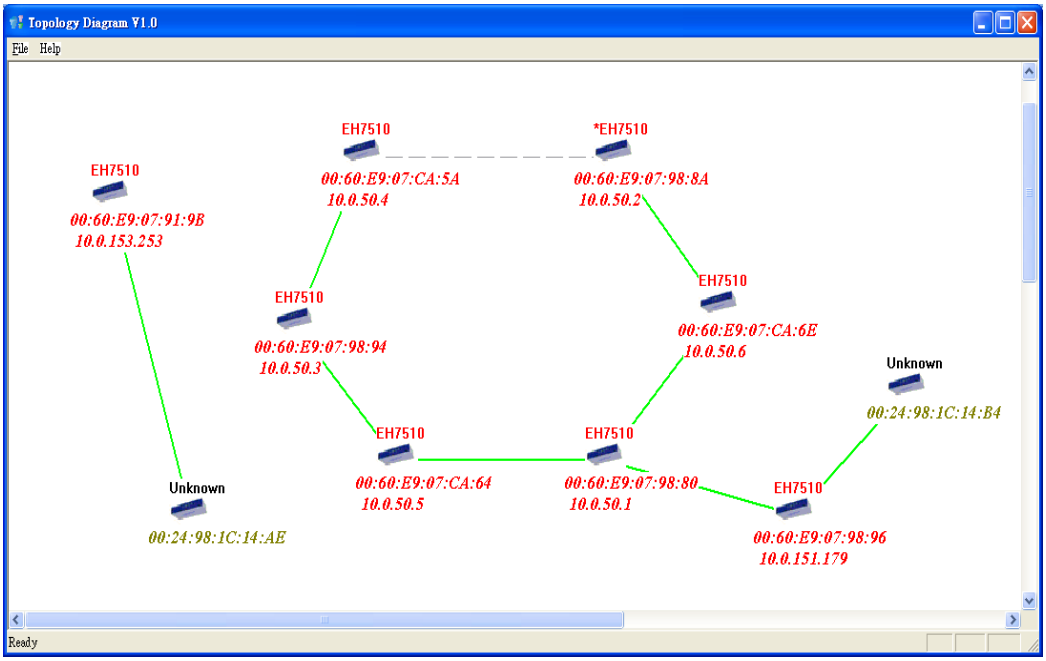


Fig. 4.4

Notes:

1. *** means the device is a Ring Master or RPL Owner.**
2. **Means this path is blocked.**
3. **Right click the device icon to show more port link details.**
4. **When double clicking the device icon, a periodic beep will sound .**
5. **Left click the device icon to launch the device's web.**

Appendix A. ModBus Management Memory Map

1. Read Registers (Support Function Code 3, 4).
2. Write Register (Support Function Code 6).
3. 1 Word = 2 Bytes.

Address	Data Type	Read/Write	Description
System Information			
0x0000 (0)	32 words	R	System Description = "Managed Switch EH7510" Word 0 Hi byte = 'M' Word 0 Lo byte = 'a' Word 1 Hi byte = 'n' Word 1 Lo byte = 'a' Word 2 Hi byte = 'g' Word 2 Lo byte = 'e' Word 3 Hi byte = 'd' Word 3 Lo byte = ' ' Word 4 Hi byte = 'S' Word 4 Lo byte = 'w' Word 5 Hi byte = 'i' Word 5 Lo byte = 't' Word 6 Hi byte = 'c' Word 6 Lo byte = 'h' Word 7 Hi byte = ' ' Word 7 Lo byte = 'E' Word 8 Hi byte = 'H' Word 8 Lo byte = '7' Word 9 Hi byte = '5' Word 9 Lo byte = '1' Word 10 Hi byte = '0' Word 10 Lo byte = '\0'
0x0020 (32)	1 word	R	Firmware Version = Ex: Version = 1.02 Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x02
0x0021 (33)	3 words	R	Ethernet MAC Address Ex: MAC = 00-01-02-03-04-05 Word 0 Hi byte = 0x00 Word 0 Lo byte = 0x01 Word 1 Hi byte = 0x02 Word 1 Lo byte = 0x03 Word 2 Hi byte = 0x04 Word 2 Lo byte = 0x05
0x0024 (36)	1 word	R	Kernel Version Ex: Version = 1.03 Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x03

Console Information			
0x0030 (48)	1 word	R	Baud Rate 0x0000: 4800 0x0001: 9600 0x0002: 14400 0x0003: 19200 0x0004: 28800 0x0005: 38400 0x0006: 57600 0x0007: 144000 0x0008: 115200
0x0031 (49)	1 word	R	Data Bits 0x0007: 7 0x0008: 8
0x0032 (50)	1 word	R	Parity 0x0000: None 0x0001: Odd 0x0002: Even
0x0033 (51)	1 word	R	Stop Bit 0x0001: 1 0x0002: 2
0x0034 (52)	1 word	R	Flow Control 0x0000: None
Power Information			
0x0040 (64)	1 word	R	Power Status Power 1 OK, Hi byte = 0x01 Power 1 Fail, Hi byte = 0x00 Power 2 OK, Low byte = 0x01 Power 2 Fail, Low byte = 0x00
IP Information			
0x0050 (80)	1 word	R	DHCP Status 0x0000: Disabled 0x0001: Enabled
0x0051 (81)	2 words	R	IP Address of switch Ex: IP = 192.168.1.1 Word 0 Hi byte = 0xC0 Word 0 Lo byte = 0xA8 Word 1 Hi byte = 0x01 Word 1 Lo byte = 0x01
0x0053 (83)	2 words	R	Subnet Mask of switch Ex: IP = 255.255.255.0 Word 0 Hi byte = 0xFF Word 0 Lo byte = 0xFF Word 1 Hi byte = 0xFF Word 1 Lo byte = 0x00

0x0055 (85)	2 words	R	Gateway Address of switch Ex: IP = 192.168.1.254 Word 0 Hi byte = 0xC0 Word 0 Lo byte = 0xA8 Word 1 Hi byte = 0x01 Word 1 Lo byte = 0xFE
0x0057 (87)	2 words	R	DNS1 of switch Ex: IP = 168.95.1.1 Word 0 Hi byte = 0xA8 Word 0 Lo byte = 0x5F Word 1 Hi byte = 0x01 Word 1 Lo byte = 0x01
0x0059 (89)	2 words	R	DNS2 of switch Ex: IP = 168.95.1.1 Word 0 Hi byte = 0xA8 Word 0 Lo byte = 0x5F Word 1 Hi byte = 0x01 Word 1 Lo byte = 0x01
System Status Clear			
0x0100 (256)	1 word	W	Clear Port Statistics 0x0001: Do clear action
0x0101 (257)	1 word	W	Clear Relay Alarm 0x0001: Do clear action
0x0102 (258)	1 word	W	Clear All Warning Events 0x0001: Do clear action
Warning Events Information			
0x0200 (512)	64 words	R	1st Warning Event Information
0x0300 (768)	64 words	R	2st Warning Event Information
0x0400 (1024)	64 words	R	3st Warning Event Information
0x0500 (1280)	64 words	R	4st Warning Event Information
0x0600 (1536)	64 words	R	5st Warning Event Information
Port Status			
0x1000 (4096)	5 words	R	Port Status 0x0000: Disabled 0x0001: Enabled Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status

0x1020 (4128)	5 words	R	Port Negotiation Status, force = 0x00 Status, auto = 0x01 Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status
0x1040 (4160)	5 words	R	Port Speed Status, 10M = 0x01 Status, 100M = 0x02 Status, 1000M = 0x03 Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status
0x1060 (4192)	5 words	R	Port Duplex Status, half-duplex = 0x00 Status, full-duplex = 0x01 Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status
0x1080 (4224)	5 words	R	Port Flow Control Status, disabled = 0x00 Status, enabled = 0x01 Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status

0x10A0 (4256)	5 words	R	Port Link Status Status, down = 0x00 Status, up = 0x01 Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status
0x1200 (4608)	20 words	R	Port TX rate Ex. Port 1 runs at TX Rate(1024 Kbps = 0x400). Word 0 of Port 1 = 0x0000 Word 1 of Port 1 = 0x0400 Word 0,1 = Port 1 TX Rate Word 2,3 = Port 2 TX Rate Word 4,5 = Port 3 TX Rate Word 6,7 = Port 4 TX Rate Word 8,9 = Port 5 TX Rate Word 10,11 = Port 6 TX Rate Word 12,13 = Port 7 TX Rate Word 14,15 = Port 8 TX Rate Word 16,17 = Port 9 TX Rate Word 18,19 = Port 10 TX Rate
0x1280 (4736)	20 words	R	Port RX rate Ex. Port 1 runs at RX Rate(1024 Kbps = 0x400). Word 0 of Port 1 = 0x0000 Word 1 of Port 1 = 0x0400 Word 0,1 = Port 1 RX Rate Word 2,3 = Port 2 RX Rate Word 4,5 = Port 3 RX Rate Word 6,7 = Port 4 RX Rate Word 8,9 = Port 5 RX Rate Word 10,11 = Port 6 RX Rate Word 12,13 = Port 7 RX Rate Word 14,15 = Port 8 RX Rate Word 16,17 = Port 9 RX Rate Word 18,19 = Port 10 RX Rate

0x1300 (4864)	40 words	R	Count of Good Packets of TX Ex. Port 1 gets 0x2EEEE1FFFF good packets of TX. Word 0 of Port 1 = 0x0000 Word 1 of Port 1 = 0x002E Word 2 of Port 1 = 0xEEE1 Word 3 of Port 1 = 0xFFFF Word 0,1,2,3 = Port 1 good packets Word 4,5,6,7 = Port 2 good packets Word 8,9,10,11 = Port 3 good packets Word 12,13,14,15 = Port 4 good packets Word 16,17,18,19 = Port 5 good packets Word 20,21,22,23 = Port 6 good packets Word 24,25,26,27 = Port 7 good packets Word 28,29,30,31 = Port 8 good packets Word 32,33,34,35 = Port 9 good packets Word 36,37,38,39 = Port 10 good packets
0x1400 (5120)	40 words	R	Count of Bad Packets of TX Ex. Port 1 gets 0x2EEEE1FFFF bad packets of TX. Word 0 of Port 1 = 0x0000 Word 1 of Port 1 = 0x002E Word 2 of Port 1 = 0xEEE1 Word 3 of Port 1 = 0xFFFF Word 0,1,2,3 = Port 1 good packets Word 4,5,6,7 = Port 2 good packets Word 8,9,10,11 = Port 3 good packets Word 12,13,14,15 = Port 4 good packets Word 16,17,18,19 = Port 5 good packets Word 20,21,22,23 = Port 6 good packets Word 24,25,26,27 = Port 7 good packets Word 28,29,30,31 = Port 8 good packets Word 32,33,34,35 = Port 9 good packets Word 36,37,38,39 = Port 10 good packets
0x1500 (5376)	40 words	R	Count of Good Packets of RX Ex. Port 1 gets 0x2EEEE1FFFF good packets of RX. Word 0 of Port 1 = 0x0000 Word 1 of Port 1 = 0x002E Word 2 of Port 1 = 0xEEE1 Word 3 of Port 1 = 0xFFFF Word 0,1,2,3 = Port 1 good packets Word 4,5,6,7 = Port 2 good packets Word 8,9,10,11 = Port 3 good packets Word 12,13,14,15 = Port 4 good packets Word 16,17,18,19 = Port 5 good packets Word 20,21,22,23 = Port 6 good packets Word 24,25,26,27 = Port 7 good packets Word 28,29,30,31 = Port 8 good packets Word 32,33,34,35 = Port 9 good packets Word 36,37,38,39 = Port 10 good packets

0x1600 (5632)	40 words	R	Count of Bad Packets of RX Ex. Port 1 gets 0x2EEEE1FFFF bad packets of RX. Word 0 of Port 1 = 0x0000 Word 1 of Port 1 = 0x002E Word 2 of Port 1 = 0xEEE1 Word 3 of Port 1 = 0xFFFF Word 0,1,2,3 = Port 1 good packets Word 4,5,6,7 = Port 2 good packets Word 8,9,10,11 = Port 3 good packets Word 12,13,14,15 = Port 4 good packets Word 16,17,18,19 = Port 5 good packets Word 20,21,22,23 = Port 6 good packets Word 24,25,26,27 = Port 7 good packets Word 28,29,30,31 = Port 8 good packets Word 32,33,34,35 = Port 9 good packets Word 36,37,38,39 = Port 10 good packets
Redundancy Information			
0x2000 (8192)	1 word	R	Redundancy Protocol 0x0000: None 0x0001: STP 0x0002: RSTP 0x0004: ERPS 0x0008: iA-Ring 0x0010: Compatible-Ring
0x2100 (8448)	1 word	R	STP Root 0x0000: Not Root 0x0001: Root 0xFFFF: RSTP not enable
0x2101 (8449)	5 words	R	STP Port Status 0x00: Disabled 0x01: Listening 0x02: Learning 0x03: Forwarding 0x04: Blocking 0x05: Discarding 0xFF: RSTP Not Enable Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status

0x2200 (8704)	5 words	R	ERPS R-APS VLAN ID of the ring Ex: 3st VLAN ID = 1, Word 2 = 0x0001 1~4094: ID Value range 0x0000: VLAN ID Not Setup Word 0 = 1st VLAN ID Word 1 = 2st VLAN ID Word 2 = 3st VLAN ID Word 3 = 4st VLAN ID Word 4 = 5st VLAN ID
0x2230 (8752)	5 words	R	ERPS West Port Ex: 3st West Port = Port 2, Word 2 = 0x0002 0x0001: Port 1 0x0002: Port 2 … 0x000A: Port 10 0x000C: Trk1 0x000D: Trk2 0x000E: Trk3 0x000F: Virtual Channel 0x00FF: VLAN ID exist but no West Port be Selected 0xFFFF: ERPS Not Enable Word 0 = 1st VLAN ID West Port Word 1 = 2st VLAN ID West Port Word 2 = 3st VLAN ID West Port Word 3 = 4st VLAN ID West Port Word 4 = 5st VLAN ID West Port
0x2240 (8768)	5 words	R	ERPS East Port Ex: 3st West Port = Port 3, Word 2 = 0x0003 0x0001: Port 1 0x0002: Port 2 … 0x000A: Port 10 0x000C: Trk1 0x000D: Trk2 0x000E: Trk3 0x000F: Virtual Channel 0x00FF: VLAN ID exist but no East Port be Selected 0xFFFF: ERPS Not Enable Word 0 = 1st VLAN ID East Port Word 1 = 2st VLAN ID East Port Word 2 = 3st VLAN ID East Port Word 3 = 4st VLAN ID East Port Word 4 = 5st VLAN ID East Port

0x2250 (8784)	5 words	R	ERPS West Port Status Ex: 3st West Port Status = Forwarding, Word 2 = 0x0001 0x0001: Forwarding 0x0002: Blocking 0x0003: Signal Fail Blocking 0x000F: Virtual Channel 0x00FF: VLAN ID exist but no West Port be Selected 0xFFFF: ERPS Not Enable Word 0 = 1st VLAN ID West Port Status Word 1 = 2st VLAN ID West Port Status Word 2 = 3st VLAN ID West Port Status Word 3 = 4st VLAN ID West Port Status Word 4 = 5st VLAN ID West Port Status
0x2260 (8800)	5 words	R	ERPS East Port Status Ex: 3st East Port Status = Blocking, Word 2 = 0x0002 0x0001: Forwarding 0x0002: Blocking 0x0003: Signal Fail Blocking 0x000F: Virtual Channel 0x00FF: VLAN ID exist but no Eest Port be Selected 0xFFFF: ERPS Not Enable Word 0 = 1st VLAN ID East Port Status Word 1 = 2st VLAN ID East Port Status Word 2 = 3st VLAN ID East Port Status Word 3 = 4st VLAN ID East Port Status Word 4 = 5st VLAN ID East Port Status
0x2270 (8816)	5 words	R	ERPS Node State Ex: 3st Node State = Protection, Word 2 = 0x0002 0x0001: None 0x0002: Idle 0x0003: Protection 0xFFFF: ERPS Not Enable Word 0 = 1st VLAN ID Node State Word 1 = 2st VLAN ID Node State Word 2 = 3st VLAN ID Node State Word 3 = 4st VLAN ID Node State Word 4 = 5st VLAN ID Node State
0x2280 (8832)	5 word	R	ERPS RPL Owner 0x0000: Disabled 0x0001: Enabled
0x2300 (8960)	1 word	R	iA-Ring Master Status 0x0000: Disabled 0x0001: Enabled 0xFFFF: iA-Ring not enable

0x2301 (8961)	1 word	R	1st Ring Port Ex: 1st Ring Port = Port 2, Word 0 = 0x0002 0x0001: Port 1 0x0002: Port 2 … 0x000A: Port 10 0xFFFF: iA-Ring not enable
0x2302 (8962)	1 word	R	2st Ring Port Ex: 2st Ring Port = Port 3, Word 0 = 0x0003 0x0001: Port 1 0x0002: Port 2 … 0x000A: Port 10 0xFFFF: iA-Ring not enable

Glossary

Term	Description
802.1	A working group of IEEE standards dealing with Local Area Network.
802.1p	Provides mechanism for implementing Quality of Service (QoS) at the Media Access Control Level (MAC).
802.1x	IEEE standard for port-based Network-Access Control; provides an authentication mechanism to devices wishing to attach to a LAN or WLAN
Broadcast	Broadcasts are packets to all station of a local network.
Client	Devices that use services provided by other participants in the network.
DES	**D**ata **E**ncryption **S**tnadard; a block cipher that uses shared secret encryption. It's based on a symmetric-key algorithm that uses a 56-bit key.
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol; allows a computer to be configured automatically, eliminating the need for intervention by a network administrator. It also prevents two computers from being configured with the same IP address automatically. There are two versions of DHCP; one for IPv4 and one for IPv6.
DNS	**D**omain **N**ame **S**ystem; a hierarchical naming system built for any computers or resources connected to the Internet. It maps domain names into numerical identifiers. For example, the domain name www.google.com translates to the address 74.125.153.104.
EAP	**E**xtensible **A**uthentication **P**rotocol; an authentication framework widely used by IEEE.
Ethernet	Star-formed physical transport medium; all stations can send data simultaneously; collisions are detected and corrected through network protocols.
Gateway	Provides access to other network components on a layer of the OSI model; packets not going to a local partner are sent to the gateway. The gateway takes care of communication with remote network.
IEEE	Institute of Electrical and Electronics Engineers.
IGMP	**I**nternet **G**roup **M**anagement **P**rotocol; used on IPv4 networks for establishing multicast group memberships.
IP	Internet Protocol
IPv4	**I**nternet **P**rotocol **v**ersion **4**; fourth revision of the Internet Protocol. Together with IPv6, it is the core of internet network. It uses 32-bit addresses, which means there are only 2^32 possible unique addresses. Because of this limitation, an IPv4 addresses shortage has been developing. This has stimulated the development of IPv6, which is still in its early stage of development.
LAN	Local Area Network. Network that connects devices in a limited geographical area such as company or computer lab.
MAC	Media Access Control. A sub-layer of the Data Link Layer specified in the OSI model. It provides addressing and channel access control mechanisms to allow network nodes to communicate within a LAN.
MAC Address	A unique identifier assigned to network interfaces for communications on network segment. Formed according to the rules of numbering name space managed by IEEE.
MD5	Message-Digest algorithm 5; widely used cryptographic has function with a 128-bit hash value.
Multicast	This type of transmission sends messages from one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive the multicast. Also, networks that support multicast send only one copy of the information across the network until the delivery path that reaches group members diverges. At these diverges points, multicast packets will be copied and forwarded. This method can manage high volume of traffic with different destinations while using network bandwidth efficiently.

OSI Model	**O**pen **S**ystem **I**nterconnection mode; a way of sub-dividing a communication system into smaller parts called layers. A layer is a collection of conceptually similar functions that provide services to the layer above it and receives services from the layer below it.
QoS	Quality of Service.
RADIUS	**R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice. Authentication and monitoring protocol on the application level for authentication, integrity protection and accounting for network access.
Server`	Devices that provide services over the network.
SMTP	**S**imple **M**ail **T**transfer **P**rotocal (**SMTP**); an internet standard for email transmission across IP network.
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol is a protocol for managing devices on IP networks. It exposes management data in the form of variables on the managed systems, which describe the system configuration.