Industrial Managed Ethernet Switch

User's Manual

Series covered by this manual:
XEG7504, XEG7506, XEG7508, XEG7512, XEG7512,
XEG7520, XEG9512, XEG9508, XEM8508, XEM8510
XE7506*, XE7508*, XE7512*, XE7516*, XE7520*

* The user interface on these products may be slightly different from the one shown on this user manual

Version 1.2

June 2016

Tel: +44 121 809 8855
www.agatel.co.uk

Important Announcement

The information contained in this document is the property of Agatel Ethernet Switching. and is supplied for the sole purpose of operation and maintenance of Agatel Ethernet Switching 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 Agatel Ethernet Switching.

Published by

Agatel-Reliable Secure Connectivity.

Agatel Ltd

1st Floor, Apex House
Calthorpe Road, Edgbaston
Birmingham B15 1TR
United Kingdom

Tel: +44 121 809 8855
E-mail: info@agatel.co.uk
Website: www.agatel.co.uk

Copyright © 2016 Agatel Ethernet Switching. All rights reserved.
All other product names referenced herein are registered trademarks of their respective companies.

Table of Contents

1 Introduction 2

1.1 Introduction to Industrial Managed Switch 2

1.2 Software Features 3

2 Configuring with a Web Browser 4

2.1 Web-based Management Basics 4

2.1.1 Default Settings 4

2.1.2 Login Process and Main Window Interface 5

2.2 Basic Information 6

2.2.1 Sys Info 6

2.2.2 Dev Info Setting 7

2.2.3 Console Setting 8

2.2.4 Protocols Status 9

2.2.5 Power Status 10

2.2.6 Temperature Log 10

2.3 Administration 12

2.3.1 Password 12

2.3.2 IP Setting 15

2.3.3 IPv6 Setting 16

2.3.4 Ping 17

2.3.5 Ping6 18

2.3.6 Mirror Port 19

2.3.7 System Time 20

2.3.8 Modbus Setting 21

2.3.9 PTP 29

2.3.9.1 PTP Setting 29

2.3.9.2 H/W PTP Setting 32

2.3.10 SSH 32

2.3.11 Telnet 33

2.3.12 DIP Switch 34

2.4 Forwarding 35

2.4.1 QoS 35

2.4.1.1 QoS Setting 36

2.4.1.2 CoS Queue Mapping 38

2.4.1.3 DSCP Mapping 39
2.4.2 Rate Control 40
2.4.3 Strom Control 42
2.5 Port 44
2.5.1 Port Setting 44
2.5.2 Port Status 46
2.5.3 Mini-GBIC Port Status 47
2.5.4 Port Statistics 47
2.6 Power over Ethernet 49
2.6.1 PoE Setting 49
2.6.2 PoE Status 50
2.6.3 PoE Alarm Setting 51
2.7 Trunking 53
2.7.1 Trunking Setting 53
2.7.2 LACP Status 55
2.8 Unicast/Multicast MAC 57
2.8.1 Add Static MAC 58
2.8.2 Black-List MAC 59
2.8.3 MAC Aging Time 60
2.8.4 MAC Table 60
2.9 GARP/GVRP/GMRP 62
2.9.1 Multicast Group Table 63
2.9.2 GARP Setting 63
2.9.1 GVRP Setting 64
2.9.2 GMRP Setting 65
2.10 IP Multicast 67
2.10.1 IGMP 68
2.10.1.1 IGMP Settings 68
2.10.1.2 IGMP IP Multicast Table 69
2.10.1.3 IGMP Statistics 70
2.10.2 Static IP Multicast 72
2.11 SNMP 74
2.11.1 SNMP Agent 75
2.11.2 SNMP V1/V2c Community Setting 76
2.11.3 Trap Setting 76
2.11.4 SNMPv3 Auth. Setting 77
2.12 Spanning Tree 79

2.12.1 Spanning Tree Setting 80
2.12.2 Bridge Info 83
2.12.3 Port Setting 84
2.12.4 MSTP Instance 86
2.13 VLAN 88
2.13.1 VLAN Setting 89
2.13.2 802.1Q VLAN 90
2.13.2.1 802.1Q VLAN Settings 91
2.13.2.2 802.1Q VLAN PVID Settings 92
2.13.2.3 802.1Q VLAN Table 93
2.13.3 Port-Based VLAN 94
2.13.4 MAC-Based VLAN 95
2.13.5 IP Subnet-Based VLAN 96
2.13.6 Protocol-Based VLAN 96
2.13.6.1 Protocol to Group Settings 96
2.13.6.2 Group to VLAN Settings 97
2.13.7 QinQ 97
2.14 Security 100
2.14.1 Port Security 101
2.14.1.1 Port Security Settings 101
2.14.1.2 Port Security White-List MAC 101
2.14.2 802.1X 102
2.14.2.1 802.1X Settings 103
2.14.2.2 802.1X Parameters Settings 104
2.14.2.3 802.1x Port Setting 105
2.14.3 ACL 106
2.15 ERPS/Ring 110
2.15.1 ESRP Setting 111
2.15.1.1 Example of ERPS Settings 113
2.15.1.2 UERPS Settings (Optional) 115
2.15.2 iA-Ring Settings 117
2.15.3 C-Ring (Compatible-Ring) Settings 118
2.15.4 U-Ring 119
2.15.5 Compatible-Chain Settings 123
2.16 LLDP 125
2.16.1 LLDP Settings 126
2.16.2 LLDP Neighbors 126

2.17 PROFINET 128
2.17.1 PROFINET Settings 128
2.17.2 PROFINET's I&M 129
2.17.3 PROFINET MRP 130
2.18 EtherNet/IP 132
2.18.1 EtherNet/IP Settings 133
2.19 Client IP Setting 134
2.19.1 DHCP Relay Agent 134
2.19.2 DHCP Mapping IP 135
2.20 System 137
2.20.1 System Log 138
2.20.1.1 System Log Settings 138
2.20.1.2 System Log - Log 139
2.20.2 Warning/Alarm 139
2.20.2.1 Warning/Alarm Settings 140
2.20.2.2 SMTP Settings 142
2.20.2.3 Log 144
2.20.3 Denial of Service 145
2.20.4 Backup/Restore Config 147
2.20.4.1 Backup/Restore Config. Via HTTP 148
2.20.4.2 Backup/Restore Config. Via TFTP 148
2.20.5 Firmware Update 150
2.20.6 Factory Default Setting 150
2.20.7 Reboot 150

3 Configuring with a Serial Console 151

3.1 Serial Console Setup 151
3.2 Command Line Interface Introduction 153
3.3 General Commands 154
3.4 Command Example 155
3.4.1 Administration Setup using Serial Console 155
3.4.2 Spanning Tree Setup using Serial Console 156

4 Configuring with a Telnet Console 157

4.1 Telnet 157
4.2 Telnet Log-in 157
4.3 Command Line Interface for Telnet 158

4.4 Commands in the Privileged Mode 158
4.5 Commands in the Configuration Mode 159

5 Device Management Utility 161

5.1 Network Setting 162
5.2 Topology Diagram 163
5.3 Firmware Update 165

Appendix A: Glossary 167

Appendix B: Modbus Memory Map 169

Preface

This manual contains some advanced network management knowledge, instructions, examples, guidelines, and general theories. The contents are designed to help users manage the switch 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, and 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. If they are unable to assist you, please redirect your inquiries to www.agatel.co.uk.

Warranty Period

Agatel Ethernet Switching provides a limited 5-year warranty for managed Ethernet switches.

1 Introduction

1.1 Introduction to Industrial Managed Switch

Agatel's Ethernet Switching are productlines of powerful industrial managed switch which are referred to as Open Systems Interconnection (OSI) Layer 2* bridging devices. Unlike an "**unmanaged**" switch, which is normally found in homes orin Small Office/Home Office (SOHO) environments and runs in "auto-negotiation" mode, each port ona "**managed switch**" can be configured for its link bandwidth, priority, security, and duplex settings. The managed switches can be managed by Simple Network Management Protocol (SNMP) software,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.

Agatel's managed switch is also an industrial switch and not a commercial switch. A commercial switch simply works in a comfortable office environment. However, an industrial switch 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. Agatel's managed switch works fine even in these environments.

Agatel's managed switch is designed to provide faster, secure, and more stable network. One advantage that makes it a powerful switch is that it supports network redundancy protocols/technologies such as Ethernet Ring Protection Switching (ERPS), iA-Ring, Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and Media Redundancy Protocol (MRP). These protocols provide better network reliability and decrease recovery time down to less than 20 ms.

Agatel's managed switch supports a wide range of IEEE standard protocols. This switch is excellent forkeeping systems running smoothly, reliable for preventing system damage or losses, and friendly to alllevels of users. The goal of this innovative product is to bring users an enhanced 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 or as a footnote.

1.2 Software Features

Agatel's industrial managed switches come with a wide range of network protocols and software features. These protocols and software features allow the network administrator to implement security and reliability into their network. These features enable Agatel's switches to be used in safety applications, and factory and process automation. The followings are the list of protocols and software features.

- Three User Interfaces
  - Web browser
  - Telnet Console
  - Serial Console
- Dynamic Host Configuration Protocol (DHCP) Server/Relay/Client with Option 66/67/68
- Network Time Protocol (NTP) Server/Client
- Simplified Network Time Protocol (SNTP)
- IEEE 1588 Precision Clock Synchronization Protocol (PTP) V2 and Transparent Clock
- Port Mirror
- Quality of Service (QoS) Traffic Regulation
- Link Aggregation Control Protocol (LACP)
- Medium Access Control (MAC) Filter
- Generic Attribute Registration Protocol (GARP)/ GARP Multicast Registration Protocol (GMRP)/ GARP VLAN Registration Protocol (GVRP)
- Internet Group Management Protocol (IGMP)
- Simple Network Management Protocol (SNMP) v1/v2/v3 (with MD5 Authentication and DES encryption)
- SNMP Inform
- Spanning Tree Protocol (STP) / Rapid Spanning Tree Protocol (RSTP)/ Multiple Spanning Tree Protocol (MSTP)/ Media Redundancy Protocol (MRP)
- Virtual Local Area Network (VLAN)
  - IEEE 802.1x / Extensible Authentication Protocol (EAP) / Remote Authentication Dial-In User Service (RADIUS) / Terminal Access Controller Access-Control System (TACACS+)
- Ring
  - Ethernet Ring Protection Switching (ERPS)
  - iA-Ring
  - Compatible-Ring
  - Compatible-Chain
  - U-Ring
- Link Layer Discovery Protocol (LLDP)
- Profinet
- Alarm System (with E-mail Notification or Relay Output)
- Modbus/TCP
- Ethernet/IP

2 Configuring with a Web Browser

Chapter 2 explains how to access the industrial managed switch 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 the 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 console and the switch. There are only a few differences among these three methods. Users are recommended to use the web browser method to configure the system because of its user-friendly interface.

2.1 Web-based Management Basics

Users can access the managed switch easily using their web browsers (Internet Explorer 8 or 11, Firefox 44, Chrome 48 or later versions are recommended). We will proceed to use a web browser to introduce the managed switch's functions.

2.1.1 Default Settings

Below is a list of default factory settings. This information will be used during the login process. Make sure that the computer accessing the switch has an IP address in the same subnet and the subnet mask is the same.

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

2.1.2 Login Process and Main Window Interface

Before users can access the configuration, they have to log in. This can simply be done in two steps.

1. Launch a web browser.
2. Type in the switch IP address (e.g. http://10.0.50.1), as shown in Figure 2.1).

   Note:

   When the user name and password is left empty, the login prompt will not show.

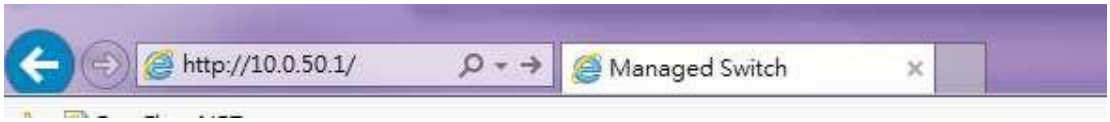


Figure 2.1 IP Address for Web-based Setting

After the login process, the main interface will show up, as shown in
Figure 2.2. The main menu (left side of the screen) provides the links at the top level links of the menu hierarchy and by clicking each item allows lower level links to be displayed. Note that in this case the Port 5 is highlighted in green, indicating that the port is being connected. Detailed explanations of each subsection will be addressed later as necessary.

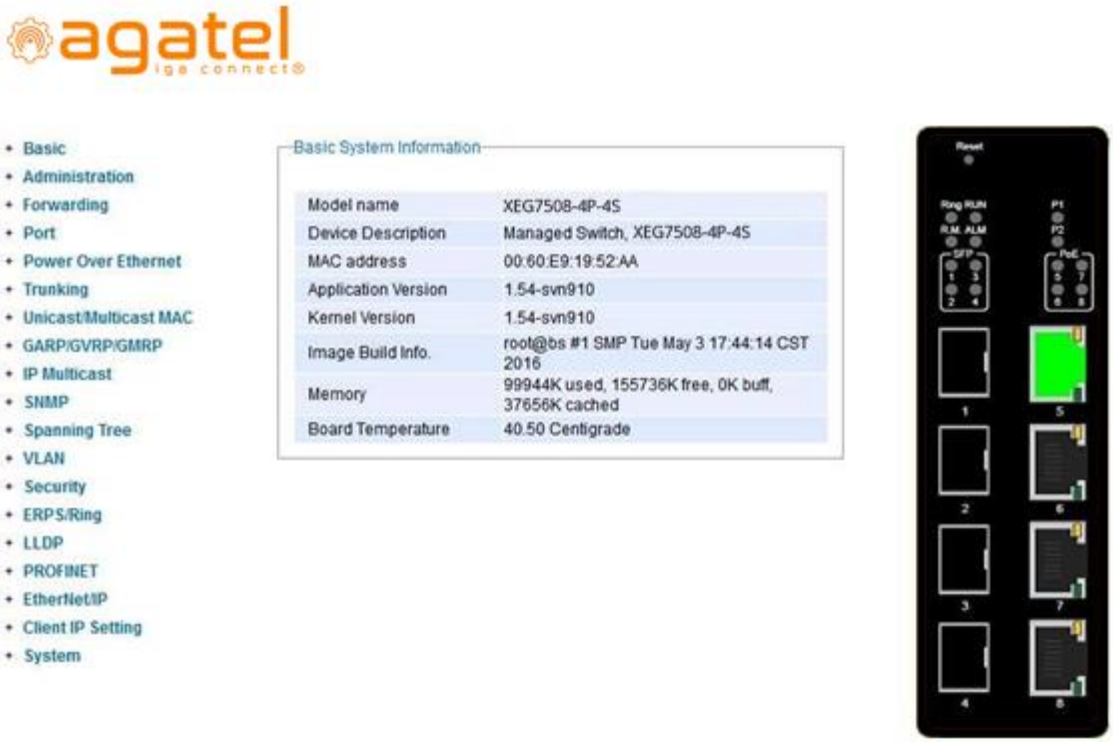


Figure 2.2 Default Web Interface

2.2 Basic Information

To help users become familiar with the device, the **Basic** section provides important details of the switch. This is also the main welcome screen once the user has logged in. The details make it easier to identify different switches connected to the network. The Basic section is categorized into six subsections as shown in the left panel of Figure 2.3.

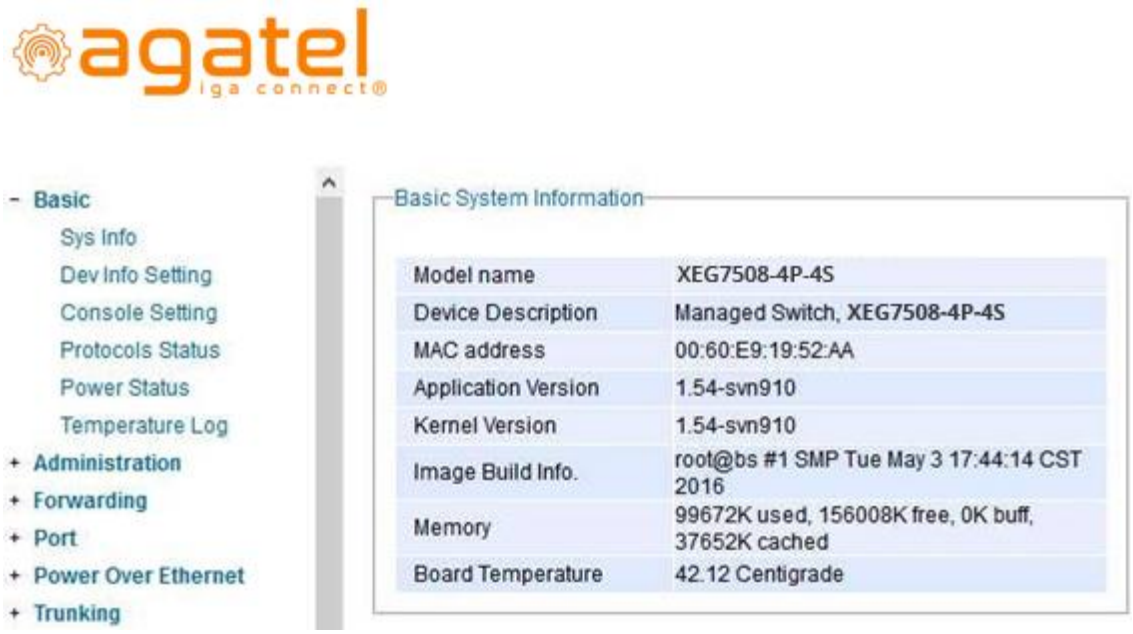


Figure 2.3 Basic Information Dropdown Menu

2.2.1 Sys Info

This subsection provides basic system information of Agatel's industrial managed switch. The user can check the model name, device description, MAC address, firmware version, image build information, memory usage of the switch, and current board's temperature. Note that Agatel's firmware generally consists of application version and kernel version. Figure 2.4 depicts an example of Basic System Information of XEG7508-4P-4S. Table 2.1 summarizes the description of each basic information.



Figure 2.4 Details of Sys Info Webpage

Table 2.1 Descriptions of the Basic information

Label	Description
Model name	The device's complete model name
Device Description	The model type of the device
MAC address	The MAC address of the device
Application Version	The current application version of the device.
Kernel Version	The current kernel version of the device.
Image Build Info.	Information about the firmware image such as date of creation
Memory	The current RAM's availability and the size of cached and shared memory.
Board Temperature	The current temperature of the board inside the chassis in degree Celsius (a.k.a. Centigrade)

2.2.2 Dev Info Setting

Users can assign device's details to Agatel's switch in this subsection. By entering unique and relevant system information such as device name, device description, location, and contact, this information can help identify one specific switch among all other devices in the network that supports SNMP. Please click on the "**Update**" button to update the information on the switch. Figure 2.5 shows Device Information Setting page of an XEG7508 managed switch model. Table 2.2 summarizes the device information setting descriptions and corresponding default factory settings.



Figure 2.5 Details of Device Information Settings Webpage

Table 2.2 Descriptions of the System Settings

Label	Description	Factory Default
Device Name	Specifies a particular role or application of different switches. The name entered here will also be shown in Switch View and Device View applications such as Agatel's Device Management Utility. Max. 63 Characters.	(Model name)
Device Description	Detailed description of the unit. Max. 63 Characters.	Managed Switch + (Model name)
Location	Location of the switch. Max. 63 Characters.	Switch Location
Contact	Provides contact information for maintenance. Enter the name of whom to contact in case a problem occurs. Max. 63 Characters.	www.agatel.co.uk

2.2.3 Console Setting

In this chapter, we use a web browser for configuring the switch. For the serial console method, please go to Chapter 3 Configuring with Serial Console for more detail on how to connect console to the switch. The **Console Setting** here only shows the setting parameters of a serial console's connection, which can be used by a console software such as Tera Term. Figure 2.6 below shows an example of the serial console's connection parameters.

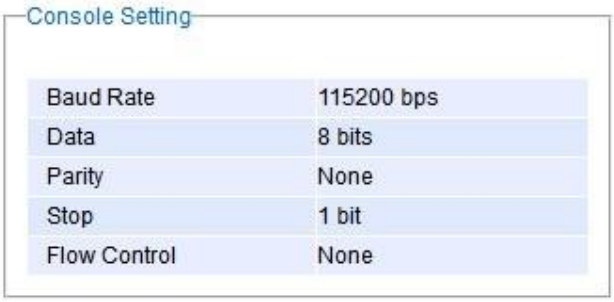


Figure 2.6 Setting Parameters for the Console Method

2.2.4 Protocols Status

Protocols Status subsection reports status of all protocols in the switch. While users can view status of all protocols at once in this webpage, the detailed explanation of each protocol and method will be provided in the following sections. Figure 2.7 shows the web interface for the Protocol Status page.



Figure 2.7 Protocol Status Webpage

2.2.5 Power Status

Agatel's managed switch features dual VDC power supply inputs. For Non-PoE models, 9-57VDC can be supplied to Power Input 1 (V1+ and V1- pins) and/or Power Input 2 (V2+ and V2- pins). For PoE models, 45-57VDC should be supplied under 802.3af mode and 51-57VDC should be supplied under 802.3at mode. For instance, the XEG7508-4P-4S has the following three power ratings: 9-57VDC with a maximum current of 2.8 Amperes (No PoE mode), 45-57VDC with a maximum current of 1.7 Amperes (802.3af mode), and 51-57VDC with a maximum current of 2.3 Amperes (802.3at mode). Figure 2.8 shows the status of each power input. A "**Fault**" status means that the power on that supplyinput is either not connected or the power is not supplied properly.



Figure 2.8 Power Status Webpage

2.2.6 Temperature Log

This subsection provides user and system temperature logs. There are summary statistics and distribution of temperature information for each log. The highest temperature, the lowest temperature and the average temperature are reported in degree Celsius. Additionally, there is a recorded time which shows the time since the temperature log were recorded. Under the summary statistics, there is a table showing the ranges of temperature, percentages of time in each range, and amount of time in each range. The user can reset the user statistics by clicking on the **Reset** button at the bottom of User Temperature Log. However, the system temperature log cannot be reset by the users. Note that the information is not automatically update. Information provided in this webpage will help the users to monitor the status of the industrial managed switch in harsh environment. The users have to click reload on the web browser to update for the latest statistics. Figure 2.9 shows the **User Temperature Log** box and Figure 2.10 shows the System Temperature Log box.

Note that there is a sensor component in the industrial managed switch which can detect the inside temperature. The software inside the switch can read the sensor's data and transform it into temperature in a unit of degree Celsius. Because the device is airtight, the inside temperature will be higher than the outside temperature around 20 degrees. For the industry level switches, the lowest operating temperature (outside) will be around -20 to -40 degrees Celsius and the highest operating temperature (outside) will be around 70 to 85 degrees Celsius.

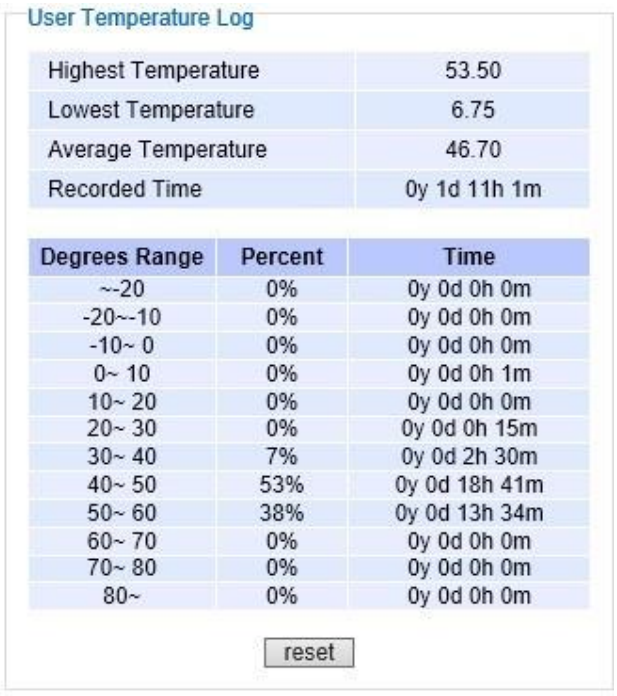


Figure 2.9 User Temperature Log

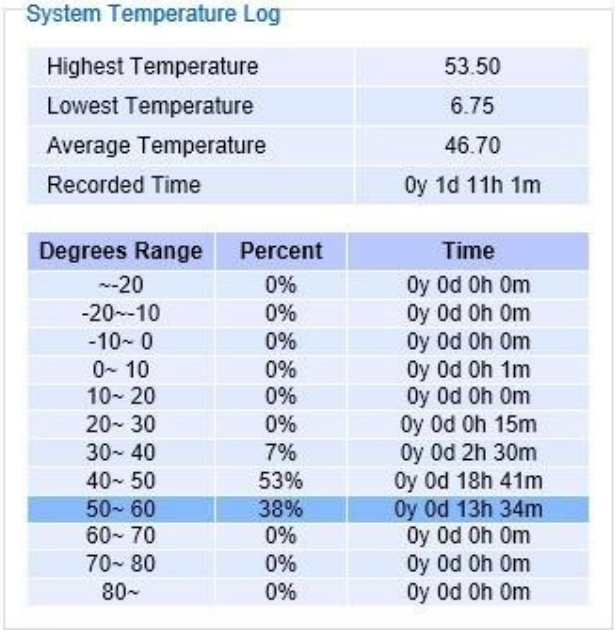


Figure 2.10 System Temperature Log

2.3 Administration

In this section, users will be able to configure **Password, IP Settings, IPv6 Setting, Ping, Ping6, Mirror Port, System Time, Modbus Setting, PTP, SSH, Telnet, and DIP Switch**. Figure 2.11 shows the Administration section with the list of its subsections on the left of the screen.



Figure 2.11 Administration Dropdown Menu

2.3.1 Password

Although no password is set for the device when it is manufactured, users can set a password to assure overall system security. The user name and password can be updated in this page as shown in Figure 2.12. Setting for a local authentication is introduced in this subsection, while setting for a remote authentication is described in later sections. The user name and password set here are applied to all types of access to Agatel's switch: web management user interface (UI), secure shell (SSH), and command line interface (CLI). Please click on the "**Update**" button to update the user name and

password information on the switch. Table 2.3 summarizes the description of each field.



Figure 2.12 Password Setting Webpage

Table 2.3 Descriptions of Password Setting

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

In addition to the local authentication, the switch can be configured to request for authentication through a centralized RADIUS or TACACS+ server when the local authentication fails. Figure 2.13 shows the setting parameters for authentication server while Table 2.4 summarizes the authentication server settings. For the RADIUS and TACACS+ comparison, please refer to Table 2.5 so that you can choose the solution that best suits your needs.



Figure 2.13 Authentication Server Setting

Table 2.4 Authentication Server Settings

Label	Description	Factory Default
Authentication Server	Enable / disable authentication through a remote authentication server	Disabled
Server Type	Choose Authentication Server type: RADIUS or TACACS+. See notes below for a detailed explanation.	RADIUS
Server IP/Name	IP address of the authentication server	NULL
Server Port	Communication port of the authentication server	1812
Shared Key	The key used to authenticate with the server. Max 15 characters.	12345678
Confirmed Shared Key	Re-type the shared key. Max 15 characters.	NULL
Authentication Type	Authentication mechanism. For RADIUS: MD5. For TACACS+: ASCII, PAP, CHAP, MSCHAP.	RADIUS is MD5 TACACS+ is ASCII
Server Timeout (1~255 sec)	The time out period of waiting for a response from the authentication server. This will affect the time that the next login prompt shows up in case that the server is not available.	5

***NOTE:**

RADIUS (Remote Authentication Dial in User Service):

RADIUS is an access server that uses authentication, authorization, and accounting (AAA) protocol for authentication and authorization. It is a distributed security system that secures remote access to networks and network services against unauthorized access. The RADIUS specification is described in RFC 2865, which obsoletes RFC 2138.

TACACS+ (Terminal Access Controller Access-Control System Plus):

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server. The TACACS+ specification is described in Cisco's TACACS+ RFC draft.

Table 2.5 Comparison of Authentication Server Settings between RADIUS and TACACS+

	RADIUS	TACACS+
Transport Protocol	UDP	TCP
Authentication and Authorization	Separates AAA	Combines authentication and authorization
Multiprotocol Support	No	Yes, support AppleTalk Remote Access (ARA) and NetBIOS protocol
Confidentiality	Only password is encrypted	Entire packet is encrypted

2.3.2 IP Setting

In this subsection, users may modify network settings for Internet Protocol version 4 (IPv4) of the switch, e.g., static IP address, subnet mask, gateway, primary domain name server (DNS), and secondary DNS. As shown in Figure 2.14, users can choose to enable Dynamic Host Configuration Protocol (DHCP) by checking the box to obtain an IP address automatically. That is the IP address and related information can be automatically obtained from a DHCP server thus reducing the work for an administrator. By disabling this function, the users have an option to set up the static IP address and related fields manually. Please click on the "**Update**" button to update the IP configuration on the switch. A system reboot is required after each update, so the new network settings can take effect. The user will need to manually update the new IP address in the URL field of the web browser if the IP address of the managed switch is change. The description of each field and its default value are summarized in Table 2.6.

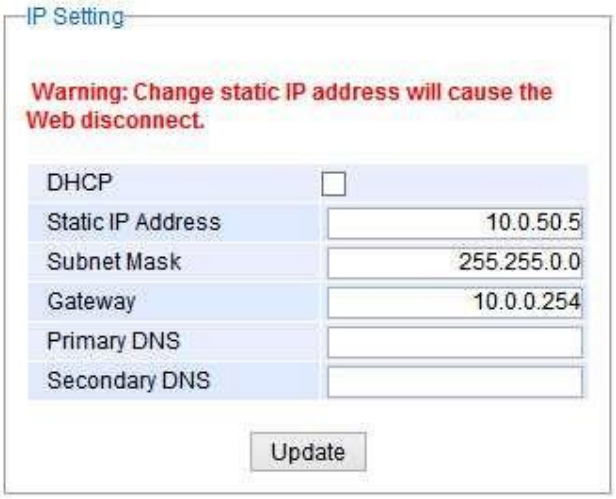


Figure 2.14 Webpage of IP Setting

Table 2.6 Descriptions of IP Settings

Label	Description	Factory Default
DHCP	By checking this box, an IP address and related fields will be automatically assigned. Otherwise, users can set up the static IP address and related fields manually.	Uncheck
Static IP Address	Display current IP address. Users can also set a new static IP address for the device.	10.0.50.1
Subnet Mask	Display current Subnet Mask or set a new subnet mask.	255.255.0.0
Gateway	Show current Gateway or set a new one.	10.0.0.254
Primary DNS	Set the primary DNS IP address to be used by your network.	NULL
Secondary DNS	Set the secondary DNS IP address. The Ethernet switch will locate the secondary DNS server if it fails to connect to the Primary DNS Server.	NULL

2.3.3 IPv6 Setting [P1]

This subsection enables Agatel's switch to operate in Internet Protocol version 6 (IPv6) network. The users have options to enable Autoconfig, DHCPv6, or Manual setting as shown in Figure 2.15. Note that in IPv6 network, there are three types of auto configuration: stateless, stateful, and a combination of both. The "**Autoconfig**" option here is the stateless configuration, while the "**DHCPv6**" option is the stateful configuration. If the users check both the Autoconfig and the DHCPv6 options, the switch will use the combination of stateless and stateful configuration. When selecting the "**Manual**" option, the users will have to enter the Global Unicast Address, Prefix Length, and Gateway. The Manual DNS option also requires the users to fill in the Primary DNS and Secondary DNS addresses. The lower portion of the page summarizes the current IPv6 address information of the switch which are the Global Unicast Address, Link-Local Address, Gateway, Primary DNS, and Secondary DNS. Table 2.7 explains each field in the IPv6 setting webpage.

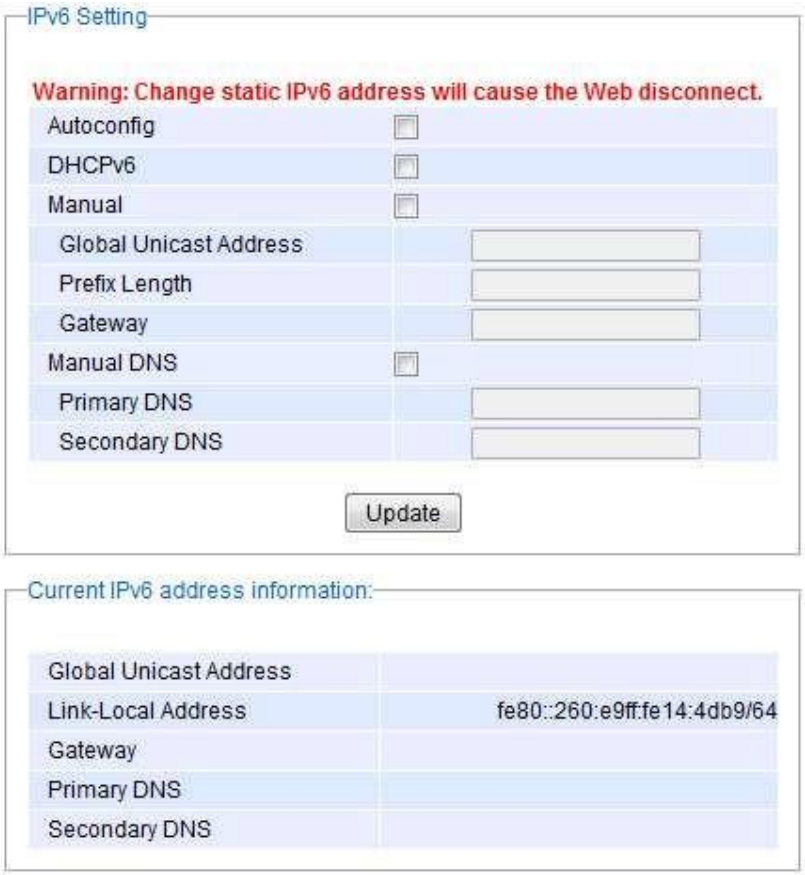


Figure 2.15 Webpage of IPv6 Setting

Table 2.7 Description of IPv6 Setting

Label	Description	Factory Default
Autoconfig	By checking this box, all IPv6 setting will be automatically configured for the users. This option is based on the stateless autoconfiguration in which the switch uses information in router advertisement messages to configure an IPv6 address. The	Uncheck

	address will be a concatenation of first 64 bits from the router advertisement source address with the Extended Unique Identifier (EUI-64).	
DHCPv6	By checking this box, an IPv6 address and related fields will be automatically assigned from a DHCPv6 server in the network. This is a stateful auto configuration in which the switch will generate a DHCP solicit message to the ALL-DHCP-Agents multicast address to find DHCPv6 server. Otherwise, users can set up the IPv6 address manually.	Uncheck
Manual	By checking this box, users must provide Global Unicast Address, Prefix Length, and Gateway address in the following fields. Note that when this option is checked, the next three fields will become active for setting.	Uncheck
Global Unicast Address	Set an IPv6 address that is routable across the Internet and its three high-level bits are 001. The IPv6 address is in the format 2XXX::/3.	NULL
Prefix Length	Set a prefix length for the IPv6 address in previous field.	NULL
Gateway	Set the IPv6 address of an IPv6 Gateway	NULL
Manual DNS	By checking this box, user must manually provide Primary and Secondary DNS addresses for IPv6. Note that when this option is checked, the next two fields will become active for setting.	Uncheck
Primary DNS	Set the primary DNS IPv6 address to be used by your network.	NULL
Secondary DNS	Set the secondary DNS IPv6 address. The Ethernet switch will locate the secondary DNS server if it fails to connect to the Primary DNS Server.	NULL

2.3.4 Ping

Agatel's managed switch provides a network tool called Ping for testing network connectivity in this subsection. Ping is a network diagnostic utility for testing reachability between a destination device and the managed switch. Note that this utility is only for IPv4 address. The Ping utility for IPv6 will be provided in the next subsection. Figure 2.16 shows the user interface for using the Ping command.



Figure 2.16 Ping Webpage

Users can enter an IP address or a domain name into the field to verify network connectivity as shown in Figure 2.17. After entering the IP address/name, please click "**Ping**" button to run the ping function.

Example of successful ping result is shown in Figure 2.18 while a failure ping result is depicted in Figure 2.19.



Figure 2.17 Example of Ping Command



Figure 2.18 Example of successful ping command result



Figure 2.19 Example of unsuccessful ping command result

***Note:**

If users enter a domain name instead of an IP address, they should assign a DNS first. This can be done through **Administration** > IP Setting as shown in Section 2.3.2.

2.3.5 Ping6 [P2]

Ping6 is a corresponding network diagnostic utility for testing reachability between a destination device and the managed switch in IPv6 network. Figure 2.20 shows the user interface for using the Ping command.



Figure 2.20 Ping6 Webpage

Users can enter an IPv6 address into the field to verify network connectivity. After entering the IPv6 address, please click "**Ping6**" button to start the ping function. Examples of successful ping6 results are shown in Figure 2.21.



Figure 2.21 Example of Successful Ping6 Result

2.3.6 Mirror Port

In order to help the network administrator keeps track of network activities, the managed switch supports port mirroring, which allows incoming and/or outgoing traffic to be monitored by a single port that is defined as a **mirror port.** Note that the mirrored network traffic can be analyzed by a network analyzer or a sniffer for network performance or security monitoring purposes. Figure 2.22 shows the Mirror Port webpage. The descriptions of port mirroring options are summarized in Table 2.8.



Figure 2.22 Mirror Port Webpage

***Note:**

Overflow will occur if the total throughput of the monitoring ports exceeds what the mirror port can support.

Table 2.8 Description of Port Mirroring Options

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

Mirror-to-port	Select the mirror port that will be used to monitor the activity of the monitored ports	Port1

2.3.7 System Time

Agatel's industrial managed switch has internal calendar (date) and clock (or system time) which can beset manually or automatically. Figure 2.23 shows the System Time and SNTP webpage. The users have options to configure **Current Date** and **Current Time** manually. There is a drop-down list of **Time Zone** which can be selected for the local time zone. If the switch is deployed in a region where daylight saving time is practiced (see note below for explanation), please check the **Enable** option for **Daylight Saving Time**. Then, the users will have to enter the **Start Date**, **End Date**, and **Offset** in hour(s).

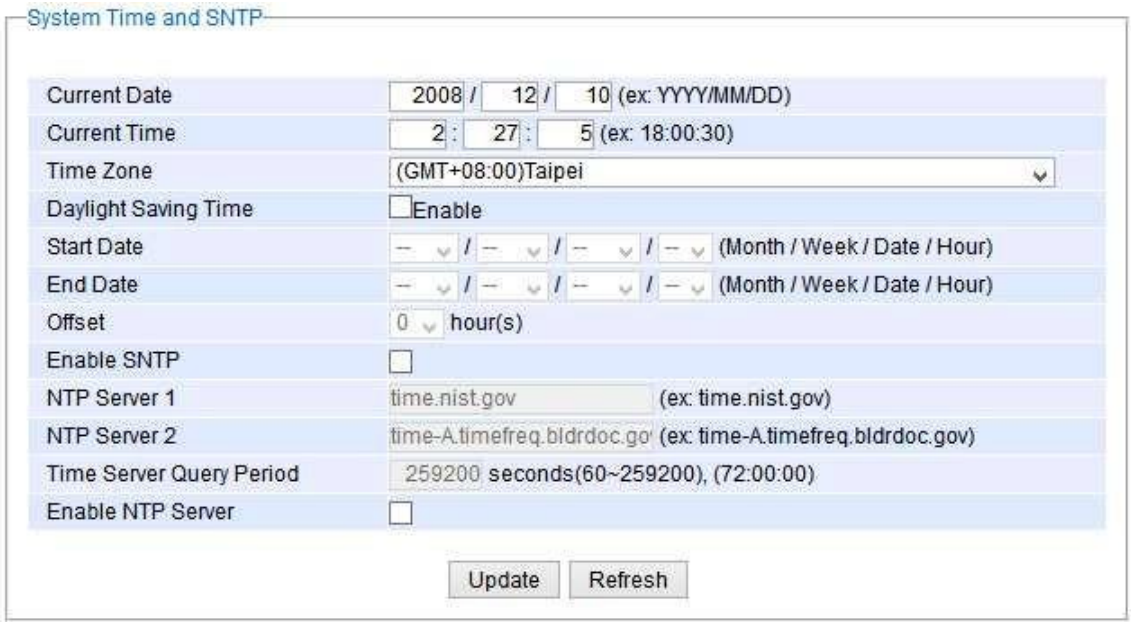


Figure 2.23 Webpage for Setting System Time and SNTP

For automatically date and time setting, the users can enable Simple Network Time Protocol (SNTP) by checking the **Enable SNTP** option (see note below for explanation). Then, the users must enter the NTP Server 1 and NTP Server 2 which will be used as the reference servers to synchronize date and time to. The users can specify the Time Server Query Period for synchronization which is in the order of seconds. The value for this period will depend on how much clock accuracy the users want the switch to be. Finally, the managed switch can become a network time protocol server for the local devices by checking the box behind the **Enable NTP Server** option. Description of each option is provided in Table 2.9.

Table 2.9 Descriptions of the System Time and the SNTP

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
Time Zone	The user's current local time	(GMT+08:00) Taipei
Daylight	Enable or disable Daylight Saving Time function	Unchecked

Saving Time		
Start Date	Define the start date of daylight saving	NULL
End Date	Define the end date of daylight saving	NULL
Offset	Decide how many hours to be shifted forward/backward when daylight saving time begins and ends. See note below.	0
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 Server Query Period	This parameter determines how frequently the time is updated from the NTP server. If the end devices require less accuracy, longer query time is more suitable since it will cause less load to the switch. The setting value can be in between 60 – 259200 (72 hours) seconds.	259,200 seconds.
Enable NTP Server	This option will enable network time protocol (NTP) daemon inside the managed switch which allows other devices in the network to synchronize their clock with this managed switch using NTP.	Unchecked

Note:

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

- SNTP: **S**imple **N**etwork **T**ime **P**rotocol is used to synchronize the computer systems' clocks with a standard NTP server. Examples of two NTP servers are *time.nist.gov* and *time-A.timefreq .bldrdoc.gov.*

2.3.8 Modbus Setting

Agatel's managed switch can be connected to a Modbus network using Modbus TCP/IP protocol which is an industrial network protocol for controlling automation equipment. The managed switch's status and settings can be read and written through Modbus TCP/IP protocol which operates similar to a Management Information Base (MIB) browser. The managed switch will be a Modbus slave which can be remotely configured by a Modbus master. The Modbus slave address must be set to match the setting inside the Modbus master. In order to access the managed switch, a **Modbus Address** must be assigned as described in this subsection. A Modbus memory mapping table, which lists all the register's addresses inside the managed switch and their descriptions, is provide in Appendix B: Modbus Memory Map. Figure 2.24 shows the Modbus Setting webpage.

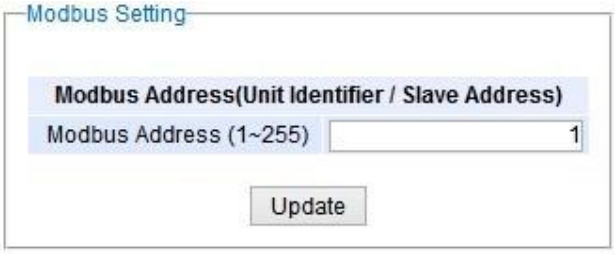


Figure 2.24 Webpage for Setting the Modbus Address

Figure 2.24 shows the webpage that users can set up the Modbus ID address. Users can use Modbus TCP/IP compatible applications such as **Modbus Poll** to configure the switch. Note that Modbus Poll can be download from http://www.modbustools.com/download.html. The Modbus Poll 64-bit version 7.0.0, Build 1027 was used in this document. Agatel does not provide this software to the users. Tutorial of Modbus read and write examples are illustrated below.

Note: The switch only supports Modbus function code 03, 04 (for Read) and 06 (for Write).

Read Registers (This example show how to read the switch's IP address.)

Address	Data Type	Read/Write	Description
0x0051 (81)	2 words	R	IP Address of switch Ex: IP = 10.0.50.1 Word 0 Hi byte = 0x0A Word 0 Lo byte = 0x00 Word 1 Hi byte = 0x32 Word 1 Lo byte = 0x01

Figure 2.25 Mapping Table of Modbus Address for Switch's IP Address

1. Make sure that a supervising computer (Modbus Master) is connected to your target switch (Modbus Slave) over Ethernet network.
2. Launch **Modbus Poll** in the supervising computer. Note a registration key may be required for a long term use of Modbus Poll after 30-day evaluation period. Additionally, there is a 10-minute trial limitation for the connection to the managed switch.
3. Click **Connect** button on the top toolbar to enter Connection Setup dialog by selecting **Connect…** menu as shown in Figure 2.26.

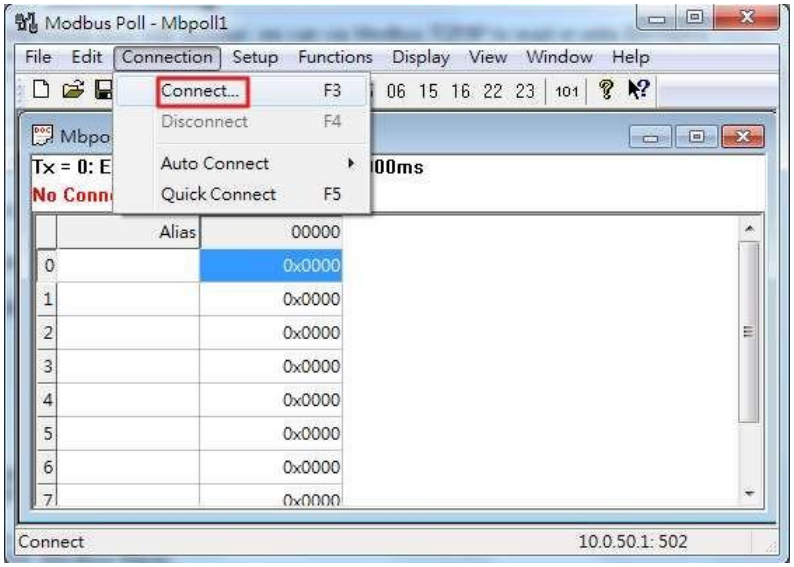


Figure 2.26 Entering Connection Setup Menu of the Modbus Poll

4. Select **Modbus TCP/IP** as the **Connection** mode and enter the switch's IP address inside the **Remote Modbus Server**'s **IP Address or Node Name** field at the bottom as shown in Figure 2.27. The **Port** number should be set to 502. Then click **OK** button.

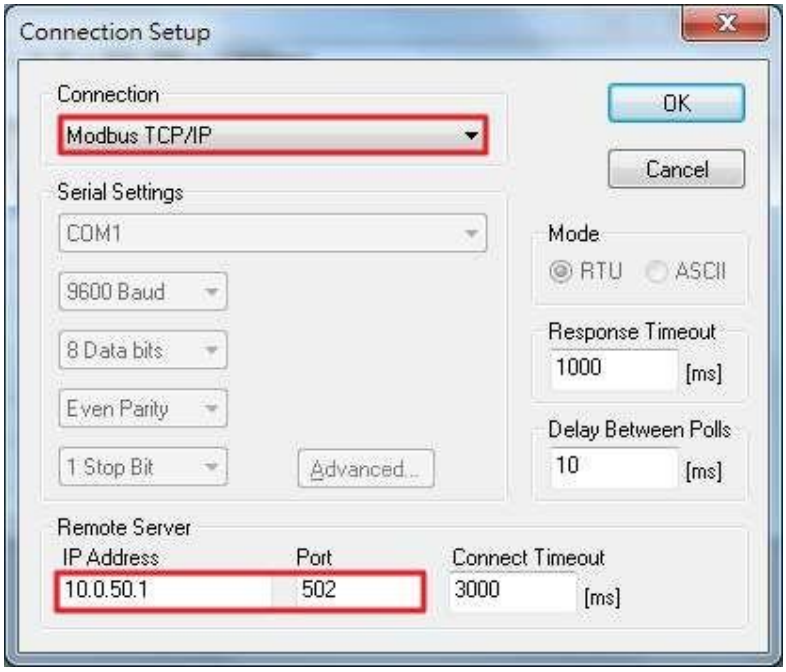


Figure 2.27 Modbus Poll Connection Setup

5. On the window Mbpoll1, select multiple cells from row 0 to row 2 by clicking on cells in second column of row 0 and row 2 while holding the shift key as shown in Figure 2.28.

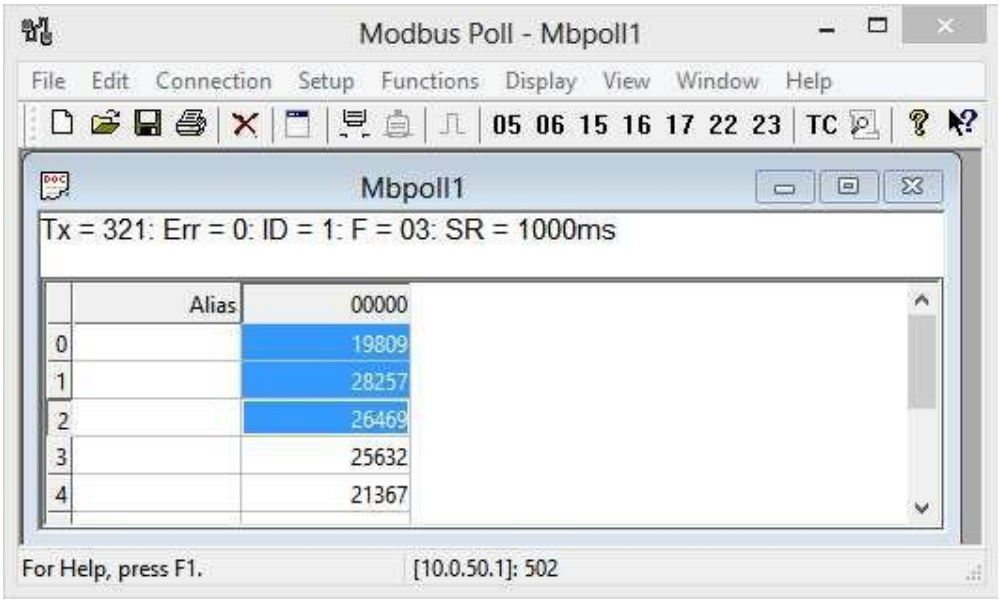


Figure 2.28 Mulitple Cell Section in Modbus Poll

6. Set **Display** mode of the selected cells in previous step to HEX (hexadecimal) by selecting **Display** pull-down menu and choosing the **Hex** as shown in Figure 2.29.

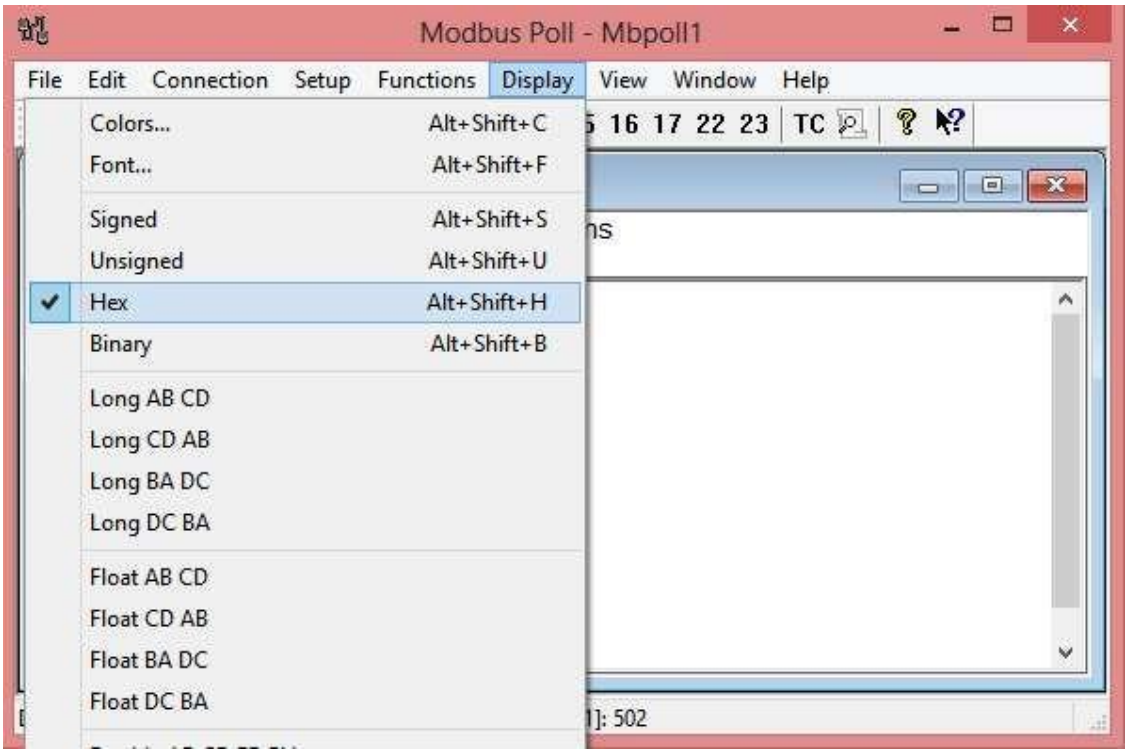


Figure 2.29 Set Display Mode to Hex in Modbus Poll

7. Click on the **Setup** pull-down menu and choose **Read/Write Definition…** as shown in Figure 2.30.

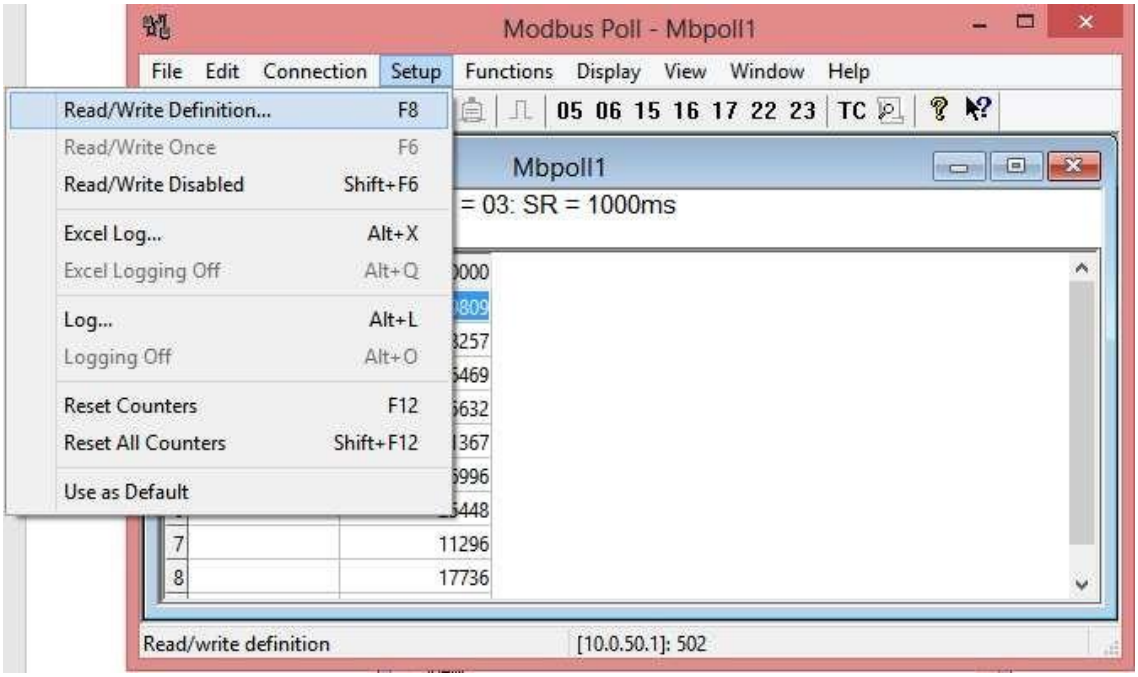


Figure 2.30 Modbus Poll Setup Read/Write Definition

8. Enter the **Slave ID** in the Modbus Poll function as shown in Figure 2.31, which should match the Modbus Address = 1 entered in Figure 2.24 in Section 2.3.8 (Modbus Setting).

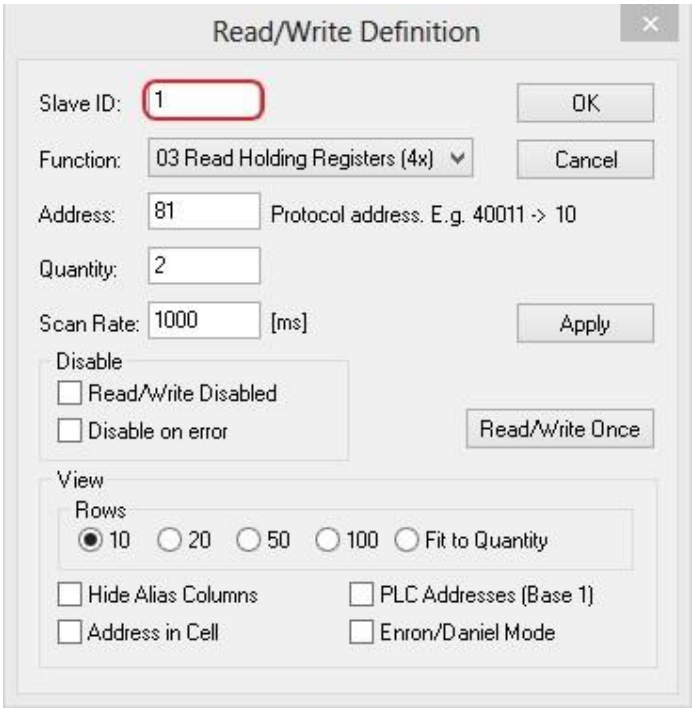


Figure 2.31 Slave ID in the Modbus Poll Function is set to 1

9. Select **Function 03** or **04** because the managed switch supports function code 03 and 04 as shown in Figure 2.32.



Figure 2.32 Set Code 03 in the Modbus Poll Function

10. Set starting **Address** to 81 and **Quantity** to 2 as shown in Figure 2.33.

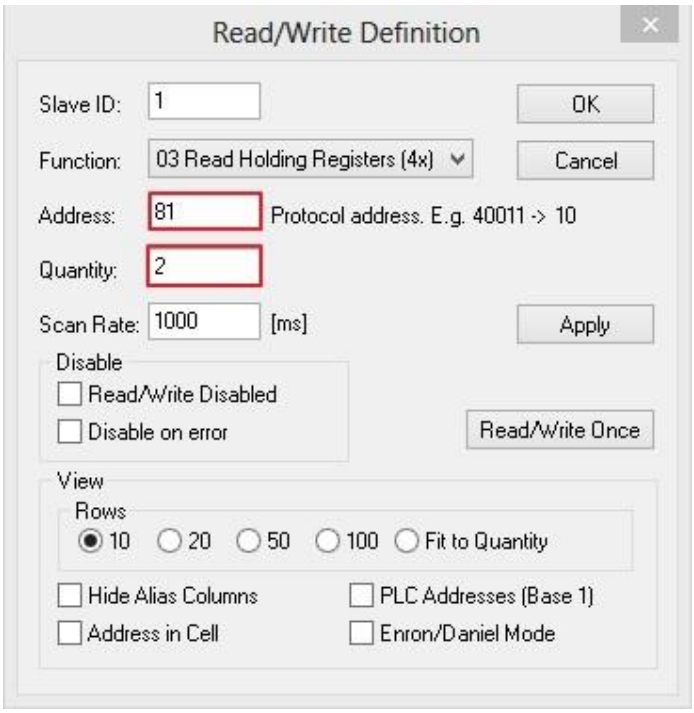


Figure 2.33 Setup Starting Address and Quantity in Modbus Poll

11. Click **OK** button to read the IP address of the switch.

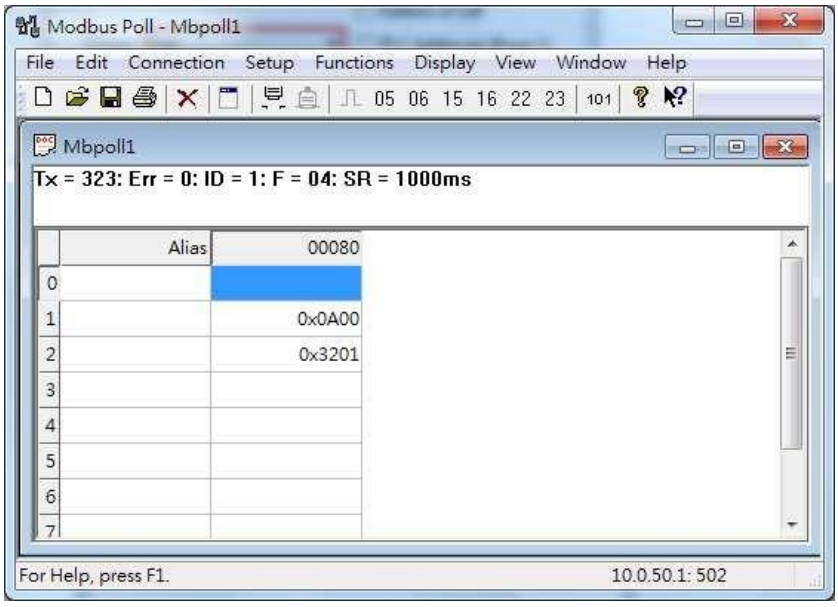


Figure 2.34 Modbus Memory Address 81 and 82 are the location of XEG7508's IP Address

12. Modbus Poll will get the values 0x0A, 0x00, 0x32, 0x01, which means that the switch's IP is 10.0.50.1 as shown in Figure 2.34.

Write Registers (This example shows how to clear the switch's Port Count (Statistics).)

Address	Data Type	Read/Write	Description
0x0100 (256)	1 word	W	Clear Port Statistics 0x0001: Do clear action

Figure 2.35 Mapping Table of Modbus Address for Clearing Port Statistics

1. Check the switch's Port TX/RX counts in **Port Statistics** page (described in Section 2.5.4) as shown in Figure 2.36.

Port Statistics

Port	Enable	Link	Tx	Tx Error	Tx Rate(Kbps)	Rx	Rx Error	Rx Rate(Kbps)
Port1	On	Up	11700	0	0	35115	0	0
Port2	On	Down	0	0	0	0	0	0
Port3	On	Down	0	0	0	0	0	0
Port4	On	Down	0	0	0	0	0	0
PortG1	On	Down	0	0	0	0	0	0
PortG2	On	Down	0	0	0	0	0	0

Clear Refresh

Figure 2.36 Port Count in Port Statistics Webpage

2. Click function **06** on the toolbar as shown in Figure 2.37.

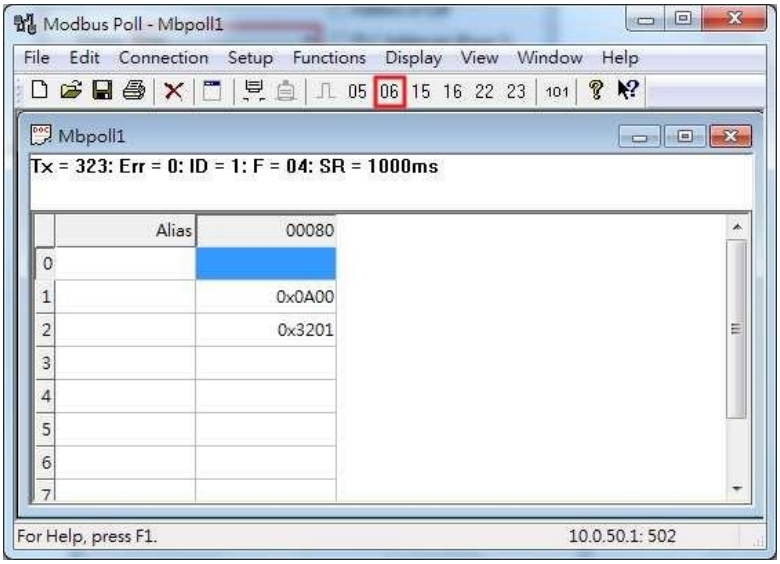


Figure 2.37 Click on Function 06 in the Modbus Poll

3. Set **Address** to 256 and **Value (HEX)** to 1 as shown in Figure 2.38, then click "**Send**" button.

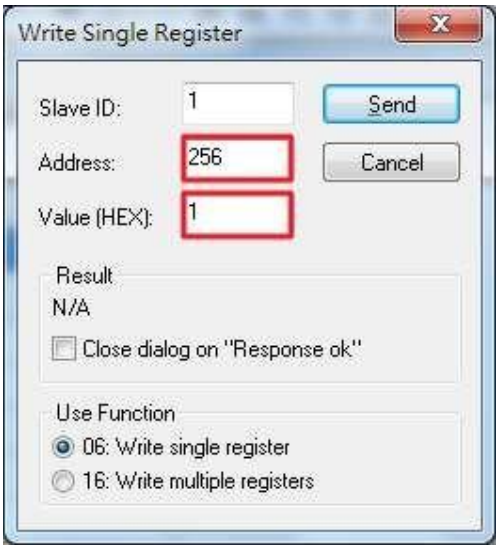


Figure 2.38 Use Modbus Poll to Clear Switch's Port Count

4. Check **Port Statistics** (described in Section 2.5.4) in the managed switch's Web UI as shown in Figure 2.39. The packet count is now cleared.

Port Statistics

Port	Enable	Link	Tx	Tx Error	Tx Rate(Kbps)	Rx	Rx Error	Rx Rate(Kbps)
Port1	On	Up	8	0	0	27	0	0
Port2	On	Down	0	0	0	0	0	0
Port3	On	Down	0	0	0	0	0	0
Port4	On	Down	0	0	0	0	0	0
PortG1	On	Down	0	0	0	0	0	0
PortG2	On	Down	0	0	0	0	0	0

Clear Refresh

Figure 2.39 Cleared Port Statistics

2.3.9 PTP

The Precision Time Protocol (PTP) is a high-precision time protocol. It can be used with measurement and control systems in local area network that require precise time synchronization. This menu is divided into two submenus: **PTP Setting** and **H/W PTP** as shown in Figure 2.40.



Figure 2.40 PTP's Submenu

2.3.9.1 PTP Setting

The PTP can be set in this PTP Setting webpage Figure 2.41 shows the PTP Configuration webpage in which the user can configure PTP and check its status. The lower part of Figure 2.41 allows the users to enable or disable the PTP function per port and check their current status.

To enable PTP on the managed switch, please check the **Enabled** box behind the **State** option as shown in Figure 2.41. Note that the PTP will not be enabled per port if this State option is not checked. Please see description of PTP configuration in Table 2.10 and description of PTP port information in Table 2.11. Note that after setting the desired PTP options, please click **Update** button to allow the new configuration to take effect.

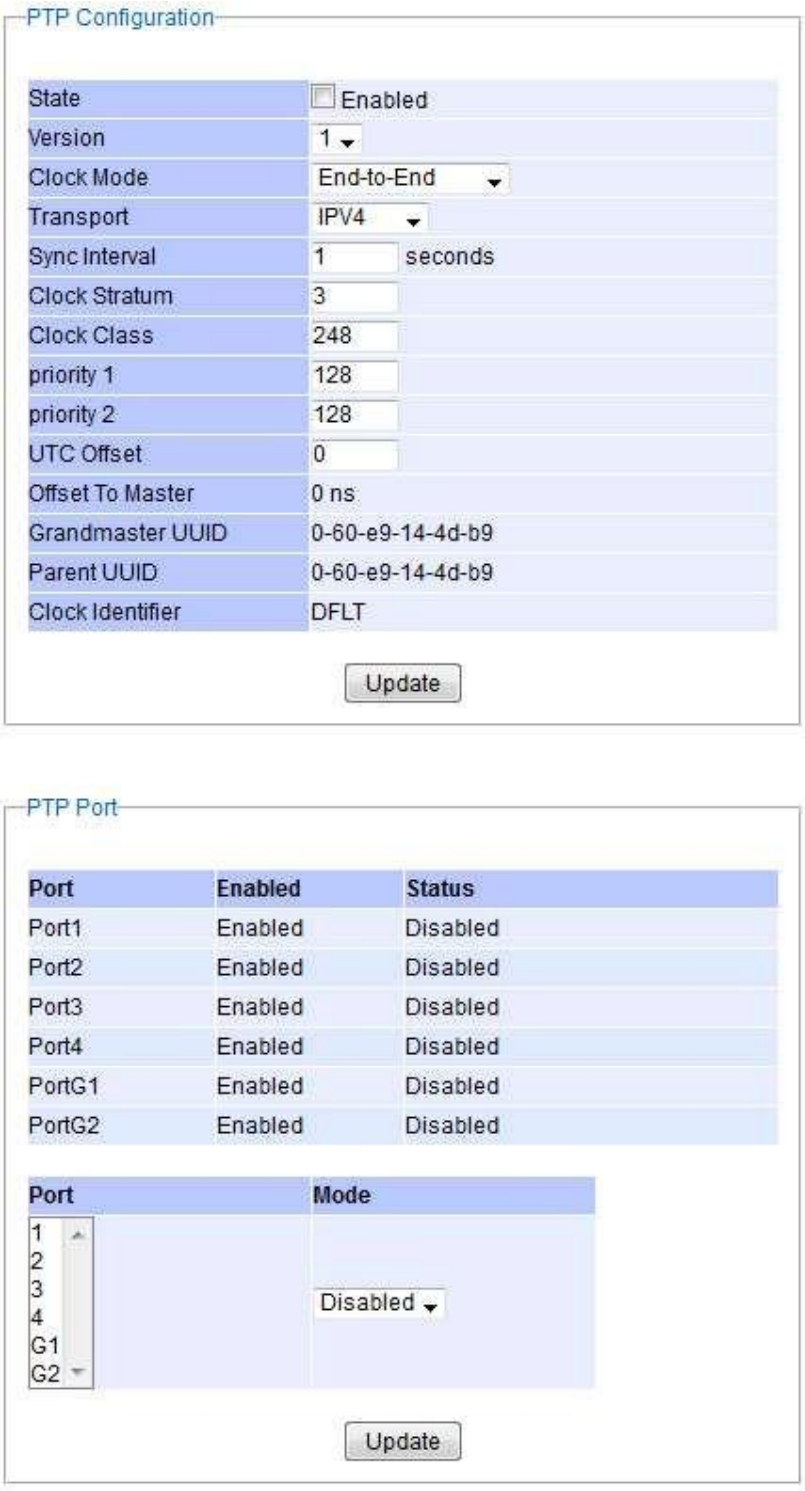


Figure 2.41 PTP Setting Webpage, example taken from XE75XX series

Table 2.10 Description of PTP Setting

Label	Description	Factory Default
State	Enabled/Disable the PTP function. This is the main option that needs to be enabled so that the port's PTP function will work according to other parameters defined in this table (Table 2.10).	Unchecked
Version	Set the PTP operation version. Note that v1 (IEEE 1588-2002) and v2 (IEEE 1588-2008) are supported.	1
Clock Mode	Select clock type of the PTP (Precision Time Protocol). The switch has four modes: End-End Boundary Clock, End-End Transparent Clock (TC), Peer-Peer Boundary Clock, and Peer-Peer Transparent Clock (TC).	End-to-End
Transport	Select Ethernet (layer 2) multicast transport or layer 3 (UDP/IPv4) multicast transports for PTP (Precision Time Protocol) messages.	IPV4
Sync Interval	Set the interval of the sync packet transmitted time. Small interval causes too frequent sync, which will cause more load to the device and network.	1
Clock Stratum	Set the Clock Stratum value. The lower values take precedence to be selected as the master clock in the best master clock algorithm (BMCA).	3
Clock Class	Clock Class represents clock's accuracy level. It is an attribute of an ordinary or boundary clock. It 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	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, 0 = highest priority, 255 = lowest priority.	128
priority 2	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 (BMCA), 0 = highest priority, 255 = lowest priority.	128
UTC Offset	Coordinated Universal Time (UTC) offset value	0
Offset to Master	The offset time to the master clock	None
Grandmaster UUID	The Grandmaster 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

Note: The Best Master Clock Algorithm (BMCA) is a key to the resiliency of the Precision Time Protocol (PTP). In a time synchronized network, there usually is a Grandmaster clock who synchronizes its clock with the UTC accurate clock from Global Positioning System (GPS). If a Grandmaster clock loses its GPS synchronization or gets disconnected due to a network fault or for other unknown reasons, the BMCA will allows another clock to automatically take over the duties of the Grandmaster clock and continue as a new Grandmaster.

Table 2.11 Description of PTP Port Setting

Label	Description	Factory Default
Port	Port number	-
Enabled	This is the port's mode information which indicates whether the port's PTP function is enabled or disabled.	Enabled
Status	This is PTP's per port operation status. If the per port	Disabled

	function is enabled, but the status is still disabled, please enable the PTP master option (State option in Table 2.10).	
Mode	Enabled/Disabled PTP per port function	Disabled

2.3.9.2 H/W PTP Setting

This subsection allows the user to enable the hardware Transparent Clock (TC). The TC can correct variable switch latency. This can be done by measuring the time that a PTP event message has spent in the switch called residence time. The residence time is reported to the receiver by the PTP event message itself. For this purpose, a new message field has been added called Correction Field which is a type of time interval that can be used to accumulate residence time along the path (possibly after multiple switches) of the message. To enable the hardware transparent clock, check the box behind **H/W TC Enabled** and then click on the **Update** button as shown in Figure 2.42.



Figure 2.42 H/W PTP Setting

2.3.10 SSH

The managed switch can be managed using command line interface (CLI) as described in Chapter 4. The users have option to remotely connect to the managed switch using either secure shell (SSH) or Telnet through any of its port. In this subsection, SSH will be introduced and then Telnet will be discussed in the next subsection. SSH was designed to replace Telnet and other insecure remote shell protocols that sends data or command in plaintext. SSH uses encryption to secure its data or command over an unsecure network.

To enable the SSH, please check the **Enabled** box behind the **SSH** option in Figure 2.43. At the beginning, the Server will send a public key to a Client, and the Client will check if the received public key is correct. If it is not correct, the Server will refuse the connection. Please click "**Generate**" button to change and regenerate the Server Key then obtain another public key from Server as shown in Figure 2.43.



Figure 2.43 SSH Setting Webpage

Note:

1. The managed switch supports both SSH version 1 (SSH1) and SSH version 2 (SSH2).
2. The server key is re-generated when the managed switch is reset to its factory default setting or a received key is non-existent.

SSH version 1 and SSH version 2 share the following features:

1. Client programs that use SSH can perform remote logins, remote command execution, and secure file copying across a network.
2. Several selectable encryption algorithms and authentication mechanisms are supported by the SSH.
3. An SSH agent can cache keys for easy access in later session.

A number of new features are added to SSH version 2 for a stronger and more comprehensive product. These features include:

1. Encryption ciphers, such as Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES).
2. The use of sound cryptographic Message Authentication Code (MAC) algorithms for integrity checking. Examples of secure hash (functions) algorithms which are MAC algorithms in SSH version 2 are the Message Digest algorithm 5 (MD5) and Secure Hash Algorithm 1 (SHA-1).
3. Support for public key certificates.

2.3.11 Telnet

This subsection allows the users to set the Telnet option for the managed switch. The command line interface (CLI) configuration using Telnet (as described in Chapter 4) or SSH (previous section) are the same except that the SSH encrypts the communication data. For the Telnet administration, the managed switch only provides the enable or disable function selectable in this webpage. The default setting for Telnet is enabled. Clicking on the **Update** button when you change the option to update it on

the managed switch. Figure 2.44 shows the Telnet setting webpage. Note that the users are recommended to use SSH instead of Telnet for higher security protection of your managed switch.



Figure 2.44 Telnet Setting Webpage

2.3.12 DIP Switch

This subsection reports the status of the DIP switch on the top of managed switch's housing. Figure 2.45 shows the DIP switch webpage. The bottom portion allows the users to enable or disable the physical control of the DIP Switch by checking on the **DIP Switch Control** option. This is another easy and convenient way to configure ERPS or iA-ring or Compatible-Ring using the DIP Switches instead of modifying configuration on a web browser. After checking or unchecking the option, please click **Update** button to allow the setting to take effect on the managed switch.



Figure 2.45 DIP Switch Status Webpage

2.4 Forwarding

There are many network technologies for forwarding packets over network. In this industrial managed switch, three main technologies are implemented: QoS, rate control, and storm control. Figure 2.46 depicts the submenus under the Forwarding section.



Figure 2.46 Forwarding Dropdown Menu

2.4.1 QoS

Quality of Service (QoS) is the ability to provide different priority to different applications, users, or data flows. QoS guarantees a certain level of performance to a data flow by using the following metrics: transmitted bit rate, bit error rate, delay, jitter, and probability of packet dropping. QoS guarantees are important if the network capacity is insufficient, especially for application that requires certain bit rate and is delay sensitive. For any network that is best effort, QoS cannot be guaranteed, except that resource is more than sufficient to serve users.

Controlling network traffic needs a set of rules to help classify different types of traffic and define how each of them should be treated as they’re being transmitted. This managed switch can inspect both 802.1p Class of Service (CoS) tags and DiffServ tags called Differentiated Services Code Point (DSCP) to provide consistent classification.

In the QoS section, three QoS mechanisms are included: queuing methods or packet scheduling disciplines in **Setting** section, **CoS Queuing Mapping** section, and **DSCP Mapping** section, as shown in Figure 2.47. Table 2.12 summarizes the descriptions of QoS Setting.



Figure 2.47 QoS Dropdown Menu

Table 2.12 Descriptions of QoS Setting

Label	Description	Factory Default
Setting	Queuing Methods **(**packet scheduling disciplines**)** includes **Strict Priority, Weighted Round-Robin,** and **Deficit Round Robin** See notes in the following subsection for detailed descriptions and comparison.	Strict Priority
Header Mapping	**CoS Queuing Mapping** and **DSCP Mapping** **For 802.1p CoS only**, switch only checks Layer 2 (L2) 802.1p CoS priority bits. **For DiffServ**, switch checks DiffServ Code Point (DSCP). See notes below for a detailed description.	Both 802.1p CoS and DiffServ

2.4.1.1 QoS Setting

Three types of queuing methods are configurable in this managed switch**:** Strict Priority, Weighted Round**-**Robin, and Deficit Round**-**Robin**.**

In **Strict Priority**, the QoS scheduler allows the highest priority queue to preempt other queues as long as there are still packets waiting to be transmitted in the highest priority queue. This mode guarantees that traffic in the highest queue is always transmitted first. Only if the high priority queues are empty, the lower priority queues can be transmitted**.** Queue 0 **(**Q0**)** to Queue 7 **(**Q7**)** are ranked from the lowest priority queue to the highest priority queue**.** Therefore, packets in Q7 will be all transmitted first before packets in Q6, and packets in Q6 will all be sent first before packets in Q5, and so on in this order**.**

Weighted Round Robin (WRR) is the simplest approximation of generalized processor sharing **(**GPS**).** In WRR, each packet flow or connection has its own packet queue in a network interface controller**.** It ensures that all service classes have access to at least some configured amount of network bandwidth to avoid bandwidth starvation**.** But WRR has a limitation, as it is unfair with variable length packets**.** It only provides the correct percentage of bandwidth to each service class only if all of the packets in all the queues are the same size or when the mean packet size is known in advance**.** Usually, a weight of each queue is set proportion to requested bit rate**.** Each queue is served proportionally to its weight for a service cycle**.**

Deficit WRR (DWRR) addressed the limitation of WRR on unfairness over variable size**.** Each queueis configured with a weight, a deficit counter **(**total number of bytes that the queue is permitted to transmit each time visited by the scheduler**)** , and a quantum of service **(** bytes**) .** DWRR scans all non**-** empty queues in sequence**.** When a non**-** empty queue is selected, its deficit counter is incremented by its quantum value**.** Then, the value of the deficit counter is the maximal amount of bytes that can be sentat this turn**.** If the deficit counter is greater than the packet' s size at the head of the queue, this packet can be sent and the value of the counter is decremented by the packet size**.** Then the size of the nextpackets is compared to the counter value**.** Once the queue is empty or the value of the counter is insufficient, the scheduler will skip to the next queue**.** If the queue is empty, the value of the deficit counter is reset to 0**.** If the packet size is too small, the scheduler has to visit queues too many times before serving a queue**.** But if the packet size is too large, some short term unfairness may arise**.** It is fair only over a time scale longer than a round time**.** At the shorter time scale, some flows may get moreservice**.** Small packet size or high transmission speed reduce the round time**.**

Figure 2.48 depicts the QoS Setting webpage. By default, the QoS in the managed switch works under the Strict Priority mode. For Weighted Round Robin, packet weights of Q0 to Q7 are set in term of packet as followings.

- COS Q0 = 2 packets
- COS Q1 = 1 packet
- COS Q2 = 4 packets
- COS Q3 = 8 packets
- COS Q4 =16 packets
- COS Q5 = 32 packets
- COS Q6 = 64 packet
- COS Q7 = 127 packets

Weight of Deficit Round Robin is double the number of packets of WRR, but it is in term of Kbytes instead as shown in the last column of Figure 2.48.

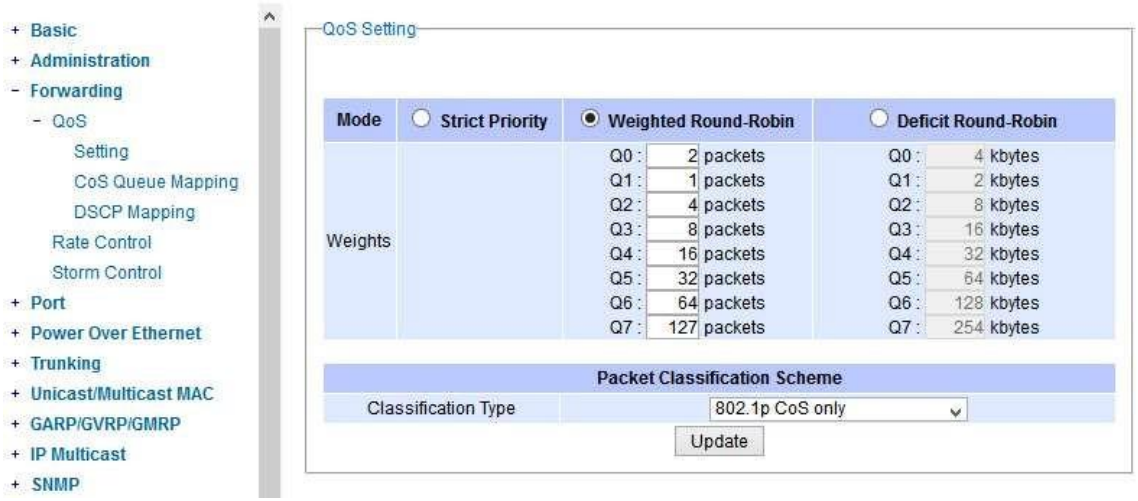


Figure 2.48 QoS Setting Webpage

At the bottom of the QoS Setting webpage in Figure 2.48, the users can select the packet classification scheme that will be used by the managed switch. There are two classification types to choose from the drop-down list: **802.1p CoS only** or **Both 802.1p CoS and DiffServ**. The default classification type is **802.1p CoS only**. Note that after changing the schedule discipline, setting the desired weights if any for the WRR or DWRR, or selecting the classification type, please click on the **Update** button to enable them on the switch.

2.4.1.2 CoS Queue Mapping

802.1p CoS is the QoS technique developed by the IEEE P802.1p working group, known as Class of Service (CoS) mechanism at Media Access Control (MAC) level. It is a 3-bit field called the priority code point (PCP) within an Ethernet frame header (Layer 2) when using VLAN tagged frames as defined by IEEE 802.1Q. It specifies a priority value between 0 and 7 that can be used by QoS to differentiate traffic. When this option is enabled, the switch inspects the 802.1p CoS tag in the MAC frame to determine the priority of each frame.

The switch can classify traffic based on a valid 802.1p (CoS – Class of Service) priority tag. These options allow users to map Priority Code Point (PCP) within an Ethernet frame header to different CoS priority queues as shown in Figure 2.49. The user can choose the desired CoS Priority Queue from the drop-down list from Q1 to Q7 for each PCP value. Descriptions of priority queue in CoS Queue Mapping page are summarized in Table 2.13.

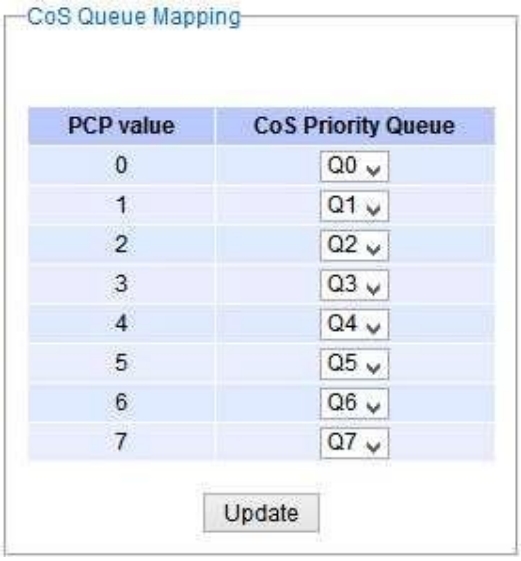


Figure 2.49 Mapping Table of CoS Webpage

Table 2.13 Priority queue descriptions

Label	Description	Factory Default
PCP	Priority Code Point within the Ethernet frame header. PCP 0 is the lowest priority and 7 is the highest priority.	PCP 0 -> Q0 PCP 1 -> Q0 PCP 2 -> Q1 PCP 3 -> Q1 PCP 4 -> Q2 PCP 5 -> Q2 PCP 6 -> Q3 PCP 7 -> Q3
CoS Priority Queue	The priority queue that a specific Ethernet frame needs to be assigned into.	

2.4.1.3 DSCP Mapping

DiffServ/ToS stands for Differentiated Services/Type of Services. It's a networking architecture that specifies a simple but scalable mechanism for classifying network traffic and providing QoS guarantees on networks. DiffServ uses a 6-bit Differentiated Service Code Point (DSCP) in the 8-bit differentiated services field (DS field) in the IP header for packet classification purposes. The DS field and ECN field replace the outdated IPv4 TOS field in IPv4 to make per-hop behavior decisions about packet classification and traffic conditioning functions, such as metering, marking, shaping, and policing.

The RFCs (Request for Comments) do not dictate the way to implement Per-Hop Behaviors (PHBs). Agatel implements queuing techniques that can base their PHB on the IP precedence or DSCP value inthe IP header of a packet. Based on DSCP or IP precedence, traffic can be put into a particular service class. Packets within a service class are treated the same way.

DiffServ allows compatibility with legacy routers, which only supports IP Precedence, since it uses the DiffServ Code Point (DSCP), which is the combination of IP precedence and Type of Service fields.

TOS (Type of Service) of the switch can be configured with the default queue weights as shown in Figure 2.50. Note that the TOS consists of DSCP (Differentiated Service Code Point (6 bits)) and ECN (Explicit Congestion Notification (2 bits)). The users can assign TOS values (**DSCP**) to predefined queue types (**Priority**) manually using DSCP Mapping web page in Figure 2.50. The priority number can be between 0 to 7 where the number 7 is the highest priority and 0 is the lowest priority. After assigning any new priority to a DSCP, please click the **Update** button at the bottom of the page to allow the new mapping to take effect.

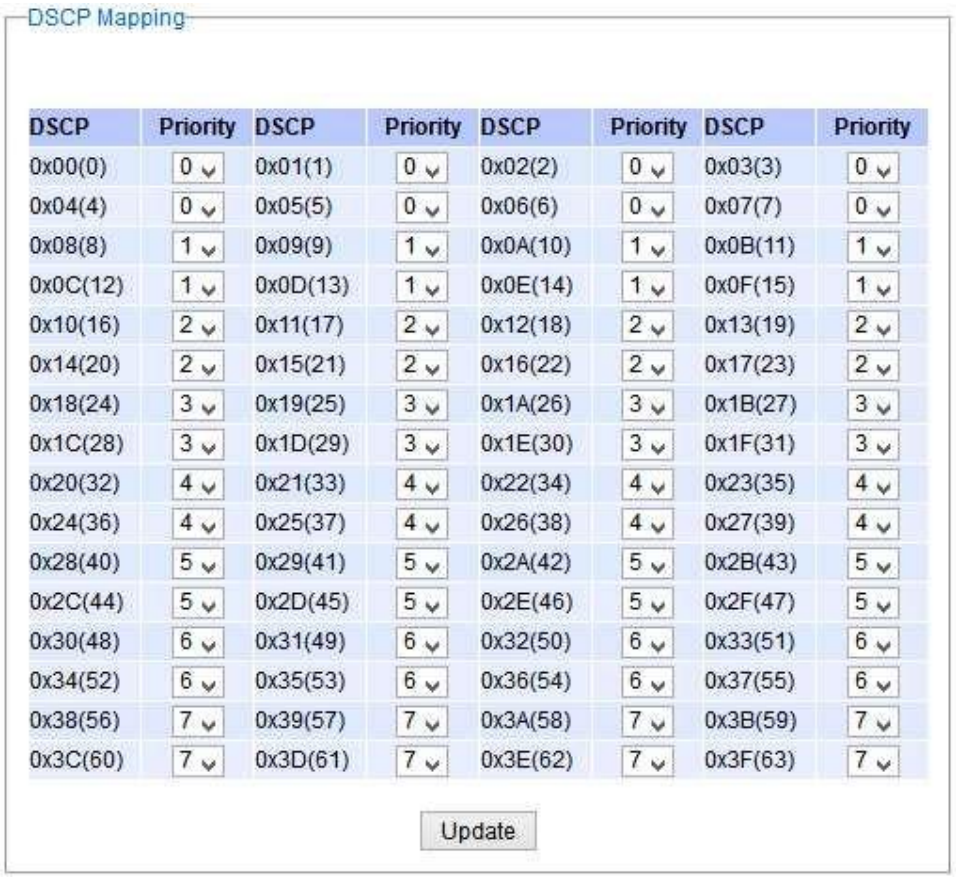


Figure 2.50 Mapping Table of DSCP and ECN Webpage

2.4.2 Rate Control

The users have options to set the Rate Control for each port on the managed switch as shown in Figure 2.51. The rate control mechanism will set a limit or maximum data rate which the port can transmit. Moreover, the rate control can be imposed on both directions: the incoming traffic (**Ingress**) and the outgoing traffic (**Egress**). However, there are some restrictions on the values that can be set on these two rate control parameters. Here is the summary of the rules for Rate Control settings:

- The outgoing (Egress) and incoming (Ingress) values have to be set between 0 and 102,400 (for 100 Mbps) or 1,024,000 (for 1000 Mbps).
- The value 0 is set to turn off the rate control mechanism.
- The values have to be integer and multiple of 64 when the transmission rate is less than 1,792

Kbps. For example: 64 Kbps, 128 Kbps, 512 Kbps, and 1,792 Kbps.

- The values have to be integer and multiple of 1,024 when the transmission rate is between 1,792 Kbps and 102,400 Kbps (for 100Mbps) or 106,496 Kbps (for 1000M). Ex: 2,048Kbps, 3,072 Kbps… 102,400Kbps.
- The values have to be integer and multiple of 8,192 when the transmission rate is greater than 106,496 Kbps.

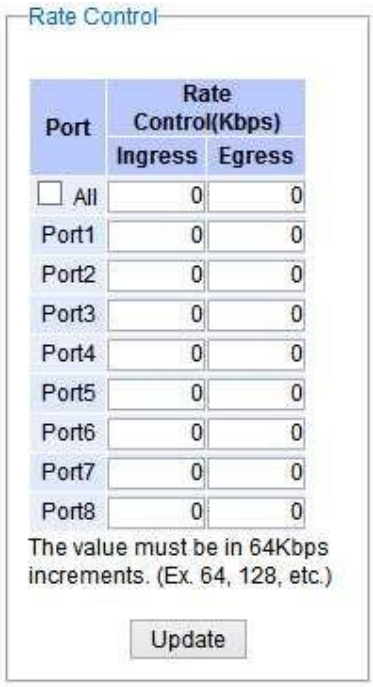


Figure 2.51 Rate Control Webpage

Table 2.14 provides descriptions of rate control setting. Note that after configuring the rate control in each port, please click on the **Update** button to enable it on the switch.

Table 2.14 Descriptions of Rate Control Setting

Label		Description	Factory Default
Port		Port number on the managed switch.	-
Rate Control (Kbps)	**Ingress**	Sets limits on its transmission rates for the incoming (**Ingress**) traffic. Note that the unit is in kilo-bits per second (Kbps).	0 (Disabled)
	Egress	Sets limits on its transmission rates for the outgoing (**Egress**) traffic. Note that the unit is in kilo-bits per second (Kbps).	0 (Disabled)

2.4.3 Strom Control

This subsection provides the storm control or storm filter features of the managed switch. Storm control prevents traffic on a LAN from being disrupted by ingress traffic of broadcast, multicast, and destination lookup failure (DLF) on a port. Figure 2.52 depicts the Strom Control webpage. The users can impose the same limiting parameters on all ports at the same time by clicking on the box in front of the **all** line and set the storm control data rate under each limiting columns (DLF, Multicast, Broadcast). The storm control limiting can also be independently control on each port. Note that the limiting value of 0 means that the storm control is disable and the value must be in multiples of 64kbps. Additional ingress storm traffic will be dropped after the limit has reached.

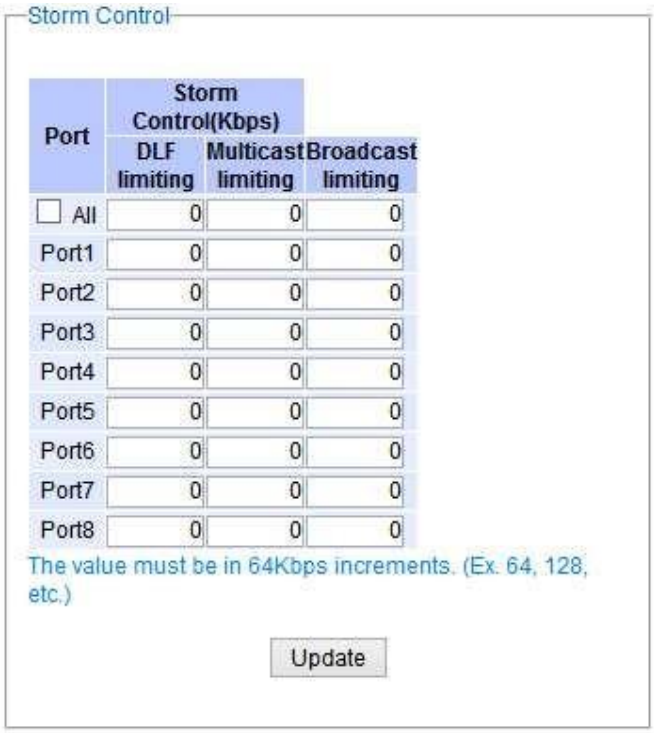


Figure 2.52 Strom Control Webpage

Table 2.15 summarizes the descriptions of storm control.**Error! Reference source not found.** Table 2.16 summarizes the descriptions of limiting parameters for storm control.

Table 2.15 Descriptions of Strom Control

Label	Description	Factory Default
All	Enable or Disable the storm control or filter on all ports at the same time. The limiting data rate for each type of storm packets (**DLF**, **Multicast**, and **Broadcast**) can be controlled by changing the number under each column. Note that the value must be in multiples of 64kbps.	Uncheck and Disable
Port1 - Port8	Set the limiting data rate of storm packets that can be controlled for each Port, which are **DLF**, **Multicast**, and **Broadcast**. Note that the value must be in multiples of 64kbps. See notes below for the detailed description and comparison.	Disable

Table 2.16 Descriptions of Limiting Parameters

Label	Description	Factory Default
DLF limiting (Destination Lookup Failure)	DLF limiting (0~9876480) Kb	0 (Disable)
Multicast limiting	Multicast limiting (0~9876480) Kb	0 (Disable)
Broadcast limiting	Broadcast limiting (0~9876480) Kb	0 (Disable)

Type of Storm Packets:

- **DLF**: **D**estination **L**ookup **F**ailure. The switch will always look for a destination MAC address in its MAC Table first. In case that a MAC address cannot be found in the Table, which means DLF occurs, the switch will forward the packets to all ports that are in the same LAN.
- **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. Network devices 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 helps reducing high traffic volumes due to large number of destinations, using network bandwidth efficiently.
- **Broadcast**: Messages are sent to all devices in the network.

2.5 Port

Agatel's industrial managed switch provides full control on all of its network interfaces. In this section, theusers can enable or disable each port and set preferred physical layer mode such as copper or fiber. Moreover, the users will be able to configure negotiation mechanism, data rate (speed), duplexing, andflow control for each port. All port's status and statistics can be viewed in this section. Figure 2.53 illustrates the Port webpage. The Port section is subdivided into four subsections which are:

- **Port Setting**
- **Port Status**
- **Mini-GBIC Port Status**
- **Port Statistics**

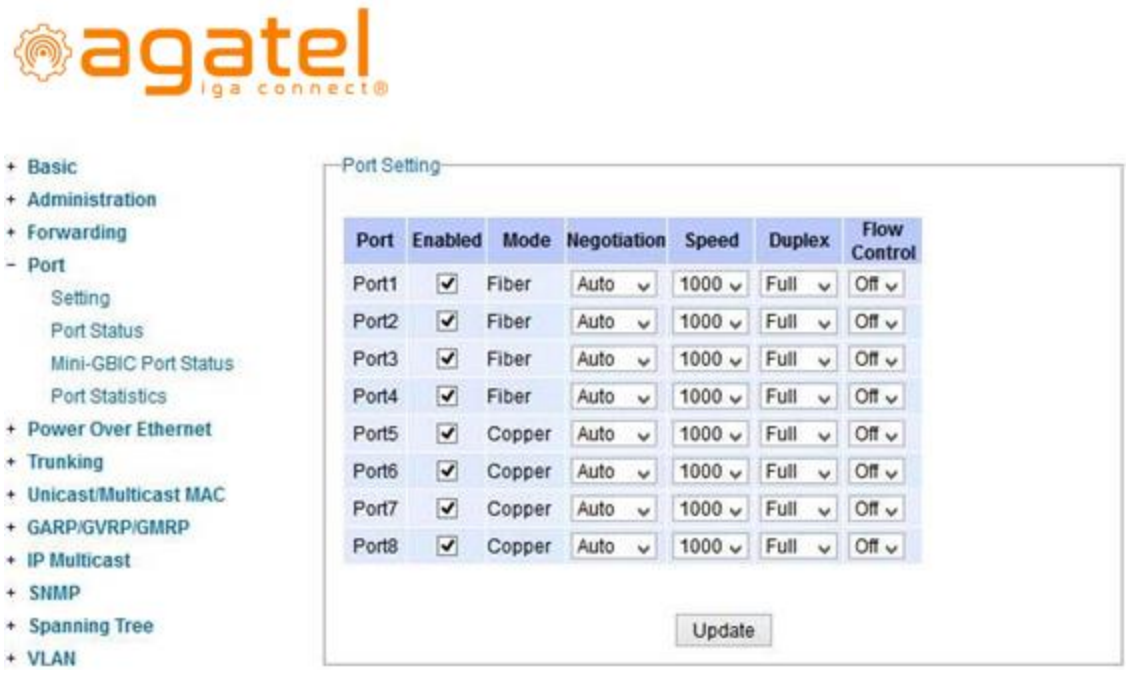


Figure 2.53 Port Dropdown Menu

2.5.1 Port Setting

Port Setting webpage is shown in Figure 2.54. The users can control the state of each port by checking on the corresponding **Enable** box. The possible physical layer connections of each port are listed on the **Mode** column. In some of Agatel's managed switches (XE75xx Series), the users can then select one of the physical media to be a preferred mode of operation. For instance, a gigabit Ethernet port (PortG1) can support either copper or fiber physical layer connections. The users can click on the radio button behind the Fiber option to set the fiber optical mode as its preferred physical medium connection. Notethat when both modes are selected, this means that the port is a combo port. However, the example in

Figure 2.54 is based on XEG7508-4P-4S which does not have a combo port and cannot select preferred mode of operation.

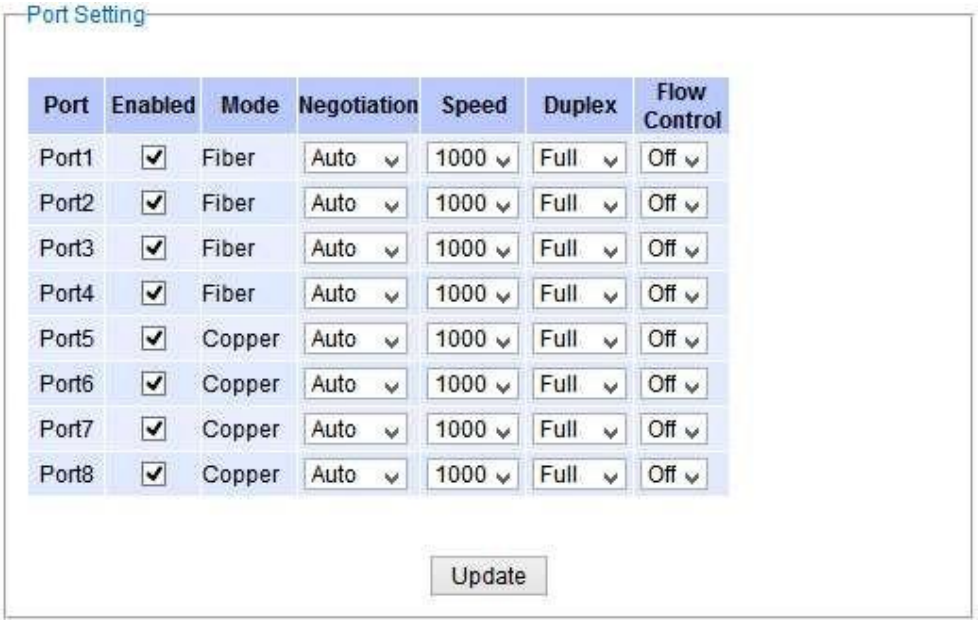


Figure 2.54 Port Setting Webpage

Next on the fourth column of Figure 2.54, the users can select from the dropdown list the port's **Negotiation** mechanism which can be either **Auto** or **Force**. When selecting the **Force** negotiation, the port's speed and duplexing will be locked to the settings configured by the users. On the other hand, the **Auto** negotiation will allow the switch to determine the actual speed and duplexing for that port. Note that the Gigabit Small Form-factor Pluggable (SFP) Port of the XE Series switch is downward compatible with 125/155Mbps Transceivers; however, the speed needs to be set to 100 manually. The Gigabit SFP Port of the XEG/XEM Series is not downward compatible.

On the fifth column, the transmission **Speed** of each port can be chosen from the dropdown list which could be **10**, **100**, or **1000** Mbps. The default speed is set to the highest possible rate in Mbps. Next the port's duplexing (**Duplex**) can be either **Full** duplex or **Half** duplex. The **Half duplex** option allows one-way communication at a time, while the **Full duplex** option allows simultaneous two-way communication.

Each port can set the **Flow Control** mechanism to either **On** or **Off** on the eighth column. This flow control will be useful to avoid packet loss when there is a network congestion. However, the **Flow Control** setting is **Off** by default. After configuring the port setting, please click on the **Update** button to enable any of your new configuration on the switch. Descriptions of port setting options are summarized in Table 2.17.

Table 2.17 Descriptions of Port Settings

Label	Description	Factory Default
Port	Port number on the managed switch.	-
Enable	Check the box to allow data to be transmitted and received through this port	All ports are enabled
Mode	Copper and/or Fiber modes. When both Copper and Fiber are listed, it means that this is a Combo port	Depend
Negotiation	Choose from either **Force** or **Auto**. See description in the paragraph above.	Auto-negotiation is enabled to all ports.
Speed	Select either **10**, **100,** or **1000**Mbps	Highest Speed
Duplex	Select either **Half** or **Full Duplex.** See description in the paragraph above.	Full-Duplex
Flow Control	Either **on** or **off.** The **Flow Control** mechanism can be enabled (**On**) to avoid packet loss when congestion occurs.	Off

2.5.2 Port Status

The overview of port status on the managed switch can be viewed in this webpage. The users can compare the actual status and the configured options described in previous subsection for each port. The rate control (ingress and egress) can be configured based on the instructions on Section 2.4.2. Figure 2.55 shows the Port Status webpage. Note that the last column also reports the security status whether it is turned on or off on each port, which can be either static security or 802.1x (See how to set security option for each port in Section 2.14). To check the latest status of all port, click the **Refresh** button either on the top or the bottom of the webpage.



Figure 2.55 Port Status Webpage

The header in each column and its possible values of the ports's status are listed here:

- **Mode** (Copper (C) or Fiber (F))
- **Enable** (Yes or No)
- **Link** (Up or Down)

- **Negotiation** (Auto or Force)
- **Speed** (unit: Mbps)
- **Duplex** (Full or Half)
- **Flow Control** (On or Off)
- **Rate Control** (On or Off)
- **Security** (On or Off): Either static security or 802.1x port security is turned on or off.

2.5.3 Mini-GBIC Port Status

The Small Form-factor Pluggable (SFP) port is sometimes referred to as a Mini-GBIC (**G**iga **B**itrate **I**nterface **C**onverter). In this subsection, all Mini-GBIC ports status can be shown if supported by the managed switch. Figure 2.56 depicts the Module (or Mini-GBIC Port) Status webpage. Note that the status here only provides the Ethernet compliance codes and vendor name. The link status (up or down) can be viewed in the previous subsection.



Figure 2.56 Mini-GBIC Port Status Webpage

2.5.4 Port Statistics

The Port Statistics are summarized in this webpage as shown in Figure 2.57. The users can use this subsection to help them diagnose the problem such as link quality of each port. The key statistics are the total number of normal (**OK**) frames, the number of discarded (**Error**) frames, and the speed of the transmission (**Rate** in Bps) for both transmitted (**Tx**) and received (**Rx**) traffic in each port. To clear or reset all the statistics to zero on this page, click on the **Clear** button. To obtain the latest statistics on this page, click on the **Refresh** button.

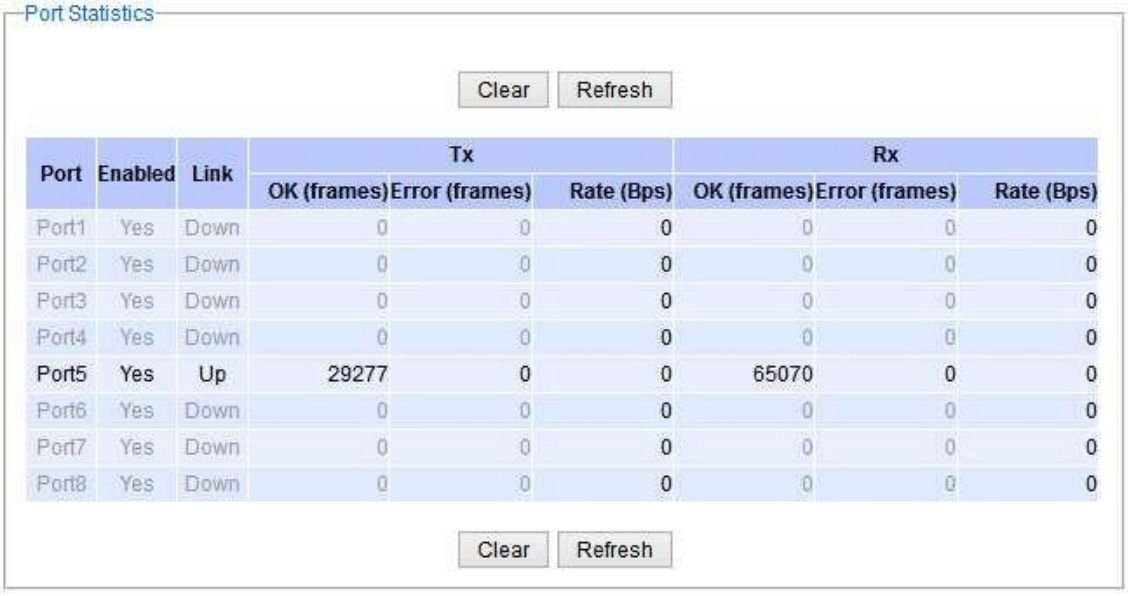


Figure 2.57 Port Statistics Webpage

The header in each column and its possible values of the ports's statistics are listed here:

- **Enable** (Yes or No): The port is enabled (Yes) or disabled (No).
- **Link** (Up or Down): Actual link status of the port.
- **Tx OK (frames)**: Total number of packets transmitted**.**
- **Tx Error (frames)**: The number of outbound packets which were chosen to be discarded even though no errors have been detected to prevent them from being transmitted.
- **Tx Rate (Bps)**: Speed of transmission in Bytes per second.
- **Rx OK (frames):** Total number of packets **(**not including faulty packets**)** received**.**
- **Rx Error (frames):** Total number of faulty packets **(**including Oversize, Undersize, Frame Check Sequence (FCS), Alignment, Jabber and Fragment Errors in packets**)** received**.**
- **Rx Rate (Bps)**: Receiving speed in Bytes per second.

2.6 Power over Ethernet

Power over Ethernet (PoE) is an optional function for the managed switches which enables the switch to provide power supply to end devices called Powered Device (PD) connected on the other side of the Ethernet ports. This means that the electrical power is delivered along with data over the Ethernet cables. This will be useful for the end devices that are located in the area that has no power supply and the users can save additional wiring for the end devices. To find out whether this function is supported or not by your managed switch, please look for the keyword “PoE” in Agatel’s model name. If the switch has “PoE” in its model name, it means that the switch is a Power Sourcing Equipment (PSE) that can provide power output to a Powered Device (PD). Figure 2.58 shows the Power over Ethernet dropdown menu.

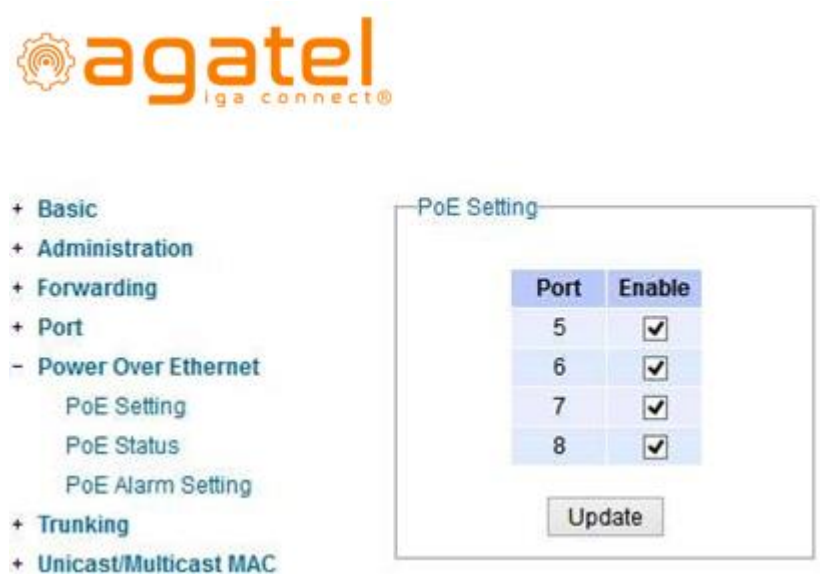


Figure 2.58 Power over Ethernet Dropdown Menu example on XEG7508-4S-4P

2.6.1 PoE Setting

The PoE function for each port in the supported managed switch model can be set in this webpage as shown in Figure 2.59. The users can check the **Enable** box for corresponding port. Please also click on the **Update** button to allow the setting on PoE taking effect on the switch.



Figure 2.59 PoE Setting Webpage example on XEG7508-8P

Note that the number of ports depends of the XEG model of the user's managed switch.

Table 2.18 Descriptions of PoE Setting

Label	Description	Factory Default
Port1	Enable or Disable PoE function of the Port 1	Enable
Port2	Enable or Disable PoE function of the Port 2	Enable
Port3	Enable or Disable PoE function of the Port 3	Enable
Port4	Enable or Disable PoE function of the Port 4	Enable
Port5	Enable or Disable PoE function of the Port 5	Enable
Port6	Enable or Disable PoE function of the Port 6	Enable
Port7	Enable or Disable PoE function of the Port 7	Enable
Port8	Enable or Disable PoE function of the Port 8	Enable

2.6.2 PoE Status

This webpage summarizes the status of each PoE port. For example, in Figure 2.60, **Port8** was enabled and is supplying power to a Class 2 Powered Device (PD) indicated under the **Classification** column. The PD device is rated at 49V and 33mA. The total power consumption for this PD is 1.617W. To check the status of the PoE port, please click on the **Refresh** button. Table 2.19 provides descriptions of each column in the table of PoE Status.

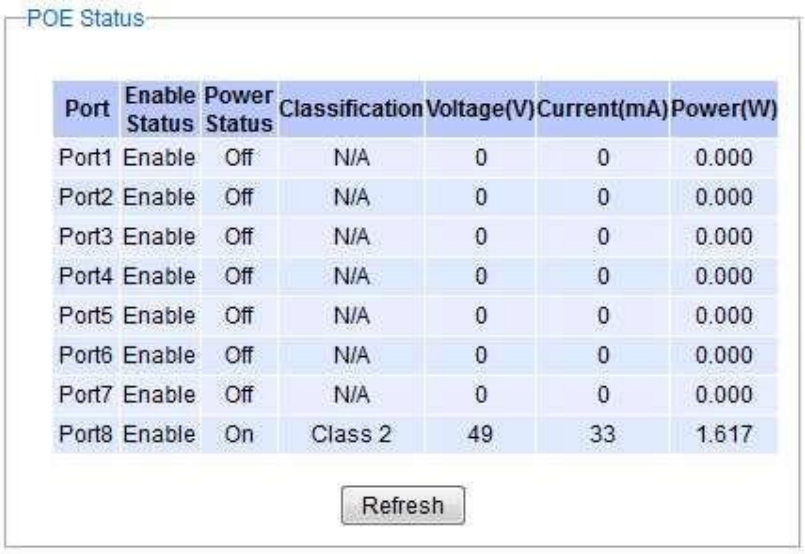


Figure 2.60 PoE Status Webpage, example on XEG7508-8P

Table 2.19 Descriptions of PoE Status

Label	Description	Factory Default
Port	Port number	-
Enable Status	**Enable** or **Disable** PoE function	Enable
Power Status	**On** when there is a power device on the other end or **Off** when there is no PD on the other end.	-
Classification	Display the classification of power device on the other end	-
Voltage (V)	Display the voltage supplied to this port in Volts	-
Current (mA)	Display the current supplied to this port in milli-Amperes	-
Power (W)	Display the power supplied to this port in Watts	-

2.6.3 PoE Alarm Setting [P3]

Alarm events can be set up to warn on unintended interruption in the PoE function or change(s) in status of the PoE power device (PD) or exceeding of total power level set in this webpage. Figure 2.61 shows the PoE Alarm Setting webpage in which the user can set the total power value in Watts that the managed switch can detect and trigger an alarm. Then, the uses will have options to enable all alarm events or individual alarm event. There are three categories of **PoE Alarm Event** listed here: **PoE PD Power On**, **PoE PD Power Off**, and **Detect Total Power**. The users also have choices for notification of the alarm(s) by Relay, Email, or Alarm LED. The user can check the corresponding box for each type of notification. Please refer to Table 2.20 for the descriptions of PoE Alarm Setting. Note that the alarm events can also be found in the Event Log (when “Enabled” is checked - see explanation in Section 2.20.1.2) or notified by Email (when “Email” is checked - see explanation in Section 2.20.2.2).

When “Relay”, “Alarm” and “Email” are checked, eventlog will show Warning/ Alarm log.



Figure 2.61 PoE Alarm Setting

Table 2.20 Descriptions of PoE Alarm Setting

Label		Description	Factory Default
Detect Total Power Value		Set the total power value in Watts which will trigger alarm event. Note that the value '0' means that the alarm event will not trigger.	0
Enable		Check the box(s) to enable alarm event	Unchecked
PoE Alarm Event	**Select All**	Check the box in front of this option to enable all alarm events	-
	PoE PD Power On	Check the box in front of this option to enable alarm event when PoE PD is power on.	-
	PoE PD Power Off	Check the box in front of this option to enable alarm event when PoE PD is power off.	-
	Detect Total Power	Check the box in front of this option to enable alarm event when managed switch can detect total power exceeding the value set in the **Detect Totalw Power Value** above.	-
Relay		Check the box in this column so that alarm will turn on an external relay circuit.	Unchecked
Email		Check the box in this column so that alarm will send out an email notification.	Unchecked
Alarm LED		Check the box in this column so that alarm will turn on an external LED circuit.	Unchecked

2.7 Trunking

The managed switch supports Link Trunking, which allows one or more links to be combined together as a group of links to form a single logical link with larger capacity. The advantage of this function is that it gives the users more flexibility while setting up network connections. The bandwidth of a logical link can be doubled or tripled. In addition, if one of links in the group is disconnected, the remaining trunked ports can share the traffic within the trunk group. This function creates redundancy for the links, which also implies a higher reliability for network communication. Figure 2.62 shows the Trunking dropdown menu.

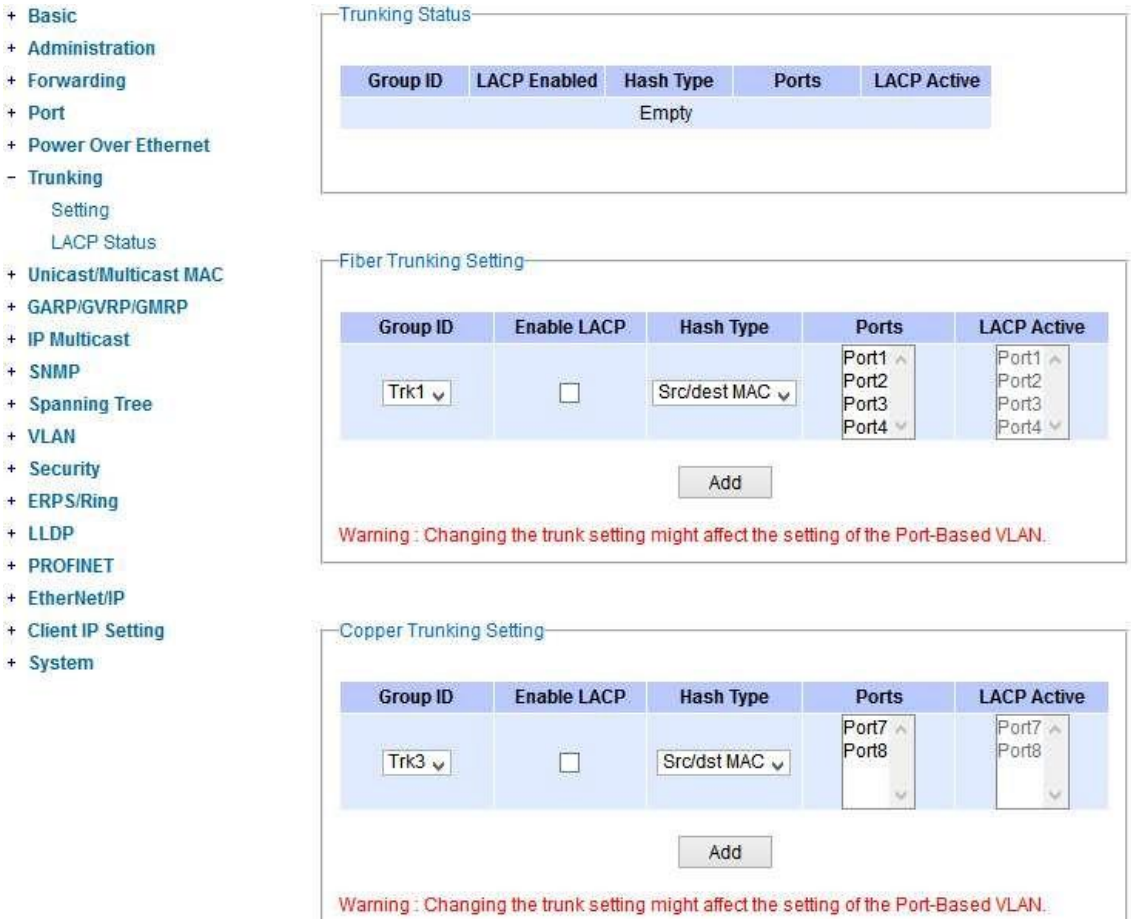


Figure 2.62 Trunking Dropdown Menu

2.7.1 Trunking Setting

In this subsection, the user can create new trunking assignment(s) and remove existing trunking assignment(s). Figure 2.63 illustrates the **Trunking Setting** webpage. The top part of the page called **Trunking** lists existing trunk(s) which can be removed by pressing the **Remove** button in the last column. Each line of the trunking provides information about the group of links (Trunk) based on **Group ID** labeled with **Trk*x*** where ***x*** is the integer number between 1 to 8. The managed switch can support up to 8 trunk groups. Note that for the difference media types (for example Fast Ethernet, Gigabit

Ethernet and Fiber), port trunking needs to be combined separately. Therefore, there are two sections for creating trunking: **Fast Ethernet Trunking Setting** and **Giga Ethernet Trunking Setting** as shown in the lower sections of the webpage.

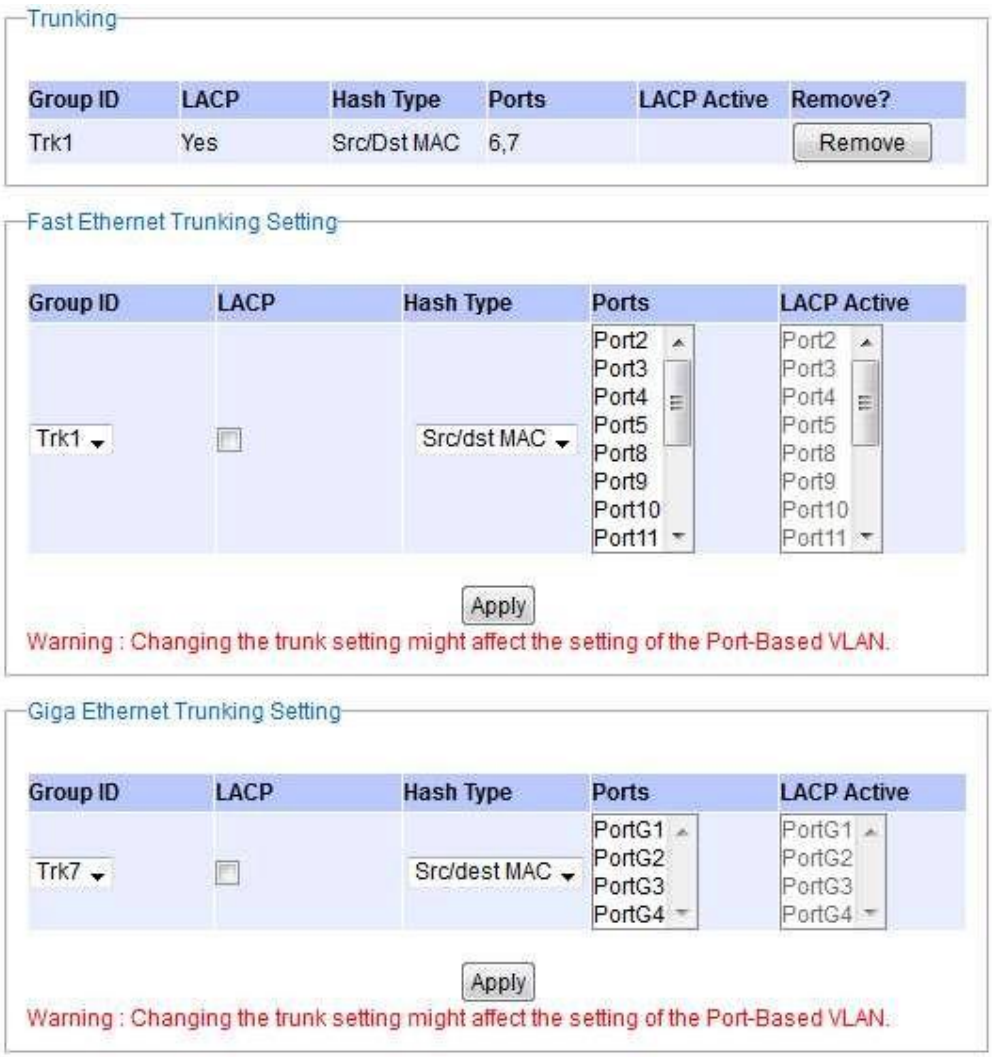


Figure 2.63 Trunking Setting Webpage, example with XE7520

The users have an option to enable Link Aggregation Control Protocol (LACP) which is an IEEE standard (IEEE 802.3ad, IEEE 802.1AX-2008) by checking on the box under the LACP column for each group. LACP allows the managed switch to negotiate an automatic bundling of links by sending LACP packets to the LACP partner or another device that is directly connected to the managed switch and also implements LACP. The LACP packets will be sent within a multicast group MAC address. If LACP finds a device on the other end of the link that also has LACP enabled, it will also independently send packets along the same links enabling the two units to detect multiple links between themselves and then combine them into a single logical link. During the detection period LACP packets are transmitted every second. Subsequently, keep alive mechanism for link membership will be sent periodically. Each port in the group can also operate in either LACP active or LACP passive modes. The LACP active mode means that the port will enable LACP unconditionally, while LACP passive mode means that the

port will enable LACP only when an LACP partner is detected. Note that in active mode LACP port will always send LACP packets along the configured links. In passive mode however, LACP port acts as "speak when spoken to", and therefore can be used as a way of controlling accidental loops (as long as the other device is in active mode). To enable trunking over multiple ports, the users can follow the steps below:

Step 1: Select Trkx (x = 1 to 8) from Group ID dropdown list.

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

Step 3: Select the Hash Type from the dropdown list.

Step 4: Select specific ports to be in this trunk group from the text box.

Step 5: Select specific ports in this trunk group to be LACP active.

Step 6: Click **Apply** button to set the configuration on the managed switch.

Descriptions of trunking settings are summarized in Table 2.21.

Table 2.21 Descriptions of Trunking Settings

Label	Description
Group ID	Up to 8 trunk groups can be created: Trk1~Trk8. Note that it is not possible to mix Fast Ethernet ports and Gigabit Ethernet ports into the same trunk group.
LACP	Enable/Disable LACP (**L**ink **A**ggregation **C**ontrol **P**rotocol). Brief explanation of LACP is discussed in previous paragraph.
Hash Type	The hash result determines which port to use for a specific frame. The available hash options are: Src MAC, Dst MAC, Src/dst MAC, Src IP, Dst IP, and Src/dst IP.
Ports	Specify the member ports for this trunking group. Please hold **Contro**l key to select more than one port at a time.
LACP Active	Specify which ports within the group should be in LACP Active mode. The ports that are not selected will be in LACP Passive mode.
Apply	Click **Apply** button to confirm the changes.
Remove	Click this button to remove any existing trunking group.

2.7.2 LACP Status

Figure 2.64 lists the current switch's trunking information. At the top of the page, the status of LACP on the managed switch is reported whether it is enabled or disabled. Next, the users can also specify the system priority here. LACP uses the system priority with the switch's MAC address to form the system ID and also during negotiation with its LACP partner. The LACP system ID is the combination of the LACP system priority value (defined in this webpage) and the MAC address of the managed switch. The system priority determines which managed switch makes the decisions on ports that will be bundled into a logical link. The lowest value determines who has higher priority and is in charge. The table of LACP status provides information per port which are port number, status of LACP, group ID, and LACP partner. Table 2.22 explains the descriptions of LACP status. To change system priority, enter the desired number in the number box behind the system priority field and then click **Update** button. To obtain the latest status of the LACP, click on the **Refresh** button.

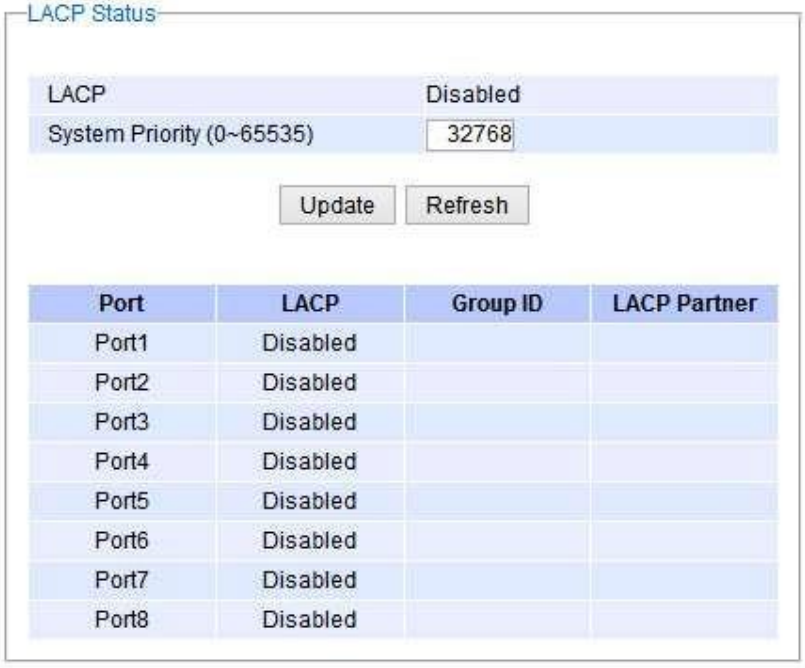


Figure 2.64 LACP Webpage

Table 2.22 Descriptions of LACP Status

Label	Description	Factory Default
System Priority	Indicate the system priority value of the managed switch in the range of 1 ~ 65535. System priority is used during the negotiation with other systems. System priority and switch's MAC address is used to form a system ID. Note that a higher number means a lower priority.	32768
Group ID	Show which trunk group that this port belongs to.	-
LACP	**Disabled:** LACP is disabled. **Passive:** LACP will only passively respond to LACP requests. **Active:** LACP will be actively searching for LACP Partner.	-
LACP Partner	Indicates whether a **LACP Partner** can be located on the other side.	-

2.8 Unicast/Multicast MAC

The managed switch is a network device which operate at the OSI layer 2 or medium access control (MAC) layer. It forwards frames of OSI layer 2 based on the MAC addresses. Generally, the layer 2 switch will learn about the destination MAC addresses of the end devices which are connected to the switch over time based on the exchanged traffic. For instance, in the beginning if the switch does not know which port a destination MAC address is, it will forward or broadcast a frame to all of its ports and wait for a response from end device connected to one of the port. This way the switch will learn of the MAC address and corresponding port number. Later on, the switch will forward the frame to the destination port only thus saving the traffic on other ports.

The managed switch typically maintains the learned MAC addresses in its memory which is usually called a MAC Address table. In this section, the managed switch allows the users to control the MAC Address table by adding static MAC addresses into the table or filtering certain MAC addresses so that they will not be forwarded by the managed switch. Agatel's manage switch also provides the users with the ability to set the MAC address age-out manually. Note that the age-out period is a duration of time that a learned MAC address will be maintained in the MAC address table before it was removed to save the memory.

The MAC addresses that can be managed by the switch can be both Unicast and Multicast MAC addresses. This section will briefly explain the concept of Unicast and Multicast forwarding as well as their benefits. Please see Figure 2.65 for illustrations of the Unicast versus the Multicast concept.

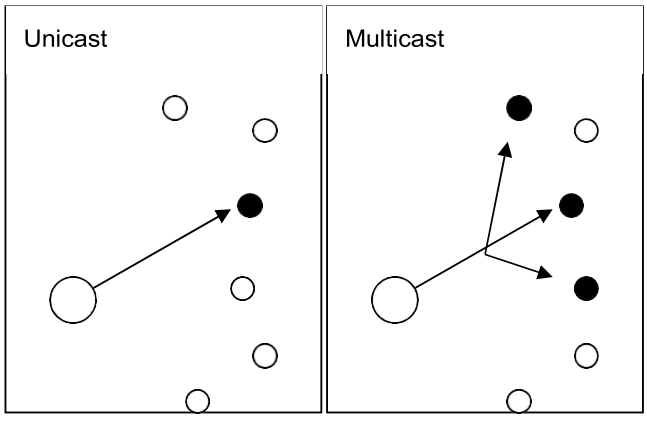


Figure 2.65 Unicast vs. Multicast

- **Unicast:** This type of transmission sends messages to a single network destination identified by a unique MAC address. This method is simple with one source and one destination.
- **Multicast:** This type of transmission is more complicated. It sends messages from one source to multiple destinations. Only those destinations or hosts that belong to a specific multicast group will receive the multicast packets. In addition, 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. Multicast filtering improves the performance of networks that carry multicast traffic.

Figure 2.66 shows the Unicast/Multicast dropdown menu which allows the users to manage and view the status of MAC address table.

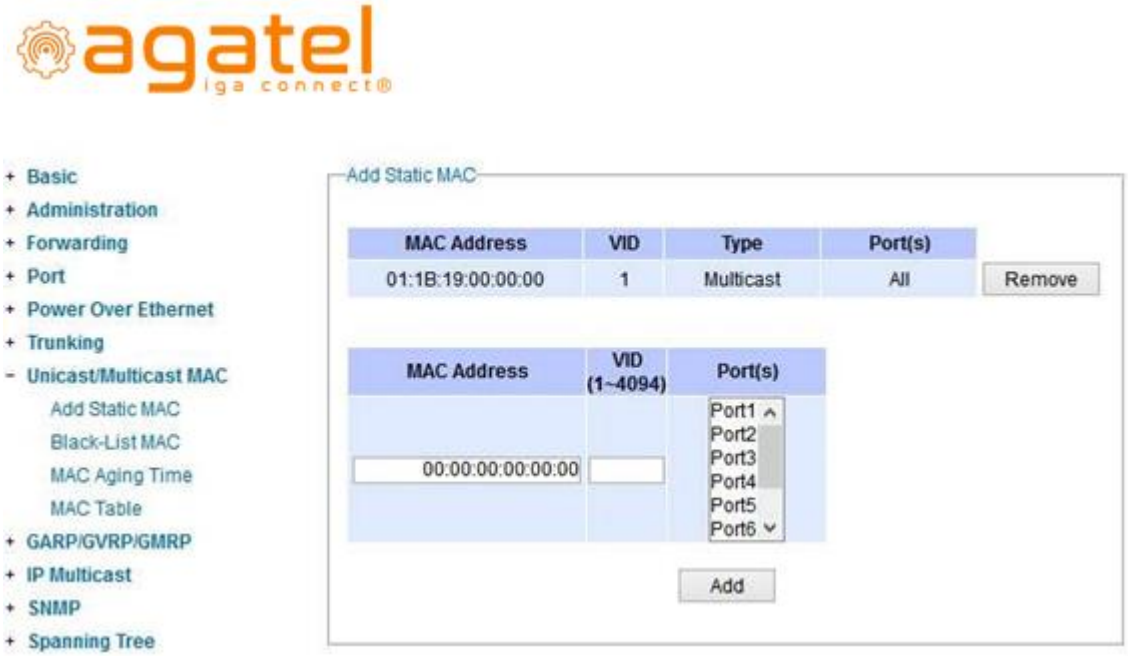


Figure 2.66 Unicast/Multicast Dropdown Menu

2.8.1 Add Static MAC

The managed switch allows the users to manually add static MAC addresses into its memory. The static MAC addresses will enable the managed switch to forward the traffic based on the MAC addresses in its memory to the destination port with specific virtual local area network (VLAN) identification (**VID**). Following the simple steps here to add a static MAC address.

Step 1: Enter a **MAC Address** which can be either Unicast or Multicast MAC Address.

Step 2: Specify VLAN ID (**VID**).

Step 3: Select the ports to apply this static MAC address. Use **Ctrl-key** to add more than one port.

Step 4: Click on **Add** button.

Figure 2.67 depicts the **Add Unicast/Multicast MAC** webpage. There is an example of a table of static MAC address in the upper part of the webpage where the last column of the table has **Remove** buttons for each entry. The users can remove any existing static MAC address by clicking on the **Remove** button. The lower part of the webpage is where the user can enter a new static **MAC address** along with its VLAN ID (**VID**) as outline by the procedure above. Table 2.23 summarizes the fields in this Add Static MAC webpage.

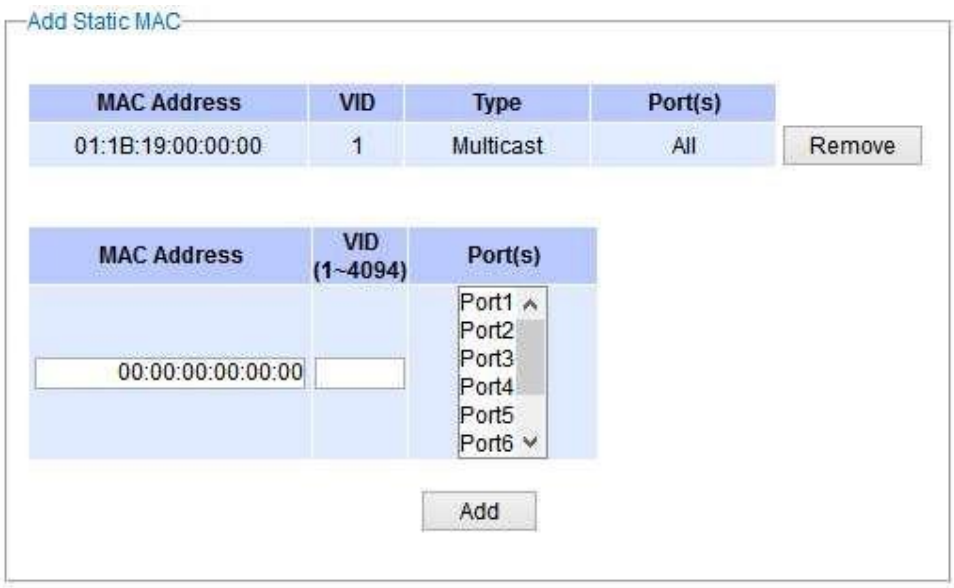


Figure 2.67 Add Static MAC Webpage

Table 2.23 Description of fields in Add Static MAC Webpage

Label	Description
MAC address	Enter a MAC address manually**.**
VID	Specify VLAN ID that this static MAC belongs to**. (**1 **–** 4096**)**
Type	Multicast or Unicast MAC address**.**
Port(s)	Define which ports to apply this static MAC address.
Add	Confirm and add the MAC address by clicking on this button
Remove	Click on this button to remove existing static MAC address in the table**.**

2.8.2 Black-List MAC

As discussed earlier, the managed switch also allows users to set MAC filtering manually. Figure 2.68 show the Black-List MAC webpage. The upper part of the page is the table of existing filtered MAC address where the users can remove the filter by clicking on the **Remove** button on each entry. The lower part of the page is where a new **source MAC address** that the users would like to filter can be entered into the MAC filtering table (black-list). Table 2.24 summarizes the fields in the **MAC Filter** webpage.



Figure 2.68 Black-List MAC Setting Webpage

Table 2.24 Descriptions of MAC Filtering Webpage

Label	Description
MAC Address	Enter MAC address to be black-listed or filtered manually.
Remove	**Remove** the corresponding entry in MAC filtering table.
Add	**Add** a MAC addresses to the MAC filtering table

2.8.3 MAC Aging Time

This function allows users to set MAC address age-out or aging time manually as shown in Figure 2.69. The users can specify the **Age-out Time** between 0 and 600 seconds in the following field. Note that the default value of age-out time is 300 seconds. In the managed switch, a MAC address table is stored in the memory to map a MAC address and a port number to forward frames. The aging time is the duration of time to keep MAC addresses in the MAC address table. For a longer aging time, the learnedMAC address will stay in the memory longer. As a result, the switch will be able to forward the framesto a specific port quickly instead of forwarding to all the ports to prevent frame flooding. A shorter agingtime will allow the switch to free up the old MAC addresses in the table to learn new MAC addresses. This will be useful when there are large number of MAC addresses (or end devices) in the network andwhen the traffic between any two end devices are short-lived.



Figure 2.69 MAC Aging Time Webpage

2.8.4 MAC Table

Information of current Unicast and Multicast MAC addresses in the memory (MAC Table) of the managed switch is displayed in this webpage as shown in Figure 2.70. The list of Unicast MAC addresses is shown first and follows by the list of Multicast MAC addresses. If there are more entries to be displayed, the users can click on the **Next Page** button to see other entries. The users also have an option to clear dynamic entries in the MAC address table by clicking on the **Clear Dynamic Entries** button at the bottom of the webpage. The descriptions of the MAC Address table are summarized in Table 2.25.

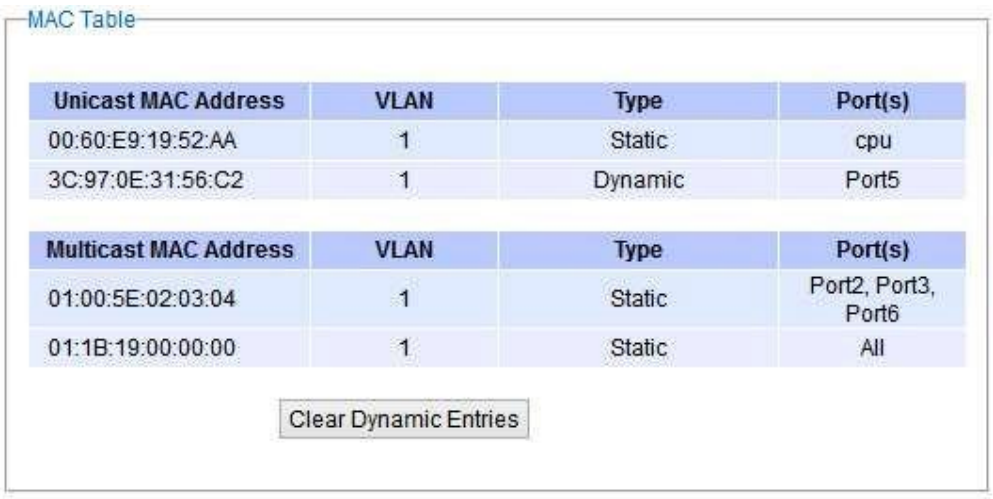


Figure 2.70 MAC Table Webpage

Note: the static multicast address can be set from "Add Static MAC" (Section 2.8.1) in "Unicast/Multicast MAC" (Section 2.8) or from "Static IP Multicast" (Section 2.10.2) in "IP multicast" (Section 2.10).

Table 2.25 Descriptions of MAC Address Table

Label	Description
Unicast/Multicast MAC	Displays MAC address.
VLAN	Displays VLAN ID.
Type	Displays whether the MAC address is dynamic or static. Note that dynamic is the address that is learned automatically, while static is the address that is entered by the users.
Ports	Displays which port that this MAC address belongs to.
Clear Dynamic Entries	Clears all Dynamic MAC addresses by clicking this button.
Next Page	Clicking on this button to continue to the next page when there are more MACs available.

2.9 GARP/GVRP/GMRP

This page includes three options, **GARP, GVRP, and GMRP** settings. Main concept of all three protocols are to eliminate unnecessary network traffic by preventing transmission/retransmission to unregistered users. These functions are enabled by default. They can only be disabled if no MAC addresses are added in the multicast group table.

GARP: Generic **A**ttribute **R**egistration **P**rotocol, previously called **A**ddress **R**egistration **P**rotocol, is a LAN protocol that defines procedures by which end stations and switches can register and de-register attributes, such as network identifiers or addresses with each other. Every end station and switch thus has a record, or list, of all the other end stations and switches that can be reached at a given time. Specific rules are used to modify set of participants in the network topology, or so called reachability tree.

GVRP: GARP **V**LAN **R**egistration **P**rotocol. GVRP is similar to GARP, but work with VLAN instead of other network identifiers. It provides a method to exchange VLAN configuration information with other devices, and conforms to IEEE 802.1Q.

GMRP: **G**ARP **M**ulticast **R**egistration **P**rotocol provides a mechanism that allows bridges (or switches in this case) and end stations to dynamically register group membership information with the MACs of bridges (switches) attached to the same LAN segment and for that information to be disseminated across all bridges (switches) in the Bridged (switched) LAN that supports extend filtering services. GMRP provides a constrained multicast flooding facility similar to IGMP snooping. The difference is that IGMP is IP-based while GMRP is MAC-based.



Figure 2.71 GARP/GVRP/GMRP Dropdown Menu

2.9.1 Multicast Group Table

In this subsection, the list of MAC addresses which were dynamically registered by GMRP into the Multicast Group Table can be viewed. The multicast group table in Figure 2.72 displays the following information for each MAC Address: VLAN ID (VID), Static Port(s), and GMRP Dynamic Port(s). The user can clear the table by clicking on the **Clear GMRP Dynamic Entries** button or obtain the latest update on the table by clicking on the **Refresh** button.

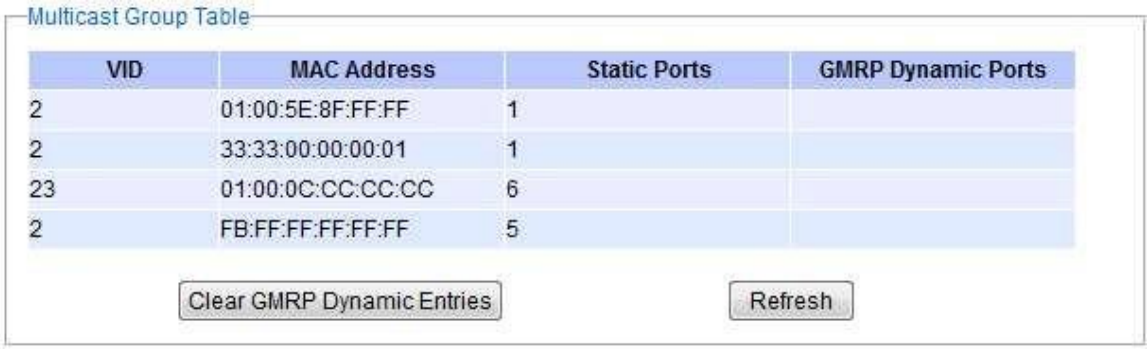


Figure 2.72 Multicast Group Table

2.9.2 GARP Setting

Figure 2.73 shows GARP Setting webpage where different Timers (Join, Leave, and LeaveAll) can be set. All devices that are exchanging attributes must set these timers to the same values. Note that the GARP Timer values are in multiple of 10 milliseconds. Table 2.26 summarized the descriptions and values of all Timers for GARP setting. Please click the **Update** button after setting your new values.



Figure 2.73 GARP Setting Webpage

Table 2.26 Descriptions of GARP Timer Settings

Label	Description	Factory Default
Join Timer	Indicates the GARP **Join timer,** in 0 ~ 65535 seconds**.**	200 milliseconds
Leave Timer	Indicates the GARP **Leave timer,** in 0 ~ 65535 seconds.	600 milliseconds
Leave All Timer	Indicates the GARP **Leave All timer**, in 0 ~ 65535 seconds.	10000 milliseconds or 10 seconds

2.9.1 GVRP Setting

In this section, GVRP can be enabled on the switch and then it can be enabled for all ports or specific port(s) and trunking group(s). The multicast IP address with designated VLAN ID can be accessed from each ports. Figure 2.74 and Figure 2.75 below illustrate GVRP Setting and Statistics. When GVRP is enabled, the switch which is an end node of a network needs to add static VLANs locally. Others switches can dynamically learn the rest of the VLANs configured elsewhere in the network via GVRP.



Figure 2.74 GVRP Setting Box with Port Enabling



Figure 2.75 GVRP Statistics

To enable GVRP in Figure 2.74, check the **Enabled**'s box and then select the desired port(s) by flagging the corresponding checkbox(es). Please click **Update** button to save the change to the switch. Figure 2.75 provides summarized statistics on the packet count of GVRP based on the following packet types: Rx Join Empty, Tx Join Empty, Rx Join In, Tx Join In, Rx Empty, Tx Empty, Rx Leave In, Tx Leave In, Rx Leave Empty, Tx Leave Empty, Rx Leave All, and Tx Leave All. To clear the statistics on this table, please click on the **Clear** button at the bottom of the table. Table 2.27 describes the GVRP setting's options.

Table 2.27 GVRP Setting Descriptions

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 defined trunking group (e.g. Trk1), it can also be selected to be enabled. If you check the **All** Port's box, all ports will be enabled**.**	All ports are disabled
Clear Statistics	Clears all GVRP statistics counts	Clears the record

2.9.2 GMRP Setting

The users can use this subsection to enable GMRP and enable GMRP for all ports or specified port(s) and trunking group(s) as shown in Figure 2.77. To enable GMRP in Figure 2.76, check the **Enabled**'s box and then select the desired port(s) by flagging the corresponding checkbox(es). Please click **Update** button to save the change to the switch.



Figure 2.76 GMRP Setting Box

The GMRP Statistics can also be viewed on the bottom of this page as shown in Figure 2.77. The GMRP Statistics provides summarized statistics on the packet count of GMRP based on the following packet types: Rx Join Empty, Tx Join Empty, Rx Join In, Tx Join In, Rx Empty, Tx Empty, Rx Leave In, Tx Leave In, Rx Leave Empty, Tx Leave Empty, Rx Leave All, and Tx Leave All. To clear the statistics on this table, please click on the **Clear** button at the bottom of the table. Table 2.28 briefly describes GMRP setting and statistics.

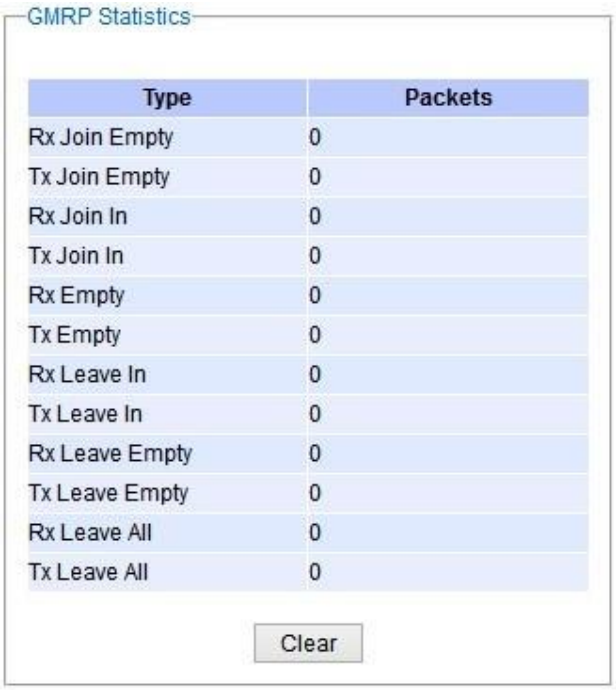


Figure 2.77 GMRP Statistics

Table 2.28 Descriptions of GMRP Settings and Statistics

Field	Field Description	Factory Default
GMRP	You can enable or disable GMRP by enabling the checkbox. To enables GMRP, the switch must be in 802.1q VLAN mode.	Disabled.
Port	You can enable or disable GMRP on specified ports by clicking the corresponding checkbox. If you have already defined trunking group (e.g. Trk1), you can also enable it. If you check the **All** Port's box, all ports will be enabled**.**	All Ports are disabled.
Clear Statistics	You can clear all GMRP Statistics	Clears the records

2.10 IP Multicast

The managed switch supports Internet Group Management Protocol (IGMP) which is a communication protocol used on IP version 4 networks to establish multicast group memberships among switches in the network. IGMP is an integral part of IPv4 multicast. It operates above the network layer of OSI model. One of the most important features related to this protocol is IGMP snooping, which is supported by the managed switch and greatly strengthens network functionality. The IGMP snooping is a process of "listening" to IGMP network traffic. By listening to conversations between different devices, it maintains a map of links and IP multicast streams. This means that multicast traffic may be filtered from the links of the managed switch which do not need them. Therefore, IGMP snooping enables the managed switch to only forward multicast traffic to the links that have requested it. This section contains two submenus as shown in Figure 2.80Figure 2.78 which are:

- **IGMP**
- **Static IP Multicast**
-



Figure 2.78 IP Multicast Dropdown Menu

2.10.1 IGMP

The **IGMP** (Internet Group Management Protocol) submenu is further divided into three options which are: **Setting**, **IP Multicast Table**, and **Statistics**. Figure 2.79 shows the three options under the IGMP submenu.



Figure 2.79 IGMP's Options

2.10.1.1 IGMP Settings

This webpage allows the users to set IGMP features on the managed switch as shown in Figure 2.80. There are three features that can be enabled: **IGMP Snooping**, **IGMP Proxy**, and **IGMP Fast-leave**. After checking the desired feature's boxes, please click on the **Update** button to allow the options to take effect. The lower part of the page lists **Router and Multicast Groups Information** which are router's IP and port information. Table 2.29 summarizes the descriptions of IGMP's Settings.



Figure 2.80 IGMP Setting Webpage

Table 2.29 Descriptions of IGMP's Settings

Label	Description	Factory Default
IGMP Snooping	Check the box to enable IGMP snooping.	Disabled
IGMP Proxy	Check the box to enable IGMP proxy. See note below.	Disabled
IGMP Fast-leave	Check the box 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, as shown in Figure 2.81. When it receives a membership query message from the router, it sends a membership report message to the router port. When it receives a membership report message from a computer in a new multicast group, it sends a membership report message back to the router port. When it receives a leave group message from a computer which is the only one in the group, it sends a leave group message to the router port and removes the computer from multicast group. Proxy is like a middle man that handles information about multicast group in between routers and computers.

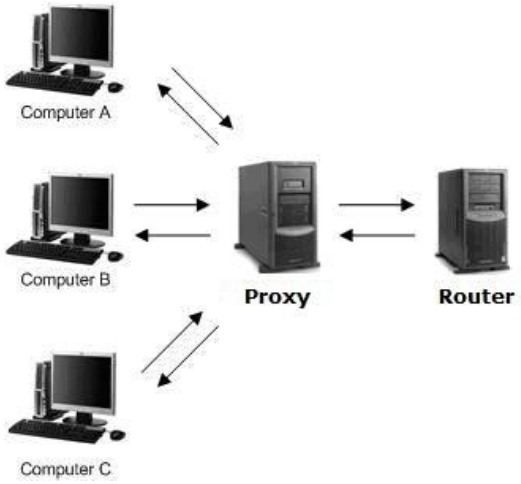


Figure 2.81 Example of IGMP Proxy

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

2.10.1.2 IGMP IP Multicast Table

This webpage provides information about IGMP membership table and IP multicast table. Figure 2.82 depicts the IGMP's IP Multicast Table webpage. The upper table is an IGMP membership table and the lower table is IP multicast table which contain both static configured IP multicast addresses and dynamically joined IP multicast addresses. The static configured port is manually added by the users, while the dynamically joined port is added by the managed switch's IGMP snooping feature. To get the latest update information on each table please click on the **Refresh** button.



Figure 2.82 IGMP's IP Multicast Table Webpage

Figure 2.83 shows examples of IGMP membership table and IP multicast table. Note that the display format in Figure 2.83 is from an early version of managed switch firmware which may have a slightly different display format from Figure 2.82. These tables are based on the information in the memory of the managed switch. The IGMP membership table contains IP Multicast Address, VLAN ID (**VID**), Joined Port (port number) and Life Time. Note that the Life Time is in the unit of second. The IP multicast table has only IP Multicast Address, VLAN ID (**VID**), and Joined Port. Note that the joined port can be labelled with (S) or (D) which refer to as Static Configured or Dynamically Joined, respectively.

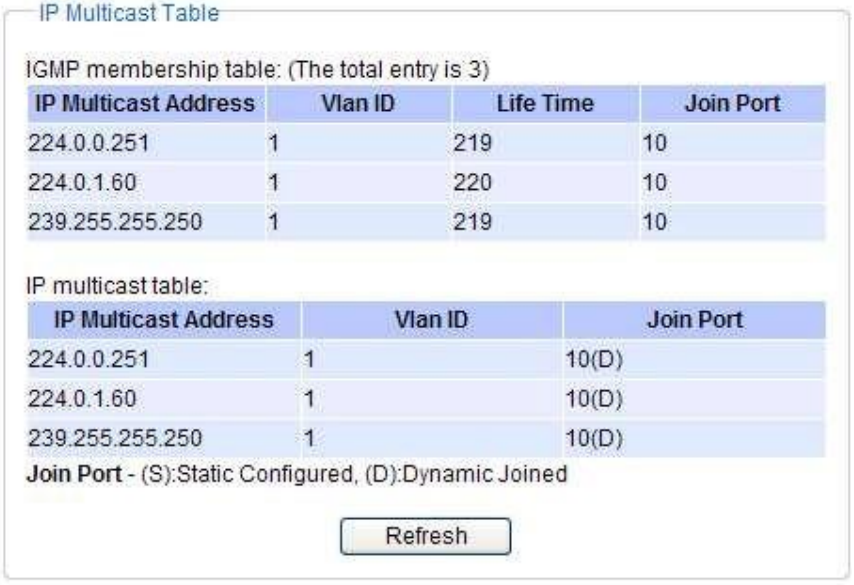


Figure 2.83 Example of IGMP's IP Multicast Table

2.10.1.3 IGMP Statistics

This webpage provides information about IGMP statistics as shown in Figure 2.84. The users can view the number of IGMP packets in different categories: Rx Total, Rx Valid, Rx Invalid, Rx General Queries,

Tx General Queries, Rx Group-Specific Queries, Tx Group-Specific Queries, Rx Leaves, Tx Leaves, Rx Reports, Tx Reports, and Rx Others. The users can reset the numbers in all categories by clicking on the **Clear** button.

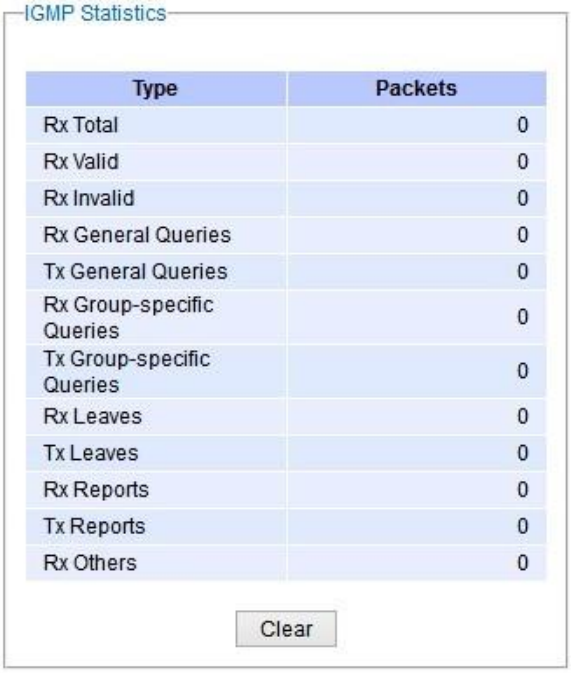


Figure 2.84 IGMP Statistics Webpage

Example of IGMP statistics are shown in Figure 2.85. Note that the display format in Figure 2.85 is from an early version of managed switch firmware which may have a slightly different display format from Figure 2.84. It shows the statistical values of IGMP packets which the managed switch received and transmitted over time. Table 2.30 summarizes the descriptions of the IGMP statistics.

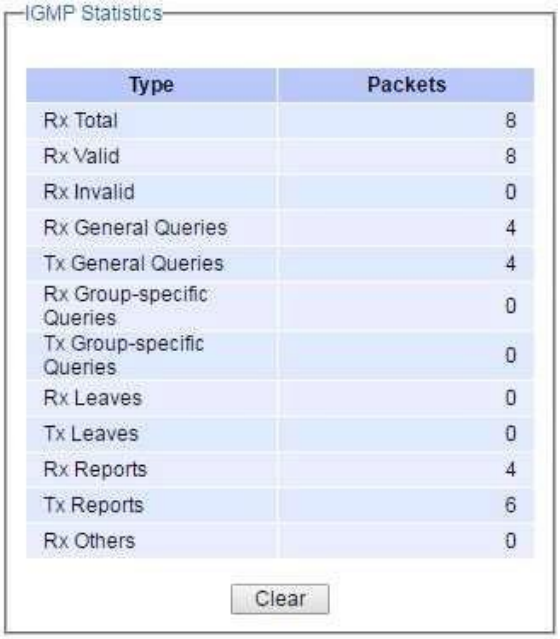


Figure 2.85 Example of IGMP's Statistics

Table 2.30 Descriptions of IGMP Statistics

Statistics Label	Description	Factory Default
Rx Total	Total number of IGMP packets received by the managed switch	-
Rx Valid	Number of valid IGMP packets received by the managed switch	-
Rx Invalid	Number of invalid IGMP packets received by the managed switch	-
Rx General Queries	Number of IGMP's Membership General Query packets received by the managed switch	-
Tx General Queries	Number of IGMP's Membership General Query packets transmitted by the managed switch	-
Rx Group Specific Queries	Number of IGMP's Membership Group Specific Query packets received by the managed switch	-
Tx Group Specific Queries	Number of IGMP's Membership Group Specific Query packets transmitted by the managed switch	-
Rx Leaves	Number of IGMP's Leave Group packets received by the managed switch	-
Tx Leaves	Number of IGMP's Leave Group packets transmitted by the managed switch	-
Rx Reports	Number of IGMP's Membership Report packets received by the managed switch	-
Tx Reports	Number of IGMP's Membership Report packets transmitted by the managed switch	-
Rx Others	Number of IGMP's other packets received by the managed switch	-

2.10.2 Static IP Multicast

This subsection allows the users to manually add new or remove existing static IP multicast and the joined port(s). Figure 2.86 shows the Static IP Multicast webpage where the upper part of the page is a table of existing IP Multicast Address entries and the lower part of the page contains the fields for adding new IP Multicast Address entry to the table. The users are required to supply the IP Multicast Address, VLAN ID (**VID**), and the lists of the port numbers which will join the static IP multicasting group (joined port).

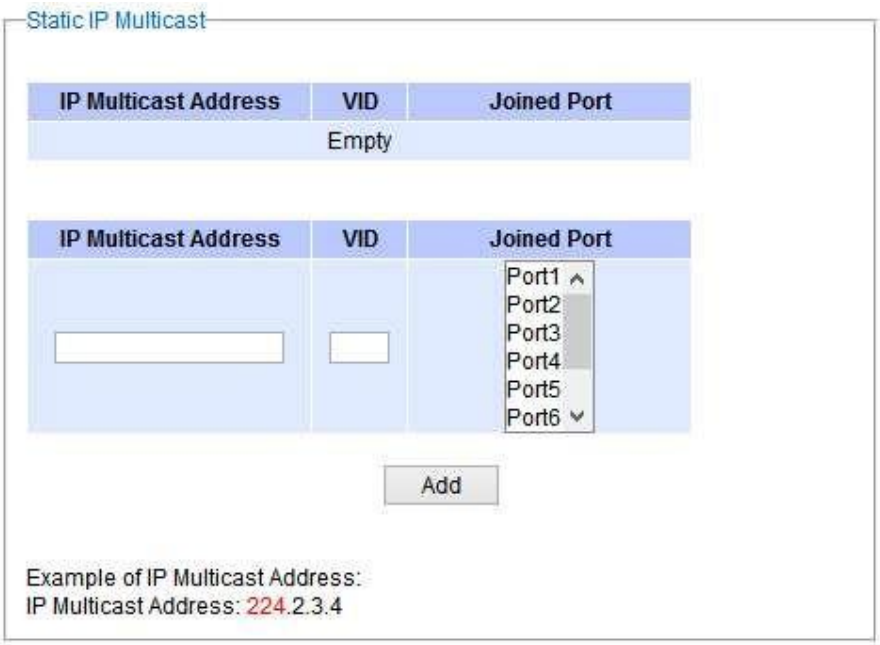


Figure 2.86 Static IP Multicast Setting Webpage

An example of an entry of IP multicast group is shown in Figure 2.87 where there is an existing IP Multicast Address of 224.2.3.4 which belongs to VLAN 1 and has port number 2, 3, and 6 in the group. The following procedures outline how to add a new IP multicast group. For example, an IP multicast group address is 224.1.1.1 and the joining ports are Port1, Port2 and Port5 with VLAN = 1.

- First, the users should enter the IP = 224.1.1.1 in the **IP Multicast Address** column.
- Then, the users should enter the VLAN ID = 1 in the VLAN ID (**VID**) column.
- Then, while holding the "Ctrl" key on the keyboard, click on all corresponding port numbers under the Join Port column (Port1, Port2, and Port5 in this example) to select which port(s) will join in the IP multicast group.
- Finally, click on the Add button. The IP address is then added as it shows on Figure 2.87.
- To remove an existing static IP multicast address from the table, click the Remove button of that entry.

These procedures are similar to the procedures for adding or removing the Unicast/Multicast MAC address explained in Section 2.8.1. The only difference is that the IP multicast address has the form of 224.XX.XX.XX. Note that IPv4 multicast address (Class D) is in between 224.0.0.0 and 239.255.255.255.

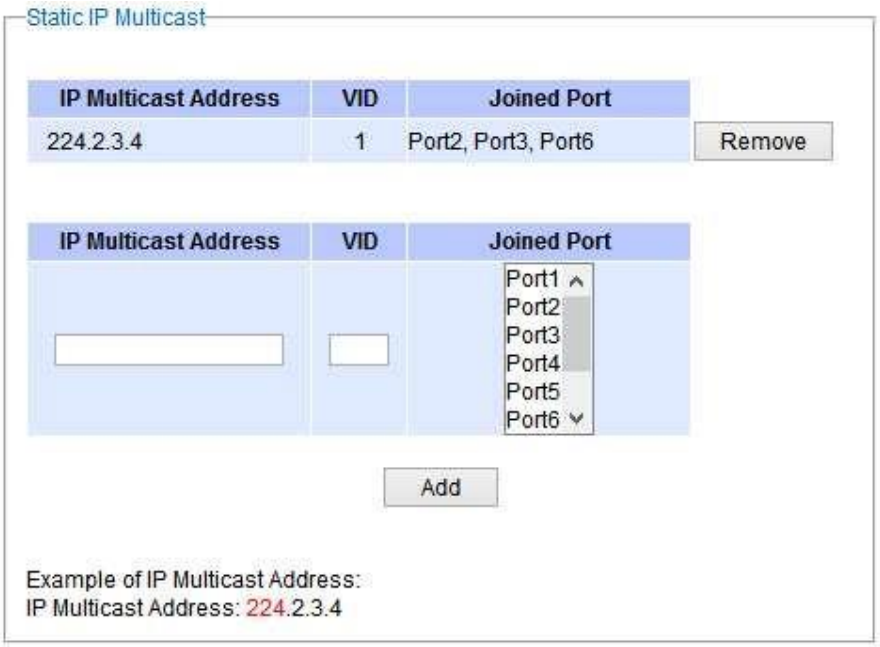


Figure 2.87 Example of Static IP Multicast Setting

2.11 SNMP

Simple **N**etwork **M**anagement **P**rotocol **(SNMP)** 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 or defined by the users**.** The SNMP is used by network management system or third-party software to monitor devices such as managed switches in a network to retrieve network status information and to configure network parameters. The Agatel's managed switch support SNMP and can be configured in this section. The SNMP setting has four categories and its dropdown menu is shown in Figure 2.88, which are**:**

- **SNMP Agent**
- **SNMP V1/V2c Community Setting**
- **Trap Setting**
- **SNMP V3 Authentication (Auth.) Setting**



Figure 2.88 SNMP Dropdown Menu

2.11.1 SNMP Agent

To enable SNMP agent on the managed switch, please check the **Enabled** box and click **Update** button as shown in Figure 2.89**.** The SNMP version 1 **(**V1**)**, version 2c **(**V2c**)** and version 3 are supported by Agatel**'**s managed switches as summarized in Table 2.31**.** Basically, SNMP V1 and SNMP V2c have simple community string based authentication protocol for their security mechanism, while SNMP V3 is improved with cryptographic security**.**

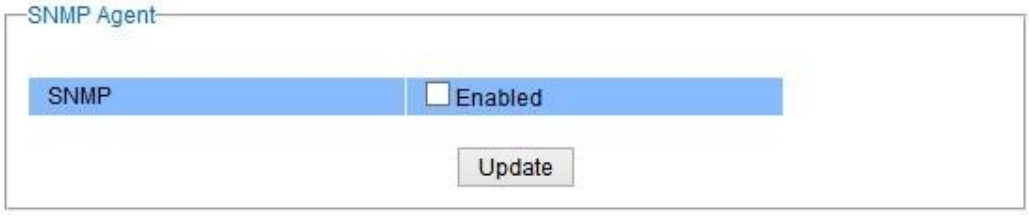


Figure 2.89 SNMP Enabling Box

Table 2.31 Description of SNMP Setting

Label	Description	Factory Default
SNMP	Check the box to enable SNMP V1/V2c/V3.	Disabled

2.11.2 SNMP V1/V2c Community Setting

The managed switch supports SNMP V1, V2c, and V3. SNMP V1 and SNMP V2c use a community string matching for authentication. This authentication will allow network management software to access the information or data objects defined by Management Information Bases (MIBs) on the managed switch. Note that this simple authentication is considered a weak security mechanism. It is recommended to use SNMP V3, if possible. There are two levels of authentications or permission type in XEG75XX series, which are read-all-only or read-write-all. For example, in our default setting as shown in Figure 2.90, an SNMP agent, which is a network management software module residing on the managed switch, can access all objects with read-all-only permissions using the string *public*. Another setting example is that the string *private* has permission of read-write-all.

This community string option allows the users to set a community string for authentication or remove existing community string from the list by clicking on the **Remove** button at the end of each community string item**.** The users can specify the string names on the **String** field and the type of permissions from the dropdown list as shown in Figure 2.90**.** Table 2.32 briefly provides descriptions of SNMP's community string setting.



Figure 2.90 SNMP Community Strings

Table 2.32 Descriptions of Community String Settings

Label	Description	Factory Default
(Community) Strings	Define name of strings for authentication. Max. 15 Characters.	**Public** (read-all-only) **Private** (read-write-all)
Permission Type	Choose a type from the dropdown list: read-all-only and read-write-all. See notes below for a briefed explanation.	-

***NOTE:**

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

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

2.11.3 Trap Setting

The managed switch provides a trap function that allows switch to send notification to agents with SNMP traps or inform. The notifications are based on the status changes of the switch such as link up, link down, warm start, and could start. For inform mode, after sending SNMP inform requests, switch will

resends inform request if it does not receive response within 10 seconds. The switch will try re-send three times. This option allows users to configure SNMP Trap Setting by setting the destination IP Address of the Trap server, Port Number of the Trap server, and Community String for authentication. Figure 2.91 shows these Tap Setting's options. The first line enables the users to select the Trap Mode which can be either **Trap** or **Inform**. Please click on the **Update** button after selecting the desired Trap Mode. After entering all required fields for Trap Setting in the last line, please click on the **Add** button. Table 2.33 summarizes the descriptions of trap receiver settings.

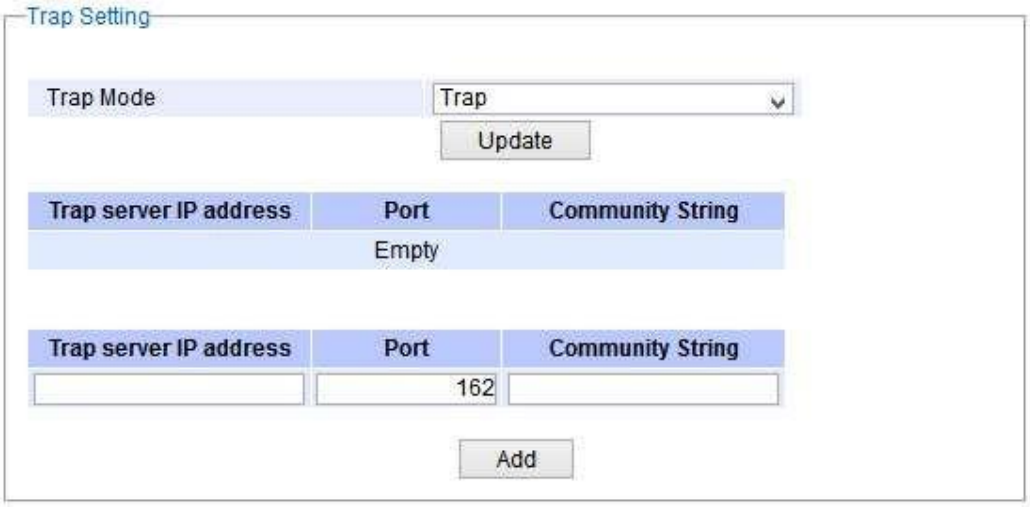


Figure 2.91 Example of Trap Receiver Setting

Table 2.33 Descriptions of Trap Receiver Settings

Label	Description	Factory Default
Trap Mode	Choose between Trap and Inform	Trap
Trap server IP address	Enter the IP address of your Trap Server**.**	NULL
Port	Enter the trap Server service port**.**	162
Community String	Enter the community string for authentication**.** Max. 15 characters.	NULL

2.11.4 SNMPv3 Auth. Setting

As mentioned earlier, SNMP V3 is a more secure SNMP protocol**.** In this part, the users will be able to set a password and an encryption key to enhance the data security**.** When choosing this option, the users can configure SNMP V3's authentication and encryption. MD5 (Message-Digest algorithm 5) is used for authentication password and DES (Data Encryption Standard) is used for data encryption algorithm. Figure 2.92 shows the SNMP V3 Authentication Setting' options. The users can view existing SNMP V3 users' setting on the upper table where it provides information about user name, authentication type, and data encryption. The users have an option to remove existing SNMP V3 user by clicking on the **Remove** button in the last column of each entry. To add a new SNMP V3 user, the users have to select the user **Name** from the dropdown list which can be either **Admin** or **User**. Then, the authentication password with a maximum length of 31 characters has to be entered in the **Auth. Password** field and re-entered again in the **Confirmed Password** field. Note that if no password is

provided, there will be no authentication for SNMP V3. Finally, the encryption key with a maximum length of 31 characters can be entered in the **Encryption Key** and re-entered again in **Confirmed Key** field. After filling all the required fields, please click on **Add** button to update the information on the managed switch. Table 2.34 lists the descriptions of SNMP V3 settings.



Figure 2.92 SNMPv3 Users' Options

Table 2.34 Descriptions of SNMP V3 Settings

Label	Description	Factory Default
Name	Choose from one of the following options**:** **Admin**: Administration level. **User**: Normal user level.	Admin
Auth. (Authentication) Password	Set an authentication password for the user name specified above. If the field is left blank, there will be no authentication. Note that the authentication password is based on MD5. Max. 31 characters.	NULL
Confirmed Password	Re-type the Authentication Password to confirm**.**	NULL
Encryption Key	Set encryption key for more secure protection of SNMP communication. Note that the encryption algorithm is based on DES (. Max. 31 characters.	NULL
Confirmed Key	Re-type the Encryption Key	NULL

2.12 Spanning Tree

IEEE 802.1D Standard spanning tree functionality is supported by Agatel's managed switches. The **S**panning **T**ree **P**rotocol (**STP**) provides a function to prevent switching loops and broadcast radiation at the OSI layer 2. A switching loop occurs in a network when there are multiple connections or redundant paths between two network switches or at least two ports are connected on both sides of the two network switches. The switching loop can create a broadcast radiation, which is the accumulation of broadcast and multicast traffics in a computer network. As broadcast and multicast messages are forwarded by bridges/switches to every port, the bridges/switches will repeatedly rebroadcast the broadcast messages, and this accumulation of traffic can flood the network. STP creates a spanning tree topology and disables those links of the network that are not part of the spanning tree, which leaves only a single active path between two nodes. This function can avoid flooding and increase network efficiency. Therefore, Agatel's managed switches deploy spanning tree as a tool when the users set upconnection or port redundancy or fault-tolerance in their network.

RSTP (**R**apid **S**panning **T**ree **P**rotocol), IEEE 802.1W, is also supported in Agatel's managed switches. It is an evolution of the STP, but it is still backwards compatible with standard STP. RSTP has the advantage over the STP. When there is a topology change such as link failure in the network, the RSTP will converge significantly faster to a new spanning tree topology. RSTP improves convergence on point-to-point links by reducing the Max-Age time to 3 times Hello interval, removing the STP listeningstate, and exchanging a handshake between two switches to quickly transition the port to forwarding state.

MSTP (**M**ultiple **S**panning **T**ree **P**rotocol) is also a standard defined by the IEEE 802.1s that allows multiple VLANs to be mapped to a single spanning tree instance called MST Instance, which will provide multiple pathways across the network. It is compatible with STP and RSTP. To support lager network, MSTP groups bridges/switches into regions that appear as a single bridge to other devices. Within each region, there can be multiple MST instances. MSTP shares common parameters as RSTP such as port path costs. MSTP also help prevent swithing loop and has rapid convergence when there is a topology change. It is possible to have different forwarding paths for different MST instances. This enables load balancing of network traffic across redundant links.

This section describes how to setup the spanning tree protocol (STP), rapid spanning tree protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). Figure 2.93 depicts the dropdown menu for Spanning Tree.

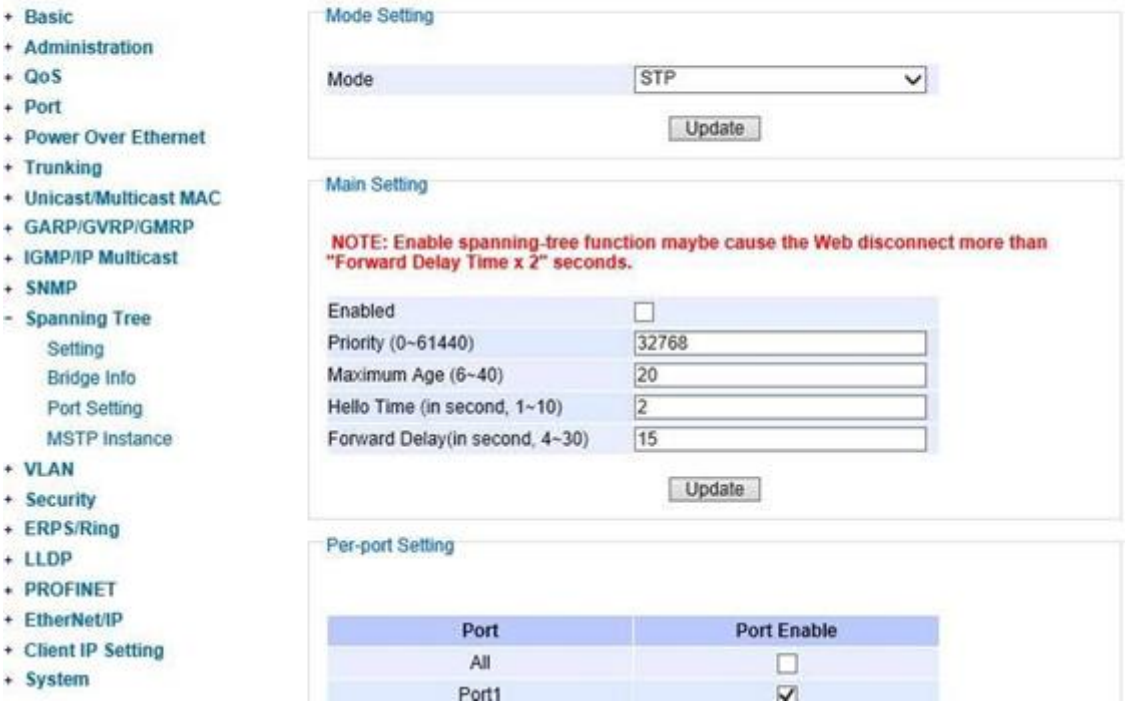


Figure 2.93 Spanning Tree Dropdown Menu

2.12.1 Spanning Tree Setting

The users can select the spanning tree mode which are based on different spanning tree protocols in this webpage. Figure 2.94 shows the mode setting for spanning tree. There are three spanning tree modes to choose from the dropdown menu, which are spanning tree protocol (STP), rapid spanning tree protocol (RSTP), and multiple spanning tree protocol (MSTP). After choosing the desired mode, please click **Update** button to allow the change to take effect.



Figure 2.94 Spanning Tree Mode Setting

Under the mode setting, there is a box for Main Setting of spanning tree's parameters as showed in Figure 2.95. The users can enable or disable spanning tree protocol in the **Main Setting** by checking the box behind the **Enabled** option. The users can fine tune the **Priority**, **Maximum Age**, **Hello Time**, and **Forward Delay**. After configuring the spanning tree's main parameters, please click **Update** button to allow the change to take effect. The description of each parameter is listed in Table 2.35.

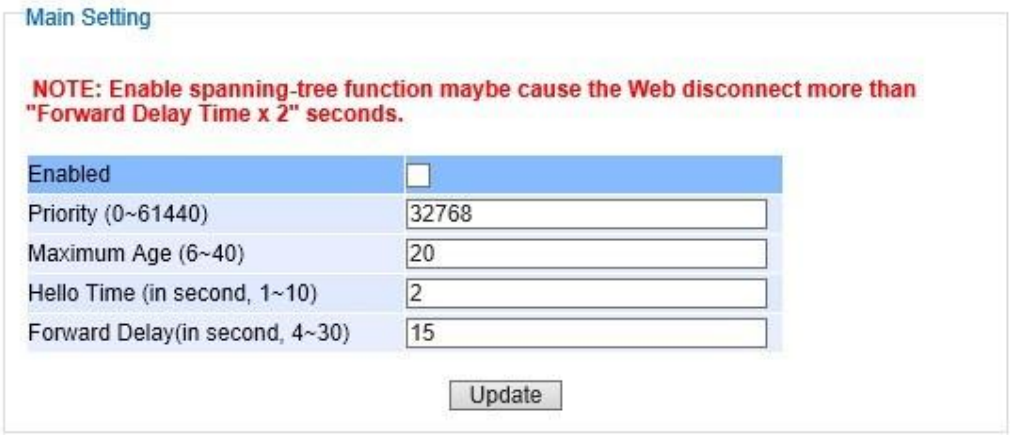


Figure 2.95 Spanning Tree Main Setting for STP and RSTP

When the users change the spanning tree mode setting to **MSTP** and click the **Update** button in the **Mode Setting** box Figure 2.94, the **Main Setting** box in Figure 2.95 will be changed to Figure 2.96. The user can notice that the **Priority** field is disappeared while there are three more fields show up which are **Max Hops**, **Revision Level**, and **Region Name**. Additionally, there will be a note add to the Per-port Setting box that currently MSTP mode does not support trunk port now.

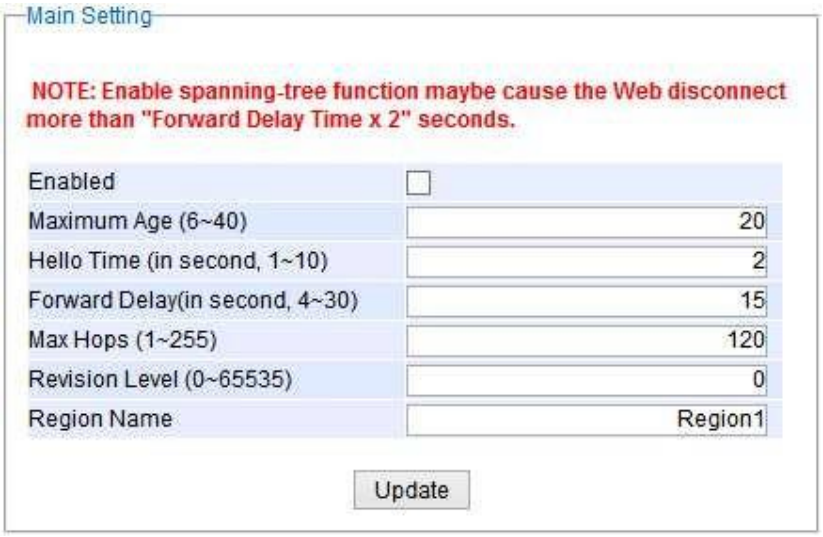


Figure 2.96 Spanning Tree Main Setting for MSTP

Table 2.35 Descriptions of Spanning Tree Parameters

Label	Description	Default Factory
Enabled	Check the box to enable spanning tree functionality.	Disable
Priority	Enter a number to set the device priority**.** The value is in between 0 and 61440**.** The lower number gives higher priority**.**	32768
Maximum Age	Maximum expected arrival time for a hello message**.** It should be longer than Hello Time**.**	20
Hello Time	Hello time interval is given in seconds. The value is in between 1 to 10.	2
Forward Delay	Specify the time spent in the listening and learning states in seconds. The value is in between 4 to 30.	15
Max Hops (Only for MSTP)	The value is between 1 to 255.	120
Revision Level (Only for MSTP)	The value is between 0 to 65535.	0
Region Name (Only for MSTP)	Text string indicate the region name	Region1

The bottom part of the Spanning Tree Setting is the Per-port setting as shown in Figure 2.97. The users can enable spanning tree functionality individually on each port or on all port by checking on the box under the **Port Enable** column. The default setting is checking on all port. After making any change onthe per-port setting, please click on the **Update** button to update the change on the managed switch.

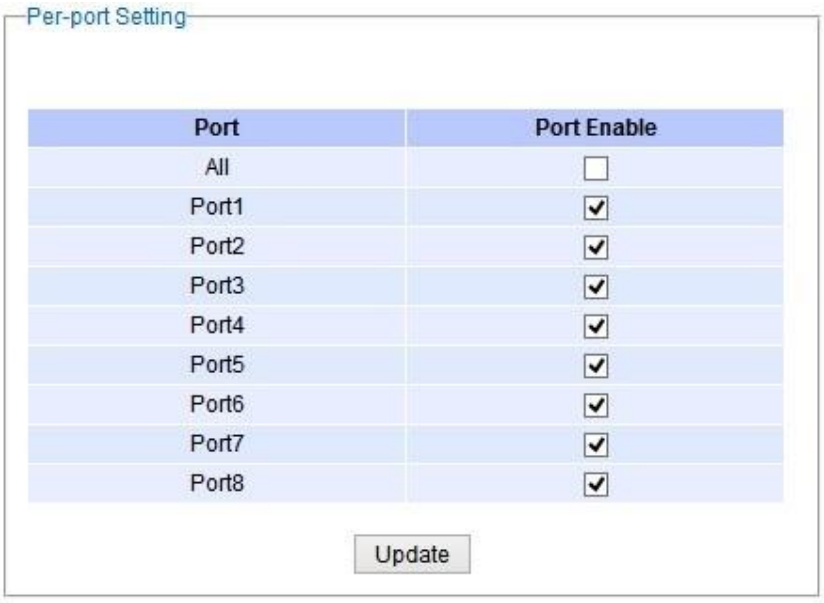


Figure 2.97 Spanning Tree Per-port Setting for STP and RSTP

2.12.2 Bridge Info

Bridge Info (information) provides the statistical value of spanning tree protocol as shown in Figure 2.98. The information is subdivided into two parts: Root Information and Topology Information. To check the latest information, please click on the **Refresh** button. Table 2.36 and Table 2.37 summarize the descriptions of each entry in the root information table and topology information table, respectively.

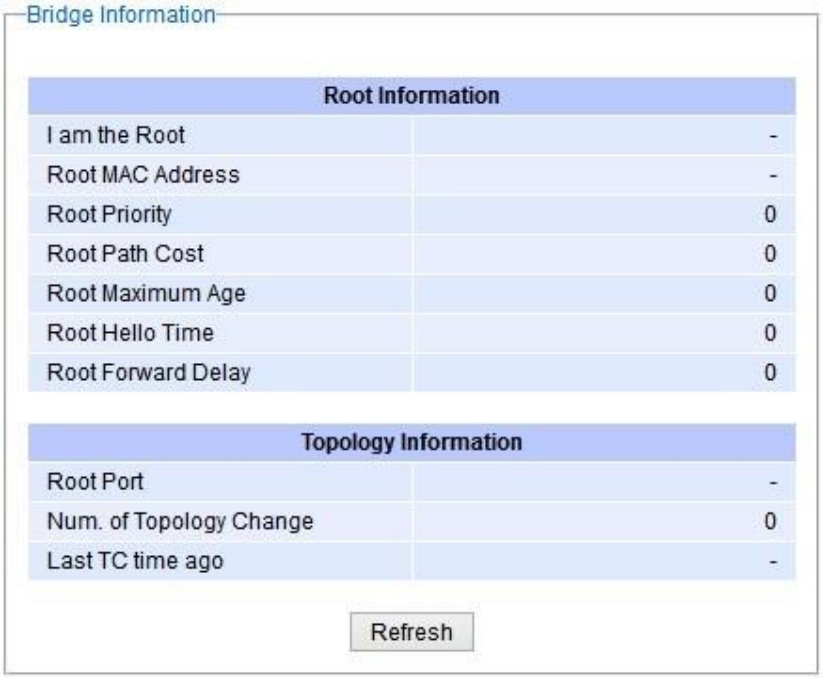


Figure 2.98 Bridge Information Webpage

Table 2.36 Bridge Root Information

Label	Description	Factory Default
I am the Root	Indicator that this switch is elected as the root switch of the spanning tree topology	-
Root MAC Address	MAC address of the root of the spanning tree	-
Root Priority	Root's priority value: The switch with highest priority has the lowest priority value and it will be elected as the root of the spanning tree.	0
Root Path Cost	Root's path cost is calculated from the data rate of the switch's port.	0
Root Maximum Age	Root's maximum age is the maximum amount of time that the switch will maintain protocol information received on a link.	0
Root Hello Time	Root's hello time which is the time interval for RSTP to send out a hello message to the neighboring nodes to detect any change in the topology.	0
Root Forward Delay	Root's forward delay is the duration that the switch will be	0

	in learning and listening states before a link begins forwarding.	

Table 2.37 Bridge Topology Information

Label	Description	Factory Default
Root Port	A forwarding port that is thebest port from non-root bridge/switch to root bridge/switch. Note that for a root switch there is no root port.	-
Num. of Topology Change	The total number of spanning topology change over time.	0
Last TC time ago	The duration of time since last spanning topology change.	-

2.12.3 Port Setting

Spanning Tree Port Setting shows the configured value of spanning tree protocol for each port, as shown in Figure 2.99. The configured information for each port is state, role, path cost, path priority, link type, edge, cost, and designated information. To check the latest update on the statistics, please click on the **Refresh** button. Table 2.38 summarizes the descriptions of spanning three port setting. If Spanning Tree is enabled, the table below becomes editable. Use the **Update** button to save the settings.

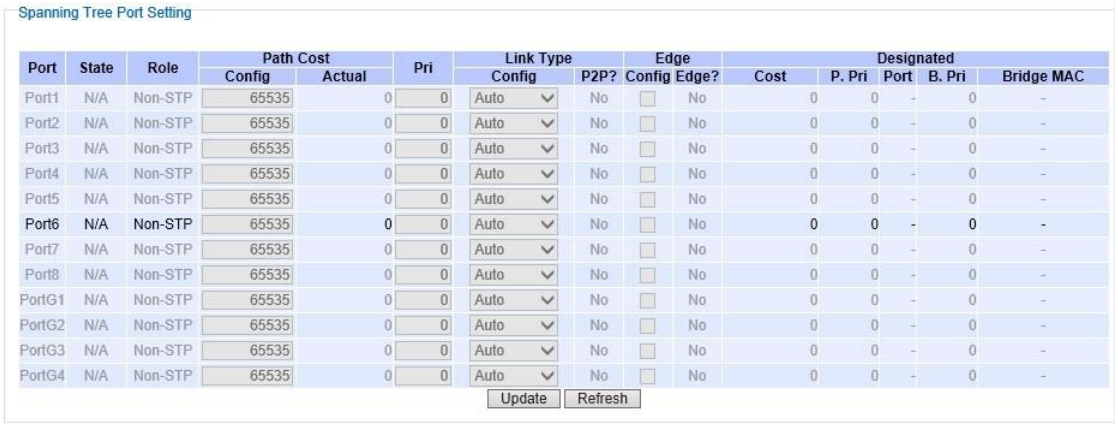


Figure 2.99 Spanning Tree Port Setting Webpage

Table 2.38 Descriptions of Spanning Tree Port Setting

Label	Description	Factory Default
Port	The name of the switch port	-
State	State of the port: '**Disc**': Discarding – No user data is sent over the port. '**Lrn**': Learning – The port is not forwarding frames yet, but it is populating its MAC Address Table. '**Fwd**': Forwarding – The port is fully operational.	N/A
Role	**Non-STP** or **STP** RSTP bridge port roles: '**Root**' – A forwarding port that is the best	Non-STP

		port from non-root bridge to root bridge. '**Designated**' – A forwarding port for every LAN segment. '**Alternate**' – An alternate path to the root bridge. This path is different from using the root port. '**Backup**' – A backup/redundant path to a segment whose another bridge port already connects. '**Disabled**' – Note strictly part of STP, a network administrator can manually disable a port.	
Path Cost		Setting the path cost for each switch port	
	Config	Setting path cost (default: 0, meaning that using the system default value (depending on link speed))	0
	Actual	The actual value path cost (For STP and RSTP, please see Note 1 below and Table 2.39.)	0
Pri		Setting the port priority, used in the Port ID field of BPDU packet, value = 16 × N, (N:0~15) See Note 2 below.	128
Link Type		The connection between two or more switches (for RSTP)	
	Config	Setting of the Link Type P2P: A port that operates in full-duplex mode is assumed to be point-to-pint link. Non-P2P: A half-duplex port (through a hub) Auto: Detect link type automatically	Auto
	P2P?	Yes: This port is a Point-to-Point (P2P). No: This port is not Point-to-Point (Non-P2P).	No
Edge		Edge port is a port which no other STP/RSTP switch connect to (for RSTP). An edge port can be set to forwarding state directly.	
	Config	Edge functional is set: Yes or No	No
	Edge?	Yes: This port is an edge port. No: This port is not an edge port.	No
Designated		This shows some information of the best BPDU packet through this port.	
	Cost	Root path cost	0
	P. Pri. (Port Priority)	Port priority (high 4 bits of the Port ID), Value = 16 × N, (N: 0~15)	128
	Port	Interface number (lower 12 bits of the Port ID)	-
	Bri. Pri. (Bridge Priority)	Bridge priority, (value = 4096 × N, (N: 0~15)	32768
	Bridge MAC	The MAC address of the switch which sent this BPDU	-

Note:

1. In general, the path cost is dependent on the link speed. Table 2.39 lists the default values of path cost for STP and RSTP.

Table 2.39 Default Path Cost for STP and RSTP

Data Rate	STP Cost (802.1D-1998)	RSTP Cost (802.1W-2004)
4 Mbits/s	250	5,000,000
10 Mbits/s	100	2,000,000
16 Mbits/s	62	1,250,000
100 Mbits/s	19	200,000
1 Gbits/s	4	20,000
2 Gbits/s	3	10,000
10 Gbits/s	2	2,000

2. The sequence of events to determine the best received BPDU (which is the best path to the root).

- Lowest root bridge ID determines the root bridge.
- Lowest cost to the root bridge favors the upstream switch with the least cost to root.
- Lowest sender bridge ID serves as a tie breaker if multiple upstream switches have equal cost to root.
- Lowest sender port ID serves as a tie breaker if a switch has multiple (non-Ether channel) links to a single upstream switch.

Bridge ID = priority (4 bits) + locally assigned system ID extension (12 bits) + ID [MAC Address] 48 bits

The default bridge priority is 32768.

Port ID = priority (4 bits) + ID (Interface number) (12 bits)

The default port priority is 128.

2.12.4 MSTP Instance

MSTP enables the grouping and mapping of VLANs to different spanning tree instances. Therefore, an MST Instance (MSTI) is a particular set of VLANs that are all using the same spanning tree. Note that MSTI is identified by MSTI number and locally significant within MST region. Figure 2.100 illustrates the MSTP Instance webpage. In this section, the uses can add or remove MSTP instance. The upper part of the webpage is a table of existing MSTP instance in the managed switch. The users can add a new MSTP instance by choosing an Instance ID from the dropdown list, enter the VLAN Identification in the VID field, and set the desired priority in the Priority field. After filling all information, please click the **Add/Modify** button to update the MSTP instance. The procedure for setting up an MSTP instance is as follows:

- Enable MSTP protocol in Section 2.12.1
- Modify spanning tree main setting as described in Section 2.12.1
- Select ports that you want to enable MSTP function in Section 2.12.1.
- Add a Multiple Spanning Tree Instance (MSTI) in MSTP Instance webpage (this section).
    - Choose an Instance Identification
    - Add VLAN Identifications (VIDs) that will be member(s) of MSTP instance.
    - Set Priority value of the switch.
    - Click **Add/Modify** button.

Table 2.40 summarizes the descriptions of MSTP Information.



Figure 2.100 MSTP Instance Webpage

Table 2.40 Description of MSTP Information

Label	Description	Factory Default
Instance ID	Choose from dropdown list of CIST (Common and Internal Spanning Tree) or choose value from 1 to 63	CIST
VID	Enter a value for VLAN ID between 1 to 4094	-
Priority	Enter a value for priority value for the managed switch between 0 – 61440. The lower value means the higher priority. If the priority value is 0, the switch will be the Root Bridge in this MSTI.	32768
Root Priority	Display root priority value	32768
Root MAC	Display MAC address of the Root Bridge	-
Internal Root Path Cost	Display internal root path cost	0
Root Port	Display root port	-
Topology Change	Display Yes or No	No

2.13 VLAN

A **V**irtual **L**ocal **A**rea **N**etwork (**VLAN**) is a group of devices that can be located anywhere on a network, but all devices in the group are logically connected together. In other words, VLAN allows end stations to be grouped together even if they are not located on the same network switch. With a 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 increases traffic efficiency (see Figure 2.101).

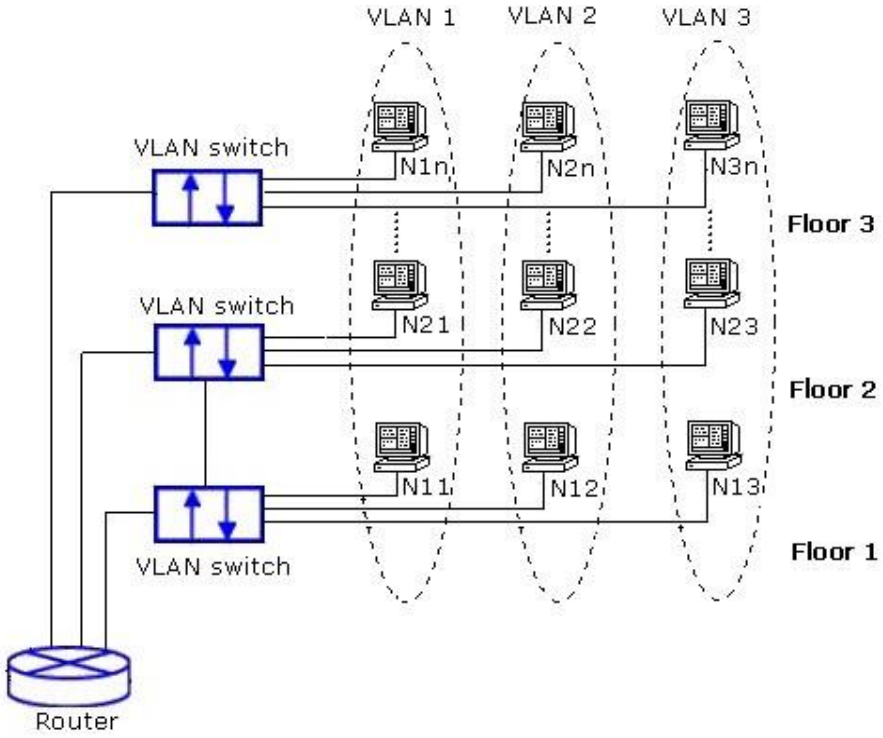


Figure 2.101 Example of VLAN Configuration

Agatel's managed switch XEG75XX series provide six approaches to create VLAN as follows:

- **Tagging-based (802.1Q) VLAN**
- **Port-based VLAN**
- **MAC-based VLAN**
- **IP Subnet-Based VLAN**
- **Protocol-Based VLAN**
- **QinQ or Double Tagging-based VLAN**

Figure 2.102 shows the drop-down menu under the VLAN section.

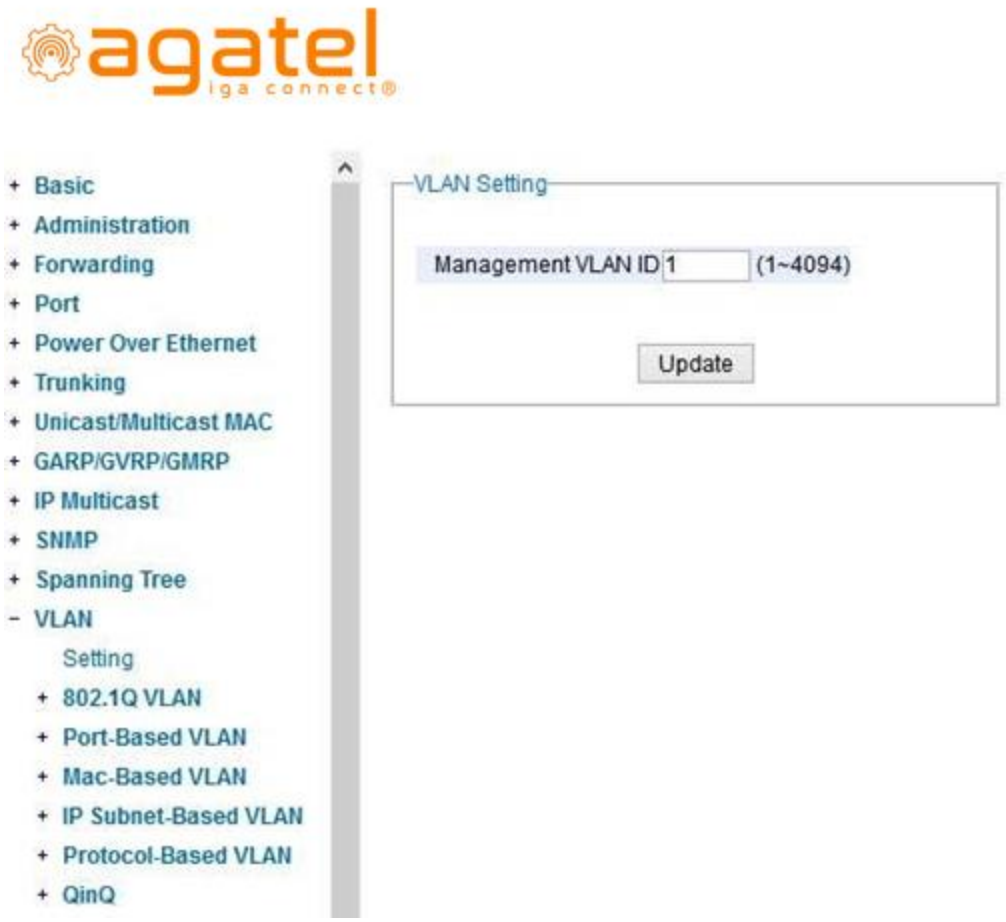


Figure 2.102 VLAN Dropdown Menu

2.13.1 VLAN Setting

The first menu under the VLAN section is the VLAN Setting. Here the management VLAN Identification number (ID) is configured based on the IEEE 802.1Q standard. The default value is VID = 1. Note that the ID can be the number from 1 to 4096. If the users change the management VLAN ID to other number, please click the **Update** button to set it on the managed switch. Figure 2.103 depicts the VLAN Setting webpage. Table 2.41 describes the VLAN Setting option.



Figure 2.103 VLAN Setting Webpage

Table 2.41 Description of VLAN Setting

Label	Description	Factory Default
Management VLAN ID	Configure the management VLAN ID that can be accessed this switch. Range from 1 to 4095.	1

2.13.2 802.1Q VLAN

Tagging-based (802.1Q) VLAN is the networking standard that supports virtual LAN (VLANs) on an Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures for bridges and switches in handling such frames. The standard also contains provisions for a quality of service prioritization scheme commonly known as IEEE 802.1Q.

VLAN tagging frames are frames with 802.1Q (VLAN) tags that specify a valid VLAN identifier (VID). Whereas, 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.

For a 802.1Q VLAN packet, it adds a tag **(**32**-**bit field**)** to the original packet**.** The tag is between the source MAC address and the EtherType**/**length fields of the original frame**.** For the tag, the first 16 bits is the Tag protocol identifier **(**TPID**)** field which set to a value of 0x8100 in order to identify the frame as an IEEE 802**.**1Q**-**tagged frame**.** This field is located at the same position as the EtherType**/**length field in untagged frames, and is thus used to distinguish the frame from untagged frames**.** The next 3 bits is the Tag control information **(**TCI**)** field which refers to the IEEE 802**.**1p class of service and maps to the frame priority level**.** The next one bit is the Drop Eligible Indicator **(**DEI**)** field which may be used separately or in conjunction with PCP to indicate frames eligible to be dropped in the presence of congestion**.** The last 12 bits is the VLAN identifier **(**VID**)** field specifying the VLAN to which the frame belongs**.**

Under the 802**.**1Q VLAN menu, there are three submenus which are **Setting**, **PVID Setting**, and **VLAN Table** as shown in Figure 2.104**.**



Figure 2.104 802.1Q VLAN Dropdown Menu

2.13.2.1 802.1Q VLAN Settings

Figure 2.105 shows the 802.1Q VLAN Setting webpage which allow the users to add new tagged-based VLAN to the managed switch. Please follow the following procedure to setting up the 802.1Q VLAN on the switch.

1. Go to **802.1Q VLAN,** then select **Setting** submenu.
2. Fill in appropriate Name, VID, Member Ports, and Tagged Ports as show in Figure 2.105. The description of each fields is summarized in Table 2.42. Then, click **Add/Modify** button. Note to select multiple **Member Ports** or multiple **Tagged Port**s, press and hold the **Ctrl** key while selecting multiple ports.
3. Go to **802.1Q VLAN's PVID Setting** described in the next subsection.
4. Choose the same ports, and enter PVID (which is the same as VID), see Figure 2.106.

To remove any of the VLAN from the 802.1Q VLAN setting, click the **Remove** button at the end of that particular VLAN record as shown in Figure 2.105.

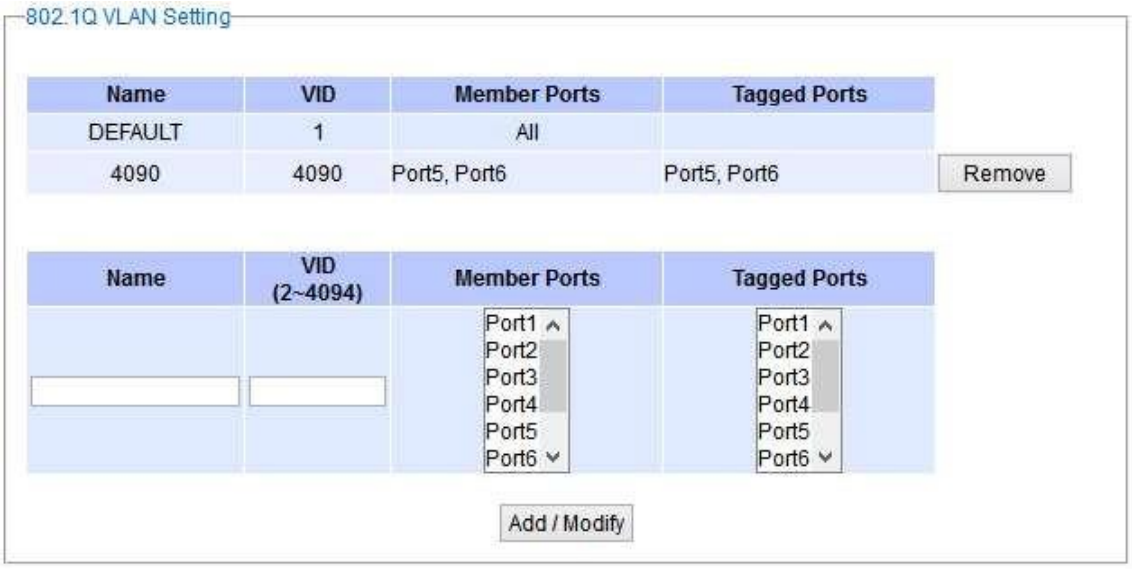


Figure 2.105 802.1Q VLAN's Setting Webpage

Table 2.42 Setting Descriptions of 802.1Q VLAN Settings

Label	Description	Factory Default
Name	The VLAN ID name that can be assigned by the user.	DEFAULT
VID	Configure the VLAN ID that will be added in static VLAN table in the switch. The VLAN ID is in the range 2~4094.	Dependent
Member Ports	Configure the port to this specific VID.	All Ports
Tagged Ports	Configure the port 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.	Dependent

***NOTE:** Default settings only have VLAN ID on 1. To set VLAN ID to other value beside 1, users will have to assign ports to be in that VLAN group.

2.13.2.2 802.1Q VLAN PVID Settings

Each port is assigned a native VLAN number called the Port VLAN ID (PVID). When an untagged frame goes through a port, the frame is assigned to the port's PVID. That is the frame will be tagged with the configured VLAN ID defined in this subsection. Figure 2.106 shows the PVID Setting for 802.1Q VLAN where the upper table lists the current PVID assigned to each port. The users can configure the PVID by select either on or multiple ports (by clicking and holding the **Ctrl** key) and enter the desired PVID value between 2 to 4094. Please click **Update** button to allow the configuration to take effect on the switch. Table 2.43 summarizes the PVID Setting's descriptions.

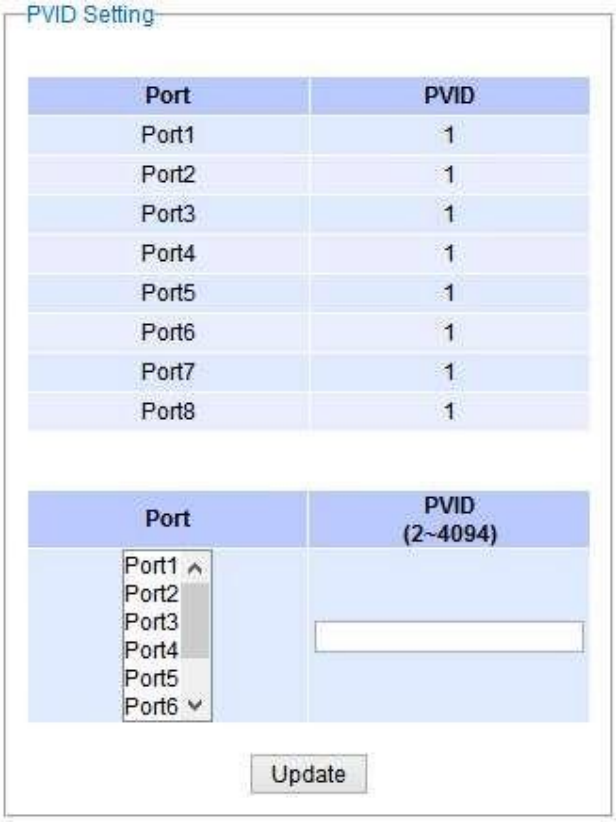


Figure 2.106 802.1Q VLAN PVID Setting Webpage

Table 2.43 Setting Descriptions of 802.1Q VLAN PVID

Label	Description	Factory Default
Port	Select specific port(s) to set the PVID value	-
PVID	Configure the default 802.1Q VID tag assigned to specific Port. The VLAN ID is in the range 1~4094.	1

2.13.2.3 802.1Q VLAN Table

This webpage shown in Figure 2.107 displays the 802.1Q VLAN table which lists all the VLANs that are automatically and manually added/modified to the managed switch. Figure 2.108 illustrates examples of the static and dynamic VLAN information of each VID. Table 2.44 summarizes the descriptions of VLAN Table.

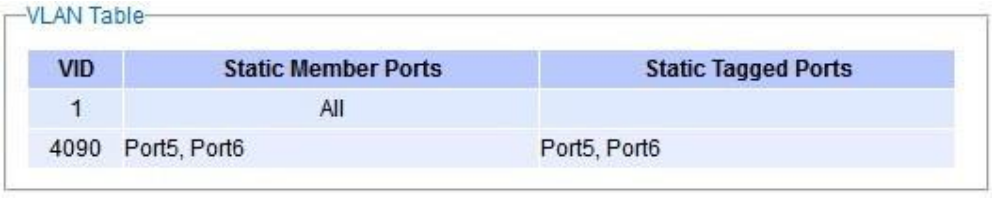
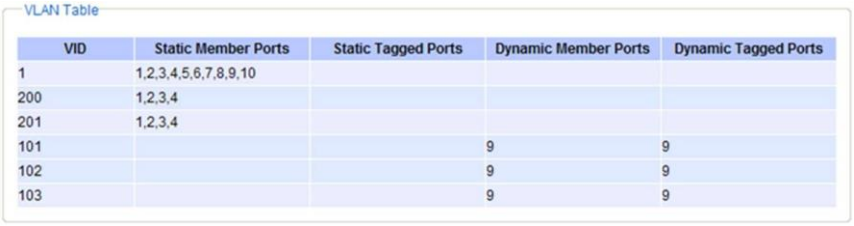


Figure 2.107 802.1Q VLAN Table Webpage


VLAN Table

VID	Static Member Ports	Static Tagged Ports	Dynamic Member Ports	Dynamic Tagged Ports
1	1,2,3,4,5,6,7,8,9,10			
200	1,2,3,4			
201	1,2,3,4			
101			9	9
102			9	9
103			9	9

Figure 2.108 Example of 802.1Q VLAN Table

Table 2.44 Descriptions of 802.1Q VLAN Table

Label	Description	Factory Default
VID	Indicate the VLAN ID number	Dependent
Static Member Ports	Indicate the member ports to this VID. This entry is created by user.	All ports
Static Tagged Ports	Indicate the ports that outgoing packet is tagged or untagged. **Displayed**: The outgoing packet is tagged from this port. **Non-displayed**: The outgoing packet is untagged from this port. This entry is created by user.	Dependent
Dynamic Member Ports	Indicate the member ports to this VID. This entry is created by GVRP (discussed in Section 2.9.1).	Dependent
Dynamic Tagged Ports	Indicate the member ports that outgoing packet is tagged or untagged. **Displayed**: The outgoing packet is tagged from this port. **Non-displayed**: The outgoing packet is untagged from this port. This entry is created by GVRP (discussed in Section 2.9.1).	Dependent

2.13.3 Port-Based VLAN

Port-Based VLAN (or Static VLAN equivalent) assignments are created by assigning ports to a VLAN. If a device is connected to a certain port, the device will be assigned a VLAN to that specific port. If a user changes the connected port, a new port-VLAN assignment must be reconfigured for this new connection. To setup port-based VLAN, please follow the following steps:

1. Click on **Port-Based VLAN setting** page as shown in Figure 2.109.
2. Select specific ports to be included in certain group by checking the corresponding box under the Member ports on particular row of port-based VLANs' Group ID. Note that if the users check the box under the Group ID column, all of the Member Ports will belong to that VLAN's Group ID.
3. Click on the **Update** button to allow the setting to take effect on the managed switch.

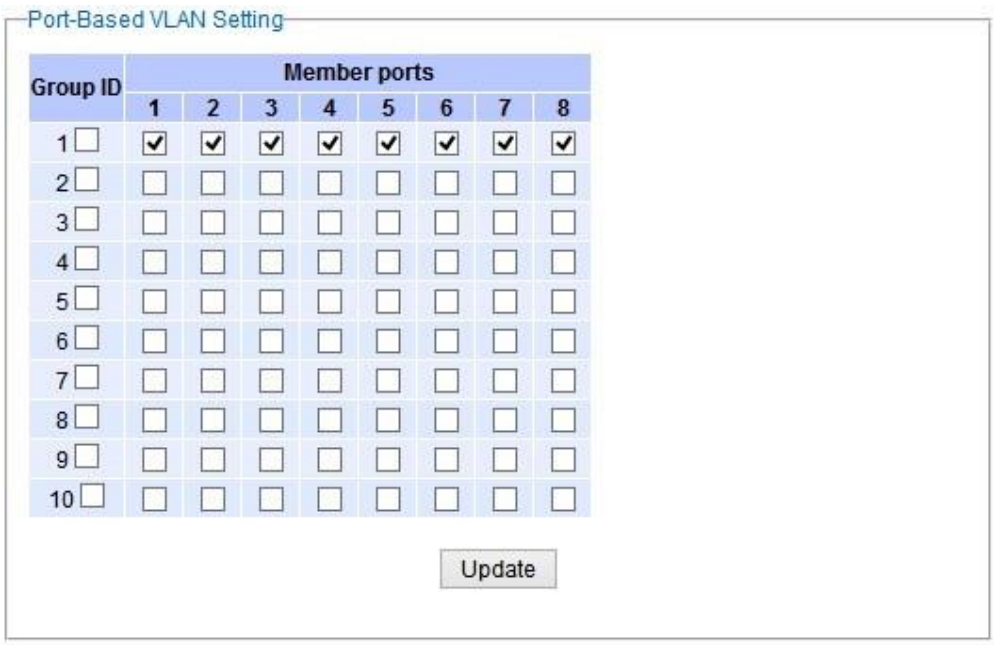


Figure 2.109 Port-based VLAN Setting Webpage

2.13.4 MAC-Based VLAN

The managed switch also supports the ability to assign a VLAN ID (VID) to an untagged packet based on the source MAC address. This can be set in this sub-menu as shown in Figure 2.110. There are maximum 512 entries in the MAC-based VLAN table (Source MAC address + VLAN ID) in the lower part of this webpage. If the users enter a duplicated MAC address into the MAC-based VLAN table, the old VLAN ID will be overwritten by the new VLAN ID. The VLAN ID range is between 1 to 4096. If the source MAC address of a packet is matched with any entry inside the MAC-based VLAN table here, the mapped VLAN ID will be added to the packet.



Figure 2.110 MAC-Based VLAN Setting Webpage

2.13.5 IP Subnet-Based VLAN

This sub-menu allows the user to assign a VLAN ID to an untagged packet based on the source IP address and the prefix length which is called IP subnet-based VLAN. Figure 2.111 shows the webpage where the users can enter the IP address, prefix length and VLAN ID (VID) for creating a VLAN based on its IP subnet. The list of existing IP subnet-based VLAN is shown in the lower part of the webpage. This feature support maximum of 64 sets (IP address + Prefix length + VLAN ID). The VLAN ID (VID) range is between 1 to 4096. This VLAN setup feature supports both IPv4 and IPv6. If a duplicated pair of IP address and prefix length is entered into the table, there will be an error message. The prefix length of IPv4 is 0 to 32 while the prefix length of IPv6 is 0 to 64.

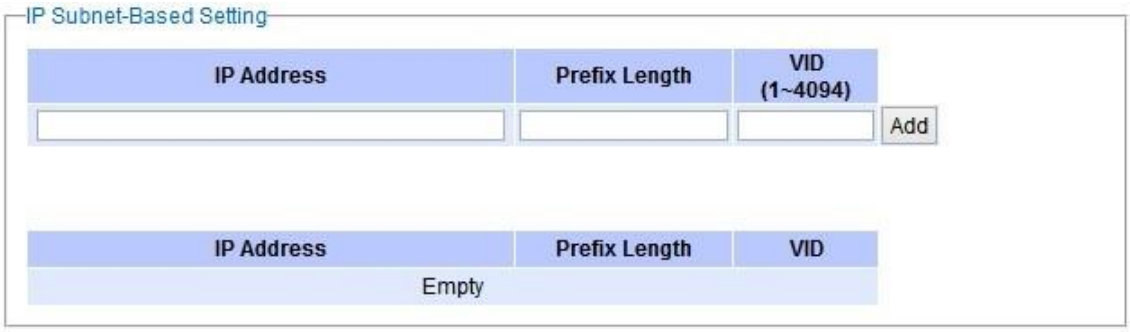


Figure 2.111 IP Subnet-Based VLAN Setting Webpage

2.13.6 Protocol-Based VLAN

For the protocol- based VLAN, the switch supports 3 Ethernet packet frame types: Ethernet II, 802. 3 LLC, and 802.3 SNAP. It uses the EtherType field (Protocol ID in these frames to assign a VLAN ID foreach untagged packets. There are two submenus for **Protocol- Based VLAN**: **Protocol to Group Setting** and **Group to VLAN Setting**.

2.13.6.1 Protocol to Group Settings

The users can add or modify the Group ID in this menu option, as shown in Figure 2.112 . Here, the maximum of 16 rules are supported. “Protocol Group Setting” is used to define the protocol rule and assign an unique ID (Group ID). The value of **Group ID** is between 1 to 2147483646. The **Frame Type** can be **Ethernet**, **SNAP**, or **LLC**. The “**Value**” field in the webpage is the EtherType (Protocol ID).

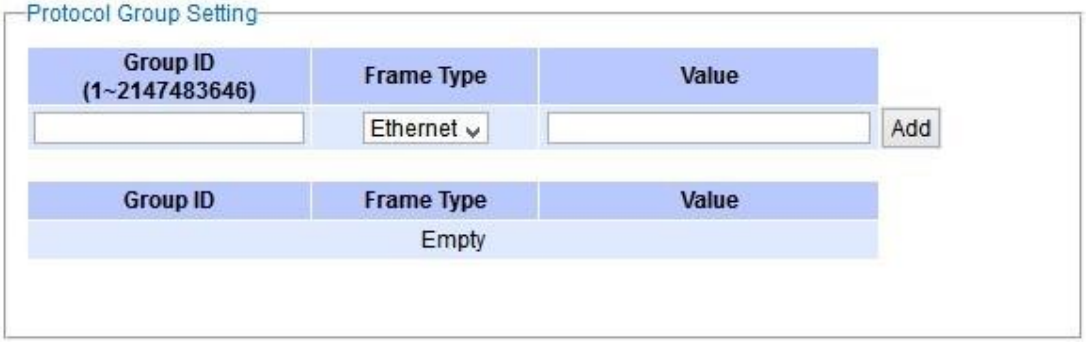


Figure 2.112 Protocol to Group Setting Webpage

2.13.6.2 Group to VLAN Settings

The users can add or modify **Group ID** and for each port or multiple ports in this menu option, as shown in Figure 2.113. “Group to VLAN Setting” is used to map the **Group ID** to a VLAN ID (**VID**). This will map the FrameType and EtherType to a VLAN ID.



Figure 2.113 Group to VLAN Setting Webpage

2.13.7 QinQ

Originally the 802.1Q standard VLAN only allowed one VLAN tag appended in a packet. But the QinQ feature in this subsection allows two VLAN tags to be appended in a packet. The main purpose of the QinQ is for service providers to place additional VLAN tag as an external network identification and to keep the original customer's VLAN tag if existed.

To understand the operation of QinQ VLAN setting, we will use an example of a network where there are two buildings called Building 1 and Building 2 that has two departments called Department A and Department B of the same company on both buildings. Department A want use the VLAN2 (TPID = 0x8100) for inside communication and Department B also want to use the VLAN2 (TPID = 0x8100) for inside communication but they do not want to communicate with each other.
The network administrators can enable the QinQ VLAN feature or double tagging VLAN function in the company managed switches. If Building 1 has the following switches: A1 (for Department A), B1 (for Department B), H1 (for Backbone network) and Building 2 has the following switches: A2 (for Department A, B2 (for Department B), and H2 (for Backbone network) then all of the switches can be configured as shown in Figure 2.114.

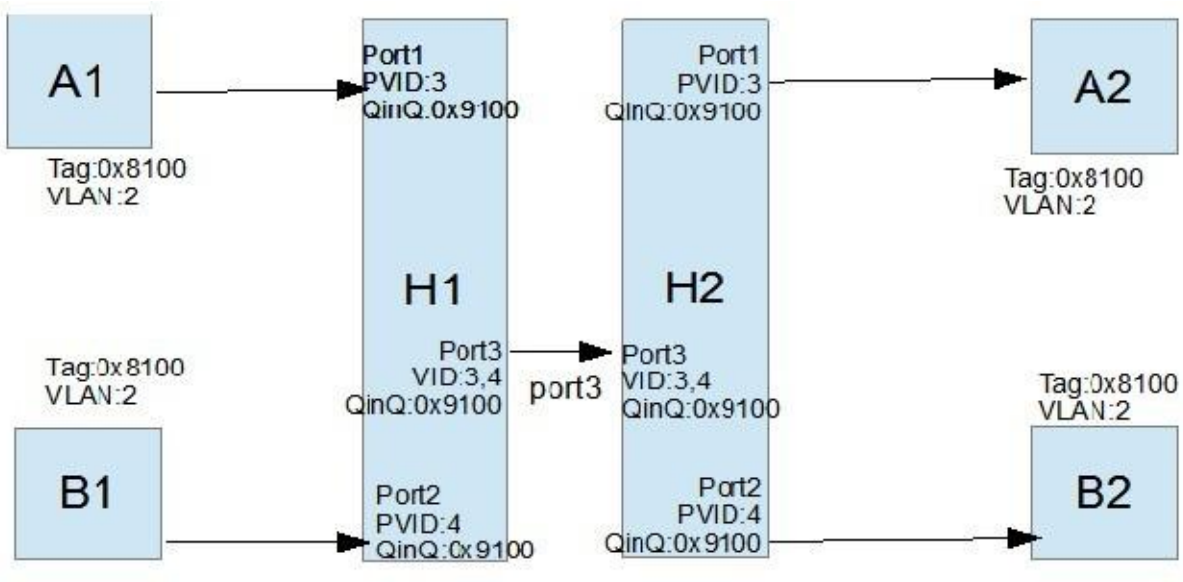


Figure 2.114 Example of QinQ Deployment

The operation of the network in Figure 2.114 based on QinQ VLAN setting rule can be described as follows.

1. Switch A1 and Switch B1 send some packets with VLAN tag (TPID=0x8100, VLAN ID=2) to H1.
2. The Switch H1 treats these received packets with VLAN tag (TPID=0x8100) as untagged packets because the receiving ports' QinQ TPID = 0x9100. These packets will be inserted the second VLAN tags (TPID=0x9100, VLAN ID = PVID).
3. The Switch H1 will switch these packets to Port3 (VLAN ID=3 or 4 depending on the incoming port number from A1 or B1).
4. The Switch H2 receives these packets and switches them by the VLAN rule. The packets with VLAN ID 3 will be sent to Port 1 and the packets with VLAN ID 4 will be sent to Port 2.
5. Before Switch H2 sends these packets out from Port 1 or Port 2, the VLAN tags (TPID=0x9100, VLAN ID=3 or 4) will be removed from these packets.

Figure 2.115 shows the QinQ Setting webpage where the QinQ function can be enabled for each port on the managed switch. When checking the corresponding enabled box behind each port, the TPID field will become active. The default TPID is set to 0x8100 which means that the QinQ feature is disable. To enable the QinQ for a port, the users need to set the TPID value. In general, it should be set to 0x9100 which must be different from the original tag's 0x8100 as described in Section 2.13.2. The TPID value should be between 0x0000 to 0xFFFF. When setting a trunk port with QinQ, it is not allow eachphysical port with different QinQ setting. This means that the QinQ enabled fields and TPID fields of allphysical ports in a trunk port must be the same.

The QinQ setting rule is summarized as follows:

- For ingress ports and egress ports, they use the TPID field to decide whether a packet is being with a VLAN tag or not.

- A packet is untagged (without VLAN tag) if its TPID field is not the same as the TPID that we set for the port in the QinQ configuration.
- A packet is tagged (with VLAN tag) if its TPID field is the same as the TPID that we set for the port in the QinQ configuration.

- Either tagged packet or untagged packet are processed by the general VLAN rule to tag a packet, untag a packet, or keep the same packet, and do the switching.
- When a packet is tagged with a VLAN tag. The tag's TPID is from the input port's QinQ setting and the tag's VLAN ID is from the input port's PVID setting.

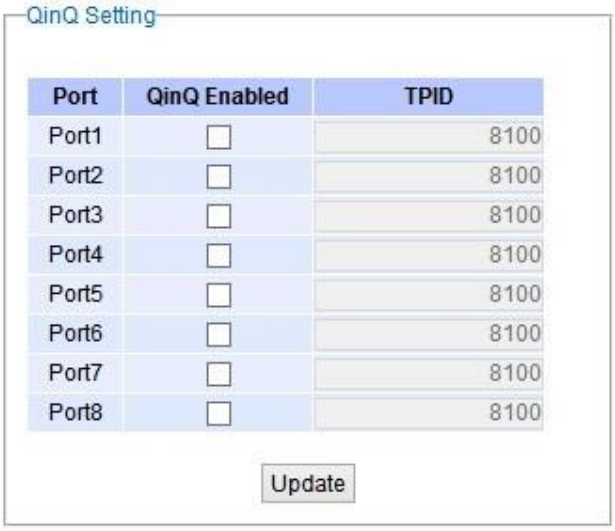


Figure 2.115 QinQ Setting Webpage

After finish setting the QinQ feature for any of the port, please click the **Update** button to allow the setting take effect on the managed switch.

2.14 Security

Three security features are provided in XEG75XX series:

- **Port Security (Static)**
- **802.1X**
- **Access Control List (ACL)**

Figure 2.116 shows the dropdown menu for security section on the managed switch.



Figure 2.116 Security Dropdown Menu

2.14.1 Port Security

Port Security or static port security subsection allows the users to control security on each port of the managed switch and create a table of MAC addresses allowed to access the switch. The **Port Security** menu is subdivided into two sub-menus which are **Setting** and **White-List MAC**.

2.14.1.1 Port Security Settings

Figure 2.117 displays the Port Security Setting webpage where the users can enable or disable static security on one or multiple ports. To enable or disable multiple ports at the same time please hold the **Ctrl** key and select multiple ports under the **Port** list and choose **Enable** or **Disable** and then click **Update** button. The lower part of the Port Security Setting webpage shows the current status of security setting for each port on the managed switch.

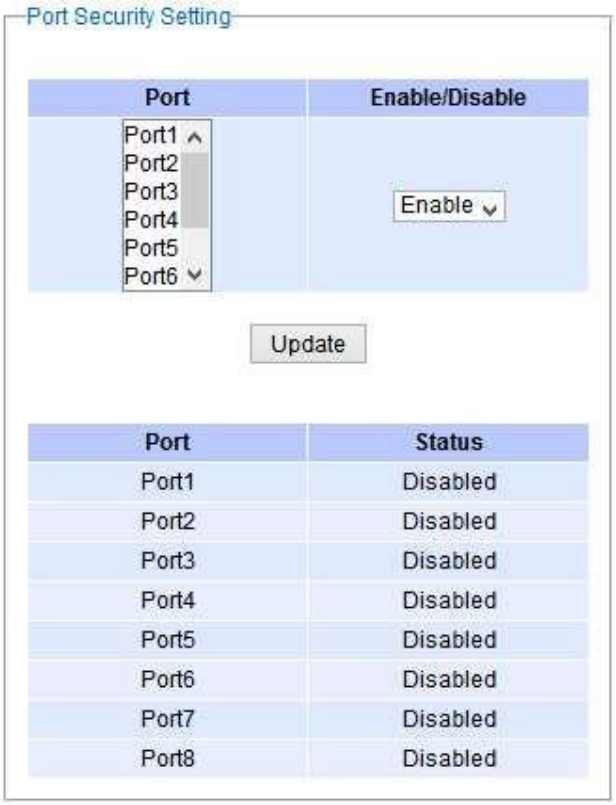


Figure 2.117 Port Security Setting Webpage

2.14.1.2 Port Security White-List MAC

The White-List MAC webpage is depicted in Figure 2.118. The users can create a list of MAC address that will be allowed to access the managed switch. The users will need to specify the VLAN ID (VID) and port number for each particular MAC address added to this list. After entering all required fields, please click on the **Add** button to add the new MAC address into the white list. Please remember that the same MAC address cannot be assigned to two different ports. This will cause an error message. Note that if there are existing MAC address on the list and the users would like to remove them, please

click on the **Remove** button at the end of each record. Image below summarizes the descriptions of the fields in White-List MAC webpage.



Figure 2.118 White-List MAC Webpage

Table 2.45 Description of Fields in White-List MAC Webpage

Label	Description
MAC Address	Type the suitable MAC address
Ports	Choose the desired 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.

2.14.2 802.1X

802.1 X is an IEEE standard for port-based Network-Access Control. It provides an authentication mechanism to devices that want to attach to a LAN or WLAN. This protocol restricts unauthorized clients from connecting to a LAN through ports that are opened to the Internet. The authentication basically involves three parties (see Figure 2.119): a supplicant, an authenticator, and an authentication server.

- Supplicant: A client device that requests access to the LAN.
- Authentication Server: This server performs the actual authentication. We utilize RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) as the authentication server.
- Authenticator: The Authenticator is a network device (I.e. the XEG75XX Industrial Managed Switch) that acts as a proxy between the supplicant and the authentication server. It passes around information, verifies information with the server, and relays responses to the supplicant.

The authenticator acts like a security guard to a protected network. The supplicant is not allowed accessing to the protected side of the network through the authenticator 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: The RADIUS is a networking protocol that provides authentication, authorization and accounting (AAA) management for devices to connect and use a network service. Figure 2.119 shows a diagram of RADIUS authentication sequence.

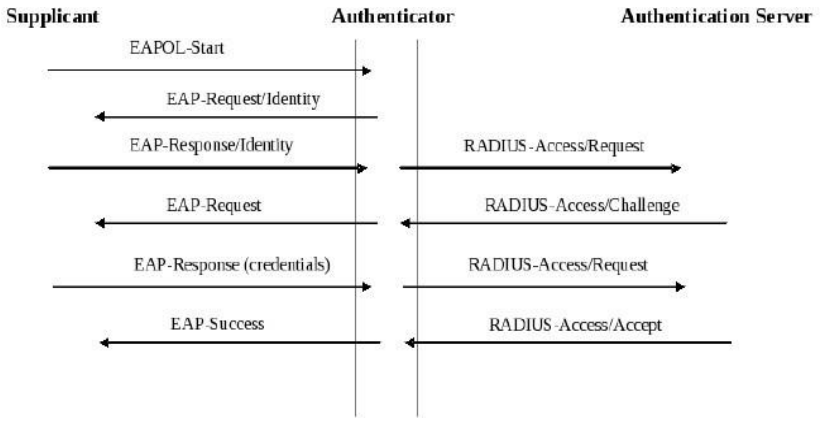


Figure 2.119 RADIUS Authentication Sequence

The **802.1X** option under the Security section is subdivided into three sub-menus which are: **Setting**, **Parameters Setting**, and **Port Setting**.

2.14.2.1 802.1X Settings

The 802.1X security mechanism can be enabled in this webpage as shown in Figure 2.120. When the users check the Enabled box, the rest of the option fields will become active. The users then have to enter all the required fields to configure the 802.1X Setting which are the IP address of RADIUS server, the RADIUS server's port number, RADIUS server's accounting port number, NAS identifier, and shared key. Summary of 802.1X Setting options are given in Table 2.46. After changing all the required fields, please click on the **Update** button.



Figure 2.120 802.1X Setting Webpage

Table 2.46 Descriptions of 802.1X Setting

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	0.0.0.0
Server Port	Set RADIUS server port number. The range is 0 ~ 65535.	1812
Accounting Port	Set the accounting port number of the RADIUS server. The range is 0 ~ 65535.	1813
NAS Identifier	Specify the identifier string for 802.1X Network Access Server (NAS). Max. Of 30 characters.	Managed Switch
Shared Key	A shared key between the managed switch and the RADIUS Server. Both ends must be configured to use the same key. Max. Of 30 characters.	NULL
Confirm Shared Key	Re-type the shared key string.	Dependent

2.14.2.2 802.1X Parameters Settings

There are a number of 802.1X parameters that the users might want to fine tune. This can be done on this webpage as shown in Figure 2.121. These parameters are related to the authentication periods or timeout durations and maximum number of authentication requests. Table 2.47 summarizes the descriptions of these parameters and their default setting. Please clicking on the Update button after the users changed any of the parameters.

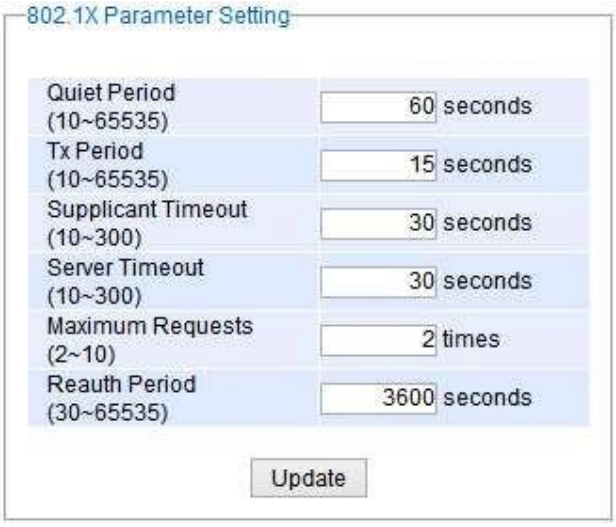


Figure 2.121 802.1X's Parameters Setting Webpage

Table 2.47 Descriptions of 802.1X Parameters

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 to response to the authentication server's EAP packet. Range from 10 to 300 seconds.	30
Server Timeout	Waiting time for the authentication server to response to the supplicant's EAP packet. Range from 10 to 300 seconds.	30
Maximum Requests	Maximum number of the retransmissions that the authentication server sends EAP request 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

2.14.2.3 802.1x Port Setting

The user can individually configure 802.1x security mechanism on each port of the XEG75XX managed switch as shown in Figure 2.114. Each port can be set for any of the four authorization modes which are Force Authorization, Force Unauthorization, IEEE 802.1X Standard Authorization, and no authorization (N/A) as described in Table 2.48. The lower part of the the webpage is a table display the current status of authorization mode and state of each port on the managed switch. To enable the 802.1X security on any of the port(s), click one of the port or press **Ctrl** key and click multiple ports on the list and choose the Authorization **Mode** from the pulldown list and click the **Update** button. To check the latest status of the 802.1X port setting, please click on the **Refresh** button.

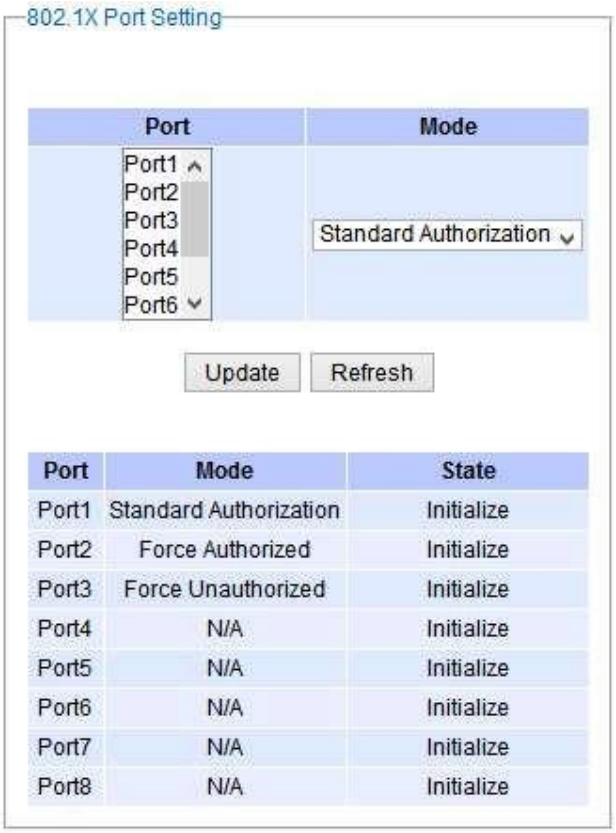


Figure 2.122 802.1x Port Setting Webpage

Table 2.48 Descriptions of 802.1X Port Setting

Label	Description	Factory Default
Port	Set specific ports to be configured.	Option
Mode	Choices: **Force Unauthorized:** Specify forced unauthorized **Force Authorized:** Specify forced authorized **Standard Authorization:** Specify authorization based on IEEE 802.1X **N/A**: Specify disable authorization	N/A

2.14.3 ACL

Access Control List (ACL) is the mechanism for network access control. The users configure the switch's filtering rules for accepting or rejecting some packets. Two types of filters are deployed in the XEG75XX series:

1) by MAC layer, and
2) by IP layer.

The numbers of matching rules can be at most 128. However, the main important rules that are mostly exercise are follows. Rules for filtering by MAC layer includes MAC address, VLAN ID or Ether type. Whereas, rules for filtering by IP layer includes IP protocol, IP address, TCP/UDP port or Type of Service (TOS). When filtering is enabled, the matching rules are used to check whether the receiving

packet is matched. If it is match, the packet will be rejected; otherwise it will be accepted. Note here that the matching rules later will be referred to as the entries of ACL.

The ACL webpage is depicted in Figure 2.123. To differentiate between each ACL entry**, Index** number from 1 to 128 is used. The ACL entry that has higher priority will be checked first before the lower priority. The **Name** field is for setting name of this rule. Type of filtering whether MAC layer ("**Mac Base**") and IP layer ("**IP Base**") can be set in the **Filter** field. Note that when change from Mac Base to IP Base the required parameters for ACL setting will be changed accordingly.

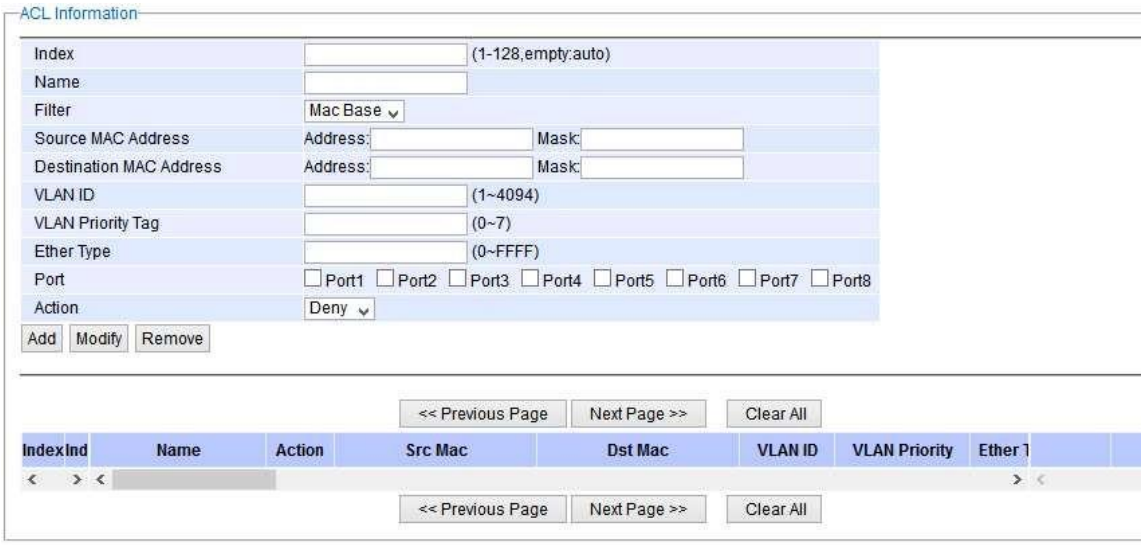


Figure 2.123 Security Access Control List Information Webpage (MAC Based Filtering)

The main ACL entries for filtering by MAC layer (also called L2 filtering) as shown in Figure 2.123 include MAC address, VLAN ID, VLAN Priority Tag and Ether Type. Table 2.49 describes definition of each in details. Here note that if any field is empty, that ACL entry will be ignored.

Table 2.49 Descriptions of Main ACL Entries for L2 Filtering in ACL Webpage

ACL Entry	Definition	Range
Source or Destination MAC Addresses	MAC address are the fields of the Ethernet frame header. The Mask item is a bit mask for comparing range.	For every non-zero bit in the Mask, its relative bit in the IP address will be compared. If the Mask is 0.0.0.0, then this condition is always accepted. If the Mask is empty, it is considered equal to the Mask of 255.255.255.255 and all of bits in the IP Address are compared.
VLAN ID	The VLAN ID field of 802.1Q VLAN tag in the Ethernet frame header. If the trunk ports are created, they will also be shown on the port list. If you want to select a trunk port, please make sure that there are no ACL entry using the physical ports which are belonging this trunk port.	The item value is between 1~4094.
VLAN Priority Tag	The Priority field of 802.1Q VLAN tag in the Ethernet frame header.	The item value is between 0~7.

Ether Type	The Ethernet type field in the Ethernet frame header. The followings are examples. The value 0x8000 is an IPv4 packet. The value 0x86DD is an IPv6 packet. The value 0x8100 is an 802.1Q packet.	The item value is between 0~0xFFFF.

The main ACL entries for filtering by IP layer (also called L3 filtering) as shown in Figure 2.124 include IP Protocol, Source IP Address, Destination IP address, TCP/UDP Source Port, TCP/UDP Destination Port and TOS. Table 2.50 describes definition of each in details. Once again, note that if any field is empty, that ACL entry will be ignored

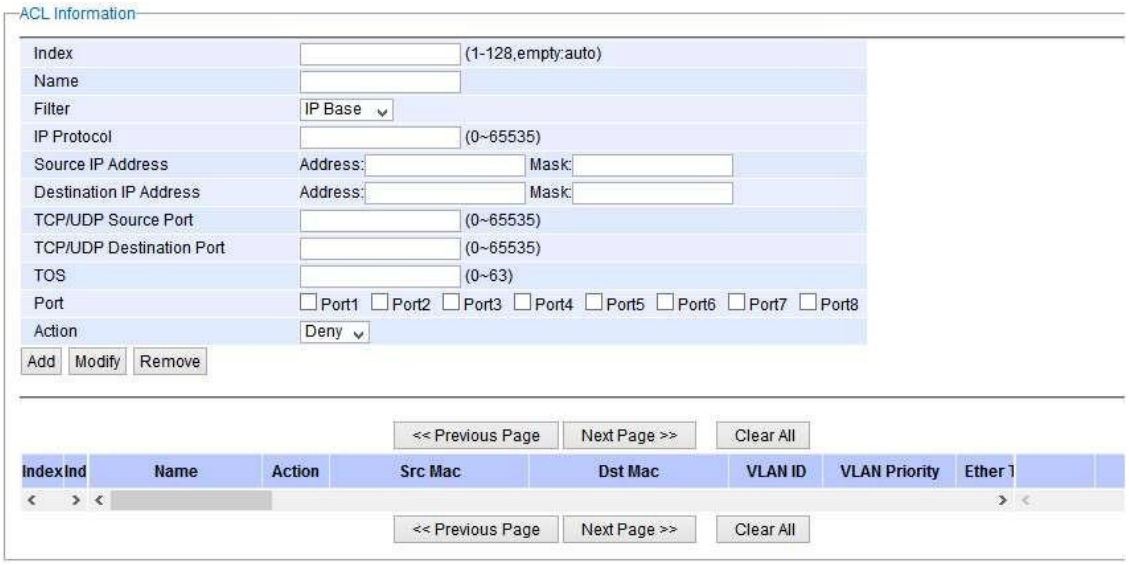


Figure 2.124 Security Access Control List Information Webpage (IP Based Filtering)

Table 2.50 Description of Main ACL Entries for L3 Filtering in ACL Webpage

ACL Entry	Definition	Range
IP Protocol	The Protocol field of the IPv4 packet header. The followings are examples. The value 1 is for an ICMP packet. The value 6 is for the TCP packet. The value 17 is for the UDP packet.	The item value is between 0~65535.
Source or Destination IP Addresses	The VLAN ID field of 802.1Q VLAN tag in the Ethernet frame header. The Mask item is a bit mask for comparing range.	For every non-zero bits in the Mask, its relative bit in the IP address will be compared. If the Mask is 0.0.0.0.0.0, then this condition is always accepted. If the Mask is empty, it is considered equal to the Mask of FF:FF:FF:FF:FF:FF and all of bits in the IP Address are compared.
TCP/UDP Source Port / TCP/UDP Destination Port	The fields of TCP/UDP frame header. It is used to filter the application services. For example, the TCP Destination Port 21 is for the FTP service, the TCP Destination Port 23 is for the Telnet service and the TCP Destination	The item value is between 0~65535.

	Port 80 is for the HTTP service. To select which ports will follow the filter rule and what action to take, check the checkbox corresponding to that port and select choice of “Deny” or “Permit” in the action field. If this ACL entry is match, rejecting packet if 'Deny' is selected, and accepting packet if ‘Permit’ is selected.	
TOS (Type of Service)	A Differentiated Service Code Point (DSCP) field in an IPv4 header. It is used for providing Quality of Service (QoS).	The item value is between 0~63.

Table 2.51 Summary of Label, Description, and Factory Default for Both ACL Filtering Method

LABEL	DESCRIPTION	FACTORY DEFAULT
Index	Priority (1-128)	NONE
Name	Max length 32	NONE
Filter	Mac Base/IP Base	Mac Base
Source MAC Address and Mask	A:B:C:D:E:F. is the MAC address. Mask is for bit mask checking. 0.0.0.0.0.0 is for accepting all. Empty is as FF:FF:FF:FF:FF:FF.	NONE
Destination MAC Address and Mask	A:B:C:D:E:F. is the MAC address. Mask is for bit mask checking. 0.0.0.0.0.0 is for accepting all. Empty is as FF:FF:FF:FF:FF:FF.	NONE
VLAN ID	1-4094	NONE
VLAN Priority Tag	0 ~ 7	NONE
Ether Type	0-FFFF	NONE
IP Protocol	0-65535	NONE
Source IP Address	A.B.C.D is the IP address. Mask is for bit mask checking. 0.0.0.0 is for accepting all. Empty is as 255.255.255.255.	NONE
Destination IP Address	A.B.C.D is the IP address. Mask is for bit mask checking. 0.0.0.0 is for accepting all. Empty is as 255.255.255.255.	NONE
TCP/UDP Source Port	0-65535	NONE
TCP/UDP Destination Port	0-65535	NONE
TOS	0-63	NONE
Port	1,2,3,4,5,6,7,8, trk1, trk2	NONE
Action	Deny/Permit	NONE

The users can **Add**, **Modify**, or **Remove** each ACL entry based on the Index number as shown in Figure 2.123 and Figure 2.124. The lower part of the ACL Information webpage is the list of all ACL entries. The user can browse through the list by using the **Previous Page** and **Next Page** buttons. To remove all of the ACL entries from the list, click on the **Clear All** button.

2.15 ERPS/Ring

Ethernet **R**ing **P**rotection **S**witching (**ERPS**) is a protocol for Ethernet layer network rings. The protocol specifies the protection mechanism for sub-50ms delay time. The ring topology provides multipoint connectivity economically by reducing the number of links. ERPS provides highly reliable and stable protection in the ring topology, and it never forms loops, which can affect network operation and service availability. Figure 2.125 depicts an example of ring topology forming by four Agatel's managed switch XE75XX series.

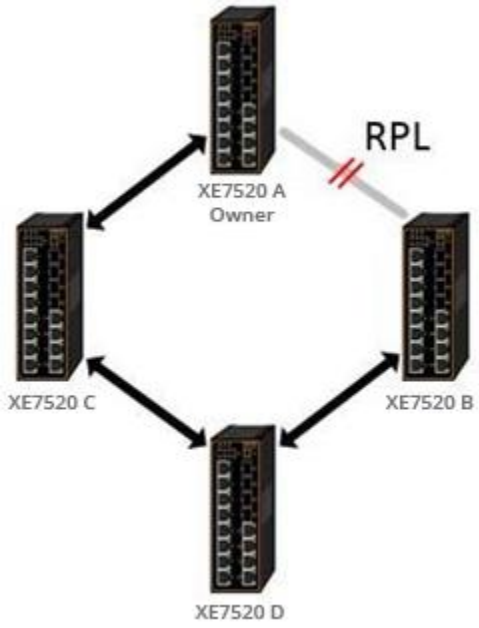


Figure 2.125 An Example of Ring Topology

Figure 2.125 shows that each Ethernet Ring Node is connected to its 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 Ring Automatic Protection Switch (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, one designated Ethernet Ring Node called the RPL Owner Node will be responsible for unblocking its end of the RPL to allow RPL to be used as a backup link. The RPL is the backup link when one link failure occurs.

Agatel's XEG/XE75XX series industrial managed switches provide a number of Ethernet ring protocol. The **ERPS/Ring** section is subdivided into five menus as shown in Figure 2.126, which are: **ERPS Setting**, **iA-Ring Setting**, **C-Ring Setting**, **U-Ring Setting**, **and Compatible-Chain Setting**.

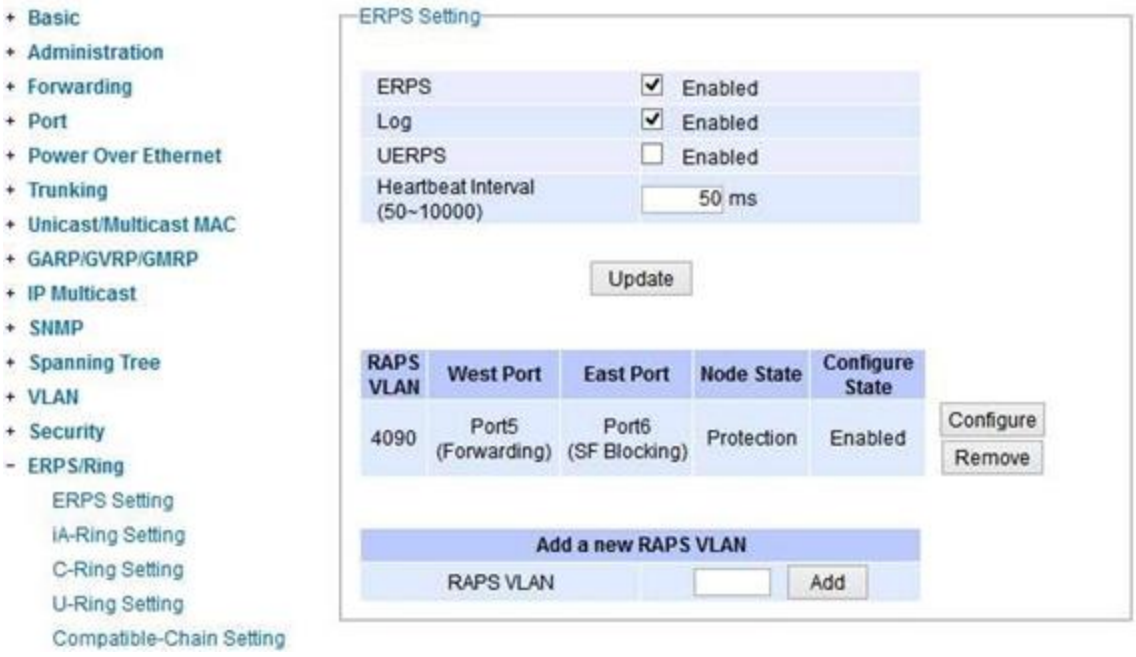


Figure 2.126 ERPS/Ring Drowdown Menu

2.15.1 ESRP Setting

ERPS Setting webpage is shown in Figure 2.127. Note that the users should disable the **DIP Switch Control** in Section 2.3.12 first in order to set up ERPS parameters. To set up ERPS on the current managed switch, please follow the following steps:

1. Enable the ERPS by checking on the **ERPS**'s **Enabled** checkbox.
2. If the users would like to keep the log, please also check the **Log**'s **Enabled** checkbox.
3. Optionally, if the users want the switch to periodically check the status of the neighboring switches on the ring topology using heartbeat packets then the user can check the **UERPS**'s **Enabled** checkbox. Note that when this feature is enabled, the recovery time of the ring topology may be longer.
4. Optionally, the users can fine tune the heartbeat interval by changing the default value 50 milli-seconds to the desired value.
5. Click on the **Update** button.
6. Skip down to **Add a new RAPS VLAN** section at the bottom of the webpage. Enter the desired **RAPS VLAN** ID in the field and click the **Add** button. The VLAN ID can be the value between 1 to 4094. Table 2.52 summarizes the fields in ERPS Setting webpage.

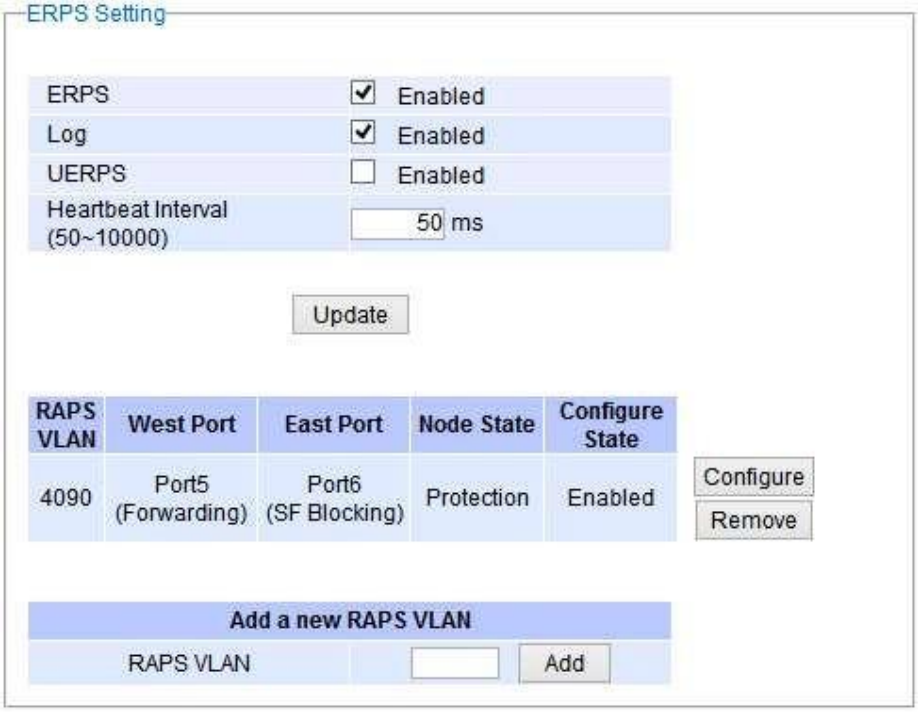


Figure 2.127 ERPS Setting Webpage

Table 2.52 Descriptions of ERPS Setting

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 affects the recovery time to more than 20 ms.	Disabled
Heartbeat Interval	Set the Heartbeat Interval. Range from 50 to 10000 milliseconds.	50 ms
RAPS VLAN	Create the ring by specifying the R-APS VLAN ID of the ring. VLAN ID ranges from 1 to 4094.	NULL

7. Click the **Configure** button on the right hand side of the webpage that corresponding to the RAPS VLAN that was entered in previous step. A new webpage will be displayed for the users to config additional parameters **for ERPS RAPS VLAN Setting** as shown in Figure 2.128.
8. Configure the RAPS VLAN’s **Status**, **West Port**, **East Port**, **RPL Owner**, **RPL Port**, **WTR Timer**, **Holdoff Timer**, **Guard Timer**, **MEL**, and **Propagate TC**. Detail description of these parameters are summarized in Table 2.53. Then, click **Update** button to finish the setting up of new RAPS VLAN.

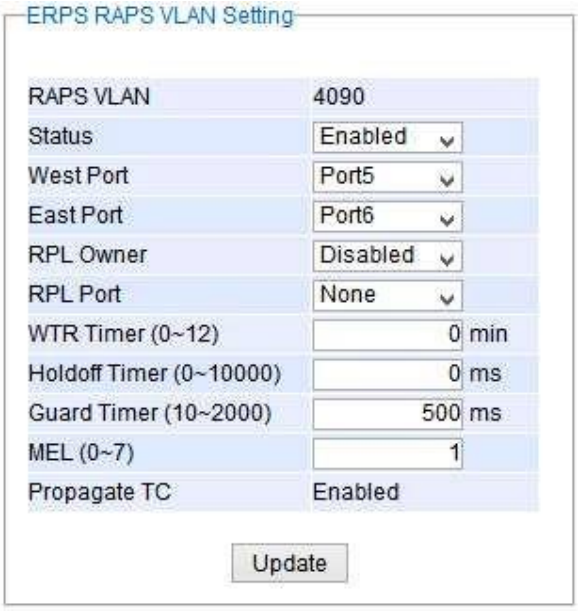


Figure 2.128 ERPS RAPS VLAN Setting Webpage

Table 2.53 Description of ERPS RAPS VLAN Setting

Label	Description	Factory Default
ERPS VLAN	Indicate current RAPS VLAN ID to be configured	None
Status	Choose to enable ERPS with this particular VLAN	Disabled
West Port	Choose the *West Por*t of the RPL	Port1
East Port	Choose the *East Por*t of the RPL	Port2
RPL Owner	Choose to enable Owner Function	Disabled
RPL Port	Select the *Owner Port* which is either West Port or East Port or None.	None
WTR Timer	Set the wait-to-restore (WTR) time of the ring in minutes. Lower value has lower protection time. Range of the WTR Timer is from 0 to 12 minutes.	5
Holdoff Timer	Set the holdoff time of the ring. Range of the Holdoff Timer is from 0 to 10000 milliseconds.	0
Guard Timer	Set the guard time of the ring. Range of the Guard Timer is from 0 to 2000 milliseconds.	500
MEL	Set the maintenance entity group level (MEL) of the ring. Range of MEL is from 0 to 7.	1
Propagate TC	Indicate the topology change propagation of the ring ability.	Enabled

2.15.1.1 Example of ERPS Settings

To allow the users to understand the setting up of ERPS on the XEG75XX industrial managed switches, this subsection provides an example of ERPS setup with four Agatel's managed switches as shown in Figure 2.129. Assuming that the ring network has XEG75XX A, XEG75XX B, XEG75XX C, and XEG75XX D. There is an RPL between XEG75XX A and XEG75XX B. Note that the figure is based on

the XE7520 model but it is applicable to any of XEG75XX models.

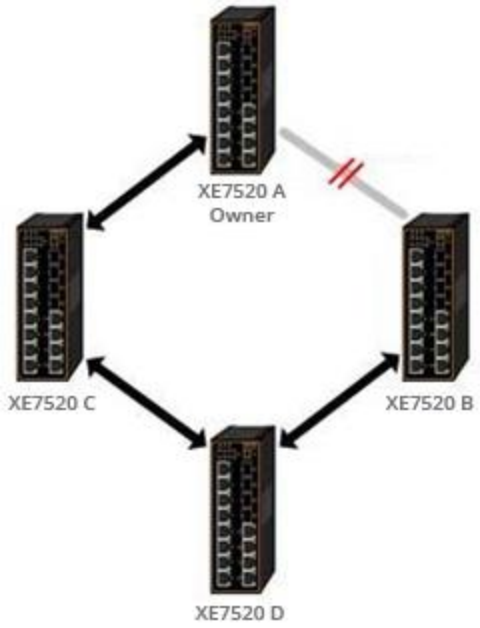


Figure 2.129 Example of Ring Topology for ERPS Setup

For each switch, please follow the procedure outline in previous section. First, enabling the ERPS and then add the RAPS VLAN = 8. On each managed switch, the users can configure ARPS VLAN Setting according to Table 2.54 and Table 2.55.

Table 2.54 Setting Configuration for Switch A and B

XEG75XX	**A**
RAPS VLAN	8
ERPS RAPS	Enabled
West Port	1
East Port	2
RPL Owner	Enabled
RPL Port	West

XEG75XX	**B**
RAPS VLAN	8
ERPS RAPS	Enabled
West Port	1
East Port	2
RPL Owner	Disabled
RPL Port	none

Table 2.55 Setting Configuration for Switch C and D

XEG75XX	**C**
RAPS VLAN	8
ERPS RAPS	Enabled
West Port	1
East Port	2
RPL Owner	Disabled
RPL Port	none

XEG75XX	**D**
RAPS VLAN	8
ERPS RAPS	Enabled
West Port	1
East Port	2
RPL Owner	Disabled
RPL Port	none

2.15.1.2 UERPS Settings (Optional)

The following procedure outlines the **UERPS** Setting under the **ERPS Setting**. The users can follow them as an exercise.

1. Prepare two managed switches (Switch A and Switch B). We will use Port 7 and Port 8 on both switches for redundancy.
2. Connect Switch A and Switch B to the network or PC so that you can access them. For simplicity, the users can use Port 1 for Web configuration on both switches.
3. Open Device Management Utility or Switch View (described in Chapter 5) and change the IP address of Switch B or both switches such that the IP addresses will not be conflicting.
4. Open Switch A and B's WebUI and setup ERPS settings like the following. Enable ERPS, Log, and UERPS accordingly as shown in Figure 2.130. Then, press **Update** button for the changes to take effect.

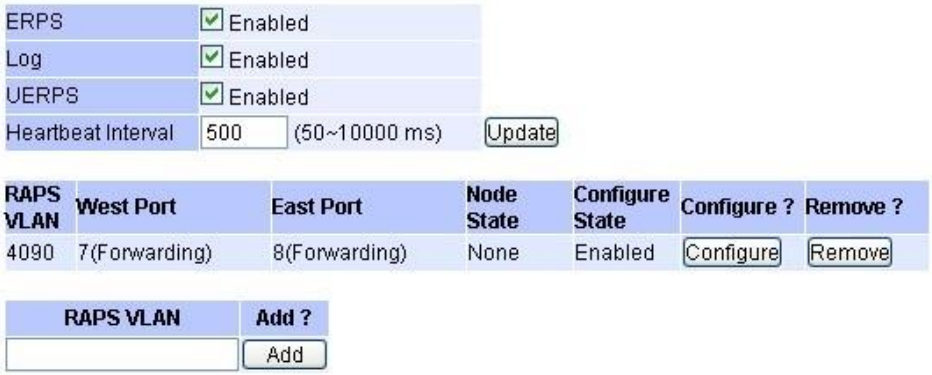


Figure 2.130 Example of Switch A's ERPS settings

5. On Switch A, Click **Configure** button on RAPS VLAN and input settings as shown in Figure 2.131.

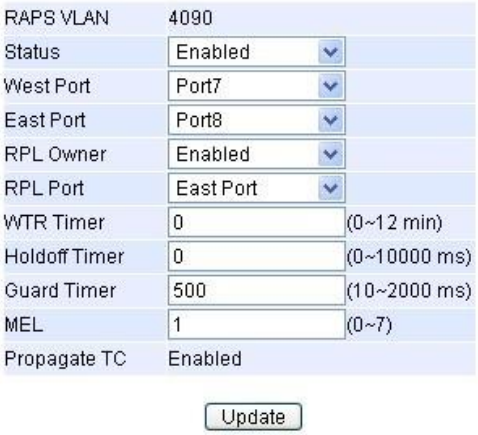


Figure 2.131 Example of Switch A's RAPS VLAN Settings

6. Open Switch B's WebUI and input settings for ERPS as shown in Figure 2.132.

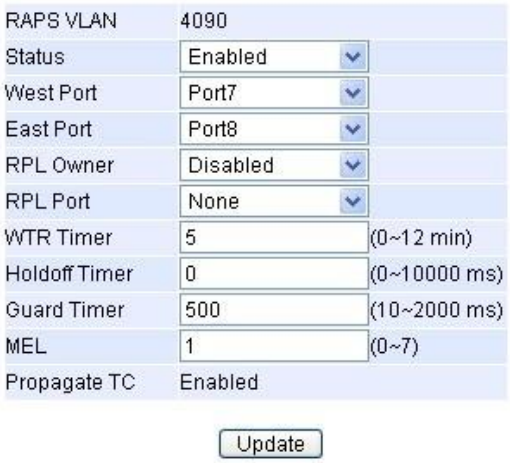


Figure 2.132 Example of Switch B's RAPS VLAN Setting

7. Connect Switch A's Port 7 to Switch B's Port 8, and connect Switch A's Port 8 to Switch B's Port 7 (like cross-over) for the redundancy port.
8. If everything is set up properly, you will find Switch A having the following ERPS state as shown in Figure 2.133. Also, it will automatically block Port 8 to prevent a network loop.

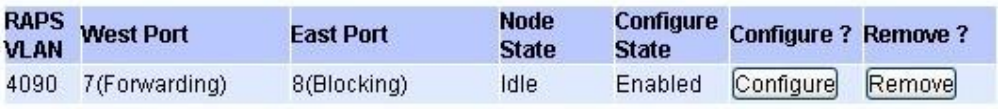


Figure 2.133 Switch A's ERPS state

9. From here on, the users can add another bridge between the two managed switches.

2.15.2 iA-Ring Settings

The Agatel's managed switch 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 in the diagram below (Figure 2.134).

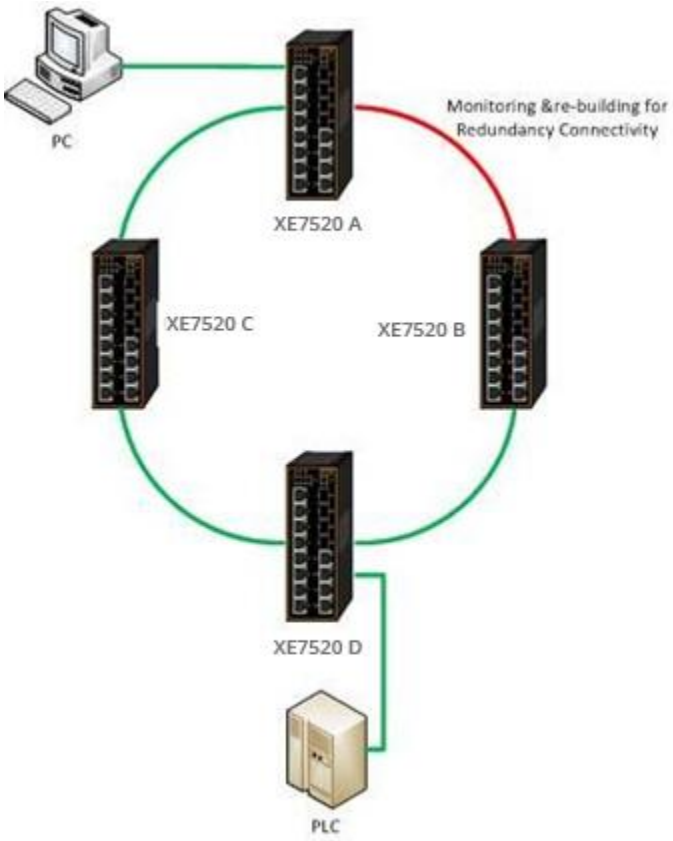


Figure 2.134 iA-Ring Example Topology

Figure 2.135 shows **iA-Ring Setting** webpage. The iA-Ring redundancy protocol can be enabled on this page. Note that the users should disable **DIP Switch Control** as described in Section 2.3.12 and disable **ERPS** as described in Section 2.15.1 first in order to enable/configure iA-Ring parameters on the web browser. Please follow the simple steps below based on Figure 2.135 to setup the iA-Ring.

1. Enable the **iA-Ring** by selecting **Enabled** from the dropdown list.
2. Choose whether the current managed switch is going to be the **Ring Master** by enabling the **Ring Master** option.
3. Select the **1st Ring Port** from the dropdown list.
4. Select the **2nd Ring Port** from the dropdown list.
5. Click on the **Update** button to save the change and allow the configuration to take effect.
6. Check the latest status of the iA-Ring configuration by clicking on the **Refresh** button.

Note that the lower part of the iA-Ring Setting webpage shows the **Status** of the iA-Ring which provides its **State**, **1st Ring Port Status** and **2nd Ring Port Status**. The description of the iA-Ring setting is summarized in Table 2.56.



Figure 2.135 iA-Ring Setting Webpage

Table 2.56 Descriptions of iA-Ring Setting

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 iA-Ring.	Port1
2nd Ring Port	Select the backup port for the iA-Ring.	Port2

2.15.3 C-Ring (Compatible-Ring) Settings

Compatible-Ring (**C-Ring**) is similar to iA-Ring. The only difference is that it can be used for MOXA rings as well. For more information about this redundant ring protocol, please contact Agatel Ethernet Switching.

Figure 2.136 shows how to set the Compatible-Ring (**C-Ring**) redundancy protocol. Note that the users should disable **DIP Switch Control** as described in Section 2.3.12 and **ERPS** as described in Section 2.15.1 first in order to enable/configure Compatible-Ring parameters on the web browser. Please follow the simple steps below based on Figure 2.136 to setup the C-Ring.

1. Enable the **C-Ring** by selecting **Enabled** from the dropdown list.
2. Select the **1st Ring Port** from the dropdown list.
3. Select the **2nd Ring Port** from the dropdown list.
4. Click on the **Update** button to save the change and allow the configuration to take effect.

Note that the lower part of the C-Ring Setting webpage shows the **Status** of the C-Ring which provides

its **State**, **1st Ring Port Status** and **2nd Ring Port Status**. The description of the C-Ring setting is summarized in Table 2.57.



Figure 2.136 Compatible-Ring (C-Ring) Setting Webpage

Table 2.57 Descriptions of Compatible-Ring Setting

Label	Description	Factory Default
C-Ring (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

2.15.4 U-Ring

This section enables the setup of U**-**Ring **(**Unicast Ring**)** on the managed switch**.** The U**-**Ring could provide redundancy connection between two XEG75XX industrial managed switches which are not directly connected by physical wires but by two additional network devices on each switch**.** There are two examples of U-Ring application presented here to provide as guidelines when to choose this U-Ring feature.

First example is depicted in Figure 2.137 where there are two XE75XX managed switches. On each switch it is connected to two wireless Access Points (AP) via two different Ethernet LAN ports. Both wireless Access Points are connected to another two wireless Access Points as two separate wireless bridge connection. Based on Figure 2.137, XE75XX A has AP 1 on port 8 and AP 3 on port 7 while XE75XX B has AP 2 on port 7 and AP 4 on port 8. The AP 1 and the AP 2 are connected as wireless Bridge Connection 1 and the AP 4 and the AP 3 are connected as wireless Bridge Connection 2.

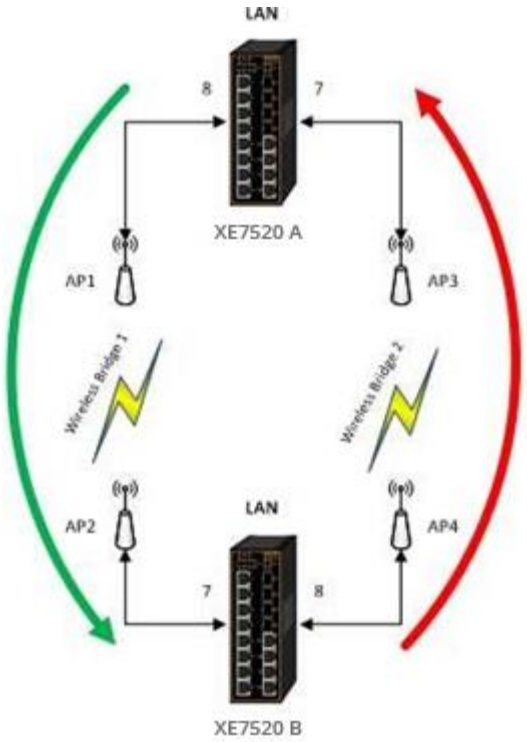


Figure 2.137 Example 1 of Two Wireless Bridge U-ring

Second example is illustrated in Figure 2.138 where there are also two XE75XX managed switches. On each switch it is connected to two wired Access Points (AP) via two different Ethernet LAN ports. Both wired Access Points are connected to another two wired Access Points as two separate wired bridge connection. Based on Figure 2.138, XE75XX A has AP 1 on port 8 and AP 3 on port 7 while XE75XX B has AP 2 on port 7 and AP 4 on port 8. The AP 1 and the AP 2 are connected as wired Bridge Connection 1 and the AP 4 and the AP 3 are connected as wired Bridge Connection 2. There are two physical lines between both pair of APs. The U-ring protocol could be used in this environment. The different of this example from the previous example is that the AP_x could be:

- **Unmanaged-switch**
- **Transceiver**
- **XDSL bridge**

Note that care should be taken that if a dumb switch is used as an AP (**A**ccess **P**oint). The one on the other side must be a dumb switch as well. Again, care should also be taken when connecting the cables to the ports.

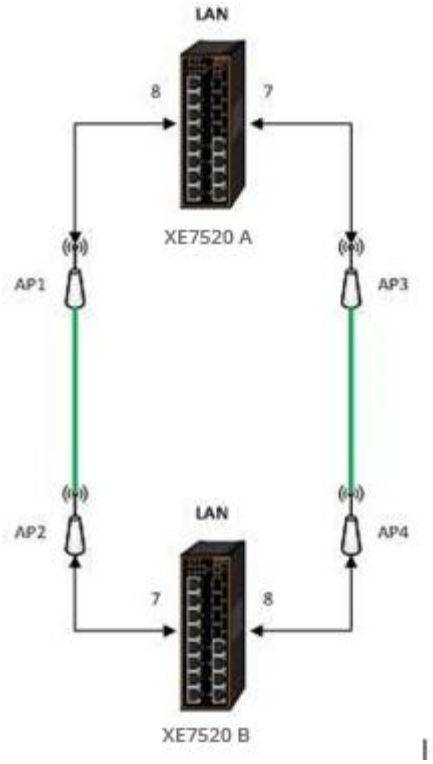


Figure 2.138 Example 2 of Two Wired Bridge U-ring

To setup the U-Ring, the users need to configure a number of parameters on U-Ring Setting webpage as shown in Figure 2.139. Please follow the simple steps below to setup the U-Ring.

1. Enable the **U-Ring** by selecting **Enabled** from the dropdown list.
2. Choose whether the current managed switch is going to be the **Ring Master** by enabling the **Ring Master** option.
3. Select the **1st Ring Port** from the dropdown list.
4. Select the **2nd Ring Port** from the dropdown list.
5. Optionally, set the **Heartbeat Expire** period which could be between 100 to 10000 milliseconds. Note that the default period is 100 ms.
6. Click on the **Update** button to save the change and allow the configuration to take effect.
7. Check the latest status of the U-Ring configuration by clicking on the **Refresh** button.

Note that the lower part of the **U-Ring Setting** webpage shows the **Status** of the U-Ring which provides its **State**, **1st Ring Port Status** and **2nd Ring Port Status**. The description of the U-Ring setting is summarized in Table 2.58.

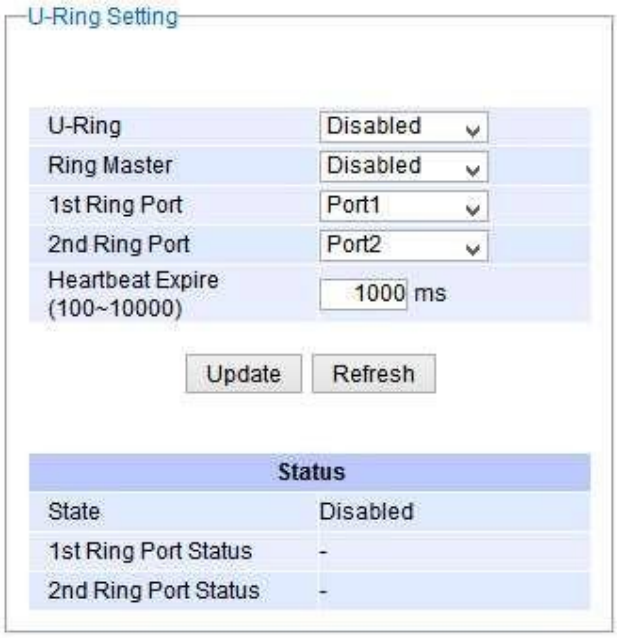


Figure 2.139 U-Ring Setting Webpage

Table 2.58 Descriptions of U-Ring Setting

Label	Description	Factory Default
U-Ring	Enabled or disabled the Unicast ring.	Disabled
Ring Master	Enabled or disabled this switch as the Ring Master of the Unicast Ring. For Ring Slave configuration, leave this option as disabled.	Disabled
1st Ring Port	Select which port on the managed switch will be the 1st Ring Port.	Port1
2nd Ring Port	Select which port on the managed switch will be the 2nd Ring Port.	Port2
Heartbeat Expire	Time interval between checking-packets.	1000
Update	Click this button to allow the configuration to take effect.	-
Refresh	Obtain the latest status of the U-Ring Setting by clicking on this button.	-
State	Shows whether the device's state is normal or protected.	Disable
1st Ring Port Status	Displays the status of the 1st Ring Port.	-
2nd Ring Port Status	Displays the status of the 2nd Ring Port.	-

2.15.5 Compatible-Chain Settings

The **Compatible-Chain Setting** is provided on Agatel's managed switches for compatible networking with Moxa switch's **Turbo Chain**. The MOXA's Turbo Chain is a technique that uses the chain network topology and links the two ends (two network devices such as industrial managed switches) of the chain to a common LAN. This can also be viewed as a form of Ring Topology. This Turbo Chain can provide redundancy on any type of network topology or on complex network topology such as multi-ring architecture. The Turbo Chain can create flexible and scalable topologies with a fast media-recovery time.

The fist switch on the **Compatible-Chain** will have a **Role State** as **Head** switch. The other switches along the **Compatible-Chain** will have a **Role State** as **Member** switches. The last switch on the **Compatible-Chain** will have a **Role State** as **Tail** switch. For Head switch, the first port which is connected to the common LAN is called **Head Port**, while the second port which is connected to the next switch in the Compatible-Chain is called **Member Port**. For **Member** switches, both ports of the Member switches are called **1st Member Port** and **2nd Member Port**. For **Tail** switch, the first port which is connected to another Member switch is call **Member Port**, while the second port which is connected to the common LAN is called **Tail Port**. In Turbo Chain configuration, the Head Port is the main path while the Tail Port is the backup path of the redundant topology. During no link-failure operation on the chain's path, all traffic will be forwarded to the Head Port to the common LAN. When there is a failure on the path of the chain, the Tail Port will be used for forwarding the traffic to the common LAN.

To configure Compatible-Chain, select the Compatible-Chain menu under the ERPS/Ring Section. Figure 2.140 shows the Compatible-Chain Setting webpage.



Figure 2.140 Compatible-Chain Setting Webpage

Please follow the simple steps below to setup the Compatible-Chain.

1. Enable the **Compatible-Chain** by selecting **Enabled** from the dropdown list.
2. Choose the **Role State** whether the current managed switch is going to be the **Head**, **Member** or **Tail** of the chain from the dropdown list of **Role State**.

3. If the current switch is the **Head** switch then select the **Head Port** from the dropdown list and select the **Member Port** from another dropdown list.
4. If the current switch is the **Member** switch then select the **1st Member Port** from the dropdown list and select the 2nd **Member Port** from another dropdown list.
5. If the current switch is the **Tail** switch then select the **Tail Port** from the dropdown list and select the **Member Port** from another dropdown list.
6. Click on the **Update** button to save the change and allow the configuration to take effect.

Note that the upper part of the **Compatible-Chain Setting** webpage shows the **Status** of the current switch in the chain which provides its **Role**, **1st Ring Port Status** and **2nd Ring Port Status**. The description of the Compatible-Chain setting is summarized in Table 2.58.

Table 2.59 Descriptions of Compatible-Chain Setting

Label	Description	Factory Default
Role	Display the role of the current switch in the Compatible-Chain: Head, Tail, or Member.	Member
1st Ring Port Status	Display the status of the 1st Ring Port.	Forwarding
2nd Ring Port Status	Display the status of the 2nd Ring Port.	Forwarding
Compatible-Chain	**Enabled** or **Disabled** the Compatible-Chain Ring	Disable
Role State	Choose the role of the current switch in the compatible chain: **Head**, **Tail**, or **Member**.	Member
Head Port	Select a particular port from the dropdown list to be the Head Port of the compatible-chain.	Port1
Tail Port	Select a particular port from the dropdown list to be the Tail Port of the compatible-chain.	Port1
Member Port	Select a particular port from the dropdown list to be the Member Port of the compatible-chain.	Port2
1st Member Port	Select a particular port from the dropdown list to be the Member Port of the compatible-chain.	Port1
2nd Member Port	Select a particular port from the dropdown list to be the Member Port of the compatible-chain.	Port2

2.16 LLDP

Link **L**ayer **D**iscovery **P**rotocol (**LLDP**) is an IEEE802.1ab standard OSI layer-2 protocol. LLDP allows Ethernet network devices to advertise details about themselves, such as device configuration, capabilities and identification. The advertise packets are periodically sent to directly connected devices on the network that are also using LLDP or so called its neighbors. LLDP is a “one hop” unidirectional protocol in an advertising mode. LLDP information can only be sent to and received by devices, no solicit information or state changes between nodes. The device has a choice to turn on and off sending and receiving function independently. Advertised information is not forward on to other devices on the network. LLDP is designed to be managed with SNMP. Applications that use this protocol include topology discovery, inventory management, emergency services, VLAN assignment, and inline power supply.

Link **L**ayer **D**iscovery Protocol (LLDP) section consists of **LLDP Setting** and **LLDP Neighbors** as shown in Figure 2.141.



Figure 2.141 LLDP Dropdown Menu

2.16.1 LLDP Settings

In Figure 2.142, the LLDP Setting webpage allows users to have options for enabling or disabling the LLDP, as well as setting LLDP transmission parameters. This LLDP function should be enabled if users want to use Agatel's Device Management Utility (formerly called Device View) to monitor the switches' topology of all LLDP devices in the network. For more information about using Device Management Utility, please refer to Chapter 5 in this document. Table 2.60 describes the LLDP Setting parameters which are transmit interval and transmit time-to-live of the LLDP advertisement packets.

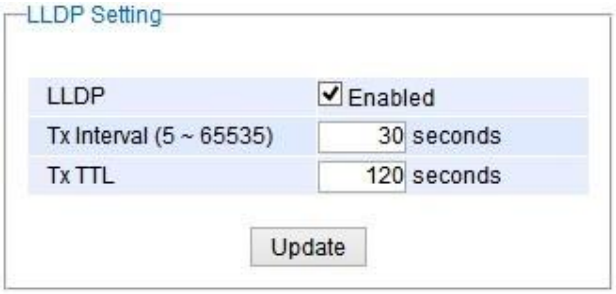


Figure 2.142 LLDP Setting Webpage

Table 2.60 Descriptions of LLDP Setting

Label	Description	Factory Default
LLDP	Choose to either enable or disable LLDP.	Enabled
Tx Interval	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*. The information is only removed when the timer is expired.Range from 5 to 65535 seconds.	120

2.16.2 LLDP Neighbors

This menu allows the user to view the LLDP's neighbor information of the managed switch as shown in Figure 2.143. The Neighbor Information table contains Chassis ID, Port ID, Port Description, Device Name, Device Description and Management Address on each Port of the managed switch. The users can click on the **Refresh** button to get the latest Neighbor Information table or click on the **Clear** button to clear all the information on the display Neighbor Information table.

An example of neighbor information table is depicted in Figure 2.144. Note that this example is based on a display format of an early version of XE75XX managed switch in which System Name is changed to Device Name and System Description is changed to Device Description in the latest version of XEG75XX's firmware. Table 2.61 summarizes the descriptions of each column of the LLDP's Neighbor Information.

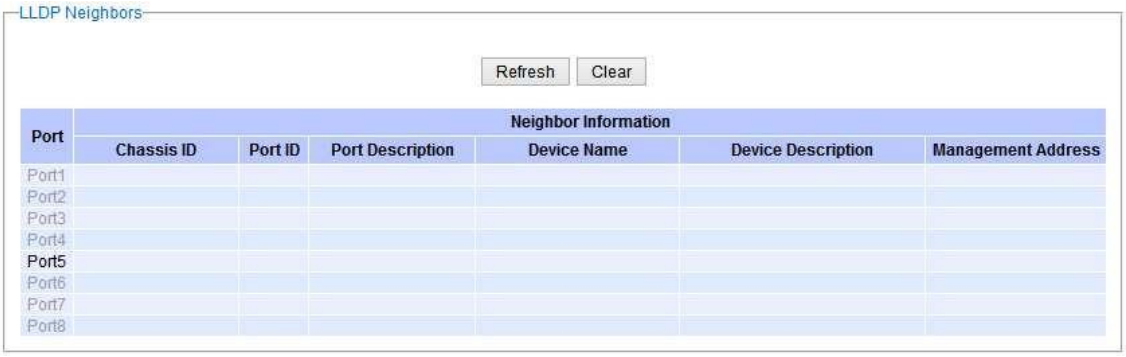


Figure 2.143 LLDP Neighbors Webpage

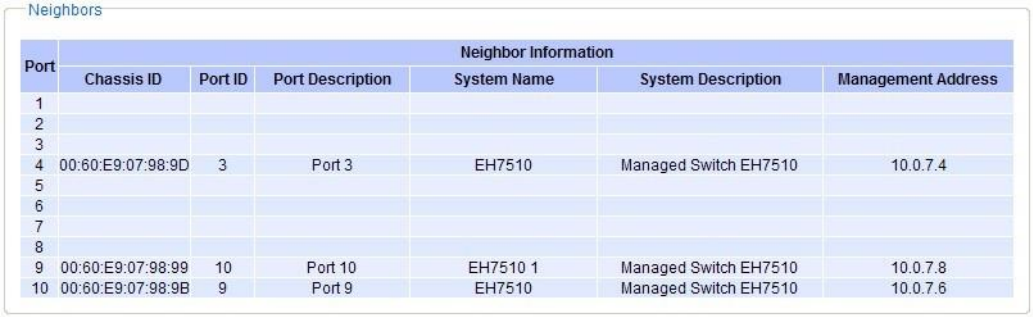


Figure 2.144 Example of LLDP Neighbors Webpage

Table 2.61 Descriptions of LLDP Neighbors Webpage

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.
Device Name	Indicates the device name/ hostname of the neighbor.
Device Description	Shows a more detailed description of the neighbor's device.
Management Address	Indicates neighbor's management IP address.

2.17 PROFINET

PROFINET (Process Field Net) is an open and advanced standard for the industrial automation based on the industrial Ethernet. PROFINET enables the users to exchange the process data with user's machines. In this case, instead of using fieldbus system, the users use the Ethernet as a communication mechanism. Figure 2.145 shows the dropdown menu of the PROFINET on an XEG75XX/XE75XX industrial managed switch. There are three subsections under the **PROFINET** which are **Setting**, **I&M**, and **MRP**.



Figure 2.145 PROFINET Dropdown Menu

2.17.1 PROFINET Settings

The PROFINET can be enabled on the XEG75XX/XE75XX industrial managed switch on this webpage.To enable the PROFINET, the users can check the **Enabled** box behind the **PROFINET** field. The webpage also displays the **Device Name** and **DIP Switch State** as shown in Figure 2.146. The PROFINET's **Packet Priority** can also be enabled on this webpage and priority **Queue** number can also be chosen from the dropdown list. Note that the higher the queue number, the higher the precedence for the packet scheduling.

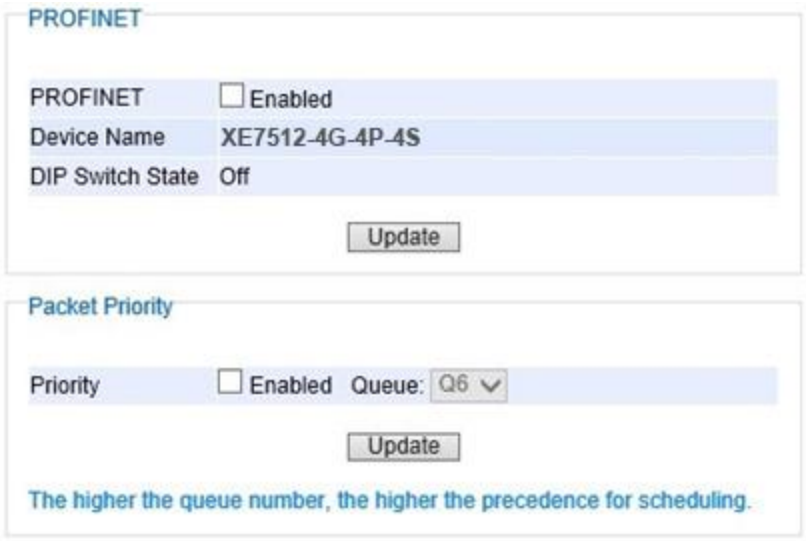


Figure 2.146 PROFINET Setting Webpage, example on XE7512

2.17.2 PROFINET's I&M

Identification and Maintenance (I&M) is an integral part of each PROFINET Device implementation. It provides standardized information about a device and its parts. I&M's Information is accessible through PROFINET Record Objects and is always bound to a sub module belonging to the item to be described. There are two I&M objects: I&M0 and I&M1. The I&M0 objects provide Vendor ID and Software (SW) Revision as shown in Figure 2.147. The I&M1 objects provide a non-volatile storage for PROFINET related information called Function Tag and Location Tag in which the users can enter the information and save them on the switch as shown in Figure 2.147. The information is stored by the device in non-volatile memory. After entering the desired information on the I&M1, please click the Update button to save them on the managed switch.

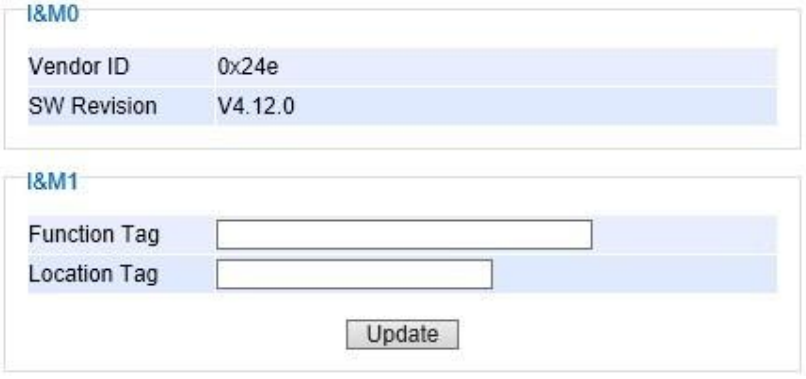


Figure 2.147 PROFINET I&M

2.17.3 PROFINET MRP

The Media Redundancy Protocol (MRP) is a data network protocol for Ethernet switch standardized by the International Electro technical Commission as IEC 62439-2. MRP is mostly used in and suitable for Industrial Ethernet applications. It allows rings of Ethernet switches to overcome any single failure with recovery time much faster than those achievable by Spanning Tree Protocol. It supports very fast failure recovery time. For example, a worst-case recovery time for 14 switches is about 10ms and for 50 switches is about 30ms.

The MRP includes following properties.

- It operates at the MAC layer of the Ethernet switches.
- It is a ring topology.
- Any single failure can be recovered.
- For switches in the network, there can be two roles:
    - Ring manager (MRM)
    - Ring client (MRC)
- For ring ports, there are three possible statuses: disabled, blocked, and forwarding.
    - Disabled ring ports drop all the received frames.
    - Blocked ring ports drop all the received frames except the MRP control frames.
    - Forwarding ring ports forward all the received frames.
- In normal case, one of the MRM ring ports is blocked to avoid looping and both ring ports of all MRCs are forwarding.
- When a path of the ring fail, the other port on the MRM will become active and forwarding.

The Media Redundancy Protocol (MRP) menu under the PROFINET section enables an implementation of a redundant PROFINET communication through ring topology without the need for switches. Figure 2.148 shows the MRP Setting webpage. Please follow the outlined steps here to setup the PROFINET's MRP:

1. Enter a desired **VLAN** ID in the field at the bottom of the **MRP** Setting webpage and click **Add** button as shown in Figure 2.148.



Figure 2.148 MRP Setting Webpage

2. After the MRP Ring is created with the desired VLAN, there will be an entry of the MRP VLAN on the table at the top of the page as shown in Figure 2.149. There will also be two new buttons

at the end of the entry: **Configure** and **Remove**. The users can click on the Configure button the continue setting up the MRP Ring on the managed switch.



Figure 2.149 Example of PROFINET's MRP VLAN Entry

Table 2.62 Description of MRP Setting Webpage

Label	Description	Factory Default
VLAN	MRP Ring **VLAN** ID	Depend
Role State	Role status setting (**Manager** or **Client**)	Client
1st Ring Port	Port number and port status (Link Down, Blocked, Forwarding).	Port1
2nd Ring Port	Port number and port status (Link Down, Blocked, Forwarding).	Port2
Configure State	**Enabled** or **Disabled** state of MRP Ring function	Disabled

3. After clicking the Configure button on the desired entry, a new webpage called MRP Ring Setting will show up as shown in Figure 2.150.



Figure 2.150 MRP Ring Setting Webpage

4. Then, the users can set MRP Ring parameters for the current switch, which are the **Status**, **1st Ring Port**, **2nd Ring Port**, and **Rote State** as described earlier. Table 2.63 summarizes the description of MRP Ring Setting parameters.
5. Click on the **Update** button to allow the configuration to take effect. Note that if there is other ERPS Ring Topology already setting up on the managed switch there may be an error message popping up as shown in Figure 2.151. Therefore, the users should disable the ERPS/Ring

(Section 2.15.1) and DIP Switch Control (Section 2.3.12) first before setting up this MRP Ring.



Figure 2.151 MRP Ring Setting Error Message

Table 2.63 Descriptions of MRP Ring Setting

Label	Description	Factory Default
Ring VLAN	Display the current MRP Ring **VLAN** ID to be configured.	Depend
Status	**Disabled** or **Enabled** the ring function**.**	Disabled
1st Ring Port	Select the **1st Ring Port** from the dropdown list.	Port1
2nd Ring Port	Select the **2nd Ring port** from the dropdown list.	Port2
Role Status	Select the role status to be either Ring **Client** or Ring **Manager**.	Client

2.18 EtherNet/IP

EtherNet/IP is an industrial Ethernet network that combines standard Ethernet technologies with the media-independent Common Industrial Protocol (CIP). EtherNet/IP uses both of the most widely deployed collections of Ethernet standards (the Internet Protocol suite and IEEE 802 standard) to define the features and functions for its transport, network, data link, and physical layers. CIP uses its object-oriented design to provide EtherNet/IP with the services and device profiles needed for real-time control applications and to promote consistent implementation of automation functions across a diverse ecosystem of products.

EtherNet/IP classifies Ethernet nodes as predefined device types with specific behaviors. EtherNet/IP has the following properties:

- Transfer of basic I/O data via User Datagram Protocol (UDP)-based implicit messaging
- Uploading and downloading of parameters, setpoints, programs and recipes via TCP (i.e., explicit messaging.
- Polled, cyclic, and change-of-state monitoring via UDP
- One-to-one (unicast), one-to-many (multicast), and one-to-all (broadcast) communication via IP
- EtherNet/IP makes use of well-known TCP port number 44818 for explicit messaging and UDP port number 2222 for implicit messaging

EtherNet/IP is an application layer protocol that is transferred inside a TCP/IP Packet. EtherNet/IP defines the way data is organized in a TCP or UDP packet. All devices on an EtherNet/IP network present data to the network as a series of data values called attributes grouped with other similar data values into sets of attributes called Objects. Figure 2.152 shows the EtherNet/IP section on the managed switch.

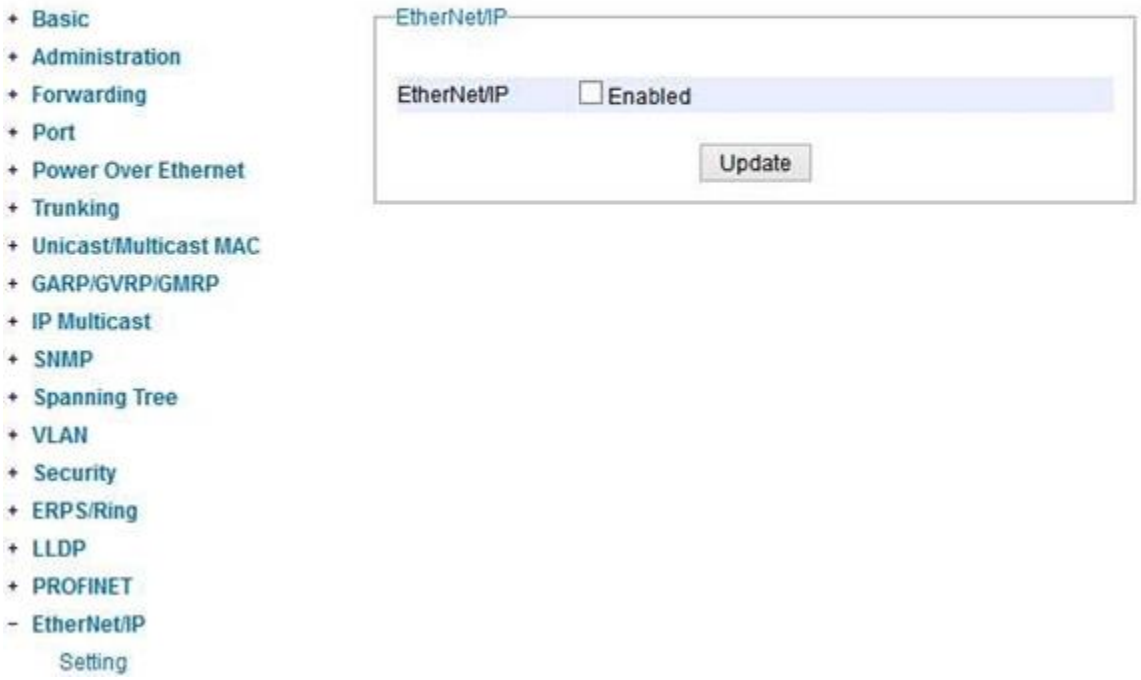


Figure 2.152 EtherNet/IP Dropdown Menu

2.18.1 EtherNet/IP Settings

To setup the EtherNet/IP feature on the XEG75XX industrial managed switch simply check the **Enabled** box behind the EtherNet/IP and click the **Update** button as shown in Figure 2.153.

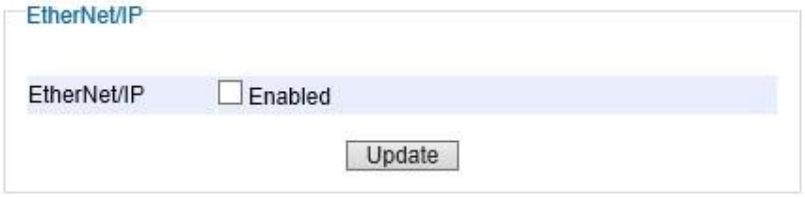


Figure 2.153 EtherNet/IP Setting Webpage

2.19 Client IP Setting

The XEG75XX industrial managed switch has two different approaches for setting up the IP addresses for the devices connected to its ports. The following are the submenus under the **Client IP Setting** section:

1. **DHCP Relay Agent**,
2. **DHCP Mapping IP**.

Figure 2.154 shows the dropdown menus under the **Client IP Setting** section.

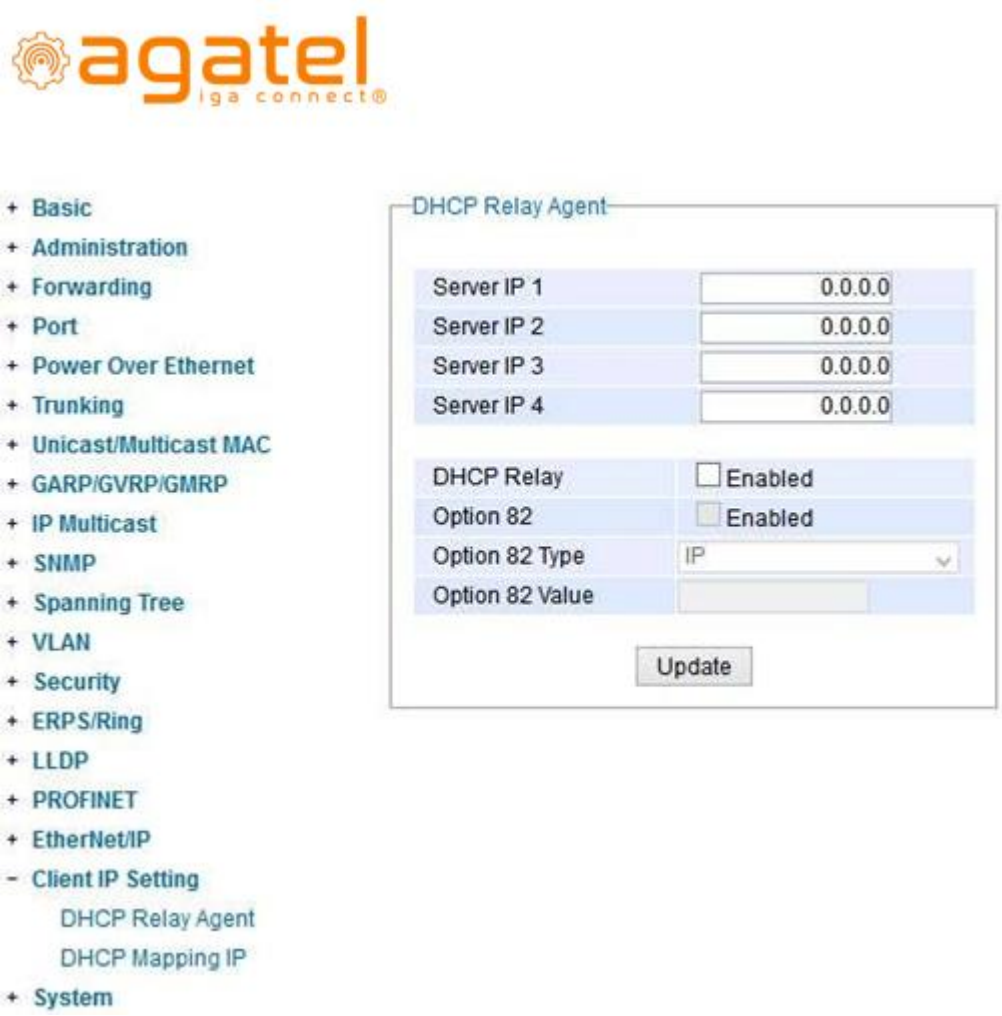


Figure 2.154 Client IP Setting Dropdown Menu

2.19.1 DHCP Relay Agent

A DHCP relay agent is a small program that relays DHCP/BOOTP messages between clients and servers on different subnets. DHCP/BOOTP relay agents are parts of the DHCP and BOOTP standards and function according to the Request for Comments (RFCs).

A relay agent relays DHCP/BOOTP messages that are broadcast on one of its connected physical interfaces, such as a network adapter, to other remote subnets to which it is connected by other physical interfaces. Figure 2.155 shows the **DHCP Relay Agent** setting webpage. The users can enter up to four DHCP/BOOTP server IP addresses in the fields: **Server IP 1**, **Server IP 2**, **Server IP 3**, and **Server IP 4**. Then the users can enable the DHCP Relay by checking the **Enabled** box behind the DHCP Relay option.

The users can also have a choice to enable DHCP's **Option 82** which is the DHCP Relay Agent Information Option. When this Option 82 is enabled, the switch will insert information about the client's network location into the packet header of DHCP request coming from the client on an untrusted interface. Then, the switch will send the modified request to the DHCP server. The DHCP server will inspect the option 82 information in the packet header and use it to generate the IP address or other parameters for the client. When the DHCP server returns the response to the switch, the switch will remove the option 82 information from the response packet and forward it to the client. The Option 82 Type field in Figure 2.155 can be chosen from **IP**, **MAC**, **Client-ID**, or **Other** in the dropdown list. When **Other** type is selected, the **Option 82 Value** field will become active for entering the desired value by the users. After finishing the DHCP Relay Agent setup, please click on the **Update** button to allow the change to take effect.



Figure 2.155 DHCP Relay Agent Webpage

2.19.2 DHCP Mapping IP

The user can reserve or map IP addresses to the device connected on the selected ports in this submenu. Figure 2.156 shows the DHCP Mapping IP webpage where the desired IP address can be enter into the field for each Port. After finishing the DHCP IP mapping to the port(s), please click on the **Update** button to allow the change to take effect.



Figure 2.156 DHCP Mapping IP Webpage

2.20 System

This last section on the WebUI interface of the XEG75XX managed switch provides miscellaneous tools for network administrator to check the internal status of the switch via system log, warning, and alarm notification. It also allows the administration to perform device maintenance operations such as backing up and restoring device's configuration, updating the firmware, reversing the device to factory default setting, or reboot the system/device. Figure 2.157 shows all the dropdown menus under the **System** section.

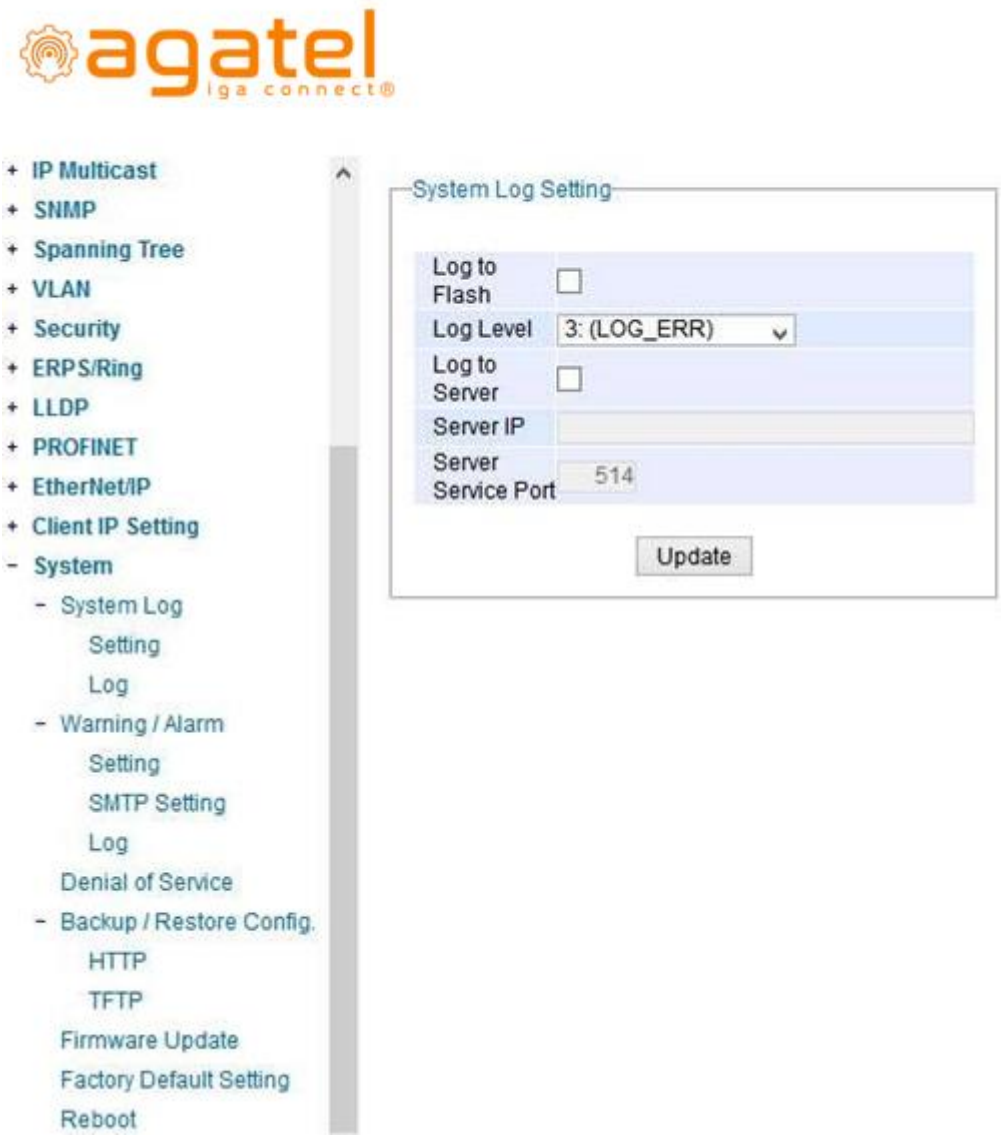


Figure 2.157 System Dropdown Menu

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 promptly 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 network administrators, so that network administrators can

be informed instantaneously when accidents happen. Email alerts and relays outputs under the System section is used to provide fast and reliable warning alerts for administrators.

2.20.1 System Log

The submenus under the System Log are: **Setting** and **Log**.

2.20.1.1 System Log Settings

Figure 2.158 shows System Log related settings configuration. The actual recorded log event will be shown in Event Log on the next subsection. Here the users can enable how the log will be saved and/or delivered to other system. The log can be save to flash memory inside the managed switch and/or it can be sent to a remote log server. The users need to select the log level and provide the IP address of a remote log server and the service log service port. Please click on the Update button after finishing the setup. Table 2.64 describes the details of parameters setting for the system log.



Figure 2.158 System Log Setting Webpage

Table 2.64 Descriptions of System Log Settings

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 webpage (**Log**). The level selection is inclusive. For example, if 3 :(Log_ERR) is selected, all 0, 1, 2 and 3 log levels will be implied. Range from Log 0 to Log 7.	3: (LOG_ERR)
Enable System Log Server	**Checked**: Enable Syslog Server. **Uncheck**: Disable Syslog Server. If enabled, all recorded log events will be sent to the remote System Log server.	Uncheck
System Log Server IP	Set the IP address of Syslog server	0.0.0.0
System Log Server Service Port	Set the service port number of System Log server. Range from Port 1 to Port 65535.	514

2.20.1.2 System Log - Log

Figure 2.159 shows an example of all of the event's logs. Note that they are sorted by date and time. Table 2.65 provides explanation of each column and the button's functions on the System Log webpage.

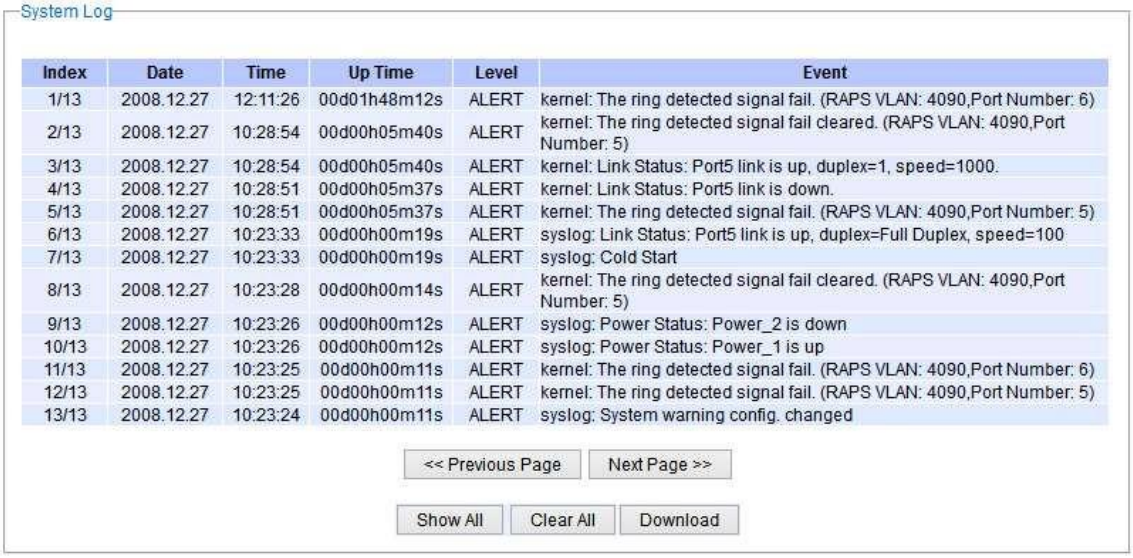


Figure 2.159 Event Log Webpage

Table 2.65 Descriptions of Event Log

Label	Description
Index	Indicate the index of a particular log event
Date	Indicate the system date of the occurred event
Time	Indicate the time stamp that this event occurred
Up Time	Indicate how long the system (managed switch) has been up since this event occurred.
Level	Indicate the level of this event.
Event	Details description of this event.
Previous Page	Display events on the previous page.
Next Page	Display events on the next page
Show All	Click to display all events.
Clear All	Click to clear all events
Download	Download or save the event log to the local computer

2.20.2 Warning/Alarm

The warning/alarm section as shown in Figure 2.160 consists of three subsections: **Setting**, **SMTP Setting**, and **Log**.



Figure 2.160 Warning/Alarm Dropdown Menu

2.20.2.1 Warning/Alarm Settings

There are three different types of Warning or Alarm: Link Status Alarms, Power Status Alarms, and System Log Alarms as shown in Figure 2.161. The Link Status Alarms are related to the activities of particular port(s). Power Status Alarms keep track of power status of the switch based on the available input connectors. System Log Alarms are related to the overall functionalities of the switch. This webpage allows the users to configure how each type of the alarm events will be sent or notify the users. For link status and power status alarms, there are three possible notification methods via Relay, E-mail, and Alarm LED. For System Log alarms, there are only two possible notification methods via Relay and E-mail. After finish configuring the alarms, please click the **Update** button. Note that there is an **Assert Relay** button which can be used to test an external Relay connected to the managed switch.

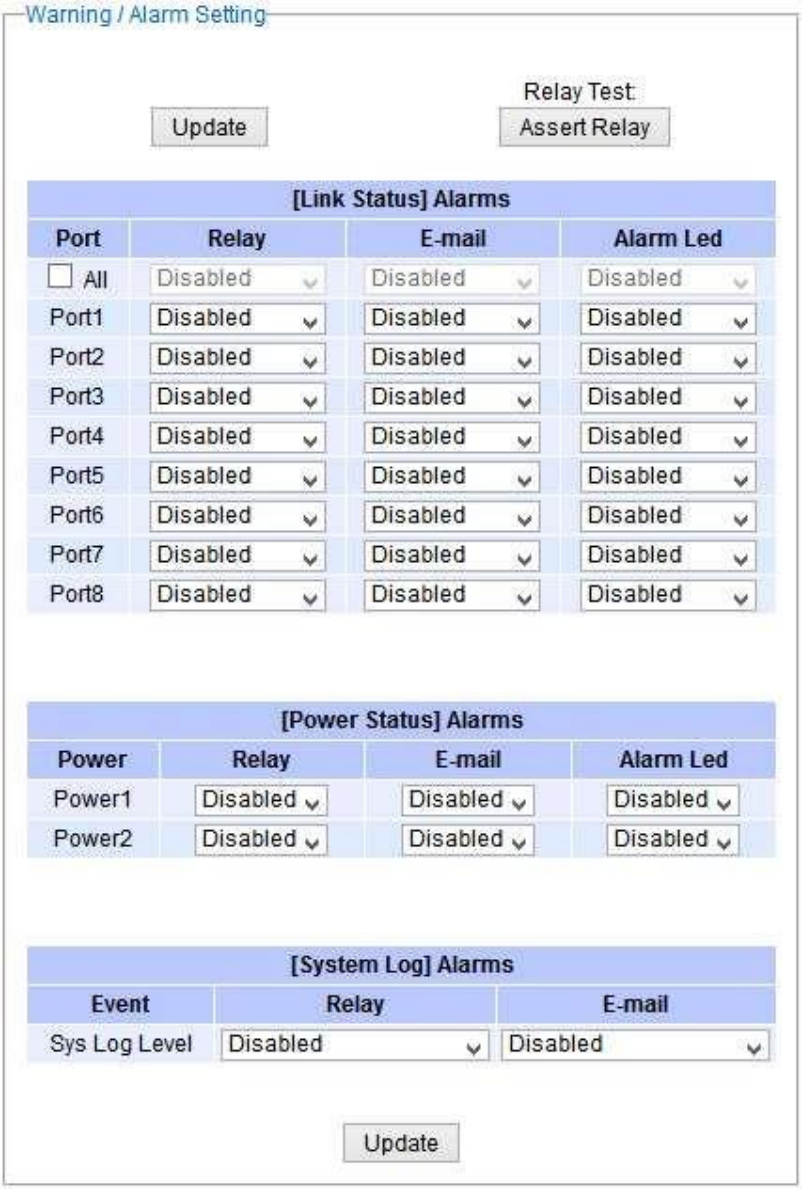


Figure 2.161 Webpage of Warning Event Selection

In Link Status Alarms, users have three conditions whether to send notifications via **Relay**, **E-mail**, or **Alarm LED** in case if Link is UP, Link is Down, or Link is UP**/**DOWN**.** Table 2**.**66 summarizes the link status alarm event selection**.** Note the users can enable the alarm events for all ports simultaneously by checking the box in front of the **All** entries**.**

Table 2.66 Descriptions of Link Status Alarm Event Selection

Label	Description	Factory Default
Port	Indicates each port number.	-
Port state event	**Disabled:** 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

In power status alarms, the users have two conditions to send notification **(**via **Relay**, **E-mail** and **Alarm LED)** which are **Power On**, or **Power Off.** Table 2**.**67 summarizes the Power Status Alarm event selection**.**

Table 2.67 Descriptions of Power Status Alarm Event Selection

Label	Description	Factory Default
Power	Indicate specific power supply	Disabled
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

In System Log Alarms, the users have can only send notification via **Relay** and **E-mail.** Table 2.68 describes the System Log Level which can be selected for the System Log Alarm event notification**.**

Table 2.68 Descriptions of System Log Alarm Event Selection

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 words, when log level is set to 0, an alarm is triggered whenever 0,

1, 2… 6, and/or 7 happens. When log level is set to 5, an alarm is triggered whenever 5, 6, and/or 7 happens.

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

2.20.2.2 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 as configured in Section 2.20.2.1, the system can send an alarm message to users by e-mail. Here, the users will be allowed to modify E-mail-related settings for sending the system alarms (Link Status, Power Status, and System Log), as shown in **Error! Reference source not found.**.

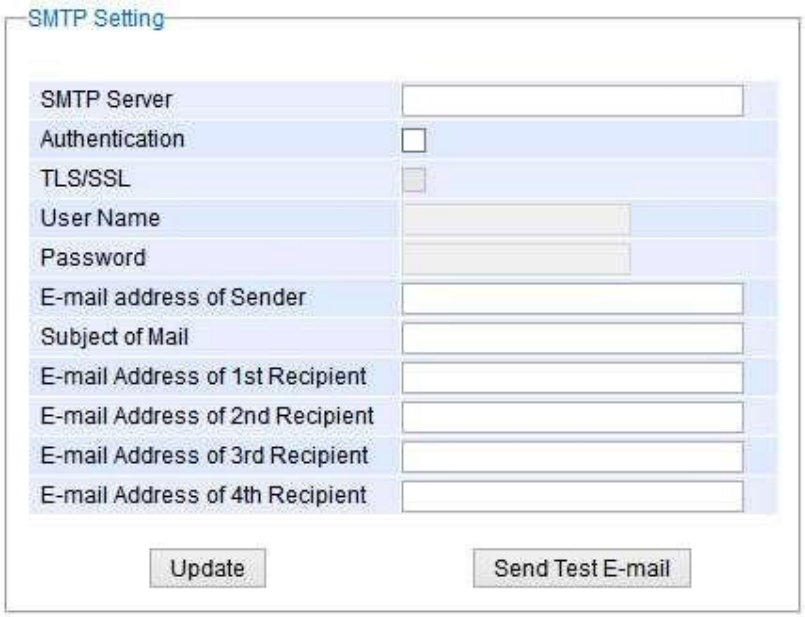


Figure 2.162 SMTP Setting Webpage

An example of SMTP Setting is shown in Figure 2.163. After entering all the necessary fields, please click on the Update button to allow the setting to take effect. Note that the users can try to send a Test E-mail according the the SMTP setting on this webpage by clicking on the **Send Test E-mail** button. The description of each SMTP Setting parameter is summarized in Table 2.69.

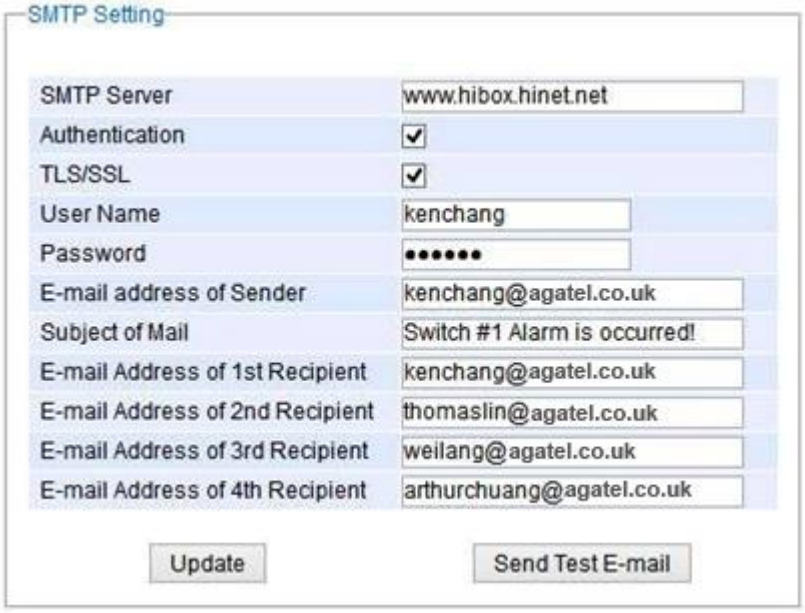


Figure 2.163 Example of SMTP Setting

Table 2.69 Descriptions of SMTP Setting

Label	Description	Factory Default
SMTP Server	Configure the IP address of an out-going e-mail server	NULL
Authentication	Enable or disable authentication login by checking on the box. If enabled, SMTP server will require authentication to login. Thus, the users will also need to setup User Name and Password to connect to the SMTP server	Disable (Unchecked)
TLS/SSL	Enable or disable Transport Layer Security (TLS) or Secure Sockets Layer (SSL) which is an encryption mechanism for communication with the SMTP Server	Disable (Unchecked)
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
E-mail Address of Sender	Configure the sender e-mail address	NULL
Mail Subject	Type the subject of this warning message. Max. 31 characters.	NULL
E-mail Address of 1st Recipient	Set the first receiver's E-mail address.	NULL
E-mail Address of 2nd Recipient	Set the second receiver's E-mail address.	NULL
E-mail Address of 3rd Recipient	Set the third receiver's E-mail address.	NULL
E-mail Address of 4th Recipient	Set the fourth receiver's E-mail address.	NULL
Update	Update these modifications on the managed switch	-
Send Test E-mail	A test email can be sent to recipient(s) above to check accuracy.	-

2.20.2.3 Log

Managed switches warns its users in case any event occurs. A table called Warning/Alarm Log in this section displays the warning events as shown in Figure 2.164 Warning/Alarm Log Webpage. At the top of the table, the users can click on the **Reset Relay** button to turn off the Relay or click on the **Clear Log** to remove all entries in the **Warning/Alarm Log** table. To obtain the latest event on the able, the users have to click on the **Refresh** button.



Figure 2.164 Warning/Alarm Log Webpage

An example of **Warning/Alarm Log** table is shown in Figure 2.165. Note that the display format and buttons is slightly different from the current XEG75XX format above. A short list of alarm messages is shown on the top portion of the web browser interface.



Figure 2.165 Example of Warning Events

Table 2.70 Descriptions of Warning / Alarm Log

Label	Description	Factory Default
Reset Relay	Sets Hardware Relay Alarm to off.	Relay is off
Clear Log	Clears all warning events that are displayed.	-
Refresh	Obtain the latest Warning / Alarm events	-
Index	Display the index of the Warning/Alarm events as an entry number over a total number of events	-
Date	The date that the alarm/event occurred.	-
Time	The time that the alarm/event occurred.	-
Startup Time	The duration of time since the start up time of the switch until the alarm/event occurred.	-
Events	Description of the alarm events	-

2.20.3 Denial of Service

Denial of Service (DoS) is a malicious attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. XEG75XX industrial managed switch is designed so that uses can filter out various types of attack as shown in Denial of Service setting webpage (Figure 2.166). The followings are some vulnerable attacks that can be prevented by the XEG75XX switch function.



Figure 2.166 Denial of Service Setting Webpage

First is the Local Area Network (LAND) DoS attack. LAND is a layer 4 DoS attack in which the attacker sets the source and destination information of a TCP segment to be the same. Specifically, TCP SYN packet is created such that the source IP and port are set to be the same as the destination address and port, which in turn is set to point to an open port on a Victim's machine. A vulnerable machine would receive such a message and reply to the destination address effectively sending the packet for reprocessing in an infinite loop. A vulnerable machine will crash and freeze due to the packet being repeatedly processed by the TCP stack. To enable/disable the protection against the Local Area Network (LAND) DoS attack, click **Enabled** box on LAND packet (SID=DID) function.

Second vulnerability attack is TCP fragmentation attacks also known as tear drop attack, which is targeting TCP/IP reassembly mechanism, preventing them from putting together fragmented data packets. As a result, the data packets overlap and quickly overwhelm the victim's servers, causing them to fail. To enable/disable the protection against the TCP fragment DoS attack, click **Enabled** box on TCP Fragment function. However, to set the mitigation method, some certain inputs are needed to set rules of filtering. For example, whether the first fragment is allowed or not and the minimum TCP header size that is allowed. In some datalink protocols such as Ethernet, only the first fragment contains the full upper layer header, meaning that other fragments look like beheaded datagrams. No additional overhead imposed over network because all fragments contains their own IP header. Only the first fragment contains the ICMP header and all remaining fragments are generated without the ICMP header.

The third vulnerability is called TCP flag DoS attack. The attack sends out TCP packets with flag indicating that they are ACK packets. This attack is similar to SYN flood except SYN flood also open a connection with the server. Although the devices are mostly tuned for more common attack as SYN flood. TCP flag DOS attack will force the server to keep dropping the packets, causing resource exhaustion. To enable/disable the protection against the TCP Flag DoS attack or called ACK flood, click **Enabled** box on TCP Flag function.

The fourth vulnerability is called L4 port DoS attack. There are various types of L4 port DoS attack. In UDP attack, a large number of UDP packets are sent to victim until it is overloaded. UDP-Lag attacks in bursts as to not hit the target offline completely. SUDP attack is the same as UDP but spoofs the request to make it harder to mitigate. SYN/SSYN/ESSYM attacks are abuse the hand shake of the TCP protocol until the victim is overloaded. DNS/NTP/CHARGEN/SNMP attacks are an amplified UDP attack that abuses vulnerable server by sending a spoofed request with the targets IP as the sender. The servers then send the target the information overloading the system. To enable/disable the protection against all these L4 Port DoS attacks, click **Enabled** box on L4 Port function.

Last vulnerability is so called ICMP fragmentation attack. The attack involves the transmission of fraudulent ICMP packets that are larger than the network's MTU. In this switch, administrators can filter these packets out by enabling ICMP function and set **Maximum ICMP size** range from 512 to 1023 bytes. As these ICMP packets are fake, and are unable to be reassembled, the target server's resources are quickly consumed, resulting in server unavailability. To enable/disable the protection against the ICMP DoS attack, click **Enabled** box on ICMP function. Table 2.71 provides descriptions of the Denial of Service Setting.

Table 2.71 Descriptions of Denial of Service Setting

Label	Description	Factory Default
LAND packets	**Enabled:** Enabled prevention over the attack using TCP SYN packet that has the same source and destination's IP and port.	Disabled
TCP Fragment	**Enabled:** Enabled prevention over the TCP fragmentation attack which is targeting TCP/IP reassembly mechanism	Disabled
TCP Flag	**Enabled:** Enabled prevention over the TCP flag DOS attack which force the server to keep dropping the packets, causing resource exhaustion.	Disabled
L4 Port	**Enabled:** Enabled prevention over various types of L4 port DoS attacks that are intended to overload the server.	Disabled
ICMP	**Enabled:** Allow filtering ICMP that has packet size higher than the maximum ICMP size defined in the next field	Disabled
Max ICMP Size	512 to 1023 bytes	512

2.20.4 Backup/Restore Config.

In **Backup/ Restore Config** function, the current configuration of the XEG75XX/XE75XX industrial managed switch can be downloaded to a local computer and saved it as a backup. Additionally, the users can restore a previously backup configuration from a local computer to the XEG75XX/XE75XX industrial managed switch. It will replace the current configuration. These backup and restore function can be done through two different protocols: **HTTP** or **TFTP**. Figure 2.167 depicts the **Backup/Restore Configuration** dropdown menu.

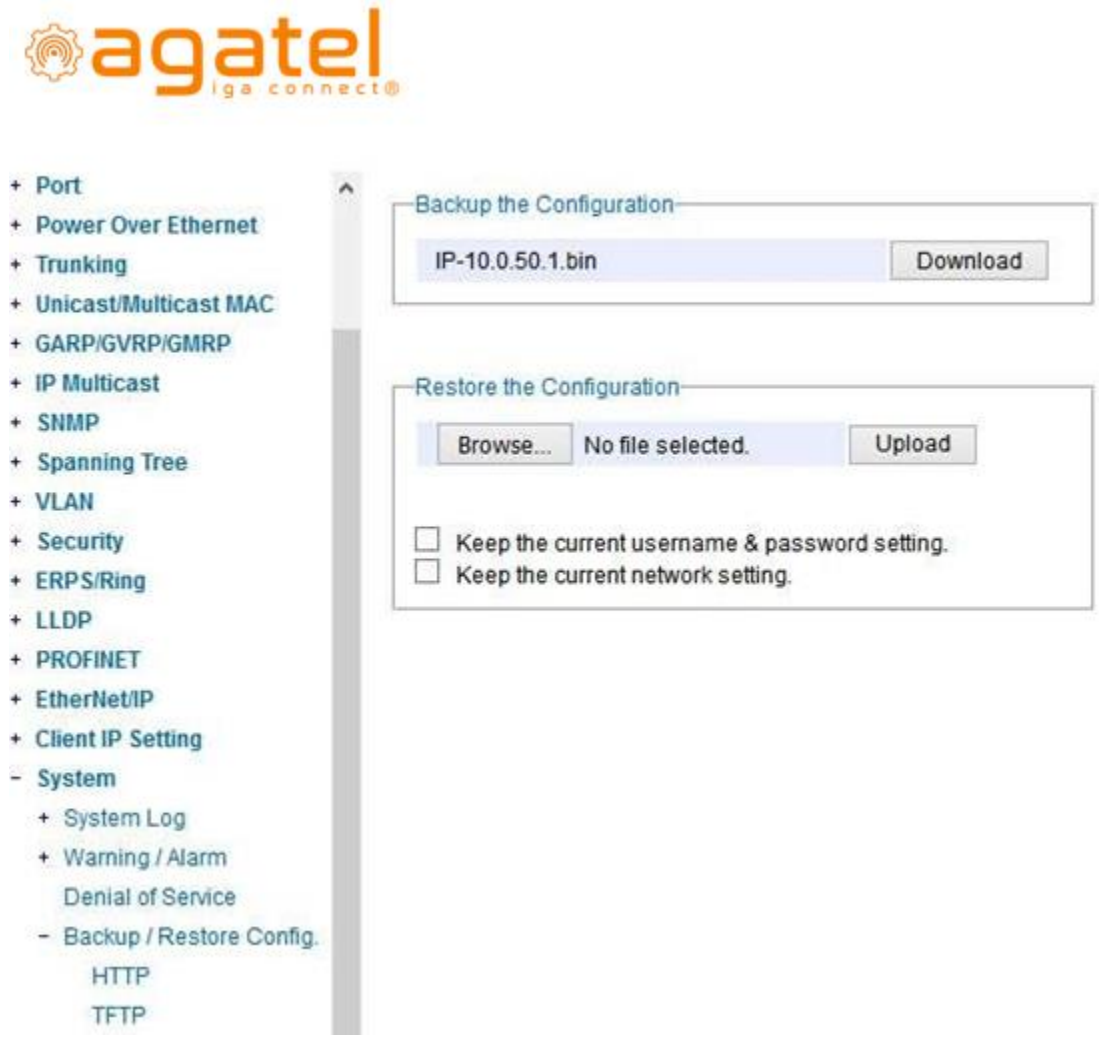


Figure 2.167 Backup/Restore Config. Dropdown Menu

2.20.4.1 Backup/Restore Config. Via HTTP

Figure 2.168 shows the webpage for Backup/Restore the configuration via HTTP. It is divided into two parts: **Backup the Configuration** and **Restore the Configuration**. When clicking on the **Download** button on the upper part of the page (**Backup the Configuration**), the users will be prompt to **Opening** the file name IP-10.0.50.1.bin by an application or to **Save File** to a destination. Choosing to Save Filewill back up the switch's current configuration to your local drive on the local computer.

To restore a configuration file to the switch, please move down to the **Restore the Configuration** part, then click the **Browse…** button to choose a configuration file from the local drive. Before clicking the **Upload** button, the users can check any of the options below the upload file which are to **Keep the current username & password setting** and to **Key the current network setting**. This will help prevent the users from the necessity to logging-in using a previously stored username, password or network configuration after settings are restored.



Figure 2.168 Backup/Restore Configuration via HTTP

2.20.4.2 Backup/Restore Config. Via TFTP

Trivial File Transfer Protocol (TFTP) is designed to be small and easy to implement. The users are allowed to upload configuration settings to a TFTP server as a backup copy, and download these settings from a TFTP server when necessary to restore or replace the configuration of the XEG75XX/XE75XX industrial managed switch. Figure 2.169 shows the TFTP webpage which is divided into three parts: **Download the Configuration from TFTP**, **Upload the Configuration to TFTP**, and**DHCP Option 66/67 Setting**. Table 2.72 summarizes the descriptions of TFTP Setting.

- To download a configuration file from a TFTP server, the user need to specify the IP address of the TFTP server and the Remote File Name. Then, click the **Download** button.

- To upload a configuration file from a TFTP server, the users need to specify the IP address of

the TFTP server and the Desired File Name. Then, click the **Upload** button.

- The last part of the TFTP page is the DHCP Option 66/67 Setting. This feature enables the managed switch to learn of the TFTP Server Name, which is a data in DHCP IPv4 packet Option 66 (RFC2132), and Filename, which is a data in DHCP IPv4 packet Option 67 (RFC2132). Checking the **Enabled** box and then click on the **Update** button to set this feature.

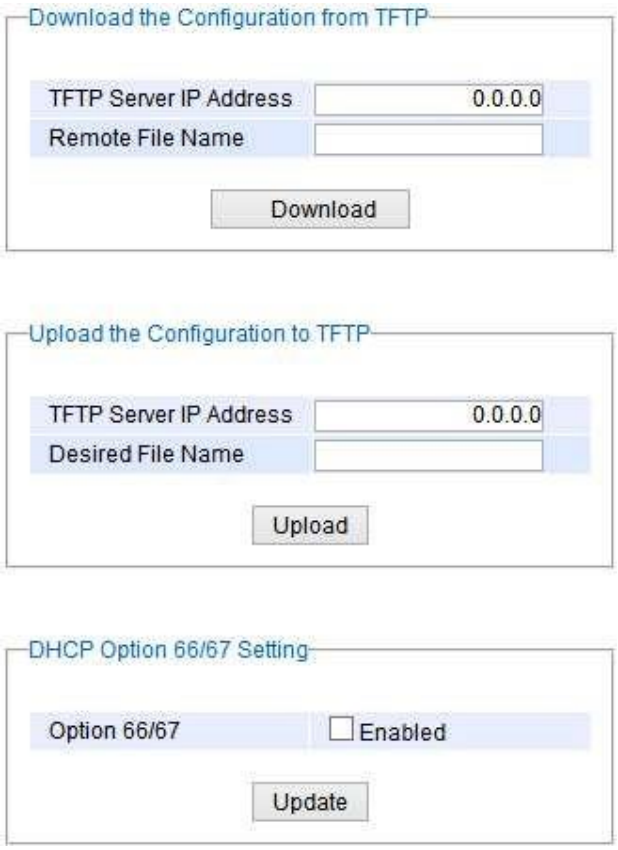


Figure 2.169 Backup/Restore Configuration via TFTP

Table 2.72 Descriptions of TFTP Settings

Label	Description	Factory Default
TFTP Server IP Address	Sets the IP address of the remote TFTP server domain name.	NULL
Remote File Name	Type in name of the file to be downloaded.	NULL
Download	Click to start download remote configuration into the Switch.	-
Desired File Name	Type in name of the file to be uploaded.	NULL
Upload	Click to start upload Switch configuration to the remote TFTP server.	-
Option 66/67	Enable this option to allow the managed switch to learn of TFTP Server Name and the filename to be used from a DHCP packet	Disable
Update	Update the setting of DHCP Option 66/67 setting	-

2.20.5 Firmware Update

The users can update the device firmware via web interface as shown in Figure 2.170. To update the firmware, the users can download a new firmware from Agatel's website and save it in a local computer. Then, the users can click **Browse…** button and choose the firmware file that is already downloaded. The switch's firmware typically has a ".dld" extension such as XEG750X-K150A150.dld. After that, the users can click **Update** button and wait for the update process to be done. Alternatively, the firmware update can also be performed using the Device Management Utility discussed in Chapter 5.

Note: please make sure that the switch is plug-in all the time during the firmware upgrade.



Figure 2.170 Firmware Update Webpage

2.20.6 Factory Default Setting

When the managed switch is not working properly, the users can reset it back to the original factory default settings by clicking on the **Reset** button as shown in Figure 2.171.



Figure 2.171 Factory Default Setting Webpage

2.20.7 Reboot

An easy reboot function is provided in this webpage requiring only one single click on the **Reboot** button as shown in Figure 2.172.



Figure 2.172 Reboot Webpage

3 Configuring with a Serial Console

A managed switch can also be configured by using a serial console. Note that a special serial console cable is required to connect to the console port on top of the XEG75XX's chassis. Please contact Agatel Technologies to obtain the cable, is needed. 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.



Figure 3.1 Setting of New Connection in Tera Term Program

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

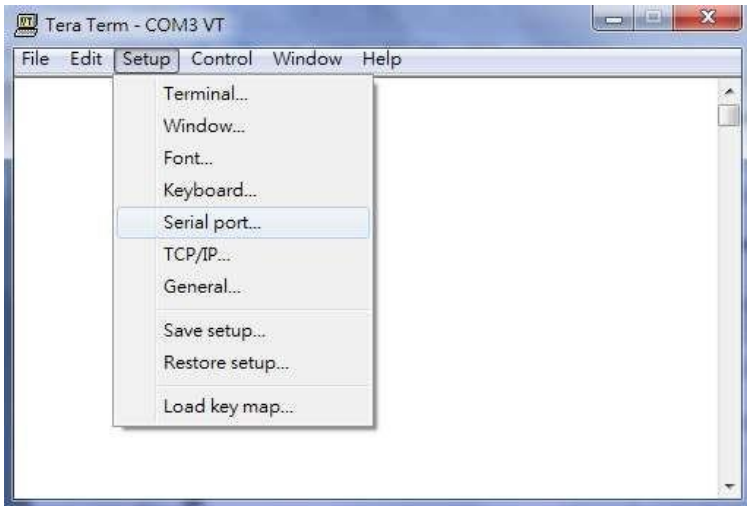


Figure 3.2 Setup Menu

3. The **Serial Port Setup** window pops up. Select an appropriate port for **Port**, **115200** for **Baud Rate**, **8 bit** for **Data**, **none** for **Parity**, and **1 bit** for **Stop**, as shown in Fig.3.3.

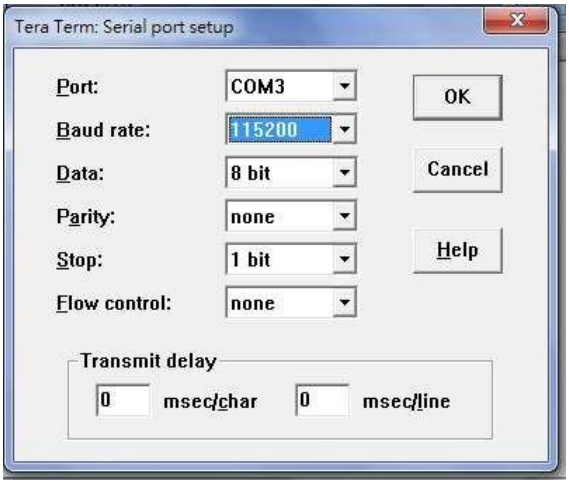


Figure 3.3 Setting for the Serial Port

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 for passwords, but a user may be assigned with a password for both the operator and manager privileges. If passwords are assigned, then when the user attempts to enter CLI on the next time, they will need to enter the correct username and password.

If a user enters the password for the operator, then the prompt changes to indicate operator privilege. User is now in the "user" mode:

Switch>

If a user enters the password for the manager, then the prompt changes to indicate manager privilege. User is now in the "privileged" mode:

Switch#

If a user is in the user mode and wants to switch to the privileged mode, he/she may simply type in the command "**enable**" and then enter the correct username and password after 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)#

An illustration of the modes, related privileges and screen prompt is shown in Figure 3.4.

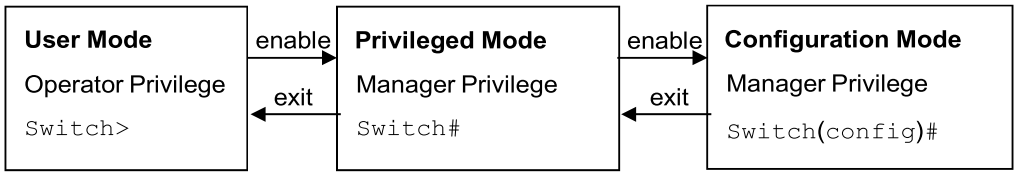


Figure 3.4 Modes, privileges and promts

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 Commands

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

Table 3.1 Command Descriptions

Commands	Descriptions
Enable	Turn on privileged mode
Disable	Turn off privileged mode
Configure	Enter configuration mode
?	List all available option.
Exit	Go back to the 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 commands.
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's username and password are also used by the web user interface (web browser method of configuration).

3.4 Command Example

The serial console is another method to add/delete/change configuration, same as 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** using serial console method, which are shown in the following sub-sections, are the same as what are explained in Chapter 2. The only difference is that the web browser method is used in Chapter 2.



Figure 3.5 Example of Commands

3.4.1 Administration Setup using Serial Console

This section shows how users can find the administrative information and make changes using commands. Detailed explanations of each technical term can be found in Chapter 2 of this manual.

Table 3.2 Descriptions of Administrative Commands for Setting Up

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 the next boot time.
Show arp	Show the IP ARP translation table
Ping ip-addr <1~999>	Send ICMP Echo-Request to the 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 commands.

Detailed explanations of each technical term can be found in Chapter 2 of this manual.

Table 3.3 Descriptions of Commands for Setting up Spanning Tree

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 20 seconds.
Spanning-tree hello-time<1~10>	Set hello time in seconds
Spanning-tree maximum-age<6~40>	Set the maximum age of the spanning tree in seconds
Spanning-tree priority<0~61440>	Set priority of the spanning tree bridge
Spanning-tree port path-cost <0 ~ 2E8><port #>	Set path cost for a specific port
Spanning-tree port priority <0 ~ 240><port #>	Set priority to a specific port
Show spanning-tree	Show spanning-tree information
Show spanning-tree port <port #>	Show port information
[no] spanning-tree debug	Enable or disable debugging of the spanning tree
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: Specify point to point link auto detection. True: Set the point to point link to true. False: Set the link to false.

4 Configuring with a Telnet Console

An alternative configuration method is the Telnet method and it is described in this chapter.

4.1 Telnet

Telnet is a remote terminal software to login to any remote telnet servers. It is typically installed in most of the operating systems. In order to use it, users open a command line terminal (e.g., cmd.exe for Windows Operating System).

4.2 Telnet Log-in

After the command line terminal is opened, type in “telnet 10.0.50.1” as shown in Figure 4.1. Note that telnet command needs to follow by IP address or domain name. In this example, the default IP address is 10.0.50.1. If users change the switch IP address, the IP address to log-in should be changed to match the new switch IP address.

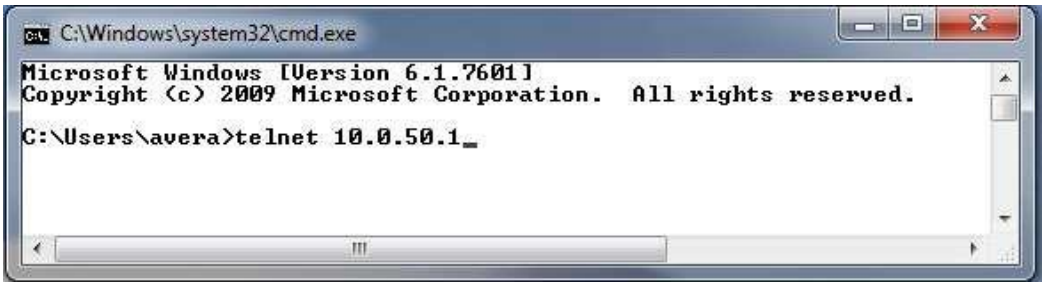


Figure 4.1 Telnet Command

4.3 Command Line Interface for Telnet

After input the telnet command line, the switch's interface is displayed as shown in Figure 4.2.

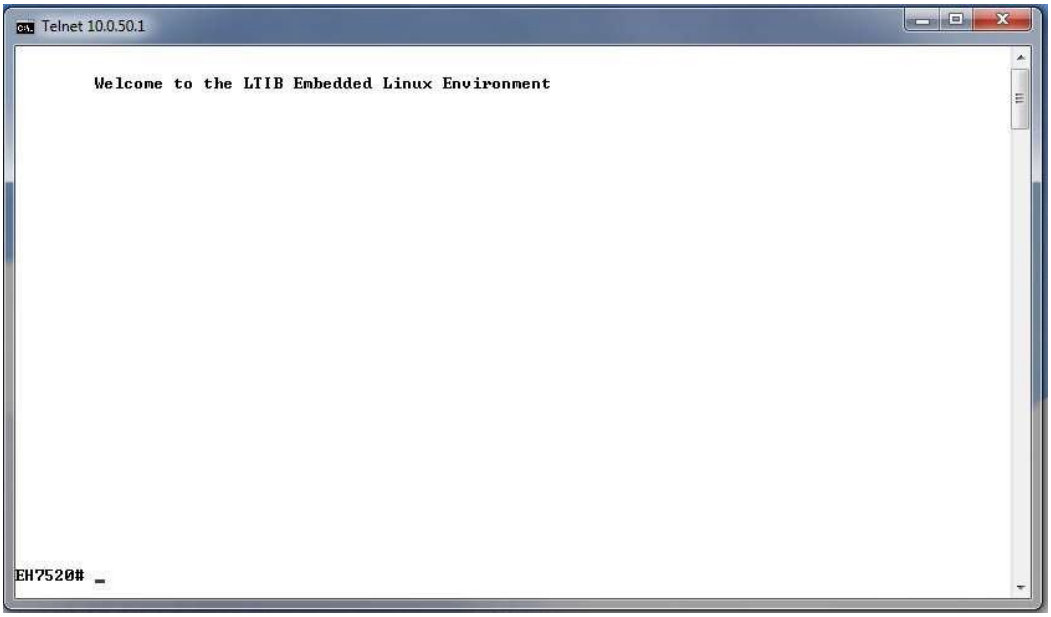


Figure 4.2 Log-in Screen using Telnet

Users will see the welcome screen to the switch interface. It is important to note that there is no password protection to the default telnet log-in method. From Chapter 3, configuring through telnet is similar to configuring through the serial console. Users are automatically logged into the privileged mode. The configuration commands are also similar to the serial console methods. (Please refer to Chapter 3 for more information on configuration.)

4.4 Commands in the Privileged Mode

When users do not know the commands to use for the command line configuration, users type in "?" and the commands are displayed on screen as shown in Figure 4.3.

```
XE7520#
  configure   Configuration
  disable     Turn off privileged mode command
  exit        Exit current mode and down to previous mode
  help        Description of the interactive help system
  history     Set the number of history commands
  logout      Log out of the system
  no          Negate a command or set its defaults
  show        Show running system information
XE7520#
```

Figure 4.3 Commands in the Privileged Mode

4.5 Commands in the Configuration Mode

When users type in “?” in configuration mode, a long list of commands is displayed on screen as shown in Figure 4.4.

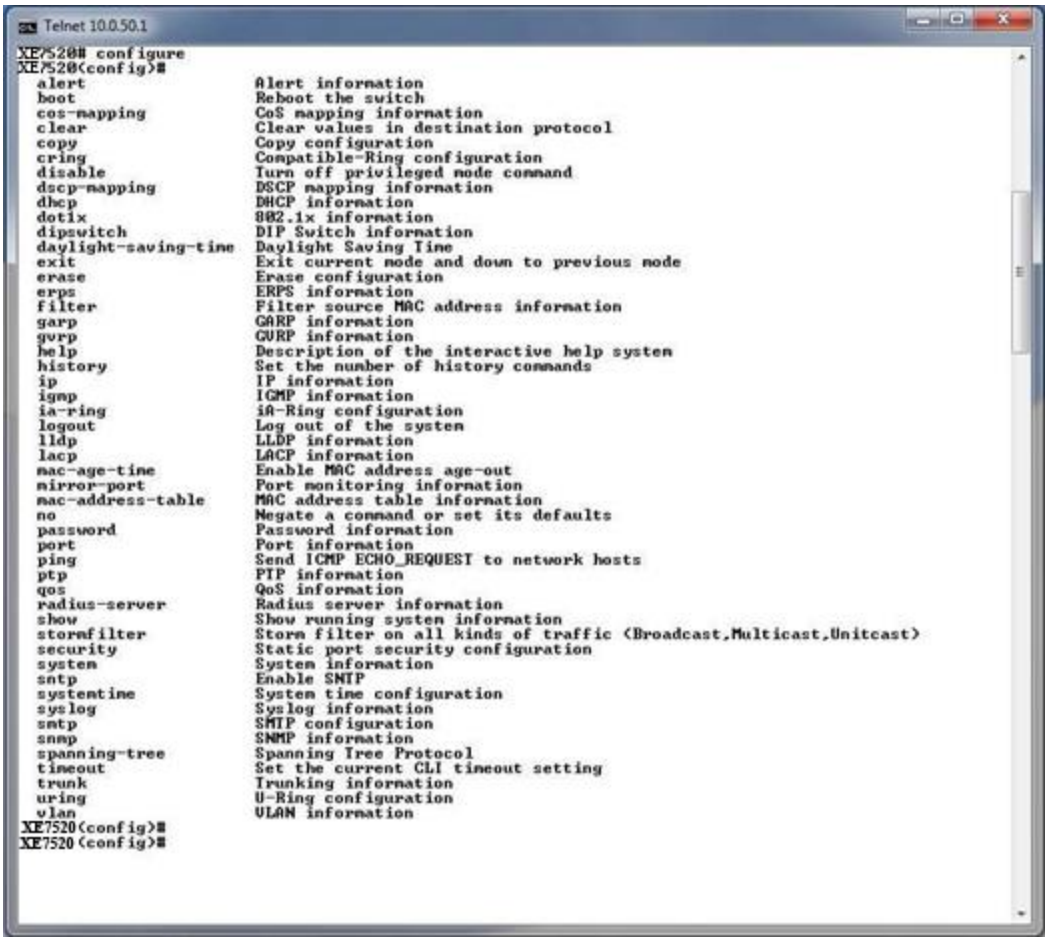


Figure 4.4 Commands in the Configuration Mode

Table 4.1 shows all commands that can be used to configure the switch in the configuration mode.

Table 4.1 Commands in the Configuration Mode

Commands	Descriptions
alert	Alert information
boot	Reboot the switch
cos-mapping	CoS mapping information
clear	Clear values in the destination protocol
copy	Copy configuration
cring	Compatible-Ring configuration
disable	Turn off the privileged mode command
dscp-mapping	DSCP mapping information
dhcp	DHCP information
dot1x	802.1x information
dipswitch	DIP Switch information
daylight-saving-time	Daylight Saving Time
exit	Exit the current mode and move to the previous mode

erase	Erase the configuration
erps	ERPS information
filter	Filter the information of the source MAC address
garp	GARP information
gvrp	GVRP information
help	Description of the interactive help system
history	Set the number of history commands
ip	IP information
igmp	IGMP information
ia-ring	iA-Ring configuration
logout	Log out of the system
lldp	LLDP information
lacp	LACP information
mac-age-time	Enable age-out time for the MAC address
mirror-port	The monitoring information of a Port
mac-address-table	Information of the MAC address table
no	Negate a command or set to its defaults
password	Password information
port	Port information
ping	Send ICMP ECHO_REQUEST to network hosts
ptp	PTP information
qos	QoS information
radius-server	Radius server information
show	Show information of the current running system
stormfilter	Storm filter on all kinds of traffic (Broadcast,Multicast,Unitcast)
security	Security configuration of a static port
system	System information
sntp	Enable SNTP
systemtime	Configuration of the system time
syslog	Syslog information
smtp	SMTP configuration
snmp	SNMP information
spanning-tree	Spanning Tree Protocol
timeout	Set the current CLI timeout
trunk	Trunking information
uring	U-Ring configuration
vlan	VLAN information

Note: Please see Chapter 3 for the details of switch configuration.

5 Device Management Utility

Agatel also provides a software utility called **Device Management Utility** to assist the users in configuring the product. The Device Management Utility was formerly called Device View or Serial Manager. The latest Device Management Utility is version 5.20. This chapter will describe how to use the Device Management Utility with the XEG75XX industrial managed switch. After installing the utility software on your PC. Please click on the Device Management Utility's icon to start the program. Figure 5.1 illustrates the GUI of the Device Management Utility.



Figure 5.1 Device Management Utility

If the managed switch is on the same subnet as the PC that runs the Device Management Utility, the users should be able to find the switch on the list of the device as shown in Figure 5.1. If for some reason, it cannot be found, the user can click the first icon called **Rescan** on the icon bar to search for the device connected to the same subnet as the Device Management Utility. Depicts the Search icon.



Figure 5.2 Rescan (Search) Icon

To perform any task on the desired device, please click to select the entry of that particular device on the list inside the window of Device Management Utility. Typically, when the users double-click the entry, the Device Management Utility will connect to the switch and perform a login process.

It is strongly recommended the users to setup the administration password for the managed switch for network security purpose. If no administration password is set, the Device Management Utility will be able to login to and change any configuration on the device.

If the **Local Login Setting** was configured in Section 2.3.1, a login dialog will pop-up as shown in when the Device Management Utility try to select the **Config by Browser** menu under the **Configuration** pulldown menu or click on the fourth icon on the icon bar. The users then can enter the **User Name** and **Password** to verify the identity. Note that the User Name is typically set to "admin" for convenient.

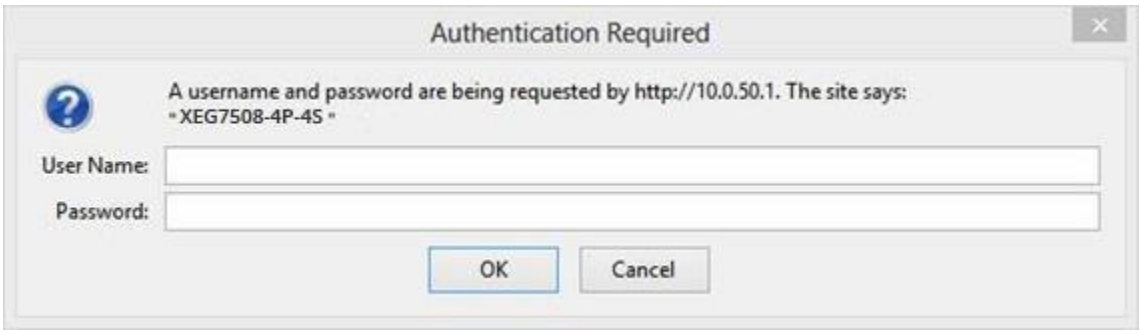


Figure 5.3 Authentiction to Login to XEG75XX switch

5.1 Network Setting

While the device is selected, the user can configure the network parameters by clicking on the Network icon, the second icon on the icon bar as depicted in Figure 5.4. Alternatively, the users can click on the pulldown menu **Configuration** and select **Network…** menu.



Figure 5.4 Network Configure Icon

The **Network Setting** dialog window will pop-up as shown in Figure 5.5. The users can enable the DHCP options by checking the box in front of **DHCP (Obtain an IP automatically)** option. This will allow the device to get its new IP address and other network parameters from a DHCP server from the network. Alternatively, the users can manually set the **IP address**, **Subnet mask**, **Gateway**, and **Host name**.

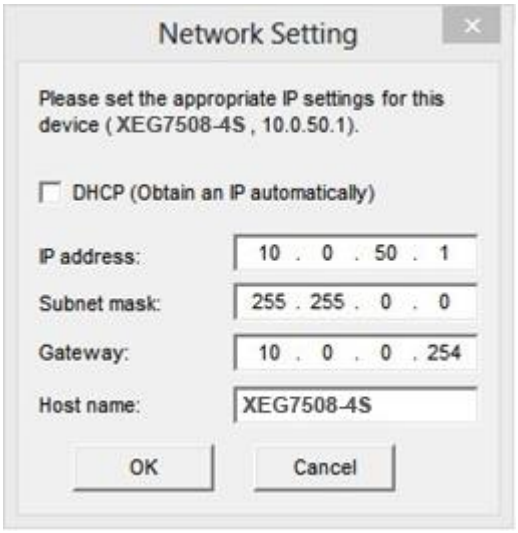


Figure 5.5 Network Setting Dialog

After clicking on the **OK** button, another dialog window will pop-up to ask for authorization in modification of this managed switch. The users are required to enter the correct **Password**. Note that the **User**

Name is default as admin which cannot be changed. Then, click the **Authorize** button to allow the change of the network parameter.



Figure 5.6 Administration Verification before Changing the Network Setting

A warning dialog will pop-up as shown in Figure 5.7 to inform the users that the device will restart after the network configuration was changed. Note that if the configurations were not changed, it may be because of the wrong user name, password, or IP configuration. The users should check these password setting or network setting of the product.



Figure 5.7 Warning Dialog before the Device Restart

If the IP address was change, the users may need to search for the device again using the **Rescan** icon or the first icon on the icon bar.

5.2 Topology Diagram

Device management Utility comes with a visualization tool called **Topology Diagram** to automatically draw a network diagram. The users can select the **Topology Diagram** menu under the **Configuration** pulldown menu to start the visualization tool as shown in Figure 5.8. The current version of the Topology Diagram is 1.4.0. Note that the tools can display the device discovered by the Device Management

Utility and draw a connection between devices in the network that can be reached by the Device Management Utility. Note that to be able to use the Topology Diagram, the switch's LLDP feature in Section 2.16.1 must be enabled.

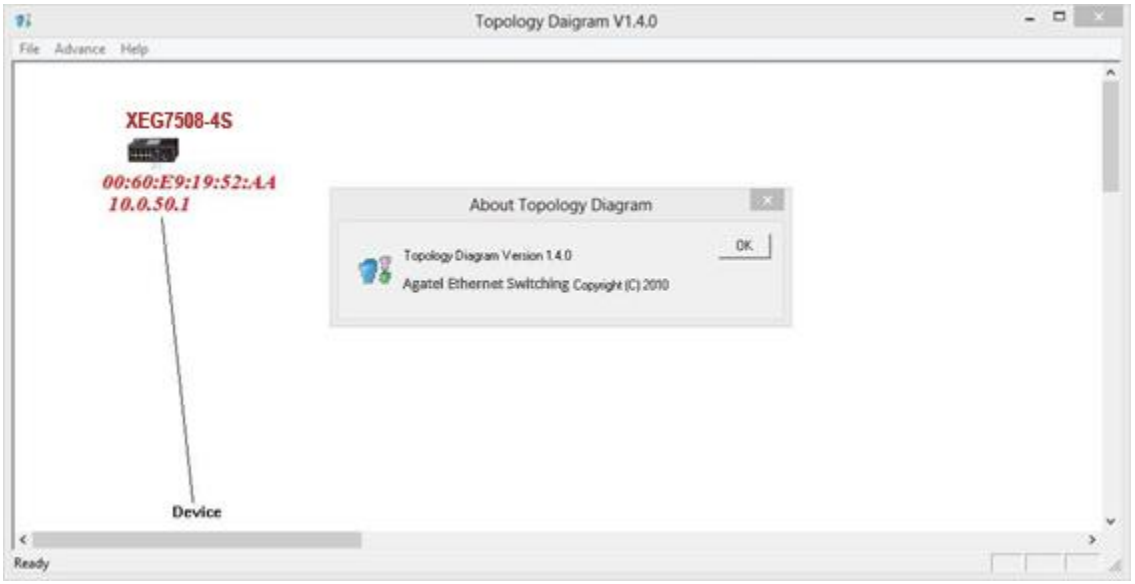


Figure 5.8 Topology Diagram

Additional information can also be display on the diagram which are the **Port** number and the **MAC address** of the device that is currently connecting to the XEG75XX switch. Please select **Show Information** menu under the **File** pulldown menu. Figure 5.9 shows the result of additional information.

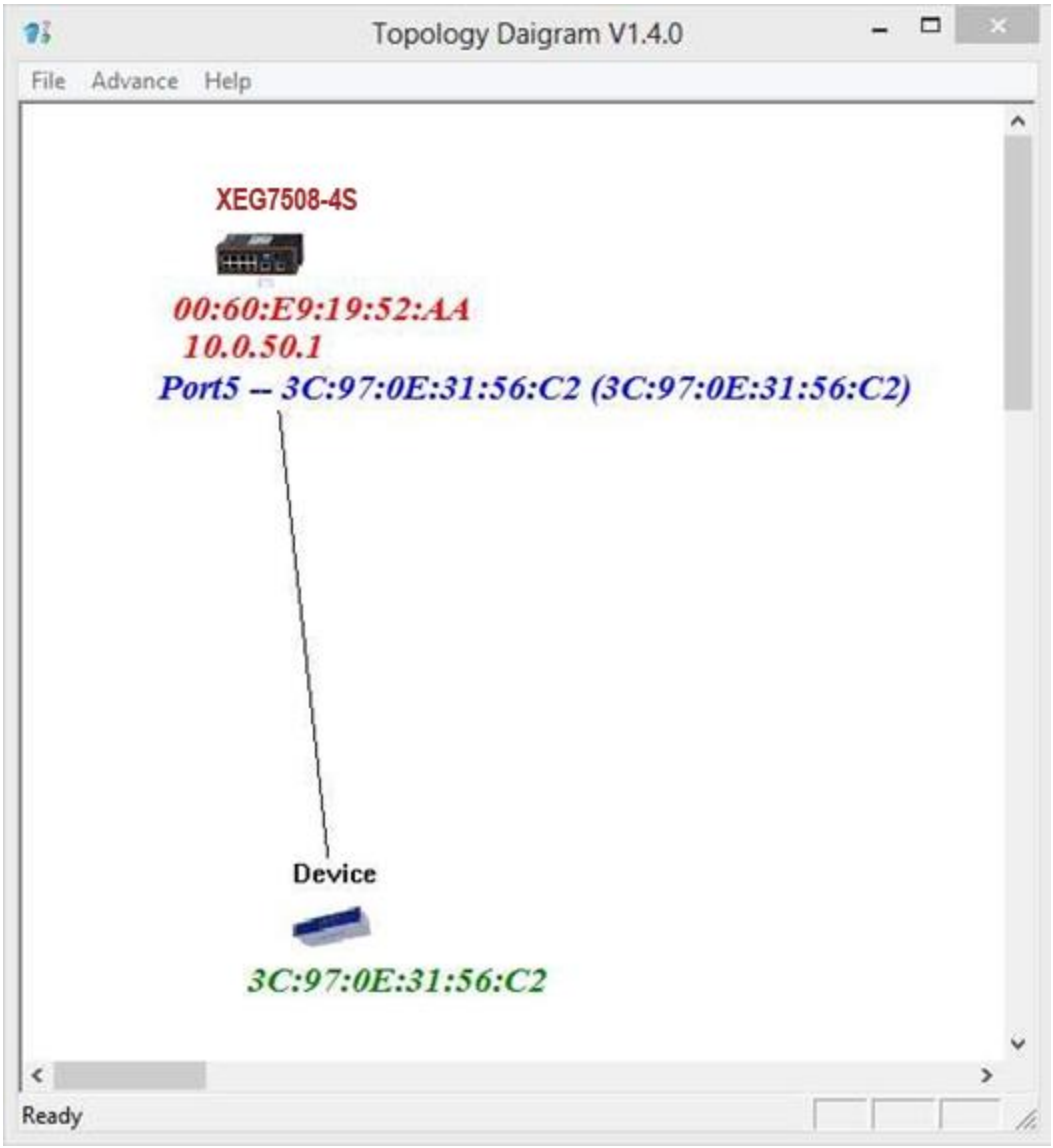


Figure 5.9 Show Information on Topology Diagram

Note that the Topology Diagram can be used to check the Ring Topology. The user can select the **RingCheck** menu from the **Advance** pulldown menu.

5.3 Firmware Update

The Device Management Utility can be used to update firmware of the switch. To perform this task, the users can click on the fifth icon on the icon bar as shown in Figure 5.10. Alternatively, the **Firmware Download…** menu under the **Firmware** pulldown menu can also perform this task.



Figure 5.10 Upgrade from Disk (Firmware Update) Icon

Figure 5.11 shows the dialog for Download Firmware from Disk. The window displays the current version of the firmware on the switch and provides the option to download either Kernel firmware or AP firmware to the switch. The users can choose a new and valid firmware (.dld extension) from the local PC and then clicking on the **Upgrade** button to perform the update.

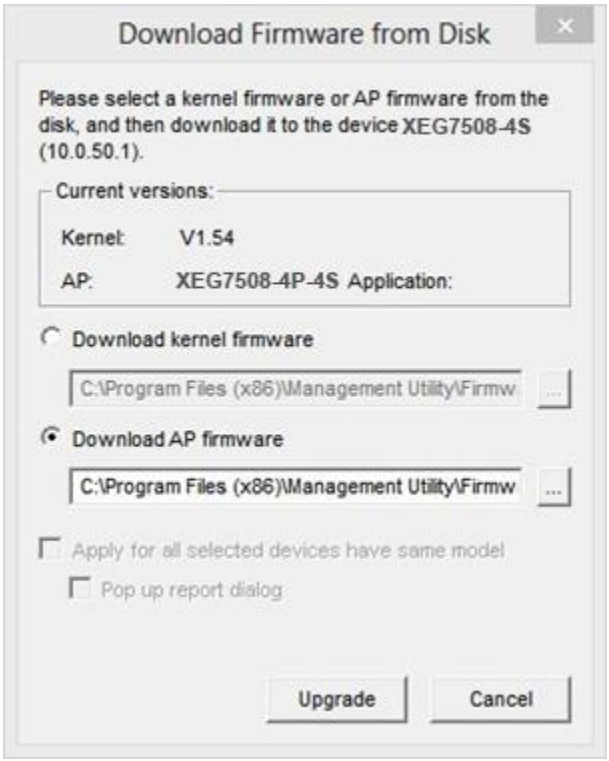


Figure 5.11 Dialog Window for Download Firmware from Disk

Appendix A: Glossary

Term	Description
802.1	A working group of IEEE standards dealing with Local Area Network.
802.1p	Provide mechanism for implementing Quality of Service (QoS) at the Media Access Control Level (MAC).
802.1x	IEEE standard for port-based Network-Access Control. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN
Broadcast	Broadcast packets to all stations of a local network.
Client	Device that use services provided by other participants in the network.
DES	**D**ata **E**ncryption **S**tandard is 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 is a hierarchical naming system built for any computers or resources connected to the Internet. It maps domain names into the numerical identifiers. For example, the domain name www.google.com is translated into the address 74.125.153.104.
EAP	**E**xtensible **A**uthentication **P**rotocol is an authentication framework widely used by IEEE.
Ethernet	In star-formed physical transport medium, all stations can send data simultaneously. Collisions are detected and corrected through network protocols.
Gateway	Provide access to other network components on the OSI layer model. Packets which are not going to a local partner are sent to the gateway. The gateway takes care of communication with the remote network.
IEEE	Institute of Electrical and Electronics Engineers
IGMP	**I**nternet **G**roup **M**anagement **P**rotocol is used on IPv4 networks for establishing multicast group memberships.
IP	Internet Protocol
IPv4	**I**nternet **P**rotocol **v**ersion **4** is the 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 became scarce resource. This has stimulated the development of IPv6, which is still in its early stage of development.
LAN	Local Area Network is the network that connects devices in a limited geographical area such as company or computer lab.
MAC	Media Access Control is 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 a network segment. It is formed according to the rules of numbering name space managed by IEEE.
MD5	Message-Digest algorithm 5 is a widely used cryptographic which has a 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 is 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 is an 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**ransfer **P**rotocol (**SMTP**) is 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**.**

Appendix B: Modbus 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 XE7510"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 = 0x01Word 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 = 0x01Word 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



Agatel Ltd:

1st Floor, Apex House
Calthorpe Road, Edgbaston
Birmingham B15 1TR
United Kingdom

Tel: +44 121 809 8855
E-mail: info@agatel.co.uk
Website: www.agatel.co.uk