Atop Technologies, Inc.

Industrial Lite-Managed Booster Switch

User Manual

V1.2

January 3th, 2024

Series covered by this manual:
EHG65XX

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

This PDF Document contains internal hyperlinks for ease of navigation.
For example, click on any item listed in the **Table of Contents** to go to that page.

Published by:

Atop Technologies, Inc.

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Chupei City, Hsinchu County
Taiwan, R.O.C.

Tel: +886-3-550-8137
Fax: +886-3-550-8131
www.atoponline.com

Important Announcement

The information contained in this document is the property of Atop Technologies, Inc., and is supplied for the sole purpose of operation and maintenance of Atop Technologies, Inc., products.

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

Offenders will be held liable for damages and prosecution.

All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Disclaimer

We have checked the contents of this manual for agreement with the hardware and the software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual is reviewed regularly and any necessary corrections will be included in subsequent editions. Suggestions for improvement are welcome. All other product's names referenced herein are registered trademarks of their respective companies.

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.atoponline.com .

Warranty Period

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

Documentation Control

Author:	Shawn Wui
Revision:	1.2
Revision History:	New features
Creation Date:	21 February 2021
Last Revision Date:	03 January 2024
Product Reference:	Layer-2 Lite Managed Switch
Document Status:	Released

Table of Contents

1 Introduction....9

1.1 Introduction to Industrial Managed Switch....9
1.2 Software Features....10

2 Configuring with a Web Browser....11

2.1 Web-based Management Basics....11
2.1.1 Default Factory Settings....11
2.1.2 Login Process and Main Window Interface....12
2.2 System Info....16
2.2.1 System Info....16
2.2.2 System Setting....17
2.3 Administration....17
2.3.1 Account....18
2.3.2 Connection....19
2.3.3 IP Setting....19
2.3.4 Ping....21
2.3.5 Mirror Port....21
2.3.6 System Time....21
2.3.7 Modbus Setting....23
2.3.8 HTTPS....25
2.3.9 Auth Server Setting....26
2.4 Forwarding....27
2.4.1 QoS....27
2.4.2 Rate Control....31
2.4.3 Storm Control....33
2.5 Port....34
2.5.1 Port Setting....34
2.5.2 Port Status....35
2.6 VLAN....36
2.6.1 VLAN Setting....37
2.6.2 802.1Q VLAN....37
2.6.3 Port-Based VLAN....41
2.7 Power over Ethernet....41
2.7.1 PoE Schedule Profile....42
2.7.2 PoE Schedule....42
2.7.3 PoE Status....43
2.8 Trunking....44
2.8.1 Trunking Setting....44
2.9 Spanning Tree....46
2.9.1 Spanning Tree Setting....46
2.9.2 Bridge Info....48
2.9.3 Port Setting....49
2.10 Security....52
2.10.1 Port Security....52
2.10.2 802.1X....53

2.10.3 ACL 58
2.11 LLDP 59
2.11.1 Setting..60
2.11.2 Neighbors 60
2.12 SNMP..61
2.12.1 SNMP Agent 62
2.12.2 SNMP V1/V2c Community Setting..63
2.12.3 Trap Setting 64
2.12.4 SNMP V3 Auth. Setting..65
2.13 System..66
2.13.1 System Log..66
2.13.2 Warning/Alarm..67
2.13.3 Backup / Restore Config. 72
2.13.4 Firmware Update..72
2.13.5 Factoty Default Setting..73
2.13.6 Reboot 73
2.13.7 Logout 73
3 Configuring with Telnet..74
3.1 Telnet 74
3.2 Telnet Log-in 74
3.3 Command Line for Telnet..74
4 Glossary 87

Table of Figures

Figure 2.1 IP Address for Web-based Setting 12
Figure 2.2 Example of Google's Chrome web brower invalid certificate authority 12
Figure 2.3 A hyperlink to proceed to the managed switch at IP address 10.0.50.1 13
Figure 2.4 Login page 13
Figure 2.5 Login timeout error notification 14
Figure 2.6 Example of error notification on blocked account 14
Figure 2.7 Notification on recording of unauthorized login 15
Figure 2.8 Default Web Interface 15
Figure 2.9 System Information Dropdown Menu 16
Figure 2.10 Details of System Info Webpage under the System Info Mainmenu.. 16
Figure 2.11 Details of System Setting Webpage 17
Figure 2.12 Administration Dropdown Menu 18
Figure 2.13 Account Setting Webpage 19
Figure 2.14 Connection Management Webpage 19
Figure 2.15 IP Setting under IP Setting Webpage 20
Figure 2.16 IP Interface Part under IP Setting Webpage 20
Figure 2.17 Webpage for Ping 21

Figure 2.18 Mirror Port Webpage 21
Figure 2.19 Webpage for Setting System Time and SNTP 22
Figure 2.20 Webpage for Setting the Modbus Address 23
Figure 2.21 HTTPS Setting Webpage 26
Figure 2.22 Authentication Server Setting 26
Figure 2.23 Forwarding Dropdown Menu 27
Figure 2.24 QoS Dropdown Menu 28
Figure 2.25 QoS Setting Webpage 29
Figure 2.26 Mapping Table of CoS Webpage 30
Figure 2.27 Mapping Table of DSCP and ECN Webpage 31
Figure 2.28 Rate Control Webpage 32
Figure 2.29 Storm Control Webpage 33
Figure 2.30 Port Dropdown Menu 34
Figure 2.31 Port Setting Webpage 34
Figure 2.32 Port Status Webpage 35
Figure 2.33 Example of VLAN Configuration 36
Figure 2.34 VLAN Dropdown Menu 37
Figure 2.35 VLAN Setting Webpage 37
Figure 2.36 802.1Q VLAN Dropdown Menu 38
Figure 2.37 802.1Q VLAN’s Setting Webpage 39
Figure 2.38 802.1Q VLAN PVID Setting Webpage 40
Figure 2.39 802.1Q VLAN Table Webpage 40
Figure 2.40 Port-based VLAN Setting Webpage 41
Figure 2.41 Power over Ethernet Dropdown Menu Example on EHG6510-8PoE-2SFP-D-24V 42
Figure 2.42 PoE Schedule Webpage with Example on EHG6510-8PoE-2SFP-D-24V 43
Figure 2.43 PoE Status Webpage 44
Figure 2.44 Trunking Dropdown Menu 44
Figure 2.45 Trunking Setting Webpage with Example on EHG6510-8PoE-2SFP-24V 45
Figure 2.46 Spanning Tree Dropdown Menu 46
Figure 2.47 Spanning Tree Mode Setting 47
Figure 2.48 Spanning Tree Main Setting for RSTP 47
Figure 2.49 Spanning Tree Per-port Setting for RSTP 48
Figure 2.50 Bridge Information Webpage 48
Figure 2.51 Spanning Tree Port Setting Webpage 50
Figure 2.52 Port Security Webpage 53
Figure 2.53 RADIUS Authentication Sequence 54
Figure 2.54 802.1X Setting Webpage 55
Figure 2.55 802.1X's Parameters Setting Webpage 56
Figure 2.56 802.1x Port Setting Webpage 57
Figure 2.57 Security Access Control List Information Webpage 58
Figure 2.58 LLDP Dropdown Menu 59
Figure 2.59 LLDP Setting Webpage 60

Figure 2.60 LLDP Neighbors Webpage 60
Figure 2.61 Example of LLDP Neighbors Webpage 60
Figure 2.62 SNMP Settings Webpage 62
Figure 2.63 SNMP Enabling Box 63
Figure 2.64 SNMP Community Strings 63
Figure 2.65 Example of Trap Receiver Setting 64
Figure 2.66 SNMPv3 Users' Options 65
Figure 2.67 System Log Setting Webpage 66
Figure 2.68 Event Log Webpage 67
Figure 2.69 Webpage of Warning Event Selection 68
Figure 2.70 SMTP Setting Webpage 70
Figure 2.71 Example of SMTP Setting 70
Figure 2.72 Warning/Alarm Log Webpage 71
Figure 2.73 Backup/Restore Configuration via HTTP 72
Figure 2.74 Firmware Update Webpage 73
Figure 2.75 Factory Default Setting Webpage 73
Figure 2.76 Reboot Webpage 73
Figure 2.77 Logout Webpage 73
Figure 3.1 Telnet Command 74

Table of Tables

Table 2.1 Descriptions of the Basic information 16
Table 2.2 Descriptions of the System Setting 17
Table 2.3 Descriptions of IP Settings 20
Table 2.4 Descriptions of the System Time and the SNTP 22
Table 2.5 Modbus Memory Map 23
Table 2.6 Descriptions of Authentication Server Settings 26
Table 2.7 Descriptions of QoS Setting 28
Table 2.8 Priority queue descriptions 30
Table 2.9 Descriptions of Rate Control Setting 32
Table 2.10 Descriptions of Limiting Parameters 33
Table 2.11 Descriptions of Port Settings 35
Table 2.12 Description of VLAN Setting 37
Table 2.13 Setting Descriptions of 802.1Q VLAN Settings 39
Table 2.14 Setting Descriptions of 802.1Q VLAN PVID 40
Table 2.15 Descriptions of 802.1Q VLAN Table 40
Table 2.16 Default value of PoE Schedule Profile 42
Table 2.17 Descriptions of PoE Status 43
Table 2.18 Descriptions of Trunking Settings 45
Table 2.19 Descriptions of Spanning Tree Parameters 47

Table 2.20 Bridge Root Information 48
Table 2.21 Bridge Topology Information 49
Table 2.22 Descriptions of Spanning Tree Port Setting 50
Table 2.23 Default Path Cost for RSTP 52
Table 2.24 Descriptions of Port Security 53
Table 2.25 Descriptions of 802.1X Setting 55
Table 2.26 Descriptions of 802.1X Parameters 56
Table 2.27 Descriptions of 802.1X Port Setting 57
Table 2.28 Descriptions of ACL Entries for in ACL Webpage 58
Table 2.29 Descriptions of LLDP Neighbors Webpage 60
Table 2.30 Descriptions of SNMP Setting 63
Table 2.31 Descriptions of Community String Settings 63
Table 2.32 Descriptions of Trap Receiver Settings 64
Table 2.33 Descriptions of SNMP V3 Settings 65
Table 2.34 Descriptions of System Log Settings 66
Table 2.35 Descriptions of Event Log 67
Table 2.36 Descriptions of Link Status Alarm Event Selection 68
Table 2.37 Descriptions of System Log Alarm Event Selection 69
Table 2.38 Descriptions of SMTP Setting 70
Table 2.39 Descriptions of Warning / Alarm Log 71

1 Introduction

1.1 Introduction to Industrial Managed Switch

Atop's EHG (**E**thernet Switching **H**ub Full **G**igabit) 65XX series are product lines of powerful industrial lite-managed booster switch which are referred to as Open Systems Interconnection (OSI) Layer 2 bridging devices. Unlike an "**unmanaged**" switch, which is normally found in homes or in Small Office/Home Office (SOHO) environments and runs in "auto-negotiation" mode, each port on a "**managed switch**" can be configured for its link bandwidth, priority, security, and duplex settings. The managed switches can be managed by Simple Network Management Protocol (SNMP) software, or web browsers. Since every single port can be configured to specific settings, network administrators can better control the network and maximize network functionality.

Atop'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. Atop's managed switch works fine even in these environments.

Atop'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 iA-Ring, and Rapid Spanning Tree Protocol (RSTP). These protocols provide better network reliability and decrease recovery time down to less than 20 ms.

Atop's managed switch supports a wide range of IEEE standard protocols. This switch is excellent for keeping systems running smoothly, reliable for preventing system damage or losses, and friendly to all levels of users. The goal of this innovative product is to bring users 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

Atop's industrial lite-managed booster 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 Atop's switches to be used in safety applications, and factory and process automation. The followings are the list of protocols and software features.

- User Interfaces
    - Web browser
- Dynamic Host Configuration Protocol (DHCP) Client
- Layer-2 Switching
- Time Synchronization
    - Network Time Protocol (NTP) Server/Client
    - Simplified Network Time Protocol (SNTP)
- Mirror Port
- Simple Network Management Protocol (SNMP) v1/v2/v3 (with MD5 Authentication and DES encryption)
- SNMP Inform
- Rapid Spanning Tree Protocol (RSTP)
- Virtual Local Area Network (VLAN)
- IEEE 802.1x / Extensible Authentication Protocol (EAP) / Remote Authentication Dial-In User Service (RADIUS)
- Trunking
- Power Over Ethernet
- Link Layer Discovery Protocol (LLDP)
- Alarm System (E-mail Notification)

2 Configuring with a Web Browser

Chapter 2 explains how to access the industrial managed switch for the first time. The web brower is the easiest way to configure this Ethernet Switch. The web browser allows users to access the switch over the Internet or the Ethernet LAN. Telnet and Command Line Interface (CLI) are not supported by EHG65xx. 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 Factory 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. Please pay attention that the username and the password are case sensitive.

IP Address: 10.0.50.1
Subnet Mask: 255.255.0.0
Default Gateway: 0.0.0.0
User Name: admin
Password: default

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 the following 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 username and the password are left empty, the login prompt will not show.

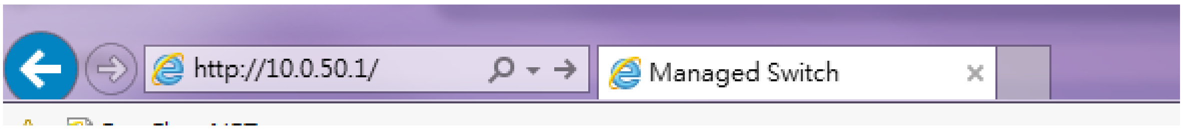
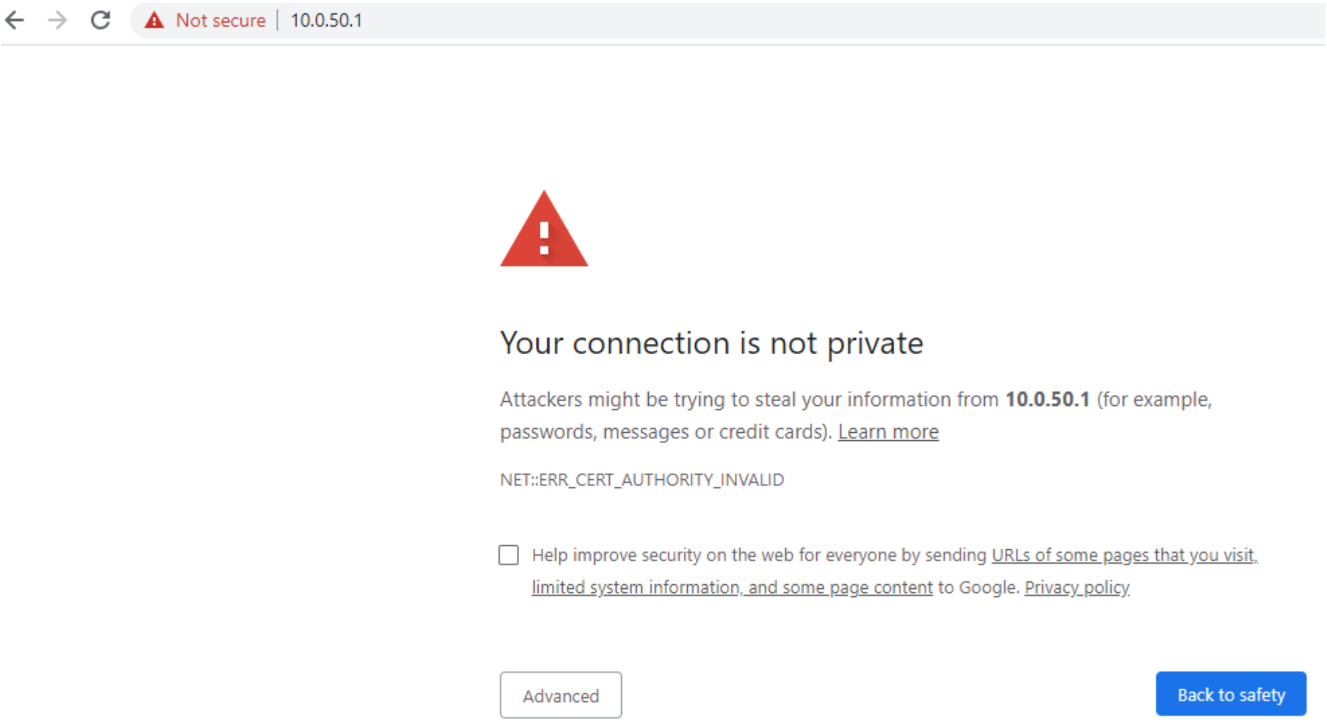


Figure 2.1 IP Address for Web-based Setting

3. If it is the first time that the users access the managed switch, the web browser such as Google Chrome may detect that the switch does not have a valid certificate authority. The users can proceed by clicking on the **Advanced** button as shown in Figure 2.2.



Your connection is not private

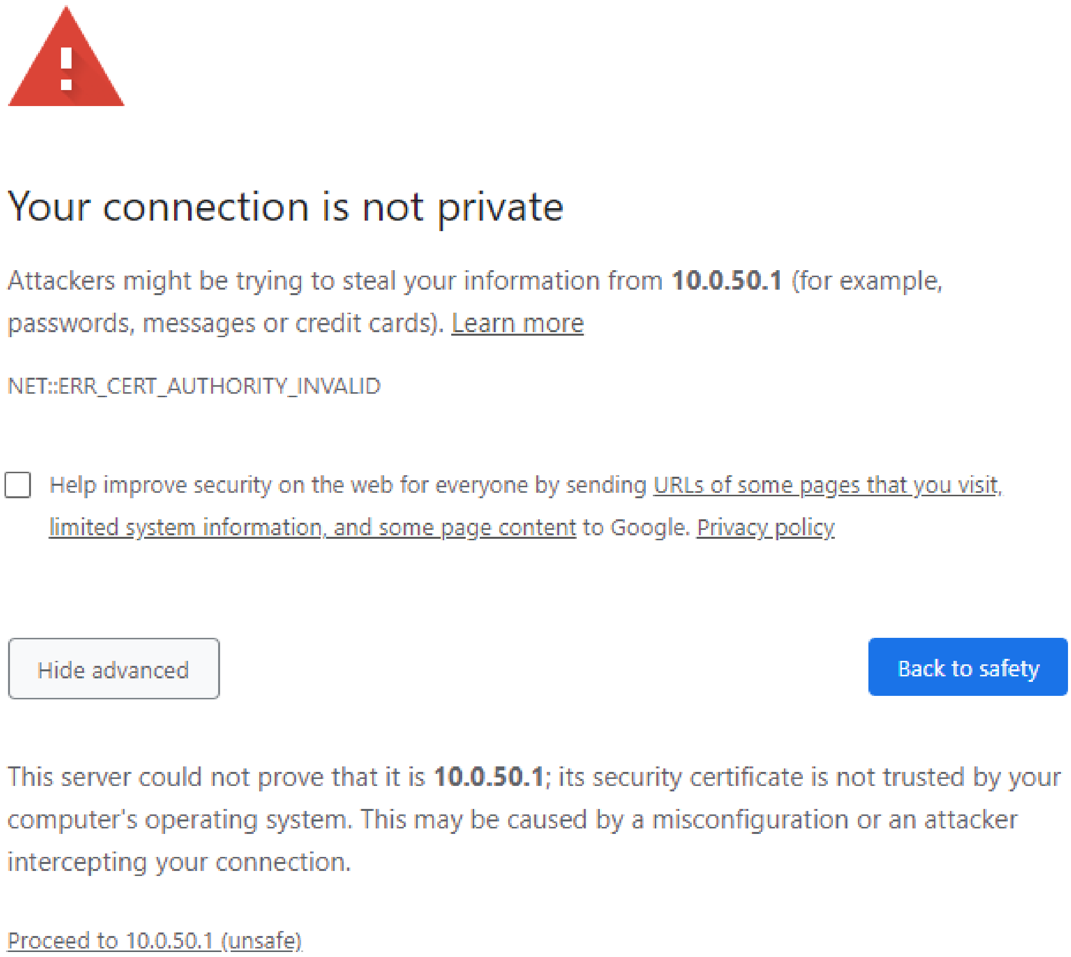
Attackers might be trying to steal your information from **10.0.50.1** (for example, passwords, messages or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve security on the web for everyone by sending URLs of some pages that you visit, limited system information, and some page content to Google. Privacy policy

Figure 2.2 Example of Google's Chrome web brower invalid certificate authority

4. Once the **Advanced** button is clicked, an explanation text will appear below the button as shown in Figure 2.3. Here at the bottom of the web page, there is a hyperlink that the users can click to access the web GUI of the managed switch.



Your connection is not private

Attackers might be trying to steal your information from **10.0.50.1** (for example, passwords, messages or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

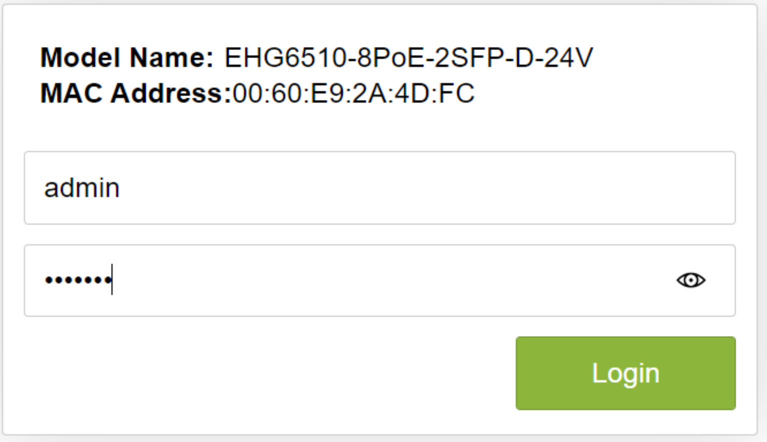
□ Help improve security on the web for everyone by sending URLs of some pages that you visit, limited system information, and some page content to Google. Privacy policy

This server could not prove that it is **10.0.50.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 10.0.50.1 (unsafe)

Figure 2.3 A hyperlink to proceed to the managed switch at IP address 10.0.50.1

5. After preceeding through the invalid certificate warning and clicking on the **Proceed to 10.0.50.1 (unsafe)** hyperlink, a login page will be presented shown in Figure 2.4. The user can enter a **Username** and a **Password** to access the managed switch. Then, clicking on the **Login** button.



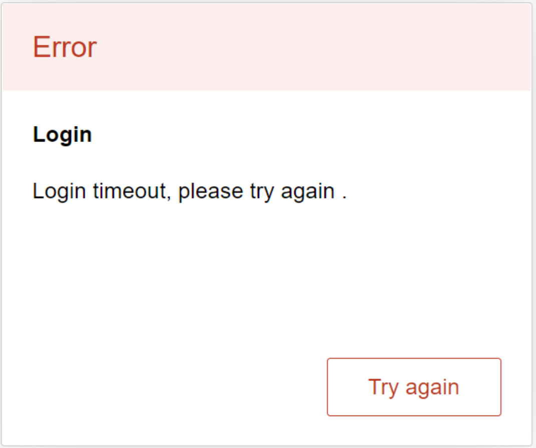
Model Name: EHG6510-8PoE-2SFP-D-24V
MAC Address:00:60:E9:2A:4D:FC

admin

•••••••

Figure 2.4 Login page

6. For security purpose, if the user did not enter the username and the password within 30 seconds, the login page will time-out and an error notification page will show up. Even though the user entered the correct username and password, the login procedure will not succeed if the login was done more than 30 seconds after the login page was first accessed. The notification page is shown in Figure 2.5. The user can click on the **Try again** button to access the login page again.



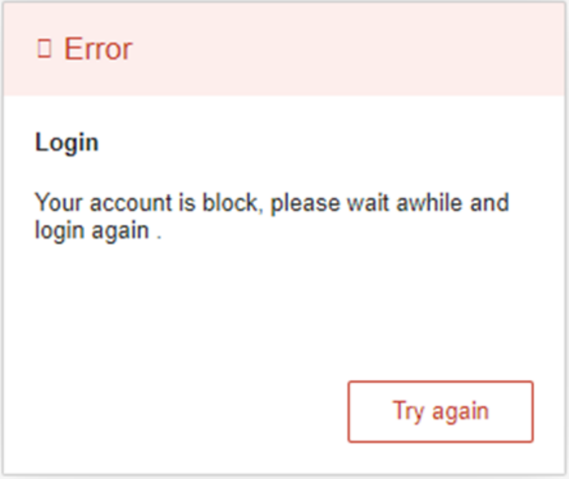
Error

Login

Login timeout, please try again .

Figure 2.5 Login timeout error notification

7. If the user entered wrong passwords more than three times within 3 minutes, the account will be temporary blocked for 15 minutes. An error pop-up notification will be shown as in Figure 2.6. The user can click **Try again** button to access the login page again after the duration of 15 minutes.



□ Error

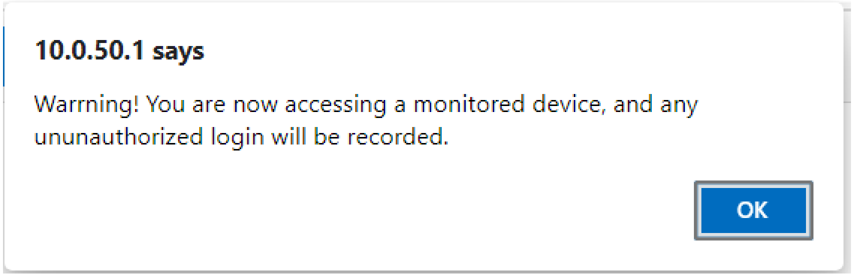
Login

Your account is block, please wait awhile and login again .

Figure 2.6 Example of error notification on blocked account

Note:

1. Any unauthorized login to the managed switch will be recorded to device’s syslog. A pop-up notification is shown in Figure 2.7.
2. After the user logins to the main interface if the user is idle or inactive for more than 5 minutes, the user will be logged out automatically.

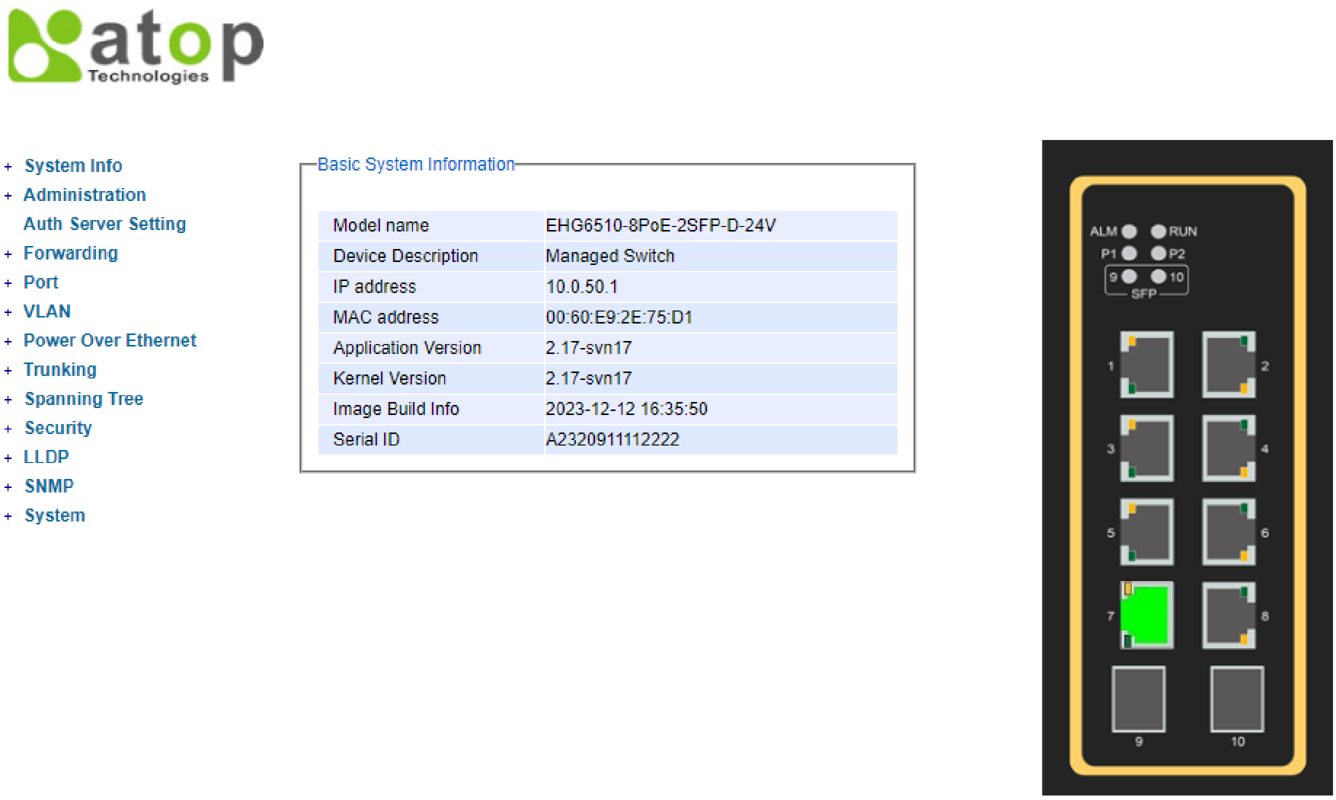


10.0.50.1 says

Warrning! You are now accessing a monitored device, and any ununauthorized login will be recorded.

Figure 2.7 Notification on recording of unauthorized login

After the login process, the main interface will show up, as shown in Figure 2.8. 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 1 is highlighted in green, indicating that the port is being connected. Detailed explanations of each subsection will be addressed later as necessary.



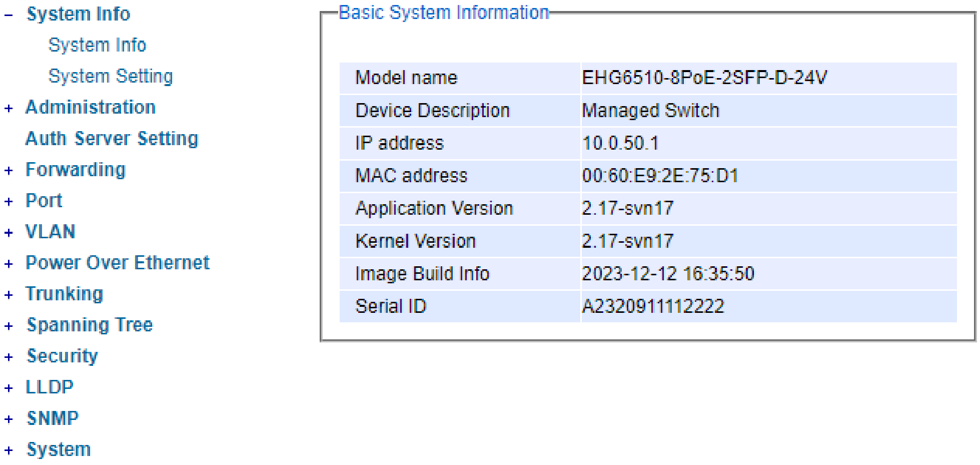
Basic System Information

Model name	EHG6510-8PoE-2SFP-D-24V
Device Description	Managed Switch
IP address	10.0.50.1
MAC address	00:60:E9:2E:75:D1
Application Version	2.17-svn17
Kernel Version	2.17-svn17
Image Build Info	2023-12-12 16:35:50
Serial ID	A2320911112222

Figure 2.8 Default Web Interface

2.2 System Info

To help users become familiar with the device, the **System Info** 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 System Info section is only categorized into one subsection as shown in the left panel of Figure 2.9.

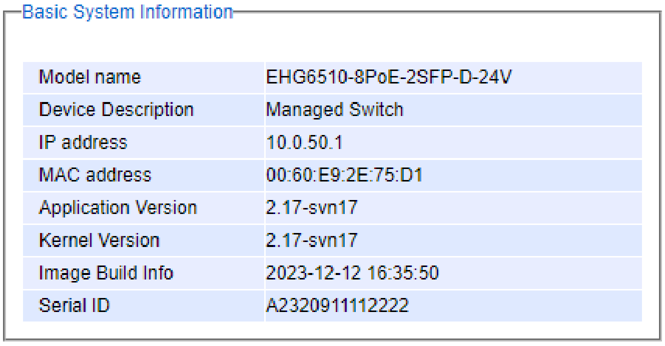


Model name	EHG6510-8PoE-2SFP-D-24V
Device Description	Managed Switch
IP address	10.0.50.1
MAC address	00:60:E9:2E:75:D1
Application Version	2.17-svn17
Kernel Version	2.17-svn17
Image Build Info	2023-12-12 16:35:50
Serial ID	A2320911112222

Figure 2.9 System Information Dropdown Menu

2.2.1 System Info

The only subsection, i.e., ***System Info***, provides basic system information of Atop's industrial managed switch. The user can check the model name, device description, IP address, MAC address, Application version, Kernel version, and image build information. Figure 2.10 depicts an example of Basic System Information of EHG6510-8PoE-2SFP-D-24V. Table 2.1 summarizes the description of each basic information.



Model name	EHG6510-8PoE-2SFP-D-24V
Device Description	Managed Switch
IP address	10.0.50.1
MAC address	00:60:E9:2E:75:D1
Application Version	2.17-svn17
Kernel Version	2.17-svn17
Image Build Info	2023-12-12 16:35:50
Serial ID	A2320911112222

Figure 2.10 Details of System Info Webpage under the System Info Mainmenu

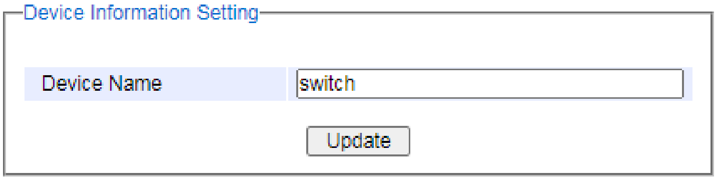
Table 2.1 Descriptions of the Basic information

Label	Description
Model name	The device's complete model name
Device Description	The model type of the device
IP address	An IP address 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
Serial ID	The serial number of the device

2.2.2 System Setting

Users can assign device’s details to Atop’s switch in this section. By entering unique and relevant system information such as device name, this information can help identify one specific switch among all other devices in the network. Please click on the “**Update**” button to update the information on the switch. Figure 2.11 shows **Device Information Setting** page of an EHG65xx Lite-Managed Booster Switch series. Table 2.2 summarizes the device information setting descriptions and corresponding default factory settings.



Device Information Setting

Device Name: switch

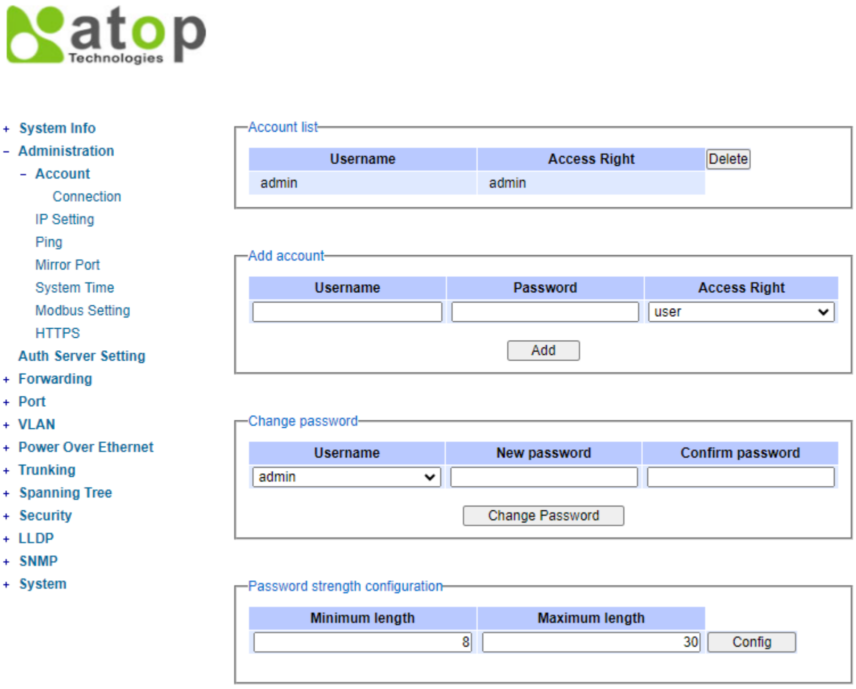
Figure 2.11 Details of System Setting Webpage

Table 2.2 Descriptions of the System Setting

Label	Description	Factory Default
Device Name	Specifies a particular role or application of different switches. The name entered here will also be shown in Atop’s Device Management Utility. Max. 63 Char.	switch

2.3 Administration

In this section, users will be able to configure **Account, IP Settings, Ping, Mirror Port, System Time, Modbus Setting,** and **HTTPs**. Figure 2.12 shows the Administration menu with the list of its sub-menus on the left of the screen.



Account list

Username	Access Right
admin	admin

Add account

Username	Password	Access Right
		user

Change password

Username	New password	Confirm password
admin		

Password strength configuration

Minimum length	Maximum length
8	30

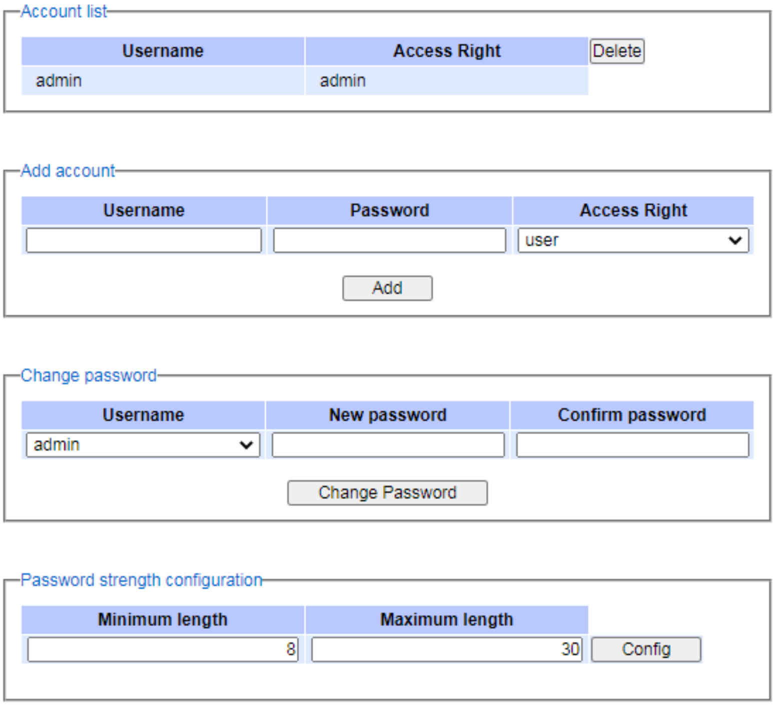
Figure 2.12 Administration Dropdown Menu

2.3.1 Account

The users with administration access right can create and delete accounts through **Account** Section. As shown in Figure 2.13, there are total of four section boxes inside **Account** page as the followings: **Account list**, **Add account**, **Change password** and **Password strength configuration.** In **Account List** box (1st row of Figure 2.13), the users and their access rights are listed. There are two types of access right: **admin** and **user**. The **admin**'s access right has **read/write** permission on the managed switch while the **user**'s access right has only **read** permission. If the user with administration access right would like to delete any account, the user can select the account that would like to be deleted and click "**Delete**" button. Note that the user cannot delete his/her own account. The user whose account was deleted will be logged out immediately.

In the **Add account** box (2nd row of Figure 2.13), the user can input a username in the **Username** textbox as well as input a password in the **Password** textbox. Then the user can select an appropriate **Access Right** from the drop-down list for the user before clicking **Add** button. After clicking it, a new account will be created in the **Account List** box. A username "admin" with an "admin" **Access Right** is created as the default. The maximum number of accounts is 15 accounts.

If the user wishes to change password for any account, the user can do so in the **Change password** box (3rd row of Figure 2.13). Here, the user has to select a user name from the **Username** dropdown box first. Then, input a password that user would like to change it to in **New password** textbox before reentering the same password in the **Confirm password** textbox. The **Minimun length** and the **Maximum length** of each password can be configured through the **Password strength configuration** box in the last row of Figure 2.13.



Account list

Username	Access Right	Delete
admin	admin	

Add account

Username	Password	Access Right
		user

Add

Change password

Username	New password	Confirm password
admin		

Change Password

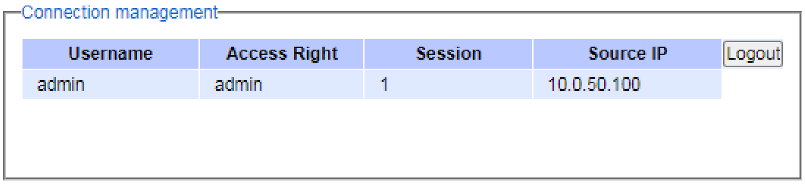
Password strength configuration

Minimum length	Maximum length	
8	30	Config

Figure 2.13 Account Setting Webpage

2.3.2 *Connection*

The **Connection** sub-menu under the **Account** menu lists the users who currently access the device under the **Connection Management** box. Inside the box, the table lists the information of the users with four columns: **Username**, **Access Right**, **Session**, and **Source IP** is shown in Figure 2.14**.**



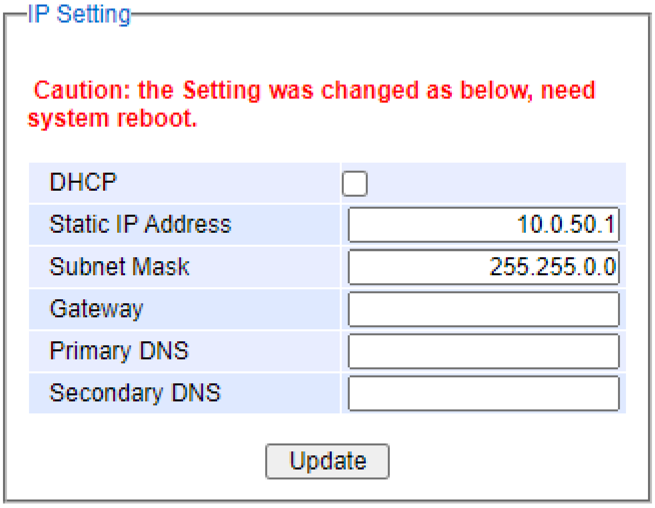
Connection management

Username	Access Right	Session	Source IP	Logout
admin	admin	1	10.0.50.100	

Figure 2.14 Connection Management Webpage

2.3.3 *IP Setting*

This subsection is divided into two parts: **IP Setting** and **Current IP address information**. In this subsection, the user may modify network settings of Internet Protocol version 4 (IPv4) for the managed switch, e.g. **Static IP Address**, **Subnet Mask**, **Gateway**, **Primary DNS** (domain name server), and **Secondary DNS**. As shown in Figure 2.15, the user can choose to enable **DHCP** (Dynamic Host Configuration Protocol) by checking the box behind it. That is the IP address and related information can be automatically obtained from a DHCP server in the local network thus reducing the work for an administrator. By disabling this function (DHCP's box is unchecked), the user has an option to setup the static IP address and related fields manually.



IP Setting

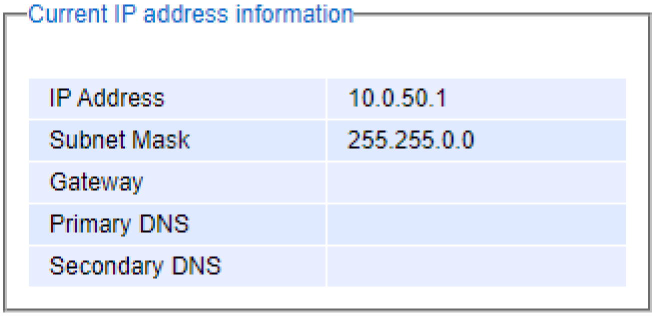
Caution: the Setting was changed as below, need system reboot.

DHCP	□
Static IP Address	10.0.50.1
Subnet Mask	255.255.0.0
Gateway	
Primary DNS	
Secondary DNS	

Figure 2.15 IP Setting under IP Setting Webpage

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 caution message is shown in red color accordingly. To launch the web configuration again, 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 changed.

The second part of IP Setting section is the **Current IP address information** part as shown in Figure 2.16. In this part, the current IP address information of the managed switch is listed. The description of each field and its default value are summarized in Table 2.3.



Current IP address information

IP Address	10.0.50.1
Subnet Mask	255.255.0.0
Gateway	
Primary DNS	
Secondary DNS	

Figure 2.16 IP Interface Part under IP Setting Webpage

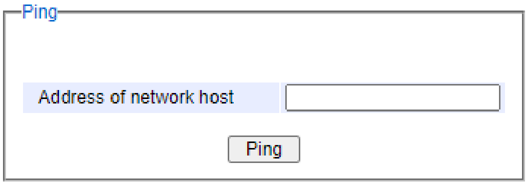
Table 2.3 Descriptions of IP Settings

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.	NULL
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

2.3.4 Ping

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. Figure 2.17 shows the user interface for using the Ping command.



Ping

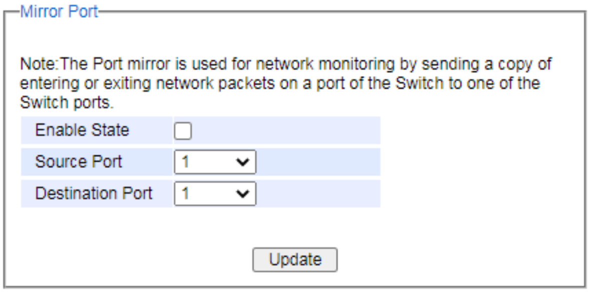
Address of network host

Figure 2.17 Webpage for Ping

2.3.5 Mirror Port

Mirror Port is used on switches to send a copy of network packets sent/received on one switch port or a range of switch ports to a network monitoring connection on another switch port (Monitor Port).
Port mirroring is used in network systems that require monitoring of network traffic, such as an IDS ("Intrusion Detection System").
Port mirroring, together with an NTA ("Network Traffic Analyzer"), can help to monitor network traffic. Users can monitor the selected ports ("Source Ports") for egress and/or ingress packets.

- "Source Port": The incoming data packets are copied and forwarded to the monitor port.
- "Destination Port": The outgoing data packets are copied and forwarded to the monitor port.



Mirror Port

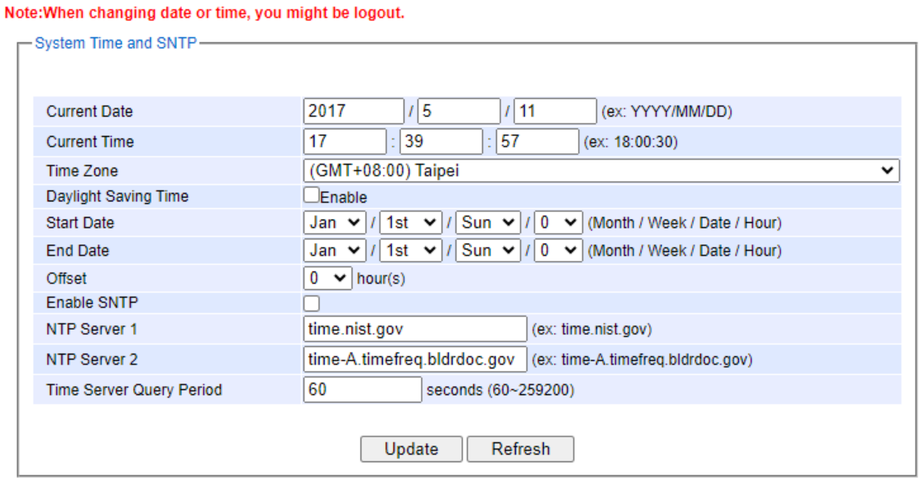
Note:The Port mirror is used for network monitoring by sending a copy of entering or exiting network packets on a port of the Switch to one of the Switch ports.

Enable State	□
Source Port	1
Destination Port	1

Figure 2.18 Mirror Port Webpage

2.3.6 System Time

Atop's industrial managed switch has internal calendar (date) and clock (or system time) which can be set manually or automatically. Figure 2.19 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).



Note:When changing date or time, you might be logout.

System Time and SNTP

Current Date	2017 / 5 / 11 (ex: YYYY/MM/DD)
Current Time	17 : 39 : 57 (ex: 18:00:30)
Time Zone	(GMT+08:00) Taipei
Daylight Saving Time	□ Enable
Start Date	Jan / 1st / Sun / 0 (Month / Week / Date / Hour)
End Date	Jan / 1st / Sun / 0 (Month / Week / Date / Hour)
Offset	0 hour(s)
Enable SNTP	□
NTP Server 1	time.nist.gov (ex: time.nist.gov)
NTP Server 2	time-A.timefreq.bldrdoc.gov (ex: time-A.timefreq.bldrdoc.gov)
Time Server Query Period	60 seconds (60~259200)

Figure 2.19 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 2.4.

Table 2.4 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 Saving	Enable or disable Daylight Saving Time function	Unchecked
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	60

Label	Description	Factory Default
	suitable since it will cause less load to the switch. The setting value can be in between 60 – 259200 (72 hours) seconds.	

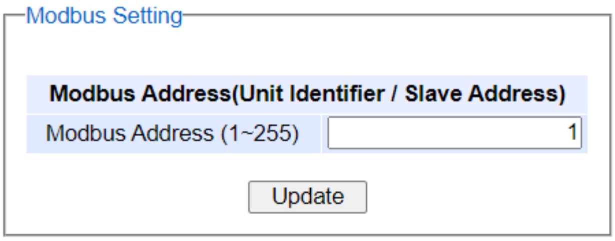
***Note:**

- **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

2.3.7 Modbus Setting

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. Figure 2.20 shows the Modbus Setting webpage, and Modbus memory mapping table lists all the register's addresses inside the managed switch and their descriptions, is provide in Table 2.5.



Modbus Setting

Modbus Address(Unit Identifier / Slave Address)

Modbus Address (1~255): 1

Figure 2.20 Webpage for Setting the Modbus Address

Table 2.5 Modbus Memory Map

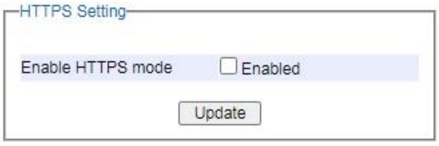
System Information			
Address	Data Type	Read/Write	Description
0x0020 (32)	1 word	R	Firmware Version Ex: Version = 1.02 Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x02
0x0021 (33)	3 words	R	Ethernet MAC Address Ex: MAC = 00-01-02-03-04-05 Word 0 Hi byte = 0x00 Word 0 Lo byte = 0x01

			Word 1 Hi byte = 0x02
			Word 1 Lo byte = 0x03
			Word 2 Hi byte = 0x04
			Word 2 Lo byte = 0x05
0x0024 (36)	1 word	R	Kernel Version
			Ex: Version = 1.03
			Word 0 Hi byte = 0x01
			Word 0 Lo byte = 0x03
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
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
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
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

2.3.8 HTTPS

This subsection enables the users to set the HTTPS (HyperText Transfer Protocol Secure) for the web-based management user interface of the switch. This option will encrypt the normal HTTP message between the switch and the client PC to secure their communication over the network. To access the web GUI when this option is enabled, the users can also access the switch via https://10.0.50.1 for enchanced security during device configuration. Clicking on the **Update** button when you change the option to update it on the managed switch.



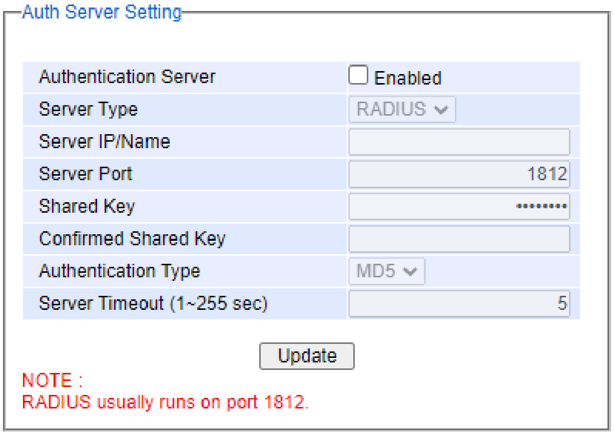
HTTPS Setting

Enable HTTPS mode □ Enabled

Figure 2.21 HTTPS Setting Webpage

2.3.9 Auth Server Setting

In addition to the local authentication, the switch can be configured to request for authentication through a centralized RADIUS Server when the local authentication fails. Figure 2.22 shows the setting parameters for authentication server while Table 2.6 summarizes the authentication server settings.



Auth Server Setting

Authentication Server	□ Enabled
Server Type	RADIUS
Server IP/Name	
Server Port	1812
Shared Key	••••••••
Confirmed Shared Key	
Authentication Type	MD5
Server Timeout (1~255 sec)	5

NOTE :
RADIUS usually runs on port 1812.

Figure 2.22 Authentication Server Setting

Table 2.6 Descriptions of 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. 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. MD5.	MD5
Server Timeout (1~255 sec)	The time out period of waiting for a response from the authentication server. This will affect	5

	the time that the next login prompt shows up in case that the server is not available.	

When configuring RADIUS as the authentication server, the system administrator of the RADIUS server must also make sure that the RADIUS's service-type attribute of each new user matches that particular user. For example, if a user has an administrative right that user should have read/write privilege, this user should be set Service-Type attribute on RADIUS server as "Administrative-User". On the other hand, if a user has only normal privilege that is only read permission, this user should be set Service-Type attribute on RADIUS server as "NAS-Prompt-User". Note that NAS is refered to Network Access Server or the EHG6510 Switch in this case. NAS is a client of RADIUS server. Depicts an example of a user called "admin1" with Cleartext-Password attribute of "default1" and Service-Type attribute of "Administrative-User".

***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.

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 2.23 depicts the submenus under the Forwarding section.

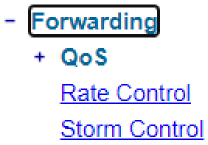


Figure 2.23 Forwarding Dropdown Menu

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 are 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 2.24. Table 2.7 summarizes the descriptions of QoS Setting. See notes in the following subsection for more details.

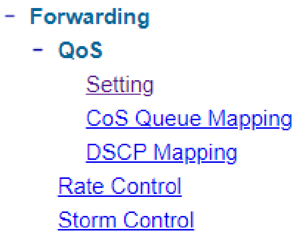


Figure 2.24 QoS Dropdown Menu

Table 2.7 Descriptions of QoS Setting

Label	Description	Factory Default
Setting	Queuing Methods (packet scheduling disciplines) includes **Strict Priority** and **Weighted Round-Robin**. The detailed descriptions and comparison are given in the following subsection.	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.	802.1p CoS only

2.4.1.1 QoS Setting

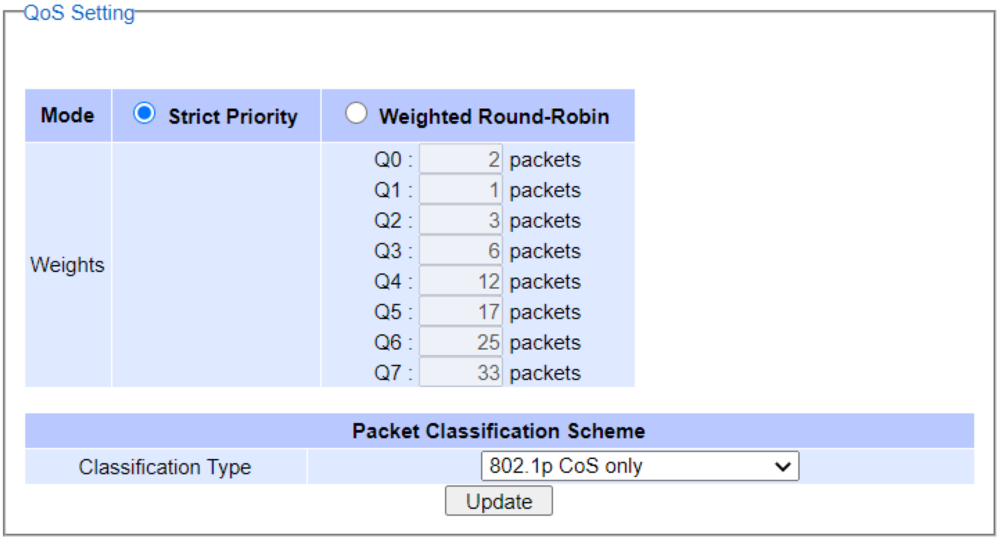
Two types of queuing methods are configurable in this managed switch: Strict Priority and Weighted Round-Robin.

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. Figure 2.25 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 = 3 packets
- COS Q3 = 6 packets
- COS Q4 = 2 packets
- COS Q5 = 17 packets
- COS Q6 = 25 packets
- COS Q7 = 33 packets



QoS Setting

Mode	● Strict Priority	○ Weighted Round-Robin
Weights		Q0 : 2 packets Q1 : 1 packets Q2 : 3 packets Q3 : 6 packets Q4 : 12 packets Q5 : 17 packets Q6 : 25 packets Q7 : 33 packets

Packet Classification Scheme	
Classification Type	802.1p CoS only

Figure 2.25 QoS Setting Webpage

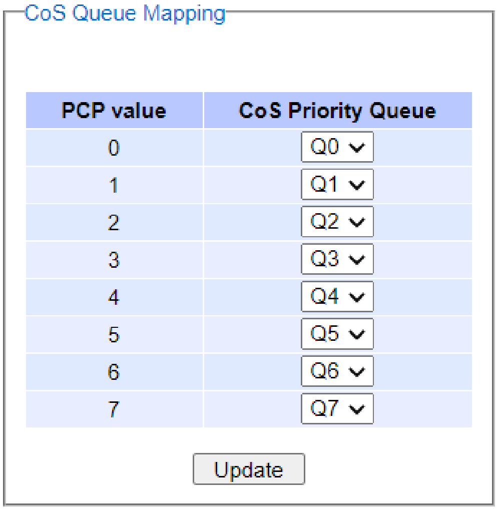
At the bottom of the QoS Setting webpage in Figure 2.25, the users can select the packet classification scheme that will be used by the managed switch. There are two classification types to choose from the drop-down list: **802.1p CoS only** or **Both 802.1p CoS and DiffServ**. The default classification type is **802.1p CoS only**. Note that after changing the schedule discipline, setting the desired weights if any for the WRR, or 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 (PC) within an Ethernet frame header to different CoS priority queues as shown in Figure 2.26. 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 2.8.



CoS Queue Mapping

PCP value	CoS Priority Queue
0	Q0
1	Q1
2	Q2
3	Q3
4	Q4
5	Q5
6	Q6
7	Q7

Figure 2.26 Mapping Table of CoS Webpage

Table 2.8 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 -> Q1 PCP 2 -> Q2 PCP 3 -> Q3 PCP 4 -> Q4 PCP 5 -> Q5 PCP 6 -> Q6 PCP 7 -> Q7
CoS Priority Queue	The priority queue that a specific Ethernet frame needs to be assigned into.	

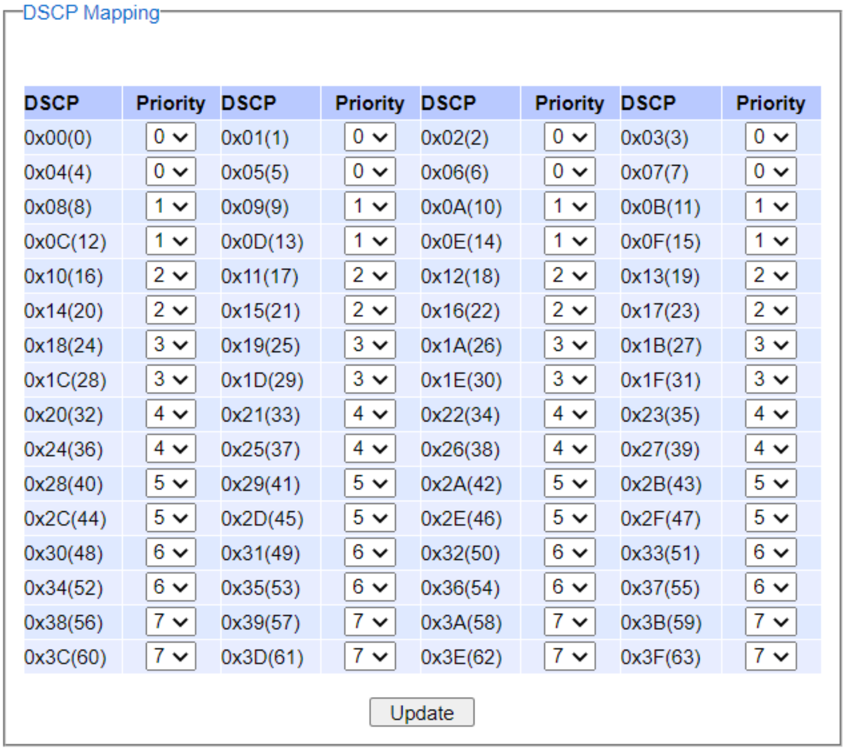
2.4.1.3 DSCP Mapping

DiffServ/ToS stands for Differentiated Services/Type of Services. It is 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). Atop implements queuing techniques that can base their PHB on the IP precedence or DSCP value in the 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 2.27. 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 2.27. 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.



DSCP Mapping

DSCP	Priority	DSCP	Priority	DSCP	Priority	DSCP	Priority
0x00(0)	0	0x01(1)	0	0x02(2)	0	0x03(3)	0
0x04(4)	0	0x05(5)	0	0x06(6)	0	0x07(7)	0
0x08(8)	1	0x09(9)	1	0x0A(10)	1	0x0B(11)	1
0x0C(12)	1	0x0D(13)	1	0x0E(14)	1	0x0F(15)	1
0x10(16)	2	0x11(17)	2	0x12(18)	2	0x13(19)	2
0x14(20)	2	0x15(21)	2	0x16(22)	2	0x17(23)	2
0x18(24)	3	0x19(25)	3	0x1A(26)	3	0x1B(27)	3
0x1C(28)	3	0x1D(29)	3	0x1E(30)	3	0x1F(31)	3
0x20(32)	4	0x21(33)	4	0x22(34)	4	0x23(35)	4
0x24(36)	4	0x25(37)	4	0x26(38)	4	0x27(39)	4
0x28(40)	5	0x29(41)	5	0x2A(42)	5	0x2B(43)	5
0x2C(44)	5	0x2D(45)	5	0x2E(46)	5	0x2F(47)	5
0x30(48)	6	0x31(49)	6	0x32(50)	6	0x33(51)	6
0x34(52)	6	0x35(53)	6	0x36(54)	6	0x37(55)	6
0x38(56)	7	0x39(57)	7	0x3A(58)	7	0x3B(59)	7
0x3C(60)	7	0x3D(61)	7	0x3E(62)	7	0x3F(63)	7

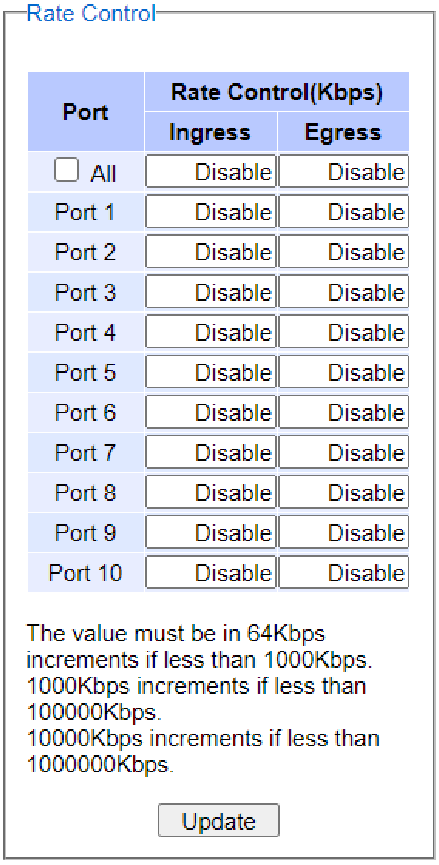
Figure 2.27 Mapping Table of DSCP and ECN Webpage

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 2.28. 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 1,000,000.
- 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 1,000 Kbps. For example: 64 Kbps, 128 Kbps, and 512 Kbps.
- The values have to be integer and multiple of 1,000 when the transmission rate is between 1,000 Kbps and 100,000 Kbps. Ex: 1,000 Kbps, 3,000 Kbps… 100,000 Kbps.
- The values have to be integer and multiple of 10,000 Kbps when transmission rate is greater than 100,000 Kbps.



Rate Control

Port	Rate Control(Kbps)	
	Ingress	Egress
□ All	Disable	Disable
Port 1	Disable	Disable
Port 2	Disable	Disable
Port 3	Disable	Disable
Port 4	Disable	Disable
Port 5	Disable	Disable
Port 6	Disable	Disable
Port 7	Disable	Disable
Port 8	Disable	Disable
Port 9	Disable	Disable
Port 10	Disable	Disable

The value must be in 64Kbps increments if less than 1000Kbps.
1000Kbps increments if less than 100000Kbps.
10000Kbps increments if less than 1000000Kbps.

Figure 2.28 Rate Control Webpage

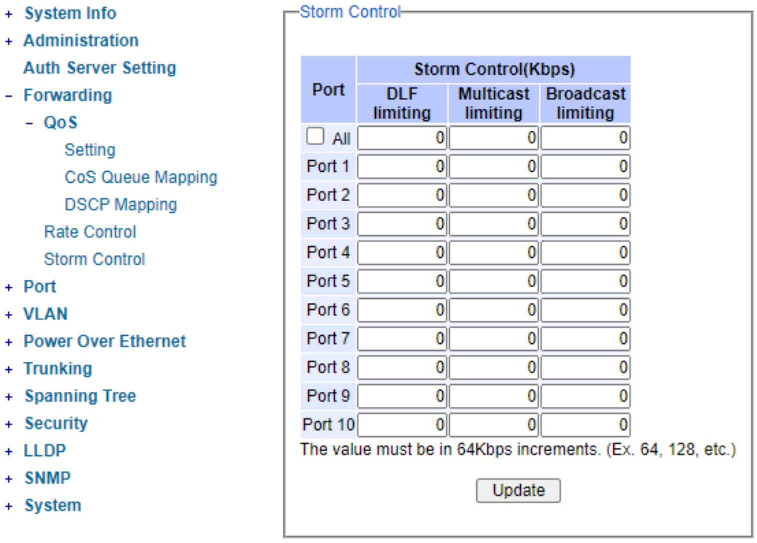
Table 2.9 provides descriptions of rate control setting. Note that after configuring the rate control in each port, please click on the **Update** button to enable it on the switch.

Table 2.9 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 Storm 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 2.29 depicts the Storm 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 **all** line and set the storm control data rate under each limiting column (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.



Storm Control

Port	Storm Control(Kbps)		
	DLF limiting	Multicast limiting	Broadcast limiting
☐ All	0	0	0
Port 1	0	0	0
Port 2	0	0	0
Port 3	0	0	0
Port 4	0	0	0
Port 5	0	0	0
Port 6	0	0	0
Port 7	0	0	0
Port 8	0	0	0
Port 9	0	0	0
Port 10	0	0	0

The value must be in 64Kbps increments. (Ex. 64, 128, etc.)

Figure 2.29 Storm Control Webpage

Table 2.10 summarizes the descriptions of storm control. 錯誤! 找不到參照來源。 summarizes the descriptions of limiting parameters for storm control.

Table 2.10 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

Industrial managed switch provides full control on all of its network interfaces. In this section, the users can enable or disable each port and set preferred physical layer mode such as copper or fiber and configure data rate (speed) for each port. All port’s status can also be viewed in this section. Figure 2.30 illustrates the Port webpage. The Port section is subdivided into five subsections which are: Setting, Port Status and Port Statistics.

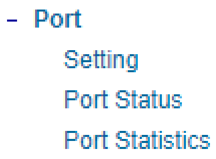
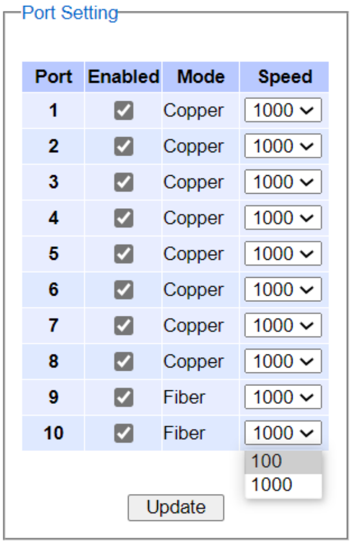


Figure 2.30 Port Dropdown Menu

2.5.1 Port Setting

Setting webpage is shown in Figure 2.31. 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. On the next column, the transmission **Speed** of each ports can be chosen from the dropdown list which could be **100**, or **1000** Mbps where the default speed is set to the highest possible rate in Mbps. After configuring the port setting, please click on the **Update** button to enable any of your new configuration on the switch.



Port Setting

Port	Enabled	Mode	Speed
1	☑	Copper	1000
2	☑	Copper	1000
3	☑	Copper	1000
4	☑	Copper	1000
5	☑	Copper	1000
6	☑	Copper	1000
7	☑	Copper	1000
8	☑	Copper	1000
9	☑	Fiber	1000
10	☑	Fiber	1000

Figure 2.31 Port Setting Webpage

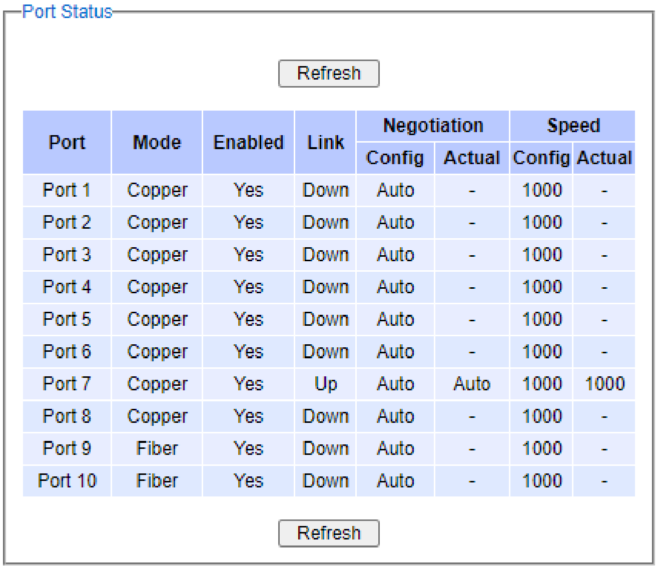
Descriptions of port setting options are summarized in Table 2.11.

Table 2.11 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
Speed	Select either 100 or 1000Mbps	1000

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. Figure 2.32 shows the Port Status webpage. To check the latest status of all port, click the **Refresh** button either on the top or the bottom of the webpage.



Port	Mode	Enabled	Link	Negotiation		Speed	
				Config	Actual	Config	Actual
Port 1	Copper	Yes	Down	Auto	-	1000	-
Port 2	Copper	Yes	Down	Auto	-	1000	-
Port 3	Copper	Yes	Down	Auto	-	1000	-
Port 4	Copper	Yes	Down	Auto	-	1000	-
Port 5	Copper	Yes	Down	Auto	-	1000	-
Port 6	Copper	Yes	Down	Auto	-	1000	-
Port 7	Copper	Yes	Up	Auto	Auto	1000	1000
Port 8	Copper	Yes	Down	Auto	-	1000	-
Port 9	Fiber	Yes	Down	Auto	-	1000	-
Port 10	Fiber	Yes	Down	Auto	-	1000	-

Figure 2.32 Port Status Webpage

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

- **Mode** (Copper or Fiber)
- **Enable** (Yes or No)
- **Link** (Up or Down)
- **Negotiation: Config** or **Actual**
- **Speed**: **Config** or **Actual** (unit: Mbps)

2.6 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 2.33).

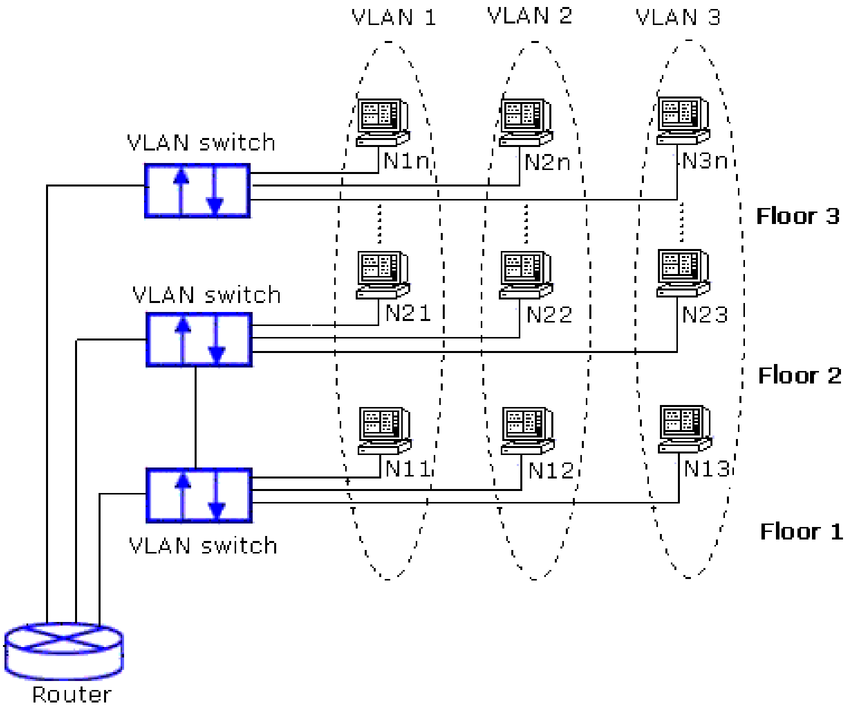


Figure 2.33 Example of VLAN Configuration

EHG65XX series managed switch provide two approaches to create VLAN as follows:

- **Tagging-based (802.1Q) VLAN**
- **Port-based VLAN**

Figure 2.34 shows the drop-down menu under the VLAN section.

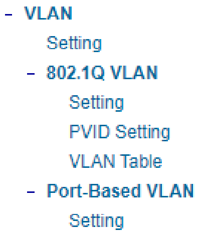
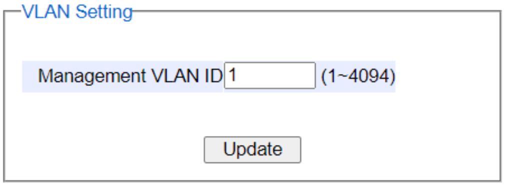


Figure 2.34 VLAN Dropdown Menu

2.6.1 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 4094. If the users change the management VLAN ID to other number, please click the **Update** button to set it on the managed switch. Figure 2.35 depicts the VLAN Setting webpage. Table 2.12 describes the VLAN Setting option.


VLAN Setting

Management VLAN ID: 1 (1~4094)

Figure 2.35 VLAN Setting Webpage

Table 2.12 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 4094.	1

2.6.2 802.1Q 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 2.36.

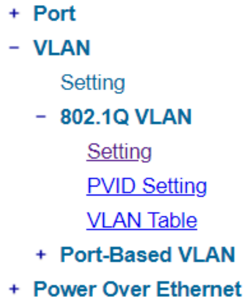


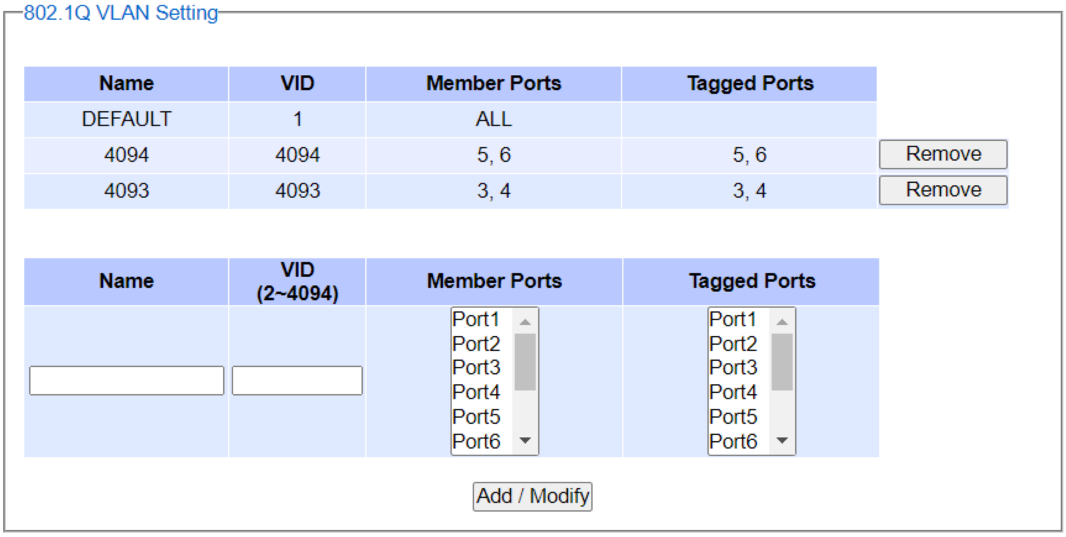
Figure 2.36 802.1Q VLAN Dropdown Menu

2.6.2.1 802.1Q VLAN Settings

Figure 2.37 shows the 802.1Q VLAN Setting webpage which allow the users to add new tagged-based VLAN to the managed switch. Please perform the following procedure to set 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 2.37. The description of each fields is summarized in Table 2.13. Then, click **Add/Modify** button. Note to select multiple **Member Ports** or multiple **Tagged Port**s, press and hold the **shift**/**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 2.37.

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 2.37.



802.1Q VLAN Setting

Name	VID	Member Ports	Tagged Ports	
DEFAULT	1	ALL		
4094	4094	5, 6	5, 6	Remove
4093	4093	3, 4	3, 4	Remove

Name	VID (2~4094)	Member Ports	Tagged Ports
		Port1 Port2 Port3 Port4 Port5 Port6	Port1 Port2 Port3 Port4 Port5 Port6

Figure 2.37 802.1Q VLAN's Setting Webpage

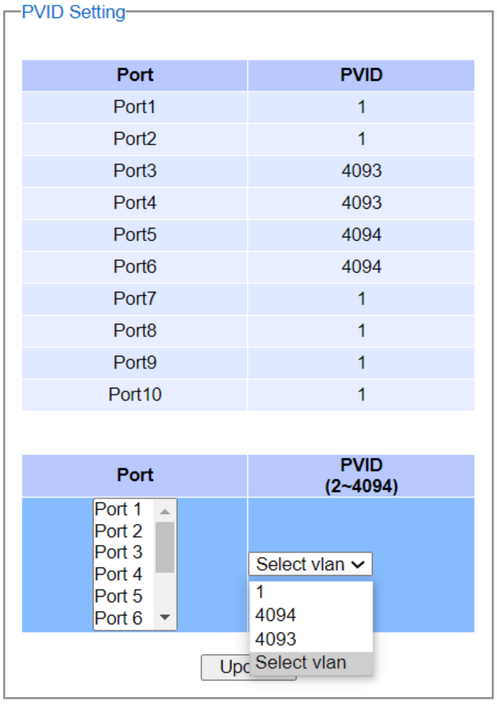
Table 2.13 Setting Descriptions of 802.1Q VLAN Settings

Label	**Description**	**Factory Default**
Name	**The VLAN ID name that can be assigned by the user.**	**Factory 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.

2.6.2.2 802.1Q 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 2.38 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 2.14 summarizes the PVID Setting's descriptions.



PVID Setting

Port	PVID
Port1	1
Port2	1
Port3	4093
Port4	4093
Port5	4094
Port6	4094
Port7	1
Port8	1
Port9	1
Port10	1

Port	PVID (2~4094)

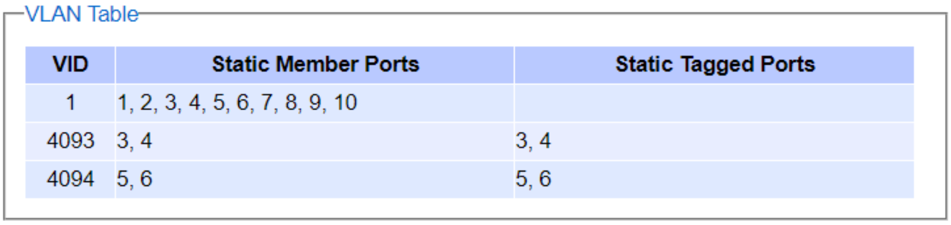
Figure 2.38 802.1Q VLAN PVID Setting Webpage

Table 2.14 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

2.6.2.3 802.1Q VLAN Table

This webpage shown in Figure 2.39 displays the 802.1Q VLAN table which lists all the VLANs that are automatically and manually added/modified to the managed switch. Table 2.15 summarizes the descriptions of VLAN Table.



VLAN Table

VID	Static Member Ports	Static Tagged Ports
1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	
4093	3, 4	3, 4
4094	5, 6	5, 6

Figure 2.39 802.1Q VLAN Table Webpage

Table 2.15 Descriptions of 802.1Q VLAN Table

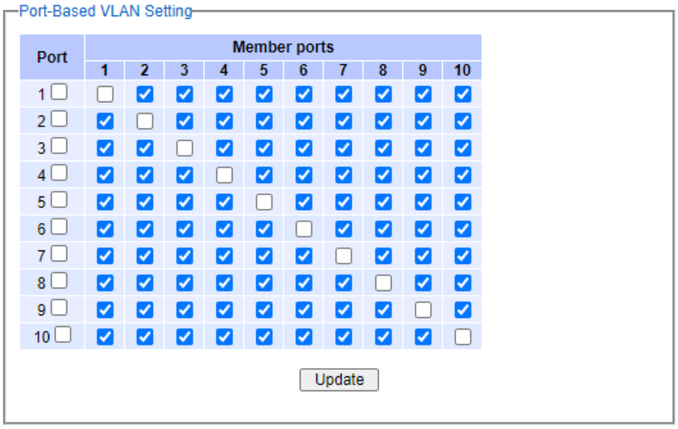
Label	Description	Factory Default
VID	Indicate the VLAN ID number	Dependent

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

2.6.3 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. If you want to allow communication between two subscriber ports, you must define the egress port for both ports. To setup port-based VLAN, please follow the following steps:

1. Click on **Port-Based VLAN setting** page as shown in Figure 2.40.
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' Port ID. Note that if the users check the box under the Port ID column, all of the Member Ports will belong to that VLAN's Port ID.
3. Click on the **Update** button to allow the setting to take effect on the managed switch.

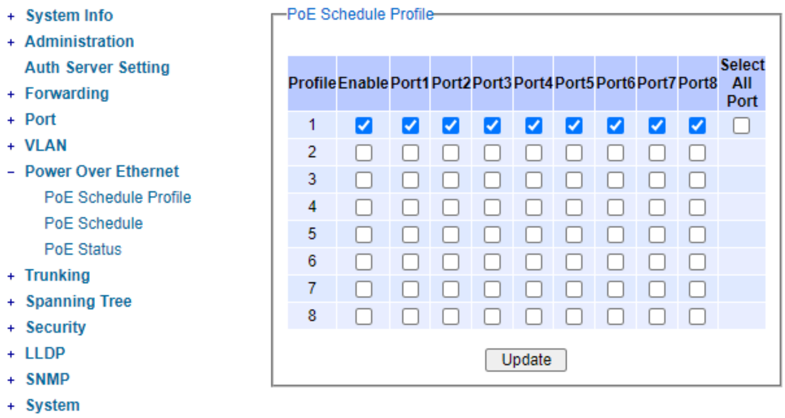


Port	Member ports									
	1	2	3	4	5	6	7	8	9	10
1 □	□	☑	☑	☑	☑	☑	☑	☑	☑	☑
2 □	☑	□	☑	☑	☑	☑	☑	☑	☑	☑
3 □	☑	☑	□	☑	☑	☑	☑	☑	☑	☑
4 □	☑	☑	☑	□	☑	☑	☑	☑	☑	☑
5 □	☑	☑	☑	☑	□	☑	☑	☑	☑	☑
6 □	☑	☑	☑	☑	☑	□	☑	☑	☑	☑
7 □	☑	☑	☑	☑	☑	☑	□	☑	☑	☑
8 □	☑	☑	☑	☑	☑	☑	☑	□	☑	☑
9 □	☑	☑	☑	☑	☑	☑	☑	☑	□	☑
10 □	☑	☑	☑	☑	☑	☑	☑	☑	☑	□

Figure 2.40 Port-based VLAN Setting Webpage

2.7 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 Atop'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 2.41 shows the Power over Ethernet dropdown menu.



PoE Schedule Profile

Profile	Enable	Port1	Port2	Port3	Port4	Port5	Port6	Port7	Port8	Select All Port
1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐
2	☐	☐	☐	☐	☐	☐	☐	☐	☐	
3	☐	☐	☐	☐	☐	☐	☐	☐	☐	
4	☐	☐	☐	☐	☐	☐	☐	☐	☐	
5	☐	☐	☐	☐	☐	☐	☐	☐	☐	
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	

Figure 2.41 Power over Ethernet Dropdown Menu Example on EHG6510-8PoE-2SFP-D-24V

2.7.1 PoE Schedule Profile

Power over Ethernet schedule is a feature which allows users to set flexible schedule for each PoE port to save power when devices are not in use. The users can set Enable status and member ports of every profile in PoE Schedule Profile page as shown in Figure 2.41. Each port can only belong to one PoE profile. If users want all ports in the same PoE setting, enable the “Select All Port” checkbox will add all port to profile 1. Disable the “Select All Port” checkbox will remove all port from profile 1. A port can provide power supply to end devices only if it belongs to a PoE schedule profile which is enabled, and the time is selected. The users can select the time they want to supply power for ports in PoE schedule page. Please also click on the **Update** button to save the setting of PoE schedule profile on the switch.

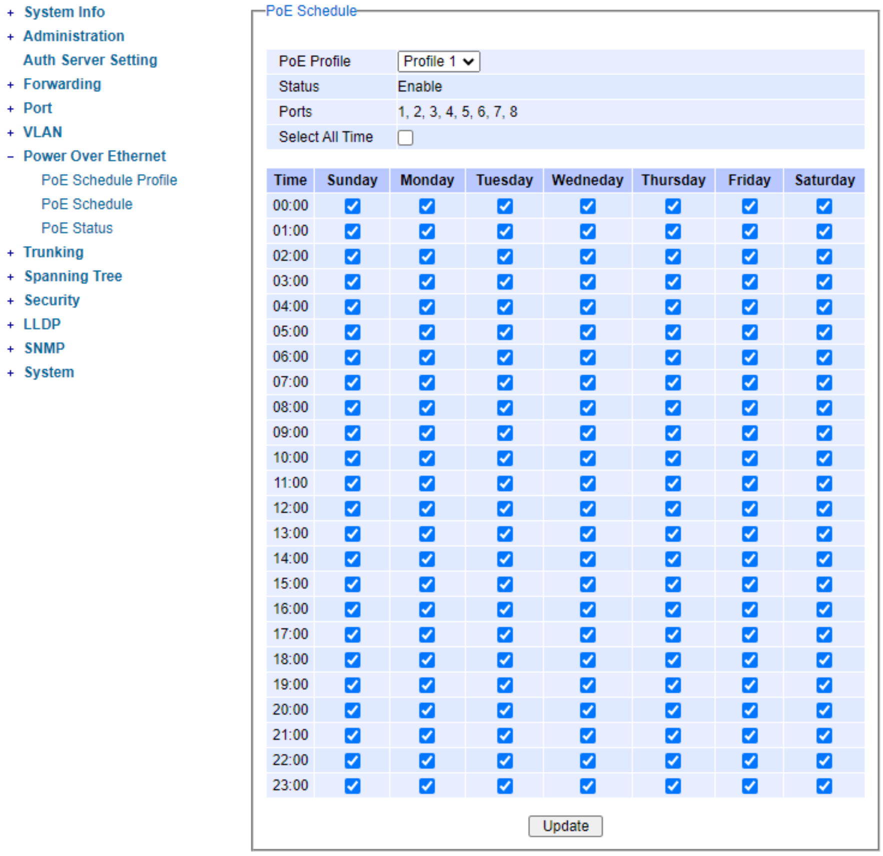
The default PoE Schedule Profile setting is all ports belong to profile 1, and only profile 1 is enable as shown in Table 2.16. The number of profiles and ports depends on the EHG model of the user’s managed switch.

Table 2.16 Default value of PoE Schedule Profile

Profile	Enable	Port1	Port2	Port3	Port4	Port5	Port6	Port7	Port8
1	Checked	Checked	Checked	Checked	Checked	Checked	Checked	Checked	Checked
2	Null	Null	Null	Null	Null	Null	Null	Null	Null
3	Null	Null	Null	Null	Null	Null	Null	Null	Null
4	Null	Null	Null	Null	Null	Null	Null	Null	Null
5	Null	Null	Null	Null	Null	Null	Null	Null	Null
6	Null	Null	Null	Null	Null	Null	Null	Null	Null
7	Null	Null	Null	Null	Null	Null	Null	Null	Null
8	Null	Null	Null	Null	Null	Null	Null	Null	Null

2.7.2 PoE Schedule

PoE Schedule page, as shown in Figure 2.42, will show Enable or Disable status and ports of every profile set in PoE Schedule Profile page. The users can select different PoE schedule profiles by PoE Profile select list and can also select the time they want to supply power for ports in this PoE schedule profile. If user wants to supply power for ports at any time, select a PoE schedule profile and enable the “Select All Time” checkbox will make all time checkbox checked. Disable the “Select All Time” checkbox will make all time checkbox unchecked. A port can provide power output to devices only if it belongs to a PoE schedule profile which is enabled, and the time is selected. The PoE status of ports might change every hour according to its PoE schedule profile. Please also click on the **Update** button to allow the setting on PoE taking effect on the switch. The default PoE Schedule setting is enable all time of profile 1 but disable all time of other profiles.



PoE Profile	Profile 1
Status	Enable
Ports	1, 2, 3, 4, 5, 6, 7, 8
Select All Time	□

Time	Sunday	Monday	Tuesday	Wedneday	Thursday	Friday	Saturday
00:00	☑	☑	☑	☑	☑	☑	☑
01:00	☑	☑	☑	☑	☑	☑	☑
02:00	☑	☑	☑	☑	☑	☑	☑
03:00	☑	☑	☑	☑	☑	☑	☑
04:00	☑	☑	☑	☑	☑	☑	☑
05:00	☑	☑	☑	☑	☑	☑	☑
06:00	☑	☑	☑	☑	☑	☑	☑
07:00	☑	☑	☑	☑	☑	☑	☑
08:00	☑	☑	☑	☑	☑	☑	☑
09:00	☑	☑	☑	☑	☑	☑	☑
10:00	☑	☑	☑	☑	☑	☑	☑
11:00	☑	☑	☑	☑	☑	☑	☑
12:00	☑	☑	☑	☑	☑	☑	☑
13:00	☑	☑	☑	☑	☑	☑	☑
14:00	☑	☑	☑	☑	☑	☑	☑
15:00	☑	☑	☑	☑	☑	☑	☑
16:00	☑	☑	☑	☑	☑	☑	☑
17:00	☑	☑	☑	☑	☑	☑	☑
18:00	☑	☑	☑	☑	☑	☑	☑
19:00	☑	☑	☑	☑	☑	☑	☑
20:00	☑	☑	☑	☑	☑	☑	☑
21:00	☑	☑	☑	☑	☑	☑	☑
22:00	☑	☑	☑	☑	☑	☑	☑
23:00	☑	☑	☑	☑	☑	☑	☑

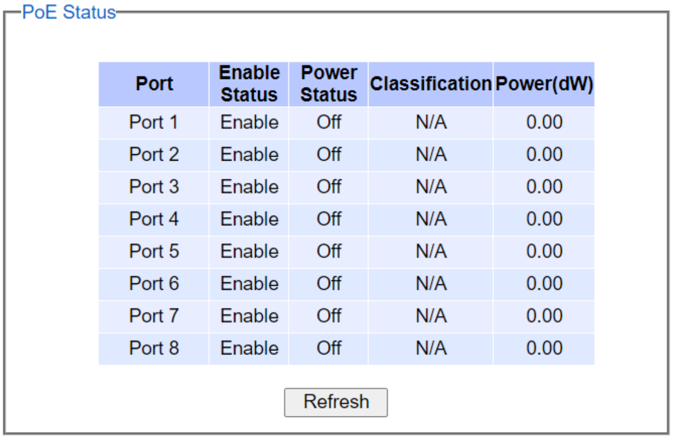
Figure 2.42 PoE Schedule Webpage with Example on EHG6510-8PoE-2SFP-D-24V

2.7.3 PoE Status

This webpage summarizes the status of each PoE port as shown in Figure 2.43. For instance, **Port4 can be** enabled and can supply power to a Class 4 Powered Device (PD) indicated under the **Classification** column. The total power consumption for a PD might be 15dW. To check the latest status of the PoE port, please click on the **Refresh** button. Table 2.17 provides descriptions of each column in the table of PoE Status.

Table 2.17 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	-
Power (dW)	Display the power supplied to this port in deciWatt	-



PoE Status

Port	Enable Status	Power Status	Classification	Power(dW)
Port 1	Enable	Off	N/A	0.00
Port 2	Enable	Off	N/A	0.00
Port 3	Enable	Off	N/A	0.00
Port 4	Enable	Off	N/A	0.00
Port 5	Enable	Off	N/A	0.00
Port 6	Enable	Off	N/A	0.00
Port 7	Enable	Off	N/A	0.00
Port 8	Enable	Off	N/A	0.00

Figure 2.43 PoE Status Webpage

2.8 Trunking

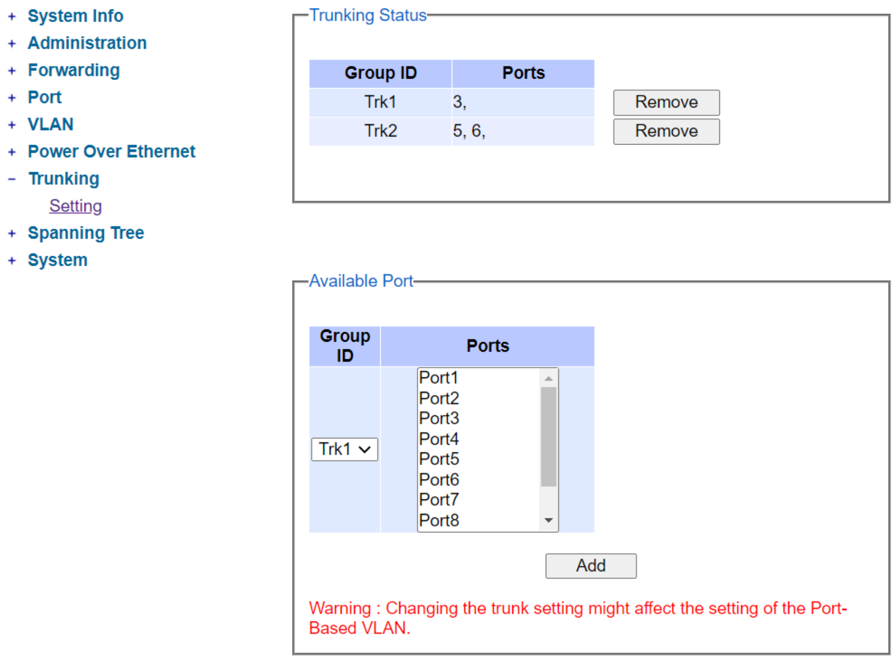
The managed switch supports Link Trunking, which allows one or more links to be combined together as a group of links to form a single logical link with larger capacity. The advantage of this function is that it gives the users more flexibility while setting up network connections. The bandwidth of a 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 2.44 shows the Trunking dropdown menu.

Figure 2.44 Trunking Dropdown Menu

2.8.1 Trunking Setting

In this subsection, the user can create new trunking assignment(s) and remove existing trunking assignment(s). Figure 2.45 illustrates the **Trunking Setting** webpage. The top part of the page called **Trunking Status** 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 from 1 to 5. The managed switch can support up to 5 trunk groups. Note that for the difference media types (for example Fast Ethernet, Gigabit Ethernet and

Fiber), port trunking needs to be combined separately. There is a section called **Available Port** for creating trunking as shown in the lower part of the webpage.



Group ID	Ports
Trk1	3,
Trk2	5, 6,

Group ID	Ports
Trk1	Port1 Port2 Port3 Port4 Port5 Port6 Port7 Port8

Warning : Changing the trunk setting might affect the setting of the Port-Based VLAN.

Figure 2.45 Trunking Setting Webpage with Example on EHG6510-8PoE-2SFP-24V

Descriptions of trunking settings are summarized in Table 2.18.

Table 2.18 Descriptions of Trunking Settings

Label	Description
Group ID	Up to 5 trunk groups can be created: Trk1~Trk5. Note that it is not possible to mix Fast Ethernet ports and Gigabit Ethernet ports into the same trunk group.
Ports	Specify the member ports for this trunking group. Please hold **Ctrl** (control) key to select more than one port at a time.
Add	Click **Add** button to confirm the changes.
Remove	Click this button to remove any existing trunking group.

2.9 Spanning Tree

IEEE 802.1D Standard spanning tree functionality is supported by Atop'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, Atop's managed switches deploy spanning tree as a tool when the users set up connection or port redundancy or fault-tolerance in their network.

RSTP (**R**apid **S**panning **T**ree **P**rotocol), IEEE 802.1W then superseded by IEEE 802.1D-2004, is also supported in ATOP'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 listening state, and exchanging a handshake between two switches to quickly transition the port to forwarding state.

This section describes how to setup the spanning tree protocol (STP), rapid spanning tree protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). Figure 2.46 depicts the dropdown menu for Spanning Tree.

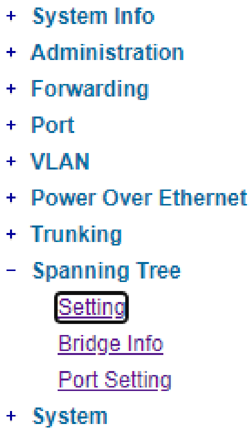
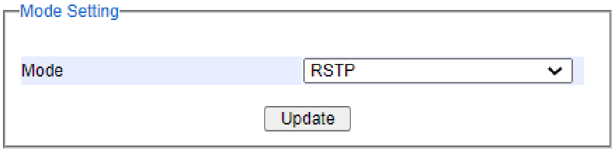


Figure 2.46 Spanning Tree Dropdown Menu

2.9.1 Spanning Tree Setting

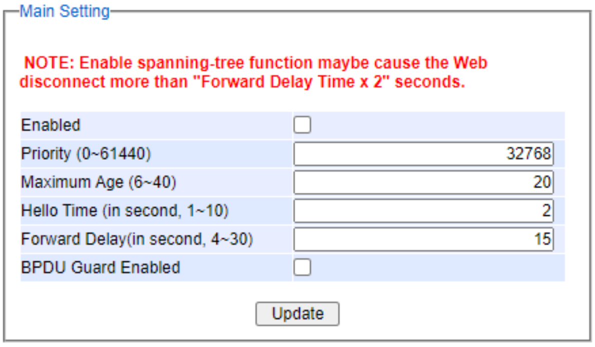
The users can select the spanning tree mode which are based on different spanning tree protocols in this webpage. Figure 2.47 shows the mode setting for spanning tree. There are one spanning tree modes to choose from the dropdown menu, which is rapid spanning tree protocol (RSTP). After choosing the desired mode, please click **Update** button to allow the change to take effect.



Mode: RSTP

Figure 2.47 Spanning Tree Mode Setting

Under the mode setting, there is a box for Main Setting of spanning tree's parameters as showed in Figure 2.48. 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**. Additonally, the BPDU Guard option can also be enabled by checking the box behind the **BPDU Guard Enabled**. Note that the Bridge Protocol Data Unit (BPDU) guard feature can be enabled to protect spanning tree protocol (RSTP) topology from BPDU related attacks. 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 2.19.



NOTE: Enable spanning-tree function maybe cause the Web disconnect more than "Forward Delay Time x 2" seconds.

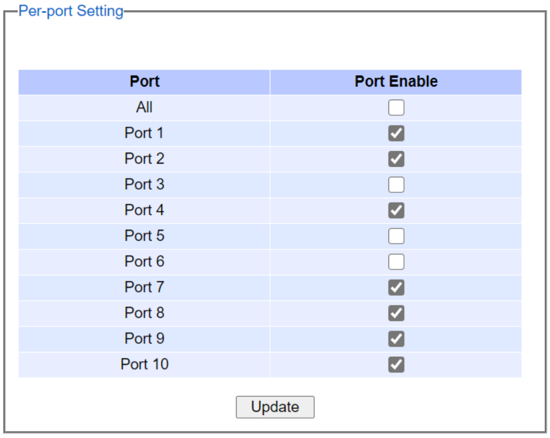
Enabled	□
Priority (0~61440)	32768
Maximum Age (6~40)	20
Hello Time (in second, 1~10)	2
Forward Delay(in second, 4~30)	15
BPDU Guard Enabled	□

Figure 2.48 Spanning Tree Main Setting for RSTP

Table 2.19 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
BPDU Guard Enabled	Check the box to enable BPDU (Bridge Protocol Data Unit) guard	Disable

The bottom part of the Spanning Tree Setting is the Per-port setting as shown in Figure 2.49. 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 on the per-port setting, please click on the **Update** button to update the change on the managed switch.



Per-port Setting

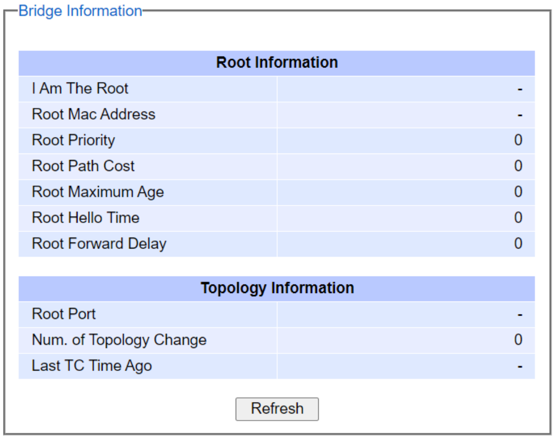
Port	Port Enable
All	□
Port 1	☑
Port 2	☑
Port 3	□
Port 4	☑
Port 5	□
Port 6	□
Port 7	☑
Port 8	☑
Port 9	☑
Port 10	☑

Figure 2.49 Spanning Tree Per-port Setting for RSTP

2.9.2 *Bridge Info*

Bridge Info (information) provides the statistical value of spanning tree protocol as shown in Figure 2.50. The information is further divided into two parts: Root Information and Topology Information. To check the latest information, please click on the **Refresh** button.

Table 20 and Table 21 summarize the descriptions of each entry in the root information table and topology information table, respectively.



Bridge Information

Root Information	
I Am The Root	-
Root Mac Address	-
Root Priority	0
Root Path Cost	0
Root Maximum Age	0
Root Hello Time	0
Root Forward Delay	0

Topology Information	
Root Port	-
Num. of Topology Change	0
Last TC Time Ago	-

Figure 2.50 Bridge Information Webpage

Table 2.20 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	-

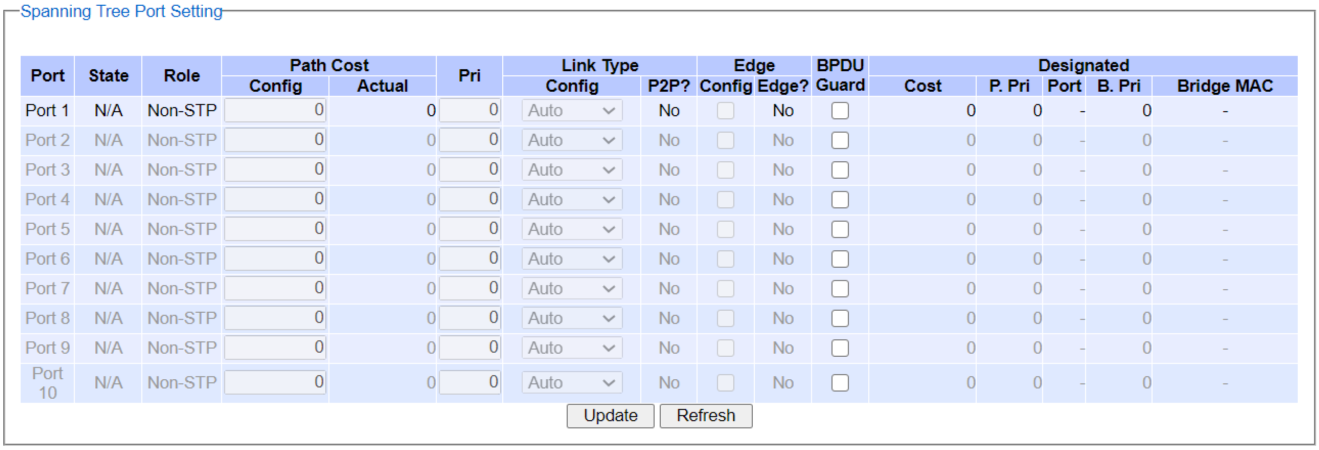
Label	Description	Factory Default
Root Priority	Root’s priority value: The switch with highest priority has the lowest priority value and it will be elected as the root of the spanning tree.	0
Root Path Cost	Roo’s path cost is calculated from the switch’s port data rate.	0
Root Maximum Age	Root’s maximum 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 in learning and listening states before a link begins forwarding.	0

Table 2.21 Bridge Topology Information

Label	Description	Factory Default
Root Port	A forwarding port that is the best 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.	-

2.9.3 Port Setting

Spanning Tree Port Setting shows the configured value of spanning tree protocol for each port, as shown in Figure 2.51. 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 2.22 summarizes the descriptions of spanning three port setting. If Spanning Tree is enabled, the table below will become editable. Use the **Update** button to save the settings.



Spanning Tree Port Setting

Port	State	Role	Path Cost		Pri	Link Type		Edge		BPDU	Designated				
			Config	Actual		Config	P2P?	Config	Edge?	Guard	Cost	P. Pri	Port	B. Pri	Bridge MAC
Port 1	N/A	Non-STP	0	0	0	Auto	No	☐	No	☐	0	0	-	0	-
Port 2	N/A	Non-STP	0	0	0	Auto	No	☐	No	☐	0	0	-	0	-
Port 3	N/A	Non-STP	0	0	0	Auto	No	☐	No	☐	0	0	-	0	-
Port 4	N/A	Non-STP	0	0	0	Auto	No	☐	No	☐	0	0	-	0	-
Port 5	N/A	Non-STP	0	0	0	Auto	No	☐	No	☐	0	0	-	0	-
Port 6	N/A	Non-STP	0	0	0	Auto	No	☐	No	☐	0	0	-	0	-
Port 7	N/A	Non-STP	0	0	0	Auto	No	☐	No	☐	0	0	-	0	-
Port 8	N/A	Non-STP	0	0	0	Auto	No	☐	No	☐	0	0	-	0	-
Port 9	N/A	Non-STP	0	0	0	Auto	No	☐	No	☐	0	0	-	0	-
Port 10	N/A	Non-STP	0	0	0	Auto	No	☐	No	☐	0	0	-	0	-

Figure 2.51 Spanning Tree Port Setting Webpage

Table 2.22 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 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.	Non-STP
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 **錯誤! 找不到參照來源。**.)	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
		The connection between two or more switches (for RSTP)	

Link Type	**Config**	Setting of the Link Type **P2P:** A port that operates in full-duplex mode is assumed to be point-to-point 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
BPDU Guard		BPDU Guard is set: **Yes** or **No**	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 2.23 lists the default values of path cost for RSTP.

Table 2.23 Default Path Cost for RSTP

Data Rate	**RSTP Cost (802.1W-2004)**
4 Mbits/s	5,000,000
10 Mbits/s	2,000,000
16 Mbits/s	1,250,000
100 Mbits/s	200,000
1 Gbits/s	20,000
2 Gbits/s	10,000
10 Gbits/s	2,000

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

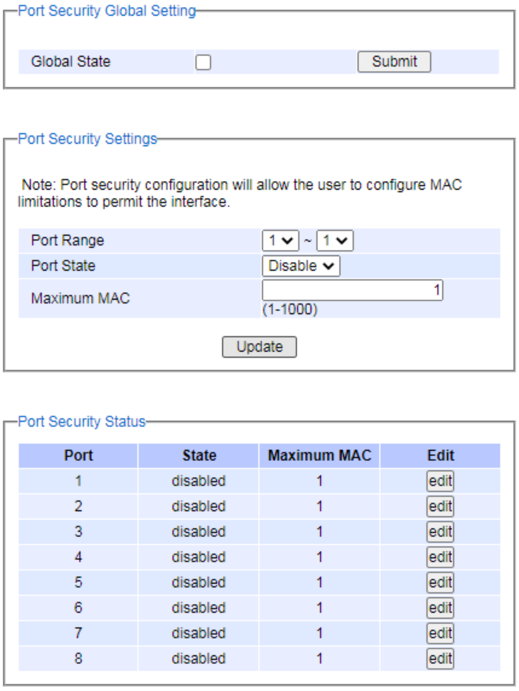
- Lowest root bridge ID determines the root bridge.
- Lowest cost to the root bridge favors the upstream switch with the least cost to root.
- Lowest sender bridge ID serves as a tie breaker if multiple upstream switches have equal cost to root.
- Lowest sender port ID serves as a tie breaker if a switch 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.

2.10 Security

2.10.1 Port Security

The switch receives the MAC address of a device that is connected to a specific port direction and allows data forwarding. The functions of the switch allow control over which and how many devices may be connected to a switch port. The “Port Security” functions can specify the maximum number of MAC addresses per interface. If this number is exceeded, incoming packets with new MAC addresses are dropped. A MAC address table can be used to check this. The static MAC addresses are included for this limit. Figure 2.52 shows the webpage fir port security settings.



Port Security Global Setting

Global State □ Submit

Port Security Settings

Note: Port security configuration will allow the user to configure MAC limitations to permit the interface.

Port Range	1 ~ 1
Port State	Disable
Maximum MAC	1 (1-1000)

Update

Port Security Status

Port	State	Maximum MAC	Edit
1	disabled	1	edit
2	disabled	1	edit
3	disabled	1	edit
4	disabled	1	edit
5	disabled	1	edit
6	disabled	1	edit
7	disabled	1	edit
8	disabled	1	edit

Figure 2.52 Port Security Webpage

Table 2.24 Descriptions of Port Security

Label	Description	Factory Default
Port Security Global Settings		
Global State	Enable/Disable port security feature	Uncheck
Port Security Settings		
Port Range	Select a port or port range in the selection box for which you want to configure the port security setting	1~1
Port State	Enable/Disable port security for a port or port range	Disable
Maximum MAC	User can enter maximum number of MAC addresses per interface	1
Port Security Status		
Port	This column shows the port numbers	1~8
State	This field indicates whether port security is enabled or disabled	disabled
Maximum MAC	This column displays the maximum number of MAC addressed	1
Edit	Preselection for editing	edit

2.10.2 802.1X

802.1X 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 2.53): 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 EHG65xx 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 2.53 shows a diagram of RADIUS authentication sequence.

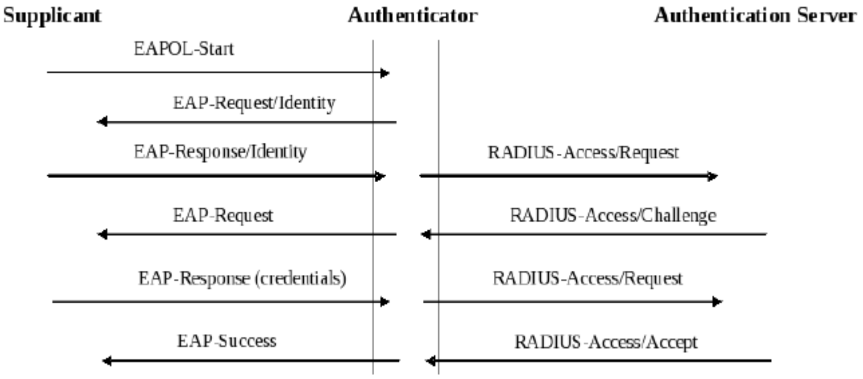
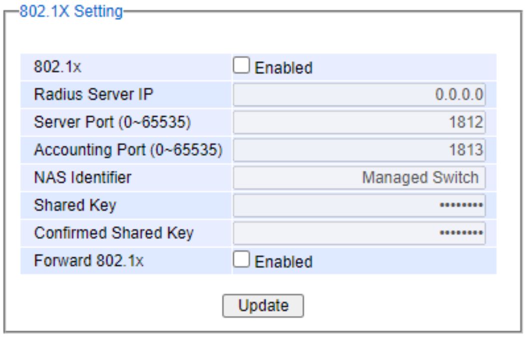


Figure 2.53 RADIUS Authentication Sequence

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

2.8.2.1 Setting

The 802.1X security mechanism can be enabled in this webpage as shown in Figure 2.54. 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, shared key and confirmed shared key. Additionally, the Forward 802.1x option can also be enabled in the last field. Summary of 802.1X Setting options are given in **錯誤! 找不到參照來源**。2.25. After changing all the required fields, please click on the **Update** button.



802.1X Setting

802.1x	☐ Enabled
Radius Server IP	0.0.0.0
Server Port (0~65535)	1812
Accounting Port (0~65535)	1813
NAS Identifier	Managed Switch
Shared Key	••••••••
Confirmed Shared Key	••••••••
Forward 802.1x	☐ Enabled

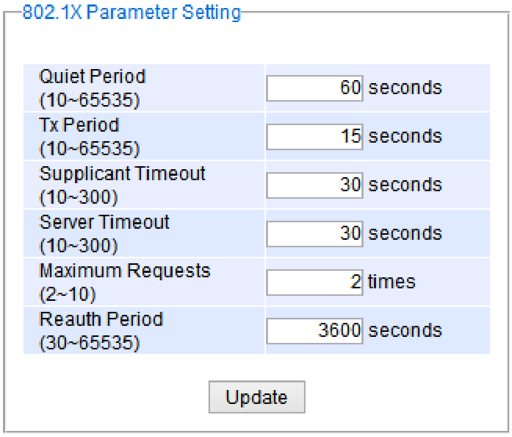
Figure 2.54 802.1X Setting Webpage

Table 2.25 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
Forward 802.1x	Choose whether to enable forwarding of 802.1x	Disable

2.8.2.2 Parameters Setting

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 2.55. These parameters are related to the authentication periods or timeout durations and maximum number of authentication requests. Table 2.26 summarizes the descriptions of these parameters and their default setting. Please clicking on the Update button after the users changed any of the parameters.



802.1X Parameter Setting

Quiet Period (10~65535)	60 seconds
Tx Period (10~65535)	15 seconds
Supplicant Timeout (10~300)	30 seconds
Server Timeout (10~300)	30 seconds
Maximum Requests (2~10)	2 times
Reauth Period (30~65535)	3600 seconds

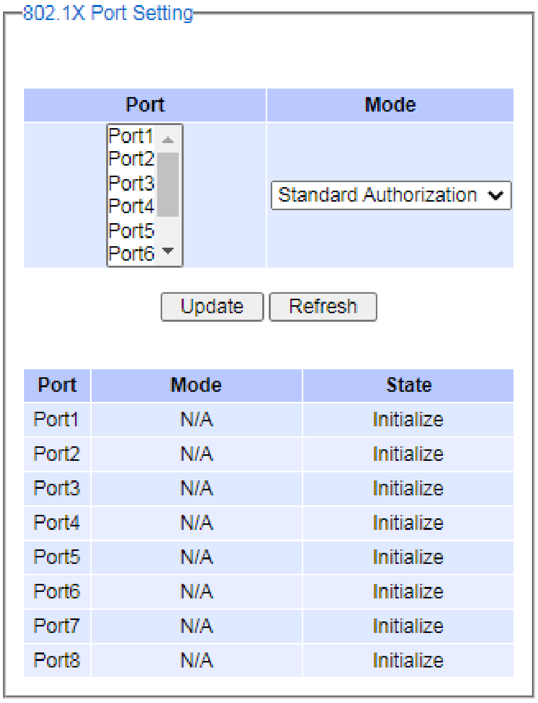
Figure 2.55 802.1X's Parameters Setting Webpage

Table 2.26 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

2.8.2.3 Port Setting

The user can individually configure 802.1x security mechanism on each port of the EHG7XXX managed switch as shown in Figure 2.56. 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 2.27. The lower part of 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.



802.1X Port Setting

Port	Mode
Port1 Port2 Port3 Port4 Port5 Port6	Standard Authorization

Port	Mode	State
Port1	N/A	Initialize
Port2	N/A	Initialize
Port3	N/A	Initialize
Port4	N/A	Initialize
Port5	N/A	Initialize
Port6	N/A	Initialize
Port7	N/A	Initialize
Port8	N/A	Initialize

Figure 2.56 802.1x Port Setting Webpage

Table 2.27 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

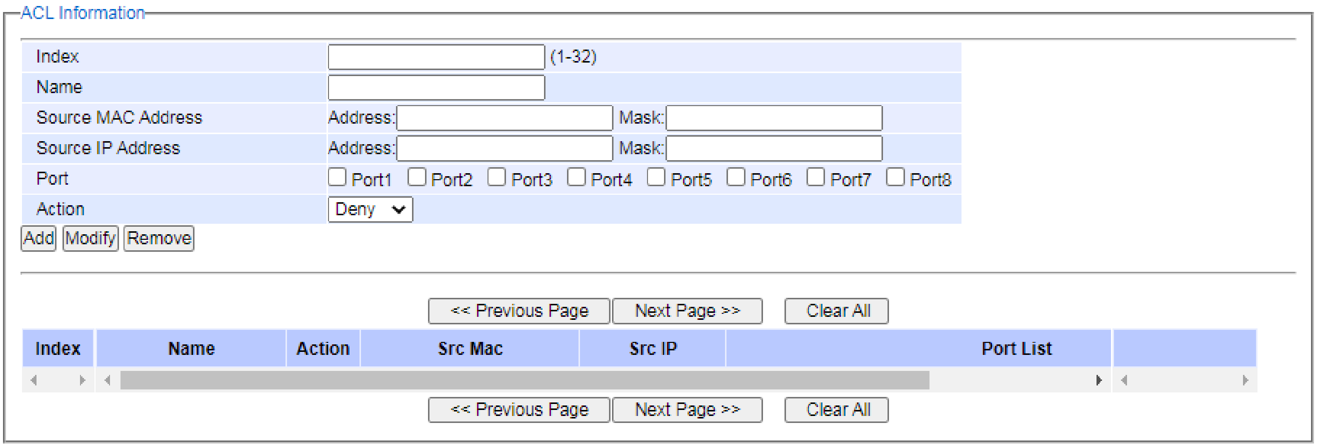
2.10.3 ACL

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.

The numbers of matching rules can be at most 32. However, the main important rules that are mostly exercise are follows. Rules for filtering includes Source MAC address and Source IP address. 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 2.31. To differentiate between each ACL entry, Index number from 1 to 32 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.

錯誤! 找不到參照來源。2.28 describes definition of each in details. Here note that if any field is empty, that ACL entry will be ignored.



ACL Information

Index	(1-32)
Name	
Source MAC Address	Address: Mask:
Source IP Address	Address: Mask:
Port	□ Port1 □ Port2 □ Port3 □ Port4 □ Port5 □ Port6 □ Port7 □ Port8
Action	Deny

Index	Name	Action	Src Mac	Src IP	Port List

Figure 2.57 Security Access Control List Information Webpage

Table 2.28 Descriptions of ACL Entries for in ACL Webpage

ACL Entry	Definition	Range
Index	ACL priority	Priority (1-32)
Name	ACL rule name	Max length 32
Source MAC Address	MAC address are the fields of 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.
Source IP Address	IP Addresses are the fields of the IPv4 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, then this condition is always accepted. If the Mask is empty, it is considered equal to the Mask of

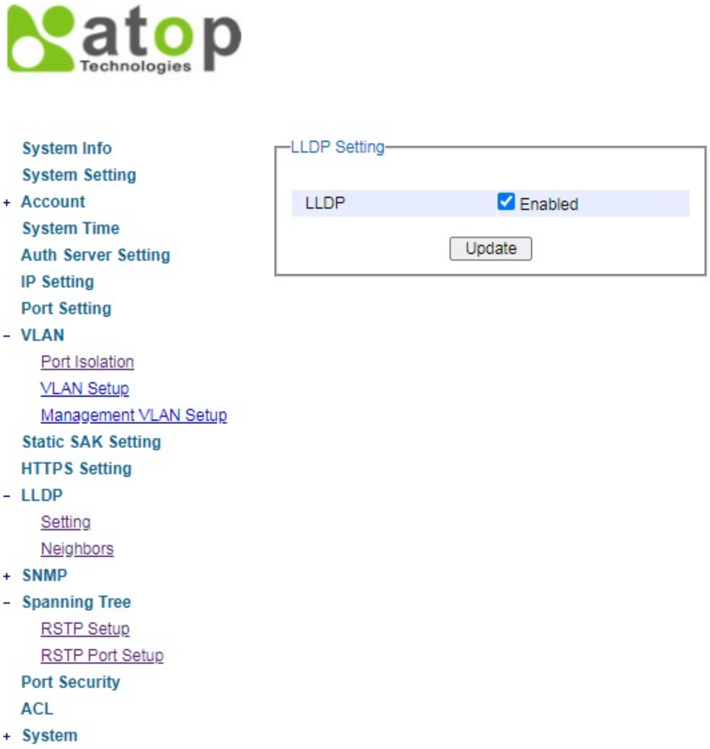
		255.255.255.255 and all of bits in the IP Address are compared.
Port	DUT's port number	1~8
Action	Configure rule to Deny or Permit	Deny / Permit

2.11 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 2.58.

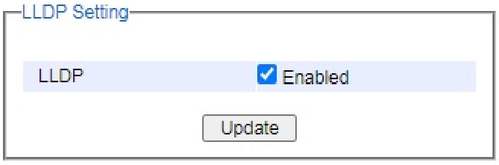


LLDP ☑ Enabled

Figure 2.58 LLDP Dropdown Menu

2.11.1 Setting

In Figure 2.59, 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 Atop's Device Management Utility (formerly called Device View) to monitor the switches' topology of all LLDP devices in the network.



LLDP Setting

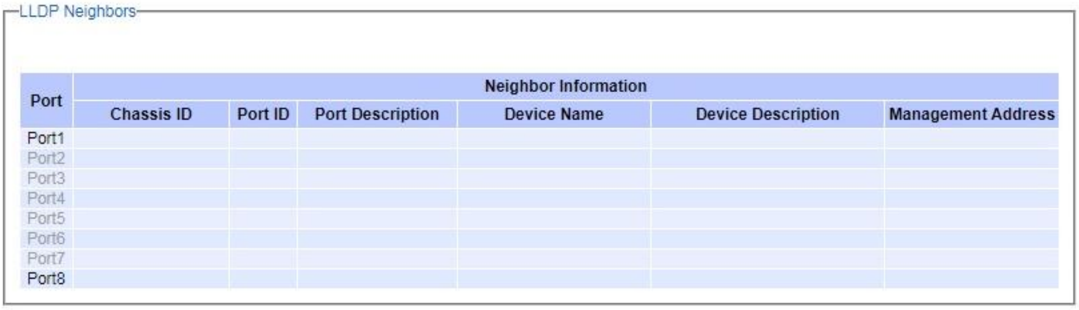
LLDP ☑ Enabled

Figure 2.59 LLDP Setting Webpage

2.11.2 Neighbors

This menu allows the user to view the LLDP's neighbor information of the managed switch as shown in Figure 2.60. 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.

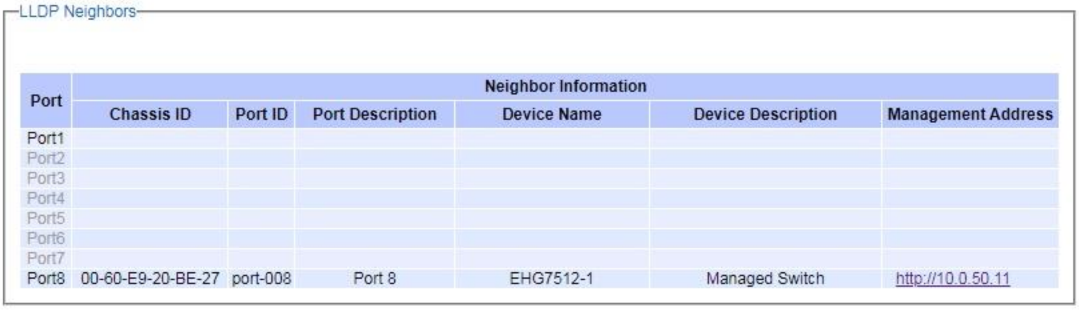
An example of neighbor information table is depicted in Figure 2.61. Note that this example is based on a display format EHG75XX managed switch in which System Name is changed to Device Name and System Description is changed to Device Description in the latest version of EHG75XX's firmware.



LLDP Neighbors

Port	Neighbor Information					
	Chassis ID	Port ID	Port Description	Device Name	Device Description	Management Address
Port1						
Port2						
Port3						
Port4						
Port5						
Port6						
Port7						
Port8						

Figure 2.60 LLDP Neighbors Webpage



LLDP Neighbors

Port	Neighbor Information					
	Chassis ID	Port ID	Port Description	Device Name	Device Description	Management Address
Port1						
Port2						
Port3						
Port4						
Port5						
Port6						
Port7						
Port8	00-60-E9-20-BE-27	port-008	Port 8	EHG7512-1	Managed Switch	http://10.0.50.11

Figure 2.61 Example of LLDP Neighbors Webpage

Table 2.29 Descriptions of LLDP Neighbors Webpage

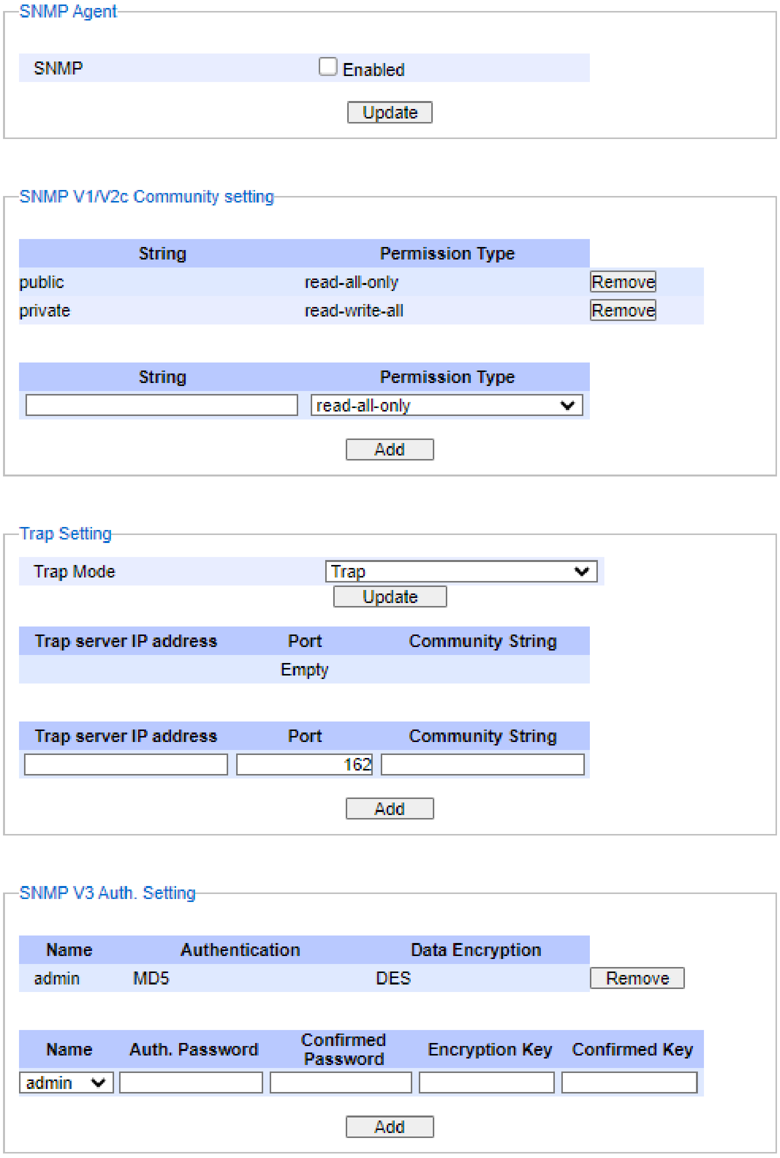
Label	Description

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.

2.12 SNMP

The SNMP ("Simple Network Management Protocol") is used in network management systems to monitor the state of attached devices that require the attention of an administrator. SNMP is a component of the "internet protocol suite" defined by the IETF ("Internet Engineering Task Force"). It consists of a set of standards for network management, including an application layer protocol, a database schema and a set of data objects. SNMP provides management data in the form of variables on the managed systems, which describe the system configuration. These variables can be queried (and sometimes changed) by managing applications. An "SNMP community string" is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (the SNMP manager) and the device (the SNMP agent). The string is included in every packet transmitted between the SNMP manager and the SNMP agent. The "SNMP community" acts like a password and is used to define the security parameters of SNMP clients in an SNMP v1 and SNMP v2c environments. The default "SNMP community" is "public" for both SNMPv1 and SNMPv2c before SNMPv3 is enabled. Once SNMPv3 is enabled, the "Communities" of SNMPv1 and v2c have to be unique and cannot be shared.

ATOP industrial managed switch support SNMP and can be configured in this tab page as shown in Figure 2.62. The SNMP setting has four parts, which are:
- SNMP Agent
- SNMP V1/V2c Community setting
- Trap Setting
- SNMP V3 Auth. Setting



SNMP Agent

SNMP	□ Enabled

SNMP V1/V2c Community setting

String	Permission Type	
public	read-all-only	Remove
private	read-write-all	Remove

String	Permission Type
	read-all-only

Trap Setting

Trap Mode	Trap

Trap server IP address	Port	Community String
	Empty	

Trap server IP address	Port	Community String
	162	

SNMP V3 Auth. Setting

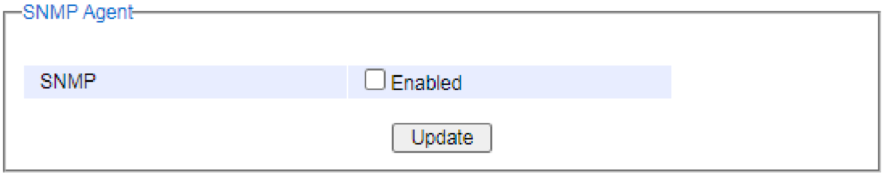
Name	Authentication	Data Encryption	
admin	MD5	DES	Remove

Name	Auth. Password	Confirmed Password	Encryption Key	Confirmed Key
admin				

Figure 2.62 SNMP Settings Webpage

2.12.1 SNMP Agent

To enable SNMP agent on the managed switch, please check the **Enabled** box and click **Update** button as shown in Figure 2.63**.** The SNMP version 1 (V1), version 2c (V2c) and version 3 are supported by managed switches. 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**.**



SNMP Agent

SNMP □ Enabled

Figure 2.63 SNMP Enabling Box

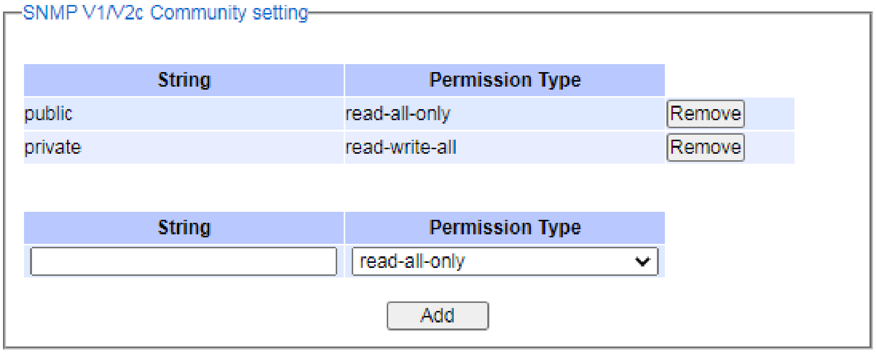
Table 2.30 Descriptions of SNMP Setting

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

2.12.2 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 EHG65XX, which are read-all-only or read-write-all. For example, in our default setting as shown in Figure 2.64, 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 2.64 briefly provides descriptions of SNMP's community string setting.



SNMP V1/V2c Community setting

String	Permission Type	
public	read-all-only	Remove
private	read-write-all	Remove

String	Permission Type
	read-all-only

Figure 2.64 SNMP Community Strings

Table 2.31 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.	-

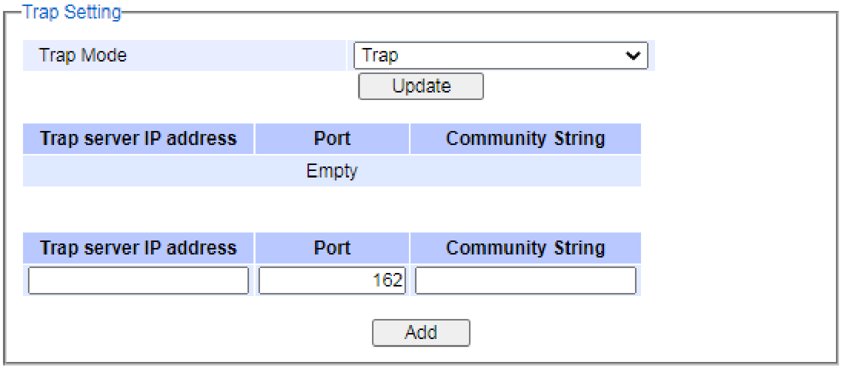
***NOTE:**

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

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

2.12.3 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 cold 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 2.65 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 2.32 summarizes the descriptions of trap receiver settings.


Trap Setting

Trap Mode: Trap

Trap server IP address	Port	Community String
Empty		

Trap server IP address	Port	Community String
	162	

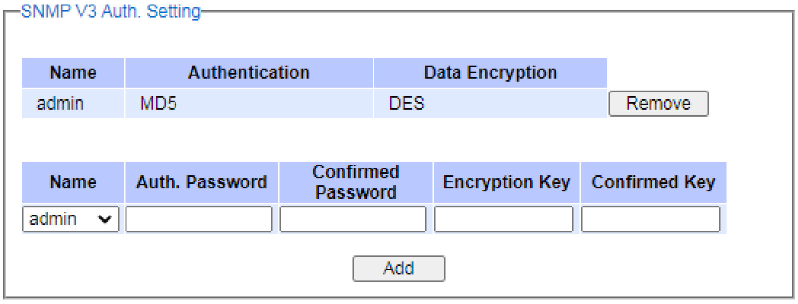
Figure 2.65 Example of Trap Receiver Setting

Table 2.32 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

2.12.4 SNMP V3 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 2.66 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 2.33 lists the descriptions of SNMP V3 settings.



SNMP V3 Auth. Setting

Name	Authentication	Data Encryption	
admin	MD5	DES	Remove

Name	Auth. Password	Confirmed Password	Encryption Key	Confirmed Key
admin				

Figure 2.66 SNMPv3 Users' Options

Table 2.33 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

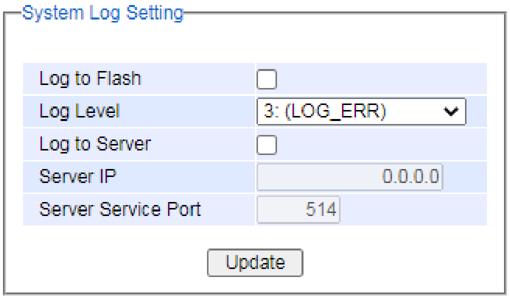
2.13 System

2.13.1 System Log

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

2.13.1.1 Setting

Figure 2.67 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 saved 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. **錯誤! 找不到參照來源。**2.34 describes the details of parameters setting for the system log.



System Log Setting

Log to Flash	□
Log Level	3: (LOG_ERR)
Log to Server	□
Server IP	0.0.0.0
Server Service Port	514

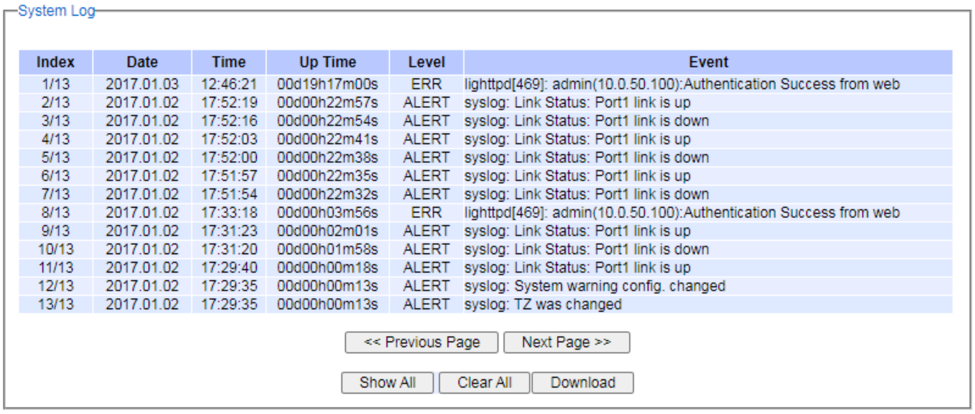
Figure 2.67 System Log Setting Webpage

Table 2.34 Descriptions of System Log Settings

Label	Description	Factory Default
Log 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 Log to 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
Server IP	Set the IP address of Syslog server	0.0.0.0
Server Service Port	Set the service port number of System Log server. Range from Port 1 to Port 65535.	514

2.13.1.2 Log

Figure 2.67 shows an example of all of the event's logs. Note that they are sorted by date and time. 錯誤! 找不到參照來源。 provides explanation of each column and the button's functions on the System Log webpage.



System Log

Index	Date	Time	Up Time	Level	Event
1/13	2017.01.03	12:46:21	00d19h17m00s	ERR	lighttpd[469]: admin(10.0.50.100):Authentication Success from web
2/13	2017.01.02	17:52:19	00d00h22m57s	ALERT	syslog: Link Status: Port1 link is up
3/13	2017.01.02	17:52:16	00d00h22m54s	ALERT	syslog: Link Status: Port1 link is down
4/13	2017.01.02	17:52:03	00d00h22m41s	ALERT	syslog: Link Status: Port1 link is up
5/13	2017.01.02	17:52:00	00d00h22m38s	ALERT	syslog: Link Status: Port1 link is down
6/13	2017.01.02	17:51:57	00d00h22m35s	ALERT	syslog: Link Status: Port1 link is up
7/13	2017.01.02	17:51:54	00d00h22m32s	ALERT	syslog: Link Status: Port1 link is down
8/13	2017.01.02	17:33:18	00d00h03m56s	ERR	lighttpd[469]: admin(10.0.50.100):Authentication Success from web
9/13	2017.01.02	17:31:23	00d00h02m01s	ALERT	syslog: Link Status: Port1 link is up
10/13	2017.01.02	17:31:20	00d00h01m58s	ALERT	syslog: Link Status: Port1 link is down
11/13	2017.01.02	17:29:40	00d00h00m18s	ALERT	syslog: Link Status: Port1 link is up
12/13	2017.01.02	17:29:35	00d00h00m13s	ALERT	syslog: System warning config. changed
13/13	2017.01.02	17:29:35	00d00h00m13s	ALERT	syslog: TZ was changed

Figure 2.68 Event Log Webpage

Table 2.35 Descriptions of Event Log

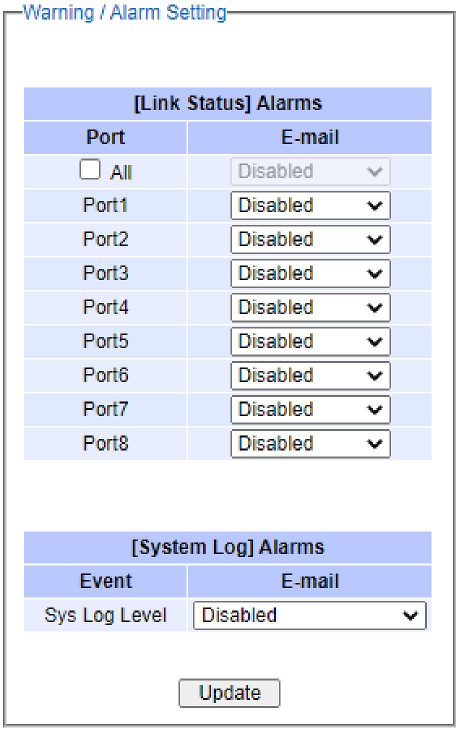
Label	Description
Index	Indicate the index of a particular log event
Date	Indicate the system date of the occurred event
Time	Indicate the time stamp that this event occurred
Up Time	Indicate how long the system (managed switch) has been up since this event occurred.
Level	Indicate the level of this 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

2.13.2 Warning/Alarm

The warning/alarm section consists of three subsections: **Setting**, **SMTP Setting**, and **Log**.

2.13.2.1 Settings

There are two different types of Warning or Alarm: Link Status Alarms and System Log Alarms as shown in Figure 2.69. The Link Status Alarms are related to the activities of particular port(s). 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 alarm mail to users. After finish configuring the alarms, please click the **Update** button.



Warning / Alarm Setting

[Link Status] Alarms	
Port	E-mail
□ All	Disabled
Port1	Disabled
Port2	Disabled
Port3	Disabled
Port4	Disabled
Port5	Disabled
Port6	Disabled
Port7	Disabled
Port8	Disabled

[System Log] Alarms	
Event	E-mail
Sys Log Level	Disabled

Figure 2.69 Webpage of Warning Event Selection

In Link Status Alarms, DUT can send notifications via **E-mail** in case if Link is UP, Link is Down, or Link is UP/DOWN**.** **錯誤! 找不到參照來源。**2.36 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 2.36 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 System Log Alarms, the users also can send notifications via **E-mail. 錯誤! 找不到參照來源。**2.37 describes the System Log Level which can be selected for the System Log Alarm event notification**.**

Table 2.37 Descriptions of System Log Alarm Event Selection

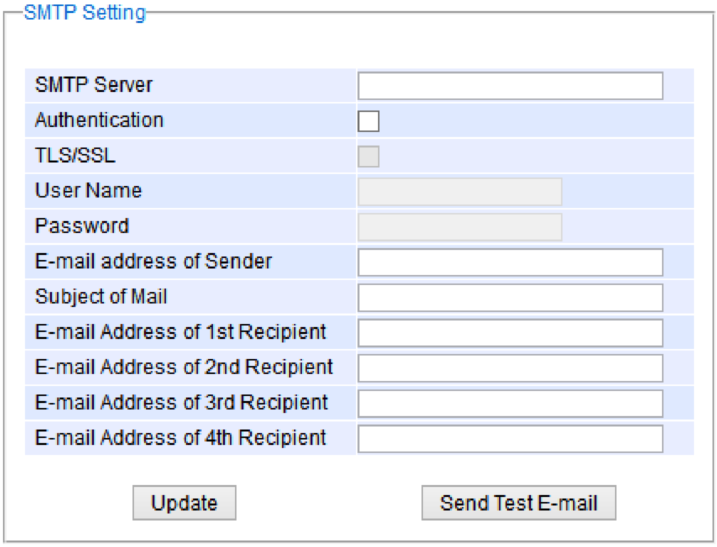
Label	Description	Factory Default
System log event	Disable**:** Disable power status detection. 0**: (LOG_EMERG):** Enable log level 0~7 detection. 1**: (LOG_ALERT):** Enable log level 1~7 detection. 2**: (LOG_CRIT):** Enable log level 2~7 detection. 3**: (LOG_ERR):** Enable log level 3~7 detection. 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

2.13.2.2 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 2.12.1.1, 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 and System Log), as shown in Figure 2.70.

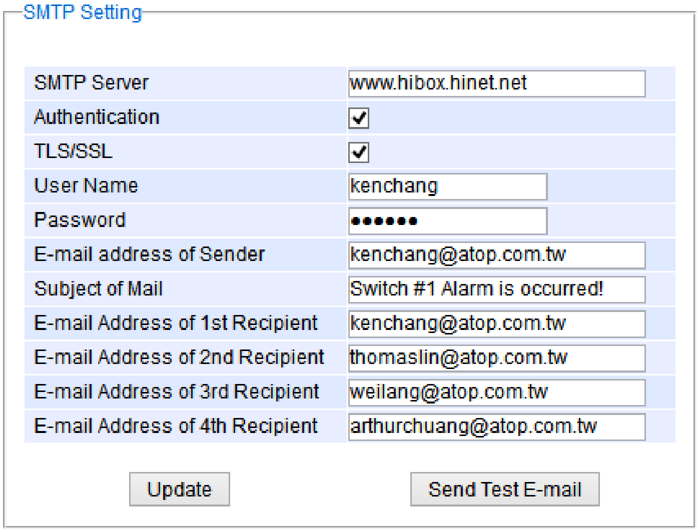


SMTP Setting

SMTP Server	
Authentication	□
TLS/SSL	□
User Name	
Password	
E-mail address of Sender	
Subject of Mail	
E-mail Address of 1st Recipient	
E-mail Address of 2nd Recipient	
E-mail Address of 3rd Recipient	
E-mail Address of 4th Recipient	

Figure 2.70 SMTP Setting Webpage

An example of SMTP Setting is shown in Figure **錯誤! 找不到參照來源**。2.71. 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 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 2.38.



SMTP Setting

SMTP Server	www.hibox.hinet.net
Authentication	☑
TLS/SSL	☑
User Name	kenchang
Password	••••••
E-mail address of Sender	kenchang@atop.com.tw
Subject of Mail	Switch #1 Alarm is occurred!
E-mail Address of 1st Recipient	kenchang@atop.com.tw
E-mail Address of 2nd Recipient	thomaslin@atop.com.tw
E-mail Address of 3rd Recipient	weilang@atop.com.tw
E-mail Address of 4th Recipient	arthurchuang@atop.com.tw

Figure 2.71 Example of SMTP Setting

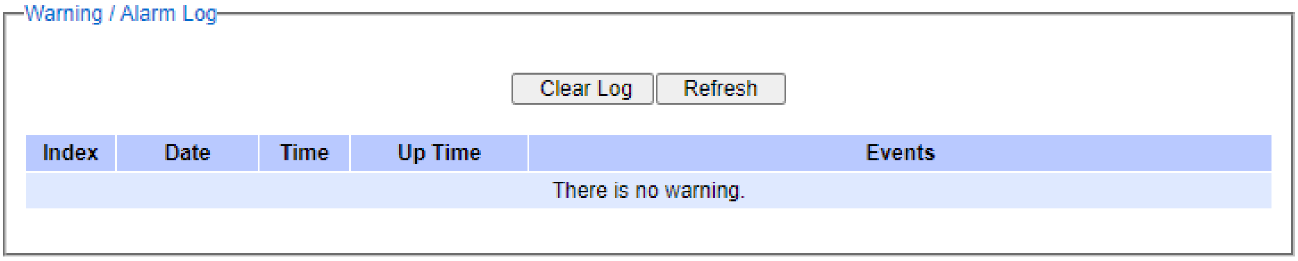
Table 2.38 Descriptions of SMTP Setting

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 char.	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	Send a test email to recipient(s) above to check accuracy.	-

2.13.2.3 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 2.72. At the top of the table, the users can 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.



Index	Date	Time	Up Time	Events
There is no warning.				

Figure 2.72 Warning/Alarm Log Webpage

Table 2.39 Descriptions of Warning / Alarm Log

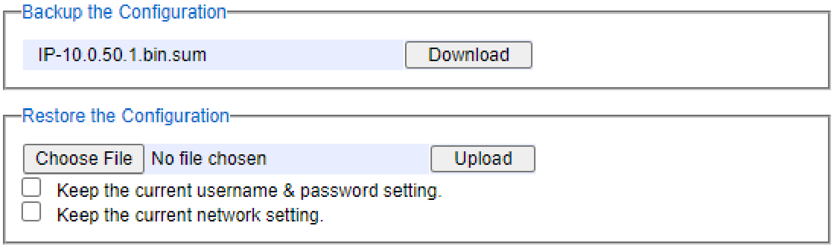
Label	Description
Clear Log	Clears all warning events that are displayed.
Refresh	Obtain the latest Warning / Alarm events
Index	Display the index of the Warning/Alarm events as an entry number over a total number of events
Date	The date that the alarm/event occurred.

Time	The time that the alarm/event occurred.
Up Time	The duration of time since the start up time of the switch until the alarm/event occurred.
Events	Description of the alarm events

2.13.3 Backup / Restore Config.

In **Backup/ Restore Config** function, the current configuration of the EHG6510 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 EHG6510 switch. It will replace the current configuration.
Figure 2.73 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.sum” by an application or to **Save File** to a destination. Choosing to Save File will 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.



Backup the Configuration

IP-10.0.50.1.bin.sum

Restore the Configuration

No file chosen

□ Keep the current username & password setting.
□ Keep the current network setting.

Figure 2.73 Backup/Restore Configuration via HTTP

2.13.4 Firmware Update

The users can update the device firmware via web interface as shown in Figure 2.74 To update the firmware, the users can download a new firmware from Atop’s website and save it in a local computer. Then, the users can click “**Choose File”** button and choose the firmware file that is already downloaded. The switch’s firmware typically has a “.dld” extension such as EHG6510-K317.dld. After that, the users can click **Update** button and wait for the update process to be done.

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

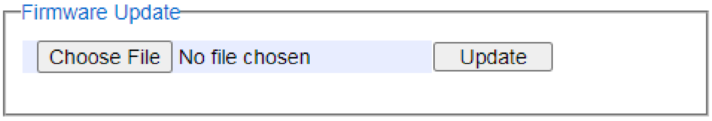
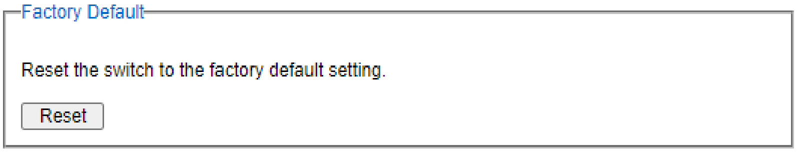


Figure 2.74 Firmware Update Webpage

2.13.5 Factoty 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 2.75



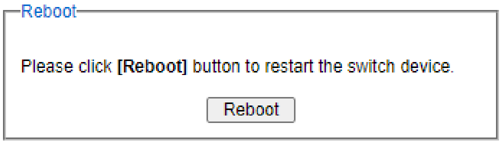
Factory Default

Reset the switch to the factory default setting.

Figure 2.75 Factory Default Setting Webpage

2.13.6 Reboot

An easy reboot function is provided in this webpage requiring only one single click on the **Reboot** button as shown in Figure 2.73.



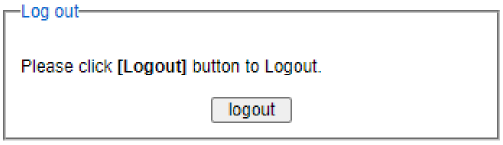
Reboot

Please click **[Reboot]** button to restart the switch device.

Figure 2.76 Reboot Webpage

2.13.7 Logout

An easy logout function is provided in this webpage requiring only one single click on the Logout button as shown in Figure 2.77.



Log out

Please click **[Logout]** button to Logout.

Figure 2.77 Logout Webpage

3 Configuring with Telnet

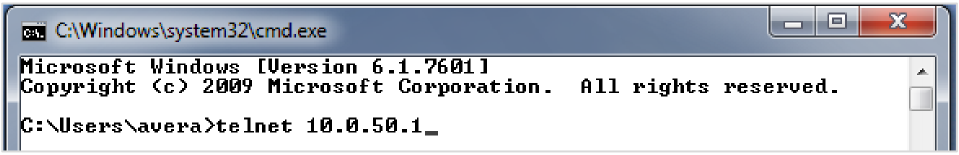
An alternative configuration method is the Telnet method and it is described in this chapter.

3.1 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). Note that only users with administrator (admin) access right as configured can use telnet to login to the device.

3.2 Telnet Log-in

After the command line terminal is opened, type in “telnet 10.0.50.1” as shown in Figure 3.1. 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.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\avera>telnet 10.0.50.1_
```

Figure 3.1 Telnet Command

Below are telnet login description :
Username ：admin
Password ：default
Mode of Operation: Three Mod of Operation

1. Privilege-Unprivileged Mode
2. Privilege Mode
3. Configuration Mode

- “disable” command is used to return or default privilege-unprivileged mode
- “enable” command is used to enters into privilege mode and password is “admin”
- “configure” command is used to enters the setting configuration mode

3.3 Command Line for Telnet

This chapter introduce EHG6510 command line descripton for Telnet. When users do not know the commands to use for the command line configuration, users can type in “?” and the commands are displayed.

Features Implemented List:

No	Feature	Settings	Show Command

1	Port Settings	Yes	Yes
2	Vlan Setup	Yes	Yes
3	Port Isolation	Yes	Yes
4	Management Vlan Setup	Yes	Yes
5	802.1x Setting	Yes	Yes
6	802.1x Parameter Settings	Yes	Yes
7	802.1x Port Settings	Yes	Yes
8	LLDP	Yes	Yes
9	SNTP	Yes	Yes
10	SNMP Setting	Yes	Yes
11	Network Settings	Yes	Yes
12	Port Mirror	Yes	Yes
13	ACL	Yes	Yes
14	RSTP	Yes	Yes
15	Modbus Settings	Yes	No
16	Systeminfo	No	Yes
17	Default Reset	Yes	No
18	System Reboot	Yes	No

Port Mirror CLI commands:

Node	Command	Description
Configure	# mirror-settings enable sourcePort 3 destPort 2	This command used to enable the “Port Mirroring” on the switch with source port and mirror destination port.
Configure	# mirror-settings disable	This command used to disable the mirror (Optional source port and destination port)
Show	# show mirror-status ----------- Port Mirror ----------- Port Mirror : Enabled Mode : BOTH_RxTx Source_Port : 3 Destination_port : 2 -----------------------------------	This command displays the current “Port Mirroring” configurations.

▪

Modbus Settings CLI commands:

Node	Command	Description
Configure	# modbus globalEnable	This command is used to set enable or disable the modbus
Configure	# modbus portValue 502	This command is used to set the modbus desire port number in the range of 1~65535.

Configure	# modbus address 33	This command is used to set modbus slave address
Show	# show modbusSettings Modbus Global State:Disabled Modbus Address:33 Modbus Port Number:502	This command displays the current Modbus Setting in the device

-

Port Setting CLI commands:

Node	Command	Description
Configure	# port-settings 3 enable	This command is used to enable the port with port number
Configure	# port-settings 3 disable	This command is used to disable the port with port number

Show	# show port-settings
	  Port | State
	----------+--------------
	    1 Enabled
	    2 Enabled
	    3 Enabled
	    4 Enabled
	    5 Enabled
	    6 Enabled
	    7 Enabled
	    8 Enabled
		This command displays the current port configurations.

-

Device Network Setting CLI commands:

Node	Command	Description
Configure Ip Settings	# ip staticIP address 10.0.50.1 netMask 255.255.0.0 gateway 10.0.50.254 primaryDNS 10.0.50.10	This command is used to set the device network ip address. Note: gateway and primaryDNS is optional parameter.
Configure dhcp	# ip dhcp enable	This command is used to enable or disable the dhcp feature in the device
Show	# show ip ------------- IP Setting ------------ DHCP : Disabled Static IP Address : 10.0.50.1 Subnet Mask : 255.255.0.0 Gateway : 10.0.50.254 Primary DNS : 10.0.50.10	This command used to view the current device network ip address configuration.

-
- LLDP Setting CLI commands:

Node	Command	Description

Configure	# lldp-globalActive enable	This command is used to enable or disable the LLDP for active global.
Show Active State	# show lldp_activeState LLDP Global State : enabled	This command used to show the active state LLDP
Show Neighbor	# show lldp_neighbor 1 LLDP Global State : Enabled ------- IIdp -> 1 ------ Port ID : 8C:16:45:C3:2B:2B Chassis ID : 8C-16-45-C3-2B-2B System Name : System Description: Management Address:	This command is used to view the LLDP Neighbor information passing with port number

-
- Port Security Setting CLI commands:

Node	Command	Description
Configure	# port-security globalActive enable	This command is used set Global enable/disable the port security feature.
Configure	# port-security settings 8 enable 1000 # port-security Settings 5 disable	This command used to set and enable/disable the individual port security functionality with desire MAC count 1 to 1000
Show	show port-security Port Security Global State:Enabled --------------------------------------- | Port | State | Maximum Mac --------------------------------------- 1 Disabled 1 2 Disabled 1 3 Disabled 1 4 Disabled 1 5 Disabled 1 6 Disabled 1 7 Disabled 1 8 Enabled 1000	This command used to view the current port security list of the device

-
- Vlan Setting CLI commands:

Node	Command	Description
Configure	# vlan-add access 4 6 # vlan-add trunk 7 1,2,4,6,7	This command is used to configure the port Vlan id & access role

Show	#show vlan-portBased
	  Port | Role | VLAN ID
	----------+----------------------
	   1 Access 1
	   2 Access 1
	   3 Access 1
	   4 Access 1
	   5 Access 1
	   6 Access 1
	   7 Trunk 1,2,4,6,7
	   8 Access 1
		This command is used to view the current setting of Vlan configuration.

configure	# port-isolation 3 egrs1 1 egrs2 2 egrs3 4 egrs6 7 egrs8 8	This command is used to set the source port isolation list of destination port. Example: Source Port : 3 Destination Port : 1 2 4 7 8
Show	# show port-isolation FW | Egress | Port | Port-1 Port-2 Port-3 Port-4 Port-5 Port-6 Port-7 Port-8 ----------+--- -------------- * 1 - V V V V V V V * 2 V - V V V V V V * 3 V V - V - - V V * 4 V V V - V V V V * 5 V V V V - V V V * 6 V V V V V - V V * 7 V V V V V V - V * 8 V V V V V V V -	This command is used to view the list of port isolation in the device.

-
- 802.1x Setting CLI commands:
-

Node	Command	Description
Configure	# 802.1X-settings enable 10.0.50.120 3456 567 Switch wago	This command is used set 802.1x Setting

<table>
<tr><td></td><td></td><td>Example:
Active Set = enable
Radius Server IP : 10.0.50.120
Server Port : 3456
Account Port: 567
NAS Identified: Switch
Shared Key: wago
Confirmed Key: wago</td></tr>
<tr><td>Show</td><td>#show 802.1X-settings
------------- 802.1X Settings ------------
802.1x : Enabled
Radius Server IP : 10.0.50.120
Server Port (0~65535) : 3456
Accounting Port (0~65535) : 567
NAS Identifier : Switch
Shared Key : wago</td><td>This command is used to view the current setting of 802.1x settings</td></tr>
<tr><td>Configure</td><td># 802.1X-parameter 120 20 100 40 5 3700</td><td>This command is used to set the 802.1x parameter setting:
Example:
Quiet Period: 120
Tx Period : 20
Supplication Timeout: 100
Server Timeout:40
Maximum Request : 5
Reauth Period : 3700</td></tr>
<tr><td>Show</td><td># show 802.1X-parameter
------------- 802.1X Parameter Settings ------------
Quiet Period(10~65535 : 120
Tx Period(10~65535) : 20
Supplicant Timeout (10~300): 100
Server Timeout (10~300) : 40
Maximum Requests (2~10) : 5
Reauth Period (30~65535) : 3700</td><td>This command is use to view the 802.1X parameter settings.</td></tr>
<tr><td>Configure</td><td># 802.1X-portSettings 3 std-auth</td><td>This command is used to configure 802.1x port authentication mode with respect to the port number.
Example:
Source Port: 3
Mode: std-auth
(na std-auth force-unAuth force-auth)</td></tr>
<tr><td>Show</td><td># show 802.1X-portSettings
+------------------------ 802.1X Port Settings -------
---------------+
| Port | Mode | State |</td><td>This command is used to view the 802.1x port settings mode list.</td></tr>
</table>

	+--- -----------+ N/A Initialize N/A Initialize Standard Authorization Initialize N/A Initialize N/A Initialize N/A Initialize N/A Initialize N/A Initialize	

-
- ACL Setting CLI commands:

Node	Command	Description
Configure	# acl-settings 4 wagoacl4 whitelist other 00:00:00:00:00:06 00:00:00:00:00:07 other 10.0.50.120 255.255.0.0 4	This command is used to configure the acl setting as example follows: Index :4 Profile Name: wagoacl4 Action: whitelist / blacklist /disable Select Mac Option: Any/Other Valid Mac Address: 00:00:00:00:00:06 Valid Mac Mask: 00:00:00:00:00:07 Select IP Option: Any/Other Valid IP Address: 10.0.50.120 2 Valid Mac Mask: 255.255.0.0 Source Port Number: 4
Show	# show acl-settings +---------------List 1---------------+ Index :4 Profile Name :wagoacl4 Action :whitelist Source Mac :00:00:00:00:00:06 Mask of Source Mac :00:00:00:00:00:07 Source IP :10.0.50.120 Mask of Source IP :255.255.0.0 Source Port :Port4 +---------------List 2---------------+ Index :5 Profile Name :wagoacl5 Action :whitelist Source Mac :00:00:00:00:00:06 Mask of Source Mac :00:00:00:00:00:07 Source IP :10.0.50.120 Mask of Source IP :255.255.0.0 Source Port :Port5	This command is used to view the ACL configured port settings list.

Configure	#acl-delete 5	This command is used to delete the Acl rule in the setting based on index. Example Index:5
Configure	# acl-clearAll yes	This command is used to delete all the Acl rules list in the settings of the device. Note: Confirmation option “yes” to proceed and “no” to discard

- SNMP Settings CLI commands:

Node	Command	Description
SNMP Global Configure	# snmp-globalActive enable	This command is used to enable and disable the SNMP feature. Example: Active: enable/disable
SNMP Version Configure	# snmp-versionSet 2_V1/V2c/V3	This command is used to set SNMP version the SNMP version Example: Version: None 1_V1/V2c 2_V1/V2c/V3 3_V3
Show SNMP Global Status	#show snmp-status SNMP is Enabled. SNMP Version Status -------------------------------- V1/V2c Enabled V3 Enabled	This command is used to view the SNMP global status and current SNMP version enabled status.
SNMP Community Configure	#snmp-community wago read-write-all	This command is use to set the SNMP community string and permission type. Example: String: Wago Permission: read-all-only/ read-write-all
Show SNMP Community Configure	# show snmp-community Community Name Access right -------------------------------------- wago read-write-all	This command is used to view the SNMP community setting list in the device.
Remove SNMP Community Configure	#snmp-community-remove wago	This command is use to remove community in the SNMP community list String: Wago

SNMP Trap Configuration	# snmp-trapAdd 10.0.50.1 102 wago	This command is used to set the SNMP trap configuration. Example: Server IP: 10.0.50.1 Port Number: 102: 10.0.50.1 Port Number: 102 Community String: Wago
Show the SNMP Trap Configuration	show snmp-trap Trap Mode: Trap Sink IP Sink Port Community Name -- 10.0.50.50 162 switch	This command is used to view the SNMP trap configuration.
Remove SNMP Trap settings	#snmp-trap-remove 10.0.50.1 102	This command is used to remove the trap setting using the ip address with port number. Example Server Ip : 10.0.50.1 Port Number:102
SNMP Trap Mode Configure	#snmp-mode Trap	This command is used to set the SNMP Trap mode Example: Mode: Trap/Inform
SNMPV3 Auth Configure	# snmp-authV3 user 12345678 123345678	This command is used to set SNMPV3 Auth configuration password and Encryption key (Note length should be 8 to 32) Name: user/admin Password: 12345678 Encryption Key: 12345678
Show SNMPV3 Auth Configure	show snmp-v3auth User Name Authentication Type Data Encryption Type --- user MD5 DES admin MD5 DES	This command is to view the SNMP V3 Auth list.
Remove SNMPV3 Auth	# snmp-removeAuthV3 user	This command is used to delete the SNMPv3 user using username. Example: Name: user

-
- SNTP Setting CLI commands:

Node	Command	Description
SNTP Manual Configure	#sntp manual 2021 08 31 11 09 30	This command is used to set the SNTP manually setting date & time. Example: Year: 2021 <1970 ~ 2038> Month: 08 <1 ~ 12> Days: 31 <1 ~ 31> Hours: 11 <0 ~ 23> Minutes: 09 <0 ~ 59> Seconds: 30 <0 ~ 59>
SNTP NTP Server Manually Configure	# sntp ntp-server server-manual ip 10.0.50.120 60 34	This command is used to set the SNTP NTP server manually. Example: NTP Server Selection: ip/domain Server IP: 10.0.50.120 Query Period: 60 Time zone: 34
SNTP NTP Server Select Configure	#sntp ntp-server server-public ntp0.fau.de 60 32	This command is used to set the SNTP NTP server by select. Example: Server IP: ntp0.fau.de / ntps1-1.cs.tu-berlin.de Query Period: 60 Time zone: 34
SNTP DayLight Active Set Configure	#sntp daylight-active enable	This command is used to set the SNTP DayLight Activate set. Example: Active: enable/disable
SNTP DayLight Start Set Configure	#sntp daylight-start Jly 4th Sun 23	This command is used to set the SNTP DayLight start time setting. (Condition: DayLigh should enabled) Example: Month: Jly Week: 4th Day: Sunday Hour: 23
SNTP DayLight End Set Configure	#sntp daylight-end Dec 2nd Fri 20	This command is used to set the SNTP DayLight end time setting. (Condition: DayLigh should enabled) Example: Month: Dec Week: 2nd Day: Friday

		Hour: 20
Show SNTP	# show sntpStatus SNTP : Disabled NTP Server 1 : time-A.timefreq.bldrdoc.gov Time Zone : 23 Time Server Query Period: 60	This command is used view the current setting of SNTP.

-
- System Information CLI commands:

Node	Command	Description

Show	# show system-information
	+----------System Information--------------+
	  Model Name : EHG2408
	  MAC Address : 00:60:E9:26:2F:E4
	  Application Version : 2.54-svn795
	  Kernel Version : 2.54-svn795
	  IP Address : 10.0.50.1
	  Default Gateway : 10.0.50.254
	  Subnet Mask : 255.255.255.0
		This command is used to view the system information

System Command	# # system-reboot	This command is used to reboot the device. Note : Confirmation option "yes" to proceed and "no" to discard
Configure system reset to default	# reset-default yes	This command is used to set the default setting of the device. Note : Confirmation option "yes" to proceed and "no" to discard Reboot the system to deflect the default setting is mandatory.

-
- Management VLAN ID Setting CLI commands:

Node	Command	Description
Management Vlan ID Config	# vlan-managementId 1	This command is used to set the management VLAN id of the system
Show Management Vlan ID	# show vlan-managementId --------------------------------- Management VLAN ID : 1 ---------------------------------	This command is used to view the management VLAN id of the system

-
- RSTP Setting CLI commands:

Node	Command	Description
RSTP Enable Configure	# rstp globalActive enable priority 0	This command is used to enable and set the RSTP priority Example: Set Active: enable/disable Priority: 32768
RSTP Disable Configure	# rstp globalActive disable	This command is used to disable the RSTP. Note: Priority Not required for disable, it is optional
RSTP Port Parameter Configure	# rstp port-settings 4 enable enable enable enable enable	This command is used to set the RSTP port Parameter settings. Example: Port Number: 4 Edge Port : enable/disable RSTP Per Port : enable/disable BPDU Filter : enable/disable BPDU Guard: enable/disable Root Guard: enable/disable
Show RSTP settings	# show rstp | Port | Role | Status | Edge | RSTP | BPDU | BPDU | Root | Port (Fact) Per Por Filter Guard Guard ----------+--- 1 Designated Disc Not edge Disable Disable Disable Disable 2 Disabled Disc Not edge Disable Disable Disable Disable 3 Disabled Disc Not edge Disable Disable Disable Disable	This command is used to view the current settings of RSTP of the system.

	4 Disabled Disc Edge Disable Enable Enable Enable 5 Disabled Disc Not edge Disable Disable Disable Disable 6 Disabled Disc Not edge Disable Disable Disable Disable 7 Disabled Disc Not edge Disable Disable Disable Disable 8 Disabled Disc Not edge Disable Disable Disable Disable	

4 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 uses 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.
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.

Atop Technologies, Inc.

www.atoponline.com

TAIWAN HEADQUARTER and INTERNATIONAL SALES:

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Chupei City, Hsinchu County
Taiwan, R.O.C.
Tel: +886-3-550-8137
Fax: +886-3-550-8131
sales@atop.com.tw

ATOP CHINA BRANCH:

3F, 75th, No. 1066 Building,
Qingzhou North Road,
Shanghai, China
Tel: +86-21-64956231