Atop Technologies, Inc.

Industrial Lite-Managed Booster Switch

User Manual

V1.1

October 27th, 2021

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

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:	Matteo Tabarelli
Revision:	1.1
Revision History:	New features
Creation Date:	21 February 2021
Last Revision Date:	27 October 2021
Product Reference:	Layer-2 Managed Switch
Document Status:	Released

Table of Contents

Table of Figures

Table of Tables

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
- Time Synchronization
  - Network Time Protocol (NTP) Client
  - Simplified Network Time Protocol (SNTP)
- Quality of Service (QoS) Traffic Regulation
- Rapid Spanning Tree Protocol (RSTP)
- Virtual Local Area Network (VLAN)
- Power over Ehternet (PoE)
- Trunking
- Alarm System (with Relay Output)
- Industrial Protocols
  - Modbus/TCP

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.

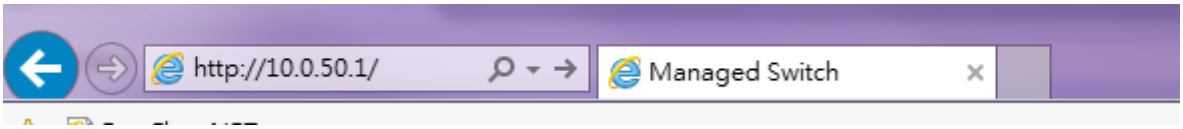


Figure 2.1 IP Address for Web-based Setting

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.

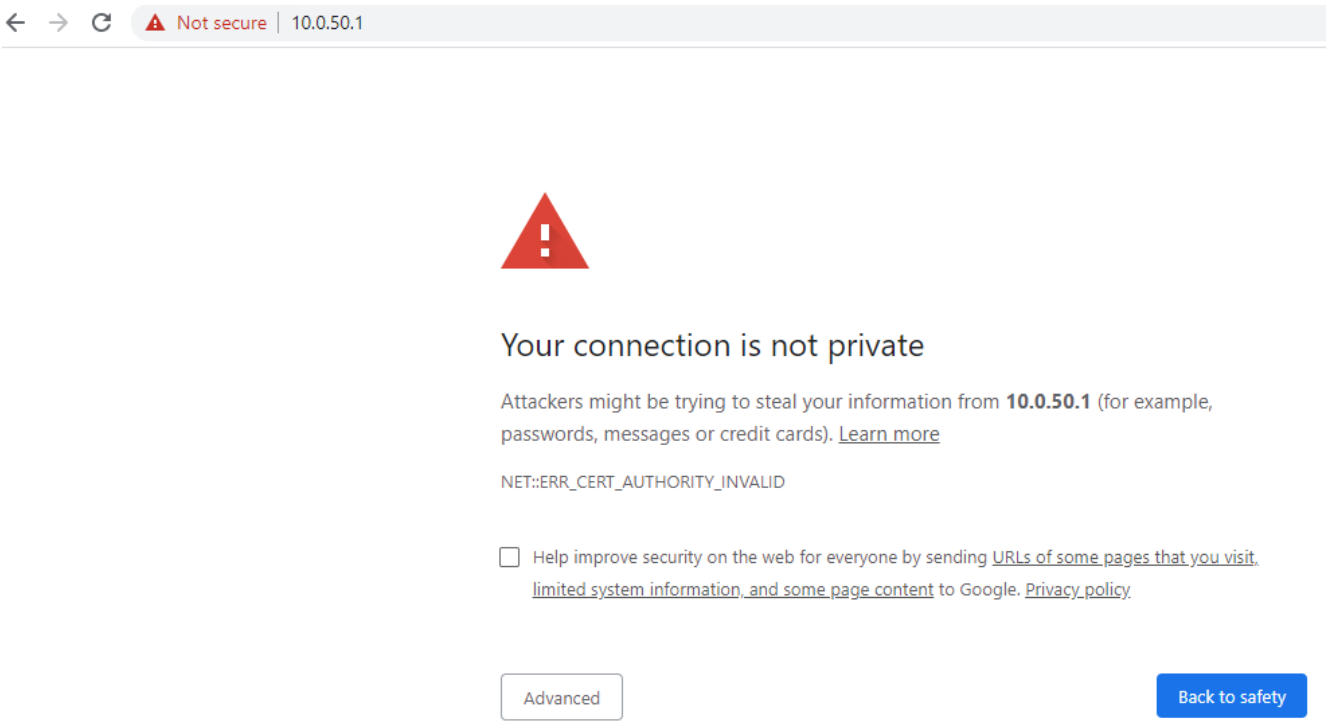


Figure 2.2 Example of Google's Chrome web brower invalid certificate authority

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.

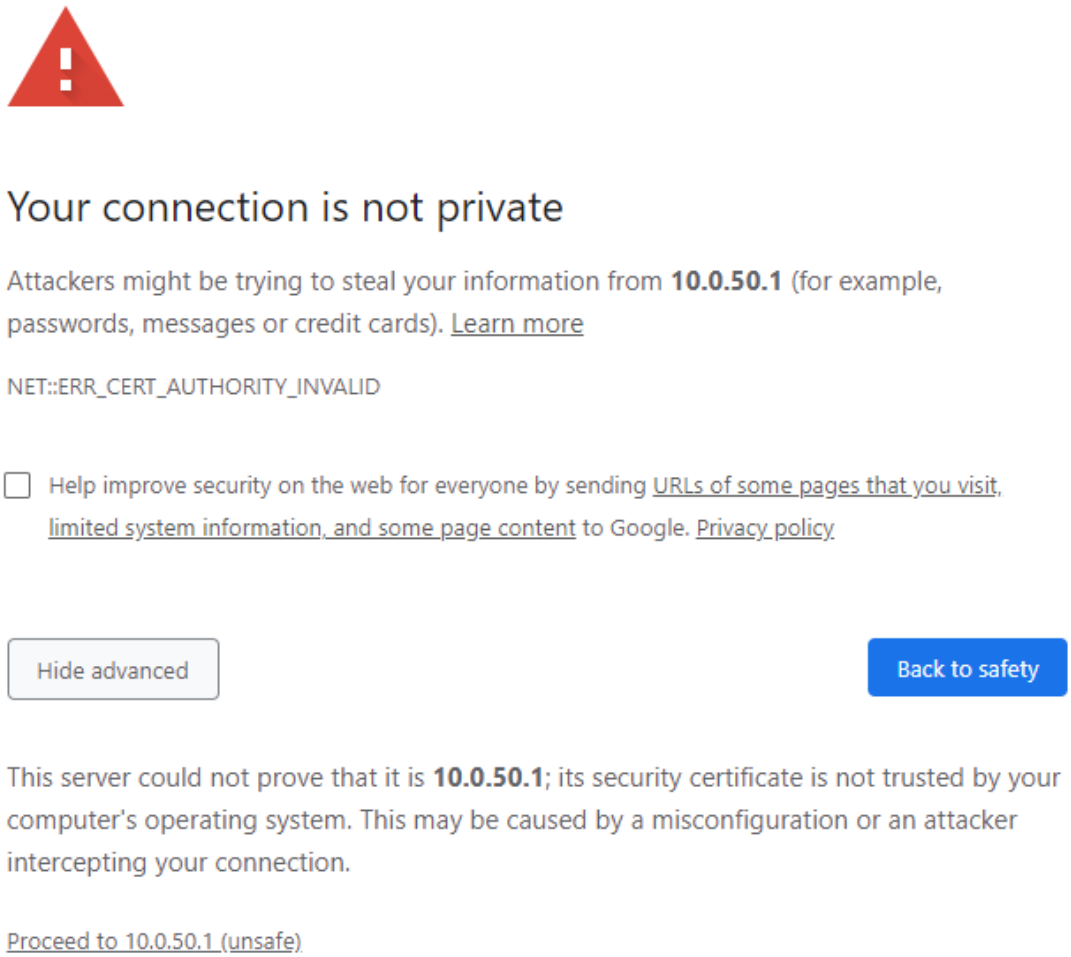


Figure 2.3 A hyperlink to proceed to the managed switch at IP address 10.0.50.1

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.

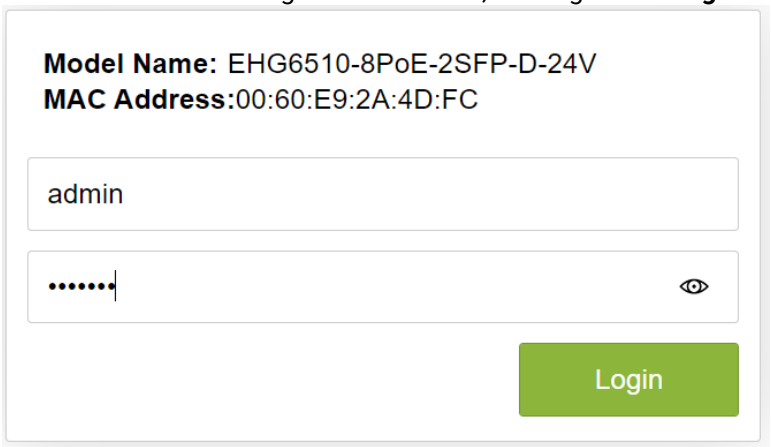


Figure 2.4 Login page

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.

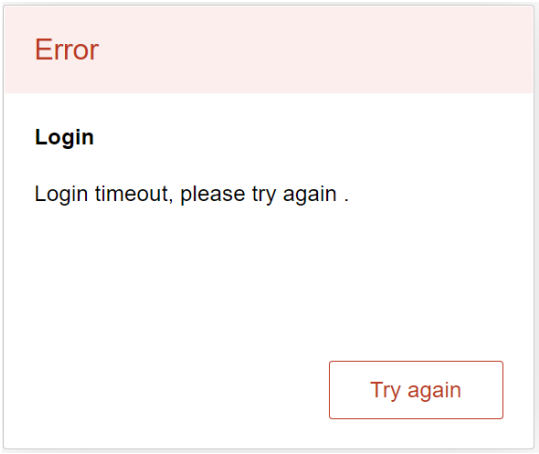


Figure 2.5 Login timeout error notification

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.

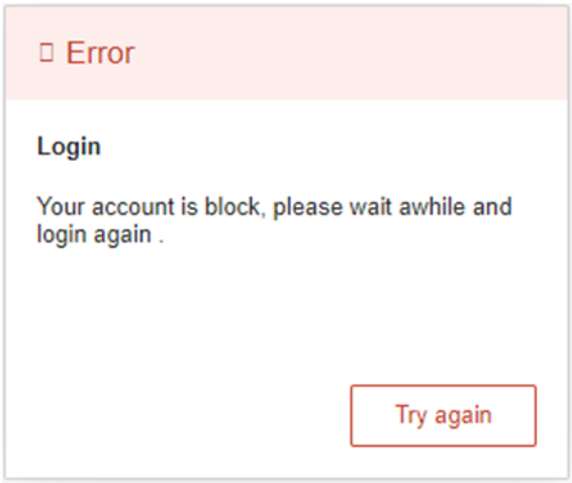


Figure 2.6 Example of error notification on blocked account

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.

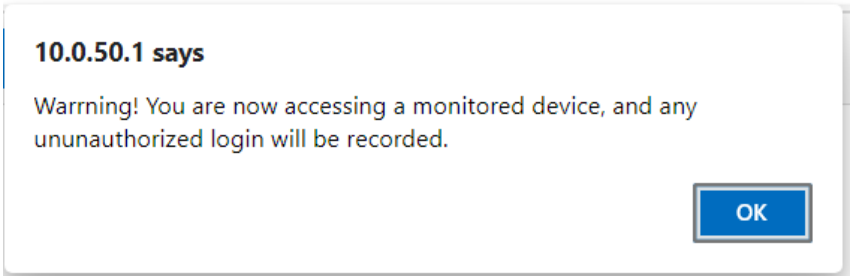


Figure 2.7 Notification on recording of unauthorized login

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.

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.

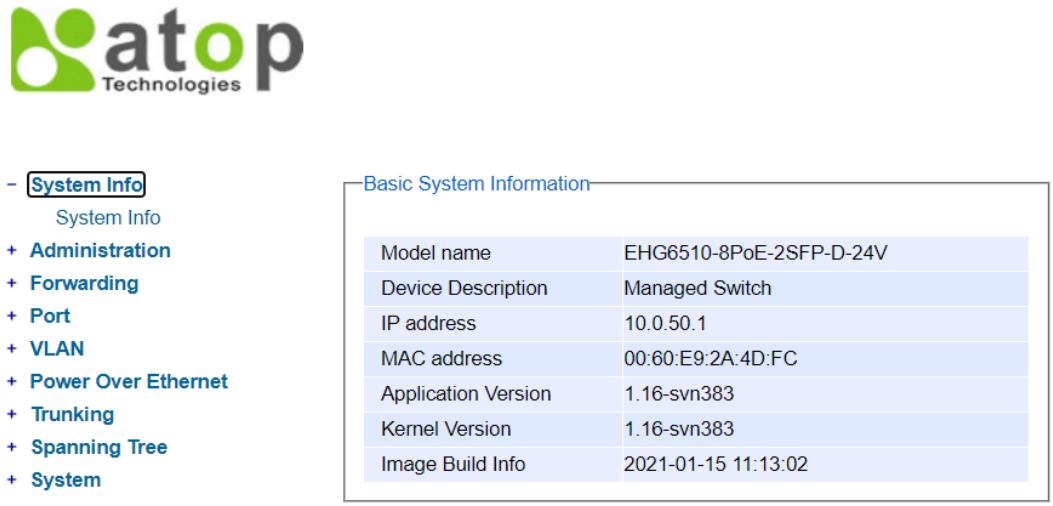


Figure 2.9 System Information Dropdown Menu

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.

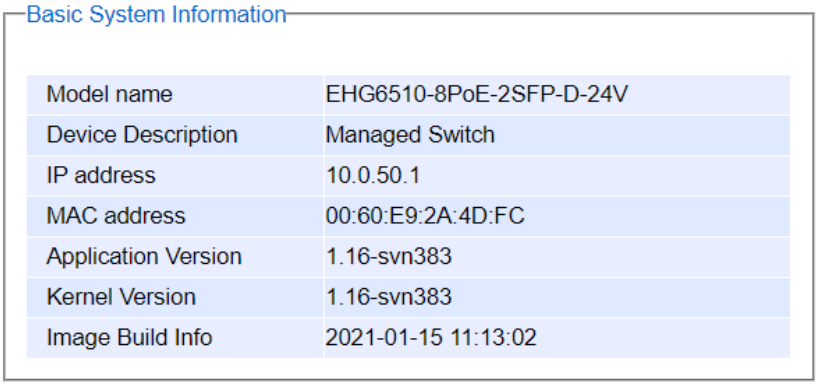


Figure 2.10 Details of System Info Webpage under the System Info Mainmenu

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

2.3 Administration

In this section, users will be able to configure **Account, IP Settings, Modbus Setting,** and **System Time**. Figure 2.11 shows the Administration menu with the list of its sub-menus on the left of the screen.

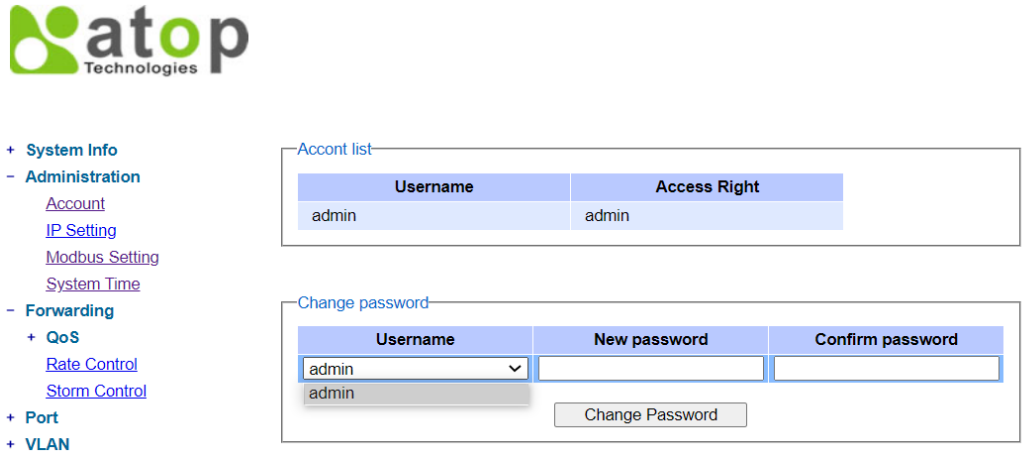


Figure 2.11 Administration Dropdown Menu

2.3.1 Account

As shown in Figure 2.12, there are two sections inside **Administration->Account** page as the followings: **Account list** and **Change password.** In **Account List** box (1st row of Figure 2.12), the users and their access rights are listed. There is only one type of access right: **admin**. The **admin**'s access right has **read/write** permission on the managed switch. If the user wishes to change password of the administrator (**admin** account), the user can do so in the **Change password** box (2nd row of Figure 2.12). Here, the user has to select **admin** account from the **Username** dropdown box first. Then, input a password that the user would like to change it to in **New password** textbox before reentering the same password in the **Confirm password** textbox. Note that the users will be reminded during the login procedure with a notification to change their passwords if the passwords have not been changed over the last 30 days. Figure 2.13 shows the pop-up notification for changing the password.

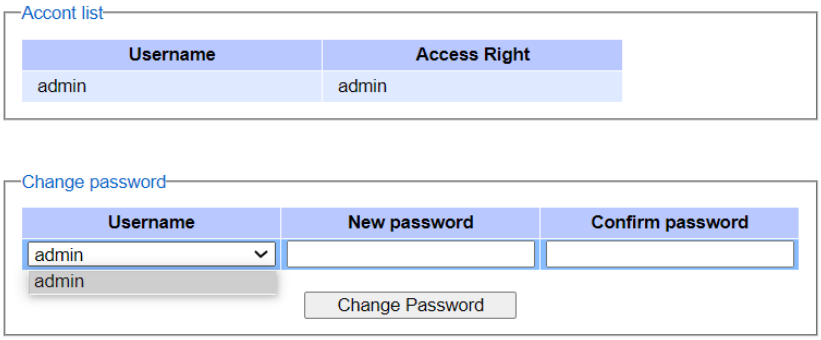


Figure 2.12 Account Setting Webpage

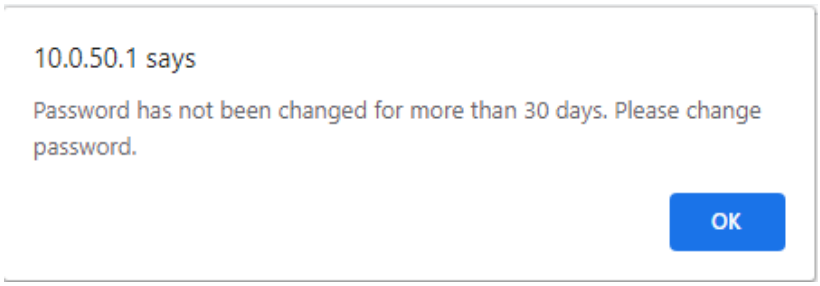


Figure 2.13 Notification of old password

2.3.2 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 2.14, 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.

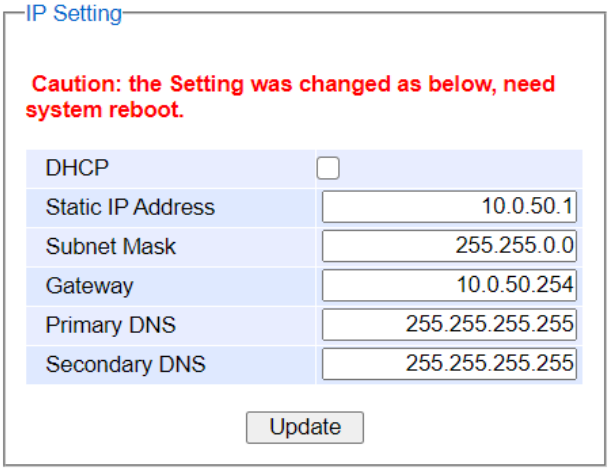


Figure 2.14 IP Setting under IP Setting Webpage

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 2.15. 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 2.2.

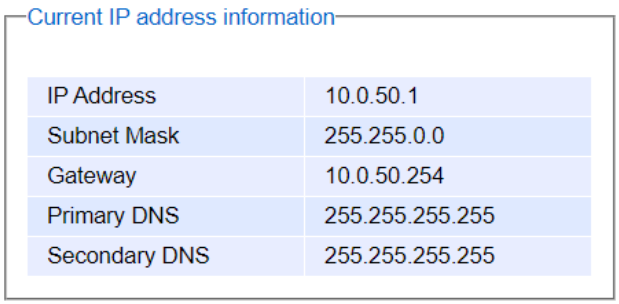


Figure 2.15 IP Interface Part under IP Setting Webpage

Table 2.2 Descriptions of IP Settings

Label	Description	Factory Default
DHCP	By checking this box, an IP address and related fields will be automatically assigned. Otherwise, users can set up the static IP address and related fields manually.	Uncheck
Static IP Address	Display current IP address. Users can also set a new static IP address for the device.	10.0.50.1
Subnet Mask	Display current Subnet Mask or set a new subnet mask.	255.255.0.0
Gateway	Show current Gateway or set a new one.	10.0.50.254
Primary DNS	Set the primary DNS IP address to be used by your network.	255.255.255.255
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.	255.255.255.255

2.3.3 Modbus Setting

Atop's managed switch can be connected to a Modbus network using Modbus TCP/IP protocol which is an industrial network protocol for controlling automation equipment. The managed switch's status and settings can be read and written through Modbus TCP/IP protocol which operates similar to a Management Information Base (MIB) browser. The managed switch will be a Modbus slave which can be remotely configured by a Modbus master. The Modbus slave address must be set to match the setting inside the Modbus master. In order to access the managed switch, a **Modbus Address** must be assigned as described in this subsection. A Modbus memory mapping table, which lists all the register's addresses inside the managed switch and their descriptions, is provide in Chapter 4 Modbus Memory Map. Figure 2.16 shows the Modbus Setting webpage.

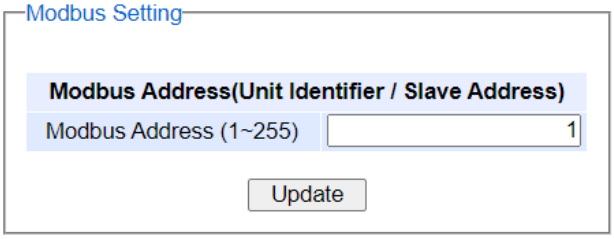


Figure 2.16 Webpage for Setting the Modbus Address

Figure 2.16 shows the webpage that users can set up the Modbus ID address. Users can use Modbus TCP/IP compatible applications such as **Modbus Poll** to configure the switch. Note that Modbus Poll can be download from http://www.modbustools.com/download.html. The Modbus Poll 64-bit version 7.0.0, Build 1027 was used in this document. However, Atop does not provide this software to the users. Tutorial of Modbus read and write examples are illustrated below. Note that the switch only supports Modbus function code 03, 04 (for Read) and 06 (for Write).

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

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

Figure 2.17 Mapping Table of Modbus Address for Switch's IP Address

1. Make sure that a supervising computer (Modbus Master) is connected to your target switch (Modbus Slave) over the Ethernet network.
2. Launch **Modbus Poll** in the supervising computer. Note a registration key may be required for a long term use of Modbus Poll after 30-days evaluation period. Additionally, there is a 10-minute trial limitation for the connection to the managed switch.
3. Click **Connect** button on the top toolbar to enter Connection Setup dialog by selecting **Connect...** menu as shown in Figure 2.18.

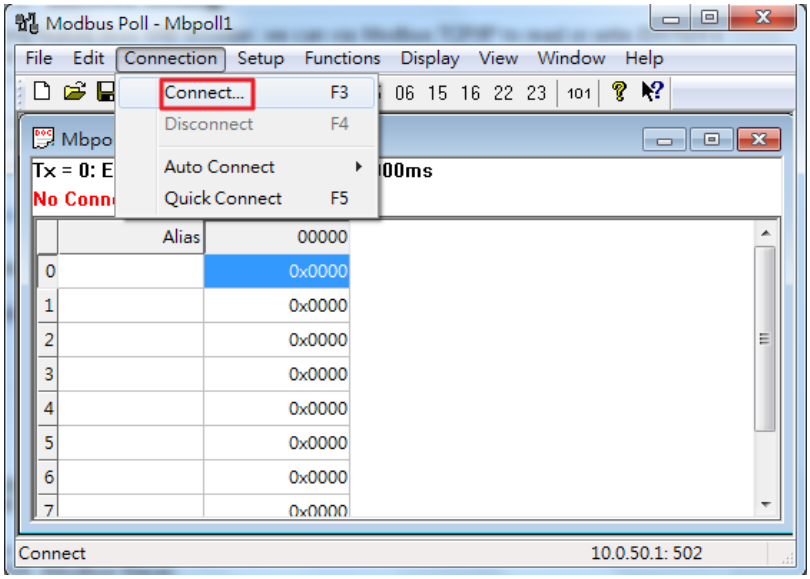


Figure 2.18 Entering Connection Setup Menu of the Modbus Poll

4. Select **Modbus TCP/IP** as the **Connection** mode and enter the switch's IP address inside the **Remote Modbus Server**'s **IP Address or Node Name** field at the bottom as shown in Figure 2.19. The **Port** number should be set to 502. Then click **OK** button.

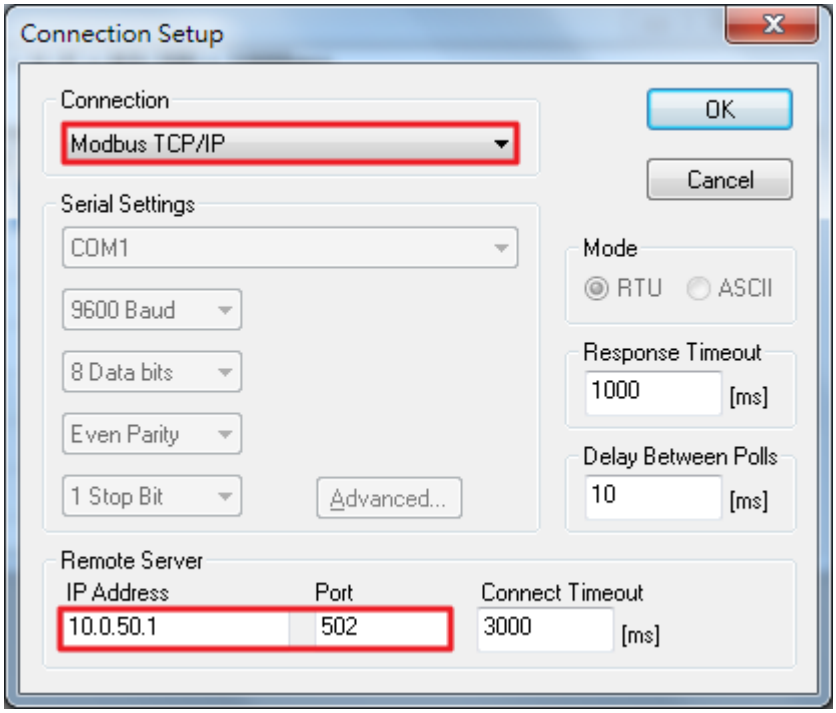


Figure 2.19 Modbus Poll Connection Setup

5. On the window Mbpoll1, select multiple cells from row 0 to row 2 by clicking on cells in second column of row 0 and row 2 while holding the shift key as shown in Figure 2.20.

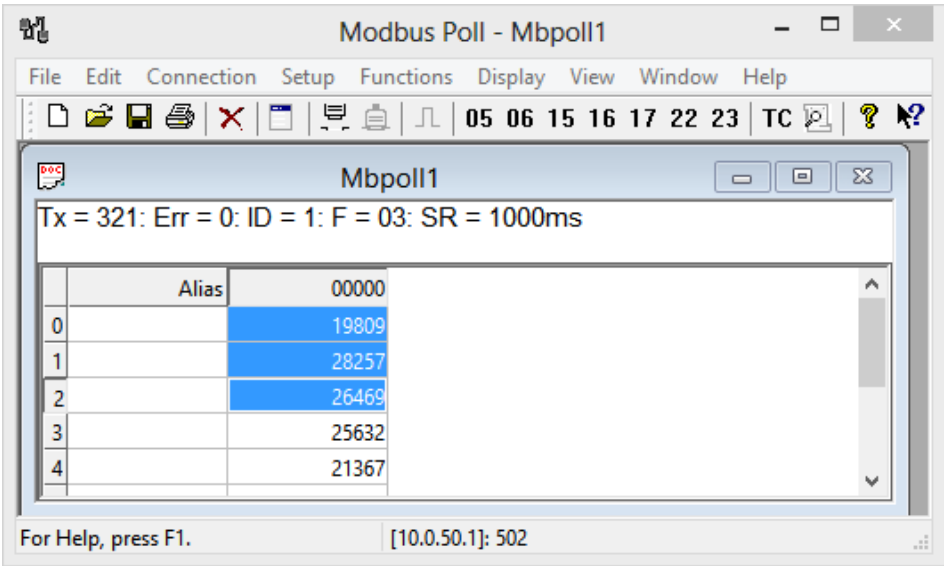


Figure 2.20 Multiple Cell Selection in Modbus Poll

6. Set **Display** mode of the selected cells in previous step to HEX (hexadecimal) by selecting **Display** pull-down menu and choosing the **Hex** as shown in Figure 2.21.

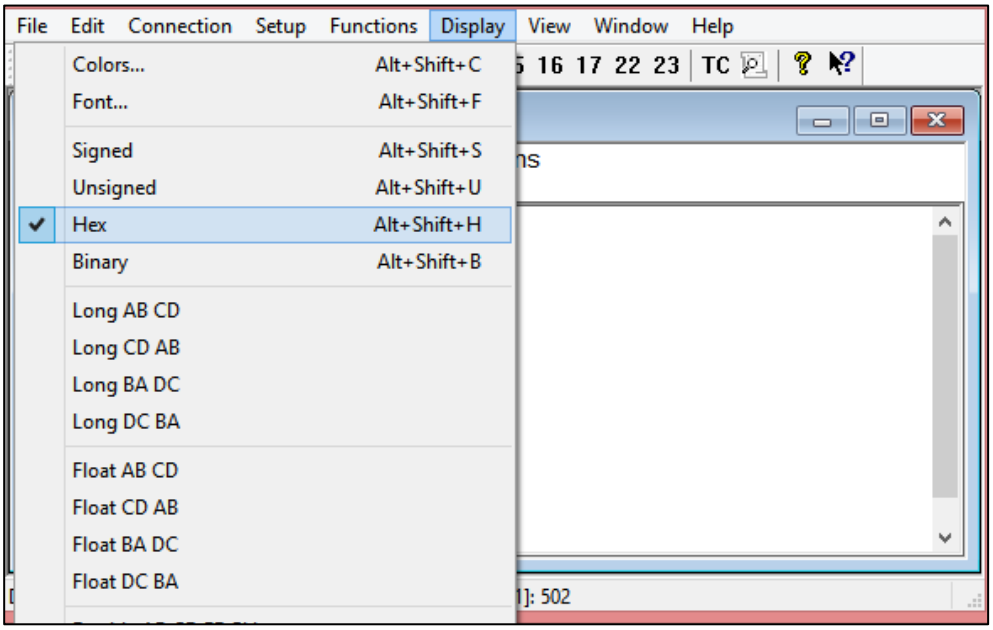


Figure 2.21 Set Display Mode to Hex in Modbus Poll

7. Click on the **Setup** pull-down menu and choose **Read/Write Definition…** as shown in Figure 2.22.

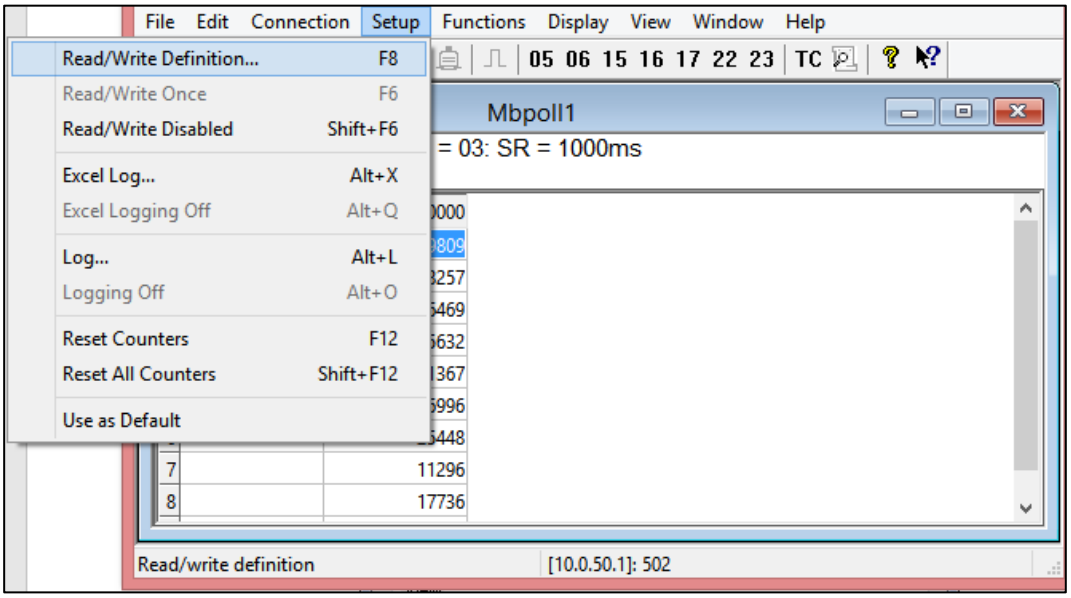


Figure 2.22 Modbus Poll Setup Read/Write Definition

8. Enter the **Slave ID** in the Modbus Poll function as shown in Figure 2.23, which should match the Modbus Address = 1 entered in Figure 2.16 in Section 0 (Modbus Setting).

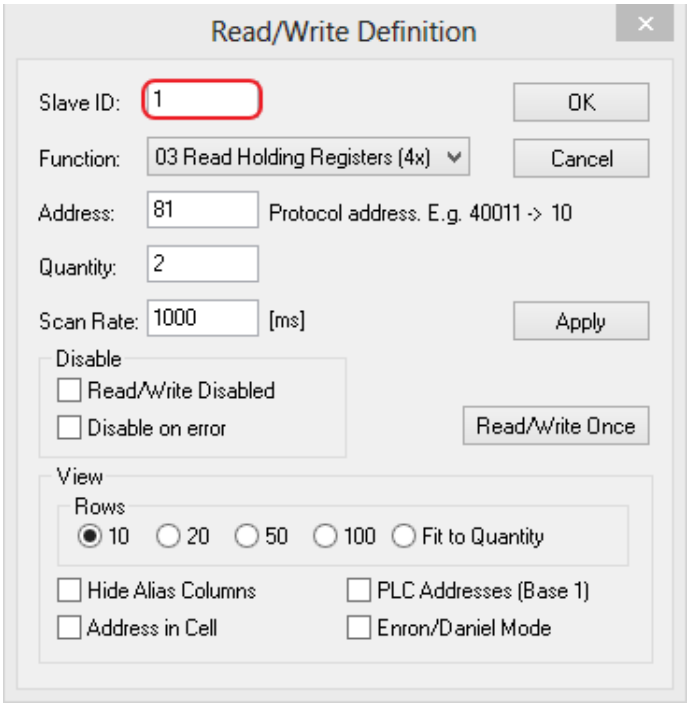


Figure 2.23 Slave ID in the Modbus Poll Function is set to 1

9. Select **Function 03** or **04** because the managed switch supports function code 03 and 04 as shown in Figure 2.24.

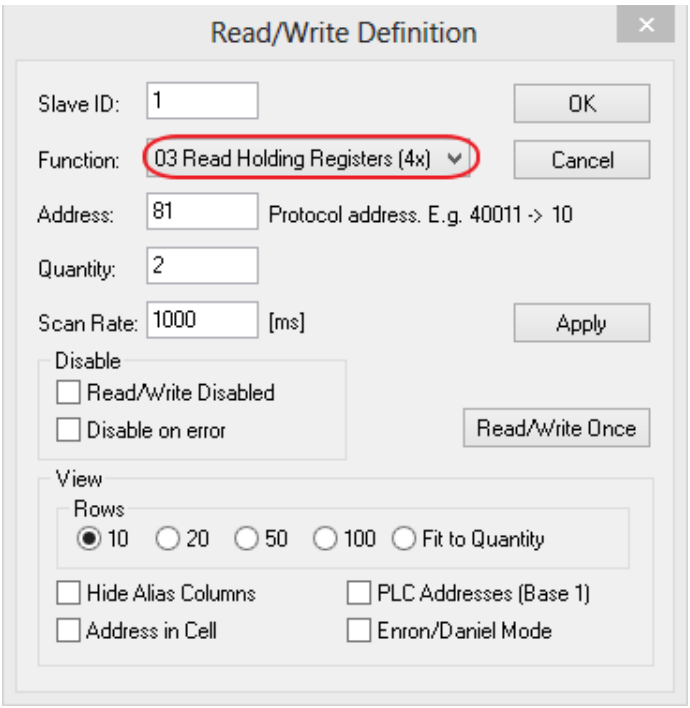


Figure 2.24 Set Code 03 in the Modbus Poll Function

10. Set starting **Address** to 81 and **Quantity** to 2 as shown in Figure 2.25.

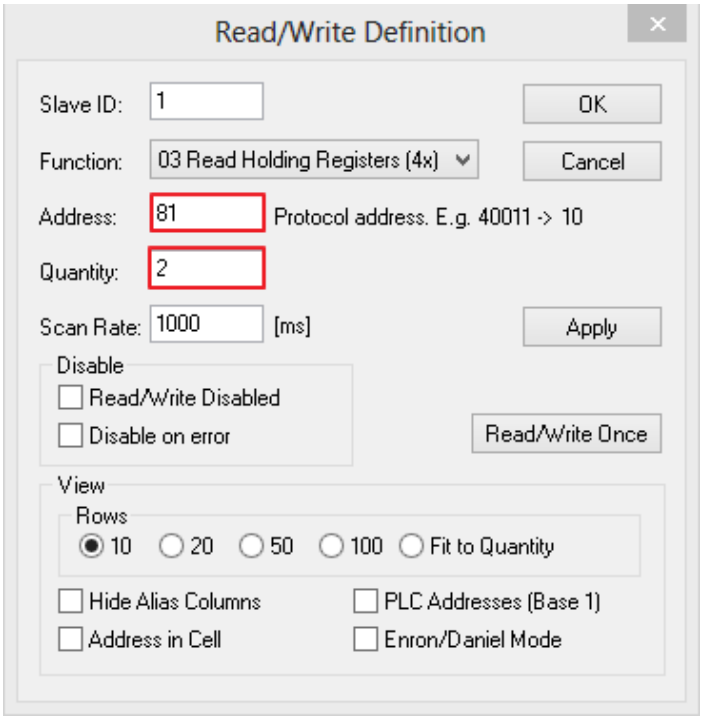


Figure 2.25 Setup Starting Address and Quantity in Modbus Poll

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

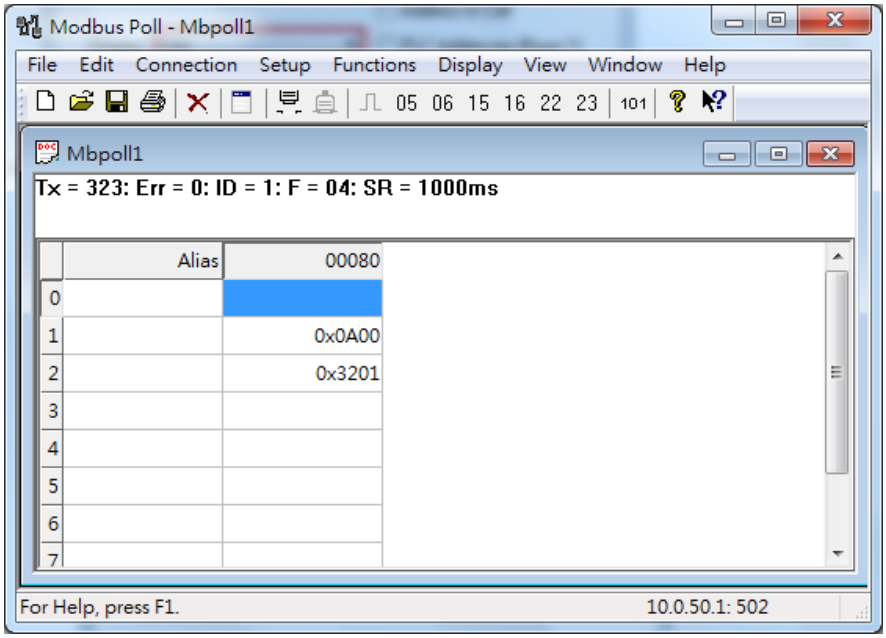


Figure 2.26 Modbus Memory Address 81 and 82 are the location of EHG6510's IP Address

12. Modbus Poll will get the values 0x0A, 0x00, 0x32, 0x01, which means that the switch's IP is 10.0.50.1 as shown in Figure 2.26.

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

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

Figure 2.27 Mapping Table of Modbus Address for Clearing Port Statistics

1. Check the switch's Port TX/RX counts in **Port Status** page (described in Section 2.5.2) as shown in Figure 2.28.

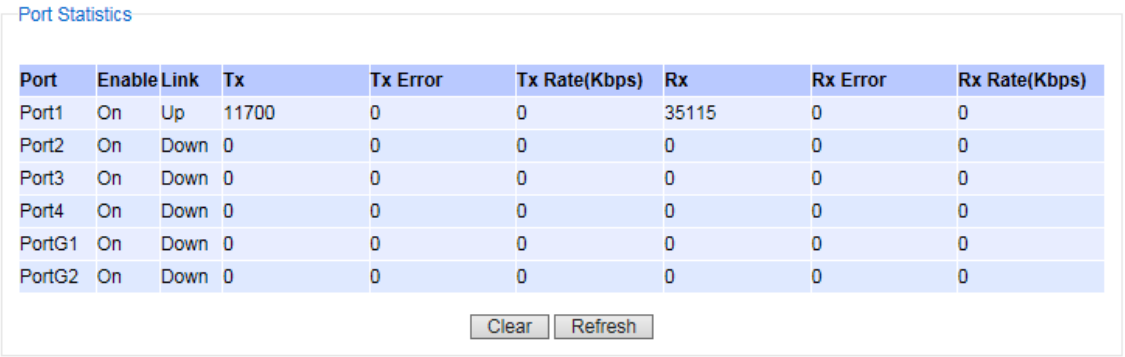


Figure 2.28 Port Count in Port Statistics Webpage

2. Click function **06** on the toolbar as shown in Figure 2.29.

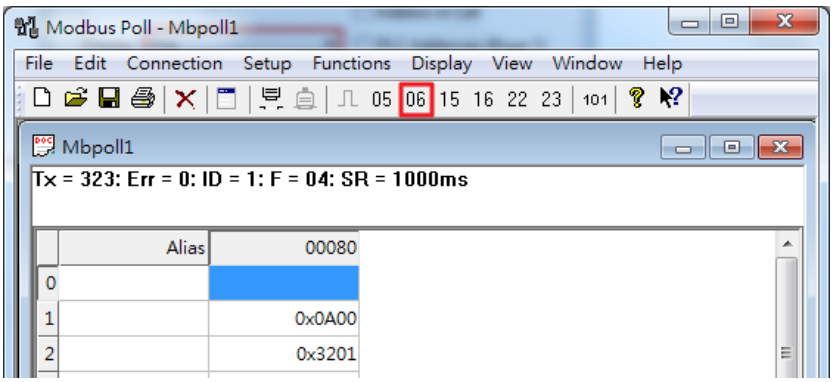


Figure 2.29 Click on Function 06 in the Modbus Poll

3. Set **Address** to 256 and **Value (HEX)** to 1 as shown in Figure 2.30, then click "**Send**" button.

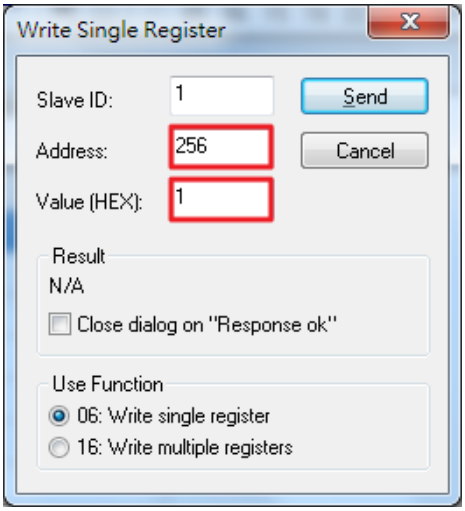


Figure 2.30 Use Modbus Poll to Clear Switch's Port Count

4. Check **Port Status** (described in Section 2.5.2) in the managed switch's Web UI as shown in Figure 2.31. The packet count is now cleared.

Port Statistics

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

Clear Refresh

Figure 2.31 Cleared Port Statistics

2.3.4 System Time

Atop's industrial managed switch has internal calendar (date) and clock (or system time) which can be set manually or automatically. Figure 2.32 and Figure 2.33 shows the System Time and SNTP webpage. The users have options to configure **Current Date** and **Current Time** manually. 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) as shown in Figure 2.33. There is a drop-down list of **Time Zone** which can be selected for the local time zone.

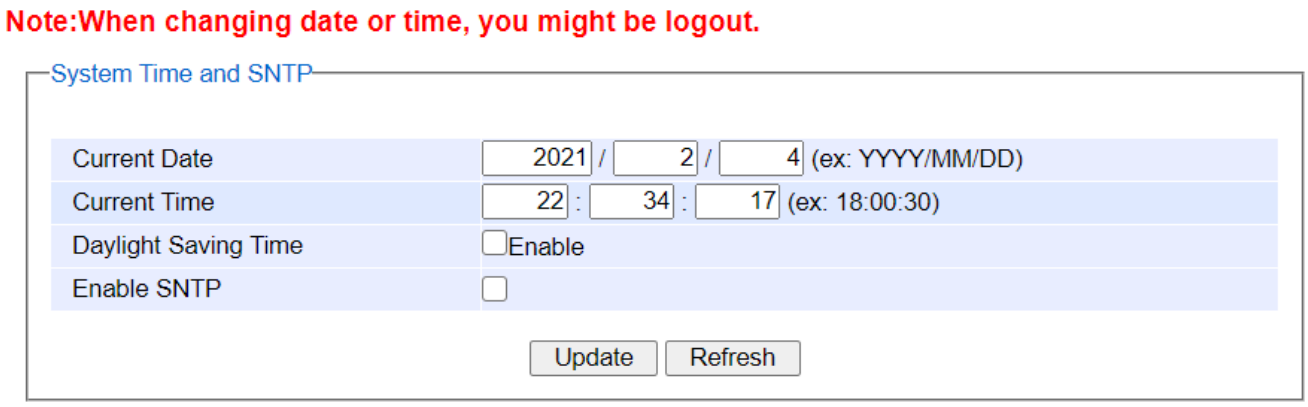


Figure 2.32 Webpage for Setting System Time **when Daylight Saving Time** and **SNTP** Functions are disabled

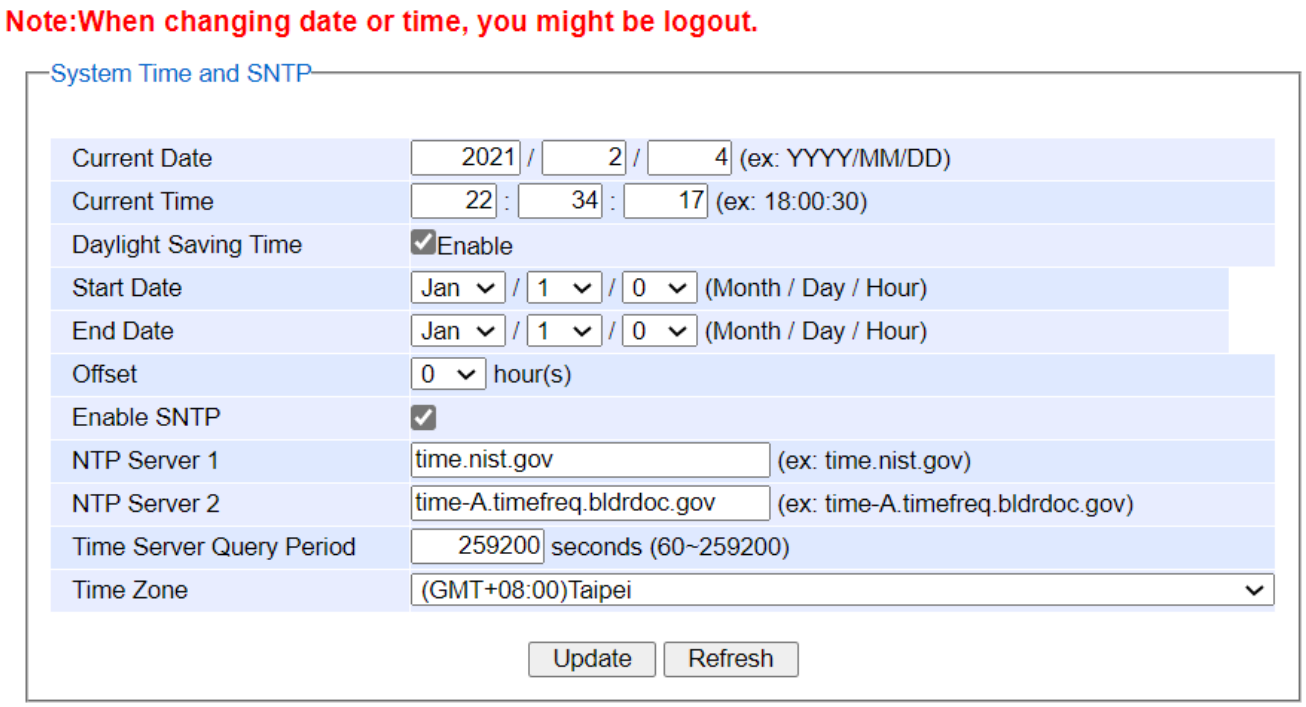


Figure 2.33 Webpage for Setting System Time **when Daylight Saving Time** and **SNTP** Functions are enabled

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. Description of each option is provided in Table 2.3.

Table 2.3 Descriptions of the System Time and the SNTP

Label	Description	Factory Default
Current Date	Allows local date configuration in yyyy/mm/dd format	2017/1/1
Current Time	Allows local time configuration in local 24-hour format	12:30:30

Label	Description	Factory Default
Daylight Saving	Enable or disable Daylight Saving Time function	Unchecked
Start Date	Define the start date of daylight saving in mm/dd/hr format	Jan/1/0
End Date	Define the end date of daylight saving in mm/dd/hr format	Jan/1/0
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. This option will enable network time protocol (NTP) daemon inside the managed switch which allows other devices in the network to synchronize their clock with this managed switch using NTP.	Unchecked
NTP Server 1	Sets the first IP or Domain address of **NTP Server**.	time.nist.gov
NTP Server 2	Sets the second IP or Domain address of NTP Server. Switch will locate the 2nd **NTP Server** if the 1st NTP Server fails to connect.	time-A.timefreq.bldrdoc.gov
Time Server Query Period	This parameter determines how frequently the time is updated from the NTP server. If the end devices require less accuracy, longer query time is more suitable since it will cause less load to the switch. The setting value can be in between 60 and 259200 (72 hours) seconds.	259,200 seconds
Time Zone	The user's current local time	(GMT+08:00) Taipei

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*.

2.4 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 2.34 depicts the submenus under the Forwarding section.

Figure 2.34 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 2.35. Table 2.4 summarizes the descriptions of QoS Setting. See notes in the following subsection for more details.

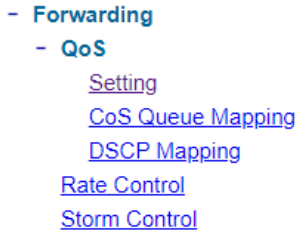


Figure 2.35 QoS Dropdown Menu

Table 2.4 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 2.36 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

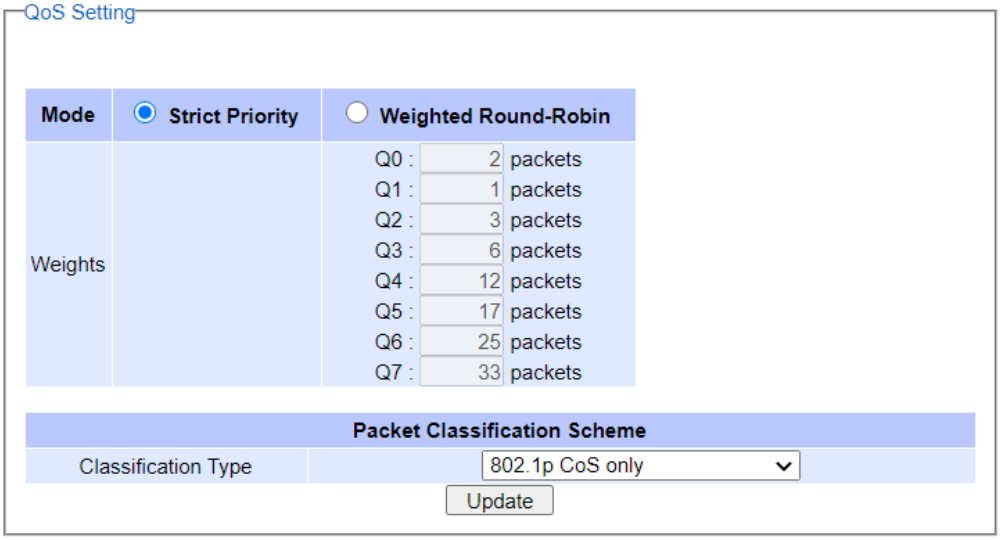


Figure 2.36 QoS Setting Webpage

At the bottom of the QoS Setting webpage in Figure 2.36, 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 2.37. 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 2.5.

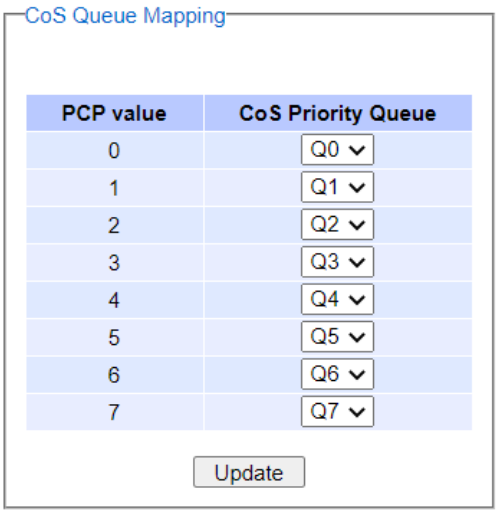


Figure 2.37 Mapping Table of CoS Webpage

Table 2.5 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.	

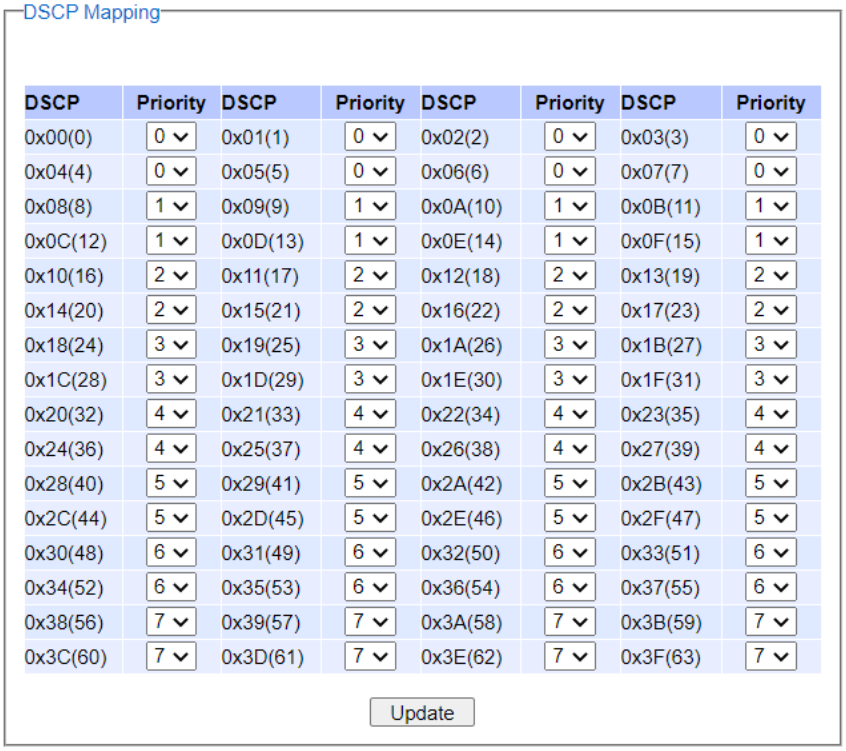
2.4.1.3 DSCP Mapping

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 2.38. 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 2.38. 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

Update

Figure 2.38 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 2.39. 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.

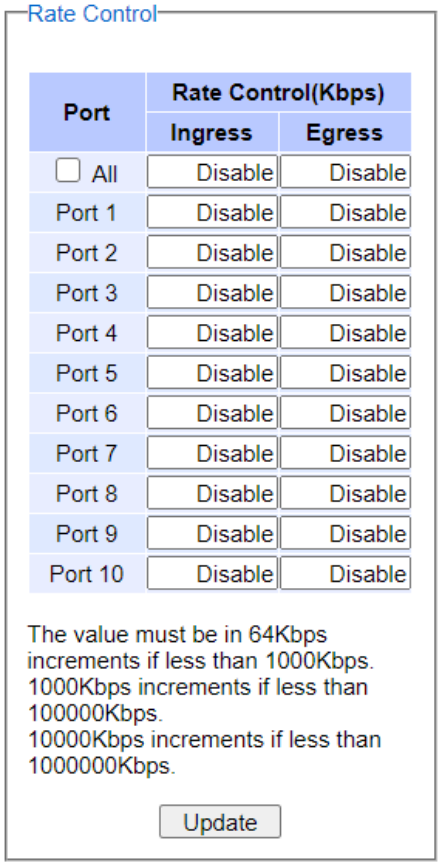


Figure 2.39 Rate Control Webpage

Table 2.6 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 2.6 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 2.40 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.

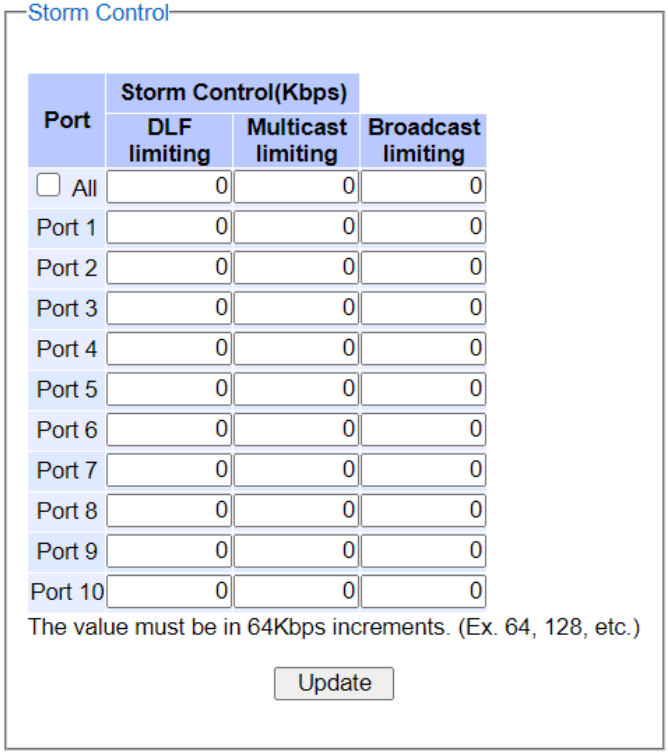


Figure 2.40 Storm Control Webpage

Table 2.7 summarizes the descriptions of storm control.

Table 2.8 summarizes the descriptions of limiting parameters for storm control.

Table 2.7 Descriptions of Storm Control

Label	Description	Factory Default
All	Enable or Disable the storm control or filter on all ports at the same time. The limiting data rate for each type of storm packets (**DLF**, **Multicast**, and **Broadcast**) can be controlled by changing the number under each column. Note that the value must be in multiples of 64kbps.	Uncheck and Disable
Port1 - Port10	Set the limiting data rate of storm packets that can be controlled for each Port, which are **DLF**, **Multicast**, and **Broadcast**. Note that the value must be in multiples of 64kbps. See notes below for the detailed description and comparison.	Disable

Table 2.8 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

Atop's 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 2.41 illustrates the Port webpage. The Port section is subdivided into five subsections which are: Setting and Port Status.

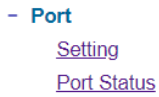


Figure 2.41 Port Dropdown Menu

2.5.1 Port Setting

Setting webpage is shown in Figure 2.42. 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 **Fiber** port 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. The speed for each **Copper** is set at **1000** Mbps. After configuring the port setting, please click on the **Update** button to enable any of your new configuration on the switch.

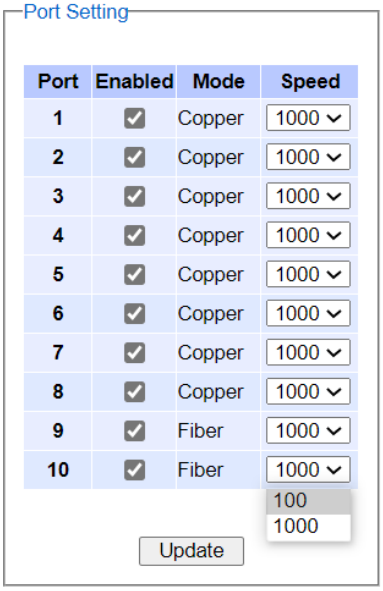


Figure 2.42 Port Setting Webpage

Descriptions of port setting options are summarized in Table 2.9.

Table 2.9 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

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 2.43 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.

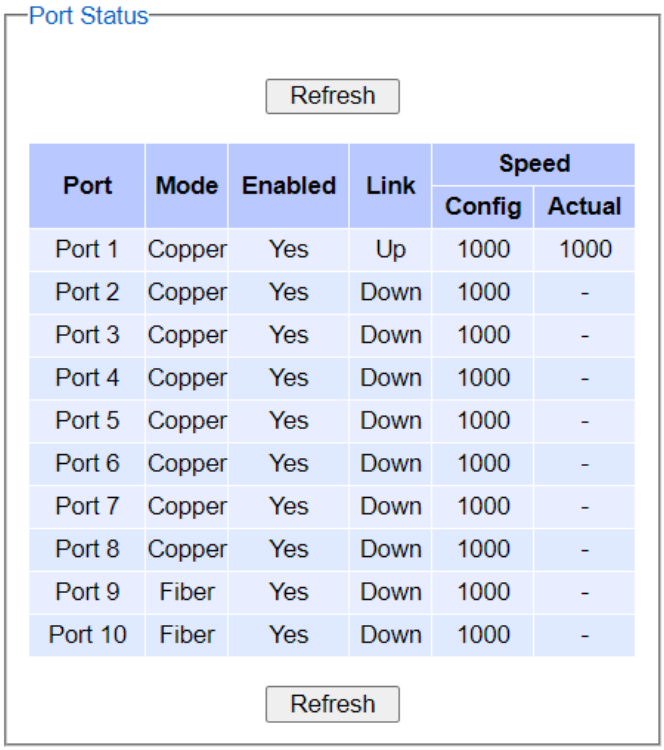


Figure 2.43 Port Status Webpage

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

- **Mode** (Copper (C) or Fiber (F))
- **Enable** (Yes or No)
- **Link** (Up or Down)
- **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 2.44).

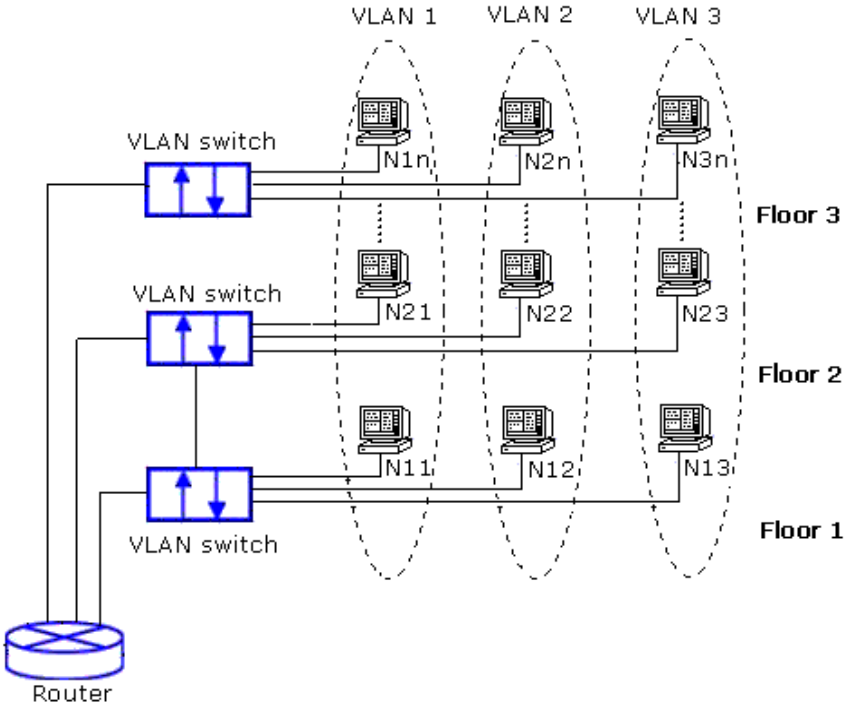


Figure 2.44 Example of VLAN Configuration

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

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

Figure 2.45 shows the drop-down menu under the VLAN section.

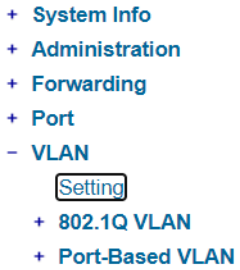


Figure 2.45 VLAN Dropdown Menu

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 2.46 depicts the VLAN Setting webpage. Table 2.10 describes the VLAN Setting option.

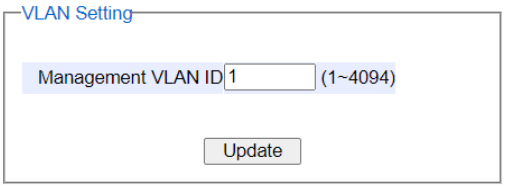


Figure 2.46 VLAN Setting Webpage

Table 2.10 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 2.47.

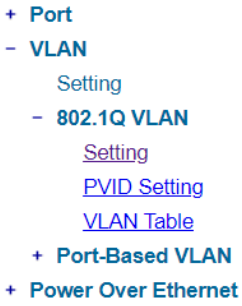


Figure 2.47 802.1Q VLAN Dropdown Menu

2.6.2.1 802.1Q VLAN Settings

Figure 2.48 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 2.48. The description of each fields is summarized in Table 2.11. 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 2.48.

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 2.48.

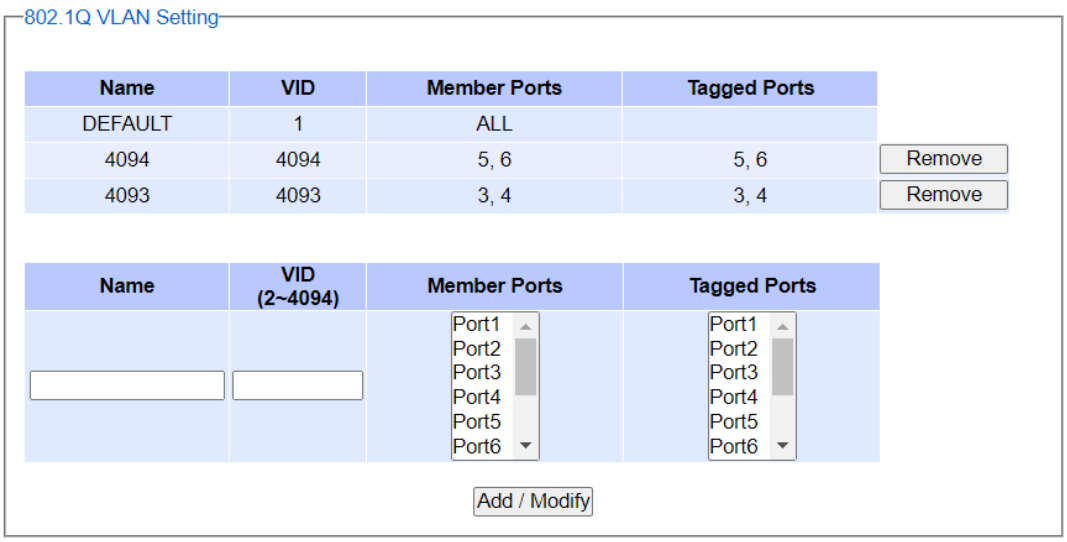


Figure 2.48 802.1Q VLAN's Setting Webpage

Table 2.11 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 2.49 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 2.12 summarizes the PVID Setting's descriptions.

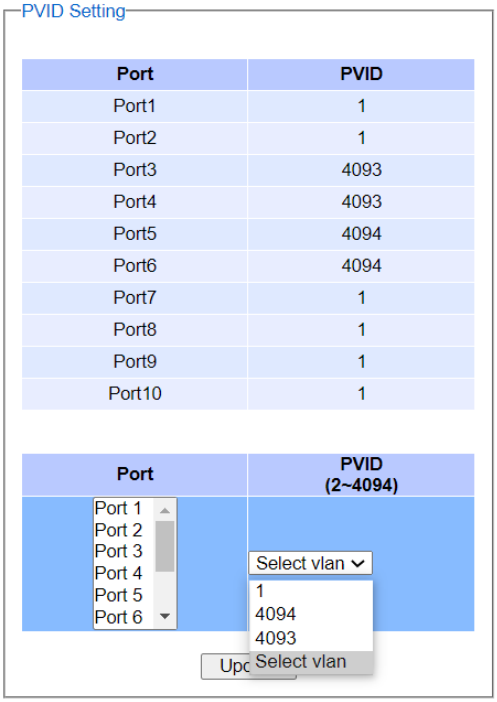


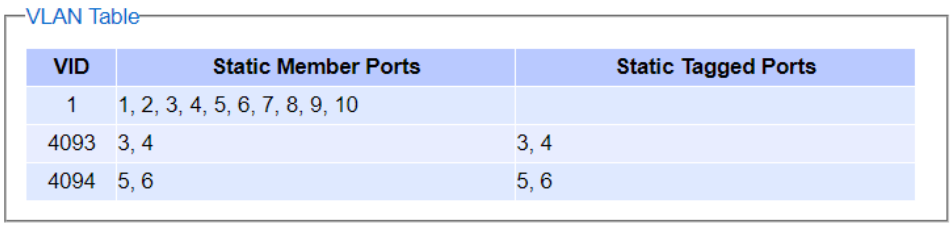
Figure 2.49 802.1Q VLAN PVID Setting Webpage

Table 2.12 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 2.50 displays the 802.1Q VLAN table which lists all the VLANs that are automatically and manually added/modified to the managed switch. Table 2.13 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 2.50 802.1Q VLAN Table Webpage

Table 2.13 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 2.51.
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.

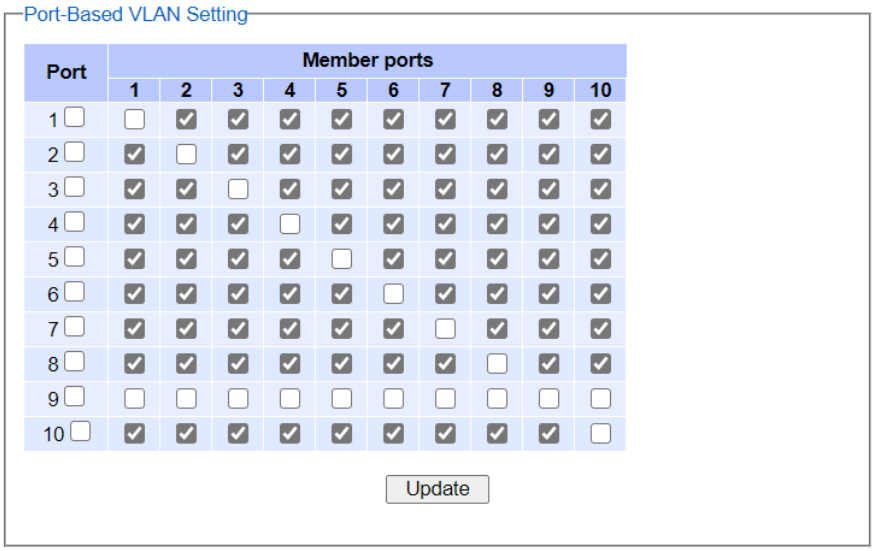


Figure 2.51 Port-based VLAN Setting Webpage

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 2.52 shows the Power over Ethernet dropdown menu.

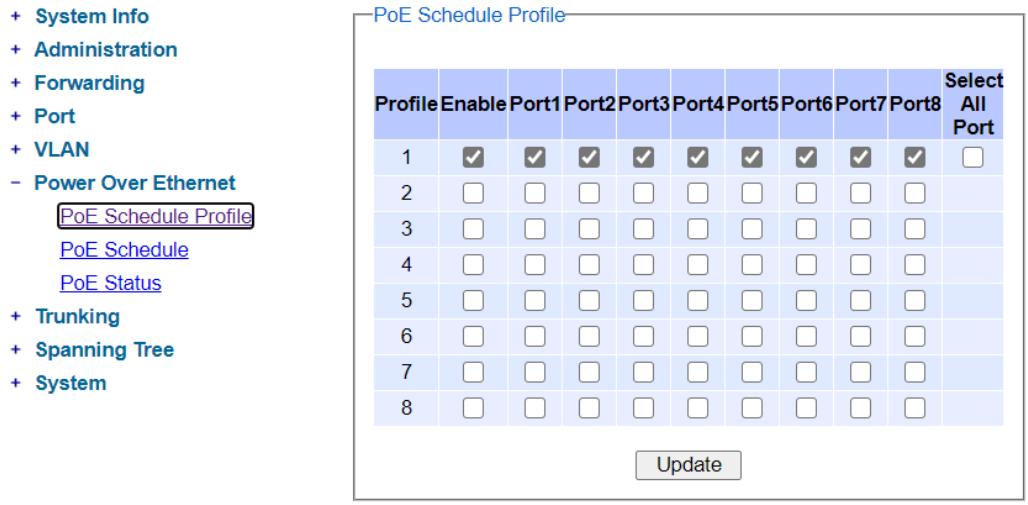


Figure 2.52 Power over Ethernet Dropdown Menu Example on EHG6510-4PoE-2SFP-24V

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 2.52. 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 2.14. The number of profiles and ports depends on the EHG model of the user's managed switch.

Table 2.14 Default value of PoE Schedule Profile

Label	Enable status	Port1	Port2	Port3	Port4
Profile1	Enable	Enable	Enable	Enable	Enable
Profile 2	Disable	Disable	Disable	Disable	Disable
Profile 3	Disable	Disable	Disable	Disable	Disable
Profile 4	Disable	Disable	Disable	Disable	Disable

2.7.2 *PoE Schedule*

PoE Schedule page, as shown in Figure 2.53, 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.

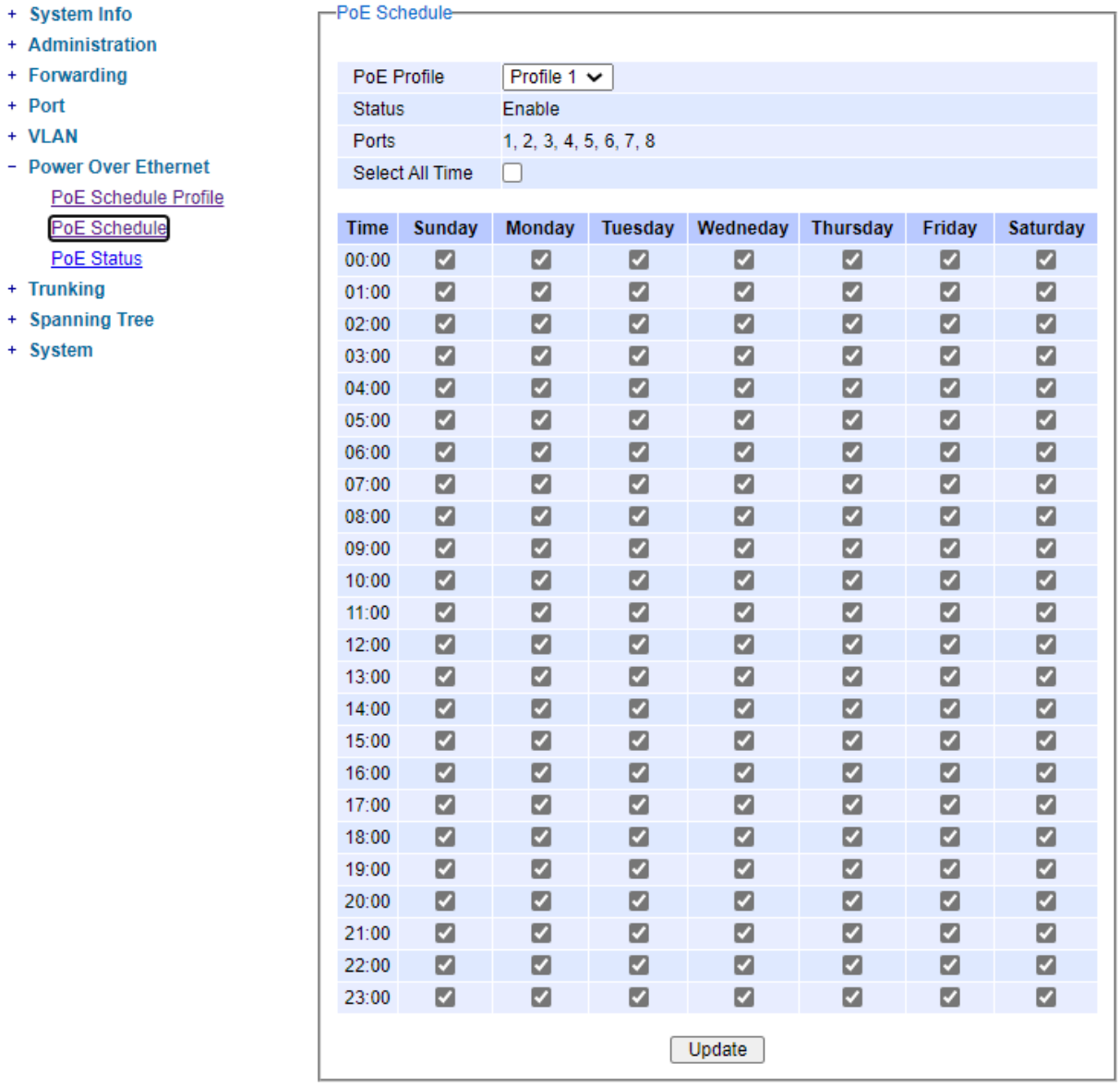


Figure 2.53 PoE Schedule Webpage with Example on EHG6510-4PoE-2SFP-24

2.7.3 *PoE Status*

This webpage summarizes the status of each PoE port as shown in Figure 2.54. 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 2.15 provides descriptions of each column in the table of PoE Status.

Table 2.15 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	-

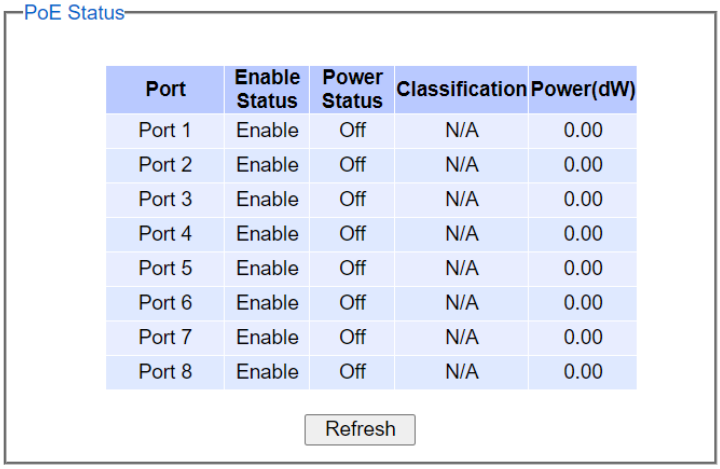


Figure 2.54 PoE Status Webpage

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 2.55 shows the Trunking dropdown menu.

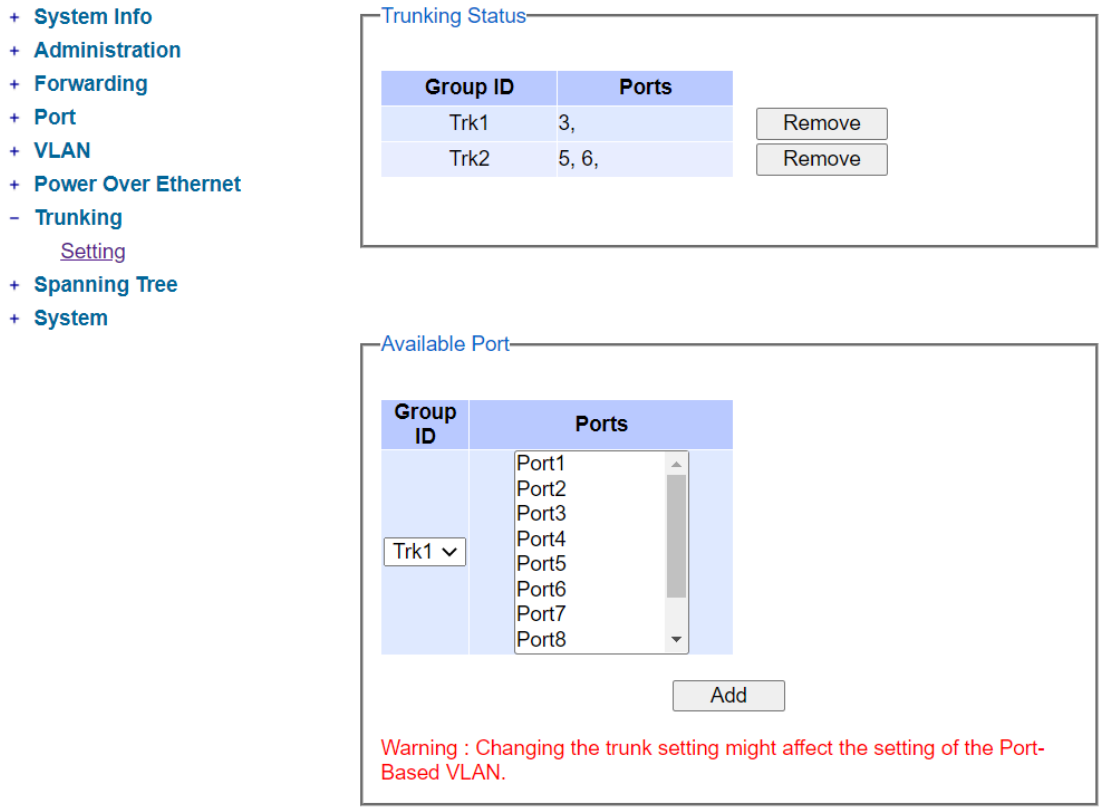


Figure 2.55 Trunking Dropdown Menu

2.8.1 Trunking Setting

In this subsection, the user can create new trunking assignment(s) and remove existing trunking assignment(s). Figure 2.56 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.

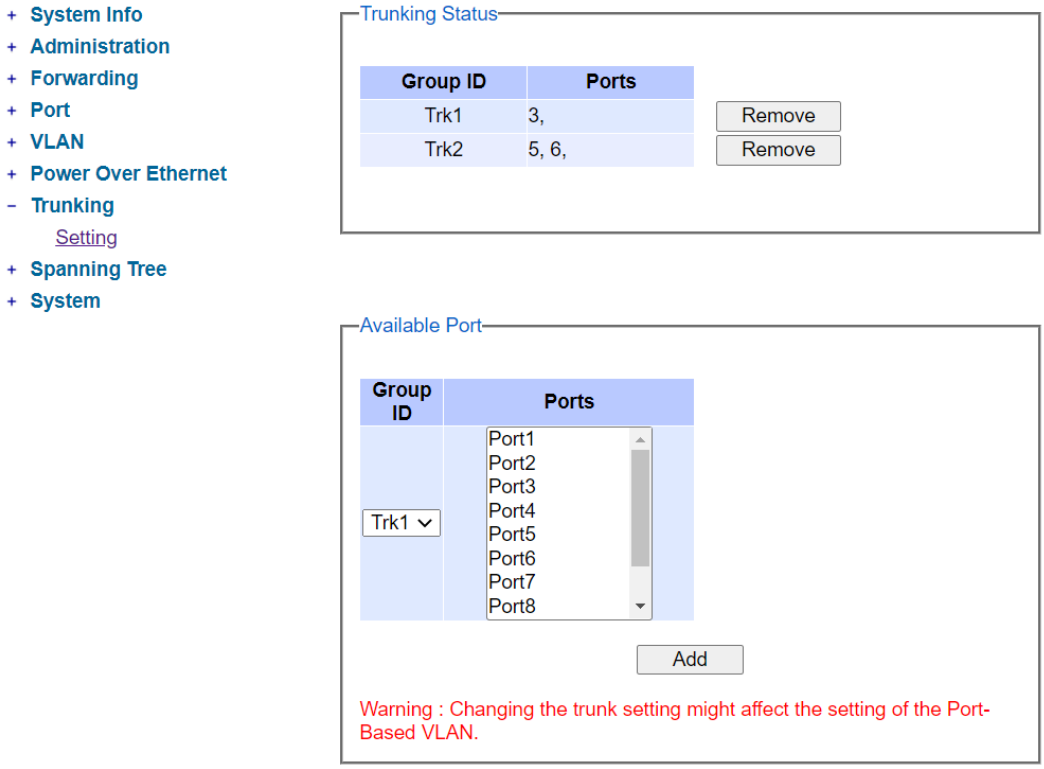


Figure 2.56 Trunking Setting Webpage with Example on EHG6510-4PoE-2SFP-24V

Descriptions of trunking settings are summarized in Table 2.16.

Table 2.16 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.
Apply	Click **Apply** 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 2.57 depicts the dropdown menu for Spanning Tree.

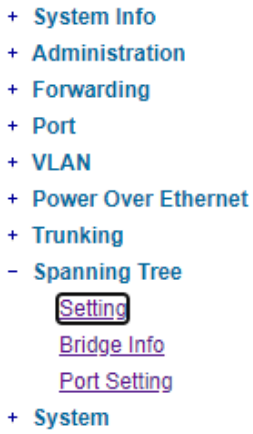


Figure 2.57 Spanning Tree Dropdown Menu

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 2.58 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.

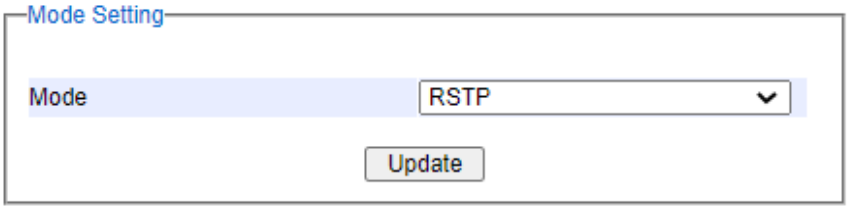


Figure 2.58 Spanning Tree Mode Setting

Under the mode setting, there is a box for Main Setting of spanning tree's parameters as showed in Figure 2.59. 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 2.17.

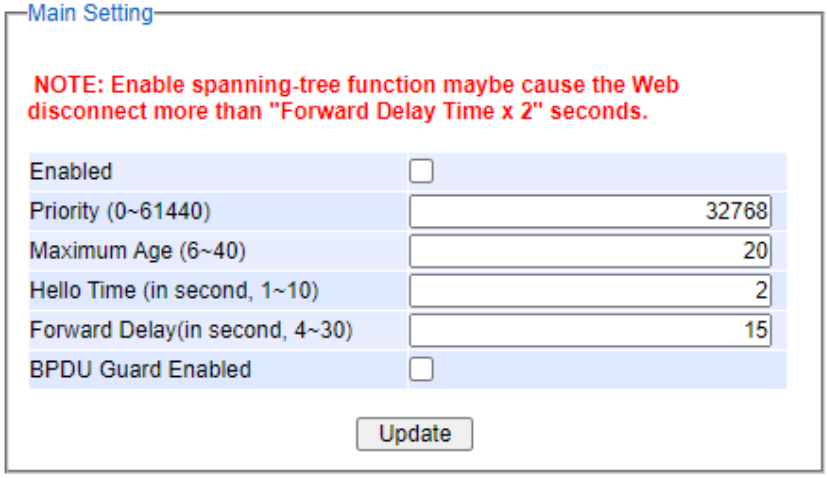


Figure 2.59 Spanning Tree Main Setting for RSTP

Table 2.17 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 2.60. 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.

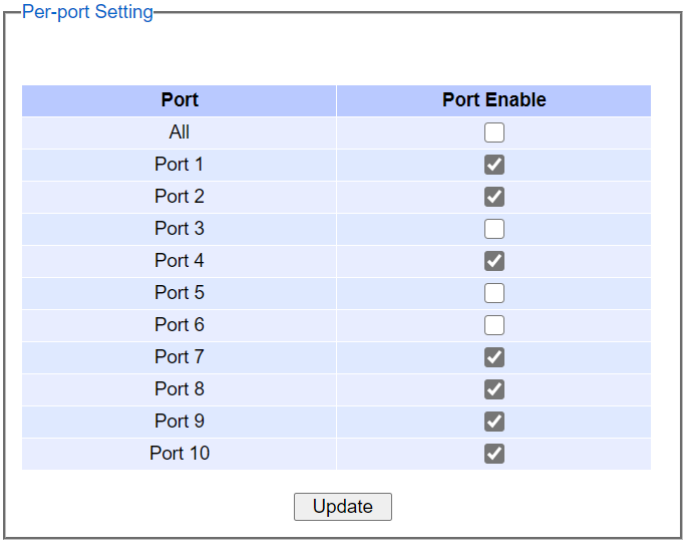


Figure 2.60 Spanning Tree Per-port Setting for STP and RSTP

2.9.2 Bridge Info

Bridge Info (information) provides the statistical value of spanning tree protocol as shown in Figure 2.61. 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 2.18 and Table 2.19 summarize the descriptions of each entry in the root information table and topology information table, respectively.

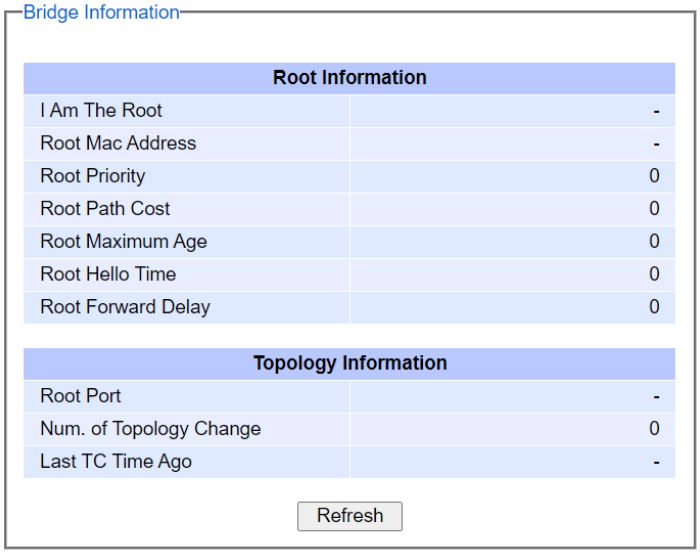


Figure 2.61 Bridge Information Webpage

Table 2.18 Bridge Root Information

Label	Description	Factory Default
I am the Root	Indicator that this switch is elected as the root switch of the spanning tree topology	-
Root MAC Address	MAC address of the root of the spanning tree	-
Root Priority	Root's priority value: The switch with highest priority has the lowest priority value and it will be elected as the root of the spanning tree.	0

Label	Description	Factory Default
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 2.19 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 2.62. 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 2.20 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.

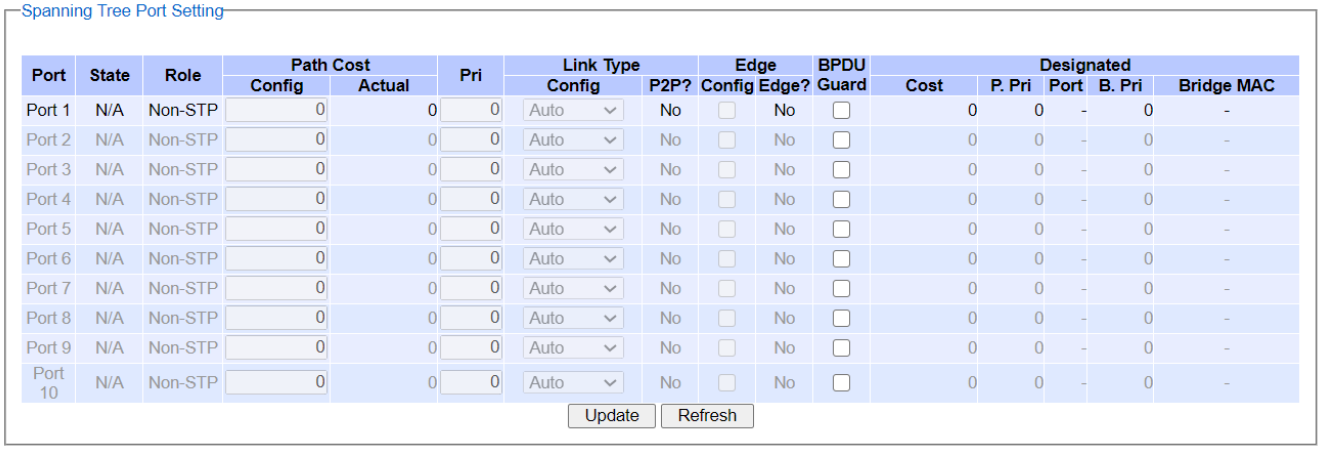


Figure 2.62 Spanning Tree Port Setting Webpage

Table 2.20 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 Table 2.21.)	0
Pri		Setting the port priority, used in the Port ID field of BPDU packet, value = 16 × N, (N:0~15) See Note 2 below.	128
Link Type		The connection between two or more switches (for RSTP)	
	Config	Setting of the Link Type **P2P:** A port that operates in full-duplex mode is assumed to be point-to-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 2.21 lists the default values of path cost for RSTP.

Table 2.21 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 System

This last section on the WebUI interface of the EHG65XX managed switch allows the administration to perform device maintenance operations such as backing up and restoring device's configuration, updating the firmware, reversing the device to factory default setting, or reboot the system/device. Figure 2.63 shows all the dropdown menus under the **System** section.

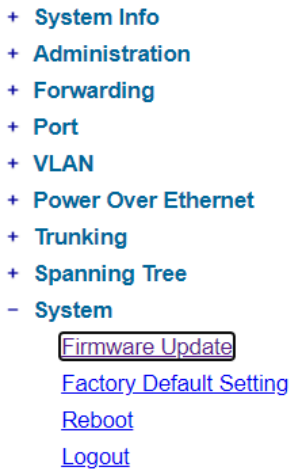


Figure 2.63 System Dropdown Menu

2.10.1 Backup/Restore

Figure 2.64 shows the **Backup/Restore** webpage for backing up or restoring the configuration via HTTP. It is divided into two parts: "Backup the Configuration" and "Restore the Configuration". When clicking the **Download** button on "Backup the Configuration" part, user will be downloading file IP-{current ip}.bin.

To restore a configuration file to the switch, go to "Restore the Configuration" part and click "**Browse**" button to choose a configuration file from the local drive. Then, select one of the two options from the checkbox on the lower part before clicking the "**Upload**" button. These two options are "Keep the current username and password setting" and "Keep the current network setting". This will allow user to log in with the previously stored username, password, and/or network configuration once the configuration is restored.

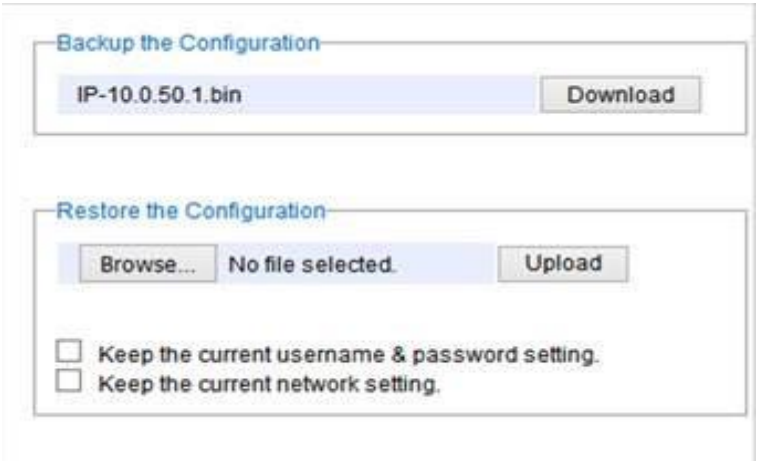


Figure 2.64 Backup/Restore Configuration via HTTP

2.10.2 Firmware Update

The users can update the device firmware via web interface as shown in Figure 2.65. 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 **Browse…** button and choose the firmware file that is already downloaded. The switch's firmware typically has a ".dld" extension such as EHG6510-8POE-2S.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.

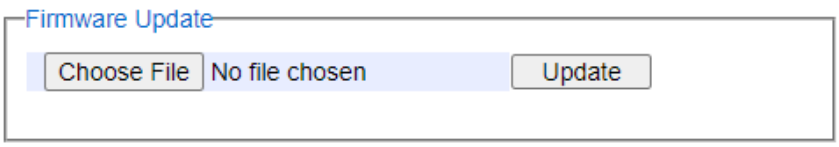


Figure 2.65 Firmware Update Webpage

2.10.3 Factory Default Setting

When the managed switch is not working properly, the users can reset it back to the original factory default settings by clicking on the **Reset** button as shown in Figure 2.66.

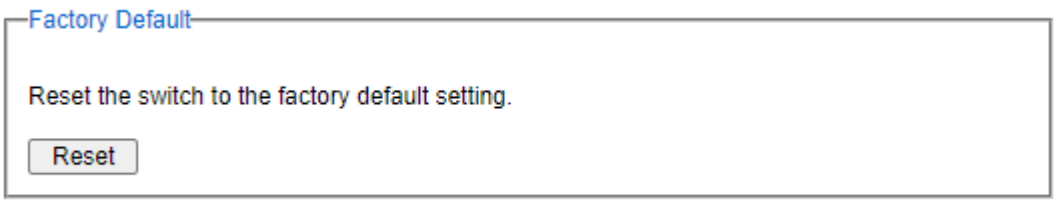


Figure 2.66 Factory Default Setting Webpage

2.10.4 Reboot

An easy reboot function is provided in this webpage requiring only one single click on the **Reboot** button as shown in Figure 2.67.

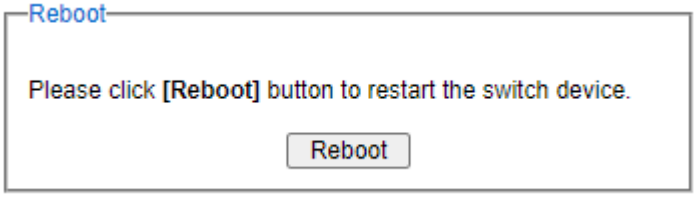


Figure 2.67 Reboot Webpage

2.10.5 Logout

An easy logout function is provided in this webpage requiring only one single click on the Logout button as shown in Figure 2.68.

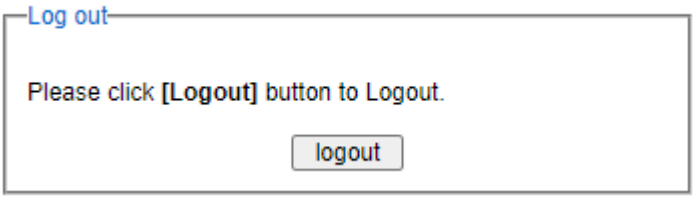


Figure 2.68 Logout Webpage

3 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.

4 Modbus Memory Map

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

Address	Data Type	Read/Write	Description
System Information			
0x0000 (0)	32 words	R	System Description = "Managed Switch EHG6510" Word 0 Hi byte = 'M' Word 0 Lo byte = 'a' Word 1 Hi byte = 'n' Word 1 Lo byte = 'a' Word 2 Hi byte = 'g' Word 2 Lo byte = 'e' Word 3 Hi byte = 'd' Word 3 Lo byte = ' ' Word 4 Hi byte = 'S' Word 4 Lo byte = 'w' Word 5 Hi byte = 'i' Word 5 Lo byte = 't' Word 6 Hi byte = 'c' Word 6 Lo byte = 'h' Word 7 Hi byte = ' ' Word 7 Lo byte = 'E' Word 8 Hi byte = 'H' Word 8 Lo byte = '6' Word 9 Hi byte = '5' Word 9 Lo byte = '1' Word 10 Hi byte = '0' Word 10 Lo byte = '\0'
0x0020 (32)	1 word	R	Firmware Version = Ex: Version = 1.02 Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x02
0x0021 (33)	3 words	R	Ethernet MAC Address Ex: MAC = 00-01-02-03-04-05 Word 0 Hi byte = 0x00 Word 0 Lo byte = 0x01 Word 1 Hi byte = 0x02 Word 1 Lo byte = 0x03 Word 2 Hi byte = 0x04 Word 2 Lo byte = 0x05
0x0024 (36)	1 word	R	Kernel Version Ex: Version = 1.03 Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x03
Console Information			
0x0030 (48)	1 word	R	Baud Rate 0x0000: 4800 0x0001: 9600

			0x0002: 14400 0x0003: 19200 0x0004: 28800 0x0005: 38400 0x0006: 57600 0x0007: 144000 0x0008: 115200
0x0031 (49)	1 word	R	Data Bits 0x0007: 7 0x0008: 8
0x0032 (50)	1 word	R	Parity 0x0000: None 0x0001: Odd 0x0002: Even
0x0033 (51)	1 word	R	Stop Bit 0x0001: 1 0x0002: 2
0x0034 (52)	1 word	R	Flow Control 0x0000: None
Power Information			
0x0040 (64)	1 word	R	Power Status Power 1 OK, Hi byte = 0x01 Power 1 Fail, Hi byte = 0x00 Power 2 OK, Low byte = 0x01 Power 2 Fail, Low byte = 0x00
IP Information			
0x0050 (80)	1 word	R	DHCP Status 0x0000: Disabled 0x0001: Enabled
0x0051 (81)	2 words	R	IP Address of switch Ex: IP = 192.168.1.1 Word 0 Hi byte = 0xC0 Word 0 Lo byte = 0xA8 Word 1 Hi byte = 0x01 Word 1 Lo byte = 0x01
0x0053 (83)	2 words	R	Subnet Mask of switch Ex: IP = 255.255.255.0 Word 0 Hi byte = 0xFF Word 0 Lo byte = 0xFF Word 1 Hi byte = 0xFF Word 1 Lo byte = 0x00
0x0055 (85)	2 words	R	Gateway Address of switch Ex: IP = 192.168.1.254 Word 0 Hi byte = 0xC0 Word 0 Lo byte = 0xA8 Word 1 Hi byte = 0x01 Word 1 Lo byte = 0xFE
0x0057 (87)	2 words	R	DNS1 of switch Ex: IP = 168.95.1.1 Word 0 Hi byte = 0xA8 Word 0 Lo byte = 0x5F Word 1 Hi byte = 0x01 Word 1 Lo byte = 0x01
0x0059 (89)	2 words	R	DNS2 of switch Ex: IP = 168.95.1.1

			Word 0 Hi byte = 0xA8 Word 0 Lo byte = 0x5F Word 1 Hi byte = 0x01 Word 1 Lo byte = 0x01
System Status Clear			
0x0100 (256)	1 word	W	Clear Port Statistics 0x0001: Do clear action
0x0101 (257)	1 word	W	Clear Relay Alarm 0x0001: Do clear action
0x0102 (258)	1 word	W	Clear All Warning Events 0x0001: Do clear action
Warning Events Information			
0x0200 (512)	64 words	R	1st Warning Event Information
0x0300 (768)	64 words	R	2st Warning Event Information
0x0400 (1024)	64 words	R	3st Warning Event Information
0x0500 (1280)	64 words	R	4st Warning Event Information
0x0600 (1536)	64 words	R	5st Warning Event Information
Port Status			
0x1000 (4096)	5 words	R	Port Status 0x0000: Disabled 0x0001: Enabled Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status
0x1020 (4128)	5 words	R	Port Negotiation Status, force = 0x00 Status, auto = 0x01 Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status
0x1040 (4160)	5 words	R	Port Speed Status, 10M = 0x01 Status, 100M = 0x02 Status, 1000M = 0x03 Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status

			Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status
0x1060 (4192)	5 words	R	Port Duplex Status, half-duplex = 0x00 Status, full-duplex = 0x01 Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status
0x1080 (4224)	5 words	R	Port Flow Control Status, disabled = 0x00 Status, enabled = 0x01 Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status
0x10A0 (4256)	5 words	R	Port Link Status Status, down = 0x00 Status, up = 0x01 Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status
0x1200 (4608)	20 words	R	Port TX rate Ex. Port 1 runs at TX Rate(1024 Kbps = 0x400). Word 0 of Port 1 = 0x0000 Word 1 of Port 1 = 0x0400 Word 0,1 = Port 1 TX Rate Word 2,3 = Port 2 TX Rate Word 4,5 = Port 3 TX Rate Word 6,7 = Port 4 TX Rate Word 8,9 = Port 5 TX Rate Word 10,11 = Port 6 TX Rate Word 12,13 = Port 7 TX Rate Word 14,15 = Port 8 TX Rate

			Word 16,17 = Port 9 TX Rate Word 18,19 = Port 10 TX Rate
0x1280 (4736)	20 words	R	Port RX rate Ex. Port 1 runs at RX Rate(1024 Kbps = 0x400). Word 0 of Port 1 = 0x0000 Word 1 of Port 1 = 0x0400 Word 0,1 = Port 1 RX Rate Word 2,3 = Port 2 RX Rate Word 4,5 = Port 3 RX Rate Word 6,7 = Port 4 RX Rate Word 8,9 = Port 5 RX Rate Word 10,11 = Port 6 RX Rate Word 12,13 = Port 7 RX Rate Word 14,15 = Port 8 RX Rate Word 16,17 = Port 9 RX Rate Word 18,19 = Port 10 RX Rate
0x1300 (4864)	40 words	R	Count of Good Packets of TX Ex. Port 1 gets 0x2EEEE1FFFF good packets of TX. Word 0 of Port 1 = 0x0000 Word 1 of Port 1 = 0x002E Word 2 of Port 1 = 0xEEE1 Word 3 of Port 1 = 0xFFFF Word 0,1,2,3 = Port 1 good packets Word 4,5,6,7 = Port 2 good packets Word 8,9,10,11 = Port 3 good packets Word 12,13,14,15 = Port 4 good packets Word 16,17,18,19 = Port 5 good packets Word 20,21,22,23 = Port 6 good packets Word 24,25,26,27 = Port 7 good packets Word 28,29,30,31 = Port 8 good packets Word 32,33,34,35 = Port 9 good packets Word 36,37,38,39 = Port 10 good packets
0x1400 (5120)	40 words	R	Count of Bad Packets of TX Ex. Port 1 gets 0x2EEEE1FFFF bad packets of TX. Word 0 of Port 1 = 0x0000 Word 1 of Port 1 = 0x002E Word 2 of Port 1 = 0xEEE1 Word 3 of Port 1 = 0xFFFF Word 0,1,2,3 = Port 1 good packets Word 4,5,6,7 = Port 2 good packets Word 8,9,10,11 = Port 3 good packets Word 12,13,14,15 = Port 4 good packets Word 16,17,18,19 = Port 5 good packets Word 20,21,22,23 = Port 6 good packets Word 24,25,26,27 = Port 7 good packets Word 28,29,30,31 = Port 8 good packets Word 32,33,34,35 = Port 9 good packets Word 36,37,38,39 = Port 10 good packets
0x1500 (5376)	40 words	R	Count of Good Packets of RX Ex. Port 1 gets 0x2EEEE1FFFF good packets of RX. Word 0 of Port 1 = 0x0000 Word 1 of Port 1 = 0x002E Word 2 of Port 1 = 0xEEE1 Word 3 of Port 1 = 0xFFFF Word 0,1,2,3 = Port 1 good packets Word 4,5,6,7 = Port 2 good packets

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

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