Atop Technologies, Inc.

NSG330X
Gigabit Ethernet Switch with NAT

User Manual

V0.3

May 24th, 2022

Series covered by this manual:
NSG3308/NSG3309

* 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
www.atop.com.tw

Important Announcement

The information contained in this document is the property of ATOP Technologies, Inc., and is supplied for the sole purpose of operation and maintenance of ATOP Technologies, Inc., products.
No part of this publication is to be used for any other purposes, and it is not to be reproduced, copied, disclosed, transmitted, stored in a retrieval system, or translated into any human or computer language, in any form, by any means, in whole or in part, without the prior explicit written consent of ATOP `Technologies, Inc.,
Offenders will be held liable for damages and prosecution.
All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Disclaimer

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

Preface

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

Who Should Use This User Manual

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

Warranty Period

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

Documentation Control

Author:	Saowanee Saewong
Revision:	0.3
Revision History:	Initial
Creation Date:	10 December 2021
Last Revision Date:	24 May 2022
Product Reference:	Gigabit Ethernet Switch with NAT - NSG series
Document Status:	Internal

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Introduction to Gigabit Ethernet Switch with NAT

ATOP's NAT NSG-3300X series are product lines of NAT industrial switch which are referred to as Open Systems Interconnection (OSI) Layer 2 bridging and Layer 3 NAT devices.

ATOP's switch is also an industrial switch and not a typical 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 NAT switch works fine even in these environments.

ATOP's switch supports essential 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 easy network management experience with robustness.

1.2 Software Features

ATOP's NAT Switches come with essential network protocols and software features. These protocol and software features allow the network administrator to implement security and reliability into their network with ease. These features enable Atop's NAT switch to be used in safety applications, and factory and process automation. The followings are the list of protocols and software features.

- User Interfaces
  - Web browser
- Dynamic Host Configuration Protocol (DHCP) Client
- Layer-2 Switching
- NAT Translation
- DMZ
- Mirror Port
- Time Synchronization
  - Network Time Protocol (NTP) Server/Client
  - Simplified Network Time Protocol (SNTP)
- Virtual Local Area Network (VLAN)
- Rapid Spanning Tree Protocol (RSTP)
- Security
  - ACL
- Simple Network Management Protocol (SNMP) v1/v2/v3 (with MD5 Authentication and DES encryption)
- SNMP Trap Inform
- Link Layer Discovery Protocol (LLDP)
- DHCP Mapping

2 Configuring with a Web Browser

Chapter 2 explains how to access the industrial smart switch for the first time by using the web browser.
The web browser allows users to access the switch over the Internet or the Ethernet LAN which has a user-friendly interface.

2.1 Web-based Management Basics

Users can access the NAT switch easily by using their web browsers (Internet Explorer 11, Edge 96, Firefox 95, Chrome 96 or later versions are recommended). We will proceed to use a web browser to introduce the NAT 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. Table 2.1 summarizes the default IP setting for NSG series.

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

Table 2.1 Default Setting for IP Network on NSG Series

Model Name	Default IP Setting			
	IP	Netmask	Gateway	Default DNS
NSG3308	10.0.50.1	255.255.0.0	0.0.0.0	0.0.0.0
NSG3308-2SFP	10.0.50.1	255.255.0.0	0.0.0.0	0.0.0.0
NSG3309	10.0.50.1	255.255.0.0	0.0.0.0	0.0.0.0
NSG3309-2SFP	10.0.50.1	255.255.0.0	0.0.0.0	0.0.0.0

2.1.2 Login Process and Main Window Interface

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

1. Launch a web browser.
2. Type in the switch IP address (e.g. http://10.0.50.1), as shown in Figure 2.1 and Figure 2.2).
   Note: After pressing the Enter key, the login page will be shown. The user has to input the default password which is set to "default".

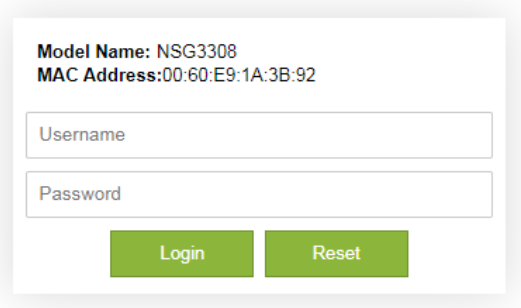


Figure 2.1 Login Page for Web-based Setting of NSG3308

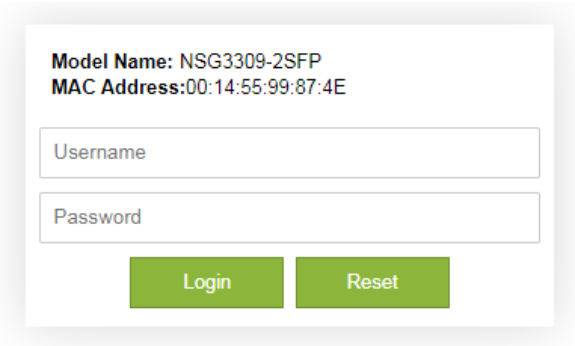


Figure 2.2 Login Page for Web-based Setting of NSG3309-2SFP

After the login process, the main interface will show up for NSG3308 and NSG3309-2SFP, as shown in Figure 2.3 and Figure 2.4, respectively. The main menu (left side of the screen) provides the links at the top-level links of the menu hierarchy and by clicking on each item it allows lower-level links to be displayed. Note that the difference between NSG3308 and NSG3309-2SFP is that the NSG3309-2SFP will have **Port Setting** menu for its optical fibre ports.

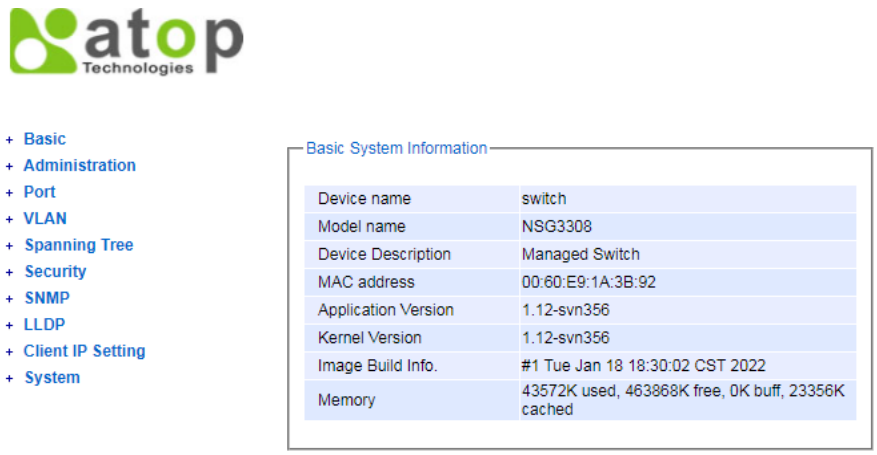


Figure 2.3 Default Web Interface of NSG3308

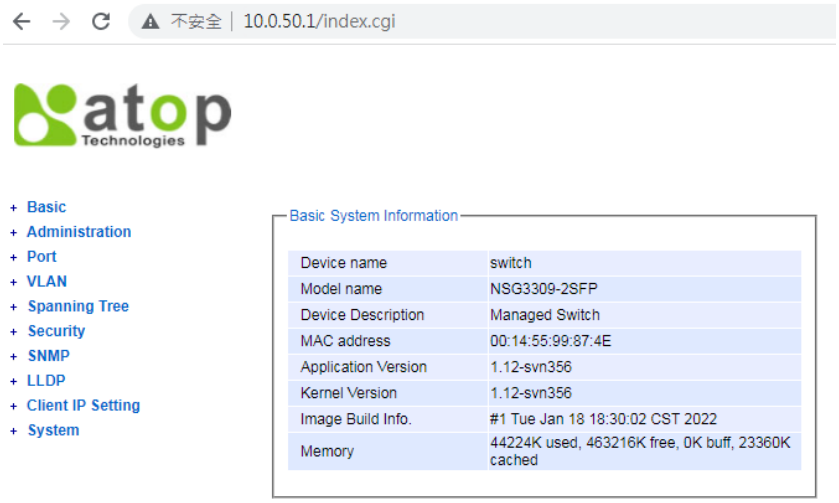


Figure 2.4 Default Web Interface of NSG3309-2SFP

2.1.3 Basic System Info

To help users become familiar with the device, the **System Information** or **System Info** subsection within **Basic** section provides important details of the ATOP's industrial smart secure 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 user can check various information such as the **Model Name**, **MAC Address**, **Application Version**, **Kernel Version**, **Image Build Information** and **Memory**. Figure 2.5 depicts an example of System Information of NSG3308. Table 2.2 summarizes the description of each field of the system information.

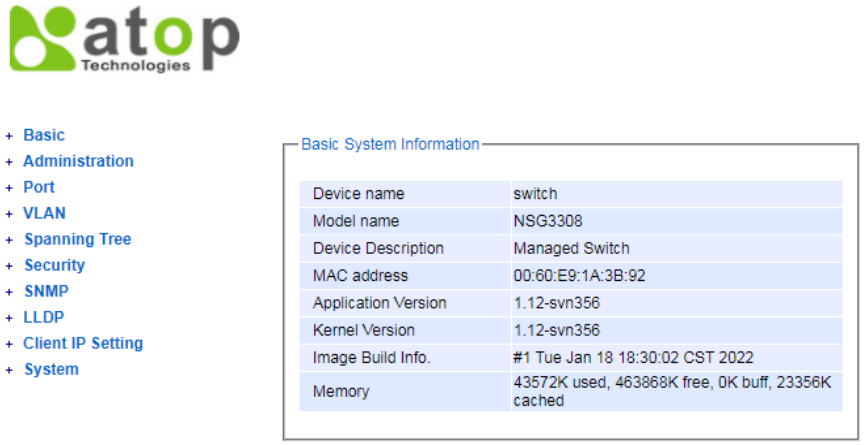


Figure 2.5 Details of System Info Webpage

Table 2.2 Descriptions of the Basic information

Label	Description
Device name	The device's given name which can be set by the user.
Model name	The device's complete model name
Device Description	The model type of the device
MAC address	The MAC address of the device
Application Version	The current application version of the device.
Kernel Version	The current kernel version of the device.
Image Build Info.	Information about the firmware image such as date of creation
Memory	The current RAM 's availability and the size of cached and shared memory.

2.1.4 Power Status

The power status of ATOP's NSG330x is provided in the **Power Status** subsection within **Basic** section. The NAT switch features dual VDC power supply inputs. 9-48VDC can be supplied to Power Input 1 (V1+ and V1- pins) and/or Power Input 2 (V2+ and V2- pins). Figure 2.6 shows the status of each power input. A "**Fault**" status means that the power on that supply input is either not connected or the power is not supplied properly.

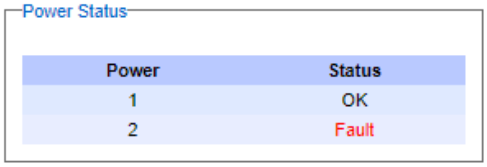


Figure 2.6 Power Status Webpage

2.2 Administration

2.2.1 Account

The users with administration access right can create and delete accounts through **Account** Section. As shown in Figure 2.7, there are total of four section boxes inside **Account** page as follows: **Account list**, **Add account**, **Change password** and **Password strength configuration.** In **Account List** box (1st box in Figure 2.7), usernames and their access rights are listed here. Within this box, each username except the admin user has a checkbox in the last column, which is named "Delete". There are two types of access right: **admin** and **user**. The **admin**'s access right has **read/write** permission on the NAT switch while the **user**'s access right has only **read** permission. If the user with administration access right would like to delete any account except the admin user, the user can select the account that would like to delete and click "**Delete**" button. Note that the user cannot delete his/her own account. The user whose account was deleted will be logged out immediately.

In the **Add account** box (2nd box of Figure 2.7), the currently logged in user can add a new user account using the following method. First, the logged in user have to input a new username and password in the **Username** textbox and the **Password** textbox respectively for this new account. Then, the logged in user have to select an appropriate **Access Right** from the drop-down list before clicking **Add** button. After clicking it, a new account will be created in the **Account List** box. An "admin" user with an "admin" **Access Right** is created as the default. The maximum number of accounts is 15 accounts.

If the logged in user wishes to change password for any account, he/she must have the admin access right. The password can be edited in the **Change password** box (3rd box of Figure 2.7). Here, the logged in user has to select a user name of the account that he/she would like to edit the password from the **Username** dropdown box first. Then, the logged in user has to input a new password in the **New password** textbox and re-entering the same password in the **Confirm password** textbox. Only a user with the admin access right can set a new level of password strength through the **Password strength configuration** box (the last box of Figure 2.7). Here, the **Minimum length** and the **Maximum length** of passwords for all users can be set. In case that a user without the administration access right try to edit the password strength configuration, the message "Only admin can modify it. Access denied." will show up.

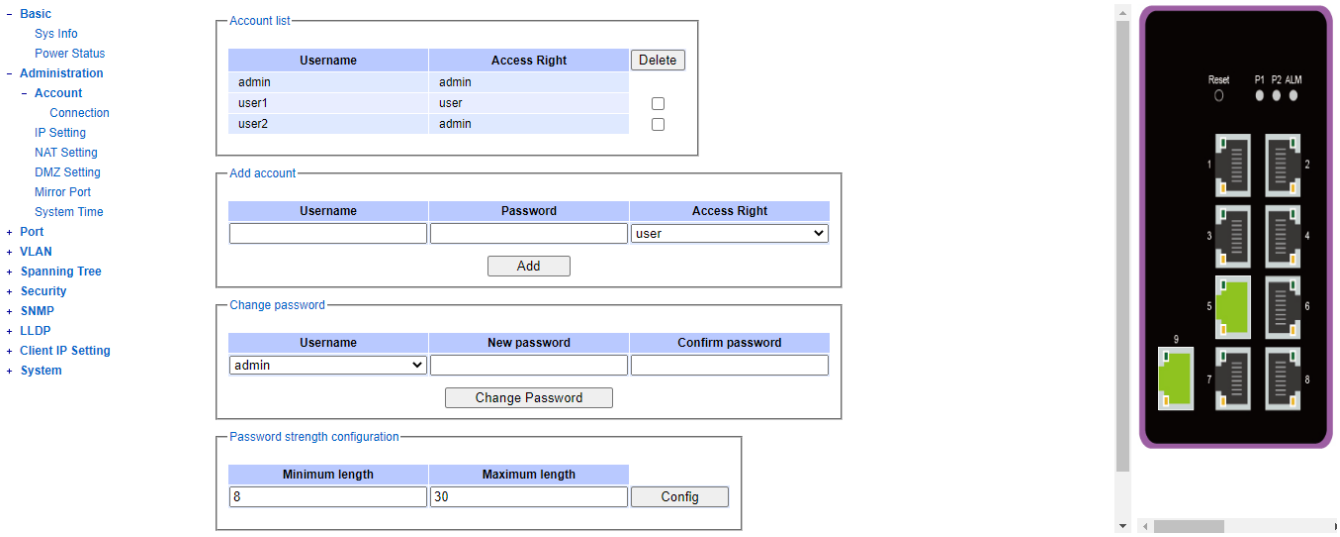


Figure 2.7 Account Setting Webpage

2.2.2 Connection

The **Connection** sub-menu under the **Administration->Account** menu lists the users who currently access the device under the **Connection Management** box. Inside the box, the table lists the information of the users with four columns: **Username**, **Access Right**, **Session**, and **Source IP**, as shown in Figure 2.8.

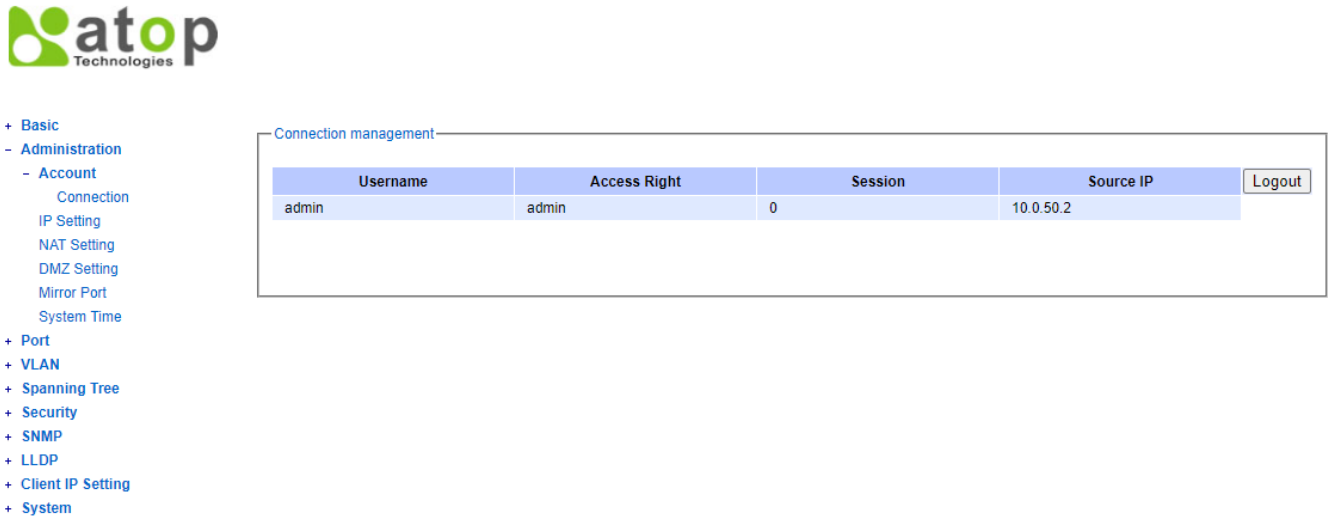


Figure 2.8 Connection Management Webpage

2.2.3 IP Setting

In this subsection, a user may modify network settings of Internet Protocol version 4 (IPv4), assign an IP interface address to a virtual local area network (VLAN) group, and check current network setting information of the NAT switch. On the switch, users can configure multiple IP interface addresses, where each IP address has a separated subnet.

This subsection is divided into three boxes: **IP Setting**, **IP Interface,** and **Current Information**. The IP Setting box is depicted in Figure 2.9. A user can input IP addresses of **Gateway**, the **Primary DNS** and the **Secondary DNS**. Change will take effect after clicking the **Update** button at the bottom of the box. If these static values are set, NAT switch will not retrieve IP addresses of gateway and DNS from the DHCP server.

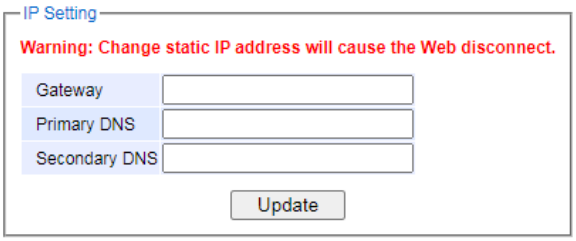


Figure 2.9 IP Setting Box under IP Setting Webpage

The second box of the IP Setting section is the **IP Interface** as shown in Figure 2.10. The box is separated into top and bottom part. At the top part of the box, if a user enables Dynamic Host Configuration Protocol (DHCP) by clicking on the **DHCP** box option to reduce an administrator's work, he/she will no longer able to enter a static IP address and a subnet mask of the VLAN ID (VID). The only field that can be selected is the **VID** which means that the VID will obtain the IPv4 address automatically for its interface. However, if the DHCP is disabled, a user can configure an IP Interface address for each VID. To change an IPv4 address of the NAT switch (default is 10.0.50.1), a user can enter a new **Static IP Address** and a new **Subnet Mask**, and select **VID = 1** from the drop-down list before clicking the **Update** button. Note that 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 NAT switch is changed. At the bottom part, there is a table that lists the current IP interface information of already configured VIDs. Note that a user can configure IP interface address for VLAN ranging from 1 to 4094, where the maximum number of IP interface is 32. If a user wishes to remove an IP interface setting of any VID in the table, he/she can simply remove that entry by clicking on the **Remove** button located at the end of each entry.

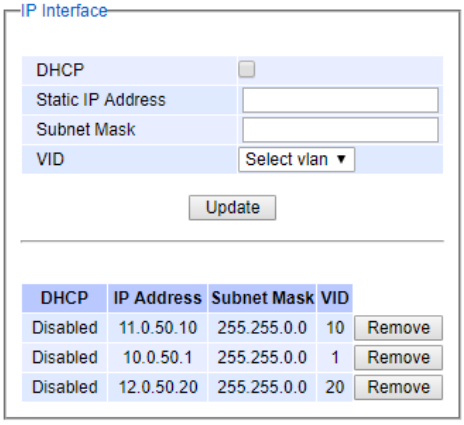


Figure 2.10 IP Interface Box under IP Setting Webpage

The third box of the IP Setting section is the **Current Information** as shown in Figure 2.10. In this box, there is a table lists the **Current Information** of each VLAN Identification number (VID) at the top part, which includes its **IP Address, Subnet Mask**, and **VID**. The **DHCP** column in the front helps users to identify whether the DHCP function of VID in that entry is enabled or disabled. At the bottom part, the information of the current setting of the **Gateway,** the **Primary DNS** and the **Secondary DNS** are shown.

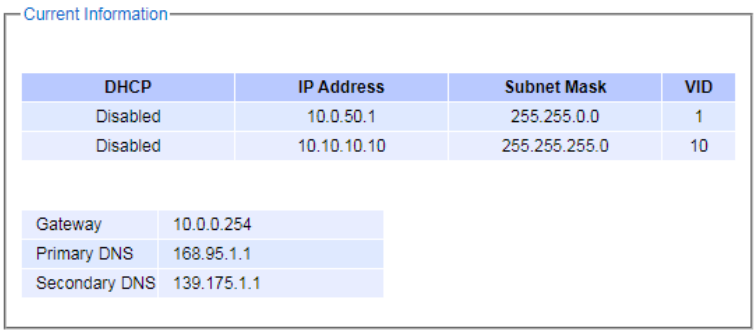


Figure 2.11 Current Information Box under IP Setting Webpage

The description of each field and its default value in the IP Setting webpage are summarized in Table 2.3.

Table 2.3 Description of Fields in the IP Setting Webpage

Label	Description	Factory Default
DHCP	By selecting this box (Checked), 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 the current IP address. Users can also set a new static IP address for the device.	10.0.50.1
Subnet Mask	Display the current Subnet Mask or set a new subnet mask	255.255.0.0
Gateway	Display/Set an IP address of the current Gateway	0.0.0.0
Primary DNS	Display/Set an IP address of the primary DNS. The Ethernet switch will locate the primary DNS server to be used by your network.	NULL
Secondary DNS	Display/Set an IP address of the secondary DNS. The Ethernet switch will locate the secondary DNS server if it fails to connect to the Primary DNS Server.	NULL
VID	Virtual Local Area Network (VLAN) Identification number (ID) is the ID value for VLAN that is needed to be configured with an IPv4 address.	NULL

2.2.4 NAT Setting

Network address translation (**NAT**) is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.[1] The technique was originally used to avoid the need to assign a new address to every host when a network was moved, or when the upstream Internet service provider was replaced, but could not route the networks address space. It has become a popular and essential tool in conserving global address space in the face of IPv4 address exhaustion. One Internet-routable IP address of a NAT gateway can be used for an entire private network.

As network address translation modifies the IP address information in packets, NAT implementations may vary in their specific behaviour in various addressing cases and their effect on network traffic.

ATOP's NAT NSG330x Series switch support three different modes of NAT setting: 1 to 1 NAT, Virtual NAT, and IP Masquerade.

- 1 to 1 NAT: This setting creates a WAN interface that uses the 1:1 NAT mechanism to translate IP addresses from a LAN area to the WAN.
- Virtual NAT: This setting creates a WAN interface that uses the virtual NAT mechanism to translate IP addresses from a LAN area to the WAN. Virtual NAT does not depend on individual instances such as VMs or a single physical gateway device. A NAT gateway will not affect the network bandwidth of your computer

resources. Software defined networking makes a NAT gateway highly resilient.

- IP Masquerade: This setting creates a WAN interface that uses the IP masquerading mechanism to translate IP addresses from a LAN area to the WAN. Masquerade NAT allows you to translate multiple IP addresses to another single IP address, allowing NAT to hide one or more IP addresses on an internal network behind a public IP address.

Note: Before setting NAT rules, users must configure VLAN ID and PVID for ports that NAT rules will be applied to. These settings are under **VLAN->802.1Q VLAN** menu. VLAN ID Setting is in **Setting** submenu, as shown in Figure 2.12. Whereas, PVID setting is under the **PVID Setting** submenu, as shown in Figure 2.13. After VLAN ID and PVID are configured, the system will create NAT rule automatically. Figure 2.14 depicts an example of NAT interface table. The table lists NAT interface information such as an **interface number**, **mode**, **VID**, **IP address**, **Subnet Mask**, and **DHCP status**.

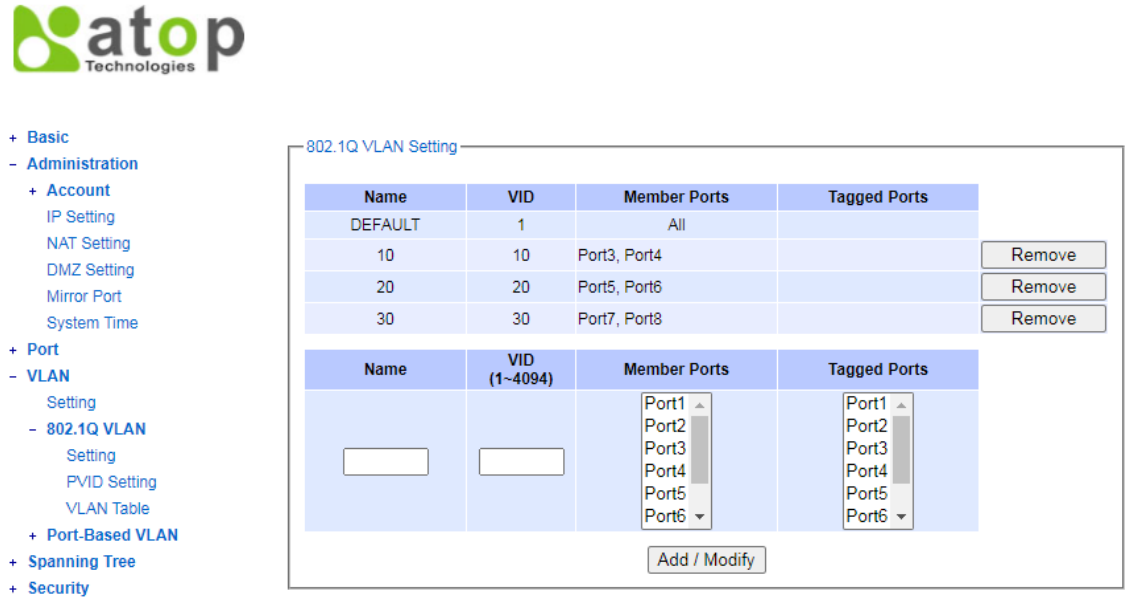


Figure 2.12 Example of VLAN Setting for NAT Rules

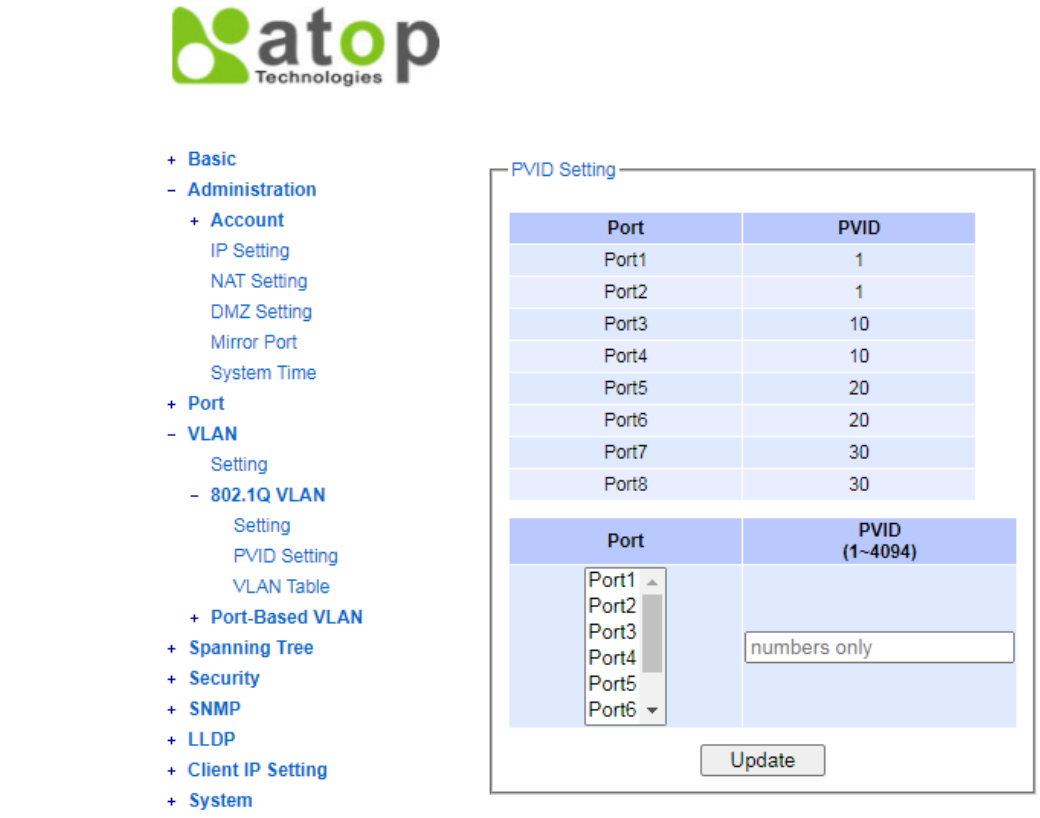


Figure 2.13 Example of PVID Setting for NAT Rules

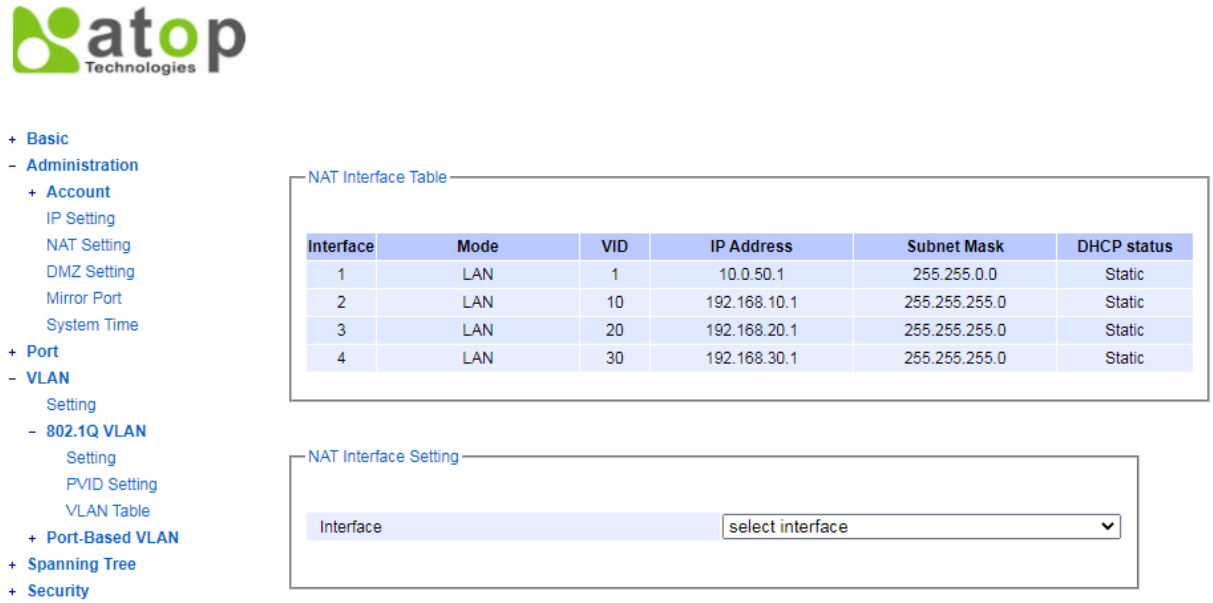


Figure 2.14 Example of NAT Interface Table

2.2.4.1 1-1 NAT

In **1-1 NAT** mode, an IP address of each device's LAN is assigned by the higher-level network (WAN). Traffic are directed to a LAN interface through the WAN interface. In WAN configuration, users do not need to set a route/gateway configuration of LAN interfaces. Traffic will be directed automatically using NAT table. Communication can be established from both LAN and WAN interfaces. An IP address must be reserved for the WAN interface.

User can change the interface mode to 1-1 NAT by choosing an interface number from the drop-down menu of the **interface** field within **NAT Interface Setting** box. Afterwards, the interface mode field and the NAT configuration field

will be appeared. **1-1 NAT** is a default value of the interface mode field, and the 1-1 NAT Setting's web-link will be shown at the right of the **NAT Configuration** field, as shown in Figure 2.15.

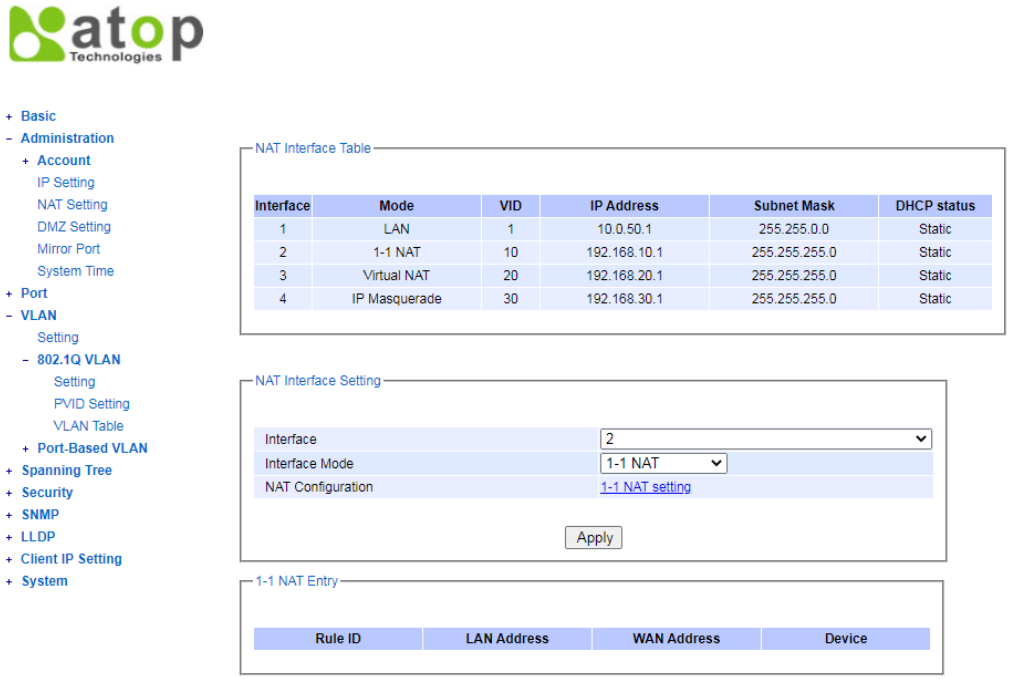


Figure 2.15 Example of NAT Interface Setting for 1-1 NAT Mode

By clicking the link, a new webpage will be displayed. There will be two boxes in that webpage; i.e., **Add new 1-1 NAT Entry**, and **1-1 NAT Entry,** as shown in Figure 2.16. In the **Add new 1-1 NAT Entry** box, there are five fields: **Interface**, **IP address**, **Start LAN IP Address**, **Start WAN IP Address**, and **Device Range**. In the first two fields, the current settings are displayed and cannot be modified. Users can add new NAT rules for the listed Interface by entering new values for the other three fields. The WAN IP Address has to be in the same subnet with the WAN device. After input new values and clicking the **APPLY** button, a new NAT entry will be added to the **1-1 NAT Entry** box. Users are allowed to add more than one new NAT rule. If users wish to remove any entry in the **1-1 NAT Entry** box, users can simply click the **Remove** button at the right most column of the box. Here, users can go back to the previous webpage (the Administration-> NAT setting webpage) by clicking the **NAT Interface Setting** button at the bottom of the box.

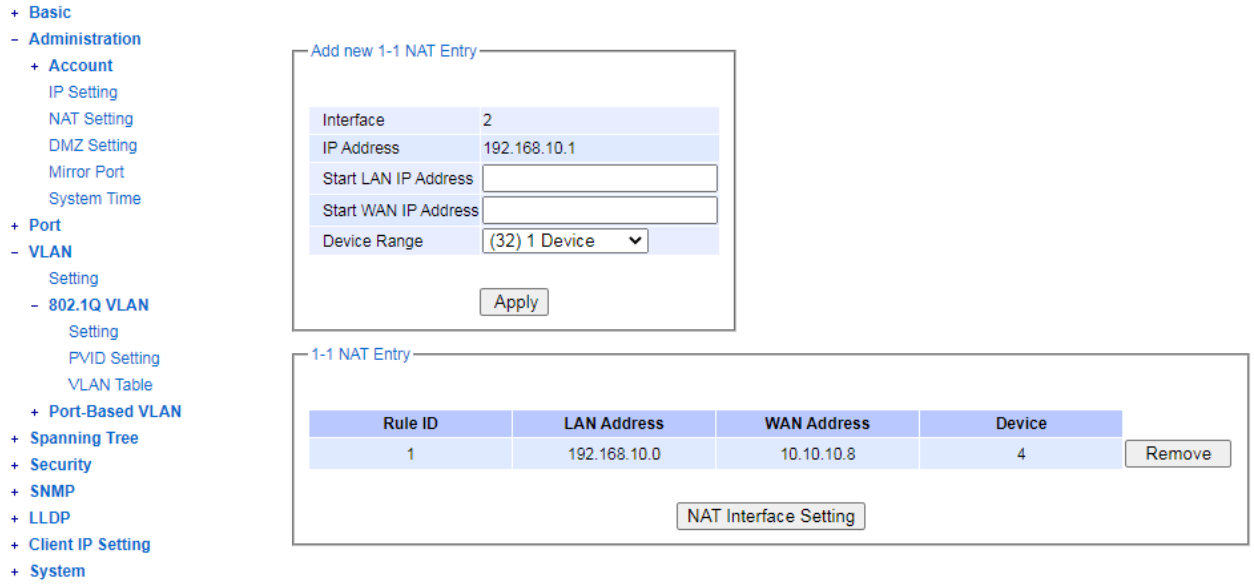


Figure 2.16 Example of 1-1 NAT Entry

2.2.4.2 Virtual NAT

In the **Virtual NAT** mode, 1:1 NAT function is combined with function of a virtual router. LAN traffic are directed to a WAN interface using NAT table in the virtual intermediate level. At this mode, only one IP address is required for the WAN interface. In WAN configuration, users must indicate route to the virtual network, and enter an address of NAT WAN interface as the next hop or gateway.

User can change the interface mode to Virtual NAT by choosing an interface number from the drop-down menu of the **interface** field within **NAT Interface Setting** box. Afterwards, the interface mode field and the NAT configuration field will be appeared. **1-1 NAT** is a default value of the interface mode field. Click on its drop-down menu to change the value to **Virtual NAT**. 1-1 NAT Setting's web-link is the default value of the **NAT Configuration** field. By clicking **Apply** button the value on the right of NAT Configuration field is changed to **Virtual NAT Setting**, as shown in Figure 2.17. By clicking the link, a new webpage will be displayed. There will be two boxes in that webpage; i.e., **Virtual NAT Setting**, and **Virtual NAT,** as shown in Figure 2.18. In the **Virtual NAT Setting** box, there are five fields: **Interface**, **IP address**, **LAN Start IP**, **Virtual Network**, and **Device Range**. In the first two fields, the current settings are displayed and cannot be modified. Users can add new Virtual NAT rules for the listed Interface by entering new values for the other three fields. The WAN IP Address has to be in the same subnet with the WAN device. After input new values and clicking the **Apply** button, a new Virtual NAT entry will be added to the **Virtual NAT** box. Users are allowed to add more than one new Virtual NAT rule. If users wish to remove any entry in the **Virtual NAT** box, users can simply click the **Remove** button at the right most column of the box. Here, users can go back to the previous webpage (the Administration-> NAT setting webpage) by clicking the **NAT Interface Setting** button at the bottom of the box.

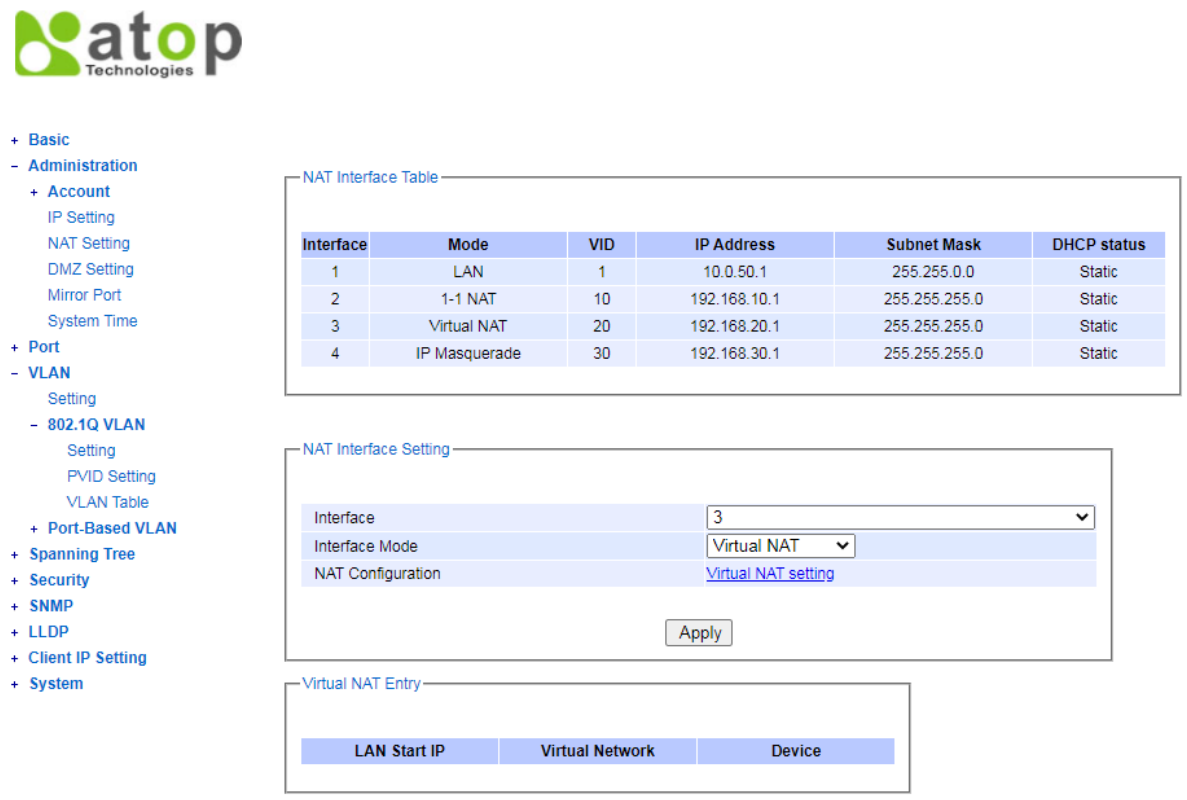


Figure 2.17 Setting Example of NAT Interface for Virtual NAT Mode

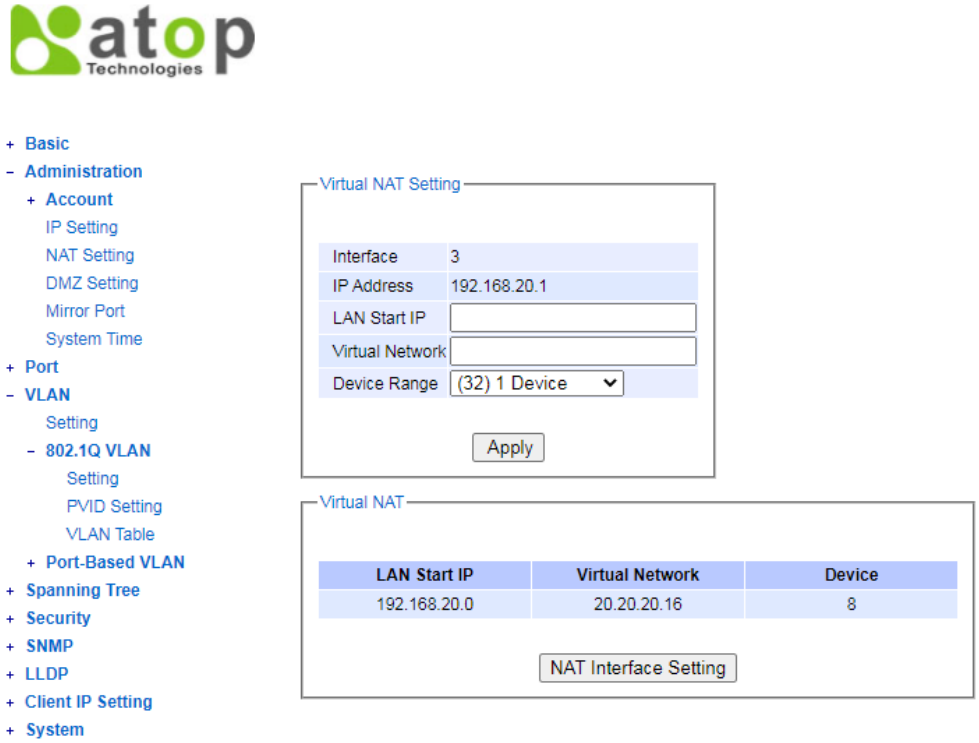


Figure 2.18 Example of Virtual NAT Entry

2.2.4.3 IP Masquerade

NAT device will act as a proxy in an IP Masquerade mode. Traffic from all LAN interfaces will be directed to the external through an IP address of the NAT/WAN port. The connected LAN devices are differentiated using TCP/UDP ports.

At this mode, users do not require any additional WAN addresses. Only an WAN address for NAT device itself is required. Also, users do not need to set route/gateway in the WAN configuration. However, WAN connected devices can only communicate with LAN connected devices via port forwarding.

User can change the interface mode to IP Masquerade by choosing an interface number from the drop-down menu of the **interface** field within **NAT Interface Setting** box. Afterwards, the interface mode field and the NAT configuration field will be appeared. **1-1 NAT** is a default value of the interface mode field. Click on its drop-down menu to change the value to **IP Masquerade**. 1-1 NAT Setting's web-link is the default value of the **NAT Configuration** field. By clicking **Apply** button the value on the right of NAT Configuration field is changed to **Port Forwarding setting**, as shown in Figure 2.19. By clicking the link, a new webpage will be displayed. There will be two boxes in that webpage; i.e., **Add New Port Forwarding Entry**, and **NAT Port Forwarding Entry,** as shown in Figure 2.20. In the **Add New Port Forwarding Entry** box, there are six fields: **Interface**, **IP address**, **Out IP Address**, **In TCP/UDP Port**, **Out TCP/UDP Port**, and **Protocol**. In the first two fields, the current settings are displayed and cannot be modified. Users can add new IP Masquerade rules for the listed Interface by entering new values for the other next three fields and choose protocol type for the last field. Users can enter an IP address of a LAN device in **Out IP Address** field, and input an incoming target port number on the WAN side in **In TCP/UDP Port** field. In **Out TCP/UDP Port** field, users should enter the port number for forwarding traffic to the connected LAN device. In the last field, Protocol, users can choose protocol type whether it is TCP or UDP or Both from the drop-down menu. After input new values and clicking the **Apply** button, a new NAT Port Forwarding rule will be added to the **NAT Port Forwarding entry** box. Users are allowed to add more than one new NAT Port Forwarding rule. If users wish to remove any entry in the **NAT Port Forwarding entry** box, users can simply click the **Remove** button at the right most column of the box. Here, users can go back to the previous webpage (the Administration-> NAT setting webpage) by clicking the **NAT Interface Setting** button at the bottom of the box.

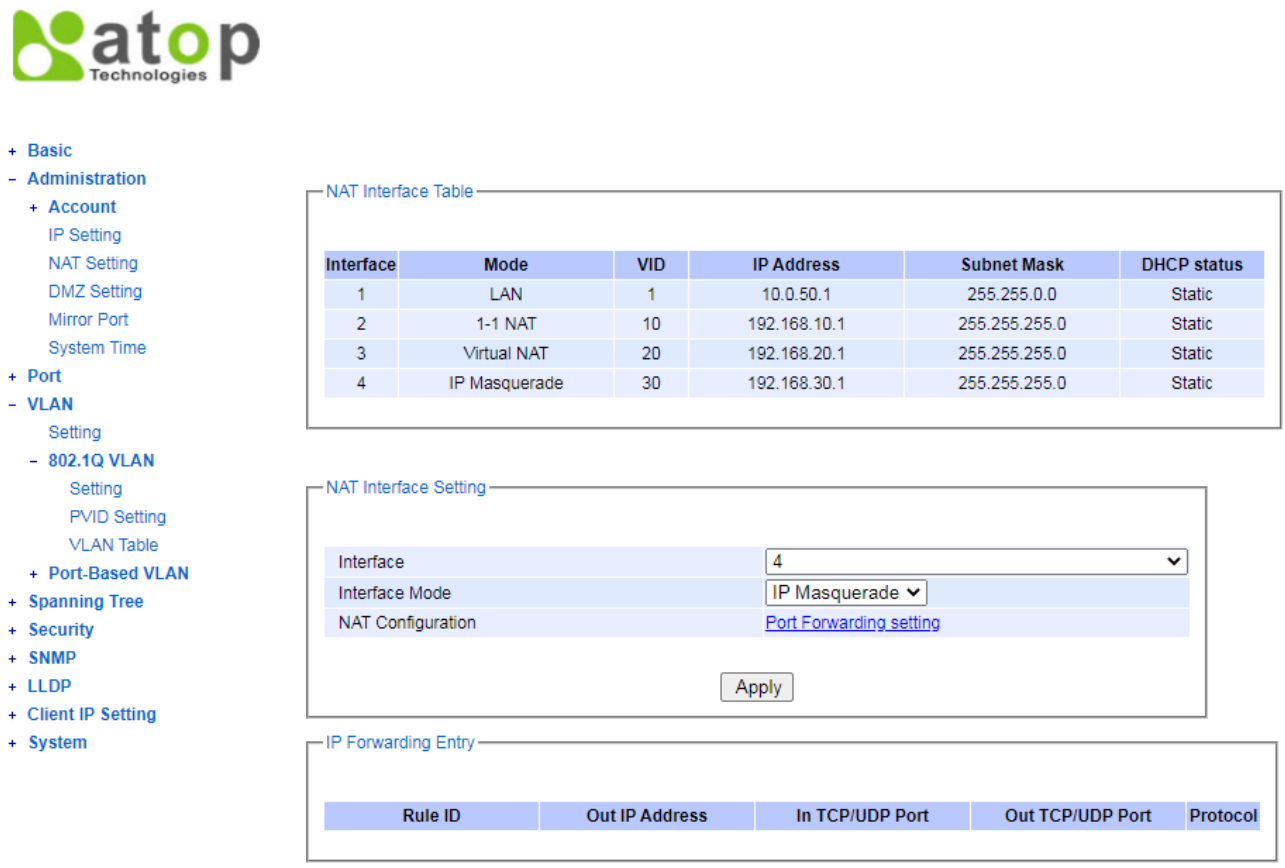


Figure 2.19 Example of NAT Interface Setting for IP Masquerade Mode

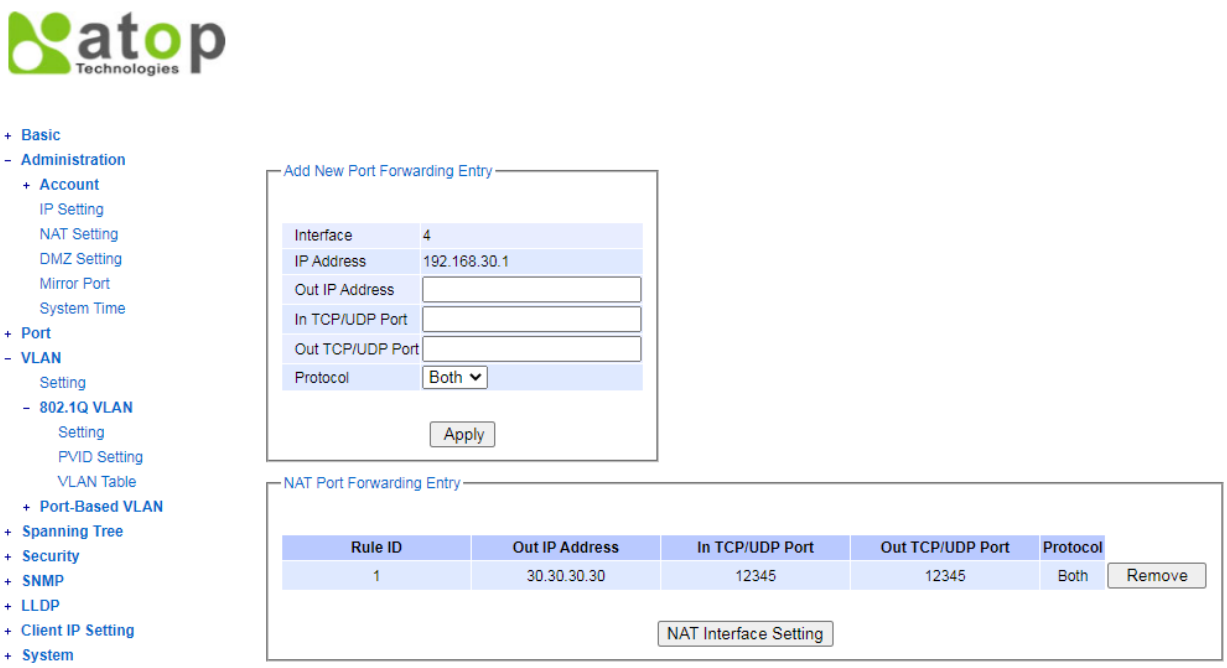


Figure 2.20 Example of Port Forwarding Entry for IP Masquerade Mode

2.2.5 DMZ Setting

A Demilitarized Zone (**DMZ) Network** is a perimeter network that protects an organization's internal local-area network (LAN) from untrusted traffic, adding an extra layer of security. A common DMZ is a subnetwork that stays between the public internet and private networks.

The objective of implementing a DMZ is to allow an organization to access untrusted networks, such as the internet, while ensuring that its private network (LAN) remains secure. Organizations typically store services and resources, as well as servers that face external network, such as the Domain Name System (DNS), File Transfer Protocol (FTP), mail, proxy, Voice over Internet Protocol (VoIP), and web servers, in the DMZ.

These servers and resources are isolated and given limited access to the LAN, to ensure that they can be accessed via the internet while the internal LAN cannot. As a result, a DMZ approach makes it more difficult for a hacker to gain a direct access to an organization's data and internal servers via the internet.

When users enable DMZ and sets its host IP Address, a connected WAN device will only be able to access the host IP address that he/she sets. The followings are the DMZ functional behaviours in the three NAT modes:

1. In 1-1 NAT mode, NAT rule has higher priority than the DMZ setting. Users can still access connected LAN hosts using NAT table which maps a connected LAN device with a WAN IP address.
2. In virtual mode, virtual NAT rule also has higher priority than the DMZ setting. Users can still access connected LAN devices using virtual NAT table, which maps a connected LAN device with a WAN IP address through a virtual IP address on the intermediate level.
3. In IP Masquerade mode that is already configured a port forwarding, port forwarding rule also has higher priority than the DMZ setting. Users can still access connected LAN devices through **Out IP Address**.

The **DMZ Setting** webpage is shown in Figure 2.21. The DMZ is disabled in the default setting and the DMZ Host IP Address is empty (null). To enable the DMZ feature, users can click **Enabled** box on the right of the **Enable DMZ** field and enter an IP address into the **DMZ Host IP Address** field.

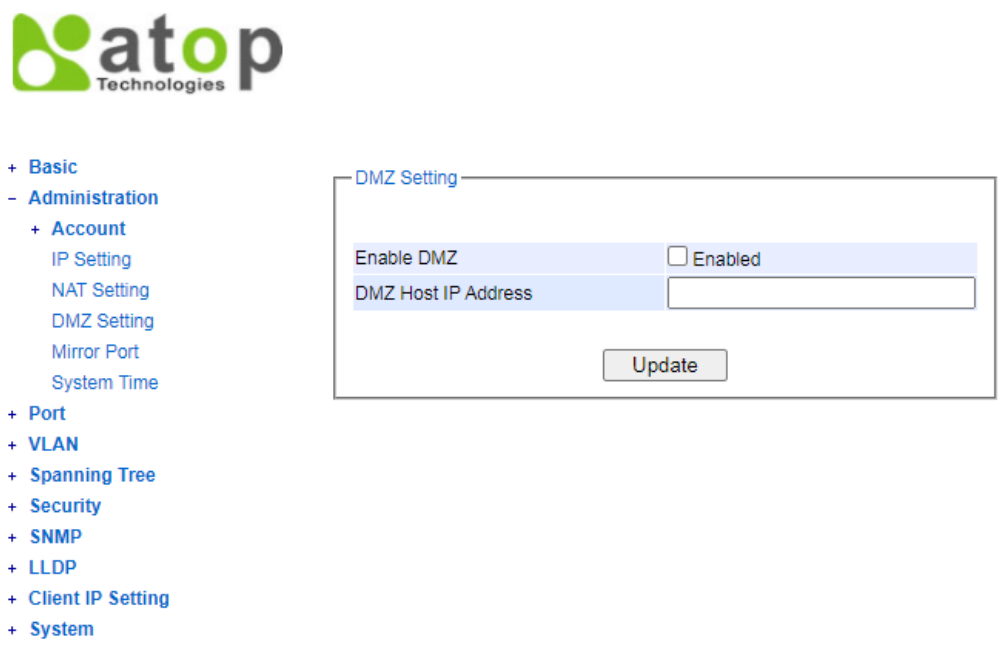


Figure 2.21 DMZ Setting Webpage

2.2.6 Mirror Port

In order to help the network administrator keeps track of network activities, the NSG330X NAT switch supports port mirroring, which allows incoming and/or outgoing traffic to be monitored by a single port that is defined as a **mirror port.** Note that the mirrored network traffic can be analysed by a network analyser or a sniffer for network performance or security monitoring purposes. Figure 2.22 shows the Mirror Port webpage. The descriptions of port mirroring options are summarized in Table 2.4.

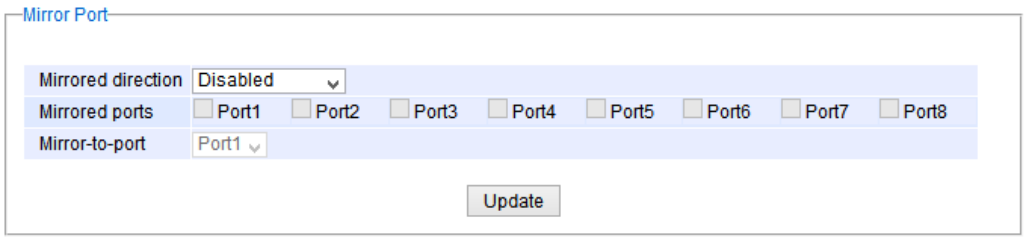


Figure 2.22 Mirror Port Webpage

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

Table 2.4 Descriptions of Port Mirroring Options

Label	Description	Factory Default
Mirrored direction	Select the monitoring direction. - **Disabled**: To disable port monitoring. - **Ingress**: To monitor input data stream of the monitored ports only. - **Egress**: To monitor output data stream of the monitored ports only - **Ingress/Egress**: To monitor both input and output data stream of the monitored ports	Disabled

Label	Description	Factory Default
Mirrored Port	Select ports that will be monitored. Port 1 to Port 9 are available to select.	Unchecked all
Mirror-to-port	Select the mirror port that will be used to monitor the activity of the monitored ports	Port1

2.2.7 System Time

Atop's NSG330X NAT switch has an internal calendar (date) and a clock (or system time), which can be set manually or automatically. Users can configure the **System Time** by clicking on **Administration->System Time** submenu. After clicking the submenu, the **System Time and SNTP** webpage will be displayed, as shown in Figure 2.23. Here, users have an option to configure the **Current Date** and **Current Time** manually. Format of the current date is Year/month/date (YYYY/MM/DD), whereas format of the current time is hour:month:second (HH:MM:SS). In **Time Zone** field, users can choose the network's local time zone from the drop-down list. If the switch is deployed in a region where daylight saving time is practiced (see note below for the explanation), please check **Enable** box in the **Daylight Saving Time** field. If enabled, users will have to enter **Start Date** and **End Date** in Month/Week/Date/Hour format, and enter **Offset** in a number of hour(s).

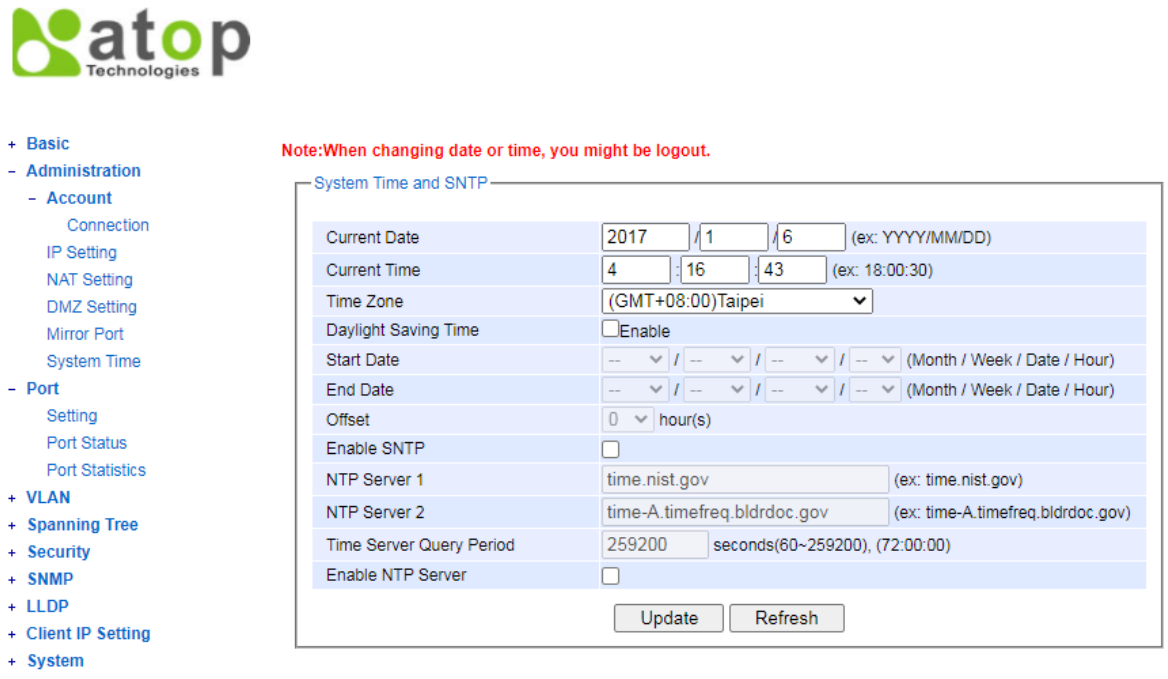


Figure 2.23 Webpage for Setting System Time and SNTP

To automatically set date and time, users can enable Simple Network Time Protocol (SNTP) by selecting the box on the right of the **Enable SNTP** field (see note below for the explanation). If enabled, 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. Users can specify the **Time Server Query Period**, which is in the order of seconds, for synchronization. The value of this period should be set based on user's determination of clock accuracy of the switch. The higher the value, the less the clock accuracy. The NAT switch can become a network time protocol (NTP) server for the local devices by checking the box on the right of the **Enable NTP Server** field. Description of each option is provided in Table 2.5.

Table 2.5 Descriptions of the System Time and the SNTP

Label	Description	Factory Default
Current Date	Allows local date configuration in yyyy/mm/dd format	None
Current Time	Allows local time configuration in local 24-hour format	None
Time Zone	The user's current local time	(GMT+08:00) Taipei

Label	Description	Factory Default
Daylight Saving	Enable or disable Daylight Saving Time function	Unchecked
Start Date	Define the start date of daylight saving	NULL
End Date	Define the end date of daylight saving	NULL
Offset	Decide how many hours to be shifted forward/backward when daylight saving time begins and ends. See note below.	0
Enable SNTP	Enables SNTP function. See note below.	Unchecked
NTP Server 1	Sets the first IP or Domain address of NTP Server.	time.nist.gov
NTP Server 2	Sets the second IP or Domain address of NTP Server. Switch will locate the 2nd NTP Server if failed to connect to the 1st NTP Server.	time-A.timefreq.bldrdoc.gov
Time Server Query Period	This parameter determines how frequently switch gets updated time 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 (1 hour) to 259200 (72 hours) seconds.	259,200 seconds.
Enable NTP Server	This option will enable network time protocol (NTP) daemon inside the NAT switch which allows other devices in the network to synchronize their clock with this NAT switch using NTP.	Unchecked

Note:

- **Daylight saving time (DST)**: In certain regions (e.g. US), local time is adjusted during summer and winter seasons. It is the practice of advancing clocks (typically by one hour) during warmer months so that darkness falls at a later clock time. The typical implementation of DST is to set clocks forward by one hour in the spring, and to set clocks back by one hour in autumn to return to standard time.

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

2.3 Port

2.3.1 Setting

Under the **Port->Setting** submenu, there are four fields in the **Port Setting** box: **Port**, **Enabled**, **Mode**, and **Speed**. Only the **Enabled** field can be configured, whereas the other fields can only be inspected. Users can control the state of each port, whether it is enabled/disabled, by selecting/deselecting the corresponding box in the **Enabled** Column. The **Mode** field displays whether that port supports copper or fibre link. In the **Speed** field, the current default value is set at 1000 (1Gbps). In Figure 2.24 and Figure 2.25, the **Port Setting** webpages of NSG3308 and NSG3309-2SFP are shown respectively.

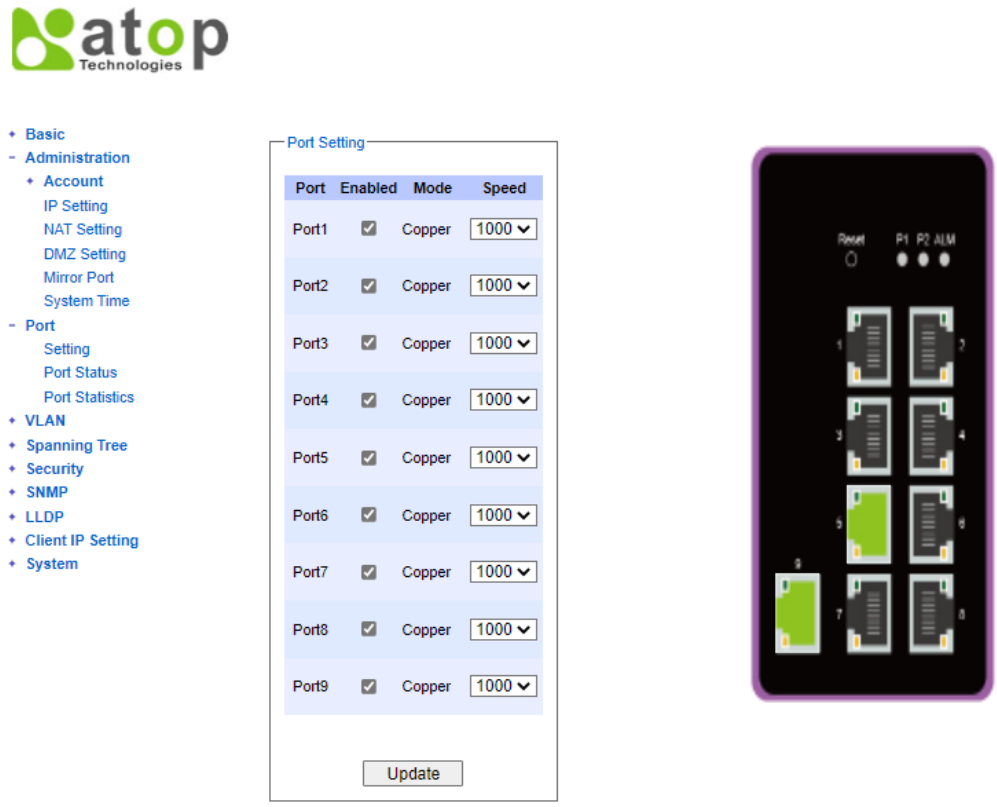


Figure 2.24 Port Setting Webpage – NSG3308

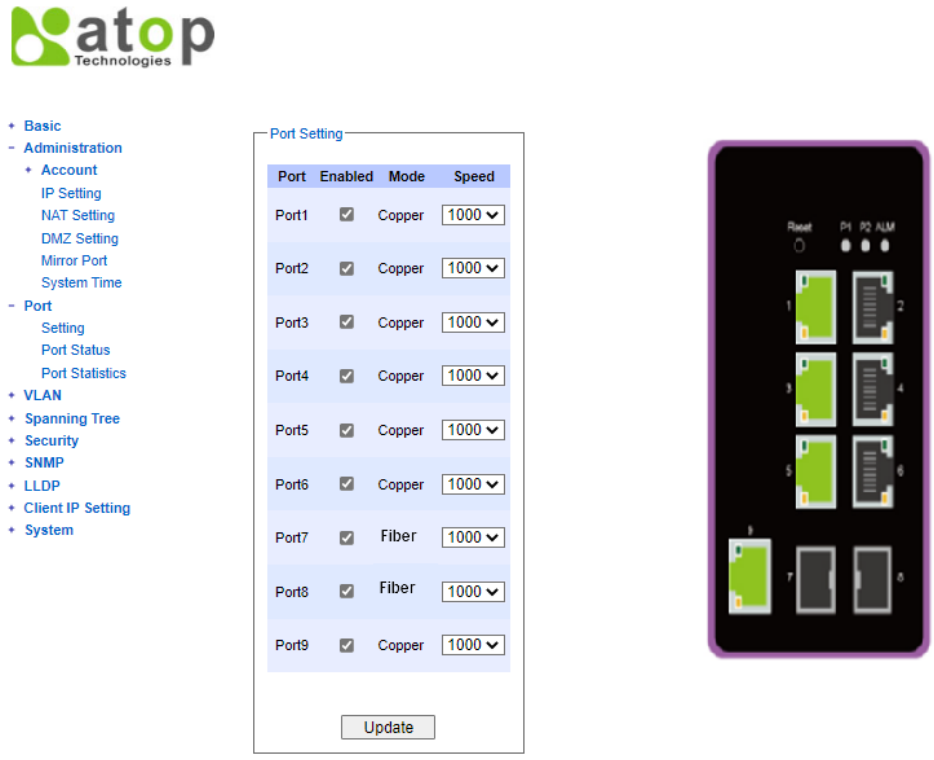


Figure 2.25 Port Setting Webpage – NSG3309-2SFP

2.3.2 Port Status

The overview of **Port Status** on the NAT switch can be viewed in this webpage. Here, there are six fields: **Port**, **Mode**, **Enabled**, **Link**, **Config Speed**, and **Actual Speed**. In **Link** field, it would show status whether it is Up or Down. The

Actual Speed field displays the actual value of link speed when link is up. Users can compare the actual status here and the setting value in Section 2.3.1. Figure 2.26 and Figure 2.26 shows the Port Status webpage of NSG3308 and NSG3309-2SFP, respectively. To check the latest status of all port, click the **Refresh** button either on the top or the bottom of the webpage.

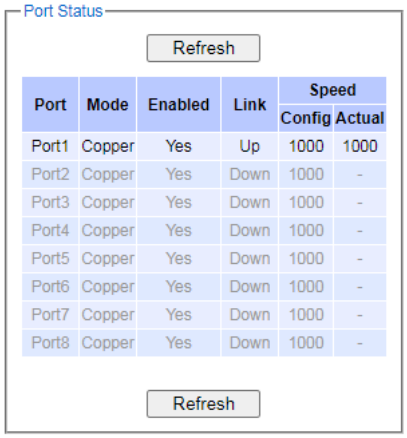


Figure 2.26 Port Status Webpage – NSG3308

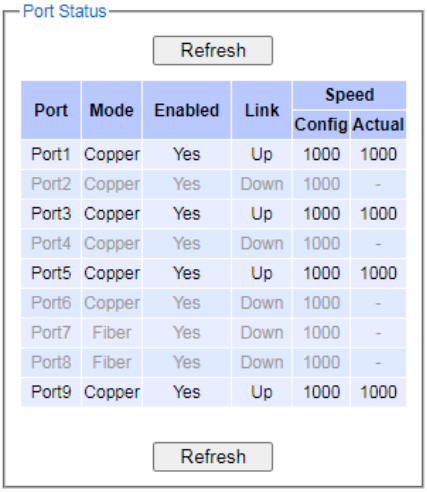


Figure 2.27 Port Status Webpage – NSG3309-2SFP

The possible values of all fields in the **Port Status** webpage are listed here.

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

2.3.3 Port Statistics

The Port Statistics are summarized in this webpage as shown in Figure 2.28. Users can use this subsection to help them diagnose the problem such as link quality of each port. The key statistics are the total number of normal **(OK) frames**, the number of discarded **(Error) frames**, and the speed of the transmission (**Rate** in Bps) for both transmitted (**Tx**) and received (**Rx**) traffic in each port. To clear or reset all the statistics to zero on this page, click on the **Clear** button. To obtain the latest statistics on this page, click on the **Refresh** button.

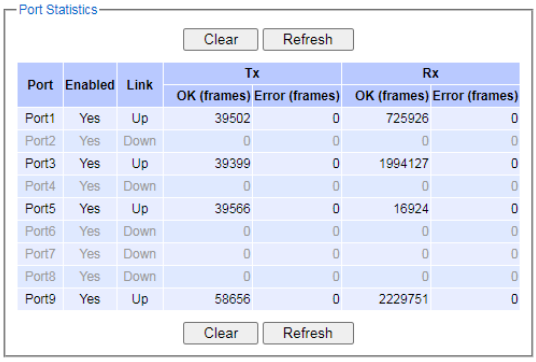


Figure 2.28 Port Statistics Webpage

All fields' names and their possible values in the **Port Status** webpage are listed here.

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

2.4 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. Users usually spend a lot of time on relocation of a device in a traditional network. With a VLAN reconfiguration, relocation can be performed in a very short time and can be done entirely through a software program. 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. In traditional network, data is broadcasted to all devices, whether or not they are needed. By allowing a member to receive data only from other members in the same VLAN group, VLAN avoids broadcasting and increases traffic efficiency.

2.4.1 VLAN Setting

The first menu under the VLAN section is the VLAN **Setting**. Here the management VLAN Identification number (ID) is configured based on the IEEE 802.1Q standard. The default value is VID = 1. Note that the ID can be the number from 1 to 4096. If users want to change the management VLAN ID to the other number, users must enter a new ID and click the **Update** button. Figure 2.29 depicts the VLAN Setting webpage. Table 2.6 describes the VLAN Setting option.

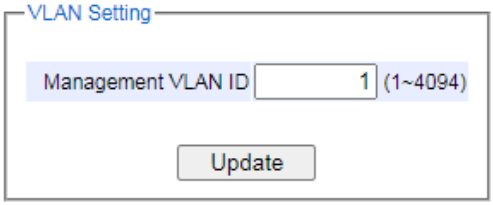


Figure 2.29 VLAN Setting Webpage

Table 2.6 Description of VLAN Setting

Label	Description	Factory Default
Management VLAN ID	Configure the management VLAN ID that can be accessed in this switch. Range from 1 to 4094.	1

2.4.2 802.1Q VLAN

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 provides a prioritization scheme for differentiating quality of service (QoS).

An VLAN tagging or un-tagging frame is a frame with or without an 802.1Q (VLAN) tag. VLAN is identified by using a valid VLAN identifier (VID) in an 802.1Q (VLAN) tag frame. In an untagged frame, only 802.1p tag which provides an information of the prioritization is carried. Here, the VID has a value of 0. When a switch received a tagged frame, it will extract the VID and then forward the frame to other ports within the same VLAN.

For an 802.1Q VLAN packet, it adds a tag (32-bit field) to the original packet. The tag is added between the source MAC address and the EtherType/length fields of the original frame. The first 16 bits of the tag named Tag protocol identifier (TPID) has the value of 0x8100. As TPID of tagged frame is located at the same position as the EtherType/length field in an untagged frame, this setting will help distinguishing them apart. The next 16 bits belongs to Tag control information (TCI) field. In TCI field, the first three bits is the Priority Code point (PCP) field, which refers to the IEEE 802.1p class of service and maps to the frame priority level. Different PCP values can be used to prioritize different classes of traffic. The next one bit belongs to the Drop Eligible Indicator (DEI) field, which may be used separately or in conjunction with PCP to indicate frames that are 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 to.

Under the 802.1Q VLAN menu, there are three submenus which are **Setting**, **PVID Setting**, and **VLAN Table** as shown in Figure 2.30.

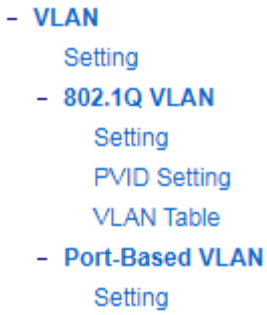


Figure 2.30 802.1Q VLAN Dropdown Menu

2.4.2.1 Settings

Figure 2.31 shows the 802.1Q VLAN Setting webpage which allows users to add new tagged-based VLAN to the NAT switch. Use the following procedure to set up the 802.1Q VLAN on the switch.

1. Go to **802.1Q VLAN,** and then select **Setting** submenu.
2. Fill in an appropriate Name, a VID, Member Ports, and Tagged Ports as show in Figure 2.31. The description of each field is summarized in Table 2.7. Then, click **Add/Modify** button. Note that, in order to select multiple **Member Ports** or multiple **Tagged Port**s, users need to press and hold the **Ctrl** key while selecting multiple ports.
3. Go to **802.1Q VLAN's PVID Setting** described in the next subsection.
4. Choose the same ports, and enter PVID (which is the same as VID), as shown in Figure 2.32.

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 2.31.

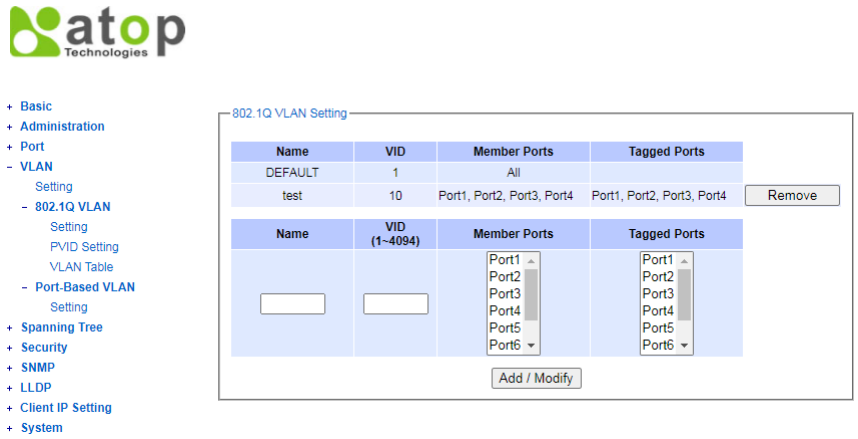


Figure 2.31 802.1Q VLAN's Setting Webpage

Table 2.7 Descriptions of 802.1Q VLAN Settings

Label	Description
Name	The VLAN ID name that can be assigned by the user.
VID	Configure the VLAN ID that will be added in the static VLAN table of the switch. The VLAN ID is in the range of 1~4094.
Member Ports	Configure ports to this specific VID.
Tagged Ports	Configure ports that outgoing packet will be tagged or untagged.

	Selected: The outgoing packet is tagged for these ports. **Unselected**: The outgoing packet is untagged for these ports.

NOTE: For the default setting, VLAN ID only has value 1. To set VLAN ID to other value, users will have to assign ports to be in that VLAN group.

2.4.2.2 PVID Setting

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 2.32 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 of each port by selecting either one or multiple ports (by clicking and holding the **Ctrl** key) and enter the desired PVID value between 1 to 4094. Please click the **Update** button to allow the configuration to take effect on the switch. Table 2.8 summarizes descriptions of the PVID setting.

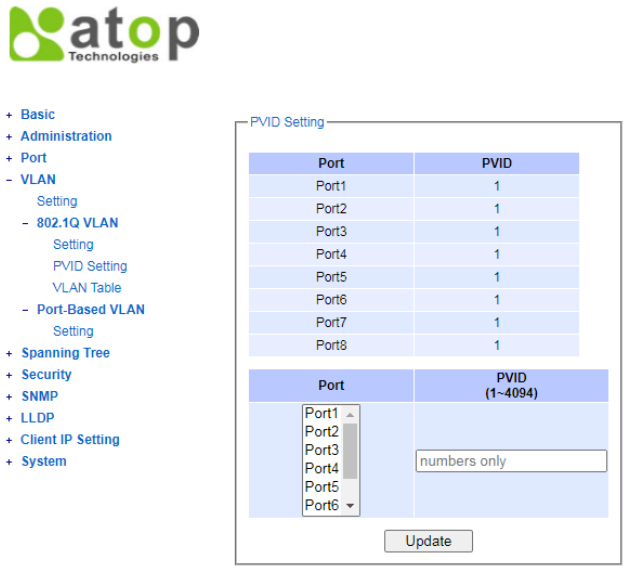


Figure 2.32 802.1Q VLAN PVID Setting Webpage

Table 2.8 Descriptions of 802.1Q VLAN PVID Setting

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

2.4.2.3 VLAN Table

This webpage shown in Figure 2.33 displays the 802.1Q VLAN table which lists all the VLANs that are automatically or manually added/modified to the NAT switch. Table 2.9 summarizes the descriptions of VLAN Table.

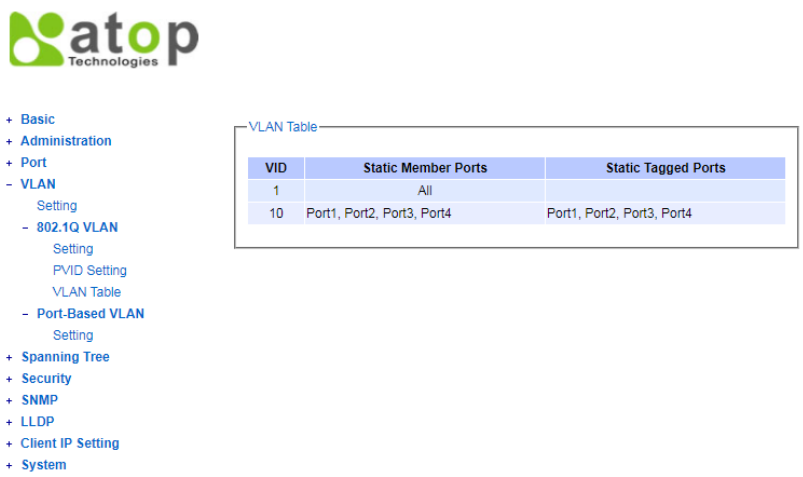


Figure 2.33 802.1Q VLAN Table Webpage

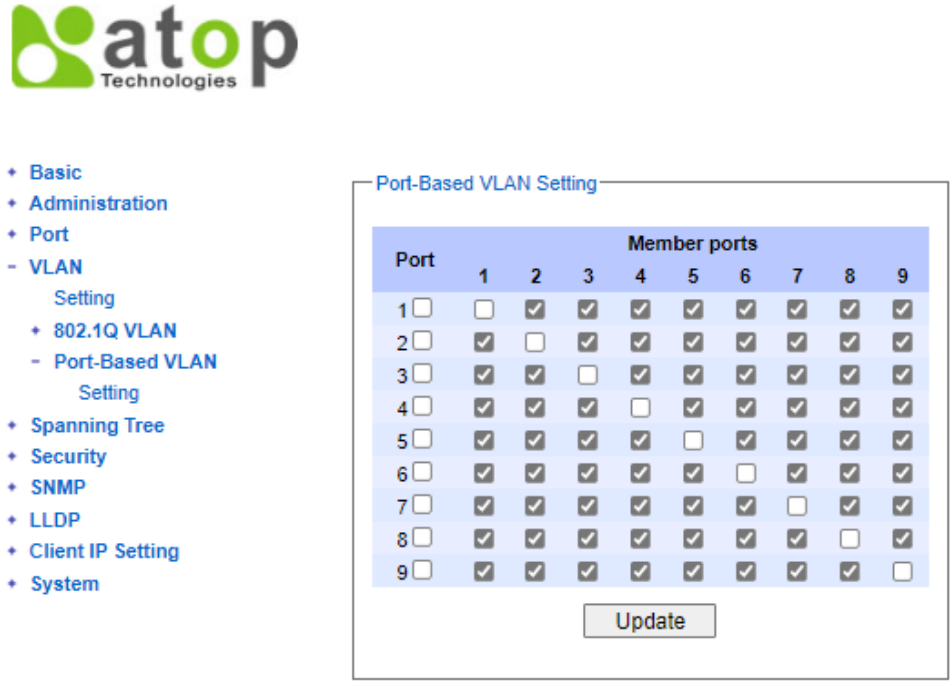
Table 2.9 Descriptions of 802.1Q VLAN Table

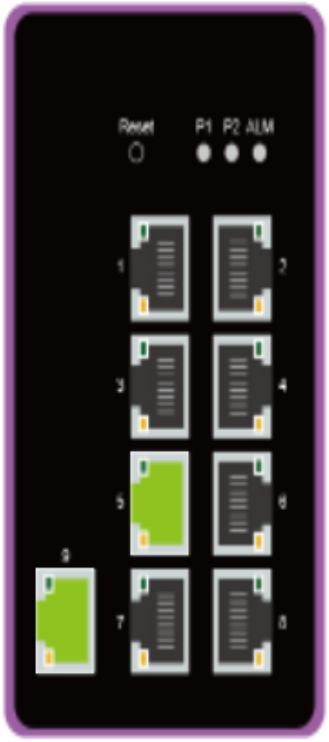
Label	Description
VID	The VLAN ID number
Static Member Ports	Member ports assigned to this VID. This entry is created by user.
Static Tagged Ports	Ports that outgoing packets are tagged or untagged. **Displayed**: The outgoing packets are tagged for these ports. **Non-displayed**: The outgoing packets are untagged for these ports. This entry is created by user.

2.4.3 Port-Based VLAN

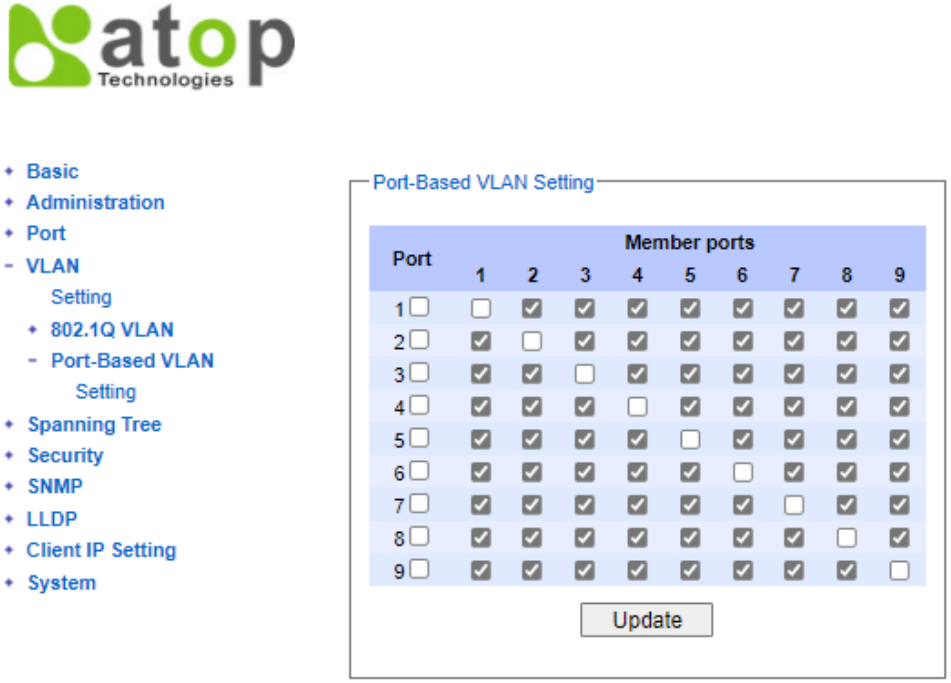
Port-Based VLAN (or Static VLAN equivalent) assignments are created by assigning ports to a VLAN. If a device is connected to a certain port, the device will be assigned a VLAN to that specific port. If a user changes the connected port, a new port-VLAN assignment must be reconfigured for this new connection.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

1. Click on **Port-Based VLAN setting** page as shown in





2.
3. Figure 2.34.
4. Include specific ports to a certain port-based VLAN group ID by selecting the corresponding boxes under the **Member ports** on that particular row. Note that if a user selects/deselects the box under the first column (**Port**, which is a VLAN's Group ID), all of the Member Ports will/will not belong to that VLAN's Group ID.
5. Click on the **Update** button to allow the setting to take effect on the NAT switch.



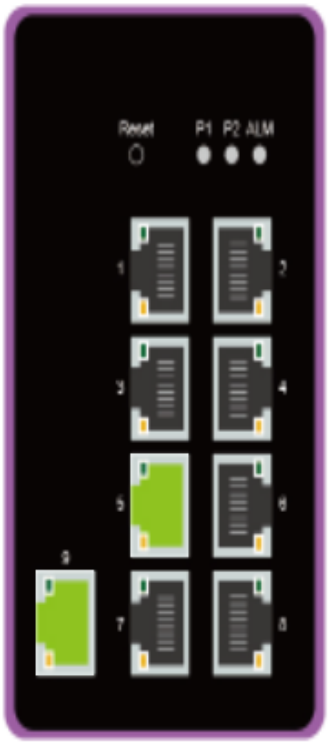


Figure 2.34 Port-based VLAN Setting Webpage

2.5 Spanning Tree

RSTP (**R**apid **S**panning **T**ree **P**rotocol), which was standardized in IEEE 802.1W and supersedes the original IEEE 802.1D-2004, is supported in ATOP's NAT switches. RSTP has more advantages over the STP. When there is a topology change such as link failure in the network, RSTP will converge significantly faster to a new spanning tree topology. RSTP improves a convergence on point-to-point links by reducing the Max-Age time to three times Hello interval, removing the STP listening state, and exchanging a handshake between two switches to quickly transition port to the forwarding state.

This section describes how to setup the rapid spanning tree protocol (RSTP). Figure 2.35 displays Spanning Tree's dropdown menu.

Figure 2.35 Spanning Tree's Dropdown Menu

2.5.1 Setting

Under the **Spanning Tree->Setting** submenu, there are three boxes: **Mode Setting**, **Main Setting**, and **Per-port Setting** boxes. Under these boxes, users can configure mode of spanning tree, necessary parameters for that mode, and ports that spanning tree setting are enabled/disabled. Figure 2.36 shows the mode setting for spanning tree. RSTP is the default setting mode for the NSG330x NAT switch.

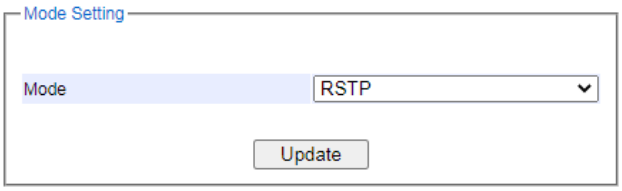


Figure 2.36 Spanning Tree Mode Setting

The **Main Setting** of spanning tree's parameters can be configured, as shown in Figure 2.37. Users can enable or disable spanning tree protocol in the **Main Setting** by checking the box behind the **Enabled** option. Users can fine tune the **Priority**, **Maximum Age**, **Hello Time**, and **Forward Delay** parameters. Please click the **Update** button to allow change to take effect. The description of each parameter is listed in Table 2.10.

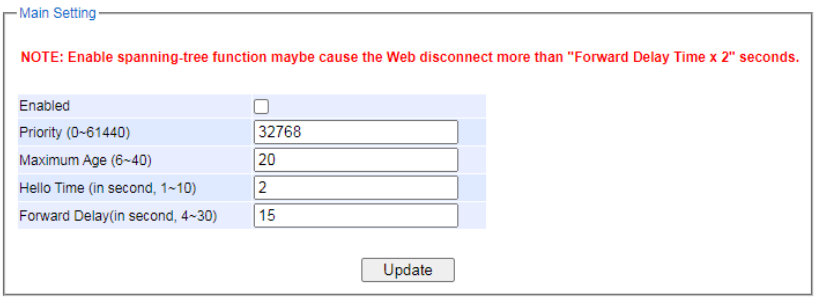


Figure 2.37 Spanning Tree Main Setting for RSTP

Table 2.10 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	Expected maximum 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

The bottom part of the RSTP webpage is the **Per-port Setting** box as shown in Figure 2.38. Users can enable RSTP functionality on each port individually or on all ports by checking on the boxes under the **Port Enable** column. The default setting is checking on all ports. Users can check/uncheck the box on the first row (behind the **All** field) to enable/disable RSTP function of all ports. After making any change on the **Per-port Setting** box, please click on the **Update** button for change to take effect.

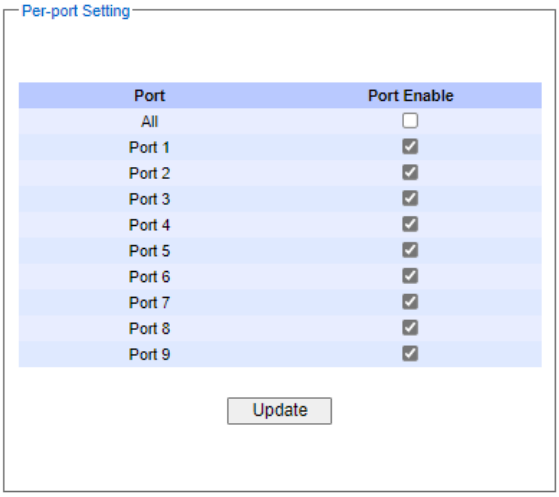


Figure 2.38 Spanning Tree Per-port Setting for RSTP

2.5.2 Bridge Info

Bridge Info (information) provides the statistical value of rapid spanning tree protocol (RSTP) as shown in Figure 2.39. 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 2.11 summarize the description of each entry in the **Root Information** table and **Topology Information** table, respectively.

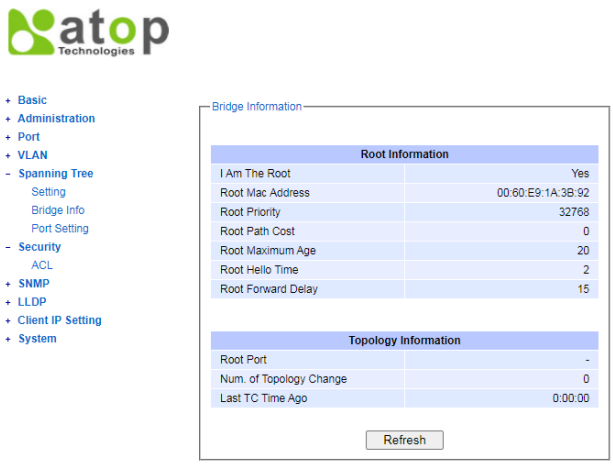


Figure 2.39 Bridge Information Webpage

Table 2.11 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 will be elected as the root of the spanning tree. The priority value sets for the root should be the lowest value, since the lower the priority value gives the higher the priority.	0
Root Path Cost	Root's path cost is calculated from the switch's port data rate**.**	0
Root Maximum Age	The maximum amount of time that the switch will maintain the received protocol information on a link**.**	0
Root Hello Time	Time interval for RSTP to send out a hello message to the neighbouring nodes to detect any change in the topology**.**	0
Root Forward Delay	The duration that the switch will be in a learning state and a listening state before a link begins forwarding **.**	0
Root Port	Root port is a best forwarding port from a non-root bridge/switch to a root bridge/switch. Note that there is no root port for a root switch.	-
Num. of Topology Change	The total number of spanning topology change over time.	0
Last TC Time Ago	The duration of time since the last spanning topology has changed.	-

2.5.3 Port Setting

Each port's spanning tree protocol parameters can be configured in the **Spanning Tree Port Setting** webpage, as shown in Figure 2.40. There are eight main parameters; i.e., **State**, **Role**, **Path cost**, **Path priority**, **Link type**, **Edge**, and **Designated** information. For the latest update on these parameters, please click on the **Refresh** button. Table 2.12 summarizes the descriptions of these parameters within the **Spanning Tree port Setting** webpage. Note that only **Path Cost**, **Path Priority**, **Link Type**, and **Edge parameters** are configurable, and that these are configurable only if Spanning Tree protocol is enabled. Please refer to 2.5.1 on how to enable spanning tree protocol. Please click on the **Update** button to save the settings.

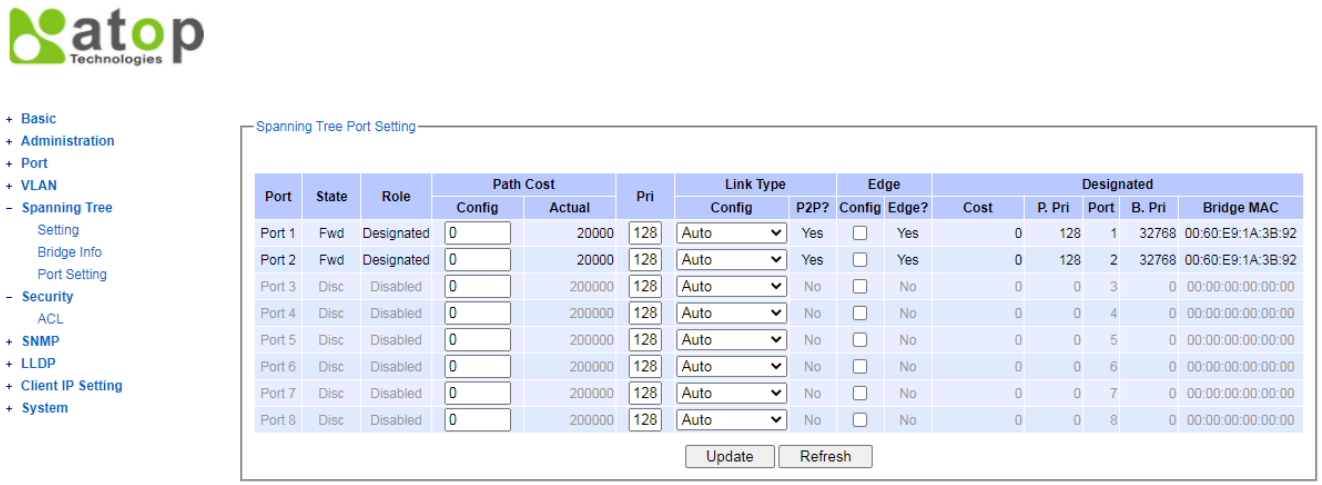


Figure 2.40 Spanning Tree Port Setting Webpage

Table 2.12 Descriptions of Spanning Tree Port Setting

Label		Description	Factory Default
Port		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 best forwarding port from non-root bridge to root bridge. '**Designated**' – A forwarding port for every LAN segment. '**Alternate**' – An alternate path to the root bridge, which is different from using the root port. '**Backup**' – A backup/redundant path to a segment whose another bridge port is already connected. '**Disabled**' – A network administrator manually disables a port.	Non-STP
Setting the path cost for each switch port			
Path Cost	**Config**	Setting the path cost depending on the link speed (default value: 0)	0
	Actual	The actual value of the path cost	0
Pri		Setting the port priority, which is used in the Port ID field of BPDU packet. Value = 16 × N where (N:0~15)	128
The connection between two or more switches (for RSTP)			
Link Type	**Config**	Setting of the Link Type **P2P**: A port that operates in full-duplex mode is assumed to be a 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 port is a port without other connected STP/RSTP switches. It can be set to the forwarding state directly.			
Edge	**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
Some information of the best BPDU packet through this port is shown here.			

Designated	Cost	Root path cost	0
	P. Pri. (Port Priority)	Port priority (higher 4 bits of the Port ID) Value = 16 × N where N: 0~15	128
	Port	Interface number (lower 12 bits of the Port ID)	-
	Bri. Pri. (Bridge Priority)	Bridge priority (value = 4096 × N where N: 0~15)	32768
	Bridge MAC	The MAC address of the switch which was sent this BPDU	-

2.6 Security

2.6.1 ACL

Access Control List (ACL) is the mechanism for network access control. Users can configure the switch's filtering rules for accepting or rejecting some packets. The ACL webpage is depicted in Figure 2.41. Two types of filters are deployed in the NSG series: 1) by MAC layer and 2) by IP layer, as shown in Figure 2.41 and Figure 2.42 respectively. Although the number of matching rules for these filtering type can be at most 128, the main important exercised rules are as follows. For a MAC layer-based filtering type, the rules include MAC address, VLAN ID, and Ether type. Whereas, for IPv4 layer-based filtering type, the rules include IP protocol, IP address, TCP/UDP port, and Type of Service (TOS). When filtering is enabled, the matching rules are used for checking whether the currently receiving packet is matched. If it is matched, the packet will be rejected; otherwise it will be accepted. Note here that later on in this document the matching rules will be referred to as the entries of ACL.

To differentiate between each ACL entry, **Index** number from 1 to 128 is used. The higher priority ACL entries will be checked for matching first before the other lower priority ACL entries. The **Name** field is for setting the name of this rule. Type of filtering whether it is based on MAC layer (**Mac Base**) and IP layer (**IPv4 Base**) can be set in the **Filter** field. Note that, when changing from **Mac Base** to **IP Base**, the setting parameters for ACL will be changed accordingly.

User can add, modify, and remove each ACL entry by filling in the required **Index** number and necessary information before clicking on **Add**, **Modify**, or **Remove** button. The lower part of the ACL Information webpage is the list of all existed ACL entries. Users can browse through the list by using the **<< Previous Page** and **Next Page >>** buttons. To remove all existing ACL entries from the list, click on the **Clear All** button.

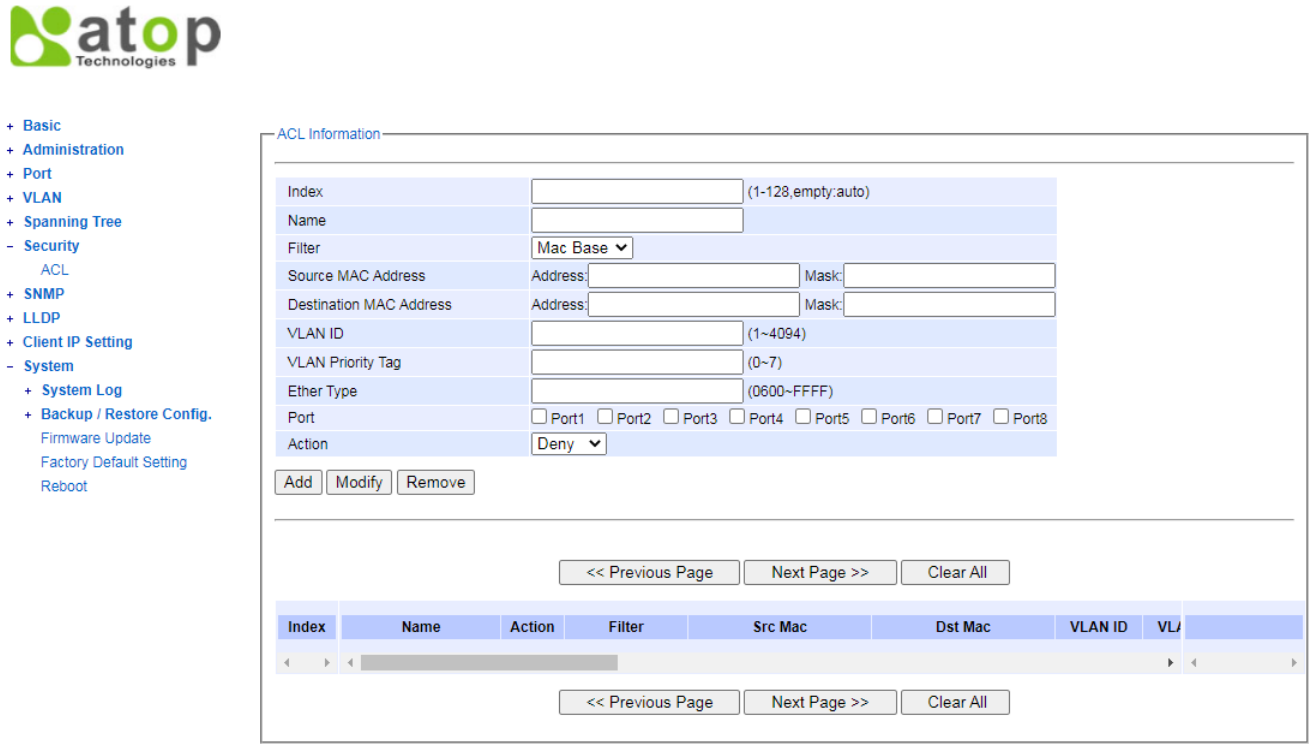


Figure 2.41 Security Access Control List Information Webpage (MAC Based Filtering)

As shown in Figure 2.41, the ACL entries for the MAC layer-based filtering type include **MAC address**, **VLAN ID**, **VLAN Priority Tag**, and **Ether Type**. Table 2.13 describes the definition of each ACL entry in details. Note that if any fields are empty, that ACL entries will be ignored.

Table 2.13 Descriptions of ACL Entries (MAC Layer-based Filtering Type)

ACL Entry	Definition	Range
Source or Destination MAC Addresses	These MAC address fields consist of 1) Address, and 2) Mask items. MAC address is the Ethernet frame header, and Mask is a bit mask for comparing range.	For every non-zero bit in the Mask, its relative bit in the IP address will be compared. If the Mask is 0.0.0.0, packet will always be accepted. If the Mask is empty, it is considered equal to the Mask of 255.255.255.255 and all of bits in the IP Address are compared.
VLAN ID	This entry is the VLAN ID field of 802.1Q VLAN tag in the Ethernet frame header. If the trunk ports are created, they will also be shown on the port list. If you want to select a trunk port, please make sure that there are no ACL entry using the physical ports which are belonging this trunk port.	The item value is between 1~4094.
VLAN Priority Tag	The Priority field of 802.1Q VLAN tag in the ethernet frame header.	The item value is between 0~7.
Ether Type	This entry is the Ethernet type field in the Ethernet frame header. The followings are example values of the Ethernet type field. The value of 0x8000 is an IPv4 packet. The value of 0x86DD is an IPv6 packet. The value of 0x8100 is an 802.1Q packet.	The item value is between 0x0600~0xFFFF.

As shown in Figure 2.42, the main ACL entries for filtering based on IPv4 layer include IP Protocol, Source IP Address, Destination IP address, TCP/UDP Source Port, TCP/UDP Destination Port, and TOS (Type of Service for IPv4). In Table 2.14, the definitions of these main entries are described in details. Note that if any field is empty, that ACL entry will be ignored. All factory default values for both ACL filtering methods are described in Table 2.15.

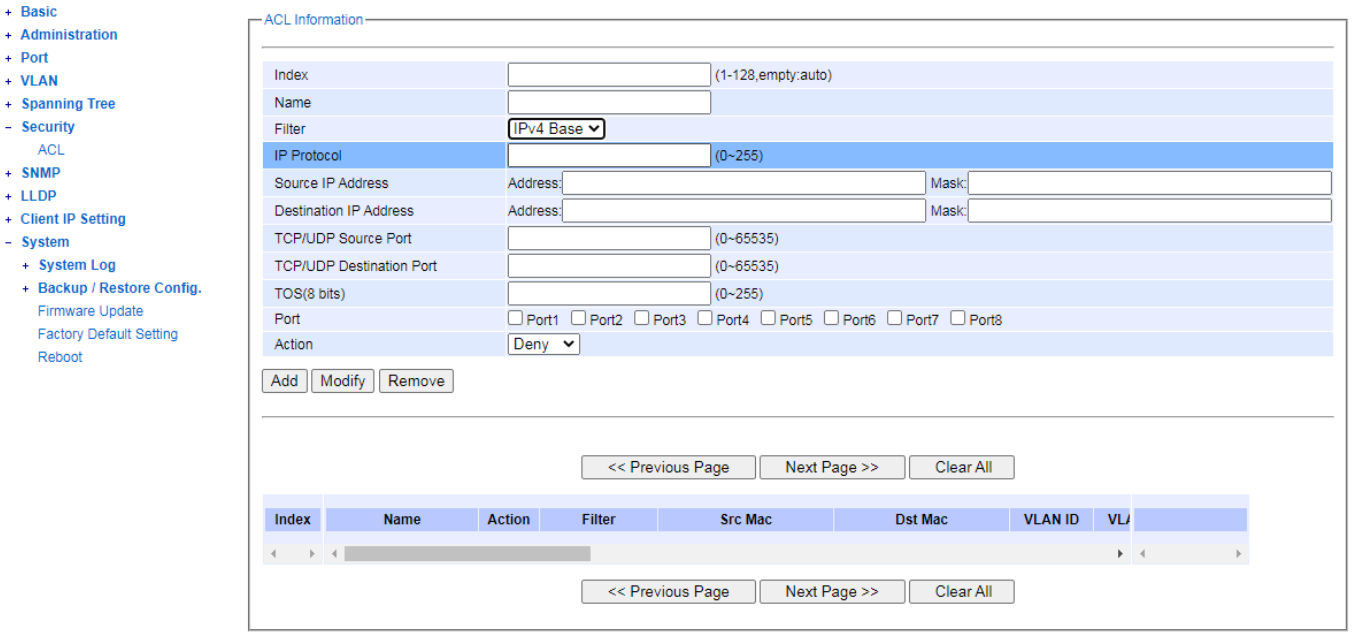


Figure 2.42 Security Access Control List Information Webpage (for IPv4 Based Filtering)

Table 2.14 Descriptions of ACL Entries (IP Layer-based Filtering Type)

ACL Entry	Definition	Range
IP Protocol	IP protocol is the Protocol field of the IPv4 packet header. The followings are example values. The value 1 is for an ICMP packet. The value 6 is for the TCP packet. The value 17 is for the UDP packet.	The item value is between 0~255
Source or Destination IP Addresses	IP Addresses are the fields of the IPv4 or IPv6 header. The Mask item is a bit mask for comparing range.	IPv4: For every non-zero bits in the Mask, its relative bit in the IP address will be compared. If the Mask is 0.0.0.0, then this condition is always accepted. If the Mask is empty, it is considered equal to the Mask of 255:255:255:255 and all of bits in the IP Address are compared IPv6: For every non-zero bits in the Mask, its relative bit in the IP address will be compared. If the Mask is 0.0.0.0.0.0, then this condition is always accepted. If the Mask is empty, it is considered equal to the Mask of FF:FF:FF:FF:FF:FF and all of bits in the IP Address are compared
TCP/UDP Source Port / TCP/UDP Destination Port	These are the fields of TCP/UDP frame header. It is used to filter the application services. For example, the TCP Destination Port 21 is for the FTP service, the TCP Destination Port 23 is for the Telnet service,	The item value is between 0~65535.

ACL Entry	Definition	Range
	and the TCP Destination Port 80 is for the HTTP service. To select which ports will follow the filter rule and what action to take, check the checkbox corresponding to that port and select “Deny” or “Permit” in the action field. If users select “Deny” option, rejecting packet. If users select “Permit” option, accepting packet. However, both scenarios occur only if this ACL entry is matched.	
TOS (Type of Service)	This entry is a Differentiated Service Code Point (DSCP) field in an IPv4 header. It is used for providing Quality of Service (QoS).	The item value is between 0~255.

Table 2.15 Factory Default Value for Main ACL Entries of Both ACL Filtering Method

LABEL	DESCRIPTION	FACTORY DEFAULT
Index	Priority (1-128)	NONE
Name	Max length 32	NONE
Filter	Mac Base/IPv4 Base	Mac Base
Source MAC Address and Mask	A:B:C:D:E:F is the source MAC address. Mask is used for bit mask checking. 0.0.0.0.0.0 means accepting all packets. Empty field means FF:FF:FF:FF:FF:FF.	NONE
Destination MAC Address and Mask	A:B:C:D:E:F is the destination MAC address. Mask is used for bit mask checking. 0.0.0.0.0.0 means accepting all packets. Empty field means FF:FF:FF:FF:FF:FF.	NONE
VLAN ID	1-4094	NONE
VLAN Priority Tag	0 ~ 7	NONE
Ether Type	0x0600-0xFFFF	NONE
IP Protocol	0-255	NONE
Source IP Address	A.B.C.D is the source IP address. Mask is used for bit mask checking. 0.0.0.0 means accepting all packets. Empty field means 255.255.255.255.	NONE
Destination IP Address	A.B.C.D is the destination IP address. Mask is used for bit mask checking. 0.0.0.0 means accepting all packets. Empty field means 255.255.255.255.	NONE
TCP/UDP Source Port	0-65535	NONE
TCP/UDP Destination Port	0-65535	NONE
TOS	0-255	NONE
Port	1,2,3,4,5,6,7,8	NONE
Action	Deny/Permit	NONE

2.7 SNMP

Simple Network Management Protocol (SNMP) is a protocol for managing devices on IP networks. SNMP exposes management data in the form of variables on the managed systems organized in a management information base (MIB) which describe the system status and configuration. These variables can then be queried

or defined by the users. The SNMP is used by network management system or third-party software to monitor devices such as NAT switches in a network to retrieve network status information and to configure network parameters. The Atop's NAT switch supports SNMP and can be configured, as described in this section. In the SNMP setting webpage, the settings are separated in four boxes: **SNMP Agent**, **SNMP V1/V2c Community Setting**, **Trap Setting**, and **SNMP V3 Authentication (Auth.)**, as shown in Figure 2.43.

Figure 2.43 SNMP Setting Menu

2.7.1 SNMP Agent

To enable SNMP agent on the NAT switch, please check the **Enabled** box and click **Update** button as shown in Figure 2.44. The SNMP version 1 (V1), version 2c (V2c) and version 3 are supported by Atop's NAT switches. Basically, SNMP V1 and SNMP V2c have simple community string-based authentication protocol for their security mechanism, while SNMP V3 is improved cryptographic security.

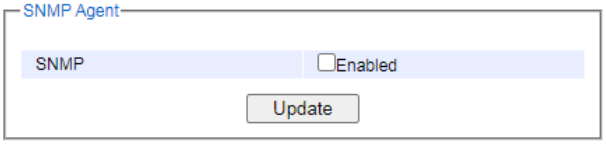


Figure 2.44 SNMP Enabling Box

2.7.2 SNMP V1/ V2c Community Setting

The NAT switch supports SNMP V1, V2c, and V3. SNMP V1 and V2c use a community string matching for authentication. This authentication will allow network management software to access the information or data objects defined by Management Information Bases (MIBs) on the NAT switch. Note that this simple authentication

is considered a weak security mechanism. It is recommended to use SNMP V3, if possible. There are two levels of authentication or permission type in NSG series, which are read-all-only or read-write-all. For example, in our default setting as shown in Figure 2.45, an SNMP agent which is a network management software module residing on the NAT switch can access all objects with read-all-only permissions using the string *public*. Another setting example is using the string *private* with the permission of read-write-all.

With this community string option as shown in Figure 2.45, a user can add or remove a new community string from the list. On the upper part, a user can view already existed community strings and their permission type, and can remove any existing community string by clicking on the **Remove** button**.** On the below part, a user can add a new community string by entering a string name on the **String** field and selecting the **Permission Type** from the dropdown list before clicking the **Add** button**.**

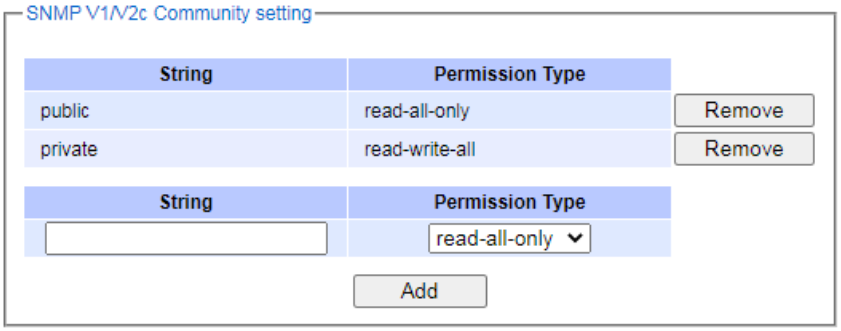


Figure 2.45 SNMP Community Strings

Table 2.16 Descriptions of Community String Settings

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

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

2.7.3 Trap Setting

The NAT switch provides a trap function that allows it to send notifications to agents with **SNMP traps** or **SNMP inform**. The notifications are based on the status changes of the switch such as link up, link down, warm start, and cold start. In SNMP traps, there will be no SNMP response sent back from the receiving end when a trap is received. Unlike SNMP traps, SNMP inform is more reliable. The switch will resend an SNMP inform request at least three times if it does not receive a response back within 10 seconds. A trap mode, either **Trap** or **Inform,** can be chosen from the drop-down list of the **Trap Mode** field, and clicking on the **Update** button. Trap Setting can be configured by entering the destination **IP Address of the Trap server**, **Port** number of the Trap server, and **Community String** before clicking on **Add** button. Figure 2.46 shows these Trap Setting's options. Table 2.17 summarizes the descriptions of trap receiver settings.

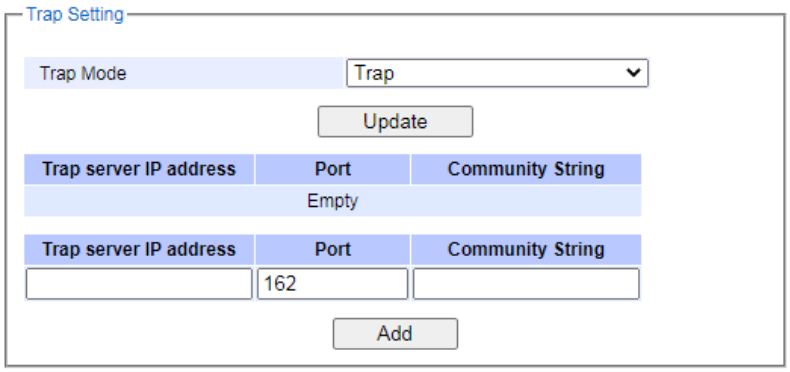


Figure 2.46 Example of Trap Receiver Setting

Table 2.17 Descriptions of Trap Receiver Settings

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

2.7.4 SNMPv3 Auth. Setting

As mentioned earlier, SNMP V3 is a more secure SNMP protocol than SNMP V1 and V2c. In this part, the users will be able to set a password and an encryption key to enhance the data security. When choosing this option, the users can configure SNMP V3's authentication and encryption. MD5 (Message-Digest algorithm 5) is used for authentication password and DES (Data Encryption Standard) is used for data encryption algorithm. Figure 2.47 shows options of the **SNMP V3 Authentication** Setting. The existing setting of SNMP V3 users can be viewed on the upper table where it provides information about user name, authentication type, and data encryption. The users have an option to remove an existing SNMP V3 user by clicking on the **Remove** button in the last column of each entry. To add a new SNMP V3 user, users have to select the user **Name** from the dropdown list which can be either **Admin** or **User**. Then, the authentication password with a maximum length of 31 characters has to be entered in the **Auth. Password** field and re-entered again in the **Confirmed Password** field. Note that if no password is provided, there will be no authentication for SNMP V3. Finally, the encryption key with a maximum length of 31 characters can be entered in the **Encryption Key** and re-entered again in **Confirmed Key** field. After filling all the required fields, please click on **Add** button to update the information on the NAT switch. Table 2.18 lists the descriptions of SNMP V3 settings.

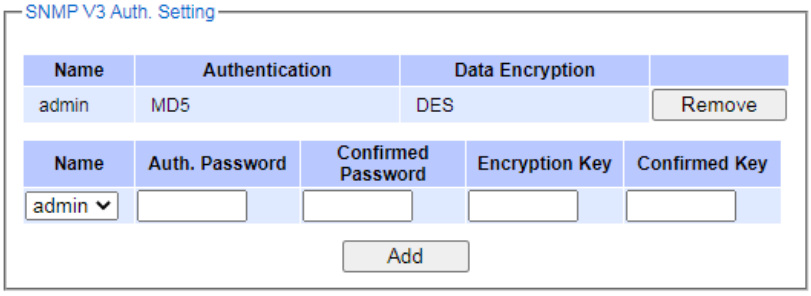


Figure 2.47 Options of SNMPv3 Users

Table 2.18 Descriptions of SNMP V3 Settings

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

To remove any of the SNMPv3 rule from the SNMP setting, click the **Remove** button at the end of that particular SNMPv3 rule record as shown in Figure 2.31.

2.8 LLDP

Link **L**ayer **D**iscovery **P**rotocol (**LLDP**) is an IEEE802.1ab standard OSI layer-2 protocol, which allows Ethernet network devices to advertise details about themselves, such as a device configuration, device capabilities, and the device identity, periodically to directly connected devices on the network that are also using LLDP. Since it runs over the data-link layer, it allows two systems with different network layer protocols to learn about each other. LLDP is a "one hop" unidirectional protocol in an advertising mode, and does not solicit information or monitor state changes between LLDP nodes. Additionally, devices can choose to turn off the send or receive functions independently. Advertisements are sent out and received on every active and enabled interface, allowing any device in a network to learn about all devices to which it is connected. LLDP is designed to be managed with SNMP. Applications that use this protocol include topology discovery, inventory management, emergency services, VLAN assignment, and inline power supply.

Link **L**ayer **D**iscovery Protocol (LLDP) menu consists of LLDP **Setting** and LLDP **Neighbors** submenu, as shown in Figure 2.48.

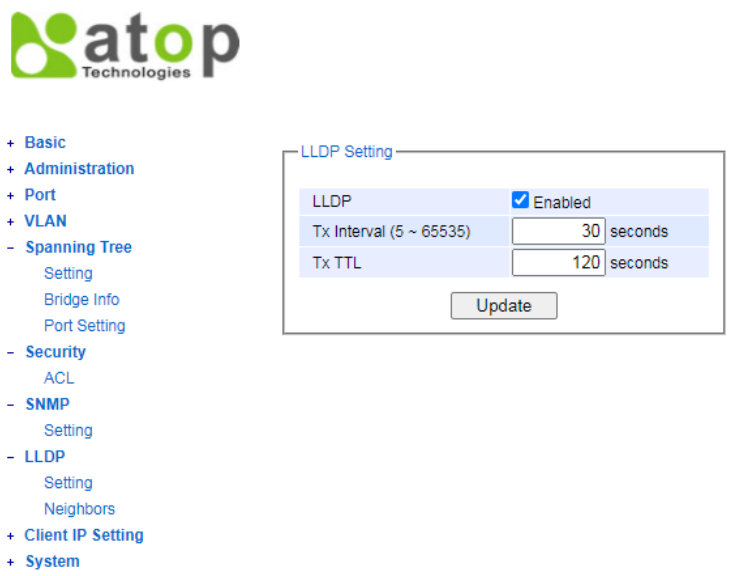


Figure 2.48 LLDP Dropdown Menu

2.8.1 Settings

In Figure 2.49, the LLDP Setting webpage allows users to have options for enabling or disabling the LLDP, as well as setting LLDP transmission parameters. This LLDP function should be enabled if users want to use Atop's Network Management Utility (formerly called NMU) to monitor the switches' topology of all LLDP devices in the network. Table 2.19 describes the LLDP Setting parameters which are transmit interval (**Tx Interval**) and transmit time-to-live (**Tx TTL**) of the LLDP advertisement packets.

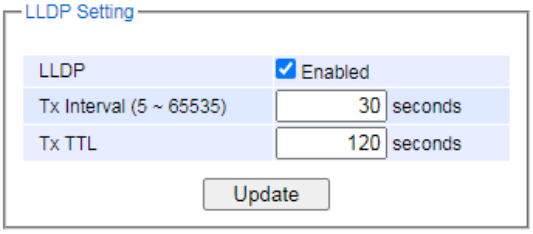


Figure 2.49 LLDP Setting Webpage

Table 2.19 Descriptions of LLDP Setting

Label	Description	Factory Default
LLDP	Choose to either enable or disable LLDP.	Enabled
Tx Interval	Set the transmit interval of LLDP messages. Range from 5 to 65535 seconds.	30
TxTTL	*Tx TTL is short for Time-To-Live*. It is an amount of time to keep neighbors' information. The recommended TTL value is 4 times of *Tx Interval*. The neighbors' information is only removed when the timer is expired. Range from 5 to 65535 seconds.	120

2.8.2 Neighbors

This menu allows the user to view the **LLDP's neighbor** information of the managed switch, as shown in Figure 2.50. The Neighbors Information table contains **Chassis ID**, **Port ID**, **Port Description**, **Device Name**, **Device Description**,

and **Management Address** on each Port of the managed switch. Users can click on the **Refresh** button to get the latest Neighbors Information table or the **Clear** button to clear all the information on the displayed Neighbors Information table.

An example of Neighbors' information table is depicted in Figure 2.51. Note that this example is based on a displayed format of an early version of NSG series NAT switch, where **System Name** is changed to **Device Name** and **System Description** is changed to **Device Description** in the latest version of NSG330X's firmware. Figure 2.20 describes the setting parameters in the LLDP Neighbors Webpage.

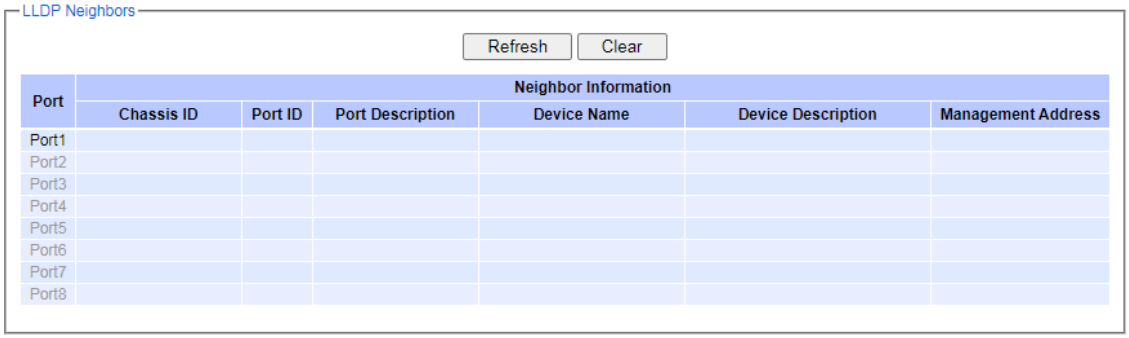


Figure 2.50 LLDP Neighbors Webpage

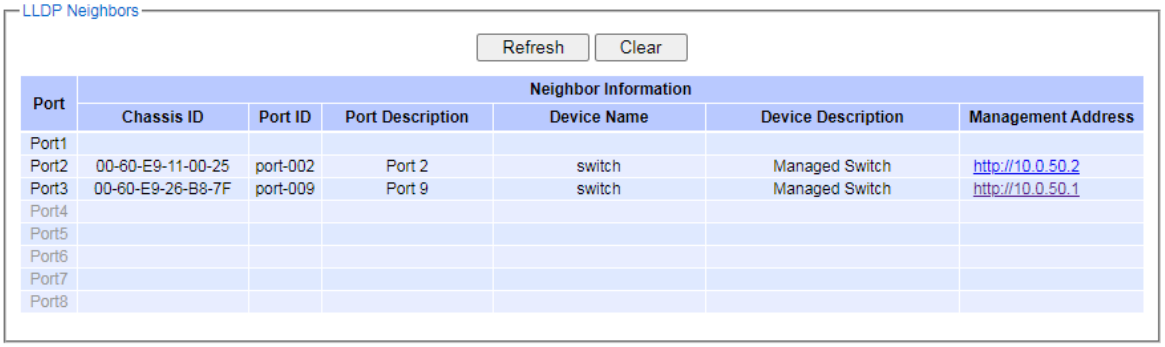


Figure 2.51 Example of LLDP Neighbors' Information

Table 2.20 Descriptions of LLDP Neighbors Webpage

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

2.9 Client IP Setting

2.9.1 DHCP Mapping IP

In **Client IP Setting->DHCP Mapping IP** submenu, a user can map an IP address to the connected device on each port. Figure 2.52 shows the DHCP Mapping IP webpage where the desired IP address can be entered into the field for each Port. After finishing the DHCP IP mapping to the port(s), please click on the **Update** button to allow the change to take effect.

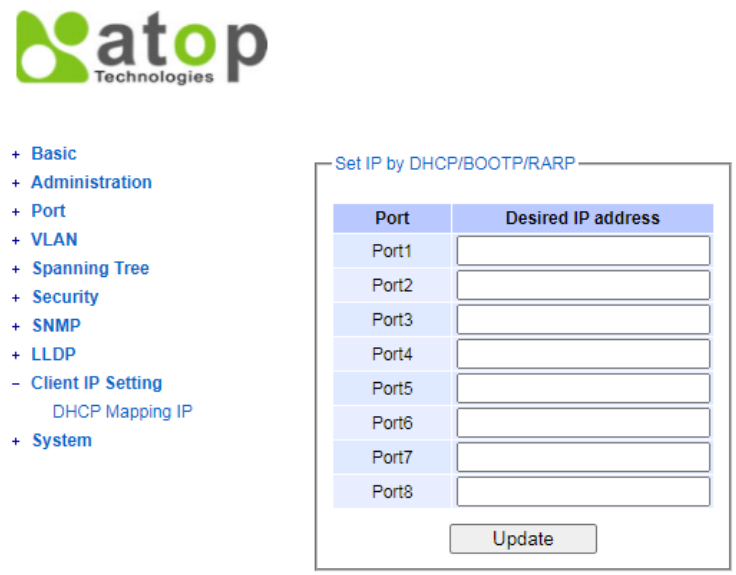


Figure 2.52 DHCP Mapping IP Webpage

2.10 System

This last section on the WebUI interface of the NSG330X switch provides miscellaneous tools for network administrator to check the internal status of the switch via system log. It also allows the administration to perform device maintenance operations such as backing up or restoring device's configuration, updating the firmware, reversing the device to factory default setting, rebooting, and logging out from the system/device. Figure 2.53 shows all the dropdown menus under the **System** section.

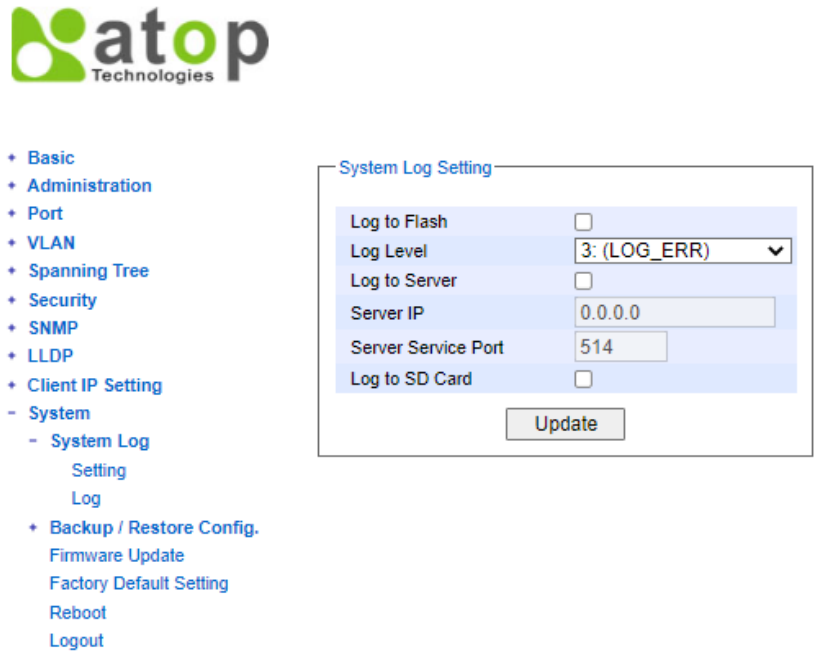


Figure 2.53 System Dropdown Menu

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

Email alerts and relays outputs under the System section is used to provide fast and reliable warning alerts for administrators.

2.10.1 System Log

2.10.1.1 Settings

Figure 2.54 shows System Log related settings configuration. The actual recorded log event will be shown in Event Log on the next subsection. Here the users can enable how the log will be saved and/or delivered to other system. The log can be saved to flash memory inside the managed switch and/or saved to SD Card and/or can be sent to a remote log server. The users need to select the log level and provide the IP address of a remote log server and the server's service port. Please click on the Update button after finishing the setup. Table 2.21 describes the details of parameters setting for the system log.

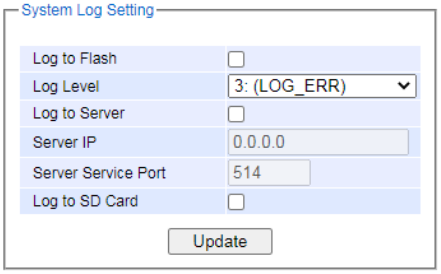


Figure 2.54 System Log Setting Webpage

Table 2.21 Descriptions of System Log Settings

Label	Description	Factory Default
Log to Flash	**Checked**: Saving log event into flash memory. The flash memory can keep the log event files even if the switch is rebooted. **Unchecked**: Saving log event into RAM memory. The RAM memory cannot keep the log event files after each reboot.	Uncheck
Log Level	Set the log level to determine what events to be displayed on the **System Log->Log** webpage. The level selection is inclusive. For example, if 3 :(Log_ERR) is selected, all 0, 1, 2 and 3 log levels will be implied. Range from Log 0 to Log 7.	3: (LOG_ERR)
Log to Server	**Checked**: Enable Syslog Server. **Uncheck**: Disable Syslog Server. If enabled, all recorded log events will be sent to the remote System Log server.	Uncheck
Server IP	Set the IP address of Syslog server	0.0.0.0
Server Service Port	Set the service port number of System Log server. Range from Port 1 to Port 65535.	514
Log to SD Card	**Checked**: Enable Log to SD Card. **Uncheck**: Disable Log to SD Card If enabled, all recorded log events will be saved to SD Card	Uncheck

2.10.1.2 Log

Figure 2.55 shows an example of all of the events' logs. Note that they are sorted by date and time. Table 2.22 provides an explanation of each column and the button's functions on the System Log webpage.

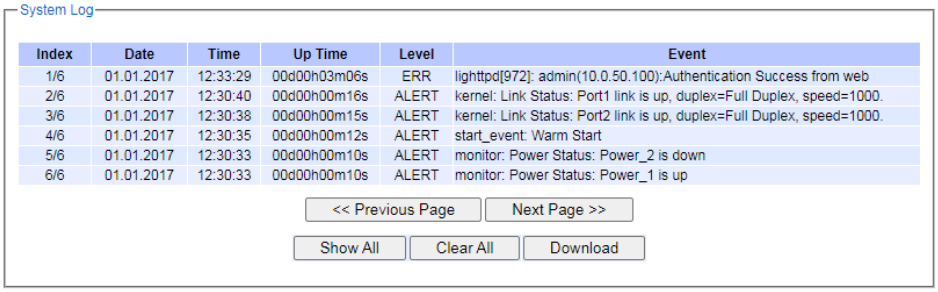


Figure 2.55 Event Log Webpage

Table 2.22 Descriptions of Event Log

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

2.10.2 Backup / Restore Config.

2.10.2.1 HTTP

Figure 2.56 shows the webpage for Backup/Restore the configuration via HTTP. It is divided into two parts: **Backup the Configuration** and **Restore the Configuration**. When clicking on the **Download** button on the upper part of the webpage, the users will be prompt to **Opening** the file name NSG330x.bin.sum by an application or to **Save File** to a destination. Choosing to Save File will back up the switch's current configuration to your local drive on the local computer.

To restore a configuration file to the switch, please move down to the **Restore the Configuration** part, then click the **Choose File** button to choose a configuration file from the local drive. Before clicking the **Upload** button, the users have a choice to select **Keep the current username & password setting** option below the uploading filename. This will help users from the necessity to logging-in again using a previously stored username and password configuration after settings are restored.

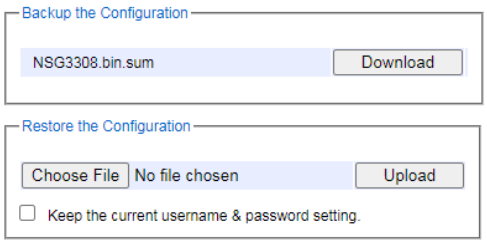


Figure 2.56 Backup/Restore Configuration via HTTP

2.10.2.2 SD Card

Figure 2.57 shows the setting configuration of a SD Card backup. The last backup configuration file in SD card (The highest serial number in the periodic backup folder) can be used as the start-up configuration during DUT boot-up. Here, users can also enable saving to SD Card automatically and/or periodically, and configure the backup period. Table 2.23 describes the setting parameters of **SD card Settings** for Backing up in details.

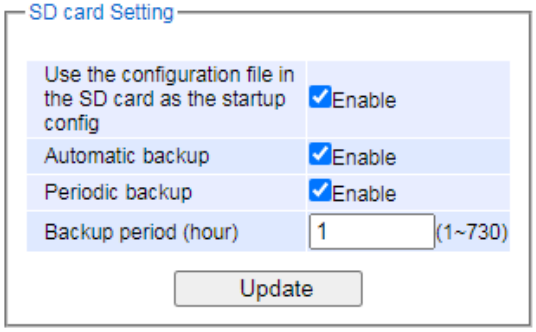


Figure 2.57 Setting Configuration's Webpage on the SD Card Backup

Table 2.24 Descriptions of Setting Configuration on the SD Card Backup

Label	Description	Factory Default
Use the configuration file in the SD card as the startup config	**Checked**: Enable feature **Uncheck**: Disable feature User can use the backup configuration file in SD card (The highest serial number in the periodic backup folder) as the start-up configuration during DUT boot-up.	Checked
Automatic backup	**Checked**: Enable automatic backup **Uncheck**: Disable automatic backup If enabled, when a user updates the settings of DUT, the system will backup configuration automatically to SD card. If the backup configuration file had existed, the backup configuration file will be overwritten.	Checked
Periodic backup	**Checked**: Enable periodic backup **Uncheck**: Disable periodic backup If enabled, the system will follow the backup period to backup configuration to SD card (The backup directory is the Periodic backup folder), and the format of backup configuration will be "flash{No.}yyyymmddThhmmss".	Checked
Backup period (hour)	Configure the backup configuration file period.	1

2.10.3 Firmware Update

The users can update the device firmware via web interface, as shown in Figure 2.58. To update the firmware, users can download a new firmware from Atop's website and save it to a local computer. Then, the users can click **Choose File** button and choose the firmware file that is already downloaded. The switch's firmware typically has a ".dld"

extension, such as nsg330x-K111A112.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 2.58 Firmware Update Webpage

2.10.4 Factory Default Setting

When the NAT switch is not working properly, users can reset it back to the original factory default settings by clicking on the **Reset** button, as shown in Figure 2.59.

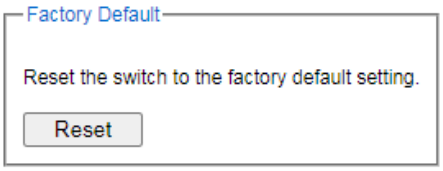


Figure 2.59 Factory Default Setting Webpage

2.10.5 Reboot

An easy reboot function is provided in this webpage requiring only one single click on the **Reboot** button, as shown in Figure 2.60.

Figure 2.60 Reboot Webpage

2.10.6 Logout

A logout function is provided in this webpage requiring only one single click on the **Logout** button, as shown in Figure 2.61.

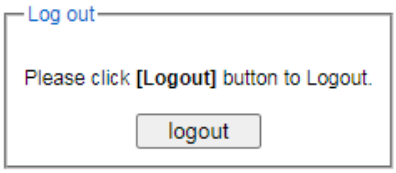


Figure 2.61 Logout Webpage

Atop Technologies, Inc.

www.atoponline.com
www.atop.com.tw

TAIWAN HEADQUARTER:

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

ATOP CHINA BRANCH:

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

ATOP INDIA OFFICE:

Abhishek Srivastava
Head of India Sales
Atop Communication Solution(P) Ltd.
No. 22, Kensington Terrace,
Kensington Rd,
Bangalore, 560008, India
Tel: +91-80-4920-6363
E-mail: Abhishek.S@atop.in

ATOP INDONESIA BRANCH:

Jopson Li
Branch Director
Wisma Lampung Jl.
No. 40, Tomang Raya
Jakarta Barat, 11430, Indonesia
Tel. +62-857-105957755
E-mail : jopsonli@atop.com.tw

ATOP EMEA OFFICE:

Bhaskar Kailas (BK)
Vice President (Business Development)
Atop Communication Solution(P) Ltd.
No. 22, Kensington Terrace,
Kensington Rd,
Bangalore, 560008, India
Tel: +91-988-0788-559
E-mail: Bhaskar.k@atop.in

ATOP AMERICAs OFFICE:

Venke Char
Sr. Vice President & Head of Business
11811 North Tatum Blvd, Suite 3031
Phoenix, AZ 85028,
United States
Tel: +1-602-953-7669
E-mail: venke@atop.in