User's Guide

Gigabit L2 Web-Smart Managed Switch Configuration Guide

(NGS-Series Smart Switch Models)

1111 W. 35th Street, Chicago, IL 60609 USA • www.tripplite.com/support

Table of Contents

Table of Contents

1. Introduction

This guide describes how to configure Tripp Lite Gigabit L2 Web-Smart Switch (NGS-Series) models by using the built-in Web-based graphical user interface (GUI). Tripp Lite Gigabit L2 Web-Smart Switch models contain an embedded web server and management software for managing and monitoring switch functions. The Web management interface can be used to configure more advanced features that can improve switch efficiency and overall network performance. The console port will allow command line interface to the switch (future use).

Note: *Gigabit L2 Web-Smart Switches are referred to as the "switch" throughout the manual. The information in this document applies to all switch models unless otherwise noted.*

1.1 Switch Configurations

The switches contain different port quantities and features, but their configuration through the Web management interface is consistent.

Section 1: Introduction. Contains the contents overview of the entire configuration manual.

Section 2: Web Management Configuration. Contains the initial configuration that needs to take place before logging in to the switch, along with instructions for logging in to the switch's Web management interface.

Section 3: Web Management Interface Homepage. This section will familiarize you with the Web management interface.

Section 4: Quick Configuration. Illustrates how to quickly set up the management features through the Web interface.

Section 5: Port Management. Presents commonly used settings for the switch ports.

Section 6: VLAN Management. Overview of the management and configuration of VLAN(s).

Section 7: Fault/Safety Management. Describes safety management and configuration, such as attack prevention, access control lists, etc.

Section 8: PoE System Management. Describes Power over Ethernet management and configuration through the Web management interface (applies only to PoE-enabled switches).

Section 9: Spanning Tree Protocol (STP) Management. Describes management of the Spanning Tree Protocol configuration of the switch.

Section 10: DHCP Relay Management. Covers setup of the DHCP relay agent and configuration of Option 82 settings to a DHCP server.

Section 11: QOS (Quality of Service) Management. Describes QoS management of each port of the switch.

Section 12: MAC Address Table Management. Covers the management of the MAC address table access list.

Section 13: SNMP Management. Covers the configuration of the SNMP management features of the switch.

Section 14: System Management. Guide to the switch system management, including software upgrades through the Web page, configuration file management, etc.

Appendix I: Default Settings. Quick reference to the default settings for login, password, etc.

2. Web Management Configuration

2.1 Initial Setup

2.1.1 Set the IP Address of the Computer

The IP address of the management computer and the switch must be set to the same subnet. (The switch's default IP address is 192.168.2.1 and its default subnet mask is 255.255.255.0). The gateway does not need to be configured for initial switch configuration.

The IP address of the management computer needs to be configured manually within the default IP address range of 192.168.2.xxx ("xxx" ranges from 2-254).

By default, all ports belong to VLAN1. The management host computer can perform switch configuration by accessing any port.

Note: *This manual is appropriate for all models in Tripp Lite's family of NGS-Series Web-Smart managed switches. This User's Guide uses one switch configuration as an example to illustrate how to configure the switch using the Web management interface.*

2.1.2 Confirm Network Connectivity Between the Computer and the Switch

Follow the steps below to confirm network connectivity between the computer and the switch:

Step 1: Press the Windows key + R, then type cmd in the input field of the "Run" window and click "OK". This brings up the command prompt window (Figure 2.1).

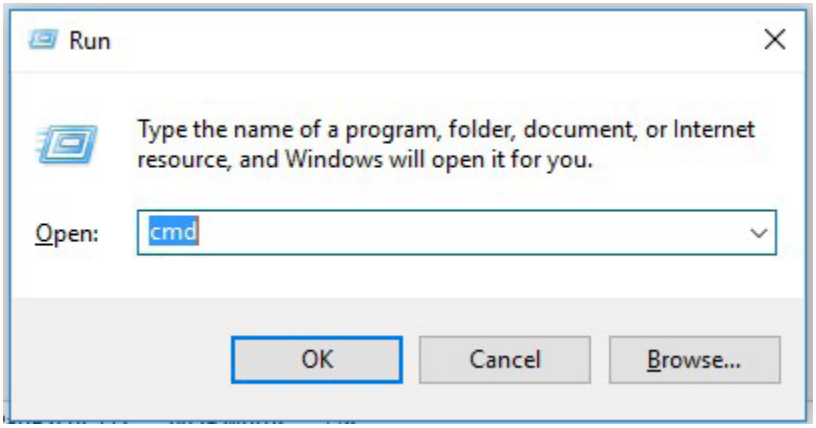


Figure 2.1: Confirming Network Connectivity

Step 2: In the command prompt dialog box, type ping 192.168.2.1 then press "Enter". If a response to the ping is returned from the switch, proper network connectivity is established. If no response is received, check the network connection.

2. Web Management Configuration

2.1.3 Access to the Web Management Interface

Open a Web browser (e.g. Internet Explorer), type **http://192.168.2.1** in the address bar, then press “Enter”. Enter the User Login interface of the switch administration page. In the login interface (Figure 2.2), select the preferred language (default language is English), then enter the user name and password. The default user name and password are both admin (case sensitive). Click the “Login” button or press “Enter” to access the Web management interface.

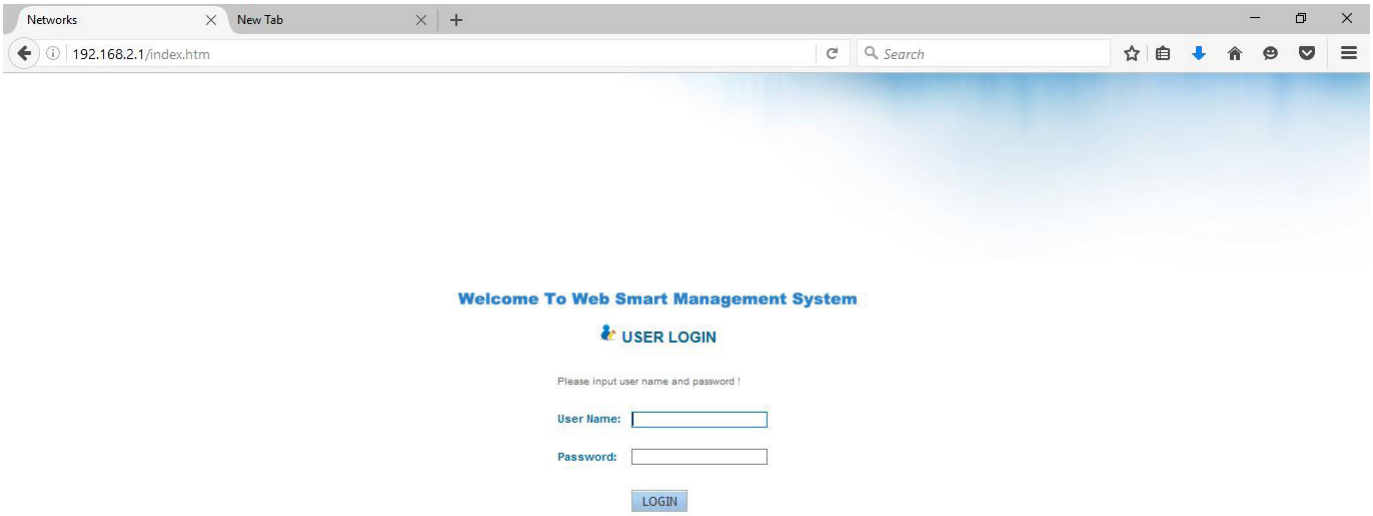


Figure 2.2 Web Login Interface Landing Page

After a successful login, the browser will show the homepage of the Web management interface corresponding to the switch, as illustrated in Figure 2.3:

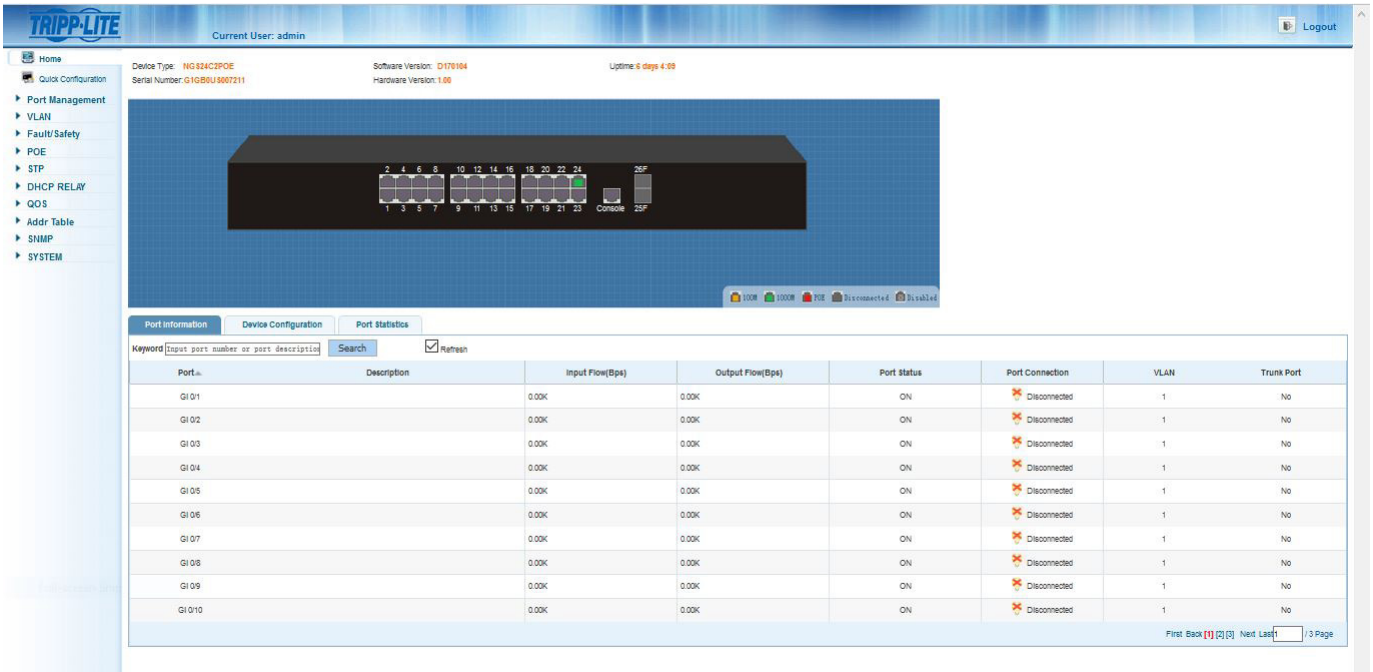


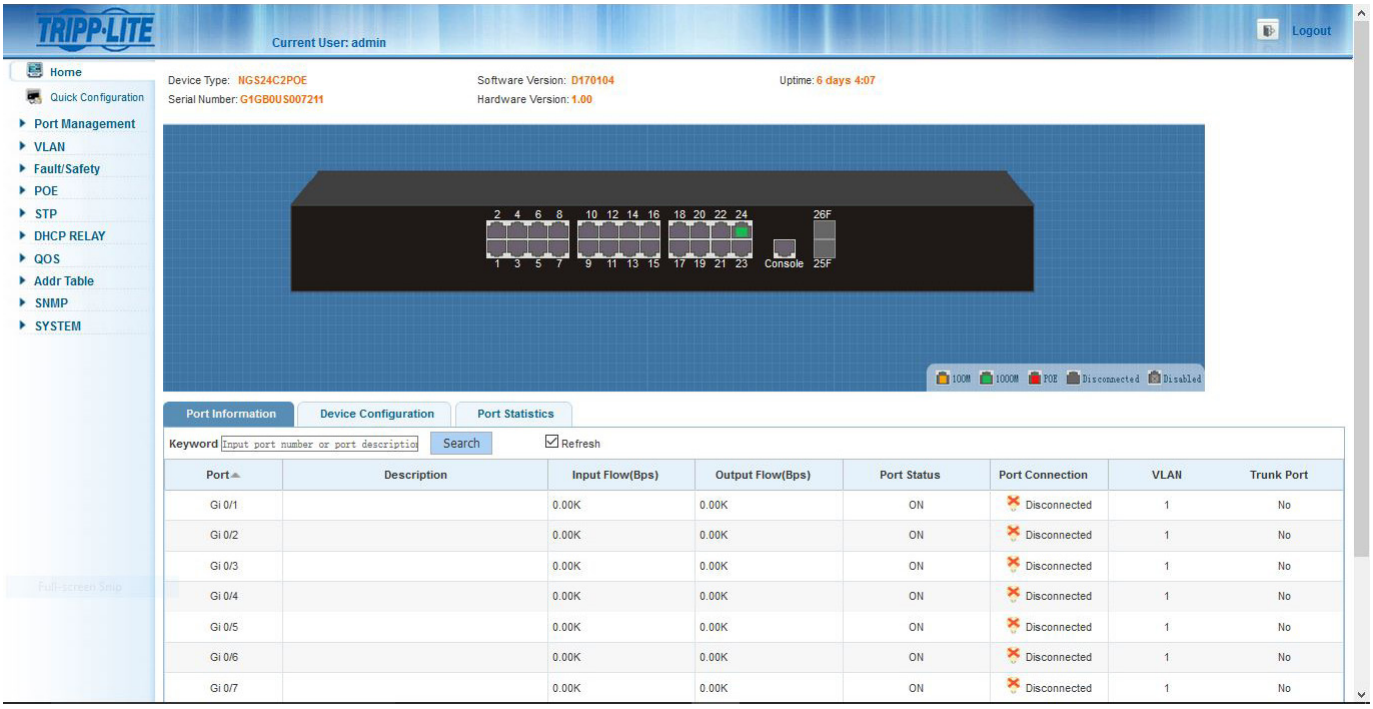
Figure 2.3 Switch Web Management Interface (Administrator View)

Notes:

- *It is recommended to use Internet Explorer 8 or higher, Firefox, or Chrome with the Web management interface.*

3. Web Management Interface Homepage

3.1 Web Management Interface Homepage Overview



The Web management interface homepage displays the current user, the switch's system information, uptime, network port Information, device configuration, and port statistics. The switch graphic displays current connections whether running at 10/100 (orange), 1000Mbps (Green), PoE active (Red), Disconnected (Grey), or Disabled (Grey with X).

3.2 Web Management Interface Menus

There are 12 primary menu options in the Web management interface: System Home, Quick Configuration, Port Management, VLAN, Fault/Safety, PoE (applicable only to PoE-enabled switches), STP, DHCP RELAY, QoS, Addr Table, SNMP and System.

Each primary menu option contains a secondary menu. By default, the secondary menus are hidden. Click on a primary menu option to expand the secondary menu.

- **Web Management Interface Homepage**
- **Quick Configuration**
  - o VLAN Settings
  - o Other Settings
- **Port Management**
  - o Basic Settings
  - o Port Aggregation
  - o Port Mirroring
  - o Port Speed Limit
  - o Storm Control
  - o Port Isolation
- **VLAN Management**
  - o VLAN Management
- **Fault/Safety Management**
  - o Attack Prevention
  - o Path Detection
  - o ACL (Access Control List)

3. Web Management Interface Homepage

- **POE System Management**
  - o PoE Config
  - o PoE Port Config
- **STP (Spanning Tree Protocol)**
  - o MSTP Region
  - o STP Bridge
- **DHCP Relay**
  - o DHCP Relay
  - o Option 82
- **QOS (Quality of Service)**
  - o QoS Remark
  - o Queue Config
  - o Queue Mapping
- **Addr Table (MAC Address Table)**
  - o Address Table
- **SNMP**
  - o SNMP Config
  - o RMON Config
- **System**
  - o System Config
  - o System Update
  - o Config Management
  - o Config Save
  - o Administrative Privileges
  - o Factory Reset
  - o Info Collect

Note: *If there is no activity in the Web management interface for 30 minutes (default setting), the system will automatically logout the user and return to the Web management interface login page.*

4. Quick Configuration

Select “Quick Configuration” to configure frequently used functions of the switch, such as VLANs, trunk ports, management system, and management interface password settings.

4.1 Adding VLANs

Select “Quick Configuration → VLAN Settings” to configure the VLANs and trunk ports (Figure 4.1). You can view and edit “VLAN Settings”, add new VLANs, modify VLAN, and delete VLAN(s). After configuring the VLAN(s), go to the “Trunk Settings” to add new trunk ports.

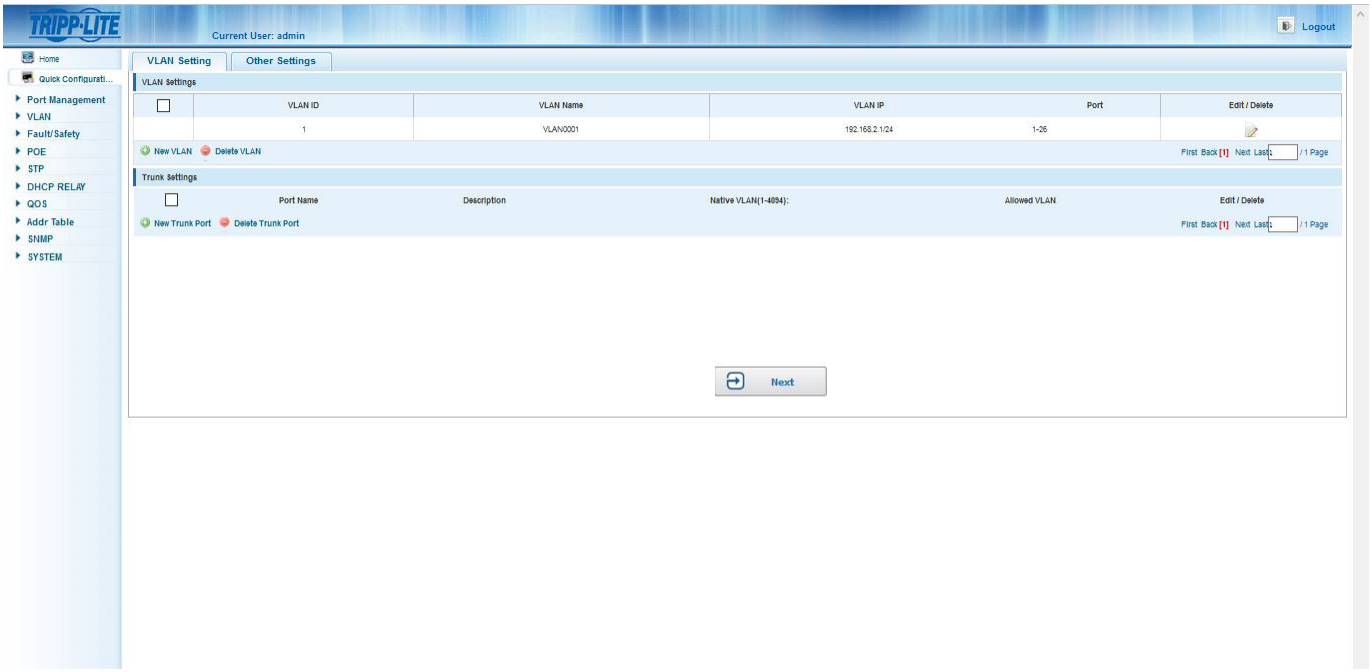


Figure 4.1: VLAN Settings

4.1.1 Adding New VLANs

Click the “New VLAN” icon and enter the new VLAN ID, VLAN Name, and then add the selected ports for that VLAN. Click “Save” once when finished. Repeat these steps to create additional VLANs.

4.1.2 Editing VLANs

Click on the “Edit” icon and to change the VLAN Name and the selected ports for that VLAN. Click “Save” once when finished editing. Repeat these steps to edit additional VLANs.

4.1.3 Deleting VLANs

To delete a VLAN, click on the red icon next to the VLAN to be deleted or click the checkbox next to the associated VLAN and click “Delete VLAN”. To delete multiple VLANs, check the boxes next to the VLANs to be deleted. Click “Delete VLAN” to delete the selected VLANs.

Note: *All ports associated with the deleted VLANs will automatically return to VLAN 1. VLAN 1 cannot be deleted.*

4. Quick Configuration

4.2 Trunk Port Settings

Select “Quick Configuration → VLAN Settings” to manage trunk port settings. You can view the trunk port settings of the switch and add new trunk ports, modify trunk ports, or delete trunk ports. After configuring the “Trunk Port Settings”, click “Next” to go to the “Other Settings” page.

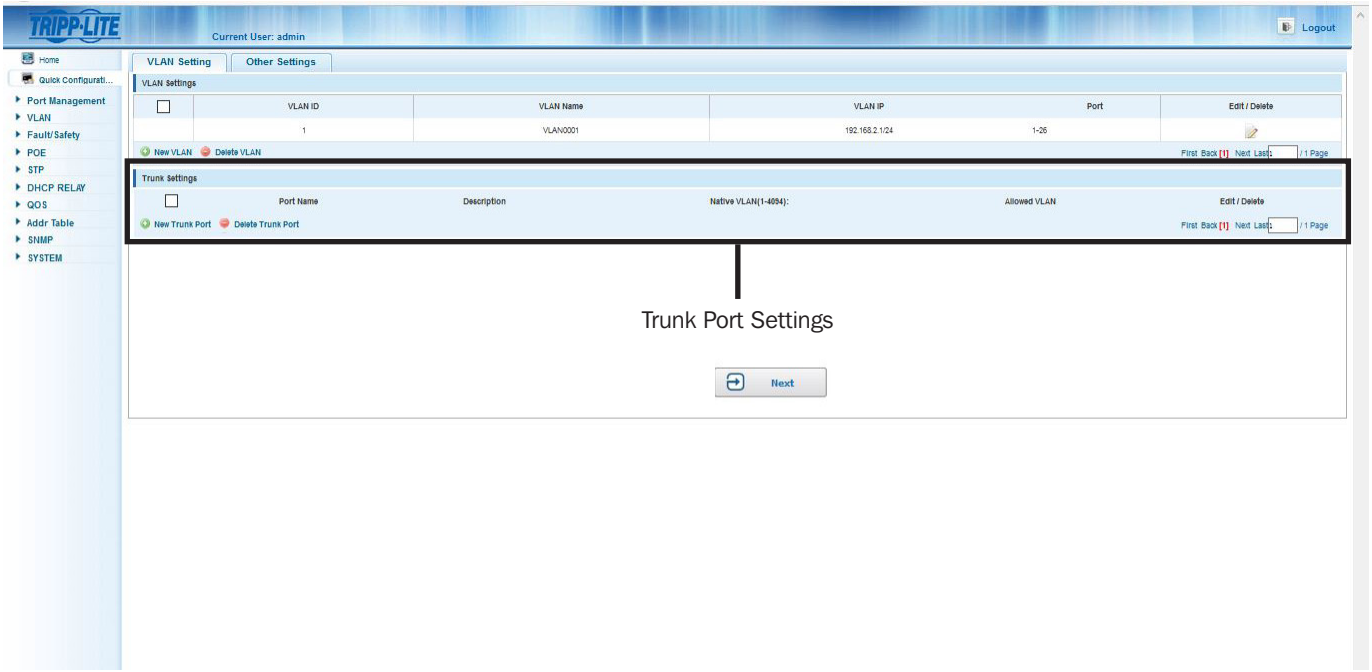


Figure 4.2 Trunk Port Settings

4.2.1 Adding Trunk Ports

Click the “New Trunk Port” icon and select the port(s) to configure. Enter the Native VLAN ID. Next, enter the IDs for the allowed VLANs that will have access through the trunk ports. Click “Save” when finished. Repeat these steps to create additional trunk ports.

4.2.2 Editing Trunk Port Settings

Click the “Edit” icon to make changes to the selected trunk ports, the Native VLAN, and Allowed VLANs. Click “Save” when finished editing. Repeat these steps to edit additional trunk ports.

4.2.3 Deleting Trunk Ports

To delete trunk ports, click on the red icon next to the trunk port to be deleted or click the checkbox next to the associated trunk port and click “Delete Trunk Port.” To delete multiple trunk ports, check the boxes next to the trunk ports to be deleted. Click “Delete Trunk Ports” to remove the selected trunk ports from the switch configuration.

4. Quick Configuration

4.3 Other Settings

Select “Quick Configuration → Other Settings” to view the system settings (Figure 4.3). From this page, you can change the switch’s management VLAN, management IP address, subnet mask, default gateway, DNS Server, device name, and management interface password. After modifying the configuration, click “Save”. Click “Finish” to return to the homepage, or click “Previous” to return to previous settings page to further modify the configuration.

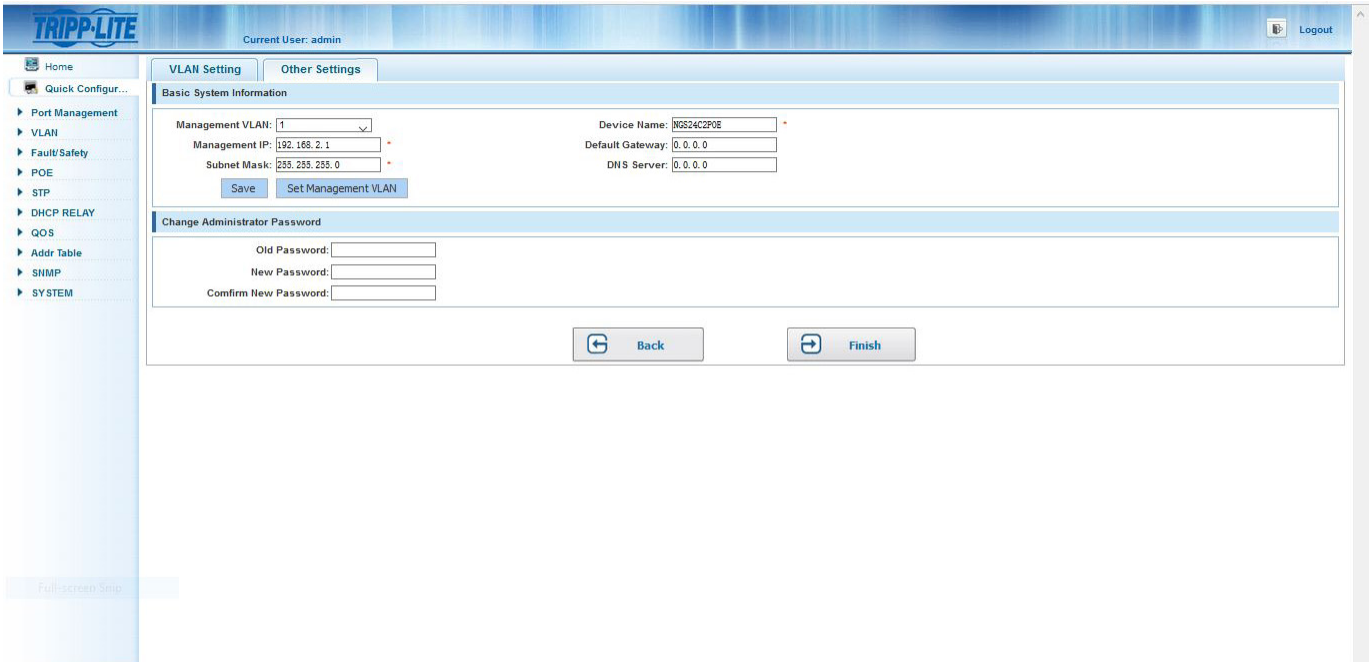


Figure 4.3: Other Settings

The Other Settings page shows basic system settings:

Management VLAN: The management VLAN ID of the switch defaults to 1.

Management IP: The IP address of the switch’s management VLAN.

Subnet Mask: The subnet mask of the switch’s management VLAN.

Device Name: The hostname of the switch.

Default Gateway: The default gateway of the switch’s management VLAN.

DNS Server: The IP address of the DNS server.

Note: *The management VLAN ID of the switch defaults to 1 and cannot be deleted.*

4.3.1 Modify Switch Management IP Address Settings

To set the management IP address of the switch, follow these steps:

1. Enter the IP address in the “Management IP” field (e.g. 192.168.100.179). Management IP is required.
2. Enter the subnet mask in the “Subnet Mask” field (e.g. 255.255.255.0). Management Subnet Mask is required.
3. Enter device name. Device name is required.
4. Enter the gateway address in the “Default Gateway” field (e.g. 192.168.100.1).
5. Enter DNS Server IP address (e.g. 192.168.10.12).
6. Click “Save” to complete the configuration.
7. Click “Set Management VLAN” to change to another VLAN other than the default VLAN ID of 1.

4. Quick Configuration

4.3.2 Change Web Management Interface Administrator Password

To edit the switch's Web management interface administrator password, enter the default password or prior password, then enter the new password (case sensitive). Enter the new password (case sensitive) again to confirm it. Click "Finish" to commit to the changes or "Back" to discard them.

5. Port Management

5.1 Basic Settings

5.1.1 View the Port Configuration

Select “Port Management → Basic Settings” to view and modify port settings (Figure 5.1).

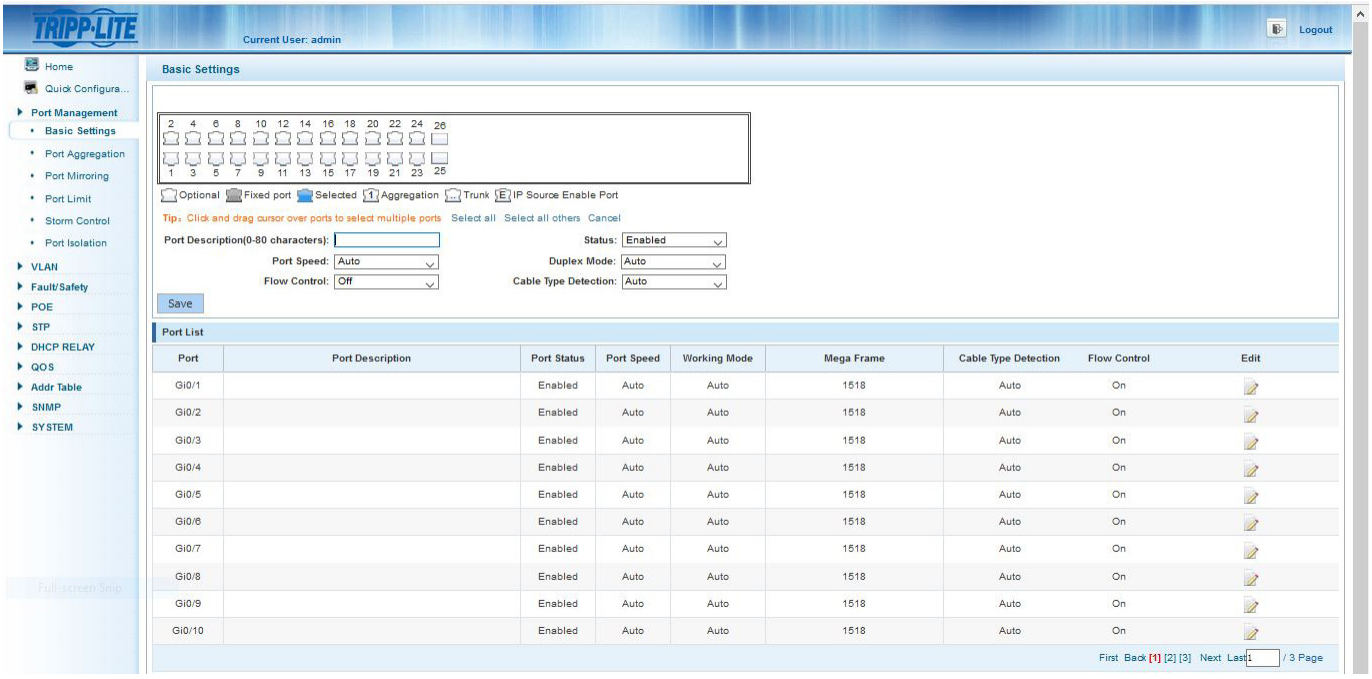


Figure 5.1: Basic Settings Page

The port list table displays the switch’s port configuration information in the following columns:

- **Port:** Displays the switch’s port number.
- **Description:** Displays the user-provided name or description given to the port.
- **Status:** Displays the port status, either “Enabled” or “Disabled”.
- **Port Speed:** Displays either auto-negotiation, 10, 100 or 1000 Mbps
- **Working Mode:** Displays port duplex configuration, auto-negotiation, full duplex or half duplex.
- **Mega Frame:** Displays the length of jumbo frames. Default mega frame length is 1518.
- **Cable Type Detection:** Displays crossover configuration, auto-negotiation, MDI or MDIX.
- **Flow Control:** Displays if port flow control is either “On” or “Off.”

Note: *The copper/fiber SFP’s rate can only be 1000 Mbps, and its working mode can only be auto/full duplex.*

5. Port Management

5.1.2 Configure Individual or Multiple Ports

Select the port(s) to be configured from the panel, then click the icon in the edit column to change the settings of each selected port.

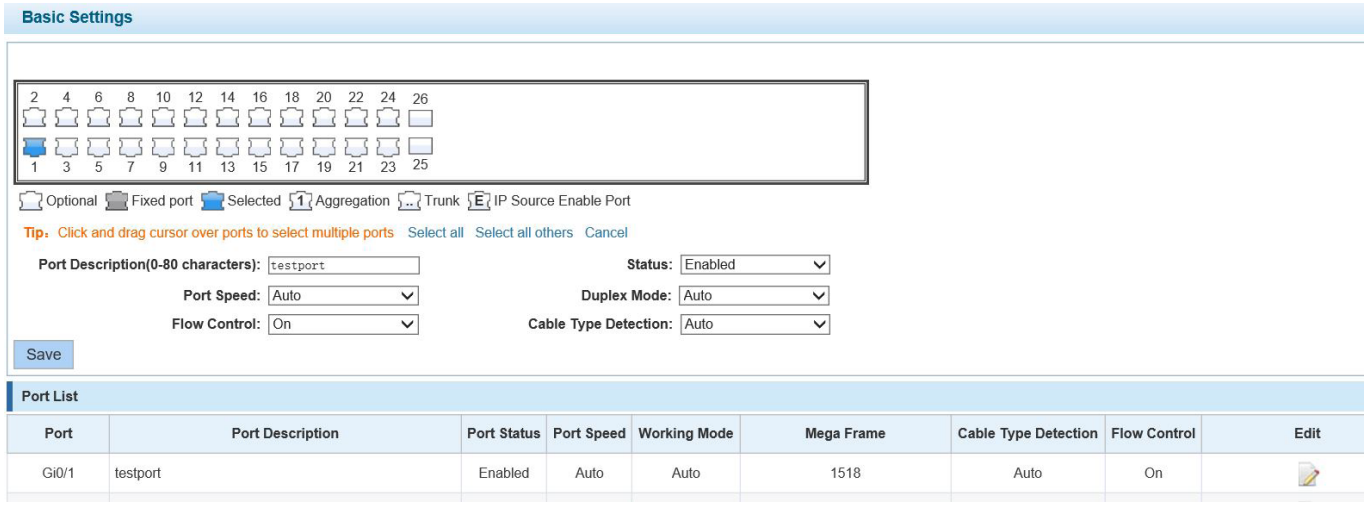


Figure 5.2: Individual Port Configuration

Note: *Within the individual port configuration screen, the following settings can be changed: Description, Status, Port Speed, Duplex Mode, Flow Control, and Cable Type Detection settings.*

5.2 Port Aggregation

5.2.1 View Port Aggregation Configuration

Select "Port Management → Port Aggregation" to view the switch's port aggregation configuration (Figure 5.3). Port Aggregation (or link aggregation) allows multiple Ethernet links to be combined into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load distribution.

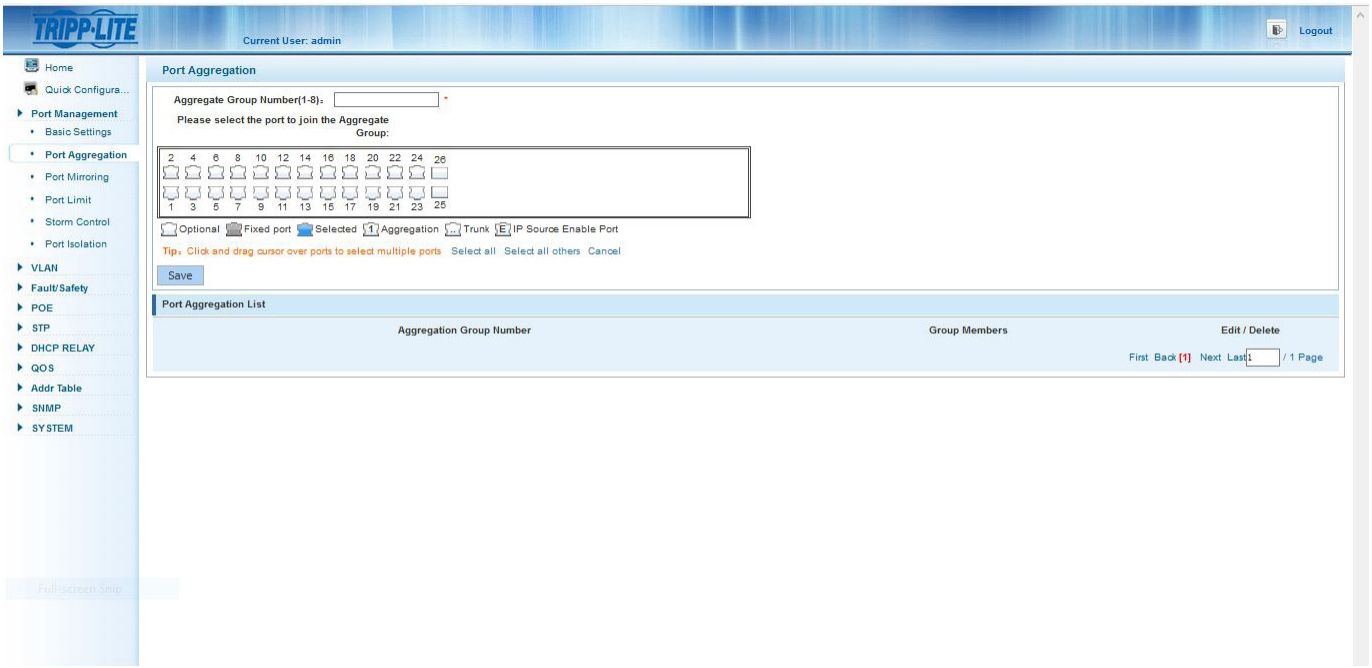


Figure 5.3: Port Aggregation

5. Port Management

The Port Aggregation table will show the switch's current configuration.

- **Aggregation Group Number:** Displays the number assigned to the aggregation group.
- **Aggregation Group Members:** Displays the port numbers that comprise a link aggregation group.

Notes:

- *Aggregation groups must contain a minimum of two ports; a maximum of eight ports can be aggregated in a group.*
- *Each port in a link aggregation group must use the same protocols and link speeds.*

5.2.2 Create a Port Aggregation Group

To create a port aggregation group, enter a port aggregation ID, then select the ports to be added to the aggregate group. Click "Save" to complete the configuration. When a port is part of an aggregation group, it will appear as shown in Figure 5.4.

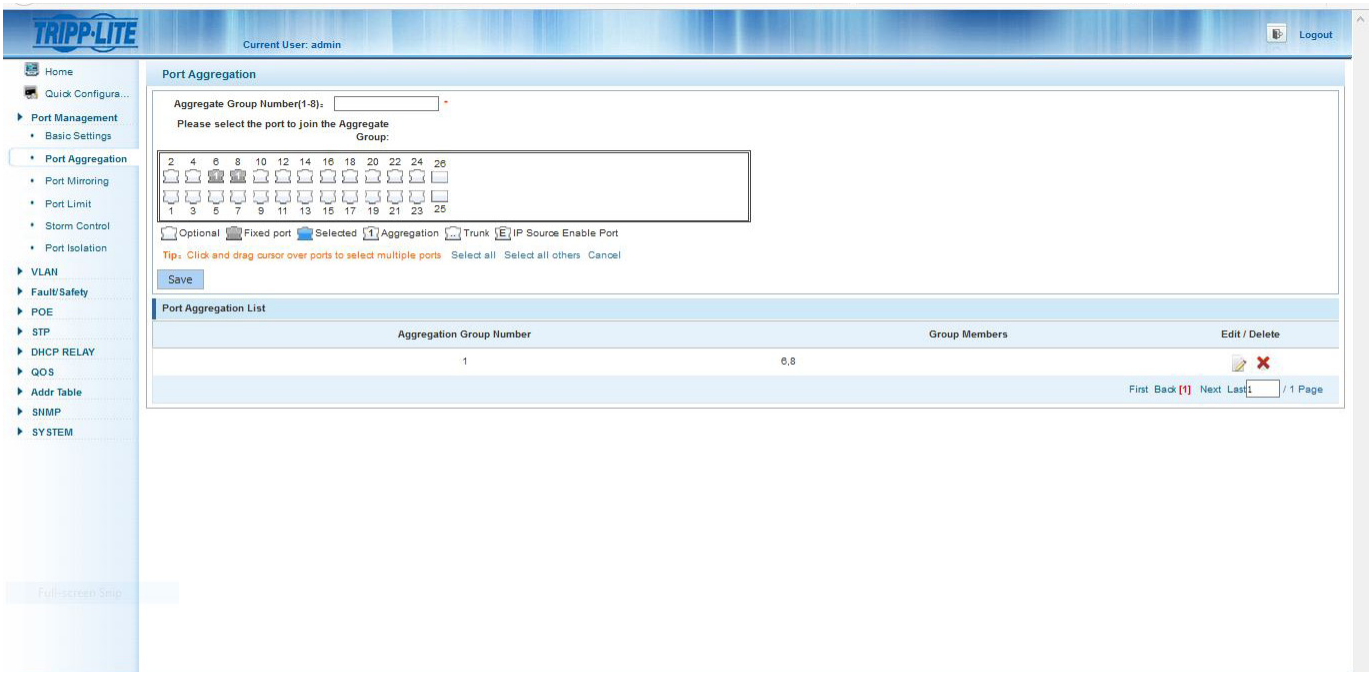


Figure 5.4: Creating a Port Aggregation Group

5. Port Management

5.2.3 Edit a Port Aggregation Group

Click the “Edit” icon to add members to the aggregation group. The aggregation group number cannot be changed once set. If you attempt to create a new aggregate group using an existing group number, it will display “The Aggregate port number already exists”. Choose another available group number to assign.

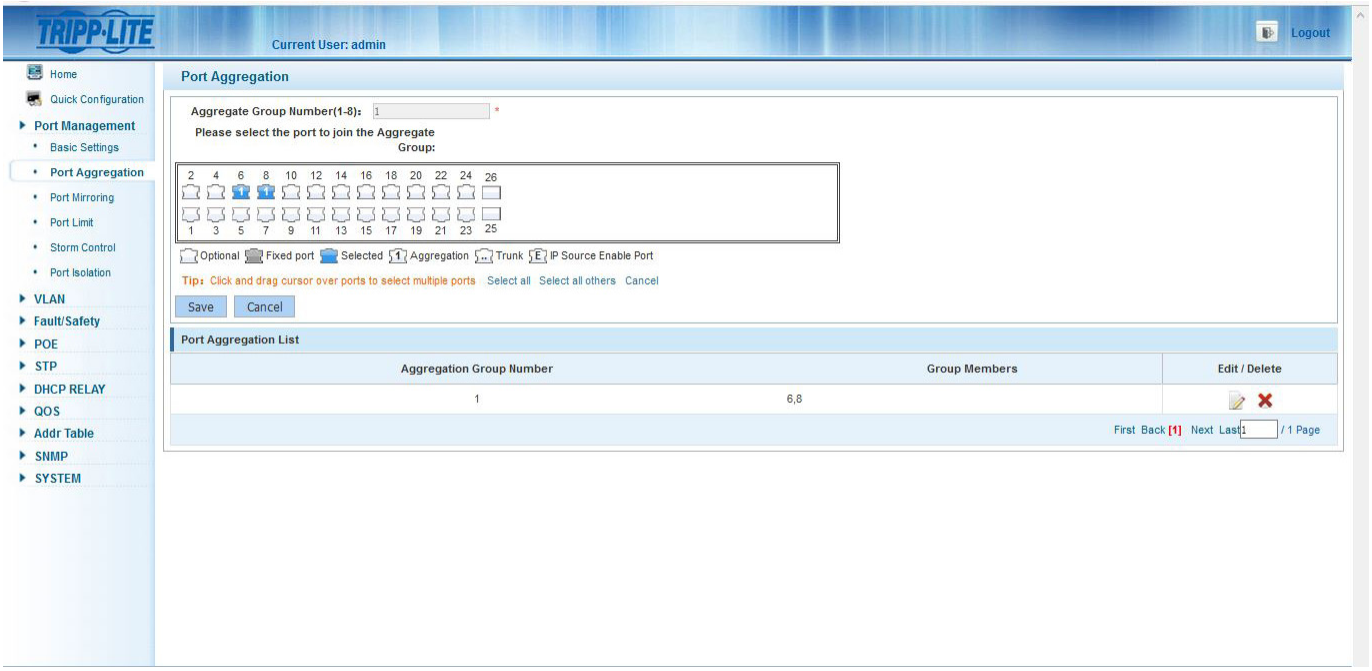


Figure 5.5: Edit or Delete Port Aggregation Group

5.2.4 Delete a Port Aggregation Group

Click the red ✖ icon next to the aggregation group to delete that port group.

5. Port Management

5.3 Port Mirroring

5.3.1 View Port Mirroring Configuration

Select “Port Management → Port Mirroring” to view the port mirroring configuration (Figure 5.6). Port mirroring selects the network traffic for analysis by a network analyzer. This can be done for specific switch ports. Many switch ports can be configured as source ports and one switch port is configured as a destination port. Packets copied to a destination port will be the same format as the original packet from the source. This means that if the mirror is copying a received packet, the copied packet will be VLAN tagged or untagged as it was received on the source port.

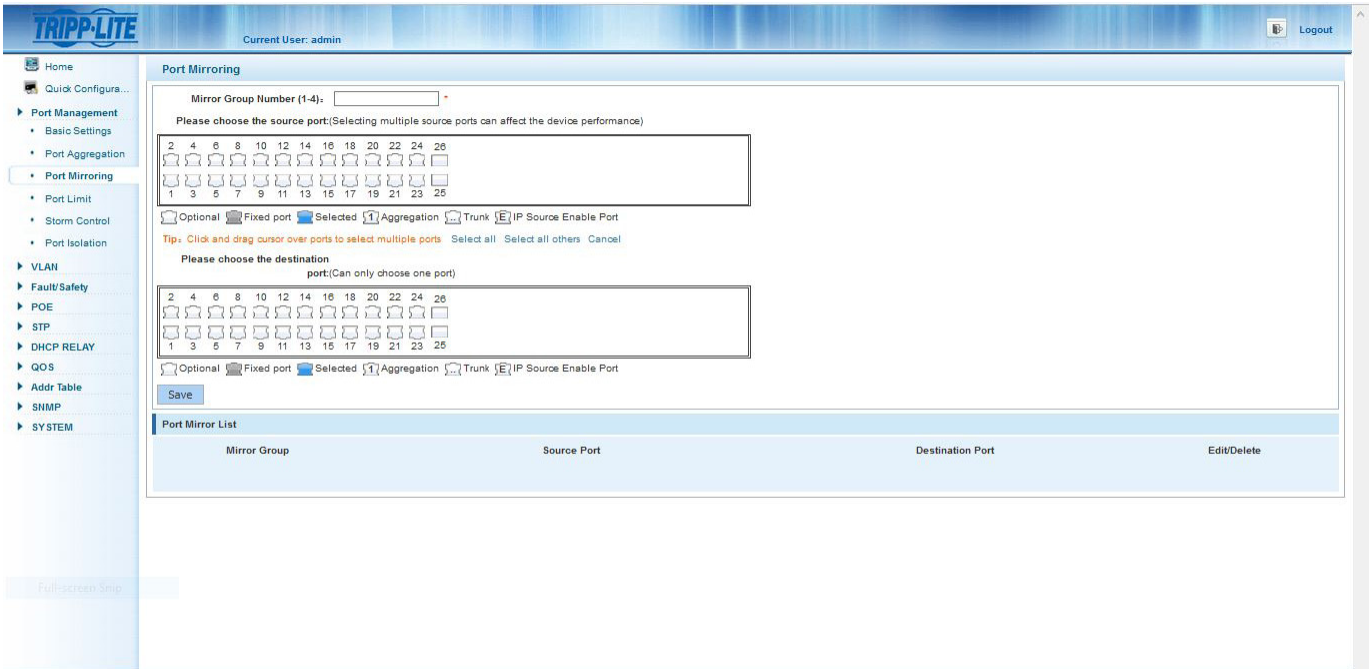


Figure 5.6: Port Mirroring Configuration

The Mirroring Port List shows the mirroring configuration of the switch.

- **Mirroring Group:** Mirror group ID; up to four mirroring groups can be created.
- **Source Port(s):** The port(s) the mirrored data comes from.
- **Destination Port:** The port receiving the mirrored data.

Notes:

- *Ports in aggregation ports cannot be designated as both the source port and the destination port.*
- *Only one destination port can be selected per mirroring group.*

5. Port Management

5.3.2 Create a Port Mirroring Group

To create a port mirroring group, select the source port(s) and the destination port, then select the mirroring group (Figure 5.7). Click “Save”.

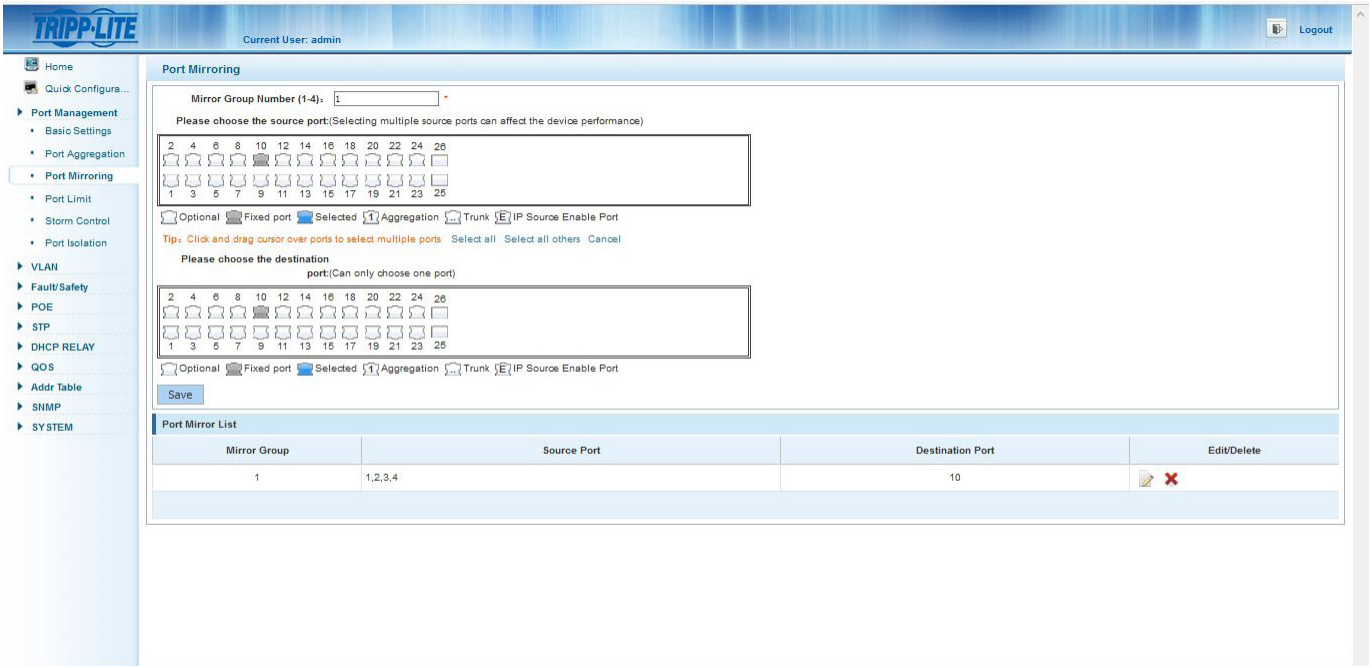


Figure 5.7: Create a Port Mirroring Group

5.3.3 Edit a Port Mirroring Group

Click the icon next to the port mirroring (Figure 5.8) group to edit its source and destination ports.

Note: *Mirror Group ID number cannot be edited once assigned.*

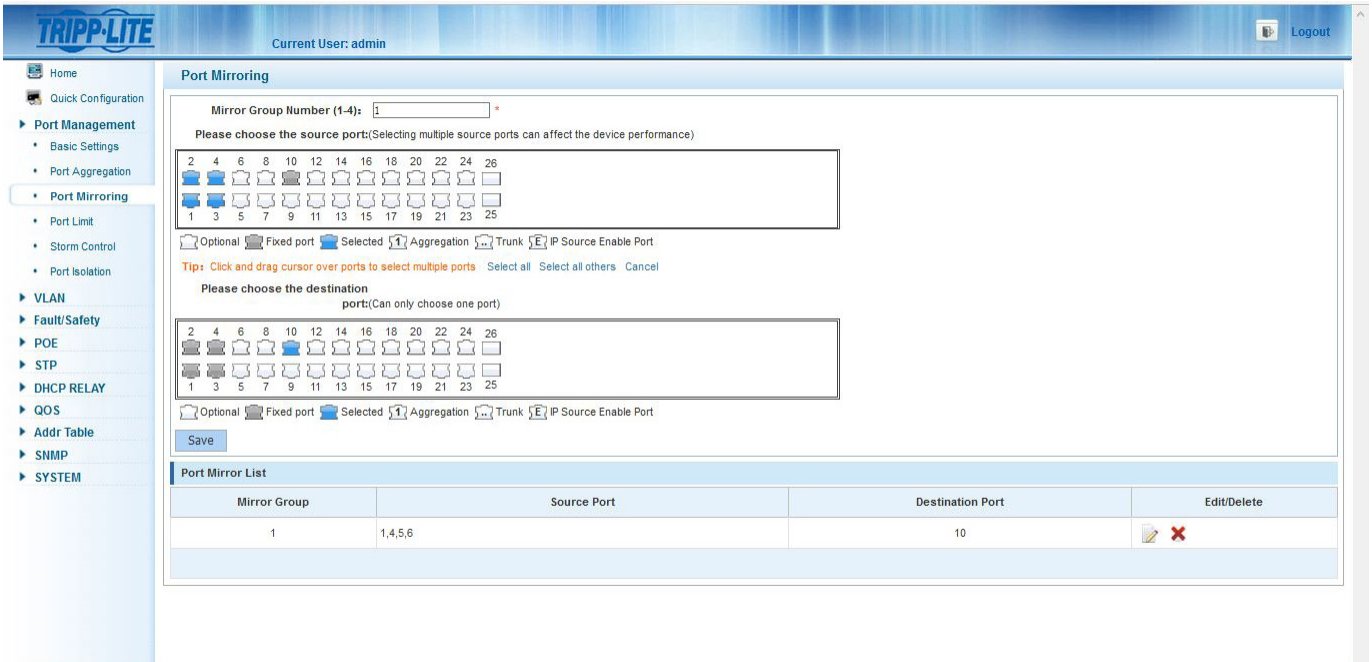


Figure 5.8: Edit or Delete a Port Mirroring Group

5. Port Management

5.3.4 Delete a Port Mirroring Group

Click the icon next to the mirror port group to delete the group.

5.4 Port Speed Limit Settings

5.4.1 View Port Speed Limit Settings

Select “Port Management → Port Limit” to view the switch’s port speed limit settings (Figure 5.9).

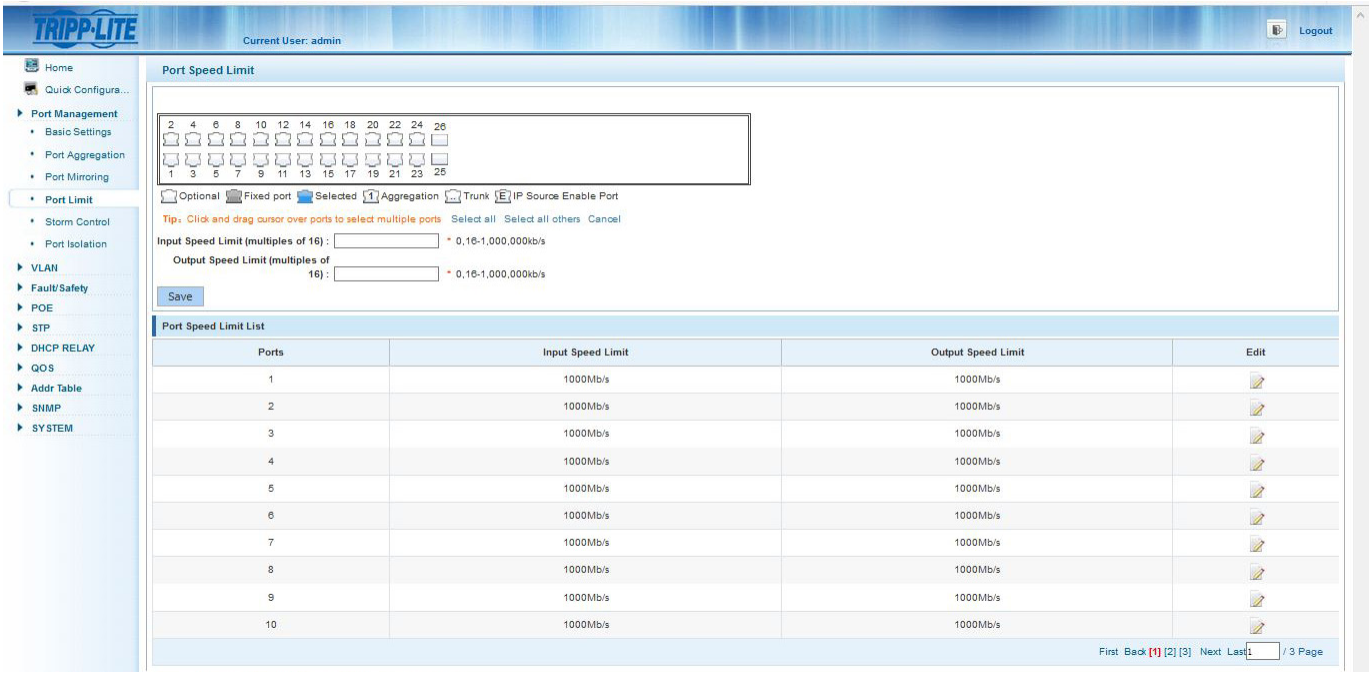


Figure 5.9: Port Speed Limit Configuration

The speed limit shows the port speed limit configurations of the switch.

- **Ports:** Shows the port number.
- **Input Speed Limit:** Upstream speed limit for the port.
- **Output Speed Limit:** Downstream speed limit for the port.

Note: *Multiple ports can be selected on the panel to modify port speed limit settings.*

5. Port Management

5.5 Storm Control Settings

5.5.1 Configure the Storm Control Settings of a Port

Storm Control ensures network performance from a flood of packets from Multicast, Unicast, or Broadcast traffic on the LAN. To configure, select “Port Management → Storm Control” to change the storm control settings of a selected port or ports (Figure 5.10). By default, this feature is disabled.

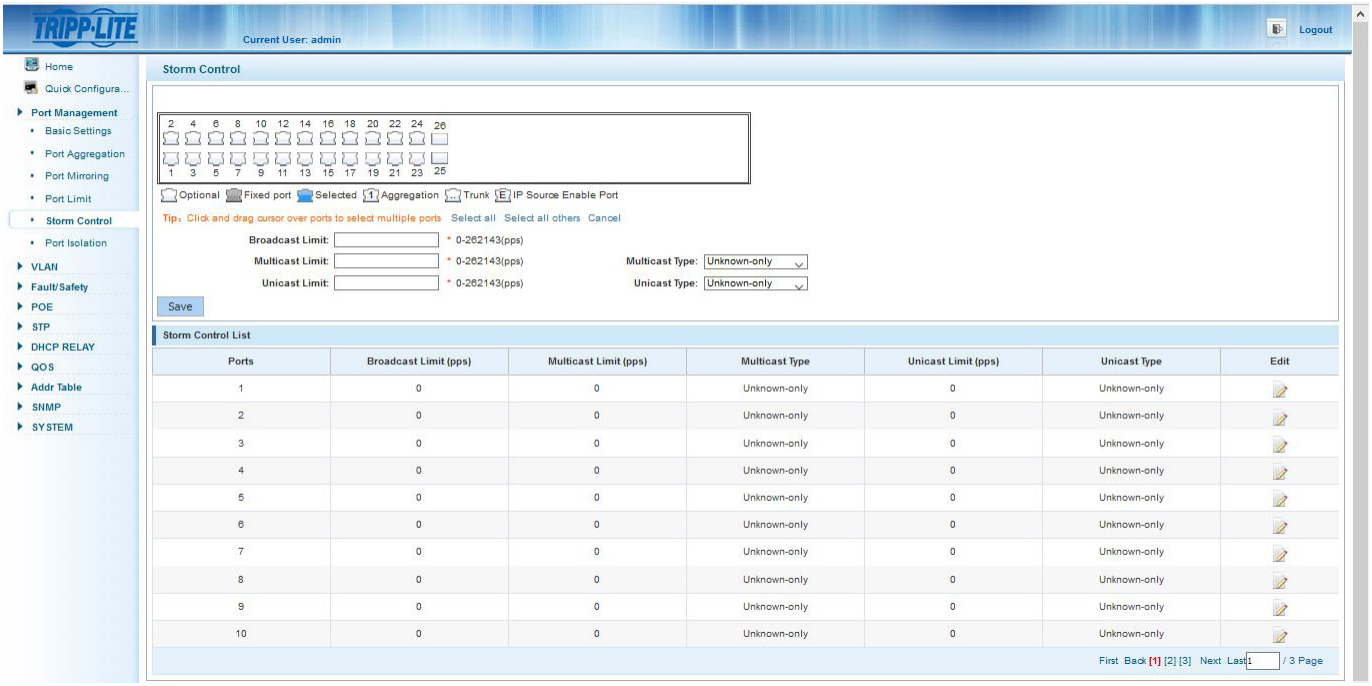


Figure 5.10: Storm Control Configuration Table

The view in Figure 5.10 displays the storm control configuration of the switch by port.

- **Ports:** Displays the switch’s port number.
- **Broadcast:** Displays whether Broadcast packet control is enabled or disabled. “0” denotes disabled.
- **Multicast:** Displays whether Multicast packet control is enabled or disabled. “0” denotes disabled.
- **Unicast:** Displays whether Unicast packet control is enabled or disabled. “0” denotes disabled.
- **Storm Control Value:** Set the rate at which storm control will be activated (between 0-262143 pps).
- **Storm Control Type:** Displays the types of storm control settings that can be configured for “Unknown-only” or “Both”. A device can implement the storm suppression to a broadcast, a multicast, or a unicast storm respectively. When excessive broadcast, multicast or unknown unicast packets are received, the switch temporarily prohibits forwarding of relevant types of packets till data streams are recovered to the normal state (then packets will be forwarded normally).

5.5.2 Edit Storm Control Settings

Select the port(s) to be configured (Figure 5.11). Click the “Storm Control Type” drop-down menu to select the type of storm control to be configured for the port. Enter a value from 0-262143 into the “Storm Control Value” fields for Broadcast, Multicast, and Unicast packets per second entries. If required, set Multicast Traffic and Unicast Traffic type to either “Unknown-only” or “Both” and then click “Save” to complete the configuration for the port or ports.

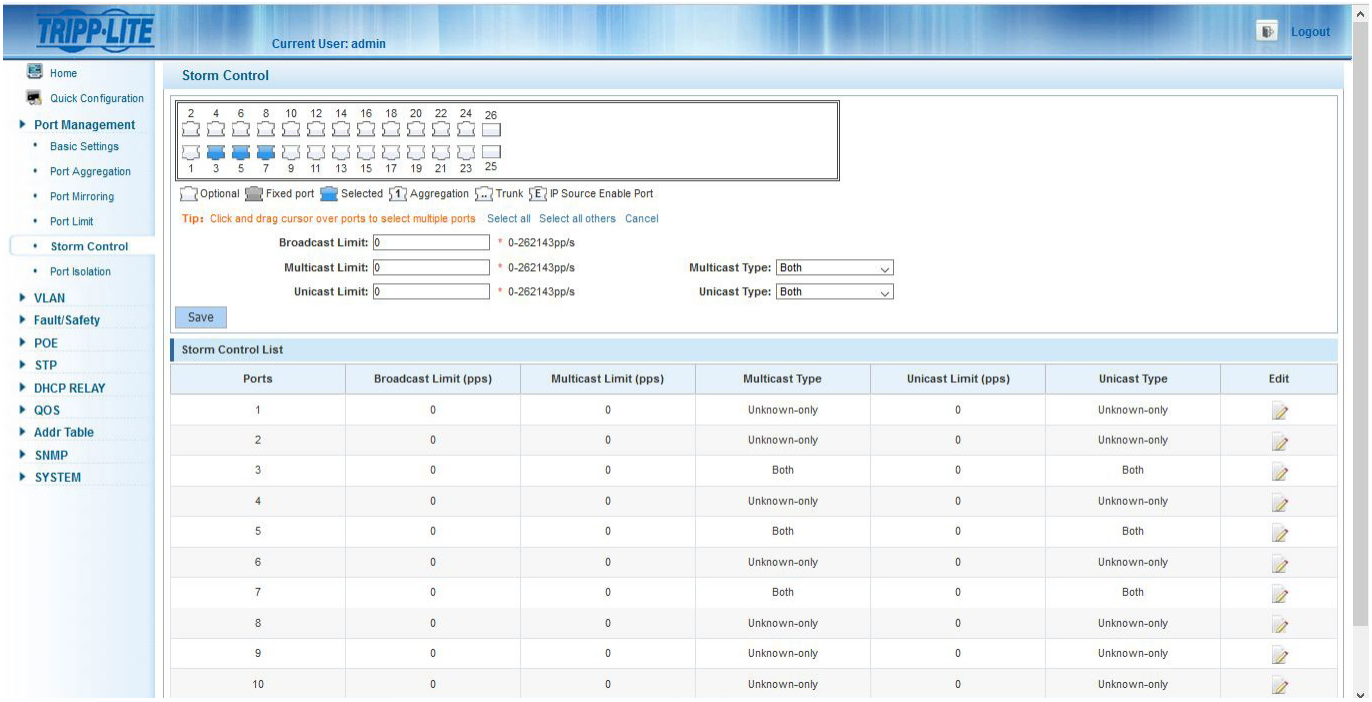


Figure 5.11: Edit Storm Control Settings

5.6 Port Isolation Settings

5.6.1 View Port Isolation Configuration

Select “Port Management Port Isolation” to view the switch’s current port isolation configuration (Figure 5.12). Port isolation prevents PCs connected to different ports from communicating with each other (without having to setup a VLAN).

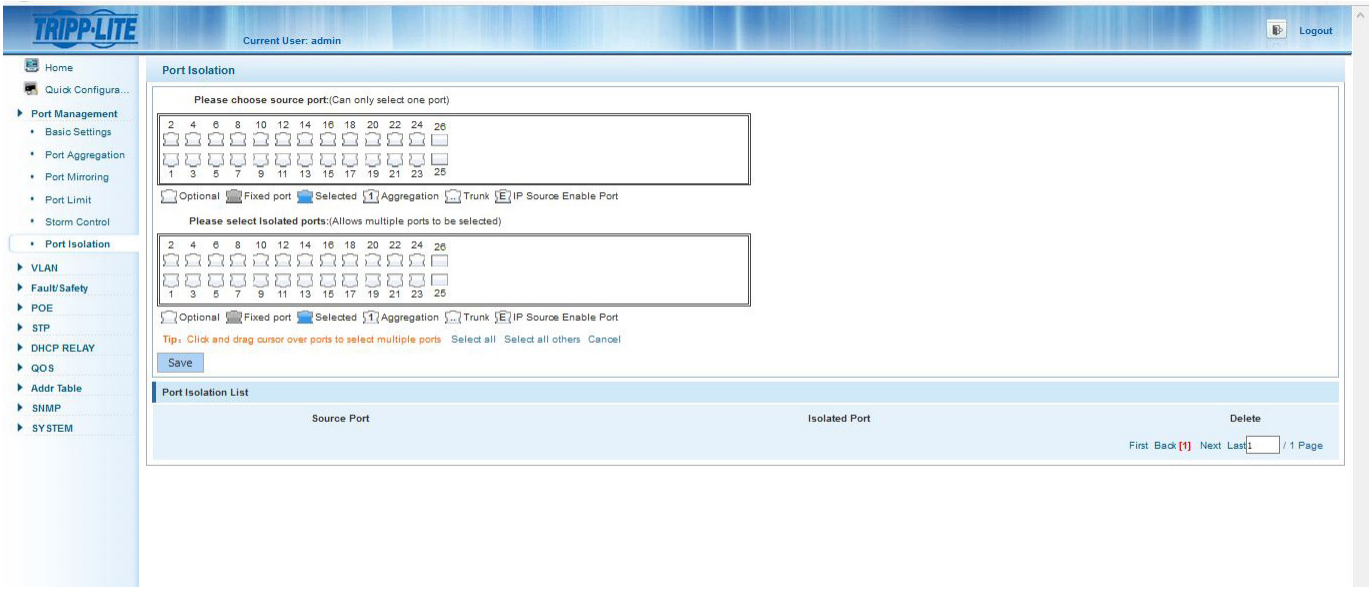


Figure 5.12 : Port Isolation Configuration

5. Port Management

5.6.2 Create a Port Isolation Group

Click the source port icon in the port list table and select the port to be isolated. The port will turn blue on the panel. Next, select the port(s) to be isolated from the selected port. The isolated ports will be blue on the panel. Finally, click “Save”. The isolated port numbers will appear in the table (Figure 5.13).

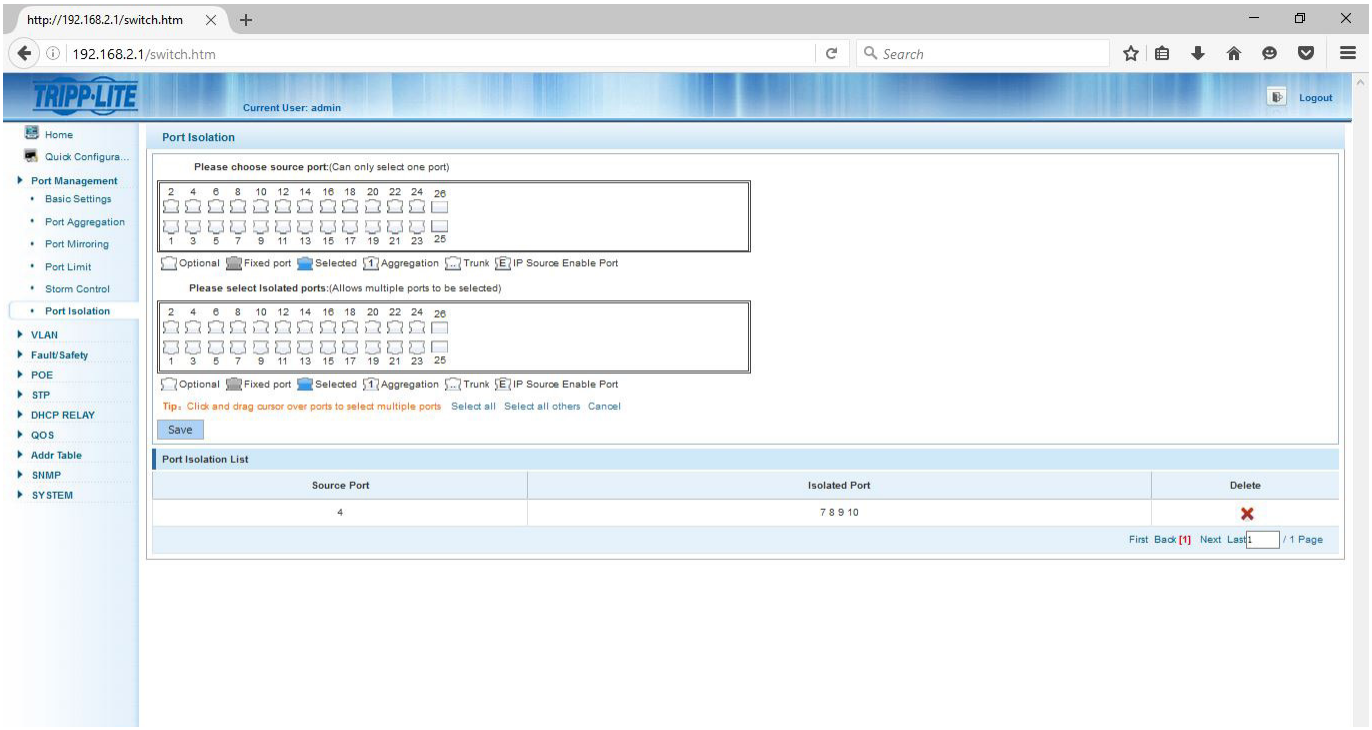


Figure 5.13 : Creating a Port Isolation Group

5.6.3 Delete a Port Isolation Group

Click the ✖ icon to delete a port isolation group from the port isolation list. Confirm deletion, and the group will be removed from the list (Figure 5.14).

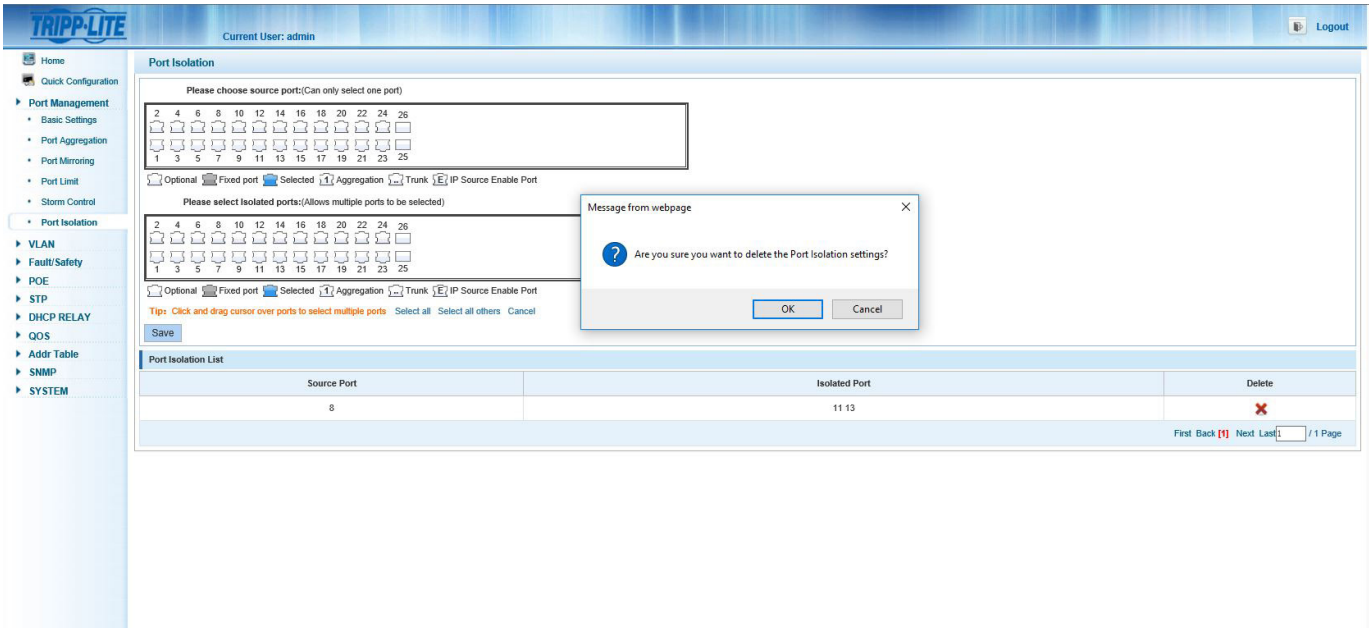


Figure 5.14 : Deleting a Port Isolation Group

6. VLAN Management

6.1 VLAN Management

6.1.1 View VLAN Configuration

Select “VLAN → VLAN Management” to view the switch’s VLAN configuration settings (Figure 6.1). A virtual LAN (VLAN) is a group of workstations, servers and other network resources that behave as if they were connected to a single network segment. VLANs allow for easy network segmentation. Users that communicate frequently with each other can be grouped into common VLANs, regardless of physical location. Each group’s traffic is contained largely within the VLAN, which reduces extraneous traffic and improves efficiency within the network. A VLAN also allows for easy network management. Changes to the number of nodes in a network and the location of the nodes can be handled through the management interface rather than in the wiring closet.

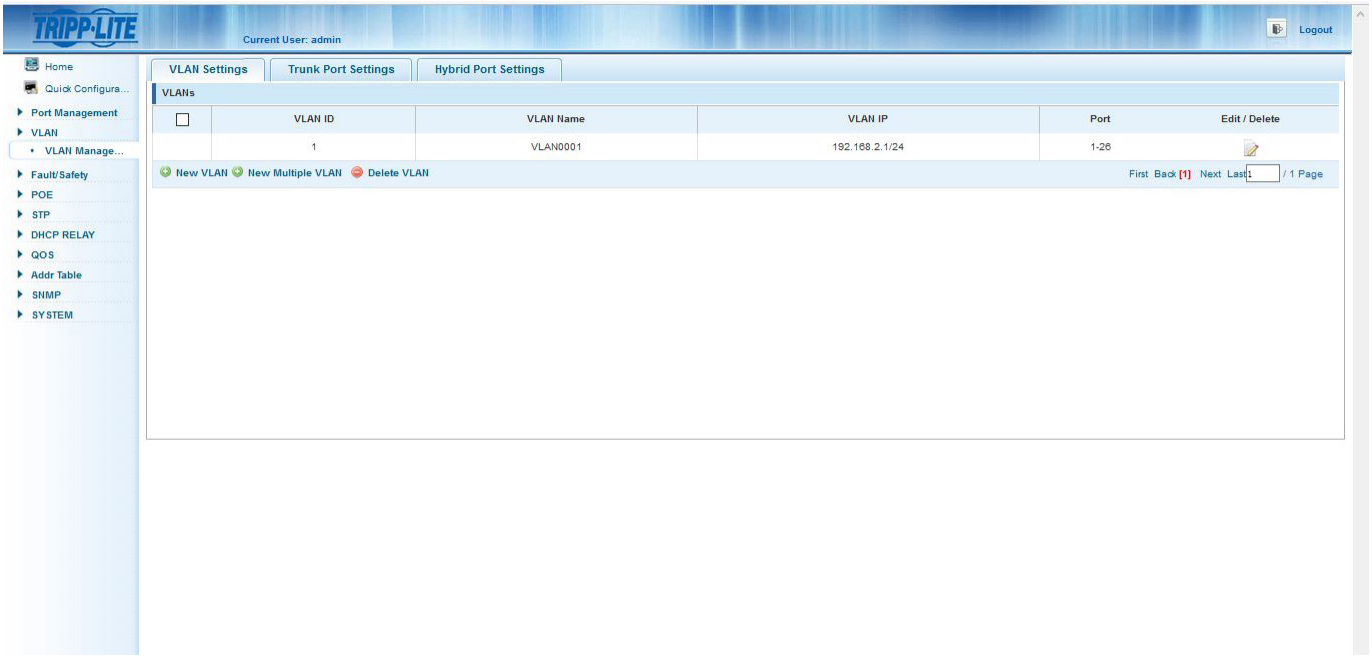


Figure 6.1: VLAN Management Information

The VLAN list shows VLAN configuration of the switch:

- **VLAN ID:** Displays the VLAN identification number.
- **VLAN Name:** Displays the name of VLAN; the default name for VLAN 1 is DEFAULT.
- **VLAN IP:** Displays the management IP address of the switch.
- **Port:** Displays the ports that belong to each VLAN.

Note: *By default, all the ports belong to VLAN 1. The management VLAN cannot be deleted.*

6. VLAN Management

6.1.2 Adding a VLAN

Select “New VLAN” and enter the VLAN ID (between 2-4094) (Figure 6.2). Enter a VLAN name (limit: 31 characters). If no name is entered, the switch defaults to a generic “VLAN0002” name. Next, select the ports to add to the VLAN and click “Save”.

Note: *The system will not allow duplicate VLAN IDs to be created.*

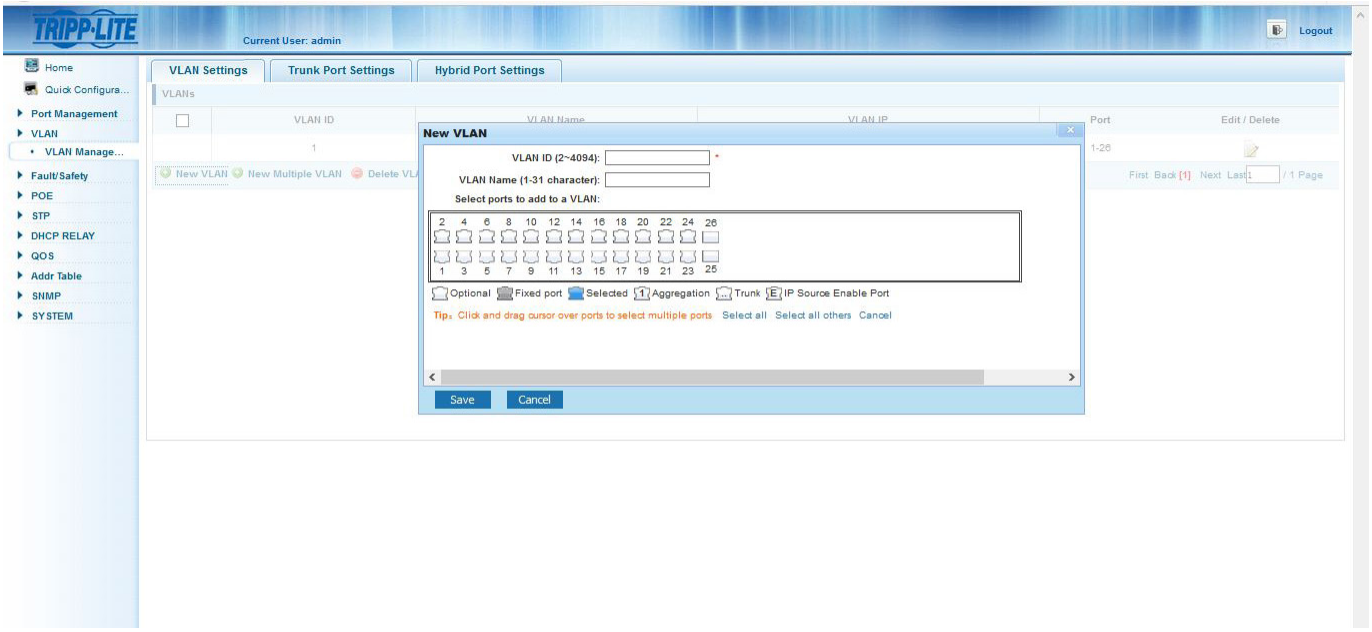


Figure 6.2: Adding a VLAN

6.1.3 Adding Multiple VLANs

To quickly add multiple VLANs to the view list, select “New Multiple VLAN”, enter the multiple VLAN IDs to be created and click “Save” (Figure 6.3). All of the VLAN(s) will be created and allow settings for each VLAN to be edited.

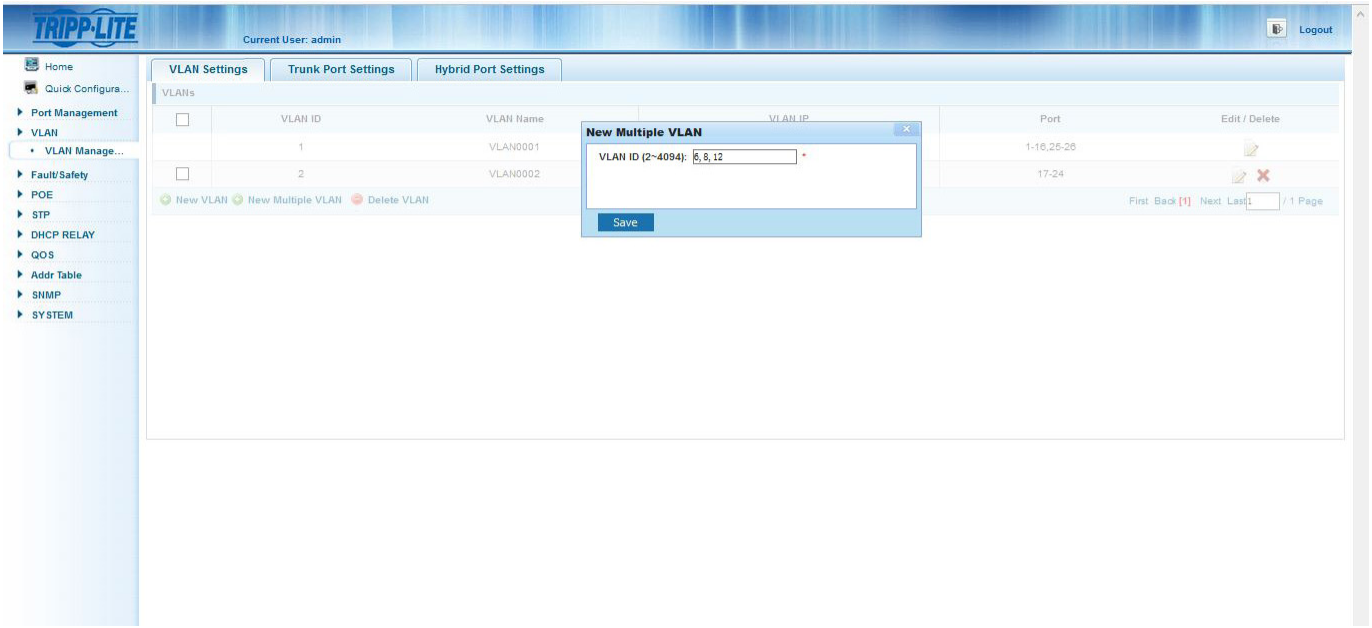


Figure 6.3: Adding Multiple VLANs

6. VLAN Management

6.1.4 Editing a VLAN

Click on the “Edit” icon of the VLAN ID that requires changes. Within the Edit VLAN window (Figure 6.4), you can change the VLAN Name and associated ports. Once the edits are made, click “Save” to save your edits. Click “Cancel” to discard changes.

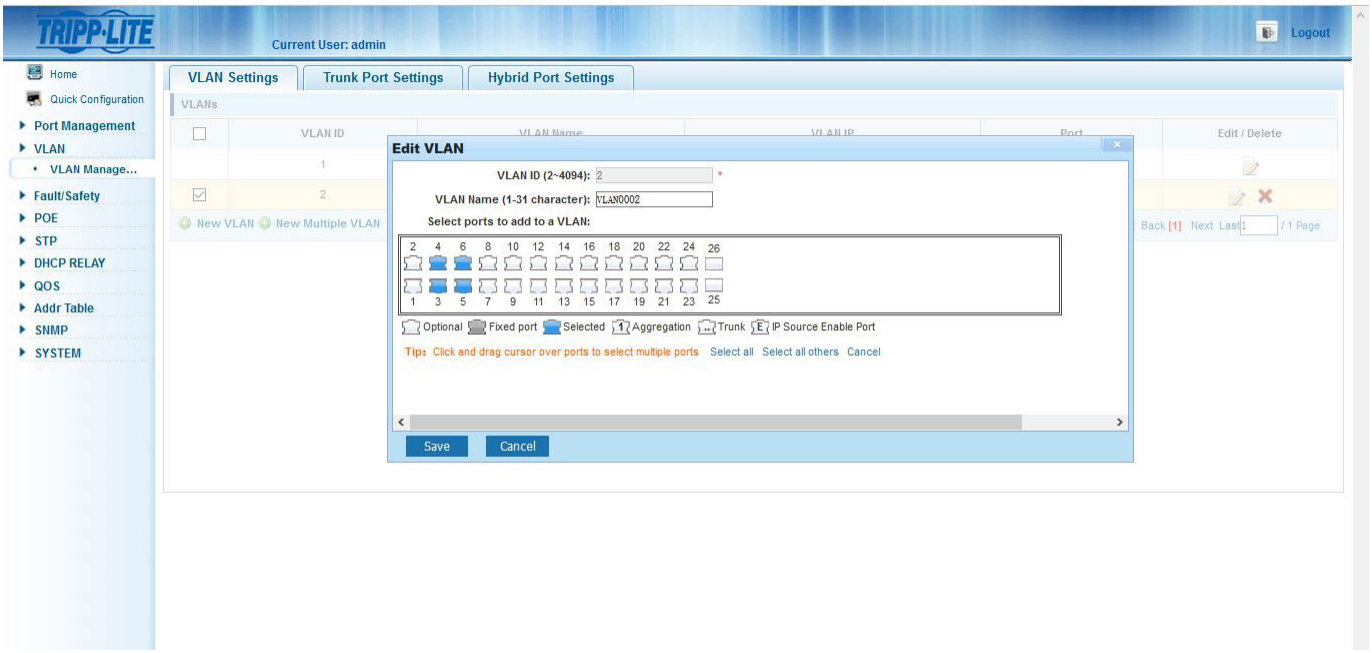


Figure 6.4: Editing a VLAN

6.1.5 Deleting VLAN(s).

Delete a Single VLAN

Select the VLAN to be deleted from the list and click the icon to remove the selected VLAN (Figure 6.5).

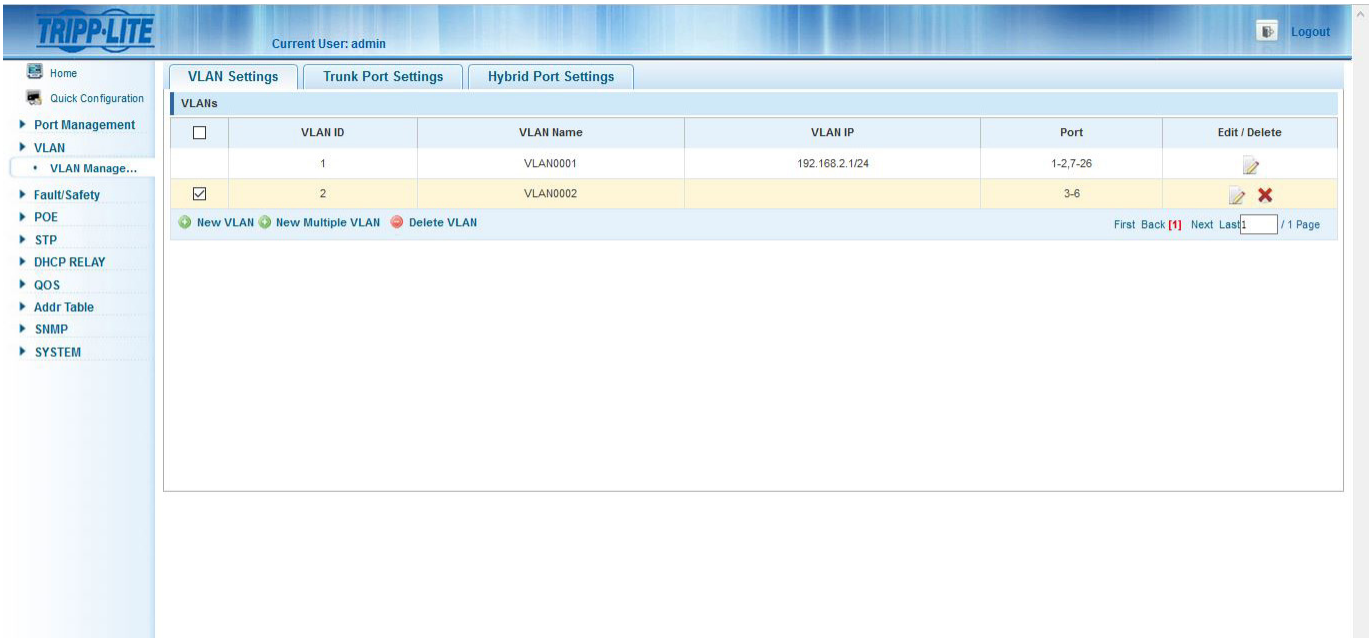


Figure 6.5: Delete a Single VLAN

Delete Multiple VLANs:

Click the checkbox next to the VLAN(s) to be deleted, then click “Delete VLAN” to remove the selected VLAN(s) (Figure 6.6).

Note: *VLAN 1 is the default management VLAN; this setting cannot be changed.*

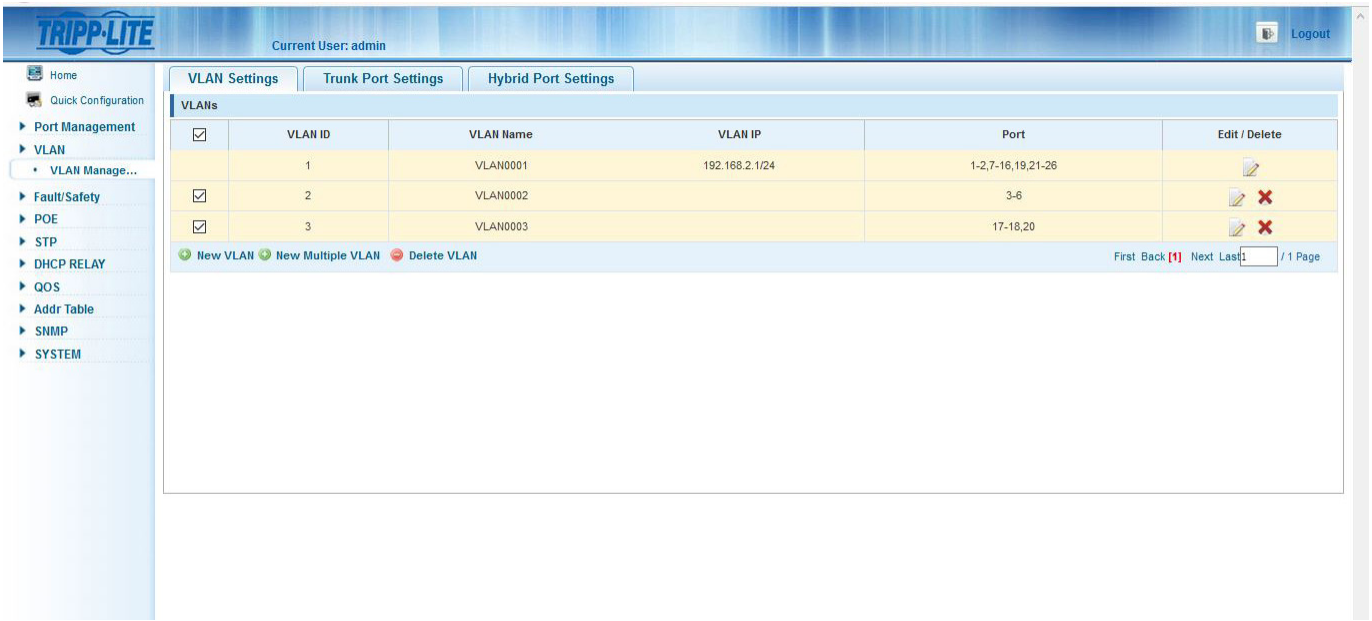


Figure 6.7: Delete Multiple VLANs Simultaneously

6.2 Trunk Port Settings

6.2.1 View Trunk Port Settings

Select “VLAN → VLAN Management → Trunk Port Settings”, to view the switch’s trunk port configuration (Figure 6.7). Trunk ports allow VLAN information to be passed between switches. By default, the native VLAN (access port) for the switch is VLAN 1. Communication between access ports will not have tagging (802.1Q). When a trunk port is configured between two switches, the traffic that passes between them will be marked with a tag to allow the switches to distinguish between packets.

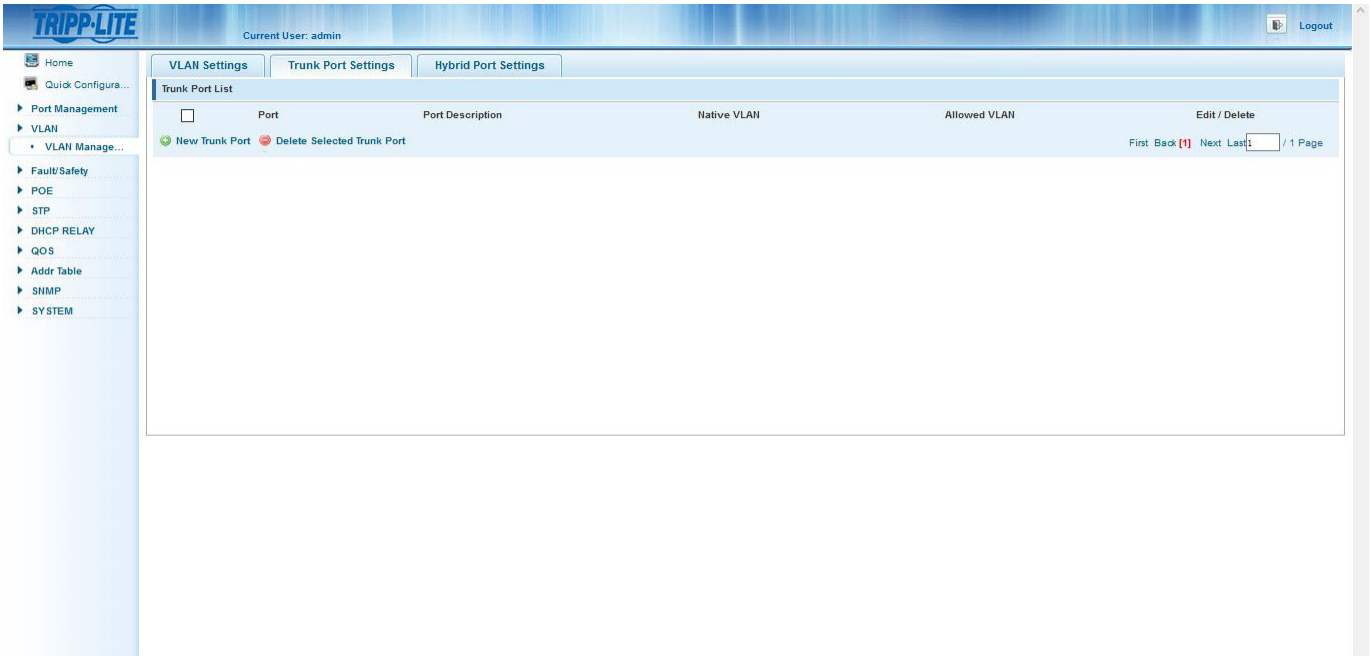


Figure 6.7 View Trunk Port Settings

6. VLAN Management

The Trunk Port List shows the trunk port configuration of the switch.

- **Port:** Displays the port number.
- **Native VLAN:** Displays the native VLAN. By default, the switch's native VLAN is VLAN1.
- **Allowed VLAN:** Displays the VLANs that will be tagged when transmitted on the trunk port.

6.2.2 Add Trunk Port Settings

To add a new trunk port, click "New Trunk Port" (Figure 6.8). Select the Native VLAN (default is 1), then select the allowed VLAN(s) and click "Save".

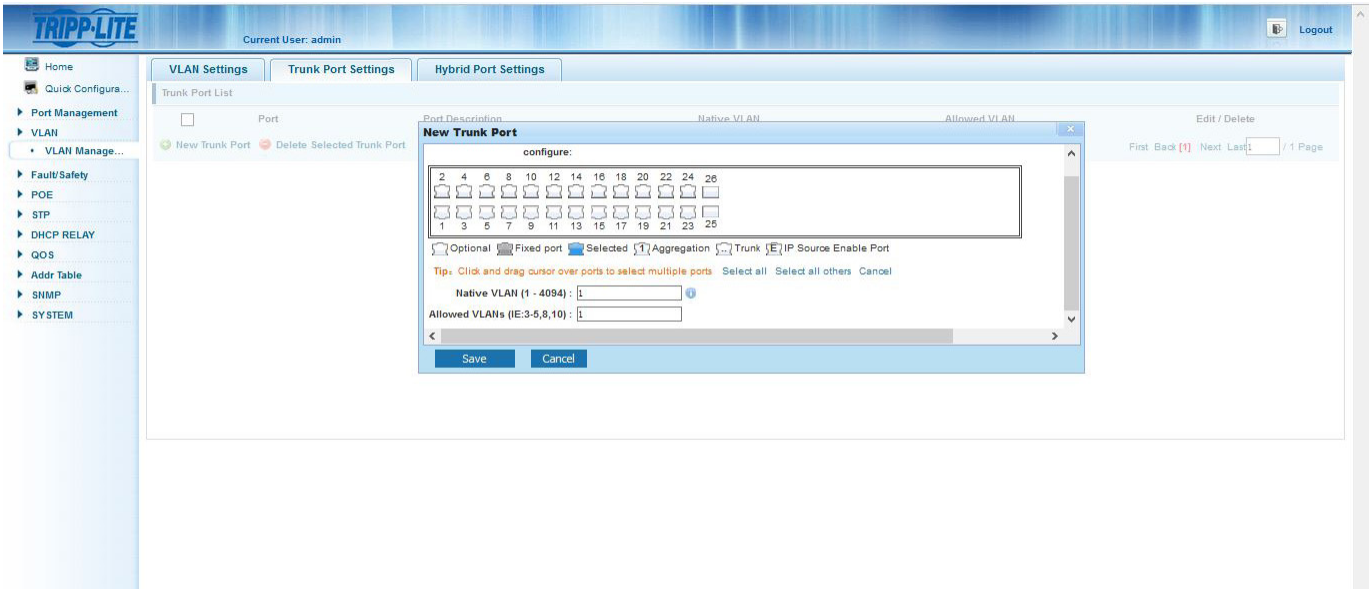


Figure 6.8: Adding Trunk Ports

Note: *The allowed VLAN(s) must be created through VLAN Management before they can be added to a trunk port.*

6.2.3 Edit Trunk Ports

Click the "Edit" icon of the Trunk Port that you want to edit. Within the Edit Trunk Port window (Figure 6.9) you can add additional trunk ports, change the Native VLAN, and change the allowed VLANs for the selected trunk port.

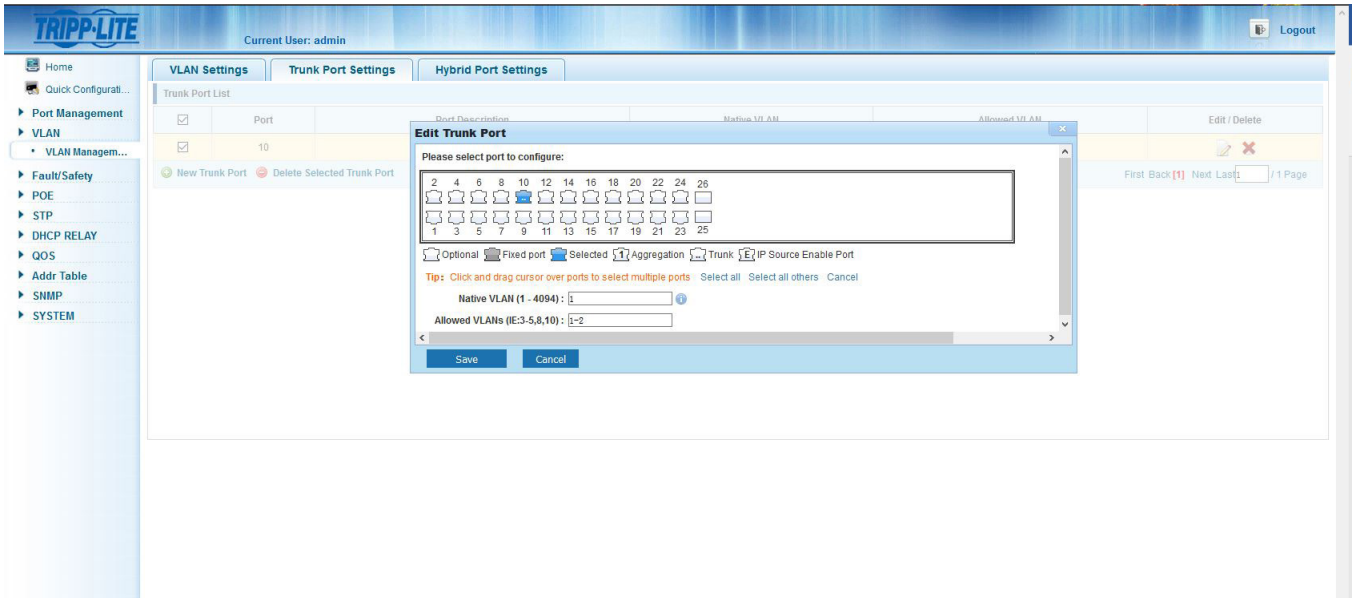


Figure 6.9: Editing a Trunk Port

6.2.4 Delete Trunk Ports

Delete a Single Trunk Port

Select the trunk port to be deleted, then click the icon (Figure 6.10).

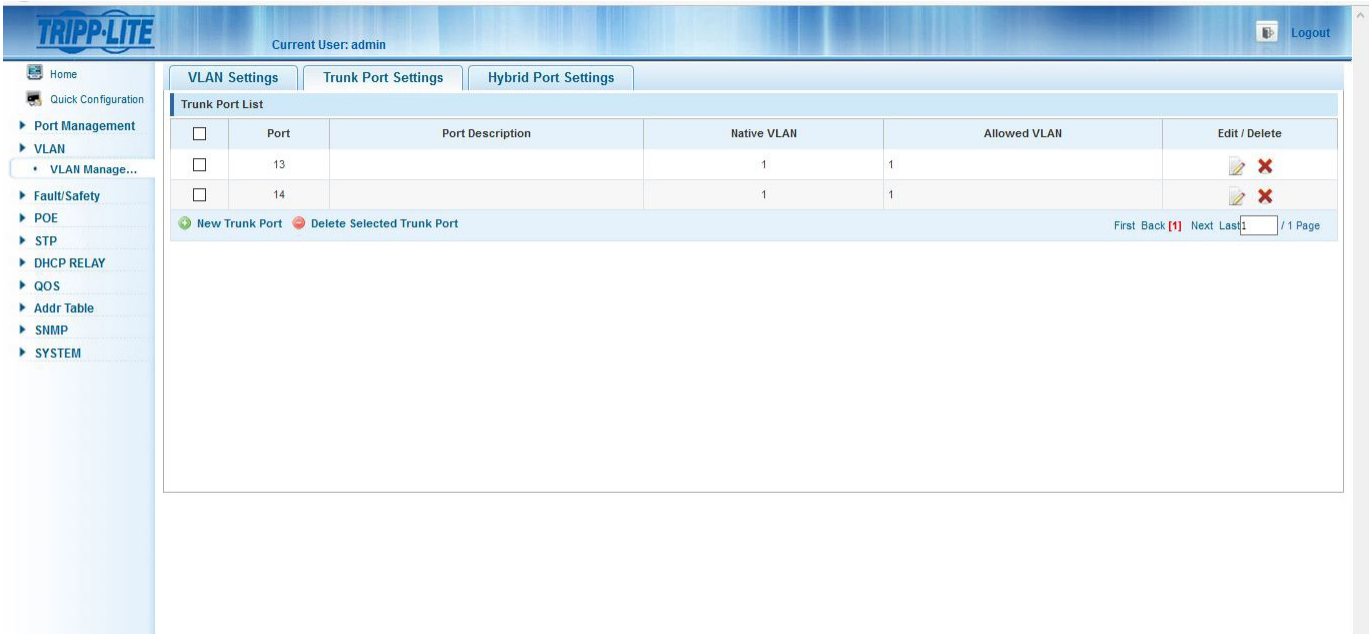


Figure 6.10: Delete a Single Trunk Port

Delete Multiple Trunk Ports

Click the checkbox of the trunk ports to be deleted, then click “Delete Selected Trunk Port” to delete the selected trunk ports (Figure 6.11).

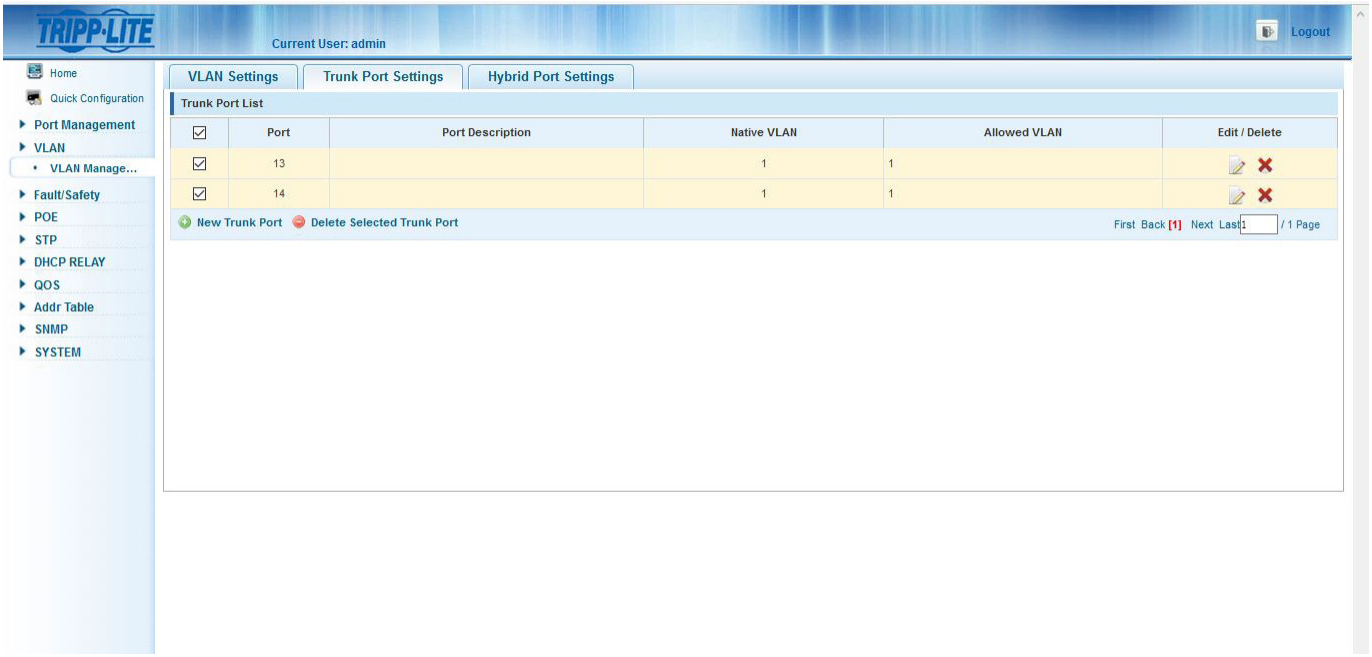


Figure 6.11: Delete Multiple Trunk Ports

6. VLAN Management

6.3 Hybrid Port Settings

Hybrid ports support tagged and untagged VLAN traffic. Usually this feature is used with VoIP phone connections or VLANs.

The Hybrid Port List shows the hybrid port configurations of the switch.

- **Port:** Displays the port number.
- **Port Name:** Displays the port name description.
- **Native VLAN:** Displays the native VLAN. By default, the switch's native VLAN is VLAN1.
- **Added VLAN TAG:** Displays the VLANs that will be tagged when transmitted on the hybrid port.
- **Removed VLAN TAG:** Displays the VLAN that will be untagged when transmitted on the hybrid port.
- **Allowed VLAN:** Displays the VLANs that will be tagged when transmitted on the hybrid port.

6.3.1 Add New Hybrid Ports

Select the port or ports that will be part of the hybrid port configuration (Figure 6.12). Next, enter the native VLAN (between 1-4094). Then enter the VLAN IDs that are tagged (3-5,8,10). Lastly, enter the "Go to VLANs TAG IDs (3-5, 8, 10). Click "Save" to save the hybrid port settings. The view will automatically switch back to the hybrid ports overview lists.

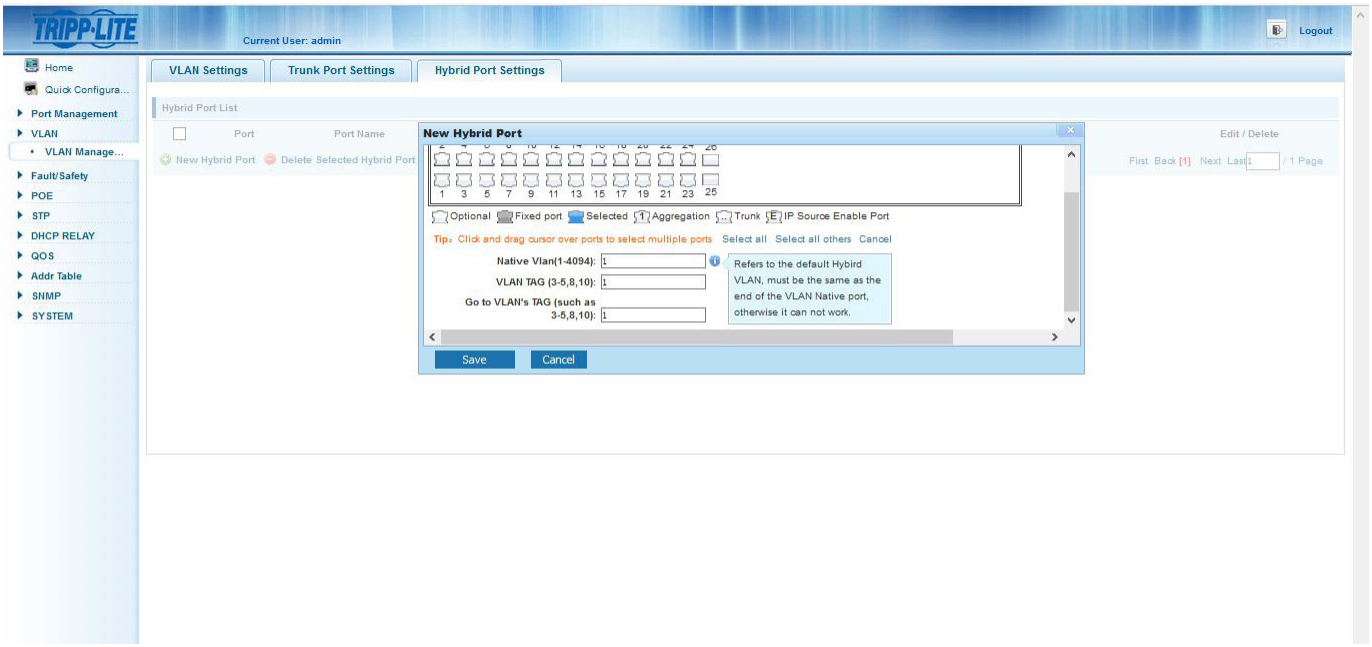


Figure 6.12: Adding New Hybrid Ports

6. VLAN Management

6.3.2 Edit Hybrid Ports

To edit, click the “Edit” icon next to the configured hybrid port to be edited. Modify the selected ports, VLAN and VLAN tag (Figure 6.13). When finished with the hybrid port modifications, click “Save.”

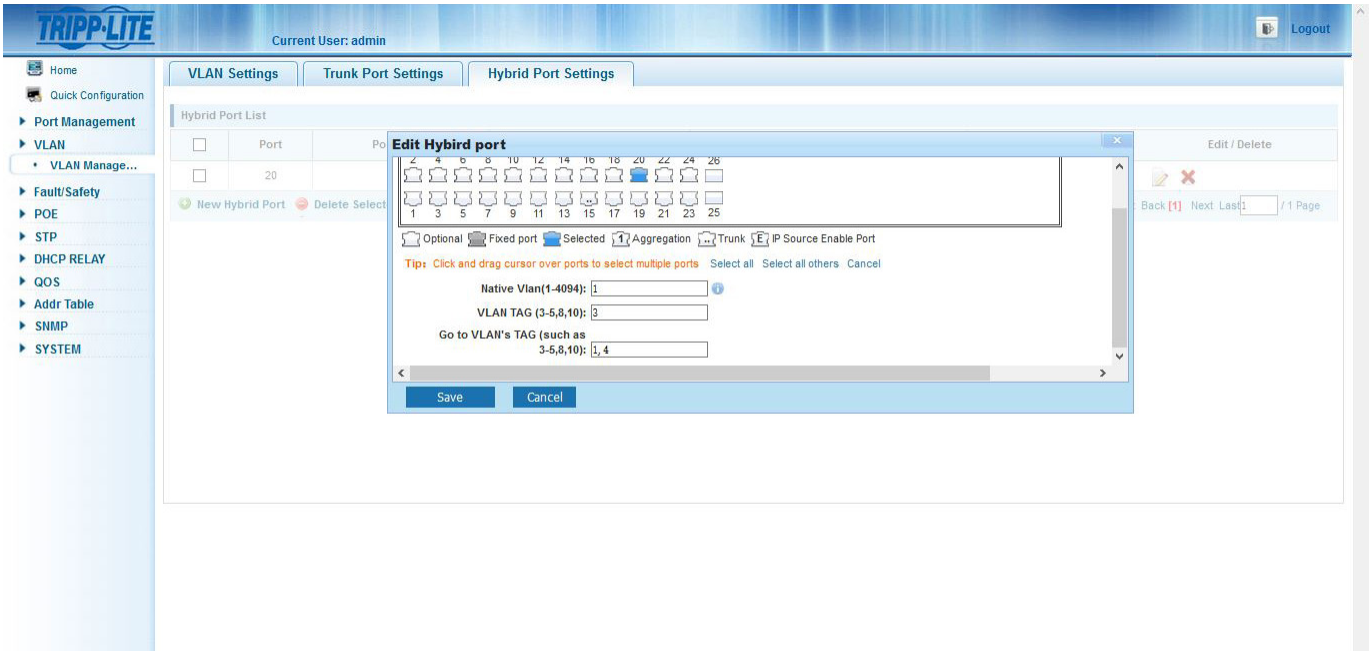


Figure 6.13: Editing a Hybrid Port

6.3.3 Delete Hybrid Ports

To delete a hybrid port, click on the icon to the right of the configured hybrid port to be deleted. To delete multiple hybrid ports, click the checkbox next to each hybrid port to be deleted (Figure 6.14). Select the “Delete Selected Hybrid Port” option to delete the ports.

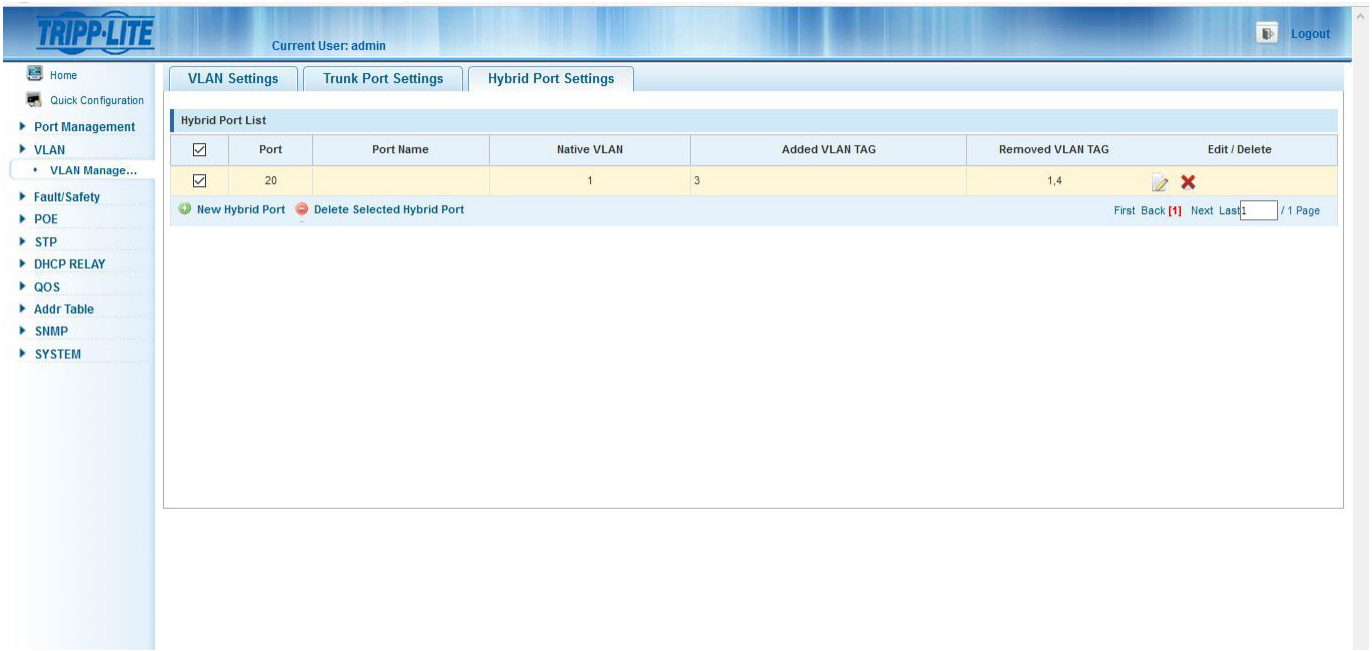


Figure 6.14: Deleting a Hybrid Port

7. Fault/Safety Management

In the navigation bar, select “Fault/Safety.” Here you can set the attack prevention functions of the switch, perform path detection, and configure ACL (access control list).

7.1 Attack Prevention

In the navigation bar, select “Fault/Safety → Attack Prevention → DHCP.” Enabling and configuring the DHCP Protection Suite provides security by filtering untrusted DHCP messages. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network. DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. It also provides a way to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

7.1.1 Enabling the DHCP Protection Suite

To enable the protection suite, click on the orange Disabled button to enable it (Figures 7.1-7.2). Follow the steps below through Section 7.1.1.8 to configure the features of the protection suite.

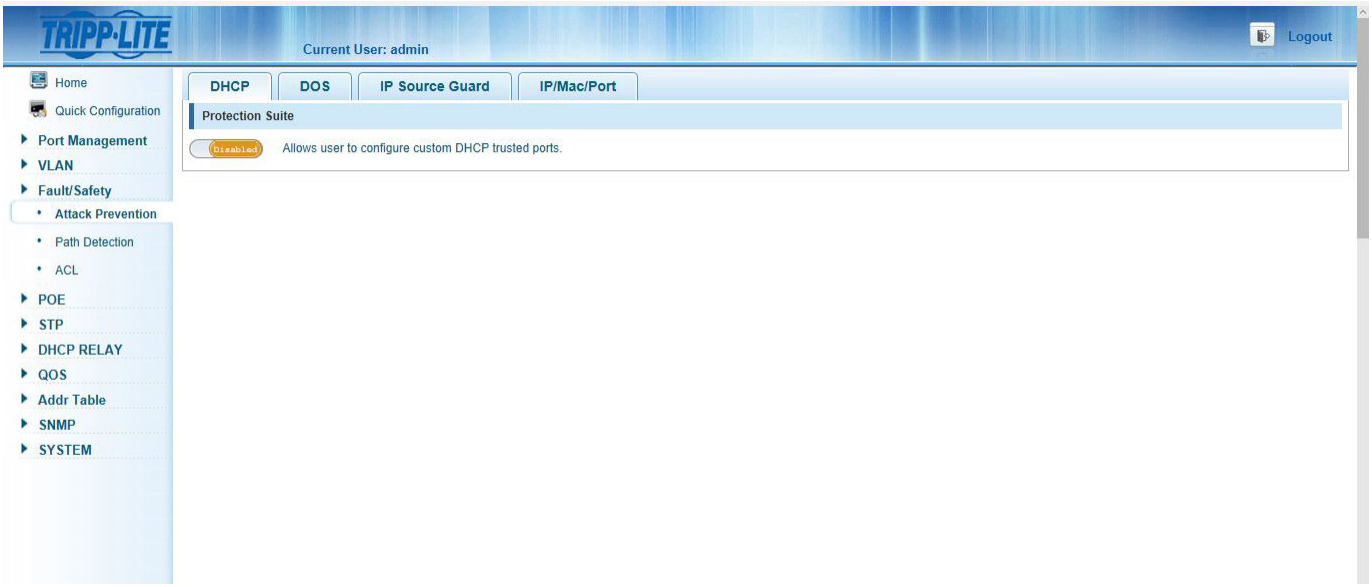


Figure 7.1: DHCP Disabled (Default)

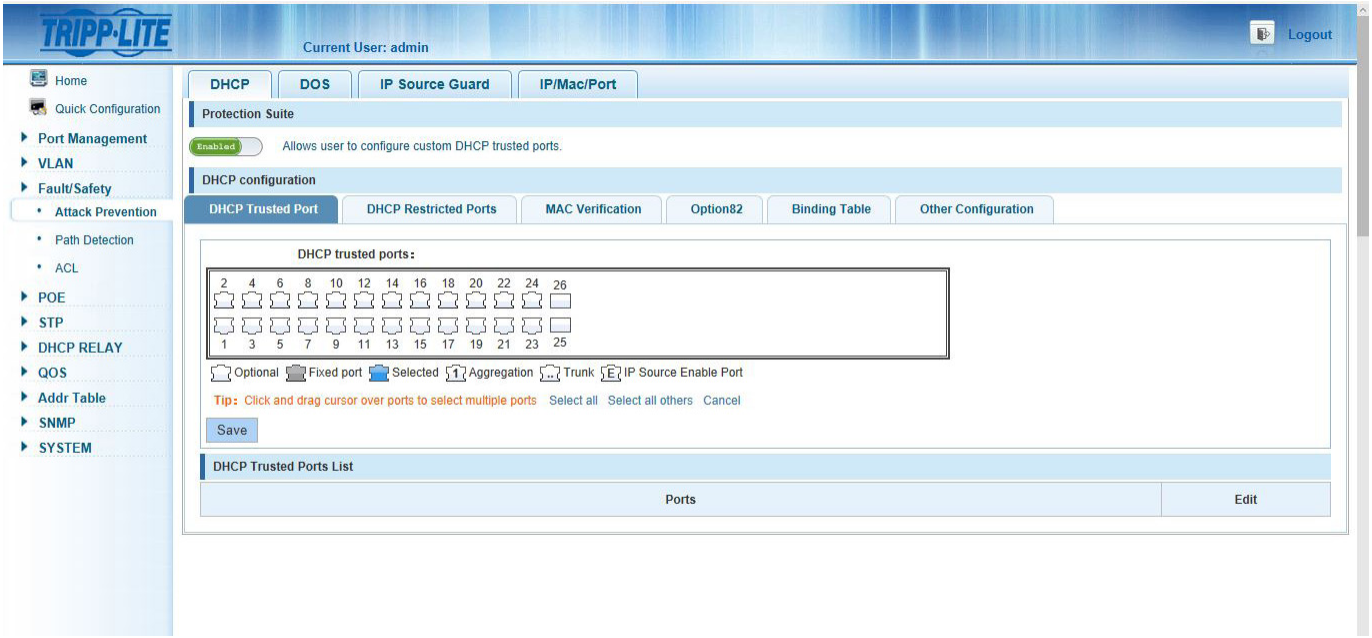


Figure 7.2: DHCP Enabled

7. Fault/Safety Management

7.1.2 Configure DHCP Snooping VLAN

Select the “Other Configuration” tab and enter the DHCP Snooping VLAN (Figure 7.3). Click “Save” when finished.

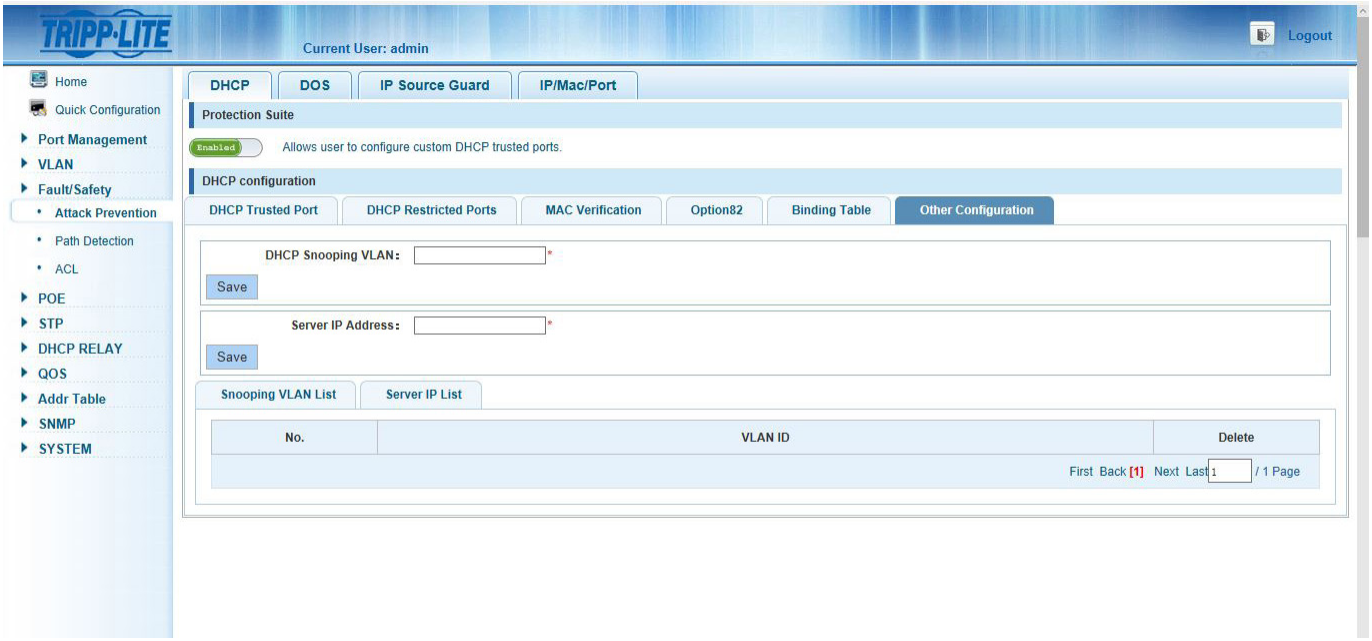


Figure 7.3: DHCP Snooping VLAN

7.1.3 Configure Trusted DHCP Servers

Select the “Other Configuration” tab and enter the IP addresses of trusted DHCP server(s). Click “Save” when finished.

7.1.4 Add DHCP Trusted Ports

Select the port(s) to be configured as part of the DHCP trusted port or port group (Figure 7.4). Once the port(s) have been selected, click “Save.” To edit or remove DHCP Trusted Ports, click on the edit icon next to the trusted port list and de-select the port(s) from the list. When finished editing, click “Save.”

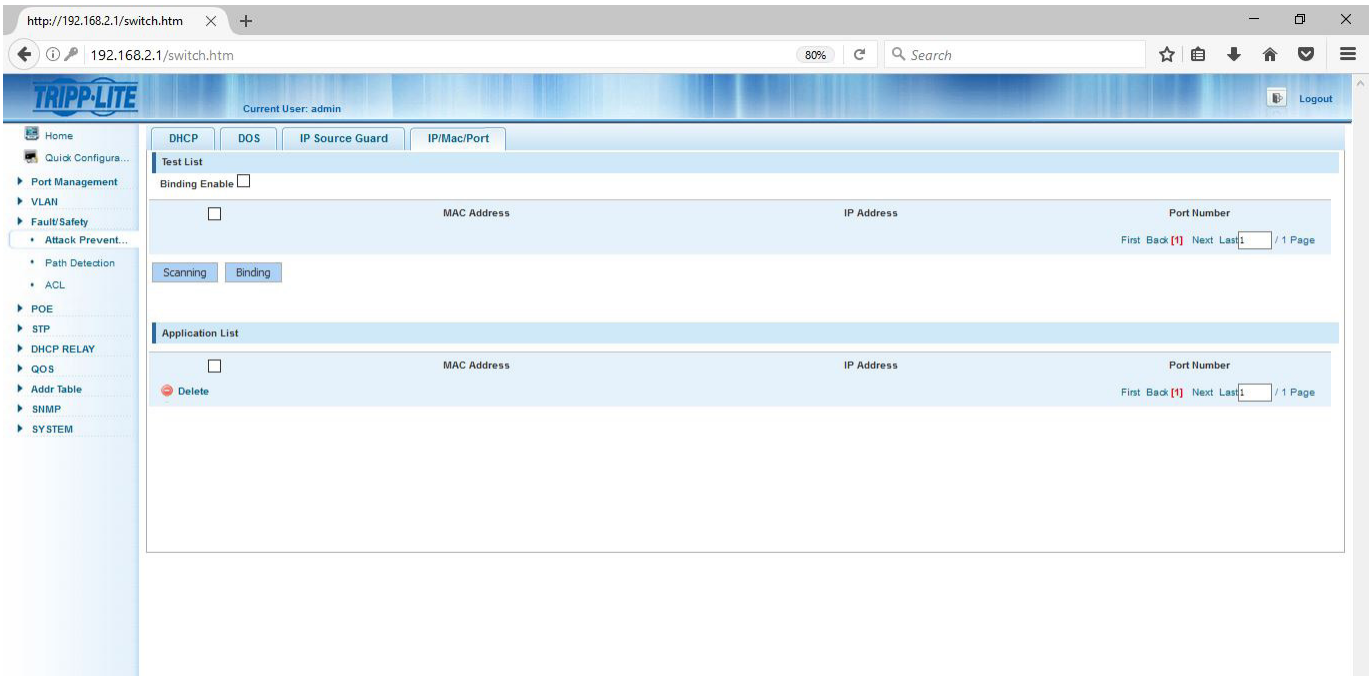


Figure 7.4: Add DHCP Trusted Ports

7. Fault/Safety Management

7.1.5 Add Edit DHCP Restricted Ports

To add DHCP Restricted Ports, go to Fault/Safety → DHCP → DHCP Restricted Ports. Configure the list of ports to be blocked from receiving a DHCP addresses by selecting those ports. Once you have selected the port(s), click "Save." To edit or remove DHCP trusted ports, click on the "Edit" icon next to the "Prohibit DHCP for Address Port List." Next, de-select the port or ports to be removed from the prohibited list. When finished editing, click "Save."

Note: *Removing all ports from the list deactivates the feature.*

7.1.6 Source MAC Verification

Enabling MAC Verification ensures that if a packet is received from an untrusted interface and the source MAC and the DHCP client mac address do not match, the switch will drop the packet.

To enable, click the "MAC Verification Enable" checkbox (Figure 7.5). Next, add the source MAC address and click "Save." Once enabled it will provide the status of various devices enabled or set to have packet traffic intentionally blocked.

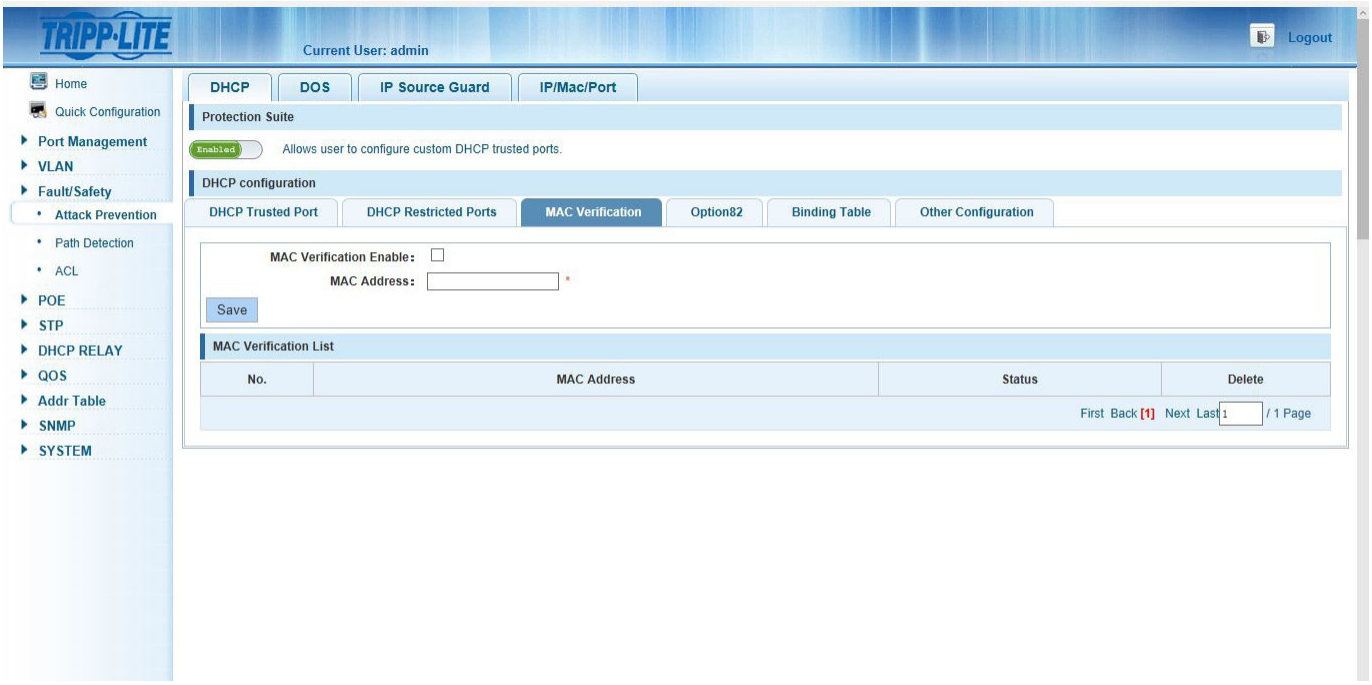


Figure 7.5: MAC Verification

7. Fault/Safety Management

7.1.7 Set Option82 Information

Enabling Option82 allows a device to be uniquely identified on the network when a broadcast request is sent through the switch by adding the Option82 packet information to be read by the DHCP server. To enable, click the “Client Option82 Enable” checkbox (Figure 7.6).

Provide the circuit control circuit name and VLAN ID (Figure 7.7). Once entered, click “Save”. To edit, click the edit option next to the circuit control name. Click “Save” when finished editing. Click “Cancel” to discard edits. To delete a circuit control entry from the list, click the icon next to the circuit name to be deleted. The setting is saved to the system automatically once delete is selected.

Next, enter the remote agent “Remote Name” and VLAN ID (Figure 7.8). Click “Save” once finished. To edit, click the edit option next to the remote agent to be changed. Click “Save” when you are finished editing. Click cancel to discard edits. To delete a remote agent entry from the list, click the red icon next to the remote agent you want to delete. The setting is saved to the system automatically once delete is selected.

Select the IP Address tab and enter the IP address and VLAN ID of the client

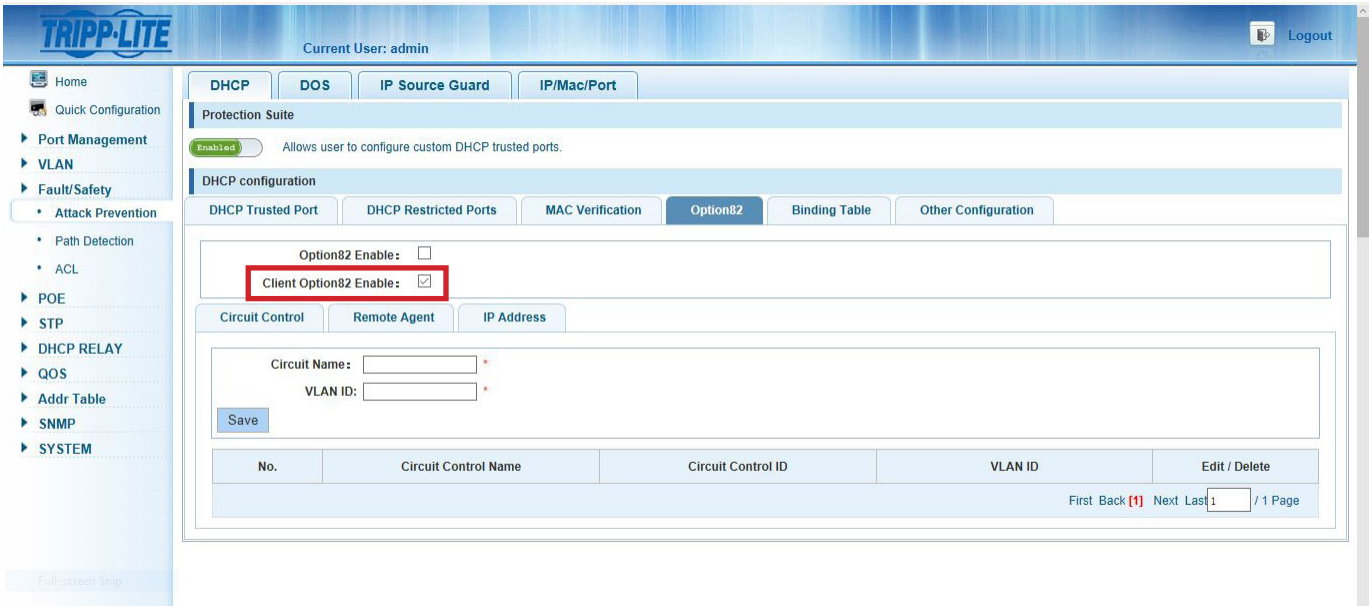


Figure 7.6: Client Option82 Enable

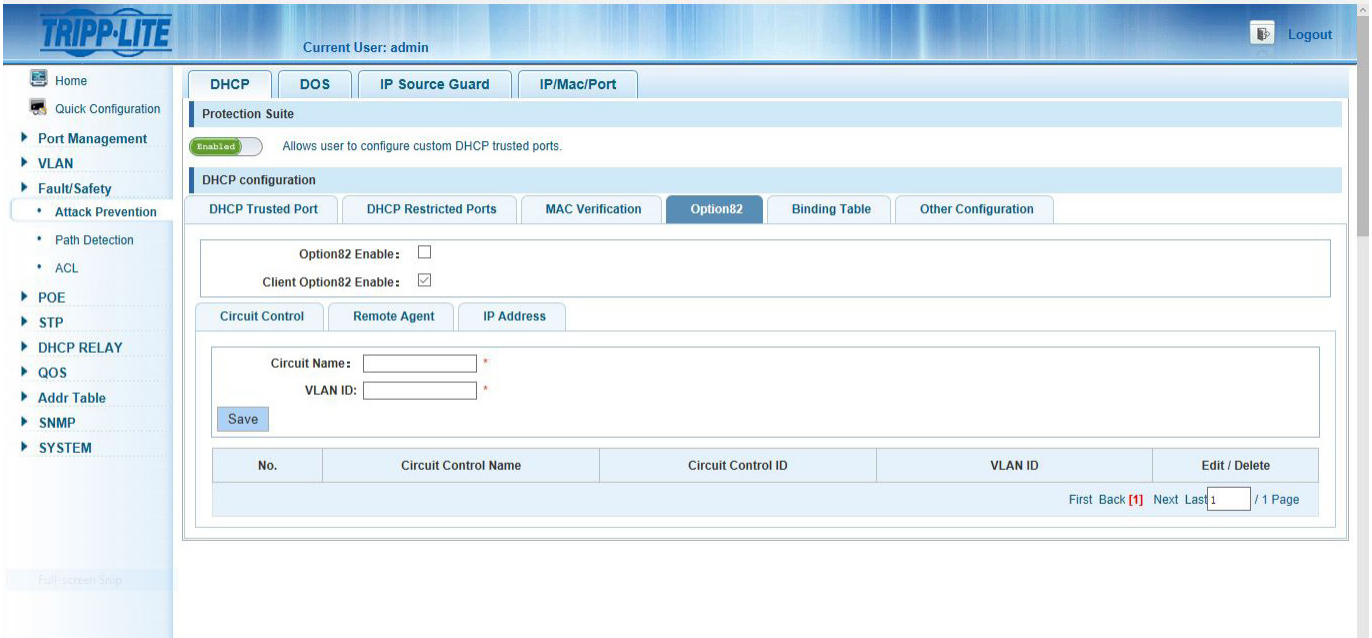


Figure 7.7: Option82 Circuit Control

7. Fault/Safety Management

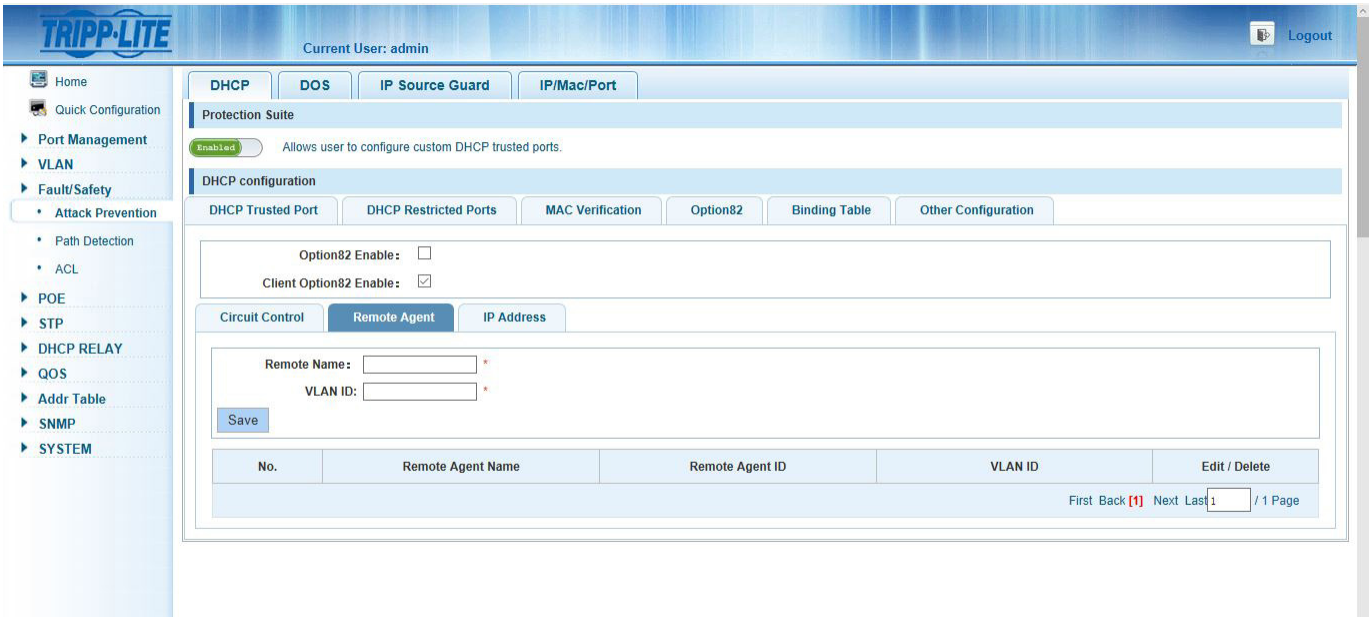


Figure 7.8: Option82 Remote Agent

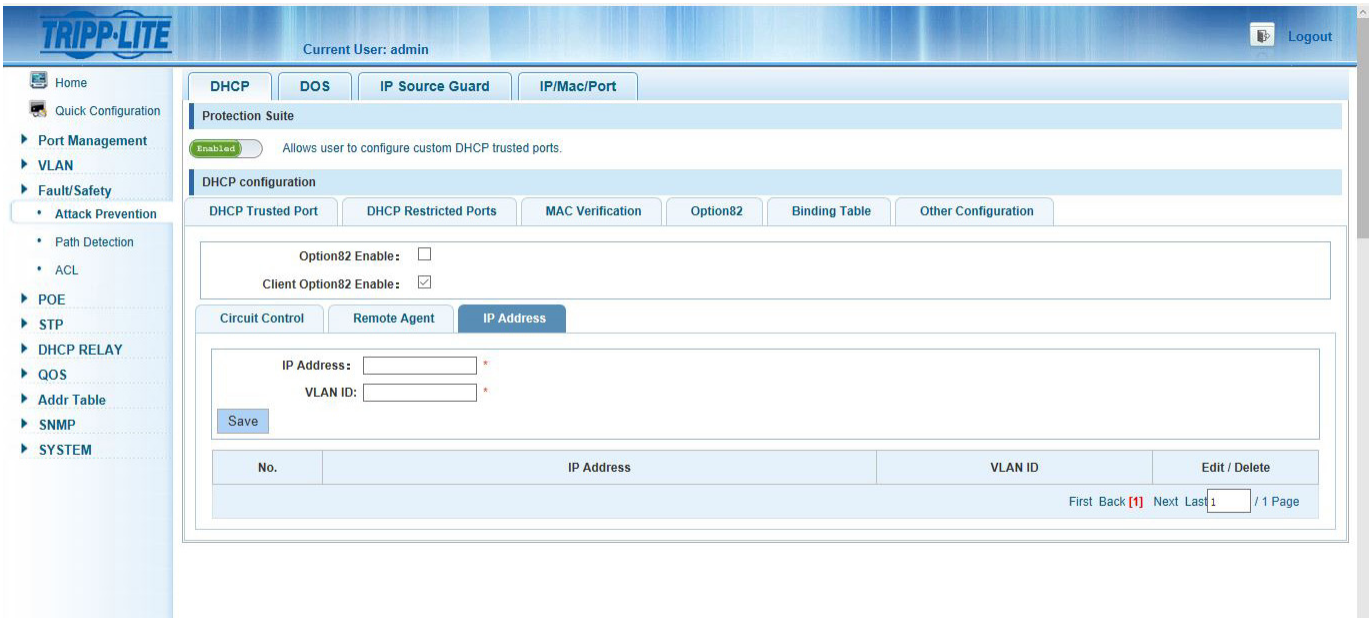


Figure 7.9: Option82 IP Address

Next, provide the circuit control circuit name and VLAN ID. Once entered, click “Save”. To edit, click the edit option next to the circuit control came. Click “Save” when finished editing or “Cancel” to discard edits. To delete a circuit control entry from the list, click the ✖ icon next to the circuit name to be deleted. It will automatically save the setting to the system once delete is selected.

Next, enter the remote agent “Remote Name” and VLAN ID. Click “Save” when finished. To edit, click the edit option next to the remote agent to be changed. Click “Save” when finished editing or “Cancel” to discard edits. To Delete a Remote Agent entry from the list, click the red ✖ icon next to the remote agent to be deleted. The settings will be saved automatically to the system once “Delete” is selected.

Select the IP Address tab and enter the IP address and VLAN ID of the client (Figure 7.9).

7. Fault/Safety Management

7.1.8 Create DHCP Snooping Binding Table

The DHCP Snooping Binding Table contains binding entries that correlate to untrusted ports. To create the binding table, enter the MAC address, VLAN ID, and select the port number from the drop-down menu (Figure 7.10).

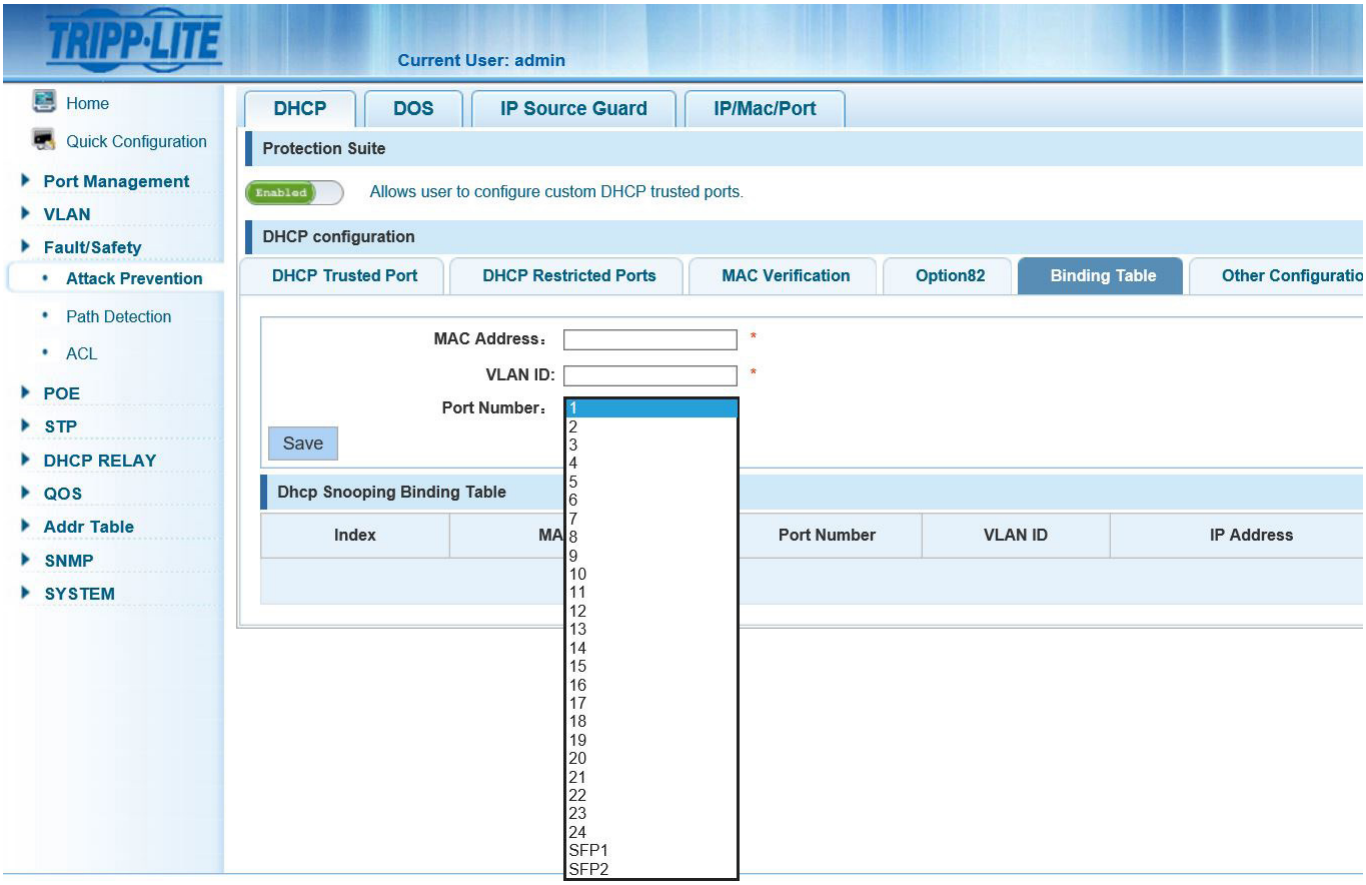


Figure 7.10: DHCP Binding Table

7.1.9 DoS (Denial of Service) Attack Prevention

Go to Fault/Safety → Attack Prevention → DOS to enable the DoS Attack Prevention feature (Figure 7.11). It will stop attempts to make connected computers and network resources unavailable to their intended users.

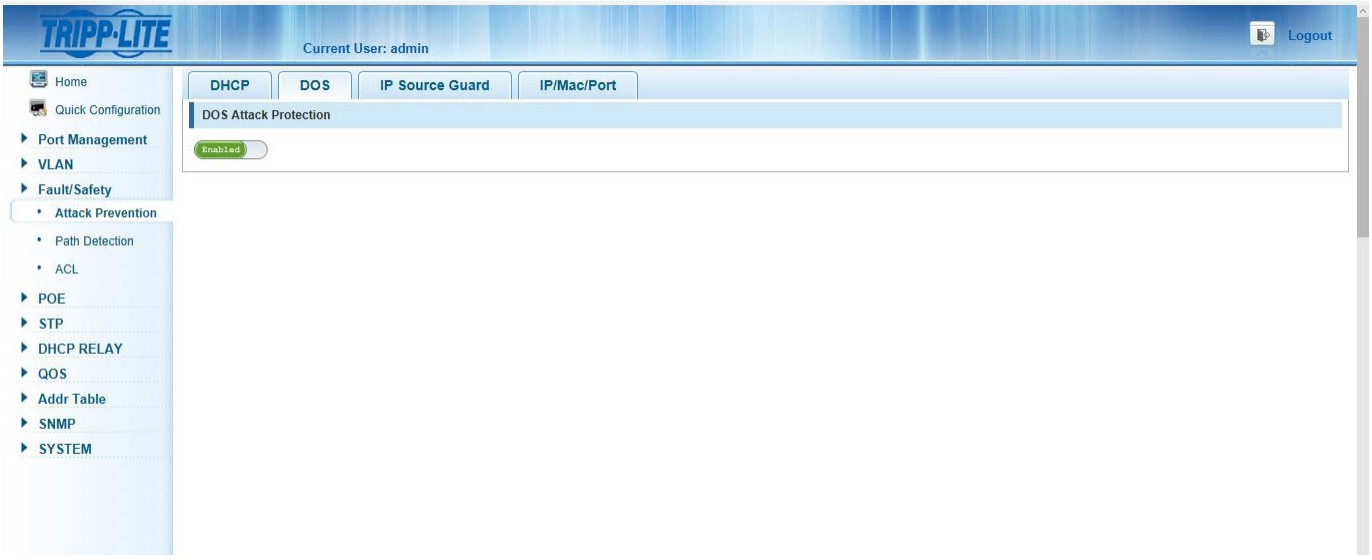


Figure 7.11: Denial of Service Attack Prevention

7. Fault/Safety Management

7.1.10 IP Source Guard Protection

IP Source Guard protection helps to prevent illegal messages through a port by blocking communications with network resources to improve the overall safety of the port. To manually add IP Source Protection, select one or multiple source ports and click “Save” (Figure 7.12).

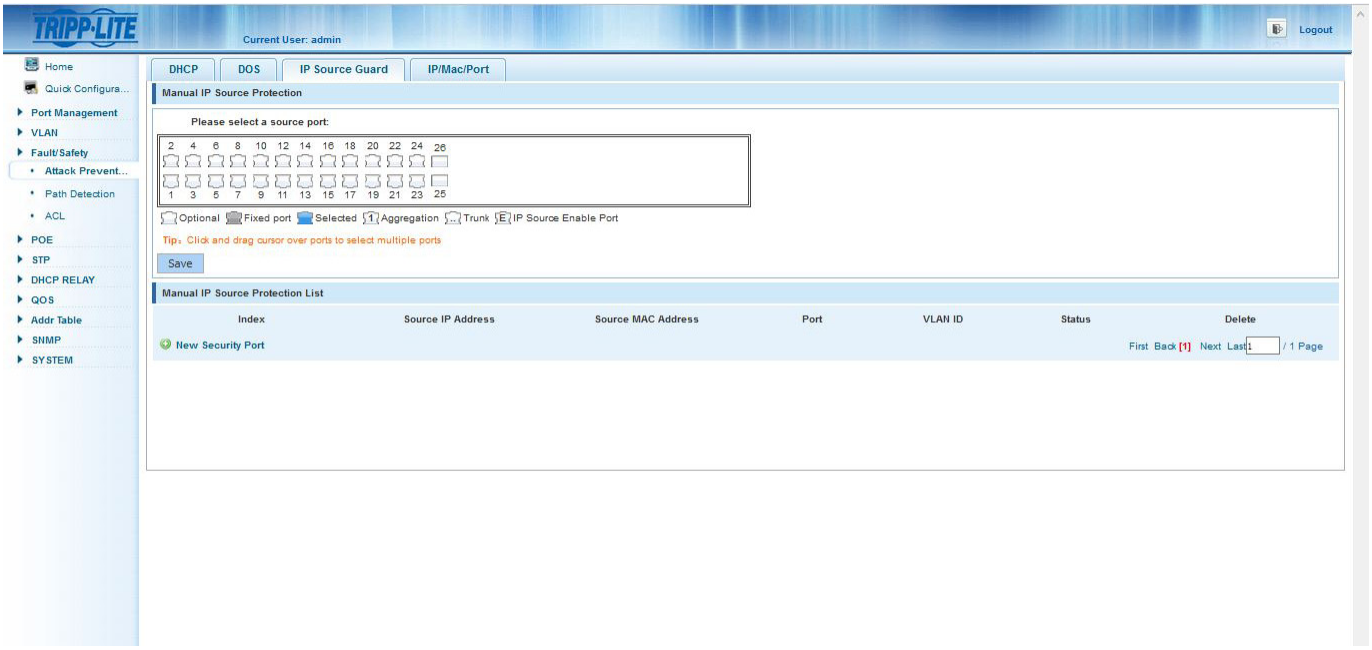


Figure 7.12: IP Source Guard Protection

Next, click the “New Security Port” button below the list. A window will open to select the security port (Figure 7.13). Enter the VLAN ID, the Source IP Address, the Source MAC address, then select the security port. Click “Save” when finished.

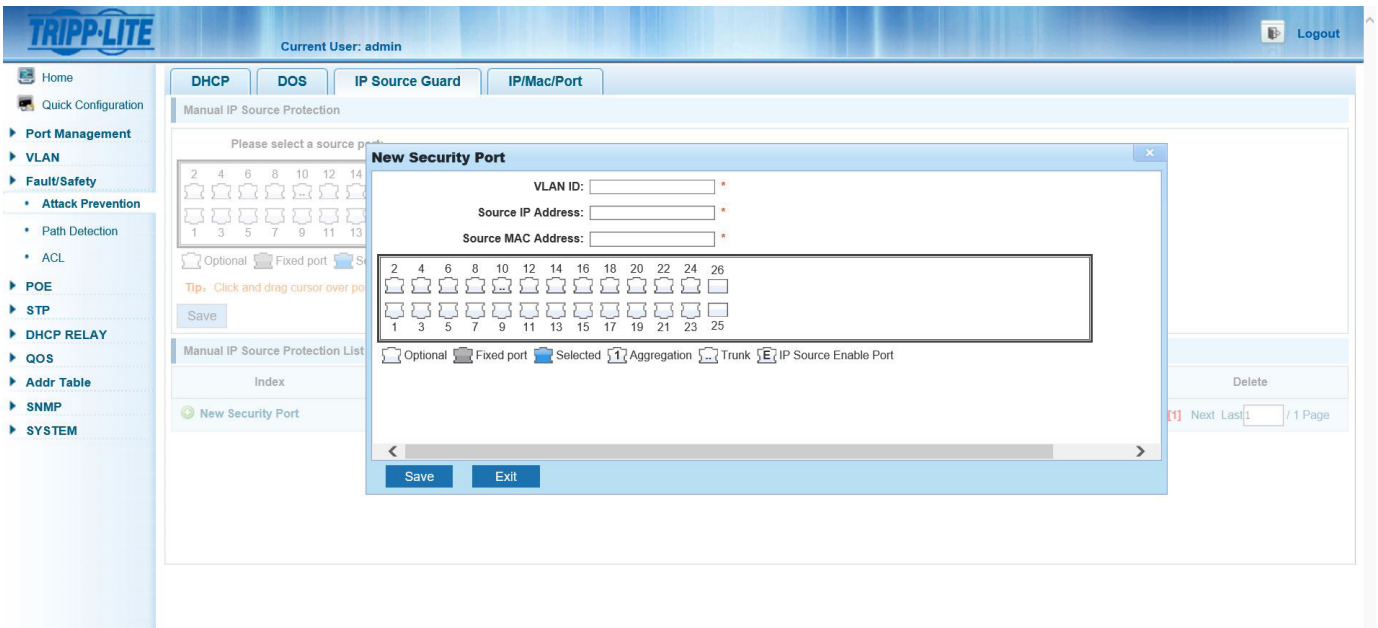


Figure 7.13: Adding Security Ports

7. Fault/Safety Management

7.1.11 IP/MAC/Port Binding List

To automatically let the switch learn the port-based IP addresses and MAC mapping relationships, perform the following steps (Figure 7.14):

1) Click the checkbox for “Binding enable”.
2) Scan the ports to gather the port mapping.
3) Next, select the port to bind and it will be added to the Application List.

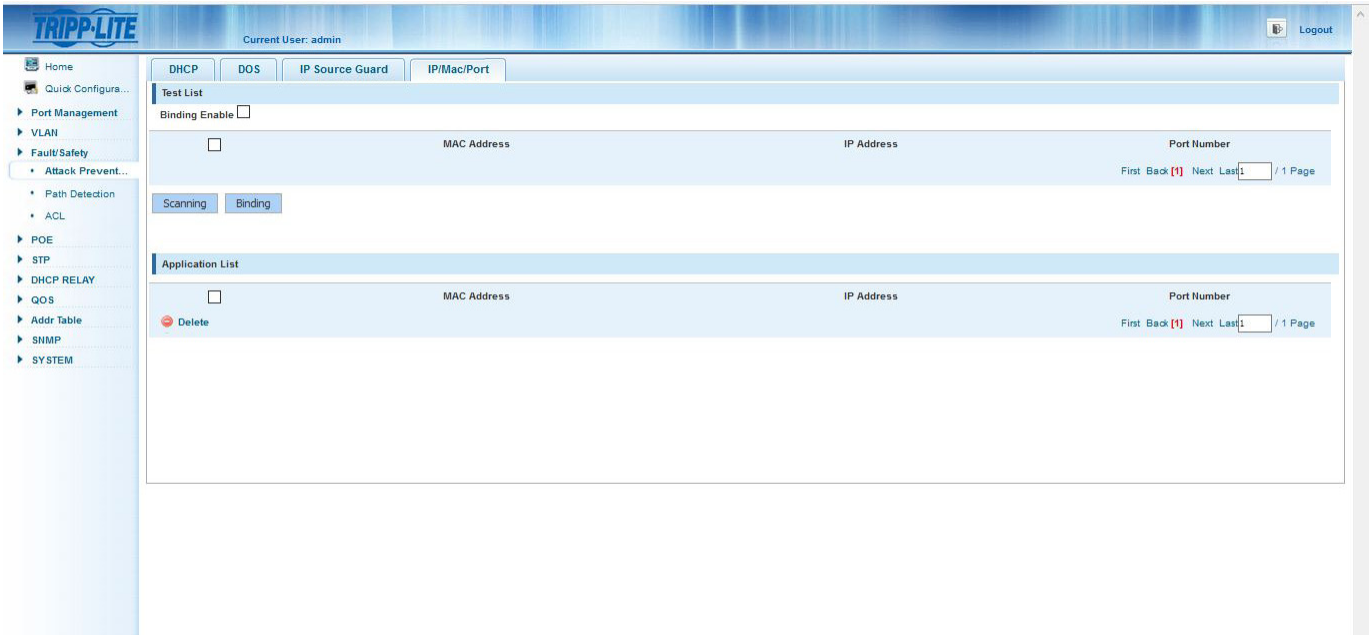


Figure 7.14: IP/MAC/Port Binding List Overview

To delete a binding, click the checkbox next the binding relationship to be removed, then select the “Delete” icon. Settings will be saved automatically.

7. Fault/Safety Management

7.2 Path Detection

The Path Detection → Ping feature helps to verify the status of a connection, while the Tracert shows how many routes and how long it takes to reach a destination.

7.2.1 Ping Test

Select “Fault/Safety → Path Detection” to determine if a host is responding (Figure 7.15). Enter the IP address to ping in the “Destination IP” field, the timeout period from 1-10 seconds (default is 2), and the repeat ping number from 1-1000 (default is 5). Select “Start Test” to begin the test and display the results.

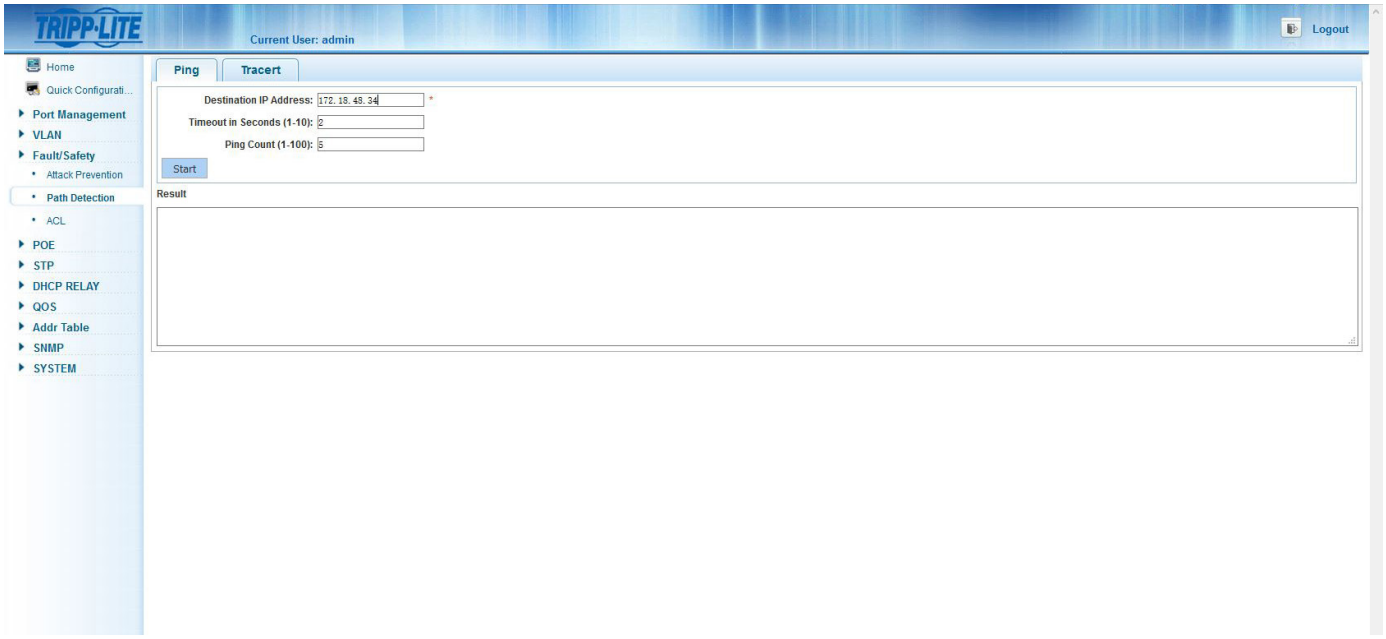


Figure 7.15: Ping Test

7.2.2 Tracert

Use the Tracert function to trace the route of every router a data packet goes through before it reaches its destination. Select “Fault/Safety → Tracert” and enter the IP address in the “Destination IP address” field (Figure 7.16). Next, enter the timeout period between 1-10 (default is 2 milliseconds).

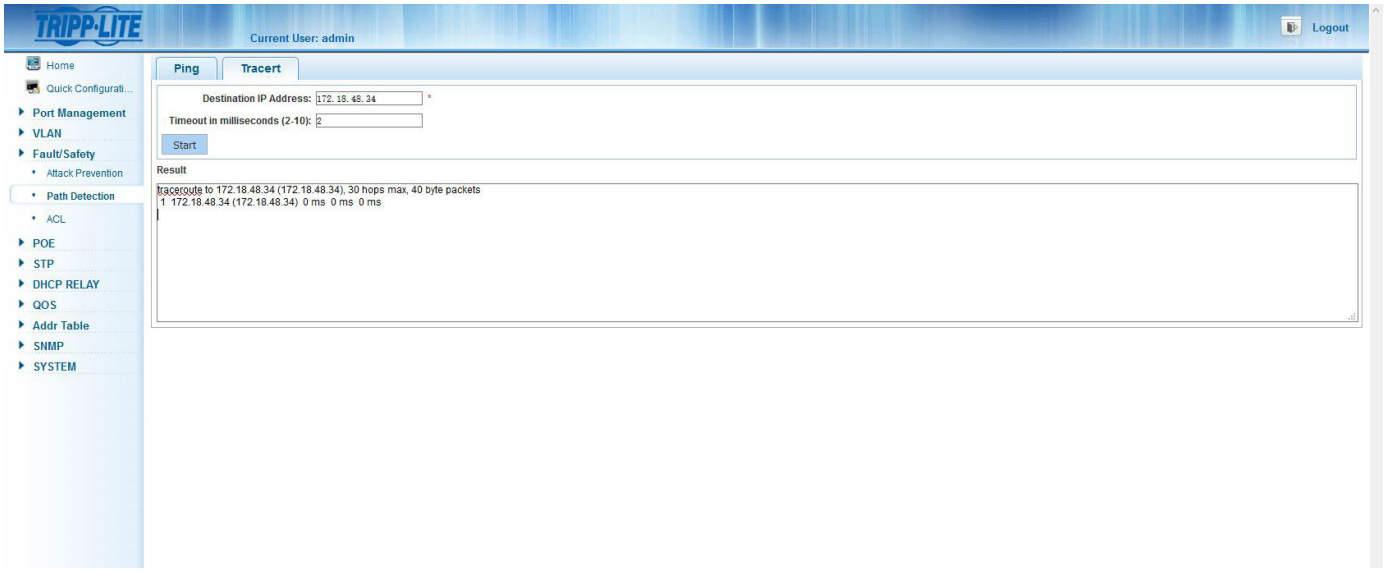


Figure 7.16: Tracert Function

7. Fault/Safety Management

7.3 Access Control Lists (ACLs)

Access Control Lists give devices on the network the ability to grant access to or ignore requests from certain users and systems to available network resources.

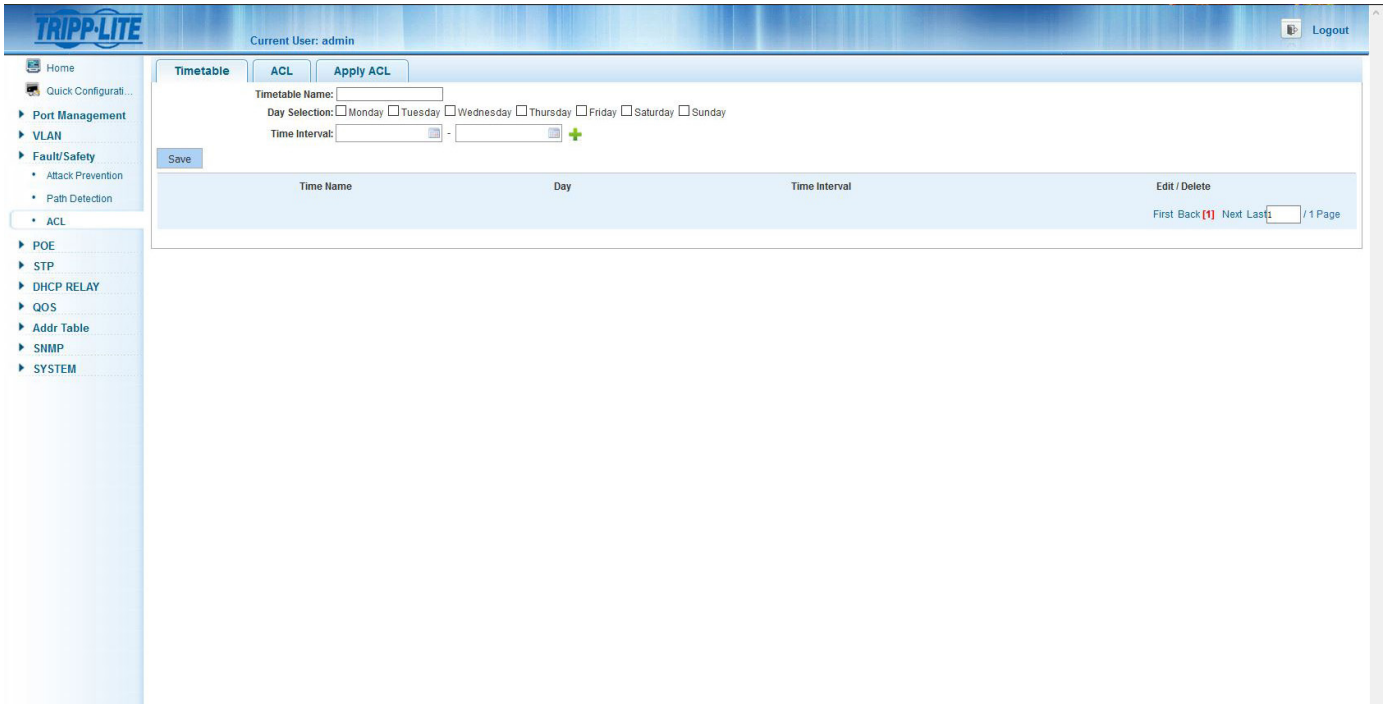


Figure 7.17: ACL Overview

To configure the ACL, go to "Fault/Safety → ACL" and perform the following actions:

1. Name the timetable. Enter a check mark for the days you want the timetable to be applied. Next, enter the interval times for the timetable. (Figure 7.18). Multiple timetables per group can be created. You can edit ACL timetables by clicking the edit icon and adjusting the days and times. To save edits, click the "Save" button. Click "Cancel" to discard changes. If a timetable is no longer needed, click the delete icon to remove it from the list.
2. Next, create a rule to permit or deny access by configuring the ACL against the timetables. Select the ACL tab and click the "Create ACL" button. In the new ACL access rule window (Figure 7.19), set the ACL Number from 100-199, the permission action of Permit or Deny, the Protocol Type (IP, UDP, or TCP), and the ACL Name to which the rule will apply from the drop-down list. If the rule will apply to any source or destination IP addresses, leave the default boxes checked for these two options. To specify a single source or destination IP address, uncheck the applicable box to get the option to enter the single IP address or the IP address and subnet mask. If configuring the rule for TCP or UDP for a single source or destination port, uncheck any source port check box. Next, enter the single source or destination port addresses from 0-65535. Once configured, click the "Save" button. To delete the rule to set to permit or deny ACL configuration, click the red ✖ icon.
3. Select the Apply ACL tab, to configure ACLs to a single or to multiple Ethernet ports. Enter the ACL Number of the applicable rule, then click "Save".

Note: *Configured and active ACLs may be deleted by following the steps above in the reverse order.*

7. Fault/Safety Management

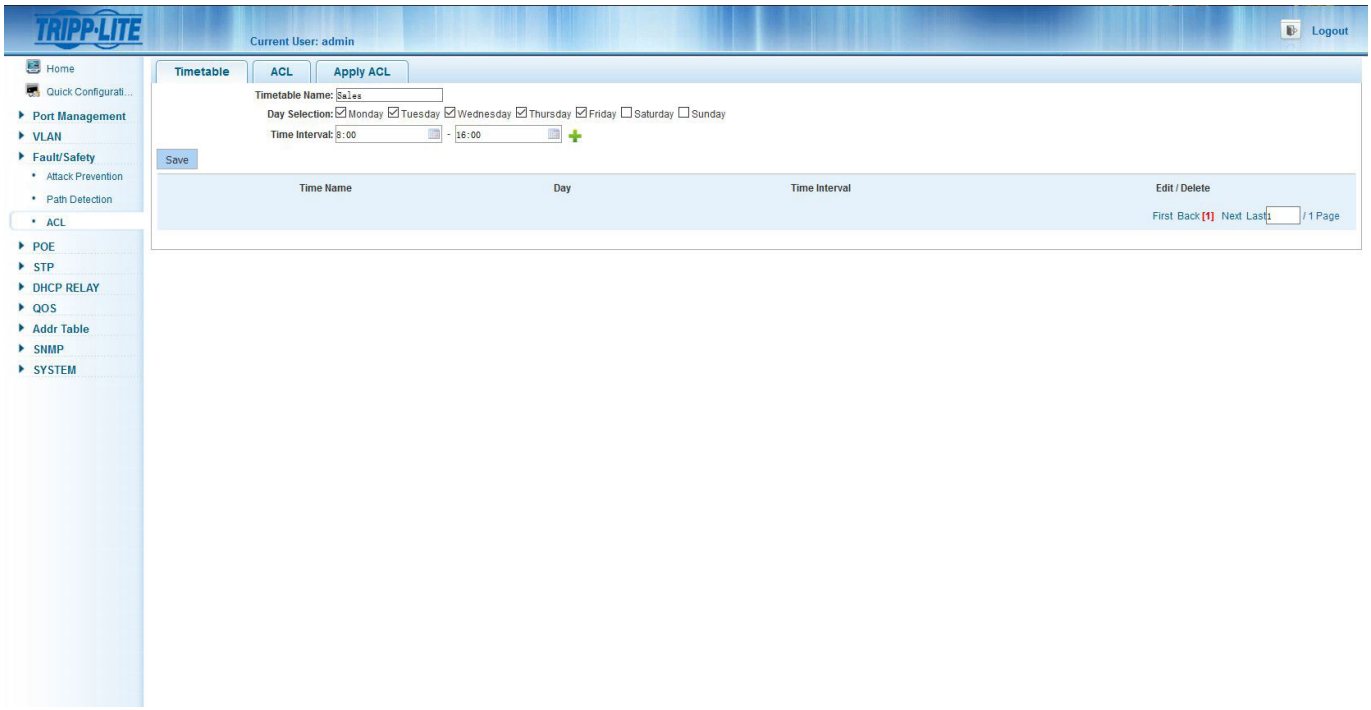


Figure 7.18: Create Timetable

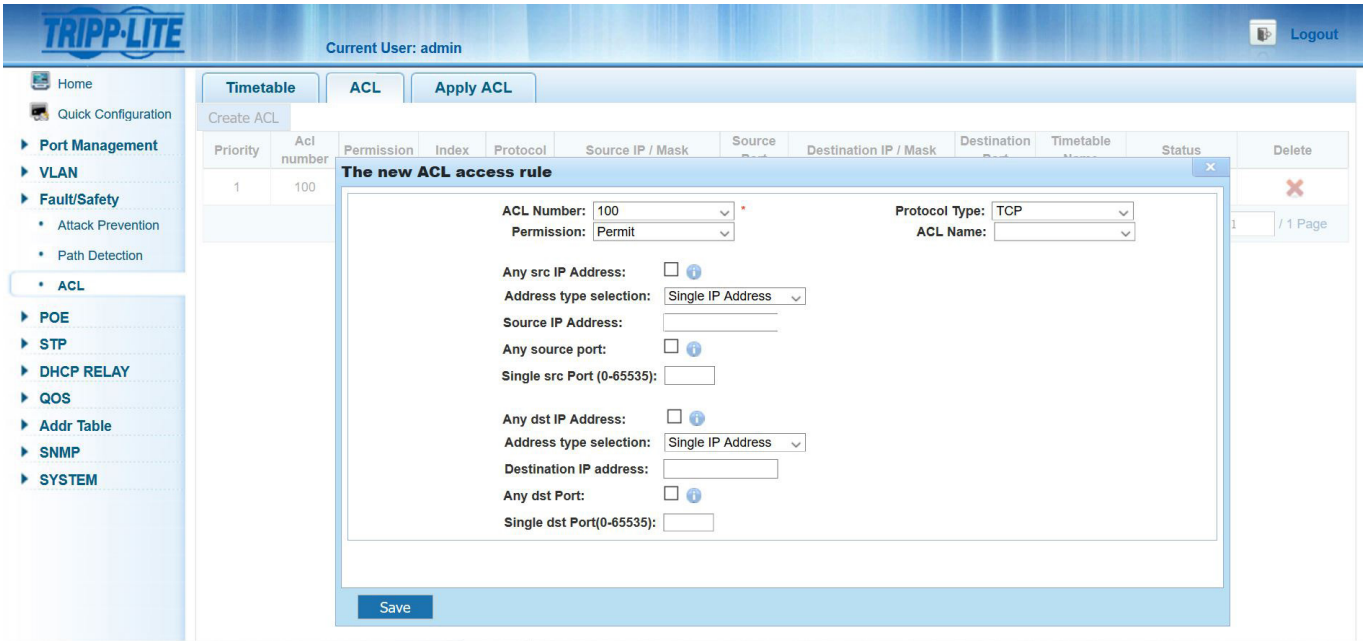


Figure 7.19: Creating an ACL Access Rule

8. PoE (Power over Ethernet, supported by select models)

PoE (available on select switches) provides both power to and communication with multiple PoE and PoE+ enabled devices. Each port is capable of supporting up to 32W of PoE power. The maximum voltage supplied by the PoE system is 51.2V.

8.1 PoE Management Configuration

Select PoE → PoE Config → Management → PoE Status Information (Figure 8.1). View the network switch's PoE status information related to its operation, rated total power, current limit power, alarm threshold, current voltage and the reserve power percentage that is available.

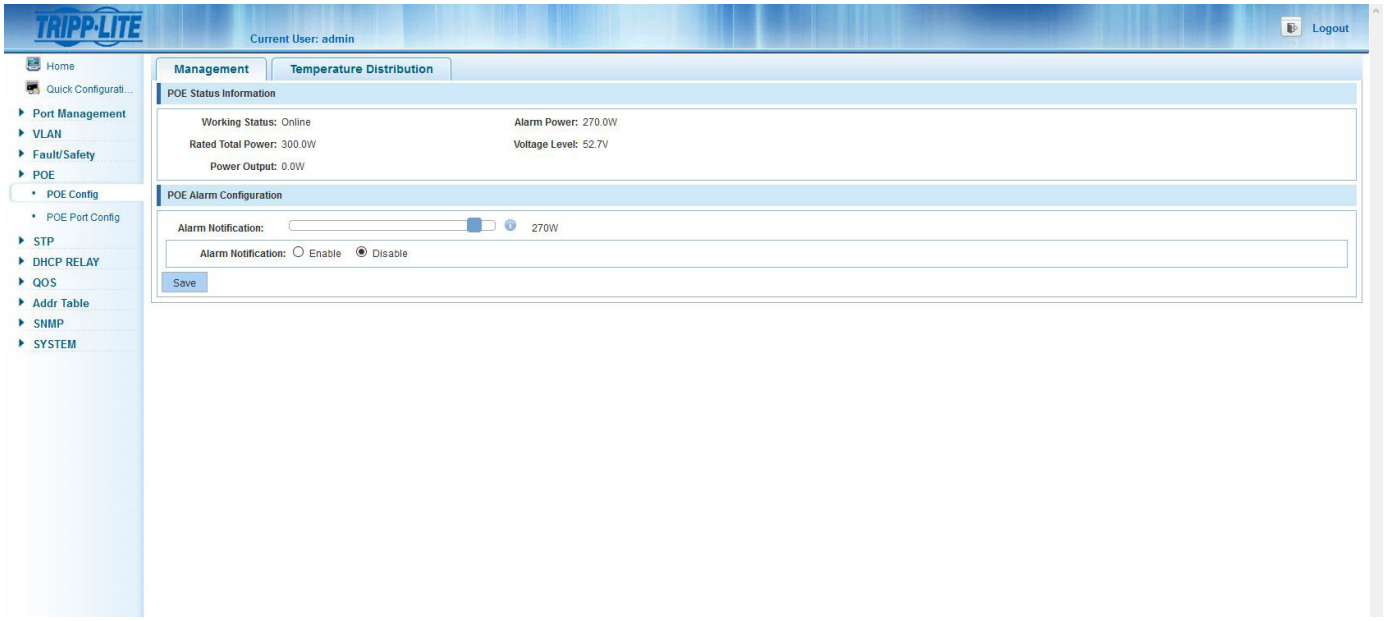


Figure 8.1: PoE Management

8.1.1 PoE Power Consumption Alarm Threshold

Select PoE → PoE Config → Management → PoE Alarm Configuration (Figure 8.2). This function sets the total power threshold to trigger a trap notification if the PoE wattage level is exceeded. Use the Reserve power slider to adjust how much reserve power you want to allocate for future application usage. Once the alarm and reserve thresholds are set, click "Save."

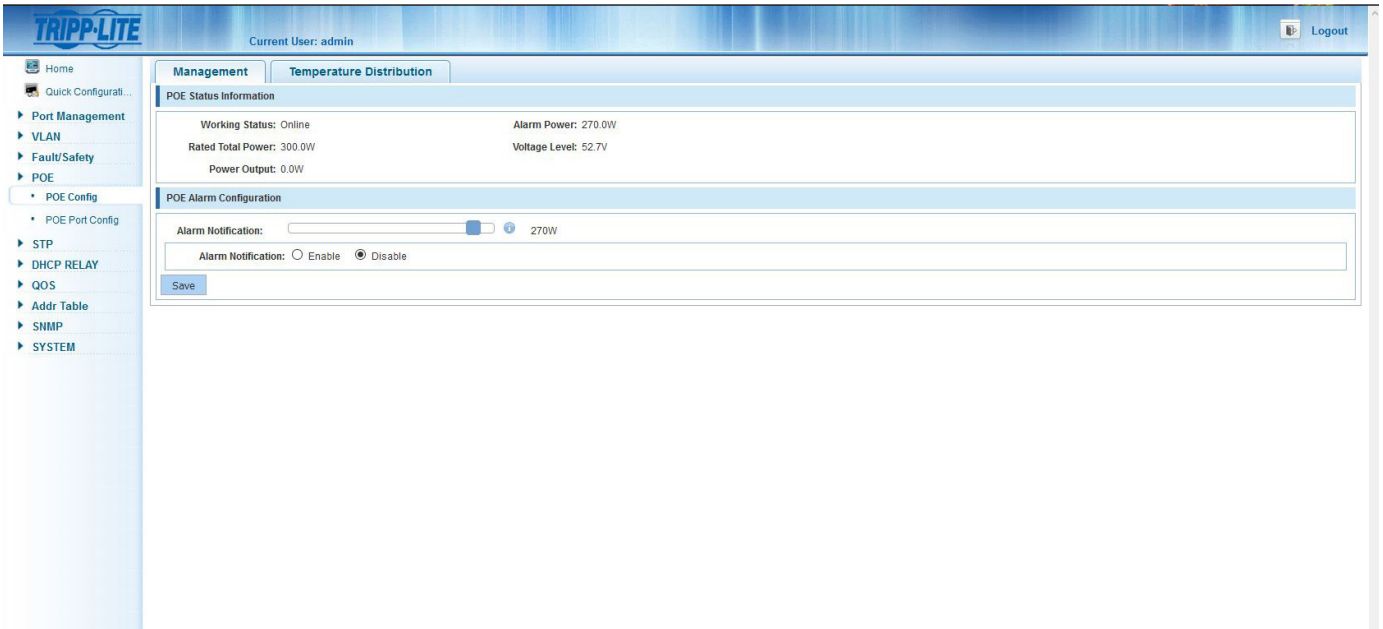


Figure 8.2: PoE Alarm Configuration

8. PoE (Power over Ethernet, supported by select models)

8.1.2 PoE Temperature Distribution/Alarm Thresholds

Sets the alarm temperature threshold for each of the three PoE chipsets. The temperature alarm range is 158-300°F (70-149°C).

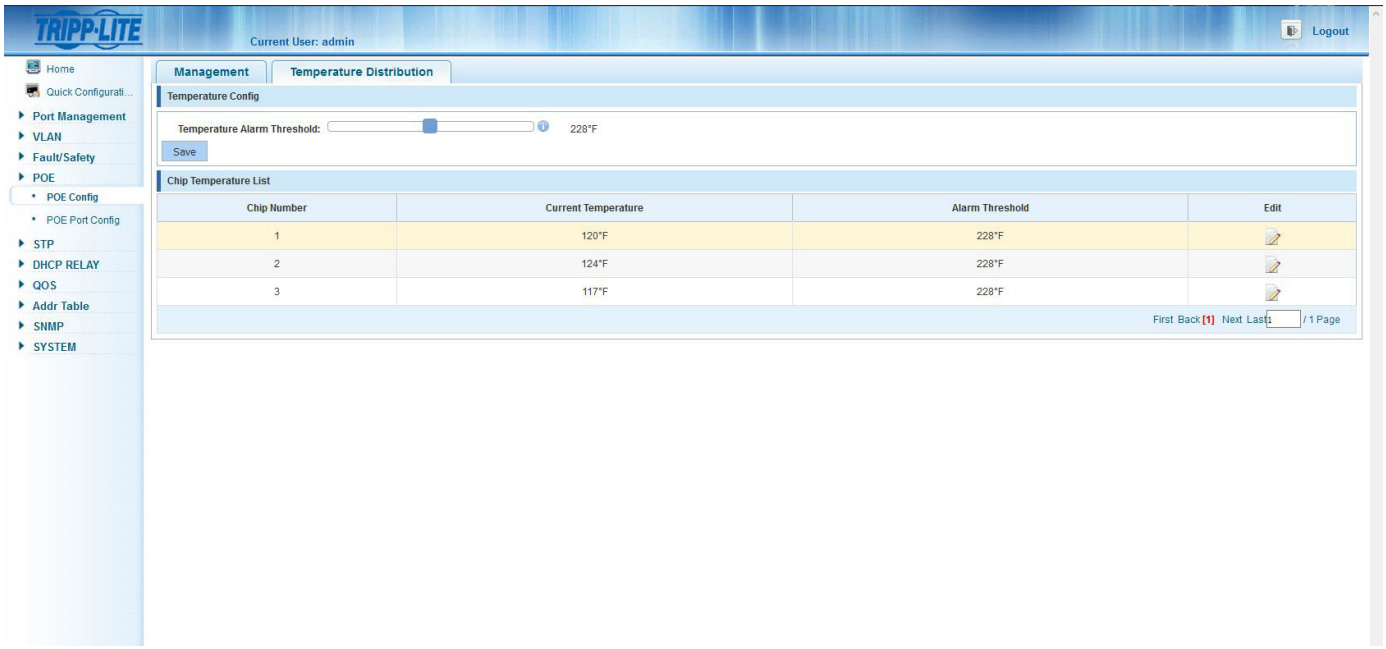


Figure 8.3: PoE Temperature Distribution

8.2 PoE Port Configuration

Select PoE → PoE Port Config (Figure 8.4). Adjusts the PoE capabilities of each port. Click the edit icon to enable or disable PoE, change the maximum power usage, set the priority and set detection mode AF, AT, AT&F for connected devices.

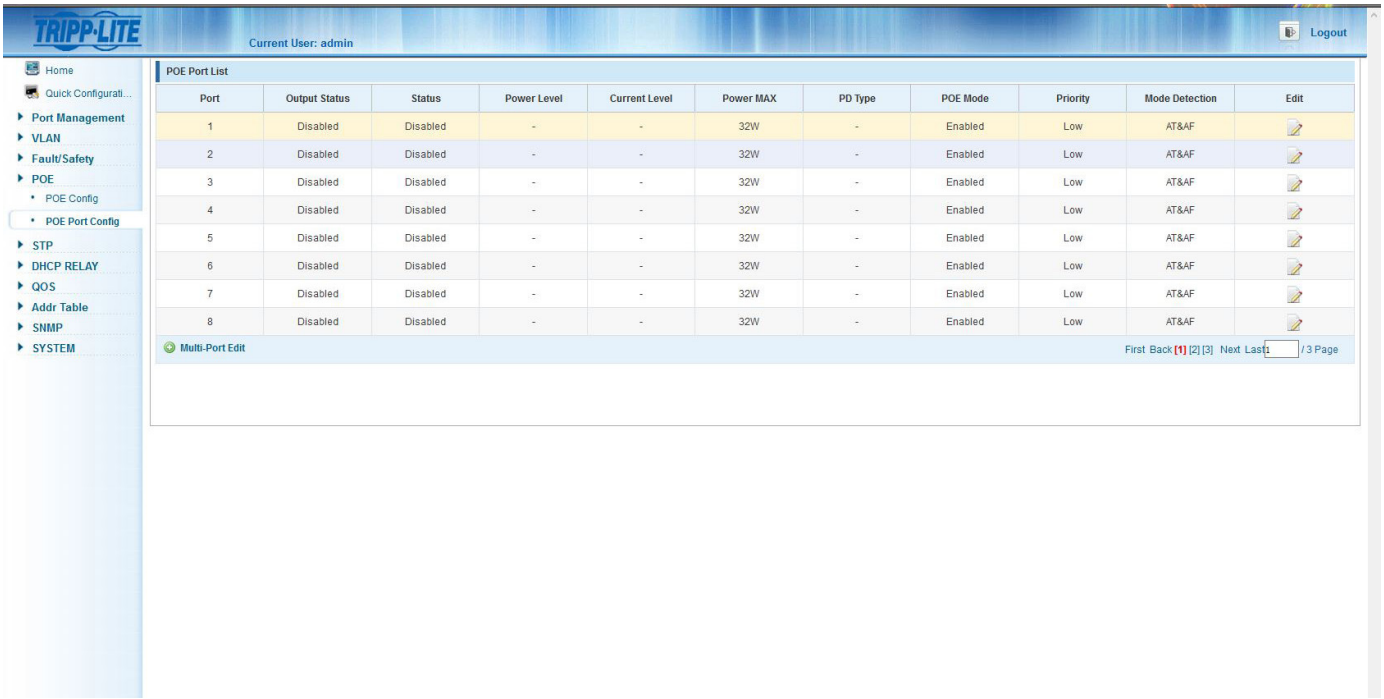


Figure 8.4: PoE Port Configuration

9. Multiple Spanning Tree Protocol (MSTP) Management

Multiple Spanning Tree Protocol Management provides a logical loop-free topology for Ethernet networks. The MSTP prevents bridge loops and resulting broadcast storms. Link redundancy is another function of MSTP to ensure the network connections have a redundant path in the event an active link goes down.

9.1 MSTP Region Configuration

Select STP → MSTP Region to create MSTP instances (Figure 9.1).

9.1.1 MSTP Configuration

Enter the region name and revision level of the MSTP instance.

9.1.2 Instance Mapping

Choose an instance ID from 1-16 and the associated VLANs to which it will be assigned. (Instance 0 is assigned to all VLANs by default.)

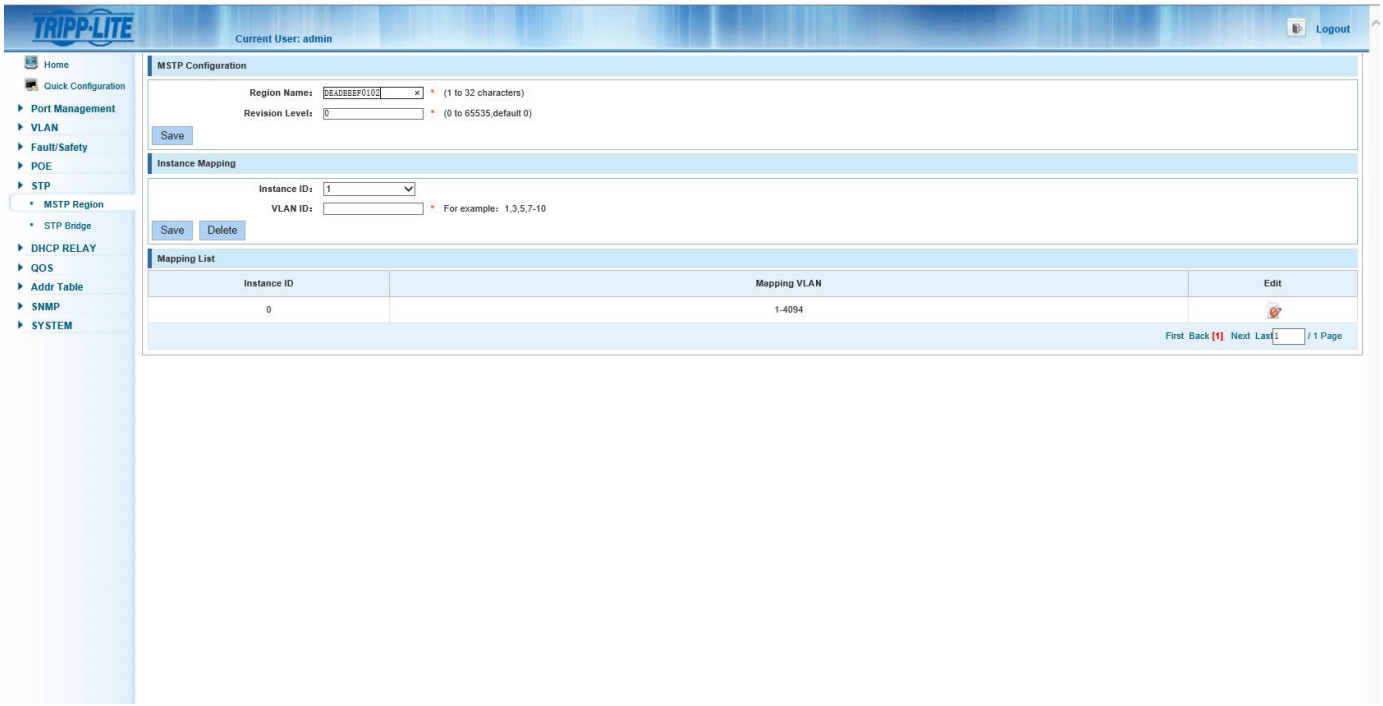


Figure 9.1: MSTP Configuration and Instance Mapping

9.1.3 Mapping List

The mapping list is a list of all MSTP region instances created. Only instances that have been created can be edited or deleted. When an instance is removed, the associated VLAN returns to the default instance ID of 0.

9. Multiple Spanning Tree Protocol (MSTP) Management

9.2 Spanning Tree Protocol (STP) Bridge Configuration

Select STP → STP Bridge Config (Figure 9.2) and perform the following steps:

1. Enable Instance Priority by clicking the checkbox.
2. Select the instance ID from 0-16.
3. Select the priority from 0 through 61440 (default: 32768).
4. Enable the STP bridge by selecting ON, enter Hello Time from 1-10 seconds (default: 2s), Forward Delay from 4-30 seconds (default: 10s), Set the mode of STP, RSTP, MSTP; MAX Age from 6-40 seconds (default: 10s); and Max Hops from 1-40 seconds (default: 10). Click “Save”.
5. “Show Bridge Info” displays the current configured STP bridge information (Figure 9.3).

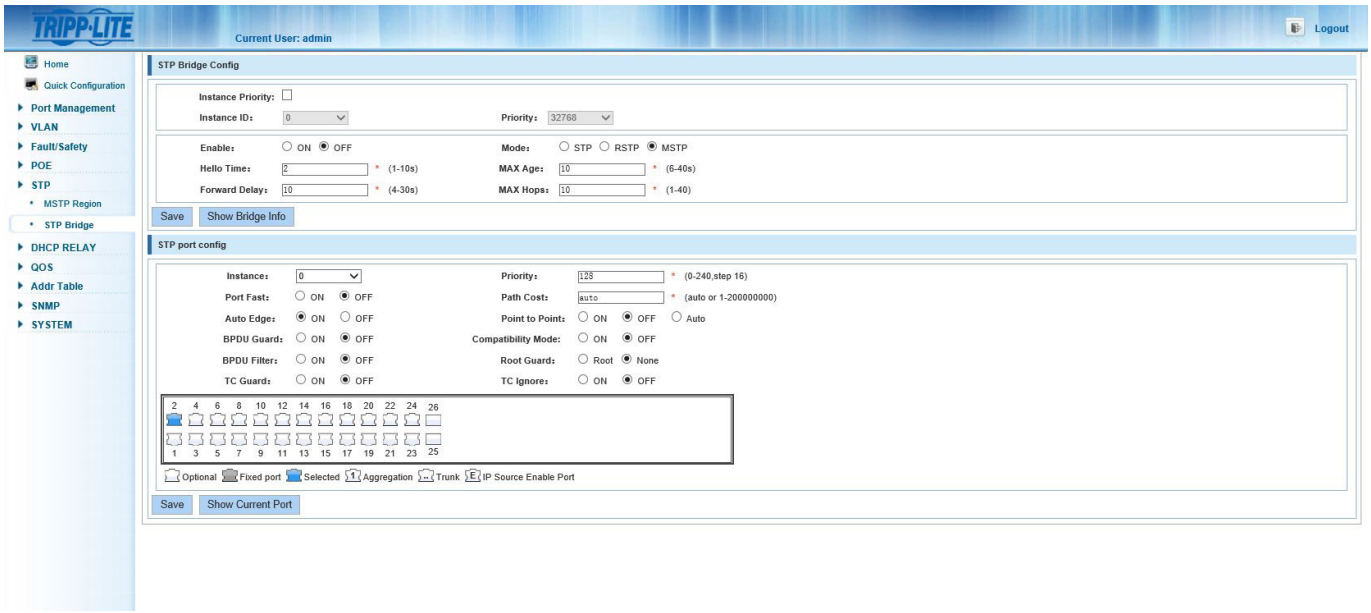


Figure 9.2: STP Bridge Config and STP Port Config

Figure 9.3: STP Bridge Information

9. Multiple Spanning Tree Protocol (MSTP) Management

9.3 STP Port Configuration

Follow the below steps to configure the STP port:

1. Select the Instance Bridge ID that was created above
2. Select Port Fast (default: OFF)
3. Select Auto Edge (default: ON)
4. Select BPDU Guard (default: OFF)
5. Select BPDU Filter (default: OFF)
6. Select TC Guard (default: OFF)
7. Select Priority from 0-240; must be entered in multiples of 16 (default: 128)
8. Select Path COS to Auto or 1-200000000 (default: Auto)
9. Set Point to Point to ON, OFF, or AUTO (default: OFF)
10. Set Compatibility Mode (default: OFF)
11. Set Root Guard to Root or None (default: None)
12. Set TC Ignore (default: OFF)
13. Click “Save”
14. Click Show Current Port to view STP current port information

Figure 9.4: STP Current Port Information

10. DHCP Relay

The DHCP Relay sends DHCP messages between DHCP clients and DHCP servers on different IP networks. In this area, relay and Option82 settings can be edited.

10.1 DHCP Relay Agent Configuration

Select DHCP RELAY → DHCP Relay (Figure 10.1). Click the checkbox to enable DHCP Relay. By default, “DHCP Option Trust Field” is already enabled.

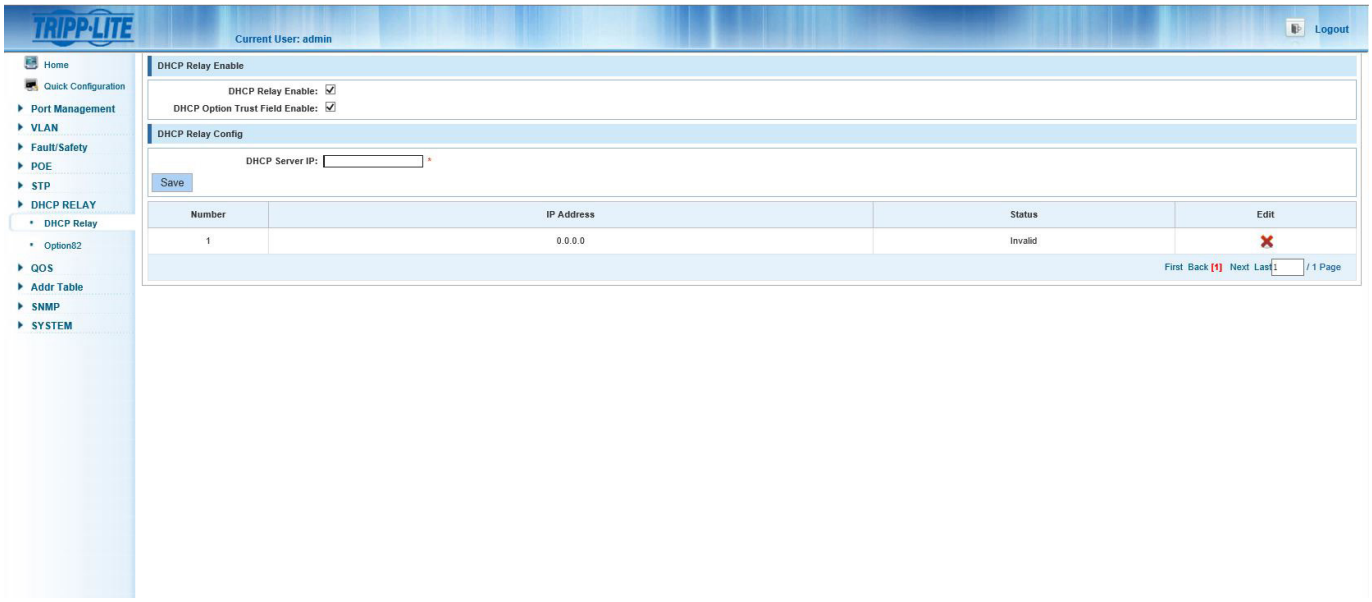


Figure 10.1: DHCP Relay Enabled

10.2 Option82 Configuration

Select DHCP RELAY → Option82. In the Option82 configuration (Figure 10.2) enter the following information:

10.2.1 Circuit Control

Enter the Circuit Control ID from 3-63 and the VLAN ID. Click “Save” and each instance will be saved to a list.

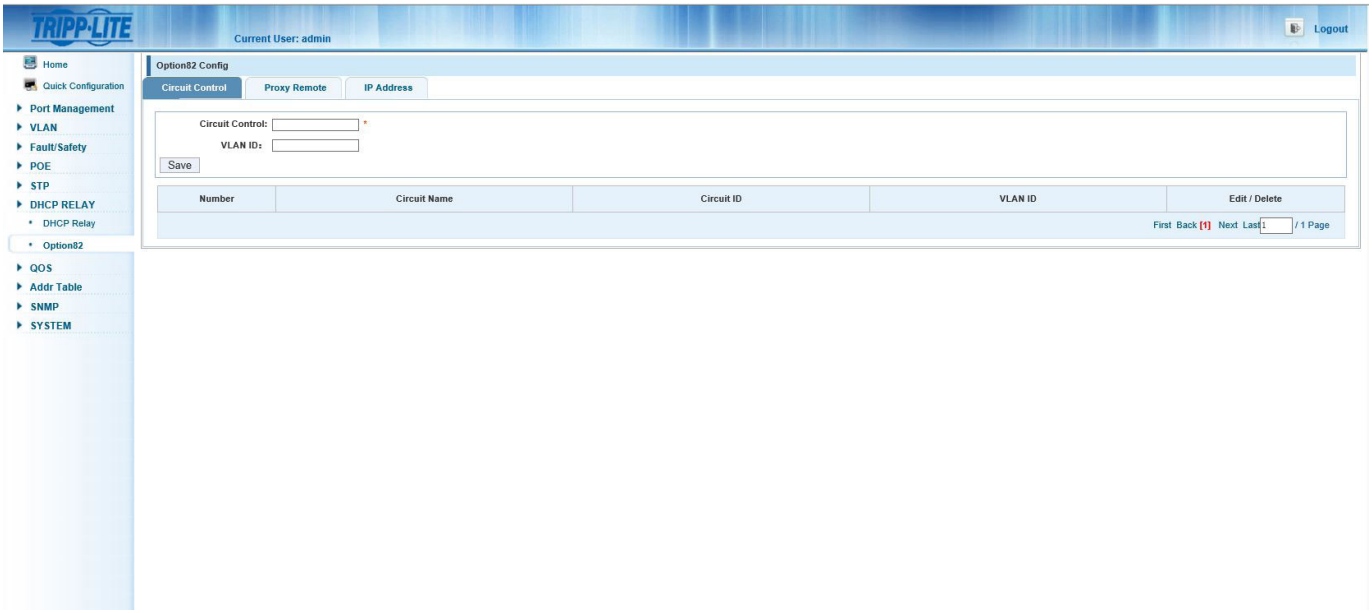


Figure 10.2: Option82 Circuit Control

10.2.2 Proxy Remote

Enter the Proxy Remote (limit: 63 characters) and the VLAN ID (Figure 10.3). Click “Save” and each entry will be saved to the list.

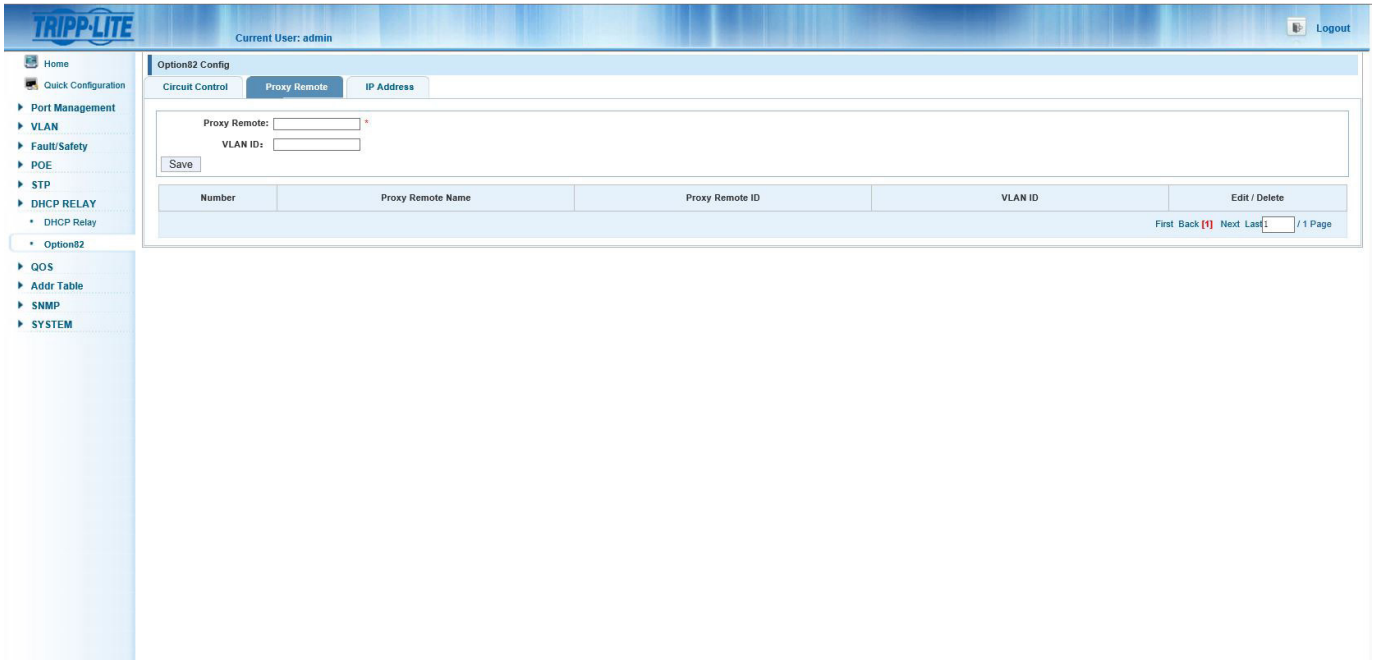


Figure 10.3: Option82 Proxy Remote

10.2.3 IP Address

Enter the IP Address of the DHCP relay server and the associated VLAN ID (Figure 10.4). Click “Save” and each instance will be saved to the list below.

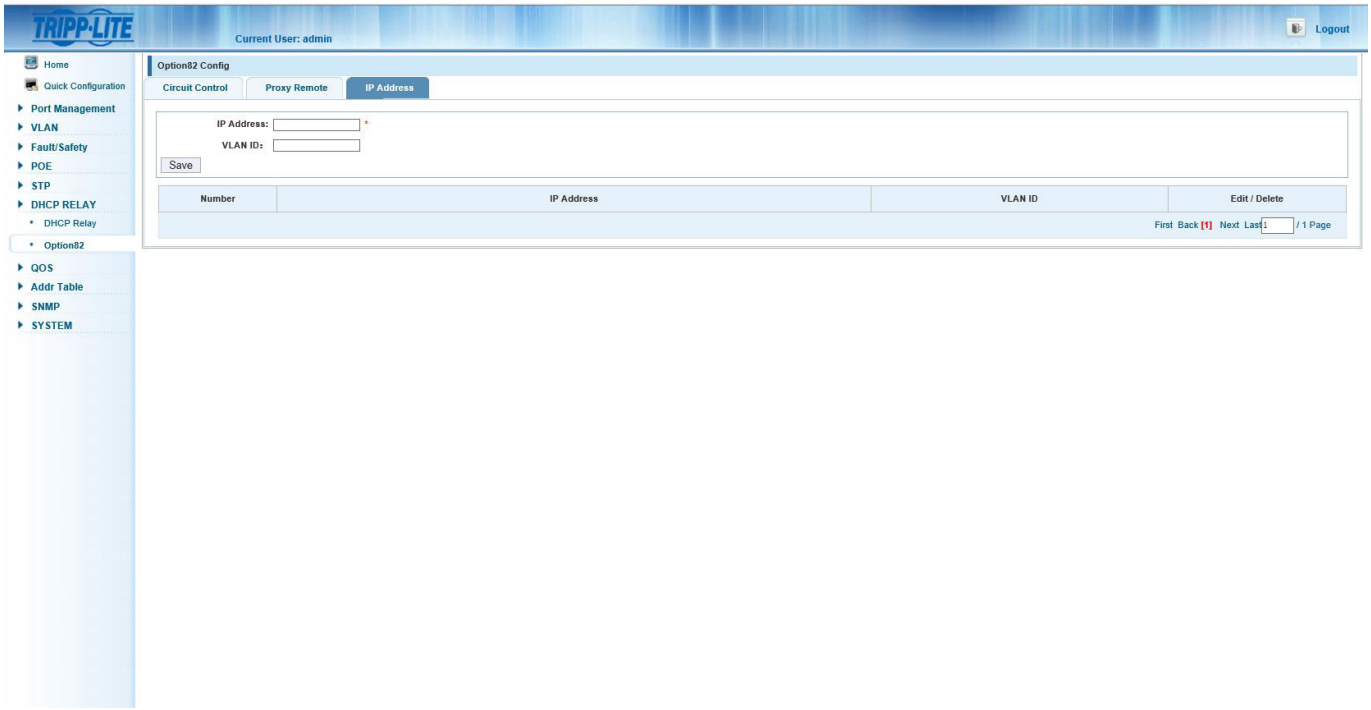


Figure 10.4: Option82 IP Address

11. Quality of Service (QoS) Management

Quality of Service ensures that the most import network traffic (e.g., VoIP, IP cameras, etc.) gets through the switch with the least interruption to its data transmission as possible. To give any network-capable device a higher transmission priority, QoS must be configured on the switch. It is disabled by default. Follow the steps below to configure the port for device traffic that requires QoS.

11.1 QoS Remark

Select QoS → Remark. Under the QoS Multi-Label section you can set the Rule Index, Operation Type, Value Type, Value, Service Class Mapping or Priority Remark to one port or multiple ports (Figure 11.1). To apply the rule to a port or set of ports, click "Save." To discard the configuration click "Cancel." The box below shows the parameters for each QoS rule:

QoS Multi-Label	Parameters	Notes
Rule Index	1-32	
Operation Type	Equal; Always-Match	
Value Type	DST Mac SRC Mac Ethernet Priority VLAN Number Ethernet Type Destination IP Source IP IP Type IPv4 Diff IPv6 Priority Layer 4 SRC Port Layer 4 DST Port	
Values	DST MAC – 00:00:00:00:00:00 SRC MAC – 00:00:00:00:00:00 Ethernet Priority – 0~7 VLAN Number – 1~4094 Ethernet Type – 0~0xFFFF Destination IP – 0.0.0.0 Source IP – 0.0.0.0 IP Type – 0~0xFF IPv4 Diff – 0~63 IPv6 Priority – 0~255 Layer 4 SRC Port – 0~65535 Layer 4 DST Port – 0~65535	Values options change based on the value type selected. Values are always required.
Port Configuration	Apply rule to one or more ports by selecting an individual port, selecting all, or selecting all others.	You can also drag the cursor to select multiple ports.
Save Configuration	Click "Save" to apply the rule or Cancel to discard changes.	

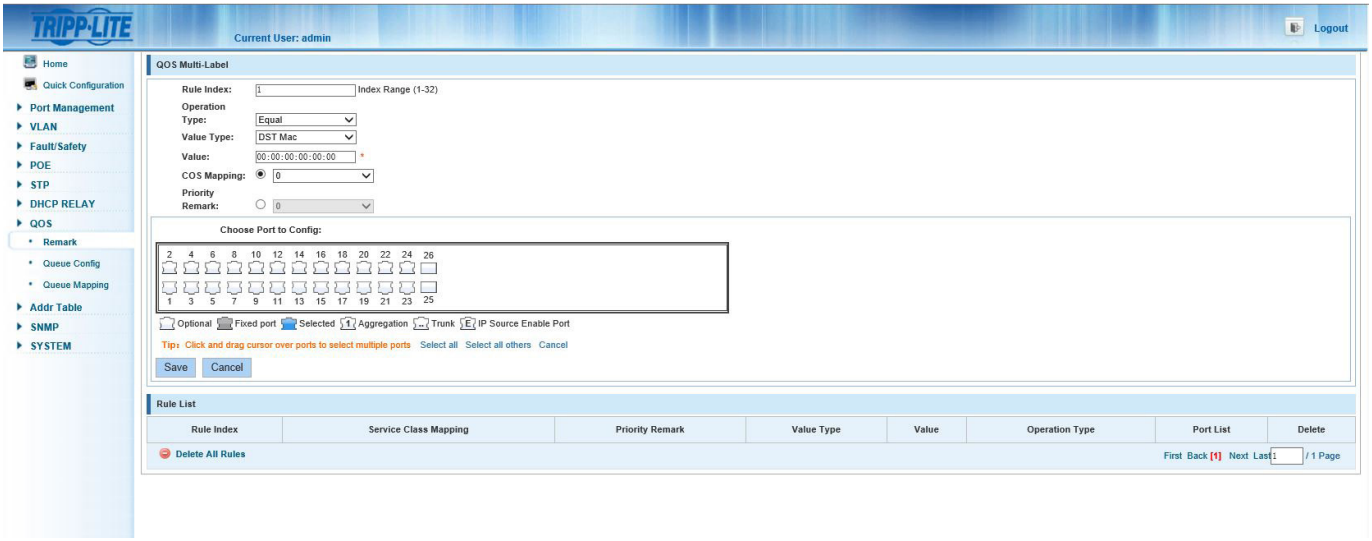


Figure 11.1: QoS Remark Overview

11. Quality of Service (QoS) Management

11.1.1 Rule List

The Rule List shows all rules information that was configured above. Delete a single rule or delete all rules as necessary.

11.2 QoS Queue Configuration

Select QoS → Queue Config to configure the Queue Mode. The available options are as follows:

Queue Mode Scheduling Options	Description
SP	Absolute Priority Scheduling
RR	Round-Robin Scheduling
WRR	Weighted Round-Robin Scheduling
WFQ	Weighted Fair Scheduling
WRR and WFQ Byte Weights	Set the byte weights from 0-127 for each queue so that they will be in proportion to occupy the bandwidth to send the data

11.3 QoS Queue Mapping

Queue mapping manages the transmission of data messages to an output queue of a port. The messages within the various output queues will contain transmission service policies of different levels and qualities. Each port has 8 output queues, 0-7. The Class of Service queue map and the DSCP to COS map must be configured on the switch to convert the DSCP value of the message into an output queue number to determine into which output queue to transfer the messages.

11.3.1 COS Queue Map Settings

Set each of the 8 output queues to the Class of Service (COS) required for the data message transmission (Figure 11.2).

Class of Service Mapping	Description
0	Best Effort
1	Class 1
2	Class 2
3	Class 3
4	Class 4
5	Express Forwarding
6	Stay the Same (IP Routing)
7	Stay the Same (Link Layer and routing stay alive)

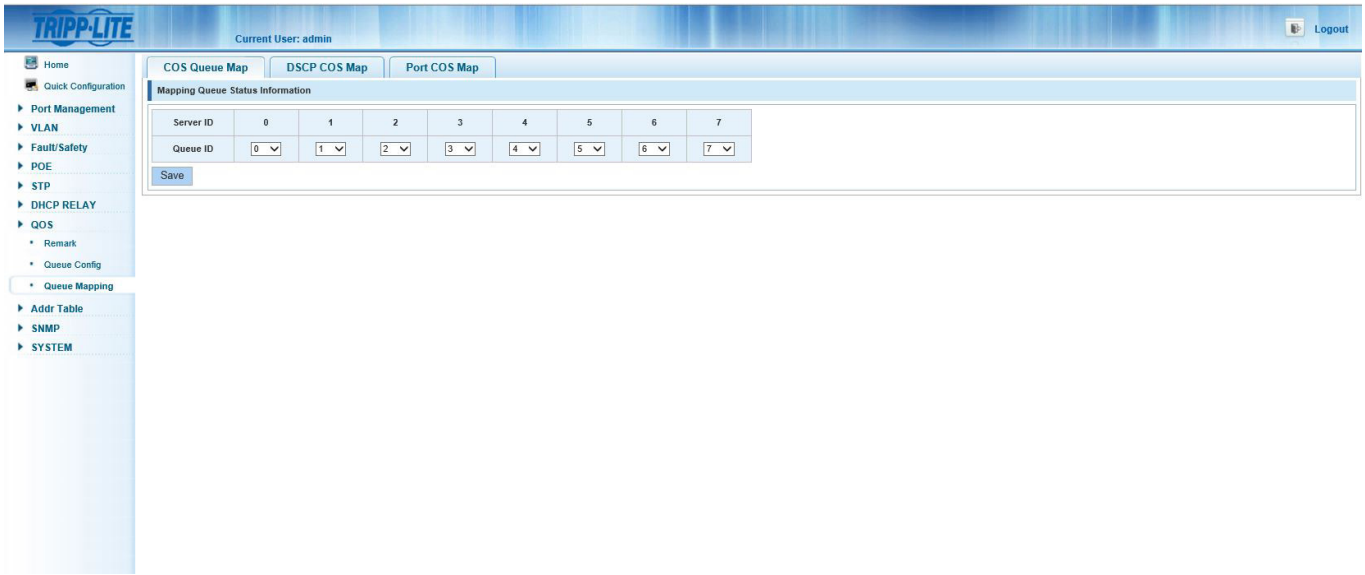


Figure 11.2: COS Queue Map

11. Quality of Service (QoS) Management

11.3.2 DSCP COS Map Settings

Select COS → Queue Mapping → DSCP COS Map – Set the Differential Service Code Point (DSCP) Mapping Team List (Figure 11.3).

Server List - DSCP field has seven COS fields (0-63) divided into four tables.

Queue ID - Mapping the DSCP to COS fields (0 to 7), based on the COSine is mapped to a queue.

Note: *COS priority is greater than the DSCP, DSCP priority is greater than the port.*

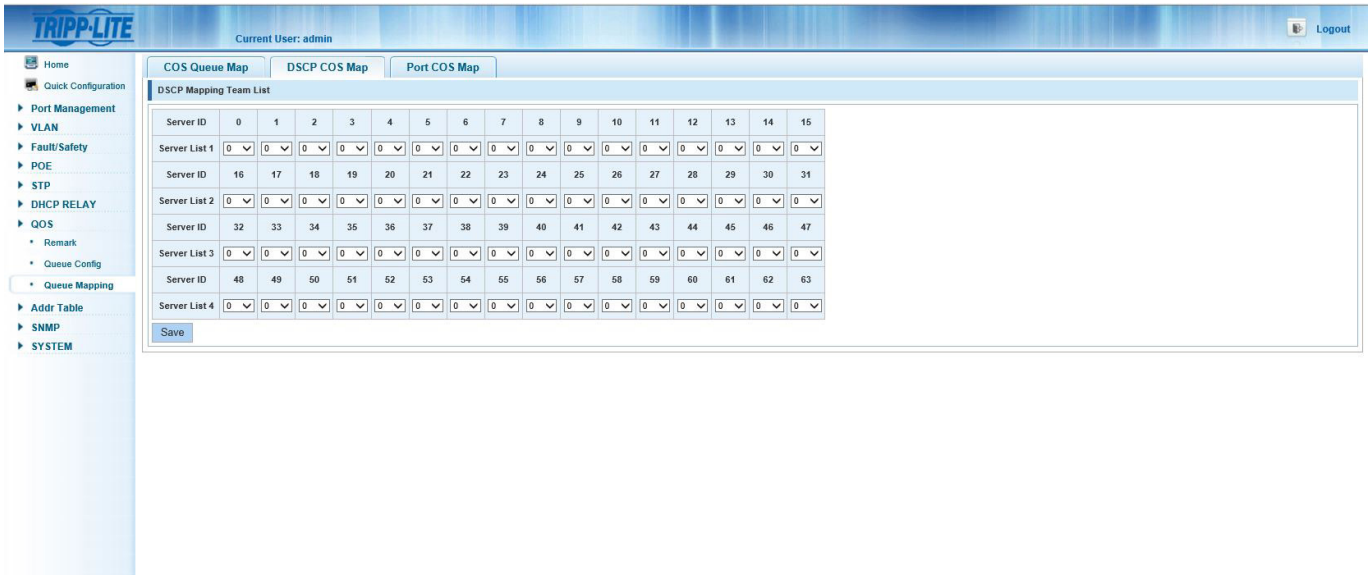


Figure 11.3: DSCP COS Map

11.3.3 Port COS Map Settings

Select COS → Queue Mapping → Port COS Map (Figure 11.4) to set the port to the service class map.

Select the port.

Select the COS Server ID from 0-7 (All ports set to COS 0 by default).

Click “Save” to apply settings. The saved settings will show in the Control List with a “T” symbol between the port number and the Server ID.

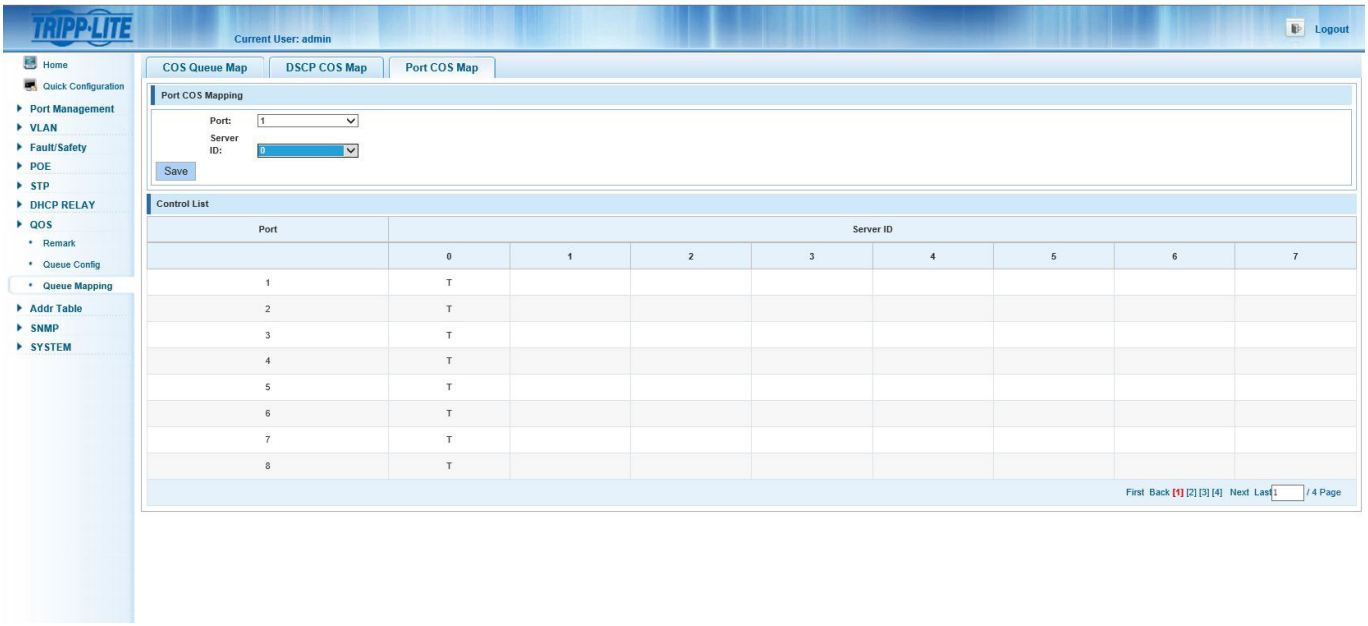


Figure 11.4: Port COS Map

12. Mac Address Table Access List Management

The MAC Address Access Control List table (Figure 12.1) allows a user to add and delete MAC addresses, set the MAC Learning and Aging, and MAC filtering.

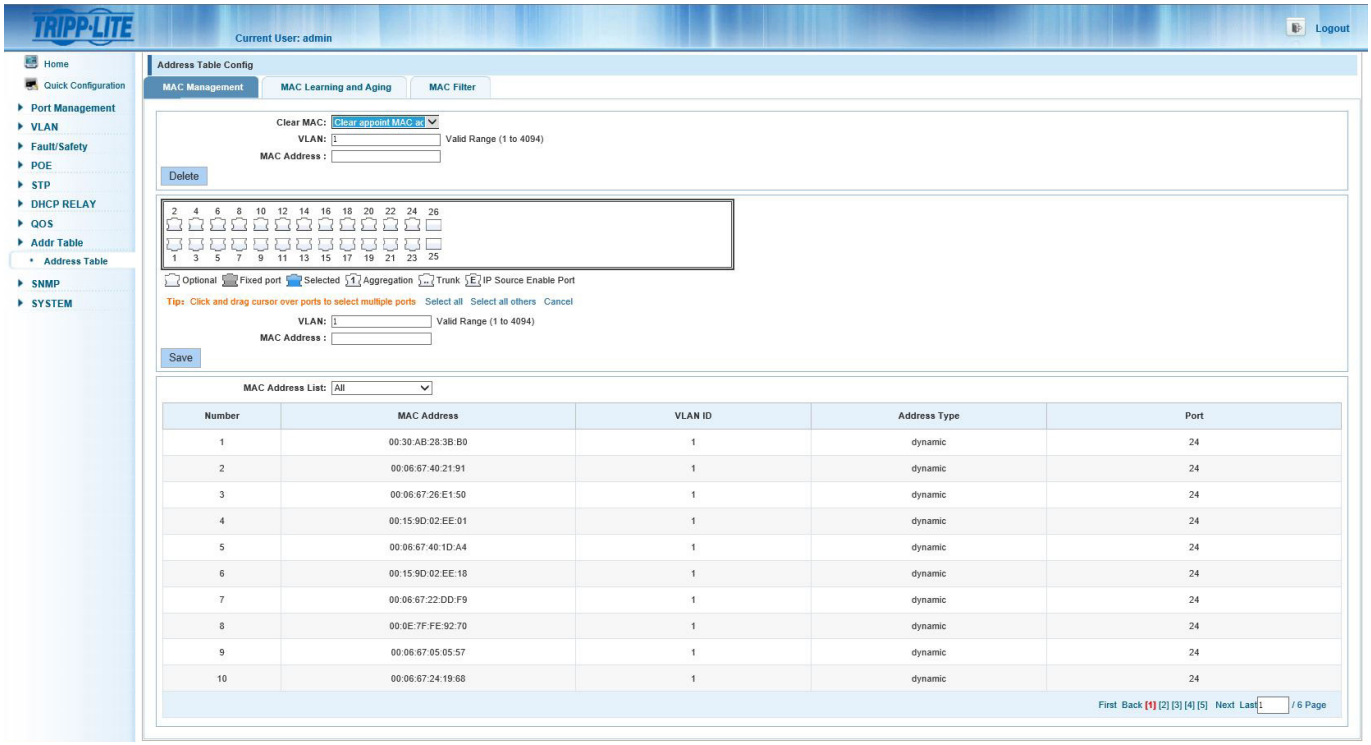


Figure 12.1: MAC Management View

12. Mac Address Table Access List Management

12.1 MAC Management

Within the MAC Management screen, you can add and delete from the MAC Address table (Figure 12.2).

12.1.1 View the MAC Address List

View the full list of MAC addresses along with the VLAN with which each is associated and the ports it has access to communicate through. Use the view filter to see all, dynamic, or static MAC addresses in the list (Figure 12.2).

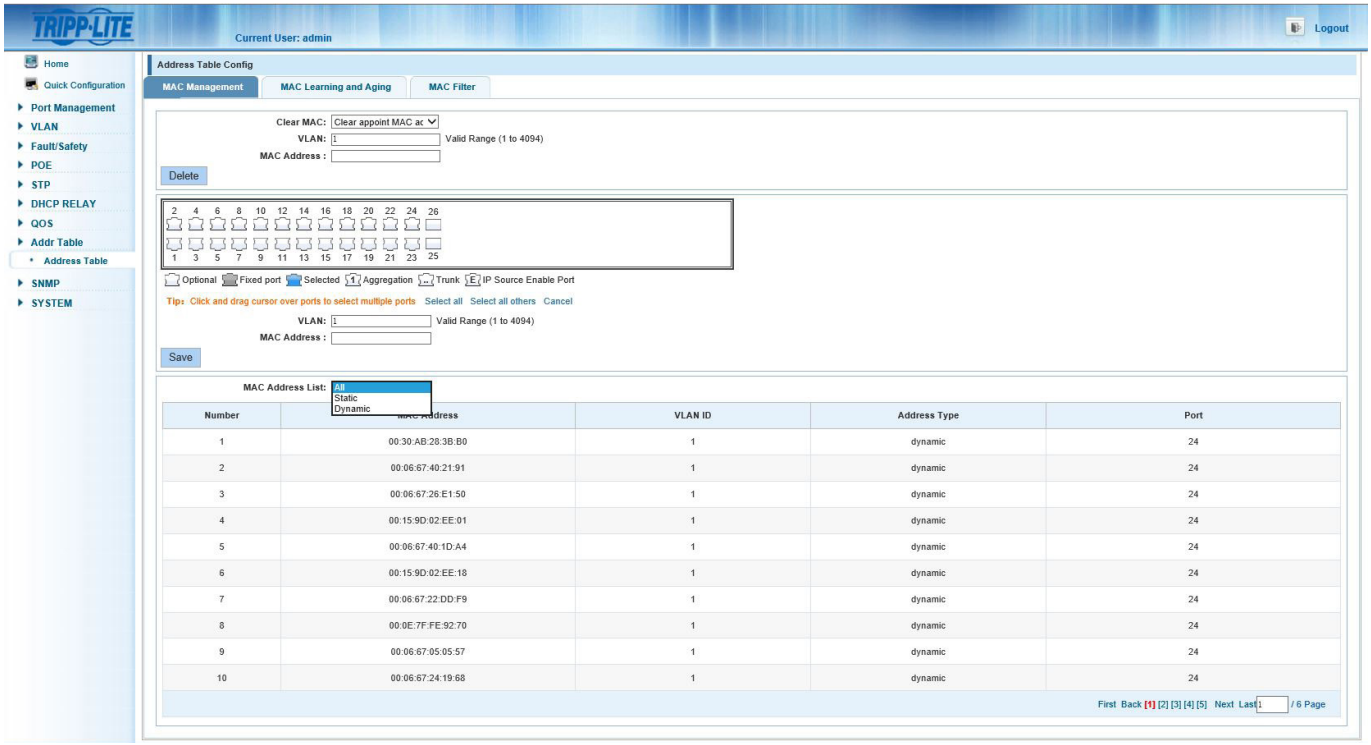


Figure 12.2: MAC Address List Filters

12.1.2 Add MAC Address

To add a static MAC address table to the MAC Address List (Figure 12.3), perform the following steps:

1. Select the port(s) you want the MAC address to be able to access.
2. Enter the VLAN ID through which the MAC address will communicate.
3. Enter the static MAC address to be added.
4. Click the “Save” button to add the MAC address to the MAC address list.

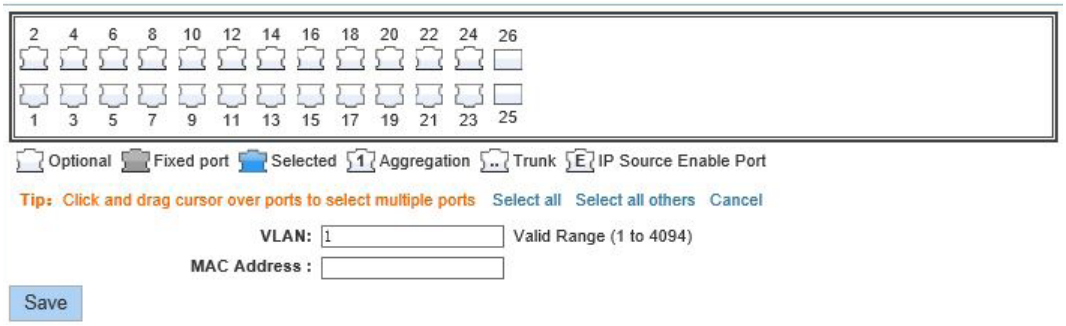


Figure 12.3: Add MAC Addresses

12. Mac Address Table Access List Management

12.1.3 Delete MAC Address

The following set of functions can be used to clear a single MAC addresses from an associated VLAN or clear the entire list:

MAC Management Functions	Description
Clear MAC	Options: clear an appointed MAC address, clear dynamic Unicast, clear static Unicast, or clear the entire MAC address list.
VLAN	Enter the VLAN ID you want to clear the MAC address from (valid ID Range: 1-4094).
MAC Address	Enter the specific MAC Address to be deleted.

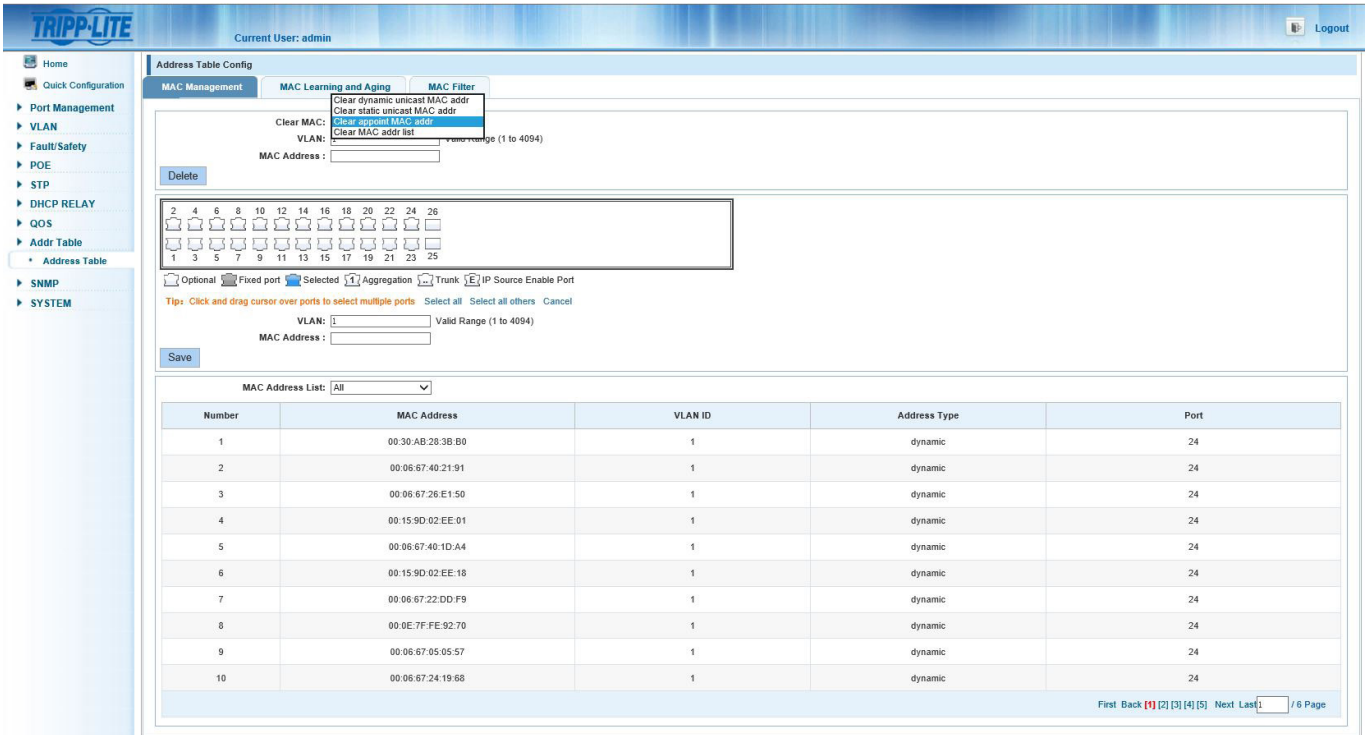


Figure 12.4: Clear MAC Addresses

12. Mac Address Table Access List Management

12.2 MAC Learning and Aging

The MAC learning limit can be set up to 8191 addresses per port. The aging time can be set to 0 (no aging) or up to 1,000,000 seconds. (See Figure 12.5.)

12.2.1 MAC Learning Limit

To change a single port, select the port number. Next, enter the Learning Range from 0-8191 (8191 is default learning range). Click “Save” to save the settings. To configure learning on multiple ports, click and drag the cursor over multiple ports or use the “Select all” or “Select all others” options to select ports. Enter the MAC Learning Limit for the ports, up to 8191 entries. Click “Save” to save settings.

12.2.2 MAC Address Aging Time

The aging time can be set to 0 (no aging) or up to 1,000,000 seconds (default setting is 300 seconds). Click “Save” to save settings.

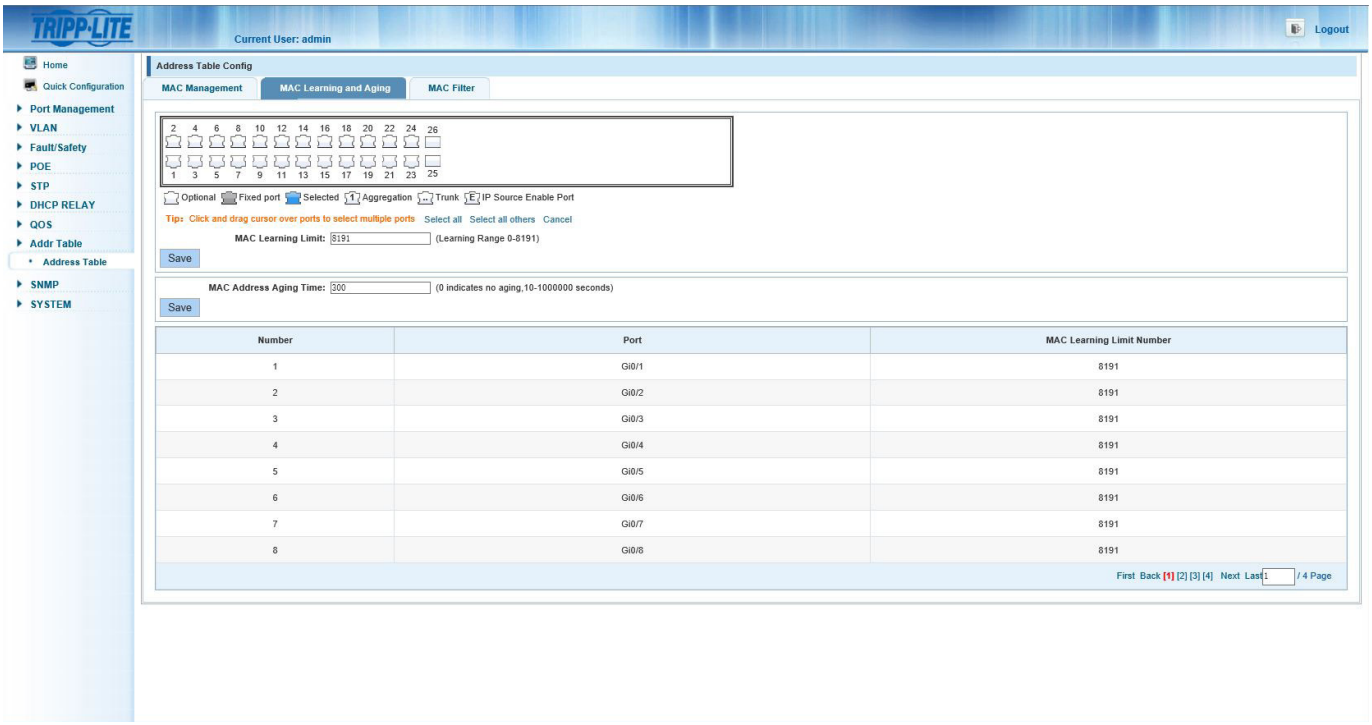


Figure 12.5: MAC Address Learning and Aging

12.3 MAC Address Filtering

To ensure a MAC address cannot access incoming or outgoing communication through the switch, perform the following steps:

1. MAC Address – Enter the MAC address to which filtering will apply
2. VLAN – Enter the VLAN ID
3. Filtering direction – Determine if the filtering will be from the source, the destination, or both.
4. Click “Save” to add to the MAC address filter to the list.

To delete a filter, click the icon next to the filtered MAC address entry.

13. Simple Network Management Protocol (SNMP) Management

Simple Network Management Protocol (SNMP) allows the switch to be monitored and controlled remotely. It can also send SNMP traps to a trap receiver service.

13.1 SNMP Configuration Settings

13.1.1 Enable/Disable SNMP Configuration

This feature is disabled by default. It can be enabled by toggling the enable/disable switch (Figure 13.1). Once enabled, you have access to configure the SNMP community, group, users, and trap settings.

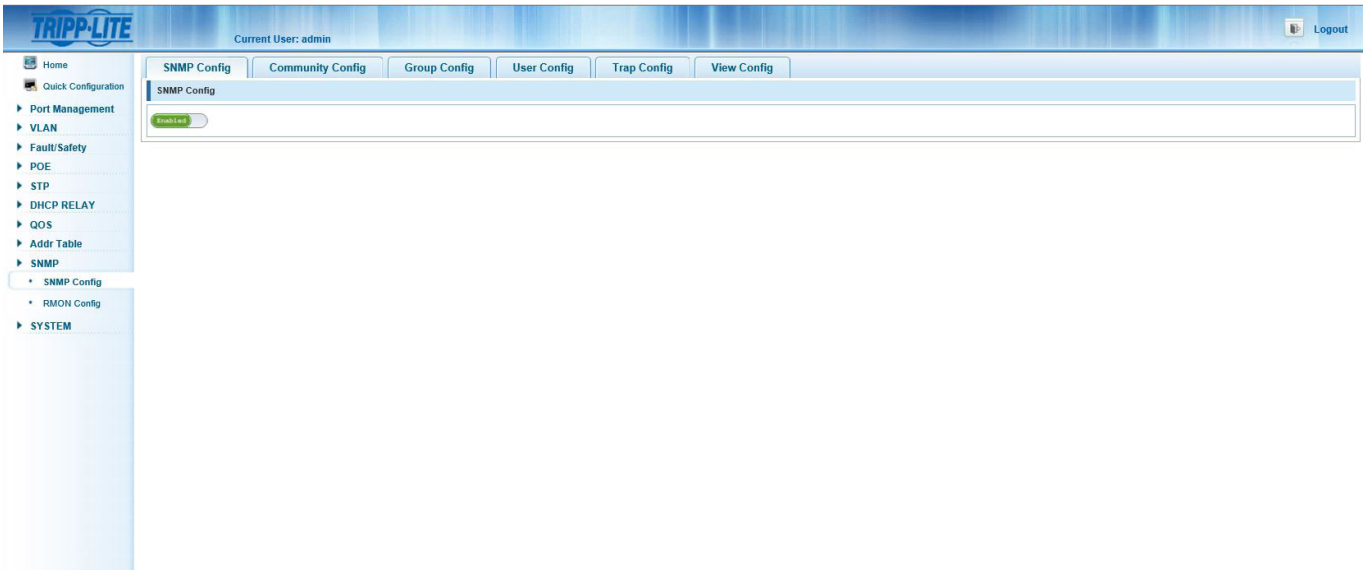


Figure 13.1: SNMP Configuration Overview

13.1.2 Community Configuration

To add the supported SNMP community strings and their permissions select SNMP → SNMP Config → Community Config. Click on the green icon to add a new Community Configuration (Figure 13.2). Add the community name (limit: 16 characters) and the access authority of either “Read Write” or “Read Only”. Click “Save” to save settings, click “Exit” to discard changes.

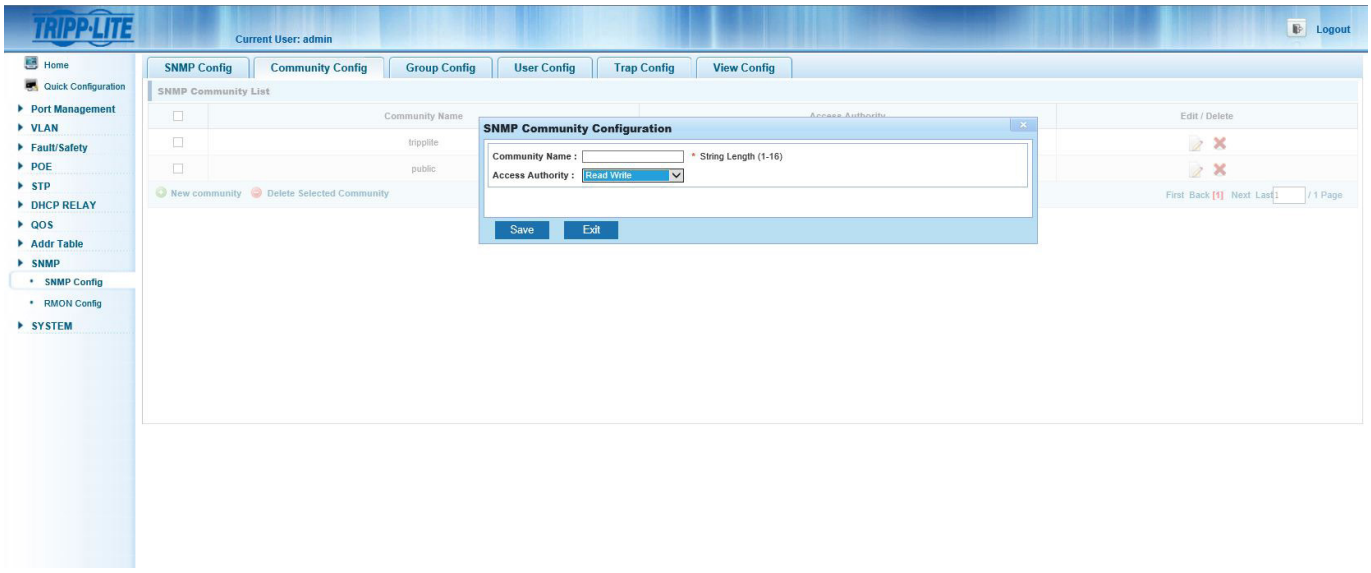


Figure 13.2: SNMP Community Configuration

To edit a Community Configuration, select the “Edit” icon and change the community name or access authority (Figure 13.3). Click “Save” to save settings, click “Exit” to discard changes.

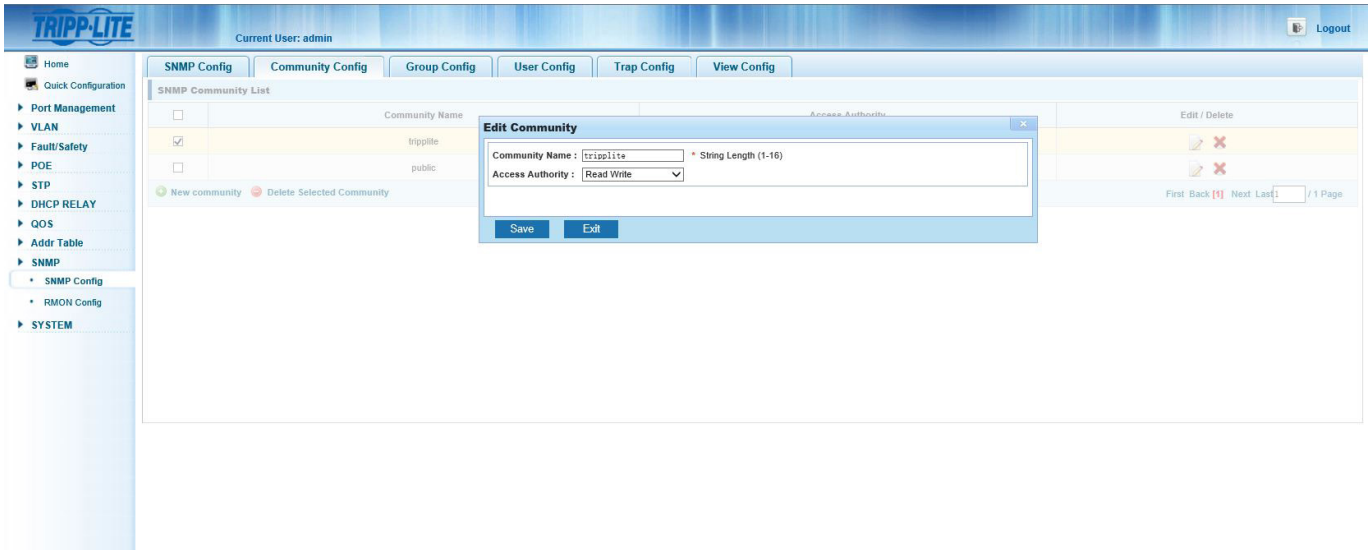


Figure 13.3: Edit Community Configuration

To delete a Community Configuration, click the red icon to delete the list entry or click the checkbox for the community string to be deleted and click “Delete Selected Community”. Delete multiple community strings by clicking the checkbox of each of the strings to be removed or by checking the main box at the top of the list to select all entries. Once all are selected, click the “Delete Selected Community” icon to remove them from the list.

Note: *You can configure a total of 8 community strings for SNMP.*

13.1.3 View SNMP Configuration

Select SNMP → SNMP Config → View Config (Figure 13.4) – Set up the viewing and managing rules for the MIB OID by creating MIB views which can then be assigned to an SNMP group. Configure a new rule for each view to avoid affecting the SNMP function.

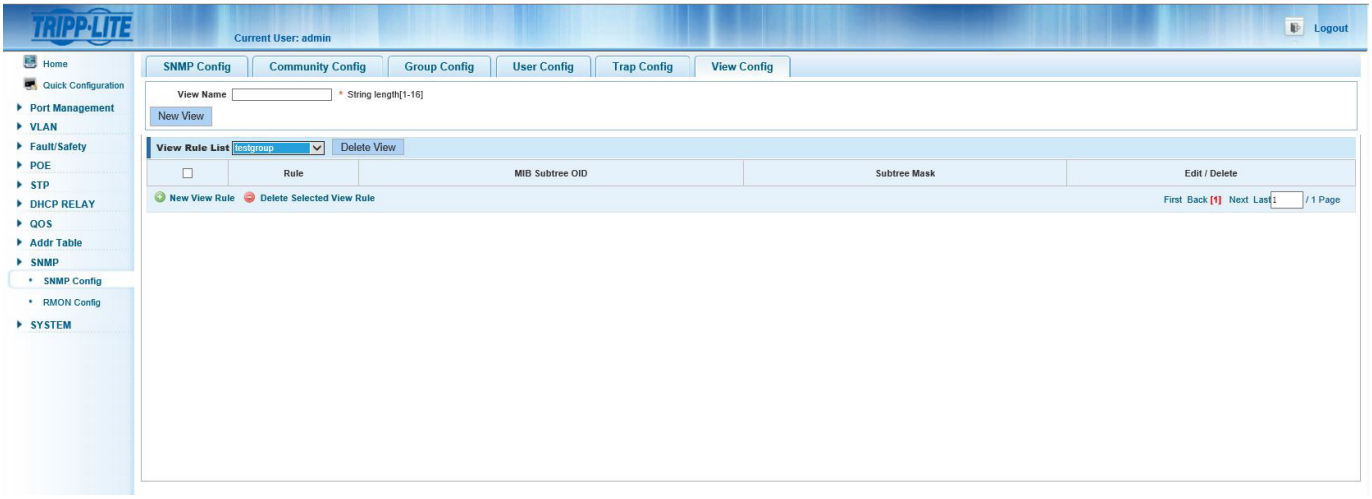


Figure 13.4: SNMP View Config

13.1.4 View Name

Enter the name of the view (limit: 16 characters). Click on the “New View” icon. This will add the view name to the drop-down of the View Rule List.

13.1.5 View Rule List

Once the view name is configured, select the Green icon to add a new view rule (Figure 13.5).

13.1.6 Edit View Rule

To include or exclude a view in a rule (Figure 13.5), follow the steps below:

1. MIB Subtree OID – Enter the OID desired for filtering for the view name (limit: 64 characters).
2. Subtree Mask – Enter the subtree mask OID if required.
3. Click “Save” to save the changes or “Exit” to discard.

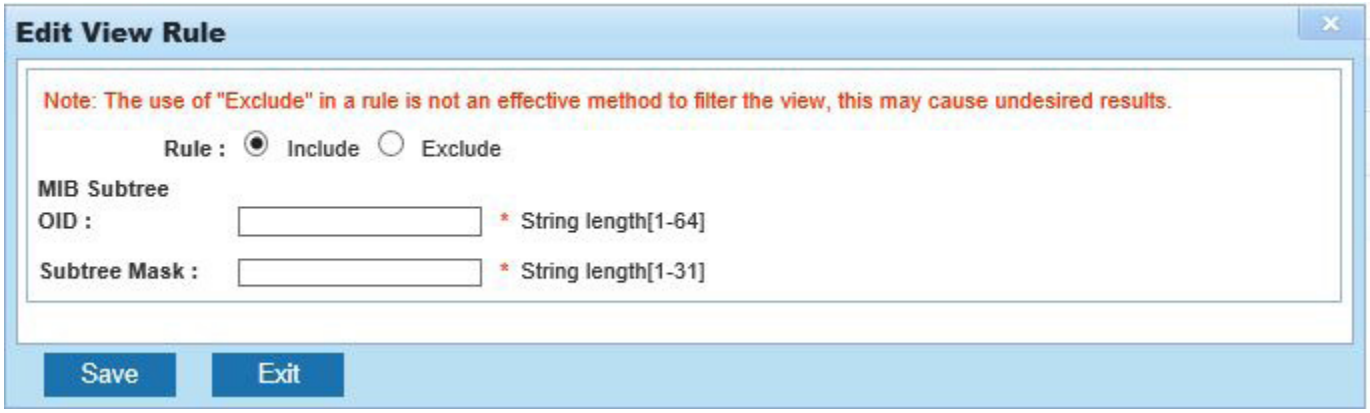


Figure 13.5: Adding or Editing a View Rule

Note: *Excluding by using a rule is not an effective method to filter the view. This setting may cause undesired results.*

13.1.7 Group Configuration

Create the SNMP groups to which the view rules will apply.

13. Simple Network Management Protocol (SNMP) Management

13.1.8 Create New SNMP Group

SNMP → SNMP Config → Group Config to configure the SNMP group (Figure 13.6) using the following steps:

1. Select the "New Group" icon to create your SNMP group.
2. Enter the Group Name (limit: 16 characters).
3. Select the security level of the transmitted info that can be viewed (Figure 13.7). Available settings are: no authentication and no encryption, authentication and no encryption, or authentication and encryption.
4. Select the group Read View rule as required. The group will be able to view only information based on the rule settings.
5. Select the Read Write View rule as required. The group will be able to view and manage the switch based on the rule settings.
6. Select the Notify View rule as required. The group will only notified of the view rule configuration selected.
7. Click "Save" to save the SNMP group. Click "Exit" to discard changes.

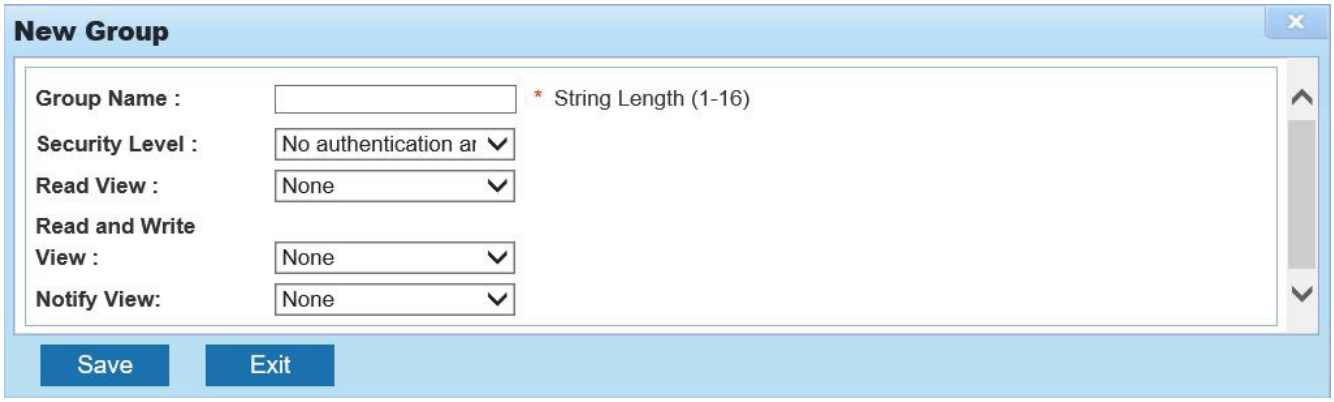


Figure 13.6: New Group

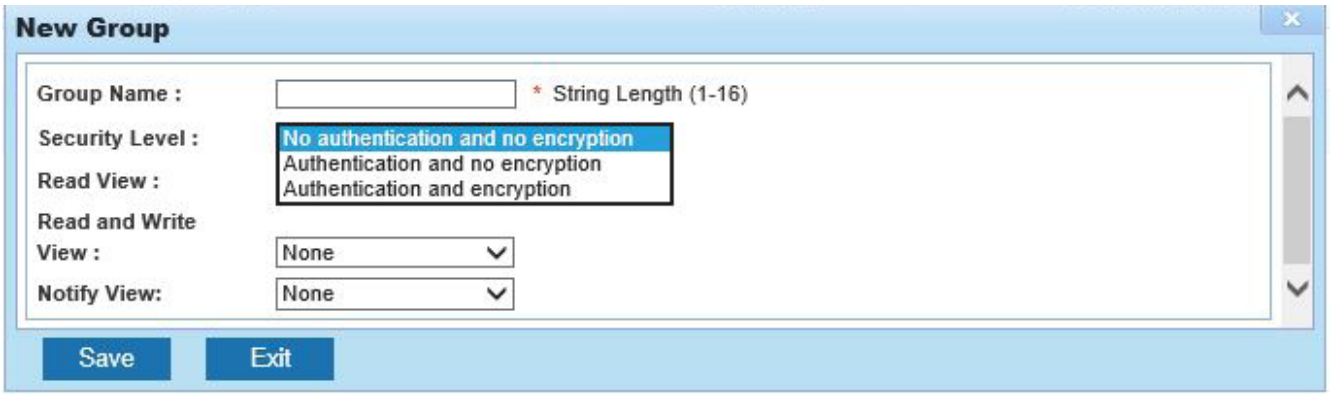


Figure 13.7: New Group Security Level

13.1.9 Edit an SNMP Group

Click the “Edit” icon to edit the group settings. Click “Save” to save edits. Click “Exit” to discard edits (Figure 13.8).

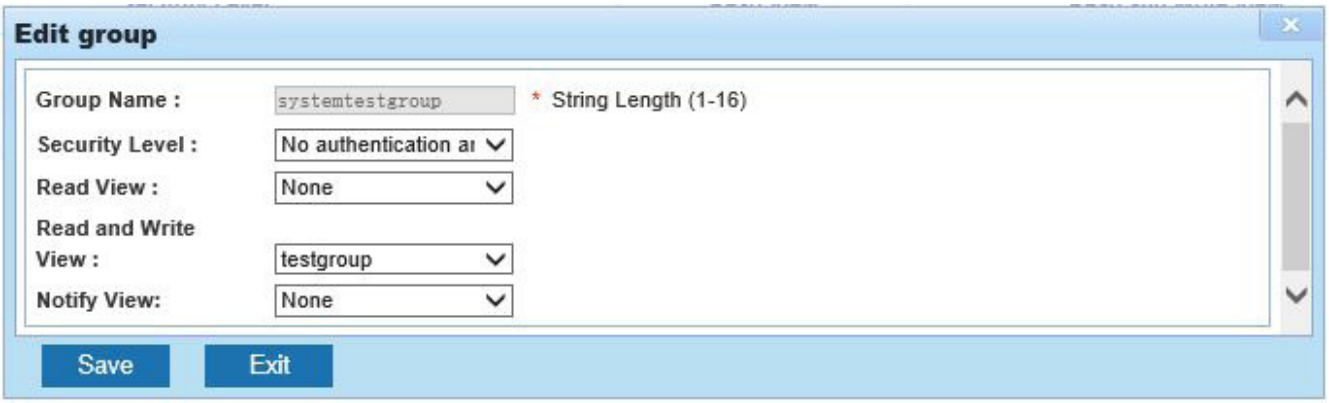


Figure 13.8: Edit Group

13.1.10 Delete an SNMP Group

To delete a single SNMP group, click the red icon or click the checkbox next to the SNMP group and click on the “Delete Selected Group” icon. To delete multiple groups, click the checkbox for each SNMP group to be deleted and click the “Delete Selected Group” icon.

13.1.11 SNMP User Configuration

Select SNMP → SNMP Config → User Config to create the users that will be assigned to the SNMP group, along with their access credentials.

To add a new SNMP user, click on the “New User” icon, then follow the steps below (Figure 13.9):

1. User Name – Enter the user name (limit: 16 characters).
2. Security Level – Enter the security level of no authentication and no encryption, authentication and no encryption, or authentication and encryption.
3. Group Name – Select the group name to which the user will be assigned from the drop-down box.
4. Authentication Mode – When authentication is required, select the correct mode of MD5 or SHA authentication.
5. Authentication Password – Enter the authentication password.
6. Confirm Authentication Password – Re-enter the authentication password for confirmation.
7. Encrypt Mode: When Encryption is selected, select the appropriate mode of DES or AES encryption.
8. Encryption Password – Enter the Encryption password.
9. Confirm Encryption Password – Re-enter the encryption password.
10. Click “Save” to add the new SNMP user. Click “Exit” to discard the changes.

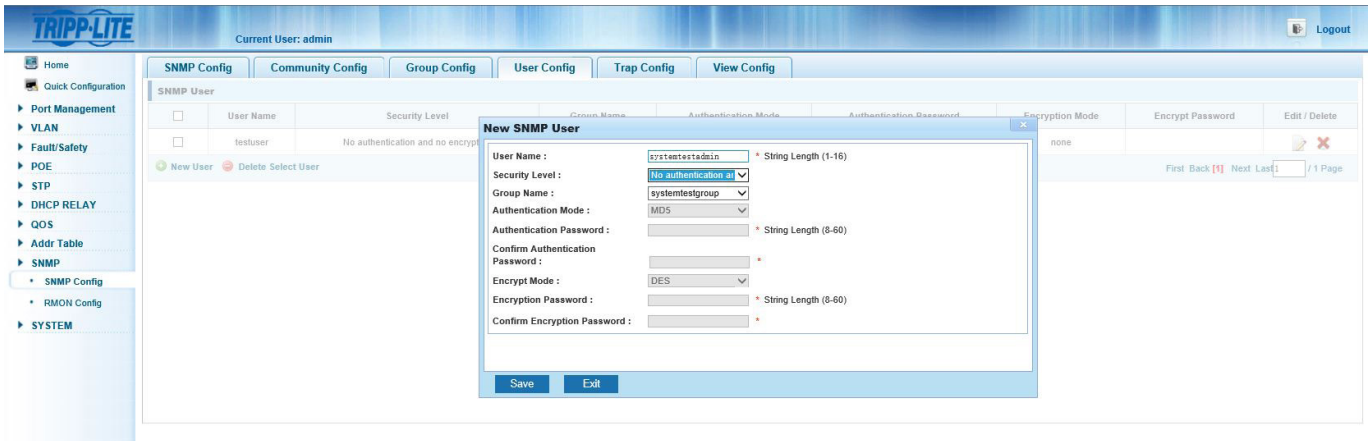


Figure 13.9: Add New SNMP User

13. Simple Network Management Protocol (SNMP) Management

To edit an SNMP user configuration, click the “Edit” icon to make changes (Figure 13.10). Click “Save” to save changes. Click “Exit” to discard changes.

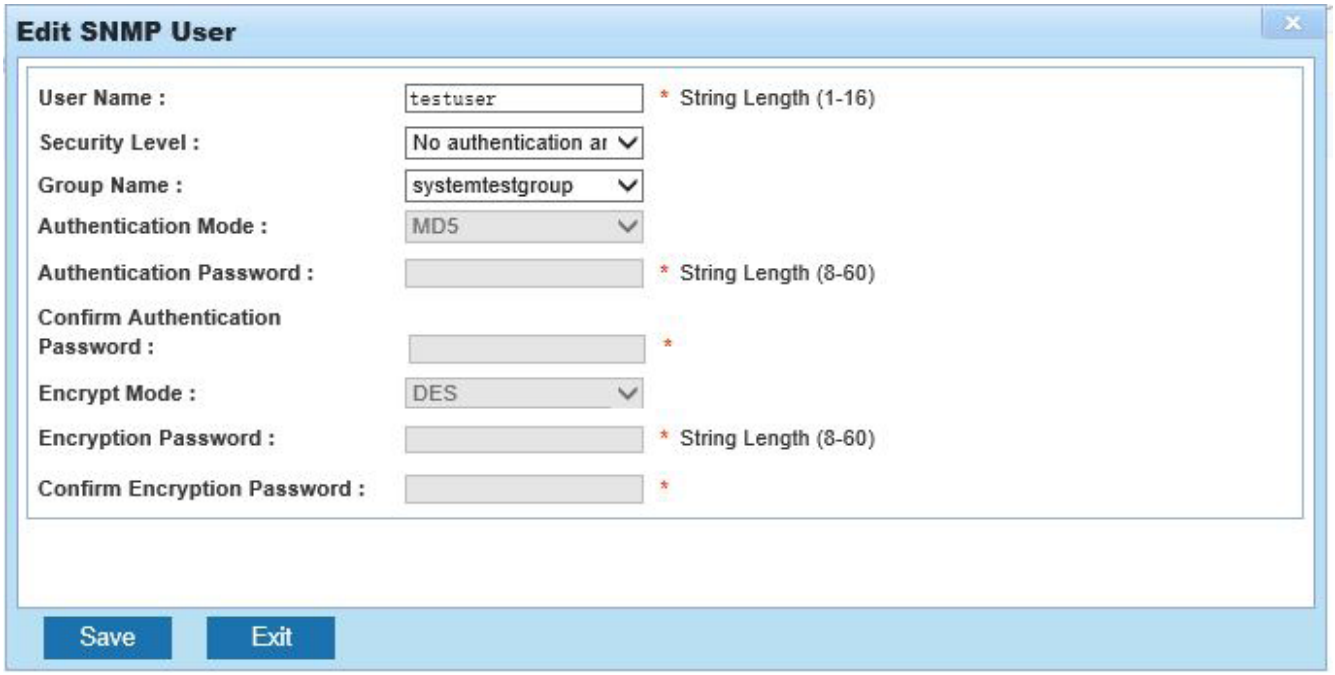


Figure 13.10: Edit SNMP User

To delete an SNMP user, click on the red delete icon next the user name to be deleted, or click the checkbox next to the user name and click the “Delete Select User” icon. Once confirmed, the SNMP user will be deleted. To delete multiple users, click the checkbox next to each of the users to be deleted, then click the “Delete Select User” icon. Once confirmed, the SNMP users will be deleted.

13. Simple Network Management Protocol (SNMP) Management

13.1.12 SNMP Trap Configuration

To set the destination for SNMP traps sent by the switch, click on the “New Trap” icon to enter the host receiver for the SNMP traps, then follow the steps below to create a new trap (Figure 13.11):

1. Destination IP – Enter the destination IP address of the trap receiver (if security mode is V1 or V2, click the “Save” icon to add the SNMP trap receiver host).
2. Security Mode – Set the destination security mode to either V1, V2, or V3. This setting must match the security mode of the trap destination host 13.1.6.4 Address Type – The switch only supports sending to IPv4 host destinations.
3. Security Name – If SNMP v3 security mode is selected, select the SNMP user from the drop-down list.
4. UDP Port Number – Default port is 162 and cannot be changed.
5. Click “Save” to save the Trap Destination Host. Click “Exit” to cancel changes.

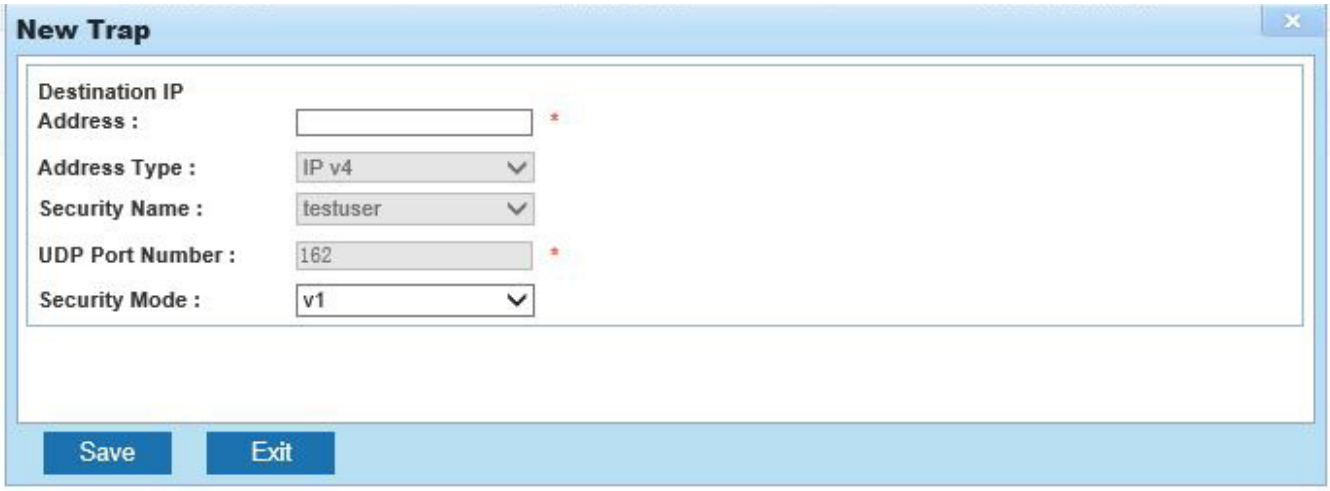


Figure 13.11: New Trap

To edit a Trap Destination Host configuration, click the “Edit” icon to make the needed changes (Figure 13.12). Click “Save” to save changes. Click “Exit” to discard changes

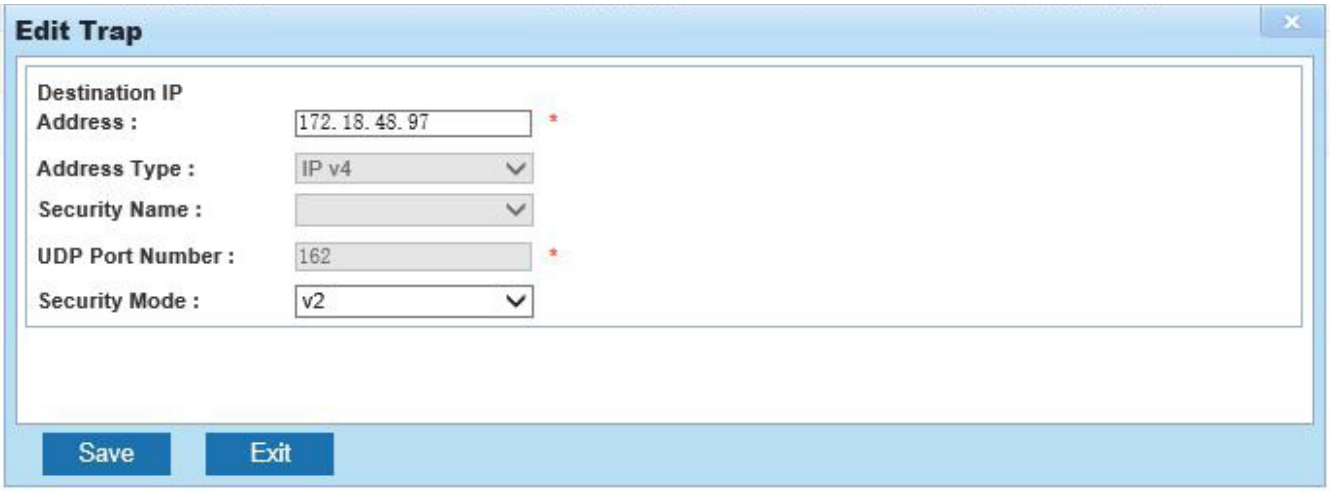


Figure 13.12: Edit Trap

To delete a trap destination host, click on the red ✖ delete icon next the host name to be deleted, click the checkbox next to the host name and click the “Delete Selected Trap” icon. Once confirmed, the trap destination host will be deleted. To delete multiple trap destination hosts, click the checkbox next to each of the entries to be deleted, then click the “Delete Select User” icon. Once confirmed, the selected trap destination hosts will be deleted.

13. Simple Network Management Protocol (SNMP) Management

13.2 Remote Monitoring Configuration Settings

Remote Monitoring (RMON) allows you to monitor network traffic and provide network statistics for Ethernet networks. The switch has the RMON probe embedded into its circuitry. The function is available through the SNMP → RMON Config option.

Note: *SNMP must be enabled to configure RMON.*

13.2.1 Statistics Group

To set up a Statistics Group Configuration (Figure 13.13), click on the "New Count Group" icon, then follow the steps below:

1. Index – Enter the index number within the value range of statistical information table from 1 ~ 65535.
2. Interface Name – Select the interface source port.
3. Owner – Set the table creator (limit: 30 characters).
4. Click "Save" to save settings. Click "Exit" to discard settings.

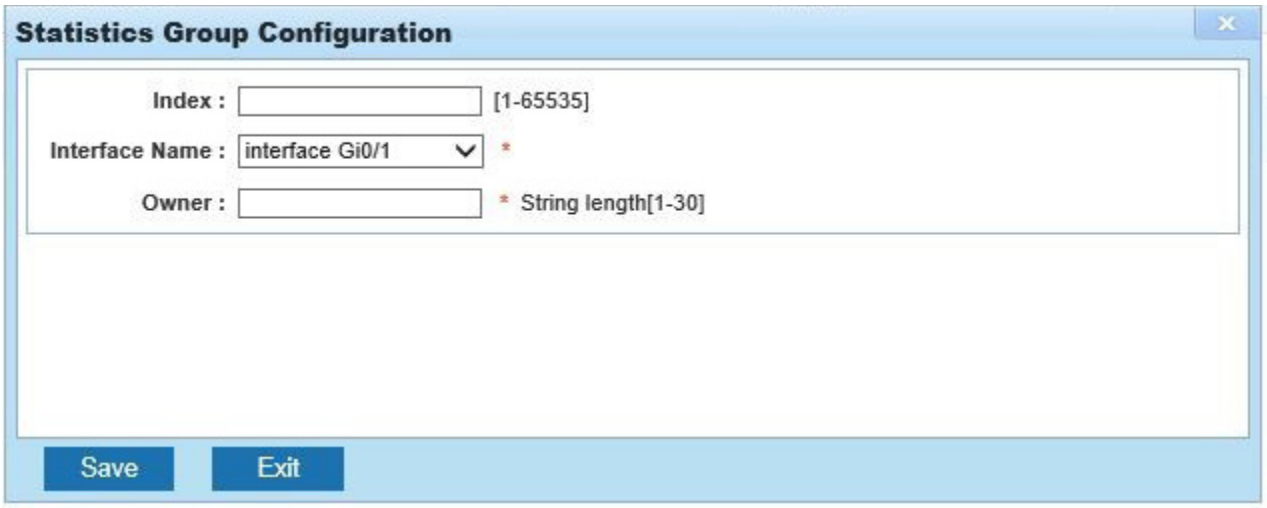


Figure 13.13: Statistics Group Configuration

To edit a Statistics Group configuration (Figure 13.14), click the "Edit" icon to make the needed changes. Click "Save" to save changes. Click "Exit" to discard changes.

Figure 13.14: Edit Statistics Group

To delete a statistics group configuration, click on the red icon next the statistics group entry to be deleted, or click the checkbox next to the entry and click the "Delete Selected Statistics Group" icon. Once confirmed, the statistics group entry will be deleted. To delete multiple statistics groups, click the checkbox next to each of the entries to be deleted, then click the "Delete Selected Statistics Group" icon. Once confirmed, the selected Statistics Group entries will be deleted.

13. Simple Network Management Protocol (SNMP) Management

Click the "View Link" icon of a statistics group entry to view its statistical information (Figure 13.15).

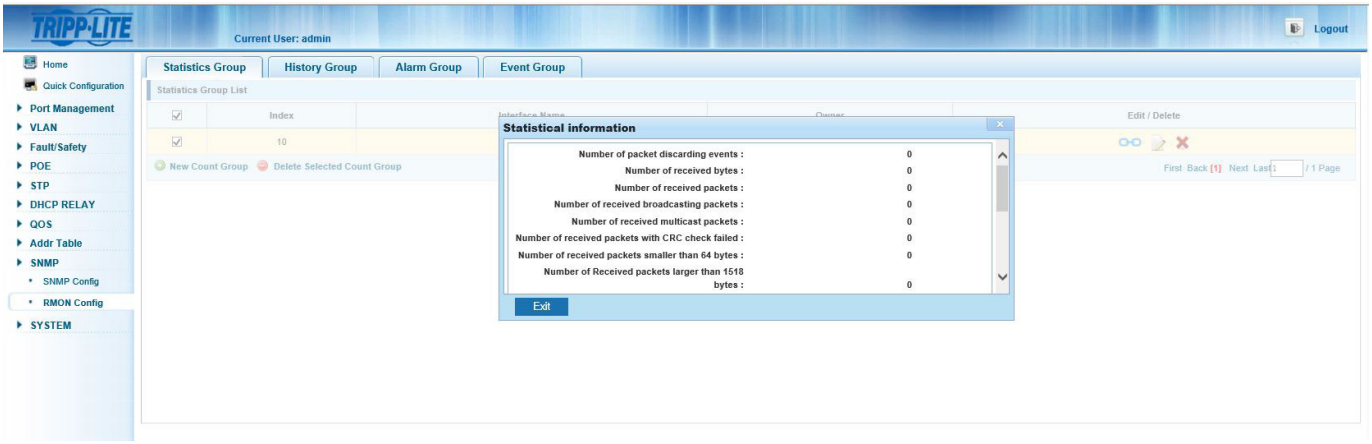


Figure 13.15: Statistical Information

13.2.2 History Group

A history group records the history of Ethernet interface information. To set up a history group, click on the "New History Group" icon, then follow the steps below (Figure 13.16):

1. Index – Enter the required index number within the value range of the statistical information table from 1~65535.
2. Interface Name – Select the required interface source port.
3. Maximum Number of Samples – Enter the required number of samples to record within the value range of 1~65535.
4. Sample Period – Enter the seconds that it will gather the samples from 5~3600 seconds.
5. Owner - Set the table creator (limit: 30 characters).
6. Click "Save" to save settings. Click "Exit" to discard settings.

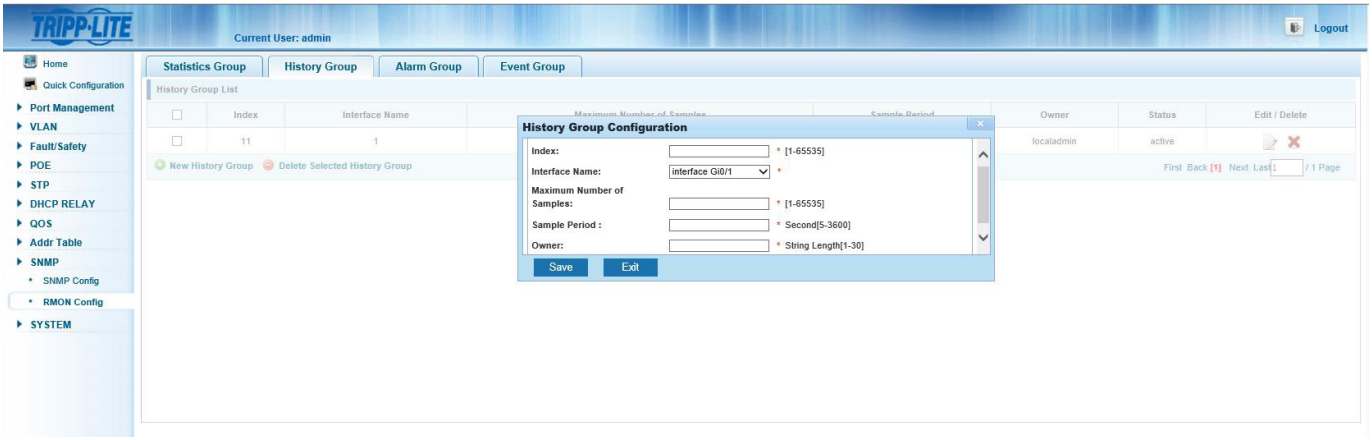


Figure 13.16: New History Group

13. Simple Network Management Protocol (SNMP) Management

To edit a History Group configuration, click the “Edit” icon to make changes (Figure 13.17). Click “Save” to save changes or “Exit” to discard.

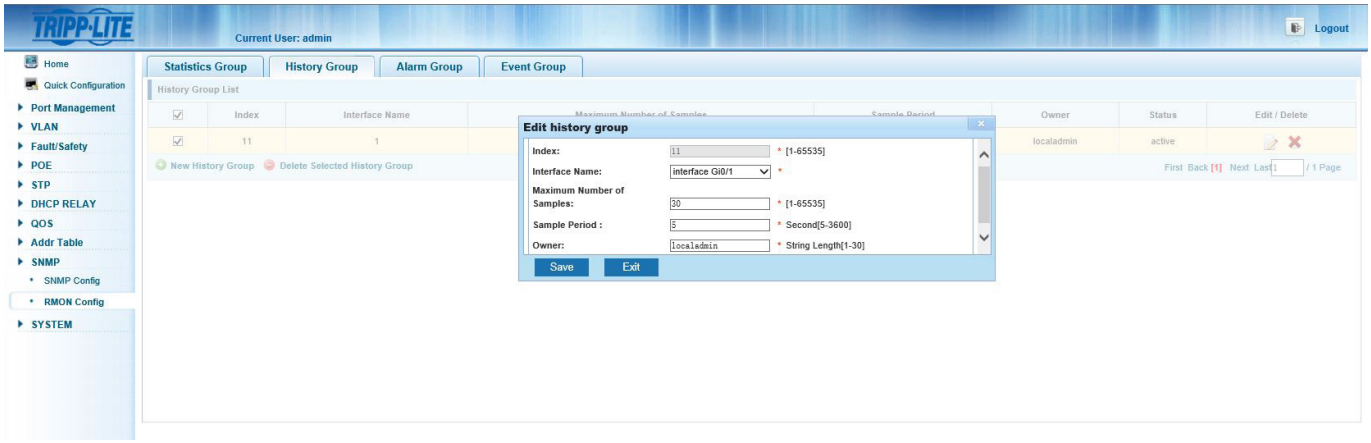


Figure 13.17: Edit History Group

To delete a history group configuration, click on the red ✖ icon next the history group entry to be deleted, or put a checkmark in the box next to the entry and click the “Delete Selected History Group” icon. Once confirmed, the history group entry will be deleted. To delete multiple history groups, click the checkbox next to each of the entries to be deleted, then click the “Delete Selected History Group” icon. Once confirmed, the selected history group entries will be deleted.

13.2.3 Event Group

The Event Group defines event triggers and allows you to set alarms to record them. To configure, go to SNMP → RMON Config → Event Config, then follow the steps below (Figure 13.18):

1. Index – Enter the index number within the value range of 1~65535.
2. Description – Enter the description of the event group (limit: 30 characters).
3. Owner – Enter the owner of the Event Group (limit: 30 characters).
4. Action – Enter a checkmark to log the event, send an SNMP trap for the event or both.
5. Click “Save” to add the event group to the list. Click “Exit” to discard configuration.

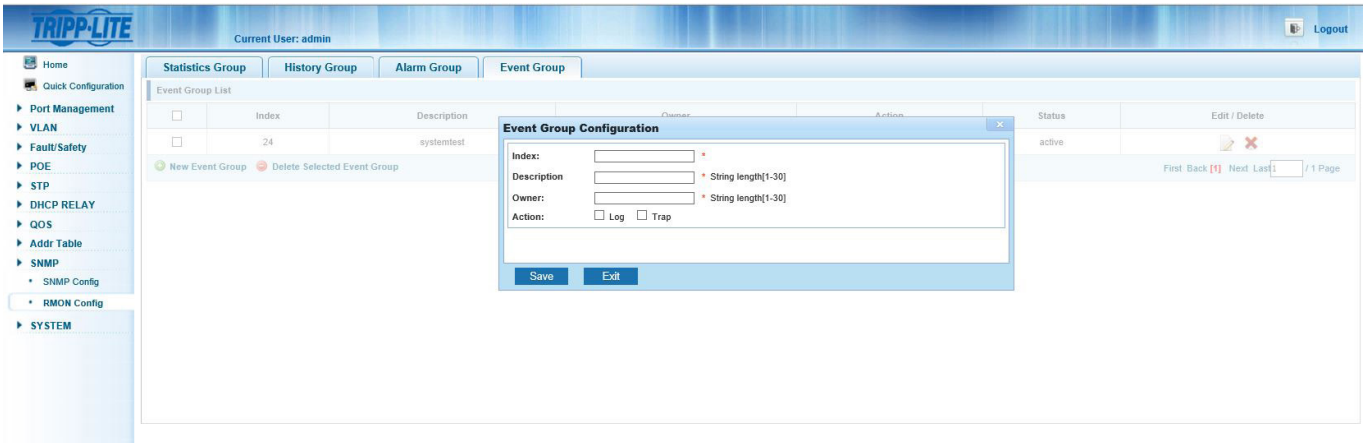


Figure 13.18: New Event Group

13. Simple Network Management Protocol (SNMP) Management

To edit an Event Group configuration, click the “Edit” icon to make changes (Figure 13.19). Click “Save” to save changes or “Exit” to discard.

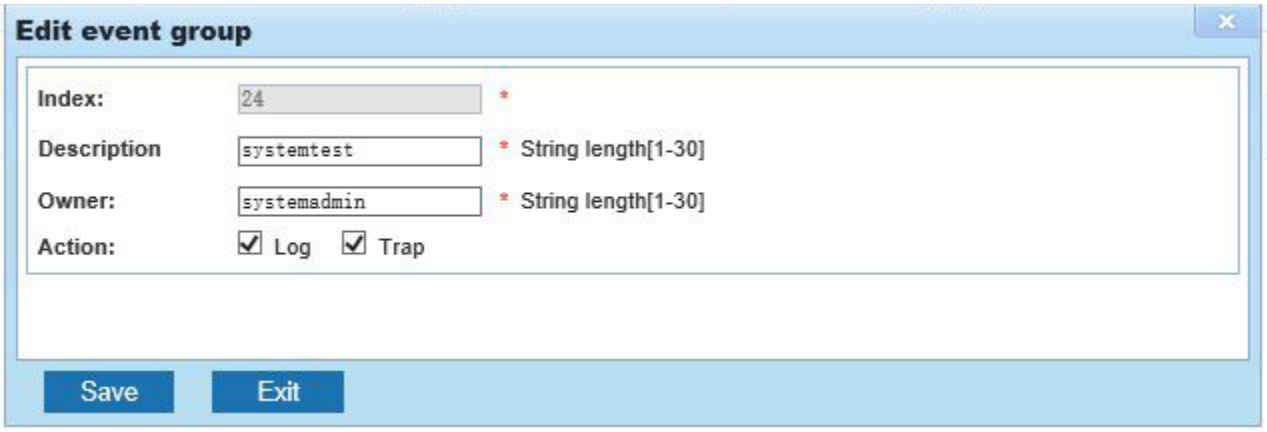


Figure 13.19: Edit Event Group

To delete an event group configuration, click on the red icon next the event group entry to be deleted, or click the checkbox next to the entry and click the “Delete Selected Event Group” icon. Once confirmed, the event group entry will be deleted. To delete multiple event groups, click the checkbox next to each of the entries to be deleted, then click the “Delete Selected Event Group” icon. Once confirmed, the selected event group entries will be deleted.

13.2.4 Alarm Group

To set up an alarm group for specified data traffic events to trigger at upper and lower thresholds, configure the following items (Figure 13.20):

1. Index – Set the alarm list index number from 1~65535.
2. Statistical Event – Set the type of event to trigger an alarm. The event types are: DropEvents, Octets, Pkts, BroadcastPkts, MulticastPkts, CRCAlignErrors, UndersizePkts, OversizePkts, Fragments, Jabbers, Collisions, Pkts64Octets, Pkts65to127Octets, Pkts128to255Octets, Pkts256to511Octets, Pkts512to1023Octets and Pkts1024to1518Octets.
3. Statistical Group Index – Enter the corresponding statistic Group Index number to monitor the port number.
4. Sampling Time Interval – Enter the sample time interval between 5~65535 seconds .
5. Sample Type – Choose the sample type of either Absolute or Delta.
6. Owner – Enter the owner's name. Supports 1-30 characters.
7. Upper Alarm Threshold Limit – Enter the amount of data traffic to set the upper threshold limit from 0-2147483647.
8. Upper Alarm Threshold Limit Events – Chose the Event Group that you want to trigger when the upper alarm threshold is reached.
9. Lower Alarm Threshold Limit – Enter the amount of data traffic to set the lower threshold limit from 0-2147483647.
10. Lower Alarm Threshold Limit Events – Chose the Event Group that you want to trigger when the lower alarm threshold is reached.
11. Click "Save" to save configuration. Click "Exit" to discard settings.

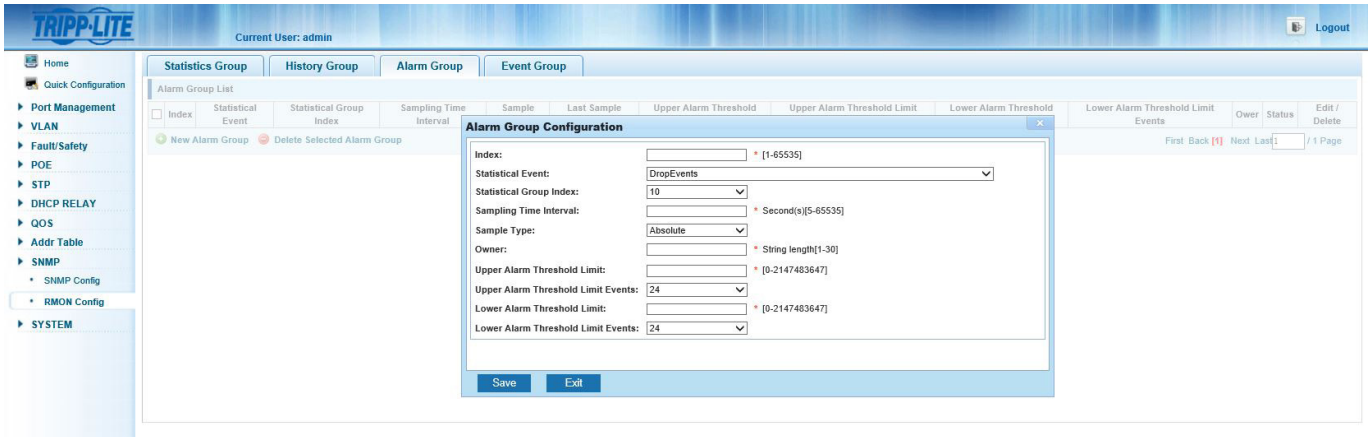


Figure 13.20: New Alarm Group

13. Simple Network Management Protocol (SNMP) Management

To edit an Alarm Group configuration, click the “Edit” icon to make changes (Figure 13.21). Click “Save” to save changes or “Exit” to discard changes.

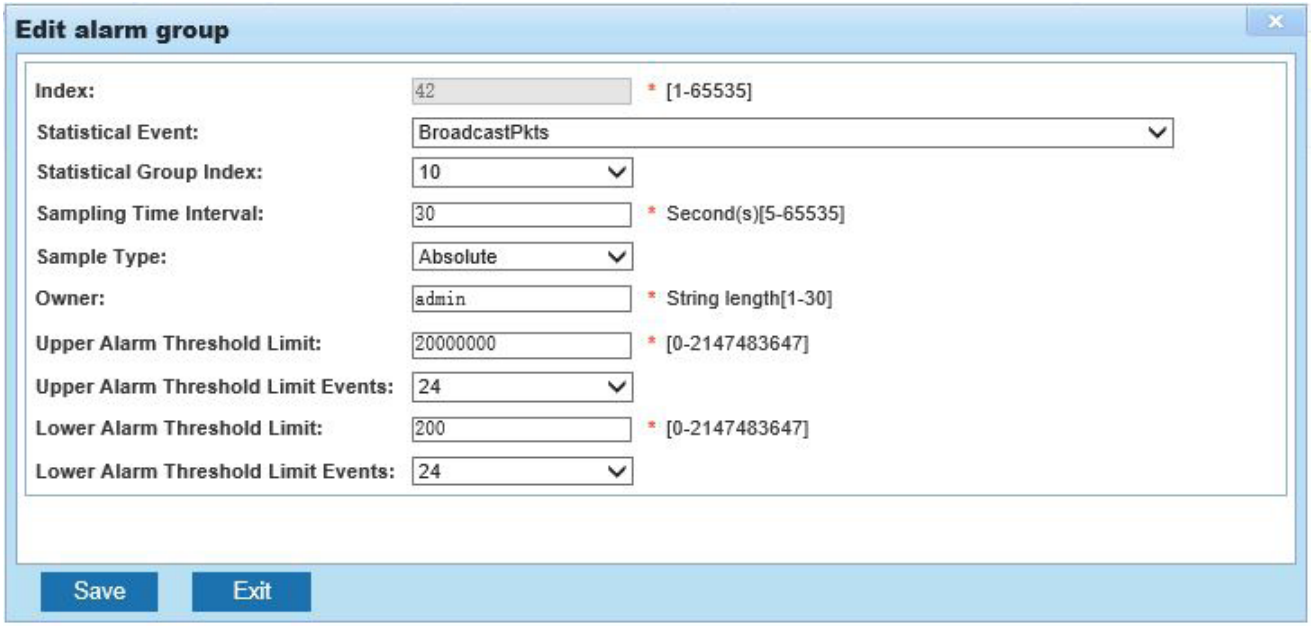


Figure 13.21: Edit Alarm Group

To delete an alarm group configuration, click on the red icon next the alarm group entry to be deleted, or put a checkmark in the box next to the entry and click the “Delete Selected Alarm Group” icon. Once confirmed, the alarm group entry will be deleted. To delete multiple alarm groups, click the checkbox next to each of the entries to be deleted, then click the “Delete Selected Alarm Group” icon. Once confirmed, the selected alarm group entries will be deleted.

14. System Management

The System Settings (Figure 14.1) allow you to set the switch's system configuration; perform system updates; save, back up and restore configurations; save boot-up configurations; set administration privileges and view information about the switch configuration.

14.1 System Configuration

To set the switch configuration and configure the system time, enter the following:

Basic System Information – Enter the required features along with the optional Information updates:

Management VLAN – Select the required Management VLAN from the drop-down list. To select another VLAN to be the management VLAN, it must first be created in the VLAN settings (Section 4.1). Click "Set Management VLAN" when finished.

Management IP – Enter the required management VLAN IP address.

Subnet Mask – Enter the required subnet mask of the management VLAN.

Default Gateway – Enter the gateway IP address if required.

Jumbo Frames – By default, the Jumbo frames are set to 1518. It can be set between 1518 ~ 9216 frames.

DNS Server – Enter the IP address of the DNS server if required.

Login Timeout (Minutes) – By default, the logout timer is set to 30 minutes. It can be set to any time period between 0 and 86400 minutes.

Device MAC – The MAC address of the switch.

Device Name – By default, the model name of the switch is entered, but can be changed to suit the application usage (limit: 32 characters).

Device Location – Enter the switch's device location (limit: 32 characters).

Contacts (included mailbox) – Enter the contacts' email addresses.

Click "Save" to save settings.

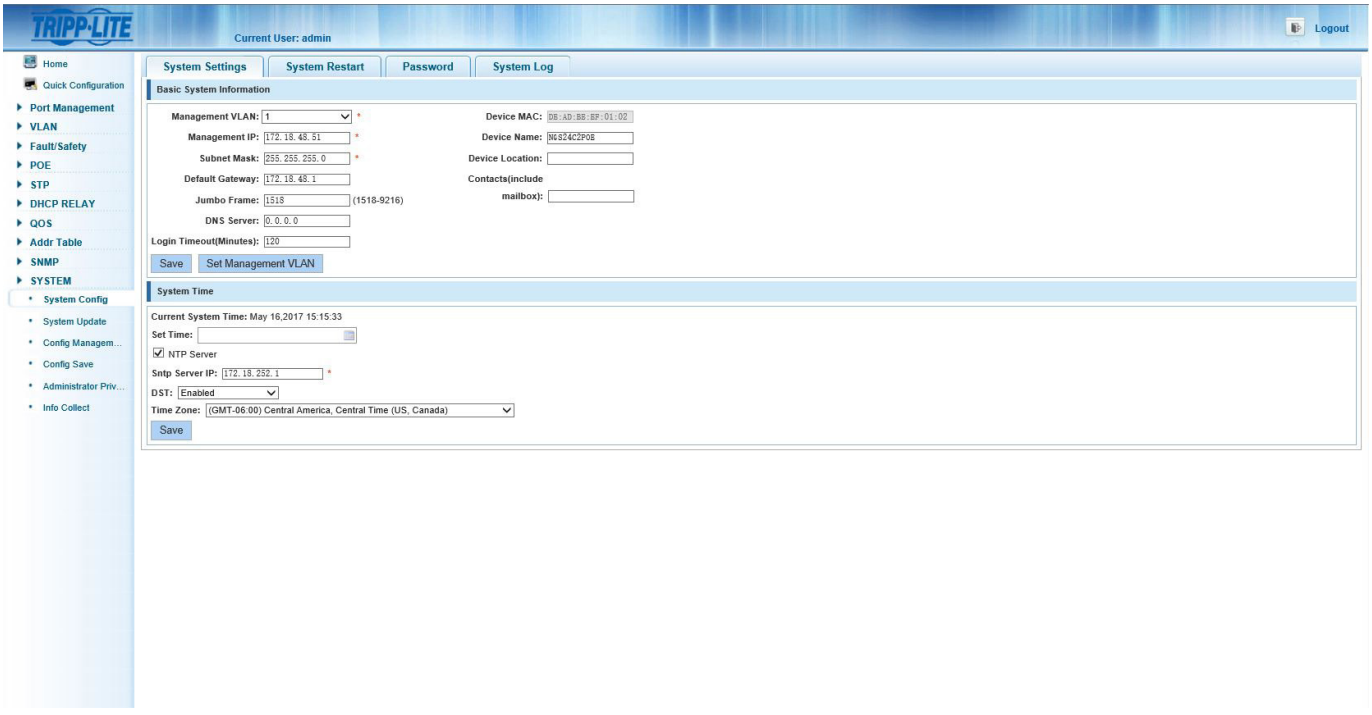


Figure 14.1: System Settings

14. System Management

14.1.1 System Time

System time displays the current System Time, which can be configured manually or be provided automatically by an NTP Server.

Set Time Manually – Enter the set time via the pop-up calendar, set the date and time manually, use the quick selection icon, or click the today button. Click "OK" to keep time settings.

Set Time Via NTP Server – If an NTP Server is used, click the checkbox of the NTP Server box. Next, set the required SNTP Server IP address. If the time zone supports daylight savings time, switch the DST option to Enabled. Then, enter the desired time zone.

Click "Save" to save system time settings

14.1.2 System Restart

To restart the switch, click the "Restart" button. The restart process may take up to one minute. The page will refresh to the login page.

Note: *To ensure your startup configuration is saved before a restart go to SYSTEM → Config Save and click the "Save Settings" button to save the startup configuration.*

14.1.3 Modify Administrator Password

To change the administrator password, enter the old password, followed by the new password. Confirm by re-entering the new password. Click "Save" to save settings. Click "Clear" to discard changes.

14.1.4 System Log Settings

This screen allows you to view and search through the current log information from the switch. If you need to set up a Syslog server to receive logs based on the log level, perform the following steps:

1. Log Switch – Enable logging (default).
2. Server IP – Enter the Syslog Server IP.
3. Send Log Level – Select the log level events to be sent such as Emergencies (0), Alerts (1), Critical (2), Errors (3), Warnings (4), Notifications (5), Informational (6), or Debugging (7). Click "Save" to save settings.

14.2 System Updates

The System Upgrade tab (Figure 14.2) allows for system firmware updates. The current firmware version is displayed at the top of the section. Click the browse button to get firmware updates. Click "Start Upgrade" when ready. The system will reboot back to the login screen when complete.

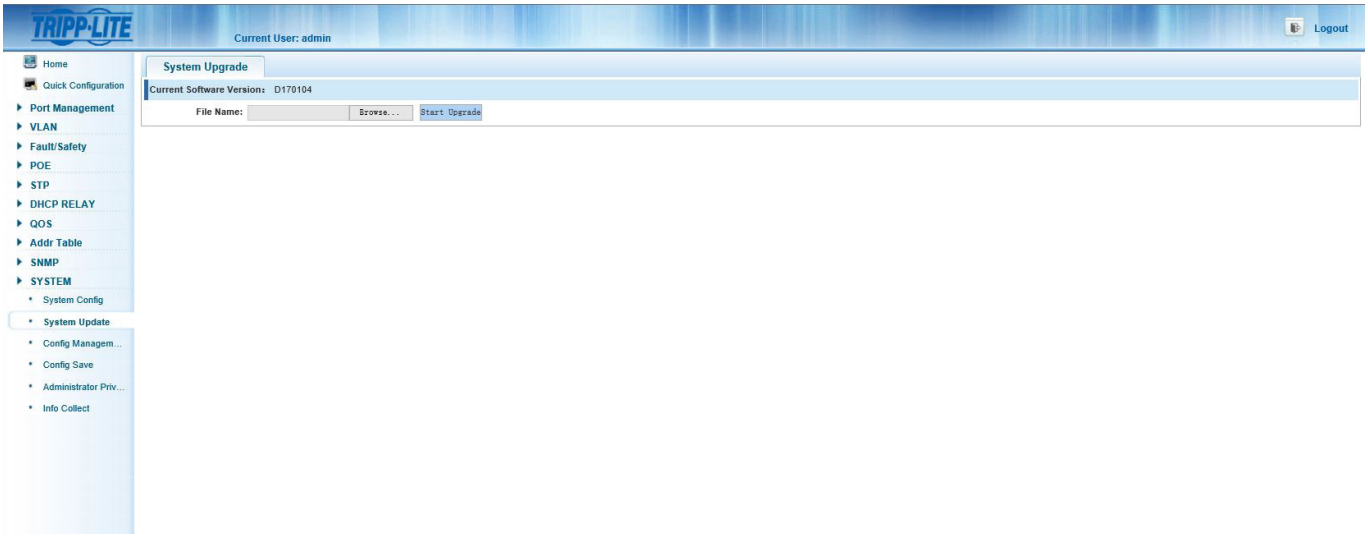


Figure 14.2: System Updates

14. System Management

14.3 System Configuration Management

14.3.1 Import/Export Configuration

This section allows you to import and export system configurations, restore previous configurations and perform a factory reset (Figure 14.3).

Figure 14.3: Import/Export Config

14.3.2 Show Current Configuration

To view the current configuration of the switch (Figure 14.4), click the “Show Current Config” button.

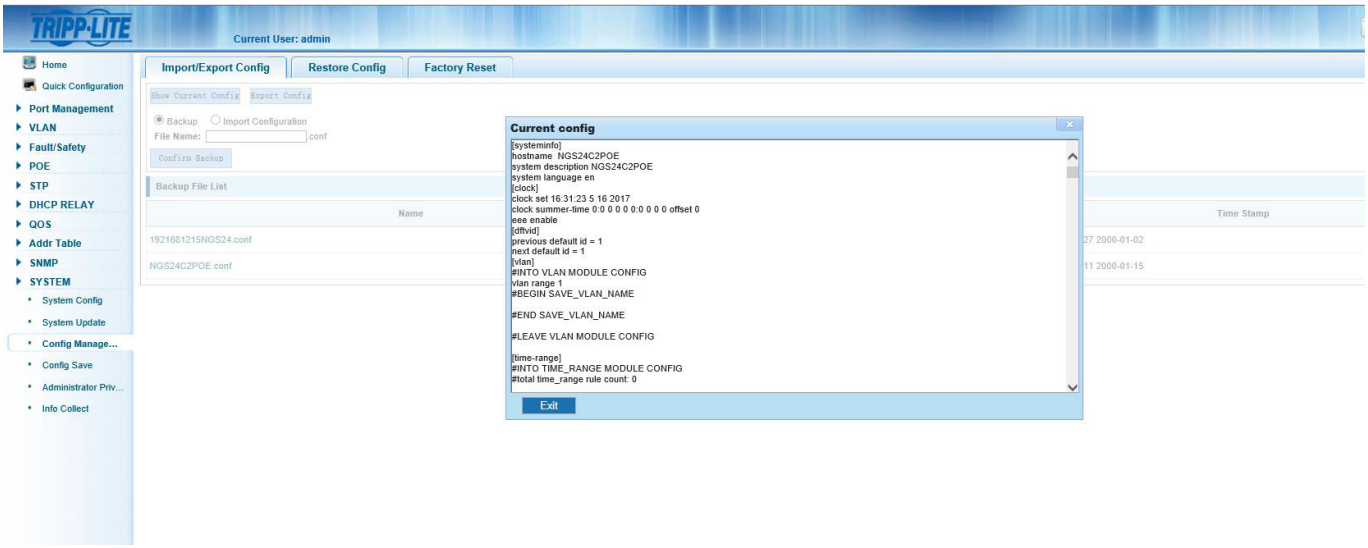


Figure 14.4: Current Configuration

14.3.3 Export Current Configuration

Click the “Show Current Config” button to view the system configuration. Click the “Export” button to save the switch configuration to a local backup system.

14.3.4 Backup Configuration

To save local backups of the configuration file, select “Backup” and enter the filename for the backup. Click “Confirm Backup” to save the configuration. Saved configurations can be viewed in the Backup File List. Up to five backup configuration files can be saved.

14.3.5 Import Configuration

Select “Import Configuration” then browse to the exported configuration file to be imported. Click the “Import Configuration” button. To enable the configuration, select “Restart Device”.

14.3.6 Restore Configuration

Allows you to manage saved backup configuration files.

14.3.7 Restore Backup

To restore a saved configuration, select the name of the configuration you want to restore. Click “Confirm Recovery” to restore the configuration to the system (Figure 14.5).

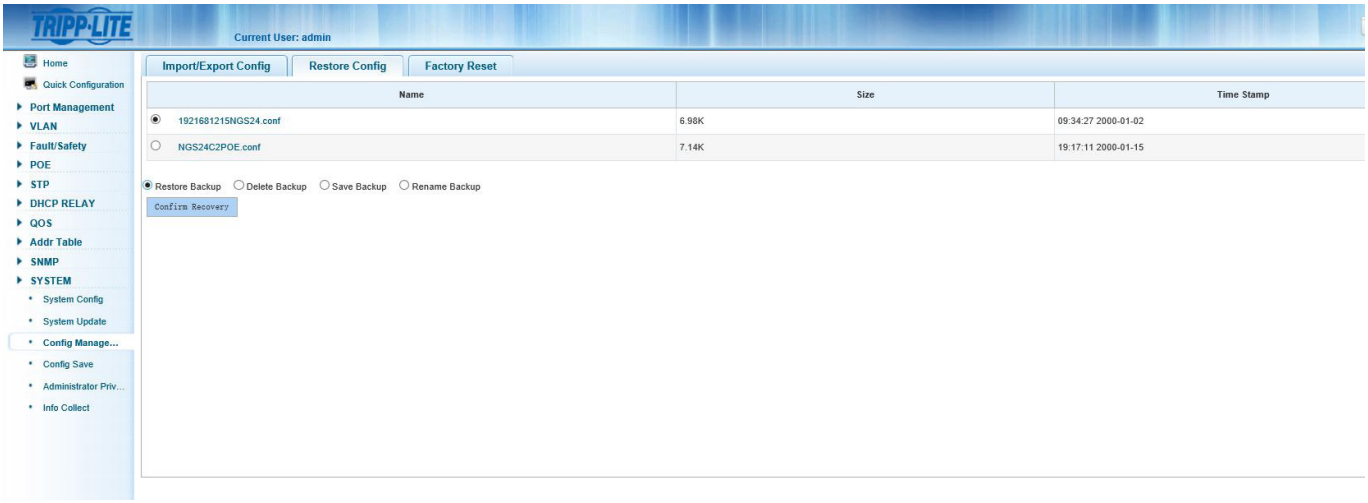


Figure 14.5: Restore Backup

14.3.8 Delete Backup

To delete a configuration backup that is no longer needed, select the name of the configuration file. Select the “Delete Backup” option. Click “Confirm Delete” to remove the configuration file from the system (Figure 14.6).

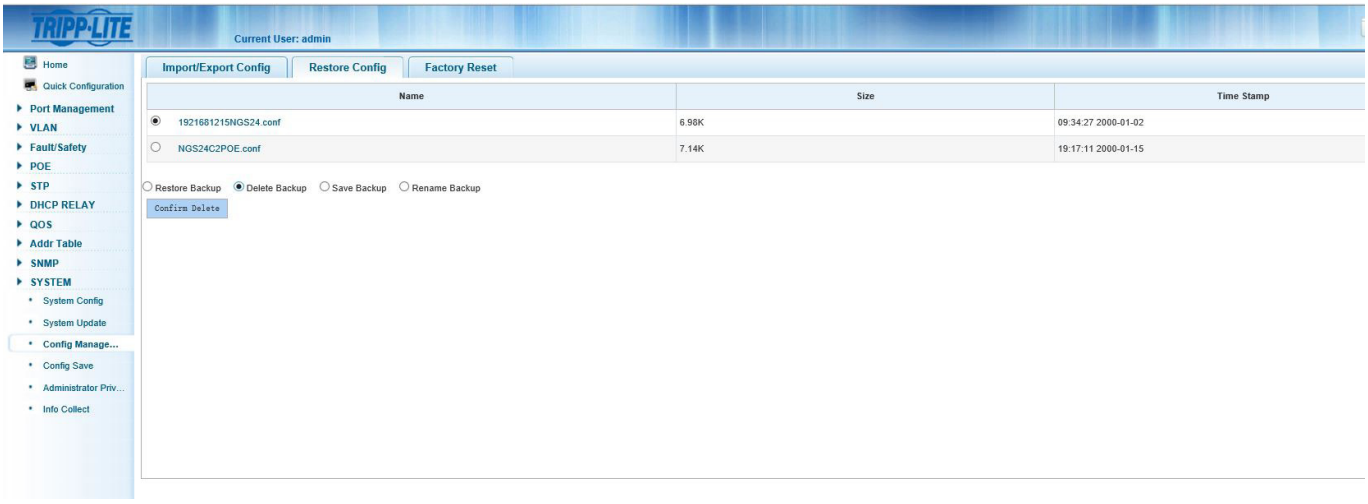


Figure 14.6: Delete Backup

14.3.9 Save Backup

When you restore, delete or rename a backup, choose “Save Backup” to save the current configuration. Click the “Confirm Save” to save configuration settings (Figure 14.7).

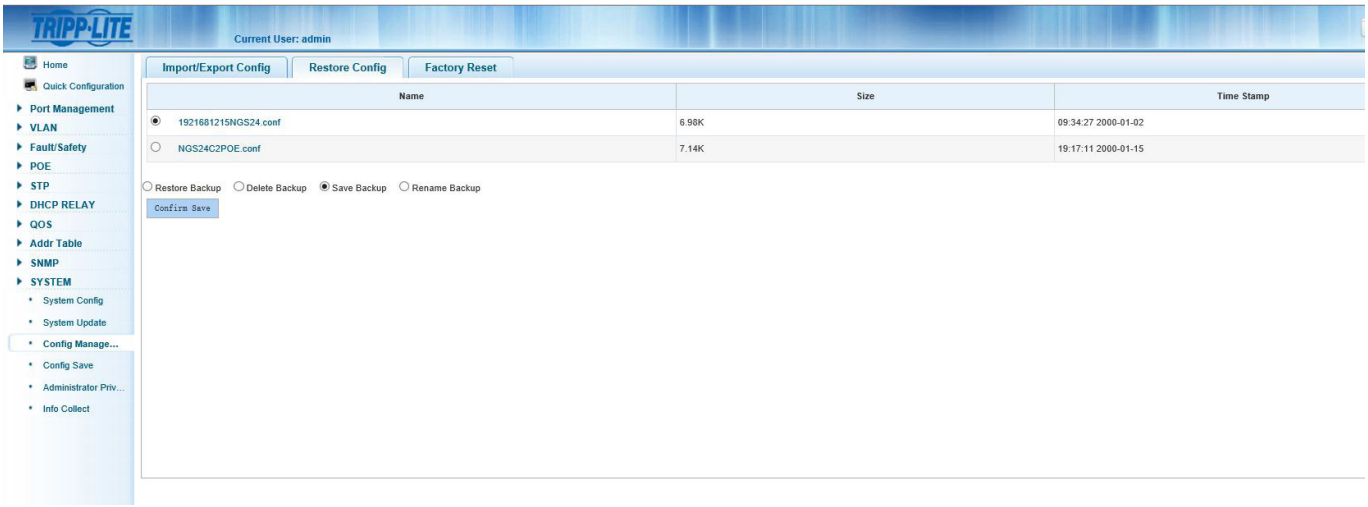


Figure 14.7: Save Backup

14.3.10 Factory Reset

To return the switch to the original factory configuration, select SYSTEM → Config Management → Factory Reset. Clicking on “Factory Reset” will remove all saved configurations from the system and restore the switch back to factory default settings (Figure 14.8).

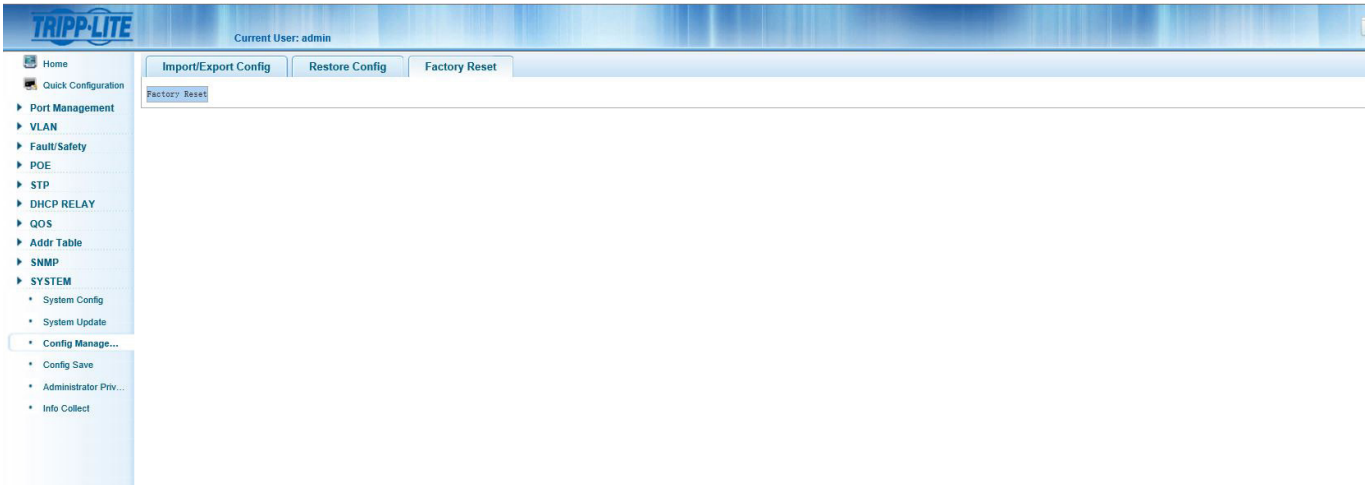


Figure 14.8: Factory Reset

14. System Management

14.4 Configuration Save

To save your start-up configuration, click the “Save Settings” button (Figure 14.9).

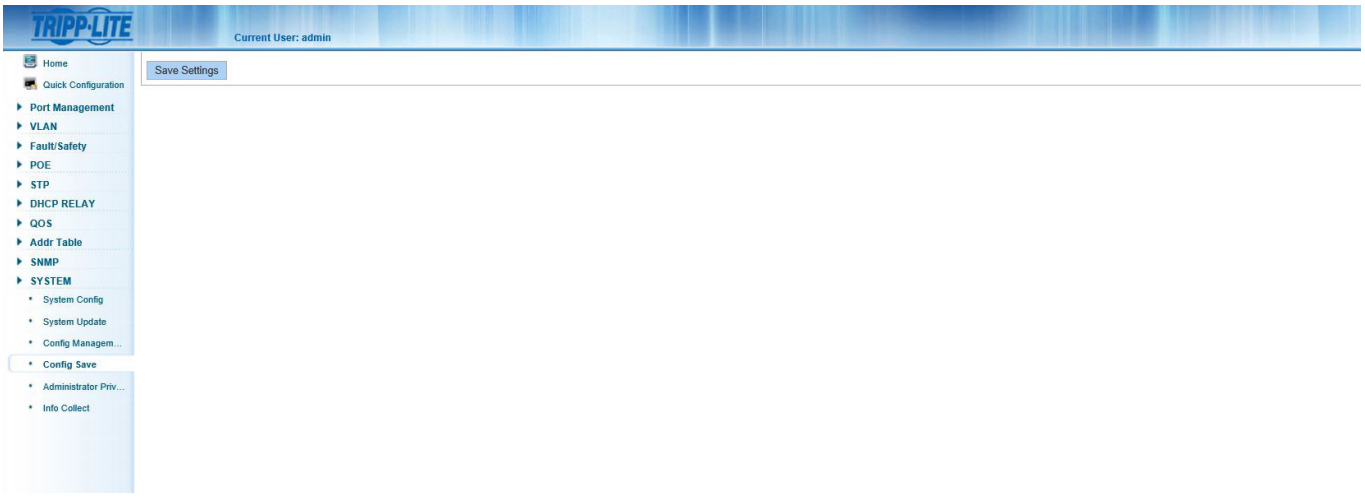


Figure 14.9: Config Save

14.5 Administrator Privileges

This section allows the administrator to add additional users to access the switch (Figure 14.10). A “user” account can log in the Web management system of equipment for routine maintenance. In addition to the admin and user, up to five additional users can be added. Ordinary users can only access the system home page. To create a new user, follow the steps below:

1. User Name – Enter the user name for the new user.
2. New Password – Enter the password for the new user.
3. Confirm Password – Re-enter the password for the new user.
4. Click the “Add User” button to add the new user to the user list.

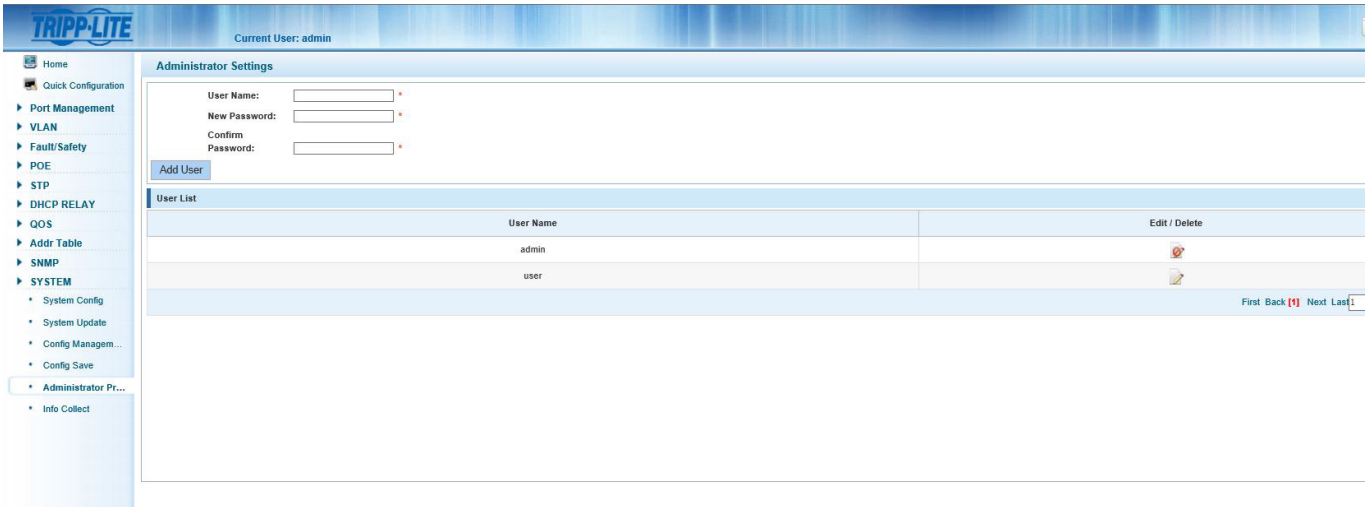


Figure 14.10: Administrator Settings View

14.5.1 Edit User Passwords

To change a user's password, select the user name and click the "Edit" icon (Figure 14.11). A new password for the user can now be created. Click "Confirm Edit" to save the new password. Click "Cancel Edit' to discard changes.

To delete a user, click the red icon to remove the user from the list.

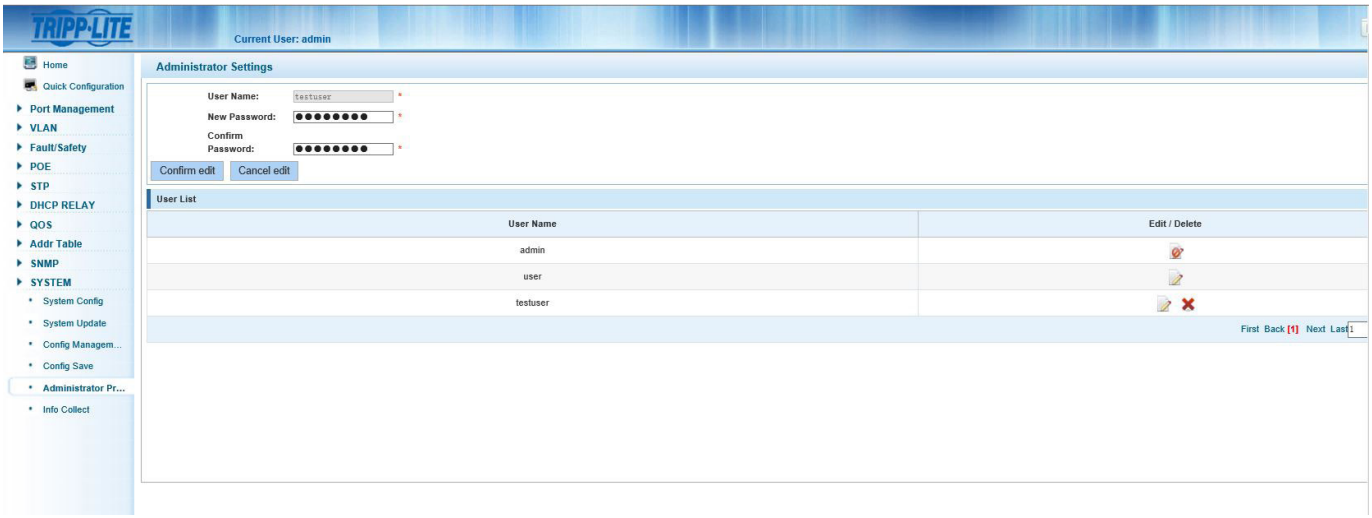


Figure 14.11: Edit User

***Note:** The "Admin" and the original "User" accounts cannot be deleted. The administrator can edit the original user account and can delete any other user accounts created by the Admin account.*

14.6 Info Collect

Click the "Collect" button (Figure 14.12) to create a debug information file with all information about the switch. A pop-up screen will appear allowing the debug information file to be saved to the local system. The debug information file can then be viewed with a text editor such as Notepad, Wordpad, etc.

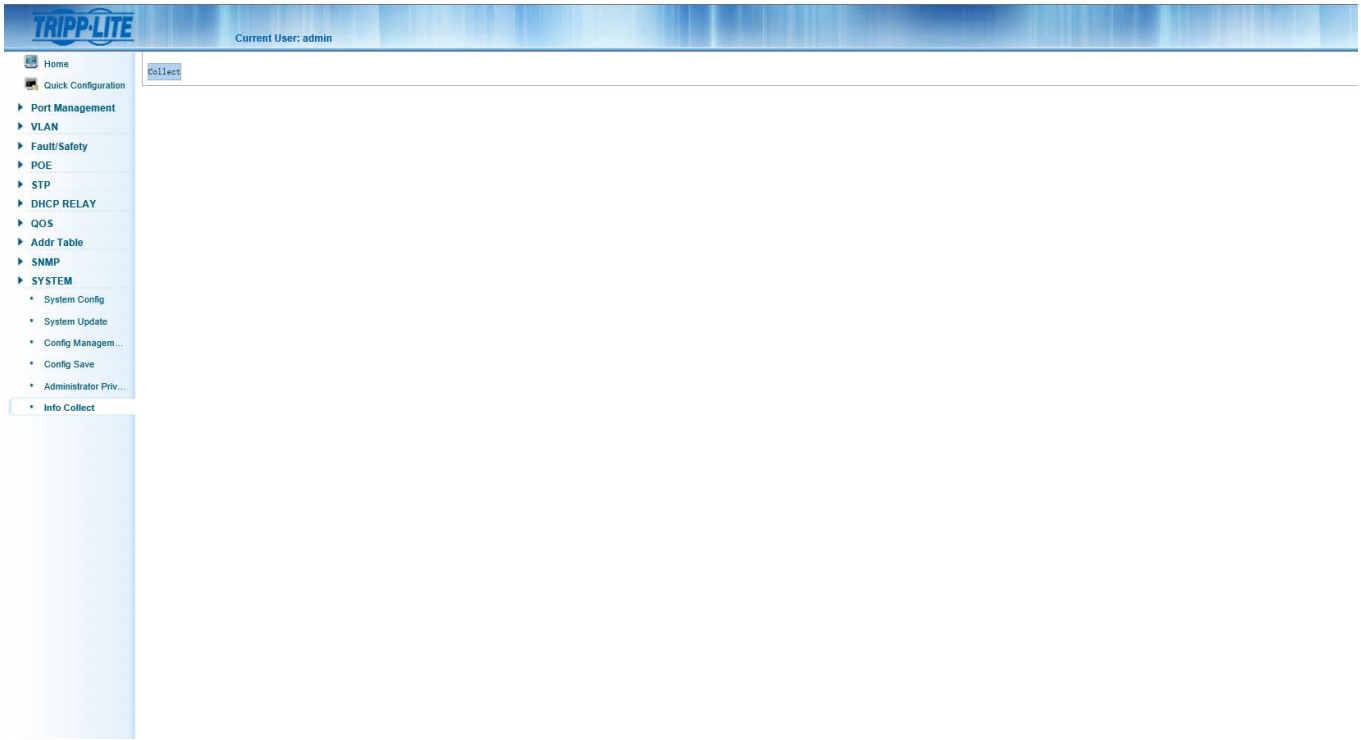


Figure 14.12: Info Collect

15. Troubleshooting

If you encounter a problem:

- Check all connections and confirm they are secure
- Restart the system and see if the problem persists
- Check tripplite.com/support for updates to the software and ensure you are using the most current version that is compatible with your device
- If the problem persists after trying the steps above, contact Tripp Lite Technical Support

16. Technical Support

Before contacting Tripp Lite Technical Support, refer to Section 15. Troubleshooting for possible solutions. If you are still unable to resolve the problem, contact Tripp Lite Technical Support at:

www.tripplite.com/support

Email: techsupport@tripplite.com

Tripp Lite has a policy of continuous improvement. Specifications are subject to change without notice.

Guía de Usuario

Guía para Configuración de Switch Administrado Web-Smart Gigabit L2

(Modelos de Switch Smart de la Serie NGS)

1111 W. 35th Street, Chicago, IL 60609 EE. UU. • www.tripplite.com/support

Índice

Índice

1. Introducción

Esta guía describe cómo configurar modelos del Switch Web-Smart Gigabit L2 (serie NGS) de Tripp Lite mediante la interfaz gráfica de usuario (GUI) incorporada basada en Web. Los modelos de Switch Web-Smart Gigabit L2 de Tripp Lite contienen un servidor de Web incrustado y software para administración y monitoreo de las funciones del switch. La interfaz de administración Web puede usarse para configurar funciones más avanzadas que pueden mejorar la eficiencia del switch y el rendimiento general de la red. El puerto de consola permitirá la interfaz de línea de comandos al switch (uso futuro).

Nota: *Los Switches Web-Smart Gigabit L2 están nombrados como el "switch" en este manual. La información contenida en este documento se aplica a todos los modelos de switch a menos que se indique lo contrario.*

1.1 Configuraciones del Switch

Los switches contienen diferentes cantidades y características de puertos, pero su configuración a través de la interfaz de administración Web es consistente.

Sección 1: Introducción. Contiene el resumen del contenido de todo el manual de configuración.

Sección 2: Configuración para Administración Web. Contiene la configuración inicial que debe tener lugar antes de iniciar sesión en el switch, junto con las instrucciones para iniciar sesión en la interfaz de administración Web del switch.

Sección 3: Página Inicial de la Interfaz de Administración Web. Esta sección lo familiarizará con la interfaz de administración Web.

Sección 4: Configuración Rápida. Muestra cómo configurar rápidamente las funciones de administración a través de la interfaz de red.

Sección 5: Administración de Puertos. Presenta los parámetros usados normalmente para los puertos del switch.

Sección 6: Administración de VLAN. Resumen de la administración y configuración de VLAN(s).

Sección 7: Administración de Fallas / Seguridad. Describe la administarción y la configuración de la seguridad, tales como prevención de ataques, listas de control de acceso, etc.

Sección 8: Administración de Sistema de PoE. Describe la administración y configuración de la Energía sobre la Ethernet [PoE] a través de la interfaz de administración de red (sólo se aplica a switches equipados con PoE).

Sección 9: Administración del Protocolo Spanning Tree [STP]. Describe la gestión de la configuración del Protocolo Spanning Tree [STP] del switch.

Sección 10: Administración del Relevador de DHCP. Cubre la configuración del agente de relevador de DHCP y la configuración de ajustes de la Option82 a un servidor DHCP.

Sección 11: Administración de QoS (Calidad de Servicio). Describe la administración de QoS de cada puerto del switch.

Sección 12: Administración de Tabla de Direcciones MAC. Cubre la administración de la lista de acceso a la tabla de direcciones MAC.

Sección 13: Administración de SNMP. Cubre la configuración de las funciones de administración de SNMP del switch.

Sección 14: Administración del Sistema. Guía para la administración del sistema del switch, incluyendo actualizaciones de software a través de la Página Web, administración de archivos de configuración, etc.

Apéndice I: Configuración Predeterminada. Referencia rápida para la configuración predeterminada de inicio de sesión, contraseña, etc.

Configuración para Administración Web

2.1 Configuración Inicial

2.1.1 Configure la Dirección IP de la Computadora

La dirección IP de la computadora de administración y el switch deben estar configuradas en la misma subred. (La dirección IP predeterminada del switch es 192.168.2.1 y su máscara de subred predeterminada es 255.255.255.0). El Portal de enlace no necesita ser configurado para la configuración inicial del switch.

La dirección IP de la computadora de administración debe configurarse manualmente en el rango de dirección IP 192.168.2.xxx ("xxx" va de 2 a 254).

De forma predeterminada, todos los puertos pertenecen a VLAN1. La computadora de administración puede realizar la configuración del switch accediendo a cualquier puerto.

Nota: *Este manual es apropiado para todos los modelos en la familia de Tripp Lite de switches administrados Web-Smart de la Serie NGS. Esta guía del usuario utiliza una configuración de switch como un ejemplo para ilustrar cómo configurar el switch mediante la interfaz de administración de Web.*

2.1.2 Confirme la Conectividad de Red Entre la Computadora y el Switch

Siga estos pasos para confirmar la conectividad de red entre la computadora y el switch:

Paso 1: Pulse la tecla de Windows + R, a continuación, escriba cmd en el campo de entrada de la ventana de "Ejecutar" y haga click en "Aceptar". Esta forma aparece la ventana de símbolo del sistema (Figura 2.1).

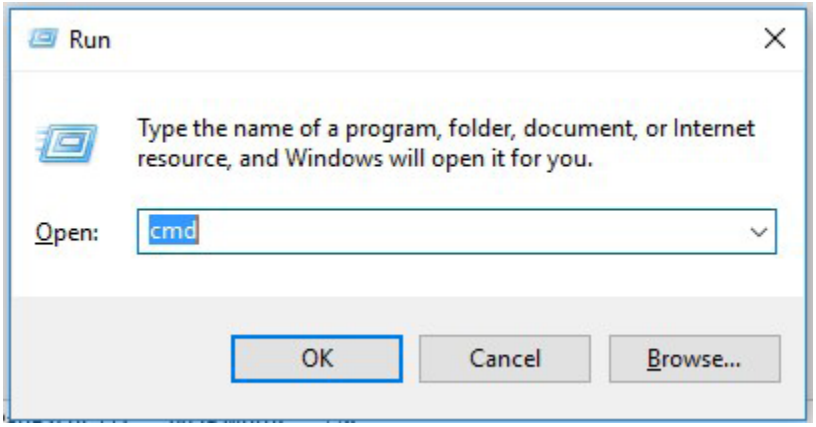


Figura 2.1: Confirmación de la Conectividad de Red

Paso 2: En el cuadro de diálogo de símbolo del sistema, escriba ping 192.168.2.1 luego pulse «Enter». Si se devuelve una respuesta al ping desde el switch, la conectividad de red correcta está establecida. Si no se recibe respuesta, compruebe la conexión de red.

2.1.3 Acceda a la Interfaz de Administración de la Web

Abra un navegador de Web (p.e. Internet Explorer), escriba **http://192.168.2.1** en la barra de dirección, luego pulse «Enter». Entre en la interfaz de Inicio de Sesión de Usuario de la página de administración del switch. En la interfaz de inicio de sesión (Figura 2.2), seleccione el idioma preferido (el idioma predeterminado es inglés), luego ingrese el nombre de usuario y la contraseña. El nombre de usuario y la contraseña predeterminadas son en ambos casos admin (sensible al caso). Haga click en el botón "Ingresar" o presione "Enter" para acceder a la interfaz de administración de Web.

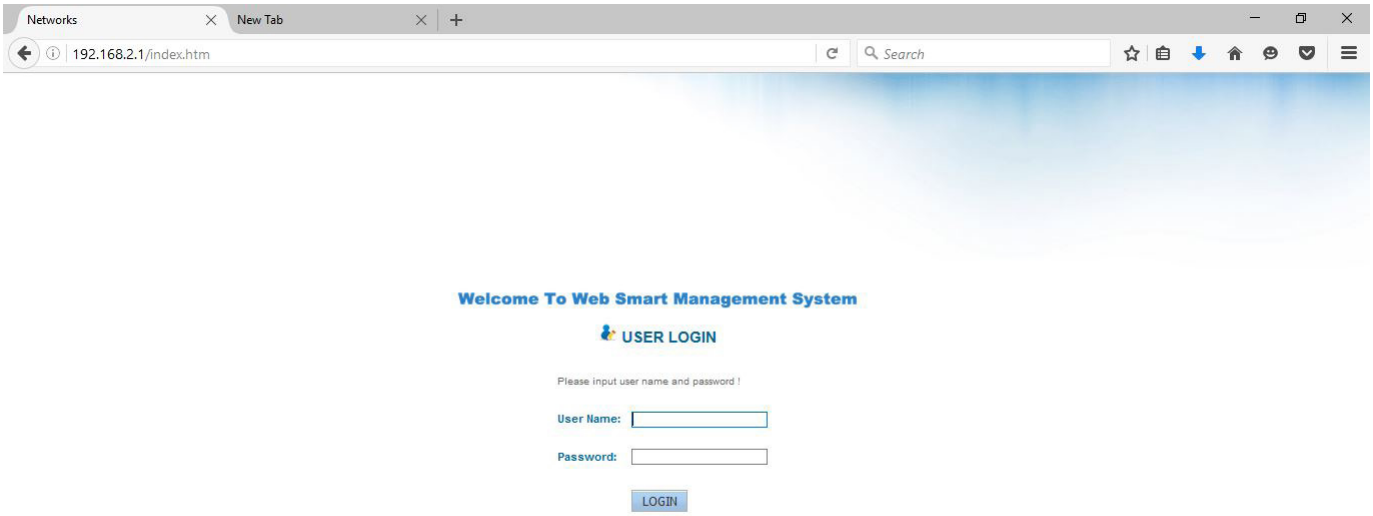


Figura 2.2 Página de Inicio de Interfaz de Inicio de Sesión de Internet

Después de un inicio de sesión exitoso, el navegador mostrará la Página Principal de la interfaz de administración Web correspondiente al switch, como se ilustra en la Figura 2.3:

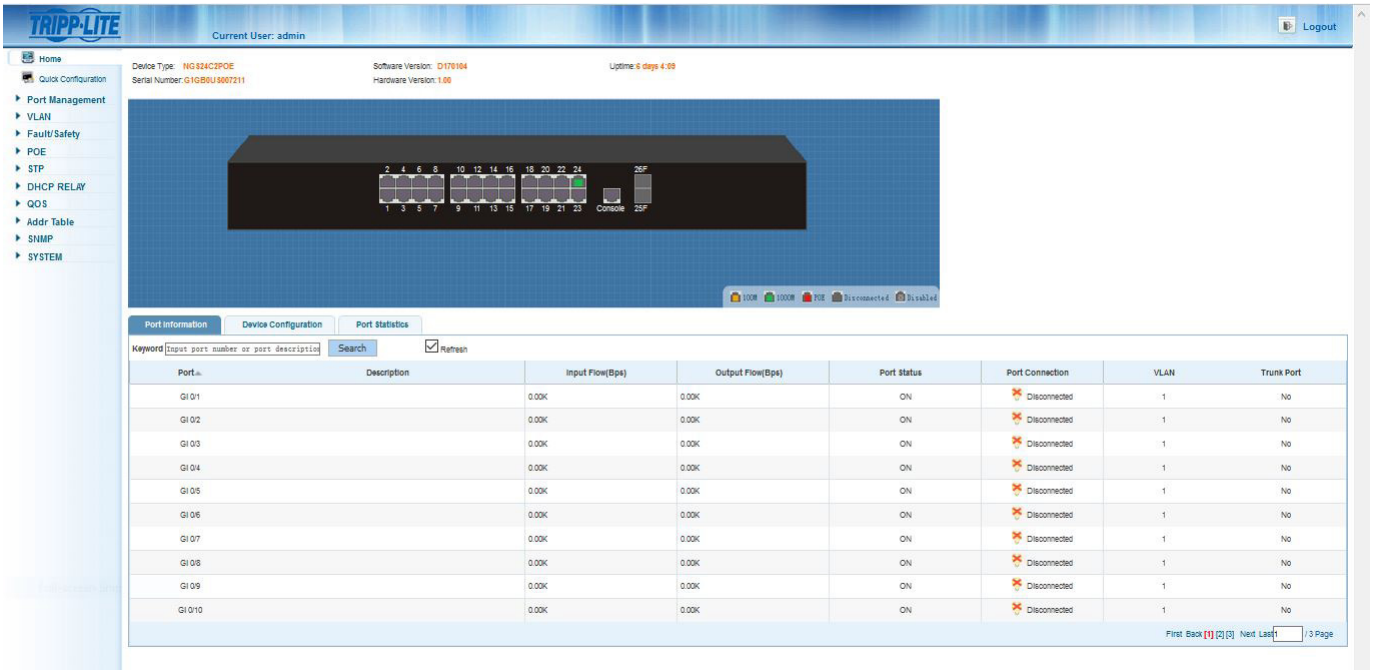


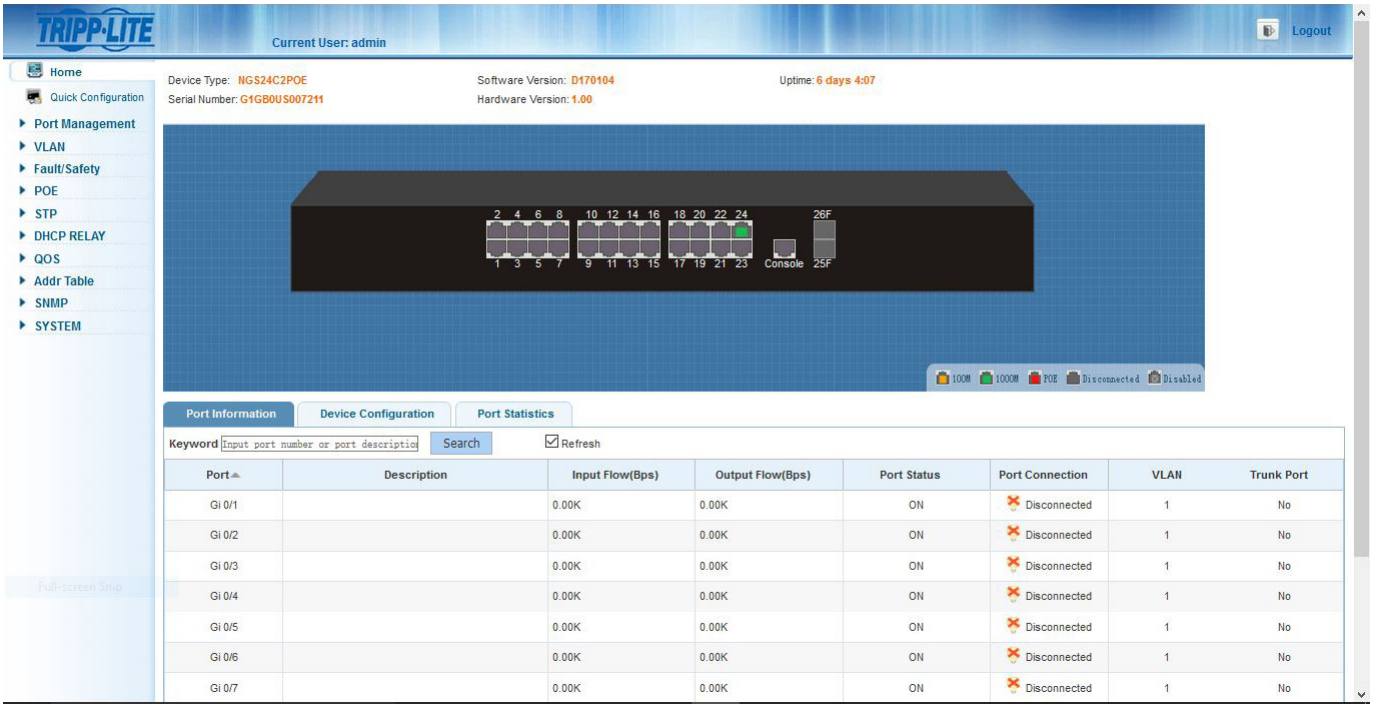
Figura 2.3 Interfaz de Administración Web del Switch (Vista del Administrador)

Notas:

- *Se recomienda utilizar Internet Explorer 8 o superior, Firefox o Chrome con la interfaz de administración de red.*

3. Página Inicial de la Interfaz de Administración Web

3.1 Vista General de la Página de Inicio de la Interfaz de Administración Web



La página de inicio de la interfaz de administración Web muestra el usuario actual, la información del sistema del switch, tiempo de actividad, información del puerto de red, configuración de dispositivos y estadísticas de puertos. El gráfico del switch muestra las conexiones actuales si funciona a 10/100 (naranja), 1000Mbps (verde), PoE activo (rojo), desconectado (gris) o desactivado (gris con X).

3.2 Menús de la Interfaz de Administración Web

Hay 12 opciones del menú principal en la interfaz de administración Web: Inicio de Sistema, Configuración Rápida, Administración de Puertos, VLAN, Fallas / Seguridad, PoE (aplicable sólo a los switches equipados con PoE), STP, RELEVADOR DHCP, QoS, Tabla de Direcciones, SNMP y Sistema.

Cada opción del menú principal contiene un menú secundario. De forma predeterminada, los menús secundarios están ocultos. Haga click en una opción del menú principal para expandir el menú secundario.

- **Página Inicial de la Interfaz de Administración Web**
- **Configuración Rápida**
  - o Parámetros de VLAN
  - o Otros Parámetros
- **Administración de Puerto**
  - o Parámetros Básicos
  - o Agregación de Puerto
  - o Puerto Espejo
  - o Límite de Velocidad del Puerto
  - o Control de Tormenta
  - o Aislamiento del Puerto
- **Administración de VLAN**
  - o Administración de VLAN
- **Administración de Fallas / Seguridad**
  - o Prevención de Ataque
  - o Detección de Ruta

  - o ACL (Lista de Control de Acceso)
- **Administración de Sistema de PoE**
  - o Configuración de PoE
  - o Configuración de Puerto de PoE
- **STP (Protocolo Spanning Tree)**
  - o Región MSTP
  - o Puente STP
- **Relevador de DHCP**
  - o Relevador de DHCP
  - o Option82
- **QoS (Calidad de Servicio)**
  - o Observación de QoS
  - o Configuración de Cola
  - o Mapeo de Colas
- **Tabla de Dirección (Tabla de Direcciones MAC)**
  - o Tabla de Direcciones
- **SNMP**
  - o Configuración de SNMP
  - o Configuración de RMON
- **Sistema**
  - o Configuración de Sistema
  - o Actualización de Sistema
  - o Administración de Configuración
  - o Guardar Configuración
  - o Privilegios Administrativos
  - o Restaurar a Condiciones de Fábrica
  - o Recopilación de Información

Nota: *Si no hay actividad en la interfaz de administración Web durante 30 minutos (valor predeterminado), el sistema automáticamente cerrará la sesión del usuario y volverá a la página de acceso de interfaz de administración Web.*

4. Configuración Rápida

Seleccione "Configuración Rápida" para configurar las funciones del switch utilizadas con frecuencia, como parámetros de VLANs, puertos troncales, sistema de administración y contraseña de la interfaz de administración.

4.1 Agregando VLANs

Seleccione “Configuración Rápida → Parámetros de VLAN” para configurar las VLANs y puertos troncales (Figura 4.1). Puede ver y editar la "Parámetros de VLAN", añadir nuevas VLANs, modificar VLAN y eliminar VLAN(s). Después de configurar la(s) VLAN(s), vaya a la "Parámetros de Troncales" para añadir nuevos puertos troncales.

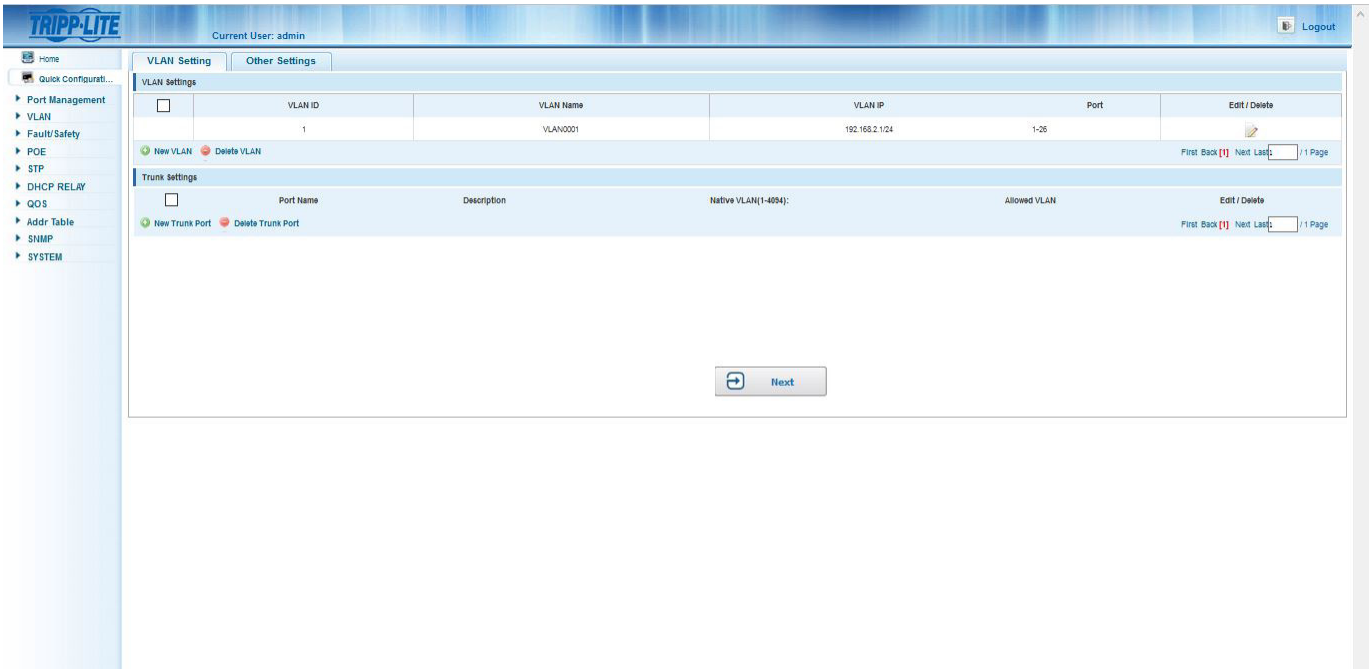


Figura 4.1: Parámetros de VLAN

4.1.1 Agregando Nuevas VLANs

Haga click en el ícono de "Nueva VLAN" e introduzca el nuevo ID de la VLAN, nombre de la VLAN y luego agregue los puertos seleccionados para esa VLAN. Cuando termine, haga click en “Guardar”. Repita estos pasos para crear VLANs adicionales.

4.1.2 Edición de VLANs

Haga click en el ícono "Editar" para cambiar el nombre de la VLAN y los puertos seleccionados para esa VLAN. Cuando termine la edición, haga click en “Guardar”. Repita estos pasos para editar las VLANs adicionales.

4.1.3 Eliminación de VLANs

Para eliminar una VLAN, haga click en el ícono rojo al lado de la VLAN a eliminar o haga click en la casilla de verificación junto a la VLAN asociada y haga click en "Eliminar VLAN". Para eliminar varias VLANs, marque las casillas junto a las VLANs que se eliminarán. Haga click en "Eliminar VLAN" para eliminar las VLANs seleccionadas.

Nota: *Todos los puertos asociados a las VLANs eliminadas regresarán automáticamente a la VLAN 1. No se puede eliminar la VLAN 1.*

4. Configuración Rápida

4.2 Parámetros del Puerto Troncal

Seleccione “Configuración Rápida → Parámetros de VLAN” para administrar los parámetros del puerto troncal. Puede ver la configuración del puerto troncal del switch y añadir nuevos puertos troncales, modificar puertos troncales o eliminar puertos troncales. Después de configurar los "Parámetros del Puerto Troncal", haga click en "Siguiente" para ir a la página de "Otros Parámetros".

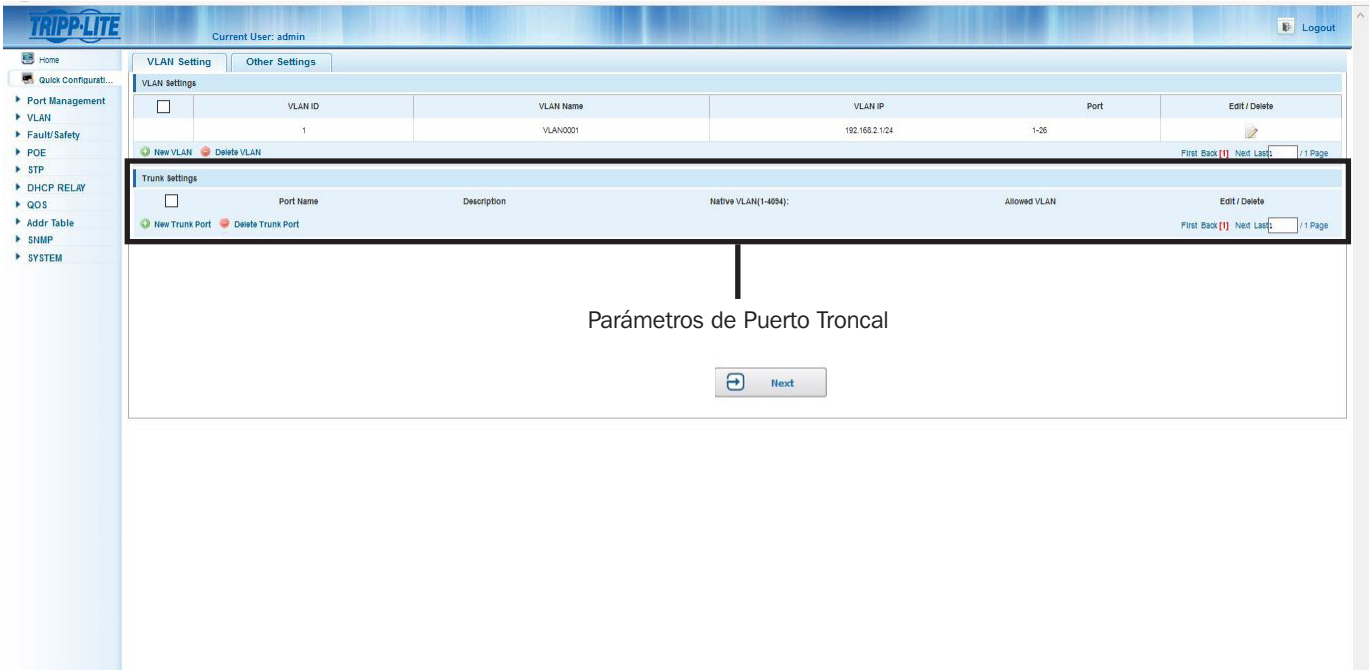


Figura 4.2 Parámetros del Puerto Troncal

4.2.1 Adición de Puertos Troncales

Haga click en el ícono de "Nuevo Puerto Troncal" y seleccione el puerto a configurar. Ingrese el ID de la VLAN Nativa. A continuación, introduzca los IDs para las VLANs permitidas que tendrán acceso a través de los puertos troncales. Cuando termine, haga click en “Guardar”. Repita estos pasos para crear los puertos troncales adicionales.

4.2.2 Edición de Parámetros de Puerto Troncal

Haga click en el ícono "Editar" para hacer cambios a los puertos troncales seleccionados, la VLAN Original y VLANs Permitidas. Cuando termine la edición, haga click en “Guardar”. Repita estos pasos para editar los puertos troncales adicionales.

4.2.3 Eliminación de Puertos Troncales

Para eliminar puertos troncales, haga click en el ícono rojo al lado del puerto troncal a eliminar o haga click en la casilla de verificación junto al puerto troncal asociado y haga click en "Eliminar Puerto Troncal". Para eliminar varios puertos troncales, marque las casillas junto a los puertos troncales que se eliminarán. Haga click en "Eliminar Puertos Troncales" para eliminar los puertos troncales seleccionados en la configuración del switch.

4. Configuración Rápida

4.3 Otros Parámetros

Seleccione "Configuración Rápida → Otros Parámetros" para ver los parámetros del sistema (Figura 4.3). Desde esta página, puede cambiar la VLAN de administración de los switches, dirección IP de administración, máscara de subred, portal de enlace predeterminado, Servidor DNS, nombre de dispositivo y contraseña interfaz de administrador. Después de modificar la configuración, haga click en "Guardar". Haga click en "Finalizar" para volver a la página principal o haga click en "Anterior" para volver a la página anterior de parámetros para modificar aún más la configuración.

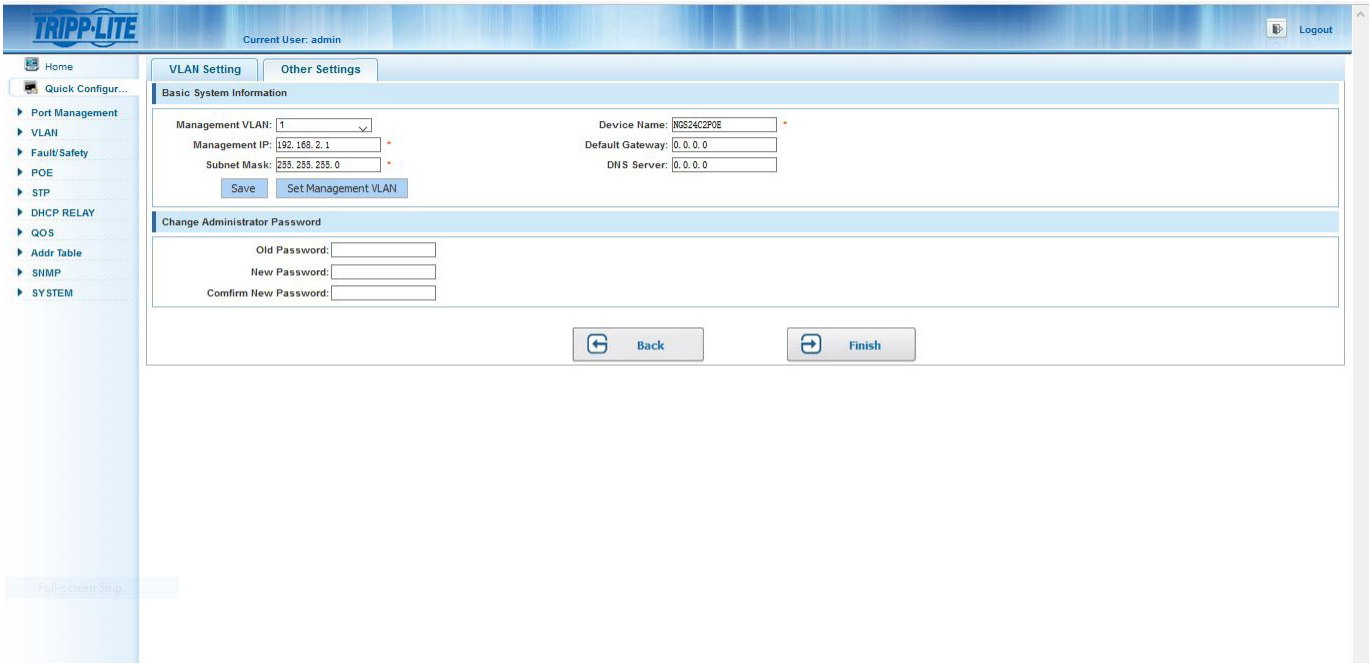


Figura 4.3 Otros Parámetros

La página de Otros Parámetros muestra la configuración del sistema básico:

VLAN de Administración: La ID de la VLAN de administración predetrminada del switch es 1.

IP de Administración: La dirección IP de la VLAN de administración del switch.

Máscara de Subred: La máscara de subred de la VLAN de administración del switch.

Nombre de Dispositivo: El nombre de anfitrión del switch.

Portal de Enlace Predeterminado: El portal de enlace predeterminado de la administración del switch VLAN.

Servidor DNS: La dirección IP del Servidor DNS.

Nota: *La ID de la VLAN de administración del switch predeterminad es 1 y no se puede eliminar.*

4.3.1 Modificación de la Parámetros de Dirección IP de Administración del Switch

Para configurar la dirección IP de administración del switch, siga estos pasos:

1. Introduzca la dirección IP en el campo "Dirección IP" (p.e. 192.168.100.179). Se requiere IP de Administración.
2. Introduzca la máscara de subred en el campo "Máscara de Subred" (p.e. 255.255.255.0). Se requiere Máscara de Subred de Administración.
3. Ingrese el nombre del dispositivo. Se requiere el nombre del dispositivo.
4. Ingrese la dirección del portal de enlace en el campo "Portal de Enlace Predeterminado" (p. ej. 192.168.100.1).
5. Introduzca la dirección IP del Servidor DNS (p.e. 192.168.10.12).
6. Para completar la configuración, haga click en “Guardar”.
7. Haga click en "Configurar VLAN de Administración" para cambiar a otra VLAN que no sea la ID de VLAN predeterminada de 1.

4.3.2 Cambio de Contraseña de Interfaz de Administrador de Administración Web

Para editar la contraseña de administrador de la interfaz de administración Web del switch, introduzca la contraseña predeterminada o anterior y a continuación, escriba la nueva contraseña (Sensible al caso). Introduzca otra vez la nueva contraseña (Sensible al caso) para confirmarla. Haga click en "Finalizar" para confirmar los cambios o "Volver" para descartarlos.

5: Administración de Puertos

5.1 Parámetros Básicos

5.1.1 Vista de Configuración de Puerto

Seleccione "Administración de Puerto→ Configuración Básica" para ver y modificar los parámetros del puerto (Figura 5.1).

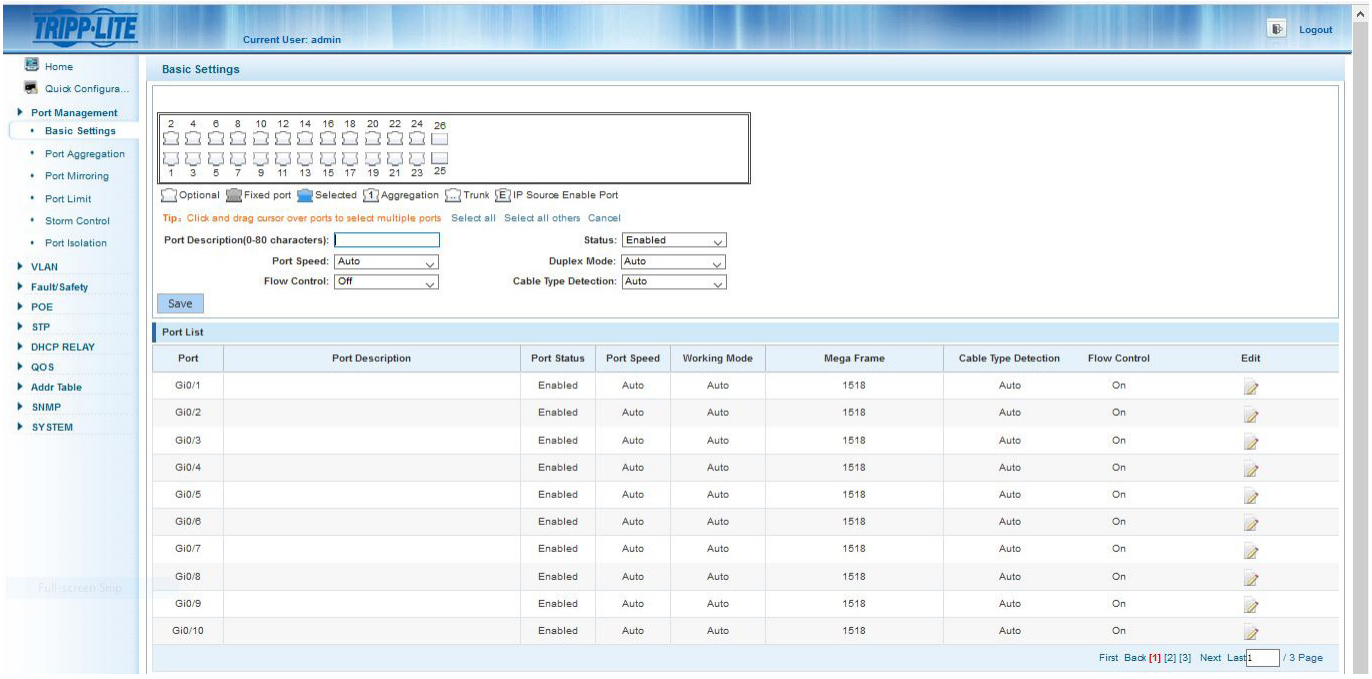


Figura 5.1: Página de Configuración Básica

La tabla de lista de puertos muestra información de configuración de puertos del switch en las siguientes columnas:

- **Puerto:** Muestra el número de puerto del switch.
- **Descripción:** Muestra el nombre proporcionado por el usuario o la descripción dada al puerto.
- **Estado:** Muestra el estado del puerto, ya sea "Activo" o "Inactivo".
- **Velocidad del Puerto:** Muestra la negociación automática, 10, 100 o 1000 Mbps
- **Modo de Trabajo:** Muestra la configuración de puerto dúplex, negociación automática, dúplex o semidúplex.
- **Mega Frame:** Muestra la longitud de los jumbo frames. La longitud predeterminada del mega frame es 1518.
- **Detección de Tipo de Cable:** Muestra configuración de cruce, negociación automática, MDI o MDIX.
- **Control de Flujo:** Muestra si el control de flujo está "Encendido" o "Apagado"

Nota: *La velocidad de SFP de cobre / fibra puede ser sólo 1000 Mbps y su modo de trabajo sólo puede ser automático / dúplex.*

5: Administración de Puertos

5.1.2 Configuración de Puertos Individuales o Múltiples

Seleccione los puertos a configurarse desde el panel, entonces haga click en el ícono en la columna de edición para cambiar la configuración de cada puerto seleccionado.

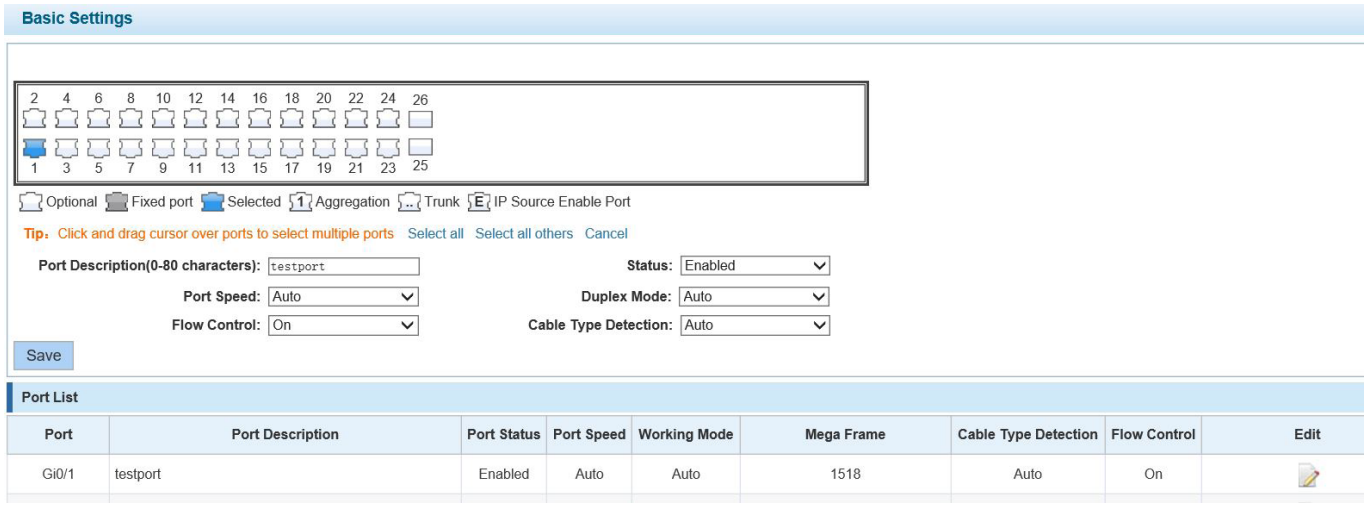


Figura 5.2: Configuración de Puerto Individual

Nota: *En la pantalla de configuración de puerto individual se pueden cambiar los siguientes parámetros: Descripción, Estado, Velocidad de Puertos, Modo Dúplex, Control de Flujo y Detección de Tipo de Cable.*

5.2 Agregación de Puerto

5.2.1 Vista de Configuración de Agregación de Puerto

Seleccione "Administración de Puerto → Agregación de Puerto" para ver la configuración de agregación de puerto del switch (Figura 5.3). Agregación de Puerto (o agregación de enlace) permite combinar múltiples enlaces de Ethernet en un único enlace lógico. Los dispositivos de red tratan la agregación como si fuera un solo link, que aumenta la tolerancia a fallas y proporciona distribución de la carga.

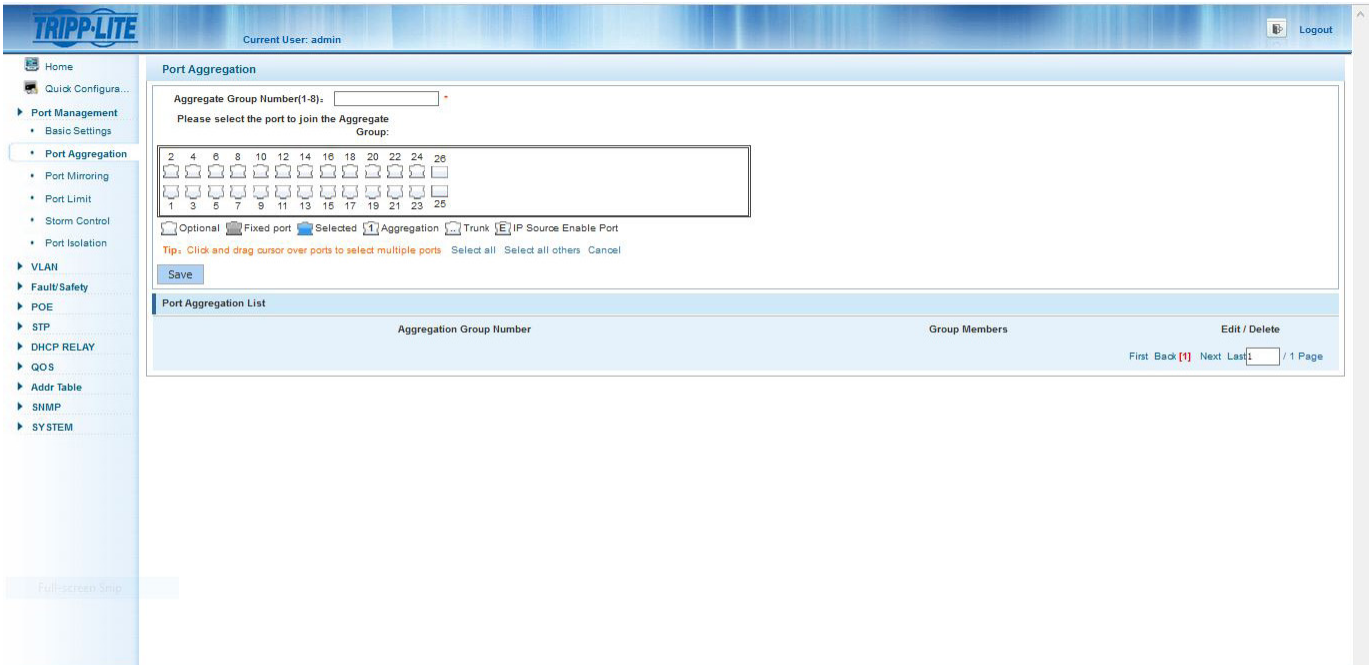


Figura 5.3: Agregación de Puerto

5: Administración de Puertos

La tabla de Agregación de Puertos mostrará la configuración actual del switch.

- **Número de Grupo de Agregación:** Muestra el número asignado al grupo de agregación.
- **Miembros del Grupos de Agregación:** Muestra los números de puerto que conforman un grupo de agregación de enlace.

Notas:

- *Los grupos de agregación deben contener un mínimo de dos puertos; puede agregarse un máximo de ocho puertos en un grupo.*
- *Cada puerto en un grupo de agregación de enlace debe utilizar los mismos protocolos y velocidades de enlace.*

5.2.2 Creación de un Grupo de Agregación de Puertos

Para crear un grupo de agregación de puertos, introduzca una ID de agregación de puerto y a continuación, seleccione los puertos que se añadirán al grupo agregado. Para completar la configuración, haga click en “Guardar”. Cuando un puerto es parte de un grupo de agregación, aparecerá como se muestra en la Figura 5.4.

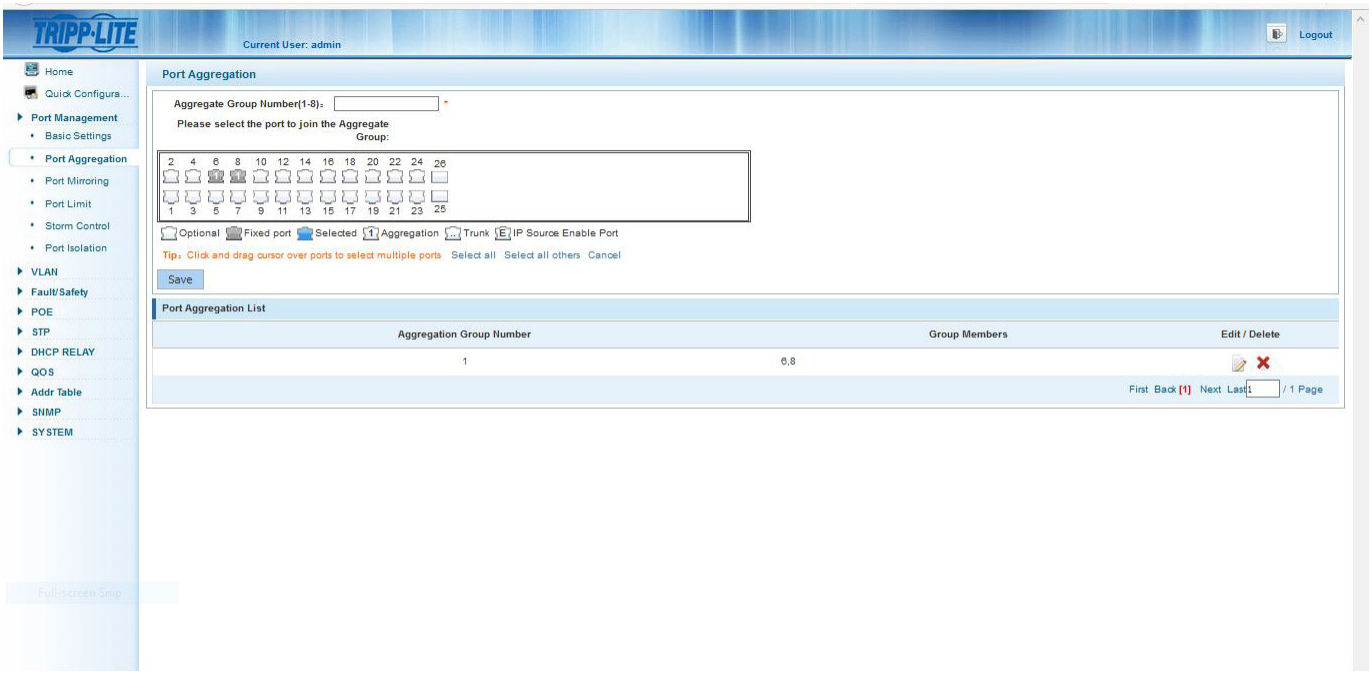


Figura 5.4: Creación de un Grupo de Agregación de Puertos

5.2.3 Edición de un Grupo de Agregación de Puertos

Haga click en el ícono "Editar" para añadir miembros al grupo de agregación. El número de grupo de agregación no se puede cambiar una vez establecido. Si intenta crear un nuevo grupo agregado usando un número de grupo existente, se mostrará "el número de puerto agregado ya existe". Elija otro número de grupo disponibles para asignar.

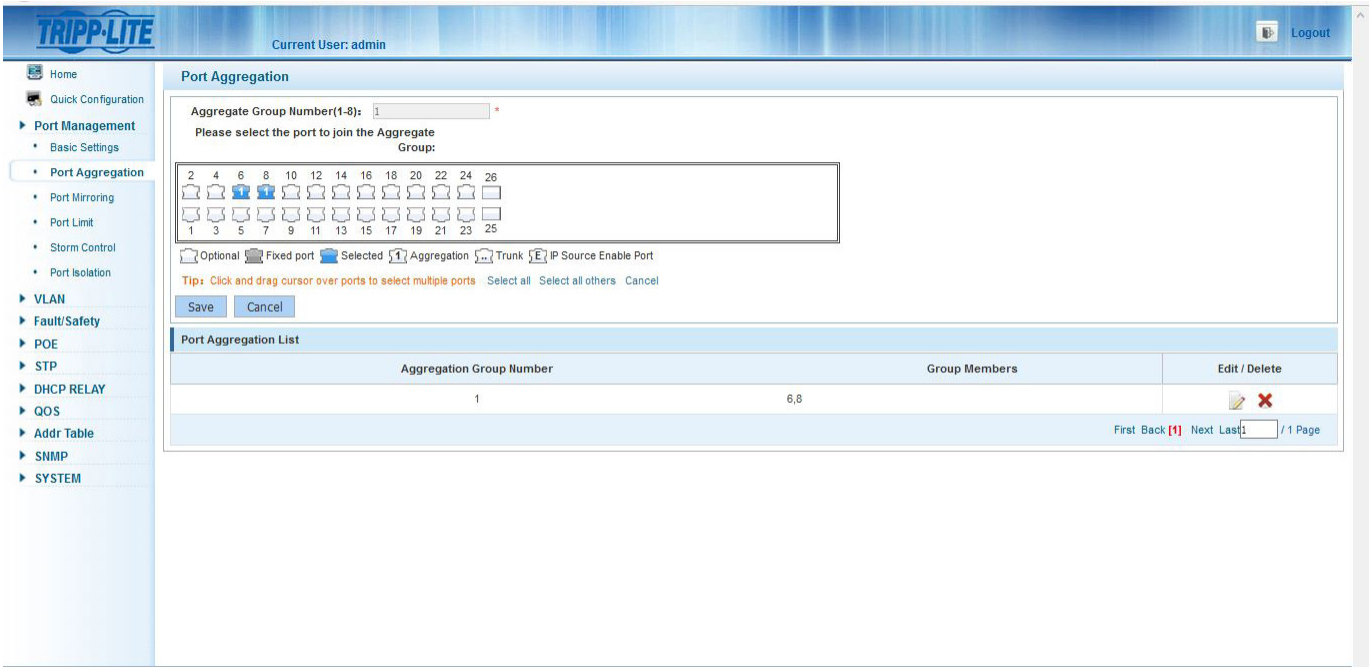


Figura 5.5: Editar o Eliminar Grupo de Agregación de Puertos

5.2.4 Eliminación de un Grupo de Agregación de Puerto

Haga click en el ícono ✖ rojo próximo al grupo de agregación para eliminar ese grupo de puertos.

5: Administración de Puertos

5.3 Puerto Espejo

5.3.1 Vista de Configuración de Puerto Espejo

Seleccione “Administración de Puerto → Puerto Espejo” para ver la configuración de puerto espejo (Figura 5.6). El puerto espejo selecciona el tráfico de red para el análisis por un analizador de red. Esto se puede hacer para puertos específicos del switch. Muchos puertos del switch se pueden configurar como puertos de origen y un puerto del switch se configura como un puerto de destino. Los paquetes copiados en un puerto de destino tendrán el mismo formato que el paquete original de la fuente. Esto significa que si el espejo está copiando un paquete recibido, el paquete copiado será etiquetado VLAN o sin etiquetar como fue recibido en el puerto de origen.

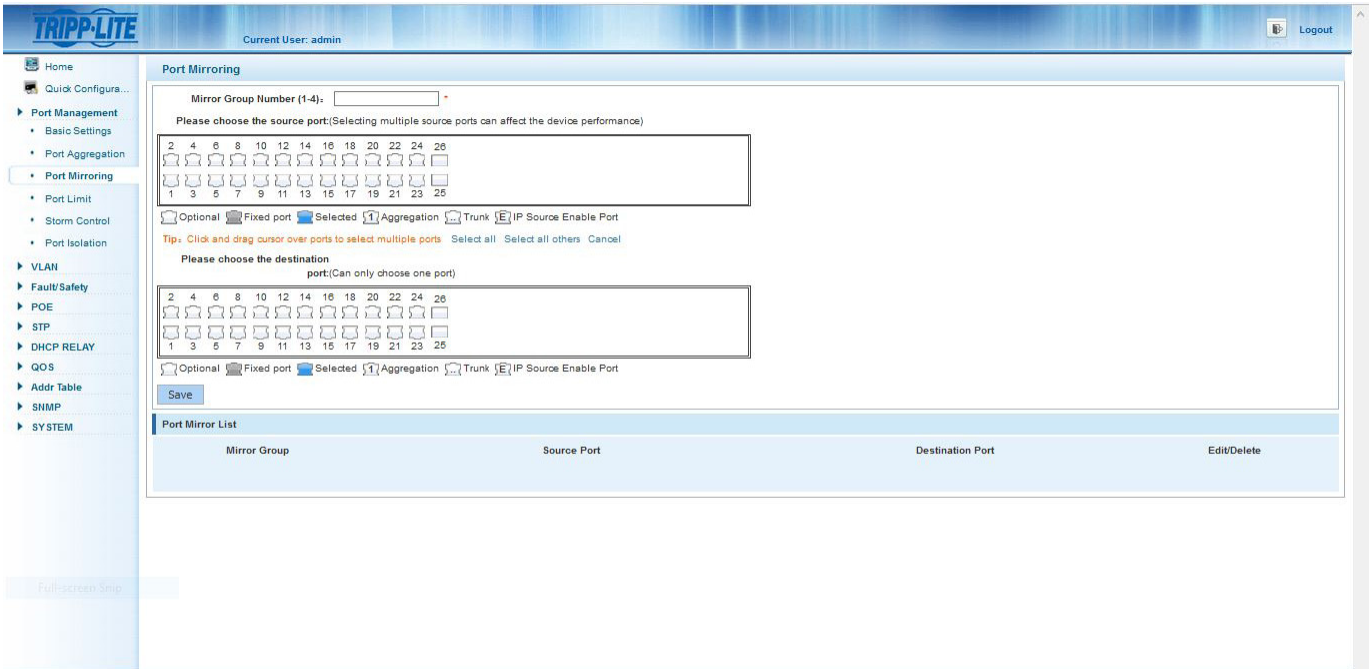


Figura 5.6: Configuración del Puerto Espejo

La lista de puertos espejado muestra la configuración de duplicación del switch.

- **Grupo Espejo:** ID de grupo espejo; pueden crearse hasta cuatro grupos espejo.
- **Puerto(s) de Origen:** El(los) puerto(s) de donde provienen los datos espejo.
- **Puerto de Destino:** El puerto que recibe los datos espejo.

Notas:

- *Los puertos en los puertos de agregación no pueden designarse como el puerto de origen y el puerto de destino.*
- *Solamente un puerto de destino puede ser seleccionado por cada grupo espejo.*

5.3.2 Creación de un Grupo de Puertos Espejo

Para crear un grupo de puertos espejo, seleccione los puertos de origen y el puerto de destino y a continuación seleccione el grupo espejo (Figura 5.7). Haga click en “Guardar”.

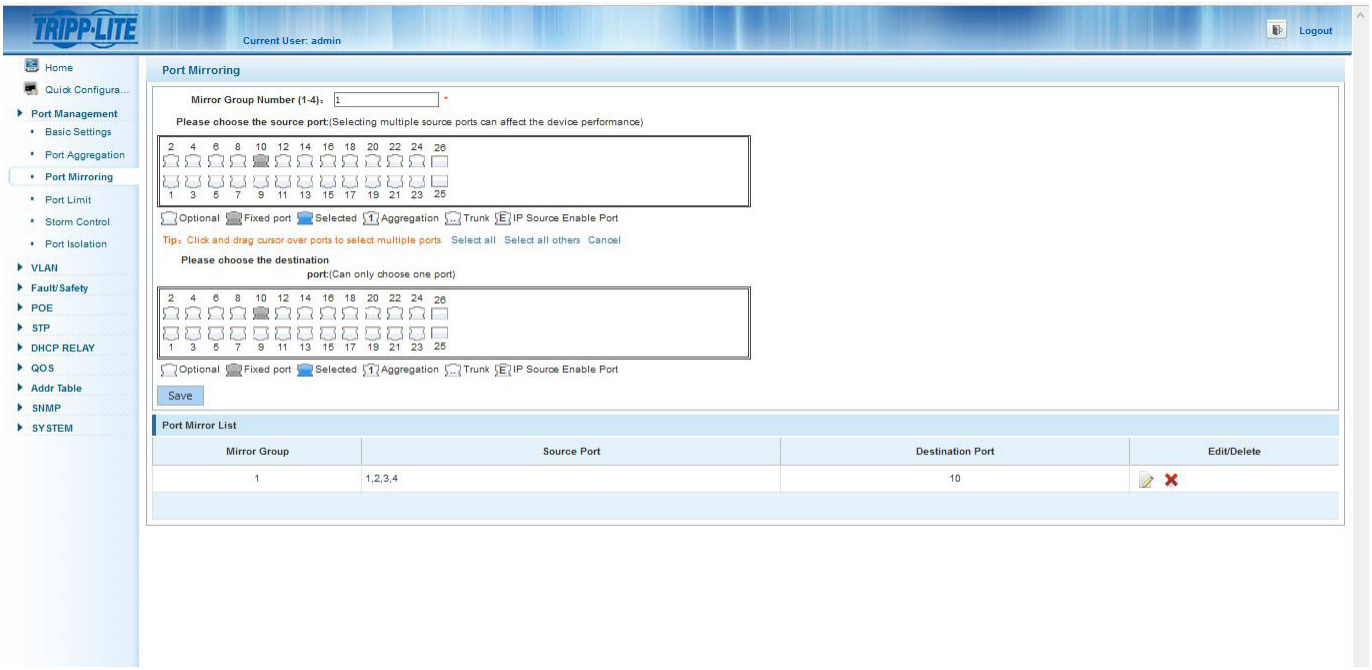


Figura 5.7 Creación de un Grupo de Puertos Espejo

5.3.3 Edición de un Grupo de Puertos Espejo

Haga click en el ícono junto al grupo de puertos espejo (Figura 5.8) para editar sus puertos de origen y destino.

Nota: *El Número de ID del Grupo Espejo no se puede editar una vez asignado.*

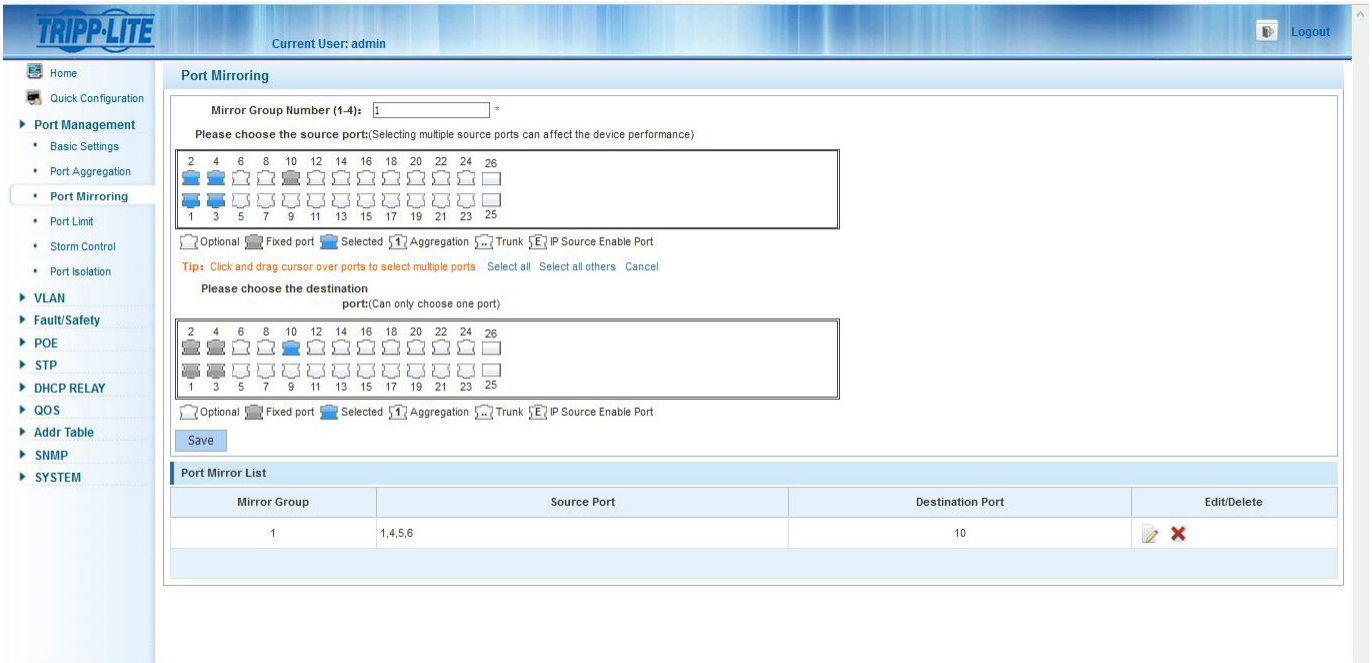


Figura 5.8 Edición o Eliminación de un Grupo de Puertos Espejo

5.3.4 Eliminación de un Grupo de Puertos Espejo

Haga click en el ícono junto al grupo de puertos espejo para eliminar el grupo.

5.4 Parámetros de Límite de Velocidad del Puerto

5.4.1 Vista de Parámetros de Límite de Velocidad de Subida del Puerto

Seleccione “Administración de Puerto → Límite de Puertos” para ver la configuración de límite de velocidad del puerto del switch (Figura 5.9).

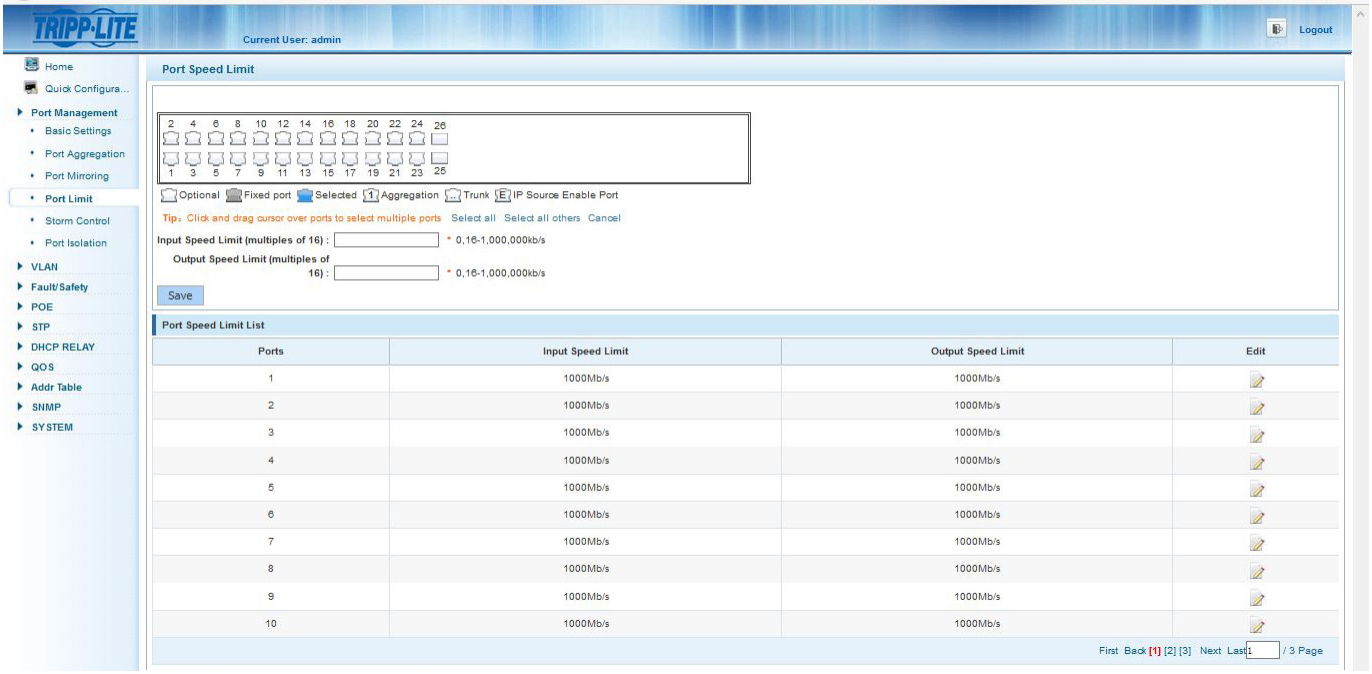


Figura 5.9: Configuración de Límite de Velocidad de Puerto

El límite de velocidad muestra las configuraciones de límite de velocidad del puerto del switch.

- **Puertos:** Muestra el número de puerto.
- **Límite de Velocidad de Entrada:** Límite de velocidad de subida para el puerto.
- **Límite de Velocidad de Salida:** Límite de velocidad de bajada para el puerto.

Nota: *Pueden seleccionarse varios puertos en el panel para modificar la configuración de límite de velocidad de puerto.*

5: Administración de Puertos

5.5 Parámetros de Control de Tormenta

5.5.1 Configuración de los Parámetros de Control de Tormenta de un Puerto

El Control de Tormenta asegura el funcionamiento de la red durante una inundación de paquetes de tráfico Multicast, Unicast o Broadcast en la LAN. Para configurar, seleccione “Administración del Puerto → Control de Tormenta” para cambiar la configuración de control de tormentas de un puerto seleccionado o puertos (Figura 5.10). De forma predeterminada, esta característica está desactivada.

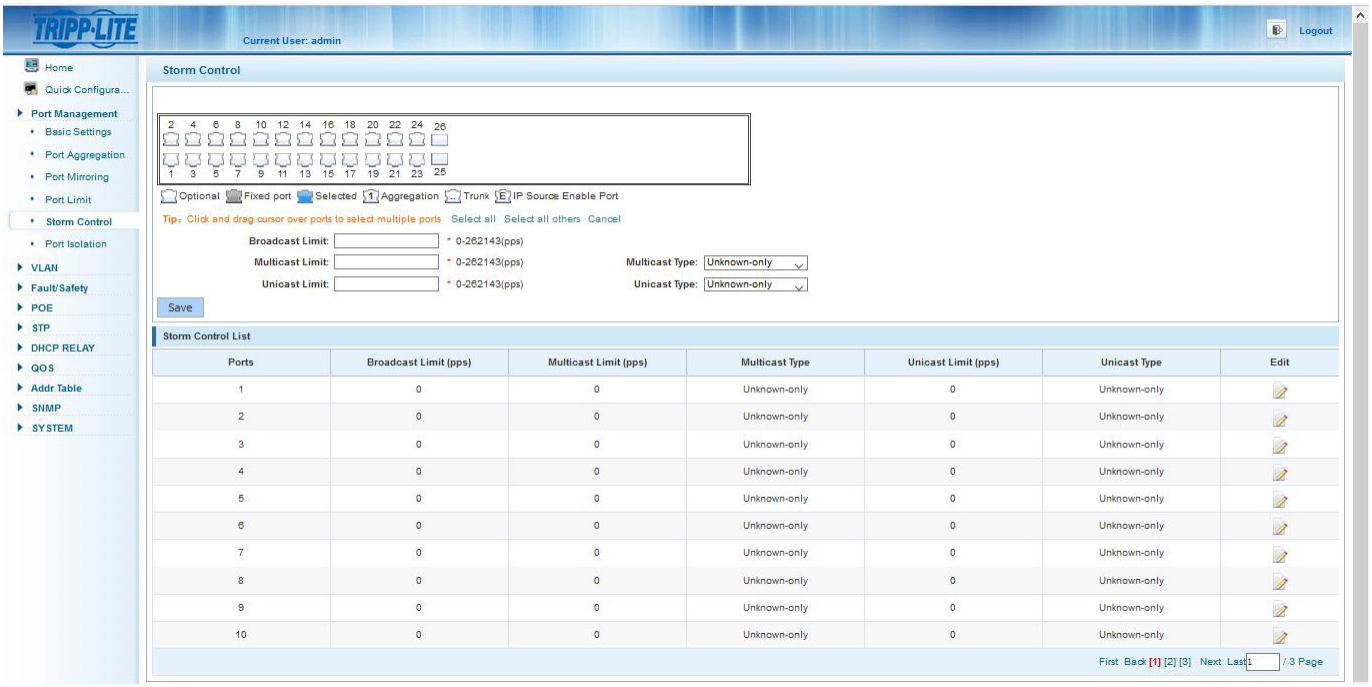


Figura 5.10: Tabla de Configuración de Control de Tormenta

La vista en la figura 5.10 muestra la configuración de control de tormenta del switch por puerto.

- **Puertos:** Muestra el número de puerto del switch.
- **Transmisión:** Muestra si el control de paquetes de transmisión está habilitado o deshabilitado. "0" denota deshabilitado.
- **Multicast:** Muestra si el control de paquetes de Multicast está habilitado o deshabilitado. "0" denota deshabilitado.
- **Unicast:** Muestra si el control de paquetes Unicast está habilitado o deshabilitado. "0" denota deshabilitado.
- **Valor de Control de Tormenta:** Establece la tasa en que se activará el control de tormenta (entre 0 y 262143 pps).
- **Tipo de Control de Tormenta:** Muestra los tipos de configuración de control de tormenta que se pueden configurar para "Solamente desconocido" o "Ambos”. Un dispositivo puede poner en práctica la supresión de tormenta a una transmisión, una Multicast o una Unicast respectivamente. Cuando se reciben paquetes excesivos de transmisión, Multicast o Unicast desconocida, el switch prohíbe temporalmente el reenvío de tipos de paquetes relevantes hasta que los flujos de datos son recuperados al estado normal (entonces los paquetes se reenviarán normalmente).

5.5.2 Edición de Parámetros de Control de Tormenta [Storm Control]

Seleccione el(los) puerto(s) a configurar (Figura 5.11). Haga click en el menú desplegable "Tipo de Control de Tormenta" para seleccionar el tipo de control de tormenta a ser configurado para el puerto. Introduzca un valor de 0 a 262143 en los campos "Valor de Control de Tormenta" de paquetes de transmisión, Multicast y Unicast por segundas entradas. Si es necesario, establezca tipo de tráfico de Multicast y Unicast a "Solamente desconocido" o "Ambos" y luego haga click en "Guardar" para completar la configuración del puerto o puertos.

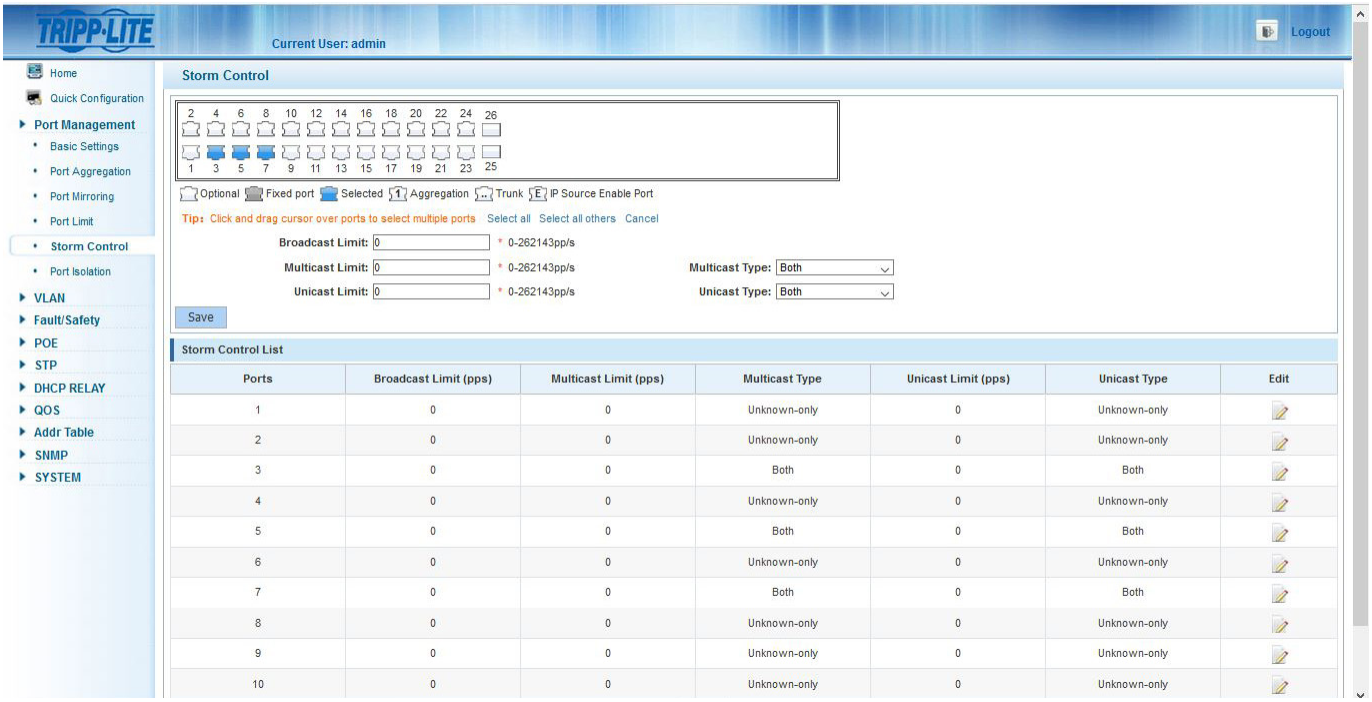


Figura 5.11: Edición de Parámetros de Control de Tormenta

5.6 Parámetros de Aislamiento de Puerto

5.6.1 Vista de Configuración de Aislamiento de Puerto

Seleccione “Administración de Puerto → Aislamiento de Puerto” para ver la configuración de aislamiento de puerto del switch (Figura 5.12). El aislamiento de puerto evita que PCs conectadas a diferentes puertos se comuniquen con las demás (sin tener que configurar una VLAN).

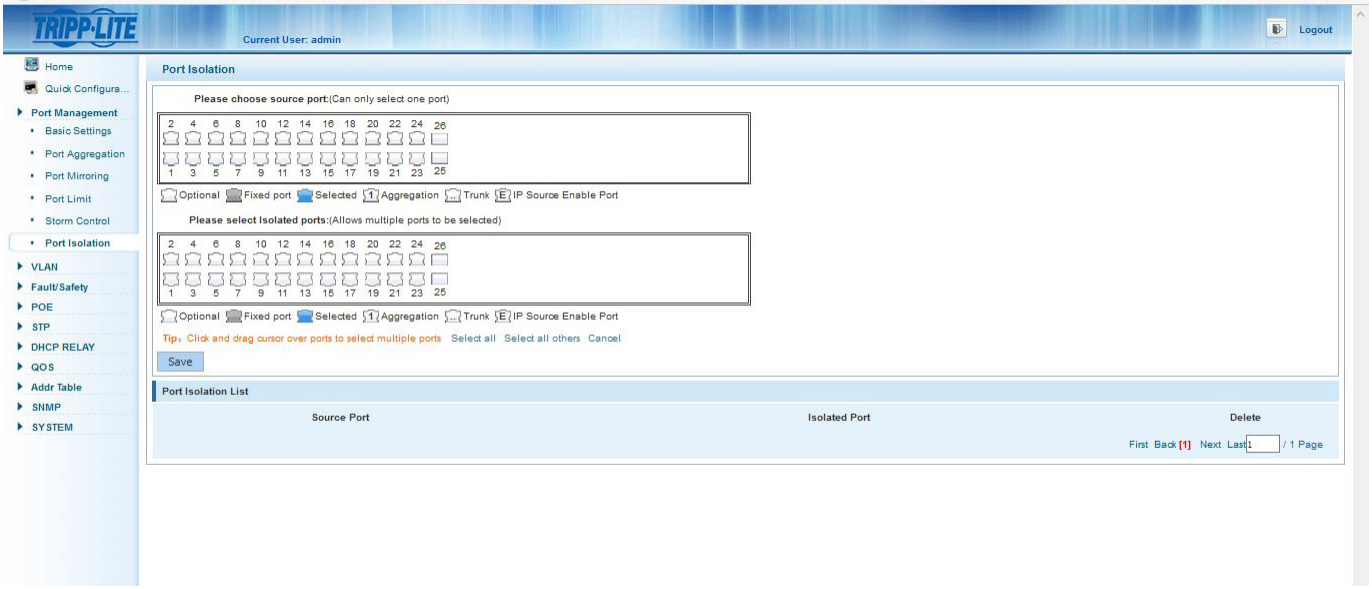


Figura 5.12: Configuración de Aislamiento de Puerto

5.6.2 Creación de un Grupo de Aislamiento de Puerto

Haga click en el ícono de puerto fuente de la tabla de lista de puertos y seleccione puerto a aislar. El puerto se pondrá azul en el panel. A continuación, seleccione el(los) puerto(s) a aislar desde el puerto seleccionado. Los puertos aislados se pondrán de color azul en el panel. Finalmente, haga click en “Guardar”. Los números de Puerto aislado aparecerán en la tabla (Figura 5.13).

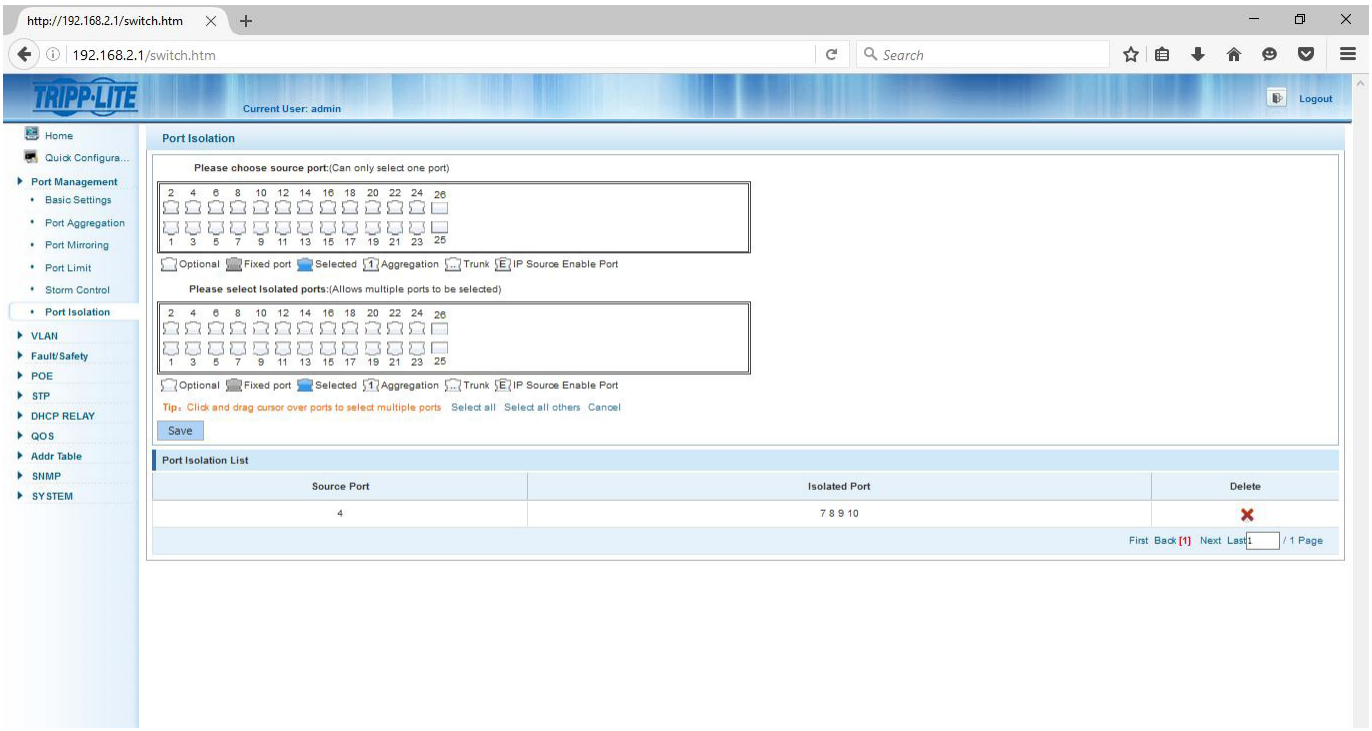


Figura 5.13: Creación de un Grupo de Aislamiento de Puertos

5.6.3 Eliminación de un Grupo de Aislamiento de Puerto

Haga click en el ícono  para borrar un grupo de aislamiento de puertos de la lista de aislamiento de puertos. Confirme la eliminación y el grupo se quitará de la lista (Figura 5.14).

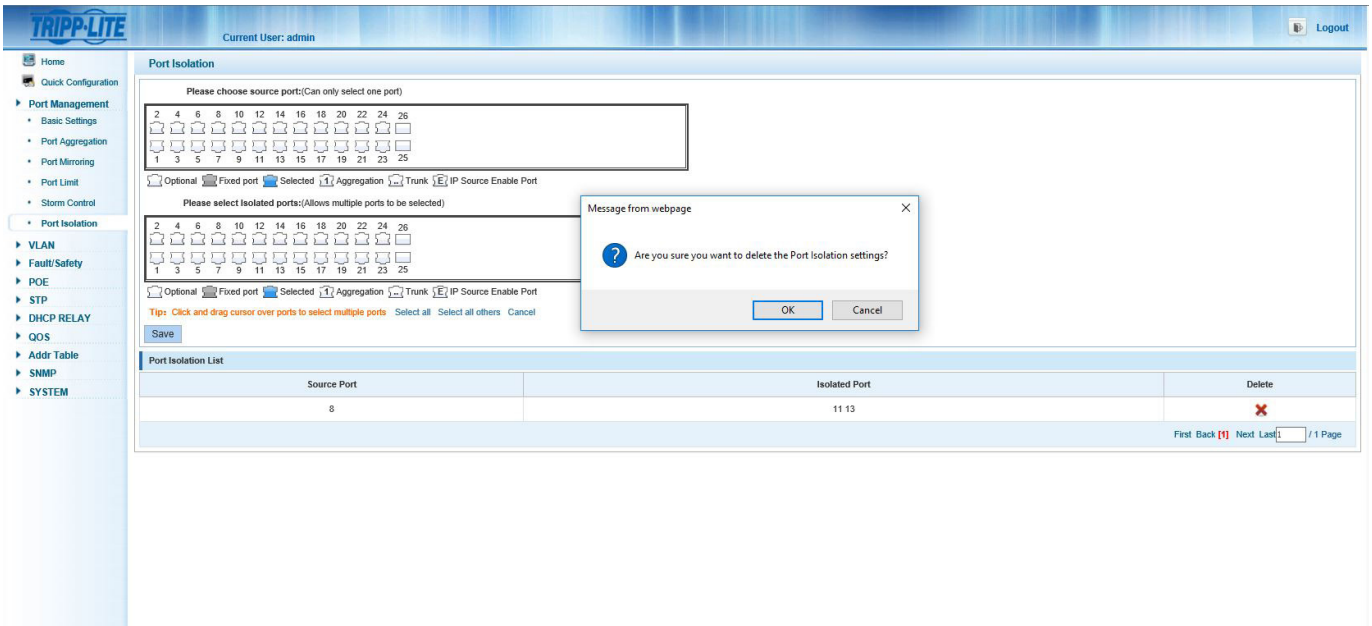


Figura 5.14: Eliminación de un Grupo de Aislamiento de Puertos

6. Administración de VLAN

6.1 Administración de VLAN

6.1.1 Vista de Configuración de VLAN

Seleccione “VLAN → Administración de VLAN” para ver los parámetros de configuración de VLAN del switch (Figura 6.1). Una LAN virtual (VLAN) es un grupo de estaciones de trabajo, servidores y otros recursos de red que se comportan como si estuviesen conectados a un solo segmento de red. Las VLANs permiten fácil segmentación de la red. Los usuarios que se comunican con frecuencia se pueden agrupar en VLANs comunes, independientemente de la ubicación física. El tráfico de cada grupo está contenido en gran parte dentro de la VLAN, lo que reduce el tráfico externo y mejora la eficiencia dentro de la red. Una VLAN también permite una administración fácil de la red. Los cambios en el número de nodos en una red y la ubicación de los nodos pueden ser manejados a través de la interfaz de administración en lugar de en los centros de distribución de cableado.

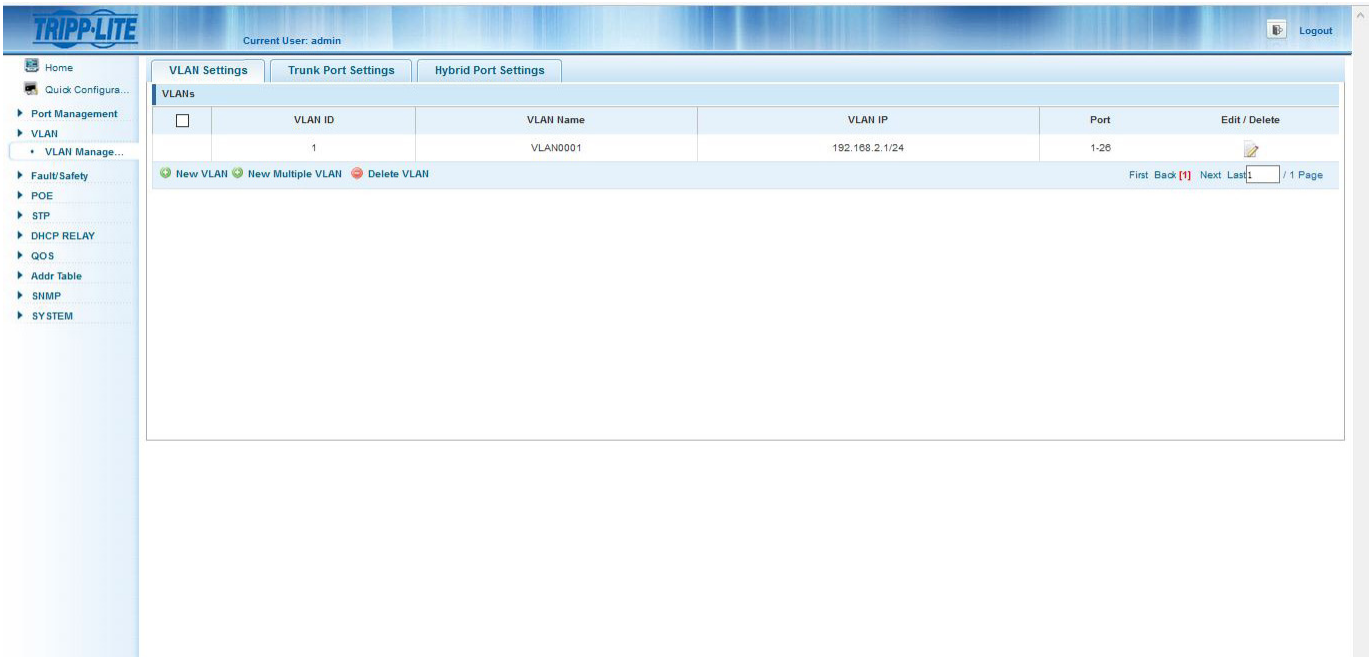


Figura 6.1: Información de Administración de la VLAN

La lista de VLAN muestra la configuración VLAN del switch:

- **VLAN ID:** Muestra el número de identificación de la VLAN.
- **Nombre de la VLAN:** Muestra el nombre de la VLAN; el nombre predeterminado para la VLAN 1 es DEFAULT.
- **VLAN IP:** Muestra la dirección IP de administración para el switch.
- **Puerto:** Muestra los puertos que pertenecen a cada VLAN.

Nota: *De forma predeterminada, todos los puertos pertenecen a la VLAN 1. No se puede eliminar la VLAN de administración.*

6. Administración de VLAN

6.1.2 Adición de una VLAN

Seleccione "Nueva VLAN" e introduzca el ID de la VLAN (entre 2 y 4094) (Figura 6.2). Introduzca un nombre de VLAN (límite: 31 caracteres). Si no se ha introducido ningún nombre, el switch asigna de forma predeterminada un nombre genérico de "VLAN0002". A continuación, seleccione los puertos que agregue a la VLAN y haga click en "Guardar".

Nota: *El sistema no permitirá crear IDs duplicados de VLANs.*

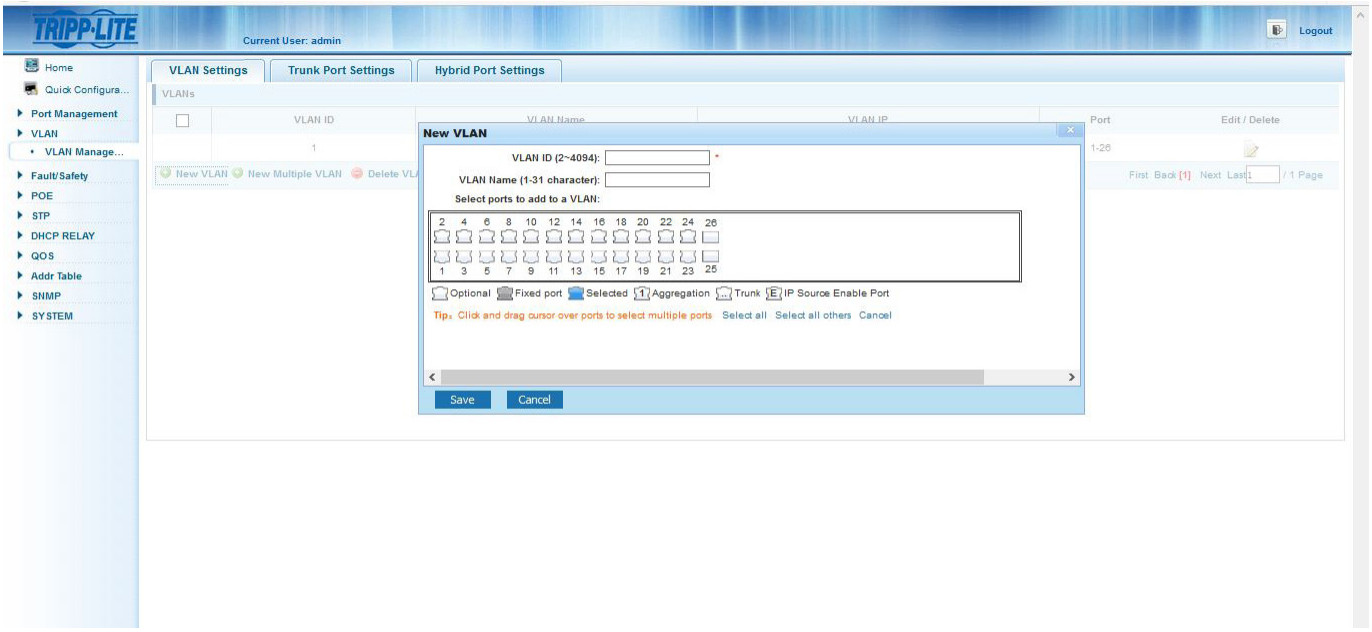


Figura 6.2: Adición de una VLAN

6.1.3 Adición de Múltiples VLANs

Para agregar rápidamente varias VLANs a la lista de visualización, seleccione "Nuevas VLAN Múltiples", introduzca las diversas IDs de las VLANs a crear y haga click en "Guardar" (Figura 6.3). Todas las VLAN(s) se crearán y permitirán ajustes para cada VLAN a editarse.

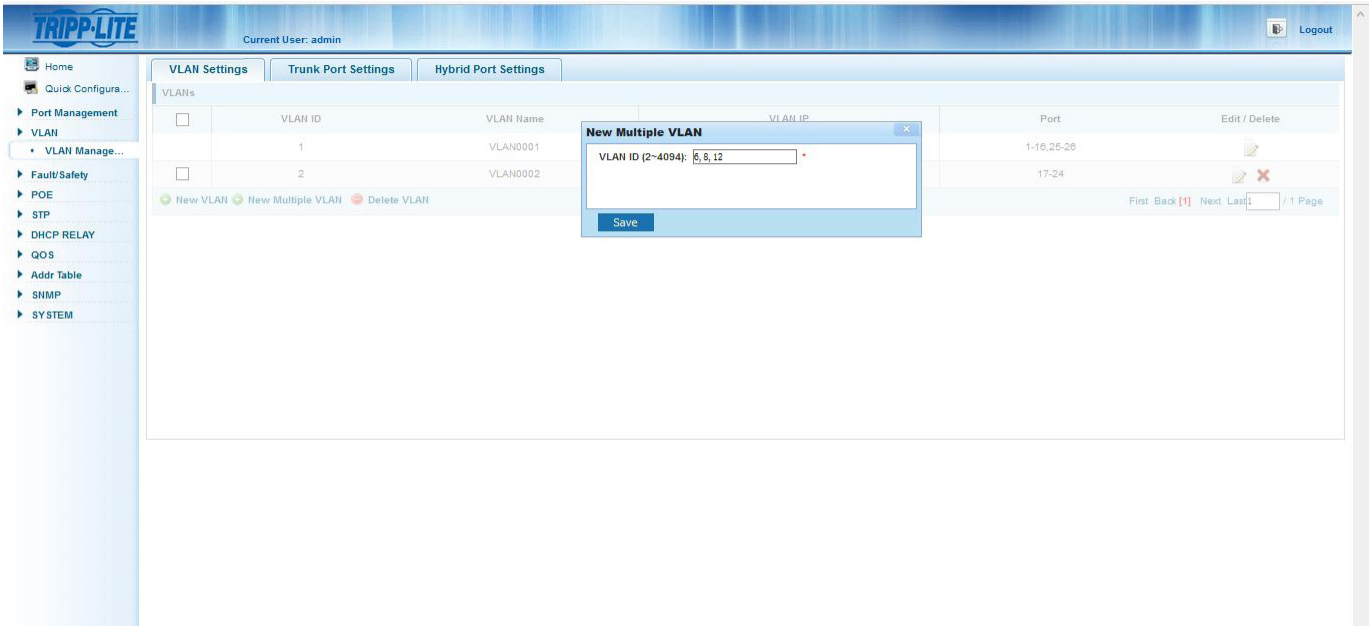


Figura 6.3: Adición de Múltiples VLANs

6. Administración de VLAN

6.1.4 Edición de una VLAN

Haga click en el ícono "Editar" de la ID de la VLAN que requiera cambios. En la ventana Editar VLAN (Figura 6.4), puede cambiar el nombre de la VLAN y puertos asociados. Una vez hechas las ediciones, haga click en "Guardar" para guardar sus ediciones. Haga click en "Cancelar" para descartar los cambios.

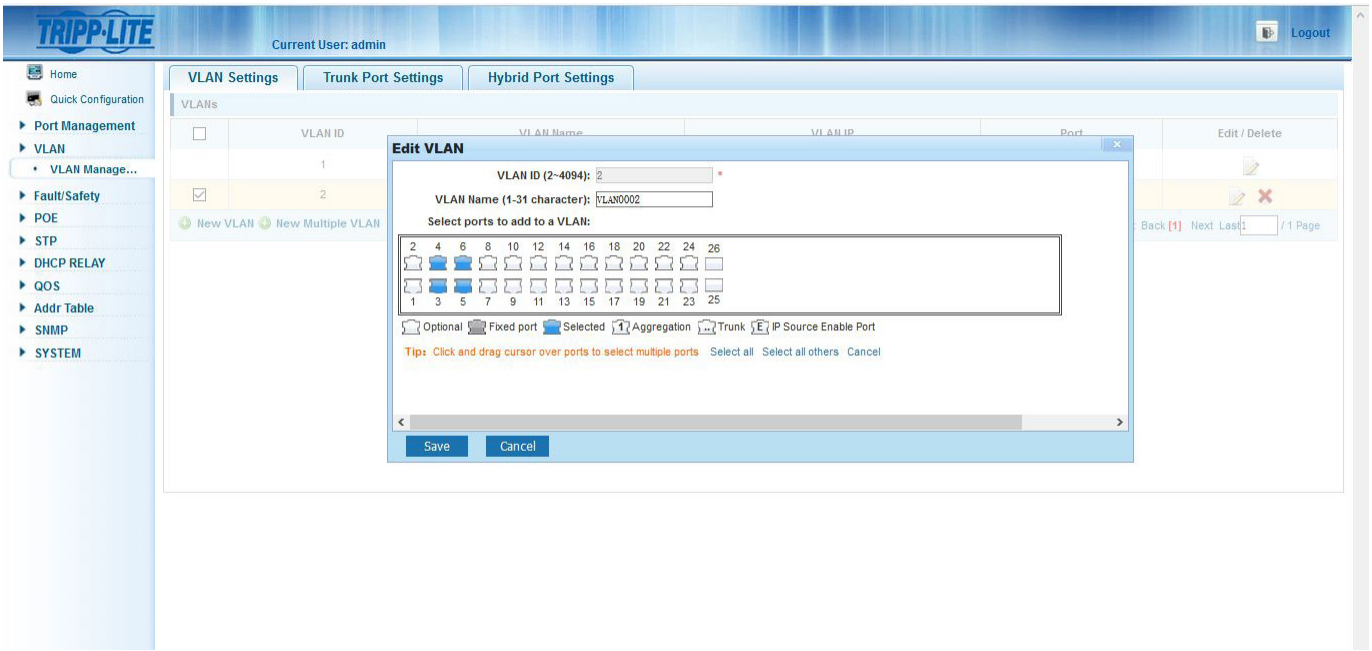


Figura 6.4: Edición de una VLAN

6.1.5 Eliminación de VLAN(s)

Eliminar una Sola VLAN

Seleccione la VLAN a ser eliminada de la lista y haga click en el ícono para eliminar la VLAN seleccionada (Figura 6.5).

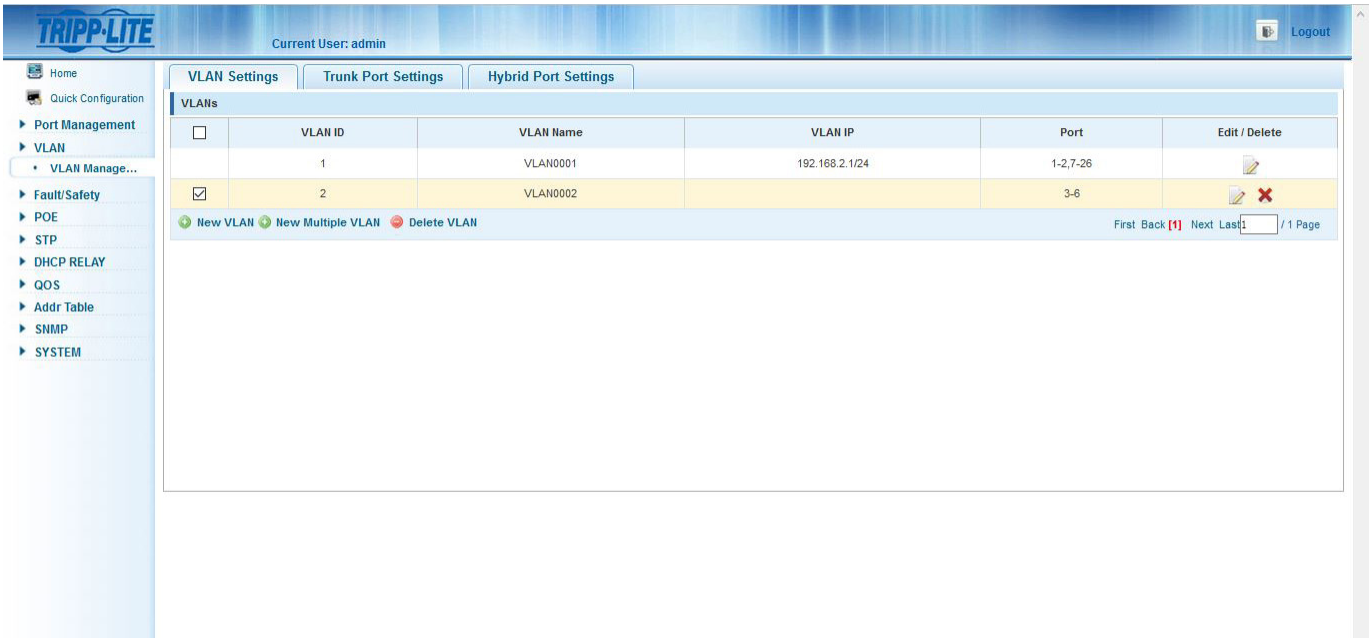


Figura 6.5: Eliminar una Sola VLAN

Eliminar Múltiples VLANs:

Haga click en la casilla de verificación junto a la(s) VLAN(s) a eliminar, haga click en "Eliminar VLAN" para quitar la(s) VLAN(s) seleccionada(s) (Figura 6.6).

Nota: *VLAN 1 es la VLAN de administración predeterminada; esta configuración no se puede cambiar.*

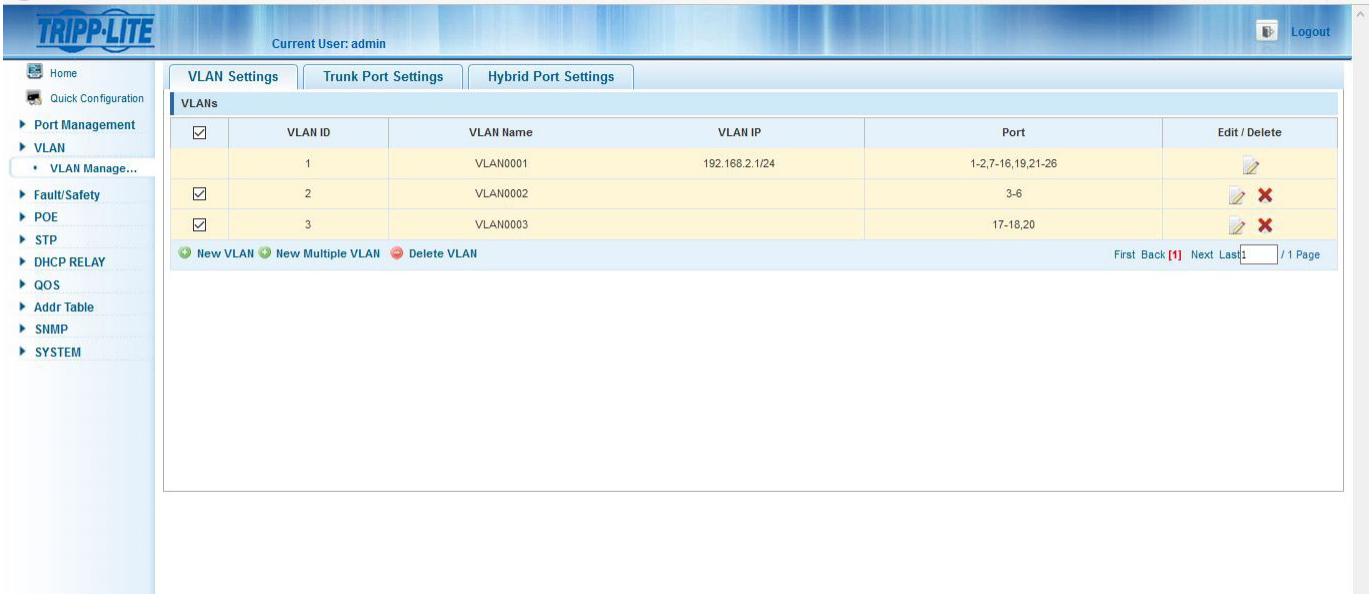


Figura 6.7: Eliminar Múltiples VLANs Simultáneamente

6.2 Parámetros de Puerto Troncal

6.2.1 Vista de Parámetros de Puerto Troncal

Seleccione “VLAN → Administración de VLAN → Parámetros de Puerto Troncal”, para ver los parámetros de configuración de puerto troncal del switch (Figura 6.7). Los puertos troncales permiten que la información de la VLAN pase entre switches. De forma predeterminada, la VLAN nativa (puerto de acceso) para el switch es VLAN 1. La comunicación entre los puertos de acceso no tendrá etiquetado (802.1Q). Cuando se configura un puerto troncal entre dos switches, el tráfico que pasa entre ellos se marcará con una etiqueta para permitir a los switches distinguir entre paquetes.

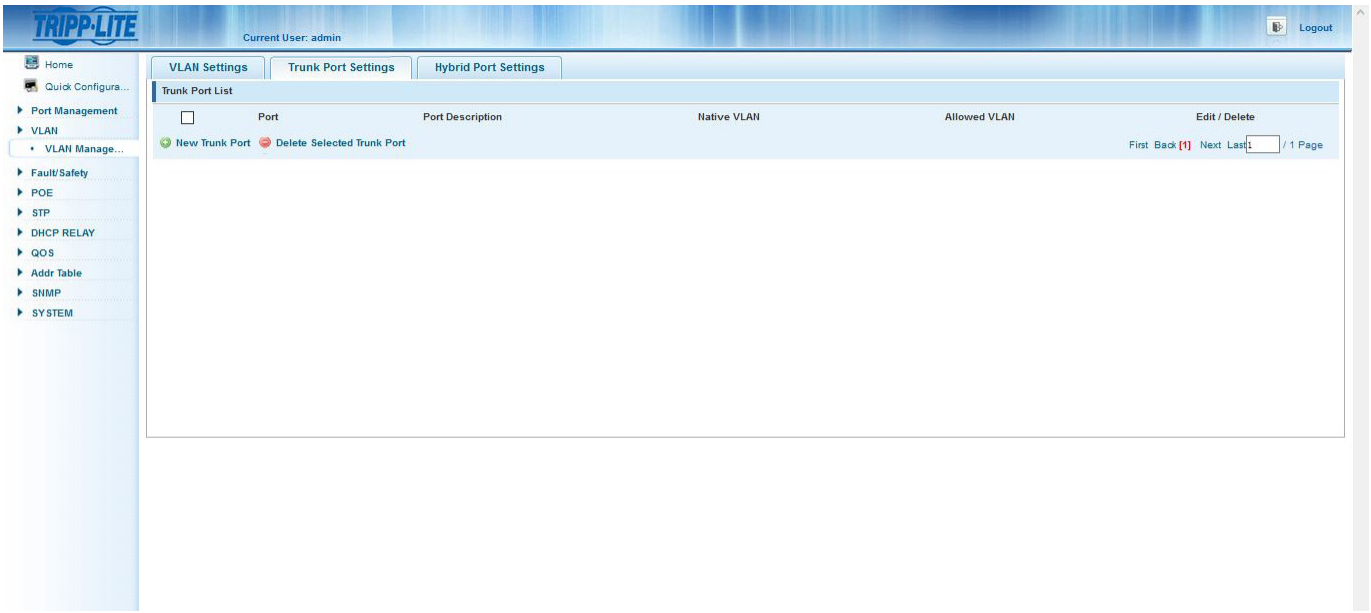


Figura 6.7: Vista de Parámetros de Puerto Troncal

6. Administración de VLAN

La lista de puertos troncales muestra la configuración del puerto troncal del switch.

- **Puerto:** Muestra el número de puerto.
- **VLAN Nativa:** Muestra la VLAN nativa. Por defecto, La VLAN nativa del switch es VLAN1.
- **VLAN Permitida:** Muestra las VLANs que serán etiquetadas cuando se transmitan en el puerto troncal.

6.2.2 Adición de Parámetros de Puerto Troncal

Para agregar un nuevo puerto troncal, haga click en "Nuevo Puerto Troncal" (Figura 6.8). Seleccione la VLAN nativa (por defecto es 1), luego seleccione la(s) VLAN(s) permitida(s) y haga click en "Guardar".

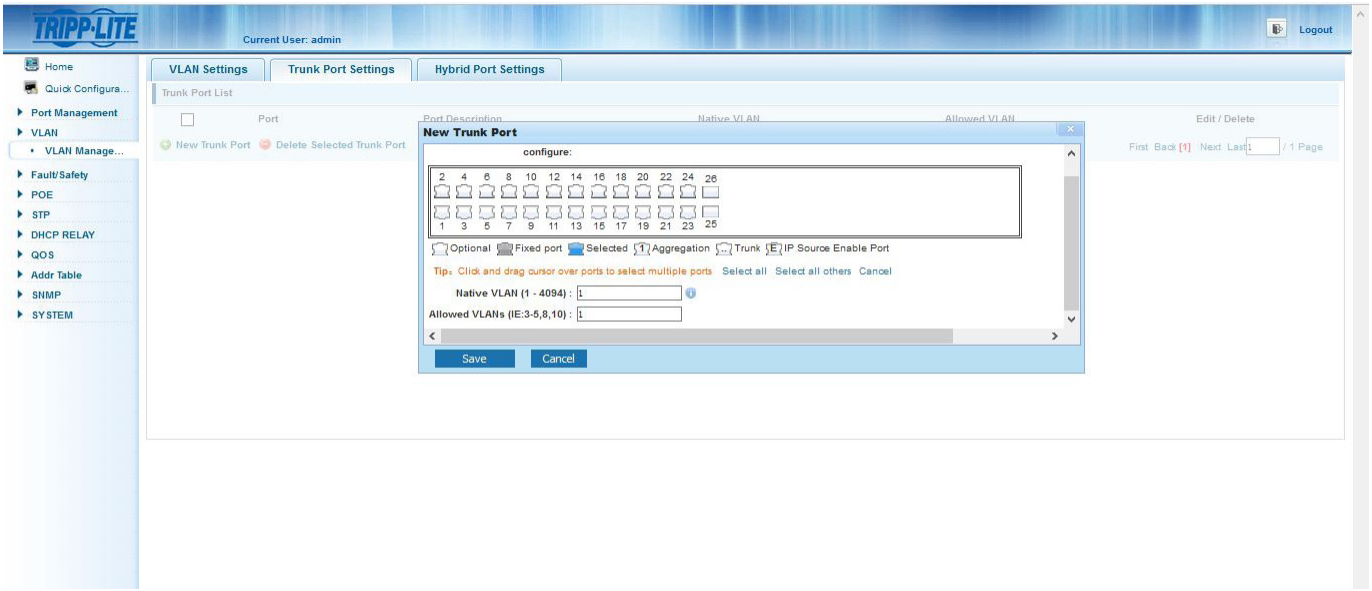


Figura 6.8: Adición de Puertos Troncales

Nota: *La(s) VLAN(s) permitida(s) deben crearse a través de la Administración de VLAN antes de que se pueda añadir a un puerto troncal.*

6.2.3 Edición de Puertos Troncales

Haga click en el ícono "Editar" del puerto troncal que desea editar. Dentro de la ventana de edición de puerto troncal (Figura 6.9) puede agregar puertos troncales adicionales, cambiar la VLAN nativa y cambiar las VLANs permitidas para el puerto troncal seleccionado.

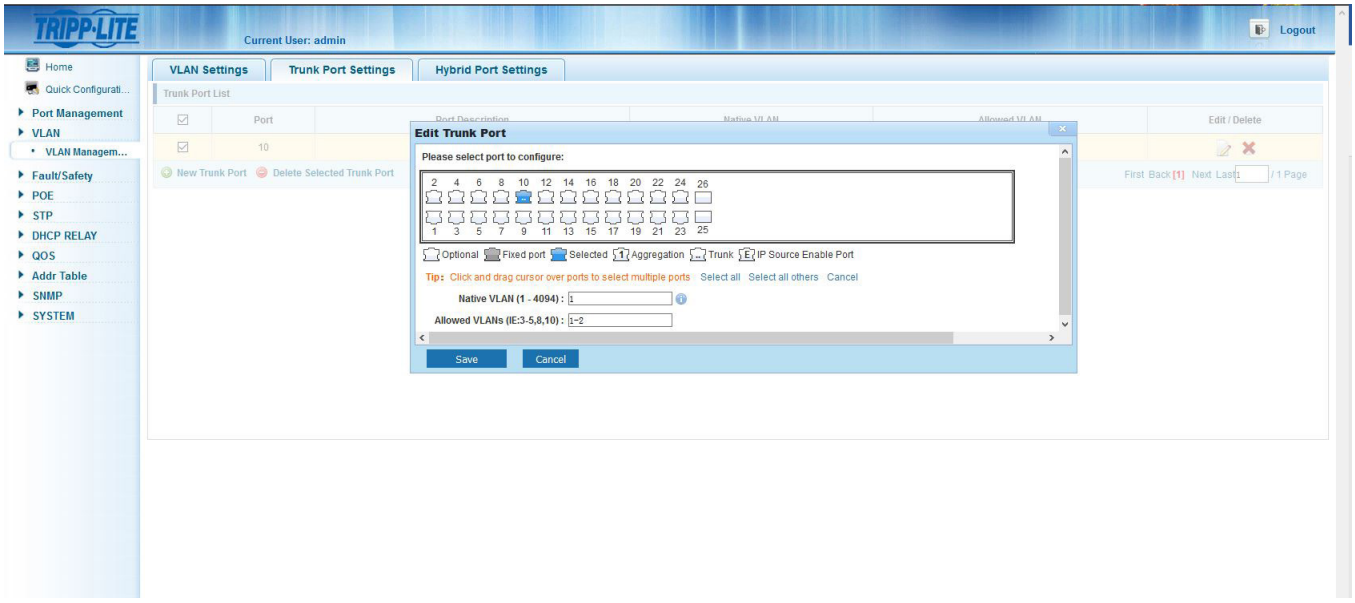


Figura 6.9: Edición de un Puerto Troncal

6.2.4 Eliminación de Puertos Troncales

Eliminar un Solo Puerto Troncal

Seleccione el puerto troncal a eliminar, luego haz click en el ícono (Figura 6.10).

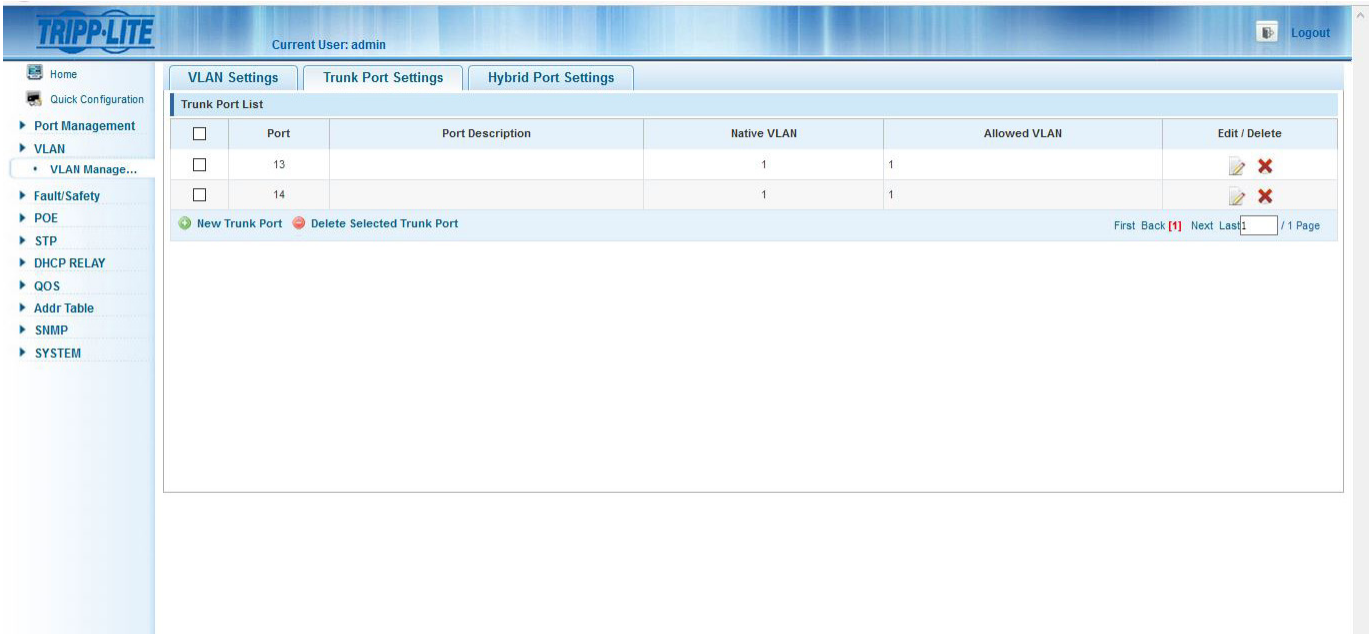


Figura 6.10: Eliminar un Solo Puerto Troncal

Eliminar Múltiples Puertos Troncales

Haga click en la casilla de verificación de los puertos troncales a eliminar, después haga click en "Eliminar Puerto Troncal Seleccionado" para eliminar los puertos troncales seleccionados (Figura 6.11).

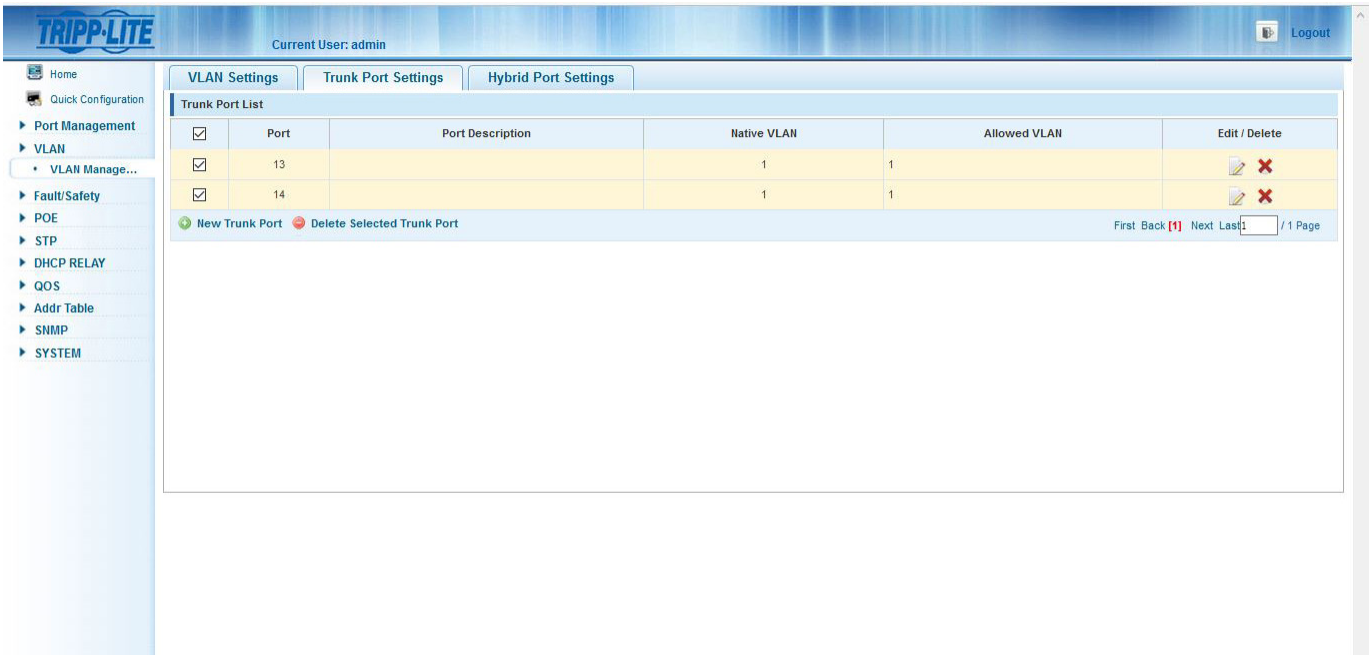


Figura 6.11: Eliminar Múltiples Puertos Troncales

6. Administración de VLAN

6.3 Parámetros de Puertos Híbridos

Los puertos híbridos soportan el tráfico de VLAN etiquetado y sin etiquetar. Esta característica se utiliza generalmente con las conexiones de teléfono de VoIP o VLANs.

La Lista de Puertos Híbridos muestra las configuraciones de puerto híbrido del switch.

- **Puerto:** Muestra el número de puerto.
- **Nombre de Puerto:** Muestra la descripción del nombre de puerto.
- **VLAN Nativa:** Muestra la VLAN nativa. Por defecto, La VLAN nativa del switch es VLAN1.
- **TAG de VLAN Agregado:** Muestra las VLANs que serán etiquetadas cuando se transmitan en el puerto híbrido.
- **TAG de VLAN Remnovido:** Muestra la VLAN que será desetiquetada cuando se transmita en el puerto híbrido.
- **VLAN Permitida:** Muestra las VLANs que serán etiquetadas cuando se transmitan en el puerto híbrido.

6.3.1 Adición de Nuevos Puertos Híbridos

Seleccione el puerto o puertos que serán parte de la configuración del puerto híbrido (Figura 6.12). A continuación, introduzca la VLAN nativa (entre 1 y 4094). Entonces, introduzca las IDs de las VLANs que están etiquetadas (3-5, 8,10). Por último, ingrese las "Ir a las IDs de las Etiquetas de las VLANs (3-5, 8, 10)". Haga click en "Guardar" para guardar la configuración del puerto híbrido. La vista cambiará automáticamente a las listas de resumen de puertos híbridos.

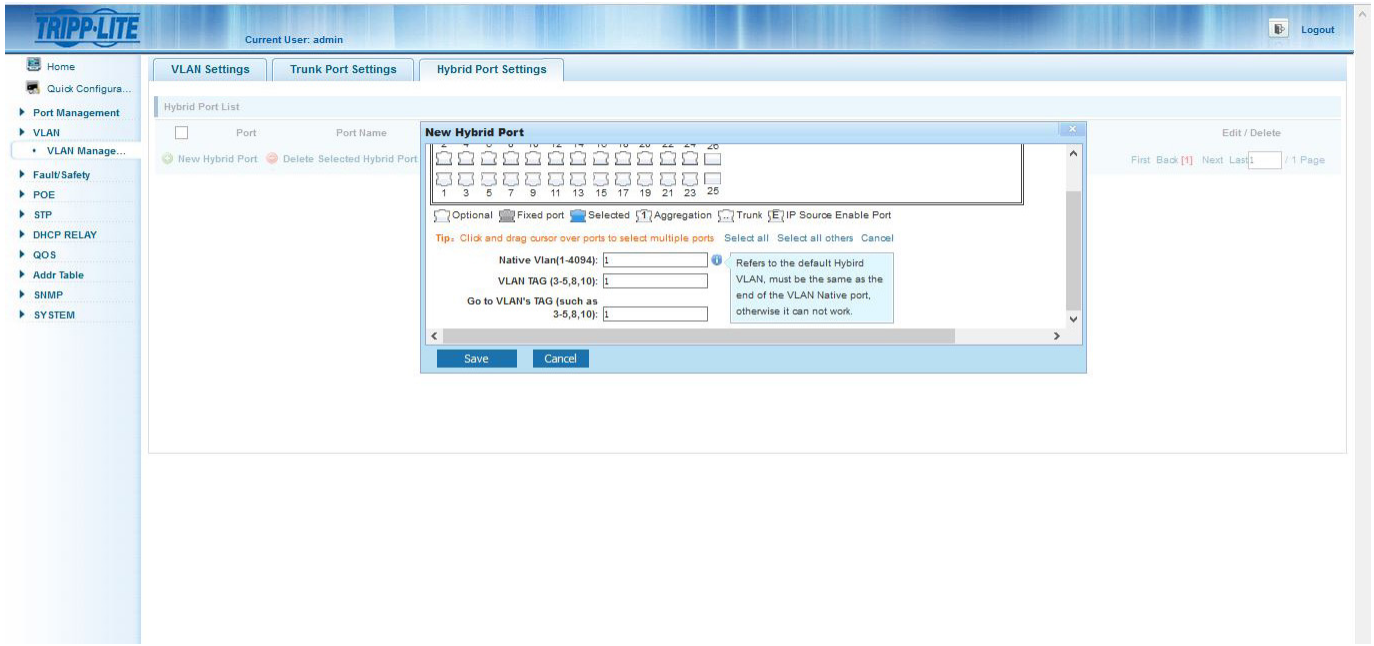


Figura 6.12: Adición de Nuevos Puertos Híbridos

6.3.2 Edición de Puertos Híbridos

Para editar, haga click en el ícono "Editar" al lado del puerto híbrido configurado a editar. Modifique los puertos seleccionados, VLAN y la etiqueta de la VLAN (Figura 6.13). Cuando haya terminado con las modificaciones del puerto híbrido, haga click en "Guardar."

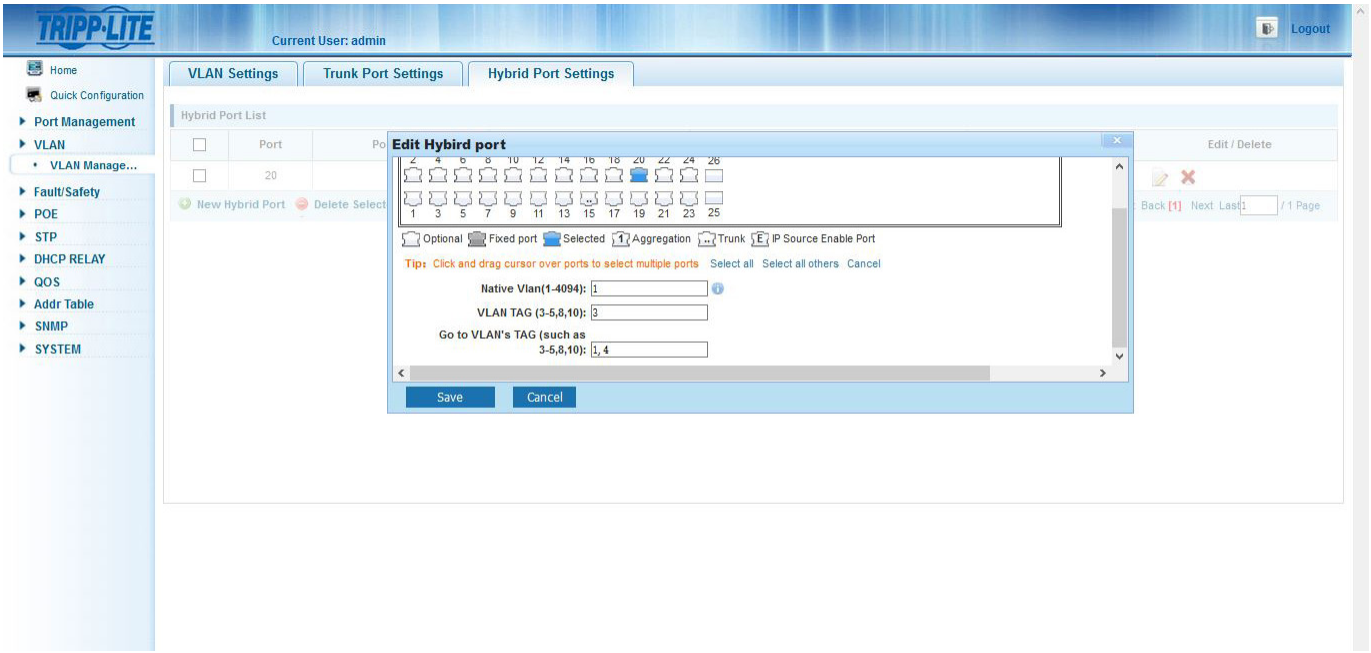


Figura 6.13: Edición de un Puerto Híbrido

6.3.3 Eliminación de Puertos Híbridos

Para eliminar un puerto híbrido, haga click en el ícono a la derecha del puerto híbrido configurado a eliminar. Para eliminar varios puertos híbridos, haga click en la casilla de verificación junto a cada puerto híbrido a ser eliminado (Figura 6.14). Seleccione la opción "Eliminar Puerto Híbrido Seleccionado" para eliminar los puertos.

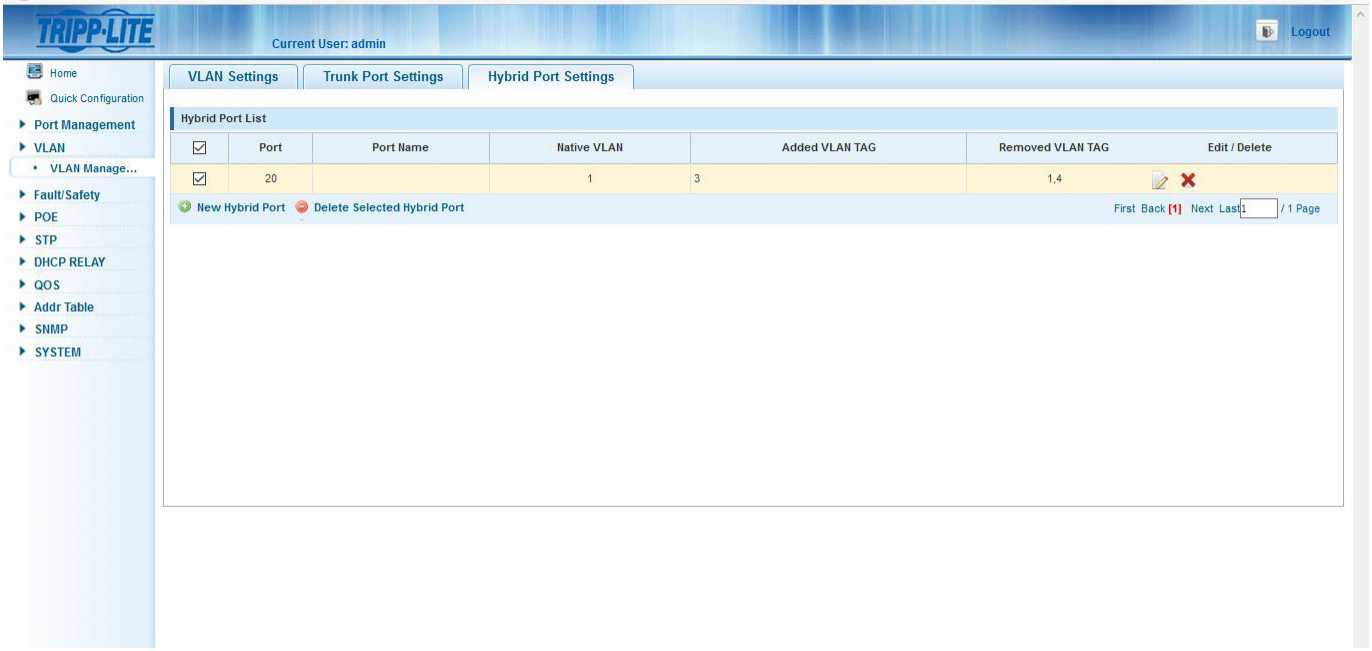


Figura 6.14: Eliminación de un Puerto Híbrido

7. Administración de Fallas / Seguridad

En la barra de navegación, seleccione “Fallas / Seguridad”. Aquí puede configurar las funciones de prevención de ataques del switch, realizar la detección de la ruta de acceso y configurar la ACL (lista de control de acceso).

7.1 Prevención de Ataques

En la barra de navegación, seleccione “Fallas / Seguridad → Prevención de Ataque → DHCP.” La activación y configuración de la Suite de Protección DHCP proporciona seguridad filtrando mensajes DHCP no confiables. Una interfaz no confiable es una interfaz que está configurada para recibir mensajes desde fuera de la red o cortafuegos. Una interfaz confiable es una interfaz que está configurada para recibir solo mensajes desde dentro de la red. La vigilancia DHCP actúa como un cortafuegos entre anfitriones y servidores DHCP no confiables. También proporciona una manera para distinguir entre interfaces no confiables conectadas al usuario final y e interfaces confiables conectadas al servidor DHCP u otro switch.

7.1.1 Activado de la Suite de Protección DHCP

Para activar la suite de protección, haga click en el botón color naranja de Desactivado para activarlo (figuras 7.1-7.2). Siga los pasos en la sección 7.1.1.8 para configurar las características de la suite de protección.

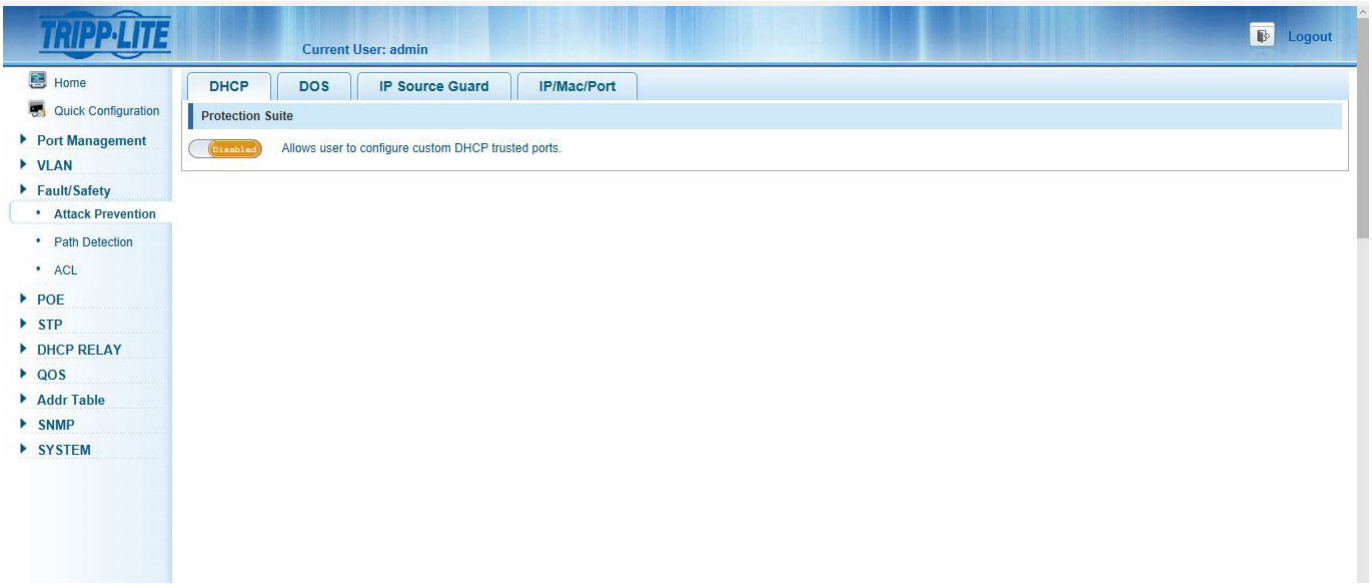


Figura 7.1: DHCP Desactivado (Predeterminado)

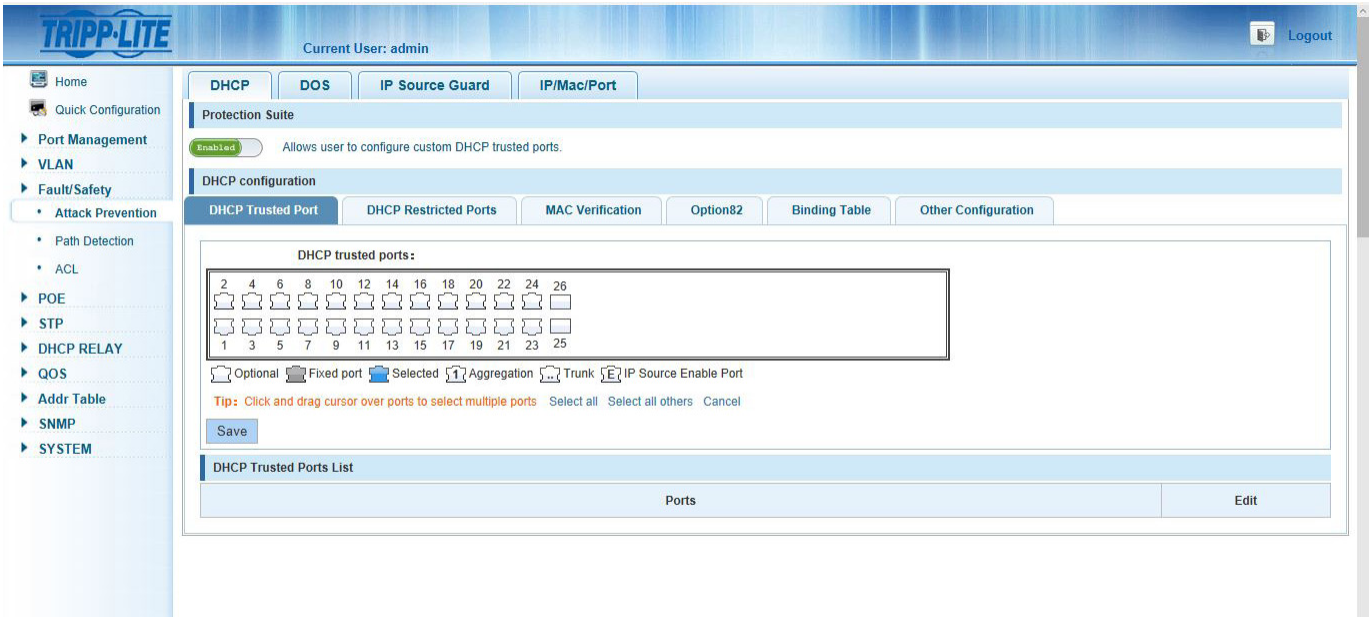


Figura 7.2: DHCP Activado

7.1.2 Configuración de VLAN de DHCP Snooping

Seleccione la pestaña "Configuración de Otros" e ingrese la VLAN de DHCP Snooping (Figura 7.3). Cuando termine, haga click en “Guardar”.

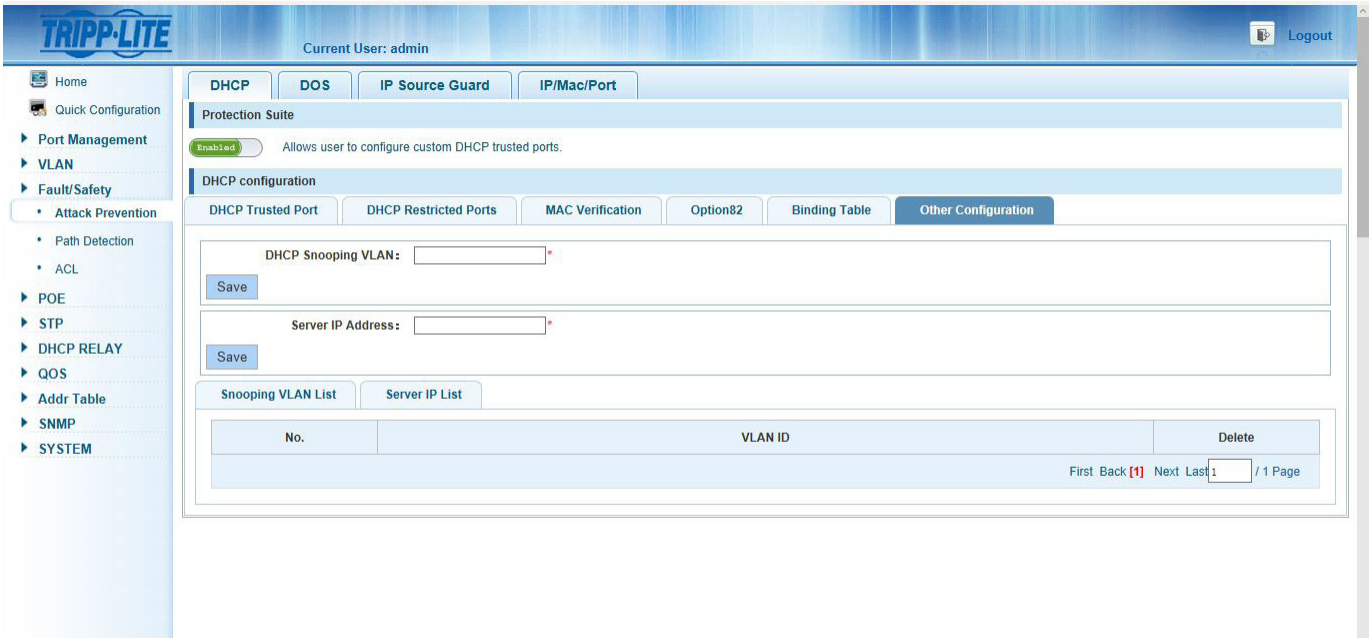


Figura 7.3: VLAN de DHCP Snooping

7.1.3 Configuración de Servidores DHCP Confiables

Seleccione la pestaña "Otras Configuraciones" y escriba las direcciones IP de los servidores DHCP confiables. Cuando termine, haga click en “Guardar”.

7.1.4 Adición de Puertos DHCP Confiables

Seleccione los puertos a configurar como parte del puerto o grupo de Puertos DHCP Confiables (Figura 7.4). Una vez los puertos han sido seleccionados, haga click en "Guardar." Para editar o eliminar Puertos DHCP Confiables, haga click en el ícono de edición junto a la lista de puertos confiables y anule la selección de los puertos de la lista. Cuando termine la edición, haga click en “Guardar”.

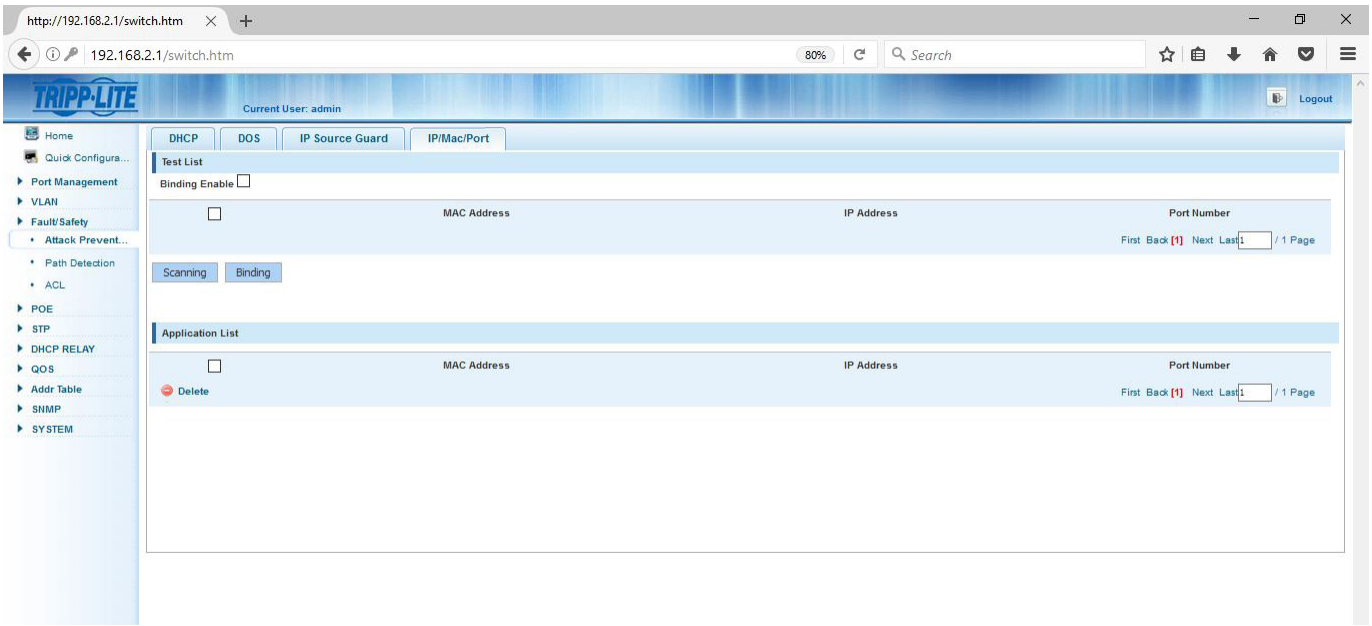


Figura 7.4: Adición de Puertos DHCP Confiables

7. Administración de Fallas / Seguridad

7.1.5 Adición y Edición de Puertos DHCP Restringidos

Para agregar Puertos DHCP Restringidos, vaya a Fallas / Seguridad → DHCP → Puertos DHCP Restringidos. Configure la lista de puertos a bloquear para que reciban direcciones DHCP mediante la selección de esos puertos. Una vez que haya seleccionado los puertos, haga click en "Guardar". Para editar o eliminar Puertos DHCP Confiables, haga click en el ícono "Editar" junto a "Prohibir DHCP para Lista de Puertos de Direcciones". A continuación, deseleccione el puerto o puertos a ser eliminados de la lista de prohibidos. Cuando termine la edición, haga click en “Guardar”.

Nota: *Eliminar todos los puertos de la lista desactiva la función.*

7.1.6 Verificación de MAC de Origen

Permitiendo la Verificación de MAC garantiza que si un paquete se recibe desde una interfaz no confiable y la MAC de origen y la dirección de MAC del cliente DHCP no coinciden, el switch desechará el paquete.

Para habilitar, haga click en la casilla de verificación "Habilitar Verificación MAC" (Figura 7.5). A continuación, añada la dirección MAC de origen y haga click en "Guardar". Una vez activado le proporcionará el estado de varios dispositivos habilitados o establece el tráfico de paquetes bloqueados intencionalmente.

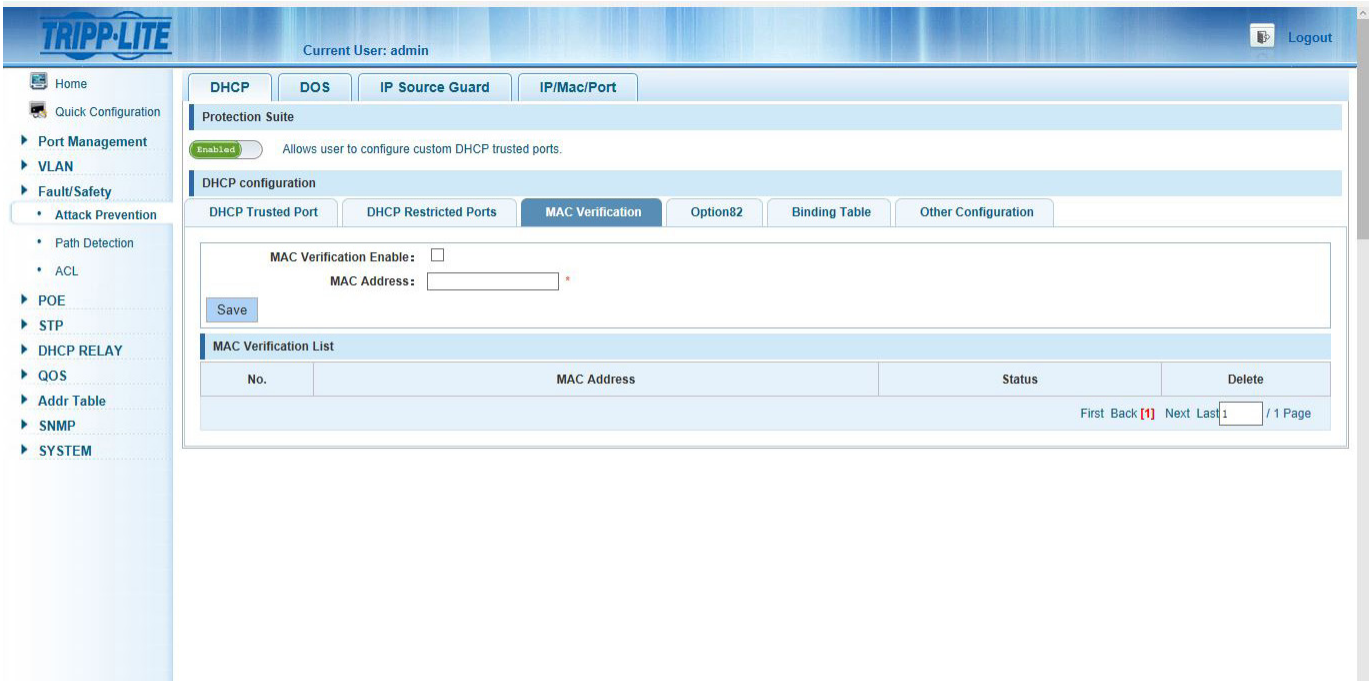


Figura 7.5: Verificación MAC

7. Administración de Fallas / Seguridad

7.1.7 Establecer Información de Option82

La habilitación de Option82 permite a un dispositivo identificarse de manera única en la red cuando se envía una solicitud de transmisión a través del switch añadiendo la información de paquetes Option82 para ser leída por el servidor DHCP. Para habilitar, haga click en la casilla de verificación "Habilitar Option82 de Cliente" (Figura 7.5).

Proporcione el nombre de circuito de control de circuito y ID de la VLAN (Figura 7.7). Una vez ingresado, haga click en “Guardar”. Para editar, haga click en la opción Editar junto al nombre de control del circuito. Cuando termine la edición, haga click en “Guardar”. Haga click en "Cancelar" para descartar las ediciones. Para eliminar una entrada de control del circuito de la lista, haga click en el ícono junto al nombre del circuito que se eliminará. La configuración se guarda en el sistema automáticamente una vez que se selecciona eliminar.

A continuación, ingrese el agente remoto "Nombre Remoto" y ID de la VLAN (Figura 7.8). Al terminar, haga click en “Guardar”. Para editar, haga click en la opción de editar junto al agente remoto a cambiarse. Cuando haya terminado la edición, haga click en “Guardar”. Haga click en "Cancelar" para descartar las ediciones. Para eliminar una entrada de agente remoto de la lista, haga click en el ícono rojo al lado del agente remoto que desea eliminar. La configuración se guarda en el sistema automáticamente una vez que se selecciona eliminar.

Seleccione la pestaña de dirección IP e introduzca la dirección IP y la ID de la VLAN del cliente

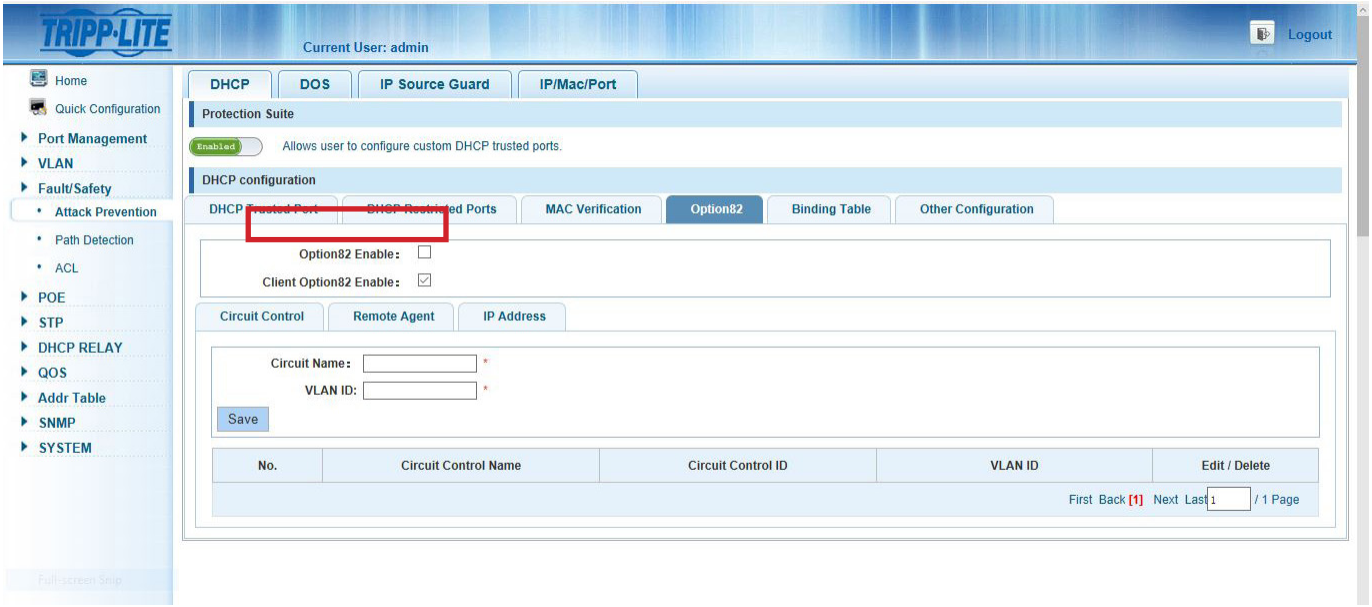


Figura 7.6: Activar Option82 de Cliente

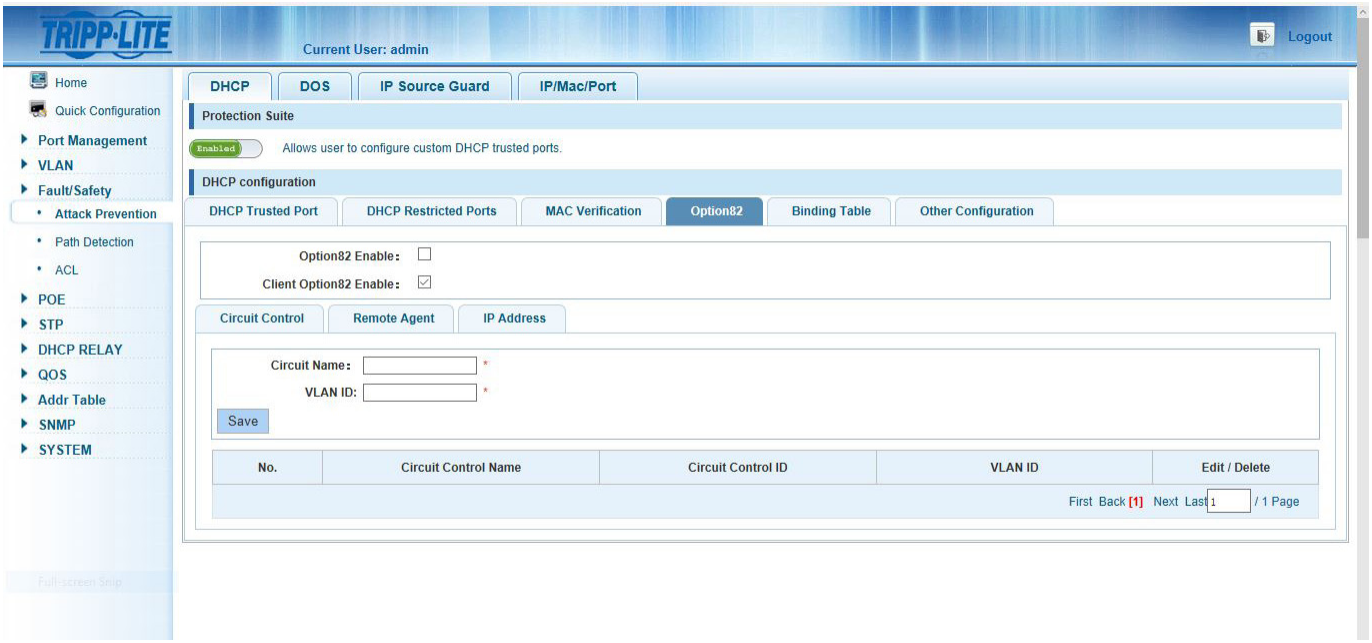


Figura 7.7: Control de Circuito de Option82

7. Administración de Fallas / Seguridad

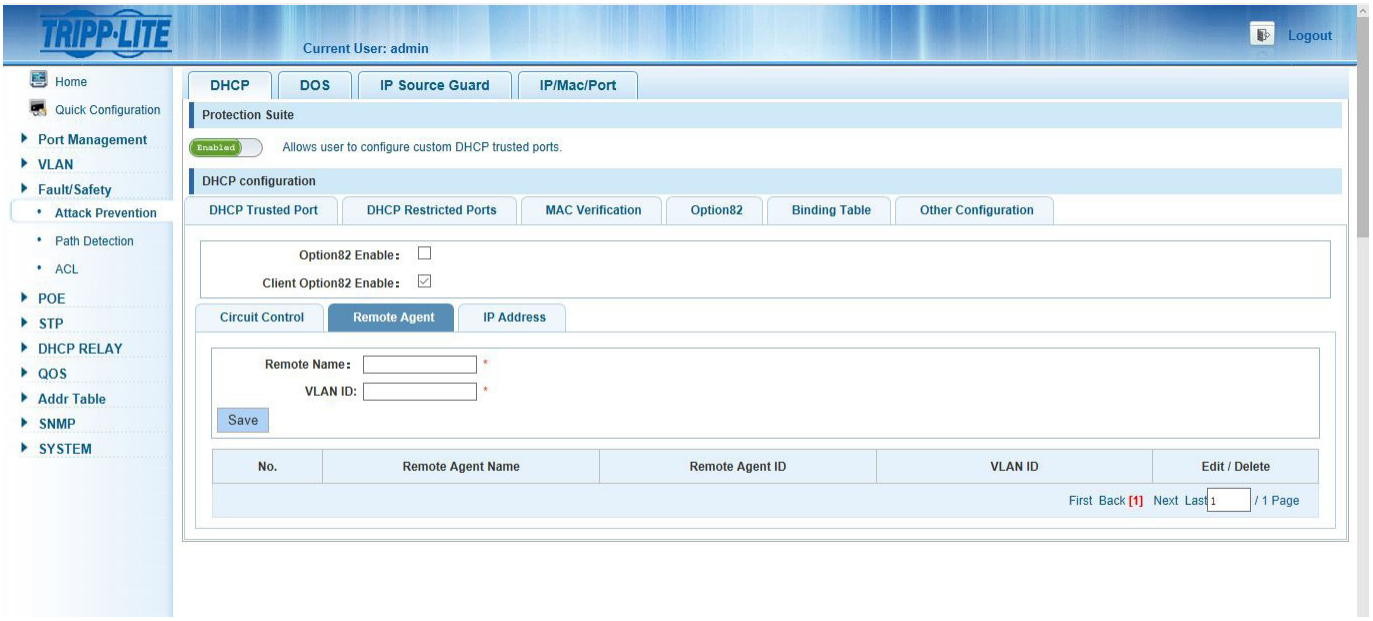


Figura 7.8: Agente Remoto de Option82

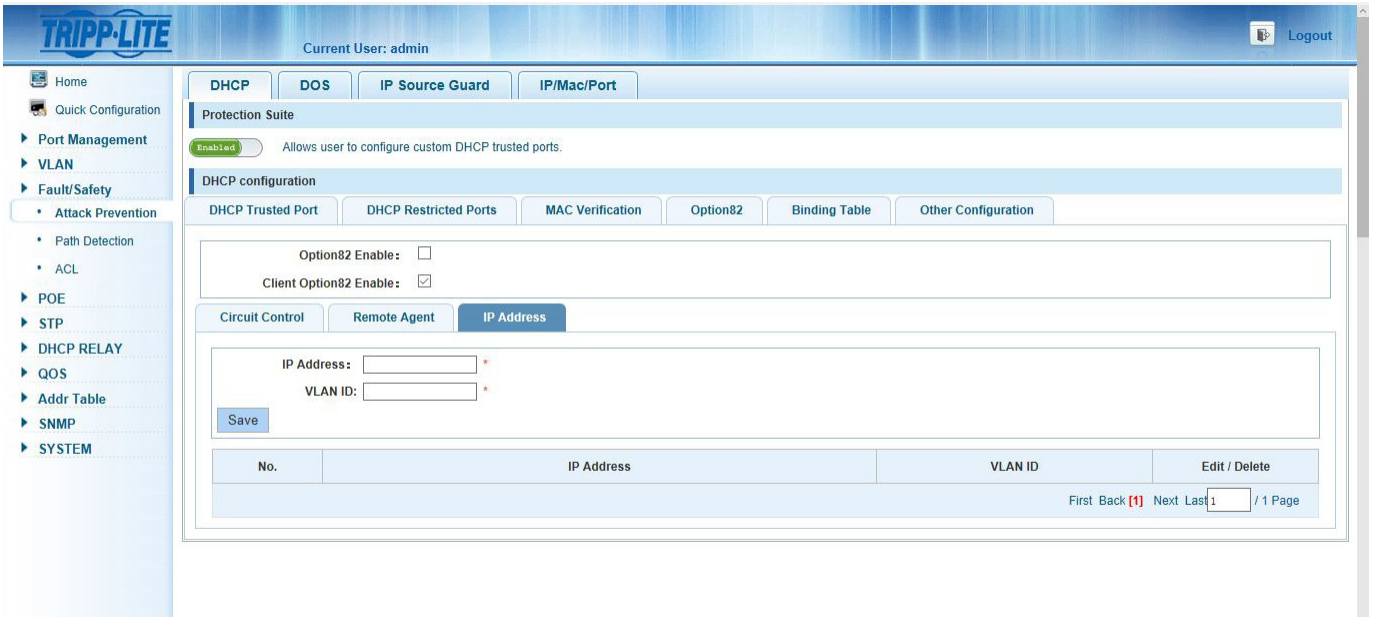


Figura 7.9: Dirección IP de Option82

A continuación, proporcione el nombre de circuito de control de circuito y la ID de la VLAN. Una vez ingresado, haga click en “Guardar”. Para editar, haga click en la opción Editar junto al nombre de control del circuito. Haga click en "Guardar" cuando haya terminado de editar o "Cancelar" para descartar ediciones. Para eliminar una entrada de control del circuito de la lista, haga click en el ícono junto al nombre del circuito que se eliminará. La configuración se guardará automáticamente en el sistema una vez que se seleccione eliminar.

A continuación, ingrese el agente remoto "Nombre Remoto" y la ID de la VLAN. Cuando termine, haga click en “Guardar”. Para editar, haga click en la opción de editar junto al agente remoto a cambiarse. Haga click en "Guardar" cuando haya terminado de editar o "Cancelar" para descartar las ediciones. Para eliminar una entrada de agente remoto de la lista, haga click en el ícono rojo al lado del agente remoto a eliminar. La configuración se guardará automáticamente en el sistema una vez que se seleccione "Eliminar".

Seleccione la pestaña de dirección IP e introduzca la dirección IP y la ID de la VLAN del cliente (Figura 7.9).

7. Administración de Fallas / Seguridad

7.1.8 Crear Tabla de Vinculación de DHCP Snooping

La Tabla de Vinculación de DHCP Snooping contiene entradas de enlace que correlacionan a los puertos no confiables. Para crear la tabla de vinculación, ingrese la dirección MAC, ID de la VLAN y seleccione el número del puerto en el menú desplegable (Figura 7.10).

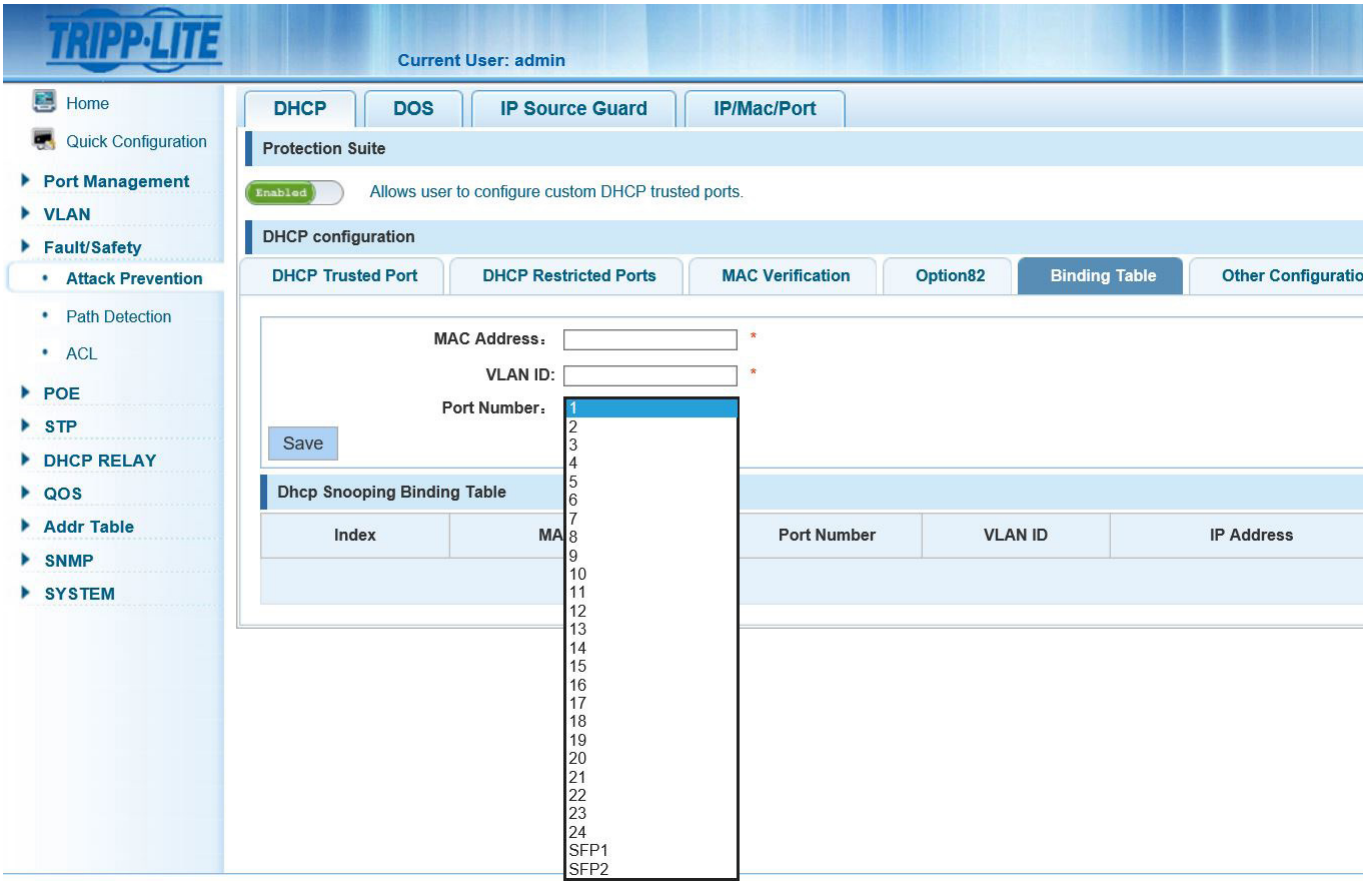


Figura 7.10: Tabla de Vinculación de DHCP

7.1.9 Prevención de Ataques por DoS [Denegación de Servicio]

Vaya a Fallas / Seguridad → Prevención de Ataque → DoS para activar la característica de Prevención de Ataque por DoS (Figura 7.11). Detendrá los intentos de que las computadoras conectadas y los recursos de red no estén disponibles para sus usuarios previstos.

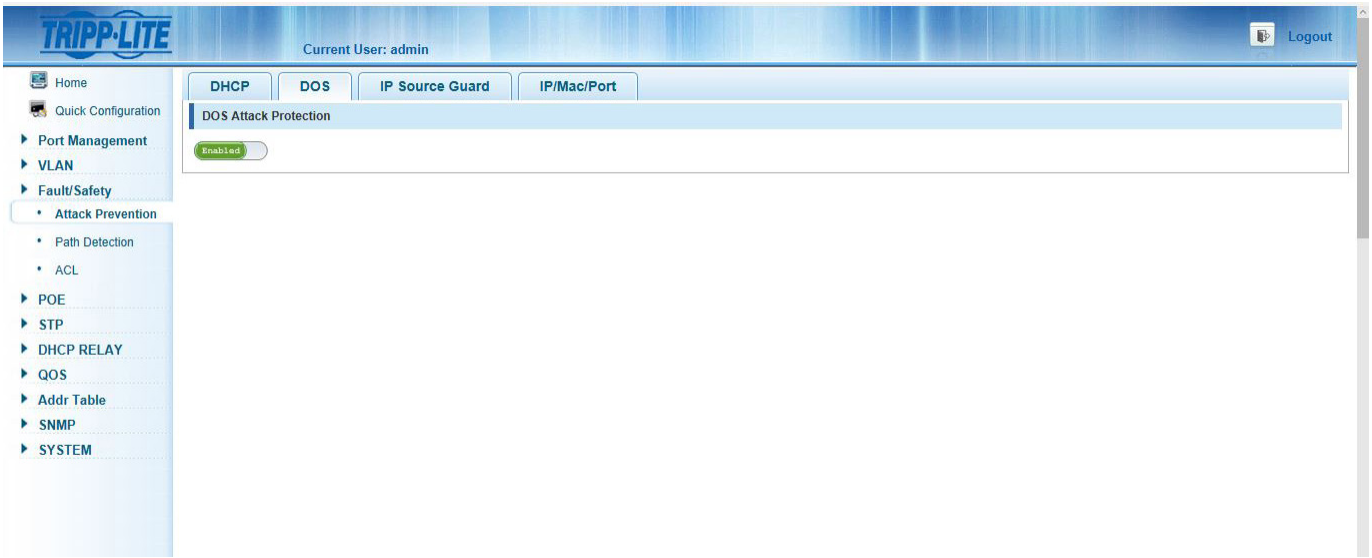


Figura 7.11: Prevención de Ataque de Denegación de Servicio

7. Administración de Fallas / Seguridad

7.1.10 Protección de la Fuente IP [IP Source Guard Protection]

La Protección de la Fuente IP ayuda a evitar mensajes ilegales a través de un puerto bloqueando las comunicaciones con recursos de red para mejorar la seguridad general del puerto. Para agregar manualmente Protección de la Fuente IP, seleccione uno o varios puertos de fuente y haga click en "Guardar" (Figura 7.12).

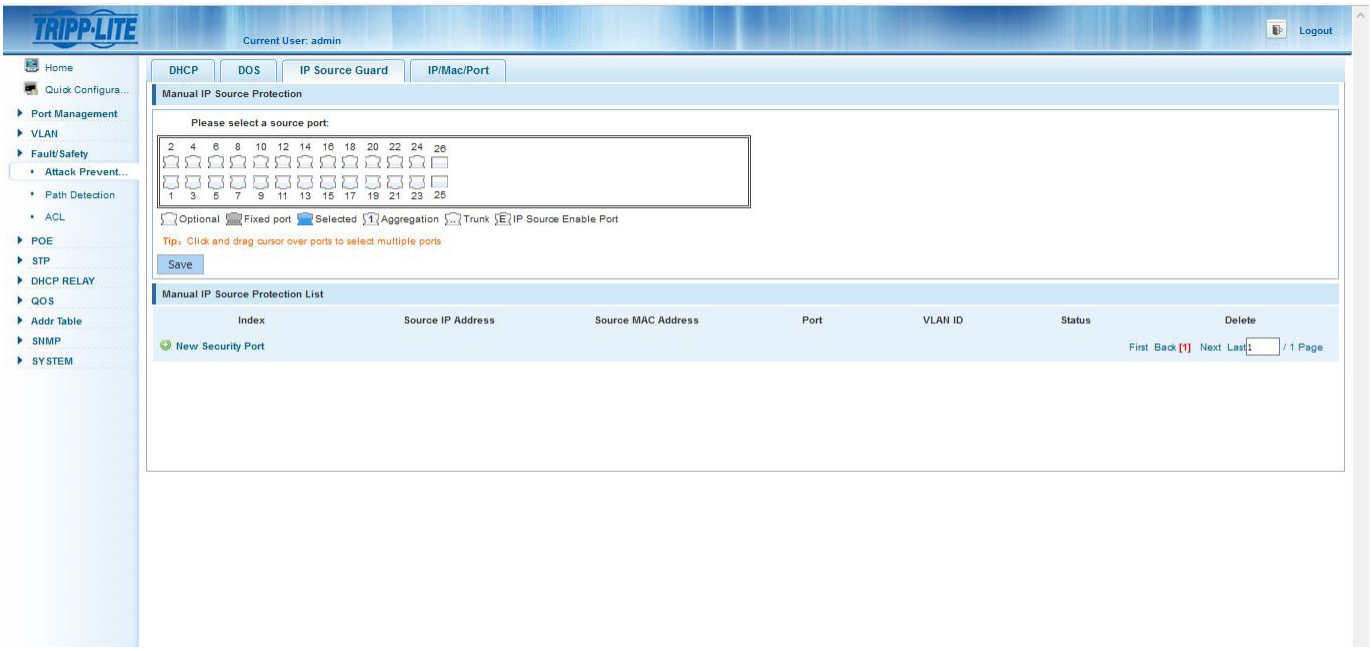


Figure 7.12: Protección de la Fuente IP

A continuación, haga click en el botón de "Nuevo Puerto de Seguridad" debajo de la lista. Se abrirá una ventana para seleccionar el puerto de seguridad (Figura 7.13). Introduzca el ID de VLAN, la dirección IP origen, la dirección MAC de origen, a continuación, seleccione el puerto de seguridad. Cuando termine, haga click en “Guardar”.

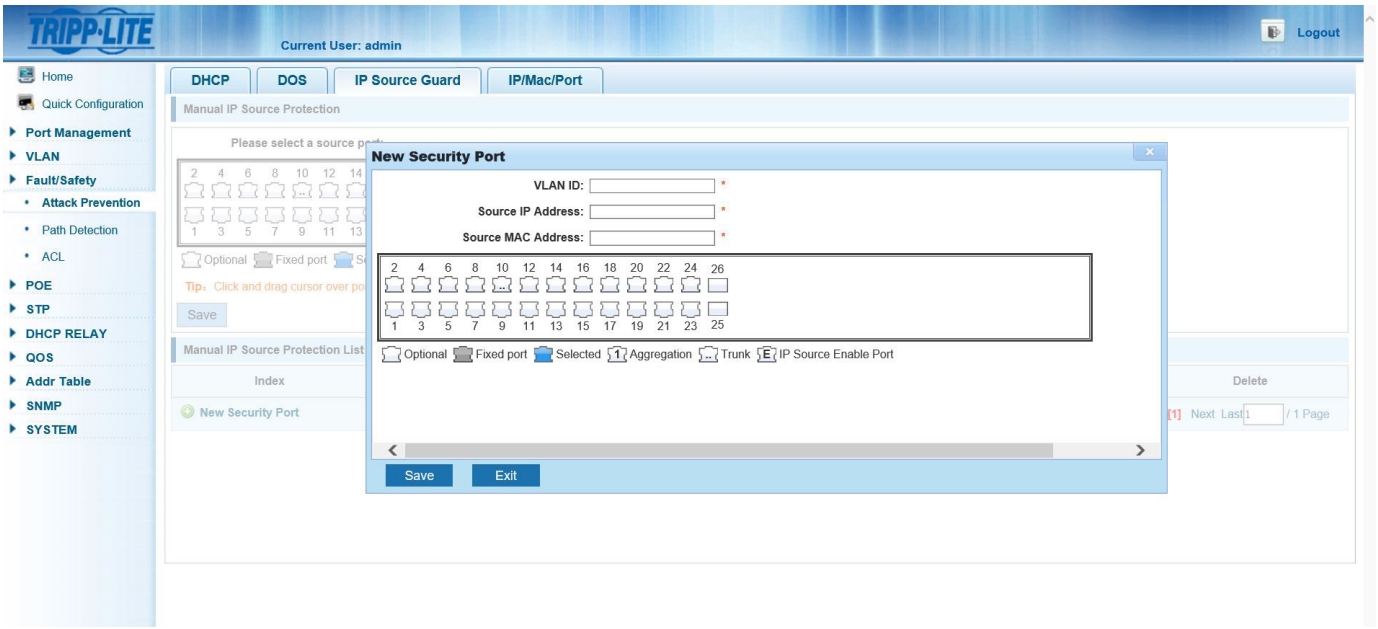


Figura 7.13: Adición de Puertos de Seguridad

7. Administración de Fallas / Seguridad

7.1.11 Lista de Vinculación IP / MAC / Puerto

Para permitir al switch aprender automáticamente las direcciones IP basadas en puerto y las relaciones de mapeo de MAC, realice los siguientes pasos (Figura 7.14):

1) Haga click en la casilla de verificación "Activar vinculación".
2) Escanee los puertos para obtener la mapeo de puerto.
3) A continuación, seleccione el puerto a vincular y éste se añadirá a la Lista de Aplicaciones.

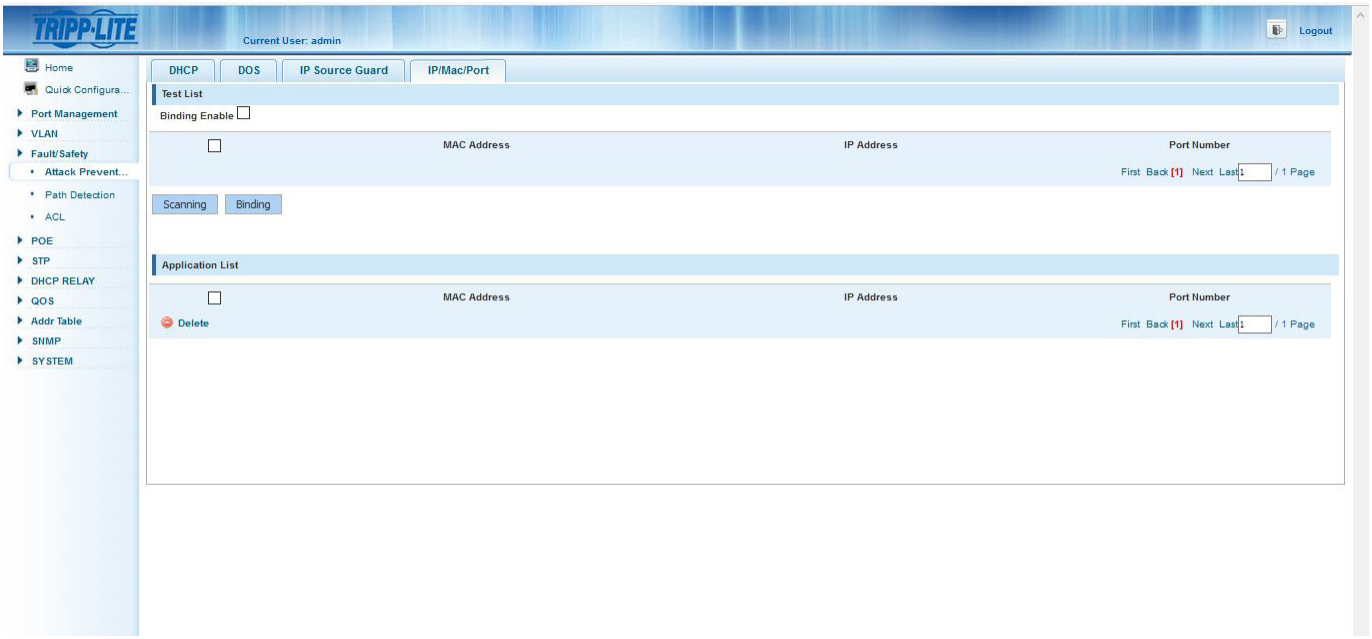


Figura 7.14: Resumen de Lista de Vinculación de IP / MAC / Puerto

Para eliminar una vinculación, haga click en la casilla de verificación junto a la relación de la vinculación a eliminar y luego seleccione el ícono "Eliminar". Los parámetros se guardarán automáticamente.

7. Administración de Fallas / Seguridad

7.2 Detección de Ruta

La función Ping de Detección de Ruta → ayuda a verificar el estado de una conexión, mientras que el Tracert muestra cuantas rutas y cuanto tardan para llegar a un destino

7.2.1 Prueba de Ping

Seleccione “Fallas / Seguridad → Detección de Ruta” para determinar si un servidor está respondiendo (Figura 7.15). Introduzca la dirección IP para hacer ping en el campo "IP de Destino", el tiempo de espera de 1 a 10 segundos (el predeterminado es 2) y el número de ping de repetición de 1 a 1000 (el valor predeterminad es 5). Seleccione "Iniciar Prueba" para comenzar la prueba y mostrar los resultados.

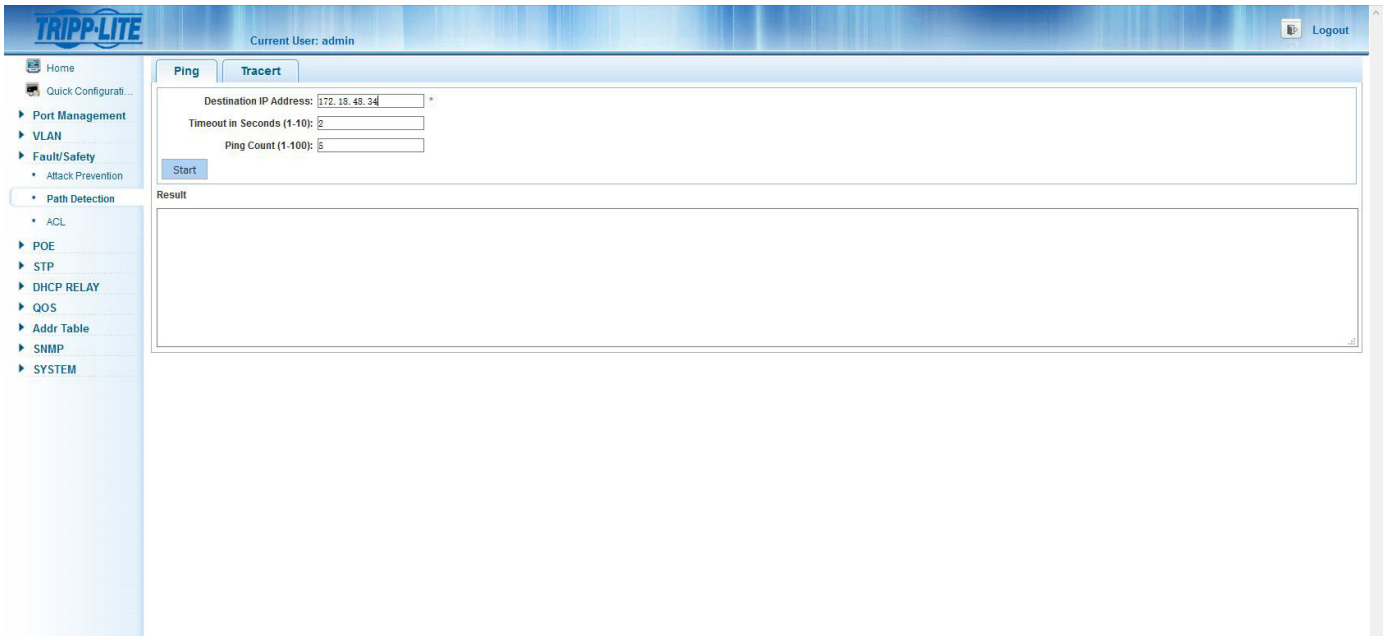


Figura 7.15: Prueba de Ping

7.2.2 Tracert

Utilice la función de Tracert para trazar la ruta de cada ruteador que un paquete de datos atraviesa antes de llegar a su destino. Seleccione “Fallas / Seguridad → Tracert” e ingrese la dirección IP en el campo de “Dirección IP de Destino” (Figura 7.16). A continuación, escriba el período de tiempo de espera entre 1y10 (el valor predeterminado es de 2 milisegundos).

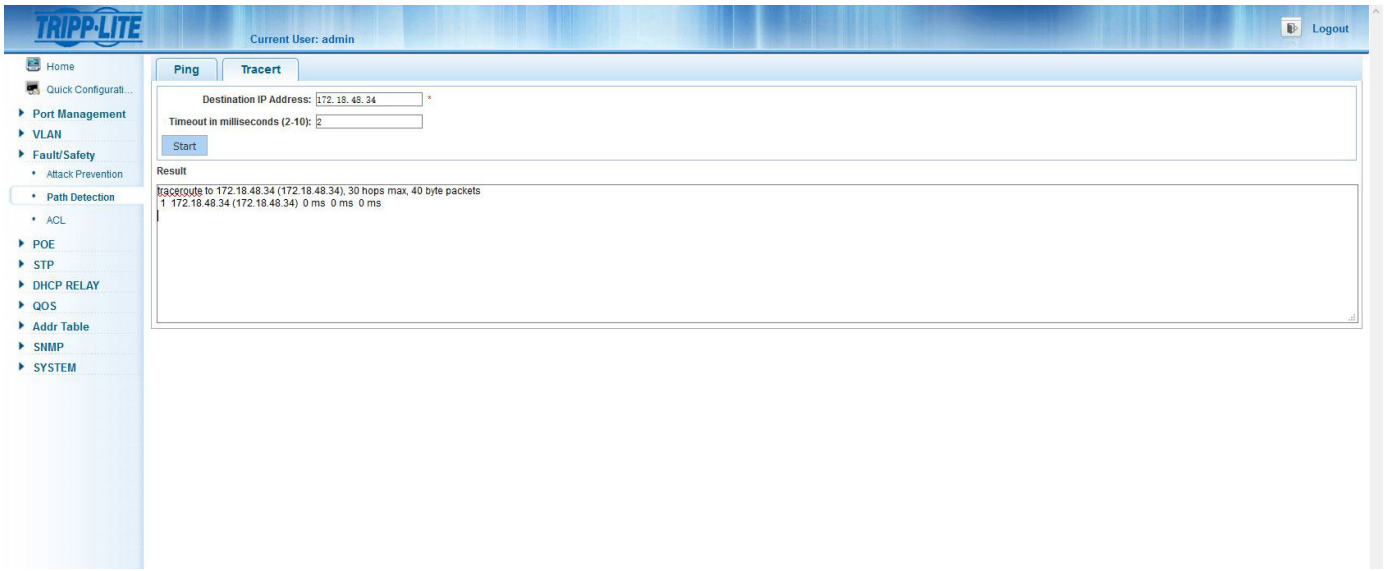


Figura 7.16: Función Tracert

7. Administración de Fallas / Seguridad

7.3 Listas de Control de Acceso [ACLs]

Las Listas de Control de Acceso dan a los dispositivos en la red la capacidad de conceder acceso o ignorar las peticiones de algunos usuarios y sistemas a los recursos de red disponibles.

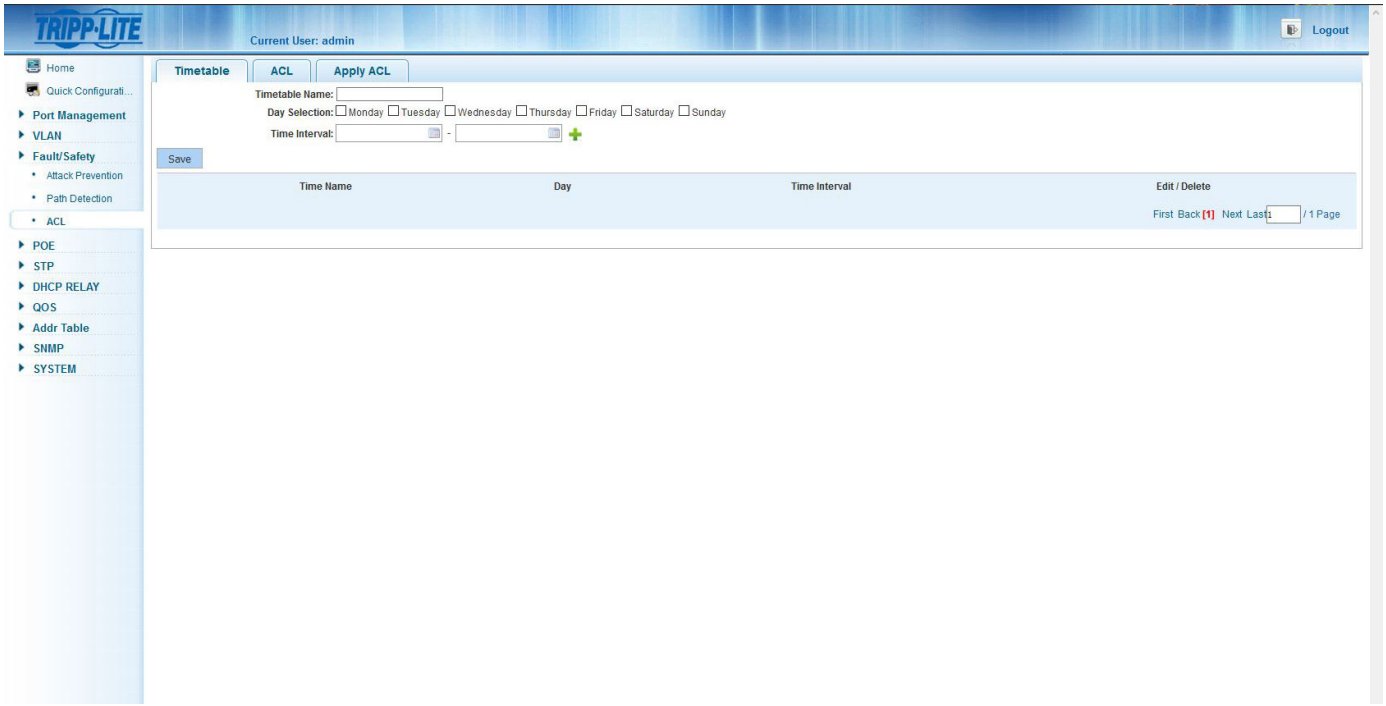


Figura 7.17: Descripción General de ACL

Para configurar las ACLs, vaya a “Fallas / Seguridad → ACL” y ejecute las siguientes acciones:

1. Nombre el cronograma. Introduzca una marca de verificación para los días en que desee que se aplique el cronograma. A continuación, ingrese los tiempos de intervalo para el cronograma. (Figura 7.18). Pueden crearse múltiples cronogramas por grupo. Puede editar los cronogramas de ACL haciendo click en el ícono Editar y ajustar los días y las horas. Para guardar los cambios, haga click en el botón "Guardar". Haga click en "Cancelar" para descartar los cambios. Si ya no es necesario un cronograma, haga click en el ícono Eliminar para eliminarlo de la lista.
2. A continuación, cree una regla para permitir o denegar el acceso mediante la configuración de la ACL contra los cronogramas. Seleccione la pestaña ACL y haga click en el botón "Crear ACL". En la nueva ventana de regla de acceso de la ACL (Figura 7.19), establezca el Número de la ACL del 100 al 199, la acción de Permitir o Denegar el permiso, el Tipo de Protocolo (IP, UDP o TCP) y el Nombre de la ACL a la que se aplicará la regla desde la lista desplegable. Si la regla se aplicará a cualquier dirección IP de fuente o destino, deje marcadas las casillas por defecto para estas dos opciones. Para especificar una fuente o la dirección IP de destino, desmarque la casilla aplicable para obtener la opción de entrar en la dirección IP única o la dirección IP y máscara de subred. Si configura la regla para TCP o UDP para una sola fuente o puerto de destino, desmarque cualquier casilla de verificación de puerto fuente. A continuación, introduzca las direcciones de un solo puerto de origen o destino del 0 al 65535. Una vez configurado, haga click en el botón "Guardar". Para borrar la regla para configurar para permitir o denegar la configuración de ACL, haga click en el ícono rojo.
3. Seleccione la pestaña Aplicar ACL, para configurar las ACLs para un solo o varios puertos Ethernet. Ingrese el Número de la ACL de la regla aplicable, luego haga click en "Guardar".

Nota: *Las ACLs configuradas y activas pueden ser eliminadas siguiendo los pasos anteriores en orden inverso.*

7. Administración de Fallas / Seguridad

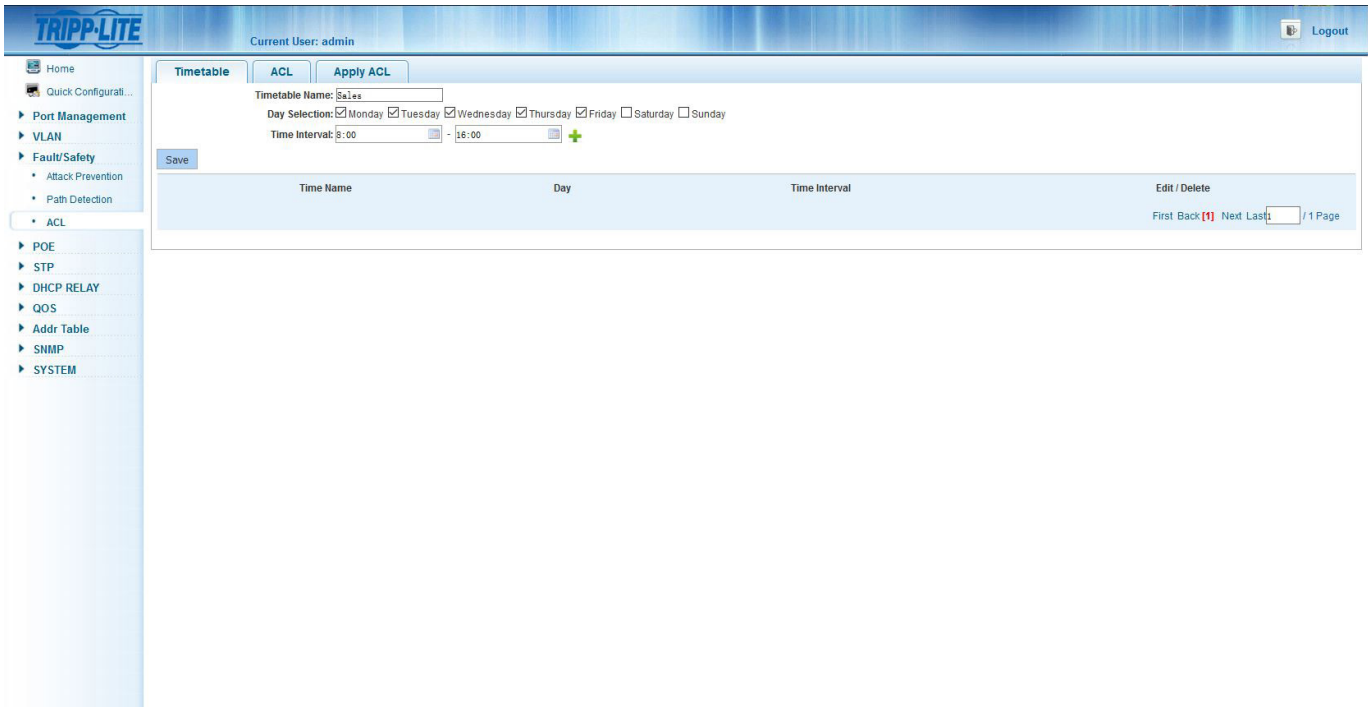


Figura 7.18: Crear Cronograma

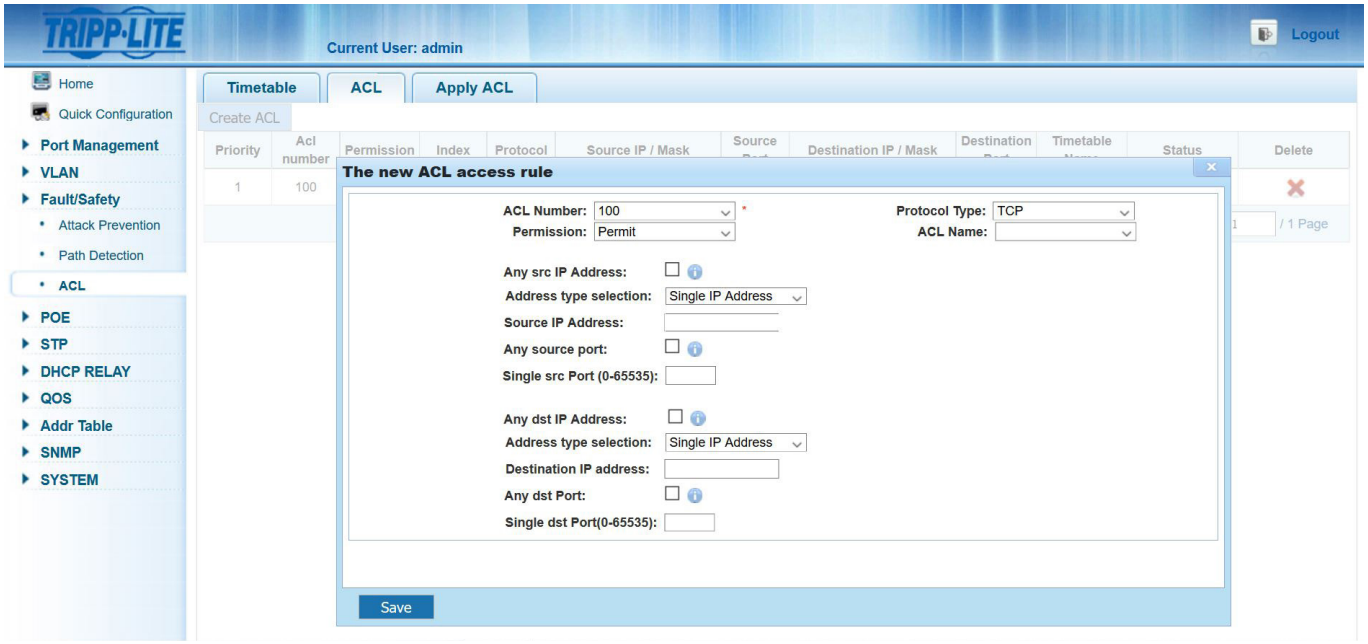


Figura 7.19: Creación de una Regla de Acceso de la ACL

8. PoE (Energía sobre la Ethernet, soportada por modelos selectos)

PoE (disponible en switches selectos) proporciona alimentación y comunicación con múltiples dispositivos habilitados para PoE y PoE+. Cada puerto es capaz de soportar hasta 32W de potencia por PoE. El voltaje máximo suministrado por el sistema de PoE es de 51.2V.

8.1 Configuración de Administración de PoE

Seleccione PoE → Configuración de PoE → Administración → Información de Estado de PoE (Figura 8.1). Vea la información del estado de PoE del switch de red relacionada con su operación, potencia nominal total, potencia límite de corriente, umbral de alarma, voltaje de la corriente y el porcentaje de energía de reserva que está disponible.

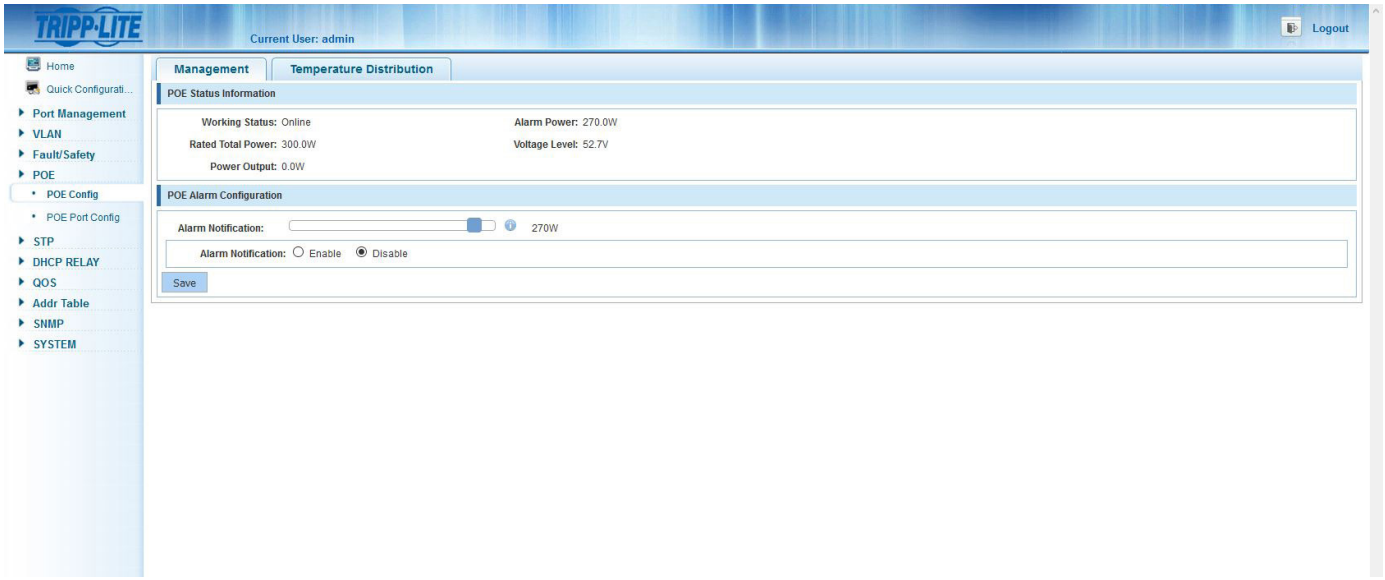


Figura 8.1: Administración de PoE

8.1.1 Umbral de Alarma de Consumo de Potencia de PoE

Seleccione PoE → Configuración de PoE → Administración → Configuración de Alarma de PoE (Figura 8.2). Esta función ajusta el umbral de potencia total para activar una notificación de trampa si se supera el nivel de potencia de PoE. Utilice el regulador de energía de Reserva para ajustar cuanta energía de reserva desea asignar para el uso de la aplicación en el futuro. Una vez establecidos la alarma y los umbrales de reserva, haga click en “Guardar”.

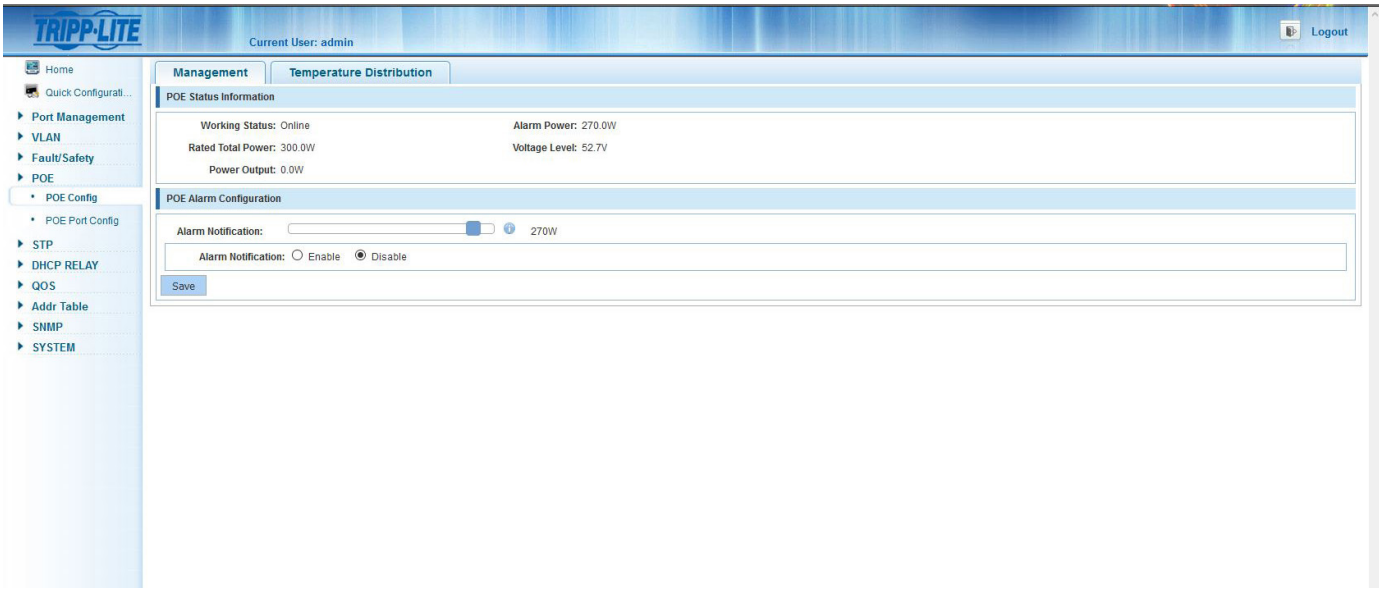


Figure 8.2: Configuración de Alarmas de PoE

8. PoE (Energía sobre la Ethernet, soportada por modelos selectos)

8.1.2 Umbrales de Distribución de Temperatura / Alarma de PoE

Establece el umbral de temperatura de alarma para cada uno de los tres chipsets de PoE. El rango de la temperatura de alarma es de 70 ºC ~ 149 °C [158 ºF ~ 300 °F].

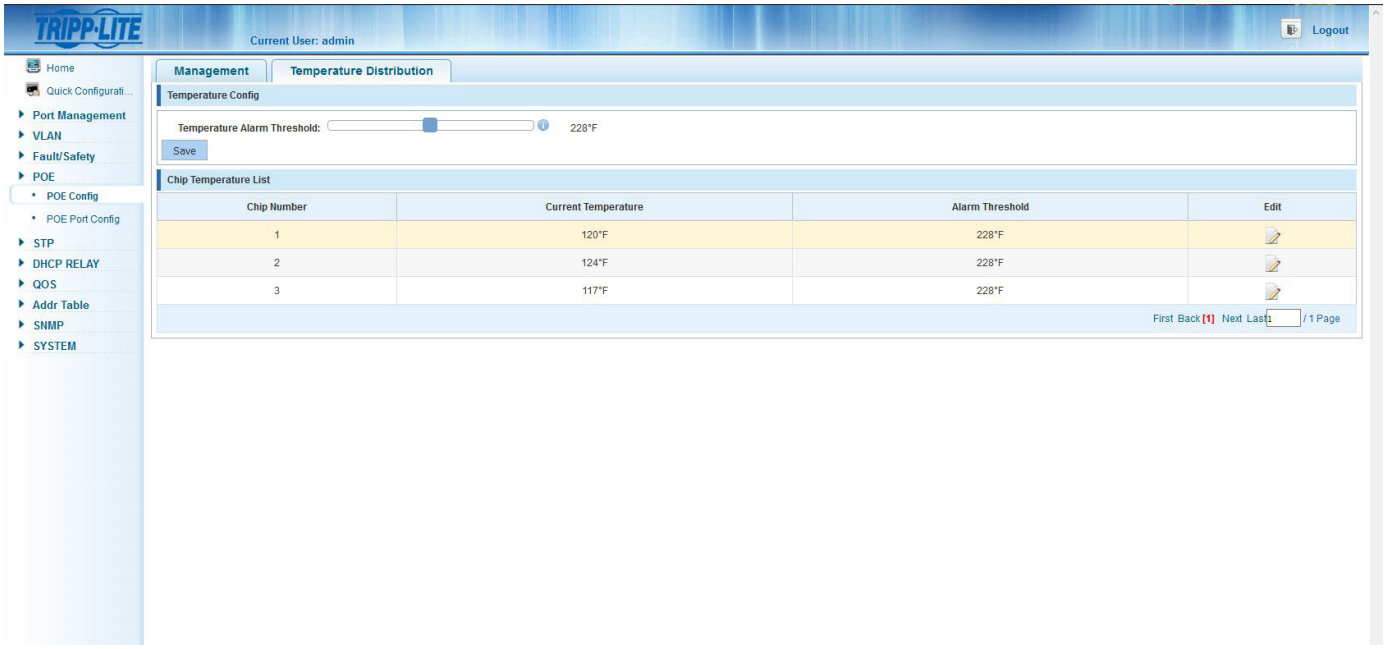


Figura 8.3: Distribución de Temperatura de PoE

8.2 Configuración de Puerto con PoE

Seleccione PoE → Configuración de Puerto de PoE (Figura 8.4). Ajusta las capacidades de PoE de cada puerto. Haga click en el ícono de edición para activar o desactivar la PoE, cambiar el uso de la potencia máxima, establecer la prioridad y configurar el modo de detección AF, AT, AT&F para los dispositivos conectados.

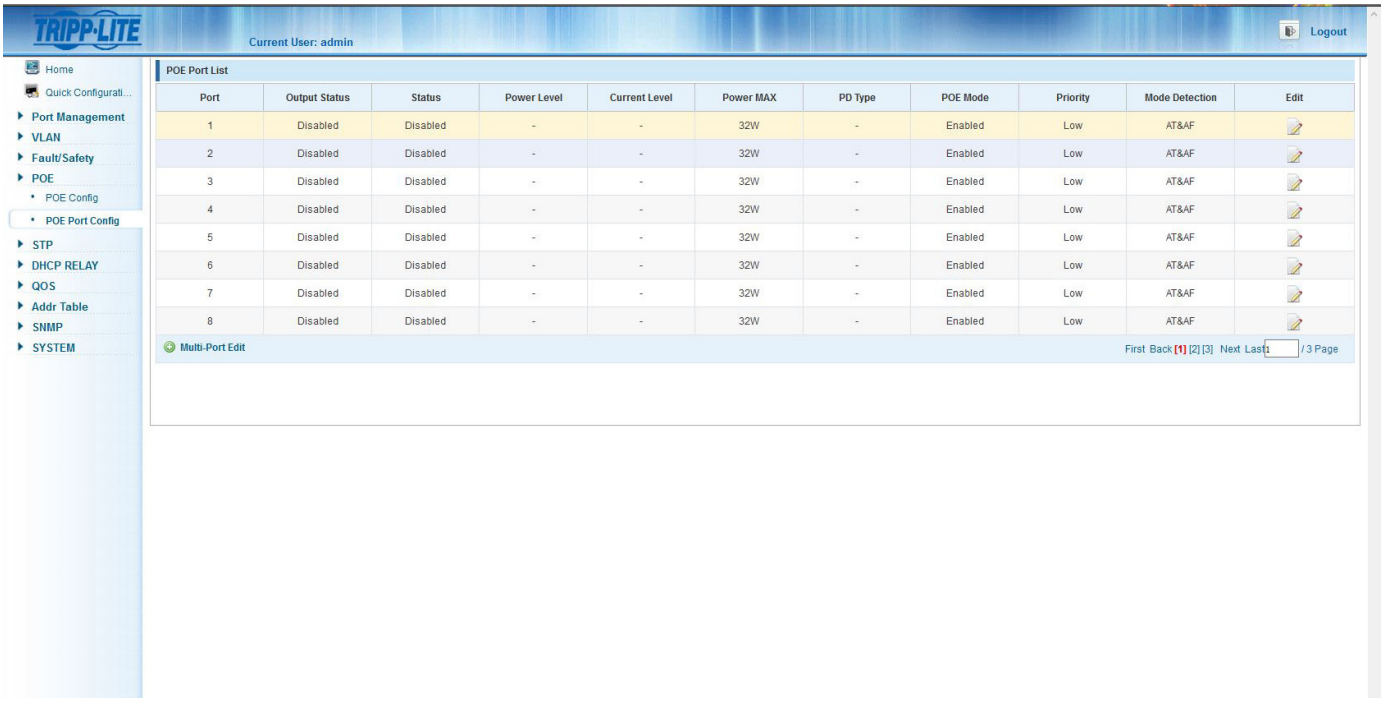


Figure 8.4: Configuración de Puerto con PoE

9. Administración de Protocolo Spanning Tree Múltiple (MSTP)

La Administración de Protocolo Spanning Tree Múltiple [MSTP] proporciona una topología lógica libre de bucles para redes Ethernet. El MSTP evita bucles de puente y tormentas de transmisión resultantes. La redundancia de enlace es otra función MSTP para asegurar que las conexiones de red tienen una ruta de acceso redundante en caso de que un enlace activo se caiga.

9.1 Configuración de Región MSTP

Seleccione STP → Región MSTP para crear instancias MSTP (Figura 9.1).

9.1.1 Configuración MSTP

Ingrese el nombre de región y el nivel de revisión de la instancia MSTP.

9.1.2 Mapeo de Instancia

Elija una ID de instancia del 1 a 16 y las VLANs asociadas a las que se asignará. (La instancia de 0 se asigna de manera predeterminadaa todas las VLANs)

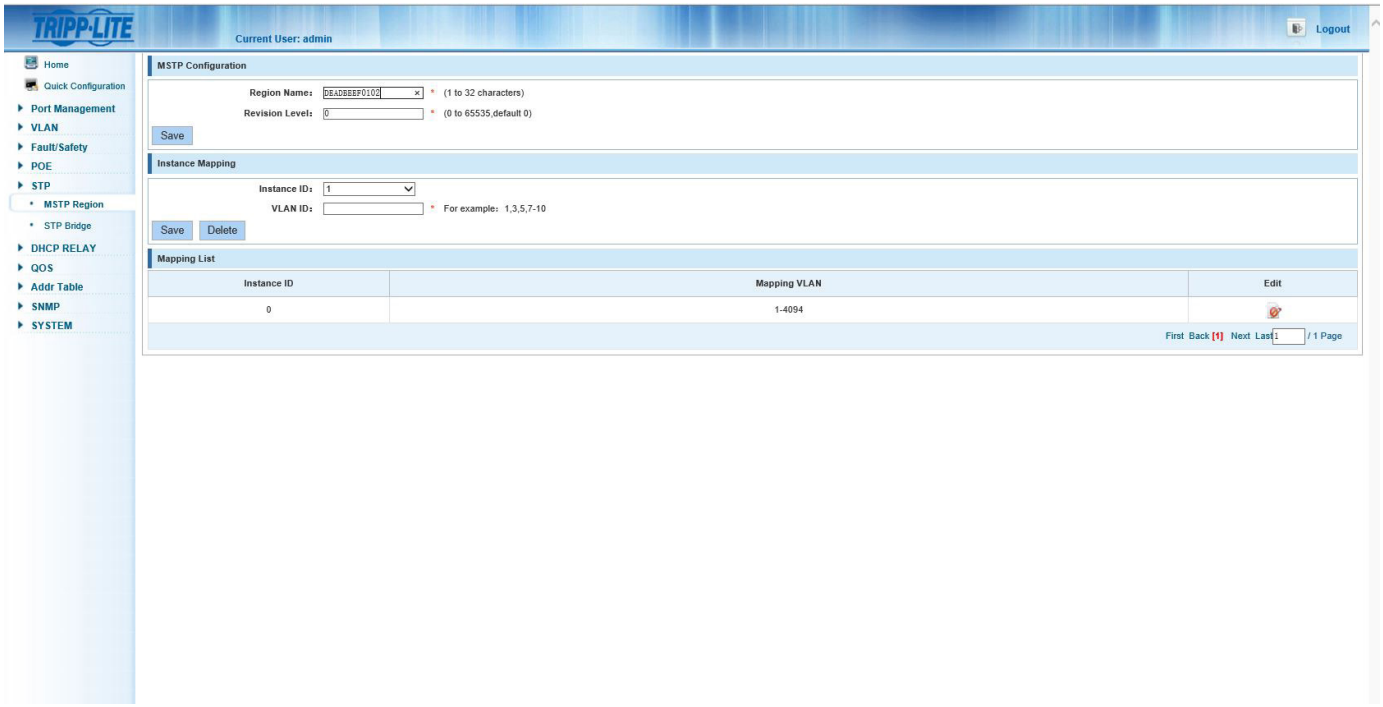


Figura 9.1: Configuración MSTP y mapeo de Instancia

9.1.3 Lista de Mapeo

La lista de mapeo es una lista de todas las instancias de región MSTP creadas. Sólo las instancias que han sido creadas se pueden editar o eliminar. Cuando se elimina una instancia, la VLAN asociada vuelve a la ID de la instancia predeterminada de 0.

9. Administración de Protocolo Spanning Tree Múltiple (MSTP)

9.2 Configuración de Puente de Protocolo Spanning Tree (STP)

Seleccione STP → Configuración de Puente STP (Figura 9.2) y ejecute los siguientes pasos:

1. Active la Prioridad de la Instancia haciendo click en la casilla de verificación.
2. Seleccione el ID de la instancia del 0 al 16.
3. Seleccione la prioridad de 0 a 61440 (predeterminada: 32768).
4. Active el puente STP seleccionando ON, ingrese Hello Time de 1 a 10 segundos (predeterminado: 2s), Retraso de Reenvío [Forward Delay] de 4 a 30 segundos (predeterminado: 10s), Establezca el modo STP, RSTP, MSTP; Edad MAX de 6 a 40 segundos (predeterminado: 10s); y Enlaces [Hops] Max de 1 a 40 segundos (predeterminado: 10). Haga click en “Guardar”.
5. “Mostrar Info de Puente” muestra la información actual del puente STP configurado (Figura 9.3).

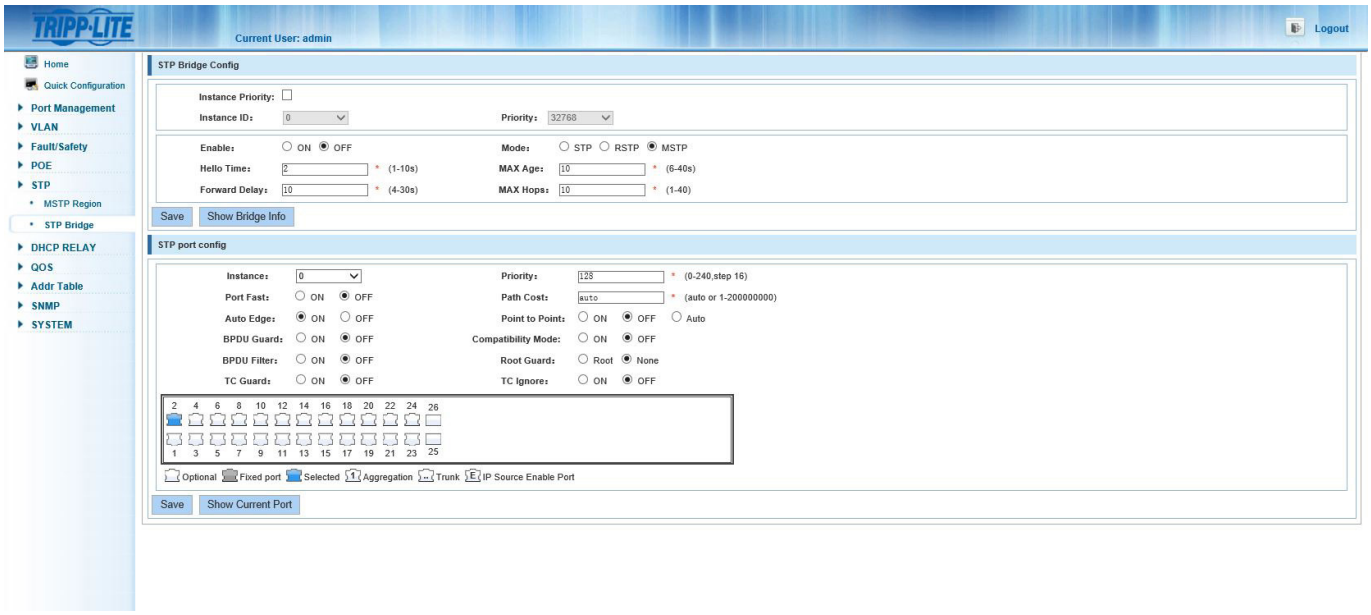


Figura 9.2: Configuración de Puente STP y Configuración del Puerto STP

Figura 9.3: Información del Puente STP

9. Administración de Protocolo Spanning Tree Múltiple (MSTP)

9.3 Configuración de Puerto STP

Siga los pasos para configurar el puerto STP:

1. Seleccione la ID de puente de instancia que fue creada antes
2. Seleccione Port Fast (predeterminado: OFF)
3. Seleccione Auto Edge (predeterminado: ON)
4. Seleccione BPDU Guard (predeterminado: OFF)
5. Seleccione Filtro BPDU (predeterminado: OFF)
6. Seleccione TC Guard (predeterminado: OFF)
7. Seleccione la prioridad de 0 a 240; debe introducirse en múltiplos de 16 (predeterminado: 128)
8. Seleccione Ruta CoS en Auto o 1 a 200000000 (predeterminado: Auto)
9. Establezca Punto a Punto en ON, OFF o AUTO (predeterminado: OFF)
10. Establezca Modo de Compatibilidad (predeterminado: OFF)
11. Establezca Root Guard en Root o Ninguno (predeterminado: Ninguno)
12. Establezca TC Ignore (predeterminado: OFF)
13. Haga click en “Guardar”
14. Haga click en Mostrar Puerto Actual para visualizar la información del puerto actual STP

Figura 9.4: Información de Puerto Actual STP

10. Relevador de DHCP

El Relevador de DHCP envía mensajes de DHCP entre clientes DHCP y servidores DHCP en diferentes redes IP. En esta área, se puede editar la configuración de relevador y Option82.

10.1 Configuración de Agente Relevador de DHCP

Seleccione RELEVADOR DE DHCP → Relevador de DHCP (Figura 10.1). Haga click en la casilla de verificación para habilitar el Relevador de DHCP. Predeterminado, “Campo Confiable de Opción DHCP” ya está activado.

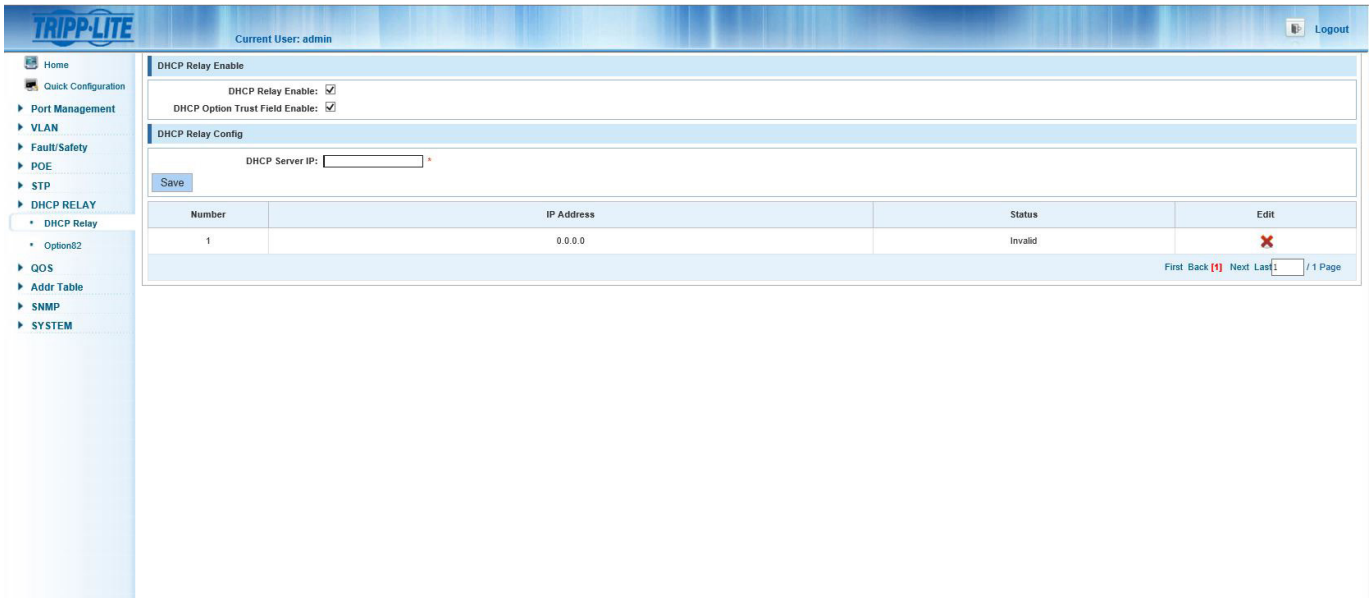


Figura 10.1: Relevador de DHCP Activado

10.2 Configuración de Option82

Seleccione RELEVADOR DE DHCP → Option82. En la configuración de Option82 (Figura 10.2) ingrese la siguiente información:

10.2.1 Control de Circuito

Introduzca la ID de Control del Circuito de 3 a 63 y el ID de VLAN. Haga click en "Guardar" y cada instancia se guardará en una lista.

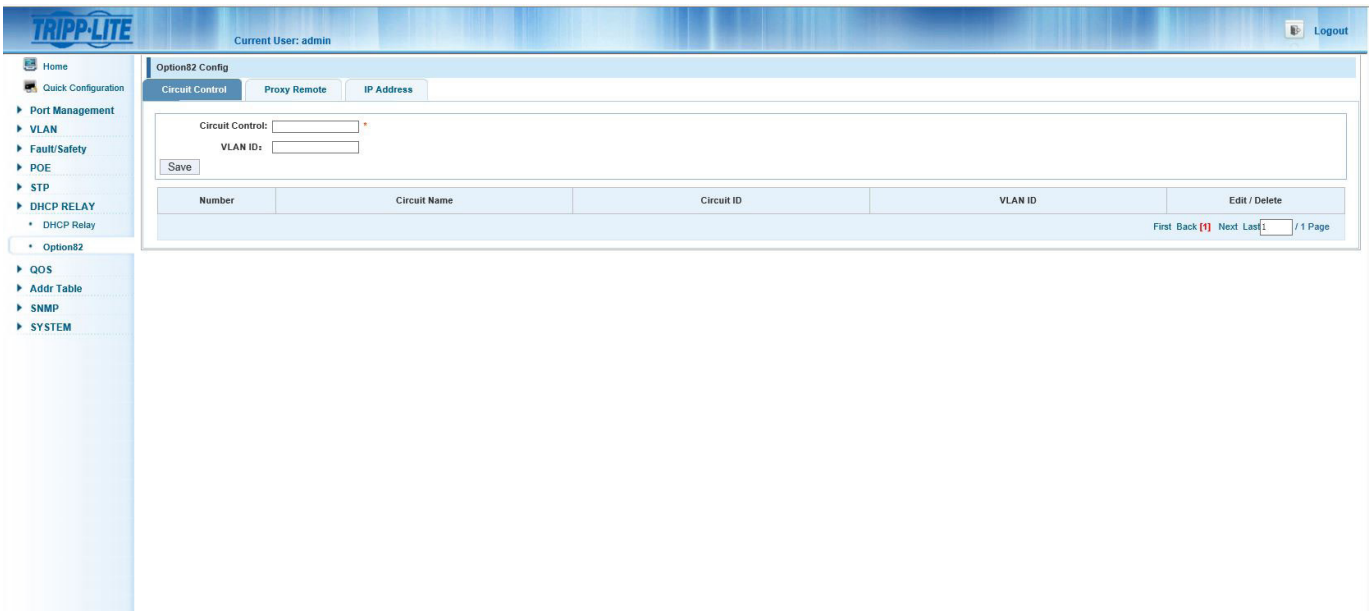


Figura 10.2: Control de Circuito de Option82

10.2.2 Proxy Remoto

Ingrese el Proxy Remoto (límite: 63 caracteres) y la ID de VLAN (Figura 10.3). Haga click en "Guardar" y cada entrada se guardará en la lista.

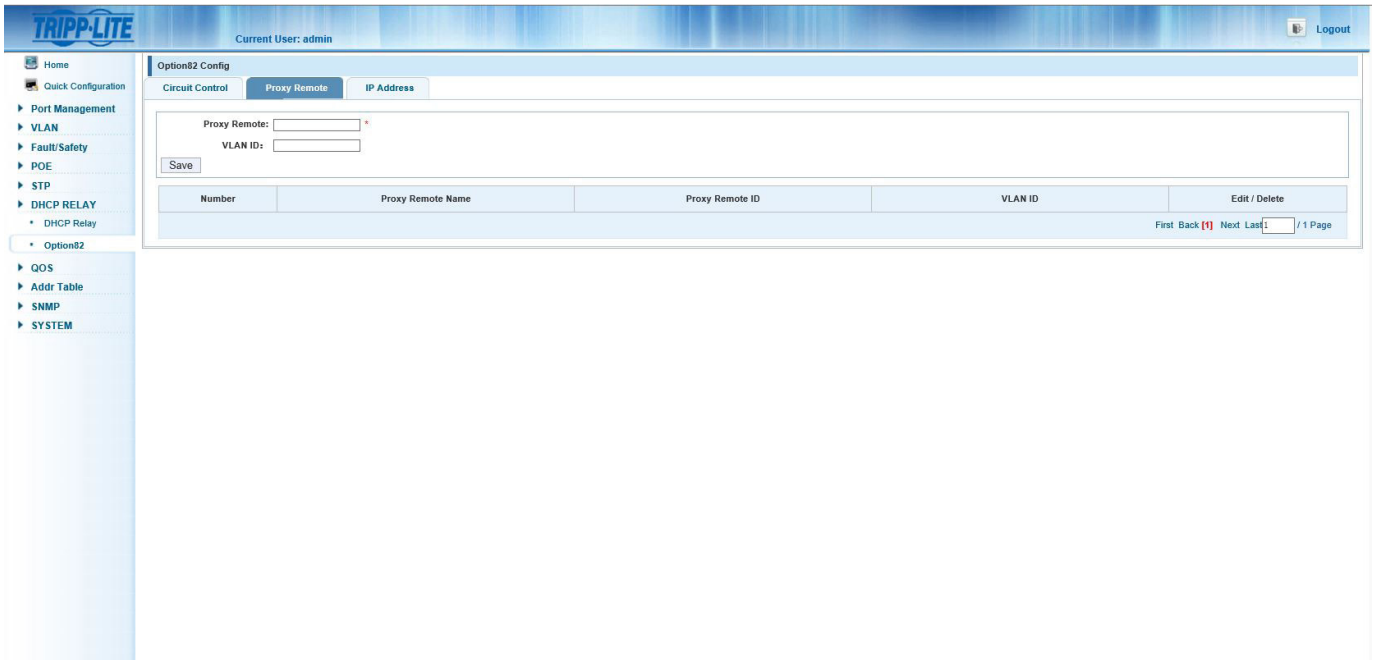


Figura 10.3: Proxy Remoto de Option82

10.2.3 Dirección IP

Introduzca la dirección IP del servidor de relevador DHCP y la ID de la VLAN asociada (Figura 10.4). Haga click en "Guardar" y cada instancia se guardará en la lista siguiente.

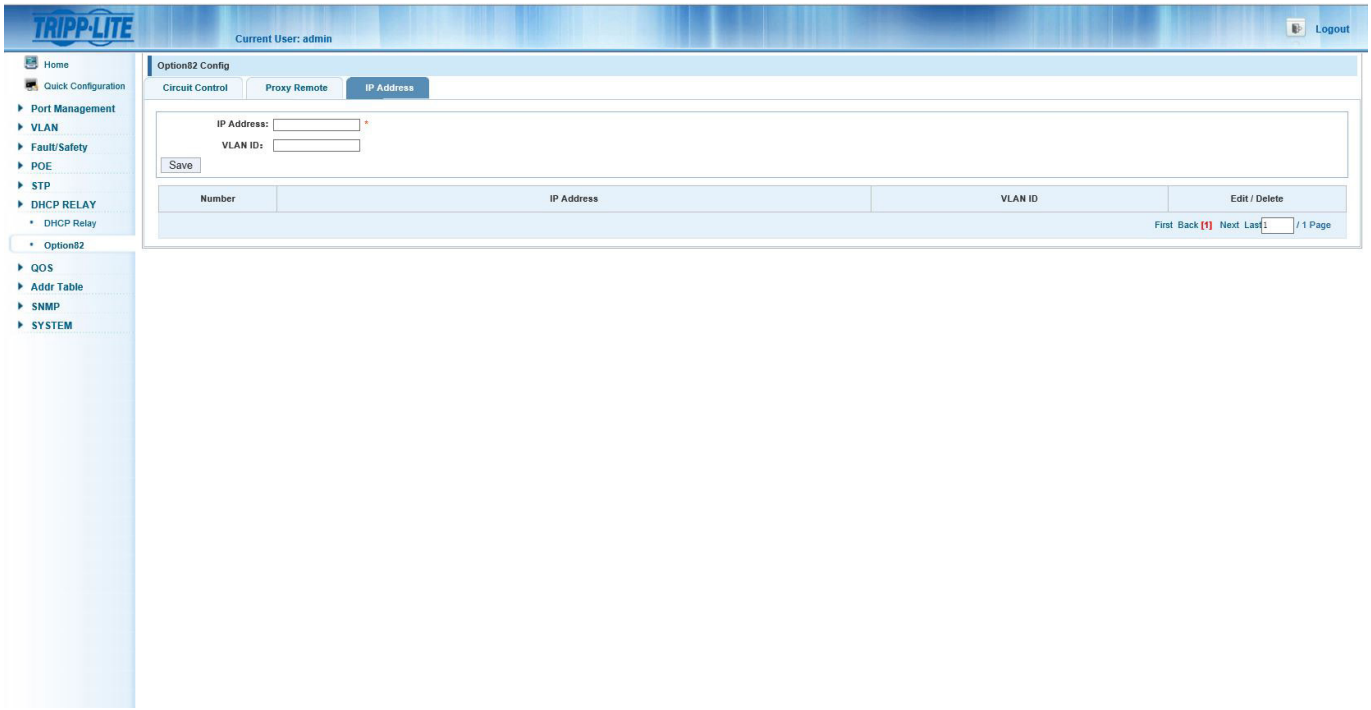


Figura 10.4: Dirección IP de Option82

11. Administración de Calidad del Servicio (QoS)

Calidad de Servicio asegura que la mayoría de la importación del tráfico de la red (por ejemplo, VoIP, cámaras IP, etc.) se obtiene a través del switch con la menor interrupción a su transmisión de datos como sea posible. Para dar a cualquier dispositivo con capacidad de red una mayor prioridad de transmisión, QoS debe estar configurado en el switch. De forma predeterminada está desactivada. Siga los pasos siguientes para configurar el puerto para el tráfico de dispositivos que requieren QoS.

11.1 Comentario de QoS

Seleccione QoS → Comentario. En la sección de etiquetas Múltiples de QoS usted puede establecer el Índice de la Regla, Tipo de Operación, Tipo de Valor, Valor, Mapeo de Clase de Servicio o la Observación de Prioridad para un puerto o múltiples puertos (Figura 11.1). Para aplicar la regla a un puerto o conjunto de puertos, haga click en "Guardar". Para descartar la configuración haga click en "Cancelar". El cuadro siguiente muestra los parámetros para cada regla de QoS:

Multi Etiqueta QoS	Parámetros	Notas
Índice de Regla	1-32	
Tipo de Operación	Igual; Siempre-Concuerda	
Tipo de Valor	DST Mac SRC Mac Prioridad de Ethernet Número de VLAN Tipo de Ethernet IP de Destino IP de Origen Tipo de IP IPv4 Diff Prioridad de IPv6 Puerto SRC de Nivel 4 Puerto DST de Nivel 4	
Valores	DST MAC – 00:00:00:00:00:00 SRC MAC – 00:00:00:00:00:00 Prioridad de Ethernet – 0~7 Número de VLAN – 1~4094 Tipo de Ethernet – 0~0xFFFF IP de Destino – 0.0.0.0 IP de Origen – 0.0.0.0 Tipo de IP – 0~0xFF IPv4 Diff – 0~63 Prioridad de IPv6 – 0~255 Puerto SRC de Nivel 4 – 0~65535 Puerto DST de Nivel 4 – 0~65535	Las opciones de valores cambian basadas en el tipo de valor seleccionado. Los valores siempre se requieren.
Configuración de Puerto	Aplique la regla a uno o más puertos seleccionando un puerto individual, seleccionando todos o seleccionando todos los demás.	También puede arrastrar el cursor para seleccionar varios puertos.
Guardar Configuración	Haga click en "Guardar" para aplicar la regla o en Cancelar para descartar los cambios.	

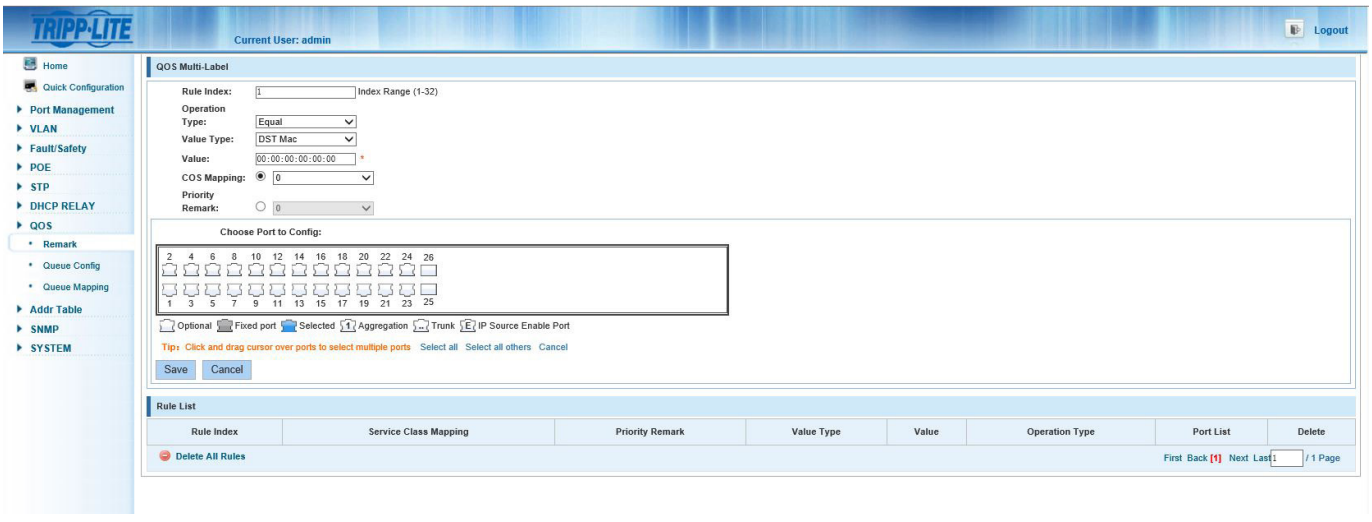


Figura 11.1: Vista General de Observación de QoS

11. Administración de Calidad del Servicio (QoS)

11.1.1 Lista de Reglas

La Lista de Reglas muestra toda la información de reglas antes configuradas. Eliminar una sola regla o eliminar todas las reglas cuando sea necesario.

11.2 Configuración de Cola de QoS

Seleccione QoS → Configuración de Cola para configurar el Modo de Cola. Las opciones disponibles son las siguientes:

Opciones de Programación de Modo de Cola	Descripción
SP	Programación de Prioridad Absoluta
RR	Programación Round-Robin
WRR	Programación Round Robin Ponderada
WFQ	Programación Equitativa Ponderada
Peso de Bytes de WRR y WFQ	Establezca los pesos de byte de 0 a 127 para cada cola para que estén en proporción a ocupar el ancho de banda para envío de los datos

11.3 Mapeo de Cola de QoS

El mapeo de cola administra la transmisión de mensajes de datos a una cola de salida de un puerto. Los mensajes dentro de las diferentes colas de salida contendrán las políticas de servicio de transmisión de diferentes niveles y calidades. Cada puerto tiene 8 colas de salida, 0 a 7. El mapeo de cola de la Clase de Servicio y el mapeo de DSCP para CoS debe estar configurada en el switch para convertir el valor de DSCP del mensaje en un número de cola de salida para determinar en qué cola de salida transferir los mensajes.

11.3.1 Parámetros del Mapeo de Cola de QoS

Establezca cada una de las 8 colas de salida para la Clase de Servicio [Cos] necesaria para la transmisión del mensaje de datos (Figura 11.2).

Mapeo de Clase de Servicio	Descripción
0	Mejor Esfuerzo
1	Clase 1
2	Clase 2
3	Clase 3
4	Clase 4
5	Reenvío Express
6	Permanecer Igual (Enrutado IP)
7	Permanecer Igual (La Capa de Enlace y enrutado permanecen activos)

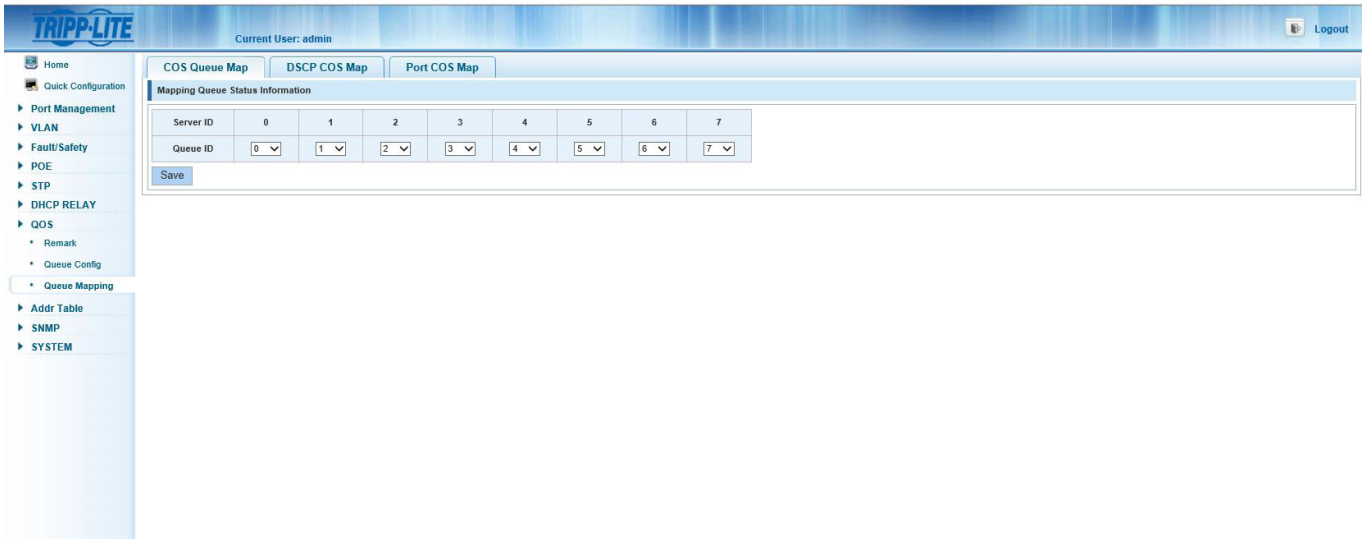


Figura 11.2: Mapeo de Cola de CoS

11. Administración de Calidad del Servicio (QoS)

11.3.2 Parámetros de Mapeo de CoS DSCP

Seleccione CoS → Mapeo de Cola → Asignación de CoS DSCP – Establece la Lista de Equipo de Mapeo de Punto de Código de Servicio Diferencial [DSCP] (Figura 11.3).

Lista de Servidores - El campo DSCP tiene siete campos de CoS (0-63) divididos en cuatro tablas.

ID de Cola - Asignando el DSCP a campos de CoS (0 a 7), con base en el CoSeno es asignado a una cola.

Nota: *La prioridad de CoS es mayor que el valor DSCP, la prioridad DSCP es mayor que el puerto.*

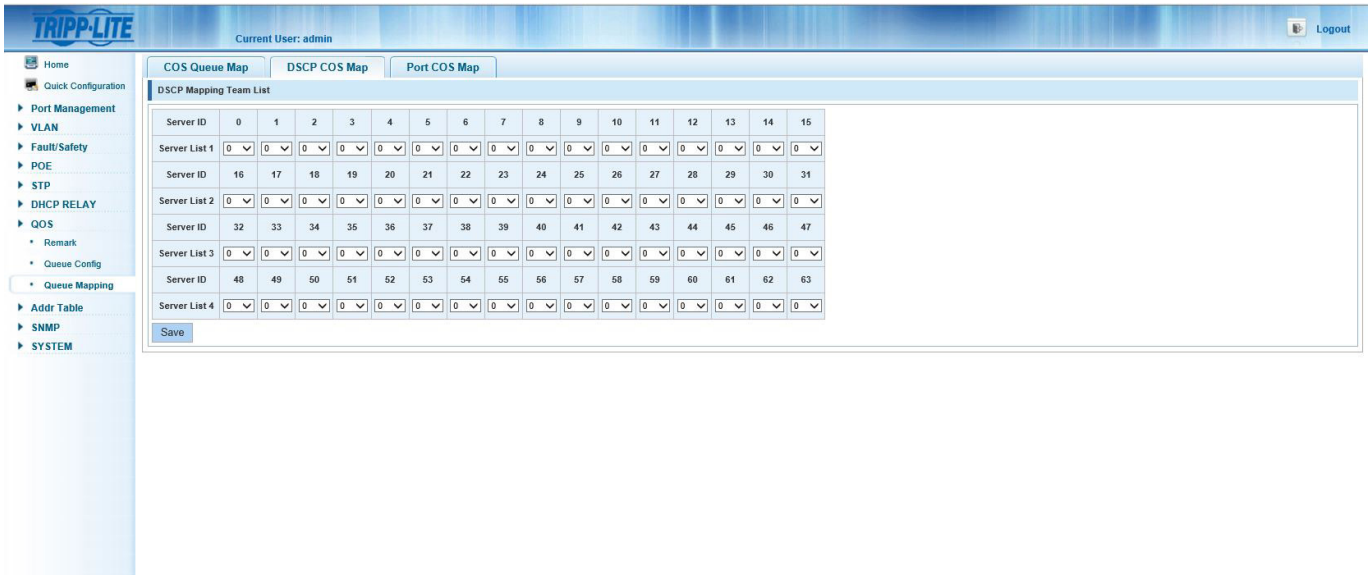


Figura 11.3: Mapeo de CoS de DSCP

11.3.3 Parámetros de Mapeo de CoS de Puerto

Seleccione CoS → Mapeo de Cola → Mapeo de CoS de Puerto (Figura 11.4) para establecer el puerto para el mapeo de clase del servicio.

Seleccione el puerto.

Seleccione la ID del Servidor de CoS de 0 a 7 (Todos los puertos están configurados a CoS 0 de fábrica).

Haga click en "Guardar" para aplicar la configuración. Los parámetros guardados se muestran en la Lista de Control con el símbolo "T" entre el número de puerto y la ID del servidor.

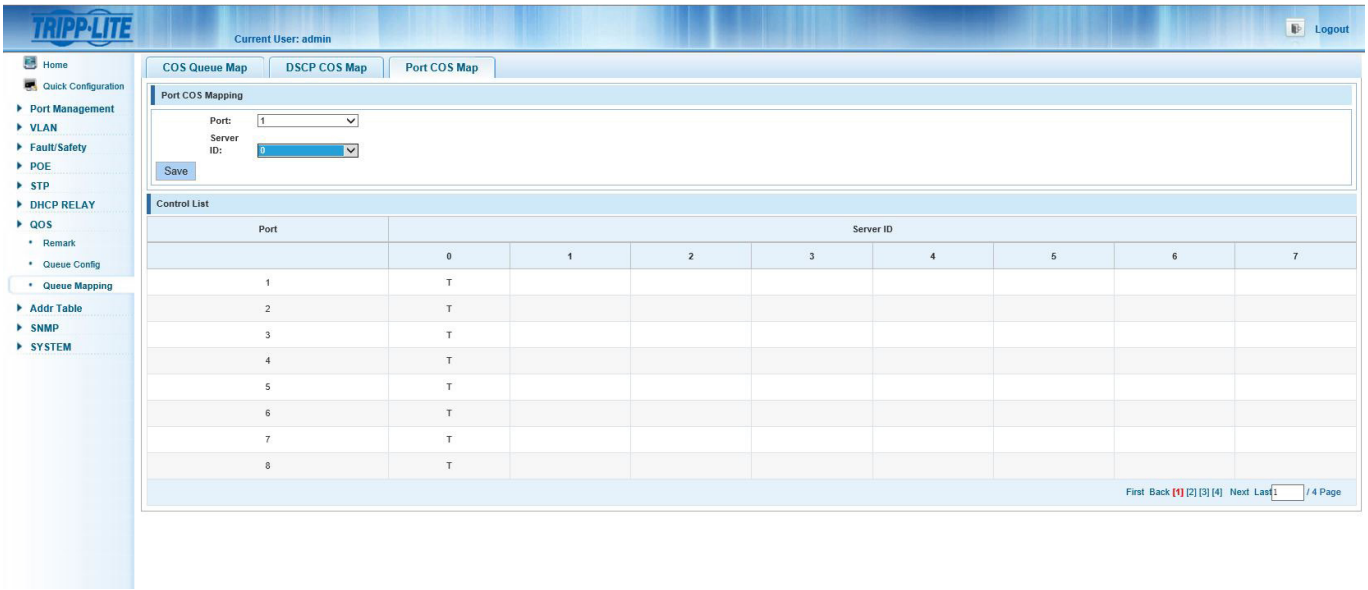


Figura 11.4: Mapeo de CoS de Puerto

12. Administración de Lista de Acceso a Tabla de Direcciones MAC

La tabla de Lista de Control de Acceso a Direcciones MAC (Figura 12.1) permite al usuario añadir y eliminar las direcciones MAC, configurar el aprendizaje y el envejecimiento de MAC y el filtrado de MAC.

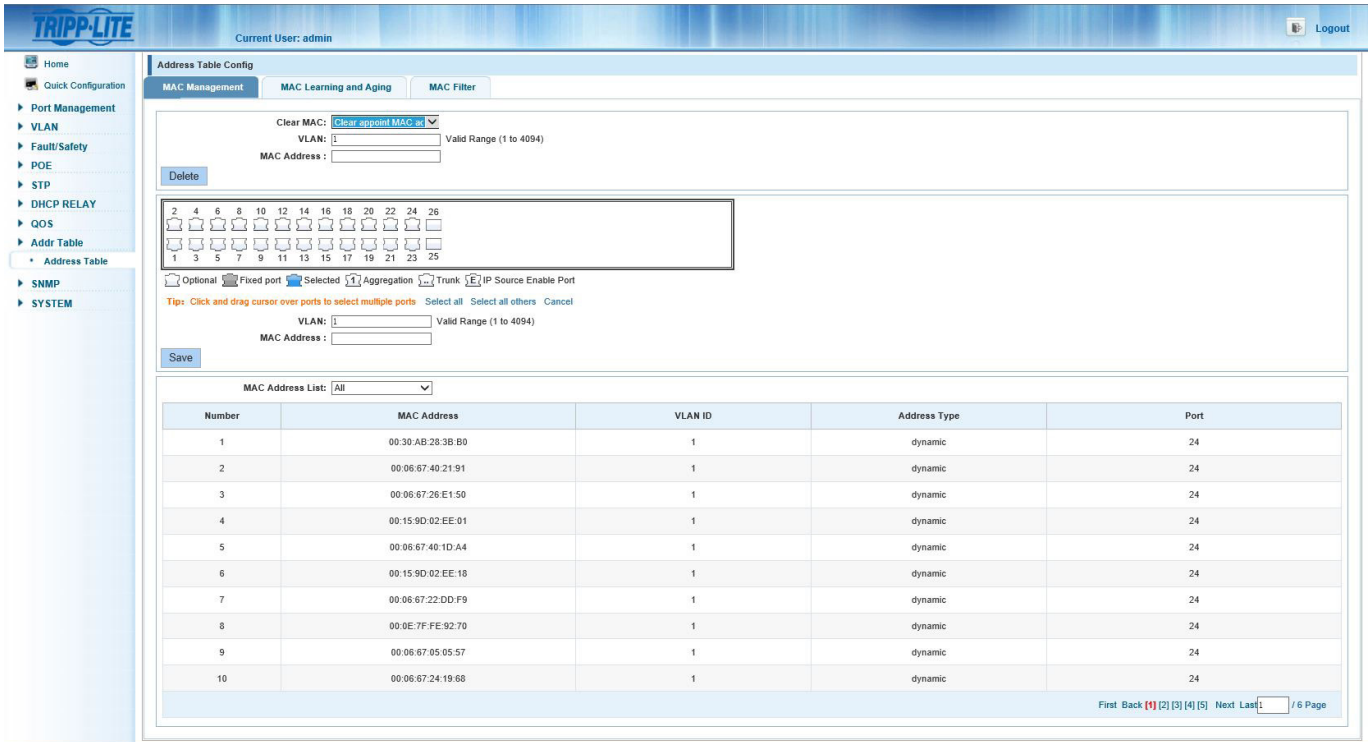


Figura 12.1: Vista de Administración de MAC

12. Administración de Lista de Acceso a Tabla de Direcciones MAC

12.1 Administración de MAC

En la pantalla de Administración de MAC, puede añadir y eliminar de la tabla de Dirección MAC (Figura 12.2).

12.1.1 Vista de la Lista de Direcciones MAC

Visualice la lista completa de direcciones MAC con la VLAN con que cada una se asocia y los puertos a que tiene acceso para comunicarse por ellos. Use el filtro de visualización para ver todas las direcciones MAC dinámicas o estáticas en la lista (Figura 12.2).

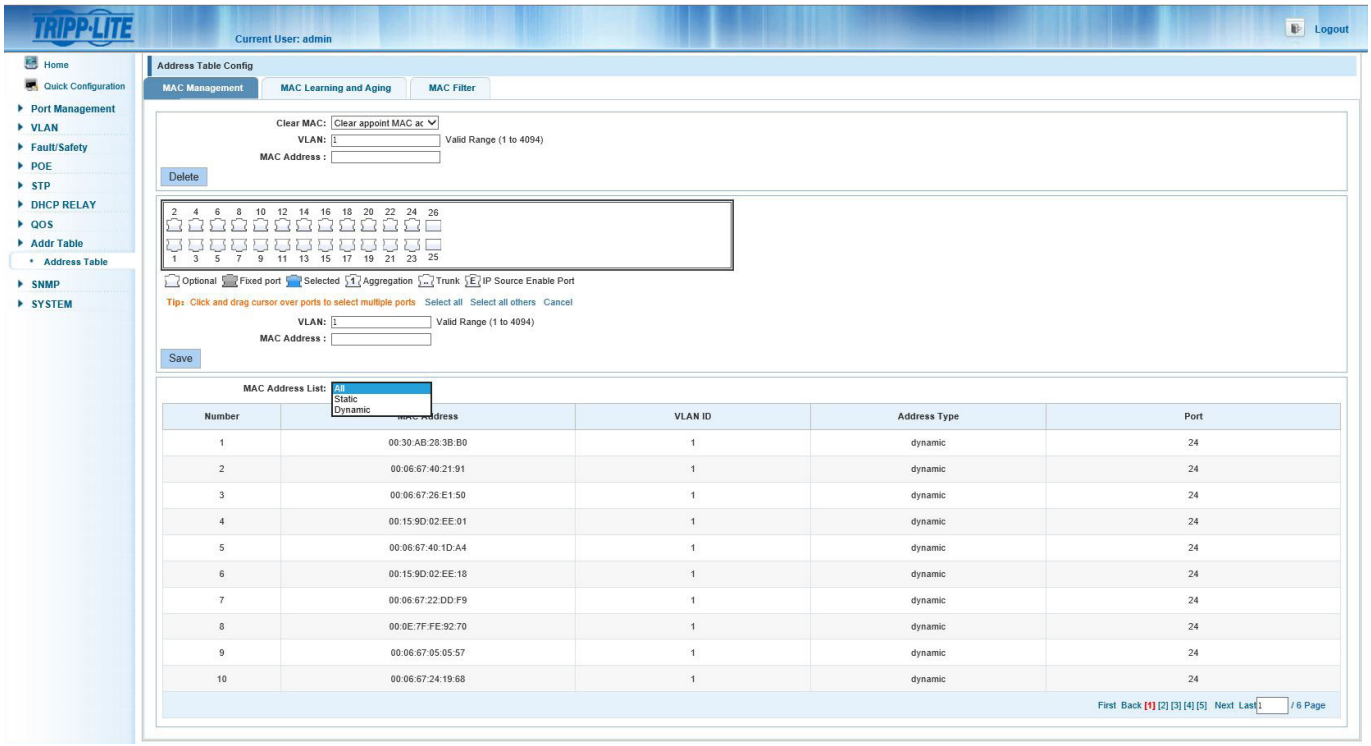


Figura 12.2: Filtros de la Lista de Direcciones MAC

12.1.2 Agregar Dirección MAC

Para agregar una tabla estática de direcciones MAC a la Lista de Direcciones MAC (Figura 12.3), realice los siguientes pasos:

1. Seleccione los puertos a los que desea que la dirección MAC pueda acceder.
2. Introduzca la ID de la VLAN a través del cual se comunicará la dirección MAC.
3. Introduzca la dirección estática MAC para añadirla.
4. Haga click en el botón "Guardar" para agregar la dirección MAC a la lista de direcciones MAC.

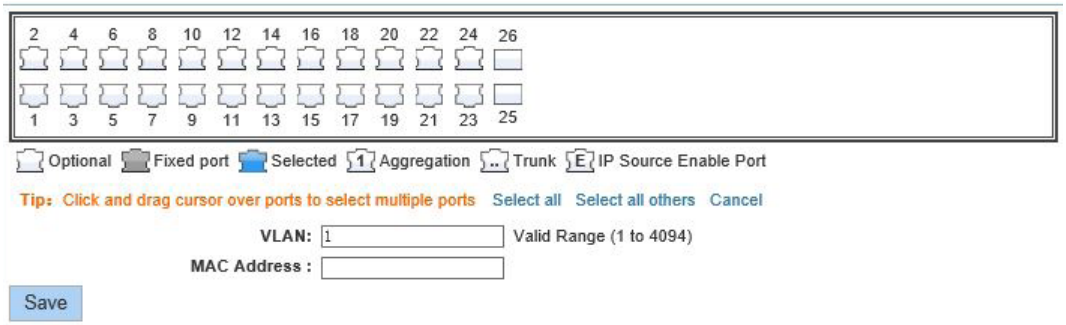


Figura 12.3: Agregar Direcciones MAC

12. Administración de Lista de Acceso a Tabla de Direcciones MAC

12.1.3 Eliminar Dirección MAC

El siguiente conjunto de funciones puede utilizarse para eliminar una sola dirección MAC de una VLAN asociada o eliminar toda la lista:

Funciones de Administración de MAC	Descripción
Eliminar MAC	Opciones: borrar una dirección MAC elegida, borrar Unicast dinámica, borrar Unicast estática o borrar toda la lista de direcciones MAC.
VLAN	Introduzca la ID de VLAN que desea borrar de la dirección MAC (intervalo de ID válida: 1 a 4094).
Dirección MAC	Introduzca la dirección MAC específica a ser borrada.

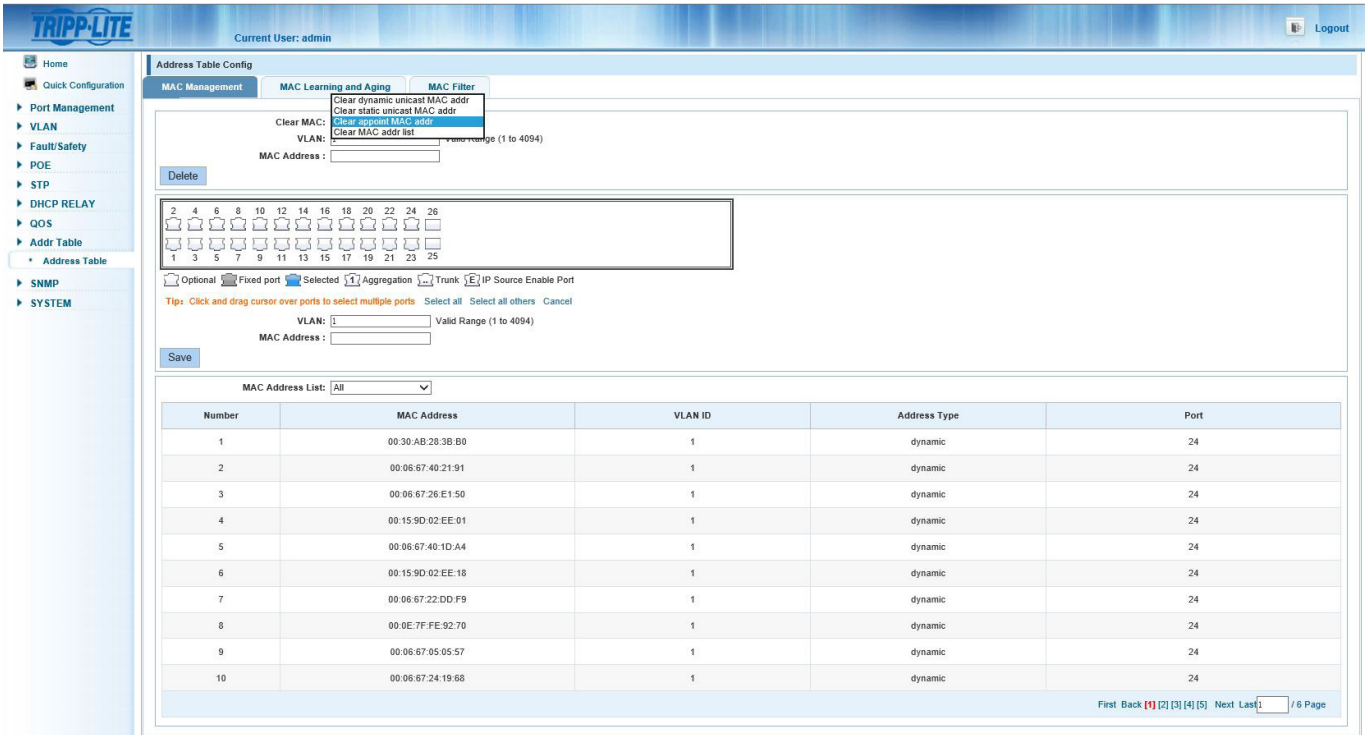


Figura 12.4: Borrar Direcciones MAC

12. Administración de Lista de Acceso a Tabla de Direcciones MAC

12.2 Aprendizaje y Envejecimiento de MAC

El límite de aprendizaje de MAC puede establecerse hasta para 8191 direcciones por puerto. El tiempo de envejecimiento se puede establecer en 0 (sin envejecimiento) o hasta 1,000,000 de segundos. (Ver Figura 12.5.)

12.2.1 Límite de Aprendizaje de MAC

Para cambiar un solo puerto, seleccione el número de puerto. A continuación, ingrese el rango de aprendizaje de 0 a 8191 (8191 es el rango de aprendizaje predeterminado). Haga click en "Guardar" para guardar los parámetros. Para configurar el aprendizaje en varios puertos, haga click y arrastre el cursor sobre varios puertos o utilice las opciones de "Seleccionar todas" o "Seleccionar todas las demás" para seleccionar los puertos. Introduzca el límite de aprendizaje MAC para los puertos, hasta 8191 registros. Haga click en "Guardar" para guardar los parámetros.

12.2.2 Tiempo de Envejecimiento de la Dirección MAC

El tiempo de envejecimiento se puede establecer en 0 (sin envejecimiento) o hasta 1,000,000 de segundos (el parámetro predeterminado es de 30 segundos). Haga click en "Guardar" para guardar los parámetros.

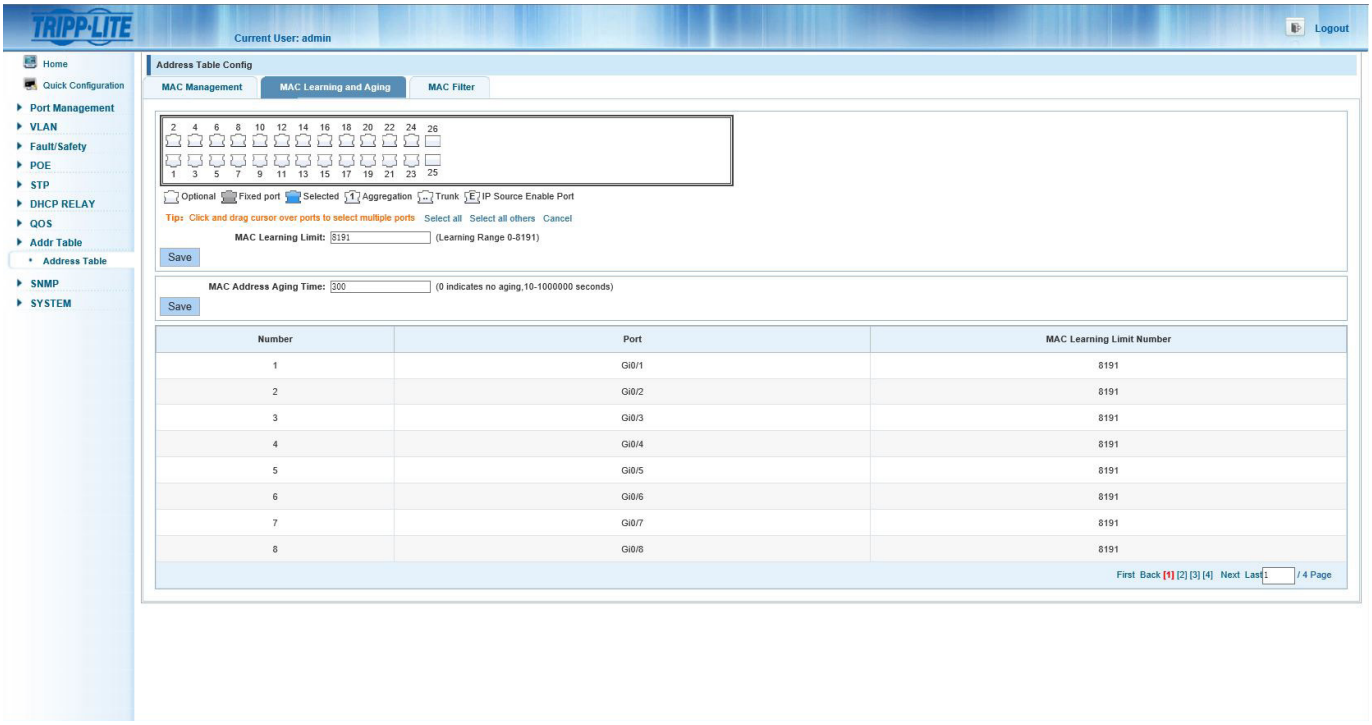


Figura 12.5: Aprendizaje y Envejecimiento de Dirección MAC

12.3 Filtrado de Direcciones MAC

Para asegurar que una dirección MAC no pueda acceder a la comunicación entrante o saliente a través del switch, realice los siguientes pasos:

1. Dirección MAC – Ingrese la dirección MAC a la que se aplicará el filtrado
2. VLAN – Ingrese la ID de la VLAN
3. Filtrado de dirección – Determine si el filtrado será de la fuente, el destino o ambos.
4. Haga click en "Guardar" para agregar al filtro de dirección MAC a la lista.

Para eliminar un filtro, haga click en el ícono junto a la entrada de dirección filtrada de MAC.

13. Administración del Protocolo Simple de Administración de Red [SNMP]

El Protocolo Simple de Administración de Red [SNMP] permite al switch ser monitoreado y controlado en forma remota. También puede enviar trampas SNMP a un servicio de receptor de la trampa.

13.1 Parámetros de Configuración de SNMP

13.1.1 Activar / Desactivar Configuración de SNMP

Esta característica está desactivada de fábrica. Se puede activar accionando el switch de activar / desactivar (Figura 13.1). Una vez activado, tienes acceso para configurar la comunidad, grupo, usuarios y configuración de trampa de SNMP.

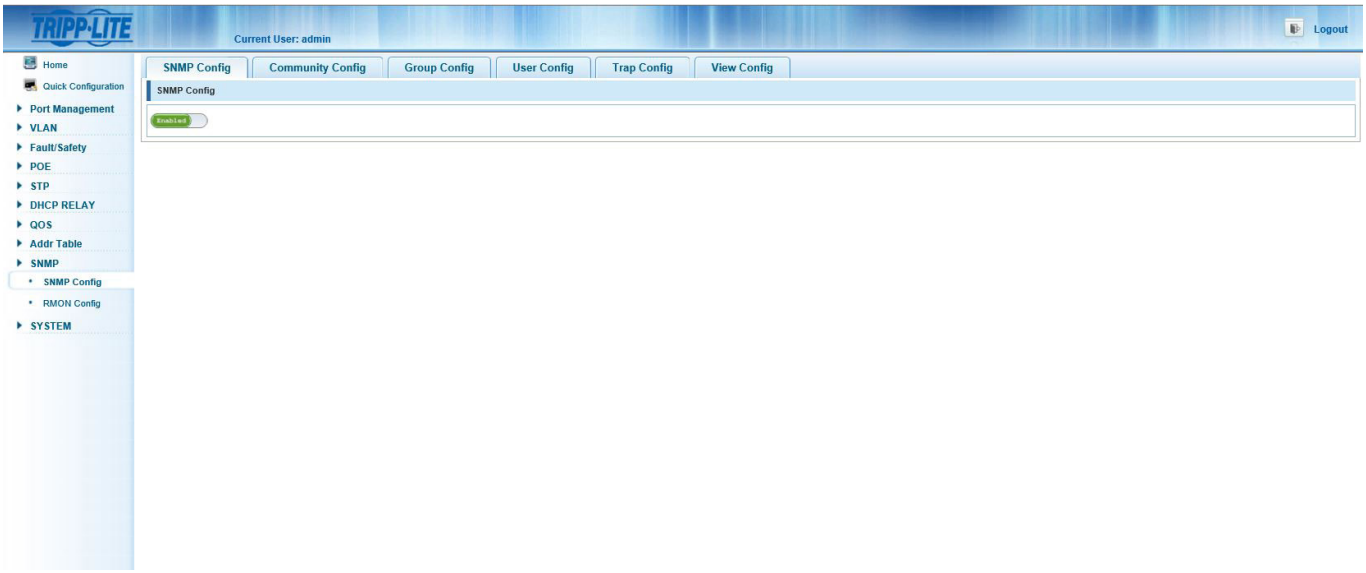


Figura 13.1: Resumen de Configuración de SNMP

13.1.2 Configuración de Comunidad

Para agregar las cadenas de comunidad SNMP psoportadas y sus permisos seleccione SNMP → SNMP Config → Config de Comunidad. Haga click en el ícono verde para agregar una nueva Configuración de Comunidad (Figura 13.2). Añada el nombre de la comunidad (límite: 16 caracteres) y la autorización de acceso de "Lectura Escritura" o "Sólo Lectura". Haga click en "Guardar" para guardar la configuración, haga click en "Salir" para descartar los cambios.

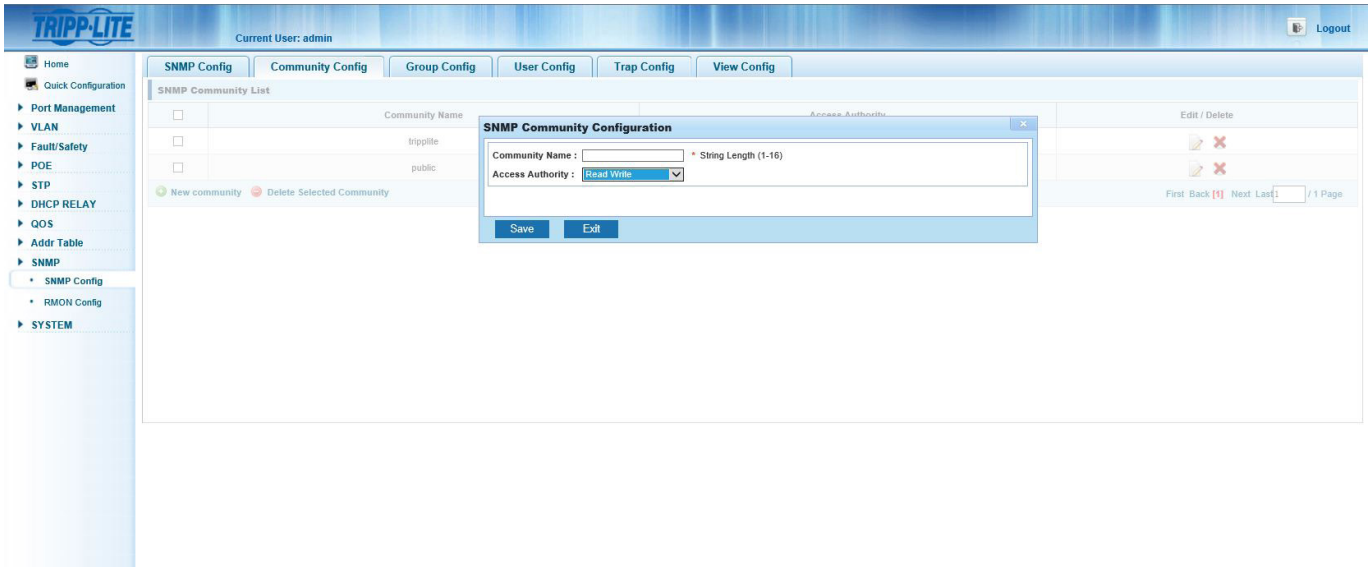


Figura 13.2: Configuración de Comunidad de SNMP

Para editar una Configuración de Comunidad, seleccione el ícono "Editar" y cambie el nombre o la autorización de acceso de la comunidad (Figura 13.3). Haga click en "Guardar" para guardar la configuración, haga click en "Salir" para descartar los cambios.

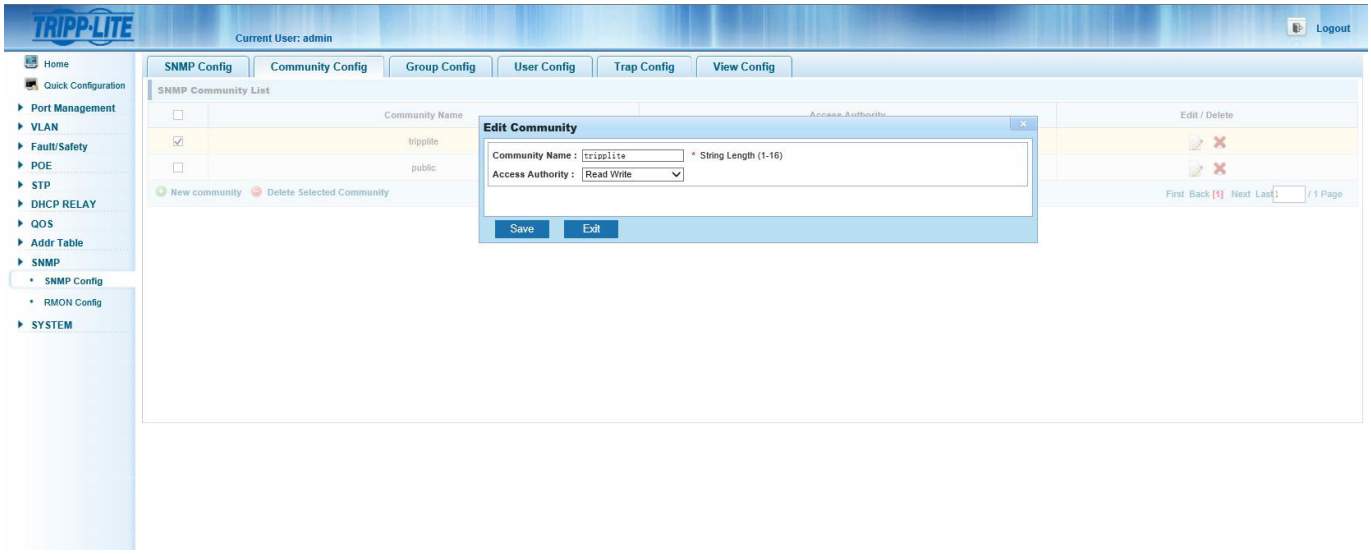


Figura 13.3: Edición de Configuración de Comunidad

Para eliminar una Configuración de Comunidad, haga click en el ícono rojo para borrar la entrada de la lista o haga click en la casilla de verificación para la cadena de comunidad a eliminar y haga click en "Eliminar Comunidad Seleccionada". Elimine varias cadenas de comunidad haciendo click en la casilla de verificación de cada una de las cadenas a eliminar o marcando la casilla principal en la parte superior de la lista para seleccionar todas las entradas. Una vez que todas están seleccionados, haga click en el ícono "Eliminar Comunidad Seleccionada" para eliminarlas de la lista.

Nota: *Puede configurar un total de 8 cadenas de comunidad SNMP.*

13.1.3 Vista de Configuración de SNMP

Seleccione SNMP → Configuración de SNMP → Configuración de Vista (Figura 13.4) – Configure la visualización y gestión de las reglas para el OID MIB mediante la creación de vistas MIB que entonces pueden ser asignados a un grupo SNMP. Configure una regla nueva para cada vista para no afectar a la función SNMP.

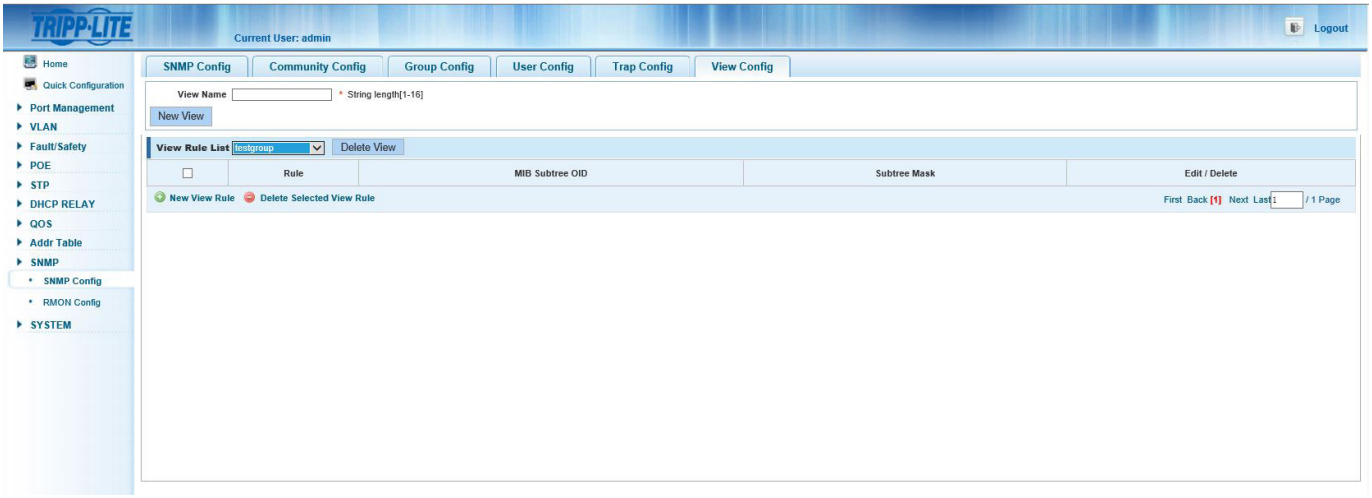


Figura 13.4: Configuración de Vista de SNMP

13.1.4 Vista de Nombre

Introduzca el nombre de la vista (límite: 16 caracteres). Haga click en el ícono “Nueva Vista”. Esto añadirá el nombre de la vista al menú desplegable de la Lista de Reglas de la vista.

13.1.5 Vista de Lista de Reglas

Una vez que se configura el nombre de la vista, seleccione el ícono verde para añadir una nueva regla de vista (Figura 13.5).

13.1.6 Editar Vista de Reglas

Para incluir o excluir una vista en una regla (Figura 13.5), siga estos pasos:

1. OID de Subtree MIB – Introduzca el OID deseado para filtrar por el nombre de la vista (límite: 64 caracteres).
2. Máscara del Subtree: Introduzca la máscara de subtree OID si es necesario.
3. Haga click en "Guardar" para guardar los cambios o haga click en "Salir" para descartarlos.

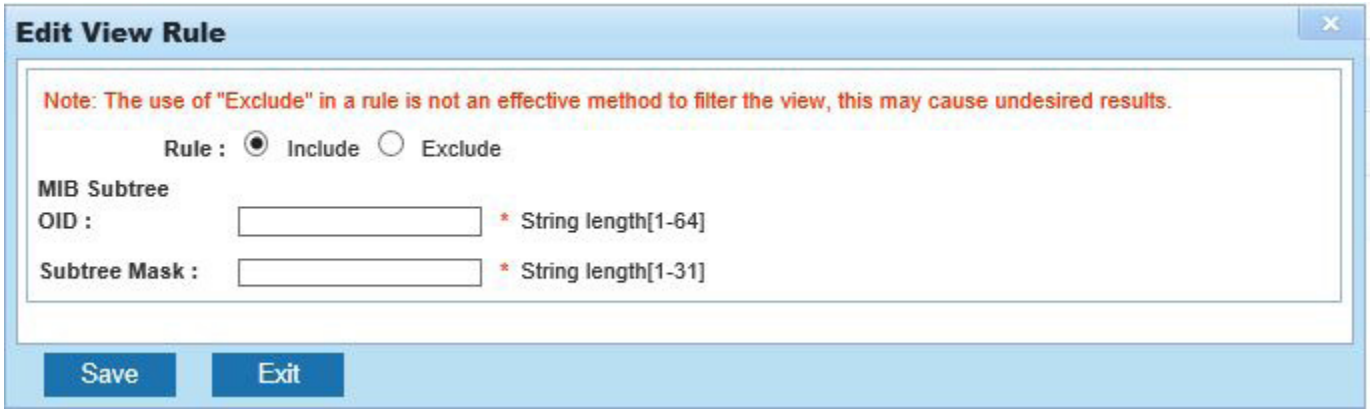


Figura 13.5: Adición o Edición de una Regla de Vista

Nota: *La exclusión mediante el uso de una regla no es un método eficaz para filtrar la vista. Esta configuración puede causar resultados indeseables.*

13.1.7 Configuración de Grupo

Cree los grupos SNMP a los que se aplicarán las reglas de la vista.

13.1.8 Crear Nuevo Grupo de SNMP

SNMP → Configuración de SNMP → Configuración de Grupo para configurar el grupo de SNMP (Figura 13.6) usando los siguientes pasos:

1. Seleccione el ícono de "Grupo Nuevo" para crear su grupo SNMP.
2. Introduzca el Nombre del Grupo (límite: 16 caracteres).
3. Seleccione el nivel de seguridad de la información transmitida que puede ser vista (Figura 13.7). Las opciones de configuración disponibles son: sin autentificación y sin cifrado, autentificación y no cifrado o autentificación y cifrado.
4. Seleccione la regla para Vista de Lectura de grupo según sea necesario. El grupo podrá ver solamente información basado en la configuración de la regla.
5. Seleccione la regla para Vista de Lectura Escritura según sea necesario. El grupo podrá ver y administrar el switch basado en la configuración de la regla.
6. Seleccione la regla para Vista de Notificación según sea necesario. El grupo será notificado solamente de la configuración de regla de vista seleccionada.
7. Haga click en "Guardar" para guardar el grupo SNMP. Haga click en "Salir" para descartar los cambios.

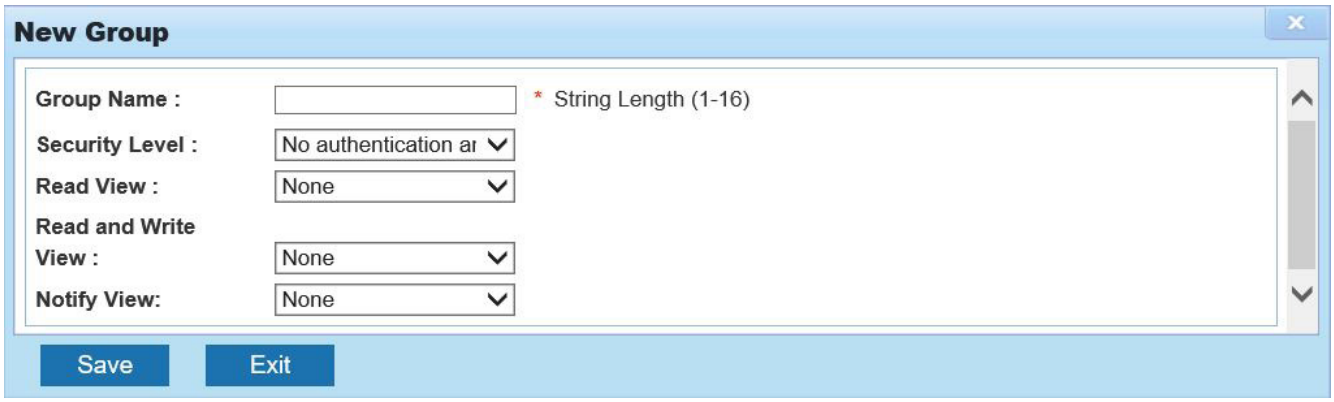


Figura 13.6: Nuevo Grupo

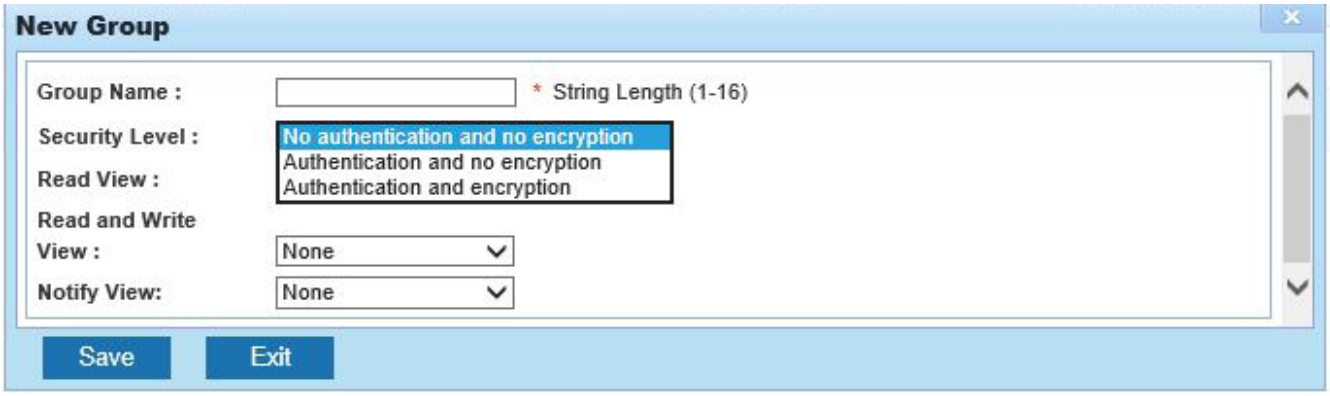


Figura 13.7: Nivel de Seguridad del Nuevo Grupo

13.1.9 Editar un Grupo de SNMP

Haga click en el ícono "Editar" para editar la configuración de grupo. Haga click en "Guardar" para guardar los cambios. Haga click en "Salir" para descartar los cambios (Figura 13.8).

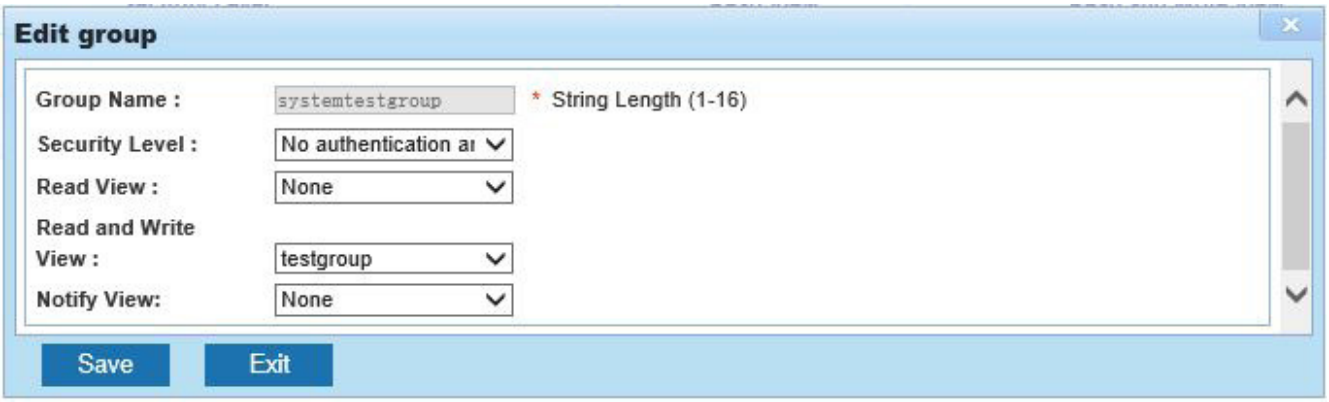


Figura 13.8: Editar Grupo

13.1.10 Eliminar un Grupo SNMP

Para eliminar un solo grupo SNMP, haga click en el ícono rojo o haga click en la casilla de verificación junto al grupo SNMP y haga click en el ícono "Borrar Grupo Seleccionado". Para eliminar varios grupos, haga click en la casilla de verificación para cada grupo SNMP a eliminar y haga click en el ícono "Borrar Grupo Seleccionado".

13.1.11 Configuración de Usuario de SNMP

Seleccione SNMP → Configuración de SNMP → Configuración del Usuario para crear los usuarios que se asignarán al grupo de SNMP, junto con sus credenciales de acceso.

Para agregar un nuevo usuario de SNMP, haga click en el ícono de "Nuevo Usuario" y, a continuación, siga los pasos indicados (Figura 13.9):

1. Nombre de Usuario – Introduzca el nombre del usuario (límite: 16 caracteres).
2. Nivel de Seguridad – Ingrese el nivel de seguridad de sin autentificación y sin cifrado, autentificación y no cifrado o autentificación y cifrado.
3. Nombre del grupo – Seleccione el nombre del grupo al que se asignará al usuario desde el cuadro de lista desplegable.
4. Modo de Autentificación – Cuando la autentificación sea necesaria, seleccione el modo correcto de autentificación MD5 o SHA.
5. Contraseña de Autentificación: Introduzca la contraseña de autentificación.
6. Confirme Contraseña de Autentificación: Reingrese la contraseña de autentificación para confirmación.
7. Modo de Cifrado: Cuando se selecciona el cifrado, seleccione el modo apropiado de cifrado DES o AES.
8. Contraseña de Cifrado – Ingrese la Contraseña de Cifrado.
9. Confirme Contraseña de Cifrado – Reingrese la contraseña de cifrado.
10. Haga click en "Guardar" para agregar el nuevo usuario de SNMP. Haga click en "Salir" para descartar los cambios.

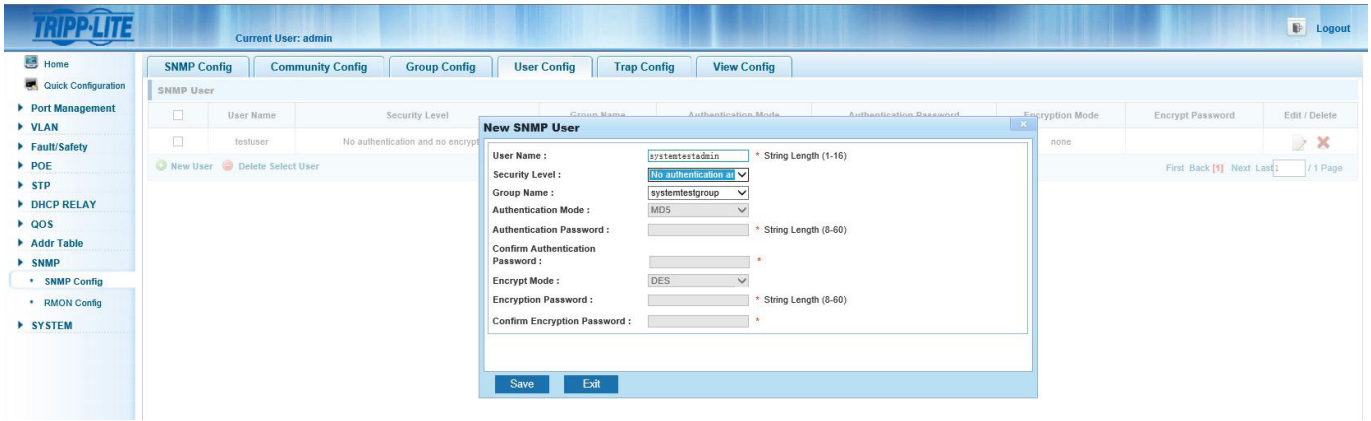


Figura 13.9: Agregar Nuevo Usuario de SNMP

13. Administración del Protocolo Simple de Administración de Red [SNMP]

Para editar una configuración de usuario de SNMP, haga click en el ícono "Editar" para hacer cambios (Figura 13.10). Haga click en "Guardar" para guardar los cambios. Haga click en "Salir" para descartar los cambios.

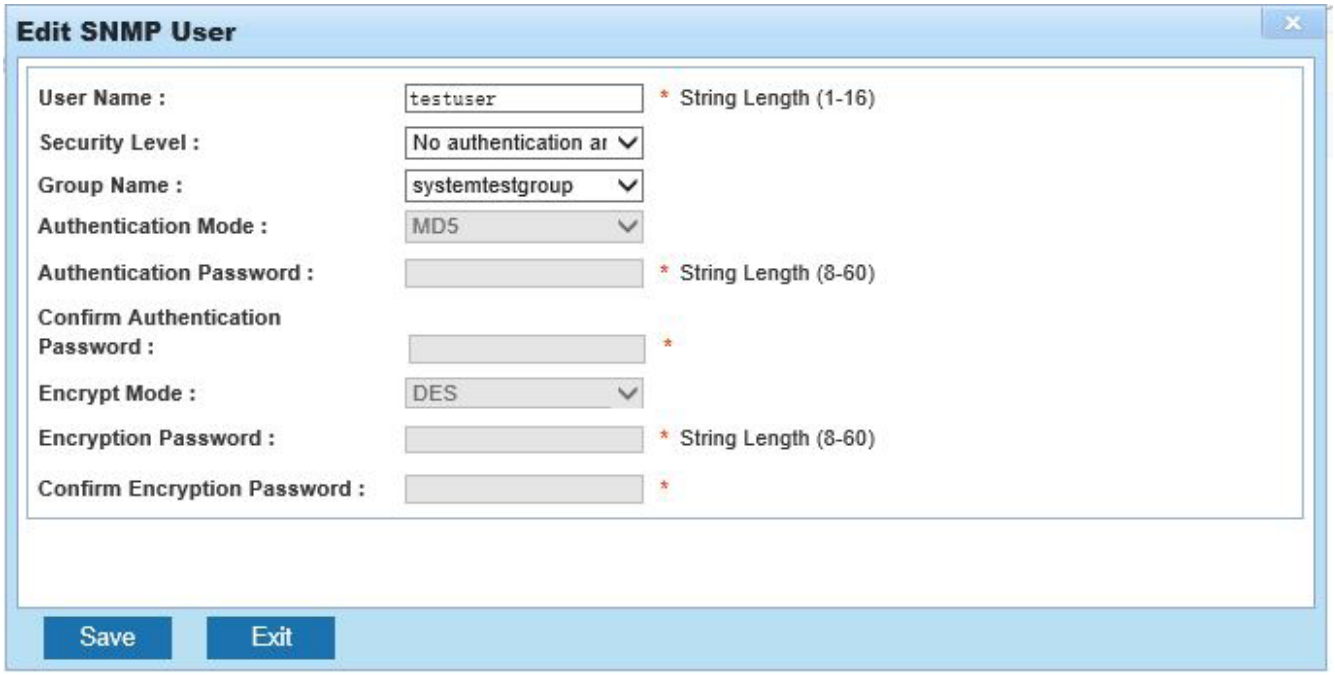


Figura 13.10: Editar Usuario de SNMP

Para eliminar un usuario de SNMP, haga click en el ícono Eliminar rojo junto al nombre de usuario a eliminar o haga click en la casilla de verificación situada junto al nombre de usuario y haga click en el ícono de "Eliminar Usuario Seleccionado". Una vez confirmado, se eliminará el usuario de SNMP. Para eliminar varios usuarios, haga click en la casilla de verificación junto a cada uno de los usuarios a eliminar, luego haga click en el ícono de "Eliminar Usuario Seleccionado". Una vez confirmado, se eliminarán los usuarios de SNMP.

13.1.12 Configuración de Trampa SNMP

Para establecer el destino para trampas SNMP enviadas por el switch, haga click en el ícono de "Nueva Trampa" para entrar en el receptor del anfitrión para las trampas SNMP y, a continuación, siga estos pasos para crear una nueva trampa (Figura 13.11):

1. IP de Destino: ingrese la dirección IP de destino del receptor de la trampa (si el modo de seguridad es V1 o V2, haga click en el ícono "Guardar" para agregar el servidor del receptor de la trampa SNMP).
2. Modo de Seguridad – Establezca el modo de seguridad de destino en V1, V2 o V3. Esta configuración debe coincidir con el modo de seguridad del servidor de destino de trampa 13.1.6.4. Tipo de Dirección – El switch solo admite envío a destinos de servidor IPv4.
3. Nombre de Seguridad – Si se selecciona el modo de seguridad SNMP v3, seleccione el usuario de SNMP de la lista desplegable.
4. Número de Puerto UDP – El puerto predeterminado es 162 y no se puede cambiar.
5. Haga click en "Guardar" para guardar al Host de destino de la trampa. Haga click en "Salir" para cancelar los cambios.

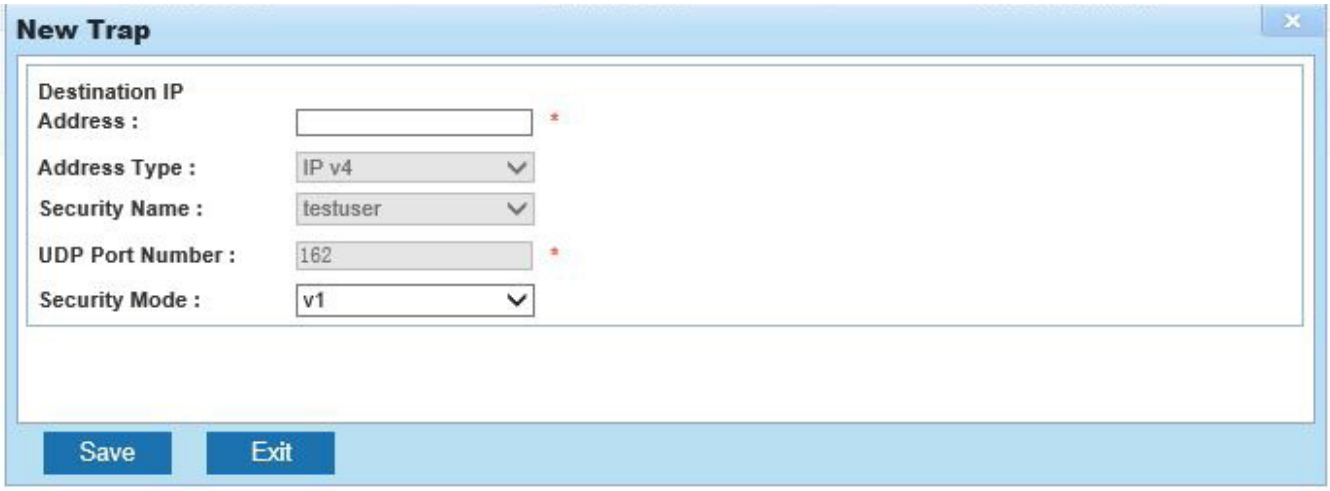


Figura 13.11: Nueva Trampa

Para editar una configuración de Servidor de Destino de Trampa, haga click en el ícono "Editar" para hacer cambios (Figura 13.12). Haga click en "Guardar" para guardar los cambios Haga click en "Salir" para descartar los cambios

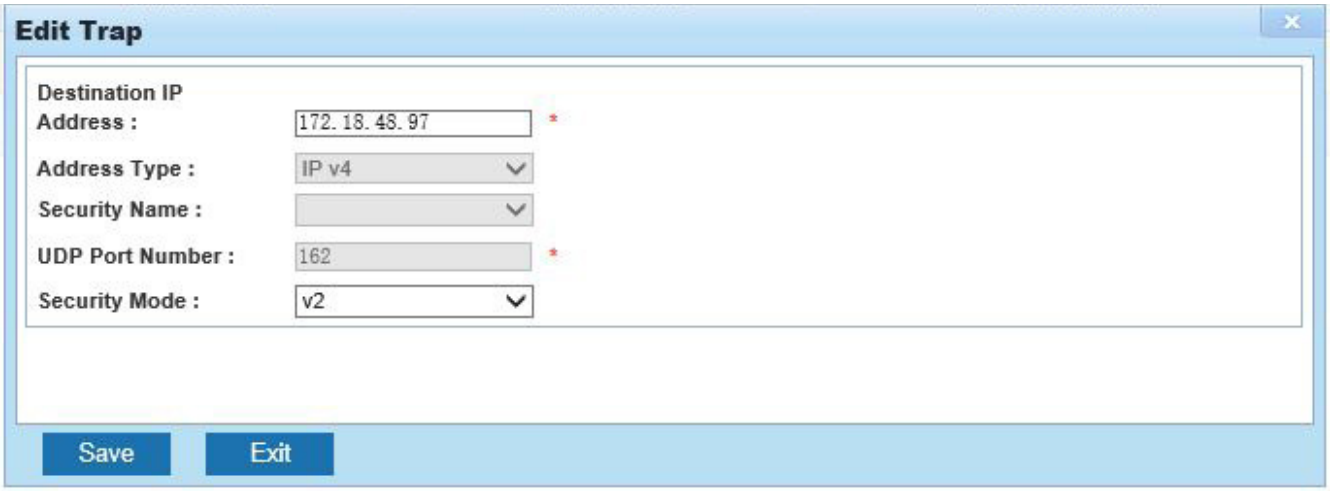


Figura 13.12: Editar Trampa

Para eliminar un servidor de destino de trampa, haga click en el ícono ✖ rojo eliminar junto al nombre de servidor a eliminar, haga click en la casilla de verificación situada junto al nombre de usuario y haga click en el ícono de "Eliminar Trampa Seleccionada". Una vez confirmado, se eliminará el servidor de destino de la trampa. Para eliminar varios servidores de destino de trampa, haga click en la casilla de verificación junto a cada una de las entradas a eliminar, luego haga click en el ícono de "Eliminar Usuario Seleccionado". Una vez confirmado, se eliminarán los servidores de destino de la trampa.

13. Administración del Protocolo Simple de Administración de Red [SNMP]

13.2 Parámetros de Configuración de Monitoreo Remoto

El Monitoreo Remoto [RMON] permite monitorear tráfico de red y proporcionar estadísticas de red para redes Ethernet. El switch tiene la sonda RMON integrada en sus circuitos. La función está disponible a través de la opción de configuración de SNMP → RMON.

Nota: *SNMP debe estar habilitado para configurar RMON.*

13.2.1 Grupo de Estadísticas

Para configurar una configuración de grupo de estadísticas (Figura 13.13), haga click en el ícono de "Nuevo Grupo de Cuenta" y, a continuación, siga estos pasos:

1. Índice – Introduzca el número de índice dentro del rango de valores de la tabla de información estadística de 1 ~ 65535.
2. Nombre de Interfaz – Seleccione el puerto fuente de la interfaz.
3. Propietario – Establezca el creador de la tabla (límite: 30 caracteres).
4. Haga click en "Guardar" para guardar los parámetros. Haga click en "Salir" para descartar los parámetros.

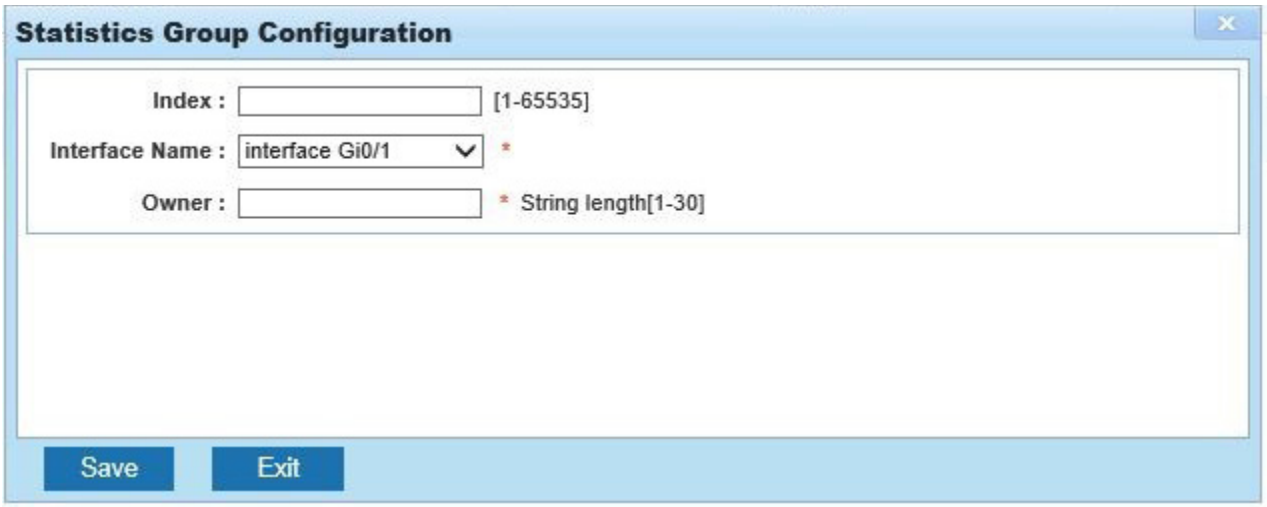


Figura 13.13: Configuración de Grupo de Estadísticas

Para editar una configuración de grupo de estadísticas (Figura 13.14), haga click en el ícono "Editar" para hacer los cambios necesarios. Haga click en "Guardar" para guardar los cambios. Haga click en "Salir" para descartar los cambios.

Figura 13.14: Edición de Grupo de Estadísticas

Para eliminar una configuración de grupo de estadísticas, haga click en el ícono rojo junto a la entrada de grupo de estadísticas a eliminarse, o haga click en la casilla de verificación junto a la entrada y haga click en el ícono "Borrar Grupo de Estadísticas Seleccionadas". Una vez confirmada, se eliminará la entrada de grupo de estadística. Para eliminar varios grupos de estadísticas, haga click en la casilla de verificación junto a cada una de las entradas a eliminar, luego haga click en el ícono de "Eliminar Grupo de Estadísticas Seleccionado". Una vez confirmada, se eliminarán las entradas de grupo de estadísticas seleccionadas.

13. Administración del Protocolo Simple de Administración de Red [SNMP]

Haga click en el ícono "Vista de Enlace" de una entrada de grupo de estadísticas para ver su información estadística (Figura 13.15).

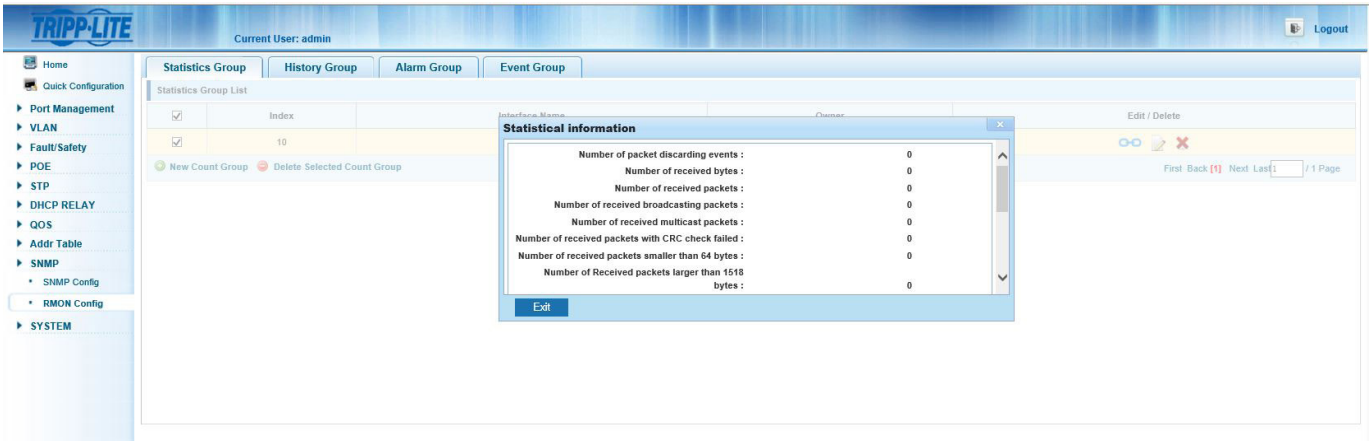


Figura 13.15: Información Estadística

13.2.2 Grupo de Historia

Un grupo de historia registra la historia de la información de la interfaz Ethernet. Para configurar un grupo de historia, haga click en el ícono de "Nuevo Grupo de Historia" y, a continuación, siga estos pasos (Figura 13.16):

1. Índice – Introduzca el número de índice requerido dentro del rango de valores de la tabla de información estadística de 1 a 65535.
2. Nombre de Interfaz – Seleccione el puerto fuente de la interfaz requerida.
3. Número máximo de muestras – Introduzca el número de muestras a registrar dentro del rango de valor de 1 a 65535.
4. Período de la Muestra – Introduzca los segundos que se reunirán las muestras de 5 a 3600 segundos.
5. Propietario – Establezca el creador de la tabla (límite: 30 caracteres).
6. Haga click en "Guardar" para guardar los parámetros. Haga click en "Salir" para descartar los parámetros.

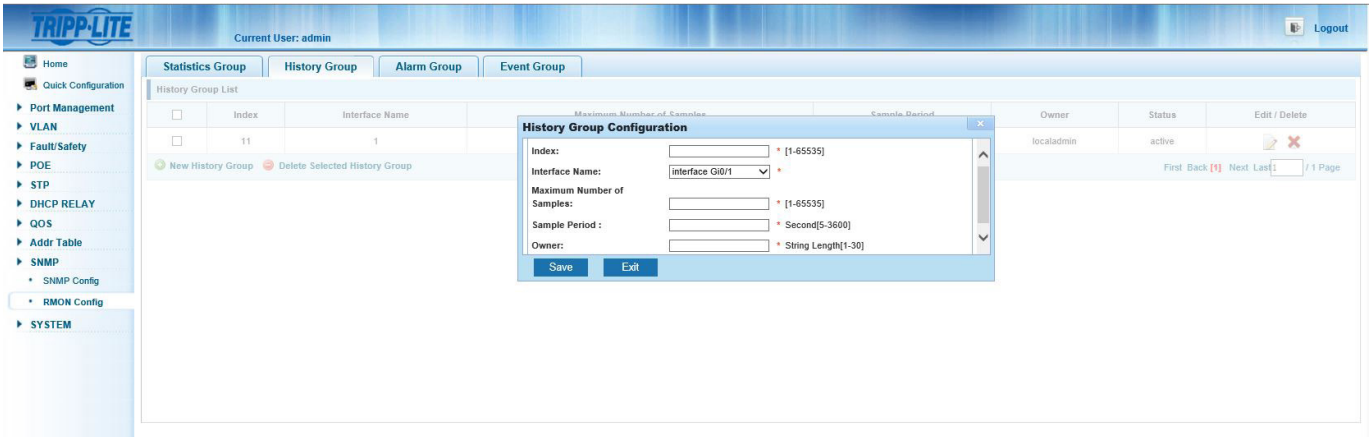


Figura 13.16: Nuevo Grupo de Historia

Para editar una configuración de Grupo de HIstoria, haga click en el ícono "Editar" para hacer cambios (Figura 13.17). Haga click en "Guardar" para guardar los cambios o haga click en "Salir" para descartarlos.

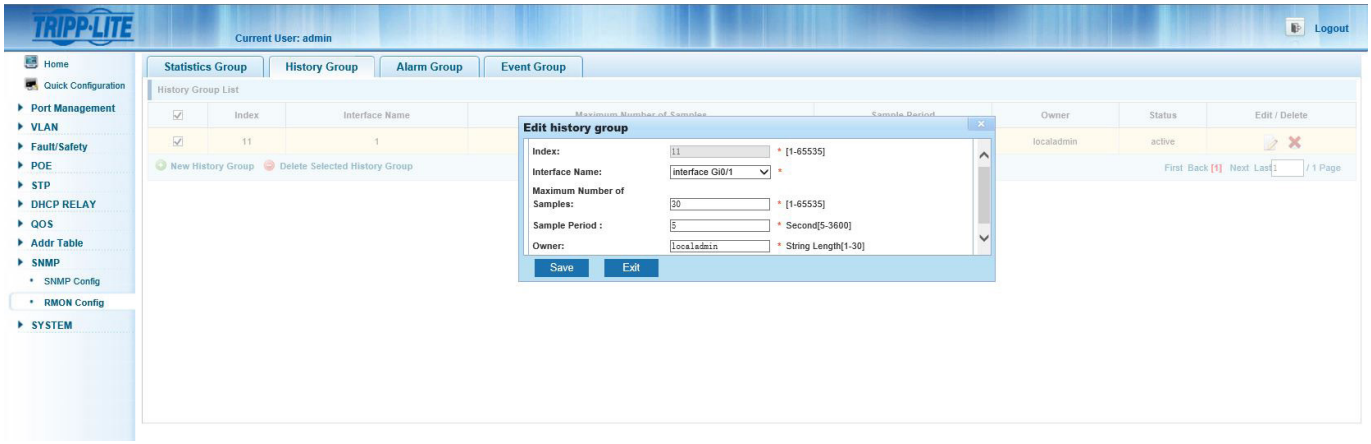


Figura 13.17: Editar Grupo de Historia

Para eliminar una configuración de grupo de historia, haga click en el ícono rojo junto a la entrada de grupo de historia a eliminarse, o marque la casilla junto a la entrada y haga click en el ícono "Borrar Grupo de Historia Seleccionado". Una vez confirmada, se eliminará la entrada de grupo de historia. Para eliminar varios grupos de histioria, haga click en la casilla de verificación junto a cada una de las entradas a eliminar, luego haga click en el ícono de "Eliminar Grupo de Historia Seleccionado". Una vez confirmada, se eliminarán las entradas de grupo de historia seleccionadas.

13.2.3 Grupo de Eventos

El grupo de eventos define disparadores de eventos y permite configurar alarmas para grabarlos. Para configurar, vaya a SNMP → Configuración de RMON → Configuración de Eventos, después siga estos pasos (Figura 13.18):

1. Índice – Ingrese el número índice dentro del rango de valores de 1a a 65535.
2. Descripción – Ingrese la descripción del grupo de eventos (límite: 30 caracteres).
3. Propietario – Ingrese el propietario del grupo de eventos (límite: 30 caracteres).
4. Acción – Ingrese una marca de verificación para registrar el evento, enviar una captura SNMP para el evento o ambos.
5. Haga click en "Guardar" para agregar el grupo de eventos a la lista. Haga click en "Salir" para descartar la configuración.

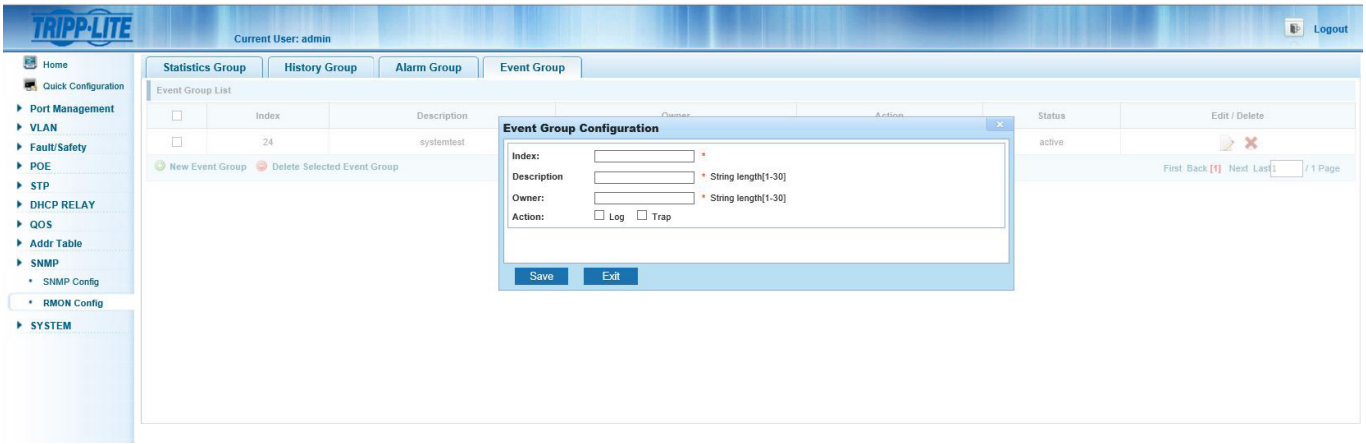


Figura 13.18: Nuevo Grupo de Eventos

Para editar una configuración de Grupo de Eventos, haga click en el ícono "Editar" para hacer cambios (Figura 13.19). Haga click en "Guardar" para guardar los cambios o haga click en "Salir" para descartarlos.

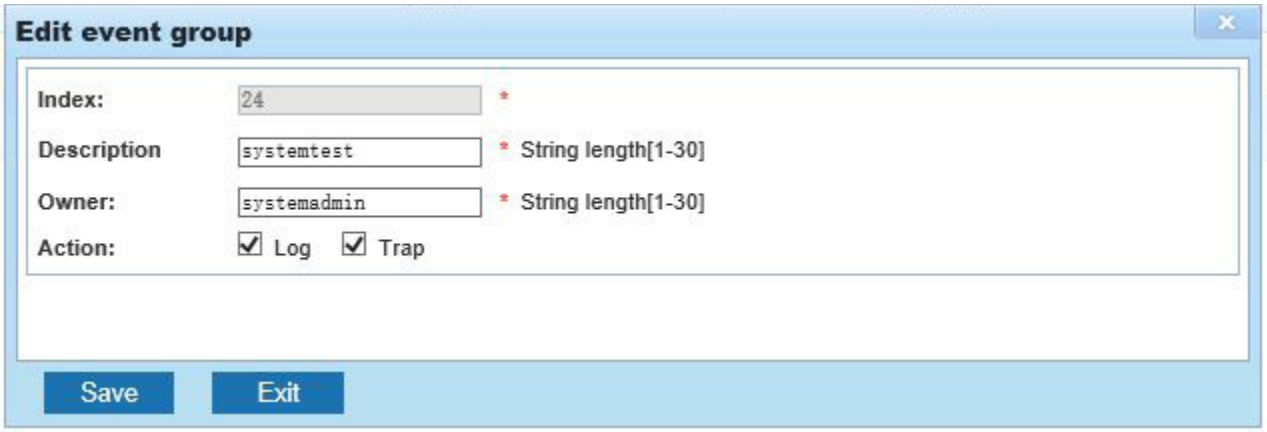


Figura 13.19: Editar Grupo de Eventos

Para eliminar una configuración de grupo de eventos, haga click en el ícono rojo junto a la entrada de grupo de eventos a eliminarse, o haga click en la casilla de verificación junto a la entrada y haga click en el ícono "Eliminar Grupo de Eventos Seleccionadas". Una vez confirmada, se eliminará la entrada de grupo de eventos. Para eliminar varios grupos de eventos, haga click en la casilla de verificación junto a cada una de las entradas a eliminar, luego haga click en el ícono de "Eliminar Grupo de Eventos Seleccionado". Una vez confirmada, se eliminarán las entradas de grupo de eventos seleccionadas.

13.2.4 Grupo de Alarmas

Para configurar un grupo de alarma para eventos de tráfico de datos especificados para desencadenar en los umbrales superiores e inferiores, configure los siguientes elementos
(Figura 13.20):

1. Índice: Coloque el número de índice de la lista de alarmas de 1 a 65535.
2. Evento Estadístico – Establece el tipo de evento para disparar una alarma. Los tipos de eventos son: DropEvents, Octets, Pkts, BroadcastPkts, MulticastPkts, CRCAlignErrors, UndersizePkts, OversizePkts, Fragments, Jabbers, Collisions, Pkts64Octets, Pkts65to127Octets, Pkts128to255Octets, Pkts256to511Octets, Pkts512to1023Octets y Pkts1024to1518Octets.
3. Índice de Grupo de Estadístico – Ingrese el Número Índice del Grupo Estadístico corresponiente para controlar el número de puerto.
4. Muestreo de Intervalo de Tiempo – Introduzca el intervalo de tiempo de la muestra entre 5 y 65535 segundos.
5. Tipo de Muestra – Elija el tipo de muestra: Absoluta o Delta.
6. Propietario – Ingrese el nombre del propietario. Permite de 1 a 30 caracteres.
7. Límite Superior de Umbral de Alarma – Anote la cantidad de tráfico de datos para definir el límite superior del rango de 0 a 2147483647.
8. Eventos de Límite Superior de Umbral de Alarma – Elija el Grupo de Eventos que desea activar cuando se alcance el umbral superior de alarma.
9. Límite Inferior de Umbral de Alarma – Ingrese la cantidad de tráfico de datos para definir el límite inferior de 0 a 2147483647.
10. Eventos de Límite Inferior de Umbral de Alarma – Elija el grupo de eventos que desea activar cuando se alcance el umbral inferior de alarma.
11. Para guardar la configuración, haga click en “Guardar”. Haga click en "Salir" para descartar los parámetros.

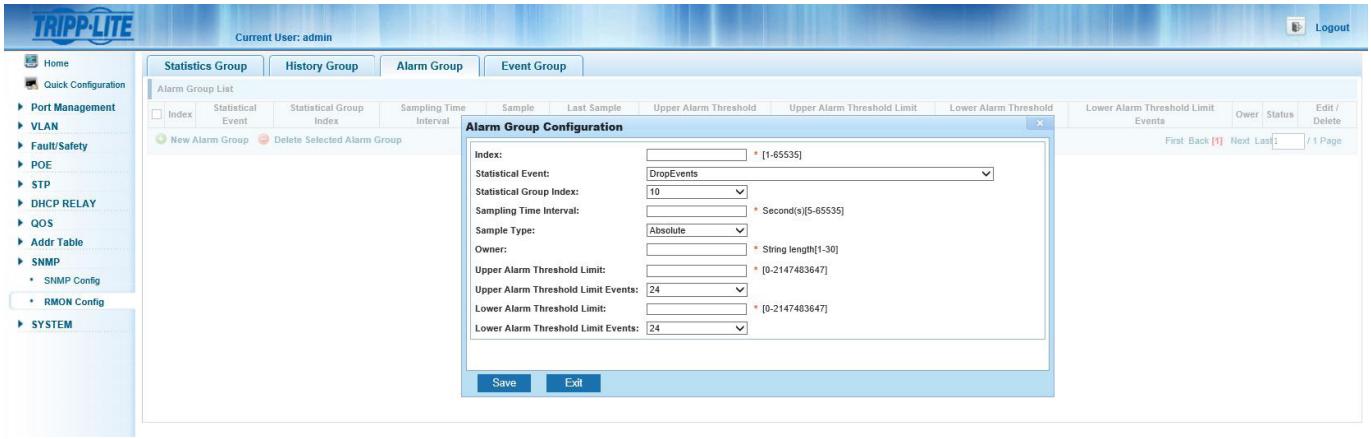


Figura 13.20: Nuevo Grupo de Alarmas

13. Administración del Protocolo Simple de Administración de Red [SNMP]

Para editar una configuración de Grupo de Alarmas, haga click en el ícono "Editar" para hacer cambios (Figura 13.21). Haga click en "Guardar" para guardar los cambios o haga click en "Salir" para descartar los cambios.

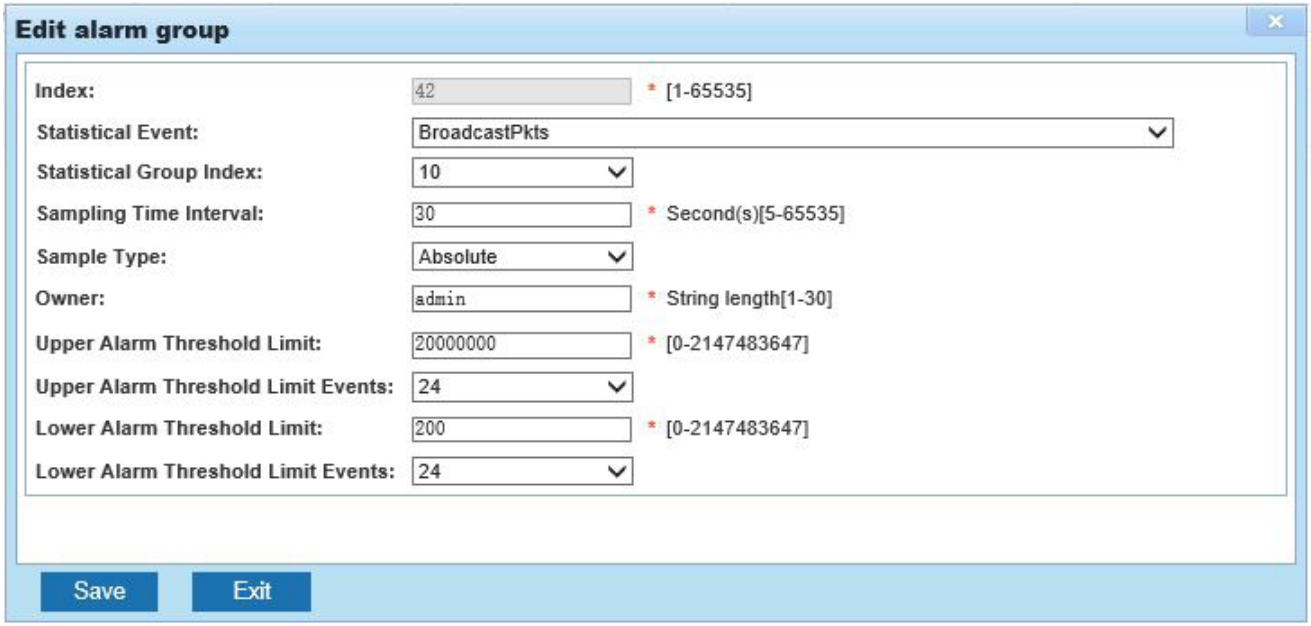


Figura 13.21: Edición de Grupo de Alarmas

Para eliminar una configuración de grupo de alarmas, haga click en el ícono rojo junto a la entrada de grupo de alarmas a eliminarse, o ponga una marca en la casilla junto a la entrada y haga click en el ícono "Borrar Grupo de Alarmas Seleccionado". Una vez confirmada, se eliminará la entrada de grupo de alarmas. Para eliminar varios grupos de alarmas, haga click en la casilla de verificación junto a cada una de las entradas a eliminar, luego haga click en el ícono de "Eliminar Grupo de Alarmas Seleccionado". Una vez confirmada, se eliminarán las entradas de grupo de alarmas seleccionadas.

14. Administración del Sistema

La Configuración del Sistema (Figura 14.1) le permite establecer la configuración del sistema del switch; realizar actualizaciones del sistema; guardar, respaldar y restaurar configuraciones; guardar configuraciones de arranque; establecer privilegios de administración y ver información acerca de la configuración del switch.

14.1 Configuración del Sistema

Para establecer la configuración del switch y configurar la hora del sistema, ingrese lo siguiente:

Información Básica del Sistema – Ingrese las funciones necesarias junto con las actualizaciones de información opcionales:

VLAN de Administración – Seleccione la VLAN de administración requerida de la lista desplegable. Para seleccionar otra VLAN para ser la VLAN de administración, primero debe ser creada en la configuración de VLAN (sección 4.1). Cuando termine, haga click en “Establecer VLAN de Administración”.

IP de Administración – Ingrese la dirección IP de la VLAN de administración requerida.

Máscara de Subred: La máscara de subred de la VLAN de administración del switch.

Portal Predeterminado – Introduzca la dirección IP del portal de enlace si es necesario.

Jumbo Frames – De forma predeterminada, los Jumbo Frames se establecen en 1518. Puede configurarse entre 1518 y 9216 frames.

Servidor DNS – Ingrese la dirección IP del servidor DNS si se requiere.

Tiempo de Espera de Inicio de Sesión (minutos) – De forma predeterminada, el temporizador de cierre de sesión se establece en 30 minutos. Se puede ajustar a cualquier período de tiempo entre 0 y 86400 minutos.

Dispositivo MAC – La dirección MAC del switch.

Nombre del Dispositivo – De forma predeterminada, se introduce el nombre del modelo del switch, pero puede ser cambiado para adaptarse a la utilización de la aplicación (límite: 32 caracteres).

Ubicación del Dispositivo – Introduzca la ubicación del dispositivo del switch (límite: 32 caracteres).

Contactos (incluido buzón) – Ingrese las direcciones de correo electrónico de los contactos.

Haga click en "Guardar" para guardar los parámetros.

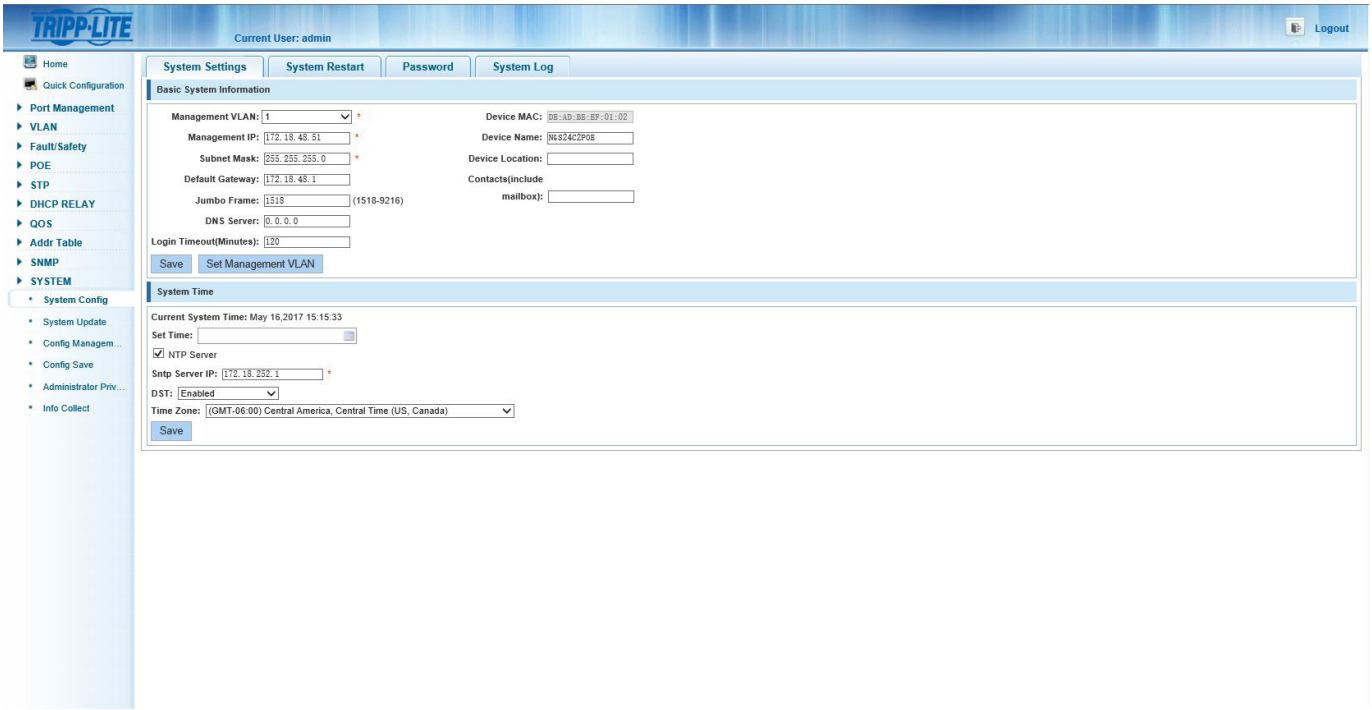


Figura 14.1: Parámetros del Sistema

14. Administración del Sistema

14.1.1 Hora del Sistema

La hora del sistema muestra la hora actual del sistema, que puede ser configurada manualmente o proporcionada automáticamente por un servidor NTP.

Establezca Manualmente la Hora – Ingrese a la hora establecida mediante el calendario emergente, ajuste manualmente la fecha y hora, utilice el ícono de selección rápida o haga click en el botón de hoy. Haga click en "Aceptar" para guardar la configuración de la hora.

Configure la Hora Mediante el Servidor NTP – Si se utiliza un servidor NTP, haga click en la casilla de verificación de la casilla de servidor NTP. A continuación, establezca la dirección IP del servidor SNTP requerida. Si la zona horaria es compatible con horario de verano, cambie la opción de DST a Habilitada. Entonces, ingrese la zona horaria deseada.

Haga click en "Guardar" para guardar la configuración de la zona horaria.

14.1.2 Reinicio del Sistema

Para reiniciar el switch, haga click en el botón "Reiniciar". El proceso de reinicio puede tardar hasta un minuto. La página se refrescará a la página de inicio de sesión.

Nota: *Para asegurar que su configuración de arranque se guarda antes de un reinicio vaya a SISTEMA → Guarde configuración y haga click en el botón "Guardar Configuraciones" para guardar la configuración de inicio.*

14.1.3 Modificar Contraseña del Administrador

Para cambiar la contraseña de administrador, escriba la contraseña anterior, luego la contraseña nueva. Reingrese la nueva contraseña para confirmar. Haga click en "Guardar" para guardar los parámetros. Haga click en "Borrar" para descartar los cambios.

14.1.4 Parámetros de Registro del Sistema

Esta pantalla le permite ver y buscar a través de la información del registro actual del switch. Si necesita configurar un servidor de Syslog para recibir registros basados en el nivel de registro, realice los siguientes pasos:

1. Switch de Registro – Activa el registro (predeterminado).
2. Servidor IP – Ingrese el Servidor IP de Syslog.
3. Nivel de Registro de Envío – Seleccione los eventos de nivel de registro para ser enviados como emergencias (0) alertas (1) críticas (2), errores (3), avisos (4), notificaciones (5), informativo (6) o depuración (7). Haga click en "Guardar" para guardar los parámetros.

14.2 Actualizaciones del Sistema

La pestaña de Actualización del Sistema (Figura 14.2) permite las actualizaciones de firmware del sistema. La versión actual de firmware aparece en la parte superior de la sección. Haga click en el botón de examinar para obtener actualizaciones de firmware. Cuando esté listo haga click en “Iniciar Actualización”. El sistema se reiniciará a la pantalla de inicio de sesión cuando termine.

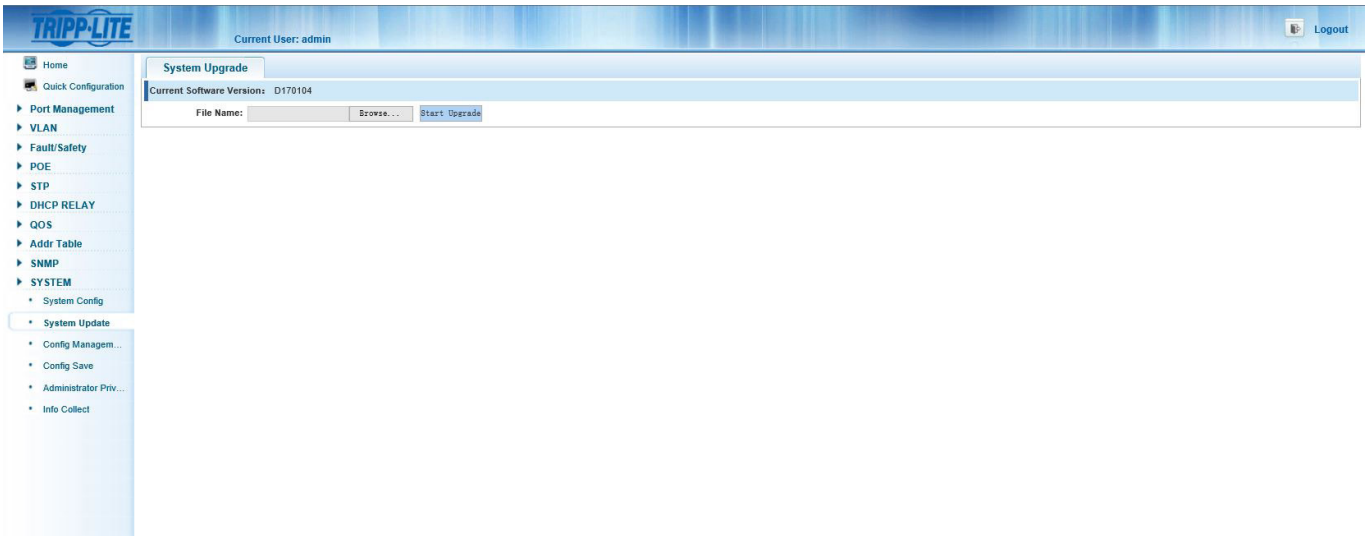


Figura 14.2: Actualizaciones del Sistema

14. Administración del Sistema

14.3 Administración de Configuración del Sistema

14.3.1 Configuración de Importar / Exportar

Esta sección le permite importar y exportar configuraciones de sistema, restaurar configuraciones anteriores y realizar un restablecimiento de fábrica (Figura 14.3).

Figura 14.3: Importar / Exportar Configuración

14.3.2 Mostrar Configuración Actual

Para ver la configuración actual del switch (Figura 14.4), haga click en el botón "Mostrar Config Actual".

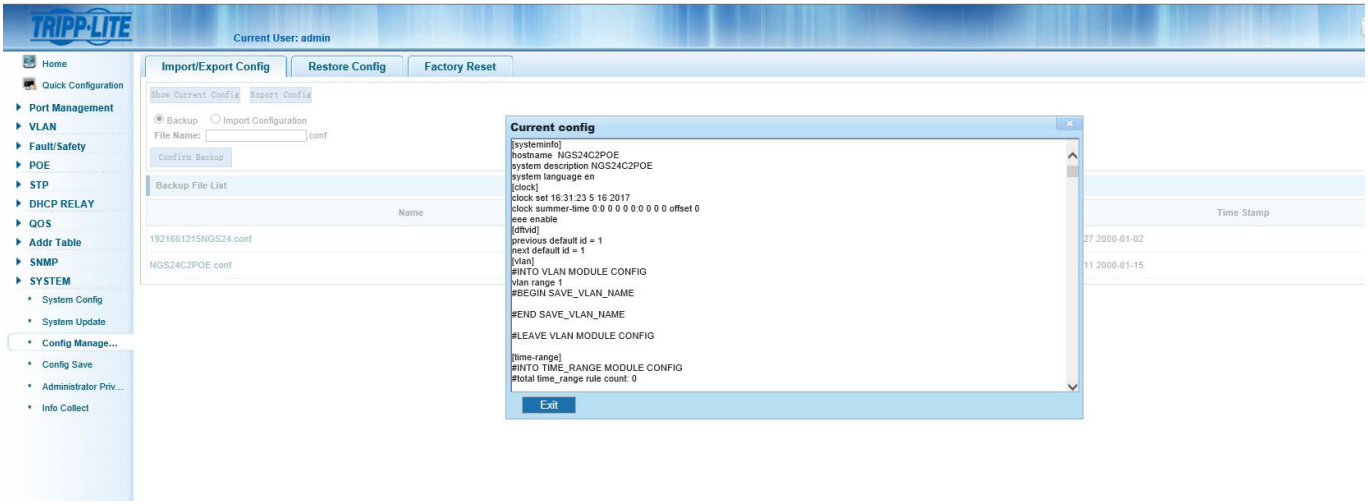


Figura 14.4: Configuración Actual

14.3.3 Exportar Configuración Actual

Haga click en el botón "Mostrar configuración actual" para ver la configuración del sistema. Haga click en el botón "Exportar" para guardar la configuración del switch en un sistema de Copia de Respaldo local.

14.3.4 Configuración de la Copia de Respaldo

Para guardar copias de seguridad locales del archivo de configuración, seleccione "Copia de Respaldo" y escriba el nombre de archivo para la Copia de Respaldo. Haga click en "Confirmar Copia de Respaldo" para guardar la configuración. Las configuraciones guardadas se pueden ver en la Lista de Archivos de Copia de Respaldo. Pueden guardarse hasta cinco archivos de configuración en Copia de Respaldo.

14.3.5 Importar Configuración

Seleccione "Importar Configuración" y busque el archivo de configuración exportado a importar. Haga click en el botón de "Importar Configuración". Para habilitar la configuración, seleccione "Reiniciar Dispositivo".

14.3.6 Restaurar Configuración

Le permite administrar los archivos de configuración de Copia de Respaldo guardados.

14.3.7 Restaurar Copia de Respaldo

Para restaurar una configuración guardada, seleccione el nombre de la configuración que desea restaurar. Haga click en "Confirmar Recuperación" para restaurar la configuración en el sistema (Figura 14.5).

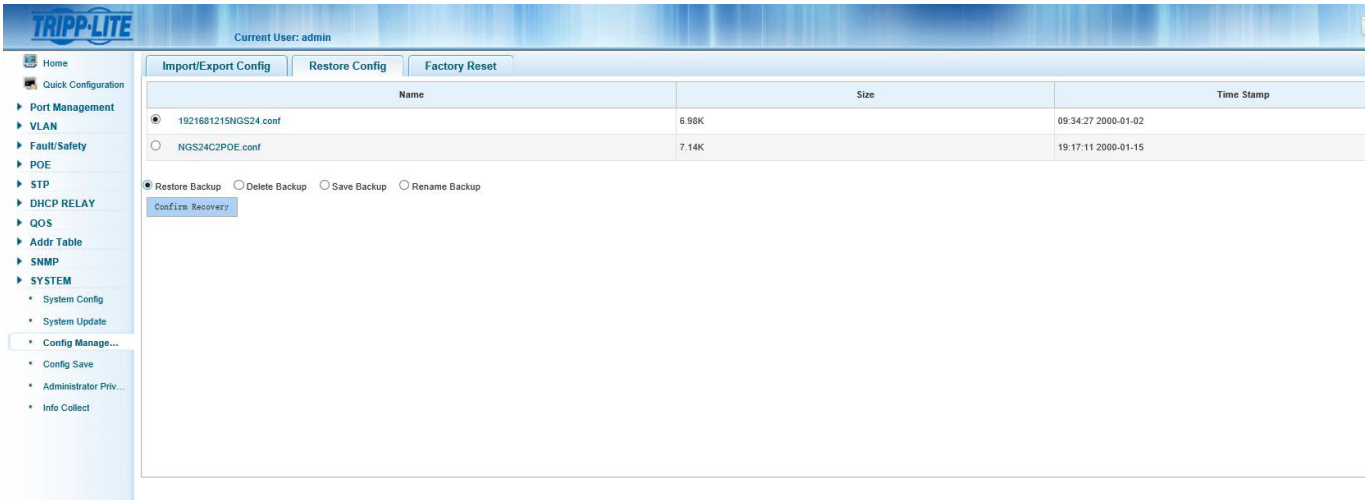


Figura 14.5: Restaurar Copia de Respaldo

14.3.8 Eliminar Copia de Respaldo

Para eliminar una Copia de Respaldo de configuración que ya no es necesaria, seleccione el nombre del archivo de configuración. Seleccione la opción "Eliminar Copia de Respaldo"". Haga click en "Confirmar Eliminación" para eliminar el archivo de configuración del sistema (Figura 14.6).

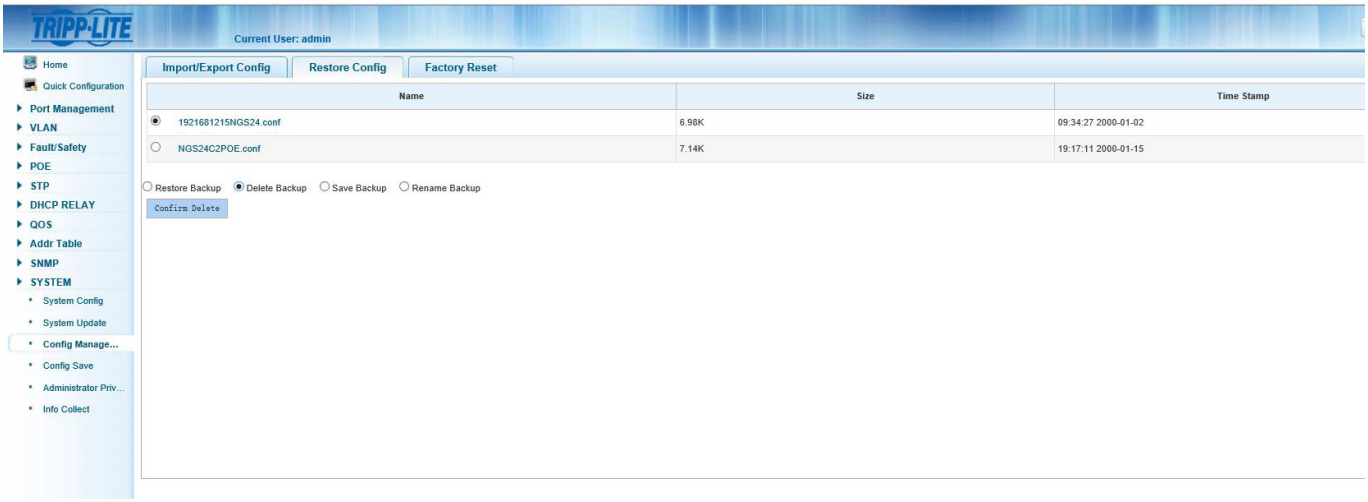


Figura 14.6: Eliminar Copia de Respaldo

14.3.9 Guardar Copia de Respaldo

Al restaurar, borrar o cambiar el nombre de una Copia de Respaldo, seleccione "Guardar Copia de Respaldo" para guardar la configuración actual. Haga click en "Confirmar Guardar" para guardar la configuración (Figura 14.7).

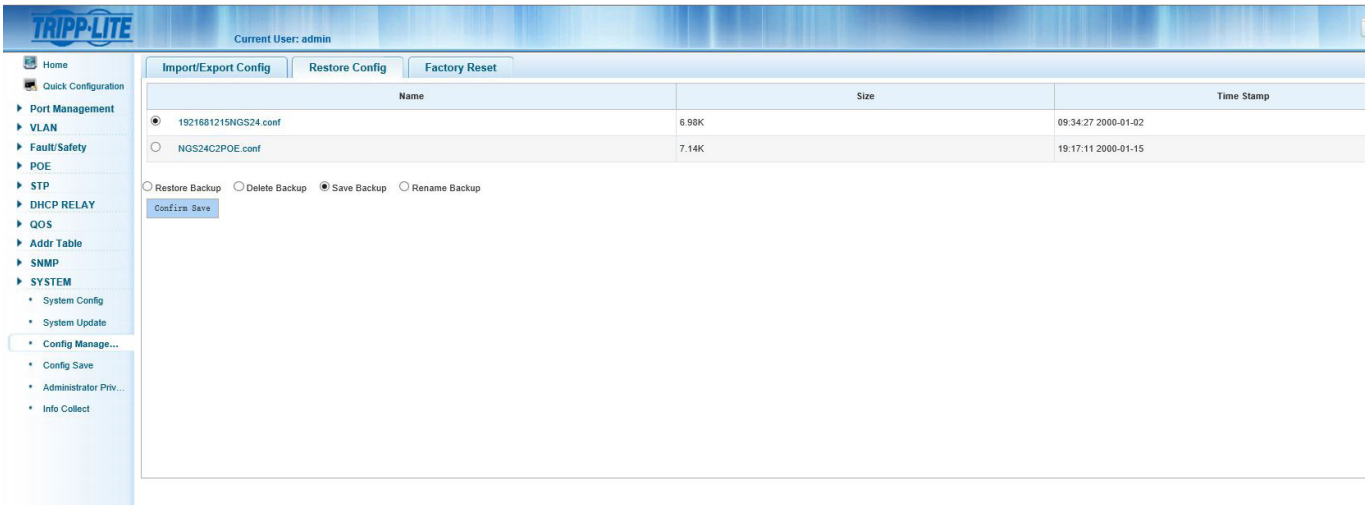


Figura 14.7: Guardar Copia de Respaldo

14.3.10 Restaurar a Condiciones de Fábrica

Para volver el switch a la configuración original de fábrica, seleccione SISTEMA → Administración de Configuración → Restaurar Condiciones de Fábrica. Al hacer click en “Restaurar Condiciones de Fábrica” se eliminarán todas las configuraciones guardadas del sistema y se restaurará el switch a las configuraciones de fábrica (Figura 14.8).

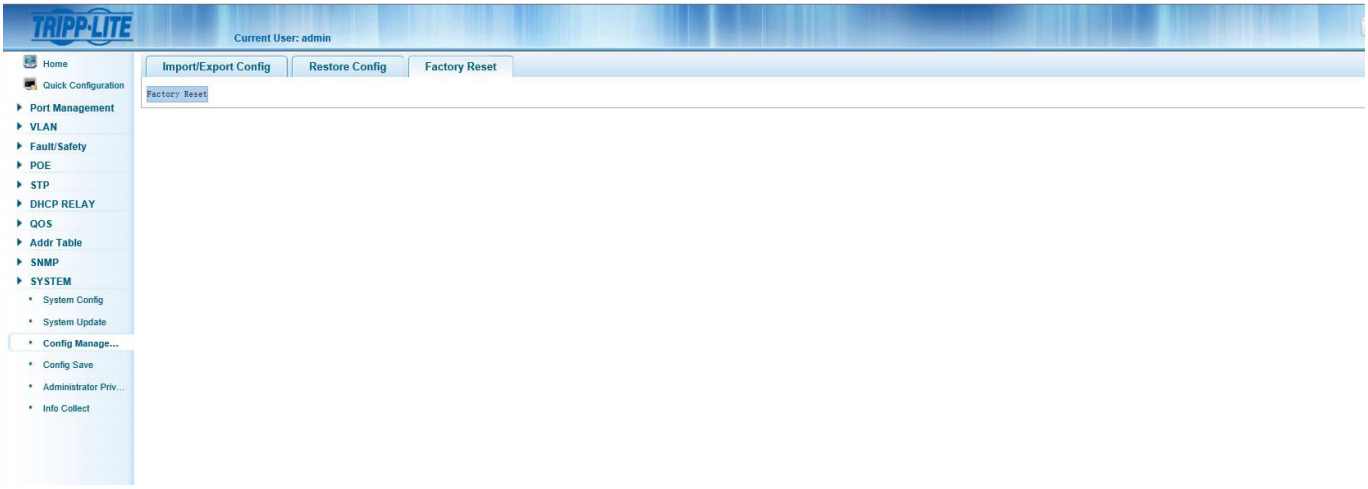


Figura 14.8: Restaurar Condiciones de Fábrica

14. Administración del Sistema

14.4 Guardar Configuración

Para guardar su configuración de arranque, haga click en el botón "Guardar Configuración" (Figura 14.9).

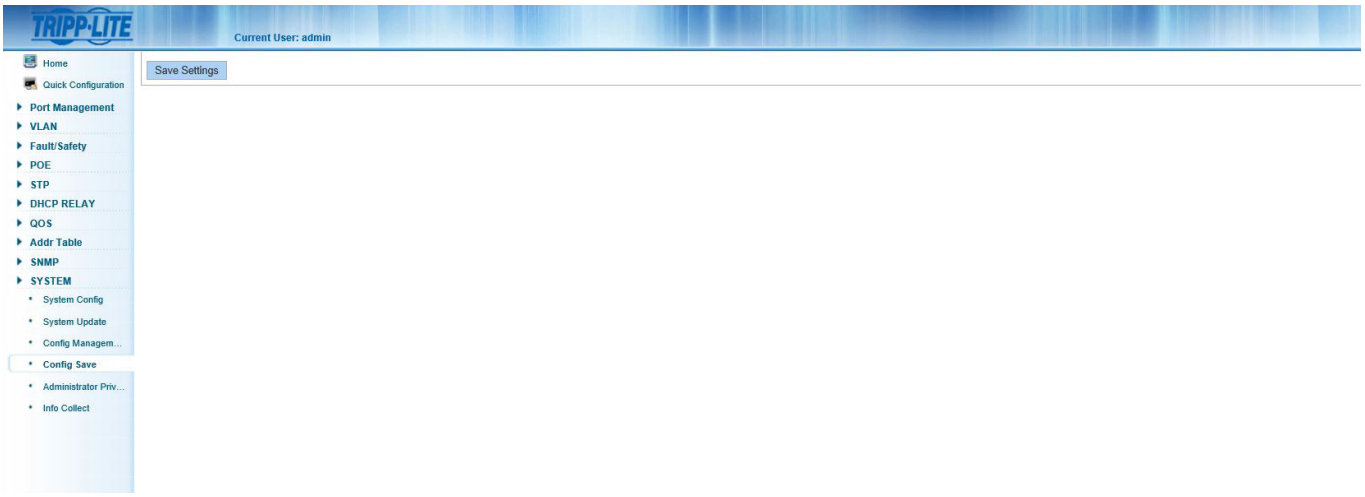


Figura 14.9: Guardar Configuración

14.5 Privilegios de Administrador

Esta sección permite al administrador agregar usuarios adicionales para acceder al switch (Figura 14.10). Una cuenta de "usuario" puede iniciar sesión en el sistema de administración de Web de equipos para mantenimiento de rutina. Además el administrador y el usuario, se pueden agregar hasta cinco usuarios adicionales. Los usuarios normales sólo pueden acceder a la página de inicio de sistema. Para crear un usuario nuevo, siga estos pasos:

1. Nombre de Usuario – Ingrese el nombre de usuario para el nuevo usuario.
2. Nueva Contraseña – Ingres la contraseña del nuevo usuario.
3. Confirme Contraseña – Vuelva a ingresar la contraseña del nuevo usuario.
4. Haga click en el botón "Agregar Usuario" para agregar el nuevo usuario a la lista de usuarios.

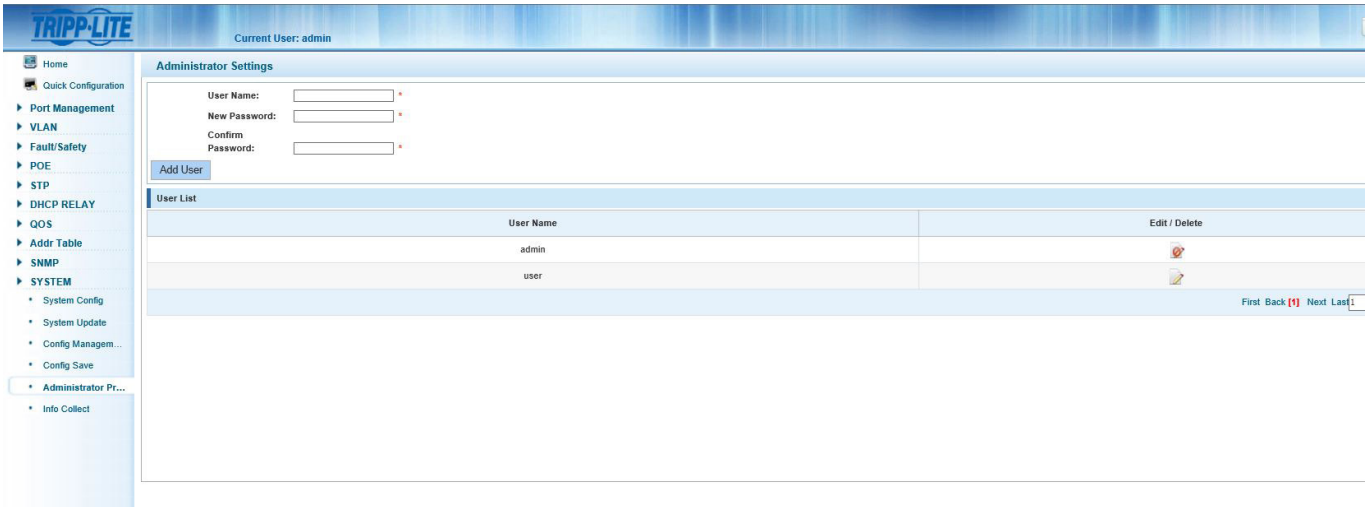


Figura 14.10: Vista de Configuraciones del Administrador

14.5.1 Editar Contraseñas de Usuarios

Para cambiar la contraseña de un usuario, seleccione el nombre de usuario y haga click en el ícono de "Editar" (Figura 14.11). Ahora se puede crear una nueva contraseña para el usuario. Haga click en "Confirmar Edición" para guardar la nueva contraseña. Haga click en "Cancelar Edición" para descartar los cambios.

Para eliminar un usuario, haga click en el ícono rojo para quitar el usuario de la lista.

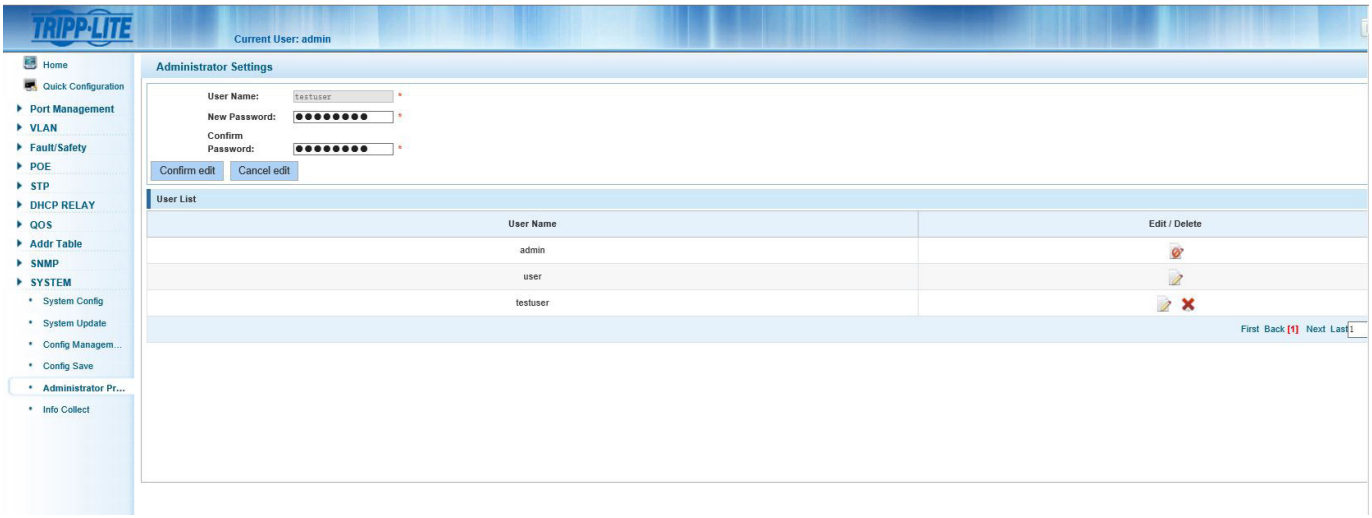


Figura 14.11: Editar Usuario

Nota: *Las cuentas de "Admin" y de "Usuario" original no se pueden eliminar. El administrador puede editar la cuenta de usuario original y eliminar otras cuentas de usuario creadas por la cuenta de Admin.*

14.6 Recolección de Información

Haga click en el botón "Recopilar" (Figura 14.12) para crear un archivo de información de depuración con toda la información sobre el switch. Aparecerá una pantalla emergente que permite que el archivo de información de depuración se guarde en el sistema local. El archivo de información de depuración puede luego verse con un editor de texto como el Block de Notas, Wordpad, etc.

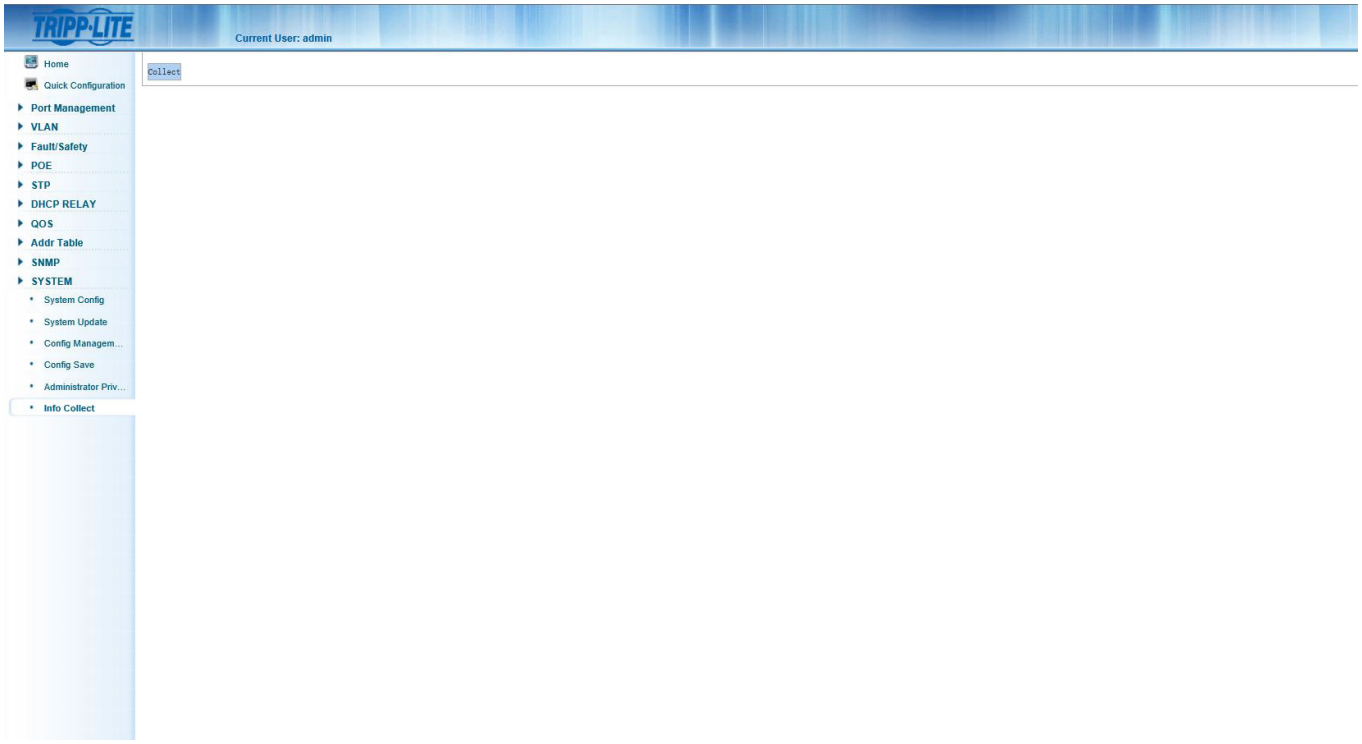


Figura 14.12: Recolección de Información

15. Solución de Problemas

Si encuentra un problema:

- Revise las conexiones y confirme que estén firmes
- Reinicie el sistema y vea si el problema persiste
- Consulte tripplite.com/support para buscar actualizaciones de software y asegurarse de que está utilizando la versión más actualizada que sea compatible con su dispositivo
- Si el problema persiste después de intentar los pasos anteriores, póngase en contacto con Soporte Técnico de Tripp Lite

16. Soporte Técnico

Antes de acudir al Soporte Técnico de Tripp Lite, refiérase a la Sección 15. Revise resolución de problemas para ver posibles soluciones. Si aún no puede resolver el problema, póngase en contacto con Soporte Técnico de Tripp Lite en:

www.tripplite.com/support

Correo Electrónico: techsupport@tripplite.com

Tripp Lite tiene una política de mejora continua. Las especificaciones están sujetas a cambios sin previo aviso.

Guide de l'utilisateur

Guide de configuration Web du commutateur intelligent Gigabit L2

(Modèles de commutateurs intelligents de la série NGS)

1111 W. 35th Street, Chicago, IL 60609 USA • www.tripplite.com/support

Table des matières

Table des matières

1. Introduction

Ce guide décrit comment configurer les modèles de commutateurs Web intelligents Gigabit L2 de Tripp Lite (série NGS) en utilisant l'interface utilisateur graphique (GUI) Web intégrée. Les modèles de commutateurs Web intelligents Gigabit L2 de Tripp Lite comprennent un serveur Web incorporé et un logiciel de gestion pour la gestion et la surveillance des fonctions du commutateur. L'interface de gestion Web peut être utilisée pour configurer des fonctionnalités plus avancées qui peuvent améliorer l'efficacité du commutateur et la performance globale du réseau. Le port de la console permettra l'interface de ligne de commande pour le commutateur (utilisation future).

Remarque : *Les commutateurs Web intelligents Gigabit L2 sont appelés le « commutateur » dans le manuel. Les informations dans le présent document s'appliquent à tous les modèles de commutateurs sauf indication contraire.*

1.1 Configurations du commutateur

Les commutateurs comprennent différentes quantités de ports et différentes fonctionnalités, mais leur configuration au moyen de l'interface de gestion Web est constante.

Section 1 : Introduction Comprend l'aperçu du contenu de l'ensemble du manuel de configuration.

Section 2 : Configuration de la gestion Web Comprend la configuration initiale qui doit avoir lieu avant la connexion au commutateur, de même que des instructions pour se connecter à l'interface de gestion Web du commutateur.

Section 3 : Page d'accueil de l'interface de gestion Web Cette section permet de se familiariser avec l'interface de gestion Web.

Section 4 : Configuration rapide Illustre comment configurer rapidement les fonctionnalités de gestion au moyen de l'interface Web.

Section 5 : Gestion des ports Présente les paramètres communément utilisés pour les ports du commutateur.

Section 6 : Gestion du réseau local virtuel Aperçu de la gestion et de la configuration des réseaux locaux virtuels

Section 7 : Gestion des défaillances et de la sécurité Décrit la gestion et la configuration de la sécurité comme la prévention des attaques, les listes de contrôle d'accès, etc.

Section 8 : Gestion du système d'alimentation électrique par câble Ethernet (PoE) Décrit la gestion et la configuration de l'alimentation électrique par câble Ethernet (PoE) au moyen de l'interface de gestion Web (s'applique uniquement aux commutateurs prévus pour l'alimentation par câble Ethernet).

Section 9 : Gestion du Spanning Tree Protocol (STP) Décrit la gestion de la configuration du Spanning Tree Protocol du commutateur.

Section 10 : Gestion du relais DHCP Couvre la configuration de l'agent du relais DHCP et la configuration des paramètres de l'Option 82 vers un serveur DHCP.

Section 11 : Gestion de la qualité du service (QOS) Décrit la gestion de la QoS de chaque port du commutateur.

Section 12 : Gestion du tableau d'adresses MAC Couvre la gestion de la liste d'accès au tableau d'adresses MAC.

Section 13 : Gestion SNMP Couvre la configuration des fonctionnalités pour la gestion SNMP du commutateur.

Section 14 : Gestion du système Guide pour la gestion du système du commutateur, y compris les mises à niveau logicielles au moyen de la page Web, la configuration de la gestion des fichiers, etc.

Annexe I : Paramètres par défaut Référence rapide aux paramètres par défaut pour la connexion, le mot de passe, etc.

2. Configuration de la gestion Web

2.1 Configuration initiale

2.1.1 Configurer l'adresse IP de l'ordinateur

L'adresse IP de l'ordinateur de gestion et le commutateur doivent être configurés sous le même sous-réseau. (L'adresse IP par défaut du commutateur est 192.168.2.1 et le masque de sous-réseau par défaut est 255.255.255.0.) Il n'est pas nécessaire de configurer la passerelle pour la configuration initiale du commutateur.

L'adresse IP de l'ordinateur de gestion doit être configurée manuellement à l'intérieur de la plage de l'adresse IP par défaut de 192.168.2.xxx (« xxx » varie entre 2 et 254).

Par défaut, tous les ports appartiennent à VLAN1 (réseau local virtuel 1). L'ordinateur de gestion hôte peut effectuer la configuration du commutateur en accédant à un port.

Remarque : *Le présent manuel convient pour tous les modèles de la famille de commutateurs Web gérés intelligents de la série NGS de Tripp Lite. Le présent guide de l'utilisateur utilise comme exemple une configuration de commutateur pour illustrer comment configurer le commutateur en utilisant l'interface de gestion Web.*

2.1.2 Confirmer la connectivité réseau entre l'ordinateur et le commutateur

Suivre les étapes ci-dessous pour confirmer la connectivité réseau entre l'ordinateur et le commutateur :

Étape 1 : Appuyer sur la touche Windows + R, taper cmd dans la zone d'entrée de la fenêtre « Run », puis cliquer sur « OK ». Le système ouvre alors la fenêtre du message-guide (Figure 2.1).

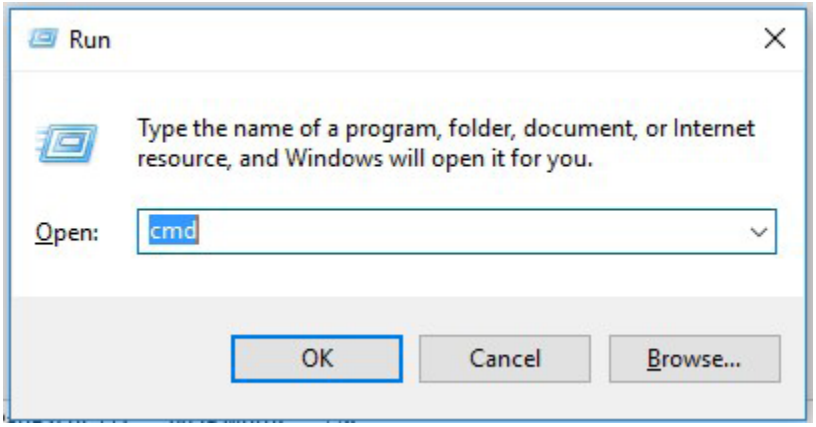


Figure 2.1 : Confirmer la connectivité de réseau

Étape 2 : Dans la fenêtre de dialogue du message-guide, taper le ping 192.168.2.1, puis appuyer sur « Enter ». Si le commutateur renvoie une réponse au ping, une connectivité de réseau appropriée est établie. Si aucune réponse n'est reçue, vérifier la connectivité de réseau.

2. Configuration de la gestion Web

2.1.3 Accès à l'interface de gestion Web

Ouvrir un navigateur Web (p. ex. Internet Explorer), taper **http://192.168.2.1** dans la barre d'adresse, puis appuyer sur « Enter » (entrée). Saisir l'interface de connexion de l'utilisateur de la page d'administration du commutateur. Dans l'interface de connexion (Figure 2.2), sélectionner la langue préférée (la langue par défaut est l'anglais), puis saisir le nom d'utilisateur et le mot de passe. Le nom d'utilisateur et le mot de passe par défaut sont tous les deux admin (sensible à la casse). Cliquer sur le bouton « Login » (connexion) ou appuyer sur « Enter » (entrée) pour accéder à l'interface de gestion Web.

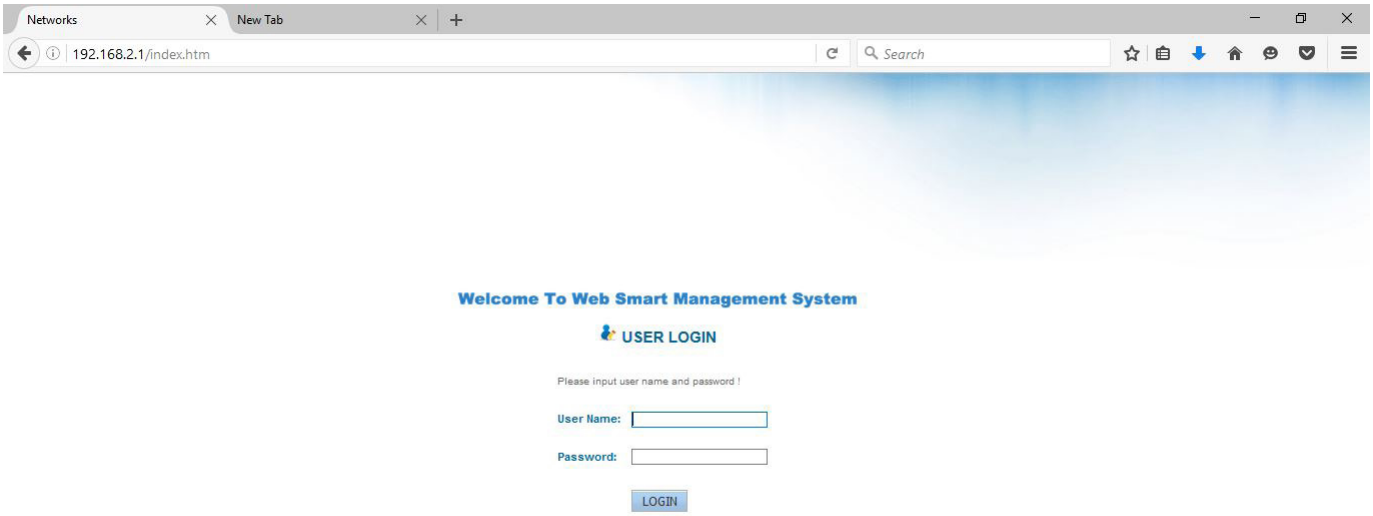


Figure 2.2 Page de renvoi de l'interface de connexion Web

Une fois la connexion réussie, le navigateur affichera la page d'accueil de l'interface de gestion Web correspondant au commutateur, comme illustré sur la Figure 2.3 :

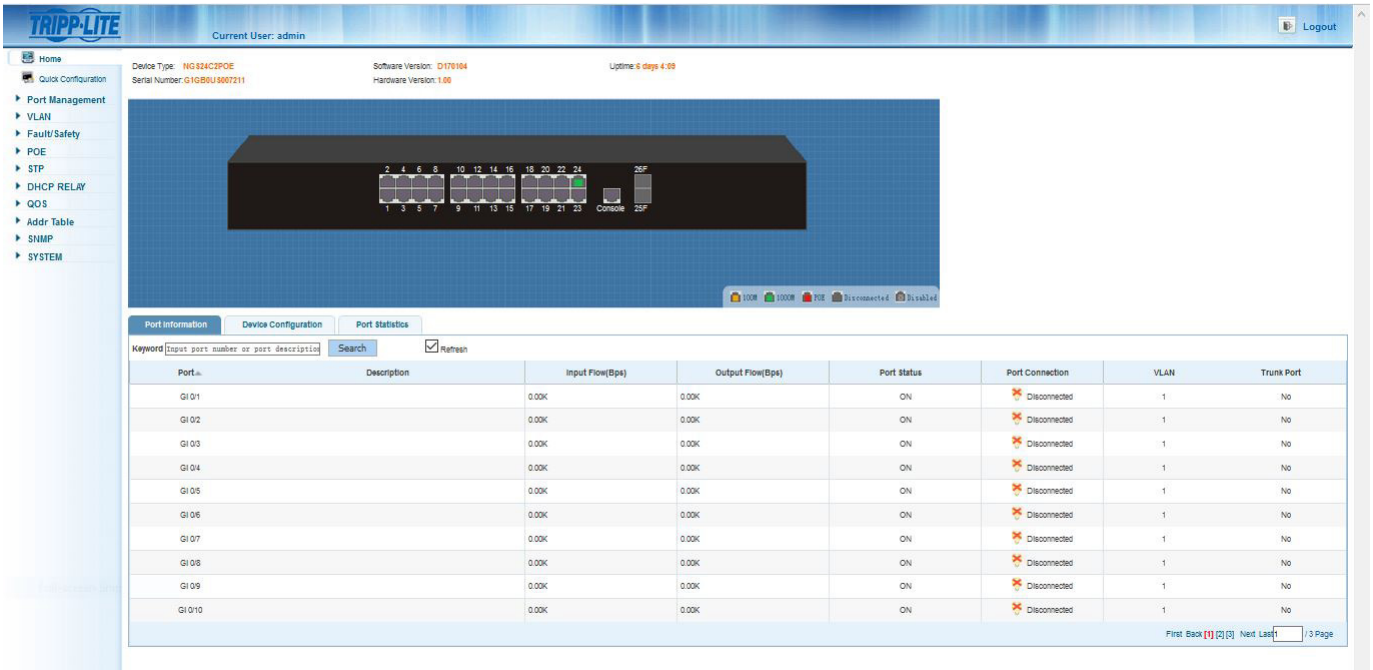


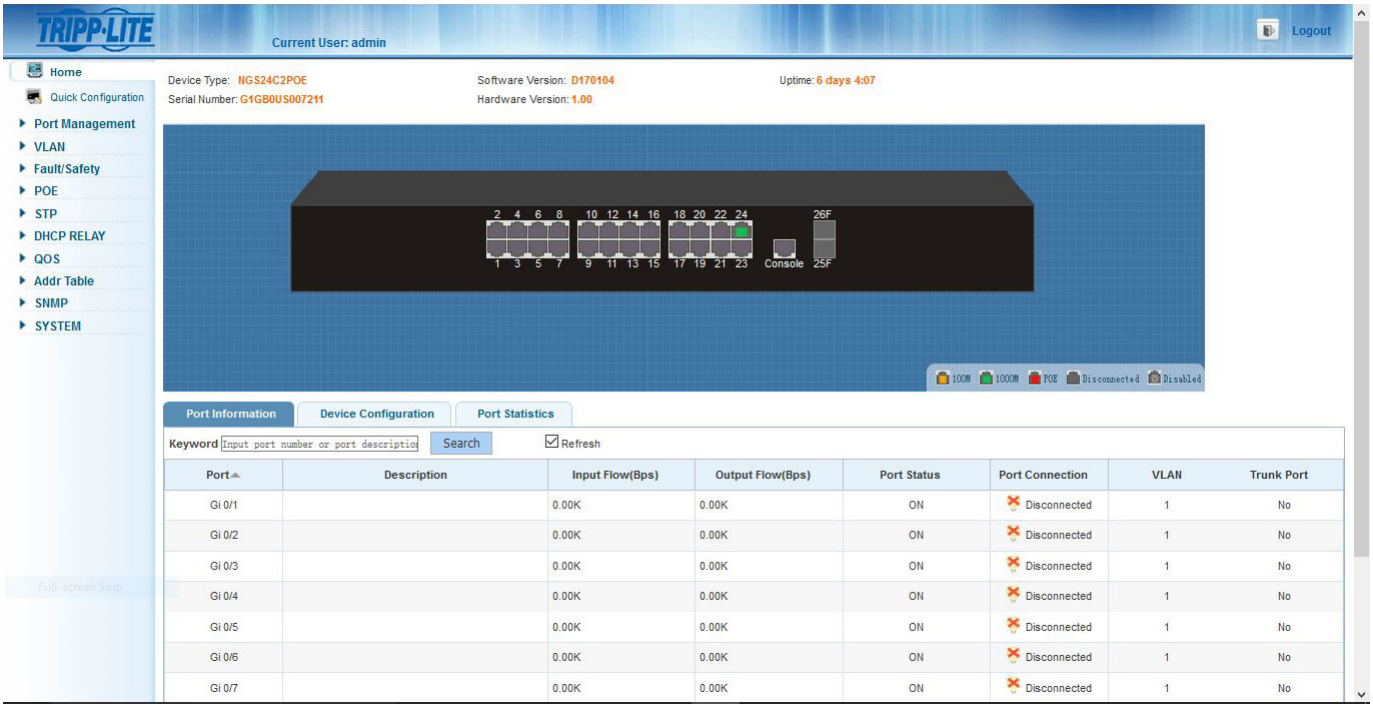
Figure 2.3 Interface de gestion Web du commutateur (vue de l'administrateur)

Remarques :

- *Il est recommandé d'utiliser Internet Explorer 8 ou une version ultérieure, Firefox ou Chrome avec l'interface de gestion Web.*

3. Page d'accueil de l'interface de gestion Web

3.1 Aperçu de la page d'accueil de l'interface de gestion Web



La page d'accueil de l'interface de gestion Web affiche l'utilisateur actuel, des informations sur le système du commutateur, le temps utilisable, des informations sur les ports du réseau, la configuration de l'appareil et les statistiques des ports. Le graphique du commutateur affiche les connexions actuelles fonctionnant à 10/100 (orange), 1 000 Mbps (vert), alimentation électrique par câble Ethernet (PoE) active (rouge), déconnecté (gris) ou désactivé (gris avec un X).

3.2 Menus de l'interface de gestion Web

Il y a 12 options de menus principaux dans l'interface de gestion Web : System Home (accueil du système), Quick Configuration (configuration rapide), Port Management (gestion des ports), VLAN (réseau local virtuel), Fault/Safety (défaillance/sécurité), PoE (alimentation électrique par câble Ethernet) (s'applique uniquement aux commutateurs prévus pour l'alimentation par câble Ethernet), STP, DHCP RELAY (relais DHCP), QoS, Addr Table (tableau des adresses), SNMP et System (système).

Chaque option de menus principaux comprend un menu secondaire. Par défaut, les menus secondaires sont dissimulés. Cliquer sur une option de menus principaux pour agrandir le menu secondaire.

- **Page d'accueil de l'interface de gestion Web**
- **Configuration rapide**
  - o Paramètres du réseau local virtuel
  - o Autres paramètres
- **Gestion des ports**
  - o Paramètres de base
  - o Agrégation de ports
  - o Miroir de port
  - o Limite de vitesse des ports
  - o Storm Control
  - o Isolation des ports
- **Gestion du réseau local virtuel**
  - o Gestion du réseau local virtuel
- **Gestion des défaillances/de la sécurité**

- o Prévention des attaques
- o Détection du cheminement
- o LCA (liste de contrôle d'accès)

- **Gestion du système d'alimentation électrique par câble Ethernet (PoE)**
  - o Configuration de l'alimentation électrique par câble Ethernet (PoE)
  - o Configuration du port de l'alimentation électrique par câble Ethernet (PoE)
- **STP (Spanning Tree Protocol)**
  - o Région MSTP
  - o Pont STP
- **Relais DHCP**
  - o Relais DHCP
  - o Option 82
- **QOS (qualité de service)**
  - o Remarque sur la QOS
  - o Configuration de la file d'attente
  - o Mappage de la file d'attente
- **Tableau des adresses (Tableau des adresses Mac)**
  - o Tableau des adresses
- **SNMP**
  - o Configuration de SNMP
  - o Configuration de RMON
- **Système**
  - o Configuration du système
  - o Mise à jour du système
  - o Gestion de la configuration
  - o Sauvegarder la configuration
  - o Privilèges administratifs
  - o Réinitialisation d'usine
  - o Recueillir des informations

Remarque : *S'il n'y a aucune activité dans l'interface de gestion Web pendant 30 minutes (paramètre par défaut), le système déconnectera automatiquement l'utilisateur et retournera à la page de renvoi de l'interface de gestion Web.*

4. Configuration rapide

Sélectionnez « Quick Configuration » (configuration rapide) pour configurer les fonctionnalités fréquemment utilisées du commutateur, comme les paramètres des réseaux locaux virtuels, des ports de la ligne réseau, du système de gestion et des mots de passe de l'interface de gestion.

4.1 Ajouter des réseaux locaux virtuels

Sélectionner « Quick Configuration → VLAN Settings » (configuration rapide des paramètres des réseaux locaux virtuels) pour configurer les réseaux locaux virtuels et les ports de la ligne réseau (Figure 4.1). Il est possible d'afficher et de modifier « VLAN Settings » (paramètres des réseaux locaux virtuels), ajouter de nouveaux réseaux locaux virtuels, de modifier un réseau local virtuel et de supprimer des réseaux locaux virtuels. Après avoir configuré le ou les réseaux locaux virtuels, se rendre à « Trunk Settings » (paramètres de la ligne réseau) pour ajouter de nouveaux ports de la ligne réseau.

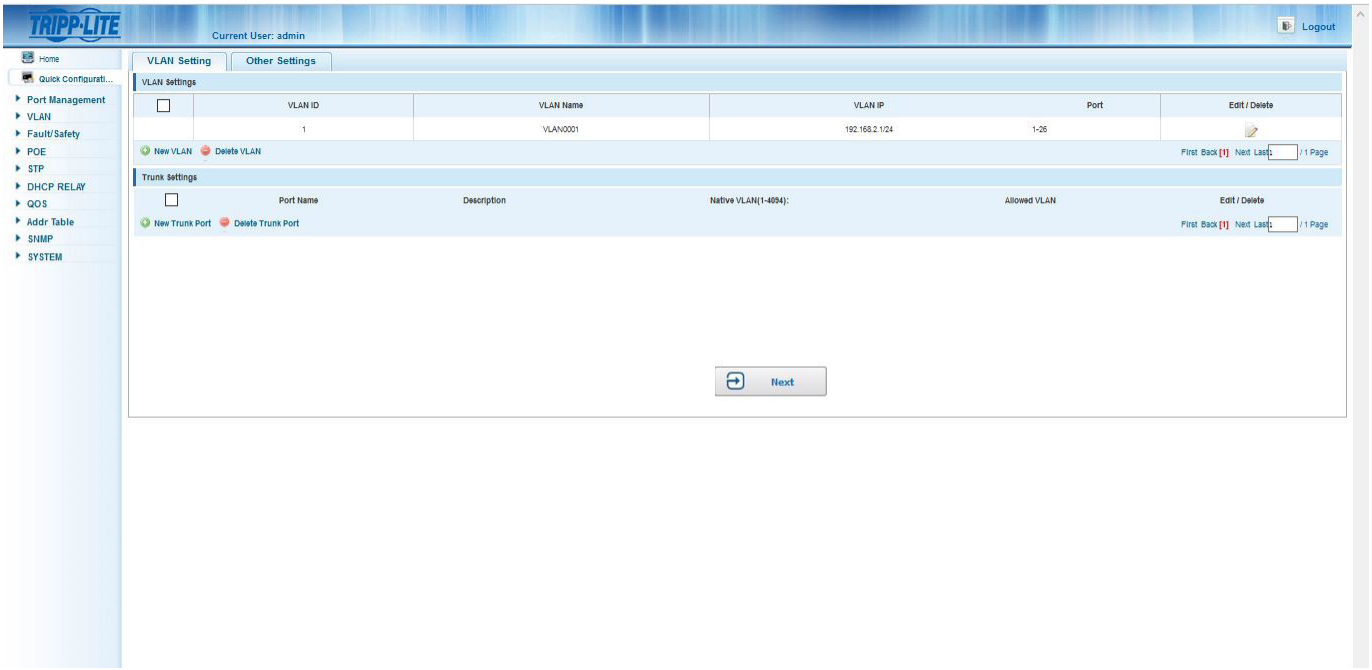


Figure 4.1 : Paramètres des réseaux locaux virtuels

4.1.1 Ajouter de nouveaux réseaux locaux virtuels

Cliquer sur l'icône « New VLAN » (nouveau réseau local virtuel), puis saisir le « VLAN ID » (nouveau numéro d'identification du réseau local virtuel), « VLAN Name » (nom du réseau local virtuel), puis ajouter les ports sélectionnés pour ce réseau local virtuel. Cliquer sur « Save » (sauvegarder) une fois l'action terminée. Répéter ces étapes pour créer des réseaux locaux virtuels supplémentaires.

4.1.2 Modifier les réseaux locaux virtuels

Cliquer sur l'icône « Edit » (modifier) pour changer le nom du réseau local virtuel et les ports sélectionnés pour ce réseau local virtuel. Cliquer sur « Sauvegarder » une fois la modification terminée. Répéter ces étapes pour modifier des réseaux locaux virtuels supplémentaires.

4.1.3 Supprimer des réseaux locaux virtuels

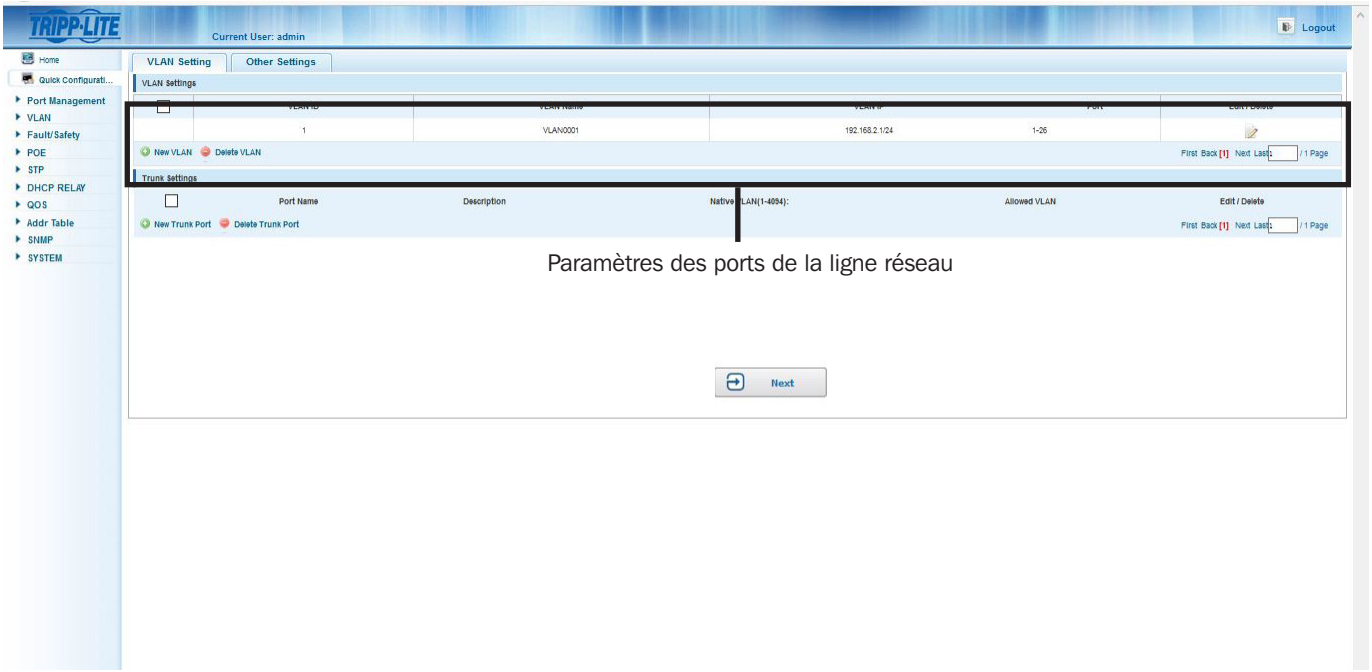
Pour supprimer un réseau local virtuel, cliquer sur l'icône rouge ✖ à côté du réseau local virtuel à supprimer ou cliquer sur la case à cocher à côté du réseau local virtuel concerné, puis cliquer sur « Delete VLAN » (supprimer le réseau local virtuel). Pour supprimer plusieurs réseaux locaux virtuels, cocher les cases à côté des réseaux locaux virtuels à supprimer. Cliquer sur « Delete VLAN » (supprimer le réseau local virtuel) pour supprimer les réseaux locaux virtuels sélectionnés.

Remarque : *Tous les ports associés aux réseaux locaux virtuels supprimés retourneront automatiquement à VLAN 1 (réseau local virtuel 1). VLAN 1 ne peut pas être supprimé.*

4. Configuration rapide

4.2 Paramètres des ports de la ligne réseau

Sélectionner « Quick Configuration → VLAN Settings » (configuration rapide des paramètres des réseaux locaux virtuels) pour gérer les paramètres des ports de la ligne réseau. Il est possible d'afficher les paramètres des ports de la ligne réseau du commutateur et d'ajouter de nouveaux ports de la ligne réseau, modifier les ports de la ligne réseau ou supprimer des ports de la ligne réseau. Après avoir configuré les « Trunk Port Settings » (paramètres des ports de la ligne réseau), cliquer sur « Next » (suivant) pour passer à la page « Other Settings » (autres paramètres).



Paramètres des ports de la ligne réseau

Figure 4.2 Paramètres des ports de la ligne réseau

4.2.1 Ajouter des ports de la ligne réseau

Cliquer sur l'icône « New Trunk Port » (nouveau port de la ligne réseau), puis sélectionner le ou les ports à configurer. Saisir le numéro d'identification du réseau local virtuel natif. Saisir ensuite les numéros d'identification pour les réseaux locaux virtuels autorisés qui auront accès aux ports de la ligne réseau. Cliquer sur « Save » (sauvegarder) une fois l'action terminée. Répéter ces étapes pour créer des ports de la ligne de réseau supplémentaires.

4.2.2 Modifier les paramètres des ports de la ligne réseau

Cliquer sur l'icône « Edit » (modifier) pour apporter des changements aux ports de la ligne réseau sélectionnés, au réseau local virtuel natif et aux réseaux locaux virtuels autorisés. Cliquer sur « Save » (sauvegarder) une fois la modification terminée. Répéter ces étapes pour modifier des ports de la ligne de réseau supplémentaires.

4.2.3 Supprimer des ports de la ligne réseau

Pour supprimer des ports de la ligne réseau, cliquer sur l'icône rouge à côté du port de la ligne réseau à supprimer ou cliquer sur la case à cocher à côté du réseau local virtuel concerné, puis cliquer sur « Delete Trunk Port » (supprimer le port de la ligne réseau). Pour supprimer plusieurs ports de la ligne réseau, cocher les cases à côté des ports de la ligne réseau à supprimer. Cliquer sur « Delete Trunk Ports » (supprimer les ports de la ligne réseau) pour supprimer de la configuration de commutateur les ports de la ligne réseau sélectionnés.

4. Configuration rapide

4.3 Autres paramètres

Sélectionner « Quick Configuration → Other Settings » (configuration rapide d'autres paramètres) pour afficher les paramètres du système (Figure 4.3). Depuis cette page, il est possible de modifier le réseau local virtuel de gestion, l'adresse IP de gestion, le masque de sous-réseau, la passerelle par défaut, le serveur DNS, le nom de l'appareil et le mot de passe de l'interface de gestion du commutateur. Après avoir modifié la configuration, cliquer sur « Save » (sauvegarder). Cliquer sur « Finish » (terminé) pour retourner à la page d'accueil ou cliquer sur « Previous » (précédent) pour retourner aux paramètres précédents pour modifier davantage la configuration.

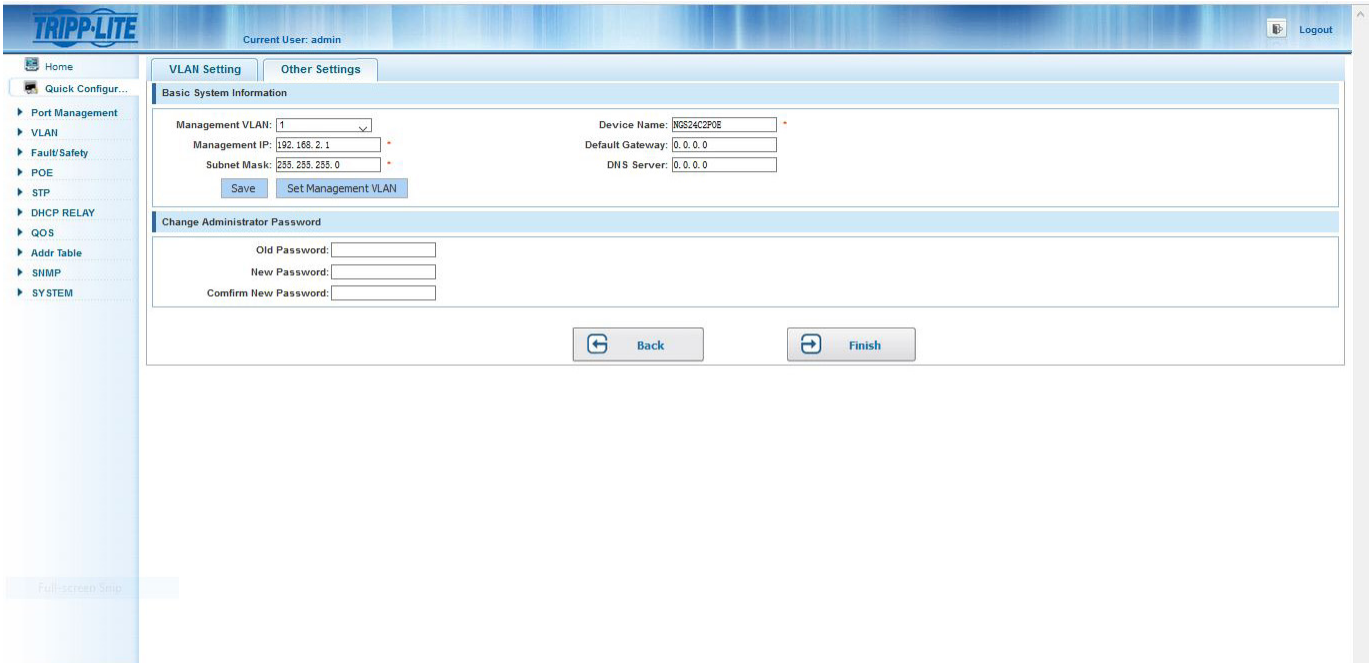


Figure 4.3 Autres paramètres

La page Other Settings (autres paramètres) affiche les paramètres de base du système.

Management VLAN : Le numéro d'identification du réseau local virtuel de gestion du commutateur par défaut est 1.

Management IP : L'adresse IP du réseau local virtuel de gestion du commutateur.

Subnet Mask : Le masque de sous-réseau du réseau local virtuel de gestion du commutateur.

Device Name : Le nom d'hôte du commutateur.

Default Gateway : La passerelle par défaut du réseau local virtuel du commutateur.

DNS Server : L'adresse IP du serveur DNS.

Remarque : *Le numéro d'identification du réseau local virtuel de gestion du commutateur est 1 par défaut et ne peut pas être supprimé.*

4.3.1 Modifier les paramètres de l'adresse IP de gestion du commutateur

Pour configurer l'adresse IP de gestion du commutateur, suivre les étapes suivantes :

1. Saisir l'adresse IP dans le champ « Management IP » (IP de gestion) (p. ex. 192.168.100.179). L'IP de gestion est obligatoire.
2. Saisir le masque de sous-réseau dans le champ « Subnet Mask » (masque de sous-réseau) (p. ex. 255.255.255.0). Le masque de sous-réseau de gestion est obligatoire.
3. Saisir le nom de l'appareil. Le nom de l'appareil est obligatoire.
4. Saisir l'adresse de la passerelle dans le champ « Default Gateway » (Passerelle par défaut) (p. ex. 192.168.100.1).
5. Saisir l'adresse IP du serveur DNS (p. ex. 192.168.10.12).
6. Cliquer sur « Save » (sauvegarder) pour terminer la configuration.
7. Cliquer sur « Set Management VLAN » (configurer le réseau local virtuel de gestion) pour passer à un réseau local virtuel autre que le numéro d'identification du réseau local virtuel par défaut de 1.

4.3.2 Modifier le mot de passe d'administrateur de l'interface de gestion Web

Pour modifier le mot de passe d'administrateur de l'interface de gestion Web, saisir le mot de passe par défaut ou l'ancien mot de passe, puis saisir le nouveau mot de passe (sensible à la casse). Saisir de nouveau le nouveau mot de passe (sensible à la casse) pour le confirmer. Cliquer sur « Finish » (terminer) pour valider les changements ou sur « Back » (retour) pour les rejeter.

5. Gestion des ports

5.1 Paramètres de base

5.1.1 Afficher la configuration des ports

Sélectionner « Port Management → Basic Settings » (paramètres de base de la gestion des ports) pour afficher et modifier les paramètres des ports (Figure 5.1).

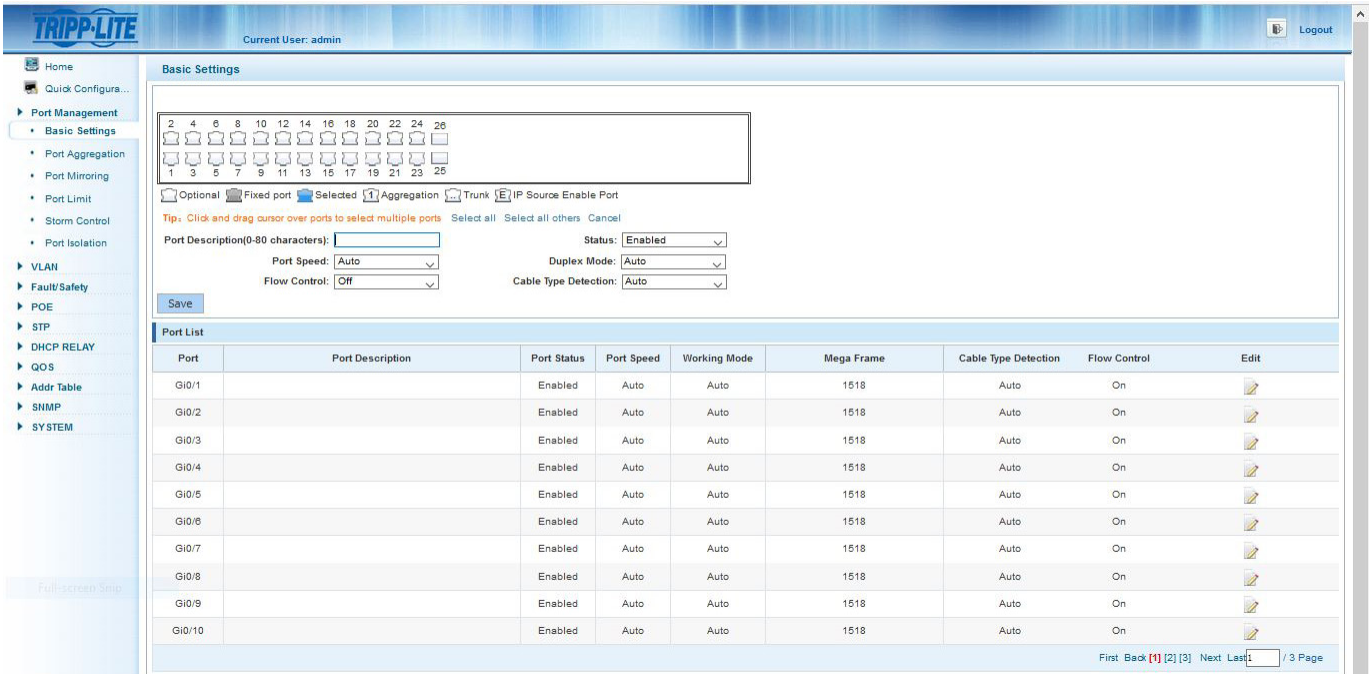


Figure 5.1 : Page des paramètres de base

Le tableau de la liste des ports affiche des informations sur la configuration des ports du commutateur dans les colonnes suivantes :

- **Port :** affiche le nombre de ports du commutateur.
- **Description :** affiche le nom fourni par l'utilisateur ou la description donnée au port.
- **Status (état) :** affiche l'état du port, soit « Enabled » (activé) ou « Disabled » (désactivé).
- **Port Speed (vitesse des ports) :** affiche soit auto-negotiation (auto-négociation), 10, 100 ou 1 000 Mbps.
- **Working Mode (mode de fonctionnement) :** affiche port duplex configuration (configuration en duplex des ports), auto-negotiation (auto-négociation), full duplex (duplex intégral) ou half duplex (semi-duplex).
- **Mega Frame (mégatrame) :** affiche la longueur des trames étendues. La longueur par défaut du mégatrame est 1 518.
- **Cable Type Detection (détection du type de câble) :** affiche crossover configuration (configuration de croisement), auto-negotiation (autonégociation), MDI ou MDIX.
- **Flow Control (contrôle de flux) :** indiquce si le contrôle de flux est à « On » (marche) ou « Off » (arrêt).

Remarque : *Le taux du SFP en laiton/fibre ne peut être que 1 000 Mbps et son mode de fonctionnement ne peut être qu'auto/duplex intégral.*

5. Gestion des ports

5.1.2 Configurer un ou plusieurs ports

Sélectionner le ou les ports à configurer à partir du panneau, puis cliquer sur l'icône dans la colonne Edit (modifier) pour modifier les paramètres de chaque port sélectionné.

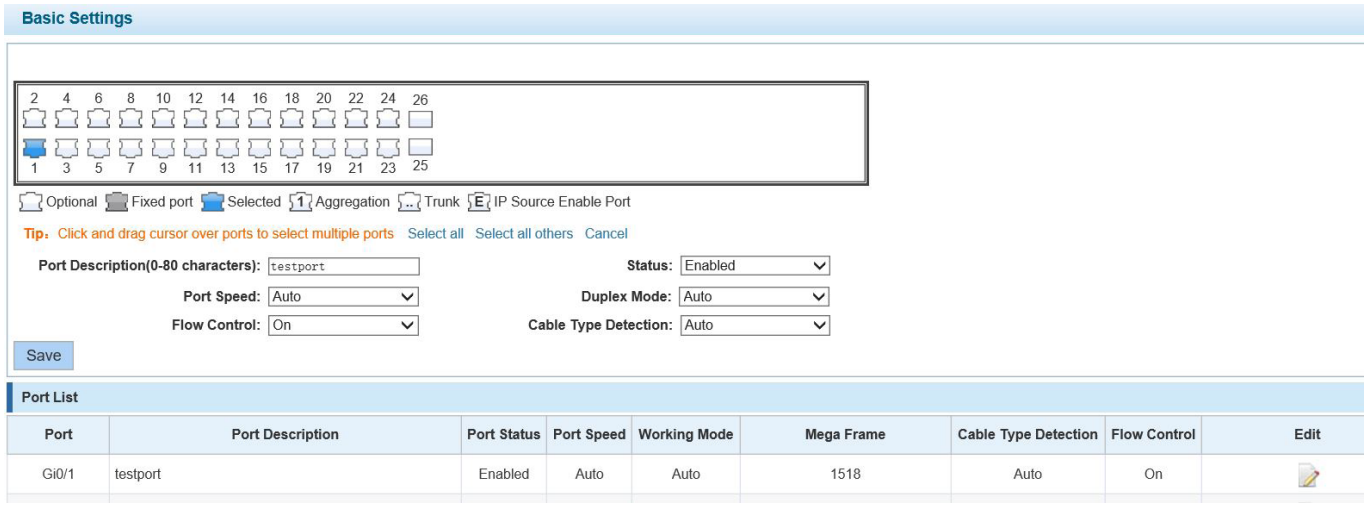


Figure 5.2: Configuration de ports individuels

Remarque : *Sur l'écran de configuration de ports individuels, les paramètres suivants peuvent être modifiés : Description, Status (état), Port Speed (vitesse des ports), Duplex Mode (mode duplex), Flow Control (contre de flux) et Cable Type (type de câble).*

5.2 Agrégation de ports

5.2.1 Afficher la configuration de l'agrégation de ports

Sélectionner « Port Management → Port Aggregation » (gestion des ports, agrégation des ports) pour afficher la configuration de l'agrégation de ports du commutateur (Figure 5.3). L'agrégation de ports (ou l'agrégation de liens) permet la combinaison de plusieurs liens Ethernet en un seul lien logique. Les appareils de réseau traitent l'agrégation comme s'il s'agissait d'un lien simple, ce qui augmente la tolérance aux pannes et fournit une répartition des charges.

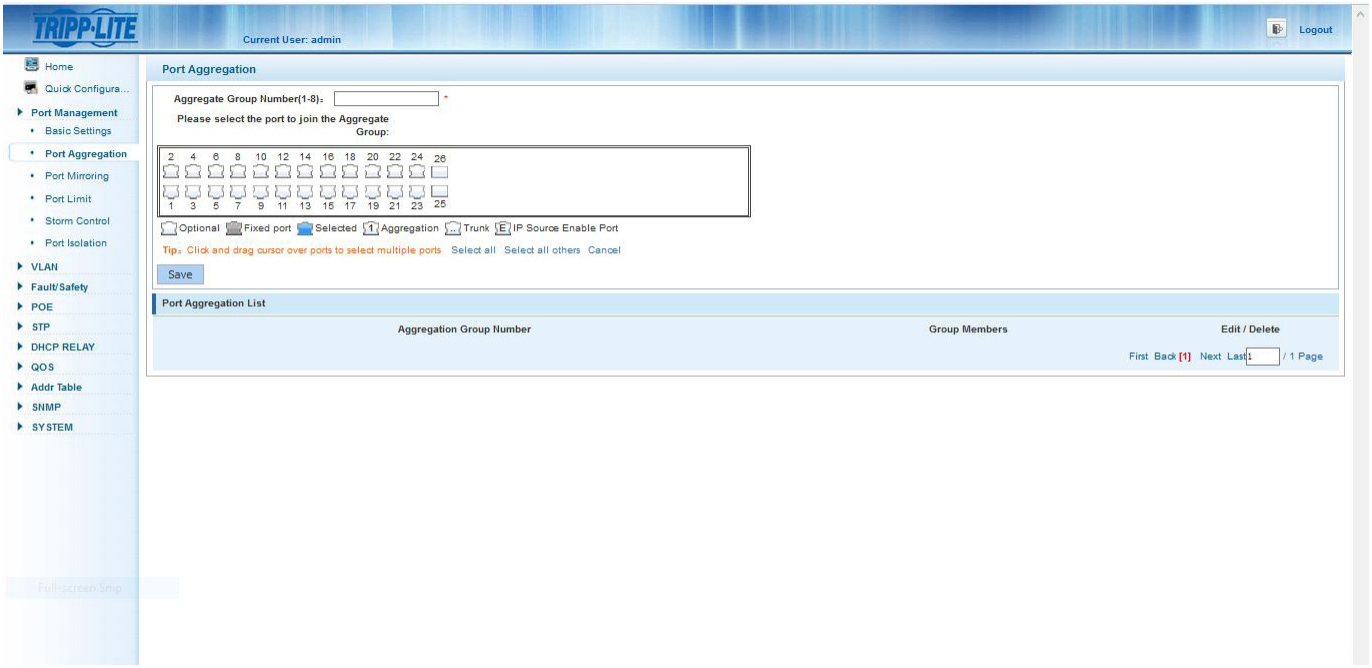


Figure 5.3 : Agrégation de ports

5. Gestion des ports

Le tableau Agrégation de ports affichera la configuration actuelle du commutateur.

- **Aggregation Group Number (numéro du groupe d'agrégation) :** affiche le numéro attribué au groupe d'agrégation.
- **Aggregation Group Members (Membres du groupe d'agrégation) :** affiche les numéros des ports qui se composent d'un groupe d'agrégation de liens.

Remarques :

- *Les groupes d'agrégation doivent comporter au moins deux ports; huit ports maximum peuvent être agrégés dans un groupe.*
- *Chaque port dans un groupe d'agrégation de liens doit utiliser les mêmes protocoles et les mêmes vitesses de lien.*

5.2.2 Créer un groupe d'agrégation de ports

Pour créer un groupe d'agrégation de ports, saisir un numéro d'identification de port, puis sélectionner les ports à ajouter au groupe d'agrégation. Cliquer sur « Save » (sauvegarder) pour terminer la configuration. Lorsqu'un port fait partie d'un groupe d'agrégation, il sera affiché comme illustré dans la Figure 5.4.

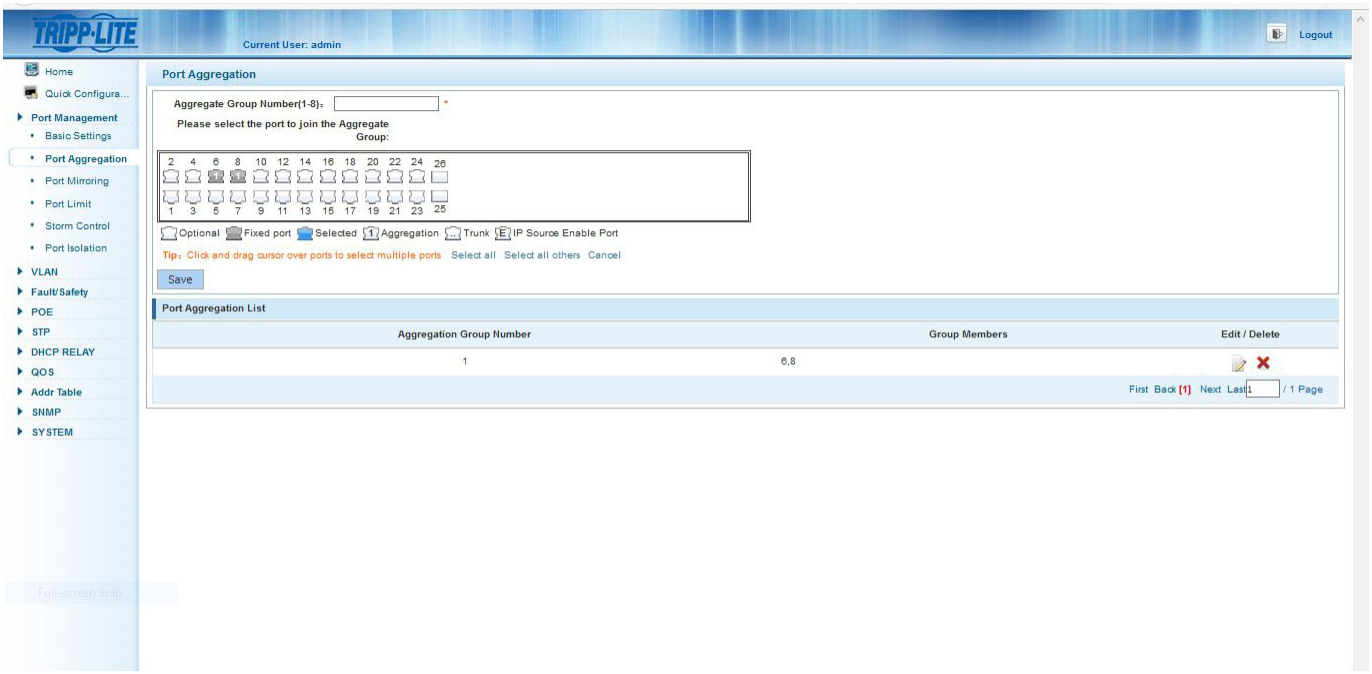


Figure 5.4 : Créer un groupe d'agrégation de ports

5.2.3 Modifier un groupe d'agrégation de ports

Cliquer sur l'icône « Edit » (modifier) pour ajouter des membres au groupe d'agrégation. Le numéro du groupe d'agrégation ne peut pas être modifié une fois qu'il a été configuré. Si un nouveau groupe d'agrégation est créé en utilisant un numéro de groupe existant, le message « The Aggregate port number already exists » (le numéro de port d'agrégation existe déjà) s'affichera. Choisir un autre numéro de groupe disponible à attribuer au port.

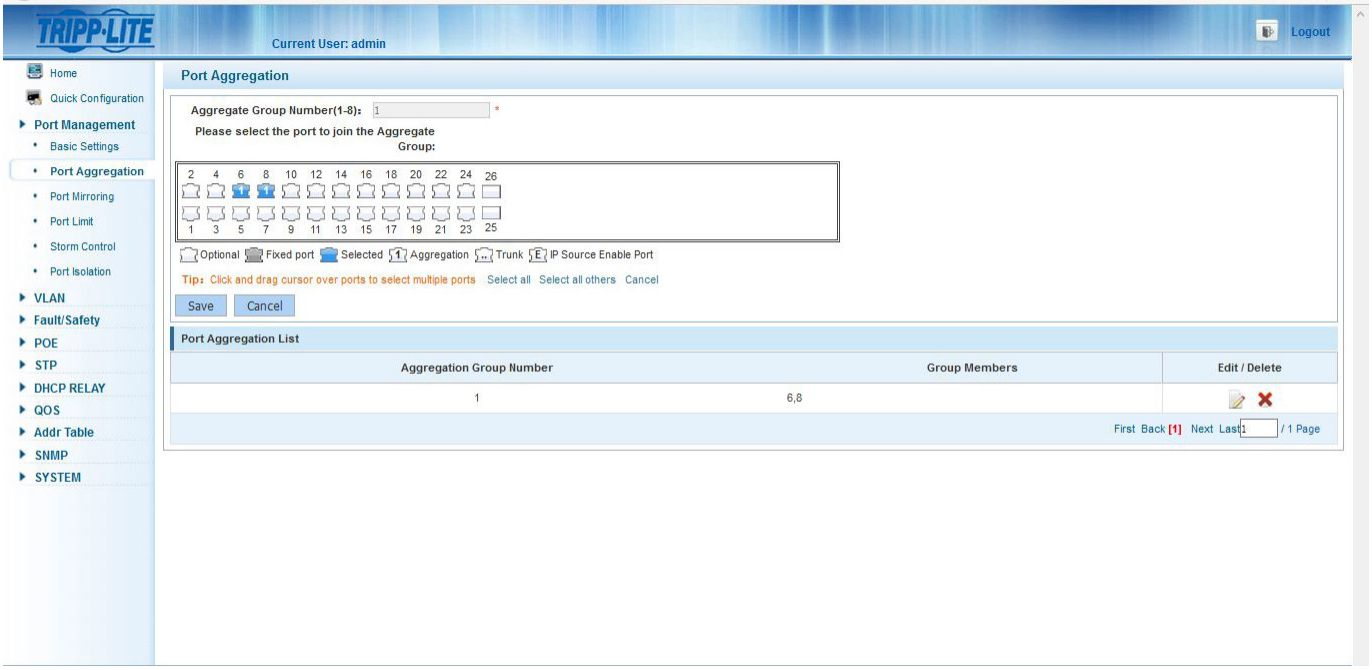


Figure 5.5 : Modifier ou supprimer un groupe d'agrégation de ports

5.2.4 Supprimer un groupe d'agrégation de ports

Cliquer sur l'icône rouge ✖ à côté du groupe d'agrégation pour supprimer ce groupe de ports.

5. Gestion des ports

5.3 Miroir de port

5.3.1 Afficher la configuration du miroir de port

Sélectionner « Port Management → Port Mirroring » (gestion des ports, miroir de port) pour afficher la configuration du miroir de port (Figure 5.6). Le miroir de port sélecte le trafic du réseau pour l'analyse par un analyseur de réseau. Cela peut être fait pour des ports de commutateur spécifiques. Plusieurs ports du commutateur peuvent être configurés comme ports éphémères et un port du commutateur est configuré comme un port réservé. Les paquets copiés vers un port réservé auront le même format que le paquet d'origine de la source. Cela signifie que si le miroir copie un paquet reçu, le paquet copié sera marqué VLAN (réseau local virtuel) ou non marqué comme il a été reçu sur le port éphémère.

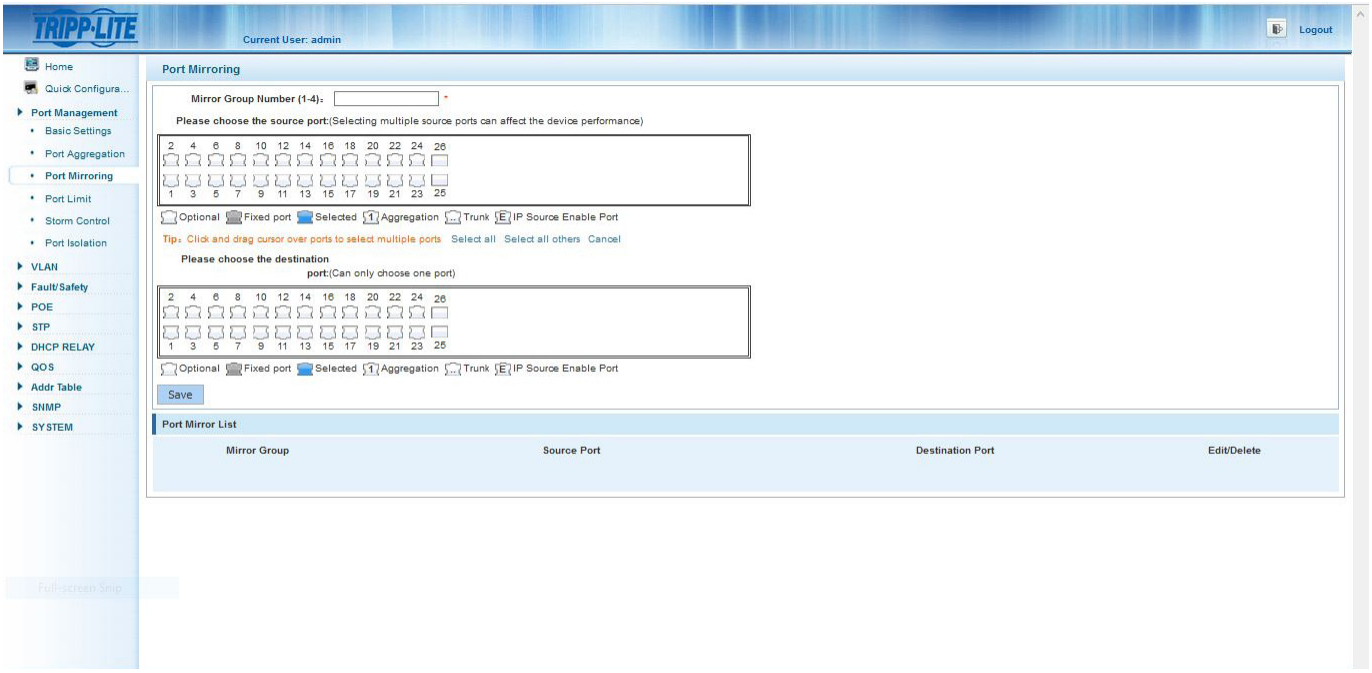


Figure 5.6 : Configuration du miroir de port

La liste de ports d'écriture miroir affiche la configuration d'écriture miroir du commutateur.

- **Mirroring Group :** Le numéro d'identification du miroir; jusqu'à quatre groupes d'écriture miroir peuvent être créés.
- **Source Port(s) :** Le port/les ports d'où proviennent les donnes d'écriture miroir.
- **Destination Port :** Le port qui reçoit les données d'écriture miroir.

Remarques :

- *Les ports dans les ports d'agrégation ne peuvent pas être désignés à la fois comme port éphémère et comme port réservé.*
- *Un seul port réservé peut être sélectionné par groupe d'écriture miroir.*

5. Gestion des ports

5.3.2 Créer un groupe de miroir de port

Pour créer un groupe de miroir de port, sélectionner le ou les ports éphémères et le port réservé, puis sélectionner le groupe d'écriture miroir (Figure 5.7). Cliquer sur « Save » (sauvegarder).

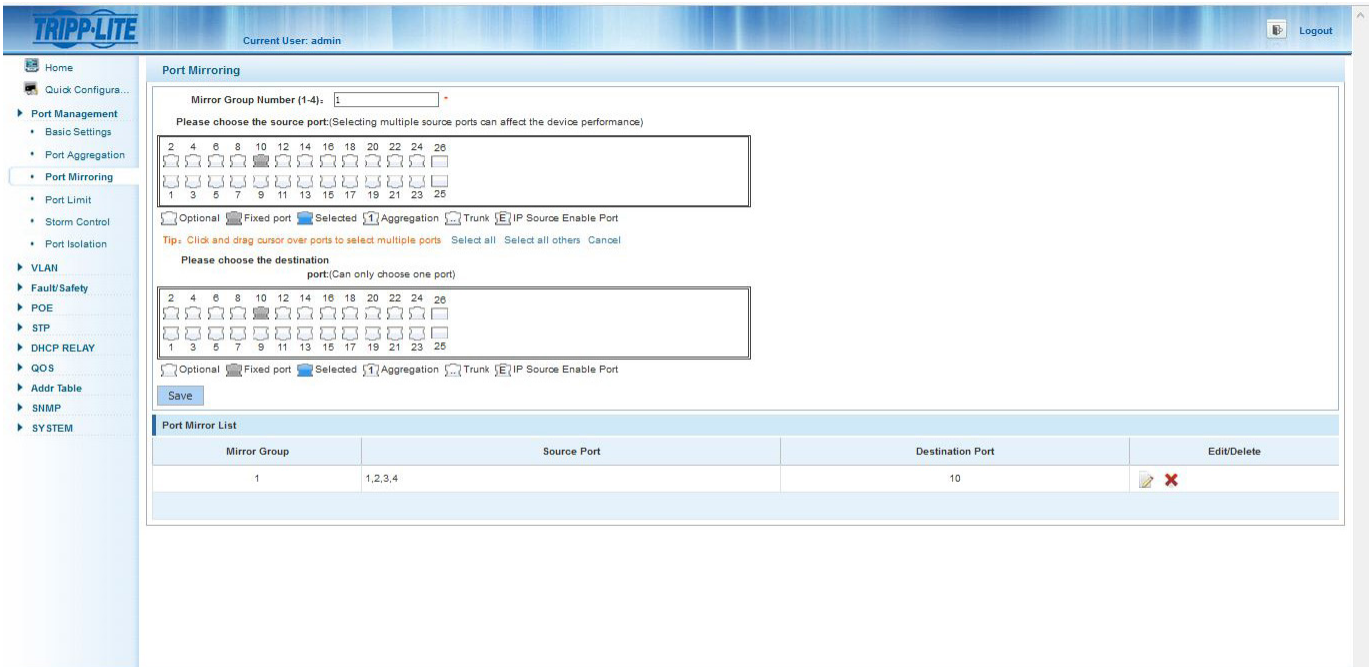


Figure 5.7 Créer un groupe de miroir de port

5.3.3 Modifier un groupe de miroir de port

Cliquer sur l'icône à côté du groupe de miroir de port (Figure 5.8) pour modifier sa source et ses ports réservés.

Remarque : *Le numéro d'identification du groupe d'écriture miroir ne peut pas être modifié une fois qu'il a été attribué.*

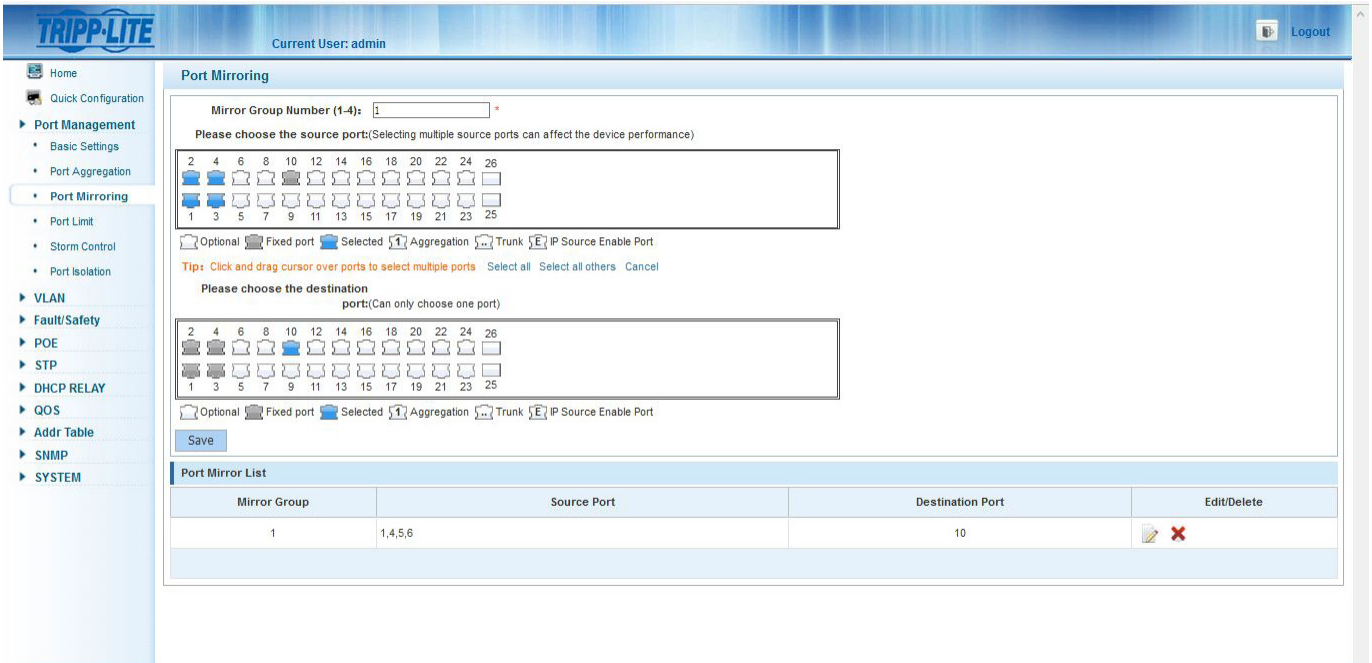


Figure 5.8 : Modifier ou supprimer un groupe de miroir de port

5. Gestion des ports

5.3.4 Supprimer un groupe de miroir de port

Cliquer sur l'icône ✖ à côté du groupe de ports d'écriture miroir pour supprimer le groupe.

5.4 Paramètres de la limite de vitesse des ports

5.4.1 Afficher les paramètres de la limite de vitesse des ports

Sélectionner « Port Management → Port Limit » (gestion des ports, limite des ports) pour afficher les paramètres de la limite de vitesse des ports du commutateur (Figure 5.9).

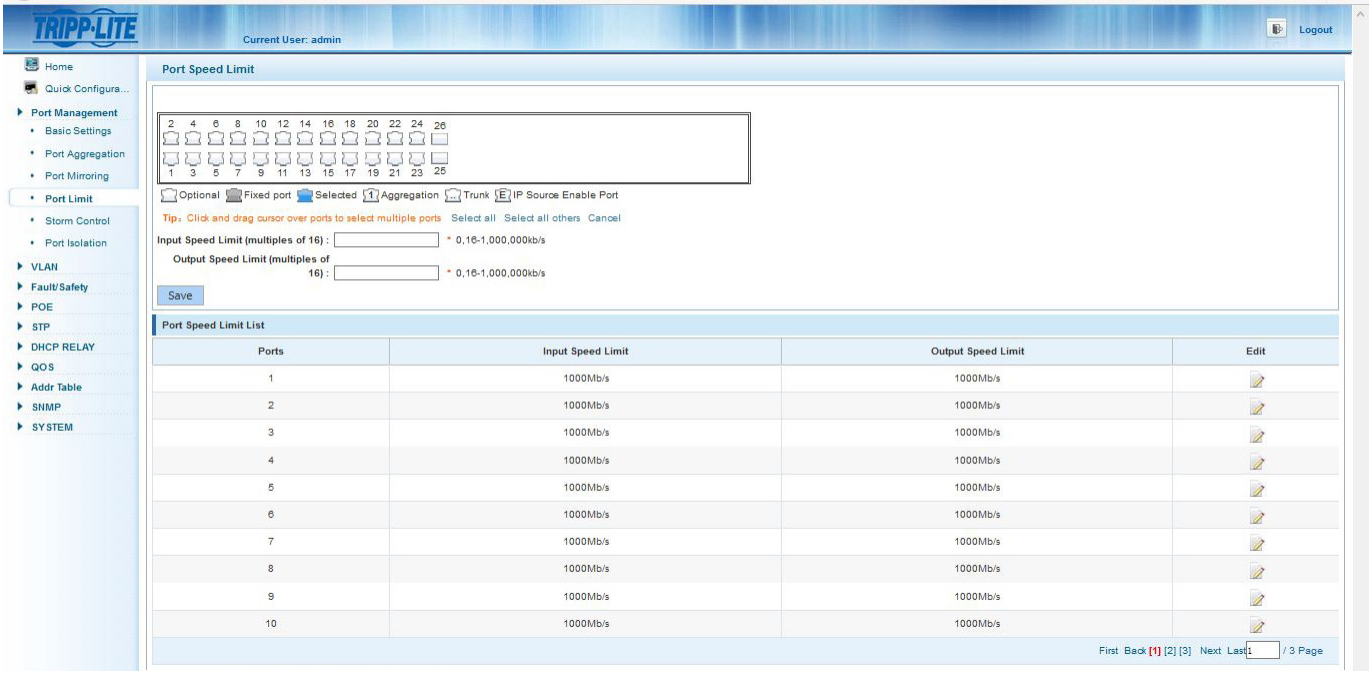


Figure 5.9 : Configuration de la limite de vitesse des ports

La limite de vitesse indique les configurations de la limite de vitesse des ports du commutateur.

- **Ports :** affiche le numéro des ports.
- **Input Speed Limit (limite de la vitesse d'entrée) :** limite de vitesse en amont pour le port.
- **Output Speed Limit (limite de la vitesse de sortie) :** limite de vitesse en aval pour le port.

Remarque : *Plusieurs ports peuvent être sélectionnés sur le panneau pour modifier les paramètres de la limite de vitesse des ports.*

5. Gestion des ports

5.5 Paramètres du Storm Control

5.5.1 Configurer les paramètres du Storm Control d'un port

Storm Control assure la performance du réseau depuis un flux de paquets du trafic d'une multidiffusion, d'un envoi individuel ou d'une diffusion générale sur le réseau local virtuel. Pour configurer, sélectionner « Port Management → Storm Control » (gestion des ports, Storm Control) pour modifier les paramètres du Storm Control d'un ou plusieurs ports sélectionnés (Figure 5.10). Par défaut, cette fonction est désactivée.

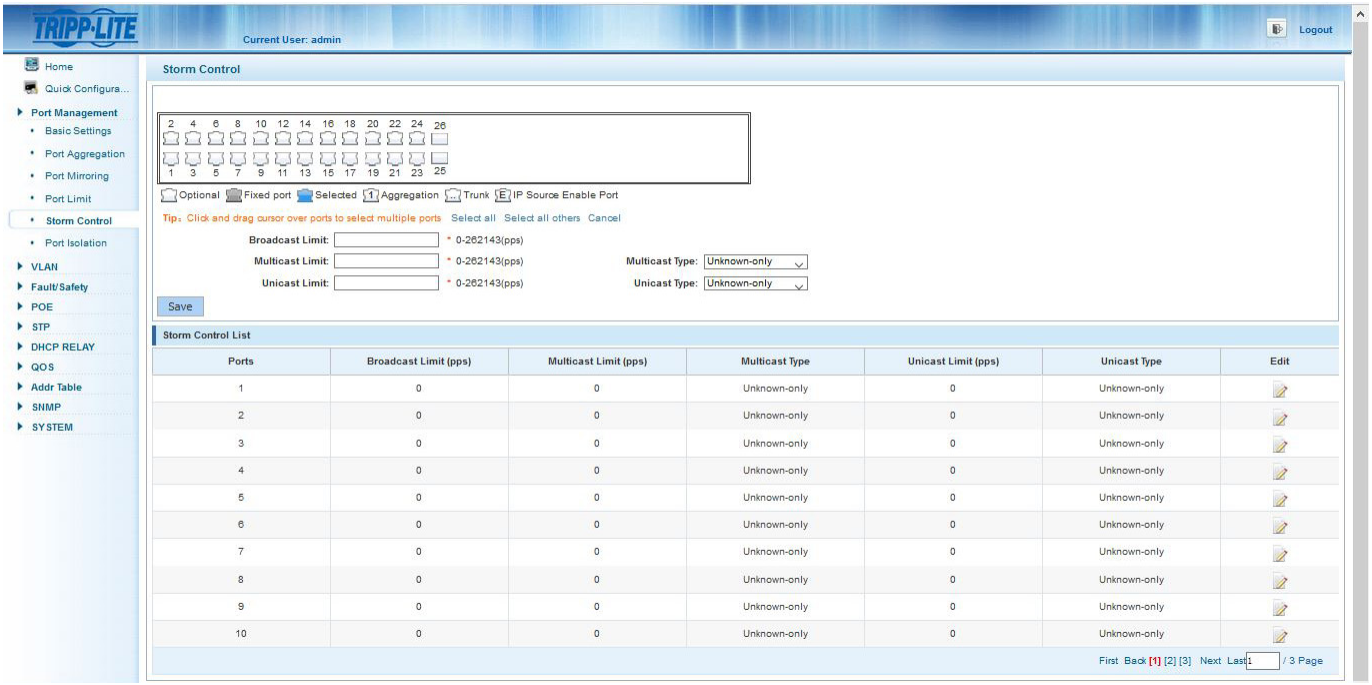


Figure 5.10 : Tableau de configuration de Storm Control

La Figure 5.10 affiche la configuration du Storm Control du commutateur par port.

- **Ports :** affiche le nombre de ports du commutateur.
- **Broadcast (diffusion générale) :** affiche si le contrôle du paquet de diffusion générale est activé ou désactivé. « 0 » signifie désactivé.
- **Multicast (multidiffusion) :** affiche si le contrôle du paquet de multidiffusion est activé ou désactivé. « 0 » signifie désactivé.
- **Unicast (envoi individuel) :** affiche si le contrôle du paquet d'envoi individuel est activé ou désactivé. « 0 » signifie désactivé.
- **Storm Control Value (valeur de Storm Control) :** fixe à quel taux Storm Control sera activé (entre 0 et 262 143 pps).
- **Storm Control Type (type de Storm Control) :** affiche les types de paramètres de Storm Control qui peuvent être configurés pour « Unknown-only » (inconnu seulement) ou « Both » (les deux). Un dispositif peut mettre en œuvre la suppression du Storm Lorsqu'un nombre excessif de paquets de diffusion générale, de multidiffusion ou d'envoi individuel inconnu est reçu, le commutateur empêche temporairement le réacheminement de types pertinents de paquets jusqu'à ce que les flux de données soient revenus à la normale (les paquets sont ensuite réacheminés normalement).

5.5.2 Modifier les paramètres du Storm Control

Sélectionner le ou les ports à configurer (Figure 5.11). Cliquer sur le menu déroulant « Storm Control Type » (type de Storm Control) pour sélectionner le type de Storm Control à configurer pour le port. Saisir une valeur entre 0 et 262 143 dans les champs « Storm Control Value » (valeur de Storm Control) pour les paquets de diffusion générale, de multidiffusion et d'envoi individuel par entrée par seconde. Si nécessaire, configurer le type de trafic de multidiffusion et de trafic d'envoi individuel à « Unknown-only » (inconnu seulement) ou « Both » (les deux), puis cliquer sur « Save » (sauvegarder) pour terminer la configuration pour le ou les ports.

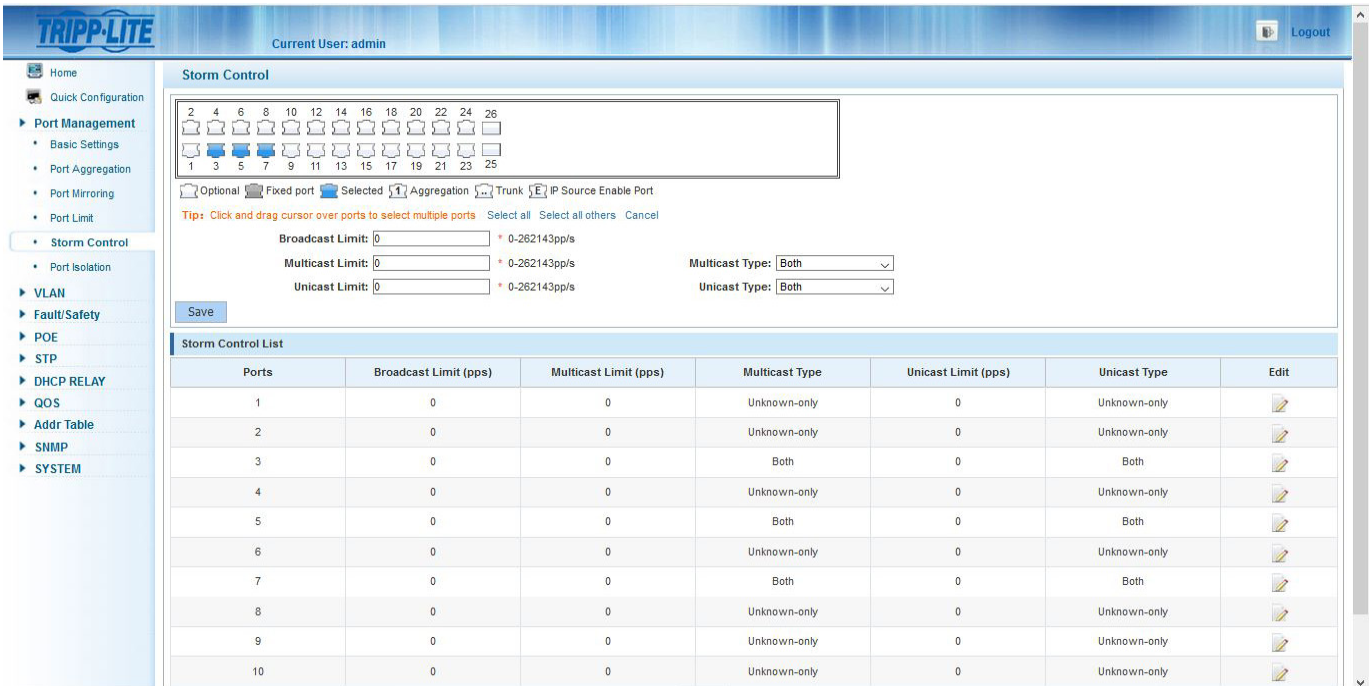


Figure 5.11 Modifier les paramètres du Storm Control

5.6 Paramètres de l'isolation des ports

5.6.1 Afficher la configuration de l'isolation des ports

Sélectionner « Port Management Port Isolation » (gestion des ports, isolation des ports) pour afficher la configuration actuelle de l'isolation des ports du commutateur (Figure 5.12). L'isolation des ports empêche les PC connectés à des ports différents de communiquer entre eux (sans avoir à configurer un réseau local virtuel).

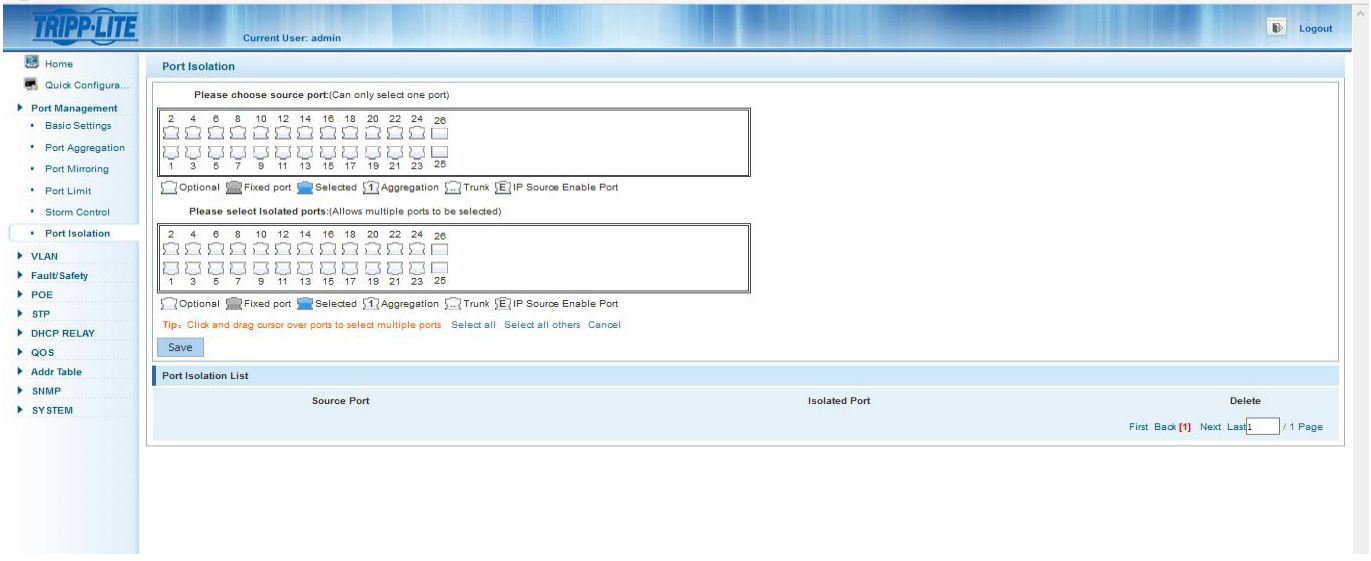


Figure 5.12 Configuration de l'isolation des ports

5.6.2 Créer un groupe d'isolation des ports

Cliquer sur l'icône du port éphémère dans le tableau de la liste des ports, puis sélectionner le port à isoler. Le port deviendra bleu sur le panneau. Sélectionner ensuite le ou les ports à isoler du port sélectionné. Les ports isolés seront bleus dans le panneau. Finalement, cliquer sur « Save » (sauvegarder). Les numéros des ports isolés seront affichés dans le tableau (Figure 5.13).

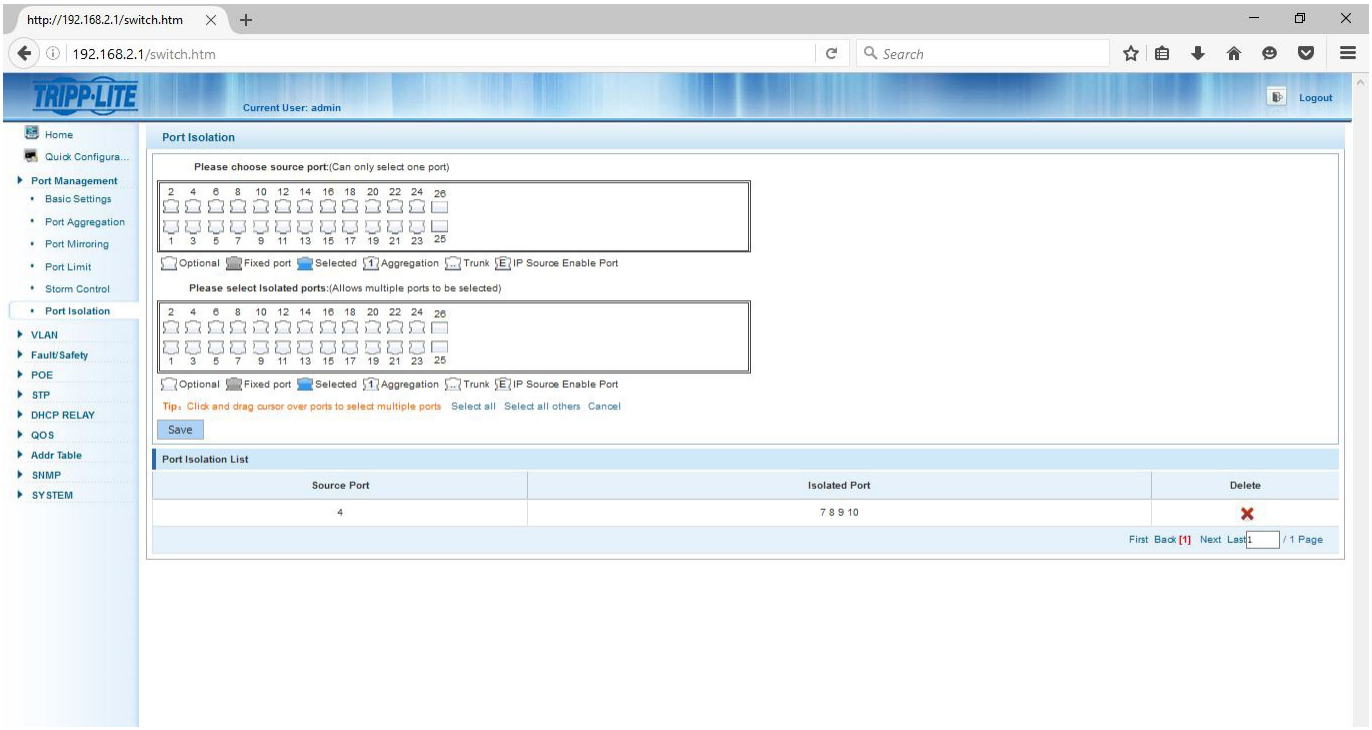


Figure 5.13 : Créer un groupe d'isolation de ports

5.6.3 Supprimer un groupe d'isolation des ports

Cliquer sur l'icône ✖ pour supprimer un groupe d'isolation de ports de la liste d'isolation de ports. Confirmer la suppression et le groupe sera supprimé de la liste (Figure 5.14).

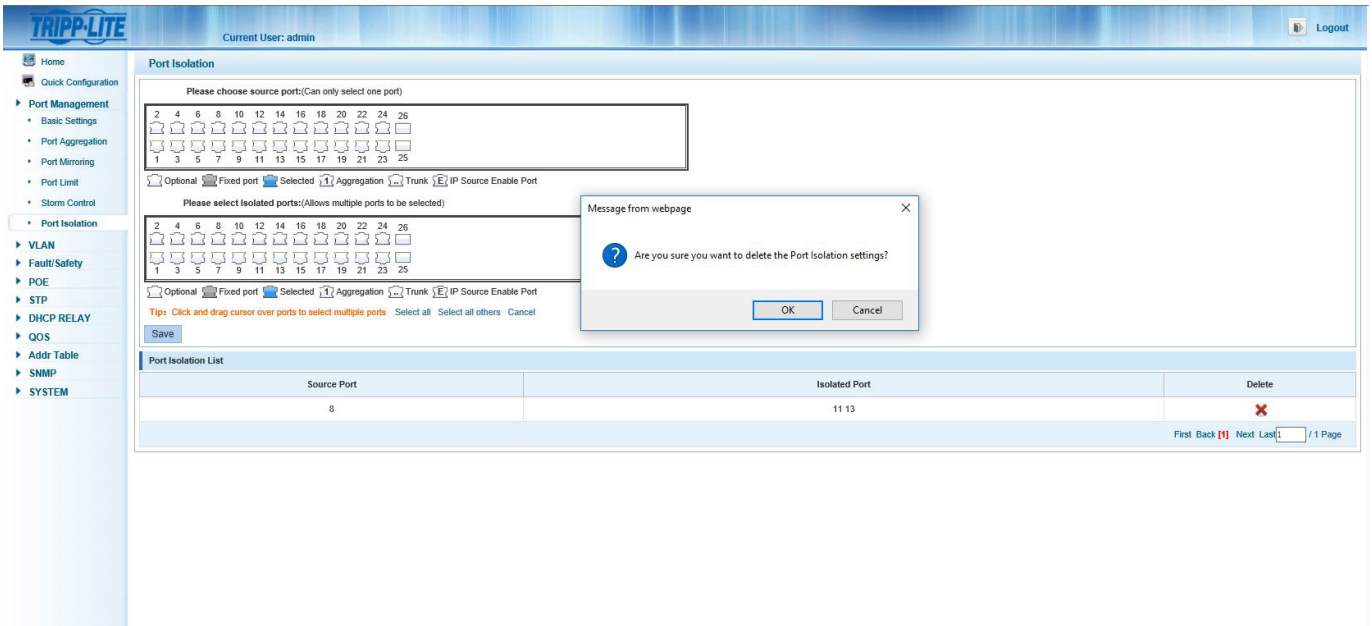


Figure 5.14 : Supprimer un groupe d'isolation de ports

6. Gestion du réseau local virtuel

6.1 Gestion du réseau local virtuel

6.1.1 Afficher la configuration du réseau local virtuel

Sélectionner « VLAN → VLAN Management » (réseau local virtuel, gestion du réseau local virtuel) pour afficher les paramètres de la configuration du réseau local virtuel du commutateur (Figure 6.1). Un réseau local virtuel est un groupe de stations de travail, de serveurs et autres ressources du réseau qui se comportent comme s'ils étaient connectés à un seul segment de réseau. Les réseaux locaux virtuels permettent de faciliter la segmentation du réseau. Les utilisateurs qui communiquent fréquemment entre eux peuvent être groupés en réseaux locaux virtuels communs, peu importe l'emplacement physique. Le trafic de chaque groupe se trouve en grande partie dans le réseau local virtuel, ce qui réduit le trafic superflu et améliore l'efficacité au sein du réseau. Un réseau local virtuel facilite également la gestion du réseau. Le changement du nombre de nœuds dans un réseau et de l'emplacement des nœuds peut être traité au moyen de l'interface de gestion plutôt que dans l'armoire de répartition.

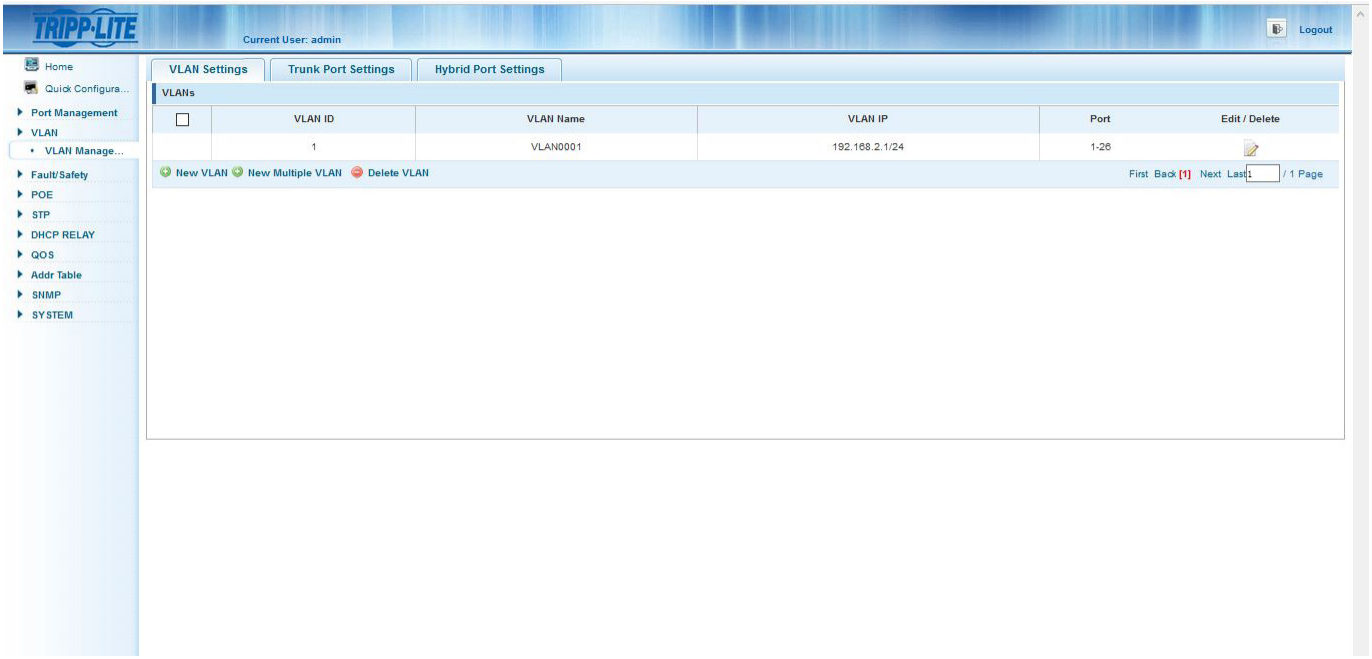


Figure 6.1 : Informations sur la gestion du réseau local virtuel

La liste des réseaux locaux virtuels indique la configuration des réseaux locaux virtuels du commutateur :

- **VLAN ID (numéro d'identification du réseau local virtuel) :** affiche le numéro d'identification du réseau local virtuel.
- **VLAN Name :** affiche le nom du réseau local virtuel; le nom par défaut pour VLAN 1 est DEFAULT.
- **VLAN IP :** affiche l'adresse IP de gestion du commutateur.
- **Port :** affiche les ports qui appartiennent à chaque réseau local virtuel.

Remarque : *Par défaut, tous les ports appartiennent à VLAN 1. Le réseau local virtuel de gestion ne peut pas être supprimé.*

6. Gestion du réseau local virtuel

6.1.2 Ajouter un réseau local virtuel

Sélectionner « New VLAN » (nouveau réseau local virtuel), puis saisir le numéro d'identification du réseau local virtuel (entre 2 et 4 094) (Figure 6.2). Saisir un nom de réseau local virtuel (limite : 31 caractères) Si aucun nom n'est saisi, le commutateur prend un nom générique par défaut « VLAN0002 ». Sélectionner ensuite les ports à ajouter au réseau local virtuel, puis cliquer sur « Save » (sauvegarder).

Remarque : *Le système ne permettra pas la création de doublons de numéros d'identification de réseau local virtuel.*

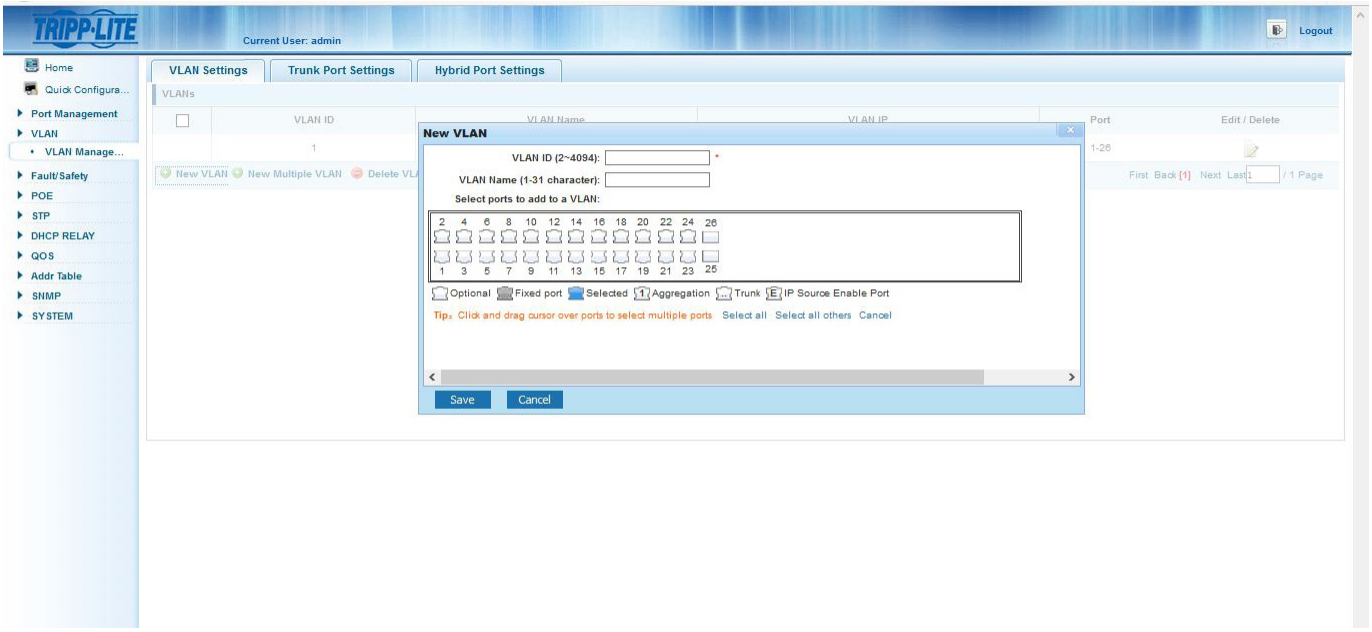


Figure 6.2 : Ajouter un réseau local virtuel

6.1.3 Ajouter plusieurs réseaux locaux virtuels

Pour ajouter rapidement plusieurs réseaux locaux virtuels à la liste, sélectionner « New Multiple VLAN » (plusieurs nouveaux réseaux locaux virtuels), saisir les numéros d'identification des réseaux locaux virtuels à créer, puis cliquer sur « Save » (sauvegarder) (Figure 6.3). Tous les réseaux locaux virtuels seront créés et permettront la modification des paramètres de chaque réseau local virtuel.

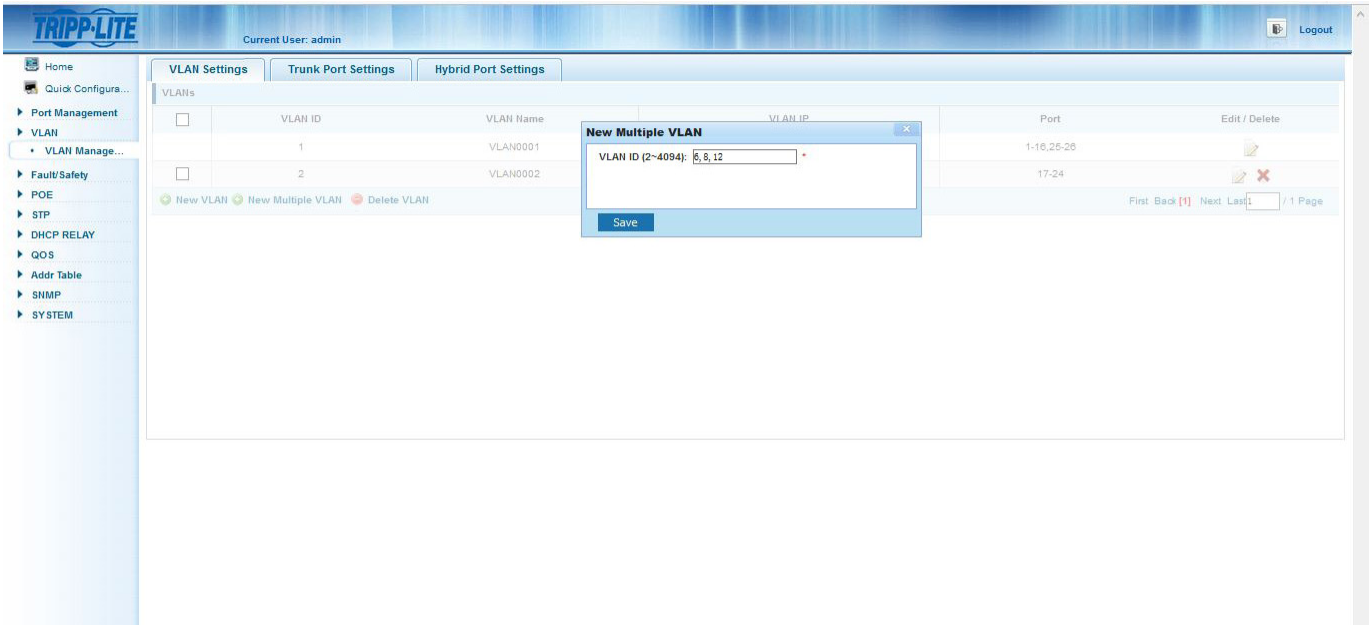


Figure 6.3 Ajouter plusieurs réseaux locaux virtuels

6. Gestion du réseau local virtuel

6.1.4 Modifier un réseau local virtuel

Cliquer sur l'icône « Edit » (modifier) du numéro d'identification du réseau local virtuel qui nécessite des modifications. Dans la fenêtre Edit VLAN (modifier le réseau local virtuel) (Figure 6.4), il est possible de changer le nom du réseau local virtuel et les ports associés. Une fois les modifications apportées, cliquer sur « Save » pour sauvegarder les modifications. Cliquer sur « Cancel » (annuler) pour rejeter les modifications.

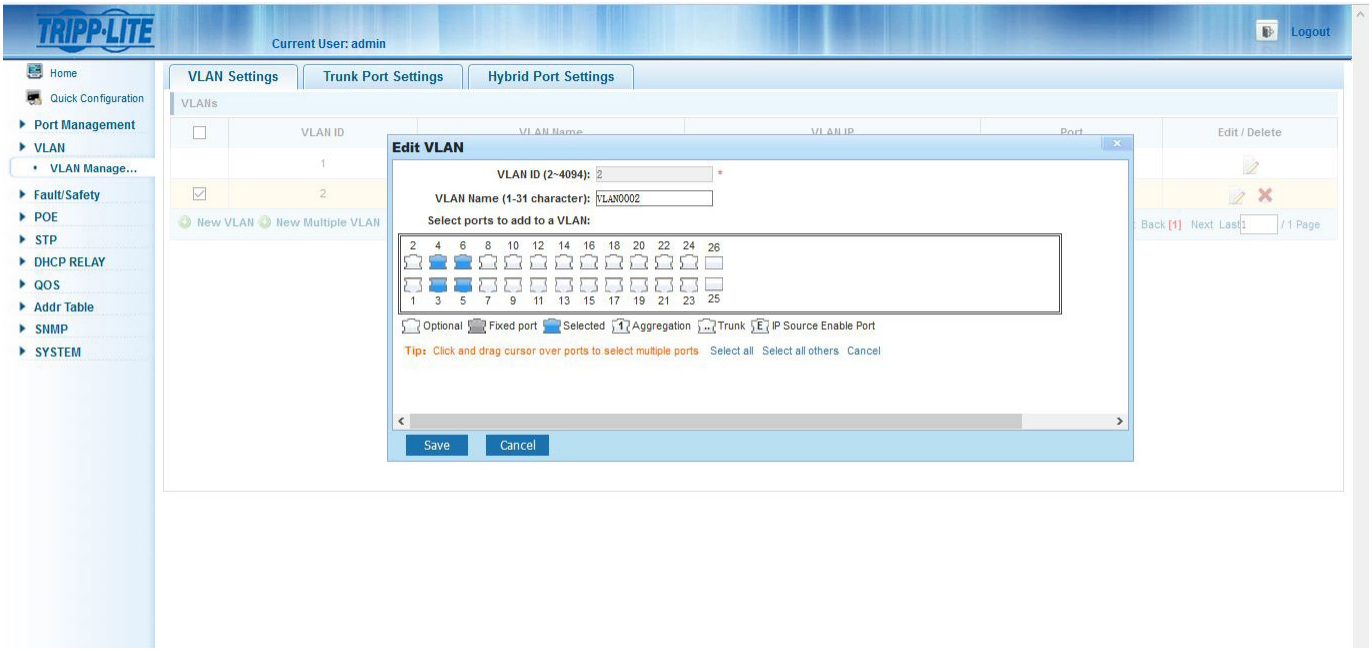


Figure 6.4 : Modifier un réseau local virtuel

6.1.5 Supprimer un ou plusieurs réseaux locaux virtuels

Supprimer un seul réseau local virtuel

Sélectionner le réseau local virtuel à supprimer dans la liste, puis cliquer sur l'icône pour supprimer le réseau local virtuel sélectionné (Figure 6.5).

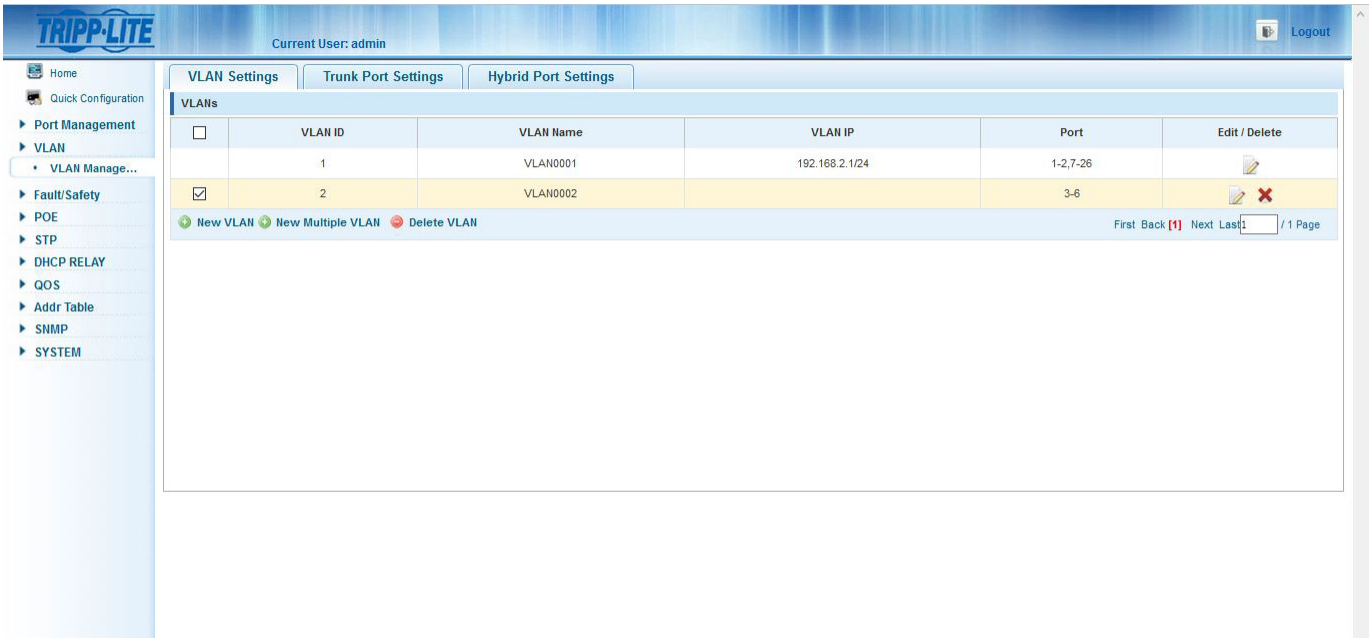


Figure 6.5 : Supprimer un seul réseau local virtuel

Supprimer plusieurs réseaux locaux virtuels :

Cliquer sur la case à cocher à côté du ou des réseaux locaux virtuels à supprimer, puis cliquer sur « Delete VLAN » (supprimer le réseau local virtuel) pour supprimer le ou les réseaux locaux virtuels sélectionnés (Figure 6.6).

Remarque : *VLAN 1 est le réseau local virtuel de gestion par défaut; ce paramètre ne peut pas être modifié.*

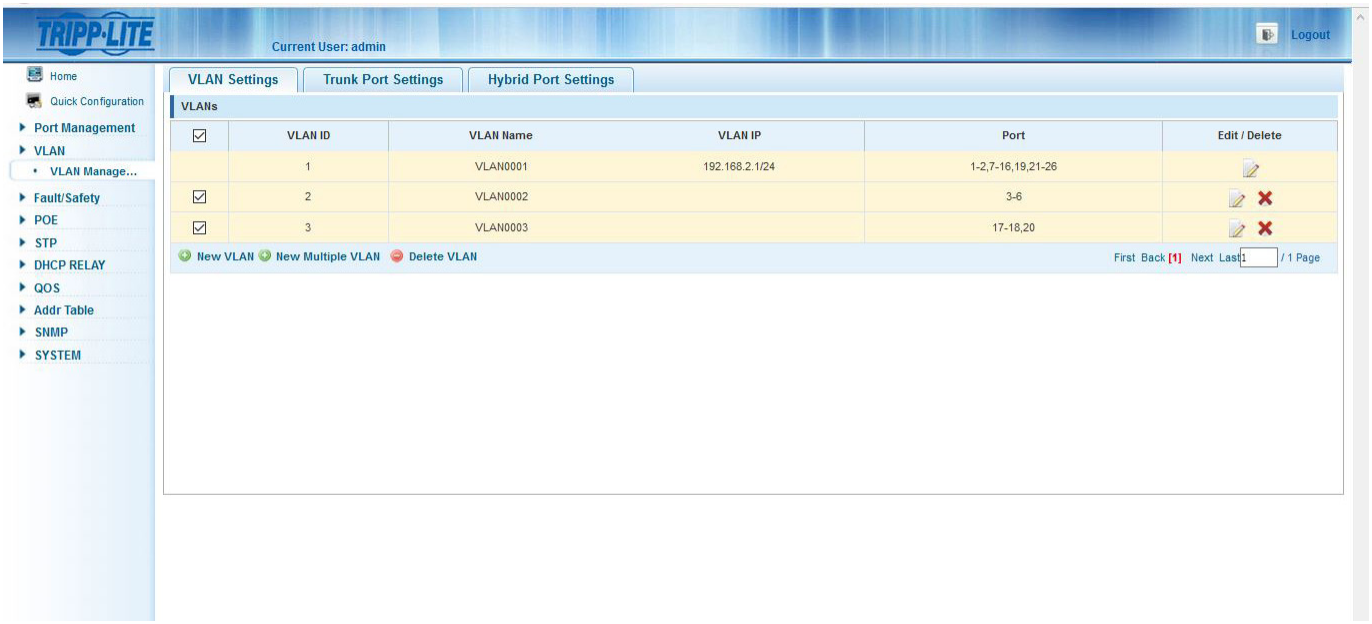


Figure 6.7 : Supprimer simultanément plusieurs réseaux locaux virtuels

6.2 Paramètres des ports de la ligne réseau

6.2.1 Afficher les paramètres des ports de la ligne réseau

Sélectionner « VLAN → VLAN Management → Trunk Port Settings » (réseau local virtuel, gestion du réseau local virtuel, paramètres des ports de la ligne réseau) pour afficher la configuration des ports de la ligne réseau (Figure 6.7). Les ports de la ligne réseau permettent le transfert des informations sur le réseau local virtuel entre des commutateurs. Par défaut, le réseau local virtuel natif (port d'accès) pour le commutateur est VLAN 1. La communication entre les ports d'accès ne sera pas marquée (802.1Q). Lorsqu'un port de la ligne réseau est configuré entre deux commutateurs, le trafic qui passe entre eux sera marqué d'un repère pour permettre aux commutateurs de distinguer les différents paquets.

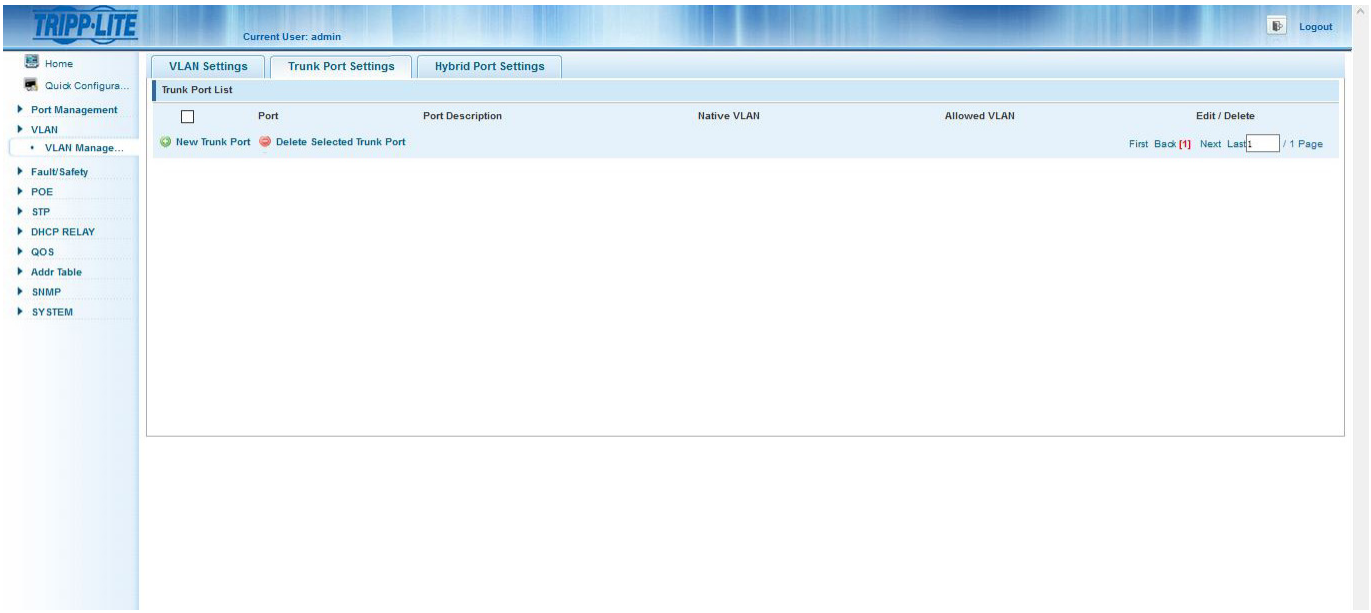


Figure 6.7 Afficher les paramètres des ports de la ligne réseau

6. Gestion du réseau local virtuel

La liste de ports de la ligne réseau affiche la configuration des ports de la ligne réseau du commutateur.

- **Port :** affiche le numéro du port.
- **Native VLAN :** affiche le réseau local virtuel. Par défaut, le réseau local virtuel natif du commutateur est VLAN1.
- **Allowed VLAN :** affiche les réseaux locaux virtuels qui seront étiquetés lors de leur transmission sur le port de la ligne réseau.

6.2.2 Ajouter des paramètres aux ports de la ligne réseau

Pour ajouter un nouveau port de la ligne réseau, cliquer sur « New Trunk Port » (nouveau port de la ligne réseau) (Figure 6.8). Sélectionner le réseau local virtuel natif (1 par défaut), puis sélectionner le ou les réseaux locaux virtuels autorisés, puis cliquer sur « Save » (sauvegarder).

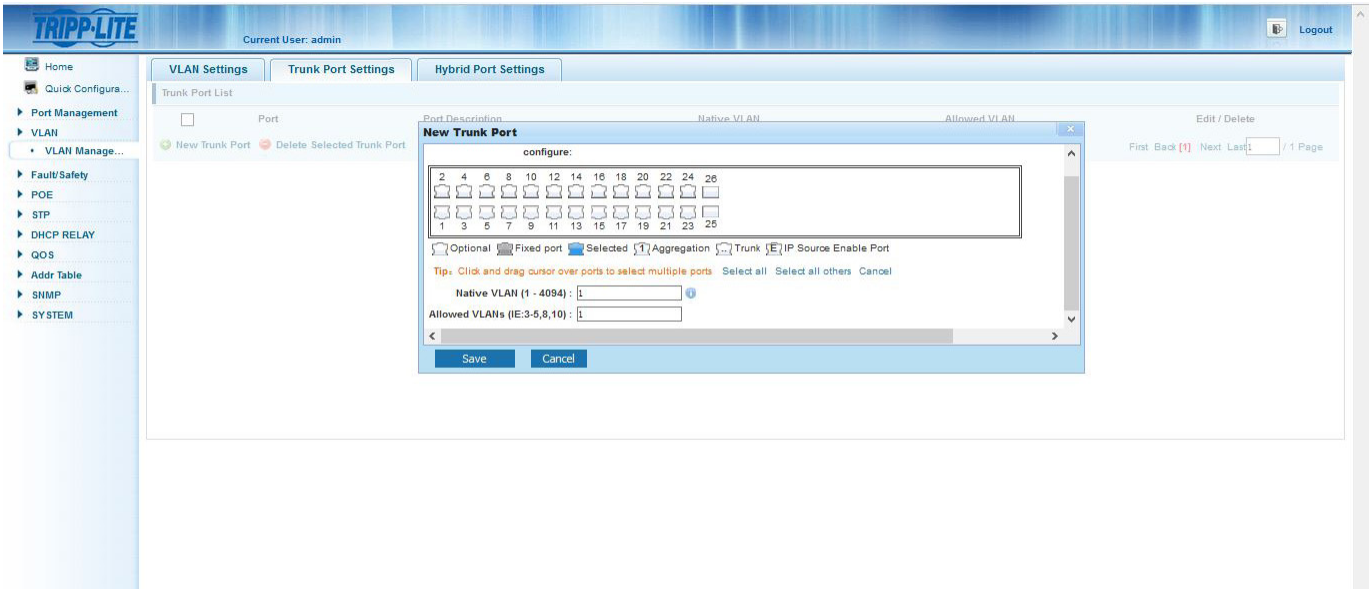


Figure 6.8 : Ajouter des ports de la ligne réseau

Remarque : *Le ou les ports de la ligne réseau autorisés doivent être créés au moyen de la gestion des réseaux locaux virtuels avant de pouvoir être ajoutés à un port de la ligne réseau.*

6.2.3 Modifier des ports de la ligne réseau

Cliquer sur l'icône « Edit » (modifier) du port de la ligne réseau à être modifié. Dans la fenêtre Edit Trunk Port (modifier le port de la ligne réseau) (Figure 6.9), il est possible d'ajouter des ports de la ligne réseau supplémentaires, de modifier le réseau local virtuel natif et de modifier les réseaux locaux virtuels autorisés pour le port de la ligne réseau sélectionné.

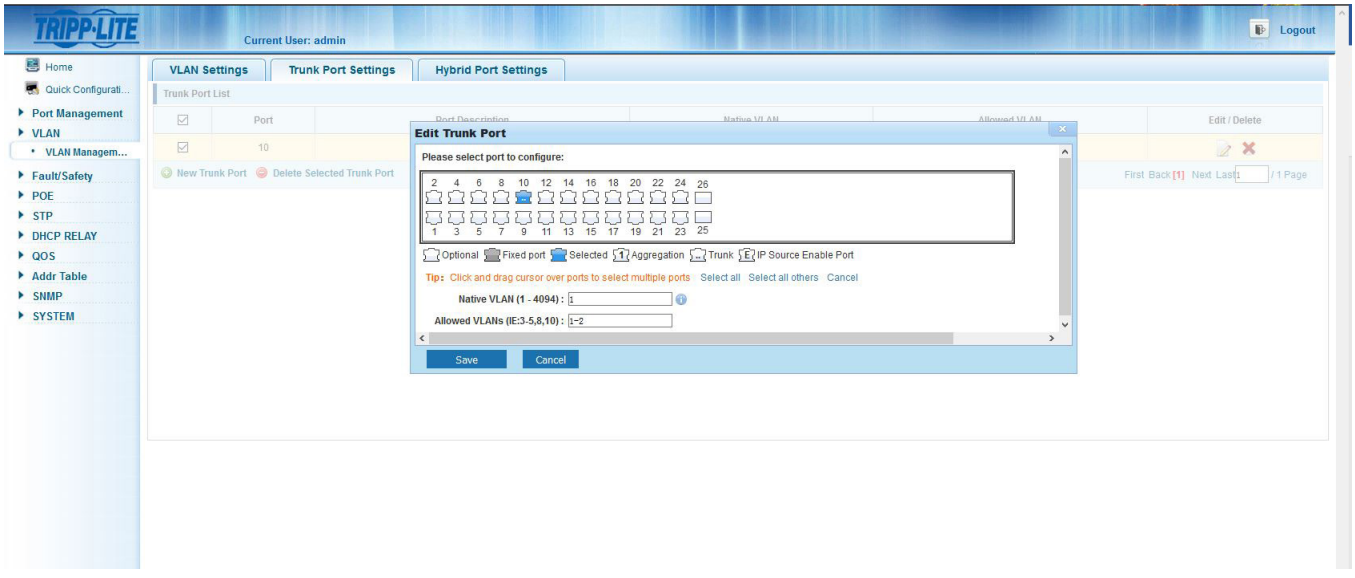


Figure 6.9 : Modifier un port de la ligne réseau

6.2.4 Supprimer des ports de la ligne réseau

Supprimer un seul port de la ligne réseau

Sélectionner le port de la ligne réseau à supprimer, puis cliquer sur l'icône (Figure 6.10).

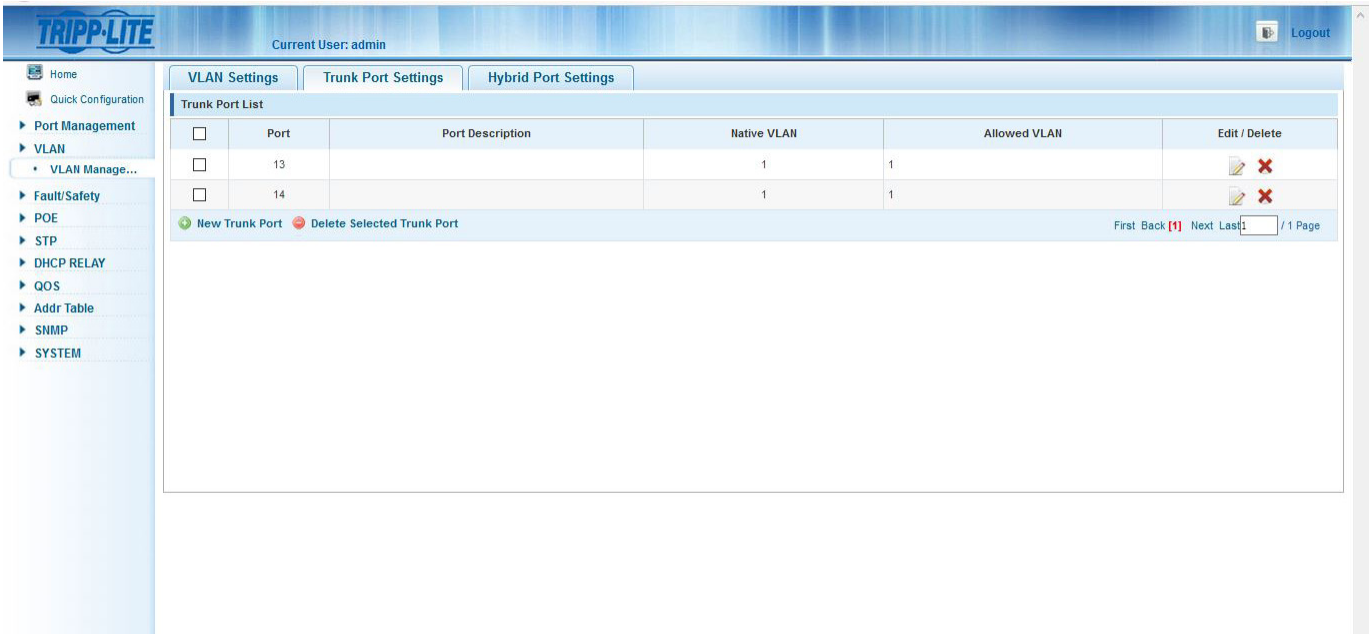


Figure 6.10 : Supprimer un seul port de la ligne réseau

Supprimer plusieurs ports de la ligne réseau

Cliquer sur la case à cocher des ports de la ligne réseau à supprimer, puis cliquer sur « Delete Selected Trunk Port » (supprimer le port de la ligne réseau sélectionné) pour supprimer les ports de la ligne réseau sélectionnés (Figure 6.11).

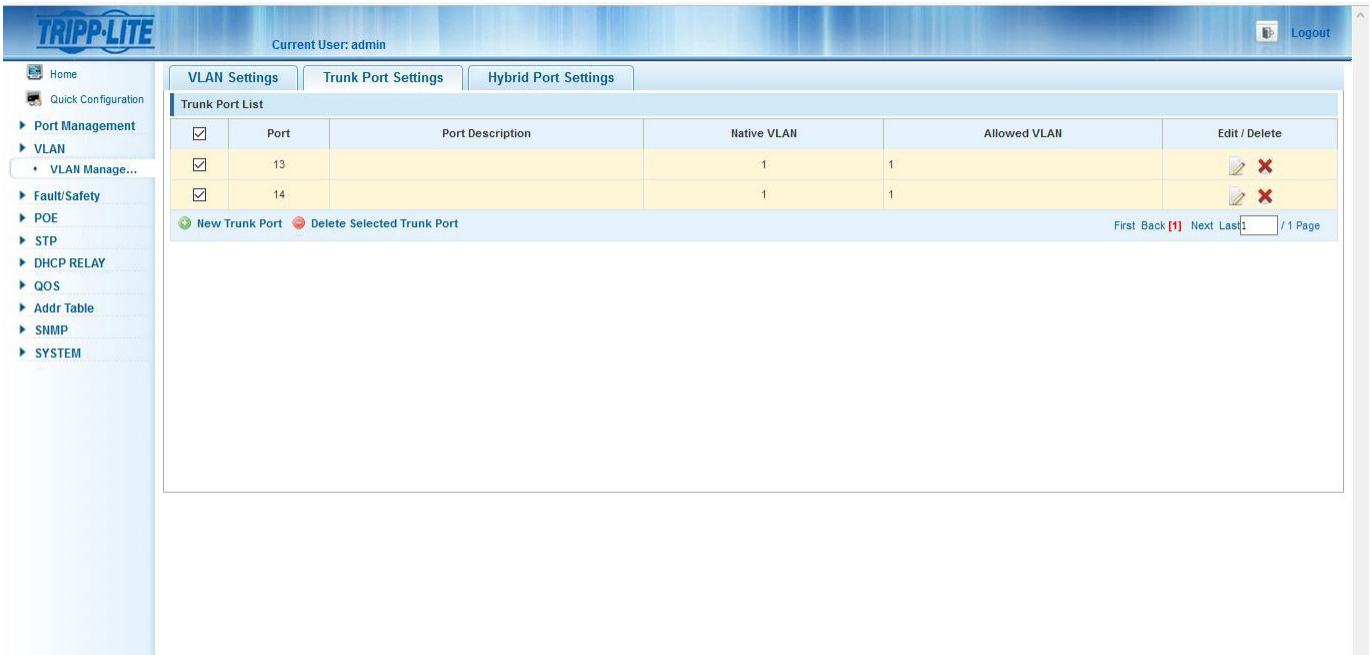


Figure 6.11 : Supprimer plusieurs ports de la ligne réseau

6. Gestion du réseau local virtuel

6.3 Paramètres des ports hybrides

Les ports hybrides prennent en charge le trafic des réseaux locaux virtuels étiquetés et non étiquetés. Cette fonctionnalité est habituellement utilisée avec les connexions téléphoniques VoIP ou les réseaux locaux virtuels.

La liste des ports hybrides indique les configurations des ports hybrides du commutateur.

- **Port :** affiche le numéro du port.
- **Port Name :** affiche la description du nom du port.
- **Native VLAN :** affiche le réseau local virtuel. Par défaut, le réseau local virtuel natif du commutateur est VLAN1.
- **Added VLAN TAG :** affiche les réseaux locaux virtuels qui seront étiquetés lors de leur transmission sur le port hybride.
- **Removed VLAN TAG :** affiche le réseau local virtuel qui sera non étiqueté lors de leur transmission sur le port hybride.
- **Allowed VLAN :** affiche les réseaux locaux virtuels qui seront étiquetés lors de leur transmission sur le port hybride.

6.3.1 Ajouter de nouveaux ports hybrides

Sélectionner le ou les ports qui feront partie de la configuration des ports hybrides (Figure 6.12). Saisir ensuite le réseau local virtuel natif (entre 1 et 4 094). Saisir ensuite le numéro d'identification des réseaux locaux virtuels qui sont étiquetés (3-5, 8, 10). Finalement, saisir le numéro d'identification des étiquettes Go to VLAN (3-5, 8, 10). Cliquer sur « Save » pour sauvegarder les paramètres des ports hybrides. L'affichage reviendra automatiquement aux listes d'aperçus des ports hybrides.

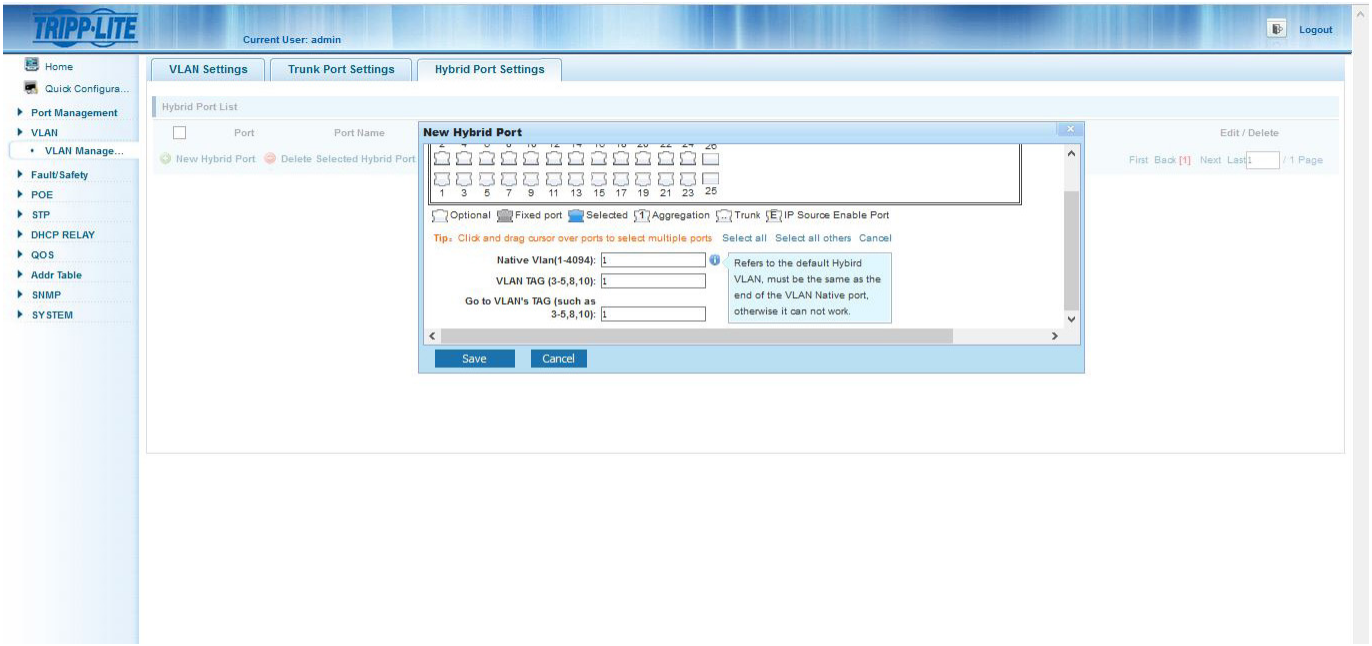


Figure 6.12 : Ajouter de nouveaux ports hybrides

6. Gestion du réseau local virtuel

6.3.2 Modifier les ports hybrides

Pour modifier, cliquer sur l'icône « Edit » à côté du prochain port hybride configuré à modifier. Modifier les ports sélectionnés, le réseau local virtuel et l'étiquette du réseau local virtuel (Figure 6.13). Une fois les modifications des ports hybrides terminées, cliquer sur « Save » (sauvegarder).

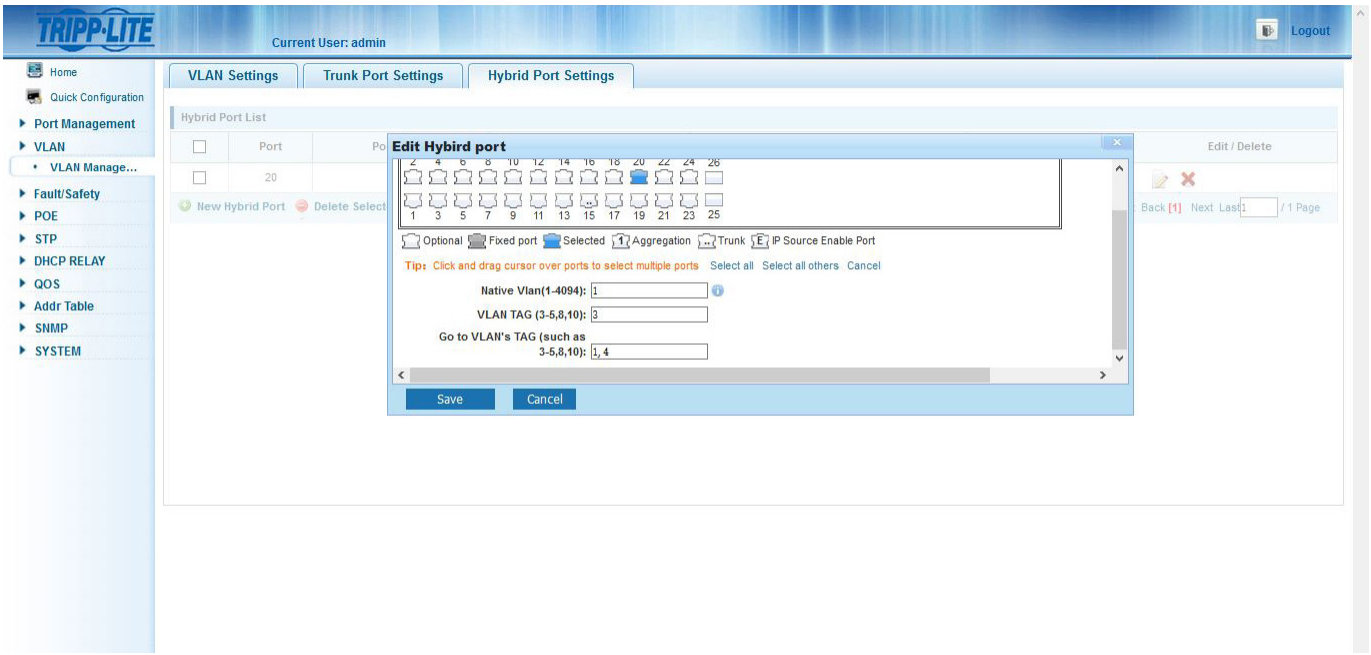


Figure 6.13 : Modifier un port hybride

6.3.3 Supprimer les ports hybrides

Pour supprimer un port hybride, cliquer sur l'icône ✖ à droite du port hybride configuré à supprimer. Pour supprimer plusieurs ports hybrides, cliquer sur la case à cocher à côté de chaque port hybride à supprimer (Figure 6.14). Sélectionner l'option « Delete Selected Hybrid Port » (supprimer le port hybride sélectionné) pour supprimer les ports.

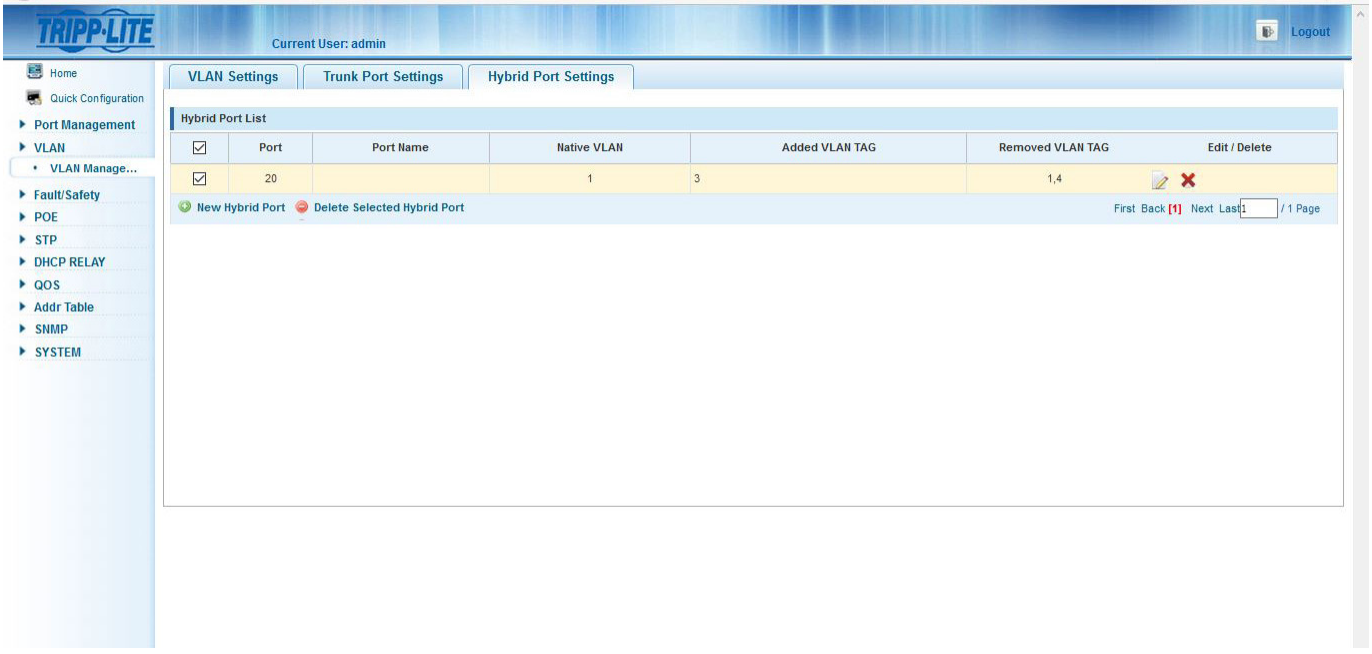


Figure 6.14 : Supprimer un port hybride

7. Gestion des défaillances/de la sécurité

Dans la barre de navigation, sélectionner « Fault/Safety » (défaillance/sécurité). Ici, il est possible de voir les fonctions de prévention des attaques du commutateur, effectuer la détection du cheminement et configurer la LCA (liste de contrôle d'accès).

7.1 Prévention des attaques

Dans la barre de navigation, sélectionner « Fault/Safety → Attack Prevention → DHCP » (défaillance/sécurité, prévention des attaques, DHCP). Activer et configurer la suite de protection DHCP permet de fournir une certaine sécurité en filtrant les messages DHCP non sécurisés. Une interface non sécurisée est une interface qui est configurée pour recevoir des messages de l'extérieur du réseau ou du pare-feu. Une interface sécurisée est une interface qui est configurée pour recevoir des messages uniquement au sein du réseau. La surveillance DHCP agit comme un pare-feu entre les hôtes non sécurisés et les serveurs DHCP. Elle fournit également une façon d'établir une distinction entre les interfaces non sécurisées connectées à l'utilisateur final et les interfaces sécurisées connectées au serveur DHCP ou à un autre commutateur.

7.1.1 Activer la suite de protection DHCP

Pour activer la suite de protection, cliquer sur le bouton orange Disabled (désactivé) pour l'activer (Figures 7.1-7.2). Suivre les étapes ci-dessous jusqu'à la Section 7.1.1.8 pour configurer les fonctionnalités de la suite de protection.

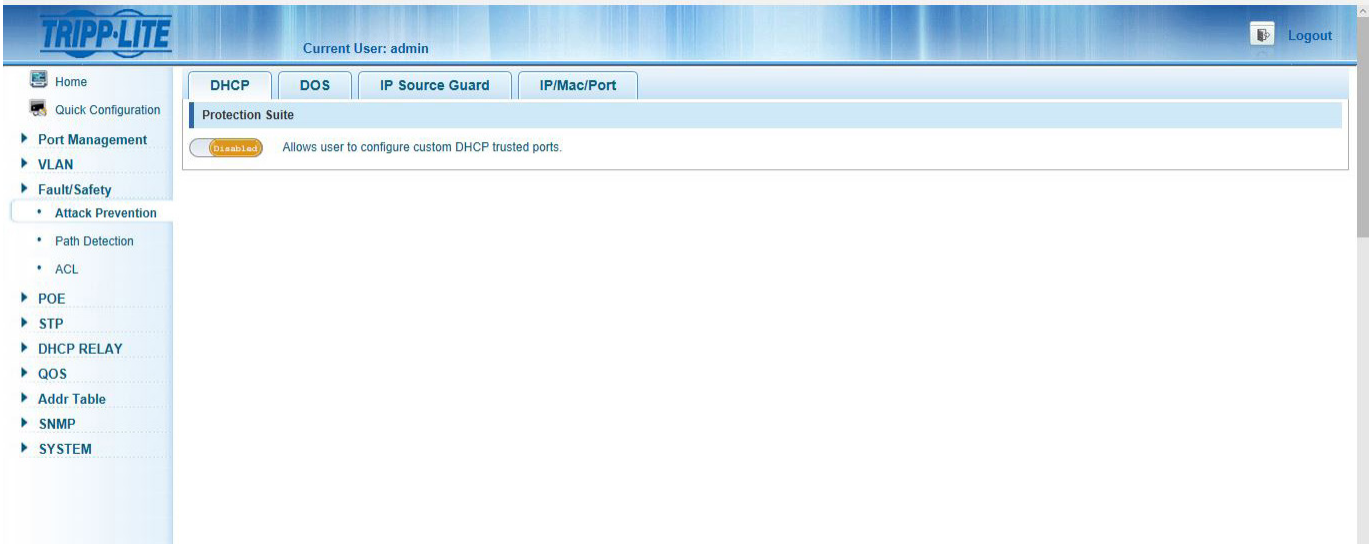


Figure 7.1 : DHCP désactivé (par défaut)

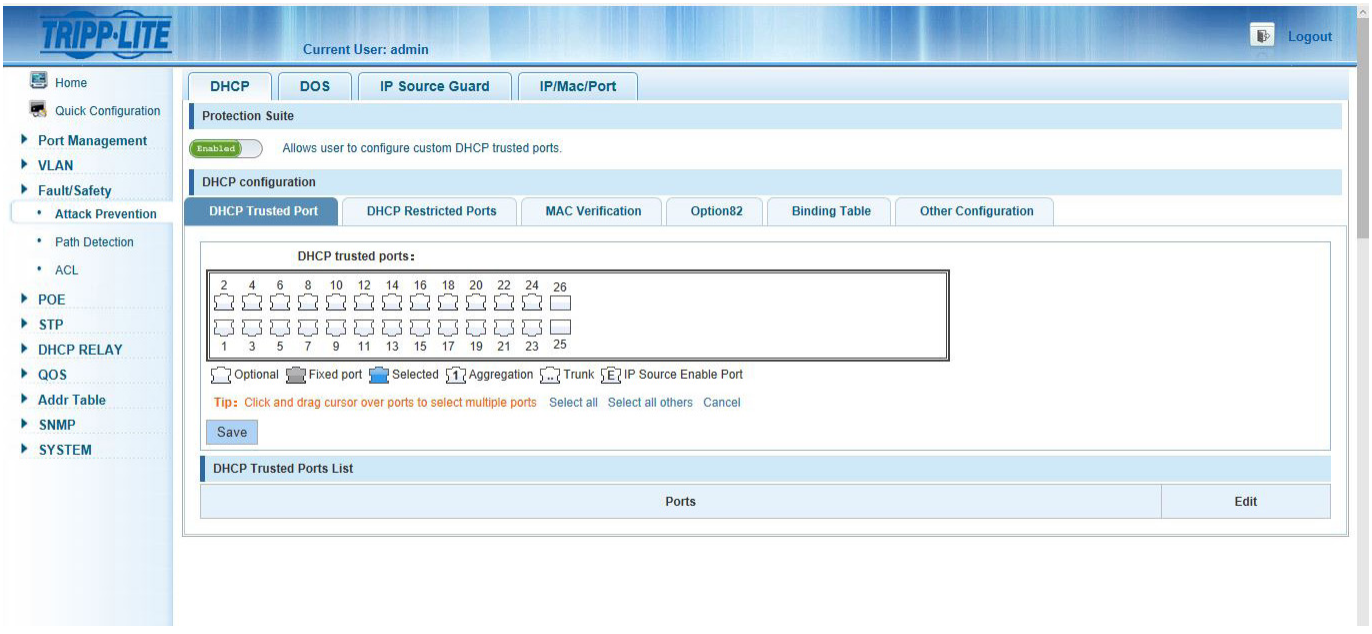


Figure 7.2 : DHCP activé

7. Gestion des défaillances/de la sécurité

7.1.2 Configurer le réseau local virtuel de surveillance de trafic DHCP

Sélectionner l'onglet « Other Configuration » (autre configuration), puis saisir le réseau local virtuel de surveillance DHCP (Figure 7.3). Cliquer sur « Save » (sauvegarder) une fois l'action terminée.

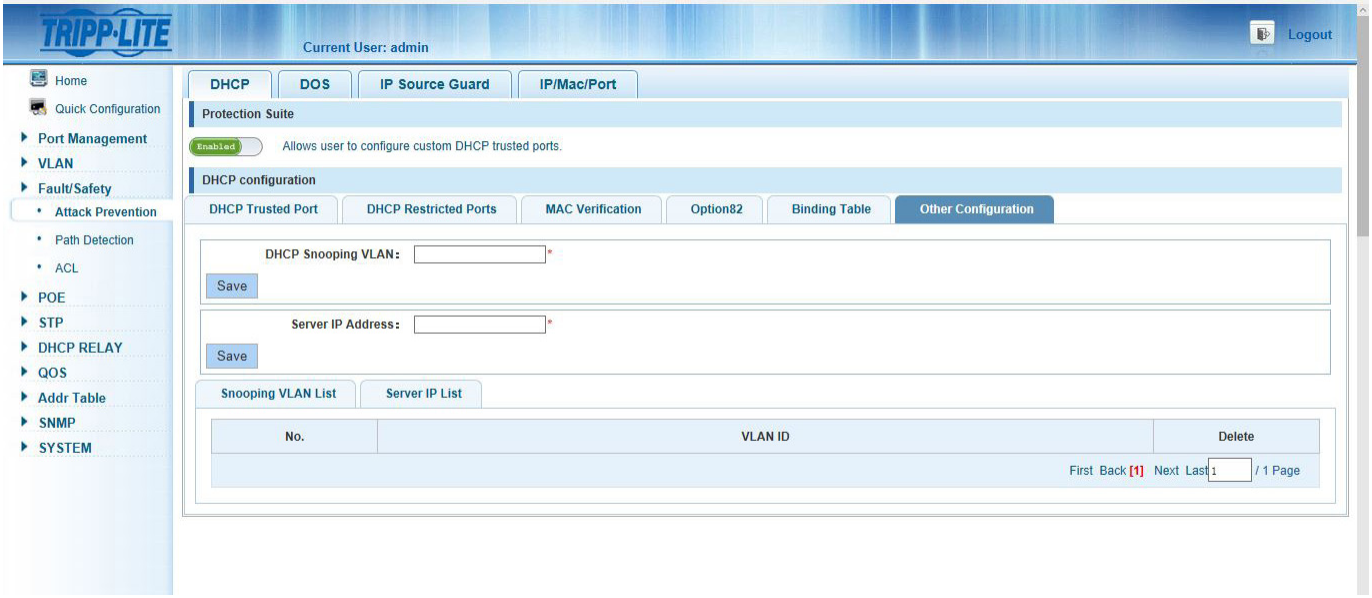


Figure 7.3 : Réseau local virtuel de surveillance de trafic DHCP

7.1.3 Configurer les serveurs DHCP sécurisés

Sélectionner l'onglet « Other Configuration » (autre configuration), puis saisir les adresses IP du ou des serveurs DHCP sécurisés. Cliquer sur « Save » (sauvegarder) une fois l'action terminée.

7.1.4 Ajouter des ports DHCP sécurisés

Sélectionner le ou les ports à configurer faisant partie du groupe de ports sécurisés DHCP ou du groupe de ports (Figure 7.4). Une fois le ou les ports sélectionnés, cliquer sur « Save » (sauvegarder). Pour modifier ou supprimer des ports sécurisés DHCP, cliquer sur l'icône Edit (modifier) à côté de la liste de ports sécurisés, puis désélectionner le ou les ports de la liste. Une fois les modifications terminées, cliquer sur « Save » (sauvegarder).

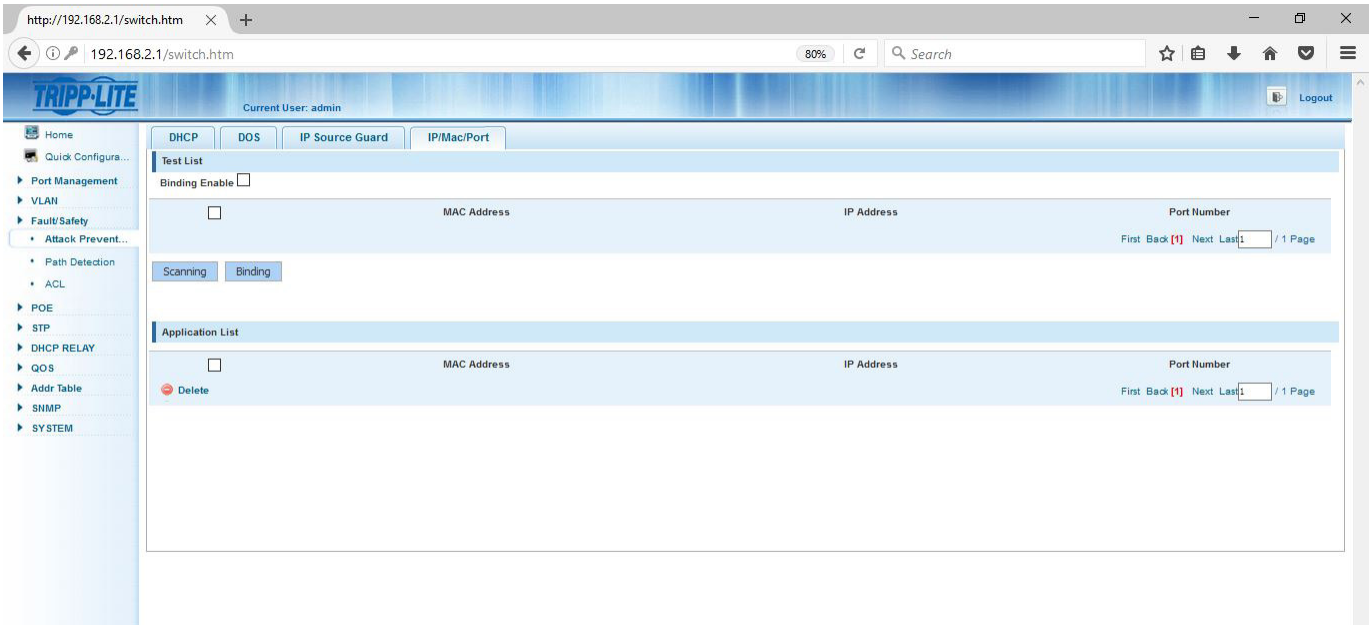


Figure 7.4 Ajouter des ports DHCP sécurisés

7. Gestion des défaillances/de la sécurité

7.1.5 Ajouter/modifier des ports DHCP à accès restreint

Pour ajouter des ports à accès restreint DHCP, se rendre à Fault/Safety → DHCP → DHCP Restricted Ports (défaillance/sécurité, DHCP, ports à accès restreint DHCP). Configurer la liste de ports à bloquer afin de ne pas recevoir d'adresses DHCP en sélectionnant ces ports. Une fois le ou les ports sélectionnés, cliquer sur « Save » (sauvegarder). Pour modifier ou supprimer les ports sécurisés DHCP, cliquer sur l'icône « Edit » à côté de « Prohibit DHCP for Address Port List » (interdire DHCP pour la liste de ports d'adresse). Ensuite, désélectionner le ou les ports à supprimer de la liste des interdictions. Une fois les modifications terminées, cliquer sur « Save » (sauvegarder).

Remarque : *Supprimer tous les ports de la liste désactive la fonctionnalité.*

7.1.6 Vérification de la source d'origine MAC

Activer la vérification d'adresse MAC permet d'assurer que si un paquet est reçu d'une interface non sécurisée, et que la source d'origine MAC et l'adresse MAC du client DHCP ne correspondent pas, le commutateur va abandonner le paquet.

Pour activer, cliquer sur la case à cocher « MAC Verification Enable » (activer la vérification de l'adresse MAC) (Figure 7.5). Ajouter ensuite l'adresse de la source d'origine MAC, puis cliquer sur « Save » (sauvegarder). Une fois activée, elle fournira l'état des différents dispositifs activés ou configurés pour bloquer intentionnellement le trafic des paquets.

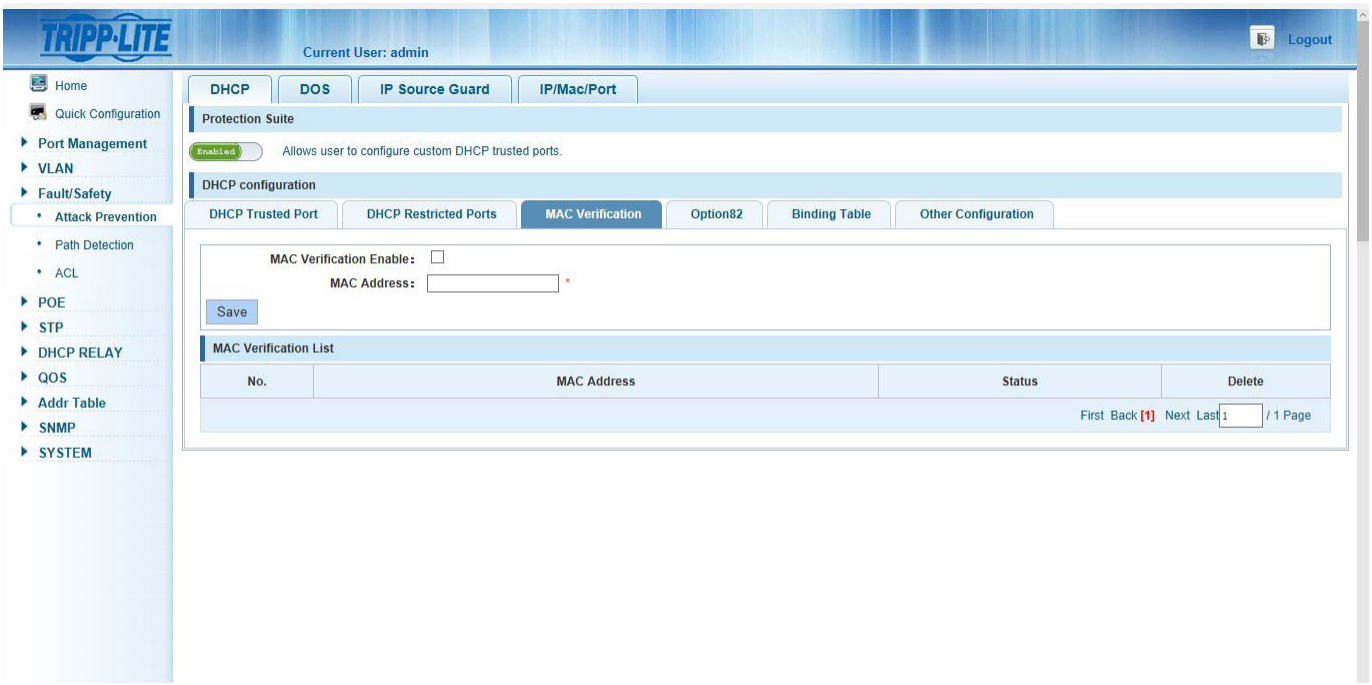


Figure 7.5 : Vérification de l'adresse MAC

7. Gestion des défaillances/de la sécurité

7.1.7 Configurer les informations Option82

Activer Option82 permet l'identification distincte d'un dispositif sur le réseau lorsqu'une demande de diffusion générale est envoyée au moyen du commutateur en ajoutant les informations du paquet Option82 à être lues par le serveur DHCP. Pour activer, cliquer sur la case à cocher « Client Options82 Enable » (activer l'Option82 du client) (Figure 7.6).

Fournir le nom du circuit de contrôle et le numéro d'identification du réseau local virtuel (Figure 7.7). Une fois le nom saisi, cliquer sur « Save » (sauvegarder). Pour modifier, cliquer sur l'option Edit (modifier) à côté du nom du contrôle du circuit. Cliquer sur « Save » (sauvegarder) une fois la modification terminée. Cliquer sur « Cancel » (annuler) pour rejeter les modifications. Pour supprimer une saisie du contrôle du circuit de la liste, cliquer sur l'icône à côté du nom du circuit à supprimer. Le paramètre est automatiquement sauvegardé dans le système une fois la suppression sélectionnée.

Saisir ensuite l'agent à distance « Remote Name » (nom à distance) et le numéro d'identification du réseau local virtuel (Figure 7.8). Cliquer sur « Save » (sauvegarder) une fois l'action terminée. Pour modifier, cliquer sur l'option Edit (modifier) à côté de l'agent à distance à modifier. Cliquer sur « Save » (sauvegarder) une fois la modification terminée. Cliquer sur Cancel (annuler) pour rejeter les modifications. Pour supprimer une saisie de l'agent à distance de la liste, cliquer sur l'icône rouge à côté de l'agent à distance à supprimer. Le paramètre est automatiquement sauvegardé dans le système une fois la suppression sélectionnée.

Sélectionner l'onglet IP Address (adresse IP), puis saisir l'adresse IP et le numéro d'identification du réseau local virtuel du client.

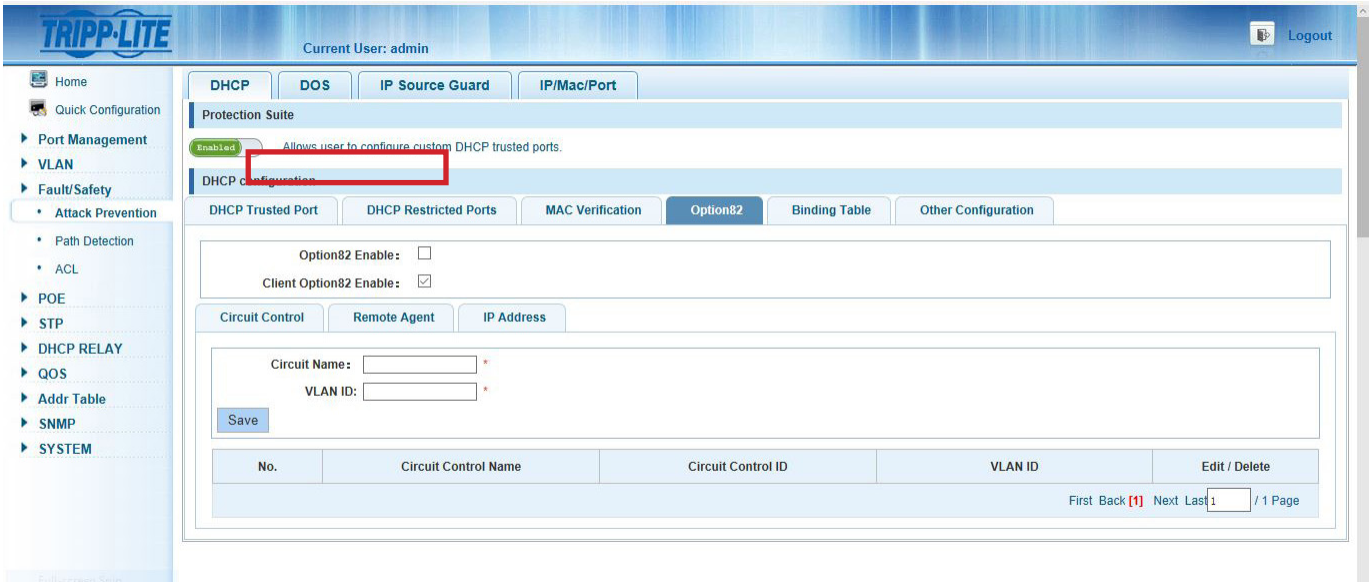


Figure 7.6 : Activer Option82 du client

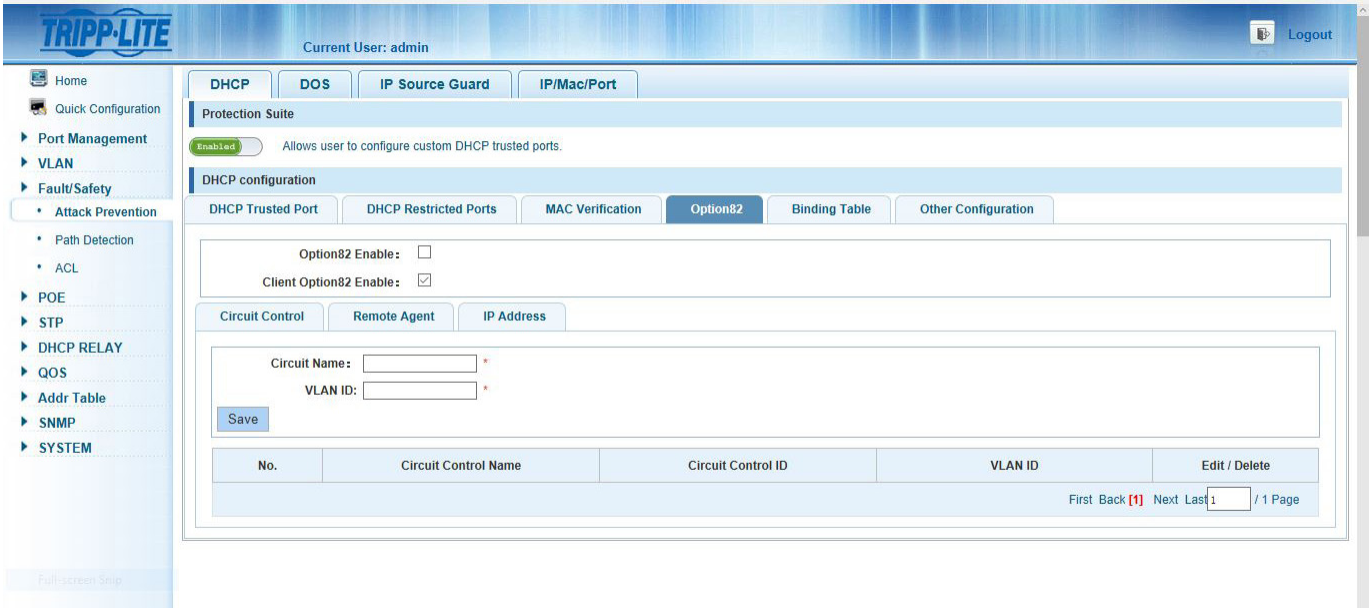


Figure 7.7 : Contrôle du circuit Option82

7. Gestion des défaillances/de la sécurité

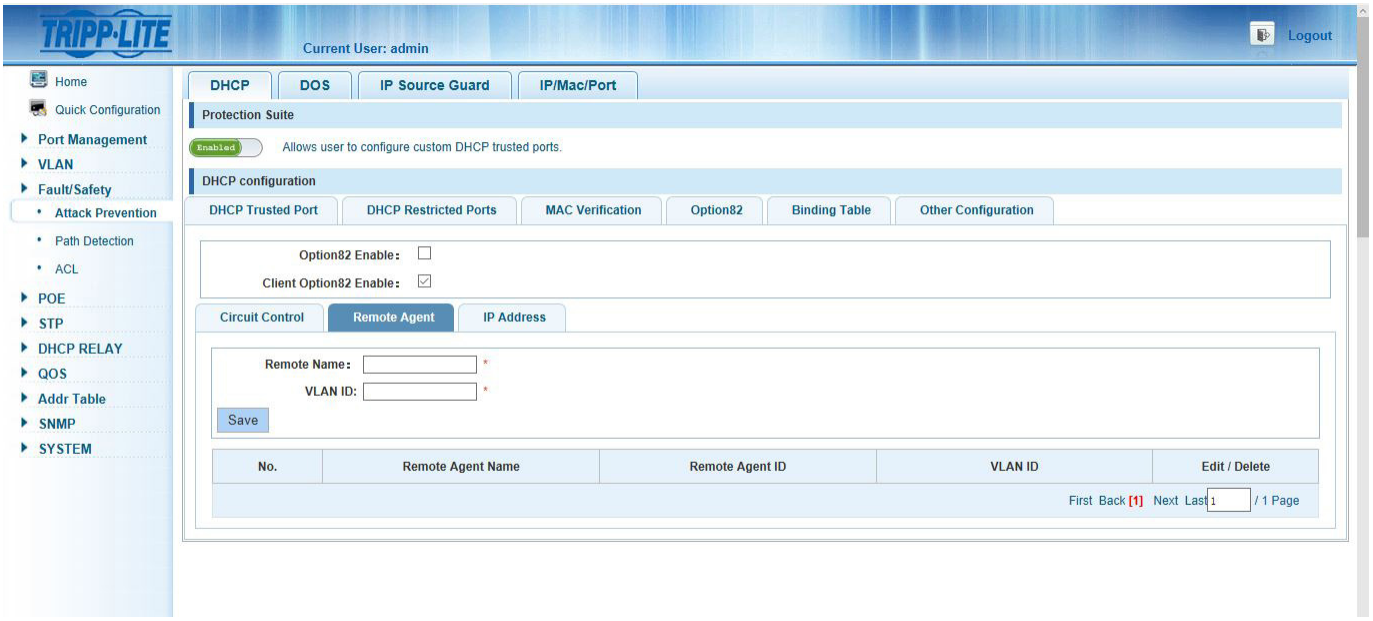


Figure 7.8 : Agent à distance Option82

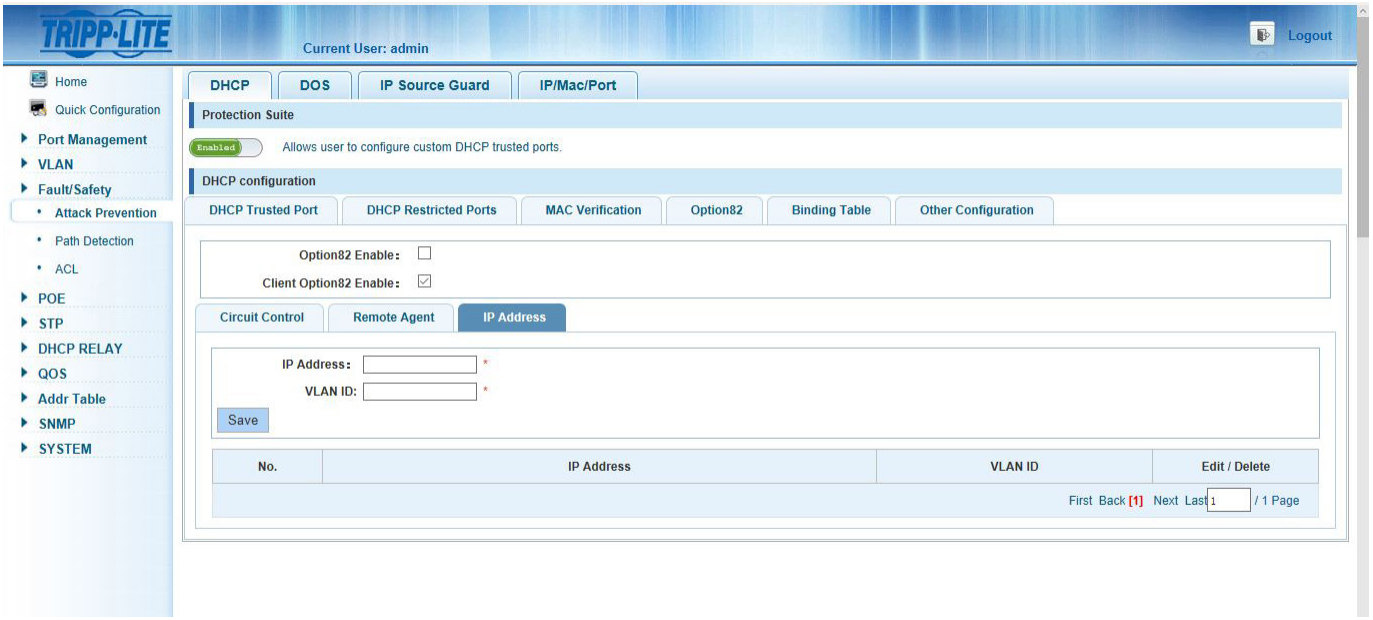


Figure 7.9 : Adresse IP Option82

Fournir ensuite le nom du circuit de contrôle du circuit et le numéro d'identification du réseau local virtuel. Une fois le nom saisi, cliquer sur « Save » (sauvegarder). Pour modifier, cliquer sur l'option Edit (modifier) à côté du nom du contrôle du circuit. Cliquer sur « Save » (sauvegarder) pour accepter les modifications ou sur « Cancel » (annuler) pour les rejeter. Pour supprimer une saisie du contrôle du circuit de la liste, cliquer sur l'icône ✖ à côté du nom du circuit à supprimer. Le système sauvegardera automatiquement le paramètre une fois la suppression sélectionnée.

Saisir ensuite l'agent à distance « Remote Name » (nom à distance) et le numéro d'identification du réseau local virtuel. Cliquer sur « Save » (sauvegarder) une fois l'action terminée. Pour modifier, cliquer sur l'option Edit (modifier) à côté de l'agent à distance à modifier. Cliquer sur « Save » (sauvegarder) pour accepter les modifications ou sur « Cancel » (annuler) pour les rejeter. Pour supprimer une saisie de l'agent à distance de la liste, cliquer sur l'icône rouge ✖ à côté de l'agent à distance à supprimer. Le système sauvegardera automatiquement les paramètres une fois que « Delete » (supprimer) est sélectionné.

Sélectionner l'onglet IP Address (adresse IP), puis saisir l'adresse IP et le numéro d'identification du réseau local virtuel du client (figure 7.9).

7. Gestion des défaillances/de la sécurité

7.1.8 Créer un tableau de liaison de surveillance de trafic DHCP

Le tableau de liaison de surveillance de trafic DHCP comprend des saisies de liaison vers des ports non sécurisés. Pour créer le tableau de liaison, saisir l'adresse MAC et le numéro d'identification du réseau local virtuel, puis sélectionner le numéro du port depuis le menu déroulant (Figure 7.10).

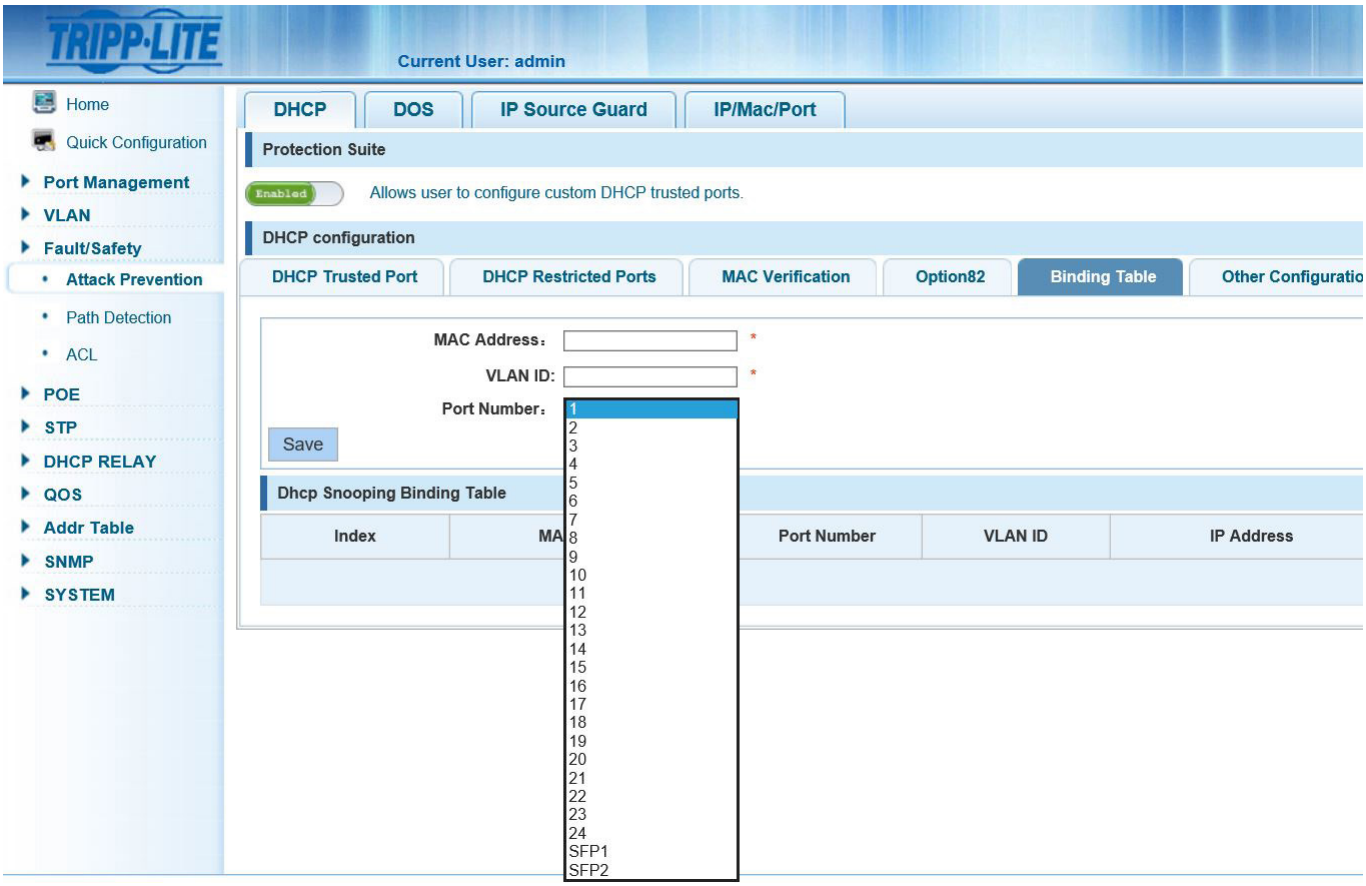


Figure 7.10 : Tableau de liaison DHCP

7.1.9 DDS (déni de service) Prévention des attaques

Aller à Fault/Safety (défaillance/sécurité) → Attack Prevention (prévention des attaques) → DOS (DDS) pour activer la fonctionnalité de prévention des attaques, DDS (Figure 7.11). Elle stoppera les tentatives de rendre les ordinateurs connectés et les ressources du réseau indisponibles à leurs utilisateurs prévus.

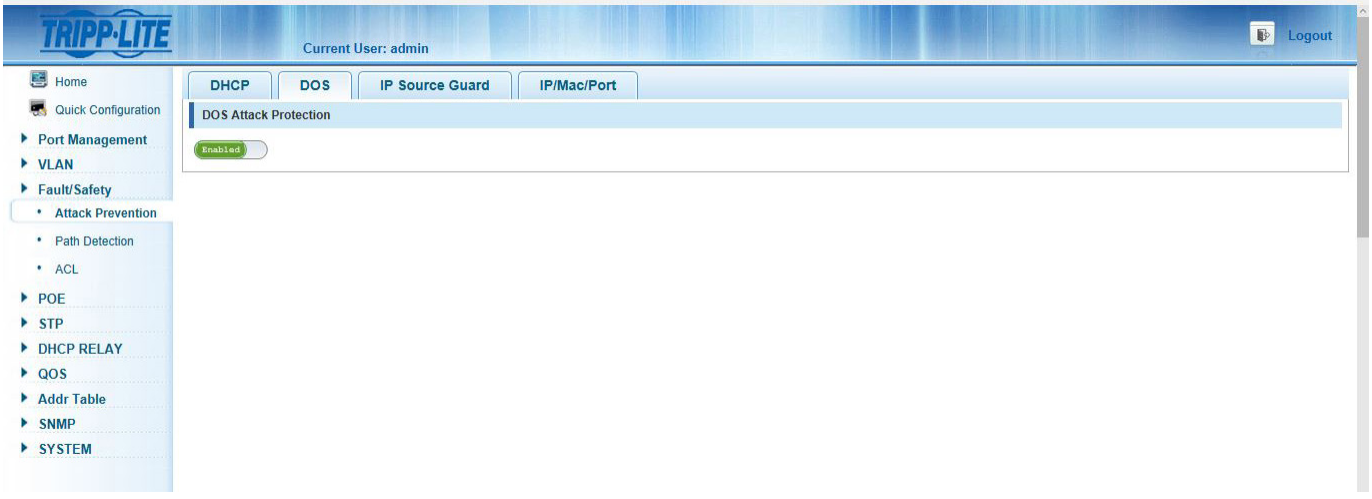


Figure 7.11 : Déni de service, prévention des attaques

7. Gestion des défaillances/de la sécurité

7.1.10 Protection de la source IP

La protection de la source IP aide à prévenir les messages illégaux au moyen d'un port en bloquant les communications avec les ressources du réseau pour améliorer la sécurité générale du port. Pour ajouter manuellement une protection de la source IP, sélectionner un ou plusieurs ports éphémères, puis cliquer sur « Save » (Figure 7.12).

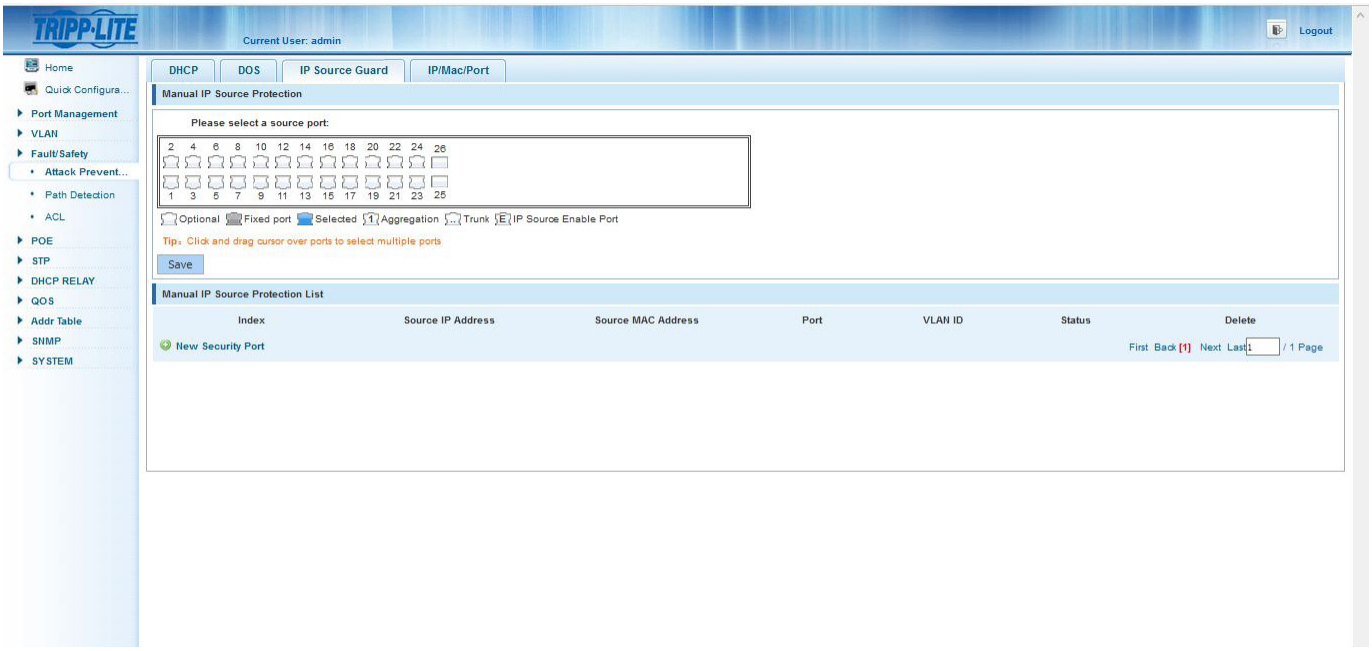


Figure 7.12 Protection de la source IP

Cliquer ensuite sur le bouton « New Security Port » (nouveau port de sécurité) sous la liste. Une fenêtre s'ouvrira pour sélectionner le port de sécurité (Figure 7.13). Saisir le numéro d'identification du réseau local virtuel, l'adresse IP de la source, l'adresse MAC de la source, puis sélectionner le port de sécurité. Cliquer sur « Save » (sauvegarder) une fois l'action terminée.

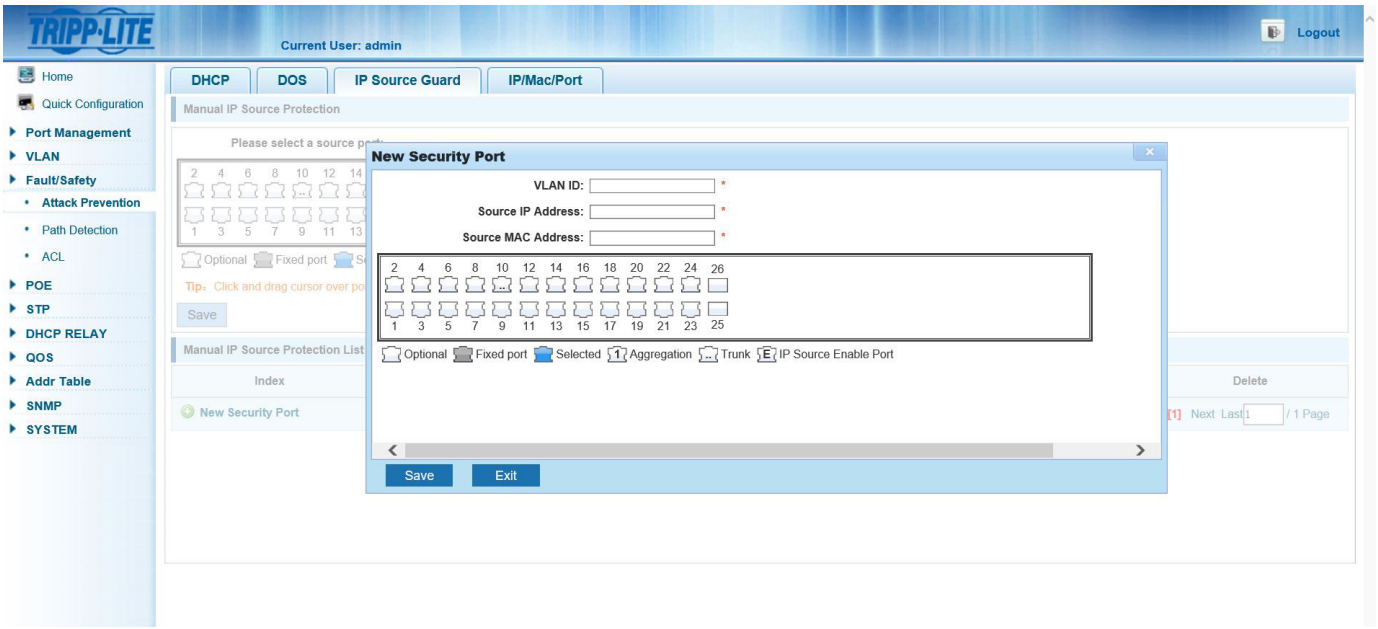


Figure 7.13 : Ajouter des ports de sécurité

7. Gestion des défaillances/de la sécurité

7.1.11 Liste des liaisons IP/MAC/Port

Pour laisser le commutateur apprendre les adresses IP basées sur les ports et les relations de mappage d'adresses MAC, suivre les étapes suivantes (Figure 7.14) :

1) Cliquer sur la case à cocher pour « Binding enable » (Activer les liaisons).
2) Balayer les ports pour réunir le mappage du port.
3) Sélectionner ensuite le port à lier et il sera ajouté à la liste des applications.

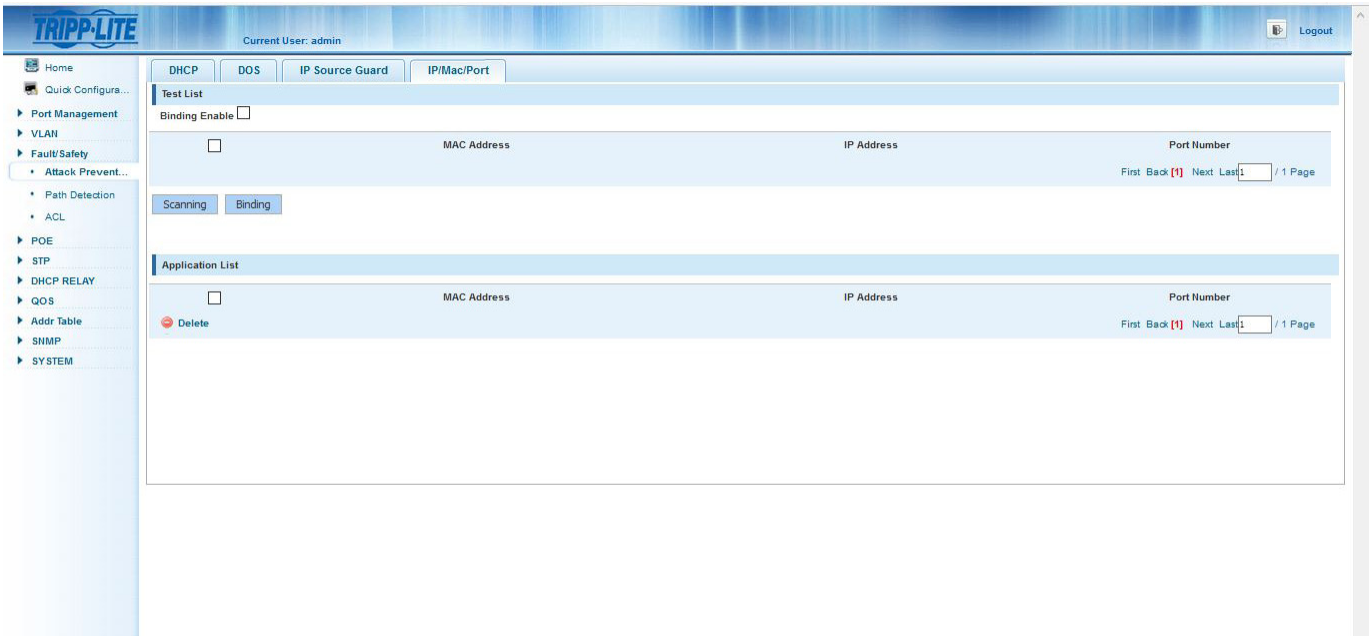


Figure 7.14 : Aperçu de la liste des liaisons IP/MAC/Port

Pour supprimer une liaison, cliquer sur la case à cocher à côté de la relation qui lie à supprimer, puis sélectionner l'icône « Delete » (supprimer). Les paramètres seront sauvegardés automatiquement.

7. Gestion des défaillances/de la sécurité

7.2 Détection du cheminement

La fonctionnalité Ping Détection du cheminement → aide à vérifier l'état d'une connexion, tandis que Tracert indique combien de chemins et combien de temps il faut pour atteindre une destination.

7.2.1 Test Ping

Sélectionner « Fault/Safety → Path Detection » (défaillance/sécurité, détection du cheminement) pour déterminer si un hôte répond (Figure 7.15). Saisir l'adresse IP du ping dans le champ « Destination IP » (IP de destination), la période de temporisation de 1 à 10 secondes (est 2 par défaut) et le numéro du ping à répétition de 1 à 1 000 (est 5 par défaut). Sélectionner « Start Test » (commencer le test) pour commencer le test et afficher les résultats.

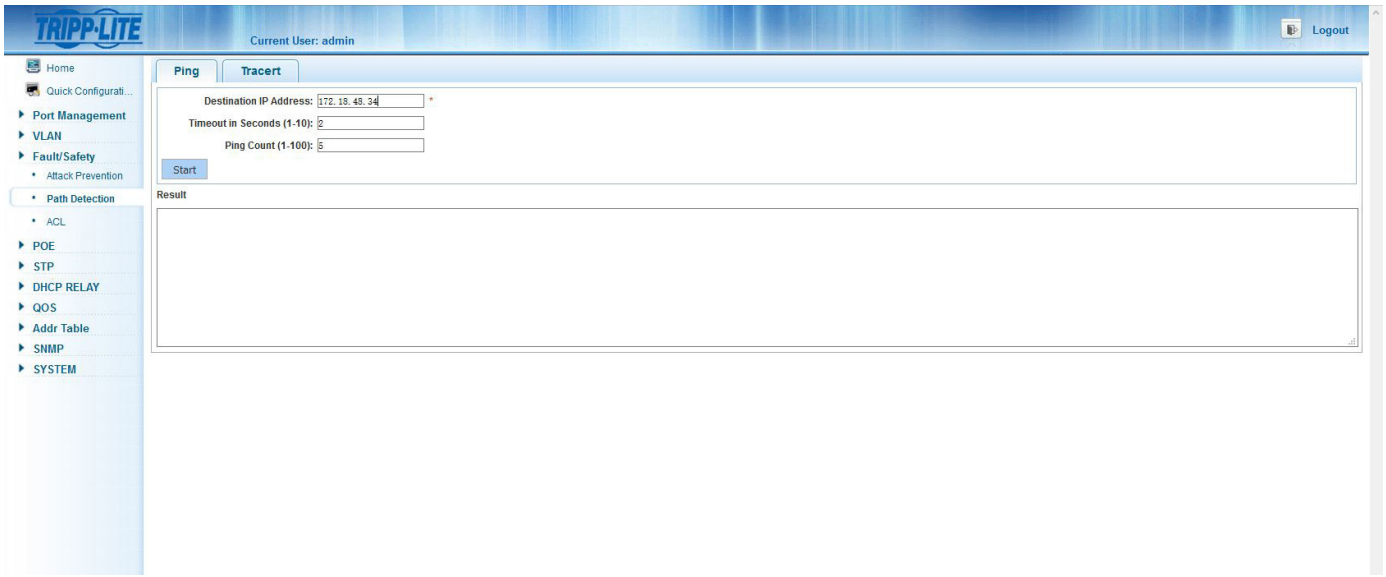


Figure 7.15: Test Ping

7.2.2 Tracert

Utiliser la fonction Tracert pour tracer le chemin de chaque routeur à travers lequel passe un paquet de données avant d'atteindre sa destination. Sélectionner « Fault/Safety → Tracert » (défaillance/sécurité, Tracert), puis saisir l'adresse IP dans le champ « Destination IP address » (adresse IP de destination) (Figure 7.16). Saisir ensuite la période de temporisation entre 1 et 10 (est 2 millisecondes par défaut).

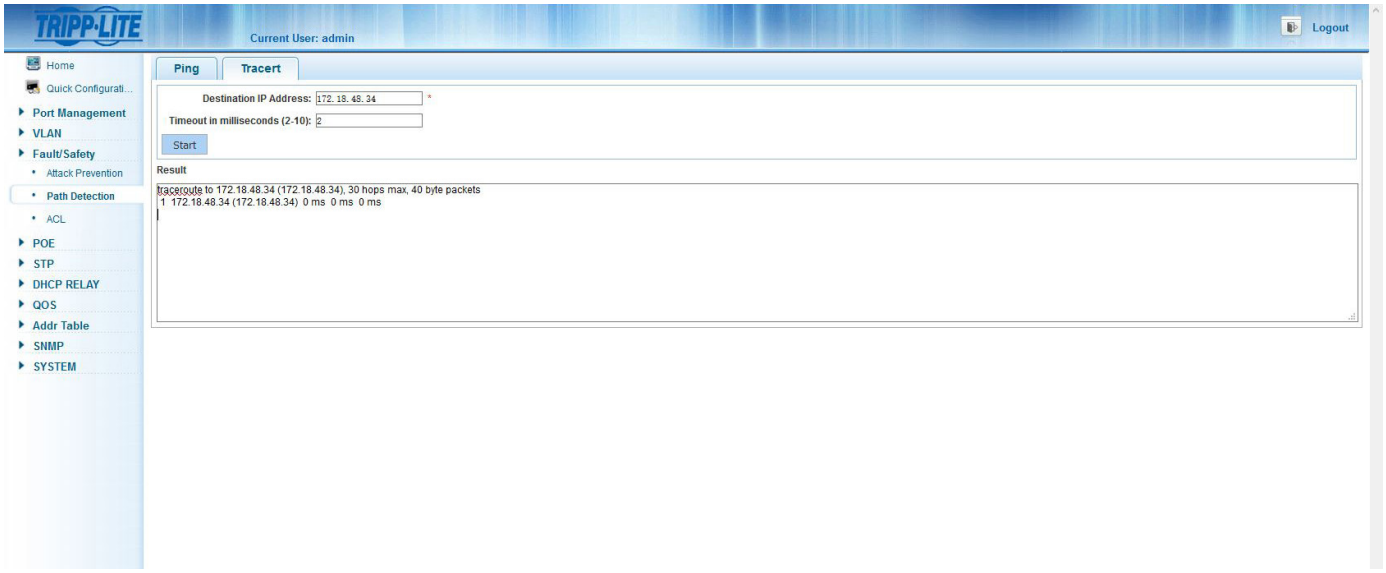


Figure 7.16 : Fonction Tracert

7. Gestion des défaillances/de la sécurité

7.3 Listes de contrôle d'accès (LCA)

Les listes de contrôle d'accès permettent aux dispositifs sur le réseau d'accorder l'accès à certains utilisateurs et certains systèmes à des ressources du réseau disponibles ou d'ignorer leurs demandes.

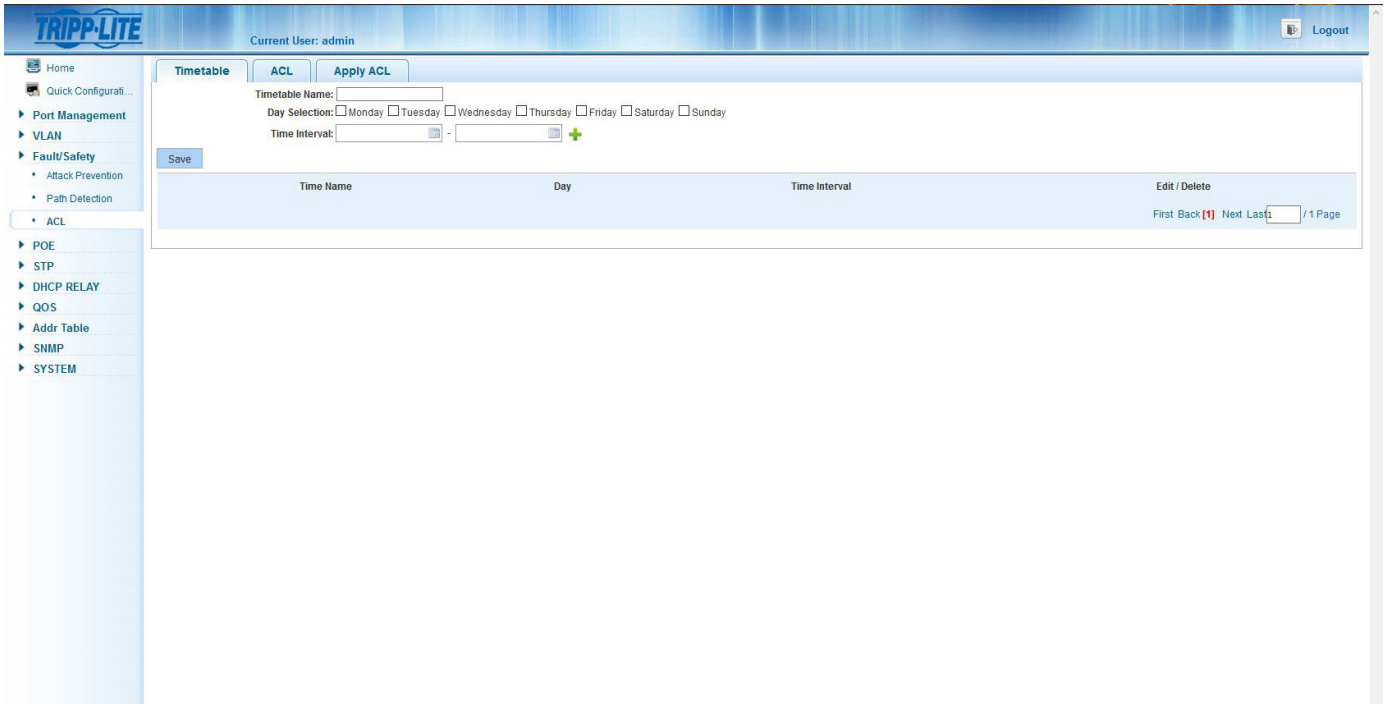


Figure 7.17 : Aperçu de la LCA

Pour configurer la LCA, aller à « Fault/Safety → ACL » (défaillance/sécurité, LCA) et effectuer les actions suivantes :

1. Nom du calendrier. Inscrire un crochet pour les jours auxquels vous voulez appliquer le calendrier. Saisir ensuite les intervalles de temps pour le calendrier. (Figure 7.18). Plusieurs calendriers par groupe peuvent être créés. Il est possible de modifier les calendriers de la LCA en cliquant sur l'icône Edit (modifier), puis définir les jours et les heures. Pour sauvegarder les modifications, cliquer sur le bouton « Save » (sauvegarder). Cliquer sur « Cancel » (annuler) pour rejeter les modifications. Si un calendrier n'est plus nécessaire, cliquer sur l'icône Delete (supprimer) pour le supprimer de la liste.
2. Créer ensuite une règle pour permettre ou refuser l'accès en configurant la LCA aux calendriers. Sélectionner l'onglet ACL (LCA) Dans la nouvelle fenêtre de la règle d'accès de la LCA (Figure 7.19), configurer le numéro de la LCA de 100 à 199, l'action de permission de Permit (permettre) ou Deny (refuser), le Protocol Type (type de protocole) (IP, UDP ou TCP) et l'ACL Name (nom de la LCA) auquel la règle s'appliquera depuis la liste déroulante. Si la règle s'applique à n'importe quelle source ou à des adresses IP de destination, laisser les cases par défaut cochées pour ces deux options. Pour préciser une seule source ou une seule adresse IP de destination, décocher la case appropriée pour permettre à l'option de saisir la seule adresse IP et l'adresse IP et le masque de sous-réseau. Pour la configuration de la règle pour TCP ou UDP pour une seule source ou un seul port éphémère, décocher la case à cocher d'un port éphémère. Saisir ensuite la seule source ou les adresses de ports éphémères de 0 à 65 535. Une fois la configuration terminée, cliquer sur le bouton « Save » (sauvegarder). Pour supprimer la règle de la configuration pour permettre ou refuser une configuration de la LCA, cliquer sur l'icône rouge .
3. Sélectionner l'onglet Apply ACL (appliquer la LCA) pour configurer les LCA à un seul ou plusieurs ports Ethernet. Saisir le numéro de la LCA de la règle applicable, puis cliquer sur « Save » (sauvegarder).

Remarque : *Les LCA configurées et actives peuvent être supprimées en suivant les étapes ci-dessus dans l'ordre inverse.*

7. Gestion des défaillances/de la sécurité

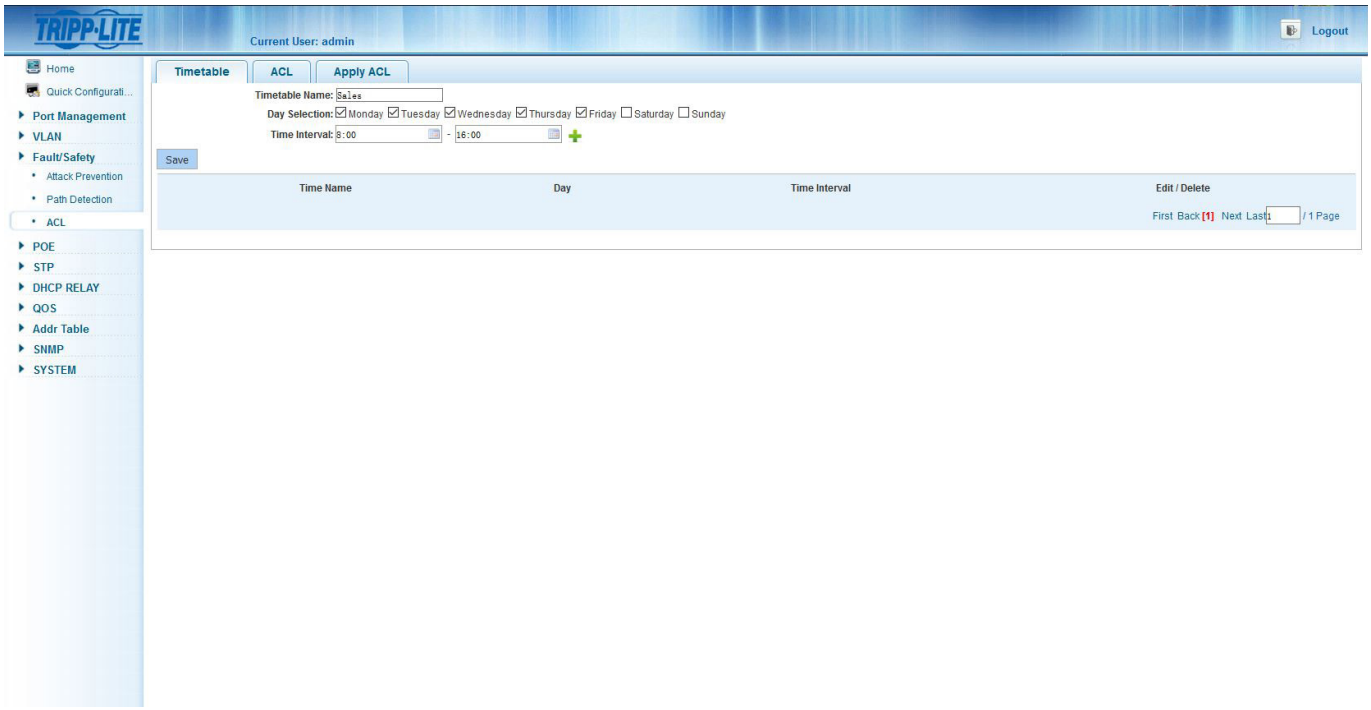


Figure 7.18 : Créer un calendrier

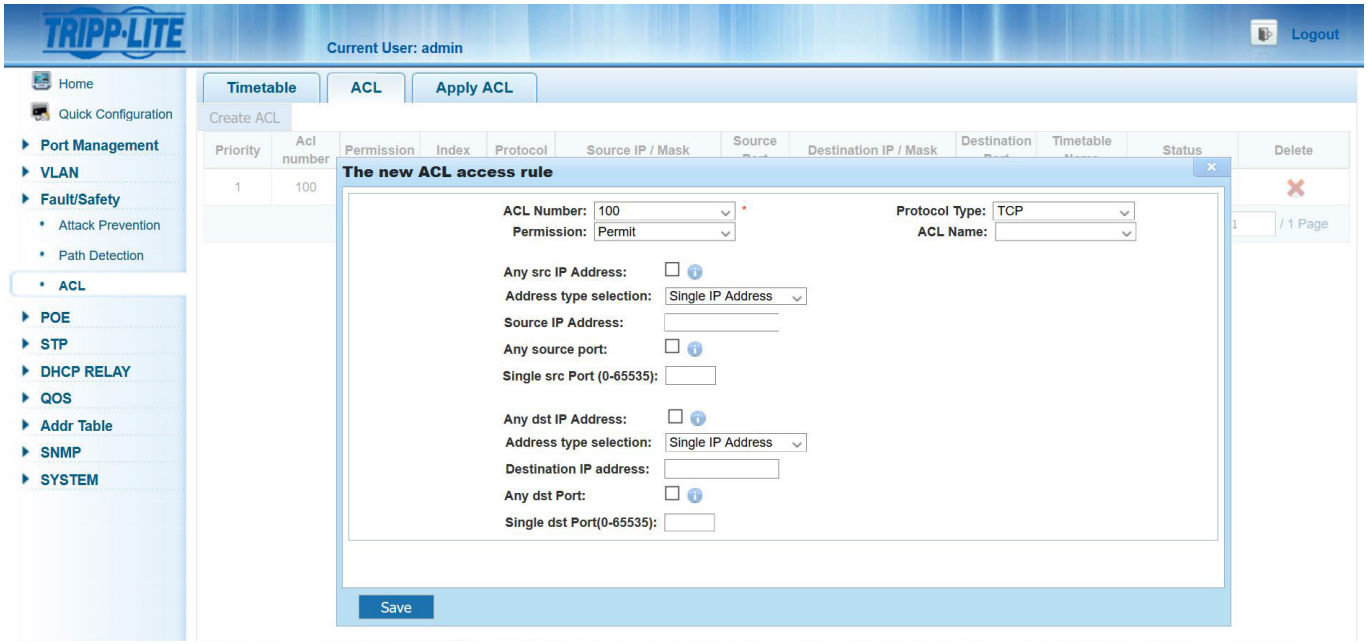


Figure 7.19 : Créer une règle d'accès de la LCA

8. PoE (alimentation électrique par câble Ethernet, prise en charge par certains modèles)

Alimentation électrique par câble Ethernet (PoE) (disponible sur certains commutateurs) fournit l'alimentation à plusieurs dispositifs munis de PoE et PoE+ et la communication avec eux. Chaque port est capable de prendre en charge jusqu'à 32 W d'alimentation électrique par câble Ethernet (PoE). La tension maximale fournie par le système d'alimentation électrique par câble Ethernet (PoE) est 51,2 V.

8.1 Configuration de la gestion de l'alimentation électrique par câble Ethernet (PoE)

Sélectionner PoE (alimentation électrique par câble Ethernet) → PoE Config (configuration de l'alimentation électrique par câble Ethernet) → Management (gestion) → PoE Status Information (informations sur l'état de l'alimentation électrique par câble Ethernet) (Figure 8.1). Afficher les informations sur l'état de l'alimentation électrique par câble Ethernet (PoE) du commutateur de réseau liées à son fonctionnement, la puissance nominale totale, la limite de puissance actuelle, le seuil de l'alarme, la tension actuelle et le pourcentage de puissance de réserve disponible.

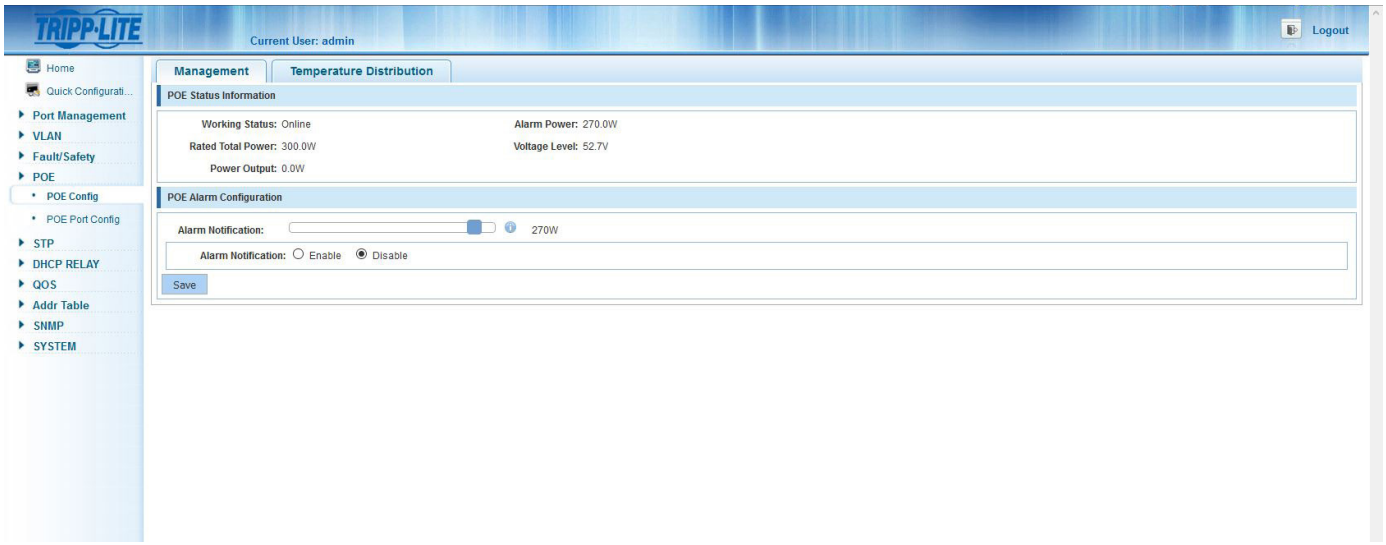


Figure 8.1 : Gestion de l'alimentation électrique par câble Ethernet (PoE)

8.1.1 Seuil d'alarme de la consommation d'alimentation électrique par câble Ethernet (PoE)

Sélectionner PoE (alimentation électrique par câble Ethernet) → PoE Config (configuration de l'alimentation électrique par câble Ethernet) → Management (gestion) → PoE Alarm Configuration (configuration de l'alarme de l'alimentation électrique par câble Ethernet) (Figure 8.2). Cette fonction configure le seuil de la puissance totale pour déclencher un avis de déroutement si le niveau de puissance de l'alimentation électrique par câble Ethernet (PoE) est excédé. Utiliser la glissière de l'alimentation Reserve (réserve) pour ajuster combien d'alimentation de réserve allouer à l'utilisation future d'applications. Une fois les seuils de l'alarme et de la réserve configurés, cliquer sur « Save » (sauvegarder).

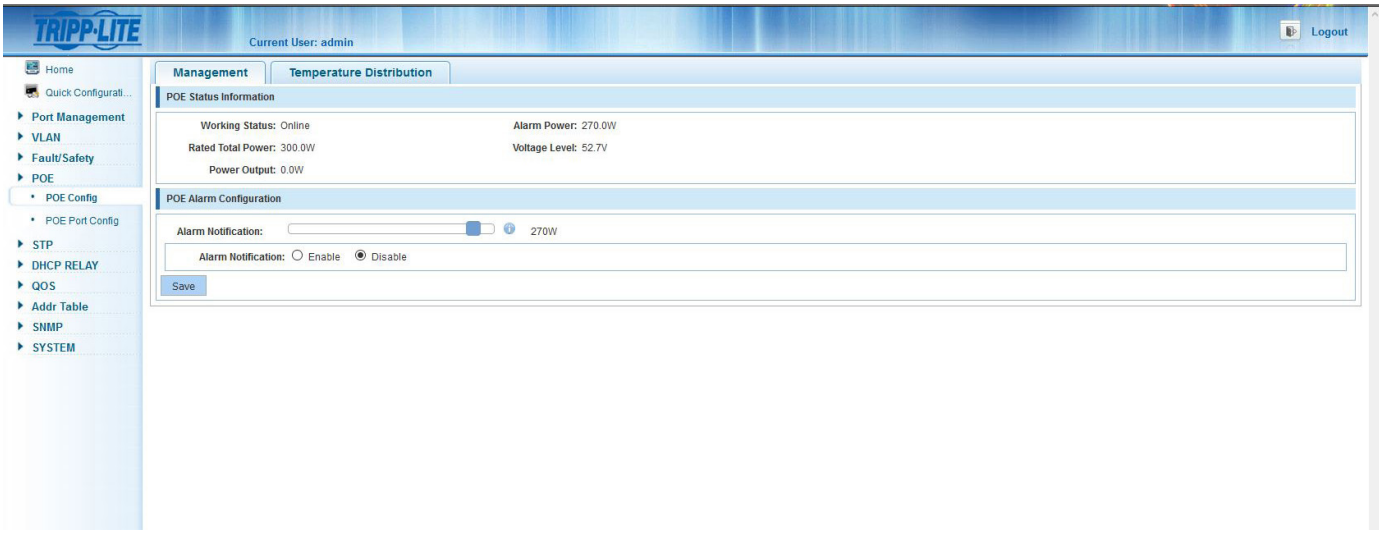


Figure 8.2 : Configuration de l'alarme de l'alimentation électrique par câble Ethernet (PoE)

8. PoE (alimentation électrique par câble Ethernet, prise en charge par certains modèles)

8.1.2 Distribution de la température de l'alimentation électrique par câble Ethernet (PoE)/ seuils d'alarme

Configure le seuil de température de l'alarme pour chacun des trois jeux de puces de l'alimentation électrique par câble Ethernet (PoE). La plage de l'alarme de température est 70 à 149 °C (158 à 300 °F).

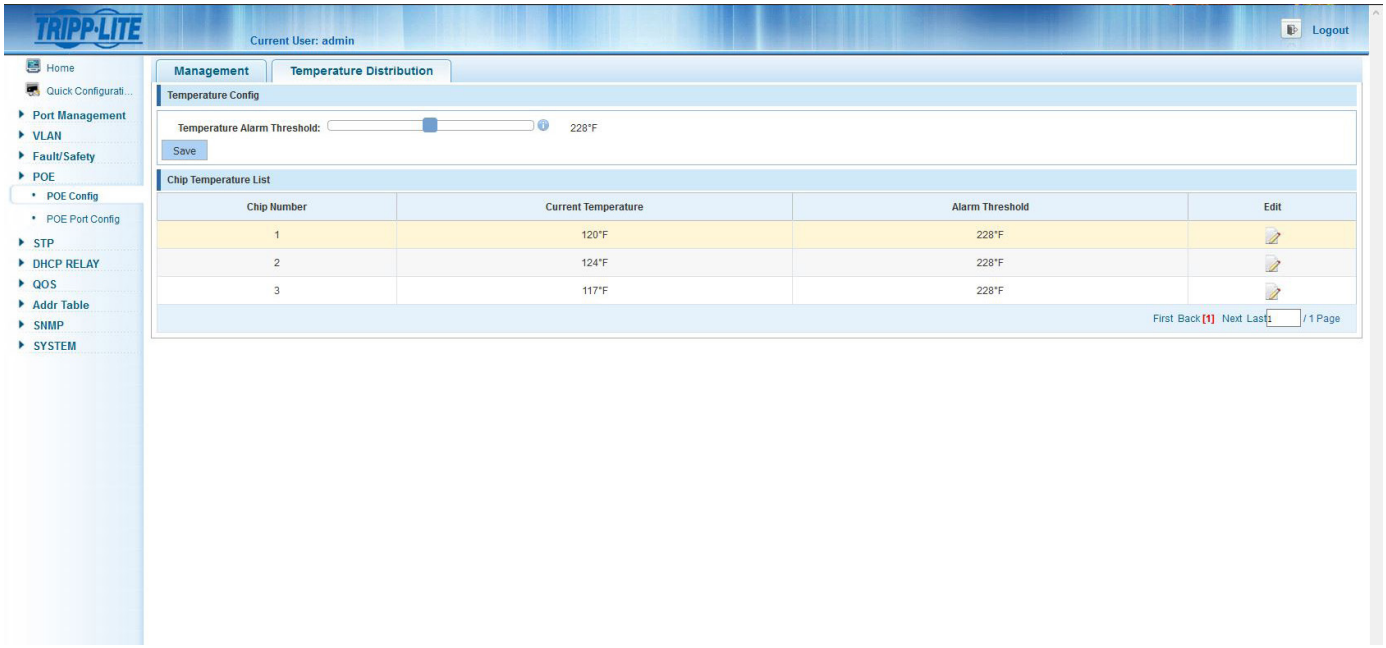


Figure 8.3 : Distribution de la température de l'alimentation électrique par câble Ethernet (PoE)

8.2 Configuration des ports de l'alimentation électrique par câble Ethernet (PoE)

Sélectionner PoE (alimentation électrique par câble Ethernet) → PoE Port Config (configuration des ports de l'alimentation électrique par câble Ethernet) (Figure 8.4). Ajuste les capacités de l'alimentation électrique par câble Ethernet (PoE) de chaque port. Cliquer sur l'icône Edit (modifier) pour activer ou désactiver l'alimentation électrique par câble Ethernet), modifier l'utilisation de puissance maximale, configurer la priorité et configurer le mode de détection AF, AT, AT&F pour les dispositifs connectés.

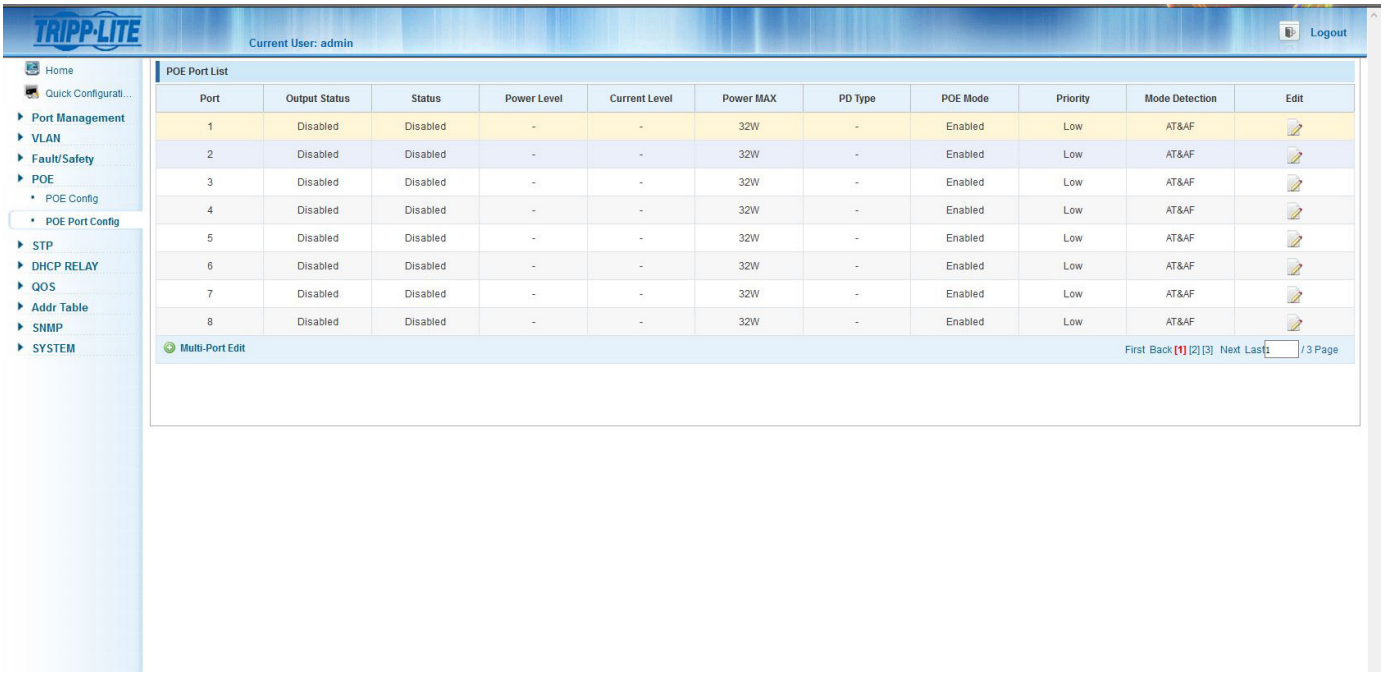


Figure 8.4 Configuration des ports de l'alimentation électrique par câble Ethernet (PoE)

9. Gestion du protocole Multiple Spanning Tree (MSTP)

La gestion du protocole Multiple Spanning Tree fournit une topologie logique exempte de boucle pour les réseaux Ethernet. Le MSTP empêche les boucles au niveau du pont et les afflux de diffusion générale qui en résultent. La redondance de lien est une autre fonction de MSTP pour assurer que les connexions du réseau ont un chemin redondant dans l'éventualité de la défaillance d'un lien actif.

9.1 Configuration de la région MSTP

Sélectionner STP → MSTP Region (région MSTP) pour créer des instances MSTP (Figure 9.1).

9.1.1 Configuration MSTP

Saisir le nom de la région et le niveau de révision de l'instance MSTP.

9.1.2 Mappage des instances

Choisir un numéro d'identification d'instance entre 1 et 16 et les réseaux locaux virtuels associés auxquels elle sera attribuée. (L'instance 0 est attribuée par défaut à tous les réseaux locaux virtuels.)

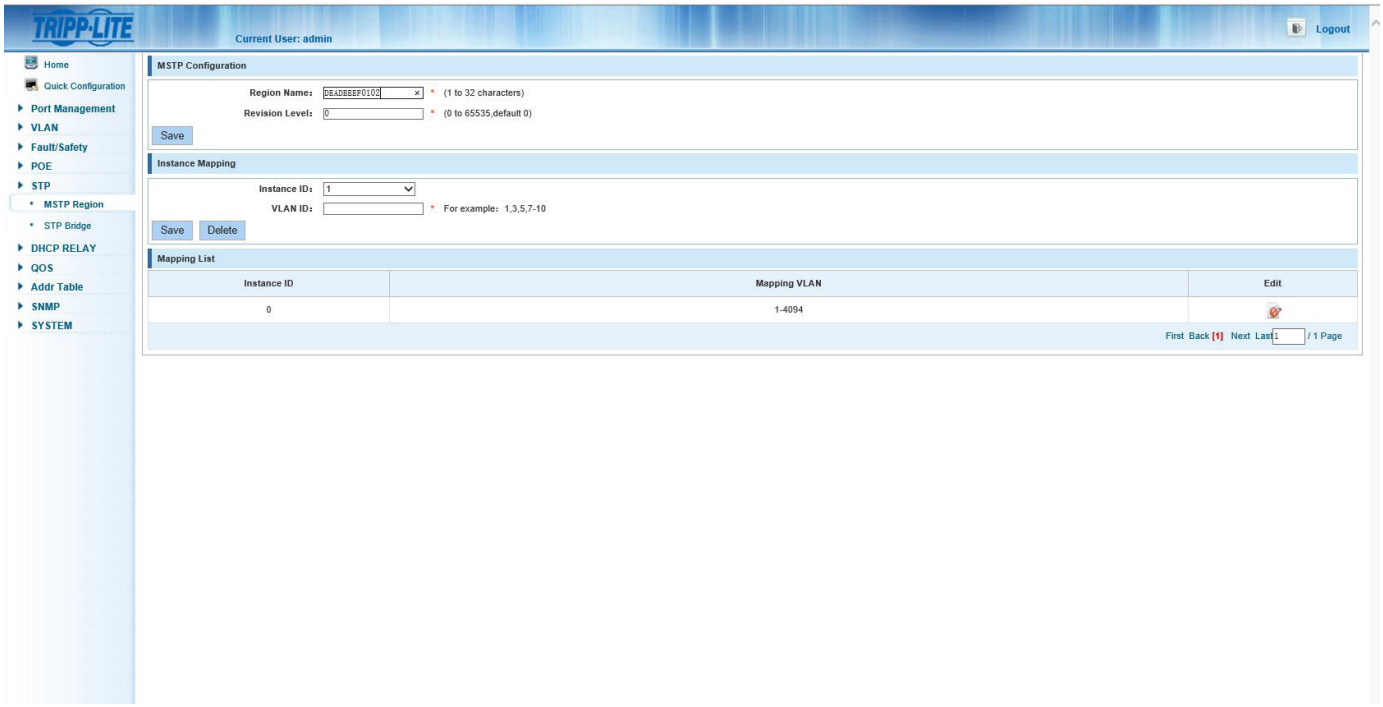


Figure 9.1 : Configuration MSTP et mappage des instances

9.1.3 Liste des mappages

La liste des mappages est une liste de toutes les instances des régions MSTP créées. Seules les instances qui ont été créées peuvent être modifiées ou supprimées. Lorsqu'une instance est supprimée, le réseau local virtuel associé revient au niveau d'identification d'instance par défaut de 0.

9. Gestion du protocole Multiple Spanning Tree (MSTP)

9.2 Configuration du pont Spanning Tree Protocol (STP)

Sélectionner STP → STP Bridge Config (configuration du pont STP) (Figure 9.2) et suivre les étapes suivantes :

1. Activer la priorité des instances en cliquant sur la case à cocher.
2. Sélectionner un numéro d'instance entre 0 et 16.
3. Sélectionner la priorité entre 0 et 61 440 (par défaut : 32 768).
4. Activer le pont STP en sélectionnant ON (activé), saisir Hello Time entre 1 et 10 secondes (par défaut : 2 sec.), Forward Delay entre 4 et 30 secondes (par défaut : 10 sec.), définir le mode de STP, RSTP, MSTP; MAX Age entre 6 et 40 sec. (par défaut 10 sec.) et Max Hops entre 1 et 40 secondes (par défaut : 10 sec.). Cliquer sur « Save » (sauvegarder).
5. « Show Bridge Info » affiche des informations sur le pont STP actuel configuré (Figure 9.3).

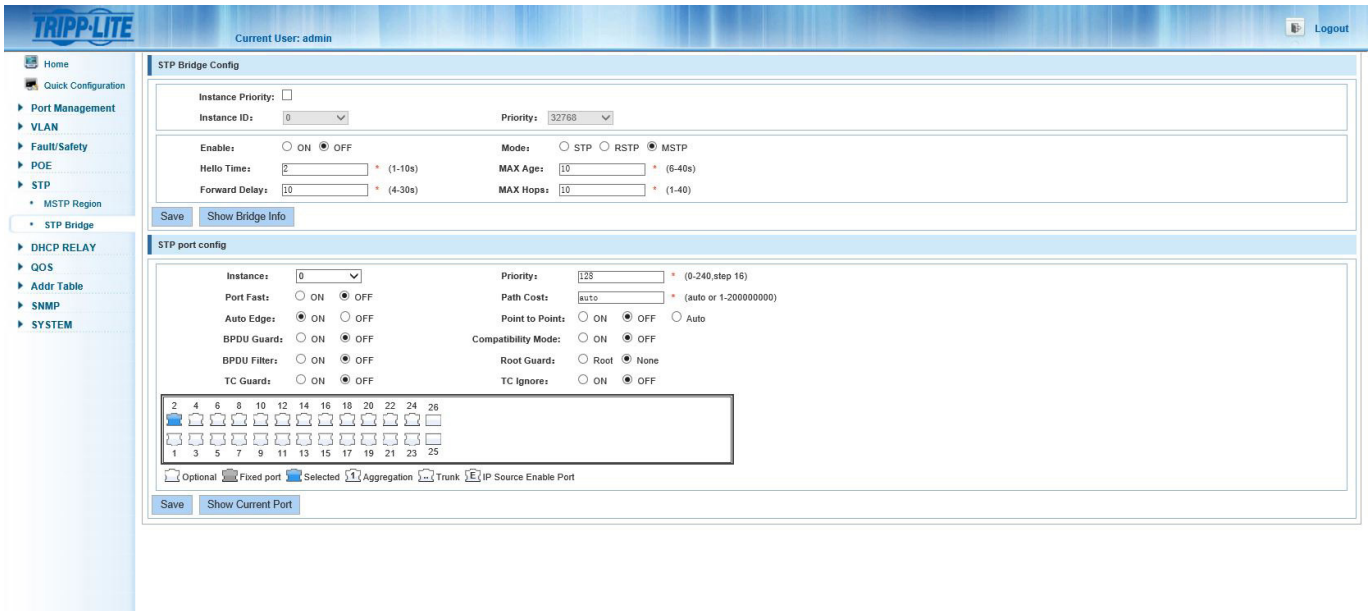


Figure 9.2 : Configuration du pont STP et configuration du port STP

Figure 9.3 : Informations sur le pont STP

9. Gestion du protocole Multiple Spanning Tree (MSTP)

9.3 Configuration du port STP

Suivre les étapes ci-dessous pour configurer le port STP :

1. Sélectionner le numéro d'identification du pont d'instance qui a été créé ci-dessus.
2. Sélectionner Port Fast (par défaut : OFF (désactivé)).
3. Sélectionner Auto Edge (par défaut : ON (activé)).
4. Sélectionner BPDU Guard (par défaut : OFF (désactivé)).
5. Sélectionner BPDU Filter (par défaut : OFF (désactivé)).
6. Sélectionner TC Guard (par défaut : OFF (désactivé)).
7. Sélectionner la priorité entre 0 et 240; la valeur doit être saisie en multiples de 16 (par défaut : 128).
8. Sélectionner Path COS à Auto ou 1 à 200 000 000 (par défaut : Auto).
9. Configurer Point to Point à ON (activé), OFF (désactivé) ou AUTO (par défaut : OFF (désactivé)).
10. Configurer Compatibility Mode (mode de compatibilité) (par défaut : OFF (désactivé)).
11. Configurer Root Guard à Root ou None (aucun) (par défaut : None (aucun)).
12. Configurer TC Ignore (par défaut : OFF (désactivé)).
13. Cliquer sur « Save » (sauvegarder).
14. Cliquer sur Show Current Port (afficher le port actuel) pour afficher les informations sur le port STP actuel.

Figure 9.4 : Informations sur le port STP actuel

10. Relais DHCP

Le relais DHCP envoie des messages DHCP entre les clients DHCP et les serveurs DHCP sur différents réseaux IP. À cet endroit, les paramètres du relais et d'Option82 peuvent être modifiés.

10.1 Configuration de l'agent du relais DHCP

Sélectionner DHCP RELAY (relais DHCP) → DHCP Relay (relais DHCP) (Figure 10.1). Cliquer sur la case à cocher pour activer le relais DHCP. Par défaut, « DHCP Option Trust Field » est déjà activé.

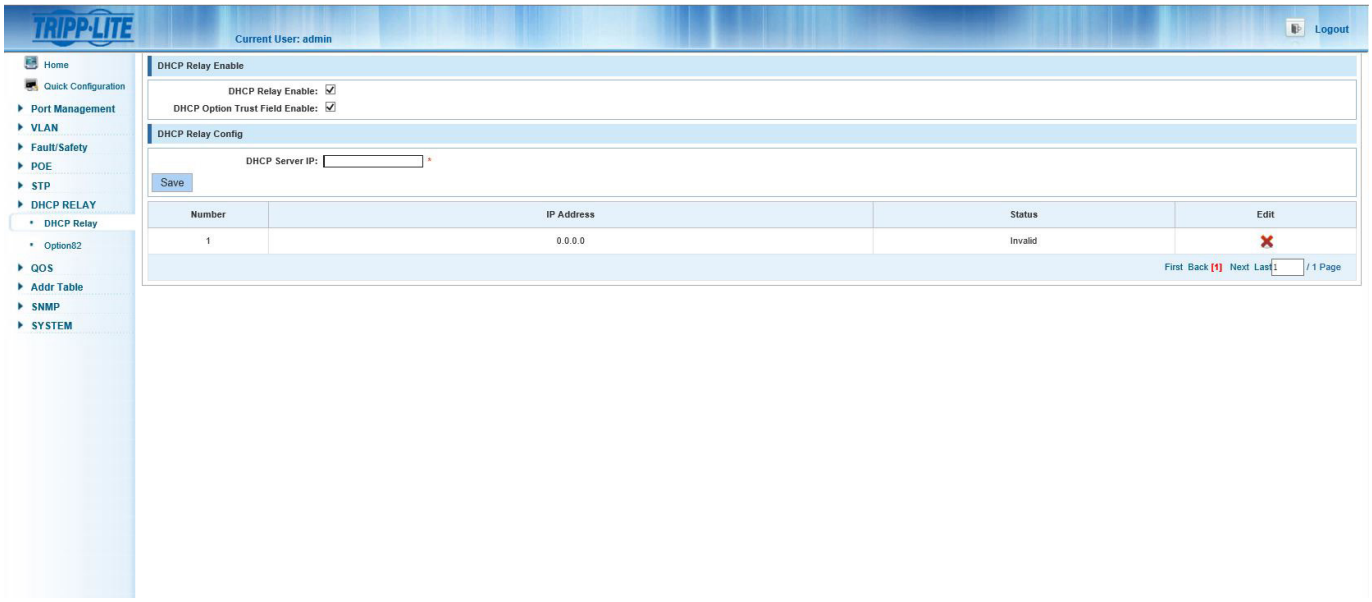


Figure 10.1 : Relais DHCP activé

10.2 Configuration de l'Option82

Sélectionner DHCP RELAY (relais DHCP) → Option82. Dans la configuration Option82 (Figure 10.2), saisir les informations suivantes :

10.2.1 Contrôle du circuit

Saisir le numéro d'identification du contrôle du circuit entre 3 et 63 et le numéro d'identification du réseau local virtuel. Cliquer sur « Save » (sauvegarder) et chaque instance sera sauvegardée sur une liste.

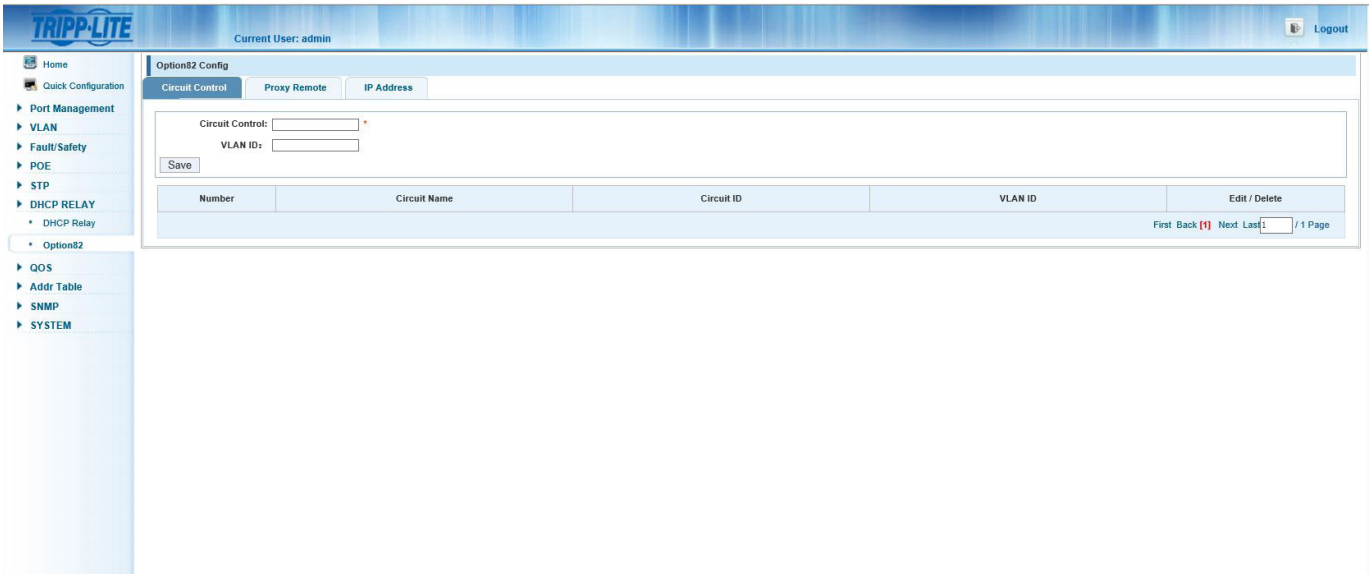


Figure 10.2 : Contrôle du circuit l'Option82

10.2.2 Télécommande Proxy

Saisir la télécommande Proxy Remote (limite : 63 caractères) et le numéro d'identification du réseau local virtuel (Figure 10.3). Cliquer sur « Save » (sauvegarder) et chaque saisie sera sauvegardée sur la liste.

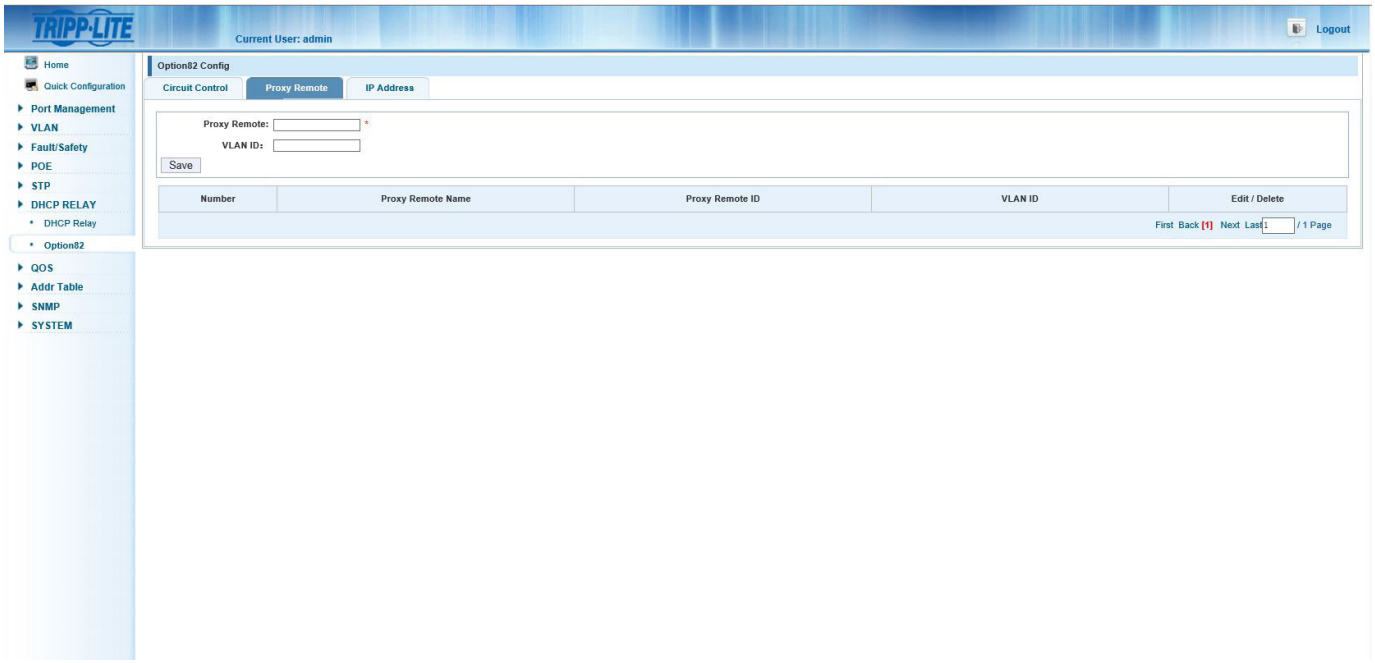


Figure 10.3 : Télécommande Proxy d'Option82

10.2.3 Adresse IP

Saisir l'adresse IP du serveur du relais DHCP et le numéro d'identification du réseau local virtuel associé (Figure 10.4). Cliquer sur « Save » (sauvegarder) et chaque instance sera sauvegardée sur la liste ci-dessous.

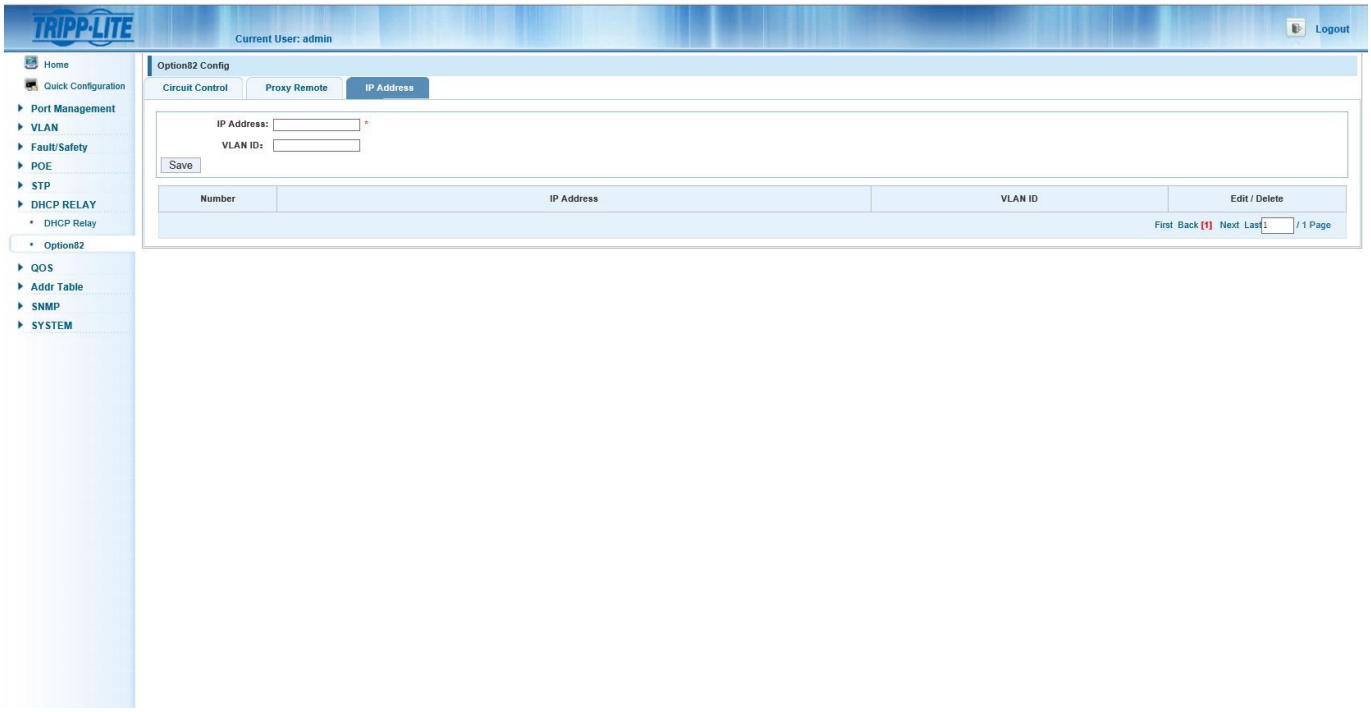


Figure 10.4 : Adresse IP Option82

11. Gestion de la qualité de service (QOS)

La qualité de service s'assure que le trafic le plus important du réseau (p. ex. VoIP, caméras IP) circule à travers le commutateur avec le moins d'interruptions possible de la transmission de ses données. Pour permettre à l'appareil pouvant fonctionner en réseau une priorité de transmission plus élevée, la QOS doit être configurée sur le commutateur. Elle est désactivée par défaut. Suivre les étapes ci-dessous pour configurer le port pour le trafic de l'appareil qui nécessite la QOS.

11.1 Remarque sur la QOS

Sélectionner QoS → Remark (remarque sur la QOS). Sous la section QoS Multi-Label (multilabel QOS), il est possible de configurer Rule Index (indice de règle), Operation Type (type de fonctionnement), Value Type (type de valeur), Value (valeur), Service Class Mapping (mappage de la catégorie de service) ou Priority Remark (remarque sur la priorité) pour un ou plusieurs ports (Figure 11.1). Pour appliquer la règle à un port ou un ensemble de ports, cliquer sur « Save » (sauvegarder). Pour rejeter la configuration, cliquer sur « Cancel » (annuler). La case ci-dessous affiche les paramètres pour chaque règle QOS :

Multilabel QOS	Paramètres	Remarques
Indice de règle	1-32	
Type d'opération	Égal; correspond toujours	
Type de valeur	DST Mac SRC Mac Priorité Ethernet Numéro du réseau local virtuel Type d'Ethernet IP de destination IP de source Type d'IP IPv4 Diff IPv6 Priorité Port SRC, couche 4 Port DST, couche 4	
Valeurs	DST MAC – 00:00:00:00:00:00 SRC MAC – 00:00:00:00:00:00 Priorité Ethernet – 0~7 Numéro du réseau local virtuel – 1~4 094 Type d'Ethernet – 0~0xFFFF IP de destination – 0.0.0.0 IP de source – 0.0.0.0 Type d'IP – 0~0xFF IPv4 Diff – 0~63 IPv6 Priorité – 0~255 Port SRC, couche 4 – 0~65 535 Layer 4 DST Port – 0~65 535	Les options des valeurs changent en fonction du type de valeur sélectionné. Les valeurs sont toujours obligatoires.
Configuration du port	Appliquer la règle à un ou plusieurs ports en sélectionnant un port individuel, en sélectionnant All (tout) ou en sélectionnant All others (tous les autres).	Il est aussi possible de faire glisser le curseur pour sélectionner plusieurs ports.
Sauvegarder la configuration	Cliquer sur « Save » pour appliquer la règle ou sur Cancel (annuler) pour rejeter les modifications.	

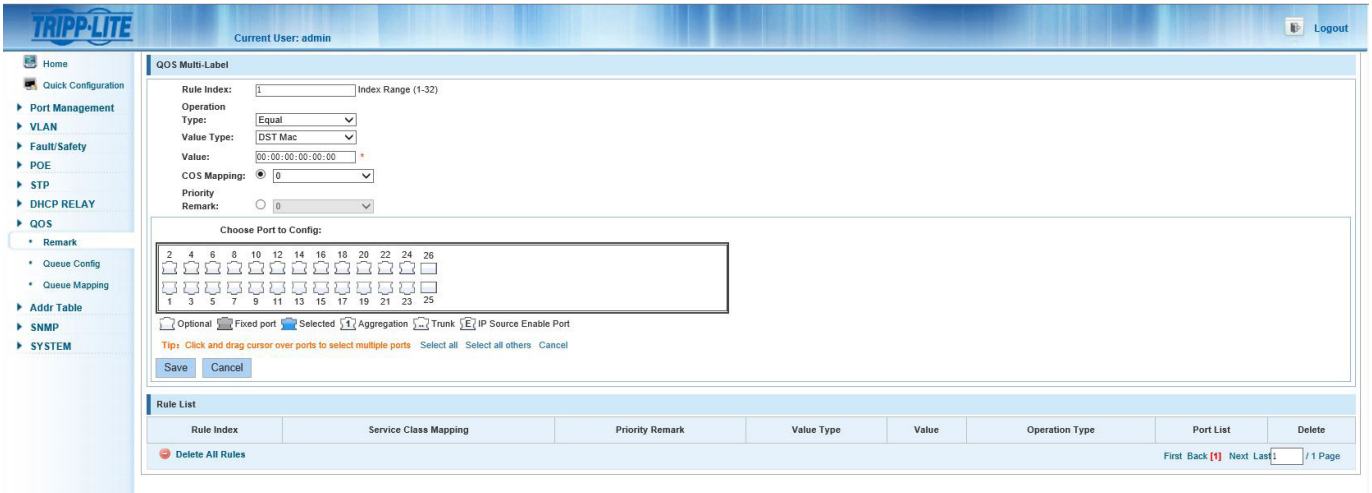


Figure 11.1 : Aperçu des remarques QOS

11. Gestion de la qualité de service (QOS)

11.1.1 Liste des règles

La liste des règles affiche les informations sur toutes les règles qui ont été configurées ci-dessus. Supprimer une seule règle ou supprimer toutes les règles si nécessaire.

11.2 Configuration de la file d'attente de la QOS

Sélectionner QoS → Queue Config (configuration de la file d'attente de la QOS) pour configurer le mode de la file d'attente. Les options disponibles sont les suivantes :

Queue Mode Scheduling Options (options de la planification du mode de file d'attente)	Description
SP	Planification de la priorité absolue
RR	Planification circulaire
WRR	Planification circulaire pondérée
WFQ	Planification pondérée équitable
Poids des octets WRR et WFQ	Configurer le poids des octets entre 0 et 127 pour chaque file d'attente de façon à ce qu'ils soient proportionnels pour occuper la largeur de bande pour envoyer les données.

11.3 Mappage de la file d'attente de la QOS

Le mappage de la file d'attente gère la transmission des messages de données vers une file d'attente des travaux en sortie d'un port. Les messages dans les différentes files d'attente des travaux en sortie comprendront des politiques sur le service de transmission de différents niveaux et de différentes qualités. Chaque port a 8 files d'attente des travaux en sortie, 1-7. La carte de de la file d'attente de la catégorie de service et la carte DSCP vers COS doivent être configurées sur le commutateur pour convertir la valeur du DSCP du message en un nombre de la file d'attente des travaux en sortie pour déterminer dans quelle file d'attente des travaux de sortie transférer les messages.

11.3.1 Paramètres de la carte de la file d'attente COS

Configurer chacune des 8 files d'attente des travaux en sortie en fonction de la catégorie de service (GOS) requise pour les transmissions des messages de données (Figure 11.2).

Mappage de la catégorie de service	Description
0	Meilleur effort
1	Catégorie 1
2	Catégorie 2
3	Catégorie 3
4	Catégorie 4
5	Réacheminement express
6	Reste le même (acheminement IP)
7	Reste le même (la couche de liaison et l'acheminement demeurent actifs)

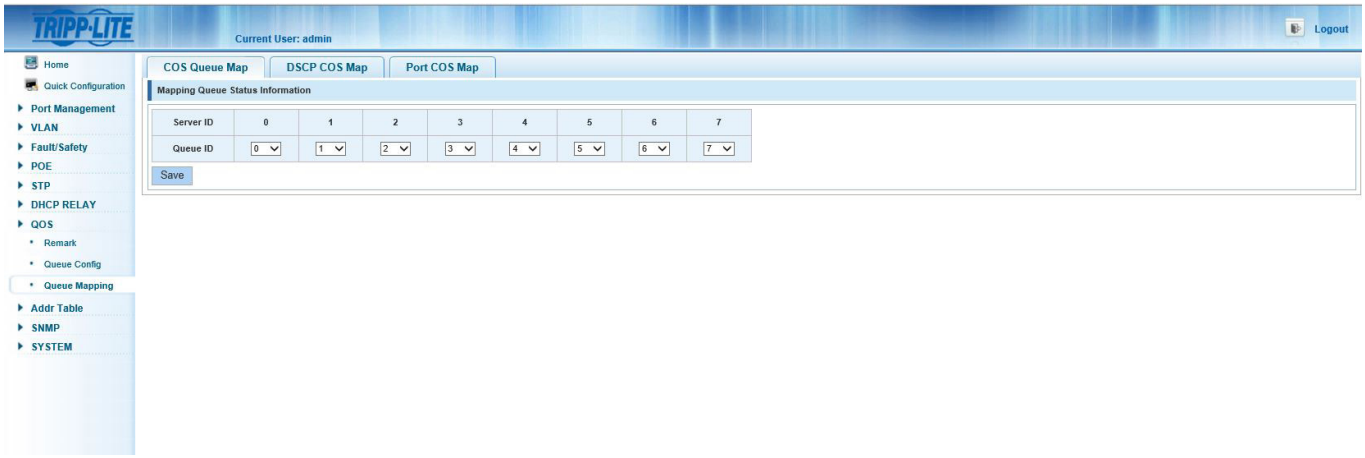


Figure 11.2 : Carte de la file d'attente COS

11. Gestion de la qualité de service (QOS)

11.3.2 Paramètres de la carte COD DSCP

Sélectionner COS → Queue Mapping (mappage COS) → DSCP COS Map (carte COS DSCP) – Configurer la liste de l'équipe de mappage du point de code du service différencié (DSCP) (Figure 11.3).

Liste des serveurs - Le champ DSCP comprend sept champs COS (0-63) divisés dans quatre tableaux.

Numéro d'identification de la file d'attente - Mappant les champs DSCP à COS (0 à 7), fondé sur le COSine étant mappé vers une file d'attente.

Remarque : *La priorité COS est supérieure à DSCP, et la priorité DSCP est supérieure au port.*

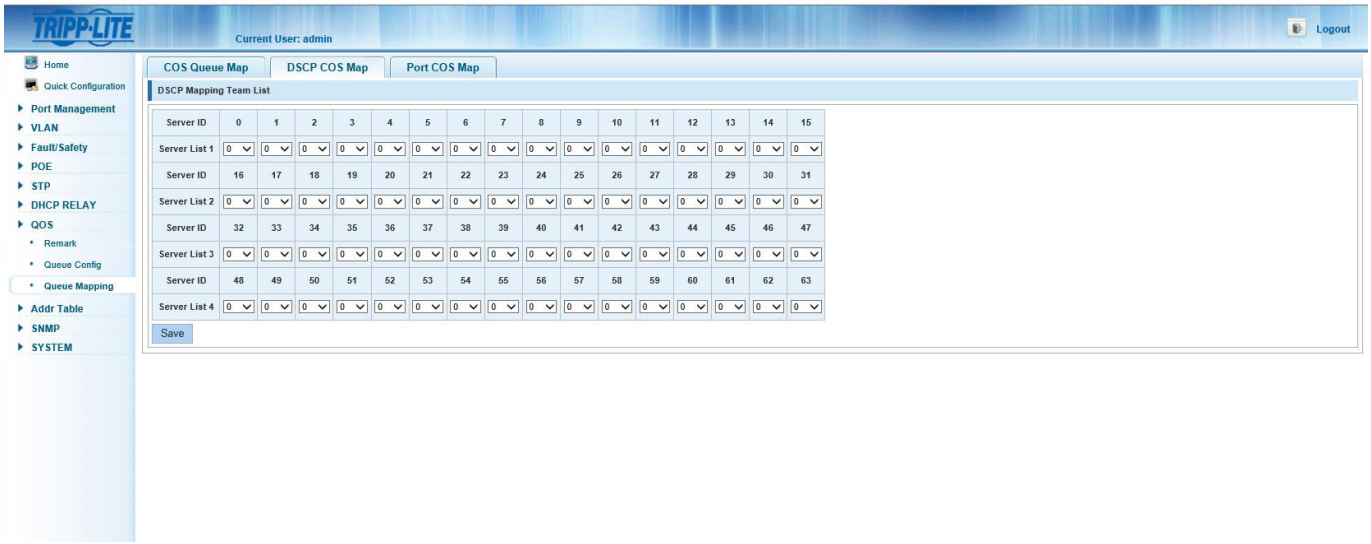


Figure 11.3 : Carte COS DSCP

11.3.3 Paramètres de la carte COS du port

Sélectionner COS → Queue Mapping (mappage de la file d'attente) → Port COS Map (carte COS du port) (Figure 11.4) pour configurer le port pour la carte de la catégorie de service.

Sélectionner le port.

Sélectionner le numéro d'identification du serveur COS entre 0 et 7 (tous les ports sont configurés à COS 0 par défaut).

Cliquer sur « Save » pour appliquer les paramètres. Les paramètres sauvegardés seront affichés dans la liste de contrôle avec le symbole « T » entre le numéro du port et le numéro d'identification du serveur.

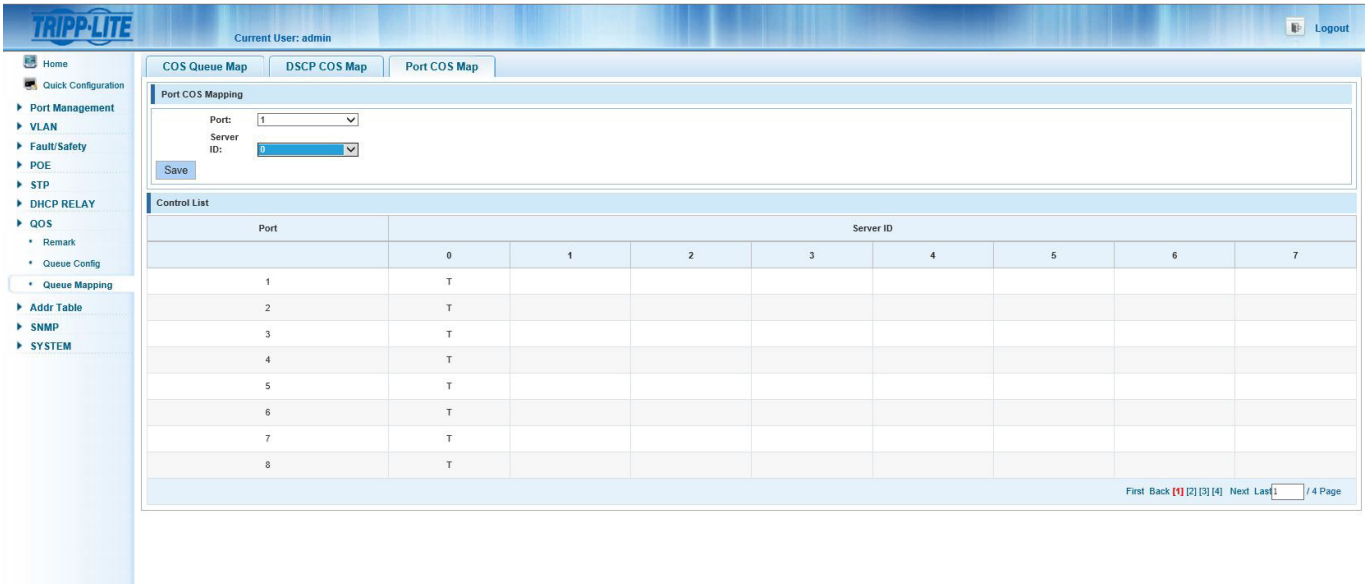


Figure 11.4 : Carte COS du port

12. Gestion de la liste d'accès au tableau d'adresses MAC

Le tableau des listes de contrôle d'accès aux adresses MAC (Figure 12.1) permet à un utilisateur d'ajouter et de supprimer des adresses MAC, de configurer l'apprentissage et le vieillissement d'adresse MAC et le filtrage par adresse MAC.

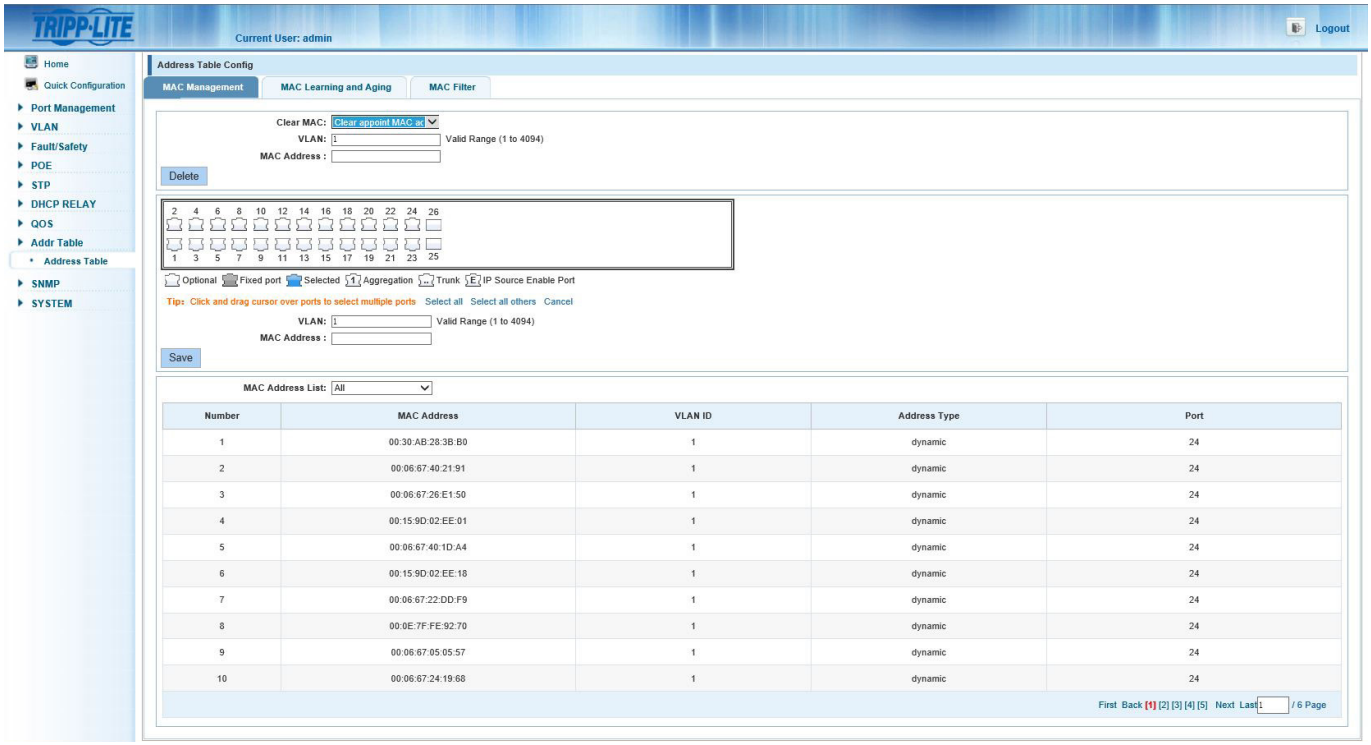


Figure 12.1 : Aperçu de la gestion d'adresses MAC

12. Gestion de la liste d'accès au tableau d'adresses MAC

12.1 Gestion d'adresses MAC

Sur l'écran MAC Management (gestion d'adresses MAC), il est possible d'ajouter et de supprimer des éléments du tableau des adresses MAC (Figure 12.2).

12.1.1 Afficher la liste d'adresses MAC

Afficher la liste complète des adresses MAC en plus du réseau local virtuel auquel chacune d'entre elles est associée et les ports auxquels elle a accès pour communiquer. Utiliser le filtre d'affichage pour afficher toutes les adresses MAC, les adresses MAC dynamiques ou les adresses MAC statiques sur la liste (Figure 12.2).

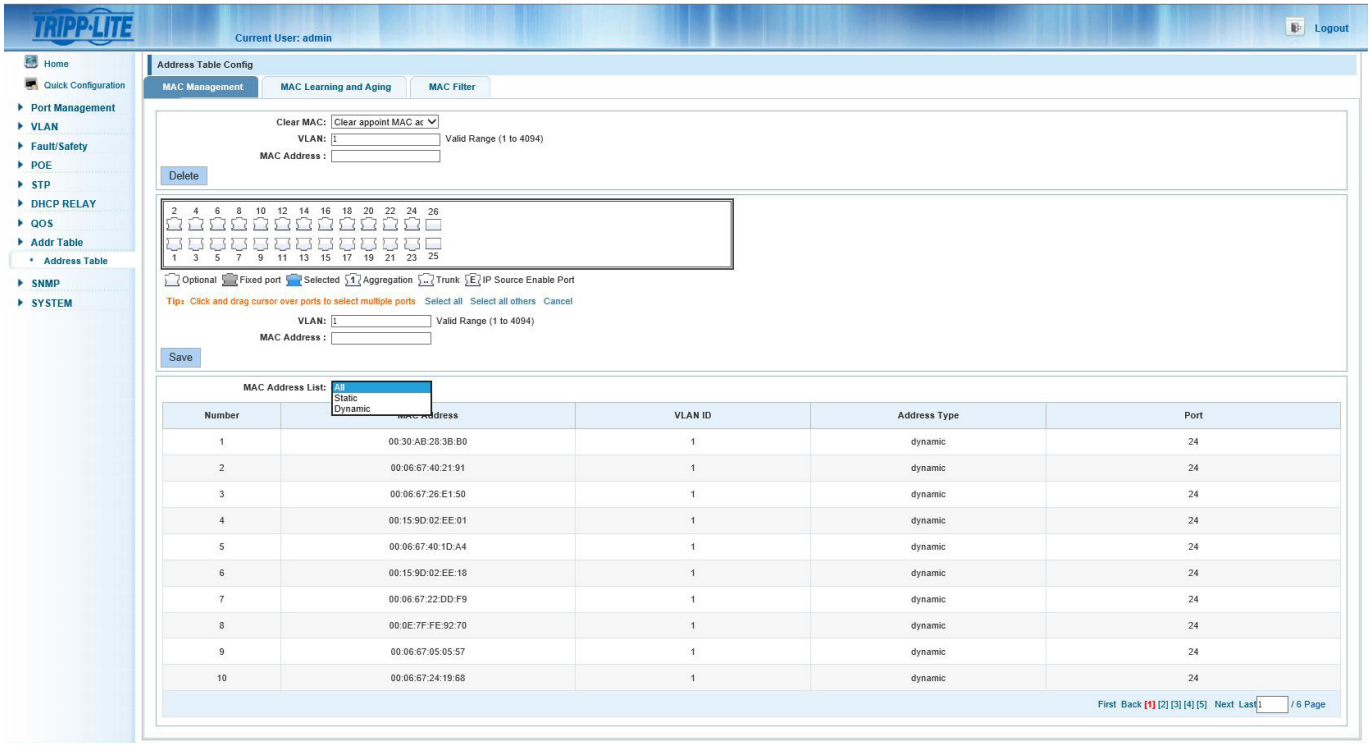


Figure 12.2 : Filtres de la liste d'adresses MAC

12.1.2 Ajouter une adresse MAC

Pour ajouter un tableau d'adresses MAC statiques à la liste d'adresses MAC (Figure 12.3), suivre les étapes suivantes :

1. Sélectionner le ou les ports auxquels l'adresse MAC devrait pouvoir accéder.
2. Saisir le numéro d'identification du réseau local virtuel par le biais duquel l'adresse MAC communiquera.
3. Saisir l'adresse MAC statique à ajouter.
4. Cliquer sur le bouton « Save » pour ajouter l'adresse MAC à la liste d'adresses MAC.

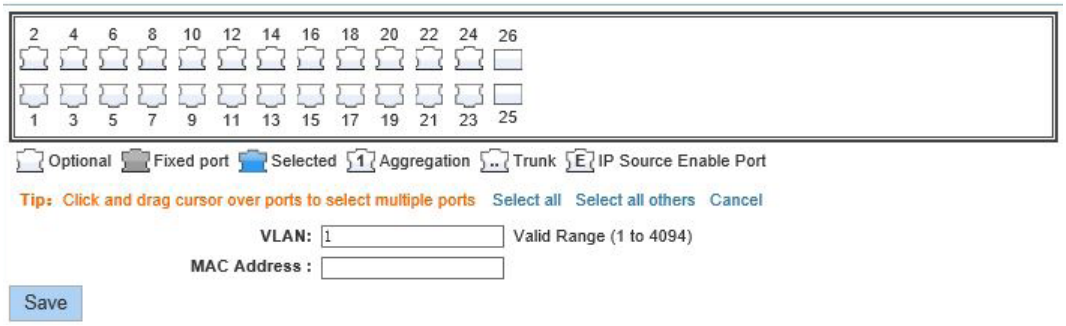


Figure 12.3 : Ajouter des adresses MAC

12. Gestion de la liste d'accès au tableau d'adresses MAC

12.1.3 Supprimer une adresse MAC

L'ensemble de fonctions suivant peut être utilisé pour supprimer une seule adresse MAC d'un réseau local virtuel associé ou pour supprimer la liste complète.

Fonctions de la gestion d'adresses MAC	Description
Supprimer une adresse MAC	Options : supprimer une adresse MAC attitrée, supprimer une adresse dynamique d'envoi individuel, supprimer une adresse statique d'envoi individuel ou supprimer toute la liste des adresses Mac.
Réseau local virtuel	Saisir le numéro d'identification du réseau local virtuel pour supprimer l'adresse MAC de (plage des numéros d'identification valides : 1 à 4 094).
Adresse MAC	Saisir l'adresse MAC spécifique à supprimer.

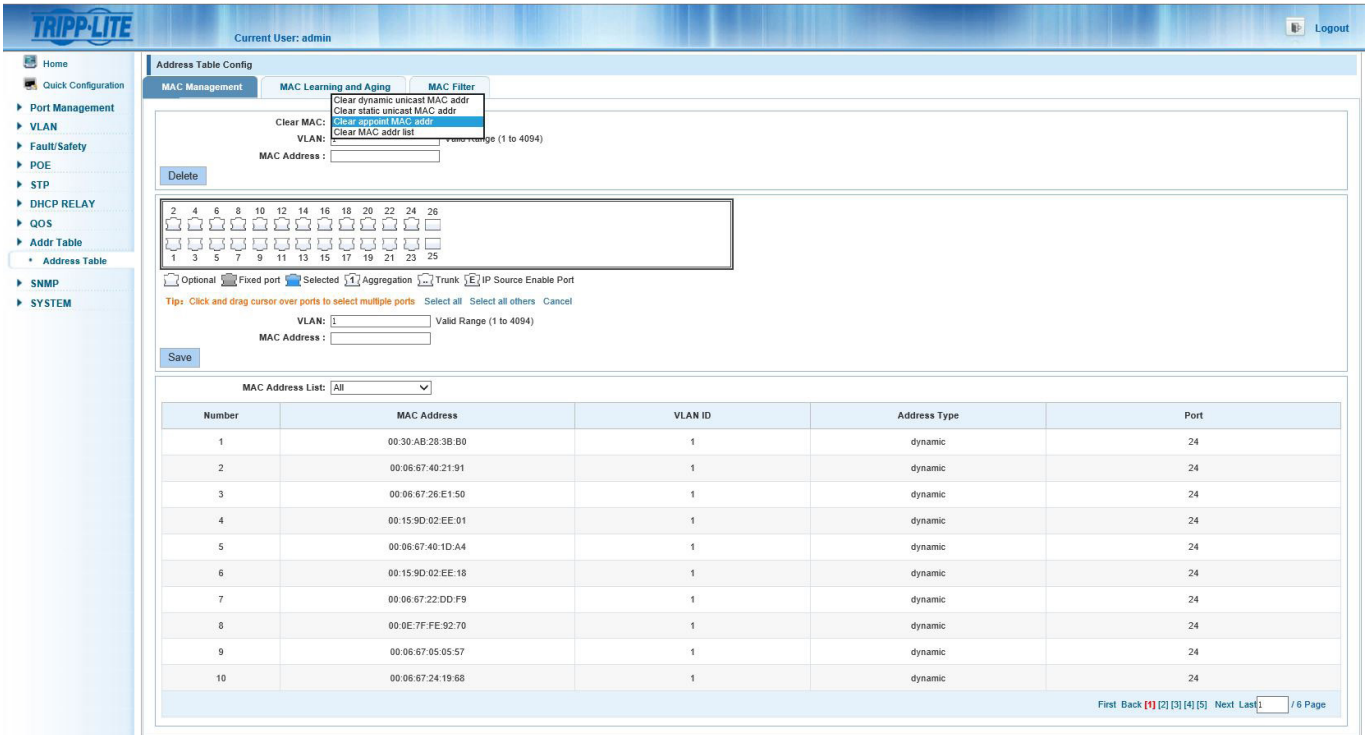


Figure 12.4 : Supprimer des adresses MAC

12. Gestion de la liste d'accès au tableau d'adresses MAC

12.2 Apprentissage et vieillissement d'adresses MAC

La limite d'apprentissage d'adresses MAC peut être configurée jusqu'à 8 191 adresses par part. La durée de vieillissement peut être configurée à 0 (aucun vieillissement) ou jusqu'à 1 000 000 secondes. (Consulter la Figure 12.5.)

12.2.1 Limite d'apprentissage d'adresses MAC

Pour modifier un seul port, sélectionner le numéro du port. Saisir ensuite la plage d'apprentissage entre 0 et 9 191 (8 191 est la plage d'apprentissage par défaut). Cliquer sur « Save » (sauvegarder) pour sauvegarder les paramètres. Pour configurer l'apprentissage sur plusieurs ports, cliquer et faire glisser le curseur sur plusieurs ports ou utiliser les options « Select All » (tout sélectionner) ou « Select all others » (sélectionner tous les autres) pour sélectionner les ports. Saisir la limite d'apprentissage d'adresses MAC pour les ports, jusqu'à 8 191 saisies. Cliquer sur « Save » pour sauvegarder les paramètres.

12.2.2 Durée de vieillissement des adresses MAC

La durée de vieillissement peut être configurée à 0 (aucun vieillissement) ou jusqu'à 1 000 000 secondes (le paramètre par défaut est 300 secondes). Cliquer sur « Save » pour sauvegarder les paramètres.

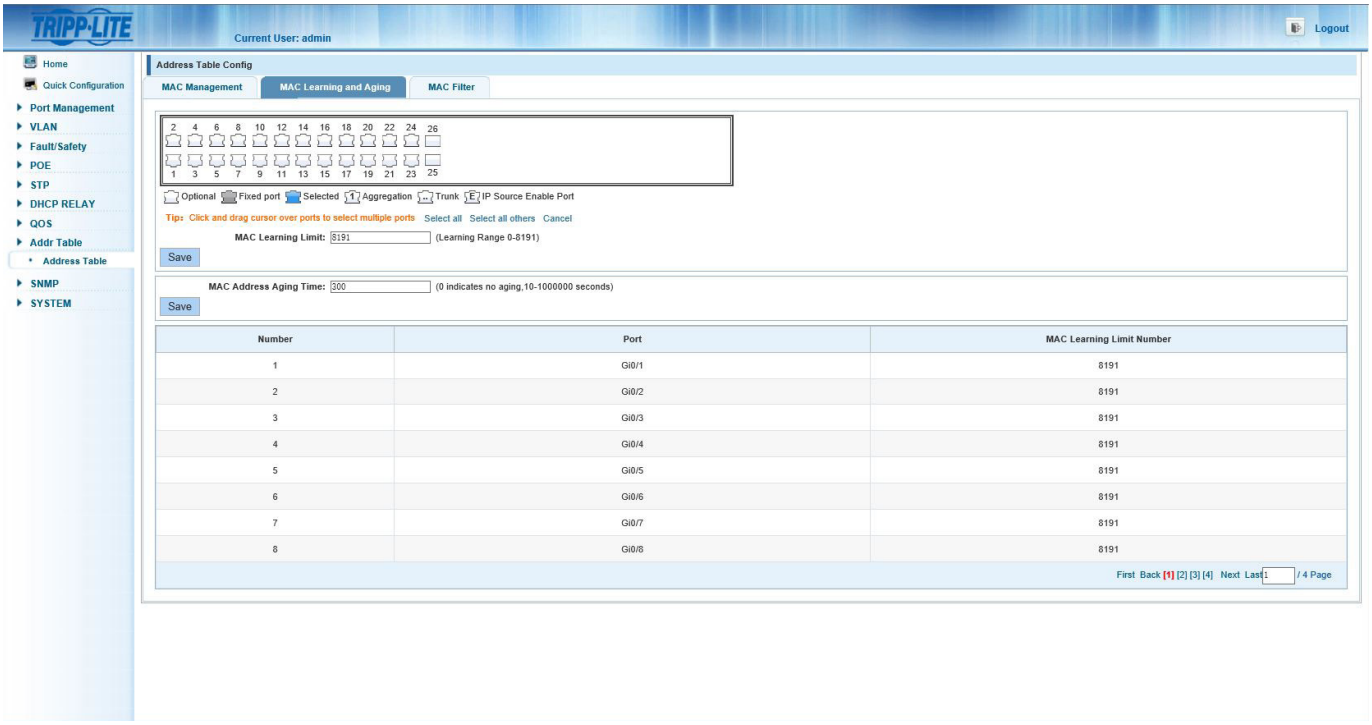


Figure 12.5 : Apprentissage et vieillissement des adresses MAC

12.3 Filtrage des adresses MAC

Pour s'assurer qu'une adresse MAC ne puisse pas accéder à la communication entrante ou sortante au moyen du commutateur, suivre les étapes suivantes :

1. Adresse MAC – Saisir l'adresse MAC à laquelle le filtrage sera appliqué.
2. Réseau local virtuel – Saisir le numéro d'identification du réseau local virtuel.
3. Direction du filtrage – Déterminer si le filtrage sera de la source, de la destination ou les deux.
4. Cliquer sur « Save » (sauvegarder) pour ajouter le filtre des adresses MAC à la liste.

Pour supprimer un filtre, cliquer sur l'icône ✖ à côté de la saisie de l'adresse MAC filtrée.

13. Gestion du protocole de gestion de réseau simple (SNMP)

Le protocole de gestion de réseau simple (SNMP) permet la surveillance et le contrôle à distance du commutateur. Il peut également envoyer des déroutements SNMP vers un service de récepteur de déroutement.

13.1 Paramètres de configuration SNMP

13.1.1 Activer/désactiver la configuration SNMP

Cette fonction est désactivée par défaut. Elle peut être activée en faisant basculer le commutateur d'activation/de désactivation. (Figure 13.1). Une fois activée, il est possible de configurer la communauté SNMP, le groupe, les utilisateurs et les paramètres des déroutements.

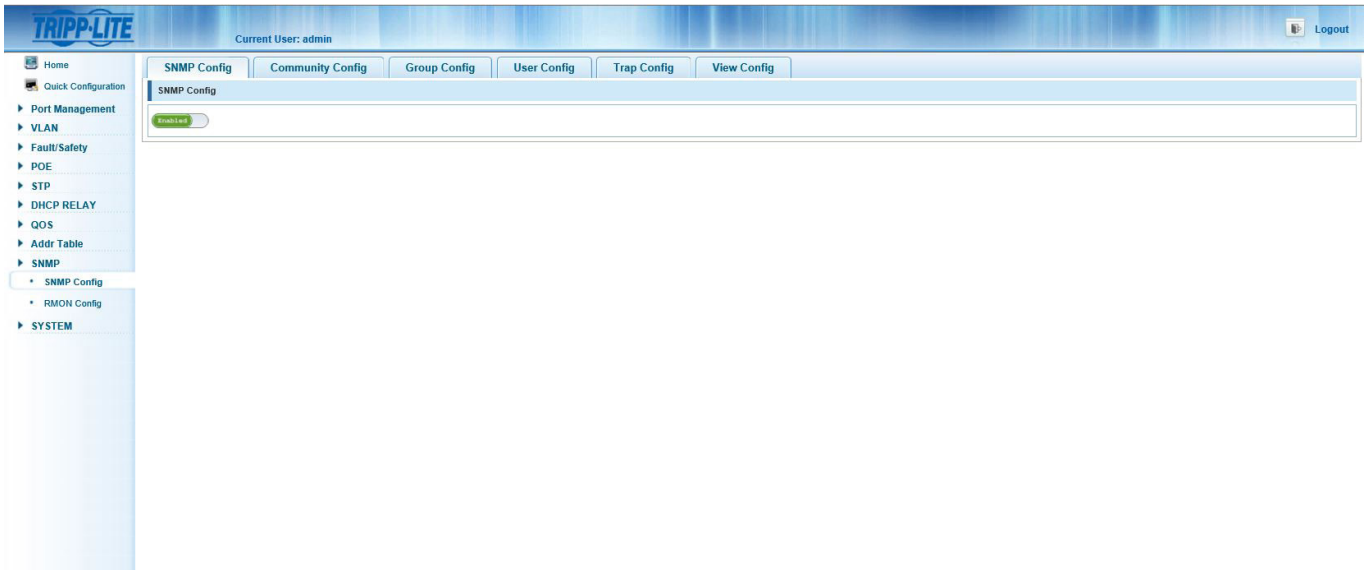


Figure 13.1 : Aperçu de la configuration SNMP

13.1.2 Configuration d'une communauté

Pour ajouter les chaînes communautaires SNMP prises en charge et leurs permissions, sélectionner SNMP → SNMP Config (configuration de SNMP) → Community Config (configuration de la communauté). Cliquer sur l'icône vert pour ajouter une nouvelle configuration de la communauté (Figure 13.2). Ajouter le nom de la communauté (limite : 16 caractères) et l'autorité d'accès « Read Write » (lecture-écriture) ou « Read Only » (lecture seule). Cliquer sur « Save » (sauvegarder pour sauvegarder les paramètres, cliquer sur « Exit » (quitter) pour rejeter les modifications.

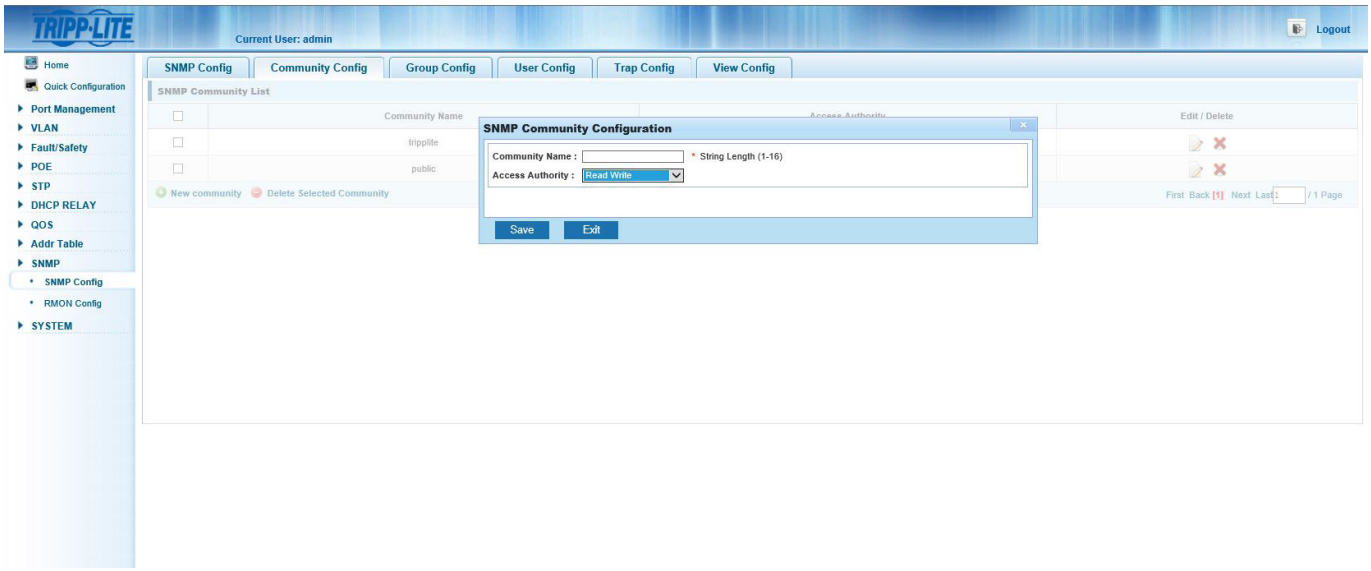


Figure 13.2 : Configuration de la communauté SNMP

13. Gestion du protocole de gestion de réseau simple (SNMP)

Pour modifier la configuration d'une communauté, sélectionner l'icône « Edit » (modifier), puis modifier le nom de la communauté ou l'autorité d'accès (Figure 13.3). Cliquer sur « Save » (sauvegarder) pour sauvegarder les paramètres, cliquer sur « Exit » (quitter) pour rejeter les modifications.

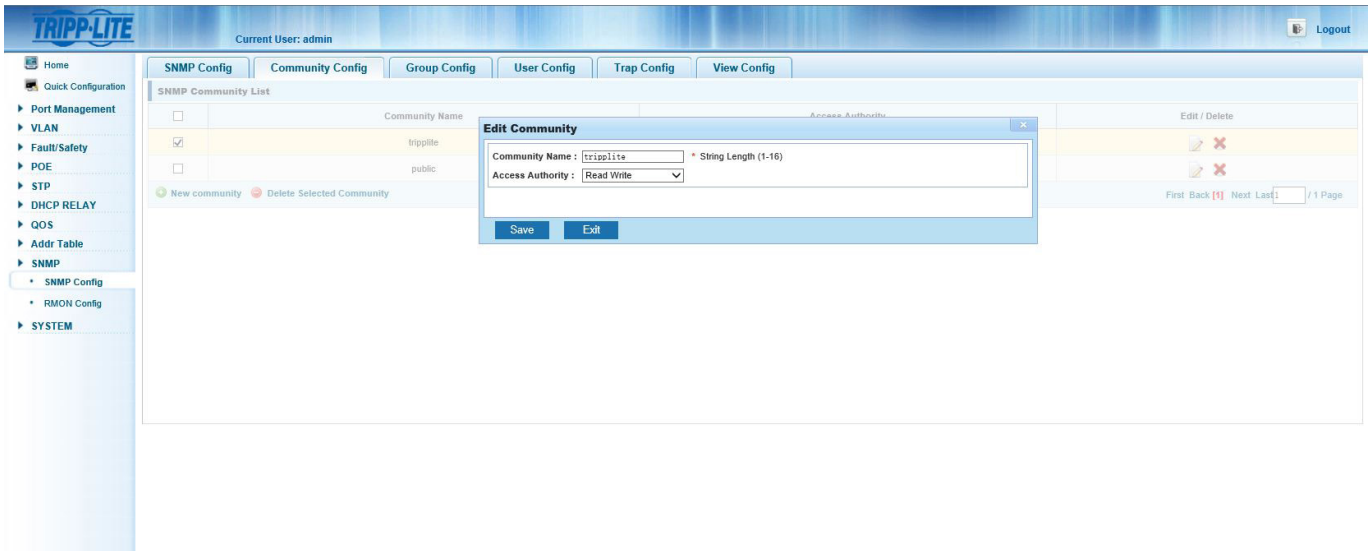


Figure 13.3 : Modifier la configuration de la communauté

Pour supprimer une configuration d'une communauté, cliquer sur l'icône rouge pour supprimer la saisie de la liste ou cliquer sur la case à cocher pour la chaîne communautaire à supprimer, puis cliquer sur « Delete Selected Community » (supprimer la communauté sélectionnée). Supprimer plusieurs chaînes communautaires en cliquant sur la case à cocher de chacune des chaînes à supprimer ou en cochant la case principale dans la partie supérieure de la liste pour sélectionner toutes les entrées. Une fois la sélection terminée, cliquer sur l'icône « Delete Selected Community » pour les supprimer de la liste.

Remarque : *Il est possible de configurer un total de 8 chaînes communautaires pour SNMP.*

13.1.3 Afficher la configuration SNMP

Sélectionner SNMP → SNMP Config (configuration SNMP) → View Config (afficher la configuration) (Figure 13.4) – Configurer les règles d'affichage et de gestion pour le MIB OID en créant les vues MIB qui peuvent ensuite être attribuées à un groupe SNMP. Configurer une nouvelle règle pour chaque affichage pour éviter de toucher à la fonction SNMP.

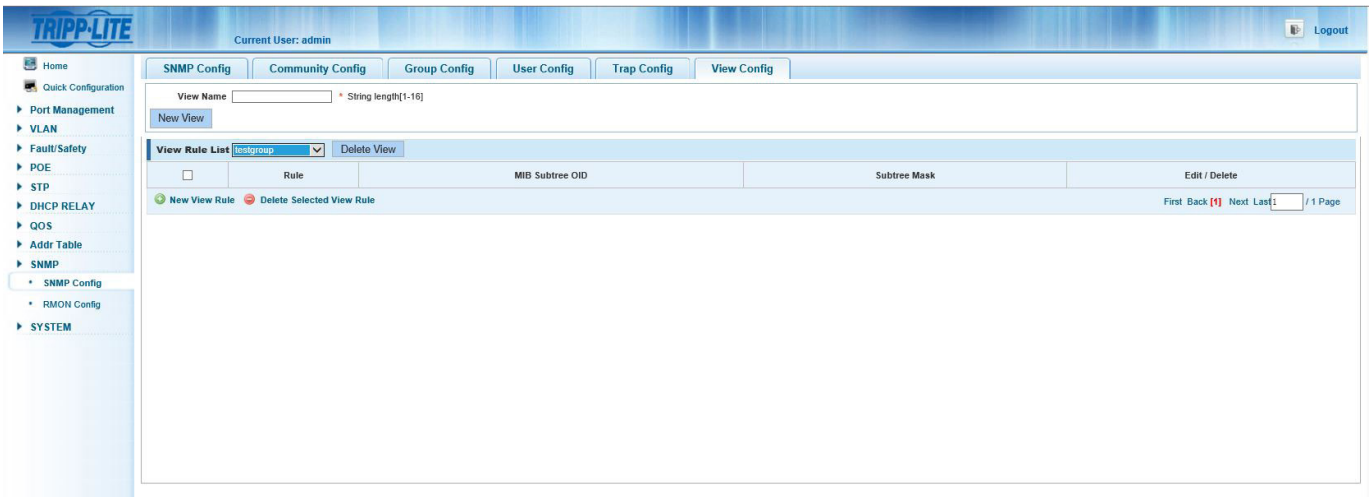


Figure 13.4 : Configuration de l'affichage SNMP

13.1.4 Afficher le nom

Saisir le nom de l'affichage (limite : 16 caractères). Cliquer sur l'icône « New View » (nouvel affichage). Cela permettra d'ajouter le nom de l'affichage au menu déroulant de la liste de règle de l'affichage.

13. Gestion du protocole de gestion de réseau simple (SNMP)

13.1.5 Afficher la liste des règles

Une fois le nom de l'affichage configuré, sélectionner l'icône vert pour ajouter une nouvelle règle d'affichage (Figure 13.5).

13.1.6 Modifier l'affichage des règles

Pour inclure ou exclure un affichage dans une règle (Figure 13.5), suivre les étapes ci-dessous :

1. OID sous-arbre MIB – Saisir l'OID souhaité pour le filtrage du nom de l'affichage (limite : 64 caractères).
2. Masque de sous-arbre – Saisir l'OID du masque de sous-arbre le cas échéant.
3. Cliquer sur « Save » (sauvegarder) pour sauvegarder les changements et « Exit » (quitter) pour les rejeter.

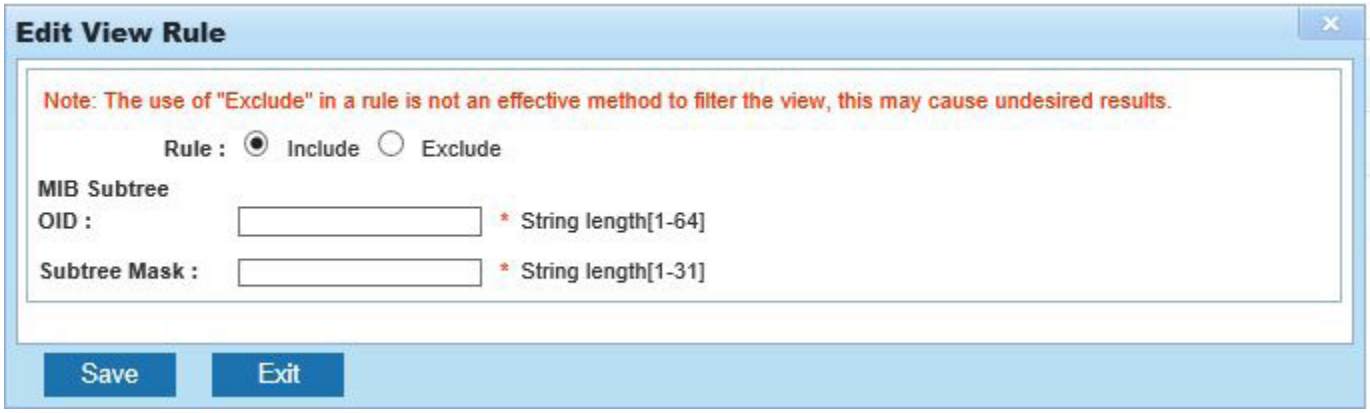


Figure 13.5 : Ajouter ou modifier une règle d'affichage

Remarque : *Exclure en utilisant une règle n'est pas une méthode efficace pour filtrer l'affichage. Ce paramètre peut engendrer des résultats non désirés.*

13.1.7 Configuration d'un groupe

Créer des groupes SNMP auxquels les règles d'affichage s'appliqueront.

13.1.8 Créer un nouveau groupe SNMP

SNMP → SNMP Config → Group Config (configuration du groupe) pour configurer le groupe SNMP (Figure 13.6) en suivant les étapes suivantes :

1. Sélectionner l'icône « New Group » (nouveau groupe) pour créer votre groupe SNMP.
2. Saisir le nom du groupe (limite : 16 caractères).
3. Sélectionner le niveau de sécurité des informations transmises qui peuvent être affichées (Figure 13.7). Les paramètres disponibles sont : aucune authentification et aucun chiffrement, authentification et aucun chiffrement, ou authentification et chiffrement.
4. Sélectionner la règle Read View (affichage de lecture) pour le groupe le cas échéant. Le groupe sera en mesure d'afficher seulement les informations en fonction des paramètres de la règle.
5. Sélectionner la règle Read Write View (affichage écriture-lecture) le cas échéant. Le groupe sera en mesure d'afficher et gérer le commutateur en fonction des paramètres de la règle.
6. Sélectionner la règle Notify View (affichage de notification) le cas échéant. Le groupe sera uniquement notifié de la configuration de la règle d'affichage sélectionnée.
7. Cliquer sur « Save » (sauvegarder) pour sauvegarder le groupe SNMP. Cliquer sur « Exit » (quitter) pour rejeter les modifications.

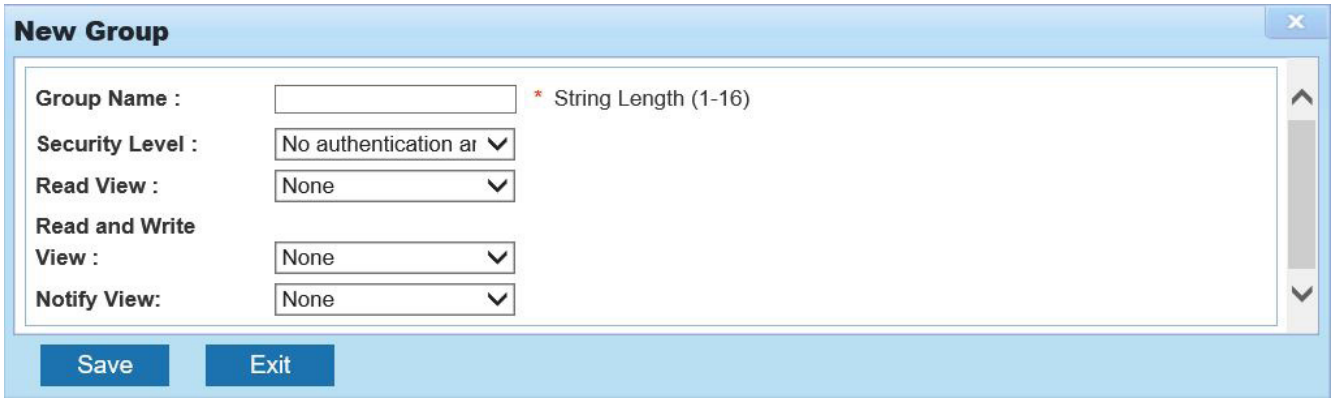


Figure 13.6 : Nouveau groupe

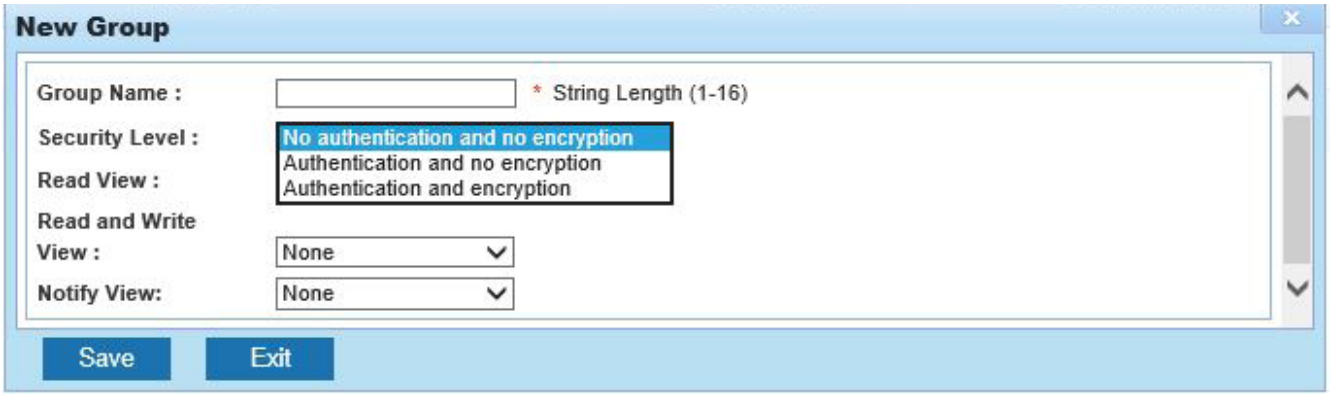


Figure 13.7 : Niveau de sécurité du nouveau groupe

13.1.9 Modifier un groupe SNMP

Cliquer sur l'icône « Edit » (modifier) pour modifier les paramètres du groupe. Cliquer sur « Save » (sauvegarder) pour sauvegarder les modifications. Cliquer sur « Exit » (quitter) pour rejeter les modifications (Figure 13.8).

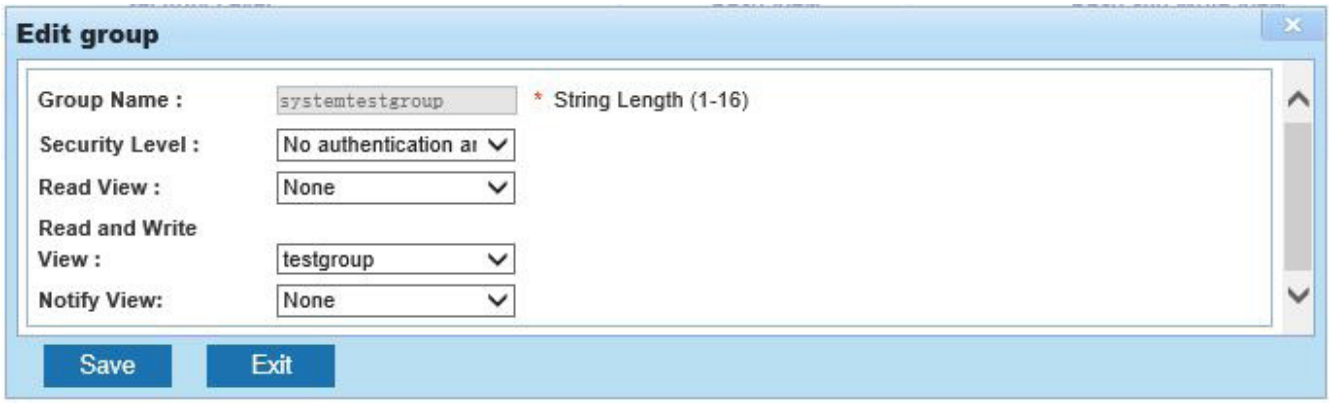


Figure 13.8 : Modifier le groupe

13.1.10 Supprimer un groupe SNMP

Pour supprimer un seul groupe SNMP, cliquer sur l'icône rouge ou cliquer sur la case à cocher à côté du groupe SNMP, puis cliquer sur l'icône « Delete Selected Group » (supprimer le groupe sélectionné). Pour supprimer plusieurs groupes, cliquer sur la case à cocher pour chaque groupe SNMP à supprimer, puis cliquer sur l'icône « Delete Selected Group » (supprimer le groupe sélectionné).

13.1.11 Configuration d'un utilisateur SNMP

Sélectionner SNMP → SNMP Config (configuration de SNMP) → User Config (configuration d'un utilisateur) pour créer les utilisateurs qui seront attribués au groupe SNMP, de même que leurs données d'accès.

Pour ajouter un nouvel utilisateur SNMP, cliquer sur l'icône « New User » (nouvel utilisateur), puis suivre les étapes ci-dessous (Figure 13.9) :

1. User Name (nom d'utilisateur) – Saisir le nom d'utilisateur (limite : 16 caractères).
2. Security Level (niveau de sécurité) – Saisir le niveau de sécurité d'aucune authentification et aucun chiffrement, authentification et aucun chiffrement, ou authentification et chiffrement.
3. Group Name (non du groupe) – Sélectionner le nom du groupe auquel l'utilisateur sera attribué depuis le menu déroulant.
4. Authentication Mode (mode d'authentification) – Lorsqu'une authentification est requise, sélectionner le bon mode d'authentification MD5 ou SHA.
5. Authentication Password (mot de passe d'authentification) – Saisir le mot de passe d'authentification.
6. Confirm Authentication Password (confirmer le mot de passe d'authentification) – Saisir de nouveau le mot de passe d'authentification pour confirmation.
7. Encrypt Mode (mode de chiffrement) : Lorsque Encryption (chiffrement) est sélectionné, sélectionner le mode approprié de chiffrement DES ou AES.
8. Encryption Password (mot de passe de chiffrement) – Saisir le mot de passe de chiffrement.
9. Confirm Encryption Password (confirmer le mot de passe de chiffrement) – Saisir de nouveau le mot de passe de chiffrement.
10. Cliquer sur « Save » (sauvegarder) pour ajouter le nouvel utilisateur SNMP. Cliquer sur « Exit » (quitter) pour rejeter les modifications.

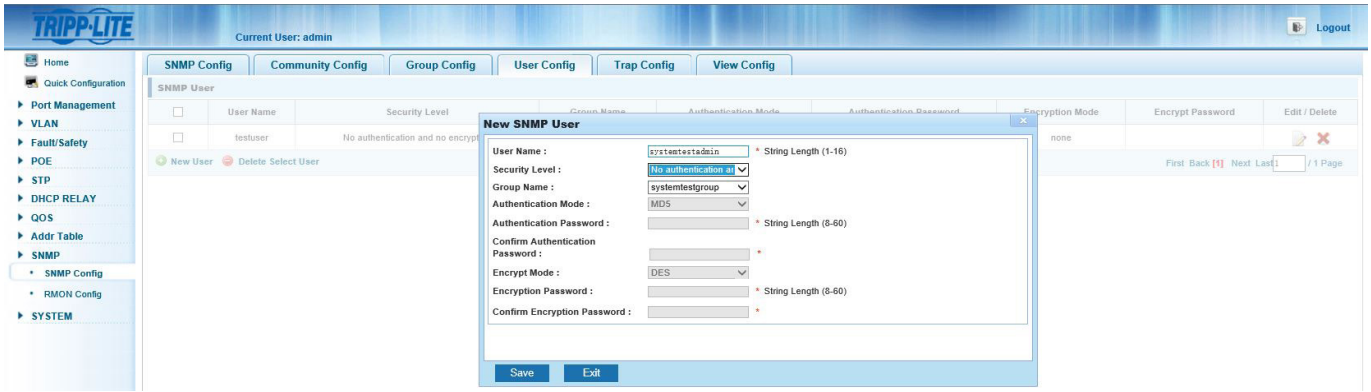


Figure 13.9 : Ajouter un nouvel utilisateur SNMP

13. Gestion du protocole de gestion de réseau simple (SNMP)

Pour modifier la configuration d'un utilisateur SNMP, cliquer sur l'icône « Edit » (modifier) pour apporter des changements (Figure 13.10). Cliquer sur « Save » (sauvegarder) pour sauvegarder les modifications. Cliquer sur « Exit » (quitter) pour rejeter les modifications.

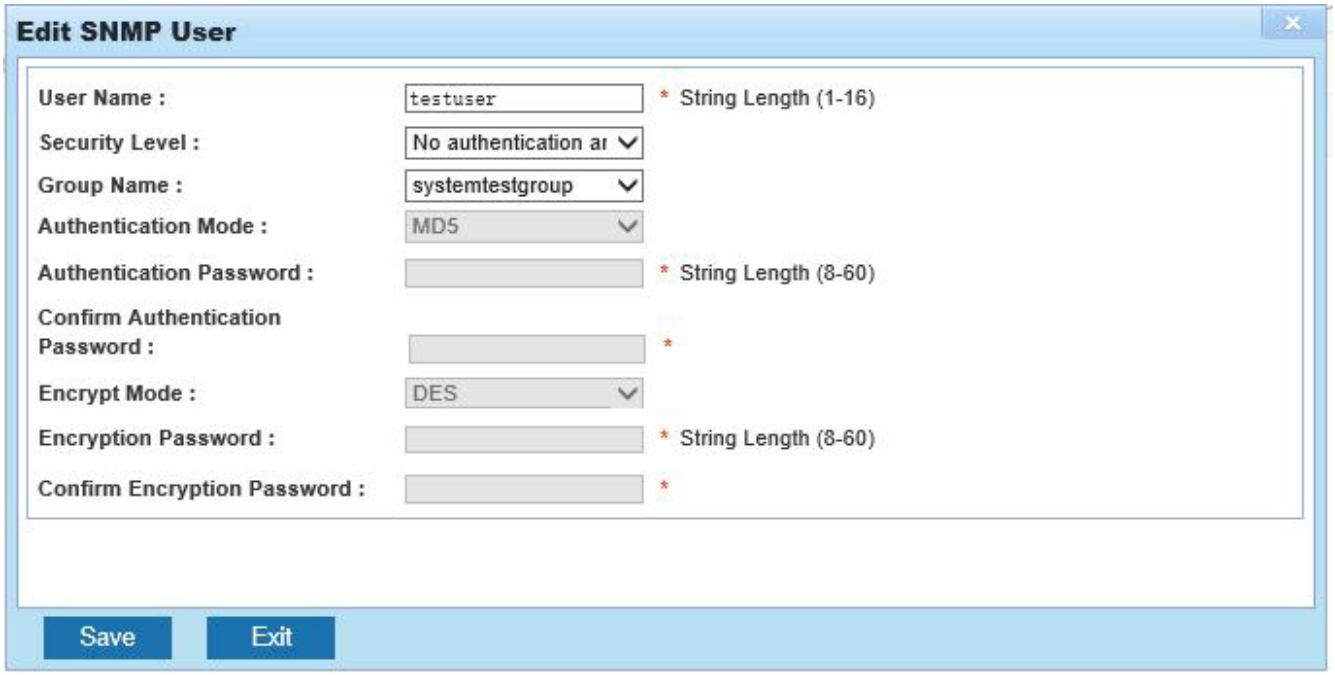


Figure 13.10 : Modifier l'utilisateur SNMP

Pour supprimer un utilisateur SNMP, cliquer sur l'icône de suppression rouge ✖ à côté du nom de l'utilisateur à supprimer ou cliquer sur la case à cocher à côté du nom de l'utilisateur, puis cliquer sur l'icône « Delete Select User » (supprimer l'utilisateur sélectionné). Une fois confirmé, l'utilisateur SNMP sera supprimé. Pour supprimer plusieurs utilisateurs, cliquer sur la case à cocher à côté de chaque utilisateur à supprimer, puis cliquer sur l'icône « Delete Select User » (supprimer l'utilisateur sélectionné). Une fois confirmés, les utilisateurs SNMP seront supprimés.

13. Gestion du protocole de gestion de réseau simple (SNMP)

13.1.12 Configuration d'un déroutement SNMP

Pour configurer la destination des déroutements SNMP envoyés par le commutateur, cliquer sur l'icône « New Trap » (nouveau déroutement) pour saisir le récepteur hôte pour les déroutements SNMP, puis suivre les étapes ci-dessous pour créer un nouveau déroutement (Figure 13.11) :

1. Destination IP (IP de destination) – Saisir l'adresse IP de destination du récepteur du déroutement (si le mode de sécurité V1 ou V2, cliquer sur l'icône « Save » (sauvegarder) pour ajouter l'hôte du récepteur de déroutement SNMP).
2. Security Mode (mode de sécurité) – Configurer le mode de sécurité de destination pour V1, V2 ou V3. Ce paramètre doit correspondre au mode de sécurité de l'hôte de destination de déroutement. 13.1.6.4 Address Type (type d'adresse) – Le commutateur ne prend en charge que l'envoi vers des destinations hôtes IPv4.
3. Security Name (nom de sécurité) – Si le mode de sécurité v3 SNMP est sélectionné, sélectionner l'utilisateur SNMP depuis la liste déroulante.
4. UDP Port Number (numéro du port UDP) – Le port par défaut est 162 et ne peut pas être changé.
5. Cliquer sur « Save » (sauvegarder) pour sauvegarder l'hôte de destination de déroutement. Cliquer sur « Exit » (quitter) pour rejeter les modifications.

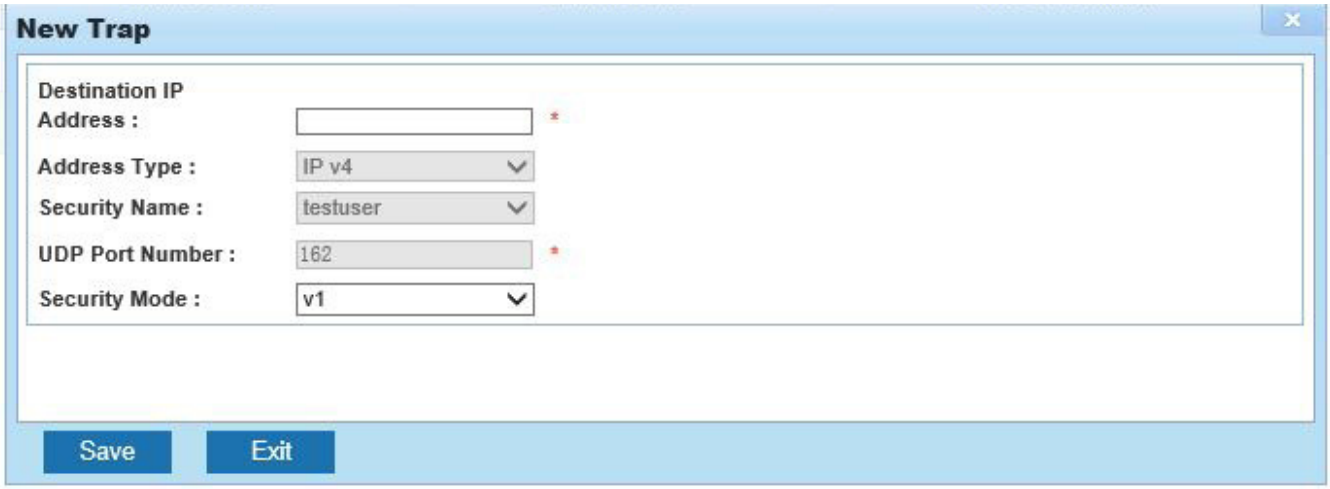


Figure 13.11 : Nouveau déroutement

Pour modifier la configuration d'un hôte de destination de déroutement, cliquer sur l'icône « Edit » (modifier) pour apporter les changements nécessaires (Figure 13.12). Cliquer sur « Save » (sauvegarder) pour sauvegarder les modifications. Cliquer sur « Exit » (quitter) pour rejeter les modifications.

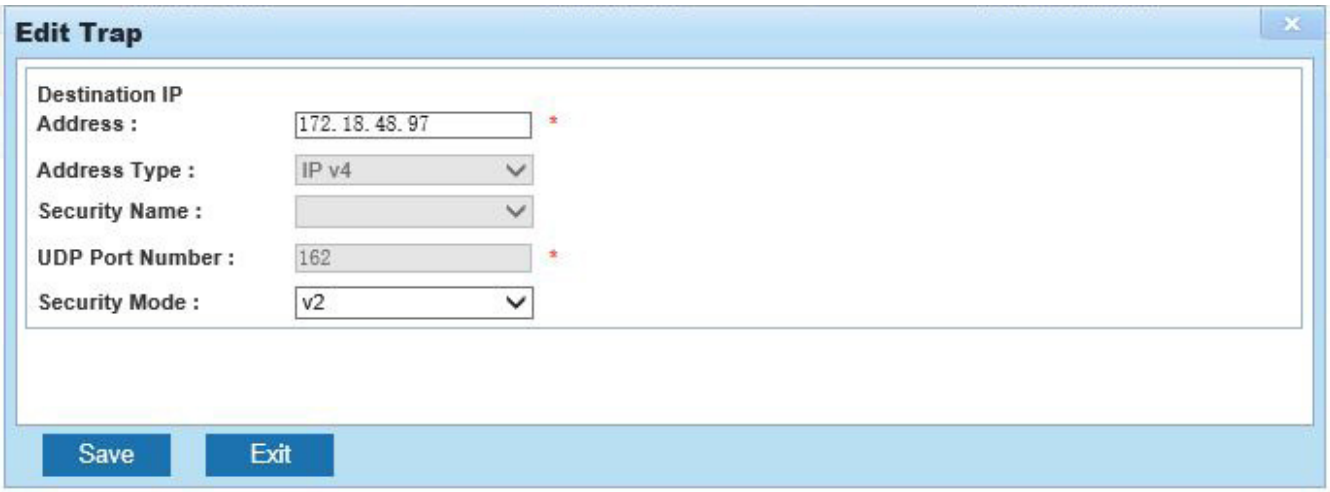


Figure 13.12 : Modifier un déroutement

Pour supprimer un hôte de destination de déroutement, cliquer sur l'icône de suppression rouge ✖ à côté du nom de l'hôte à supprimer, cliquer sur la case à cocher à côté du nom de l'hôte, puis cliquer sur l'icône « Delete Select Trap » (supprimer le déroutement sélectionné). Une fois confirmé, l'hôte de destination de déroutement sera supprimé. Pour supprimer plusieurs hôtes de destination de déroutement, cliquer sur la case à cocher à côté de chaque élément à supprimer, puis cliquer sur l'icône « Delete Select User » (supprimer l'utilisateur sélectionné). Une fois confirmés, les hôtes de destination de déroutement seront supprimés.

13. Gestion du protocole de gestion de réseau simple (SNMP)

13.2 Paramètres de configuration de la surveillance à distance

La télésurveillance (RMON) permet la surveillance du trafic du réseau et fournit les statistiques du réseau pour les réseaux Ethernet. Le commutateur est équipé d'une sonde RMON intégrée dans ses circuits. La fonction est disponible par le biais de l'option SNMP → RMON Config (configuration de la télésurveillance SNMP).

Remarque : *SNMP doit être activé pour configurer la télésurveillance.*

13.2.1 Groupe Statistiques

Pour définir la configuration d'un groupe Statistiques (Figure 13.13), cliquer sur l'icône « New Count Group » (nouveau groupe de comptage), puis suivre les étapes ci-dessous :

1. Index – Saisir le numéro d'index à l'intérieur de la plage de valeurs du tableau de renseignements statistiques de 1 ~ 65 535.
2. Interface Name (nom de l'interface) – Sélectionner le port éphémère de l'interface.
3. Owner (propriétaire) – Définir le créateur du tableau (limite : 30 caractères).
4. Cliquer sur « Save » (sauvegarder) pour sauvegarder les paramètres. Cliquer sur « Exit » (quitter) pour rejeter les modifications.

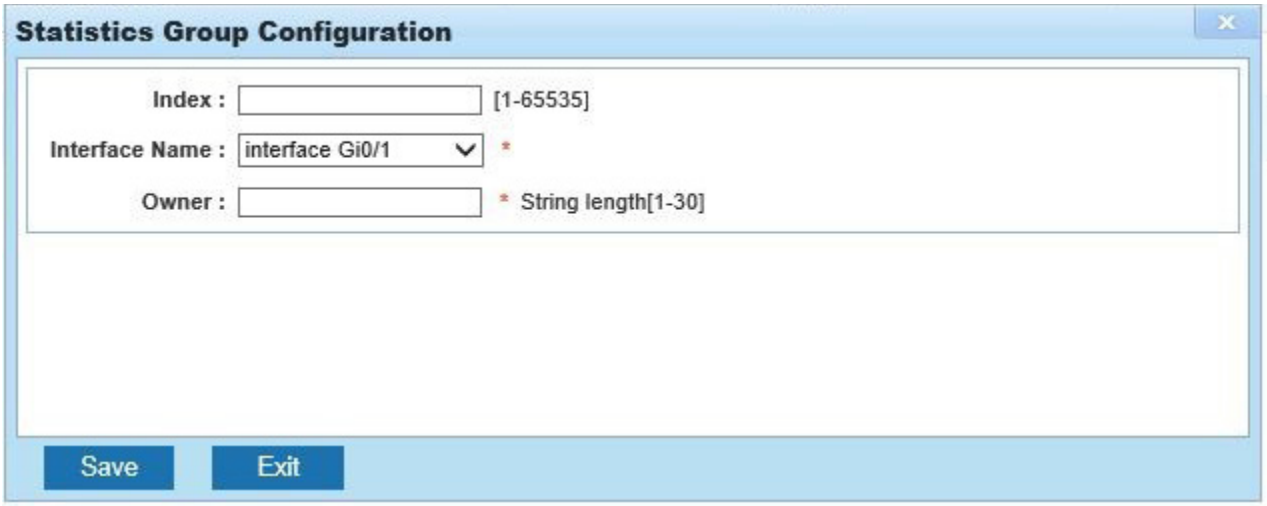


Figure 13.13 : Configuration du groupe Statistiques

Pour modifier la configuration d'un groupe Statistiques (Figure 13.14), cliquer sur l'icône « Edit » (modifier) pour apporter les changements nécessaires. Cliquer sur « Save » (sauvegarder) pour sauvegarder les modifications. Cliquer sur « Exit » (quitter) pour rejeter les modifications.

Figure 13.14 : Modifier un groupe Statistiques

Pour supprimer la configuration d'un groupe Statistiques, cliquer sur l'icône rouge ✖ à côté de l'élément à supprimer, ou cliquer sur la case à cocher à côté de l'élément, puis cliquer sur l'icône « Delete Selected Statistics Group » (supprimer le groupe Statistiques sélectionné). Une fois confirmé, le groupe Statistiques sera supprimé. Pour supprimer plusieurs groupes Statistiques, cliquer sur la case à cocher à côté de chaque élément à supprimer, puis cliquer sur l'icône « Delete Selected Statistics Group » (supprimer le groupe Statistiques sélectionné). Une fois confirmés, les éléments sélectionnés pour le groupe Statistiques seront supprimés.

13. Gestion du protocole de gestion de réseau simple (SNMP)

Cliquer sur l'icône « View Link » (afficher la liaison) d'un élément d'un groupe Statistiques pour afficher ses renseignements statistiques (Figure 13.15).

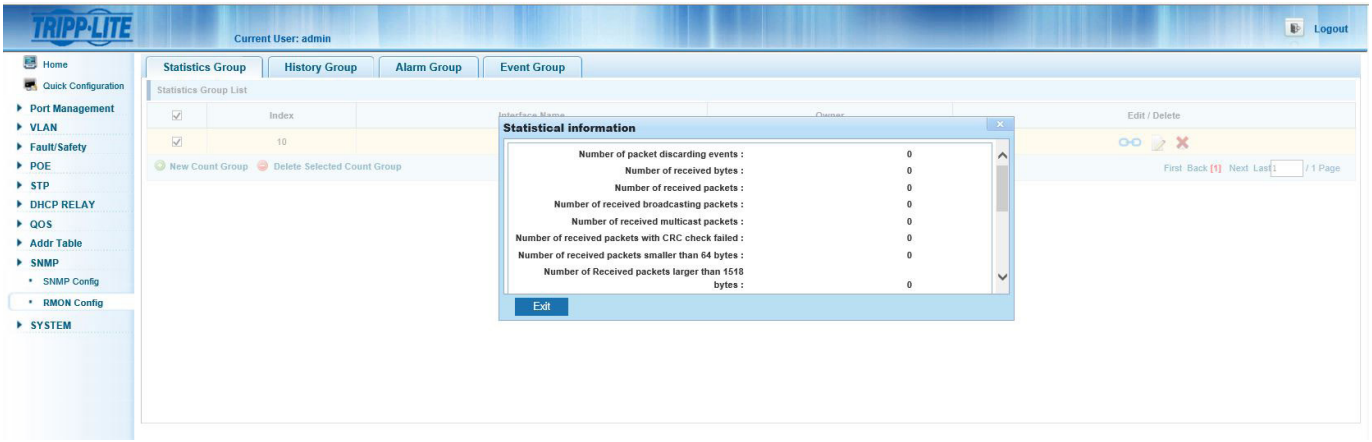


Figure 13.15 : Renseignements statistiques

13.2.2 Groupe Historique

Un groupe Historique enregistre l'historique des informations concernant l'interface Ethernet. Pour définir un groupe Historique, cliquer sur l'icône « New History Group » (nouveau groupe Historique), puis suivre les étapes ci-dessous (Figure 13.16) :

1. Index – Saisir le numéro d'index requis à l'intérieur de la plage de valeurs du tableau de renseignements statistiques de 1 ~ 65 535.
2. Interface Name (nom de l'interface) – Sélectionner le port éphémère de l'interface requis.
3. Nombre maximum d'échantillons – Saisir le nombre requis d'échantillons à enregistrer à l'intérieur de la plage des valeurs de 1 à 65 535.
4. Sample Period (période d'échantillonnage) – Saisir les secondes nécessaires entre 5 et 3 600 pour recueillir les échantillons.
5. Owner (propriétaire) – Définir le créateur du tableau (limite : 30 caractères).
6. Cliquer sur « Save » (sauvegader) pour sauvegarder les paramètres. Cliquer sur « Exit » (quitter) pour rejeter les modifications.

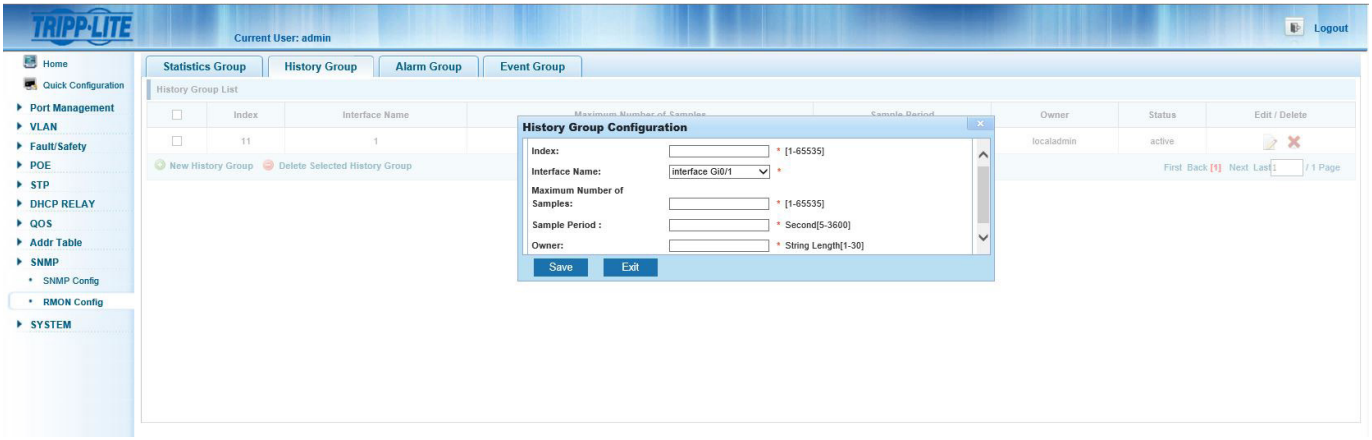


Figure 13.16 : Nouveau groupe Historique

Pour modifier la configuration d'un groupe Historique, cliquer sur l'icône « Edit » (modifier) pour apporter des changements (Figure 13.17). Cliquer sur « Save » (sauvegarder) pour sauvegarder les changements et « Exit » (quitter) pour les rejeter.

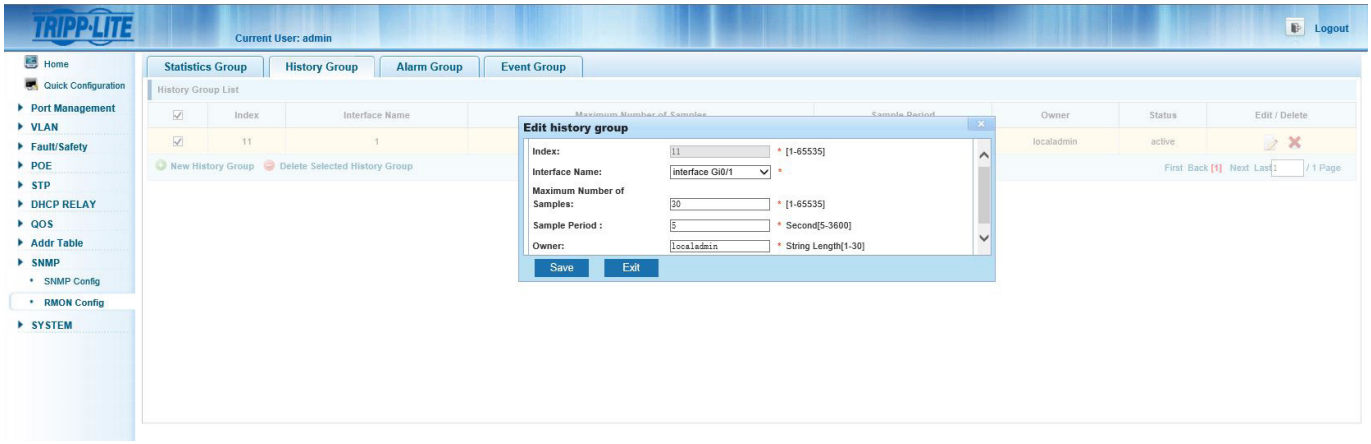


Figure 13.17 : Modifier un groupe Historique

Pour supprimer la configuration d'un groupe Historique, cliquer sur l'icône rouge ✖ à côté de l'élément du groupe Historique à supprimer, ou cocher la case à côté de l'élément, puis cliquer sur l'icône « Delete Selected History Group » (supprimer le groupe Historique sélectionné). Une fois confirmé, l'élément du groupe Historique sera supprimé. Pour supprimer plusieurs groupes Historique, cliquer sur la case à cocher à côté de chaque élément à supprimer, puis cliquer sur l'icône « Delete Selected History Group » (supprimer le groupe Historique sélectionné). Une fois confirmés, les éléments sélectionnés pour le groupe Historique seront supprimés.

13.2.3 Groupe Événements

Le groupe Événement définit les déclencheurs d'événements et permet de définir les alarmes pour les enregistrer. Pour configurer, aller à SNMP → RMON Config (configuration de la télésurveillance) → Event Config (configuration d'un événement), puis suivre les étapes ci-dessous (Figure 13.18) :

1. Index – Saisir le numéro de l'index à l'intérieur de la plage de valeurs de 1 ~ 65 535.
2. Description – Saisir la description du groupe Événement (limite : 30 caractères).
3. Owner (propriétaire) – Saisir le propriétaire du groupe Événement (limite : 30 caractères).
4. Action – Saisir un crochet pour enregistrer l'événement, envoyer un déroutement SNMP pour l'événement ou les deux.
5. Cliquer sur « Save » (sauvegarder) pour ajouter le groupe Événement à la liste. Cliquer sur « Exit » (quitter) pour rejeter la configuration.

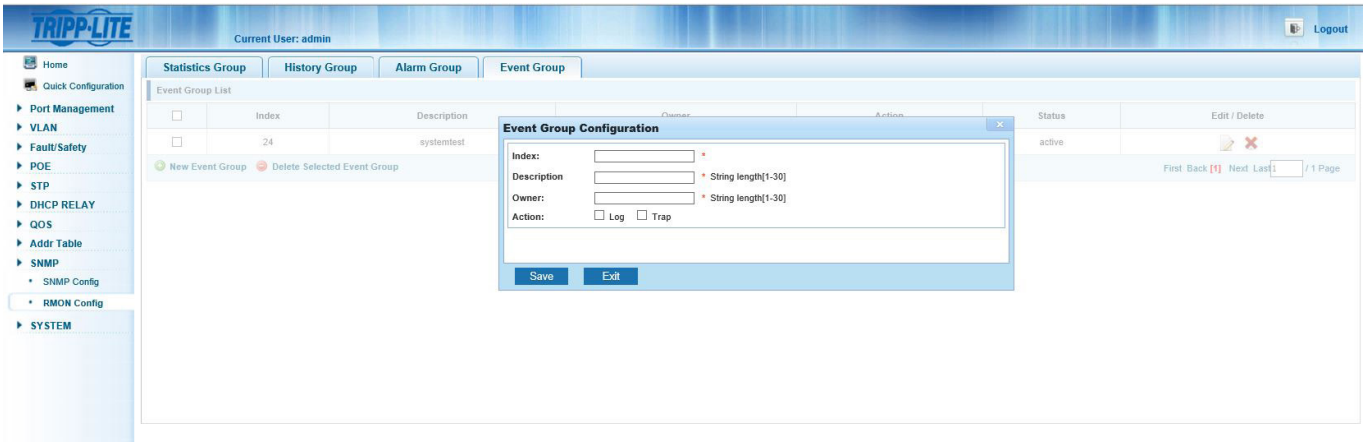


Figure 13.18 : Nouveau groupe Événement

13. Gestion du protocole de gestion de réseau simple (SNMP)

Pour modifier la configuration d'un groupe Événement, cliquer sur l'icône « Edit » (modifier) pour apporter des changements (Figure 13.19). Cliquer sur « Save » (sauvegarder) pour sauvegarder les changements et « Exit » (quitter) pour les rejeter.

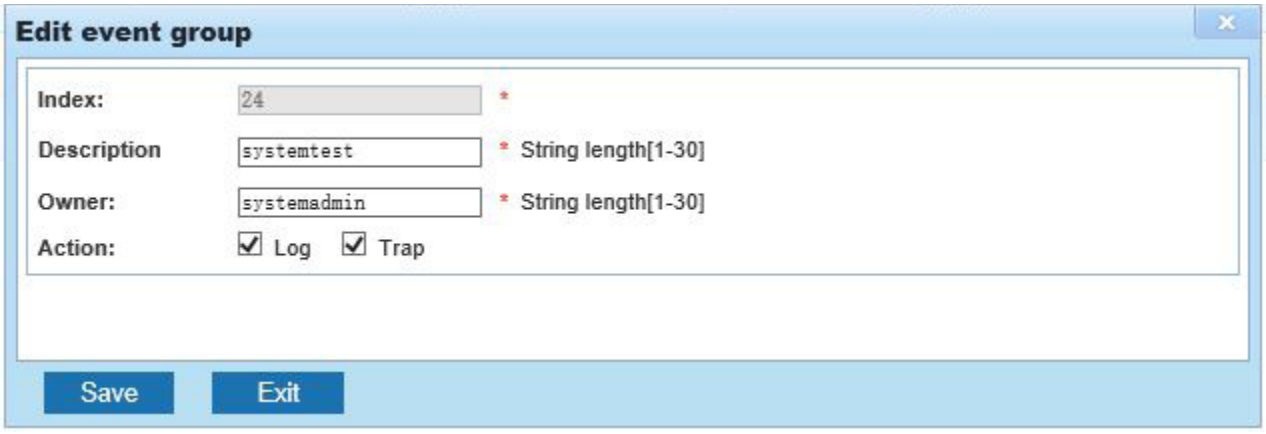


Figure 13.19 : Modifier un groupe Événement

Pour supprimer la configuration d'un groupe Événement, cliquer sur l'icône rouge à côté de l'élément du groupe Événement à supprimer, ou cliquer sur la case à cocher à côté de l'élément, puis cliquer sur l'icône « Delete Selected Event Group » (supprimer le groupe Événement sélectionné). Une fois confirmé, l'élément du groupe Événement sera supprimé. Pour supprimer plusieurs groupes Événement, cliquer sur la case à cocher à côté de chaque élément à supprimer, puis cliquer sur l'icône « Delete Selected Event Group » (supprimer le groupe Événement sélectionné). Une fois confirmés, les éléments sélectionnés pour le groupe Événement seront supprimés.

13. Gestion du protocole de gestion de réseau simple (SNMP)

13.2.4 Groupe Alarme

Pour définir un groupe Alarme pour les événements de trafic des données spécifié pour déclencher aux seuils supérieur et inférieur, configurer les éléments suivants
(Figure 13.20) :

1. Index – Définir le numéro d'index de la liste d'alarmes entre 1 et 65 535.
2. Statistical Event (événement statistique) – Définir le type d'événement pour déclencher une alarme. Les types d'événements sont : DropEvents, Octets, Pkts, BroadcastPkts, MulticastPkts, CRCAlignErrors, UndersizePkts, OversizePkts, Fragments, Jabbers, Collisions, Pkts64Octets, Pkts65to127Octets, Pkts128to255Octets, Pkts256to511Octets, Pkts512to1023Octets et Pkts1024to1518Octets.
3. Statistical Group Index (index du groupe Statistique) – Saisir le numéro d'index du groupe Statistique pour surveiller le numéro de port.
4. Sampling Time Interval (intervalle de temps d'échantillonnage) – Saisir l'intervalle de temps de l'échantillon entre 5 et 65 535 secondes.
5. Sample Type (type d'échantillon) – Choisir le type d'échantillon : Absolute ou Delta.
6. Owner (propriétaire) – Saisir le nom du propriétaire. Prend en charge 1 à 30 caractères.
7. Upper Alarm Threshold Limit (seuil limite d'alarme supérieur) – Saisir la quantité de trafic de données à laquelle configurer le seuil limite supérieur, entre 0 et 2 147 483 647.
8. Upper Alarm Threshold Limit Events (seuil limite d'alarme supérieur, Événement) – Choisir le groupe Événement à déclencher lorsque le seuil limite supérieur est atteint.
9. Lower Alarm Threshold Limit (seuil limite d'alarme inférieur) – Saisir la quantité de trafic de données à laquelle configurer le seuil limite inférieur, entre 0 et 2 147 483 647.
10. Lower Alarm Threshold Limit Events (seuil limite d'alarme inférieur, Événement) – Choisir le groupe Événement à déclencher lorsque le seuil limite inférieur est atteint.
11. Cliquer sur « Save » (sauvegarder) pour sauvegarder la configuration. Cliquer sur « Exit » (quitter) pour rejeter les modifications.

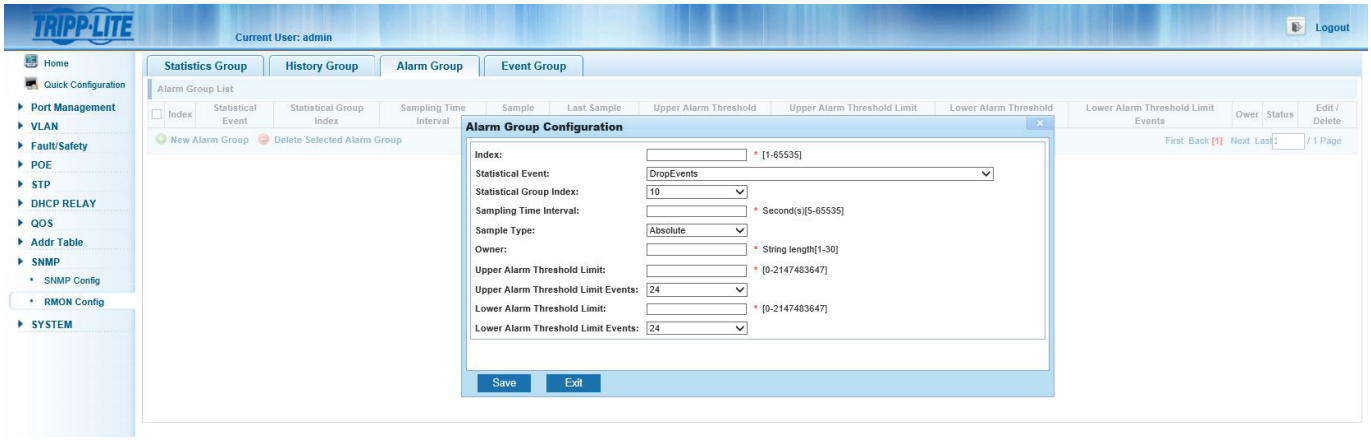


Figure 13.20 : Nouveau groupe Alarme

13. Gestion du protocole de gestion de réseau simple (SNMP)

Pour modifier la configuration d'un groupe Alarme, cliquer sur l'icône « Edit » (modifier) pour apporter des changements (Figure 13.21). Cliquer sur « Save » (sauvegarder) pour sauvegarder les changements et « Exit » (quitter) pour les rejeter.

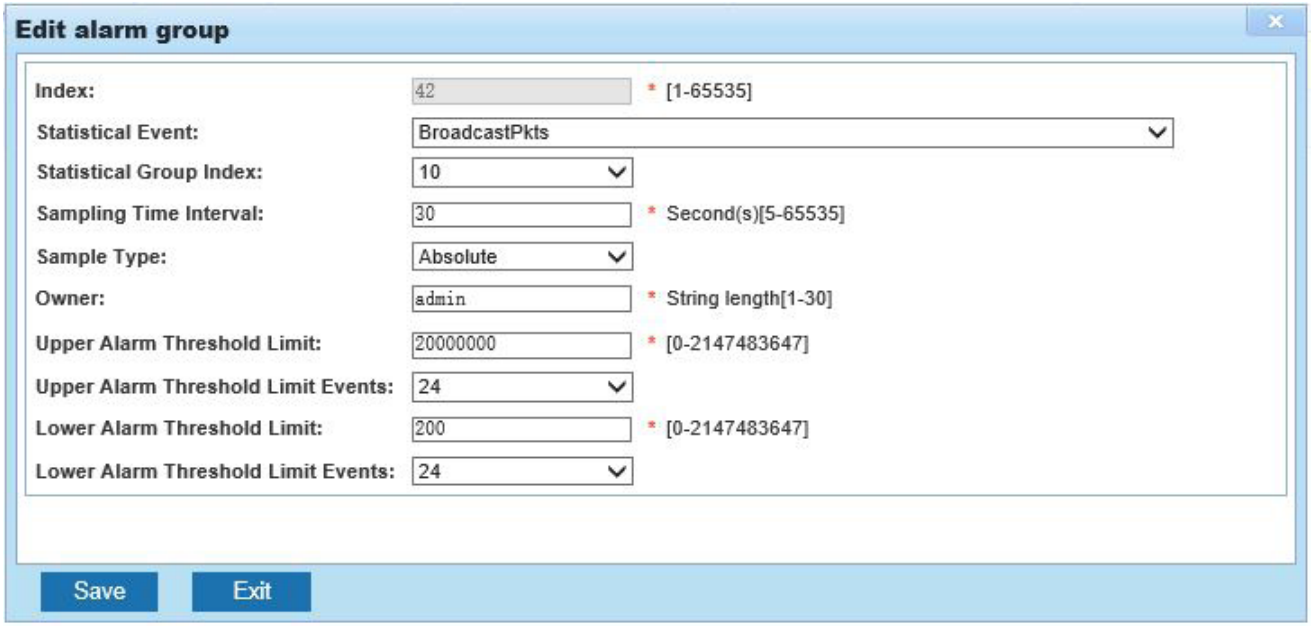


Figure 13.21 : Modifier un groupe Alarme

Pour supprimer la configuration d'un groupe Alarme, cliquer sur l'icône rouge à côté de l'élément du groupe Alarme à supprimer, ou cocher la case à côté de l'élément, puis cliquer sur l'icône « Delete Selected Alarm Group » (supprimer le groupe Alarme sélectionné). Une fois confirmé, l'élément du groupe Alarme sera supprimé. Pour supprimer plusieurs groupes Alarme, cliquer sur la case à cocher à côté de chaque élément à supprimer, puis cliquer sur l'icône « Delete Selected Alarm Group » (supprimer le groupe Alarme sélectionné). Une fois confirmés, les éléments sélectionnés pour le groupe Alarme seront supprimés.

14. Gestion du système

Les paramètres du système (Figure 14.1) permettent de définir la configuration du système du commutateur; effectuer les mises à jour du système, sauvegarder, sauvegarder et restaurer les configurations; sauvegarder les configurations d'amorçage; définir les privilèges d'administration et afficher les informations au sujet de la configuration du commutateur.

14.1 Configuration du système

Pour définir la configuration du commutateur et configurer l'heure du système, saisir ce qui suit :

Basic System Information (informations de base sur le système) – Saisir les fonctionnalités requises avec les mises à jour des informations facultatives :

Management VLAN (réseau local virtuel de gestion) – Sélectionner le réseau local virtuel de gestion depuis la liste déroulante. Pour sélectionner un autre réseau local virtuel pour être le réseau local virtuel de gestion, il doit d'abord être créé dans les paramètres du réseau local virtuel (Section 4.1). Cliquer sur « Set Management VLAN » (définir le réseau local virtuel) une fois l'action terminée.

Management IP (IP de gestion) – Saisir l'adresse IP du réseau local virtuel de gestion requise.

Subnet Mask (masque de sous-réseau) : Saisir le masque de sous-réseau requis du réseau local virtuel de gestion.

Default Gateway (passerelle par défaut) – Saisir l'adresse IP de la passerelle le cas échéant.

Jumbo Frames (trames étendues) – Par défaut, les trames étendues sont définies à 1 518. Elle peut être définie entre 1 518 et 9 216 trames.

DNS Server (serveur DNS) – Saisir l'adresse IP du serveur DNS le cas échéant.

Login Timeout (temporisation de connexion) (Minutes) – Par défaut, la minuterie de déconnexion est configurée à 30 minutes. La minuterie peut être configurée à n'importe quelle période de temps entre 0 et
86 400 minutes.

Device MAC (adresse MAC du dispositif) – L'adresse MAC du commutateur.

Device Name (nom du dispositif) – Par défaut, le nom du modèle du commutateur est saisi, mais peut être changé pour être adapté à l'utilisation de l'application
(limite : 32 caractères).

Device Location (emplacement du dispositif) – Saisir l'emplacement du dispositif du commutateur (limite : 32 caractères).

Contacts (boîte aux lettres incluse) – Saisir les adresses électroniques des contacts.

Cliquer sur « Save » (sauvegarder) pour sauvegarder les paramètres.

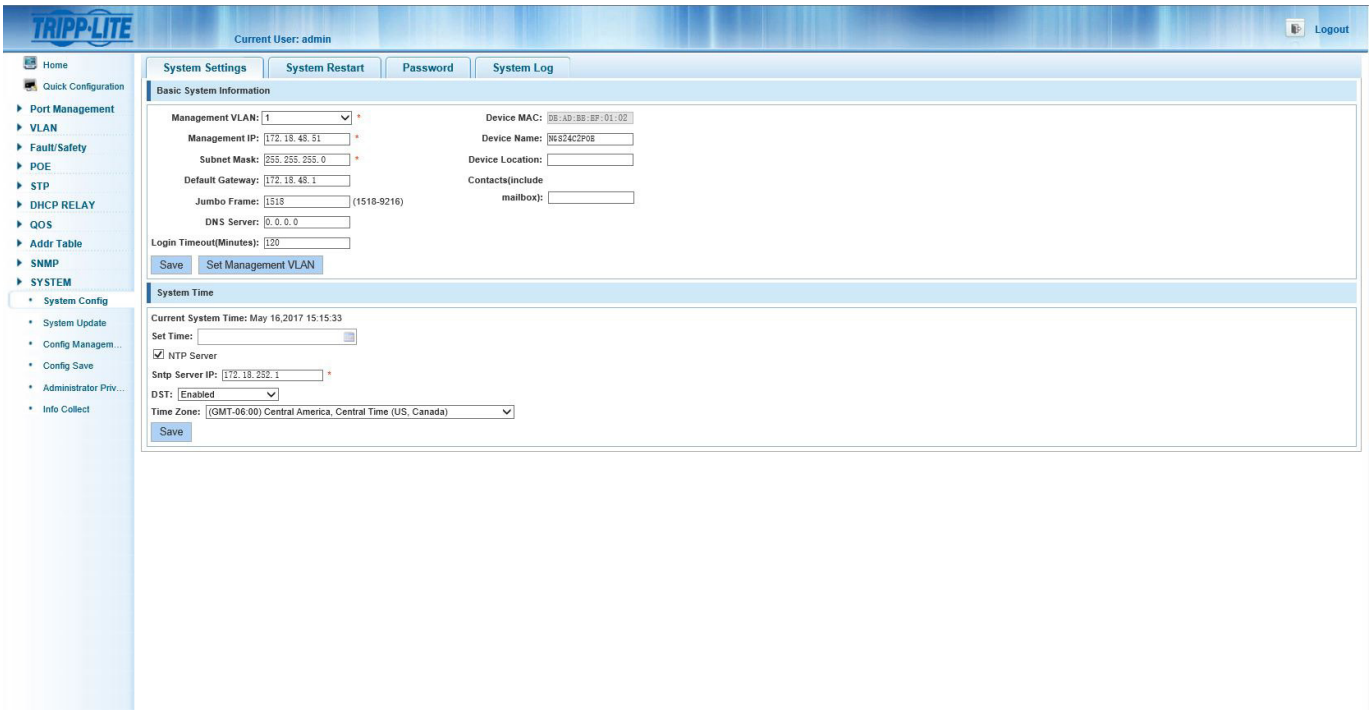


Figure 14.1 : Paramètres du système

14. Gestion du système

14.1.1 Heure du système

L'heure du système affiche l'heure du système actuelle qui peut être configurée manuellement ou être fournie automatiquement par un serveur NTP.

Set Time Manually (définir l'heure manuellement) – Saisir l'heure configurée via le calendrier contextuel, définir la date et l'heure manuellement, utiliser l'icône de sélection rapide ou cliquer sur le bouton Aujourd'hui. Cliquer sur « OK » pour garder les paramètres de l'heure.

Définir l'heure via un serveur NTP – Si un serveur NTP est utilisé, cliquer sur la case à cocher de la case du serveur NTP. Définir ensuite l'adresse IP requise du serveur SNTP. Si le fuseau horaire prend en charge l'heure avancée, changer l'option DST à Enabled (activé). Saisir ensuite le fuseau horaire souhaité.

Cliquer sur « Save » (sauvegarder) pour sauvegarder les paramètres de l'heure du système.

14.1.2 Redémarrage du système

Pour redémarrer le commutateur, cliquer sur le bouton « Restart » (redémarrer). Le processus de redémarrage peut prendre jusqu'à une minute. La page sera actualisée à la page d'accueil.

Remarque : *Pour s'assurer que la configuration de démarrage est sauvegardée avant un redémarrage, aller à SYSTEM (système)* → *Config Save (sauvegarder la configuration), puis cliquer sur le bouton « Save Settings » (sauvegarder les paramètres) pour sauvegarder la configuration de démarrage.*

14.1.3 Modifier le mot de passe d'administrateur

Pour changer le mot de passe d'administrateur, saisir l'ancien mot de passe, suivi du nouveau mot de passe. Confirmer en saisissant de nouveau le nouveau mot de passe. Cliquer sur « Save » (sauvegarder) pour sauvegarder les paramètres. Cliquer sur « Clear » (supprimer) pour rejeter les modifications.

14.1.4 Paramètres des registres du système

Cet écran permet d'afficher et de chercher parmi les informations du journal actuelles du commutateur. Si un serveur Syslog doit être configuré pour recevoir les journaux en fonction du niveau de journalisation, suivre les étapes suivantes :

1. Log Switch (commutateur du journal) – Journalisation activée (par défaut).
2. Server IP (IP du serveur) – Saisir l'IP du serveur Syslog.
3. Send Log Level (envoyer le niveau de journalisation) – Sélectionner les événements du niveau de journalisation à être envoyés comme Emergencies (urgences) (0), Alerts (alertes) (1), Critical (critique) (2), Errors (erreurs) (3), Warnings (avertissements) (4), Notifications (5), Informational (informationnel) (6) ou Debugging (débogage) (7). Cliquer sur « Save » (sauvegarder) pour sauvegarder les paramètres.

14.2 Mises à jour du système

L'onglet System Upgrade (mise à niveau du système) (Figure 14.2) permet les mises à jour du micrologiciel du système. La version courante du micrologiciel est affichée dans la partie supérieure de la section. Cliquer sur le bouton du navigateur pour obtenir des mises à jour du micrologiciel. Cliquer sur « Start Upgrade » (commencer la mise à niveau) le moment venu. Le système redémarrera à l'écran de connexion une fois l'action terminée.

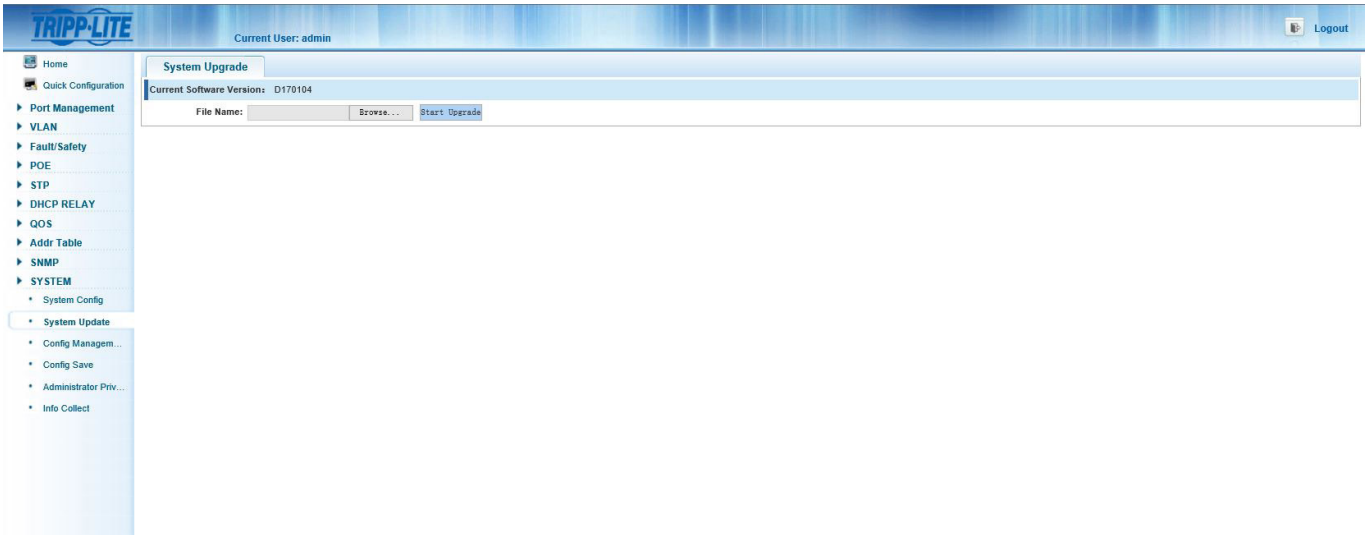


Figure 14.2 Mises à jour du système

14. Gestion du système

14.3 Gestion de la configuration du système

14.3.1 Importer/exporter une configuration

Cette section permet d'importer et d'exporter les configurations du système, restaurer les configurations précédentes et effectuer une réinitialisation d'usine (Figure 14.3).

Figure 14.3 : Importer/exporter la configuration

14.3.2 Afficher la configuration actuelle

Pour afficher la configuration actuelle du commutateur (Figure 14.4), cliquer sur le bouton « Show Current Config » (afficher la configuration actuelle).

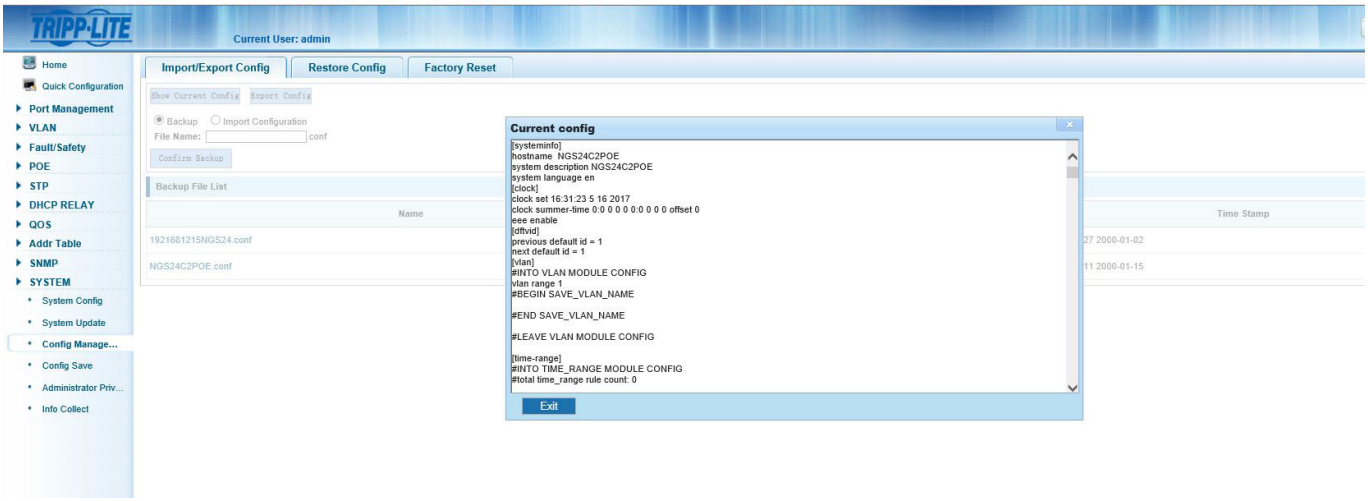


Figure 14.4 : Configuration actuelle

14.3.3 Exporter la configuration actuelle

Cliquer sur le bouton « Show Current Config » (afficher la configuration actuelle) pour afficher la configuration du système. Cliquer sur le bouton « Export » (exporter) pour sauvegarder la configuration du commutateur vers un système de secours local.

14.3.4 Sauvegarde de la configuration

Pour sauvegarder les sauvegardes locales du fichier de configuration, sélectionner « Backup » (sauvegarde), puis saisir le nom de fichier pour la sauvegarde. Cliquer sur « Confirm Backup » (confirmer la sauvegarde) pour sauvegarder la configuration. Les configurations sauvegardées peuvent être affichées sur la liste de fichiers de sauvegarde. Jusqu'à cinq fichiers de configuration de sauvegarde peuvent être sauvegardés.

14.3.5 Importer la configuration

Sélectionner « Import Configuration » (importer la configuration) puis naviguer vers le fichier de configuration exporté à importer. Cliquer sur le bouton « Import Configuration » (importer la configuration). Pour activer la configuration, sélectionner « Restart Device » (redémarrer le dispositif).

14.3.6 Rétablir la configuration

Permet de gérer les fichiers de configuration de sauvegarde sauvegardés.

14.3.7 Rétablir la sauvegarde

Pour rétablir une configuration sauvegardée, sélectionner le nom de la configuration à rétablir. Cliquer sur « Confirm Recovery » (confirmer la restauration) pour rétablir la configuration du système (Figure 14.5).

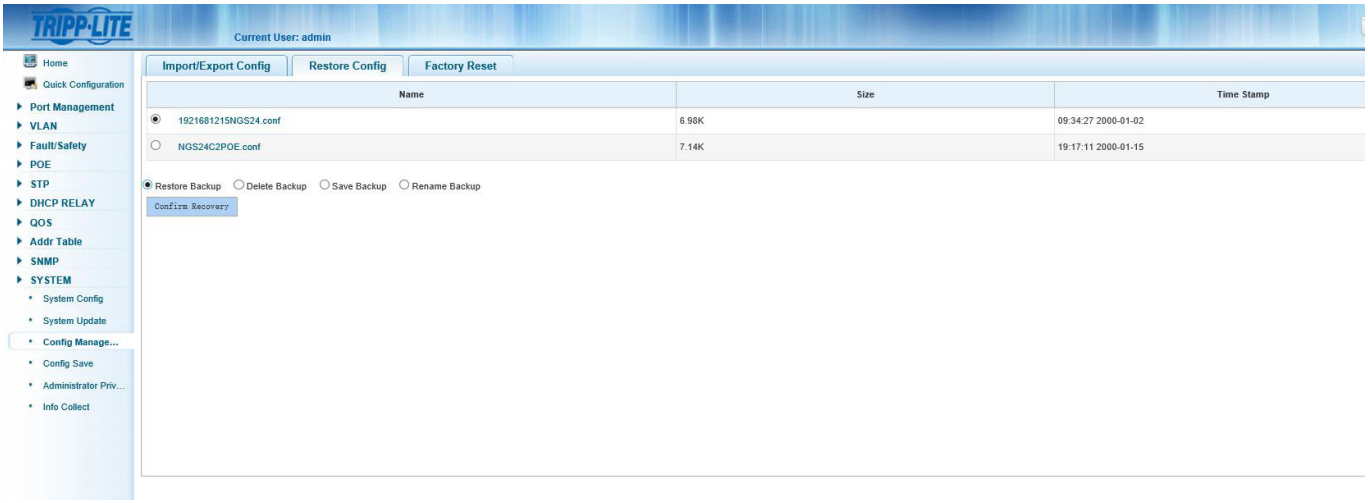


Figure 14.5 : Rétablir la sauvegarde

14.3.8 Supprimer la sauvegarde

Pour supprimer une sauvegarde de la configuration qui n'est désormais plus nécessaire, sélectionner le nom du fichier de configuration. Sélectionner l'option « Delete Backup » (supprimer la sauvegarde). Cliquer sur « Confirm Delete » (confirmer la suppression) pour supprimer le fichier de configuration du système (Figure 14.6).

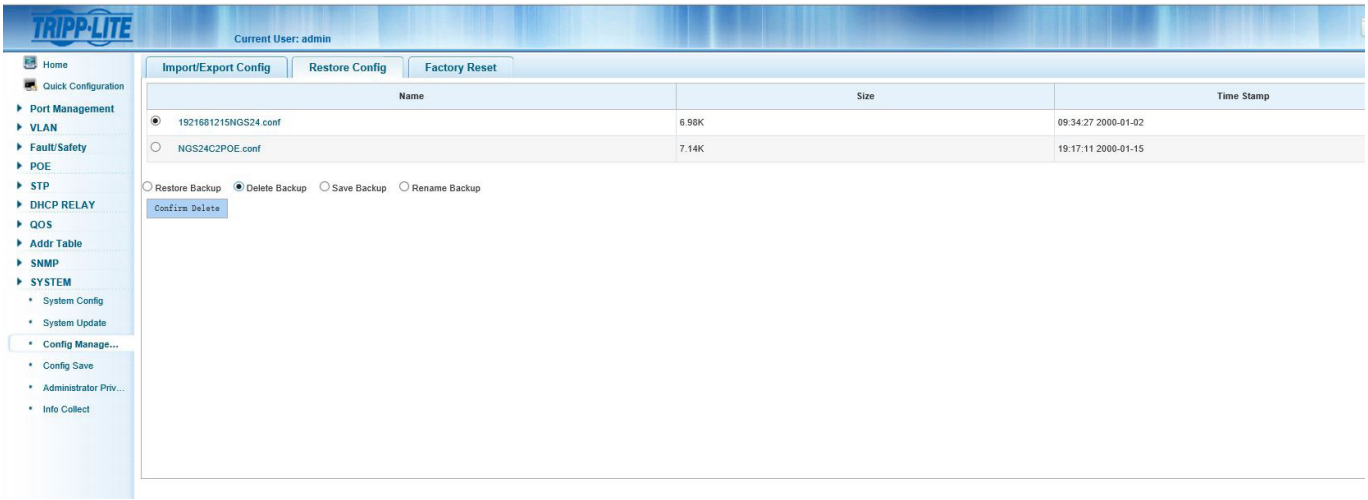


Figure 14.6 : Supprimer la sauvegarde

14. Gestion du système

14.3.9 Sauvegarder la sauvegarde

Lorsqu'il s'agit de restaurer, supprimer ou renommer une sauvegarde, choisir « Save Backup » (sauvegarder la sauvegarde) pour sauvegarder la configuration actuelle. Cliquer sur « Confirm Save » (confirmer la sauvegarde) pour sauvegarder les paramètres de la configuration (Figure 14.7).

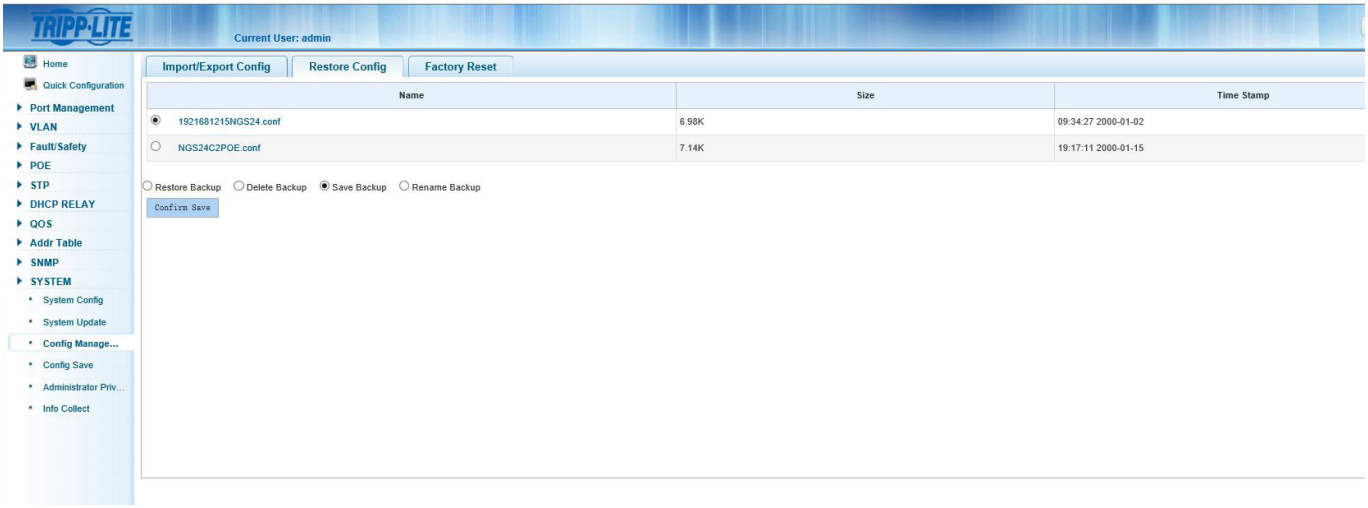


Figure 14.7 : Sauvegarder la sauvegarde

14.3.10 Réinitialisation d'usine

Pour remettre le commutateur à sa configuration d'usine d'origine, sélectionner SYSTEM (système) → Config Management (gestion de la configuration) → Factory Reset (réinitialisation d'usine). Cliquer sur « Factory Reset » (réinitialisation d'usine) permet de supprimer toutes les configurations sauvegardées du système et de restaurer le commutateur aux paramètres d'usine par défaut (Figure 14.8).

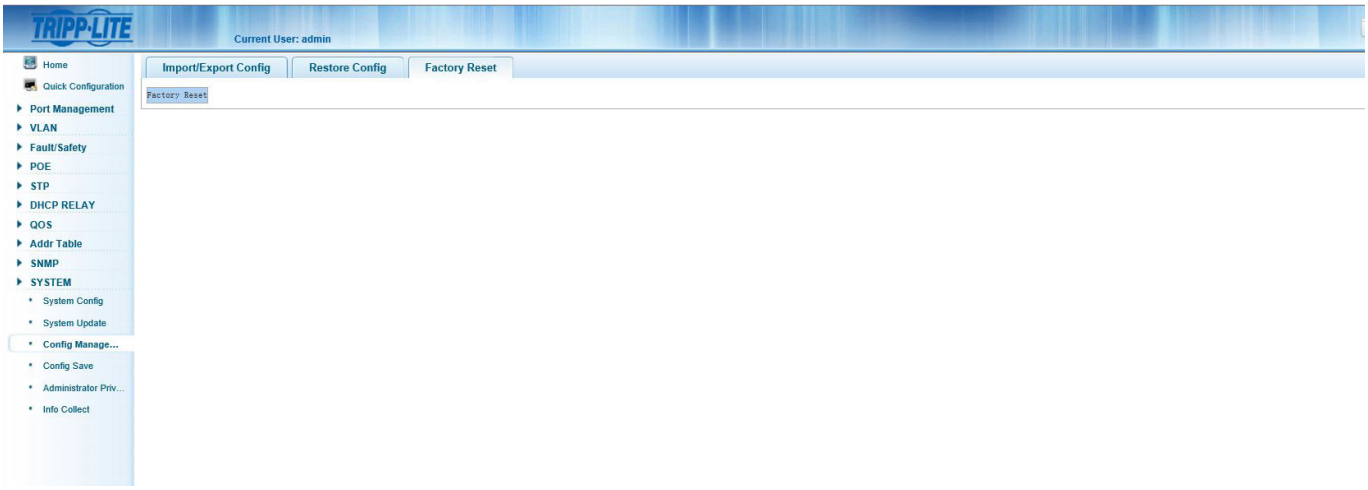


Figure 14.8 : Réinitialisation d'usine

14. Gestion du système

14.4 Sauvegarder la configuration

Pour sauvegarder la configuration de démarrage, cliquer sur le bouton « Save Settings » (sauvegarder les paramètres) (Figure 14.9).

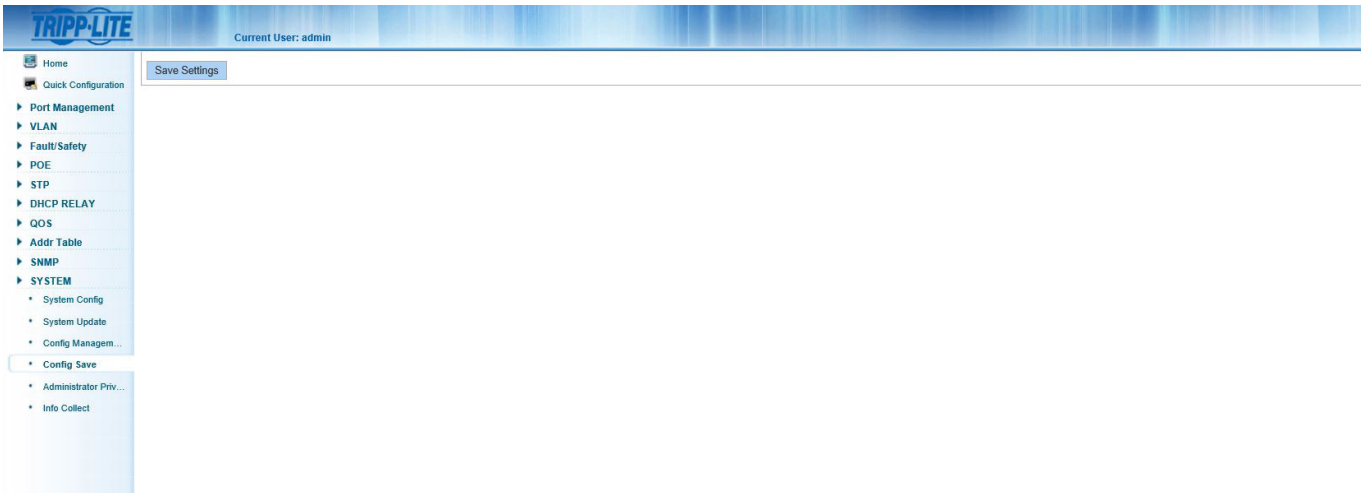


Figure 14.9 : Sauvegarde de la configuration

14.5 Privilèges d'administrateur

Cette section permet à l'administrateur d'ajouter des utilisateurs supplémentaires pour accéder au commutateur (Figure 14.10). Un compte « user » (utilisateur) peut se connecter au système de gestion Web de l'équipement pour un entretien courant. En plus de l'administrateur et de l'utilisateur, jusqu'à cinq utilisateurs supplémentaires peuvent être ajoutés. Les utilisateurs ordinaires peuvent accéder uniquement à la page d'accueil du système. Pour créer un nouvel utilisateur, suivre les étapes ci-dessous :

1. User Name (nom d'utilisateur) – Saisir le nom d'utilisateur pour le nouvel utilisateur.
2. New Password (nouveau mot de passe) – Saisir le mot de passe pour le nouvel utilisateur.
3. Confirm Password (confirmer le mot de passe) – Saisir de nouveau le mot de passe pour le nouvel utilisateur.
4. Cliquer sur le bouton « Add User » (ajouter un utilisateur) pour ajouter le nouvel utilisateur à la liste d'utilisateurs.

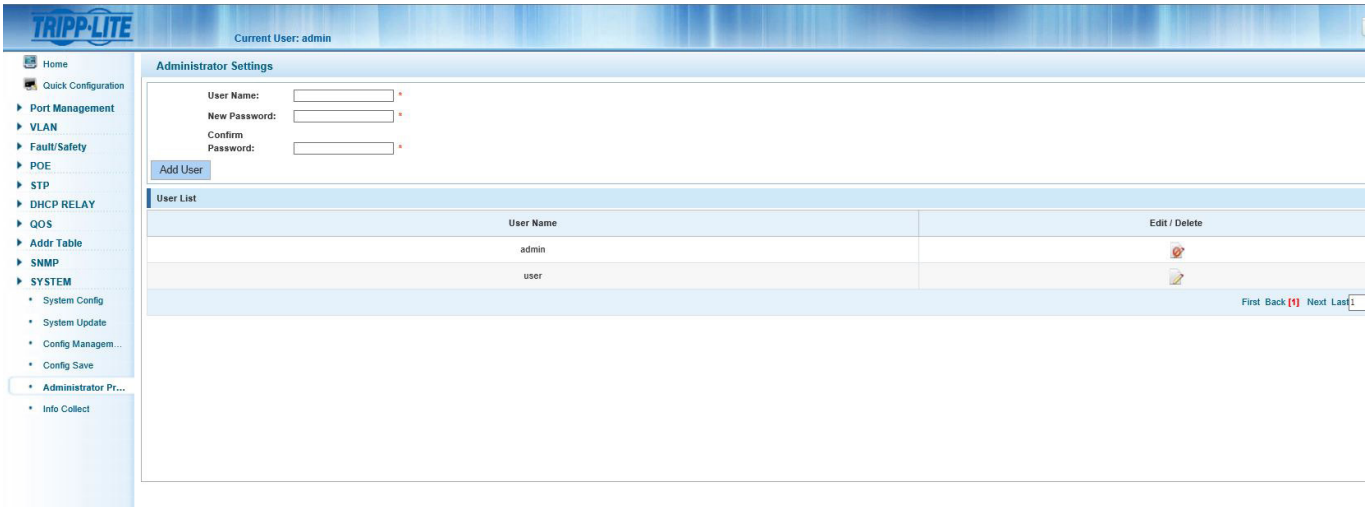


Figure 14.10 : Afficher les paramètres d'administrateur

14.5.1 Modifier les mots de passe de l'utilisateur

Pour changer le mot de passe d'un utilisateur, sélectionner le nom d'utilisateur, puis cliquer sur l'icône « Edit » (modifier) (Figure 14.11). Un nouveau mot de passe pour l'utilisateur peut maintenant être créé. Cliquer sur « Confirm Edit » (confirmer la modification) pour sauvegarder le nouveau mot de passe. Cliquer sur « Cancel Edit » (annuler la modification) pour rejeter les modifications.

Pour supprimer un utilisateur, cliquer sur l'icône rouge pour supprimer l'utilisateur de la liste.

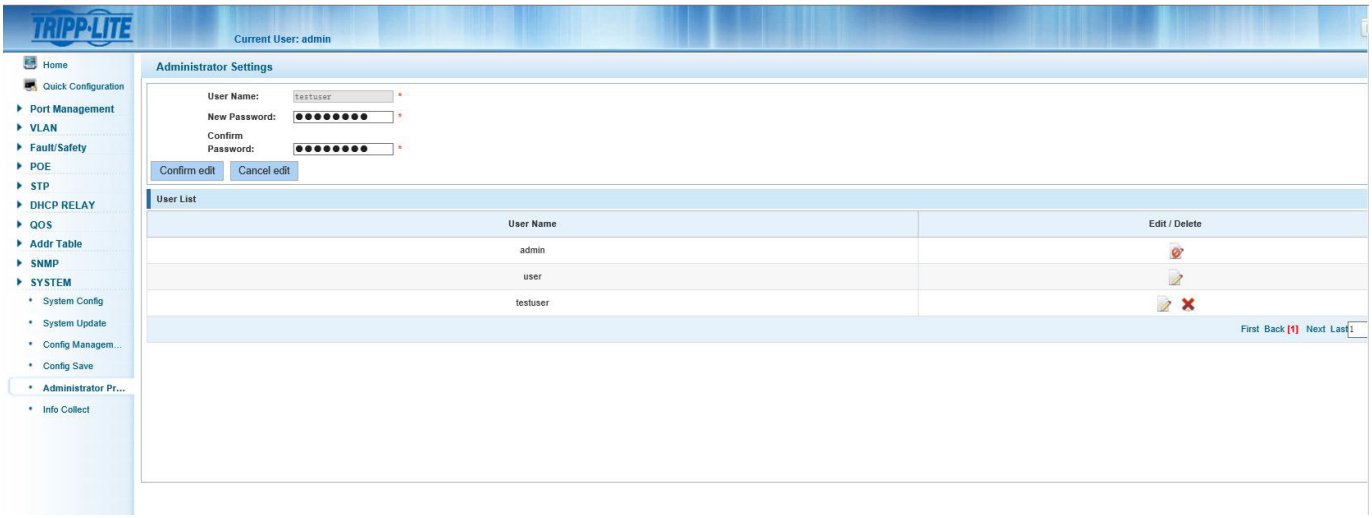


Figure 14.11 : Modifier l'utilisateur

Remarque : *Les comptes « Admin » (administrateur) et « User » (utilisateur) d'origine ne peuvent pas être supprimés. L'administrateur peut modifier le compte utilisateur d'origine et peut supprimer tout autre compte utilisateur créé par le compte administrateur.*

14.6 Recueillir des informations

Cliquer sur le bouton « Collect » (recueillir) (Figure 14.12) pour créer un fichier d'information de débogage avec toutes les informations au sujet du commutateur. Un écran contextuel s'affichera permettant la sauvegarde du fichier d'information de débogage dans le système local. Le fichier d'information de débogage peut ensuite être affiché avec un éditeur de texte comme Notepad, Wordpad, etc.

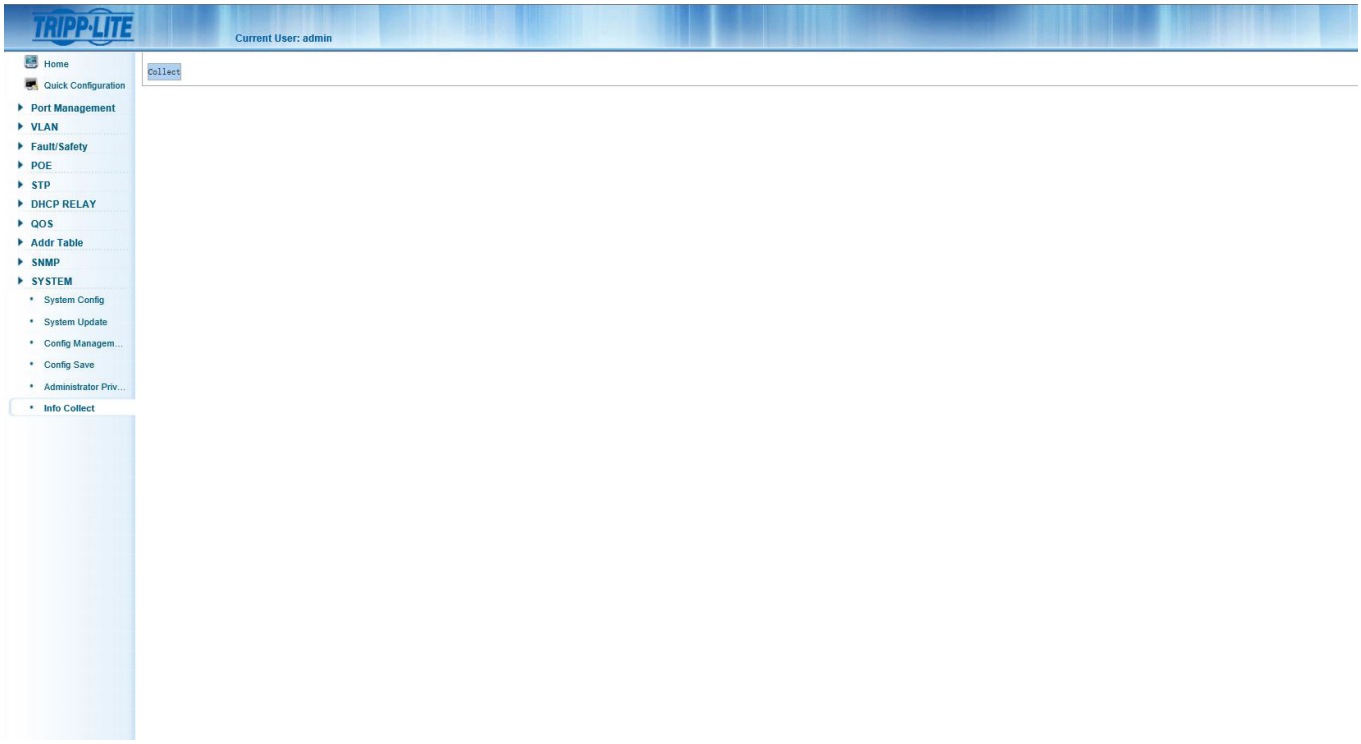


Figure 14.12 : Collecte d'informations

15. Dépannage

Si un problème se pose :

- Vérifier toutes les connexions et confirmer qu'elles sont sécurisées.
- Redémarrer le système et voir si le problème persiste.
- Consulter tripplite.com/support pour des mises à jour du logiciel et s'assurer que la version la plus récente compatible avec l'appareil est utilisée.
- Si le problème persiste après avoir essayé les étapes ci-dessus, contacter le soutien technique de Tripp Lite.

16. Soutien technique

Avant de contacter le soutien technique de Tripp Lite, consulter la Section 15. Dépannage pour des solutions possibles. Si le problème ne peut toujours pas être résolu, contacter le soutien technique de Tripp Lite Technical Support à :

www.tripplite.com/support

Adresse électronique : techsupport@tripplite.com

La politique de Tripp Lite en est une d'amélioration continue. Les caractéristiques techniques sont sujettes à changement sans préavis.