

User's Guide

Network Smart Switch Web Configuration (NSS-Series Smart Switch models)



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

Copyright © 2016 Tripp Lite. All Rights Reserved. All trademarks are the property of their respective owners.

Table of Contents

1	Introduction	4			
1.1	Switch Configurations	4		5.7	Port Speed Limit
1.2	Contents	4		5.7.1	View the Port Speed Limit Settings
2	Web Management Homepage	5		5.7.2	Port Input/Output Speed Limit Configuration
2.1	Setup	5		5.7.3	Edit Port Speed Limit Settings
2.1.1	Set the IP Address of the Computer	5	6	VLAN Management	23
2.1.2	Confirm Network Connectivity Between the Computer and the Switch	5	6.1	VLAN Management	23
2.1.3	Access to the Web Management Interface	5	6.1.1	View VLAN Configuration	23
3	Web Management Interface	7	6.1.2	How to Add a VLAN	23
3.1	Web Management Interface Overview	7	6.1.3	Delete a VLAN	24
3.2	Web Management Interface	7	6.1.4	Edit or Add Ports to an Existing VLAN	24
3.3	Introduction to Page Controls	9	6.1.5	View Trunk Port Settings	25
3.4	Web Management Interface Login Timeout Settings	9	6.1.6	Add Trunk Port Settings	25
4	Quick Configuration	10	6.1.7	Delete a Trunk Port	26
4.1	VLAN Settings	10	7	Fault/Safety	27
4.2	Trunk Port Settings	10	7.1	Attack Prevention	27
4.3	SNMP Settings	11	7.1.1	ARP Spoofing	27
4.4	PoE Settings (Compatible PoE models only)	11	7.1.2	Port Security	29
4.5	Other Settings	12	7.1.3	DHCP Snooping	31
4.5.1	Modify Switch Management IP Address Settings	12	7.2	Path Detection	33
4.5.2	Modify Super-User Password	12	7.3	Loop Detection	33
5	Port Management	13	7.3.1	View Loop Detection Configuration	33
5.1	Basic Settings	13	7.3.2	Enable Loop Detection	34
5.1.1	View the Port Configuration	13	7.3.3	Loop Detection Configuration	34
5.1.2	Configure Individual Ports	13	7.3.4	Detection Time Interval	34
5.2	Storm Control Settings	14	7.3.5	Automatic Recovery Time	35
5.2.1	Configure the Storm Control Settings of a Port	14	7.3.6	Disable Loop Detection	35
5.2.2	Storm Control Configuration	14	7.4	Access Control Lists (ACLs)	35
5.3	Flow Control	15	7.4.1	ACL	35
5.3.1	View Flow Control Settings	15	7.4.2	Apply ACL	38
5.3.2	Flow Control Configuration	15	7.5	IGMP Snooping	40
5.4	Port Isolation	16	7.5.1	IGMP Snooping Configuration	40
5.4.1	View the Port Isolation List	16	7.5.2	Activate the IGMP Snooping Function	40
5.4.2	Port Isolation Configuration	16	7.5.3	Disable the IGMP Snooping Function	41
5.5	Port Aggregation	17	7.5.4	Multicast Routing Port Settings	41
5.5.1	View Port Aggregation Configuration	17	7.5.5	IGMP Version	41
5.5.2	How to Create a Port Aggregation Group	17	8	System Management	42
5.5.3	Modify a Port Aggregation Group	18	8.1	System Settings	42
5.5.4	Delete a Port Aggregation Group	18	8.1.1	Management VLAN	42
5.6	Port Mirroring	19	8.1.2	System Restart	43
5.6.1	View Port Mirroring Configuration	19	8.1.3	Modify the Password	44
5.6.2	Create a Port Mirroring Group	19	8.1.4	System Log	44
5.6.3	Edit a Port Mirroring Group	20	8.1.5	LOG Export	45
5.6.4	Delete a Port Mirroring Group	21	8.1.6	ARP Table	45
			8.1.7	MAC Address Management	45
			8.2	System Upgrade	48

Table of Contents

8.3	System Information	48	9	Power Sourcing Equipment (PSE) System (Select models only)	54
8.3.1	Memory Information	48	9.1	PSE System Configuration	54
8.3.2	CPU Information	49	9.1.1	View PSE System Configuration	54
8.4	Configuration Management	49	9.1.2	Enable or Disable Uninterrupted PoE Power	54
8.4.1	Configuration Management	49	9.1.3	Non-standard PD Compatibility	55
8.4.2	Restore the Factory Settings	51	9.1.4	Modify Power Supply Mode	55
8.5	SNMP	51	9.1.5	PoE Guard Band Configuration	56
8.5.1	View SNMP	51	9.1.6	Abnormal Recovery Time Interval Configuration	57
8.5.2	Enable or Disable SNMP Service	51	9.2	PoE Port Configuration	58
8.5.3	Enable or Disable SNMP TRAP Service	52	9.2.1	View the PoE Port Configuration	58
8.5.4	Add Community Name	52	9.2.2	Enable Power Supply	58
8.5.5	Delete Community Name	52	9.2.3	Modify Port Description	59
8.5.6	Add SNMP TRAP Service Host	53	9.2.4	Modify Priority	60
8.5.7	Delete SNMP TRAP Service Host	53	9.2.5	Modify Port Max Power	60
8.6	System Diagnostics	53	9.2.6	Modify Recovery Mode	61
			9.2.7	Modify Distribution of Power	61
			Appendix I: Default Switch Configurations	62	
			Technical Support	62	

1 Introduction

This manual describes how to configure the Tripp Lite Network Smart Switch models by using the built-in Web-based graphical user interface (GUI). Tripp Lite Network Smart Switch models contain an embedded web server and management software for managing and monitoring switch functions. Tripp Lite Network Smart Switch models function as simple switches without the use of the management software. The management software can be used to configure more advanced features that can improve switch efficiency and overall network performance.

Note: Network 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 will be consistent.

1.2 Contents

- **Section 1:** This section contains the contents overview of the entire configuration manual.
- **Section 2: How to Access the Web Management Interface.** This section contains the setup that needs to be done before you login, along with instructions for logging into the switch's Web management interface.
- **Section 3: Introduction and Overview of the Web Management Interface.** This section will help you to become familiar with the Web management interface.
- **Section 4: Quick Configuration.** This section will illustrate how to quickly setup the management features through the Web interface.
- **Section 5: Port Management.** This section presents some commonly used settings for the switch ports.
- **Section 6: VLAN Management.** This section gives an overview of the management and configuration of VLAN(s).
- **Section 7: Fault/Safety.** This section describes safety management and configuration, such as attack prevention, access control lists, etc.
- **Section 8: System Management.** This section contains a guide to the switch system management, including software upgrades through the Web page, configuration file management, etc.
- **Section 9: PSE System Management.** This section contains a guide to setup the PoE power supply management through the Web page (only applicable in PoE enabled switches).
- **Appendix I: Default Settings.** This appendix contains the default settings for login, password, etc., for quick reference.

2 Web Management Homepage

2.1 Setup

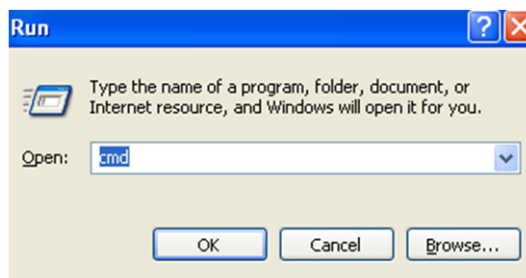
2.1.1 Set the IP Address of the Computer

- The IP address of the management computer and the switch must be set to the same subnet (switch's default IP address is 192.168.1.200 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.
- By default, all ports belong to VLAN1. The management host computer can perform switch configuration by access to any port.

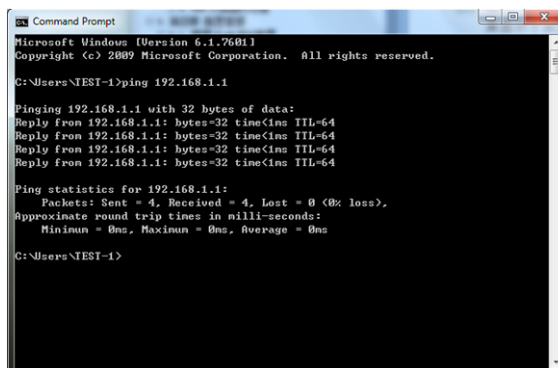
2.1.2 Confirm Network Connectivity Between the Computer and the Switch

Follow these steps 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 will bring you to the command prompt window.



Step 2: In the command prompt dialog box, type **ping 192.168.1.200** then press “Enter”. If a response to the ping is returned from the switch, you have established proper network connectivity. If no response is received, check your network connection.



2.1.3 Access to the Web Management Interface

Open a Web browser (e.g. Internet Explorer), type **http://192.168.1.200** in the address bar, then press “Enter”. You will enter the User Login interface of the switch administration page. In the Login interface, select your language then enter the user name and password. The default language is English. The default user name and password are both **admin** (case sensitive). Click the “Login” button or press “Enter” to access the Web management interface.

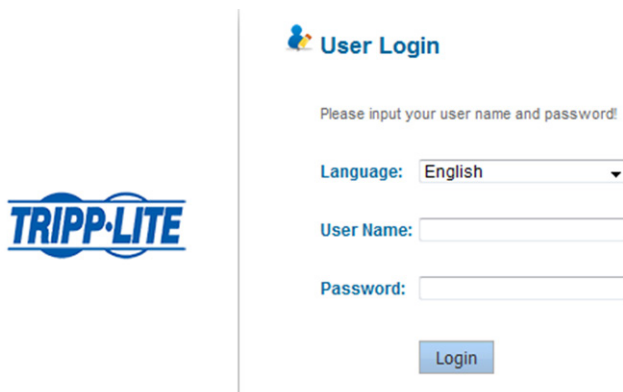


Figure 2-1 Web Landing Page

2 Web Management Homepage

After a successful login, the browser will show you the homepage of the WEB management interface corresponding to your switch, as illustrated below:

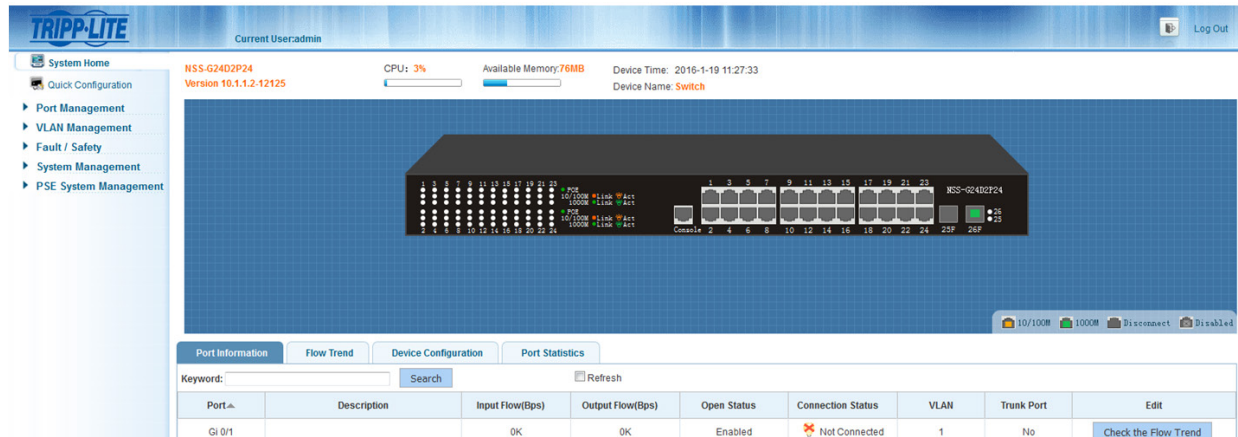


Figure 2-2 Switch Web Management Interface

Notes:

- This manual is appropriate for all models in Tripp Lite's family of web managed switches. The manual uses one switch configuration as an example to illustrate how to configure the switch using the web management interface.
- It is recommended to use Internet Explorer 8 or higher with the web management interface.

3 Web Management Interface

3.1 Web Management Interface Overview

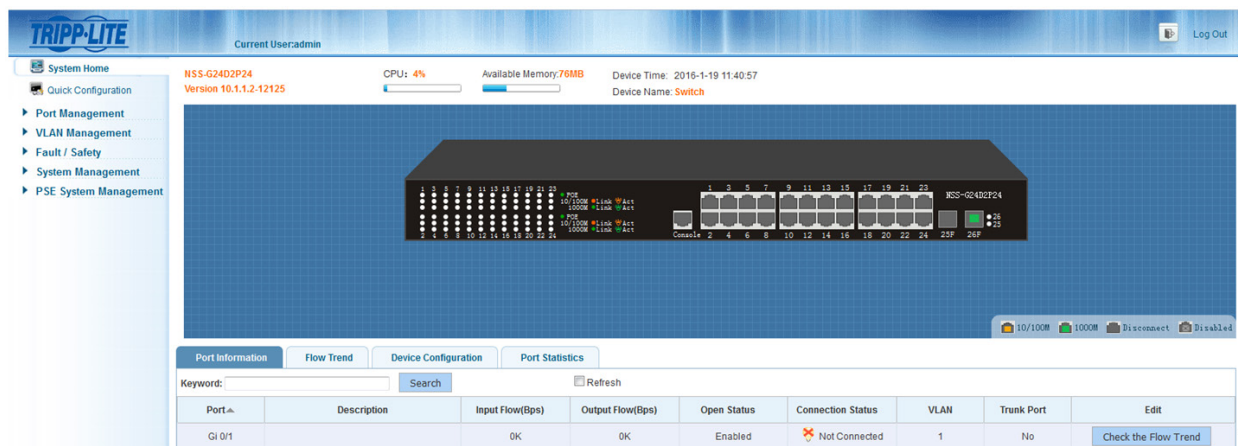


Figure 3-1 Web Management Interface

3.2 Web Management Interface



Figure 3-2 Web Management Interface Main Menu

Notes:

- In the web management interface, there are 7 primary menu options: System Home, Quick Configuration, Port Management, VLAN Management, Fault/ Safety, System Management and PSE System Management (applicable in PoE enabled switches).
- Each primary menu option contains a secondary menu. By default, the secondary menus are hidden. Click on each primary menu option to expand the secondary menu.

3 Web Management Interface

The following table lists every primary menu and its secondary menu options:

Primary Menu	Secondary Menu	Page Function
System Home	N/A	Displays the front panel of the switch, model name and SW version.
Quick Configuration	N/A	Allows for configuration of the following settings: VLAN, Trunk, SNMP and PoE (where applicable).
Port Management	Basic Settings	Port description, status, rate, working mode, MTU settings.
	Storm Control	Set the storm threshold of broadcast, multicast, and unicast storms.
	Flow Control	Adjust the flow control of any port.
	Port Isolation	Set isolation to either port to port or port to link group.
	Port Aggregation	View port aggregation groups of the switch, and add/delete/modify aggregation settings.
	Port Mirroring	Set mirroring port and mirrored port. One port can be set as a mirror port to many mirrored ports.
	Port Speed Limit	View and modify the upstream and downstream rate limits of a port.
VLAN Management	VLAN Management	1. Add or delete VLANs, add ports to a VLAN or remove ports from a VLAN. 2. Add or delete a Trunk, add ports to a Trunk or remove ports from a Trunk.
Fault/Safety	Attack Prevention	1. View the ARP state table, activate or deactivate the ARP anti-spoofing functions of a port. 2. Enable or disable port security and set up a binding IP address and MAC address for a port. 3. Prevent illegal DHCP server functions and set a port to trust/untrusted state.
	Path Detection	Used to detect the connectivity of the switch with other devices.
	Loop Detection	Enable Loop Detection to avoid broadcast storm problems caused by accidental network loops.
	Access Control	Configure ACLs (Access Control Lists) with IP addresses, IP rules and MAC rules. Set this up to allow or deny certain traffic to certain IP and MAC addresses.
	IGMP Snooping	Activate or disable IGMP Snooping, add or edit multicast configurations.
System Management	System Settings	1. Set the management VLAN IP address and subnet mask. 2. Reboot the system. 3. Change the user password and the telnet login password. 4. View and export system log. 5. Check an ARP entry. 6. Query the MAC address table, set static MAC address and add or delete static MAC Addresses.
	System Upgrade	Upgrade the switch software.
	System Information	1. Memory usage. 2. System tasks.
	Configuration Management	1. Backup, restore the system configuration backup. 2. Restore the default factory configuration.
	SNMP	Enable SNMP service, configure SNMP trap hosts, and change the SNMP version.
	System Diagnostics	Used to collect and export current switch information.
PSE System	PSE System configuration	View and modify PSE System configuration (in PoE enabled systems).
	PoE port configuration	View and modify PoE port configuration (in PoE enabled systems).

Table 3-1 Web Management Interface Menu

3 Web Management Interface

3.3 Introduction to Page Controls



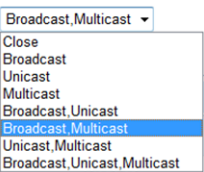







Control	Description
	Field, used for text input, such as VLAN ID, interface description, etc.
	Check box, used to select a specified item.
	Dropdown menus, used to select an item from a menu.
File Name:  No file selected.	Click “browse” to select a software version or a configuration file in the local computer.
	Edit, click to enter edit mode.
	Delete the current rules.
	Refresh the current page configuration.
	Save the current page configuration.
	Cancel the current page configuration or the current system information.
	Confirm the current system information.

Table 3-2 Web Page Controls

3.4 Web Management Interface Login Timeout Settings

If there is no activity in the Web Management Homepage for 5 minutes, the system will automatically logout the user and return to the web management interface login page, as shown in Figure 2-1.

Note: The default inactivity login timeout is set at 5 minutes.

4 Quick Configuration

Select “Quick Configuration” to configure frequently used functions of the Smart switch, such as VLAN, SNMP, PoE, and system network/password management settings.

4.1 VLAN Settings

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

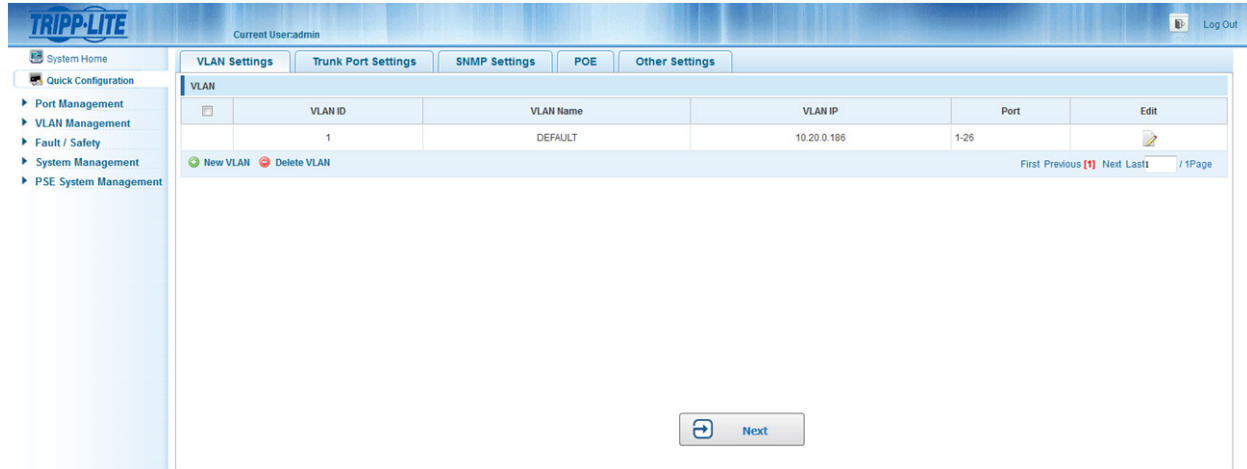


Figure 4-1 VLAN Settings

4.2 Trunk Port Settings

Select “Quick Configuration→Trunk Port 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 “SNMP Settings” page or click “Previous” to return to “VLAN Settings” page.

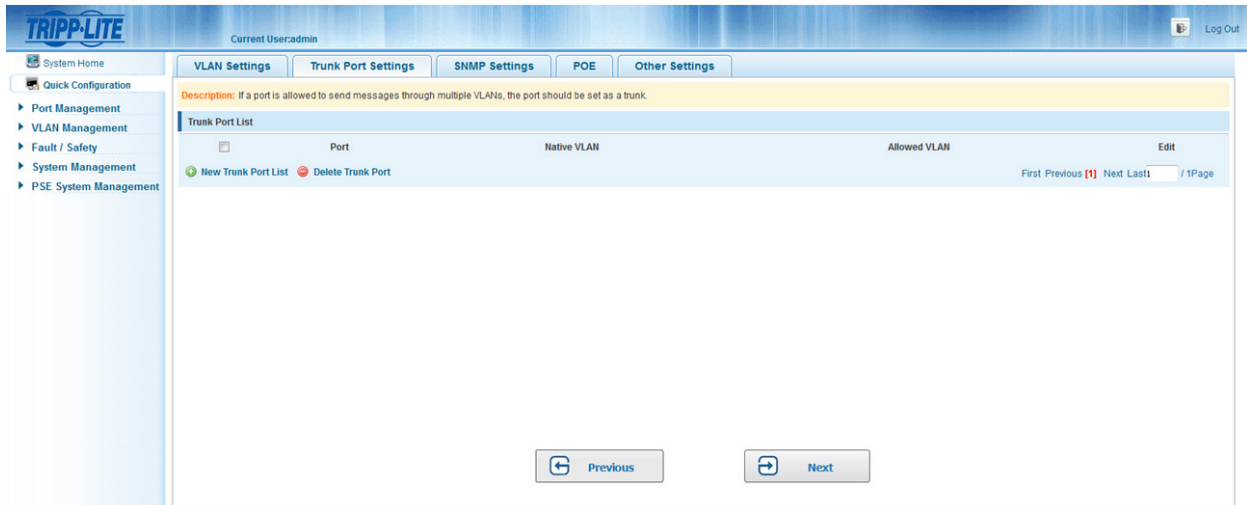


Figure 4-2 Trunk Settings

4 Quick Configuration

4.3 SNMP Settings

Select “Quick Configuration→SNMP Settings” to modify “SNMP Settings”. You can view the “SNMP Settings” for the switch and enable/disable SNMP functions and set SNMP traps. After configuring the “SNMP Settings” click “Next” to go to the “PoE” page (in compatible PoE models), or click “Previous” to return to the “Trunk Port Settings” page.

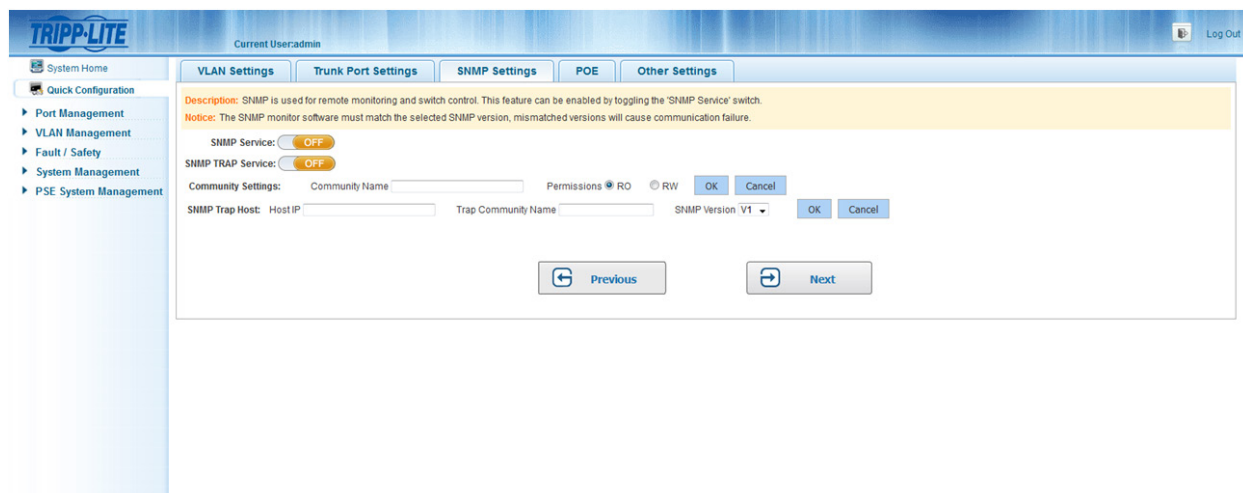


Figure 4-3 SNMP Settings

4.4 PoE Settings (Compatible PoE models only)

Select “Quick Configuration→PoE” to go to the “PoE” configuration page. On this page, you can modify PoE settings for the switch. Complete the configuration of relative port power supply mode, power settings and port priority. After applying the configuration, click “Next” to enter the “Other Settings” page, or click “Previous” to return to the “SNMP Settings” page.

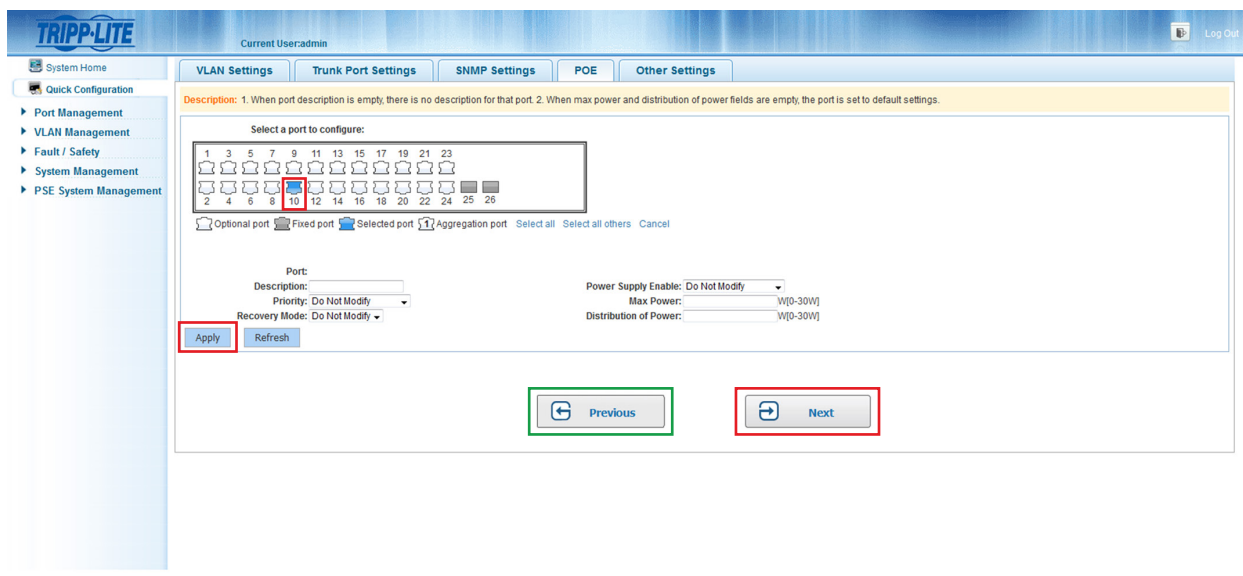


Figure 4-4 PoE Settings

4 Quick Configuration

4.5 Other Settings

Select “Quick Configuration→Other Settings” to view the system settings. From this page, you can change the switch’s IP address, subnet mask, default gateway, login timeout, device name, device location, contact name and information, and management interface password. After you modify the configuration, click “Save”. Click “Complete” to return to the homepage, or click “Previous” to return to previous settings page to further modify the configuration.

The screenshot shows the TRIPP-LITE web configuration interface. The top navigation bar includes 'System Home', 'VLAN Settings', 'Trunk Port Settings', 'SNMP Settings', and 'Other Settings'. The 'Other Settings' tab is selected. The left sidebar shows a tree view with 'Quick Configuration' expanded, containing 'Port Management', 'VLAN Management', 'Fault / Safety', and 'System Management'. The main content area is titled 'The basic information of the system settings' and contains two sections. The first section, 'VLAN Management', has a dropdown menu set to 'Vlan 1' and fields for Management IP (192.168.1.200), Subnet Mask (255.255.255.0), Default Gateway (192.168.1.1), Login Timeout (30), Management Port (80), MAC (24-05-0F-68-02-32), Device Name (Switch), Device Location, Contact Name, and Contact Information. A 'Save' button is below these fields. The second section, 'Modify the super user password', has fields for Old Password, New Password, and Confirm New Password, with 'Save' and 'Empty' buttons below. At the bottom of the page are 'Previous' and 'Complete' buttons.

Figure 4-5 Other Settings

The Other Settings page shows basic system settings.

- **VLAN Management:** 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.
- **Default Gateway:** The default gateway of the switch’s management VLAN.
- **Login Timeout:** When the web configuration interface is idle for more than five minutes, the browser will return to the login interface by default.
- **Management Port:** The Management defaults to 80.
- **MAC:** The MAC Address of the switch.
- **Device Name:** The hostname of the switch.
- **Device Location:** The location of the switch.
- **Contact Name:** Enter the name of the administrator.
- **Contact Information:** Enter administrator’s contact number or e-mail address.

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

4.5.1 Modify Switch Management IP Address Settings

To set the management IP address of the switch, do the following:

1. Enter the IP address in the “Management IP” field (e.g. 192.168.100.179).
2. Enter the subnet mask in the “Subnet Mask” field (e.g. 255.255.255.0).
3. Enter the gateway address in the “Default Gateway” field (e.g. 192.168.100.1).
4. Click “Save” to complete the configuration.

4.5.2 Modify Super-User Password

To edit the switch’s super-user password, enter the default password or prior password, then enter your new password (case sensitive), and finally enter your new password (case sensitive) again to confirm it. Click “Save” to commit to the changes or “Empty” 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.

The screenshot shows the 'Basic Settings' page for port configuration. On the left is a navigation menu with 'Port Management' expanded, showing 'Basic Settings' as the selected option. The main content area has a header 'Basic Settings' and a description: 'Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.' Below this is a grid of 24 port icons arranged in two rows of 12. A box highlights ports 1 through 10. Below the grid are radio buttons for 'Optional port', 'Fixed port', 'Selected port' (which is selected), and 'Aggregation port'. There are also links for 'Select all', 'Select all others', and 'Cancel'. Below these are input fields for 'Description:', 'Status: Do Not Modify', 'Rate: Do Not Modify', 'Duplex Mode: Do Not Modify', and 'MTU(64-10240):'. A 'Save' button is at the bottom left. At the bottom is a 'Port List' table with 7 columns: Port, Description, Status, Rate, Duplex Mode, MTU, and Edit. The table contains 3 rows of data for ports 1, 2, and 3.

Port	Description	Status	Rate	Duplex Mode	MTU	Edit
1		Enabled	Auto	Auto	1518	
2		Enabled	Auto	Auto	1518	
3		Enabled	Auto	Auto	1518	

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 name or description given to the port.
- **Status:** Displays the port status, either “Enabled” or “Disabled”.
- **Rate:** Port rate information, displays either auto-negotiation, 10, 100 or 1000 Mbps.
- **Duplex Mode:** Displays port duplex configuration, auto-negotiation, full duplex or half duplex.
- **MTU:** (Maximum Transmission Unit) displays the maximum packet size allowed by the port.

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

5.1.2 Configure Individual Ports

Select the port(s) you would like to configure from the panel, then click the icon in the edit column to change the settings of the selected port.

The screenshot shows the 'Individual Port Configuration' page. The navigation menu is the same as in Figure 5-1. The main content area has a header 'Basic Settings' and the same description. Below the port grid, the 'Selected port' radio button is selected. The 'Description:' field is empty. The 'Status:' dropdown is set to 'Enabled'. The 'Rate:' dropdown is set to 'Auto'. The 'Duplex Mode:' dropdown is set to 'Auto'. The 'MTU(64-10240):' field is set to '1518'. A 'Save' button is at the bottom left. The 'Port List' table at the bottom now contains 4 rows of data for ports 1, 2, 3, and 4.

Port	Description	Status	Rate	Duplex Mode	MTU	Edit
1		Enabled	Auto	Auto	1518	
2		Enabled	Auto	Auto	1518	
3		Enabled	Auto	Auto	1518	
4		Enabled	Auto	Auto	1518	

Figure 5-2 Individual Port Configuration

Note: Within the individual port configuration screen, the following settings can be changed: Description, Status, Rate, Duplex Mode and MTU.

5 Port Management

5.2 Storm Control Settings

5.2.1 Configure the Storm Control Settings of a Port

Select “Port Management→Storm Control” to change the “Storm Control” settings of a selected port.

Current User: admin

System Home Quick Configuration

Port Management

- Basic Settings
- Storm Control
- Flow Control
- Port Isolation
- Port Aggregation
- Port Mirroring
- Port Speed Limit

VLAN Management

Fault / Safety

System Management

PSE System Management

Storm Control

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Note: If the parameters selected are not supported, the changes will not take effect.

Select a port to configure:

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Storm Control Type: Disabled Storm Control Value: (Unit: kbps, Value: multiples of 64 between 64-200000)

Save

Port	Unicast	Broadcast	Multicast	Edit
1	Disabled	Disabled	Disabled	
2	Disabled	Disabled	Disabled	
3	Disabled	Disabled	Disabled	
4	Disabled	Disabled	Disabled	

Figure 5-3 Storm Control Configuration Table

The table above displays the storm control configuration of the switch by port.

- Storm Control Type:** Displays the types of storm control settings that can be configured (Disabled, Broadcast, Unicast, Multicast, Broadcast/Unicast, Broadcast/Multicast, Unicast/Multicast, Broadcast/Unicast/Multicast).
- Storm Control Value:** Set the rate at which storm control will be activated (between 64-200000, multiples of 64 only).
- Port:** Displays the switch's port number.
- Unicast:** Displays whether unicast packet control is enabled or disabled.
- Broadcast:** Displays whether broadcast packet control is enabled or disabled.
- Multicast:** Displays whether multicast packet control is enabled or disabled.

Notes:

- If the control value is not a multiple of 64, the system will automatically select the closest multiple of 64.
- The storm control value will be the same for unicast, broadcast and multicast.

5.2.2 Storm Control Configuration

Select the port(s) you would like to configure.

Select a port to configure:

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Storm Control Type: Disabled Storm Control Value: (Unit: kbps, Value: multiples of 64 between 64-200000)

Save

Figure 5-4 Set Multiple Ports Simultaneously

Click the “Storm Control Type” dropdown menu to select the type of storm control you would like to configure for the port. Type any multiple of 64 (from 64-200000) into the “Storm Control Value” field and then click “Save” to complete the configuration.

Storm Control Type: Broadcast, Multicast

Storm control value: 64 (Unit: kbps, value 64-200000 within a multiple of 64)

Save

Port	Unicast	Broadcast	Multicast	Operation
1	Disabled	Disabled	Disabled	

Figure 5-5 Storm Control Configuration Information

5 Port Management

After successfully configuring a port, the page will show the following:


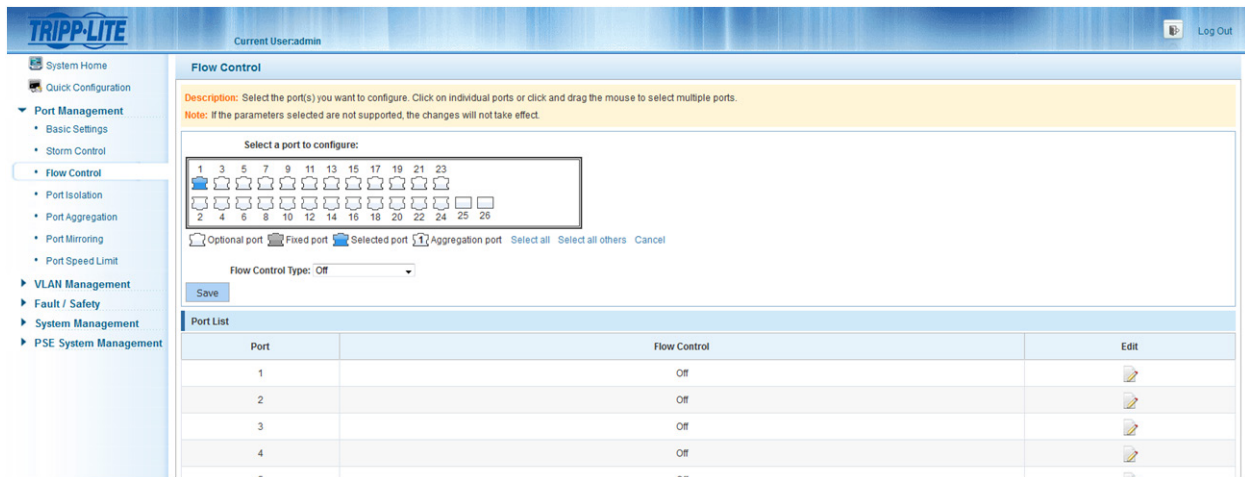
Port List				
Port	Unicast	Broadcast	Multicast	Operation
1	Disabled	64	64	

Figure 5-6 Successful Storm Control Configuration

5.3 Flow Control

5.3.1 View Flow Control Settings

Select “Port Management→Flow Control” to configure flow control settings for any port(s).



Flow Control

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Note: If the parameters selected are not supported, the changes will not take effect.

Select a port to configure:

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Flow Control Type: Off

Save





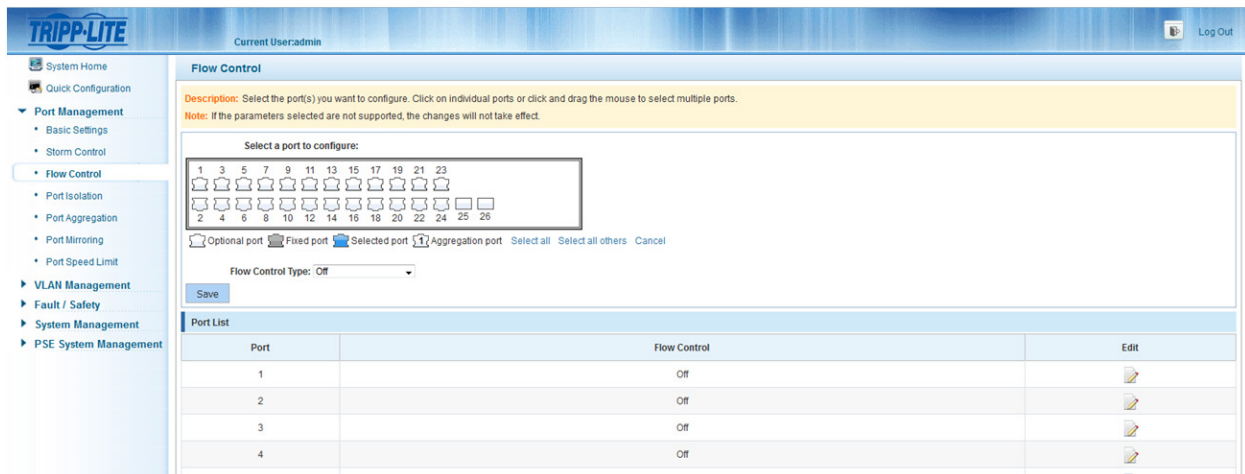
Port	Flow Control	Edit
1	Off	
2	Off	
3	Off	
4	Off	

Figure 5-7 Flow Control Configuration Table

5.3.2 Flow Control Configuration

In order to enable port flow control function, select the port(s) you want to configure, click the drop down menu “Flow Control Type”, select “On” and click “Save”.



Flow Control

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Note: If the parameters selected are not supported, the changes will not take effect.

Select a port to configure:

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Flow Control Type: On

Save





Port	Flow Control	Edit
1	On	
2	On	
3	On	
4	On	

Figure 5-8 Enable Port Flow Control Function

5 Port Management

After choosing the configuration, the port list will show the following:






Port List			
Port	Flow Control		Operation
1	On		
2	Off		
3	On		
4	Off		
5	Off		

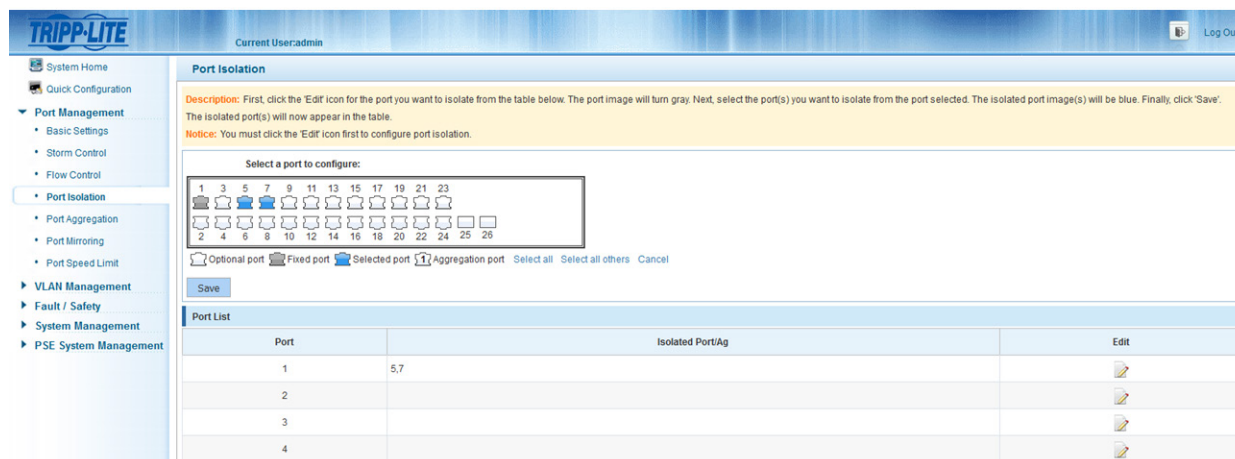
Figure 5-9 Flow Control Settings

To disable the flow control function, select the port(s) from the panel and select “Off” from the “Flow Control Type” dropdown menu. The icon can also be used to modify any individual port.

5.4 Port Isolation

5.4.1 View the Port Isolation List

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



Port Isolation

Description: First, click the 'Edit' icon for the port you want to isolate from the table below. The port image will turn gray. Next, select the port(s) you want to isolate from the port selected. The isolated port image(s) will be blue. Finally, click 'Save'. The isolated port(s) will now appear in the table.

Notice: You must click the 'Edit' icon first to configure port isolation.

Select a port to configure:

1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24 25 26

☐ Optional port ☒ Fixed port ☒ Selected port ☐ Aggregation port






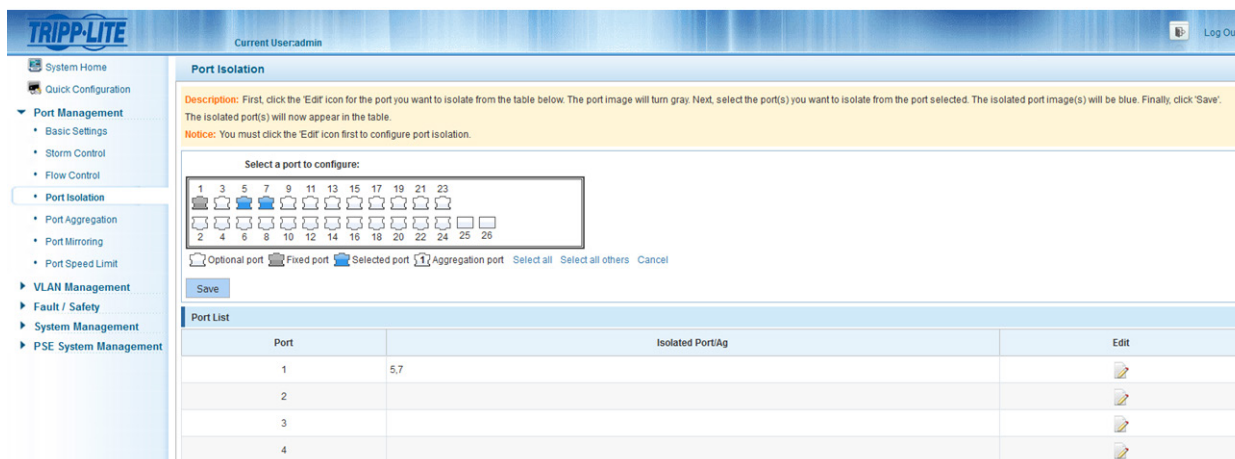
Port	Isolated Port/Ag	Edit
1	5,7	
2		
3		
4		

Figure 5-10 View Port Isolation List

5.4.2 Port Isolation Configuration

Click the  icon in the port list table and select the port you want to isolate. The port will turn gray on the panel. Next, select the ports you want to isolate 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.



Port Isolation

Description: First, click the 'Edit' icon for the port you want to isolate from the table below. The port image will turn gray. Next, select the port(s) you want to isolate from the port selected. The isolated port image(s) will be blue. Finally, click 'Save'. The isolated port(s) will now appear in the table.

Notice: You must click the 'Edit' icon first to configure port isolation.

Select a port to configure:

1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24 25 26

☐ Optional port ☒ Fixed port ☒ Selected port ☐ Aggregation port






Port	Isolated Port/Ag	Edit
1	5,7	
2		
3		
4		

Figure 5-11 Port Isolation Configuration

Note: Click the  icon first. The gray port in the port panel represents the port being configured while the blue ports represent ports from which the selected port is isolated.

5 Port Management

5.5 Port Aggregation

5.5.1 View Port Aggregation Configuration

Select “Port Management→Port Aggregation” to view the switch’s port aggregation configuration. Port Aggregation (or link aggregation) allows you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing.

Current User: admin

System Home Quick Configuration

Port Management

- Basic Settings
- Storm Control
- Flow Control
- Port Isolation
- Port Aggregation
- Port Mirroring
- Port Speed Limit

VLAN Management

- VLAN Management

Fault / Safety

- Attack Prevention
- Path Detection
- Loop Detection
- Access Control
- IGMP Snooping

Port Aggregation

Description: Port aggregation allows multiple ports to be combined to form a single logical link. Each group can contain up to 8 ports. Aggregation groups must contain an even number of ports.

Load Balancing: mac Apply

Aggregation ID (1-16):

Select a port to configure:

1	3	5	7	9	11	13	15	17	19	21	23
2	4	6	8	10	12	14	16	18	20	22	24

Optional port Fixed port Selected port 1 Aggregation port Select all Select all others Cancel

Aggregation Type: Not Selected

Save Cancel

Aggregation ID	Aggregation Type	Number of Ports	Member Port	Edit
1	Dynamic	4	1,2,3,4	

First Previous 1 Next Last 1 / 1Page

Figure 5-12 View Port Aggregation Configuration

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

- **Aggregation Number:** Displays the number assigned to the aggregation group.
- **Aggregation Type:** Displays whether the group’s aggregation type is dynamic or static.
- **Number of Ports:** Displays the number of ports in a link aggregation group.
- **Member Ports:** Displays the port numbers that comprise a link aggregation group.

Notes:

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

5.5.2 How to Create a Port Aggregation Group

To create a port aggregation group, select the type of load balancing (mac, ipmac or ip), and click ‘Apply’. Then enter a port aggregation ID, select the ports that you would like to aggregate, and select the aggregation type (dynamic or static). Click “Save” to complete the configuration. When a port is part of an aggregation group, it will appear as 1 in the panel.

Current User: admin

System Home Quick Configuration

Port Management

- Basic Settings
- Storm Control
- Flow Control
- Port Isolation
- Port Aggregation
- Port Mirroring
- Port Speed Limit

VLAN Management

- VLAN Management

Fault / Safety

- Attack Prevention
- Path Detection
- Loop Detection
- Access Control
- IGMP Snooping

Port Aggregation

Description: Port aggregation allows multiple ports to be combined to form a single logical link. Each group can contain up to 8 ports. Aggregation groups must contain an even number of ports.

Load Balancing: mac Apply

Aggregation ID (1-16):

Select a port to configure:

1	3	5	7	9	11	13	15	17	19	21	23
2	4	6	8	10	12	14	16	18	20	22	24

Optional port Fixed port Selected port 1 Aggregation port Select all Select all others Cancel

Aggregation Type: Not Selected

Save Cancel


Aggregation ID	Aggregation Type	Number of Ports	Member Port	Edit
1	Dynamic	4	1,2,3,4	

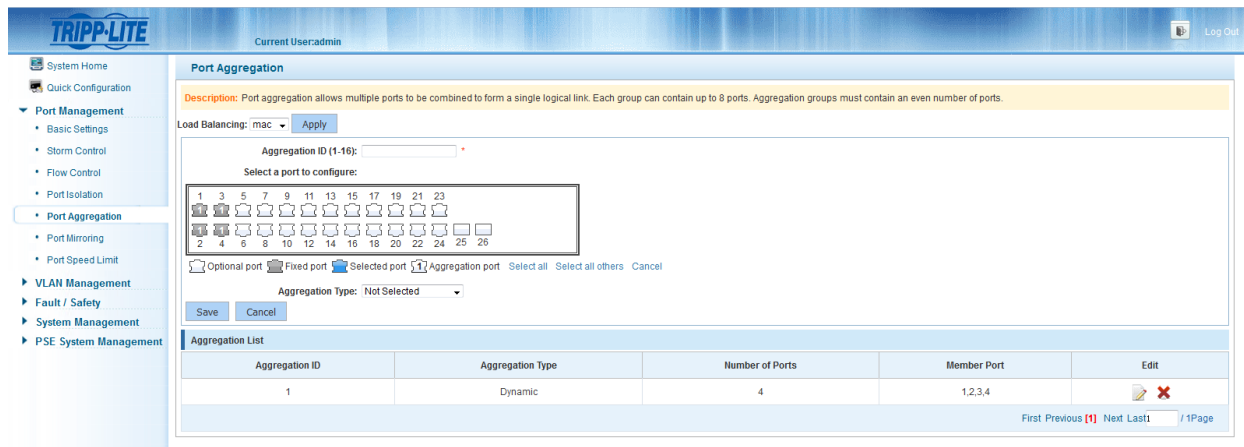
First Previous 1 Next Last 1 / 1Page

Figure 5-13 Port Aggregation Configuration

5 Port Management

5.5.3 Modify a Port Aggregation Group

Click the  icon next to the group number from the aggregation list you would like to modify. Once the group is selected, ports can be added or removed by clicking the panel. The aggregation type can also be changed from dynamic to static, or vice versa.



Tripp-Lite

Current User: admin

Log Out

System Home

Quick Configuration

Port Management

- Basic Settings
- Storm Control
- Flow Control
- Port Isolation
- Port Aggregation
- Port Mirroring
- Port Speed Limit

VLAN Management

Fault / Safety

System Management

PSE System Management

Port Aggregation

Description: Port aggregation allows multiple ports to be combined to form a single logical link. Each group can contain up to 8 ports. Aggregation groups must contain an even number of ports.

Load Balancing: mac Apply

Aggregation ID (1-16):



Select a port to configure:

1	3	5	7	9	11	13	15	17	19	21	23		
2	4	6	8	10	12	14	16	18	20	22	24	25	26

☐ Optional port ☐ Fixed port ☒ Selected port ☒ Aggregation port [Select all](#) [Select all others](#) [Cancel](#)

Aggregation Type: Not Selected

Save Cancel

Aggregation ID	Aggregation Type	Number of Ports	Member Port	Edit
1	Dynamic	4	1,2,3,4	 

First Previous **1** Next Last 1 / 1Page

Figure 5-14 Modify Port Aggregation Group

5.5.4 Delete a Port Aggregation Group

Click the  icon next to the port aggregation group you would like to delete.

Aggregation List				
Aggregation ID	Aggregation Type	Number of Ports	Member Port	Edit
1	Dynamic	4	1,2,3,4	 

First Previous **1** Next Last 1 / 1Page

Figure 5-15 Delete Port Aggregation

5 Port Management

5.6 Port Mirroring

5.6.1 View Port Mirroring Configuration

Select “Port Management→Port Mirroring” to view the port mirroring configuration. 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 that are 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 5-16 Port Mirroring Configuration

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

- **Mirroring Group:** Mirror group ID; up to 7 mirroring groups can be created.
- **Source Port(s):** The port(s) that the mirrored data comes from.
- **Destination Port:** The port to which the mirrored data will arrive.
- **S1 Mirroring Group:** Appears when a port is part of a mirroring group.

Notes:

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

5.6.2 Create a Port Mirroring Group

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

Figure 5-17 Add Port Mirroring Group

5 Port Management

Port Mirroring

Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.)

Choose the destination port:(choose only one port)

Optional port Fixed port Selected port Aggregation port Mirroring Group Select all Select all others Cancel

Save Refresh Mirroring Group Not Selected

Mirroring Group	Source Port	Destination Port	Edit
1	1	3	

First Previous (1) Next Last 1/1Page

Figure 5-18 Results after Adding Port Mirroring Group

5.6.3 Edit a Port Mirroring Group

Click the icon next to the port mirroring group you want to modify and make the changes to the mirroring group.

Port Mirroring

Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.)

Choose the destination port:(choose only one port)

Optional port Fixed port Selected port Aggregation port Mirroring Group Select all Select all others Cancel

Save Refresh Mirroring Group Session 1

Mirroring Group	Source Port	Destination Port	Edit
1	1	3	

First Previous (1) Next Last 1/1Page

Figure 5-19 Modify Port Mirroring Group

Port Mirroring

Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.)

Choose the destination port:(choose only one port)

Optional port Fixed port Selected port Aggregation port Mirroring Group Select all Select all others Cancel

Save Refresh Mirroring Group Session 1

Mirroring Group	Source Port	Destination Port	Edit
1	1,3,5	2	

First Previous (1) Next Last 1/1Page

Figure 5-20 Results after a Successful Modification of Port Mirroring

5 Port Management

5.6.4 Delete a Port Mirroring Group

Click the  icon next to the port mirroring group that you want to delete.

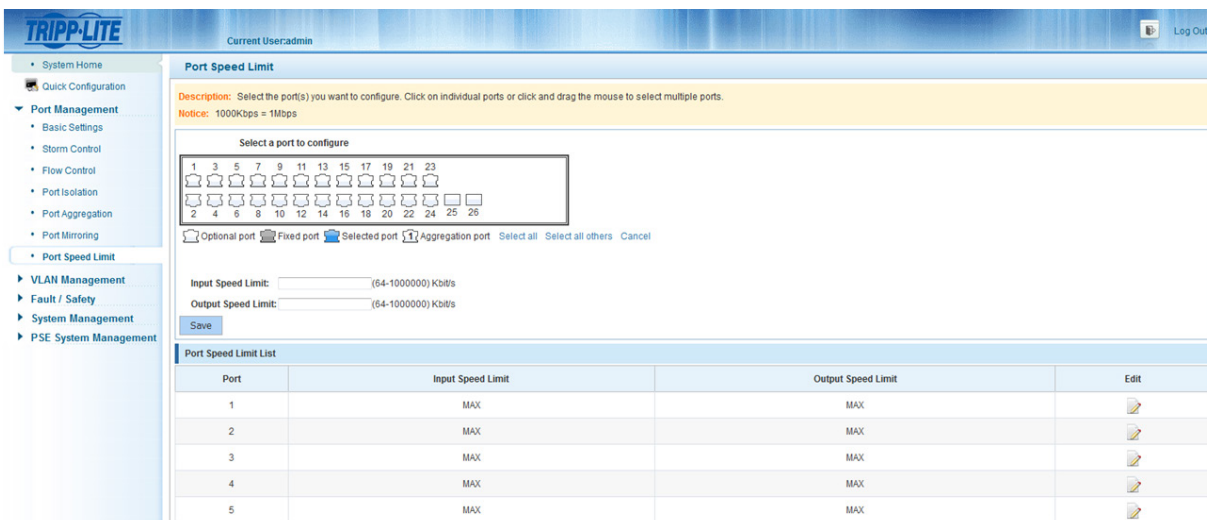
Mirroring Port List			
Mirroring Group	Source Port	Destination Port	Edit
1	1	3	 
First Previous 1 Next Last1 / 1Page			

Figure 5-21 Delete Port Mirroring Group

5.7 Port Speed Limit

5.7.1 View the Port Speed Limit Settings





Select “Port Management→View Port Speed Limit” to view the switch’s Port Speed Limit settings.



Port Speed Limit

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Notice: 100Kbps = 1Mbps

Select a port to configure

Optional port  Fixed port  Selected port  Aggregation port  Select all Select all others Cancel

Input Speed Limit: (64-1000000) Kbit/s
Output Speed Limit: (64-1000000) Kbit/s
Save






Port Speed Limit List			
Port	Input Speed Limit	Output Speed Limit	Edit
1	MAX	MAX	
2	MAX	MAX	
3	MAX	MAX	
4	MAX	MAX	
5	MAX	MAX	

Figure 5-22 View Port Speed Limit Configuration

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

- **Port:** 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

5.7.2 Port Input/Output Speed Limit Configuration

Select the port(s) you want to configure on the port panel. Complete the configuration by entering the speed limit into the field, then clicking “Save”.

TRIPP-LITE Current User: admin Log Out

Port Speed Limit

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Notice: 1000Kbps = 1Mbps

Select a port to configure

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Input Speed Limit: 10000 (64-1000000) Kbit/s
Output Speed Limit: 10000 (64-1000000) Kbit/s

Save

Port	Input Speed Limit	Output Speed Limit	Edit
1	10.000Mbit/s	10.000Mbit/s	
2	MAX	MAX	
3	MAX	MAX	
4	MAX	MAX	

Figure 5-23 Port Input/Output Speed Limit Configuration

5.7.3 Edit Port Speed Limit Settings

Click the icon on the right hand side of the table next to the port you want to modify. Enter a new speed into the field and click “Save”.

TRIPP-LITE Current User: admin Log Out

Port Speed Limit

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Notice: 1000Kbps = 1Mbps

Select a port to configure

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Input Speed Limit: 500000 (64-1000000) Kbit/s
Output Speed Limit: 500000 (64-1000000) Kbit/s

Save

Port	Input Speed Limit	Output Speed Limit	Edit
1	500.000Mbit/s	500.000Mbit/s	

Figure 5-24 Edit Port Speed Limit

6 VLAN Management

6.1 VLAN Management

6.1.1 View VLAN Configuration

Select “VLAN Management→VLAN Management” to view the switch’s VLAN configuration. 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 most 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 dealt with from the management interface rather than the wiring closet.

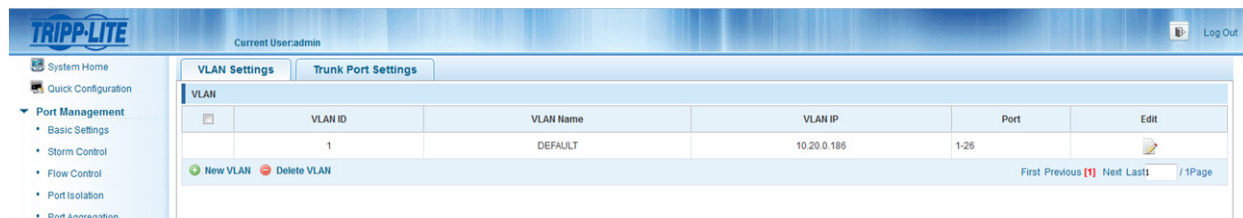


Figure 6-1 VLAN Management Information

The VLAN list shows VLAN configuration of the switch:

- **VLAN ID:** Displays the VLAN identification number.
- **VLAN Name:** Display 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.

6.1.2 How to Add a VLAN

Select “New VLAN” and then enter the VLAN ID (between 2-4094). Enter a VLAN name and click “Save”.

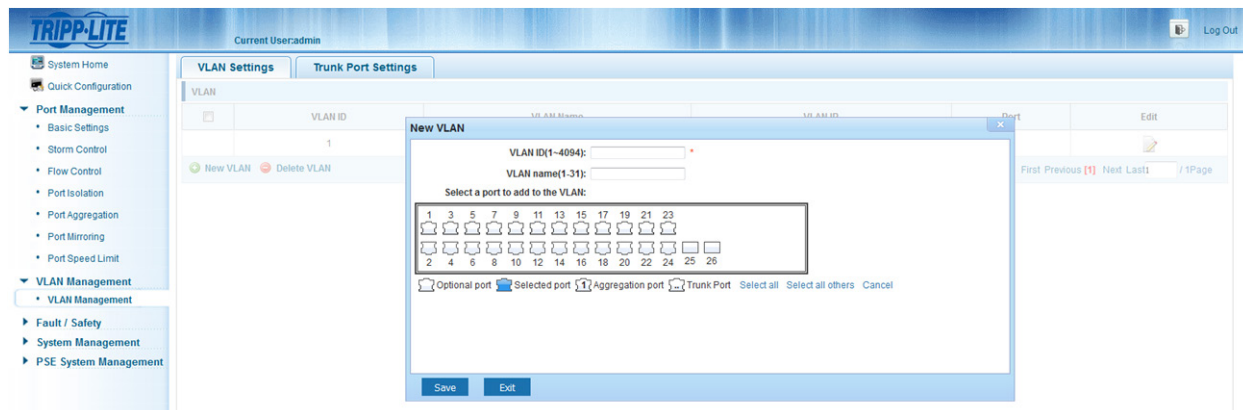


Figure 6-2 Add New VLAN

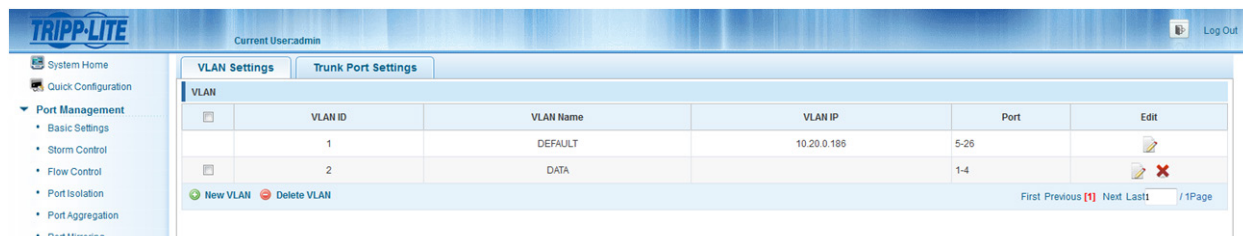


Figure 6-3 Results of Successfully Adding a VLAN

Notes:

- The range of VLAN IDs is 2-4094.
- The system will not allow duplicate VLAN IDs to be created.

6 VLAN Management

6.1.3 Delete a VLAN

1. Delete a Single VLAN:

Select the VLAN from the list that you want to delete, click the  icon to remove the selected VLAN.

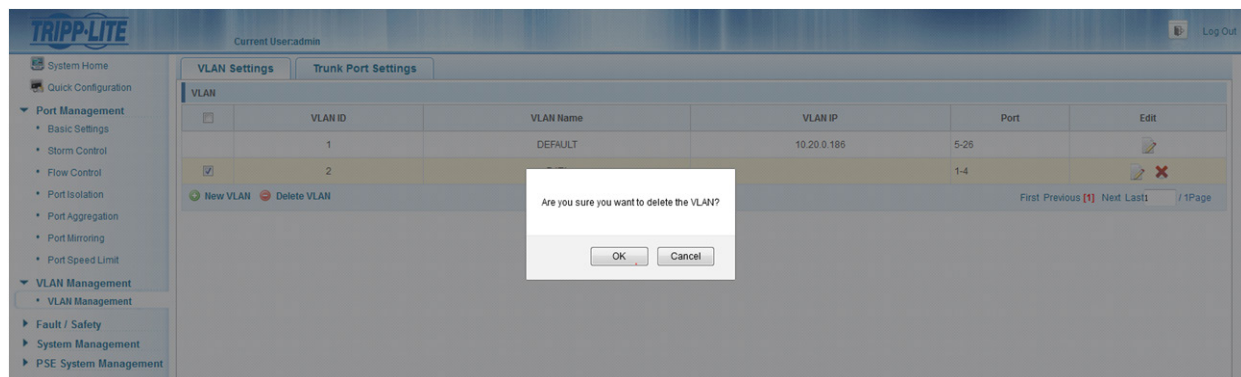


Figure 6-4 Delete a Single VLAN

2. Delete Multiple VLANs:

Click the checkbox next to the VLAN(s) that you want to delete, then click “Delete VLAN” to remove the selected VLAN(s).

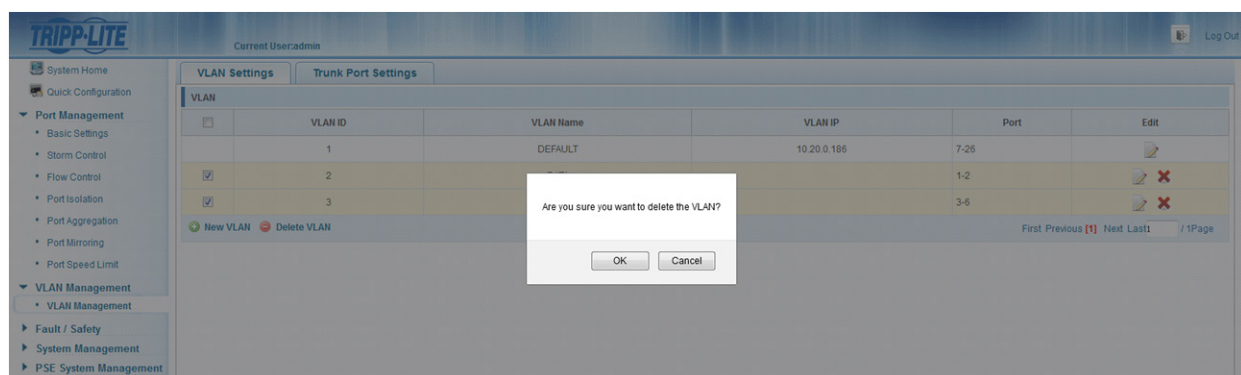


Figure 6-5 Delete Multiple VLANs Simultaneously

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

6.1.4 Edit or Add Ports to an Existing VLAN

1. To add ports to a VLAN:

Click on the  icon. Select the ports you want to add from the port panel, then click “Save”.

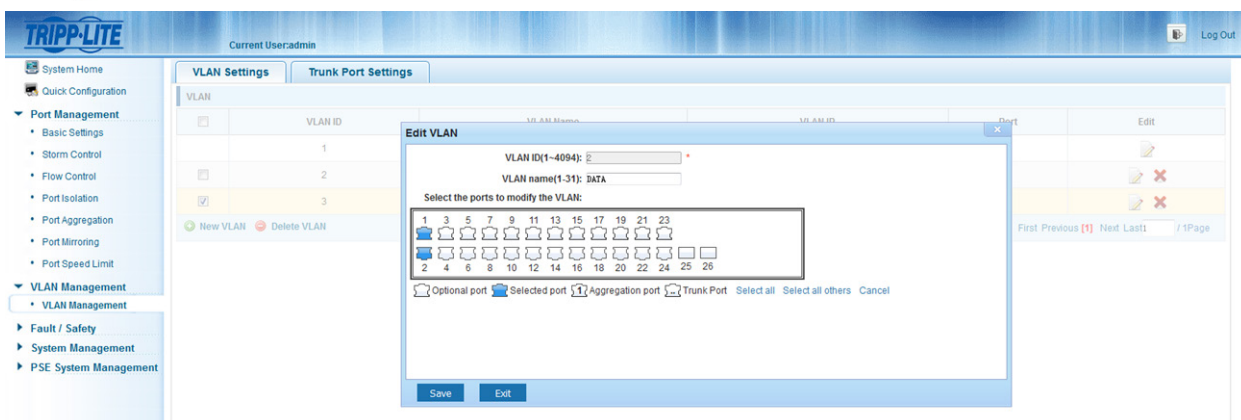


Figure 6-6 Add Ports to a VLAN

6 VLAN Management

2. To remove ports from a VLAN

Click the  icon. Select the ports you want to remove from the port panel, then click “Save”.

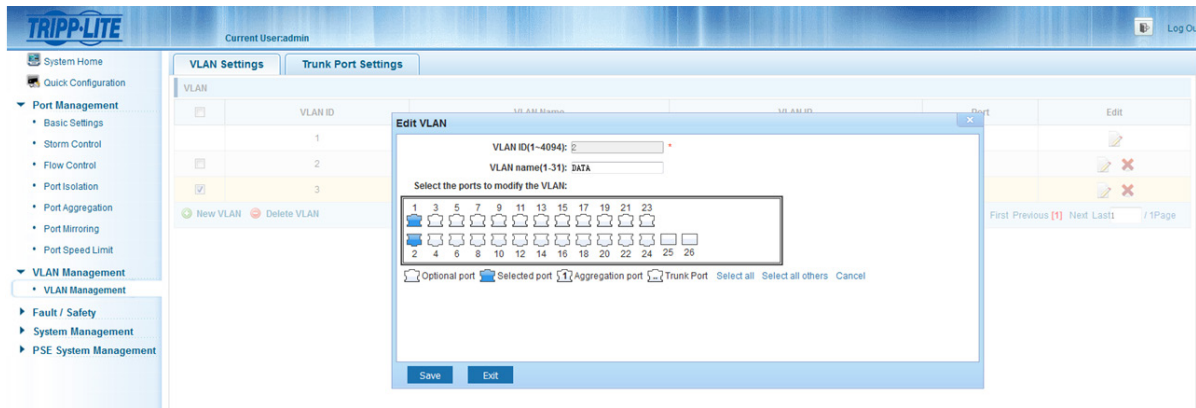


Figure 6-7 Remove Ports from a VLAN

Note: Ports in trunks default to VLAN 1 when they are removed from their original VLAN.

6.1.5 View Trunk Port Settings

Select “VLAN Management→VLAN Management→Trunk Port Settings”, to view the switch’s Trunk port configuration. Trunk ports allow for 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 any tagging (802.1Q). When a trunk port is configured between two switches, the traffic that passes between them will be marked with a tag which will allow the switches to distinguish between packets.

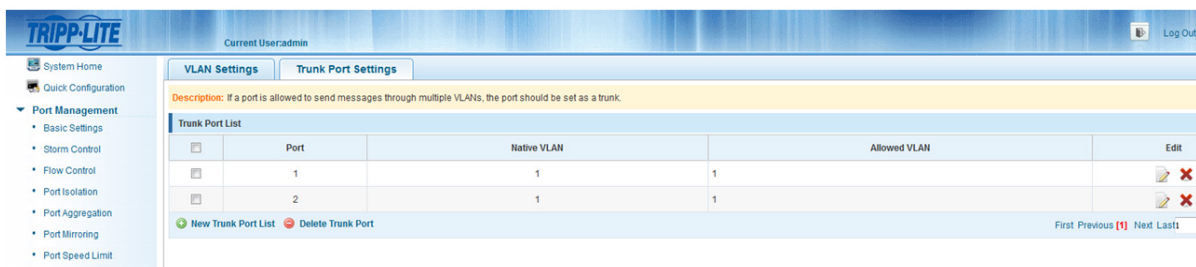


Figure 6-8 View Trunk Port Configuration Information

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.

6.1.6 Add Trunk Port Settings

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

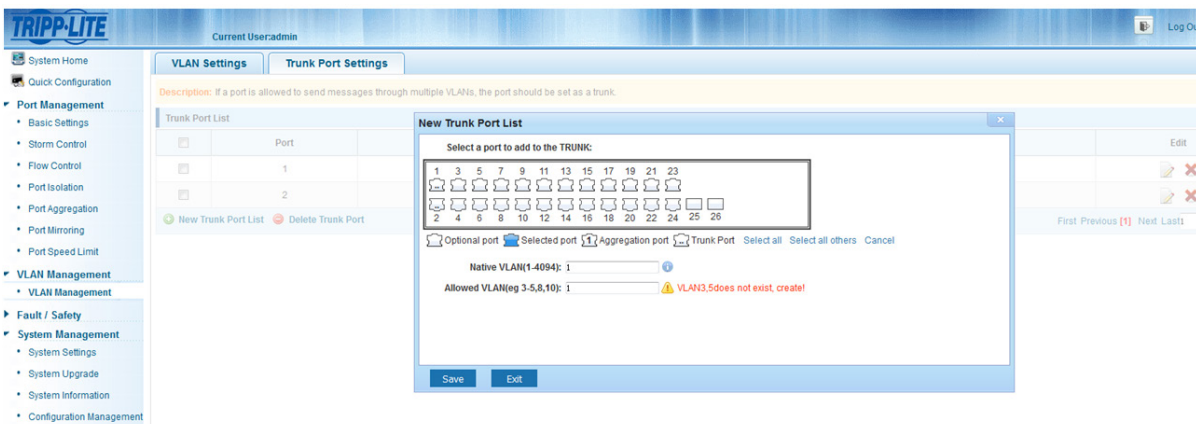



Figure 6-9 Add a Trunk Port

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

6 VLAN Management

6.1.7 Delete a Trunk Port

1. Delete a single Trunk port

Select the Trunk Port that you want to delete, then click the  icon.

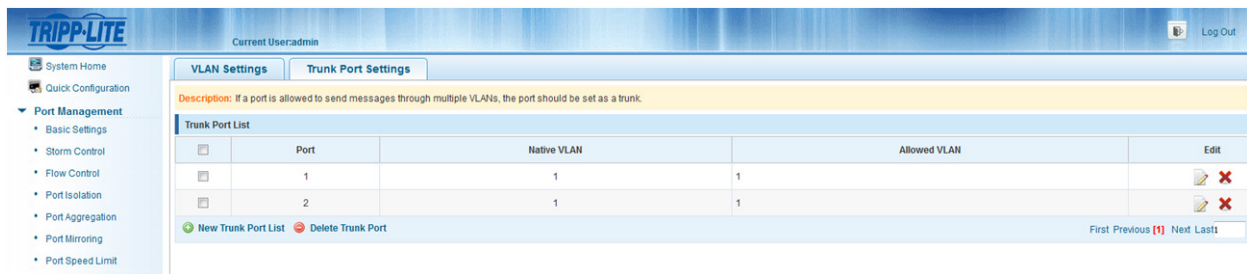


Figure 6-10 Delete a Single Trunk Port

2. Delete multiple Trunk ports

Click the checkbox of the Trunk ports you want to delete, then click “Delete Trunk Port” to delete the selected Trunk ports.

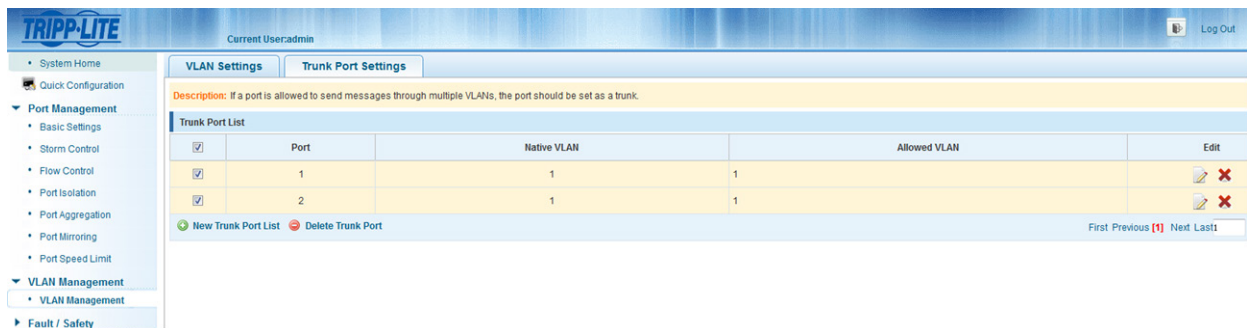


Figure 6-11 Delete Multiple Trunk Ports

7 Fault/Safety

7.1 Attack Prevention

7.1.1 ARP Spoofing

7.1.1.1 View ARP Spoofing Configuration

Select “Fault/Safety→Attack Prevention→ARP Spoofing” to view the current switch ARP Spoofing configuration. “Attack Prevention/ARP Spoofing” will prevent an attacker from sending falsified ARP (address resolution protocol) messages over the local area network.

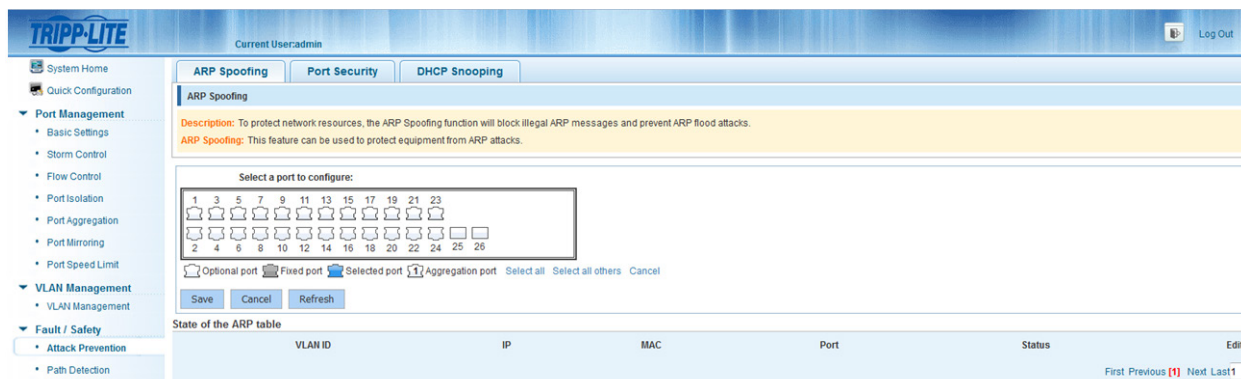


Figure 7-1 View ARP Spoofing Configuration

The figure above shows the ARP configuration property of the switch.

- **VLAN ID:** Displays the value of a VLAN ID of the switch.
- **IP:** Displays the IP address of the current switch.
- **MAC:** Displays the MAC address of the current switch.
- **Port:** Displays the switch port number.

Note: Click “Save” to save the configuration settings

7.1.1.2 Activate ARP Spoofing

In the ARP Spoofing configuration panel, select one or multiple ports to configure.

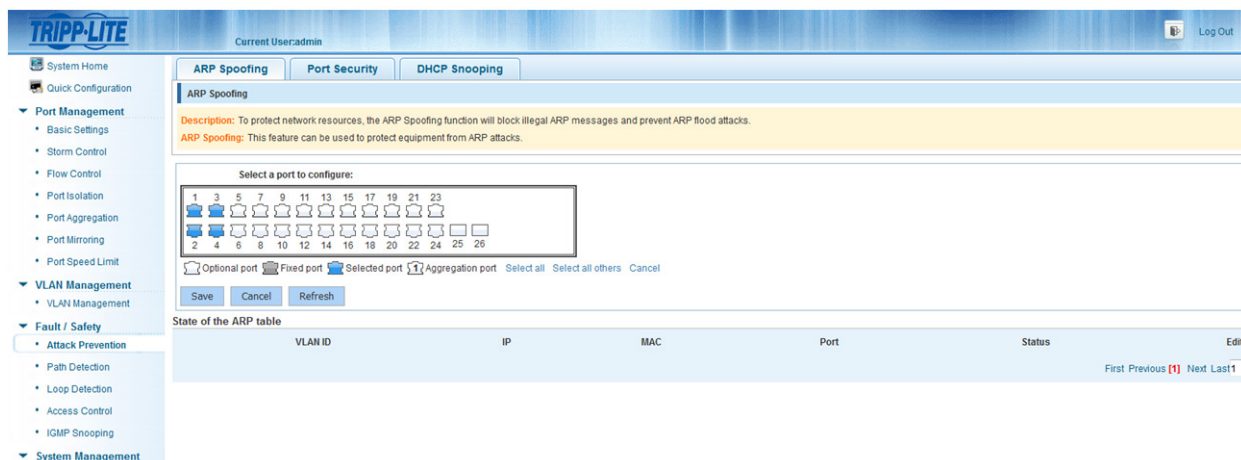


Figure 7-2 ARP Spoofing Configuration

7 Fault/Safety

Current User: admin

Description: To protect network resources, the ARP Spoofing function will block illegal ARP messages and prevent ARP flood attacks.
 ARP Spoofing: This feature can be used to protect equipment from ARP attacks.

Select a port to configure:

Optional port Fixed port Selected port 1 Aggregation port Select all Select all others Cancel

Save Cancel Refresh

VLAN ID	IP	MAC	Port	Status	Edit
1	10.30.125.104	0006.6724.810E	4	VALIDATED	X
1	10.10.0.62	0006.6723.D032	4	VALIDATED	X
1	10.28.99.43	0006.6724.832A	4	VALIDATED	X
1	10.28.99.42	0006.6724.80E7	4	VALIDATED	X
1	10.22.0.72	0006.6724.F515	4	VALIDATED	X
1	10.22.0.73	100D.7FBA.3026	4	VALIDATED	X
1	10.18.0.93	0006.6726.E151	4	VALIDATED	X
1	10.31.125.101	0006.6724.39FB	4	VALIDATED	X
1	192.168.0.120	D4AE.52D4.1645	4	ATTACK	X

First Previous [13] [14] [15] [16] [17] Next Last 17 / 17Page

Figure 7-3 ARP Status Table

Note: Each port can learn more than 200 different ARP packets. When 200 packets are exceeded, the port will enter a congestion state and will not normally forward data.

7.1.1.3 Deactivate ARP Spoofing

In the ARP Spoofing configuration page, click one or more port that you want to deactivate in the port panel, then click “Save” to complete the configuration.

Current User: admin

ARP Spoofing

Description: To protect network resources, the ARP Spoofing function will block illegal ARP messages and prevent ARP flood attacks.
 ARP Spoofing: This feature can be used to protect equipment from ARP attacks.

Select a port to configure:

Optional port Fixed port Selected port 1 Aggregation port Select all Select all others Cancel

Save Cancel Refresh

VLAN ID	IP	MAC	Port	Status	Edit
1	10.30.125.104	0006.6724.810E	4	VALIDATED	X
1	10.10.0.62	0006.6723.D032	4	VALIDATED	X
1	10.28.99.43	0006.6724.832A	4	VALIDATED	X
1	10.28.99.42	0006.6724.80E7	4	VALIDATED	X
1	10.22.0.72	0006.6724.F515	4	VALIDATED	X
1	10.22.0.73	100D.7FBA.3026	4	VALIDATED	X
1	10.18.0.93	0006.6726.E151	4	VALIDATED	X
1	10.31.125.101	0006.6724.39FB	4	VALIDATED	X
1	192.168.0.120	D4AE.52D4.1645	4	ATTACK	X

First Previous [1] Next Last 1 / 17Page

Figure 7-4 Deactivate ARP Spoofing Function

Notes:

- When an interface receives 200 ARP requests, it will consider that the PC connected to the switch contains a virus and the switch will enable ARP Spoofing.
- After you enable ARP Spoofing, it is recommended you also enable storm control.

7.1.1.4 Delete Misjudged ARPs

ARP Spoofing may misjudge some ARP packets to be ARP attacks, or regard attack packets as legal packets messages. If you encounter a misjudgment, it can be deleted by clicking the **X** icon.

State of the ARP Table

VLAN ID	IP	MAC	Port	Status	Edit
1	10.30.125.104	0006.6724.810E	4	VALIDATED	X
1	10.10.0.62	0006.6723.D032	4	VALIDATED	X
1	10.28.99.43	0006.6724.832A	4	VALIDATED	X
1	10.28.99.42	0006.6724.80E7	4	VALIDATED	X
1	10.22.0.72	0006.6724.F515	4	VALIDATED	X
1	10.22.0.73	100D.7FBA.3026	4	VALIDATED	X
1	10.18.0.93	0006.6726.E151	4	VALIDATED	X
1	10.31.125.101	0006.6724.39FB	4	VALIDATED	X
1	192.168.0.120	D4AE.52D4.1645	4	ATTACK	X

First Previous [13] [14] [15] [16] [17] Next Last 17 / 17Page

Figure 7-5 Delete Misjudged ARP

Note: After you enable ARP Spoofing, it is recommended you also enable storm control.

7 Fault/Safety

7.1.2 Port Security

7.1.2.1 Port Security Configuration

Select “Fault/Safety→Attack Prevention→Port Security” to configure the switch’s port security. Port Security can be used to lock one or more ports on the system. When a port is secured, only packets with an allowable source MAC address can be forwarded. All other packets are discarded.

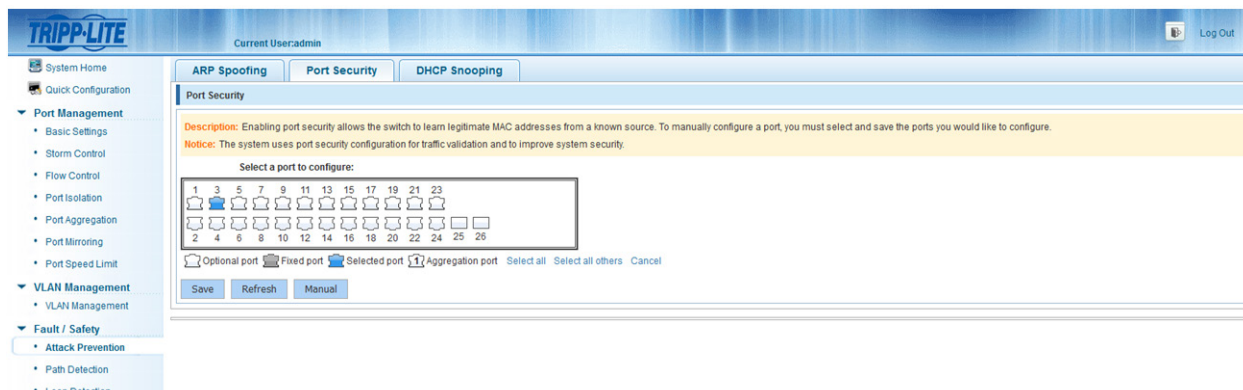


Figure 7-6 Port Security Configuration

Notes:

- Select the desired port(s) to modify port security configuration.
- Click “Save” to enable port security for the selected port(s).
- Click “Refresh” to refresh the binding information of the switch.
- Click “Manual” to manually set port binding information.

7.1.2.2 Manual Configuration

Select the binding mode “Join visitors”. Type in corresponding IP Address, MAC Address, select port number and the access time. Click “Apply” to complete the configuration.

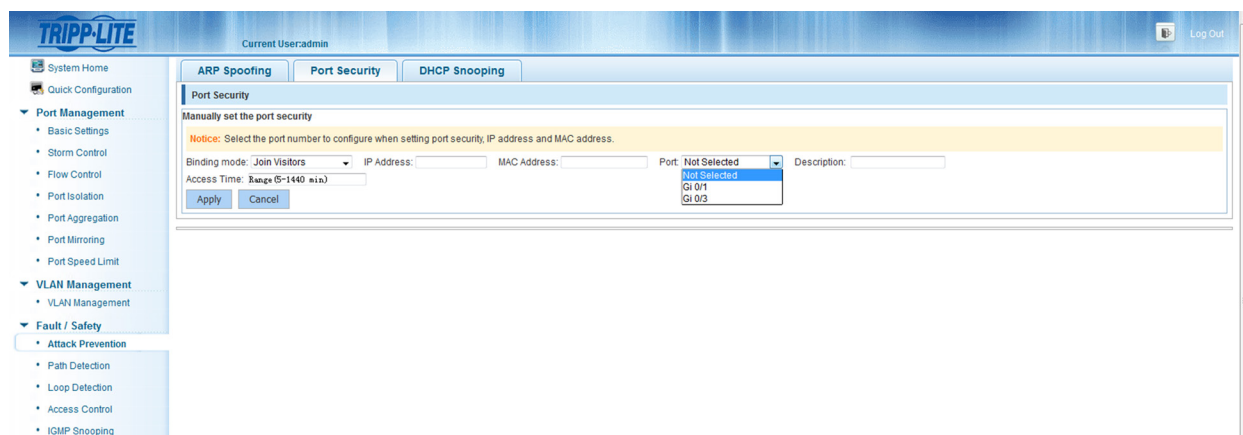


Figure 7-7 Port Security Configuration (Join Visitors)

Notes:

- Select the “Join visitors” binding mode then type in the corresponding IP Address and MAC Address. Select the port number and type in the amount of time allotted for the visitor.
- The range of visit time is between 5-1440 minutes.

7 Fault/Safety

Select the “Add bind” binding mode. Type in corresponding IP Address, MAC Address, select port number and type in the amount of time allotted for the visitor. Click “Apply” to complete the configuration.

TRIPP-LITE

Current User: admin

Log Out

System Home

Quick Configuration

Port Management

- Basic Settings
- Storm Control
- Flow Control
- Port Isolation
- Port Aggregation
- Port Mirroring
- Port Speed Limit

VLAN Management

- VLAN Management

Fault / Safety

- Attack Prevention
- Path Detection

ARP Spoofing

Port Security

DHCP Snooping

Port Security

Manually set the port security

Notice: Select the port number to configure when setting port security, IP address and MAC address.

Binding mode: Add Bind IP Address: MAC Address: Port: Not Selected Description:

Apply Cancel

Not Selected

Gi 0/1

Gi 0/2

Figure 7-8 Port Security Manual Configuration (Add bind)

Port Security is Bound List					
IP Address	MAC Address	Port	Status	Description	Edit
10.20.0.234	1414.4B7B.203D	1	Bound	PORT	✖
First Previous 1 Next Last 1 / 1Page					

Figure 7-9 Results of Port Security Manual Configuration

7.1.2.3 Cancel Port Security Configuration

In the binding list, select the desired IP address, MAC address and Port. Click the ✖ icon to cancel a configuration for an individual port.

Port Security is Bound List					
IP Address	MAC Address	Port	Status	Description	Edit
10.20.0.234	1414.4B7B.203D	1	Bound	PORT	✖
First Previous 1 Next Last 1 / 1Page					

Figure 7-10 Cancel Port Security Configuration

7 Fault/Safety

7.1.3 DHCP Snooping

7.1.3.1 View DHCP Snooping Configuration

Select “Fault/Safety→Attack Prevention→DHCP Snooping” to view the current switch DHCP Snooping configuration of the switch. This feature 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.

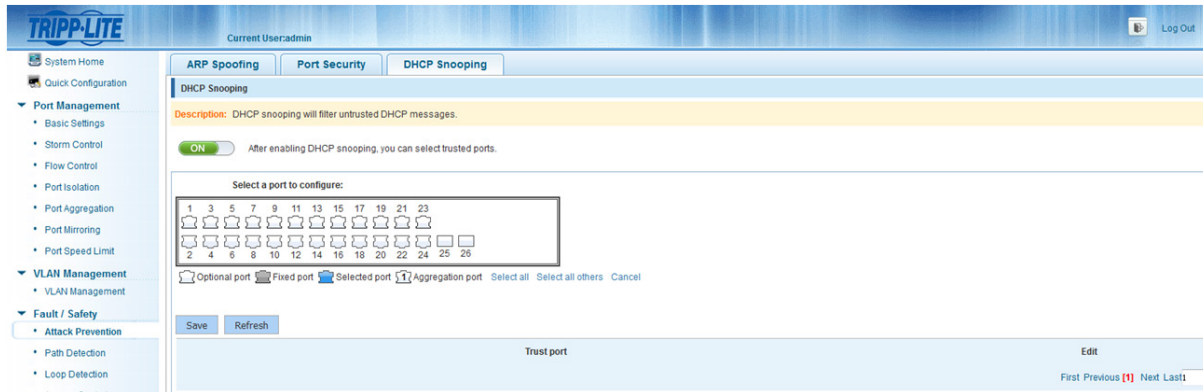


Figure 7-11 View DHCP Snooping Configuration

Notes:

- Click “Refresh” to refresh the configuration list.
- Click “Save” to save the configuration.

7.1.3.2 Activate DHCP Snooping

Select “Fault/Safety→Attack Prevention→DHCP Snooping”, then click “ON/OFF” to enable DHCP snooping for the switch.

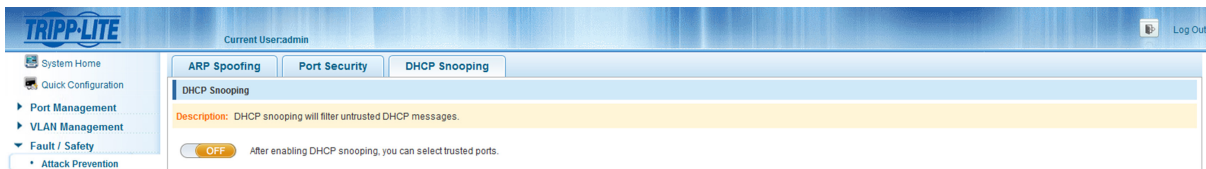


Figure 7-12 Activate DHCP Snooping

7.1.3.3 Set DHCP Trusted Port

Select the ports for which you want to enable DHCP Snooping in the port panel. Click “Save” to complete configuration. A trusted port will forward DHCP server messages without validation.

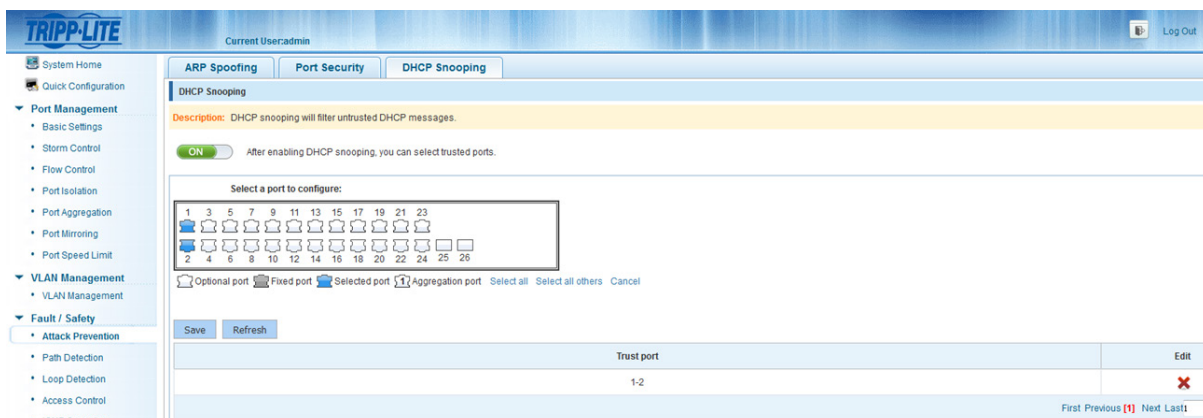


Figure 7-13 Steps to Activate DHCP Snooping

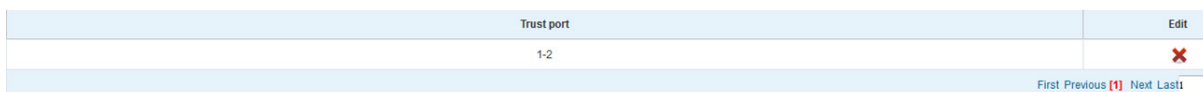


Figure 7-14 Results of Activating DHCP Snooping

7 Fault/Safety

7.1.3.4 Set the Port to Be a DHCP Trusted Port

From the trusted port list, select the ports you want to set as DHCP trusted ports and click the **X** icon to disable the function for that port. Trusted ports will have DHCP snooping enforced by following security rules to ensure DHCP packets from an untrusted DHCP server are dropped. DHCP packets will also be dropped when the source MAC address does not match the client hardware address.

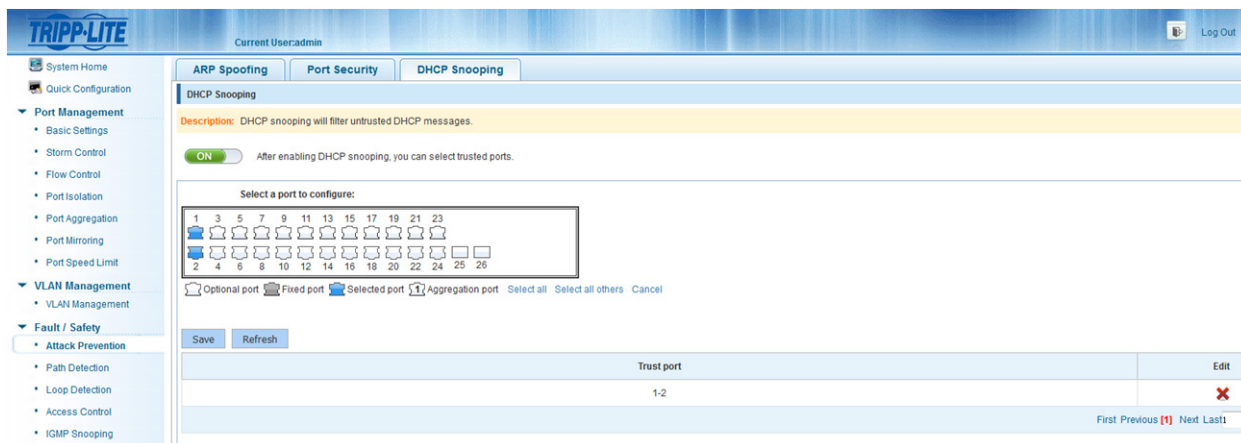


Figure 7-15 Disable the DHCP Server Snooping Function

Note: Activate DHCP Snooping to set the port to be a DHCP trusted port

7.1.3.5 Disable DHCP Snooping

Click the "ON/OFF" button to disable DHCP snooping.

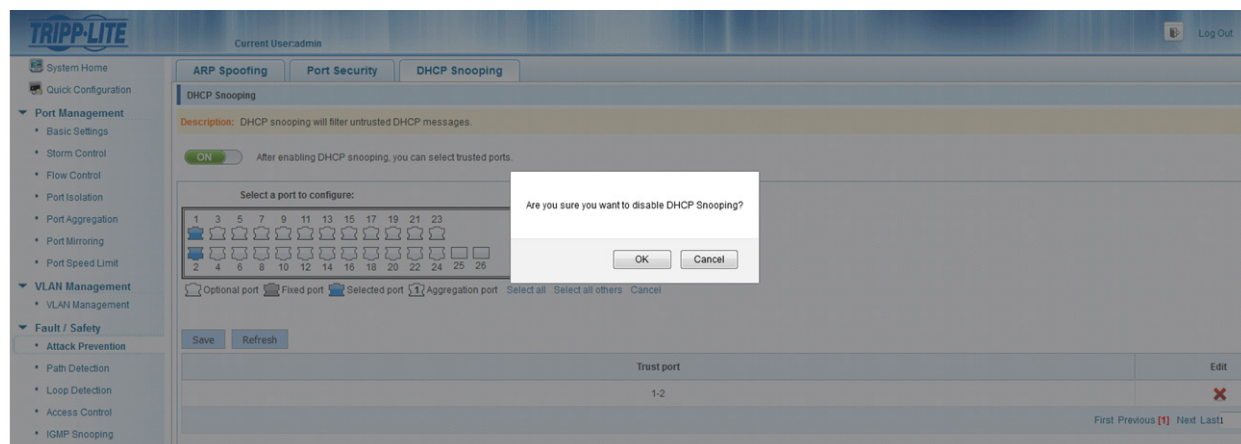


Figure 7-16 Disable DHCP Snooping

7 Fault/Safety

7.2 Path Detection

Select “Fault/Safety→Path Detection” to check the network connectivity of the switch with another device. Enter the IP address you would like to ping in the “Destination IP” field and select “Start Test”. The results of the ping will appear below the “Start Test” button.

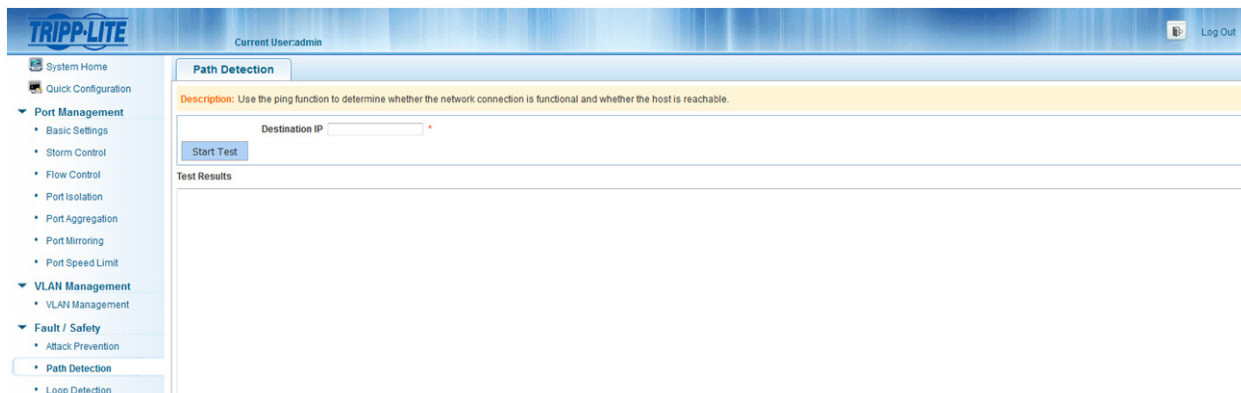


Figure 7-17 Path Detection Configuration

7.3 Loop Detection

7.3.1 View Loop Detection Configuration

Select “Fault/Safety→Loop Detection” to view the switch’s Loop Detection configuration.

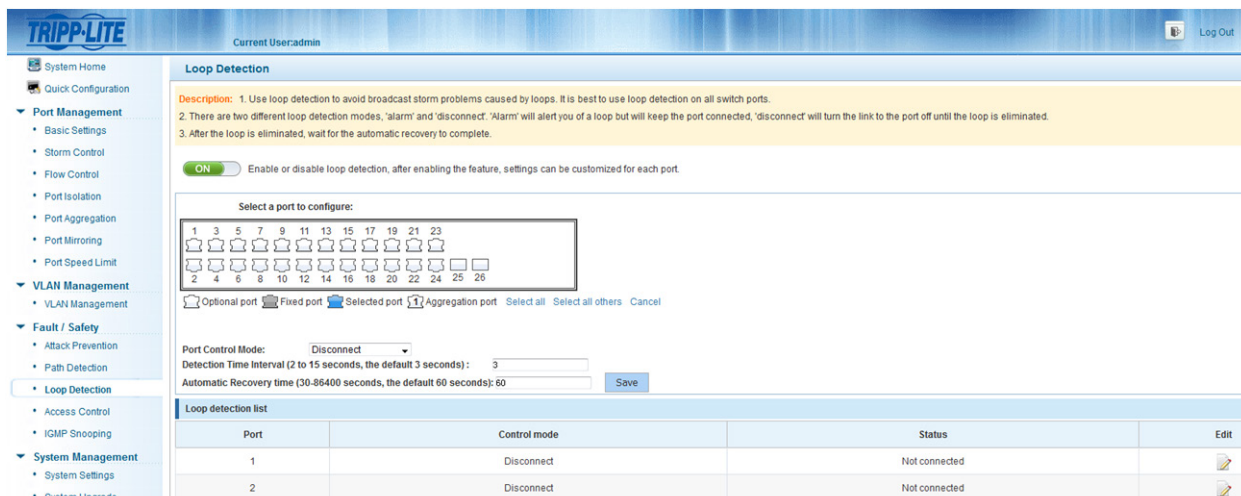


Figure 7-18 View Loop Detection Configuration

The Loop Detection List shows the Loop configuration settings of the current switch.

- **“ON/OFF” Button:** Displays whether loop detection is on or off.
- **Port Control Mode:** Two options are available, disconnect and alarm.
- **Detection Time Interval:** Display the current loop detection time interval, the default is 3 seconds.
- **Automatic Recovery Time:** Displays the automatic recovery time settings for the switch, the default time is 60 seconds.
- **Loop Detection List:** Displays the port number, the control mode and status of each port.

Notes:

- Loop detection defaults to off and the detection time defaults to 3 seconds. By default, when a loop is detected, the port will be disabled.
- When detecting a loop, the port will be disabled. When the loop is eliminated, the port will automatically be restored.

7 Fault/Safety

7.3.2 Enable Loop Detection

Click “ON/OFF” to enable Loop detection.

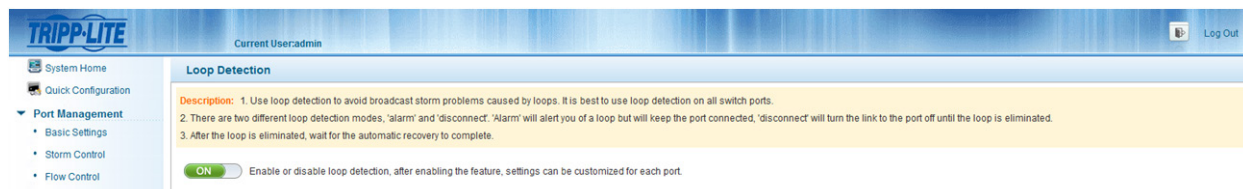


Figure 7-19 Enable Loop Detection

7.3.3 Loop Detection Configuration

Select the port that you want to enable Loop detection in the port panel, select port control mode by selecting “Alarm” from the “Port Control Mode” drop down menu then click “Save”.

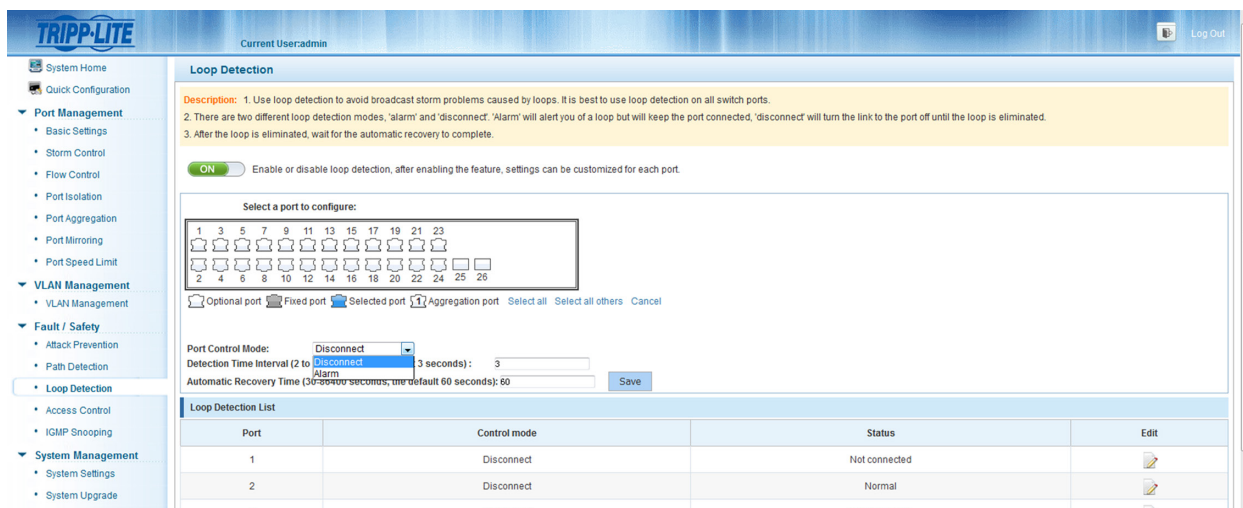


Figure 7-20 Loop Detection Configuration

Note: Loop detection supports detection for link aggregation groups (LAGs).

7.3.4 Detection Time Interval

In the “Detection Time Interval” field, type the time interval that you would like the switch to detect loops. The time interval range is 2-15 seconds and the default setting is 3 seconds.

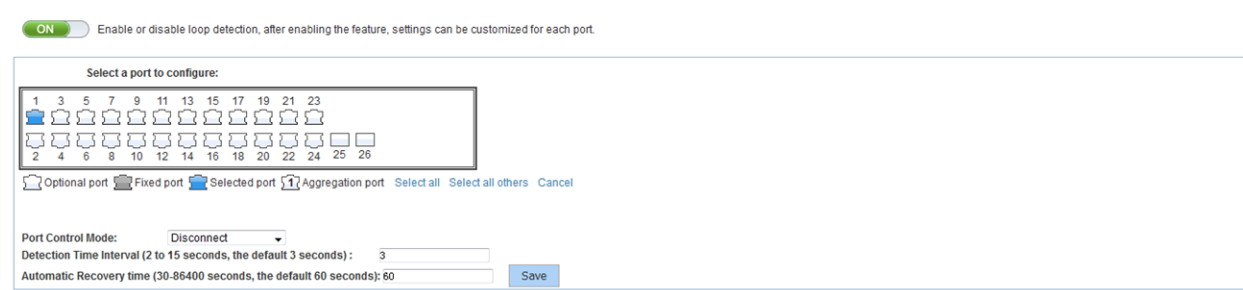


Figure 7-21 Detection Time Interval Configuration

7 Fault/Safety

7.3.5 Automatic Recovery Time

In the “Automatic Recovery Time” field, type the desired time interval for the switch to recover after a loop is removed.

ON Enable or disable loop detection, after enabling the feature, settings can be customized for each port.

Select a port to configure:

1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24 25 26

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Port Control Mode: Disconnect

Detection Time Interval (2 to 15 seconds, the default 3 seconds): 3

Automatic Recovery time (30-86400 seconds, the default 60 seconds): 60

Save

Figure 7-22 Automatic Recovery Time Configuration

7.3.6 Disable Loop Detection

Click the “ON/OFF” button to disable loop detection.

ON Enable or disable loop detection, after enabling the feature, settings can be customized for each port.

Select a port to configure:

1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24 25 26

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Port Control Mode: Disconnect

Detection Time Interval (2 to 15 seconds, the default 3 seconds): 3

Automatic Recovery Time (30-86400 seconds, the default 60 seconds): 60

Save

Are you sure you want to turn off Loop Detection?

OK Cancel

Port	Control mode	Status	Edit
1	Disconnect	Not connected	
2	Disconnect	Normal	
3	Disconnect	Not connected	
4	Disconnect	Not connected	
5	Disconnect	Not connected	

Figure 7-23 Disable Loop Detection

7.4 Access Control Lists (ACLs)

7.4.1 ACL

7.4.1.1 View ACL

Select “Fault/Safety→Access Control” to view the Access Control List (ACL) configuration of the switch. ACLs ensure only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked and provide security for the network.

ON Access control lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources.

New ACL Rules

Displaying ACL Configuration

No.	Action	Protocol	Source IP/MAC	Source Wildcard	Source Port	Destination IP / MAC	Destination Wildcard	Destination Port	Edit
-----	--------	----------	---------------	-----------------	-------------	----------------------	----------------------	------------------	------

Delete

Figure 7-24 Access Control List Settings

7 Fault/Safety

7.4.1.2 Add ACL Rules

1. To add a Standard IP ACL:

Click “New ACL Rules” button. Select “Configure Standard IP ACL” from the Select Configuration Type dropdown menu. Select the List ID “Standard IP ACL 0” and the ACE ID “ACE 0”. Set Rules to “Permit”. Click the “Any Source IP Address” radio button, then click “Save” to complete the configuration.

The screenshot shows the TRIPPLITE web interface with the 'New ACL Rules' dialog box open. The 'Select Configuration Type' dropdown is set to 'Configuration standard IP ACL'. The 'List ID' is 'Standard IP ACL 0' and the 'ACE ID' is 'ACE 0'. The 'Rules' dropdown is set to 'Permit'. Under 'IP Address', the 'Any source IP address' radio button is selected. The 'Save' button is at the bottom of the dialog. The background shows the main configuration menu with 'Fault / Safety' selected.

Figure 7-25 Standard IP ACL Configuration

2. To a Configuration Expand IP ACL

Click “New ACL Rules” button. Select “Configuration Expand IP ACL” from the Select Configuration Type dropdown menu. Select the List ID “Expand IP ACL 10” and the ACE ID “ACE 0”. Set Rules to “Permit” and select the “TCP” Protocol. Select the Source IP Address by clicking the “Any source IP Address” radio button. Do the same for the Destination IP Address. Click “Save” to complete the configuration.

The screenshot shows the TRIPPLITE web interface with the 'New ACL Rules' dialog box open. The 'Select Configuration Type' dropdown is set to 'Configuration Expand IP ACL'. The 'List ID' is 'Expand IP ACL 10' and the 'ACE ID' is 'ACE 0'. The 'Rules' dropdown is set to 'Permit' and the 'Protocol' dropdown is set to 'IGMP'. Under 'Source IP Address', the 'Any source IP address' radio button is selected. Under 'Destination IP Address', the 'Any destination IP address' radio button is selected. The 'Save' button is at the bottom of the dialog. The background shows the main configuration menu with 'Fault / Safety' selected.

Figure 7-26 Expand IP ACL Configuration

7 Fault/Safety

3. To add an Expand MAC ACL

Click “New ACL rules” button. Select “Configuration Expand MAC ACL” from the Select Configuration Type dropdown menu. Select the List ID “Expand MAC ACL 20” and the ACE ID “ACE 0”. Set Rules to “Permit”. Select the Source MAC Address by clicking the “Any source MAC Address” radio button. Do the same for the Destination MAC Address. Type “0x0086” in the MAC Protocol Type field. Click “Save” to complete configuration.

Figure 7-27 Expand MAC ACL Configuration

Notes:

- In the “ACL Rules” configuration page, the ACE ID is optional. If an ACE ID is not selected, the default is 0.
- In the “Expand IP Access Control List” page, the protocol types are TCP, UDP, IP and IGMP.

7.4.1.3 Modify ACL Configuration



To modify your ACL rules, select the rules you want to modify and click the  icon to visit the ACL rules modification page. Change Rules to “Permit”.

Figure 7-28 Modify ACL Configuration

Note: The steps to modify “Expand MAC ACL” and “Expand IP ACL” are the same as that of the standard IP ACL.

7 Fault/Safety

7.4.1.4 Delete ACL Rules

Select the desired ACL Rules, click the  icon to go to the ACL rules modification page, then select “Deny” and click “Save” to complete the deletion.

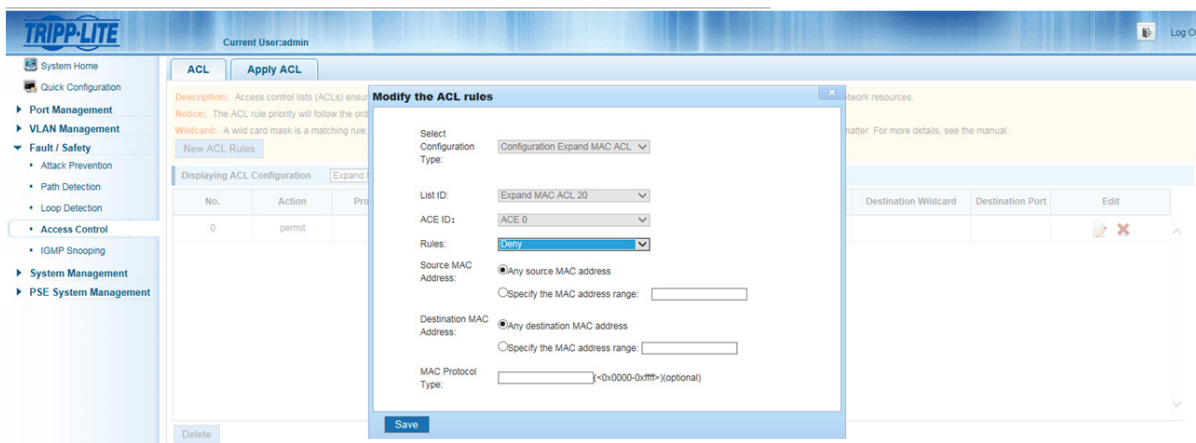


Figure 7-29 Delete ACL Rules

To delete all the ACL Rules, click the  icon then click “OK” to confirm the deletion.

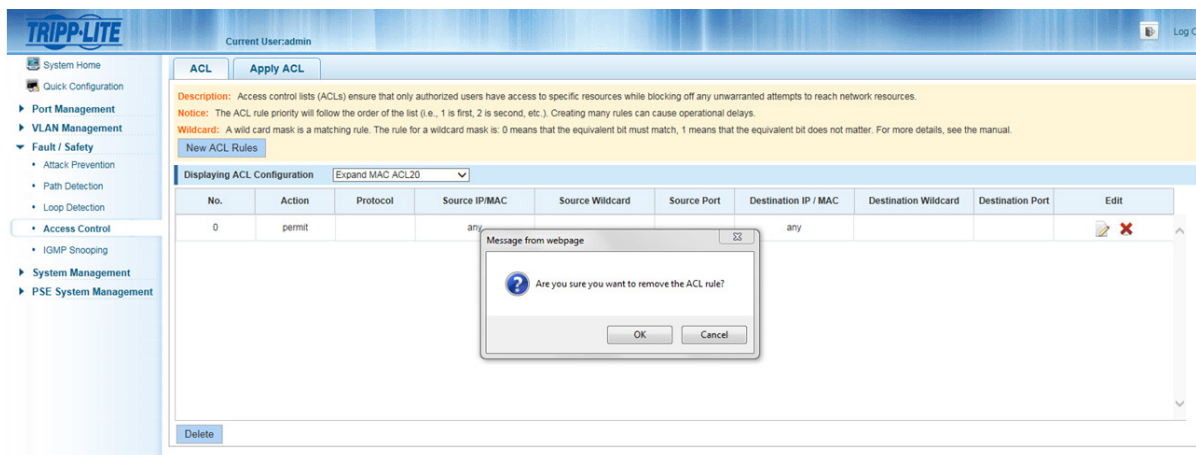


Figure 7-30 Delete All ACL Rules

Note: After a successful deletion, all of the rules on the port will removed at the same time

7.4.2 Apply ACL

7.4.2.1 Apply ACL Rule

Select “Fault/Safety→Access Control→Apply ACL” to view the access control lists and to Apply ACL Configuration.

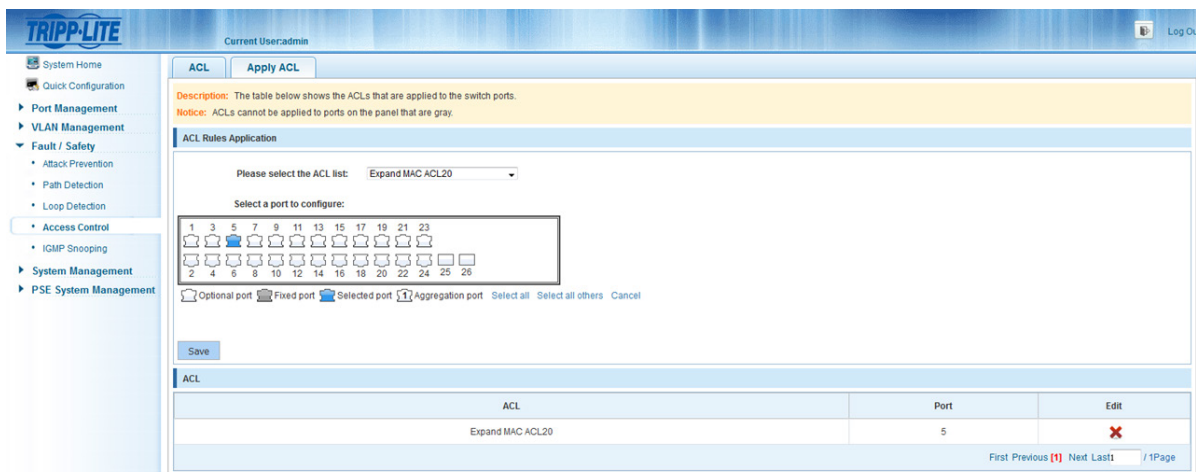


Figure 7-31 View Applied ACL Rules

7 Fault/Safety

7.4.2.2 Apply an ACL Rule

Select the ACL rule you would like to apply, then select the port to which you would like to apply the ACL rule on the port panel. Click “Save” to complete the configuration.

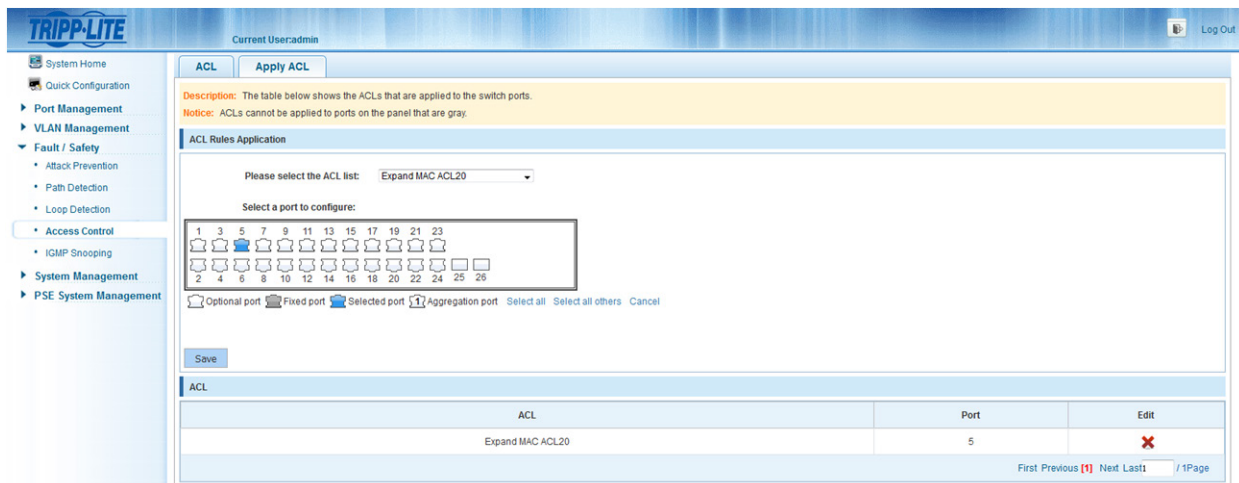



Figure 7-32 Apply ACL Rule

7.4.2.3 Delete ACL Rule

Select the ACL you would like to delete, click the  icon to the right of the ACL rule and click “OK” to cancel the application of the ACL rule for the selected port.

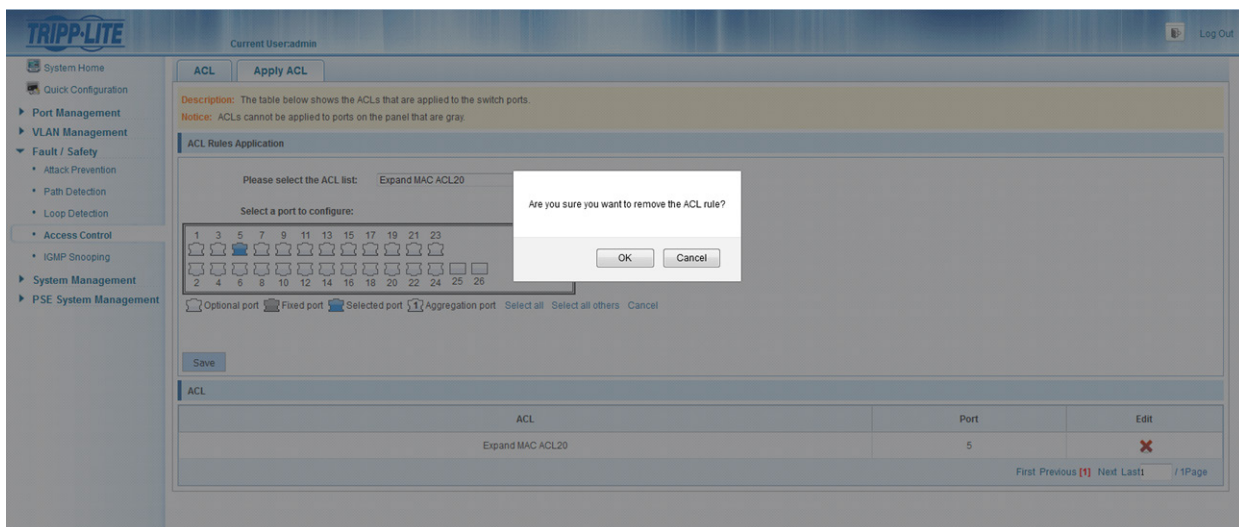


Figure 7-33 Delete an ACL Rule

7 Fault/Safety

7.5 IGMP Snooping

7.5.1 IGMP Snooping Configuration

Select “Fault/Safety→IGMP Snooping” to view the IGMP Snooping Configuration of the switch. IGMP (Internet Group Management Protocol) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch. Multicast IP traffic is traffic that is destined to a host group. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance. The use of IGMP snooping is a creative way to solve this problem. The switch uses the information in the IGMP packets as they are being forwarded throughout the network to determine which segments should receive packets directed to the group address.

TRIPPLITE

Current User: admin

Log Out

System Home

Quick Configuration

Port Management

VLAN Management

Fault / Safety

Attack Prevention

Path Detection

Loop Detection

Access Control

IGMP Snooping

System Management

PSE System Management

IGMP Snooping

Description: Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.

Notice: 1. The default multicast monitor is not a static routing port, if required, a static routing port can be set.
2. Dynamic routing ports can not be removed manually, only static routing ports can be removed manually. Dynamic routing ports will be removed through aging.

☒ ON Enable or disable the multicast listener, when enabled, the static routing port can be set.

IGMP Version Selection

IGMP Version: IGMP_V2

Save

Multicast Routing Port Settings

Select a port to configure:

1	3	5	7	9	11	13	15	17	19	21	23	
2	4	6	8	10	12	14	16	18	20	22	24	25

☐ Optional port ☒ Fixed port ☒ Selected port ☐ Aggregation port

VLAN: vlan 1 IP:

Add Routing Port

VLAN	Port	IP	Status	Edit
------	------	----	--------	------

First Previous 1 Next Last 1 / 1Page

Figure 7-34 View IGMP Snooping Configuration

7.5.2 Activate the IGMP Snooping Function

Click “Fault/Safety→IGMP Snooping” then click the “ON/OFF” button to activate the IGMP Snooping Function.

TRIPPLITE

Current User: admin

Log Out

System Home

Quick Configuration

Port Management

VLAN Management

Fault / Safety

Attack Prevention

Path Detection

Loop Detection

Access Control

IGMP Snooping

System Management

PSE System Management

IGMP Snooping

Description: Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.

Notice: 1. The default multicast monitor is not a static routing port, if required, a static routing port can be set.
2. Dynamic routing ports can not be removed manually, only static routing ports can be removed manually. Dynamic routing ports will be removed through aging.

☒ ON Enable or disable the multicast listener, when enabled, the static routing port can be set.

IGMP Version Selection

IGMP Version: IGMP_V2

Save

Multicast Routing Port Settings

Select a port to configure:

1	3	5	7	9	11	13	15	17	19	21	23	
2	4	6	8	10	12	14	16	18	20	22	24	25

☐ Optional port ☒ Fixed port ☒ Selected port ☐ Aggregation port

VLAN: vlan 1 IP:

Add Routing Port

VLAN	Port	IP	Status	Edit
------	------	----	--------	------

First Previous 1 Next Last 1 / 1Page

Figure 7-35 Activate the IGMP Snooping Function

Notes:

- By default, IGMP Snooping is disabled.
- After enabling IGMP Snooping, all VLANs are enabled by default.
- The default IGMP version is V2.

7 Fault/Safety

7.5.3 Disable the IGMP Snooping Function

Click menu “Fault/Safety→IGMP Snooping”, then click the “ON/OFF” button to disable the IGMP Snooping Function.

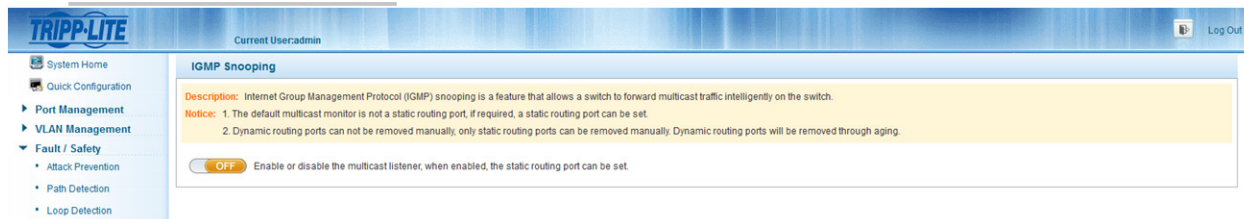


Figure 7-36 Disable the IGMP Snooping Function

7.5.4 Multicast Routing Port Settings

Select a port from the port panel, select the VLAN from the drop down menu, then click “Add Routing Port” to complete the routing port configuration.

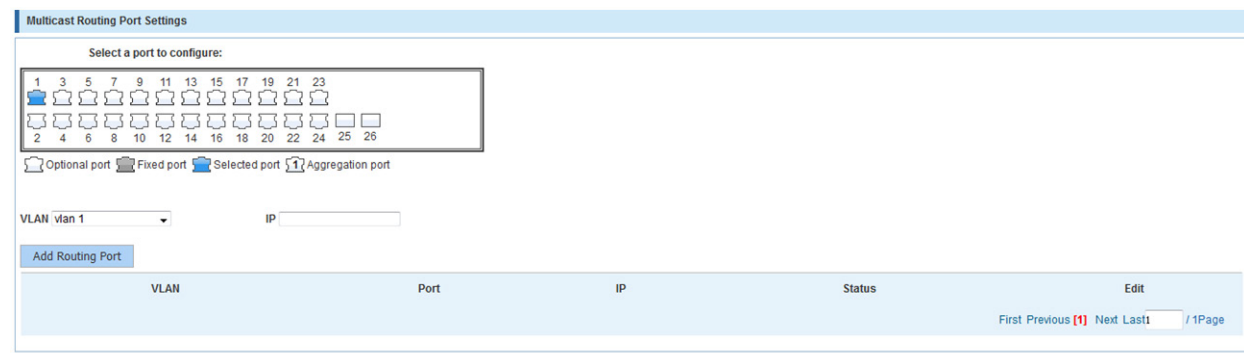


Figure 7-37 Multicast Routing Port Settings

7.5.5 IGMP Version

Select “Fault/Safety→IGMP Snooping” to change the IGMP Version. Select the desired IGMP version and click “Save”. The default IGMP version is V2.

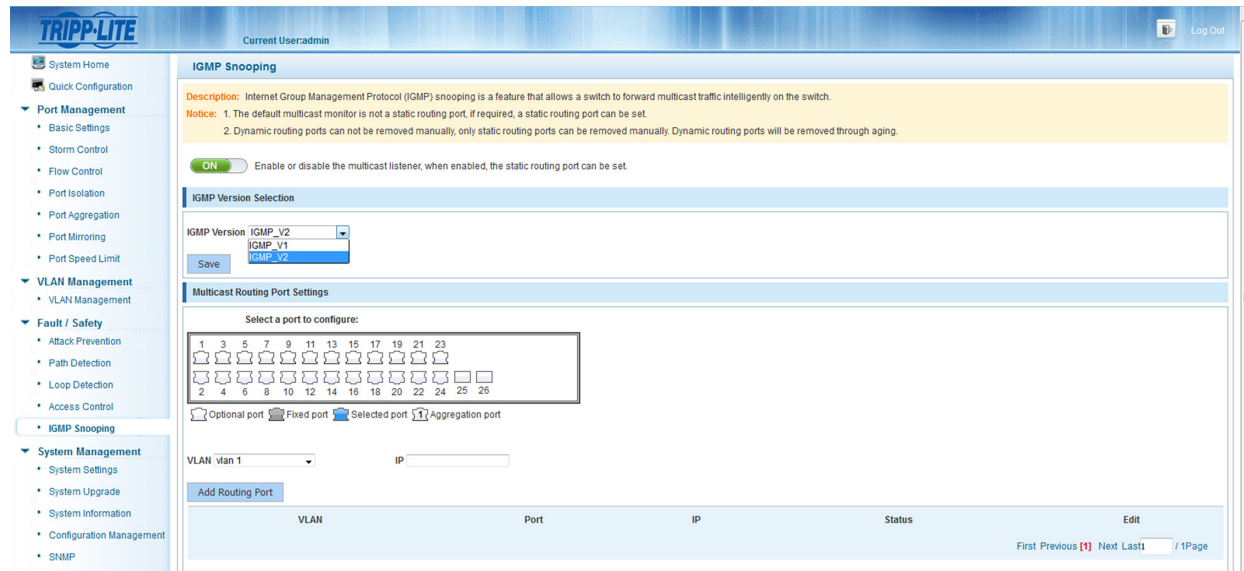


Figure 7-38 Set the IGMP Version

8 System Management

8.1 System Settings

8.1.1 Management VLAN

8.1.1.1 View Management VLAN

Select “System Management→System Settings→VLAN Management” to view the VLAN management configuration of the switch.

TRIPP-LITE

Current User: admin

System Home Quick Configuration

Port Management

- Basic Settings
- Storm Control
- Flow Control
- Port Isolation
- Port Aggregation
- Port Mirroring
- Port Speed Limit

VLAN Management

- VLAN Management

Fault / Safety

- Attack Prevention
- Path Detection
- Loop Detection
- Access Control
- IGMP Snooping

VLAN Management System Restart Change Password System Log Log Export ARP Table MAC Management

Description: Management VLAN parameters: IP, MAC, gateway and the user's contact details. "*" denotes required field.

The basic information of the system settings

VLAN Management: *

Management IP: *

Subnet Mask: *

Default Gateway: *

Login Timeout: x

Management Port:

MAC: *

Device Name: *

Device Location:

Contact Name:

Contact Information:

Save

System time synchronization

Notice: The switch time can be synchronized with the internet time by setting the time synchronization server IP address to the NTP server from your selected time zone.

Tip: The system will select a default time synchronization server if no IP address is entered.

The Current System Time:

Time Zone (T): v

NTP Server IP Address:

Daylight Saving Time: ☐ Enabled ☒ Disabled

Synchronize

Figure 8-1 View Management VLAN

The VLAN Management page shows the settings of the switch.

- **Management VLAN:** The default is VLAN1.
- **Management IP:** The IP address of the switch's management VLAN.
- **Subnet Mask:** The subnet mask of the switch's management VLAN.
- **Default Gateway:** The default gateway of the switch's management VLAN.
- **Timeout Login:** When the web interface page is idle for more than five minutes, the browser will return to the login interface by default.
- **Management Port:** The management port default is 80.
- **MAC:** The switch's MAC address.
- **Device Name:** The name of the switch.
- **Device Location:** The location of the switch.
- **Contact Name:** The name of the administrator.
- **Contact Information:** Contact number of the administrator.

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

8 System Management

8.1.1.2 Set Management IP Address

By modifying parameters in the box below, you can set the management IP address.

The screenshot shows the Tripp-Lite web interface with the 'VLAN Management' tab selected. The 'Management IP' field is highlighted, and the 'Save' button is visible. The interface includes a sidebar with navigation options like 'System Home', 'Quick Configuration', 'Port Management', 'VLAN Management', 'Fault / Safety', and 'System Management'. The main content area displays the 'Management IP' settings, including fields for Management IP, Subnet Mask, Default Gateway, Login Timeout, and Management Port. A 'Save' button is located at the bottom left of the form.

Figure 8-2 Modify the Management IP Address of the Switch

8.1.1.3 System Time Synchronization

The switch can be synchronized with the Internet time by setting the time synchronization server IP address in the “NTP Server IP Address” field.

The screenshot shows the Tripp-Lite web interface with the 'System Time Synchronization' tab selected. The 'NTP Server IP Address' field is highlighted, and the 'Synchronize' button is visible. The interface includes a sidebar with navigation options like 'System Home', 'Quick Configuration', 'Port Management', 'VLAN Management', 'Fault / Safety', and 'System Management'. The main content area displays the 'System Time Synchronization' settings, including fields for NTP Server IP Address, Time Zone, Daylight Saving Time, Date Mode, and Time Set Offset. A 'Synchronize' button is located at the bottom left of the form.

Figure 8-3 System Time Synchronization

Daylight Savings Time: Enables support for local daylight savings time (Default mode is disabled).

Note: The system will select a default time synchronization server if no IP address is entered.

8.1.2 System Restart

Select “System Management→System Settings→System Restart” to reboot the switch.

The screenshot shows the Tripp-Lite web interface with the 'System Restart' tab selected. The 'Restart the device immediately' button is highlighted. The interface includes a sidebar with navigation options like 'System Home', 'Quick Configuration', 'Port Management', 'VLAN Management', 'Fault / Safety', and 'System Management'. The main content area displays the 'System Restart' settings, including a description of the restart process and a 'Restart the device immediately' button.

Figure 8-4 System Restart

Notes:

- During the reboot process the Web page cannot be accessed.
- When the device reboots, you need to login to the switch's web interface page.
- After you select “Restart the device immediately”, you will have an option to save the current configuration before the system restarts.

8 System Management

8.1.3 Modify the Password

8.1.3.1 Modify the Super User Password

Select “System Management→System Settings→Change Password”. Enter the default password **admin** in the “Old Password” field, then enter the new password in both the “New Password” and “Confirm New Password” fields (case sensitive)*.

Figure 8-5 Modify the Super User Password

* The case sensitive password can only contain letters, numbers, and underscores.

8.1.3.2 Telnet Login Password

Select “System Management→System Settings→Change password”, in the telnet login password area, enter your desired password in both the “New Password” field and the “Confirm New Password” field. Click “Save”.

Figure 8-6 Telnet Login Password

8.1.4 System Log

Select “System Management→System Settings→System Log” to visit the system log management page. On this page you can review, search and clear the system log.

Figure 8-7 System Log Management

Notes:

- The contents of the System Log in the web interface page are the same as the results from executing the command “show logging” in the prompt command window.
- To clear the log information, click “Clear”.

8 System Management

8.1.5 LOG Export

Select “System Management→System Settings→LOG Export” to visit the system log export page. Here, you can export the system log via TFTP server.

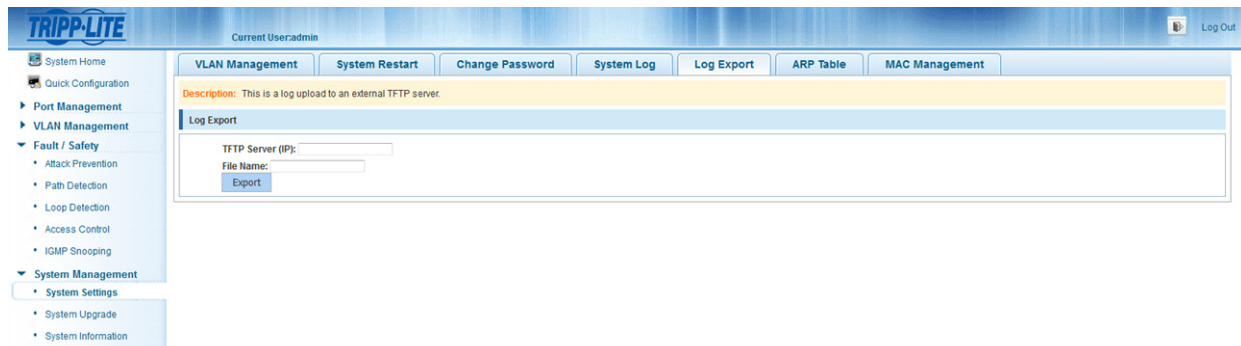


Figure 8-8 LOG Export

8.1.6 ARP Table

Select “System Management→System Settings→ARP Table” to visit the ARP Table configuration page. This view displays the ARP Table contents.

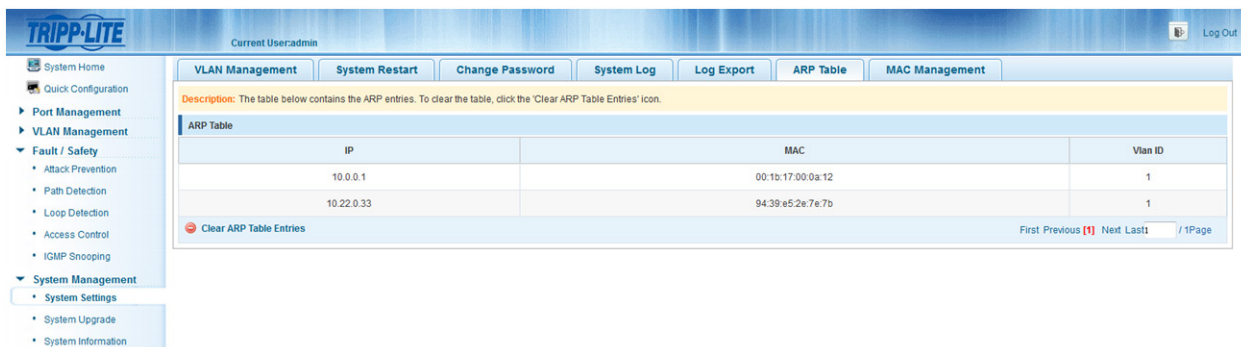


Figure 8-9 ARP Information

Note: Click “Clear ARP Table Entries” to clear the ARP information.

8.1.7 MAC Address Management

8.1.7.1 Query MAC Address

Select “System Management System→Settings→MAC Management” to query MAC address information.

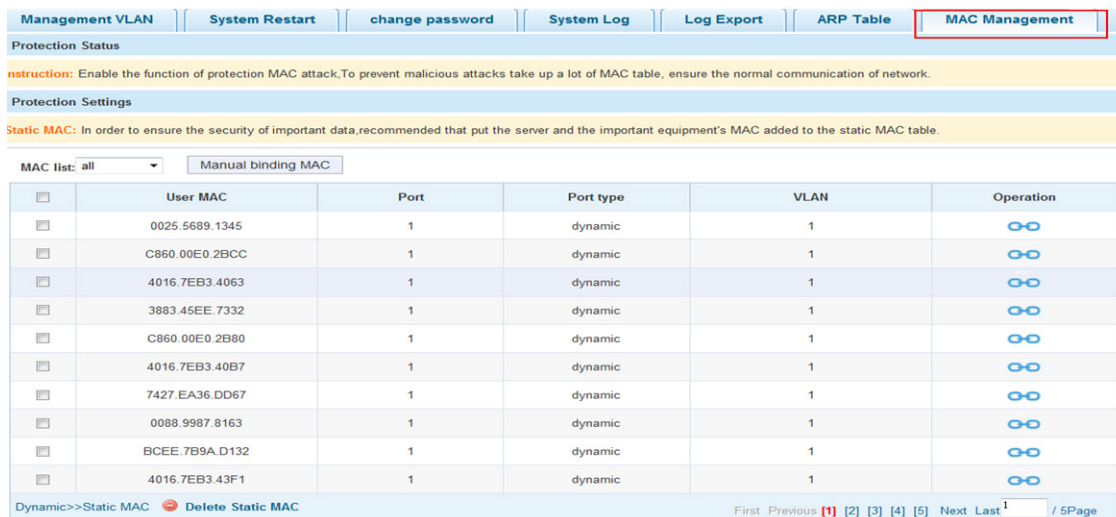



Figure 8-10 Query Results of MAC Address

8 System Management

The MAC address list shows the MAC address that the current switch learned.

- **Port:** Displays the port number of the MAC address.
- **Port Type:** One of two types will be displayed: dynamic or static.
- **VLAN:** Displays the VLAN ID.
- **Operation:** Clicking  allows you to bind the MAC address as a static MAC.

8.1.7.2 Add a Static MAC Address

Click “Configure MAC Binding”. From here you can configure static MAC addresses.

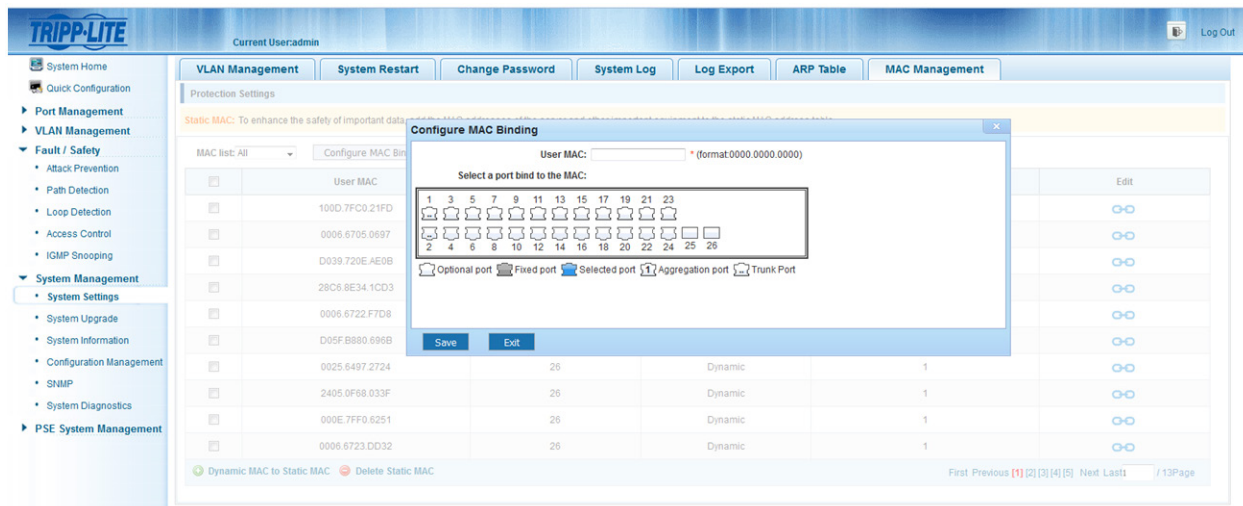



Figure 8-11 Static MAC Address Configuration

To perform a static MAC address configuration, do the following:

1. Click “Configure MAC Binding” to visit the manual configuration page.
2. Type a MAC address such as 0001.7A4F.74D2 in the “User MAC” field.
3. Select the port(s) to configure from the port panel.
4. Click “Save” to complete the configuration.

1. Set static MAC address with

In the MAC address list, select the MAC address you want to bind, then click  to complete binding.

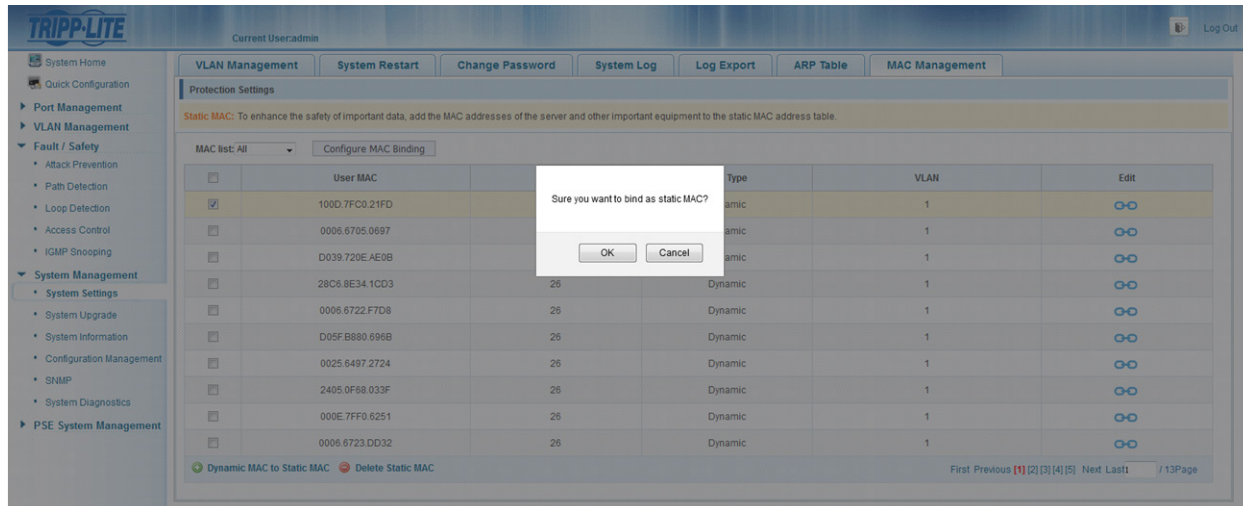
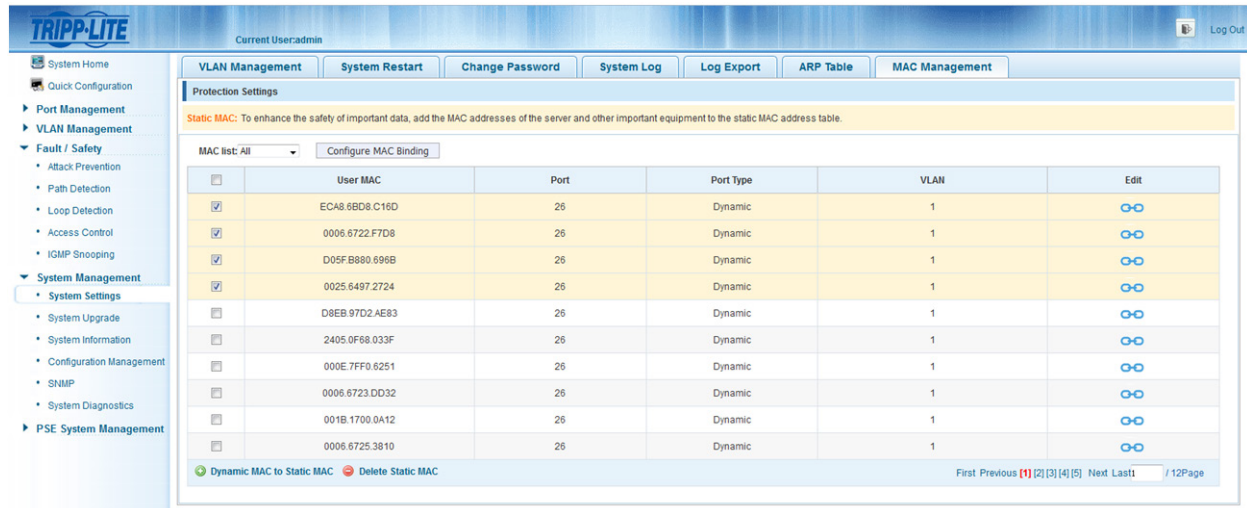


Figure 8-12 Conduct Static MAC Address Configuration

8 System Management

To select the ports to configure, click the check box ☒ next to the ports you want to bind in the MAC address list, then click the “Dynamic MAC to Static MAC” button to complete the configuration.



Current User: admin

Log Out

VLAN Management System Restart Change Password System Log Log Export ARP Table MAC Management

Protection Settings

Static MAC: To enhance the safety of important data, add the MAC addresses of the server and other important equipment to the static MAC address table.

MAC list: All

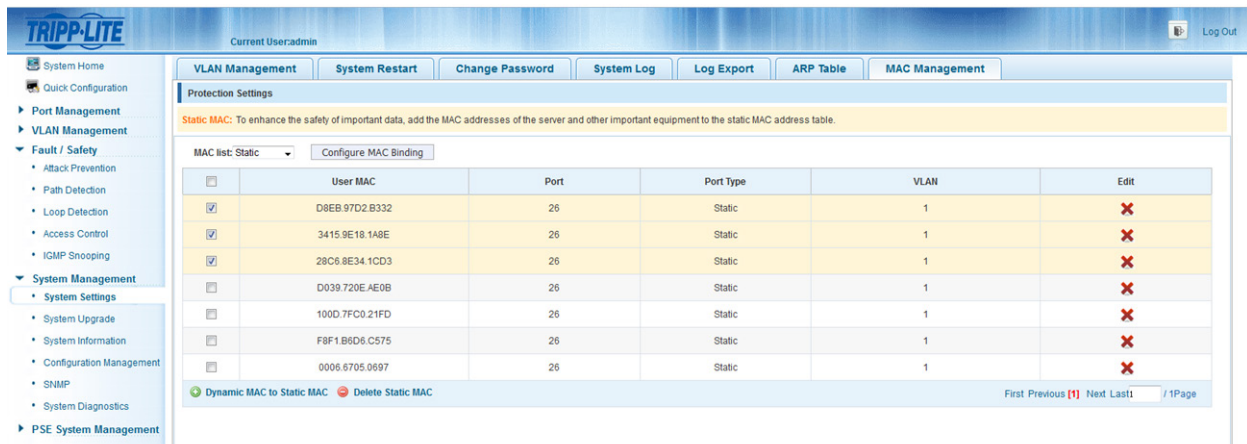
<input type="checkbox"/>	User MAC	Port	Port Type	VLAN	Edit
<input checked="" type="checkbox"/>	EC48.6BD8.C16D	26	Dynamic	1	Edit
<input checked="" type="checkbox"/>	0006.6722.F7D8	26	Dynamic	1	Edit
<input checked="" type="checkbox"/>	D05F.B980.696B	26	Dynamic	1	Edit
<input checked="" type="checkbox"/>	0025.6497.2724	26	Dynamic	1	Edit
<input type="checkbox"/>	D8EB.97D2.AE83	26	Dynamic	1	Edit
<input type="checkbox"/>	2405.0F68.033F	26	Dynamic	1	Edit
<input type="checkbox"/>	000E.7FF0.6251	26	Dynamic	1	Edit
<input type="checkbox"/>	0006.6723.DD32	26	Dynamic	1	Edit
<input type="checkbox"/>	001B.1700.0A12	26	Dynamic	1	Edit
<input type="checkbox"/>	0006.6725.3810	26	Dynamic	1	Edit

First Previous **1** [2] [3] [4] [5] Next Last 1 / 12Page

Figure 8-13 Static MAC Address Configuration for Multiple Ports

8.1.7.3 Delete Static MAC Address(es)

To select the MAC address(es) you want to delete, click the check box ☒ next to the MAC address(es). Click the “Delete Static MAC” button to delete the selected MAC(s).



Current User: admin

Log Out

VLAN Management System Restart Change Password System Log Log Export ARP Table MAC Management

Protection Settings

Static MAC: To enhance the safety of important data, add the MAC addresses of the server and other important equipment to the static MAC address table.

MAC list: Static

<input type="checkbox"/>	User MAC	Port	Port Type	VLAN	Edit
<input checked="" type="checkbox"/>	D8EB.97D2.B332	26	Static	1	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	3415.9E18.1ABE	26	Static	1	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	28C6.8E34.1CD3	26	Static	1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	D039.720E.AE0B	26	Static	1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	100D.7FC0.21FD	26	Static	1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	F8F1.B6D6.C575	26	Static	1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	0006.6705.0897	26	Static	1	<input checked="" type="checkbox"/>

First Previous **1** Next Last 1 / 12Page

Figure 8-14 Delete MAC Address(es)

8 System Management

8.2 System Upgrade

Select “System Management→System Upgrade” to upgrade switch software.

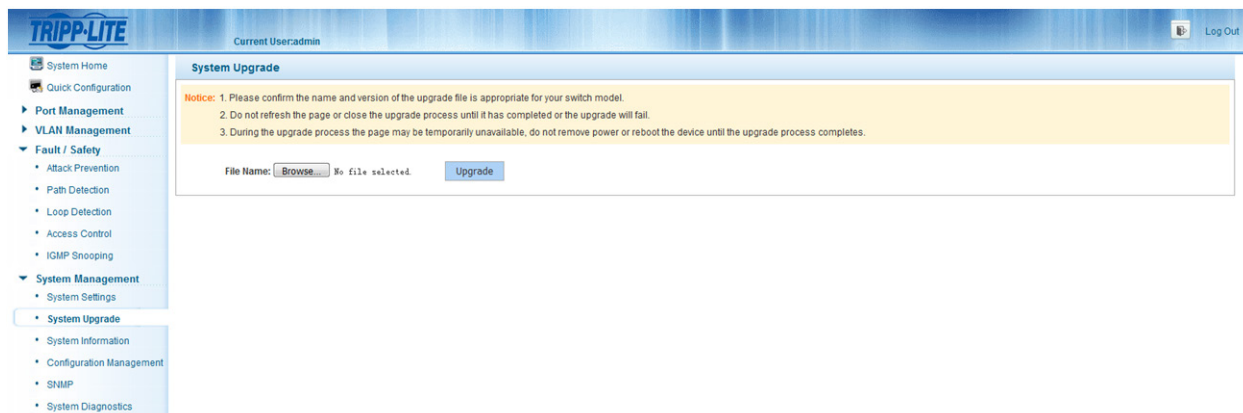


Figure 8-15 System Upgrade

Notes:

- Do not turn off the switch during the upgrade process.
- Ensure the upgrade files are correct before starting the upgrade process.
- Save your configuration before upgrading the switch.
- After the upgrade process is completed, the switch will automatically reboot and will require you to login.

8.3 System Information

8.3.1 Memory Information

Select “System Management→System Information→Memory Information” to visit the Memory Information page. This page displays the current system memory information.

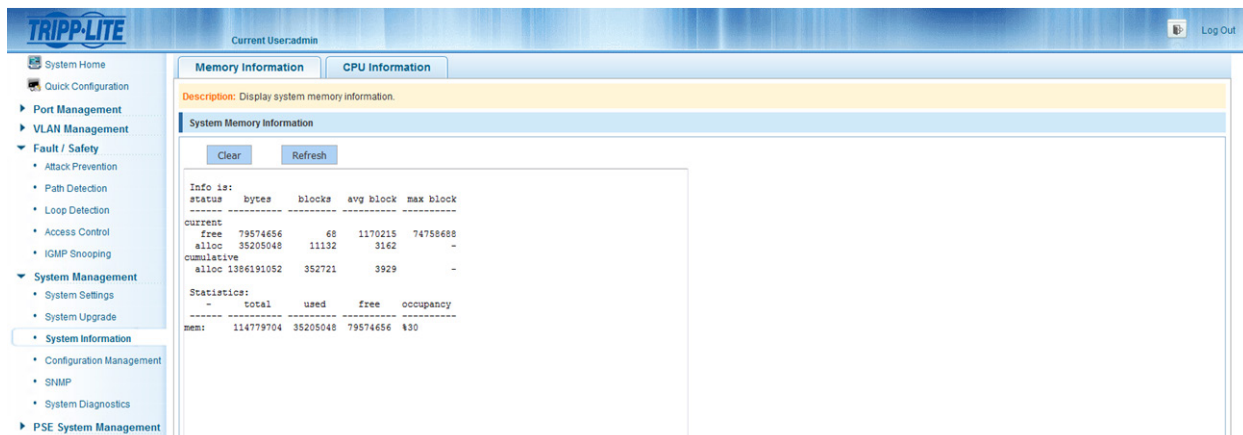


Figure 8-16 Memory Information

Notes:

- Click “Clear” to clear the memory information from the window.
- Click “Refresh” to refresh the memory information displayed for the switch.

8 System Management

8.3.2 CPU Information

Select “System Management→System Information→CPU Information” to visit CPU Information page. Here, you can view the system tasks of the switch.

TRIPP-LITE

Current User:admin

Log Out

System Home

Quick Configuration

Port Management

VLAN Management

Fault / Safety

- Attack Prevention
- Path Detection
- Loop Detection
- Access Control
- IGMP Snooping

System Management

- System Settings
- System Upgrade
- System Information
- Configuration Management
- SNMP
- System Diagnostics

PSE System Management

Memory Information

CPU Information

Description: Display system CPU information.

CPU Information

Clear

Refresh

NAME	ENTRY	IID	PRI	total % (ticks)	delta % (ticks)	
tExcTask	excTask	7f9a6804	0	0%	(4) 0%	
tLogTask	logTask	7f57a008	0	0%	(0) 0%	
tHighDog	highDogTam	5a18210	3	0%	(0) 0%	
tVlanTask	portVlan_r	5a9b7e8	19	0%	(20) 0%	
tShell	shellTask	5a11240	20	0%	(0) 0%	
tSysLog	8b36a4c4	40	0%	305%	(0) 0%	
tNetTask	netTask	79cf190	50	0%	(0) 0%	
tNotify	6f6e9b8	50	0%	(0) 0%	(0)	
tSysTimeH	8b2b9c0	50	0%	(0) 0%	(0)	
tSEvent	5b1432c	50	0%	(0) 0%	(0)	
tSysTask	5b24058	60	0%	(0) 0%	(0)	
tChkPacket	hwapi_rx_c	5a470c4	60	0%	(2683) 0%	
tHNSD	ztask_main	5a7cd58	75	0%	(0) 0%	(0)
tMSTP	mstp_job_m	5a79638	75	0%	(1) 0%	(0)
tGpmsnoop	5a24c94	75	0%	(4) 0%	(4)	(0)
tSecureP	5a2b018	80	0%	(0) 0%	(0)	(0)
tApptask	5a200a0	85	0%	(0) 0%	(0)	(0)
tSysTimeL	5b2e5a0	90	0%	(0) 0%	(0)	(0)
HEB	prvDebugCa	79c4824	100	0%	(0) 0%	(0)
tSysmgmt	sysmgmtH	5b26a90	100	0%	(0) 0%	(0)
tGoahead	webatvmain	5a3cd0c	100	0%	(3459) 0%	(1867)
tTelnetd	5a3ef04	120	0%	(0) 0%	(0)	(0)
tPoeApp	5a1a550	121	0%	(588) 0%	(498)	(0)

Figure 8-17 CPU Information

Notes:

- Click “Clear” to clear the system task log from the window.
- Click “Refresh” to refresh the system task log.

8.4 Configuration Management

8.4.1 Configuration Management

Select “System Management→Configuration Management→Configuration Management”. Click “View the current configuration” to view the switch’s configuration.

The screenshot shows the Tripp-Lite PSE System Management web interface. At the top left is the Tripp-Lite logo. To its right, it says "Current User:admin". On the far right is a "Log Out" link next to a user icon. A vertical navigation menu on the left contains links to "System Home", "Quick Configuration", "Port Management", "VLAN Management", "Fault / Safety" (with sub-links for Attack Prevention, Path Detection, Loop Detection, Access Control, and IGMP Snooping), "System Management" (with sub-links for System Settings, System Upgrade, System Information, Configuration Management - which is highlighted, SNMP, and System Diagnostics), and "PSE System Management". The main content area has two tabs at the top: "Configuration Management" (active) and "Restore the Factory Settings". Below the tabs, a yellow box contains a description: "Description: View, save or export the current running configuration. Import a previously saved configuration." Underneath is another "Configuration Management" section header. It includes buttons for "View The Current Configuration" and "Save", followed by radio buttons for "Import Configuration" (selected) and "Export Configuration". A notice states: "Notice: 1. Do not close the page or refresh the page during the import process or the import will fail. 2. After importing a configuration, the switch must be restarted in order for settings to take effect." At the bottom, there's a "File Name:" label, a "Browse..." button, the text "No file selected.", and an "Import Configuration" button.

Figure 8-18 View the Current Configuration

8 System Management

Save Configuration

Select “System Management→Configuration Management→Configuration Management”. Click “Save” to save the running configuration.

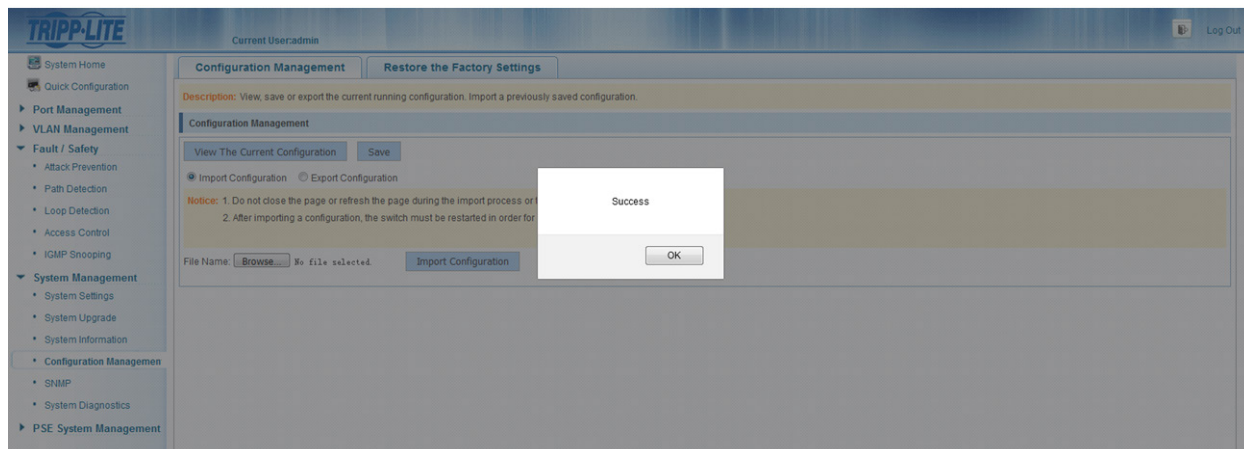


Figure 8-19 Save the Current Configuration

Import Configuration

Select “System Management→Configuration Management→Configuration Management”. Click “Import Configuration” radio button, then click “Browse” to select the file to import. Click “Import Configuration” button.

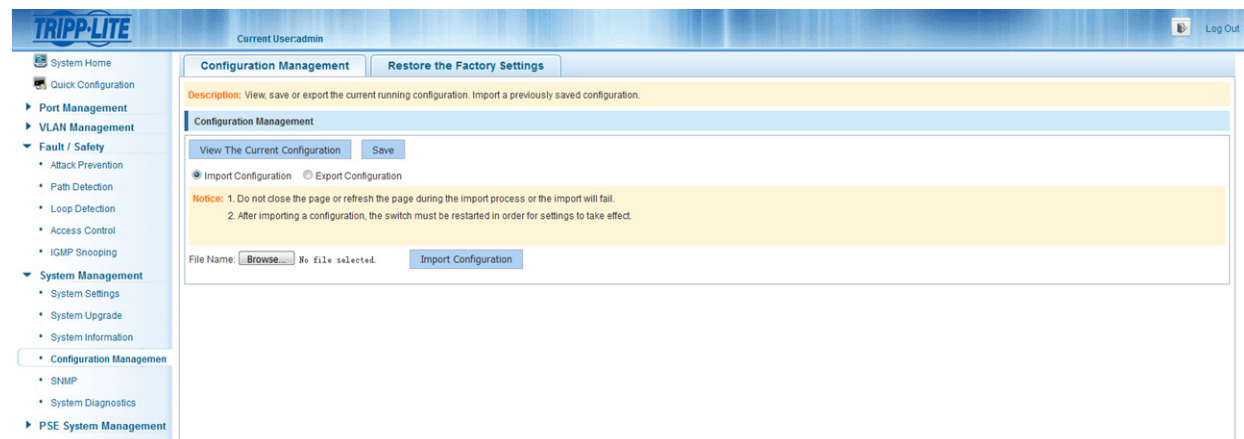


Figure 8-20 Import Configuration

Export Configuration

Select “System Management→Configuration Management→Configuration Management”. Click the “Export Configuration” radio button, then click the “Export configuration” button to export the current running configuration.

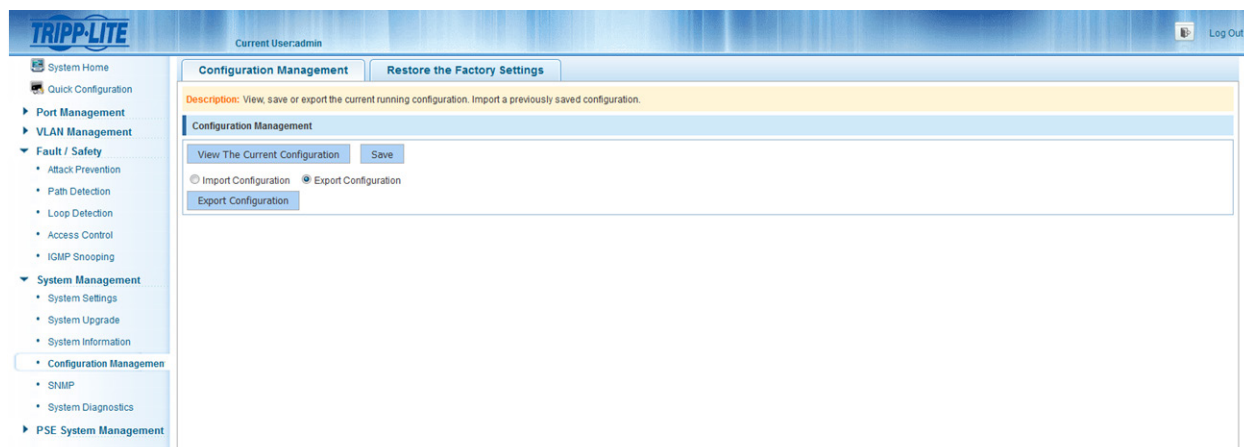


Figure 8-21 Export Configuration

8 System Management

8.4.2 Restore the Factory Settings

Select “System Management→Configuration Management→Restore the Factory Settings”. Click “Restore” to restore the factory configuration.

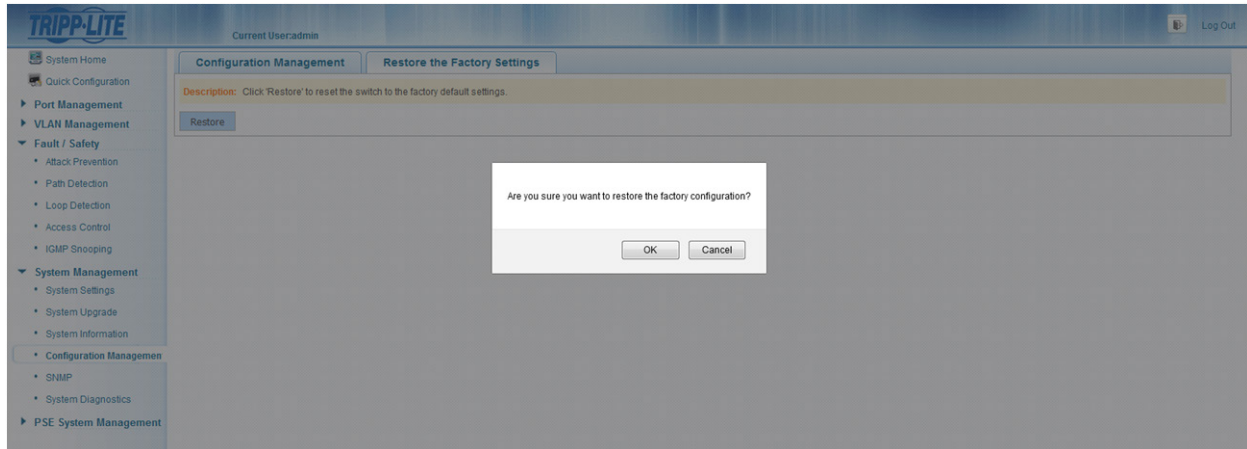


Figure 8-22 Restore the Factory Configuration

8.5 SNMP

8.5.1 View SNMP

Select “System Management→SNMP” to view the existing SNMP settings for the switch.

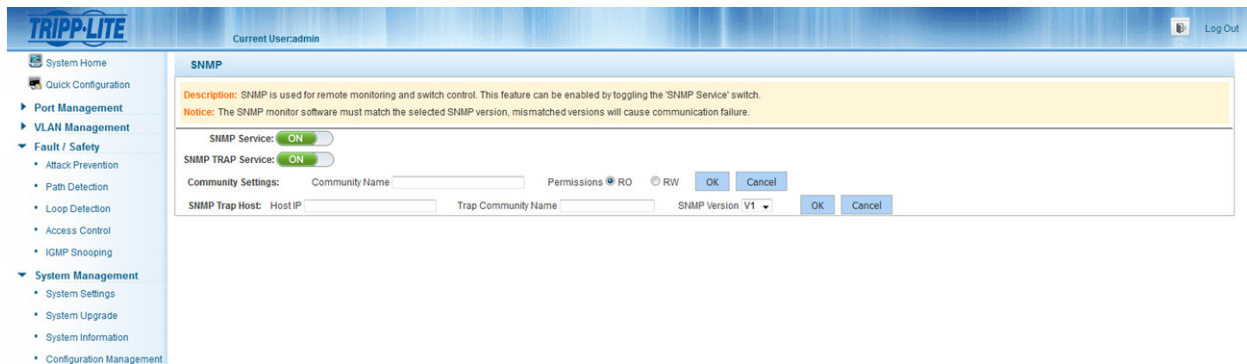


Figure 8-23 View the SNMP Configuration

Notes:

- By default, the SNMP is disabled.
- The SNMP monitor software must match the selected SNMP version; mismatched versions will cause communication failure.

8.5.2 Enable or Disable SNMP Service

Select “System Management→SNMP”. Click the ON/OFF button next to SNMP Service to enable or disable this feature.

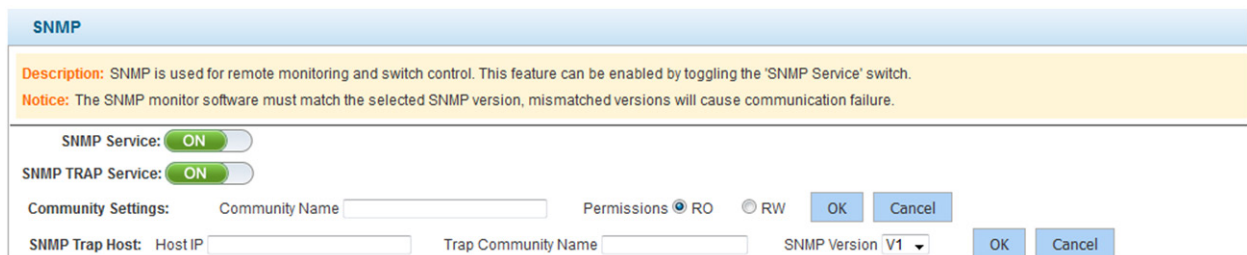


Figure 8-24 Enable or Disable SNMP Service

Note: SNMP version supports V1 and V2C.

8 System Management

8.5.3 Enable or Disable SNMP TRAP Service

Select “System Management→SNMP”. Click the ON/OFF button next to SNMP TRAP Service to enable or disable this feature.

SNMP TRAP Service: ☒ ON

Community Settings: Community Name Permissions ☒ RO ☐ RW

SNMP Trap Host: Host IP Trap Community Name SNMP Version V1

Figure 8-25 Activate SNMP TRAP Service

Note: After the TRAP function is enabled, you can send real-time TRAP messages with the use of a service host.

8.5.4 Add Community Name

Select “System Management→SNMP”. Type the community name, (e.g. **public**) in the corresponding field, then select the appropriate permission (RO or RW). Click “OK” to complete the configuration.

SNMP

Description: SNMP is used for remote monitoring and switch control. This feature can be enabled by toggling the 'SNMP Service' switch.
Notice: The SNMP monitor software must match the selected SNMP version, mismatched versions will cause communication failure.

SNMP Service: ☒ ON

SNMP TRAP Service: ☒ ON

Community Settings: Community Name Permissions ☒ RO ☐ RW

SNMP Trap Host: Host IP Trap Community Name SNMP Version V1

Community Name	Permissions	Remove
test	RO	<input checked="" type="button" value="X"/>

First Previous **1** Next Last 1 / 1Page

Figure 8-26 Add Community Name

Notes:

- Communities have two permissions options: RO (Read Only) or RW (Read/Write).
- When the SNMP Service is disabled, the community name is hidden and the SNMP TRAP service is disabled.

8.5.5 Delete Community Name

Select “System Management→SNMP”. Click the icon next to the community name you would like to delete.

SNMP

Description: SNMP is used for remote monitoring and switch control. This feature can be enabled by toggling the 'SNMP Service' switch.
Notice: The SNMP monitor software must match the selected SNMP version, mismatched versions will cause communication failure.

SNMP Service: ☒ ON

SNMP TRAP Service: ☒ ON

Community Settings: Community Name Permissions ☒ RO ☐ RW

SNMP Trap Host: Host IP Trap Community Name SNMP Version V1

Community Name	Permissions	Remove
test	RO	<input checked="" type="button" value="X"/>

First Previous **1** Next Last 1 / 1Page

Figure 8-27 Delete Community Name

8 System Management

8.5.6 Add SNMP TRAP Service Host

Select “System Management→SNMP”. Enter an IP address in the “Host IP” field, input a TRAP community name, then select an SNMP version. Click “OK” to complete the configuration.

Figure 8-28 Add SNMP TRAP Service Host

SNMP Trap service host list			
Trap Community Name	IP	Version	Remove
test	192.168.100.126	SNMP Ver 1	
First Previous [1] Next Last1 / 1Page			

Figure 8-29 Results of Adding SNMP TRAP Service Host

Note: When SNMP Service is disabled, the SNMP TRAP service host list is hidden.

8.5.7 Delete SNMP TRAP Service Host

Select “System Management→SNMP”. Select the SNMP TRAP service host you want to delete, then click the icon to complete the configuration.

SNMP Trap service host list			
Trap Community Name	IP	Version	Remove
test	192.168.100.126	SNMP Ver 1	
First Previous [1] Next Last1 / 1Page			

Figure 8-30 Delete SNMP TRAP Service Host

8.6 System Diagnostics

Select “System Management→System Diagnostics” to view the system diagnostic information for the switch.

Figure 8-31 System Diagnostics

9 Power Sourcing Equipment (PSE) System (Select models only)

9.1 PSE System Configuration

9.1.1 View PSE System Configuration

Select “PSE System→PSE System Configuration” to view the switch’s PSE configuration.

TRIPP-LITE
Current User: admin

System Home Quick Configuration

Port Management

VLAN Management

Fault / Safety

- Attack Prevention
- Path Detection
- Loop Detection
- Access Control
- IGMP Snooping

System Management

PSE System Management

- PSE System Configuration
- POE Port Configuration

PSE System Configuration

Notice: 1.Changing the Uninterrupted PoE Power setting will only take effect after saving the configuration. 2.The abnormal recovery time settings will only take effect when the power supply is set to automatic mode.

Uninterrupted PoE Power: Disabled
Non-standard PD compatible: Disabled
Power Supply Mode: Energy saving mode
PoE Guard Band: 0 %[0-10%]
Abnormal Recovery Time Interval: 10 /s(5-3600s)

Apply Settings Refresh

PSE System Information

Power supply port:	
Power management mode:	Energy saving mode
Uninterrupted PoE Power:	Disabled
Non-standard PD compatible:	Disabled
Abnormal Recovery Time Interval:	10s
System total power:	240 W
System power consumption:	0 W
System available power:	240 W (100%)
PoE Guard Band:	0%

Figure 9-1 View PSE System Configuration

9.1.2 Enable or Disable Uninterrupted PoE Power

Select “PSE System→PSE System Configuration”. From the “Uninterrupted PoE Power”, drop down menu select “Enabled” or “Disabled”. Click “Apply Settings” to save the configuration.

TRIPP-LITE
Current User: admin

System Home Quick Configuration

Port Management

VLAN Management

Fault / Safety

System Management

PSE System Management

- PSE System Configuration
- POE Port Configuration

PSE System Configuration

Notice: 1.Changing the Uninterrupted PoE Power setting will only take effect after saving the configuration. 2.The abnormal recovery time settings will only take effect when the power supply is set to automatic mode.

Uninterrupted PoE Power: Disabled
Non-Standard PD Compatible: Do Not Modify
Power Supply Mode: Energy saving mode
PoE Guard Band: 10 %[0-10%]
Abnormal Recovery Time Interval: 10 /s(5-3600s)

Apply Settings Refresh

PSE System Information

Power Supply Port:	
Power Management Mode:	Energy Saving Mode
Uninterrupted PoE Power:	Disabled
Non-Standard PD Compatible:	Disabled
Abnormal Recovery Time Interval:	10s
System Total Power:	240 W
System Power Consumption:	0 W
System Available Power:	216 W [90%]
PoE Guard Band:	10%

Figure 9-2 Enable Uninterrupted PoE Power

Note: The “Uninterrupted PoE Power” option defaults to disabled.

9 Power Sourcing Equipment (PSE) System (Select models only)

9.1.3 Non-standard PD Compatibility

Select “PSE System→PSE System Configuration”. From the “Non-standard PD compatible” drop down menu, select “Enabled” or “Disabled”. Click “Apply Settings” to save the configuration.

The screenshot shows the Tripp-Lite PSE System Configuration web interface. The left sidebar contains navigation links: System Home, Quick Configuration, Port Management, VLAN Management, Fault / Safety, System Management, PSE System Management, PSE System Configuration (selected), and POE Port Configuration. The main content area is titled "PSE System Configuration" and includes a notice: "1.Changing the Uninterrupted PoE Power setting will only take effect after saving the configuration. 2.The abnormal recovery time settings will only take effect when the power supply is set to automatic mode." Below the notice are several configuration options: Uninterrupted PoE Power (Disabled), Non-Standard PD Compatible (Disabled), Power Supply Mode (Do Not Modify), PoE Guard Band (Enabled, 10%), and Abnormal Recovery Time Interval (10s). At the bottom of the configuration section are "Apply Settings" and "Refresh" buttons. Below this is a "PSE System Information" table.

PSE System Information	
Power Supply Port:	
Power Management Mode:	Energy Saving Mode
Uninterrupted PoE Power:	Disabled
Non-Standard PD Compatible:	Disabled
Abnormal Recovery Time Interval:	10s
System Total Power:	240 W
System Power Consumption:	0 W
System Available Power:	216 W [90%]
PoE Guard Band:	10%

Figure 9-3 Non-standard PD Compatibility

9.1.4 Modify Power Supply Mode

Select “PSE System→PSE System Configuration”. From the “Power Supply Mode” drop down menu, select “Automatic Mode”, “Energy Saving Mode” or “Static Mode”. Click “Apply Settings” to complete the configuration.

The screenshot shows the Tripp-Lite PSE System Configuration web interface with the "Power Supply Mode" dropdown menu open. The mode is currently set to "Energy Saving Mode". Other settings remain the same as in Figure 9-3. The "Apply Settings" and "Refresh" buttons are visible at the bottom of the configuration section. The "PSE System Information" table is also present below.

PSE System Information	
Power Supply Port:	
Power Management Mode:	Energy Saving Mode
Uninterrupted PoE Power:	Disabled
Non-Standard PD Compatible:	Disabled
Abnormal Recovery Time Interval:	10s
System Total Power:	240 W
System Power Consumption:	0 W
System Available Power:	216 W [90%]
PoE Guard Band:	10%

Figure 9-4 Modify Power Supply Mode

Note: The default “Power Supply Mode” is “Automatic Mode”.

9 Power Sourcing Equipment (PSE) System (Select models only)

9.1.5 PoE Guard Band Configuration

Select “PSE System→PSE System Configuration” to view the “PoE Guard Band” settings for the switch. The PoE Guard Band protects the switch from an overload. To modify the setting, enter the desired value (between 0-10%) in the “PoE Guard Band” field and click “Apply Settings” to complete the configuration.

TRIPP-LITE
Current User: admin

System Home
Quick Configuration
Port Management
VLAN Management
Fault / Safety
Attack Prevention
Path Detection
Loop Detection
Access Control
IGMP Snooping
System Management
PSE System Management
PSE System Configuration
POE Port Configuration

PSE System Configuration

Notice: 1.Changing the Uninterrupted PoE Power setting will only take effect after saving the configuration. 2.The abnormal recovery time settings will only take effect when the power supply is set to automatic mode.

Uninterrupted PoE Power: Disabled
Non-standard PD compatible: Enabled
Power Supply Mode: Energy saving mode
PoE Guard Band: 0 % (0-10%)
Abnormal Recovery Time Interval: 10 /s (5-3600s)

Apply Settings Refresh

PSE System Information

Power supply port:	
Power management mode:	Energy saving mode
Uninterrupted PoE Power:	Disabled
Non-standard PD compatible:	Disabled
Abnormal Recovery Time Interval:	10s
System total power:	240 W
System power consumption:	0 W
System available power:	240 W (100%)
PoE Guard and:	0%

Figure 9-5 PoE Guard Band Configuration

Notes:

- PoE Guard Band is settable when Power Management Mode is in Energy Saving Mode.
- The range of the PoE Guard Band is 0-10%.

9 Power Sourcing Equipment (PSE) System (Select models only)

9.1.6 Abnormal Recovery Time Interval Configuration

Select “PSE System→PSE System Configuration”. Enter a value between 5-3600 seconds in the “Abnormal recovery time interval” field. Click “Apply Settings” to complete the configuration.

TRIPP-LITE

Current User: admin

Log Out

System Home

Quick Configuration

Port Management

VLAN Management

Fault / Safety

- Attack Prevention
- Path Detection
- Loop Detection
- Access Control
- IGMP Snooping

System Management

PSE System Management

- PSE System Configuration
- POE Port Configuration

PSE System Configuration

Notice: 1.Changing the Uninterrupted PoE Power setting will only take effect after saving the configuration. 2.The abnormal recovery time settings will only take effect when the power supply is set to automatic mode.

Uninterrupted PoE Power: Disabled

Non-standard PD compatible: Enabled

Power Supply Mode: Energy saving mode

PoE Guard Band: 0 % (0-10%)

Abnormal Recovery Time Interval: 10 /s (5-3600s)

Apply Settings Refresh

PSE System Information

Power supply port:	
Power management mode:	Energy saving mode
Uninterrupted PoE Power:	Disabled
Non-standard PD compatible:	Disabled
Abnormal Recovery Time Interval:	10s
System total power:	240 W
System power consumption:	0 W
System available power:	240 W (100%)
PoE Guard and:	0%

Figure 9-6 Abnormal Recovery Time Interval Configuration

Note: The abnormal recovery time interval defaults to 10 seconds.

9 Power Sourcing Equipment (PSE) System (Select models only)

9.2 PoE Port Configuration

9.2.1 View the PoE Port Configuration

Select “PSE System→PoE Port Configuration” to view the switch's PoE Port Configuration.

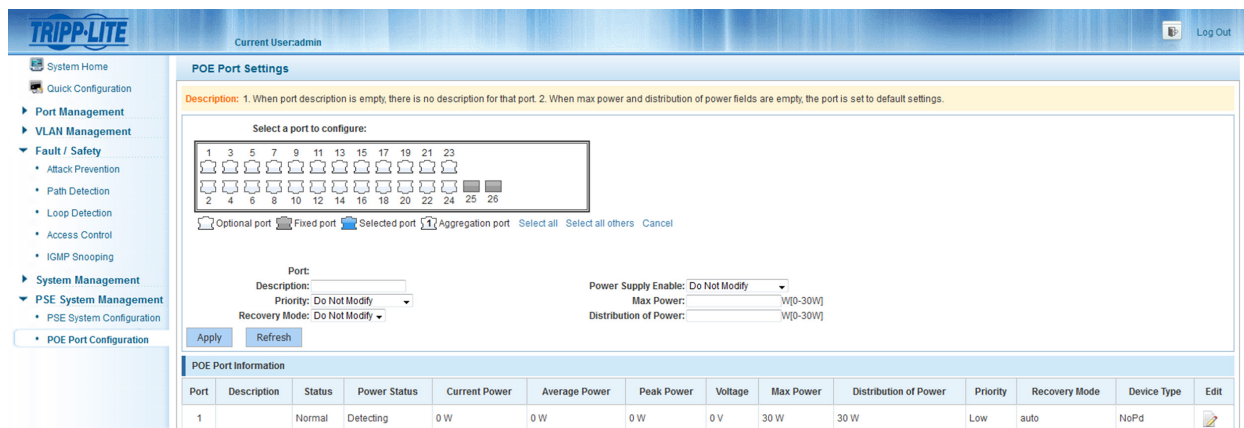


Figure 9-7 View the PoE Port Configuration

9.2.2 Enable Power Supply

Select “PSE System→PoE Port Configuration”. Select the port you want to configure from the panel. From the “Power supply enable” dropdown menu, select “Enabled” or “Disabled”. Click “Apply” to complete the configuration.

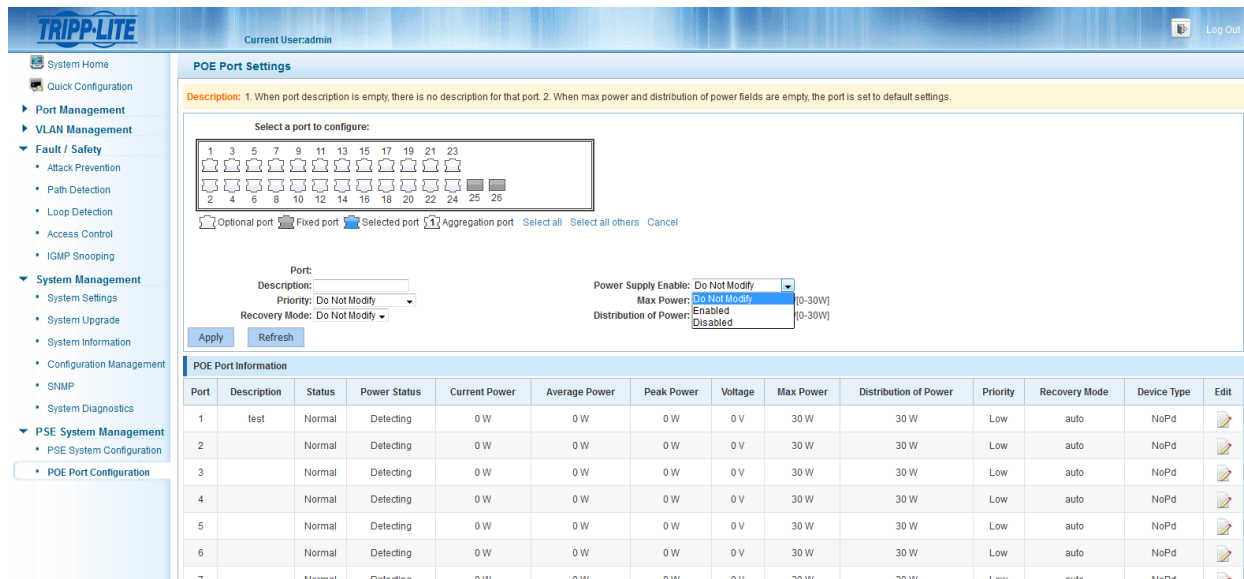


Figure 9-8 Enable or Disable Power Supply

Notes:

- Power supply enable defaults to “Enabled”.
- Multiple ports can be modified at the same time.

9 Power Sourcing Equipment (PSE) System (Select models only)

9.2.3 Modify Port Description

Select “PSE System→PoE Port Configuration”. Select the desired port from the panel and then enter a description in the “Description” field. Click “Apply” to complete the configuration.

POE Port Settings

Description: 1. When port description is empty, there is no description for that port. 2. When max power and distribution of power fields are empty, the port is set to default settings.

Select a port to configure:

1	3	5	7	9	11	13	15	17	19	21	23		
2	4	6	8	10	12	14	16	18	20	22	24	25	26

Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Port:
Description:
Priority: Do Not Modify
Recovery Mode: Do Not Modify
Apply Refresh
High Intermediate Low

Power Supply Enable: Do Not Modify
Max Power: W[0-30W]
Distribution of Power: W[0-30W]

Port	Description	Status	Power Status	Current Power	Average Power	Peak Power	Voltage	Max Power	Distribution of Power	Priority	Recovery Mode	Device Type	Edit
1	test	Normal	Detecting	0 W	0 W	0 W	0 V	30 W	30 W	Low	auto	NoPd	

Figure 9-9 Modify Port Description

Notes:

- Each port's default power supply status is “Enabled”.
- Multiple ports can be modified at the same time.

9 Power Sourcing Equipment (PSE) System (Select models only)

9.2.4 Modify Priority

Select “PSE System→PoE Port Configuration”. Select the desired port from the panel and then select “High”, “Intermediate” or “Low” from the “Priority” dropdown menu. Click “Apply” to complete the configuration.

The screenshot shows the Tripp-Lite POE Port Settings interface. On the left is a navigation menu with options like System Home, Quick Configuration, Port Management, VLAN Management, Fault / Safety, System Management, and PSE System Management. The main area is titled "POE Port Settings" and includes a description: "1. When port description is empty, there is no description for that port. 2. When max power and distribution of power fields are empty, the port is set to default settings." Below this is a "Select a port to configure:" section with a grid of port icons (1-26). Port 1 is selected. Below the grid are radio buttons for "Optional port", "Fixed port", and "Selected port" (which is selected). To the right of the grid are dropdown menus for "Port:", "Description:", "Priority:" (set to "Do Not Modify"), "Recovery Mode:" (set to "Do Not Modify"), "Power Supply Enable:" (set to "Do Not Modify"), "Max Power:" (set to "W(0-30W)"), and "Distribution of Power:" (set to "W(0-30W)"). There are "Apply" and "Refresh" buttons. Below the configuration fields is a "POE Port Information" table with columns: Port, Description, Status, Power Status, Current Power, Average Power, Peak Power, Voltage, Max Power, Distribution of Power, Priority, Recovery Mode, Device Type, and Edit. The table shows data for ports 1 through 7, all with a status of "Normal" and "Detecting", and a priority of "Low".

Figure 9-10 Modify Priority

Notes:

- The default priority is Low.
- There are three selectable priorities: High, Intermediate and Low.
- Multiple ports can be modified at the same time.

9.2.5 Modify Port Max Power

Select “PSE System→PoE Port Configuration”. Select the desired port from the panel and then enter a value between 0-30W in the “Max Power” field. Click “Apply” to complete the configuration.

The screenshot shows the Tripp-Lite POE Port Settings interface. On the left is a navigation menu with options like System Home, Quick Configuration, Port Management, VLAN Management, Fault / Safety, System Management, and PSE System Management. The main area is titled "POE Port Settings" and includes a description: "1. When port description is empty, there is no description for that port. 2. When max power and distribution of power fields are empty, the port is set to default settings." Below this is a "Select a port to configure:" section with a grid of port icons (1-26). Port 1 is selected. Below the grid are radio buttons for "Optional port", "Fixed port", and "Selected port" (which is selected). To the right of the grid are dropdown menus for "Port:", "Description:", "Priority:" (set to "Low"), "Recovery Mode:" (set to "Auto"), "Power Supply Enable:" (set to "Enabled"), "Max Power:" (set to "30 W(0-30W)"), and "Distribution of Power:" (set to "30 W(0-30W)"). There are "Apply" and "Refresh" buttons. Below the configuration fields is a "POE Port Information" table with columns: Port, Description, Status, Power Status, Current Power, Average Power, Peak Power, Voltage, Max Power, Distribution of Power, Priority, Recovery Mode, Device Type, and Edit. The table shows data for ports 1 through 7, all with a status of "Normal" and "Detecting", and a priority of "Low".

Figure 9-11 Modify Max Power of a Port

Notes:

- The default Max Power value is 30W.
- The available range is 0-30W.
- Multiple ports can be modified at the same time.

9 Power Sourcing Equipment (PSE) System (Select models only)

9.2.6 Modify Recovery Mode

Select “PSE System→PoE Port Configuration”. Select the desired port in the panel and then select “Manual” or “Auto” from the drop down menu in “Recovery Mode”. Click “Apply” to complete the configuration.

The screenshot shows the Tripp-Lite POE Port Settings interface. The left sidebar contains navigation links: System Home, Quick Configuration, Port Management, VLAN Management, Fault / Safety (Attack Prevention, Path Detection, Loop Detection, Access Control, IGMP Snooping), System Management (System Settings, System Upgrade, System Information, Configuration Management, SNMP, System Diagnostics), and PSE System Management (PSE System Configuration, POE Port Configuration). The main content area is titled "POE Port Settings" and includes a description: "Description: 1. When port description is empty, there is no description for that port. 2. When max power and distribution of power fields are empty, the port is set to default settings." Below this is a "Select a port to configure:" section with a grid of 26 port icons (1-26). Port 1 is selected. Below the grid are checkboxes for "Optional port", "Fixed port", "Selected port", and "Aggregation port", along with "Select all", "Select all others", and "Cancel" buttons. The "Port: 1" configuration section shows "Description: test", "Priority: Low", "Recovery Mode: Auto" (with a dropdown menu), and "Power Supply Enable: Enabled". The "Max Power: 30 W(0-30W)" and "Distribution of Power: 30 W(0-30W)" fields are also visible. Below the configuration section is a "POE Port Information" table with columns: Port, Description, Status, Power Status, Current Power, Average Power, Peak Power, Voltage, Max Power, Distribution of Power, Priority, Recovery Mode, Device Type, and Edit. The table lists 7 ports, all with "Normal" status and "Detecting" power status, and "Low" priority.

Port	Description	Status	Power Status	Current Power	Average Power	Peak Power	Voltage	Max Power	Distribution of Power	Priority	Recovery Mode	Device Type	Edit
1	test	Normal	Detecting	0 W	0 W	0 W	0 V	30 W	30 W	Low	auto	NoPd	
2		Normal	Detecting	0 W	0 W	0 W	0 V	30 W	30 W	Low	auto	NoPd	
3		Normal	Detecting	0 W	0 W	0 W	0 V	30 W	30 W	Low	auto	NoPd	
4		Normal	Detecting	0 W	0 W	0 W	0 V	30 W	30 W	Low	auto	NoPd	
5		Normal	Detecting	0 W	0 W	0 W	0 V	30 W	30 W	Low	auto	NoPd	
6		Normal	Detecting	0 W	0 W	0 W	0 V	30 W	30 W	Low	auto	NoPd	
7		Normal	Detecting	0 W	0 W	0 W	0 V	30 W	30 W	Low	auto	NoPd	

Figure 9-12 Modify Recovery Mode

Notes:

- Auto is the default Recovery Mode.
- There are two Recovery Modes: Auto and Manual.
- Multiple ports can be modified at the same time.

9.2.7 Modify Distribution of Power

Select “PSE System→PoE Port Configuration”. Select the desired port from the panel and then enter a value between 0-30W in the “Distribution of Power” field. Click “Apply” to complete the configuration.

The screenshot shows the Tripp-Lite POE Port Settings interface, similar to Figure 9-12, but with the "Distribution of Power" field set to 30 W(0-30W). The "POE Port Information" table is also visible, showing 7 ports with "Normal" status and "Detecting" power status.

Port	Description	Status	Power Status	Current Power	Average Power	Peak Power	Voltage	Max Power	Distribution of Power	Priority	Recovery Mode	Device Type	Edit
1		Normal	Detecting	0 W	0 W	0 W	0 V	30 W	30 W	Low	auto	NoPd	
2		Normal	Detecting	0 W	0 W	0 W	0 V	30 W	30 W	Low	auto	NoPd	
3		Normal	Detecting	0 W	0 W	0 W	0 V	30 W	30 W	Low	auto	NoPd	

Figure 9-13 Modify Distribution of Power

Notes:

- The default Distribution of Power setting of ports 1-8 is 30W.
- Distribution of Power is only enabled when the “Power Supply Mode” is set to “Static Mode”.
- The available range for the Distribution of Power field is 0-30W.
- Multiple ports can be modified at the same time.

Appendix I: Default Switch Configurations

The table below lists important default settings used in the switch.

Configuration Category		Default Setting
System	User name/password	admin/admin
	IP address	IP address: 192.168.1.200 Subnet mask: 255.255.255.0
	Serial baud rate	9600
	MAC address aging time	300s
	Device host name	TrippLite
Port	Port status	Active
	Port speed	Auto-Negotiation
	Port duplex mode	Auto-Negotiation
	Link aggregation	Unconfigured
	Broadcast storm suppression	Disable
	Port VLAN mode	Access
	NATIVE VLAN	1
VLAN	Management VLAN	VLAN 1
	VLAN function pattern	802.1Q
IGMP Snooping	Global IGMP snooping	Disabled

Technical Support

You can reach Tripp Lite Technical Support here:

E-mail

techsupport@tripplite.com

Web

The latest switch software updates are available at www.tripplite.com/software/

Technical Support Assistance

www.tripplite.com/support



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