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	Intro	oduction	4
	1.1	Switch Configurations	4
	1.2	Contents	4
2	Web	Management Homepage	5
	2.1	Setup	5
		2.1.1 Set the IP Address of the Computer	5
		2.1.2 Confirm Network Connectivity Between the Computer and the Switch	5
		2.1.3 Access to the Web Management Interface	5
3	Web	Management Interface	7
	3.1	Web Management Interface Overview	7
	3.2	Web Management Interface	7
	3.3	Introduction to Page Controls	9
	3.4	Web Management Interface Login Timeout Settings	9
4	Quic	k Configuration	10
	4.1	VLAN Settings	10
	4.2	Trunk Port Settings	10
	4.3	SNMP Settings	11
	4.4	PoE Settings (Compatible PoE models only)	11
	4.5	Other Settings	12
		4.5.1 Modify Switch Management IP Address Settings	12
		4.5.2 Modify Super-User Password	12
5	Port	Management	13
	5.1	Basic Settings	13
		5.1.1 View the Port Configuration	13
		5.1.2 Configure Individual Ports	13
	5.2	Storm Control Settings	14
		5.2.1 Configure the Storm Control Settings of a Port	14
		5.2.2 Storm Control Configuration	14
	5.3	Flow Control	15
		5.3.1 View Flow Control Settings	15
		5.3.2 Flow Control Configuration	15
	5.4	Port Isolation	16
		5.4.1 View the Port Isolation List	16
		5.4.2 Port Isolation Configuration	16
	5.5	Port Aggregation	17
		5.5.1 View Port Aggregation Configuration	17
		5.5.2 How to Create a Port Aggregation Group	17
		5.5.3 Modify a Port Aggregation Group	18
		5.5.4 Delete a Port Aggregation Group	18
	5.6	Port Mirroring	19
		5.6.1 View Port Mirroring Configuration	19
		5.6.2 Create a Port Mirroring Group	19
		5.6.3 Edit a Port Mirroring Group	20
		5.6.4 Delete a Port Mirroring Group	21

	5.7	Port Speed Limit	21
		5.7.1 View the Port Speed Limit Settings	21
		5.7.2 Port Input/Output Speed Limit Configuration	22
		5.7.3 Edit Port Speed Limit Settings	22
6	VLA	N Management	23
	6.1	VLAN Management	23
		6.1.1 View VLAN Configuration	23
		6.1.2 How to Add a VLAN	23
		6.1.3 Delete a VLAN	24
		6.1.4 Edit or Add Ports to an Existing VLAN	24
		6.1.5 View Trunk Port Settings	25
		6.1.6 Add Trunk Port Settings	25
		6.1.7 Delete a Trunk Port	26
7	Faul	t/Safety	27
	7.1	Attack Prevention	27
		7.1.1 ARP Spoofing	27
		7.1.2 Port Security	29
		7.1.3 DHCP Snooping	31
	7.2	Path Detection	33
	7.3	Loop Detection	33
		7.3.1 View Loop Detection Configuration	33
		7.3.2 Enable Loop Detection	34
		7.3.3 Loop Detection Configuration	34
		7.3.4 Detection Time Interval	34
		7.3.5 Automatic Recovery Time	35
		7.3.6 Disable Loop Detection	35
	7.4	Access Control Lists (ACLs)	35
		7.4.1 ACL	35
		7.4.2 Apply ACL	38
	7.5	IGMP Snooping	40
		7.5.1 IGMP Snooping Configuration	40
		7.5.2 Activate the IGMP Snooping Function	40
		7.5.3 Disable the IGMP Snooping Function	41
		7.5.4 Multicast Routing Port Settings	41
		7.5.5 IGMP Version	41
8	-	tem Management	42
	8.1	System Settings	42
		8.1.1 Management VLAN	42
		8.1.2 System Restart	43
		8.1.3 Modify the Password	44
		8.1.4 System Log	44
		8.1.5 LOG Export	45
		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
	8.3.1 Memory Information	48
	8.3.2 CPU Information	49
8.4	Configuration Management	49
	8.4.1 Configuration Management	49
	8.4.2 Restore the Factory Settings	51
8.5	SNMP	51
	8.5.1 View SNMP	51
	8.5.2 Enable or Disable SNMP Service	51
	8.5.3 Enable or Disable SNMP TRAP Service	52
	8.5.4 Add Community Name	52
	8.5.5 Delete Community Name	52
	8.5.6 Add SNMP TRAP Service Host	53
	8.5.7 Delete SNMP TRAP Service Host	53
8.6	System Diagnostics	53

9			urcing Equipment (PSE) System odels only)	54				
	9.1	PSE S	ystem Configuration					
		9.1.1	View PSE System Configuration	54				
		9.1.2	Enable or Disable Uninterrupted PoE Power	54				
		9.1.3	Non-standard PD Compatibility	55				
		9.1.4	Modify Power Supply Mode	55				
		9.1.5	PoE Guard Band Configuration	56				
		9.1.6	Abnormal Recovery Time Interval Configuration	57				
	9.2	PoE Po	ort Configuration	58				
		9.2.1	View the PoE Port Configuration	58				
		9.2.2	Enable Power Supply	58				
		9.2.3	Modify Port Description	59				
		9.2.4	Modify Priority	60				
		9.2.5	Modify Port Max Power	60				
		9.2.6	Modify Recovery Mode	61				
		9.2.7	Modify Distribution of Power	61				
Ар	pendi	ix I: D	efault Switch Configurations	62				
Teo	chnica	al Sup	port	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.

2.1 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.

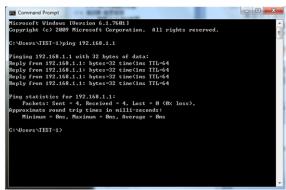
2.1.2 Confirm Network Connectivity Between the Computer and the Switch

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.

Run	? 🗵
-	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	Emd
	OK Cancel Browse

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.

	붩 User Log	in
	Please input yo	our user name and password!
	Language:	English -
TRIPP·LITE	User Name:	
	Password:	
		Login

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:

🛃 System Home										
S Quick Configuration	NSS-G24D2P24 Version 10.1.1.2-1212	:5	CPU: 3%	Available Memory:76	MB Device Time: Device Name:	2016-1-19 11:27:33				
Port Management	PROFESSION NO.				Device Maine.	Switch				
/LAN Management										
Fault / Safety										
System Management										
PSE System Management			1351	9 11 13 15 17 19 21 23	roz /100M =Link @Act 1000M =Link @Act		9 11 13 15 17 19	21 23 NSS-G24	D2P24	
					PCR				• 26	
					POE /100M -Link MAct		10 12 14 16 18 20	22 24 25F 261	• 26 • 25 F	
					POE /100M -Link MAct	Console 2 4 6 8	10 12 14 16 18 20	22 24 25F 265		
					POE /100M -Link MAct	Console 2 4 6 8	10 12 14 16 18 20	22 24 25F 265		
					POE /100M -Link MAct	Console 2 4 6 8	10 12 14 16 18 20	22 24 25F 261		
			2 4 6 9		POE /100M -Link MAct	Console 2 4 6 S	10 12 14 16 18 20	22 24 25F 26		
					POE /100M -Link MAct	Console 2 4 6 8	10 12 14 16 18 20	22 24 257 265		1000 Disconnect 💿 Disc
	Dart Information	Elow Trant	Device Continue	10 10 10 10 10 10 10 10 10 10 10	78000 - 2112 - 2421	Console 2 4 6 8	10 12 14 16 18 20	22 24 23F 261) 10001 🍙 Disconnect 🙆 Disc
	Port Information	Flow Trend	Device Configur		ng Cook the state	Cossole 2 4 6 8	10 12 14 16 18 20	22 24 235 26		1000 Directaret 🗿 dire
	Port Information Keyword:	Flow Trend	Device Configur	10 10 10 10 10 10 10 10 10 10 10	78000 - 2112 - 2421	Cossole 2 4 6 8	10 12 14 16 18 20	22 24 23F 26		1000# Directatet @Dire
		Flow Trend Descri	Search	10 10 10 10 10 10 10 10 10 10 10	ng Cook the state	Console 2 4 6 8	10 12 14 16 18 20	22 24 23F 260		10001 🍙 Disconnet 🙆 Disc Edit



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

TRIPP-LITE	Current User:a	admin							Dog Out
🖲 System Home	NSS-G24D2P24	CPU: 4%	Available Memory:76	MB Device Time:	2016-1-19 11:40:57				
SQUICK Configuration	Version 10.1.1.2-12125			Device Name:	Switch				
Port Management									
VLAN Management									
Fault / Safety									
 System Management PSE System Management 			9 11 13 15 17 19 21 23		1 3 5 7	9 11 13 15 17 19			
				or Social + Link * Art Social + Link * Art Social + Link * Art	Console 2 4 6 8	10 12 14 16 18 20	22 24 25F 26F	€ 25 • 25	
								10/1000	1000M 💼 Disconnect 💼 Disabled
	Port Information	Flow Trend Device Configura	ation Port Statist	tics					
	Keyword:	Search		Refresh					
	Port	Description	Input Flow(Bps)	Output Flow(Bps)	Open Status	Connection Status	VLAN	Trunk Port	Edit
	Gi 0/1		0K	0К	Enabled	😽 Not Connected	1	No	Check the Flow Trend

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

-							
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	1. Add or delete VLANs, add ports to a VLAN or remove ports from a VLAN.					
	Management	2. Add or delete a Trunk, add ports to a Trunk or remove ports from a Trunk.					
Fault/Safety	Attack Prevention	 View the ARP state table, activate or deactivate the ARP anti-spoofing functions of a port. Enable or disable port security and set up a binding IP address and MAC address for a port. 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	 Set the management VLAN IP address and subnet mask. Reboot the system. Change the user password and the telnet login password. View and export system log. Check an ARP entry. Query the MAC address table, set static MAC address and add or delete static MAC Addresses. 					
	System Upgrade	Upgrade the switch software.					
	System	1. Memory usage.					
	Information	2. System tasks.					
	Configuration	1. Backup, restore the system configuration backup.					
	Management	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					

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

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.
Broadcast, Multicast Close Broadcast Unicast Multicast Broadcast, Unicast Unicast, Multicast Unicast, Multicast Broadcast, Unicast, Multicast	Dropdown menus, used to select an item from a menu.
File Name: Browse 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	Refresh the current page configuration.
Save	Save the current page configuration.
Cancel	Cancel the current page configuration or the current system information.
ОК	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".

TRIPPILITE	Current Use	r:admin								🚯 Log O
🛃 System Home	VLAN Settings	Trunk Port Settings	SNMP Settings	POE	Other Set	ings				
SQuick Configuration	VLAN									
Port Management		VLAN ID	VLAN	I Name			VLAN IP	Port	Edit	
VLAN Management Fault / Safety		1	DEF	AULT			10.20.0.186	1-26		
 System Management 	🔾 New VLAN 🤤 De	lete VLAN						First Previo	ous [1] Next Last1	/ 1Page
PSE System Management										
					_					
						→ Next				
							_			

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.

TRIPPILITE	Current User	admin							Log Out		
🛃 System Home	VLAN Settings	Trunk Port Settings	SNMP Settings	POE	Other Settings						
Quick Configuration Port Management	Description: If a port is a	llowed to send messages through	multiple VLANs, the port sh	iould be set as a	a trunk.						
VLAN Management	Trunk Port List										
Fault / Safety		Port	N	ative VLAN			Allowed VLAN		Edit		
System Management	New Trunk Port List	🤤 Delete Trunk Port						First Previous [1] Next Last1	/ 1Page		
PSE System Management											
				Previo	bus	→ Next]				

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.

TRIPPILITE	Current User:	admin							🕑 Log Out
🖲 System Home	VLAN Settings	Trunk Port Settings	SNMP Settings	POE	Other Settings				
Quick Configuration Port Management VLAN Management	Notice: The SNMP monito	ed for remote monitoring and swite or software must match the selecte							
 Fault / Safety System Management 	SNMP Service:	OFF							
PSE System Management	Community Settings: SNMP Trap Host: Host	Community Name	Trap Community Name	ermissions 🖲	RO © RW OK SNMP Version	Cancel	Cancel		
	Previous Dext								

Figure 4-3 SNMP Settings

4.4 PoE Settings (Compatible PoE models only)

Select "Quick Configuration \rightarrow 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.

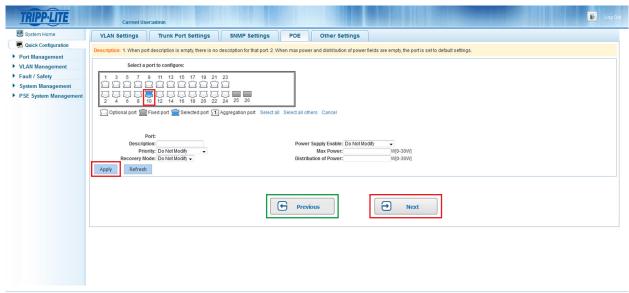


Figure 4-4 PoE Settings

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.

TRIPPILITE	Current Usersadmin	Log Out							
E System Home	VLAN Settings Trunk Port Settings SNMP Settings Other	Settings							
Quick Configuration Port Management	The basic information of the system settings								
✓ VLAN Management	VLAN Management: Vlan 1 V Management IP: [192.168.1.200	MAC: 24:05:07:66:02:02 * Device Name: Switch *							
VLAN Management Fault / Safety	Subnet Mask: [235, 235, 0] *	Device Location:							
 System Management System Settings 	Default Gateway: 192. 168. 1. 1 * Login Timeout: 30	Contact Name:							
 System Upgrade 	Management Port: 80								
System Information	Save								
Configuration Management SNMP	Modify the super user password Old Password:								
System Diagnostics	New Password:								
	Confirm New Password: * Save Empty								
		Previous Complete							

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.

5.1 Basic Settings

5.1.1 View the Port Configuration

Select "Port Management→Basic Settings" to view and modify port settings.

TRIPPILITE	Curre	int User:admin					Log Out
System Home Basic Settings							
Quick Configuration Port Management	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.						
Basic Settings Storm Control	Select a port to configure:						
Storm Control Some Ca for to Compute: Some Ca for the Ca for							
PSE System Management	Port List						
	Port	Description	Status	Rate	Duplex Mode	MTU	Edit
1 Enabled Auto Auto 1518							
	2		Enabled	Auto	Auto	1518	2
	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.

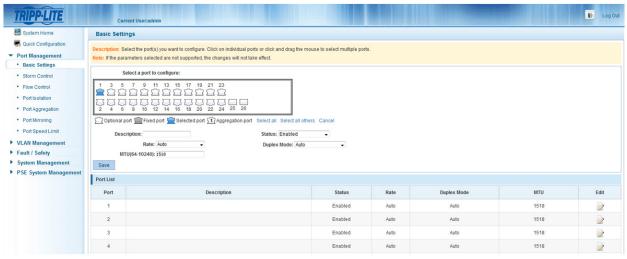


Figure 5-2 Individual Port Configuration

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

5.2 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.

System Home	Storm Control						
Quick Configuration Port Management Basic Settings	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.						
Storm Control	Select a port	to configure:					
Flow Control Four Control Port Isolation Port Magregation Port Magregation Port Management VLAN Management Save					of 64 between 64-200000)		
Fault / Safety System Management	Port List						
PSE System Management	Port	Unicast		Broadcast	Multicast	Edit	
	1	Disabled		Disabled	Disabled		
	2	Disabled		Disabled	Disabled	2	
	3	Disabled		Disabled	Disabled	2	

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, Bro
- 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:		
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	
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 👻	St	orm control value: 64	(Unit: kbps, value 64-200000 v	within a multiple of 64)
Save Port List	Close Broadcast Unicast Multicast				
Port	Broadcast,Unicast Broadcast,Multicast Unicast,Multicast		Broadcast	Multicast	Operation
1	Broadcast,Unicast,Multicast		Disabled	Disabled	

Figure 5-5 Storm Control Configuration Information

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 \rightarrow Flow Control" to configure flow control settings for any port(s).

TRIPPILITE	Current User:admin		🚯 Log Out					
😸 System Home	Flow Control							
SQUICK Configuration	Description: Select the port(s) you w	ant to configure. Click on individual ports or click and drag the mouse to select multiple ports.						
 Port Management Basic Settings 	Note: If the parameters selected are not supported, the changes will not take effect.							
Storm Control	Select a port to configure:							
Flow Control	1 3 5 7 9 11 13	15 17 19 21 23						
Port Isolation								
Port Aggregation								
Port Mirroring	Coptional port 🚔 Fixed port 🚔 Selected port 11 Apgregation port Select all Others Cancel							
Port Speed Limit	Flow Control Type: Off							
 VLAN Management Fault / Safety 	Save							
System Management	Port List							
PSE System Management	Port	Flow Control	Edit					
	1	on						
	2	Off	2					
	3	on						
	4	Off	2					
	а	∩#	B .					

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".

TRIPPILITE	Current User:admin		Dog Out				
Bystem Home Flow Control							
Quick Configuration Port Management Basic Settings	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.						
Storm Control	Select a port to config	ure:					
Flow Control Port Isolation Port Aggregation Port Mirroring Port Speed Limit VLAN Management Fault / Safety	1 3 5 7 9 11 31 15 17 19 21 22 1 1 1 1 15 17 19 21 22 24 10						
System Management	Port List						
PSE System Management	Port	Flow Control	Edit				
	1	on	2				
	2	Off					
	3	n	2				
	4	n					
	-						

Figure 5-8 Enable Port Flow Control Function

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

Flow Control	Operation
On	
Off	
On	
Off	
Off	
	On Off On

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 \rightarrow 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).

	Current User:admin		Dog				
🛃 System Home	Port Isolation						
Outlick Configuration Port Management Storm Control Flow Control Port Isolation Port Aggregation Port Aggregation Port Speed Limit VLAN Management	Description: First, click the Edit (con 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 (con first to configure port isolation. Select a port to configure: 1 5 2 4 5 7 2 4 6 10 1 15 2 4 8 10 1 15 2 4 8 10 1 15 2 4 3 10 3 10 4 10 10 12 10 12 10 12 10 12 10 12 10 12 10 12 10 12 12 12 12 12 12 12 12						
Fault / Safety System Management	Port List						
PSE System Management	Port	Isolated Port/Ag	Edit				
	1	5.7					
	2		2				
	3						

Figure 5-10 View Port Isolation List

5.4.2 Port Isolation Configuration

Click the $\boxed{2}$ 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.

TRIPP·LITE	Current User:admin		Dog Out					
🛃 System Home	Port isolation							
R Quick Configuration	Description: First, click the Edit (con 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,							
 Port Management 	The isolated port(s) will now appear in the table.							
Basic Settings	Notice: You must click the 'Edit' icon first to co	onfigure port isolation.						
Storm Control	Select a port to configure:							
Flow Control	r	7 19 21 23						
Port Isolation		7 19 21 23 注意意意						
 Port Aggregation 	8888888888	355500						
Port Mirroring		8 20 22 24 25 26						
Port Speed Limit	Optional port 💼 Fixed port 💼 Select	ted port 1 Aggregation port Select all Select all others Cancel						
VLAN Management	Save							
 Fault / Safety System Management 	Port List							
PSE System Management	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.

5.5 Port Aggregation

5.5.1 View Port Aggregation Configuration

Select "Port Management \rightarrow 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.

TRIPPILITE					🕑 🛛 Log Out
	Current User:admin				
📑 System Home	Port Aggregation				
SQUICK Configuration	Description: Port aggregation allows multiple po	te to be combined to form a single logical link. Each grou	p can contain up to 8 ports. Aggregation groups must contain	n an even number of norts	
 Port Management 					
Basic Settings	Load Balancing: mac - Apply				
Storm Control	Aggregation ID (1-16):	*			
Flow Control	Select a port to configure:				
Port Isolation	1 3 5 7 9 11 13 15 17 1	19 21 23			
Port Aggregation					
Port Mirroring		20 22 24 25 26			
Port Speed Limit	Optional port 🚍 Fixed port 🚍 Selected p	ort [1] Aggregation port Select all Select all others C	Cancel		
▼ VLAN Management	Aggregation Type: Not Se	lected -			
 VLAN Management 	Save Cancel				
▼ Fault / Safety	Save Calicel				
Attack Prevention	Aggregation List				
Path Detection	Aggregation ID	Aggregation Type	Number of Ports	Member Port	Edit
Loop Detection				First Previor	us [1] Next Last1 / 1Page
Access Control					
 IGMP Snooping 					

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 $\int 1$ in the panel.

TRIPP·LITE	Current User:admin				Deg Out				
📕 System Home	Port Aggregation								
R Quick Configuration	Description: Port aggregation allows multiple por	ts to be combined to form a single logical link. Each group	can contain up to 8 ports. Aggregation groups must con	tain an even number of ports.					
Port Management Basic Settings	Load Balancing: mac 🗸 Apply	d Balancing: mac 👻 Apply							
Storm Control	Aggregation ID (1-16):								
Flow Control	Select a port to configure:								
Port Isolation	1 3 5 7 9 11 13 15 17 19 21 23								
Port Aggregation									
Port Mirroring									
Port Speed Limit	Coptional port Rixed port Selected p	ort 77 Aggregation port Select all Select all others C	ancel						
 VLAN Management Fault / Safety System Management PSE System Management 	Aggregation Type: Not Selected Save Cancel Aggregation List								
	Aggregation ID	Aggregation Type	Number of Ports	Member Port	Edit				
	1	Dynamic	4	1,2,3,4	2 🗙				
				First Previo	ous [1] Next Last1 / 1Page				

Figure 5-13 Port Aggregation Configuration

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	Port Aggregation						
SQuick Configuration	Description: Port aggregation allows multiple por	ts to be combined to form a single logical link. Each group	can contain up to 8 ports. Addregation groups must con	tain an even number of ports			
 Port Management Basic Settings 	Load Balancing: mac 🗸 Apply	· · · · · · · · · · · · · · · · · · ·					
Storm Control	Aggregation ID (1-16):						
Flow Control	Select a port to configure:						
Port Isolation	1 3 5 7 9 11 13 15 17 19 21 23						
Port Aggregation							
Port Mirroring		0 22 24 25 26					
Port Speed Limit	Coptional port Pixed port Selected p	ort 517Aggregation port Selectall Selectall others Ca	ancel				
VLAN Management	Aggregation Type: Not Sel	ected 👻					
Fault / Safety	Save Cancel						
System Management	Aggregation List						
PSE System Management							
	Aggregation ID	Aggregation Type	Number of Ports	Member Port	Edit		
	1	Dynamic	4	1,2,3,4	📄 🗙		
				First Previo	us [1] Next Last1 / 1Page		

Figure 5-14 Modify Port Aggregation Group

5.5.4 Delete a Port Aggregation Group

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

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

Figure 5-15 Delete Port Aggregation

5.6 Port Mirroring

5.6.1 View Port Mirroring Configuration

Select "Port Management \rightarrow 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.

TRIPPILITE	Current Useradmin						
🛃 System Home	Port Mirroring						
Quick Configuration Port Management	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.						
Basic Settings	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.						
Storm Control	Choose the source port:(Selecting multiple source ports can affect the device performance.).						
Flow Control	1 3 5 7 9 11 13 15 17 19 21 23						
Port Isolation							
Port Aggregation							
Port Mirroring	🖸 Optional port 💼 Fixed port 💼 Selected port 🏦 Aggregation port 🏦 Mirroring Group 🛛 Select all Others Cancel						
Port Speed Limit	Choose the destination port:(choose only one port)						
VLAN Management	1 3 5 7 9 11 13 15 17 19 21 23						
Fault / Safety							
 System Management PSE System Management 							
· · · St. System management	🖸 Optional port 👮 Fixed port 🙀 Selected port 🕥 Aggregation port						
	Save Refresh Mirroring Group Not Selected -						
	Mirroing Port List						
	Mirroring Group Source Port Destination Port Edit						
	First Previous [1] Next Last						
	rist rienus () rek Lasti / / raye						

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.
- St 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".

TRIPPILITE	Current Useradmin							
📕 System Home	Port Mirroring							
R Quick Configuration	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.							
 Port Management 	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.							
Basic Settings	Choose the source port:/Selecting multiple source ports can affect the device performance.).							
Storm Control	1 3 5 7 9 11 13 15 17 19 21 23							
Flow Control								
Port Isolation								
Port Aggregation	2 4 6 8 10 12 14 16 18 20 22 24 25 26							
Port Mirroring	🖸 Optional port 💼 Fixed port 💼 Selected port 🏦 Aggregation port 🚳 Mirroring Group Select all Select all others Cancel							
Port Speed Limit	Choose the destination port(choose only one port)							
VLAN Management	1 3 5 7 9 11 13 15 17 19 21 23							
Fault / Safety								
System Management								
PSE System Management								
	Copional port 🚍 Fixed port 🚘 Selected port 🏦 Appregation port							
	Save Refresh Mirroring Group Not Selected -							
	Mirroring Port List							
	Mirroring Group Source Port Destination Port Edit							
	First Previous [1] Next Lasis / 1Page							

Figure 5-17 Add Port Mirroring Group

TRIPPILITE	Current User:admin			🕑 Log Out				
🛃 System Home	Port Mirroring							
Cuick Configuration Cuick Configuration Cuick Configuration Basic Settings Storm Control Flow Control Flow Control	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.). 1 3 5 7 9 11 13 15 17 19 21 23							
Port Isolation Port Aggregation Port Mirroring	Image: Contract							
PortSpeed Limit VLAN Management Fault / Safety System Management PSE System Management	Choose the destination port/choose only one port) 1 3 5 7 9 11 13 15 17 19 21 23 20 20 20 20 20 20 20 20 20 20 22 22 25 20 Contract port 20 20 22 22 25 20<							
	Mirroring Port List							
	Mirroring Group	Source Port	Destination Port	Edit				
	1	1	3	2 🗙				
			First Previo	ous [1] Next Last1 / 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.

TRIPP-LITE	Current User:admin			🕑 Log Out					
🛃 System Home	Port Mirroring								
Ouick Configuration Port Management Basic Settings Storm Control Flow Control Port Isolation Port Aggregation	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.). 1 3 5 7 9 11 13 15 17 19 21 23 9 9 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0								
Port Mirroring	🖸 Optional port 🚍 Fixed port 🚍 Selected port 🙀 Appregation port 🙀 Milmoning Group Select all Select all Others Cancel								
PortSpeed Limit VLAN Management Fault / Safey System Management PSE System Management									
	Mirroring Port List								
	Mirroring Group	Source Port	Destination Port	Edit					
	1	1	3	2 🗙					
			First Previous [1] Net Last // / Page						

Figure 5-19 Modify Port Mirroring Group

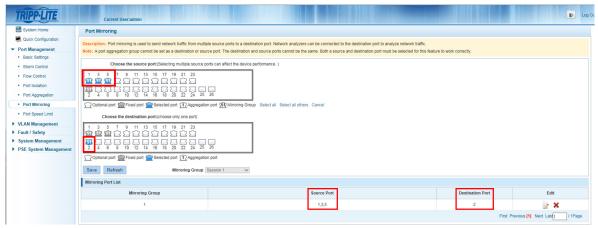


Figure 5-20 Results after a Successful Modification of Port Mirroring

5.6.4 Delete a Port Mirroring Group

Click the \mathbf{X} icon next to the port mirroring group that you want to delete.

Mirroring Group	Source Port	Destination Port	Edit
1	1	3	📝 🗙

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.

TRIPPILITE	Current User:a	idmin		Dog Out				
System Home	Port Speed Limit							
Quick Configuration Port Management Basic Settings	Description: Select the po Notice: 1000Kbps = 1Mbp	ption: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports. 1000Kbps = 1Mbps						
Storm Control		Select a port to configure						
Flow Control Port Isolation Port Aggregation Port Mirroring	□ □							
Port Speed Limit VLAN Management Fault / Safety System Management	Input Speed Limit: Output Speed Limit: Save	Input Speed Limit: (64-100000) Kbit/s Output Speed Limit: (64-100000) Kbit/s						
PSE System Management	Port Speed Limit List							
	Port	Input Speed Limit	Output Speed Limit	Edit				
	1	MAX	МАХ					
	2	MAX	MAX					
	3	MAX	MAX	2				
	4	MAX	MAX	2				
	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.

5.7.2 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".

TRIPPILITE	Current User:a	dmin		🚯 Log Out			
🛃 System Home	Port Speed Limit	Port Speed Limit					
Quick Configuration Port Management Basic Settings	Description: Select the po Notice: 1000Kbps = 1Mbp	rt(s) you want to configure. Click on individual ports or click and drag the mouse to sele is	ct multiple ports.				
Storm Control Flow Control Flow Control Port Isolation Port Aggregation Port Aggregation Port Speed Limit VLAN Management Fault / Safety System Management	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$						
PSE System Management	Port Speed Limit List						
	Port	Input Speed Limit	Output Speed Limit	Edit			
	1	10.000MbiVs	10.000Mbit/s				
	2	МАХ	MAX	2			
	3	МАХ	MAX	2			
	4	МАХ	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:ad	min		🕑 Log Out	
🛃 System Home	Port Speed Limit				
Quick Configuration Port Management Basic Settings	Notice: 1000Kbps = 1Mbps		d multiple ports.		
Storm Control Flow Control Port Isolation Port Aggregation Port Mirroring Port Speed Limit	Select a port to configure 1 3 5 7 9 11 13 15 17 19 21 23 2 1 12 13 12 <t< td=""></t<>				
 VLAN Management Fault / Safety System Management PSE System Management 	Input Speed Limit: 5000 Output Speed Limit: 5000 Save Port Speed Limit List				
	Port	Input Speed Limit	Output Speed Limit	Edit	
	1	500.000Mbit/s	500.000Mbit/s		

Figure 5-24 Edit Port Speed Limit

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.

TRIPP·LITE	Cu	urrent User:admin				Dog
🛃 System Home	VLAN Set	ttings Trunk Port Settings				
Quick Configuration	VLAN					
Port Management Basic Settings		VLAN ID	VLAN Name	VLAN IP	Port	Edit
Storm Control		1	DEFAULT	10.20.0.186	1-26	2
Flow Control	🔕 New VLA	N 🤤 Delete VLAN			First Previ	ous [1] Next Last1 / 1Page
Port Isolation						
Port Aggregation						

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".

TRIPPILITE	Current Use	radmin				🕑 Log Out
🛃 System Home	VLAN Settings	Trunk Port Setting	S			
SQUICK Configuration	VLAN					
Port Management Basic Settings		VLAN ID	New VLAN	Port	Edit	
Storm Control		1	VLAN ID(1~4094):	1		
Flow Control	O New VLAN 🤤 De	lete VLAN	VLAN name(1-31):	First Previo	ous [1] Next Last1	/ 1Page
Port Isolation			Select a port to add to the VLAN:			
Port Aggregation						
Port Mirroring						
Port Speed Limit			2 4 6 8 10 12 14 16 18 20 22 24 25 26			
 VLAN Management 			Optional port 🚍 Selected port î Aggregation port 💭 Trunk Port Select all Select all others Cancel			
VLAN Management						
Fault / Safety						
System Management						
PSE System Management						
			Save Exit			

Figure 6-2 Add New VLAN

RIPPILITE	Current	t User:admin				B
System Home	VLAN Setting	s Trunk Port Settings				
Quick Configuration	VLAN					
ort Management Basic Settings		VLAN ID	VLAN Name	VLAN IP	Port	Edit
Storm Control		1	DEFAULT	10.20.0.186	5-26	
low Control		2	DATA		1-4	📄 🗙
Port Isolation	🔘 New VLAN 🧯	Delete VLAN			First Previo	us [1] Next Last1 / 1Pa
Port Aggregation						
Port Mirroring						

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.

6.1.3 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.

System Home	VLAN Settings	Trunk Port Settings				
S Quick Configuration	VLAN					
Port Management Basic Settings		VLAN ID	VLAN Name	VLAN IP	Port	Edit
Storm Control		1	DEFAULT	10.20.0.186	5-26	2
Flow Control		2		-	1-4	2 ×
Port Isolation	New VLAN	Delete VLAN	Are you sure you want to delete the VLAN?		First Previo	ous [1] Next Last1 / 1Pag
		Delete VLAN	Are you sure you want to delete the VLAN?		First Previo	ous [1] Next Last1 / 1Pag
Port Isolation		Delete VLAN	Are you sure you want to delete the VLAN?		First Previo	ous [1] Next Lasti /1Pag
Port Isolation Port Aggregation		Delete VLAN	Are you sure you want to delete the VLAN?		First Previo	bus [1] Next Last1 / 1Pag
 Port Isolation Port Aggregation Port Mirroring Port Speed Limit 		Delete VLAN			First Previc	ous (1) Next Lasti / 1Pag
Port Isolation Port Aggregation Port Mirroring Port Speed Limit VLAN Management		Delete VLAN			First Previc	bus [1] Next Lasti / 1Pag
 Port Isolation Port Aggregation Port Mirroring 		Delete VLAN			First Previo	ous [1] Next Last1 / 1Pag

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).

System Home	VLAN Settings	Trunk Port Settings				
Quick Configuration	VLAN					
Port Management Basic Settings		VLAN ID	VLAN Name	VLAN IP	Port	Edit
Storm Control		1	DEFAULT	10.20.0.186	7-26	
Flow Control	V	2			1-2	2 X
Port Isolation		3	Are you sure you want to delete the VLAN?		3-6	🛛 🗶 🗙
Port Aggregation	🔾 New VLAN 🥥 De	lete VLAN			First Previo	us [1] Next Last1 / 1Pa
Port Mirroring Port Speed Limit			OK Cancel			
/LAN Management						
VLAN Management						

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".

TRIPPILITE	Current User	cadmin			Log Ou
System Home	VLAN Settings	Trunk Port Settings			
Port Management	VLAN	VLAN ID	VII AN Namo	Dest	Edit
Basic Settings		Edi	t VLAN	×	
Storm Control		1	VLAN ID(1~4094): 2		2
Flow Control		2	VLAN name(1-31): DATA		2 🗙
Port Isolation		3	Select the ports to modify the VLAN:		2 X
Port Aggregation Port Mirroring Port Speed Limit	O New VLAN O Del	lete VLAN	1 3 5 7 9 11 12 15 17 19 21 23 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	First Previou	ıs [1] Next Lasti /1Page
 VLAN Management VLAN Management 		Σ	Optional port 🚔 Selected port 🏦 Apgregation port 🎦 Trunk Port Select all Select all others Cancel		
 Fault / Safety System Management PSE System Management 					
			Seve Ext		

Figure 6-6 Add Ports to a VLAN

2. To remove ports from a VLAN

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

System Home	VLAN Setting	s Trunk Port Settings				
Quick Configuration	VLAN					
Port Management	10	VLAN ID	VII All Namo	MLAN ID	Port	Edit
Basic Settings			dit VLAN		×	
Storm Control		1	VLAN ID(1~4094): 2			2
Flow Control		2	VLAN name(1-31): DATA			📝 🗙
Port Isolation		3	Select the ports to modify the VLAN:			2 ×
Port Aggregation	O New VLAN	Delete VLAN			First Previou	s [1] Next Last1 / 1Pag
Port Mirroring						
Port Speed Limit			2 4 6 8 10 12 14 16 18 20 22 24 25 26			
VLAN Management			Coptional port Collected port CAggregation port C. Trunk Port	t Select all Select all others Cancel		
VLAN Management						
Fault / Safety						
System Management						

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.

TRIPPILITE	Curr	rent User:admin			E Log Out
🛃 System Home	VLAN Settin	ngs Trunk Port Settings			
S Quick Configuration	Description: If a	port is allowed to send messages through	ugh multiple VLANs, the port should be set as a trunk.		
Basic Settings	Trunk Port List				
Storm Control		Port	Native VLAN	Allowed VLAN	Edit
Flow Control		1	1	1	2 ×
Port Isolation		2	1	1	2 🗙
Port Aggregation Port Mirroring	O New Trunk F	Port List 🤤 Delete Trunk Port		First	Previous [1] Next Last1
Port Speed Limit					

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".

TRIPP·LITE	Curre	nt User:admin		🕑 Log Out
🛃 System Home	VLAN Setting	rrunk Port Settings		
Source Configuration	Departmention: If a pr	at is allowed to send messages throug	n multiple VLANs, the port should be set as a trunk.	
Port Management		ni is anowed to send messages unoug	n moliple volves, are por should be set as a runn.	
Basic Settings	Trunk Port List		New Trunk Port List	×
Storm Control		Port	Select a port to add to the TRUNK:	Edit
Flow Control		1	1 3 5 7 9 11 13 15 17 19 21 23	2 X
Port Isolation		2		× (
Port Aggregation		rt List 🤤 Delete Trunk Port		First Previous [1] Next Last1
Port Mirroring	U HOW HUNK PO		Coptional port Reserved port Aggregation port Crunk Port Select all Select all others Cancel	First Previous [1] Next Casti
Port Speed Limit				
 VLAN Management 			Native VLAN(1-4094): 1	
VLAN Management			Allowed VLAN(eg 3-5,8,10): 1	
Fault / Safety				
 System Management 				
System Settings				
System Upgrade			Save Exit	
System Information				
Configuration Management				

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.

6.1.7 Delete a Trunk Port

1. Delete a single Trunk port

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

	1.12								
System Home	VLAN Settin	ngs Trunk Port Settin	gs						
Quick Configuration	Description: If a	nort is allowed to send messages	through multiple VLANs, the port should be set as a trunk.						
ort Management									
Basic Settings	Trunk Port List	t							
Storm Control		Port	Native VLAN	Allowed VLAN	Edit				
Flow Control		1	1	1					
Port Isolation		2	1	1	2				
		2 1 1 Q New Trunk Port List Delete Trunk Port First Previous [1] Next La							

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.

TRIPP·LITE	Curr	ent User:admin			🕑 Log Out
System Home	VLAN Settin	ngs Trunk Port Sett	ings		
Quick Configuration Port Management	Description: If a	port is allowed to send message	es through multiple VLANs, the port should be set as a trunk.		
Basic Settings	Trunk Port List				
Storm Control	✓	Port	Native VLAN	Allowed VLAN	Edit
Flow Control		1	1	1	🖉 🗙
Port Isolation		2	1	1	2 ×
Port Aggregation Port Mirroring	O New Trunk F	Port List 🤤 Delete Trunk Port		Fi	st Previous [1] Next Last1
Port Speed Limit					
VLAN Management VLAN Management Fault / Safety					

Figure 6-11 Delete Multiple Trunk Ports

7.1 Attack Prevention

7.1.1 ARP Spoofing

7.1.1.1 View ARP Spoofing Configuration

Select "Fault/Safety \rightarrow Attack Prevention \rightarrow 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.

TRIPPILITE	Current Useradmin					Log Out
🛃 System Home	ARP Spoofing Port Security	DHCP Snooping				
S Quick Configuration	ARP Spoofing					
 Port Management 	Description: To protect network resources, the ARP Sp	poofing function will block illegal ARP mes	saces and prevent ARP flood at	acks.		
 Basic Settings 	ARP Spoofing: This feature can be used to protect equ					
 Storm Control 						
Flow Control	Select a port to configure:					
Port Isolation		1 23				
Port Aggregation						
Port Mirroring	2 4 6 8 10 12 14 16 18 20 2	2 24 25 26				
Port Speed Limit	Optional port 🚍 Fixed port 🚍 Selected port 🕤	Aggregation port Select all Select all	others Cancel			
▼ VLAN Management	Save Cancel Refresh					
 VLAN Management 						
 Fault / Safety 	State of the ARP table			-		
Attack Prevention	VLAN ID	IP	MAC	Port	Status	Edit
Path Detection					First Prev	ious [1] Next Last1

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.

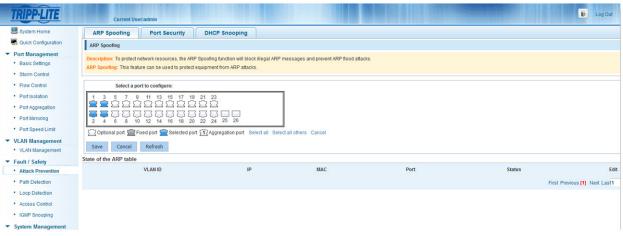


Figure 7-2 ARP Spoofing Configuration

7 Fault/Safety

		rces, the ARP Spoofing function will block illegal ARP message ed to protect equipment from ARP attacks.	s and prevent ARP flood attacks.			
t / Safety						
tack Prevention	Select a port to configure	·e:				
ath Detection	1 3 5 7 9 11 13 1	15 17 19 21 23				
op Detection	22222222					
cess Control		16 18 20 22 24 25 26				
MP Snooping						
em Management	Optional port Pixed port	Selected port 1 Aggregation port Select all Select all othe	rs Cancel			
System Management	Save Cancel Refresh					
o joten management	State of the ARP Table					
	VLAN ID	IP	MAC	Port	Status	Edit
	1	10.30.125.104	0006.6724.810E	4	VALIDATED	×
	1	10.10.0.62	0006.6723.DD32	4	VALIDATED	×
	1	10.28.99.43	0006.6724.832A	4	VALIDATED	×
	1	10.28.99.42	0006.6724.80E7	4	VALIDATED	×
	1	10.22.0.72	0006.6724.F515	4	VALIDATED	×
	1					
	1	10.22.0.73	100D.7FBA.3026	4	VALIDATED	×
		10.22.0.73	100D.7FBA.3026 0006.6726.E151	4	VALIDATED	×
	1					

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.

RIPP·LITE	Current User;admin					🚯 Log Ou
System Home	ARP Spoofing Port Security	DHCP Snooping				
Quick Configuration	ARP Spoofing					
Port Management Basic Settings Storm Control	Description: To protect network resources, the ARP Sp ARP Spoofing: This feature can be used to protect equ		messages and prevent ARP flood a	ttacks.		
Flow Control	Select a port to configure:					
Port Isolation Port Aggregation Port Mirroring	1 3 5 7 9 11 13 15 17 19 2					
Port Speed Limit	Optional port 💼 Fixed port 💼 Selected port 🖓	Aggregation port Select all Select	ect all others Cancel			
LAN Management VLAN Management	Save Cancel Refresh					
Fault / Safety	State of the ARP table					
Attack Prevention	VLAN ID	IP	MAC	Port	Status	
Path Detection					First	Previous [1] Next La:

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 💥 icon.

VLAN ID	IP	MAC	Port	Status	Edit
1	10.30.125.104	0006.6724.810E	4	VALIDATED	×
1	10.10.0.62	0006.6723.DD32	4	VALIDATED	×
1	10.28.99.43	0006.6724.832A	4	VALIDATED	×
1	10.28.99.42	0006.6724.80E7	4	VALIDATED	×
1	10.22.0.72	0006.6724.F515	4	VALIDATED	×
1	10.22.0.73	100D.7FBA.3026	4	VALIDATED	×
1	10.18.0.93	0006.6726.E151	4	VALIDATED	×
1	10.31.125.101	0006.6724.39FB	4	VALIDATED	×
1	192.168.0.120	D4AE.52D4.1645	4	ATTACK	×

Figure 7-5 Delete Misjudged ARP

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

7.1.2 Port Security

7.1.2.1 Port Security Configuration

Select "Fault/Safety \rightarrow Attack Prevention \rightarrow 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.

TRIPP·LITE	Current Useradmin
🛃 System Home	ARP Spoofing Port Security DHCP Snooping
Source Configuration	PortSecurity
▼ Port Management	
 Basic Settings 	Description: Enabling port security allows the switch to learn legitimate MAC addresses from a known source. To manually configure a port, you must select and save the ports you would like to configure.
Storm Control	Notice: The system uses port security configuration for traffic validation and to improve system security.
Flow Control	Select a port to configure:
Port Isolation	
Port Aggregation	
Port Mirroring	2 4 6 8 10 12 14 16 18 20 22 24 25 26
Port Speed Limit	🖸 Optional port 🚔 Fixed port 🚔 Selected port 🔃 Appregation port Select all Select all Others Cancel
▼ VLAN Management	Save Refresh Manual
VLAN Management	
▼ Fault / Safety	
Attack Prevention	
Path Detection	
Loop Detection	

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.

TRIPP·LITE	Current Useradmin
🛃 System Home	ARP Spoofing Port Security DHCP Snooping
Quick Configuration	Port Security
Port Management	Manually set the port security
Basic Settings	Notice: Select the port number to configure when setting port security. IP address and MAC address.
Storm Control	Binding mode: Join Visitors VIP Address: MAC Address: Port: Not Selected Description:
Flow Control	Access Time: Range 6-1440 min) Rolls Binleton Gi Off
Port Isolation	Apply Cancel Gird
Port Aggregation	
Port Mirroring	
Port Speed Limit	
VLAN Management	
 VLAN Management 	
Fault / Safety	
Attack Prevention	
Path Detection	
Loop Detection	
Access Control	
IGMP Snooping	
	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.

🐯 System Home	ARP Spoofing Port Security DHCP Snooping
S Quick Configuration	Port Security
 Port Management 	Manually set the port security
 Basic Settings 	Notice: Select the port number to configure when setting port security. IP address and MAC address.
Storm Control	Binding mode: Add Bind - IP Address: MAC Address: Port. Not Selected - Description:
Flow Control	Not Selected
Port Isolation	Apply Lancel Gi01 Gi03
Port Aggregation	
Port Mirroring	
Port Speed Limit	
 VLAN Management 	
VLAN Management	
 Fault / Safety 	
Attack Prevention	
Path Detection	

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 Last1 /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					

Figure 7-10 Cancel Port Security Configuration

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.

TRIPPILITE	Current Useradmin	Log Out
📑 System Home	ARP Spoofing Port Security DHCP Snooping	
S Quick Configuration	DHCP Smooping	
 Port Management Basic Settings 	Description: DHCP snooping will filter untrusted DHCP messages.	
Storm Control	ON After enabling DHCP snooping, you can select trusted ports.	
Flow Control		
Port Isolation	Select a port to configure:	
Port Aggregation	1 3 5 7 9 11 13 15 17 19 21 23	
Port Mirroring		
Port Speed Limit	2 4 6 8 10 12 14 16 18 20 22 24 25 26	
▼ VLAN Management	💭 Optional port 🚍 Fixed port 🚍 Selected port 😭 Aggregation port Select all Select all others Cancel	
VLAN Management		
▼ Fault / Safety		
Attack Prevention	Save Refresh	
Path Detection	Trust port	Edit
Loop Detection		First Previous [1] Next Last1
Assess Control		

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.

TRIPP·LITE	Current Useradmin
🛃 System Home	ARP Spoofing Port Security DHCP Snooping
Quick Configuration	DRCP Snooping
Port Management	Description: DHCP snooping will filter untrusted DHCP messages.
VLAN Management Fault / Safety Attack Prevention	OFF After enabling DHCP snooping, you can select trusted ports.
Path Detection	



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.

TRIPP·LITE	Current Useradmin	Log Out
🛃 System Home	ARP Spoofing Port Security DHCP Snooping	
SQuick Configuration	DHCP Snooping	
 Port Management Basic Settings 	Description: DHCP snooping will filter untrusted DHCP messages.	
Storm Control Flow Control	ON After enabling DHCP snooping, you can select trusted ports.	
Port Isolation	Select a port to configure:	
Port Aggregation Port Mirroring Port Speed Limit	1 3 5 7 9 11 13 15 17 19 21 23 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	
 VLAN Management VLAN Management 	💭 Optional port 💼 Fixed port 💼 Selected port 🕥 Aggregation port. Select all Select all Others Cancel	
Fault / Safety Attack Prevention	Save Refresh	
Path Detection	Trust port	Edit
Loop Detection	12	×
Access Control IGMP Snooping	First Prev	vious [1] Next Last1
	Figure 7-13 Steps to Activate DHCP Snooping	
	Trust port	Edit
	1-2	×
	First Previou:	s [1] Next Last1

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.

TRIPP·LITE	Current Useradmin	Dog Out
🛃 System Home	ARP Spoofing Port Security DHCP Snooping	
S Quick Configuration	DRCP Snopping	
 Port Management Basic Settings 	Description: DHCP snooping will filter untrusted DHCP messages.	
Storm Control	ON After enabling DHCP snooping, you can select trusted ports.	
Flow Control		
Port Isolation	Select a port to configure:	
Port Aggregation Port Mirroring Port Speed Limit VLAN Management	1 3 5 7 0 1 11 13 15 17 10 21 22 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	
VLAN Management	Optional port 🗮 Fixed port 🛣 Selected port î Apgregation port Select all Others Cancel	
Fault / Safety Attack Prevention	Save Rafreah	
Path Detection	Trust port	Edit
Loop Detection	1.2	×
Access Control	First Prev	ious [1] Next Last1
IGMP Snooping		

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.

TRIPPLITE	Current Use	r:admin					Log Out		
🛃 System Home	ARP Spoofing	Port Security	DHCP Snooping						
Cuick Configuration	DHCP Snooping								
 Port Management Basic Settings 	Description: DHCP snooping will filter untrusted DHCP messages.								
Storm Control	ON After en	abling DHCP snooping, y	ou can select trusted ports.						
Flow Control									
Port Isolation	Select a po	rt to configure:		Are you sure you want to disable DHCP Snooping?					
Port Aggregation Port Mirroring Port Speed Limit VLAN Management				OK Cancel					
VLAN Management Fault / Safety Attack Prevention	Save Refresh								
Path Detection				Trust port			Edit		
Loop Detection				1-2			×		
Access Control						First Previo	us [1] Next Last1		
IGMP Snooping									

Figure 7-16 Disable DHCP Snooping

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.

TRIPPILITE	Current Useradmin
🛃 System Home	Path Detection
SQuick Configuration	Description: Use the ping function to determine whether the network connection is functional and whether the host is reachable.
 Port Management 	Description. Use the ping function to determine whether the network connection is functional and whether the network connection is an control to the network connection in the network connection is an and whether the network connection is an an and whether the network connection is an and whether the network connection is an an and whether the network connection is an an an and whether the network connection is an an an and whether the network connection is an
Basic Settings	Destination IP •
Storm Control	Start Test
Flow Control	Test Results
Port Isolation	
Port Aggregation	
Port Mirroring	
Port Speed Limit	
▼ VLAN Management	
VLAN Management	
▼ Fault / Safety	
Attack Prevention	
Path Detection	
Loop Detection	

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.

TRIPPILITE	Current User:admin			🚯 Log Out						
📕 System Home	Loop Detection									
Quick Configuration Port Management Basic Settings	Description: 1. Use loop detection to avoid broadcast storm problems caused by loops. It is best to use loop detection on all switch ports. 2. There are two different loop detection modes, 'alarm' and 'disconnect'. Vlarm' will alert you of a loop but will keep the port connected, 'disconnect' will turn the link to the port off until the loop is eliminated. 3. After the loop is eliminated, wait for the automatic recovery to complete.									
Storm Control Flow Control	ON Enable or disable loop detection, after enabling the feature, settings can be customized for each port.									
Port Isolation Port Aggregation	Select a port to configure:									
Port Aggregation Port Mirroring										
Port Speed Limit										
 VLAN Management VLAN Management 	L	2 4 6 10 12 14 16 10 22 24 25 2 0 5 10 12 14 16 10 22 24 25 2 0 5 10 14 16 10 22 24 25 2 0 5 10 14 16 10 22 24 25 2 0 5 5 10 14 16 10 22 24 25 2 0 5 5 10 14 16 10 22 24 25 2 0 5								
▼ Fault / Safety										
Attack Prevention		connect -								
Path Detection	Detection Time Interval (2 to 15 se Automatic Recovery time (30,864	econds, the default 3 seconds) : 3 00 seconds, the default 60 seconds): 60 Save								
Loop Detection		Sure Sure								
Access Control	Loop detection list									
IGMP Snooping	Port	Control mode	Status	Edit						
 System Management 	1	Disconnect	Not connected							
 System Settings System Upgrade 	2	Disconnect	Not connected	2						

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.

TRIPP·LITE	Current Useradmin
🐯 System Home	Loop Detection
R Quick Configuration	Description: 1. Use loop detection to avoid broadcast storm problems caused by loops. It is best to use loop detection on all switch ports.
 Port Management Basic Settings 	2. There are two different loop detection modes, 'alarm' and 'disconnect'. 'Alarm' will alert you of a loop but will keep the port connected, 'disconnect' will turn the link to the port off until the loop is eliminated. 3. After the loop is eliminated, wait for the automatic recovery to complete.
Storm Control Flow Control	CN Enable or disable loop detection, after enabling the feature, settings can be customized for each port.



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".

TRIPP·LITE	Current User:admin			Log Out						
📑 System Home	Loop Detection									
K Quick Configuration	Description: 1 Lice loop detection									
▼ Port Management		Description: 1. Use loop detection to avoid broadcast atom problems caused by loops. It is best to use loop detection on all swinch ports. 2. There are two different loop detection modes, "alarn and "disconcert" dam will aller to use a loop but will keep the port connected, "disconcert will turn the link to the port off until the loop is eliminated.								
Basic Settings	3. After the loop is eliminated, wai	t for the automatic recovery to complete.								
Storm Control										
Flow Control	ON Enable or disable	e loop detection, after enabling the feature, settings can be customized for each port.								
Port Isolation	Salact a port to cor	Nouro:								
Port Aggregation	[[Select a port to configure:								
Port Mirroring		1 3 5 7 9 11 13 15 17 19 21 23 合わらうちっちっちっちっちっちっちっちっち								
Port Speed Limit	8888888									
▼ VLAN Management		2 4 6 8 10 12 14 16 18 20 22 24 25 26								
 VLAN Management 	Optional port 🚍 Fixed port	🖸 Optional port 💼 Fixed port 💼 Selected port î Aggregation port Select all Others Cancel								
▼ Fault / Safety										
Attack Prevention		sconnect								
Path Detection		sconnect 3 seconds): 3 Im Seconds, ine default 60 seconds): 60 Save								
Loop Detection	Automatic Recovery Time (30-8	Save Save								
Access Control	Loop Detection List									
IGMP Snooping	Port	Control mode	Status	Edit						
▼ System Management	1	Disconnect	Not connected							
 System Settings System Upgrade 	2	Disconnect	Normal							
oyotoni opyrade	2	Disconnect	Not connected							

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.

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 1 1 1 1 1 1 1 1 1 23 1	
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); 50 Save	

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.



Figure 7-22 Automatic Recovery Time Configuration

7.3.6 Disable Loop Detection

Click the "ON/OFF" button to disable loop detection.

TRIPPILITE	Current User:admin			Dog Out					
🛃 System Home	Loop Detection								
Quick Configuration Port Management Basic Settings	Description: 1. Use loop detection to avoid broadcast storm problems caused by loops. It is best to use loop detection on all switch ports. 2. There are two different loop detection modes, 'alarm' and 'disconned'. Vlarm' will alert you of a loop but will keep the port connected, 'disconned' will turn the link to the port of until the loop is eliminated. 3. After the loop is eliminated, wait for the automatic recovery to complete.								
Storm Control Flow Control	ON Enable or disable	e loop detection, after enabling the feature, settions can be customized for each not-							
Port Isolation Port Aggregation	Select a port to cor	nfigure: Are you sure you want to turn off Loop	Detection ?						
Port Mirroring Port Speed Limit									
VLAN Management VLAN Management		14 16 18 20 22 24 25 26							
Fault / Safety Attack Prevention Path Detection Loop Detection	Detection Time Interval (2 to 15	sconned • seconds, the default 3 seconds): 3 6400 seconds, the default 60 seconds): 50 Save							
Access Control	Loop Detection List								
IGMP Snooping	Port	Control mode	Status	Edit					
System Management	1	Disconnect	Not connected						
System Settings System Upgrade	2	Disconnect	Normai						
System Information	3	Disconnect	Not connected						
Configuration Management	4	Disconnect	Not connected	2					
SNMP		Discoursed	Midlanaradiad						

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.

TRIPPILITE	Currer	ıt User:admin								Log Out
🛃 System Home	ACL	oply ACL								
Quick Configuration Port Management Basic Settings Storm Control	Notice: The ACL ru	le priority will follow	the order of the list (i.	e., 1 is first, 2 is second, etc.). C	pecific resources while blockin reating many rules can cause (at the equivalent bit must match	perational delays.				
Flow Control	Displaying ACL Co	onfiguration		•						
Port Isolation Port Aggregation	No.	Action	Protocol	Source IP/MAC	Source Wildcard	Source Port	Destination IP / MAC	Destination Wildcard	Destination Port	Edit
Port Mirroring										
Port Speed Limit VLAN Management										
VLAN Management										
▼ Fault / Safety										
Attack Prevention										
Path Detection										
Loop Detection										
Access Control										
IGMP Snooping										
 System Management 	Delete									

Figure 7-24 Access Control List Settings

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.

TRIPPILITE	Current User:admin		🕑 Log Ou
System Home Auck Configuration Ouck Configuration VatA Management VLAN Management Attack Prevention Path Detection Loop Detection GACess Control GACess Control System Management PSE System Management	ACL Apply ACL Description: Access control lists (ACLs) ensure that only as Notice: Notice: The ACL, rule priority will follow the order of the list (Wildcard: Wildcard: A wild card mask is a matching rule. The rule for investment of the action of the	Select Configuration standard IP ACL ▼ Type: Let ID: Standard IP ACL 0 ▼ ACE ID: ACE 0 ▼ Rules: Permit ▼ IP Address: @Any source IP address Ospecify the IP address range: IP Address: Wildcards (optional):	a details, see the manual.
		Save	

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.

TRIPPILITE	Current Us	er:admin						E	Log Out
System Home	ACL Appl	Y ACL							
R Quick Configuration	Description: Access of	ontrol lists (ACI	s) ensure that only auth	New ACL Rules		×			
Port Management			w the order of the list (i.e						
VLAN Management	Wildcard: A wild card	mask is a matcl	hing rule. The rule for a v	Select		e details, see	the manual.		
	New ACL Rules			Configuration Type:	Configuration Expand IP ACL				
Attack Prevention	Displaying ACL Cont	figuration							
Path Detection				List ID:	Expand IP ACL 10 V				
Loop Detection	No.	Action	Protocol	ACE ID:	ACE 0	on Wildcard	Destination Port	Edit	
Access Control				Rules:	Permit V				
IGMP Snooping									
System Management				Protocol:	IGMP V				
PSE System Management				Source IP Address:	Any source IP address				
					Ospecify the IP address range:				
				Destination IP	(0.0.0) Wildcard: (optional)(0.0	.0.0)			
				Address:	Any destination IP address				
					Ospecify the IP address range:				
					(0.0.0) Wildcard: (optional)(0.0	.0.0)			
				0					
	Delete			Save					

Figure 7-26 Expand IP ACL Configuration

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.

TRIPPILITE	Current User:admin		🕑 Log Ou
System Home	ACL Apply ACL		
Quick Configuration Port Management VLAN Management Fault / Safety Attack Prevention	Description: Access control lists (ACLs) ensure that only author Notice: The ACL rule priority will follow the order of the list (i.e., Wildcard: A wild card mask is a matching rule. The rule for a will New ACL Rules Displaying ACL Configuration		ktals, see the manual.
Path Detection Loop Detection Access Control IGMP Snooping System Management PSE System Management	No. Action Protocol	List ID: Expand MAC ACL 20 ACE ID: ACE 0 Rules: Permit Source MAC Address: OSpecify the MAC address range:	WildCard Destination Port Edit
		Destination MAC @Any destination MAC address Address: Specify the MAC address range: MAC Protocol Type: Save	

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 *inclusion* to visit the ACL rules modification page. Change Rules to "Permit".

TRIPPILITE	Curre	ent User:admin								b Log Out
System Home	ACL	Apply ACL								
Quick Configuration	Description: Ac	cess control lists (Al	CLs) ensur Me	odify the ACL rules		×	work resources.			
Port Management	Notice: The ACL	L rule priority will foll	ow the ord							
VLAN Management	Wildcard: A wild	d card mask is a mat	ching rule.	Select		n	atter. For more details, see t	ne manual.		
	New ACL Rule	es		Configuration	Configuration Expand MAC ACL 🗸					
Attack Prevention Path Detection	Displaying ACL	. Configuration	Expand I	Type:						
Loop Detection	No.	Action	Pro	List ID: ACE ID:	Expand MAC ACL 20		Destination Wildcard	Destination Port	Edit	
Access Control	0	permit							2 🗙	
IGMP Snooping				Rules: Source MAC	Permit V					
System Management				Address:	Any source MAC address					
PSE System Management					Ospecify the MAC address range:					
				Destination MAC Address:	Any destination MAC address					
					Ospecify the MAC address range:					
				MAC Protocol Type:	(<0x0000-0xfff>)(optional)					
	Delete		-	Save						

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.

7.4.1.4 Delete ACL Rules

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

TRIPPILITE	Curren	nt User:admin							▶ Log Out
🛃 System Home	ACL	Apply ACL							
S Quick Configuration	Description: Acc			odify the ACL rules		twork resources.			
Port Management	Notice: The ACL								
VLAN Management	Wildcard: A wild		itching rule.	Select		natter. For more details, see t	he manual.		
✓ Fault / Safety	New ACL Rule	IS		Configuration Type:	Configuration Expand MAC ACL 🗸				
Attack Prevention	Displaying ACL	Configuration	Expand I	.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,					
Path Detection	No.	Action	Pro	List ID:	Expand MAC ACL 20 V	Destination Wildcard	Destination Port	Edit	
Loop Detection	NO.	Action	PIO	ACE ID:	ACE 0	Desunation windcard	Desunation Port		
Access Control	0	permit						2 X	
IGMP Snooping				Rules:	Deny 💌				
System Management				Source MAC Address:	Any source MAC address				
PSE System Management					Ospecify the MAC address range:				
				Destination MAC Address:	Any destination MAC address				
					Ospecify the MAC address range:				
				MAC Protocol Type:	(<0x0000-0xfff>)(optional)				
	Delete			Save					

Figure 7-29 Delete ACL Rules

To delete all the ACL Rules, click the X icon then click "OK" to confirm the deletion.

TRIPPILITE	Cum	ent User:admin									Log Out
System Home Cuick Configuration Port Management VLAN Management Fault / Safety	Notice: The AC	L rule priority will fol d card mask is a ma	llow the order of the list (i.e., 1 is first, 2 is second, e	s to specific resources while l kc.). Creating many rules can is that the equivalent bit must	cause operational dela	ays.		ne manual.		
Attack Prevention Path Detection Loop Detection Access Control	Displaying AC No.	L Configuration Action	Expand MAC ACL20 Protocol	Source IP/MAC	Source Wildcard	Source Port	Destination IP / MAC	Destination Wildcard	Destination Port	Edit	
IGMP Snooping System Management PSE System Management					om webpage Are you sure you want to rer OK	nove the ACL rule?				2.0	
	Delete										~

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.

TRIPP·LITE	Current User:admin		E Log C
🛃 System Home	ACL Apply ACL		
Quick Configuration Port Management VLAN Management	Description: The lable below shows the ACLs that are applied to the switch ports. Notice: ACLs cannot be applied to ports on the panel that are gray.		
Fault / Safety	ACL Rules Application		
Attack Prevention Path Detection	Please select the ACL list: Expand MAC ACL20		
Loop Detection	Select a port to configure:		
Access Control IGMP Snooping System Management	1 3 5 7 8 11 13 15 17 19 21 23 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		
 PSE System Management 	Coptional port Prived port Selected port Maggregation port Select all Select all others Cancel		
	ACL		
	ACL	Port	Edit
	Expand MAC ACL20	5	×
		First Previo	ous [1] Next Last1 / 1Page

Figure 7-31 View Applied ACL Rules

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.

TRIPPILITE	Current Useradmin		🕑 Log Out
System Home Cuck Configuration Port Management VLAN Management VLAN Management VLAN Management Value / Safety Adack Prevention Path Detection Loop Detection Cucces Control Cuck Panoping System Management PSE System Management	ACL Apply ACL Description: The table below shows the ACLs that are applied to the switch ports. Notice: ACLS canced be applied to ports on the panel that are gray. ACL Rules Application Please select the ACL list: Expand MAC ACL20 Select a port to configure: 1 3 5 2 4 6 3 10 12 2 4 6 Select aport on Configure:		
	ACL	Port	Edit
	Expand MAC ACL20	5	×
		First Previo	us [1] Next Last1 / 1Page

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.

TRIPPILITE	Current Useradmin		Deg Out
System Home	ACL Apply ACL		
Cuick Configuration Port Management VLAN Management VLAN Management Atlack Prevention Atlack Prevention Loop Detection Access Control IGMP Snooping System Management PES System Management	Description: The table below shows the ACLs that are applied to the switch ports. Motice: ACLS cannot be applied to ports on the panel that are gray. ACL Rules Application		
	Please select the ACL list: Expand MAC ACL20 Select a port to configure: Are you sure you want to remove the ACL rule? 1 3 5 7 9 11 13 15 17 19 21 23 1 2 2 2 2 0K Cancel		
	2 4 6 8 10 12 14 16 18 20 22 24 25 26		
	Save		
	ACL		
	ACL	Port	Edit
	Expand MAC ACL20	5	×
		First P	revious [1] Next Last1 / 1Page

Figure 7-33 Delete an ACL Rule

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.

TRIPPILITE	Current Useradmin								
🛃 System Home	IGMP Snooping								
 Quick Configuration Port Management VLAN Management 	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, frequired, 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.								
Fault / Safety Attack Prevention Path Detection	ON Enable or disable the multicast listener, when enabled, the static routing port can be set.								
Loop Detection	K0MP Version Selection								
Access Control IGMP Snooping	IGMP Version IGMP_V2 •								
System Management	Save								
System Management PSE System Management	Multicast Routing Port Settings								
	Select a port to configure:								
	1 3 5 7 9 11 13 15 17 19 21 23 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □								
	VLAN vian 1 IP Add Routing Port								
	VLAN Port IP Status Edit								
	real remove full real cases. In the								

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.

TRIPP·LITE	Current User:admin
🖲 System Home	IGMP Snooping
Quick Configuration Port Management VLAN Management	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.
Fault / Safety Attack Prevention	ON DEnable or disable the multicast listener, when enabled, the static routing port can be set.
Path Detection	KMP Version Selection
Loop Detection Access Control IGMP Snooping	KGMP Version TGMP_V2
 System Management PSE System Management 	Multicast Routing Port Settings
	Select a port to configure: 1 3 5 7 9 11 13 15 17 19 21 23 1 1 1 1 15 17 19 21 23 1 1 1 1 10 12 12 1 16 18 20 22 24 25 26 1 Optional port IP IP <t< th=""></t<>
	VLAN Port IP Status Edit
	First Previous (1) Next Lasti / 1Page

Figure 7-35 Activate the IGMP Snooping Function

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

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.

TRIPPILITE	Current Useradmin
🛃 System Home	IGMP Snooping
Source Configuration	Description: Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.
Port Management	Description: Internet storage managements in storage of the state storage as a smitch to bread on the state and state storage as a smitch to bread as a smit
VLAN Management	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.
▼ Fault / Safety	
Attack Prevention	OFF Dable or disable the multicast listener, when enabled, the static routing port can be set.
Path Detection	
Loop Detection	

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.

Multicast Routing Port Settings				
Select a port to configure:				
1 3 5 7 9 11 13 15 17 19 21 23 2 1				
Add Routing Port				
VLAN	Port	IP	Status	Edit
				First Previous [1] Next Last / 1Page

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.

TRIPP·LITE	Current Useradmin	Î						
🛃 System Home	IGMP Snooping							
Quick Configuration Port Management Basic Settings	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.							
Storm Control Flow Control	ON Enable or disable the multicast listener, when enabled, the static routing port can be set.							
Port Isolation	IGMP Version Selection							
Port Aggregation Port Mirroring Port Speed Limit	IGMP Version IGMP_V2 GMP_V1 GMP_V2 Save							
VLAN Management VLAN Management	Multicast Routing Port Settings							
Fault / Safety Attack Prevention Path Detection Loop Detection Access Control IGMP Snooping System Management	1 3 5 7 9 11 13 15 17 19 21 22 1 2 5 7 10 11 15 12 12 12 12 12 12 12 12 12 12 12 12 12 12 14 16 18 20 22 24 25 26 1 Optional port Image: Fixed port Image: Aggregation port <td< td=""><td></td></td<>							
System SettingsSystem Upgrade	VLAN vian 1 • IP Add Routing Port							
System Information Configuration Management SNMP	VLAN Port IP Status Edit First Previous [1] Next Last / 1Page							

Figure 7-38 Set the IGMP Version

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.

🛃 System Home	VLAN Management	System Restart	Change Password	System Log	Log Export	ARP Table	MAC Managemen
-	VLAW Wanagement	System Residit	change rassword	System Log	Log Export	ARP Table	WAC wanayemen
Quick Configuration	Description: Management VL/	N parameters: IP, MAC, gate	eway and the user's contact det	ails. "*" denotes required	field.		
Port Management	The basic information of the						
 Basic Settings 	The basic mormation of the	system settings					
Storm Control	VLAN Manage	ment: vlan 1 🗸 🗸	*		MAC: 24	1:05:0f:68:02:32 *	
Flow Control	Manageme	ent IP: 192. 168. 1. 100	*		Device Name: St	ritch *	
Port Isolation	Subnet	Mask: 255. 255. 255. 0	*		Device Location:		
 Port Aggregation 	Default Gat	eway: 192. 168. 1. 1	*		Contact Name:		
Port Mirroring	Login Tin	neout: 5 ×		С	ontact Information:		
Port Speed Limit	Management	Port: 80				<u>.</u>	
	Save						
VLAN Management	Jave						
 VLAN Management 	System time synchronizatio	n					
Fault / Safety	Notice: The switch time can be	and the second solds the later	at time by antiting the time avera	environtion and use ID and d	and to the NTD serves (and the second second second second	
Attack Prevention	Tip: The system will select a de			Ironization server iP add	ress to the NTP server i	form your selected time	: 20ne.
Path Detection	Tip. The system will select a de	adul ume syncronization ser	ver il no in dudress is chitered.				
Loop Detection	The Current System	Time: February 16, 2016 17	1:05:08	NTP	Server IP Address: 2:	6. 229. 0. 179	

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.

8.1.1.2 Set Management IP Address

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

TRIPPILITE	Current Useradmin
🛃 System Home	VLAN Management System Restart Change Password System Log Log Export ARP Table MAC Management
Quick Configuration Port Management	Description: Management VLAN parameters: IP, MAC, gateway and the user's contact details.*** denotes required field.
 VLAN Management 	The basic information of the system settings
 Fault / Safety Attack Prevention 	VLAN Management: Vian 1 🗸 * MAC: [14:14:4b:7b:20:34] *
Attack Prevention Path Detection	Management IP: 10.20.0.186 Device Name: Switch
Loop Detection	Default Gateway: 10.0.0.1 Contact Name:
Access Control	Login Timeout: 30 Contact Information:
IGMP Snooping	Management Port: 80
 System Management 	Save
System Settings System Upgrade	System time synchronization

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.

ization server IP address to the NTP server from your selected time zone.
NTP Server IP Address: 216. 229. 0. 179
Daylight Saving Time: Enabled Disabled
Mode: repeating -
To: 03/10 13:54
12

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 \rightarrow System Settings \rightarrow System Restart" to reboot the switch.

TRIPPILITE	Current User:admin								₽ Log Out
📑 System Home	VLAN Management	System Restart	Change Password	System Log	Log Export	ARP Table	MAC Management		
R Quick Configuration	Description: To restart the swite	h, click on the 'restart the de	wice immediately button Please	do not close the brows	ar until the process is co	ompleted The brows	er will automatically refresh whe	n the restart is completed	
Port Management									
VLAN Management	Restart the device immediate	ly							
▼ Fault / Safety									
Attack Prevention									
Path Detection									
Loop Detection									
Access Control									
IGMP Snooping									

Figure 8-4 System Restart

- 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.

8.1.3 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)*.

TRIPPILITE	Current Useradmin	Log Ou
😸 System Home	VLAN Management System Restart Change Password System Log Log Export ARP Table MAC Management	
Real Quick Configuration	Modify the super user password	
Port Management	- Notice: After setting a new password, you must logout and login again. The password can only contain letters, numbers and underscores.	
VLAN Management		
▼ Fault / Safety	Old Password:	
Attack Prevention	New Password:	
Path Detection	Confirm New Password:	
Loop Detection	Save Cancel	

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".

TRIPPILITE	Current User.admin
🛃 System Home	VLAN Management System Restart Change Password System Log Log Export ARP Table MAC Management
R Quick Configuration	Modify the Super User Password
 Port Management Basic Settings 	- Notice: After setting a new password, you must logout and login again. The password can only contain letters, numbers and underscores.
Storm Control	Old Password: *
Flow Control	New Password: *
Port Isolation	Confirm New Password: *
Port Aggregation	Save Cancel
Port Mirroring	Modify Telnet Login Password
 Port Speed Limit VLAN Management Fault / Safety System Management 	New Password:
System Settings	

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.

🛃 System Home	VLAN Management System Restart Change Password System Log Log Export ARP Table MAC Management	
R Quick Configuration	Description: The system log displays system operating information.	
Port Management		
VLAN Management	System Log	
Fault / Safety Attack Prevention	Keyword: Clear	
Path Detection	SysLog function - enabled	
Loop Detection	Console logging : level debugging Monte logging : level debugging	
Access Control	Trap logging _ enable	
IGMP Snooping	Buffer logging : level user, max size 51200	
 System Management 	The Context of logging file:	
System Settings	Jan 1 00:00.03 1970: %%SYSTEM-5-INT: Start L2 module	
System Upgrade	Jan 100:00:031970: %%MMSTP-3-NIT. MSTP Init OKI Jan 100:00:041970: %%SYSTEM-5-NIT. Start Inearbeat server	
System Information	Jan 100:00:41970. %%SYSTEM-F-INT: Start lente server Jan 100:00:41970. %%SYSTEM-F-INT: Start lente server	
Configuration Management	Jan 10000041970 %%SYSTEM-SHNT Start smp server Jan 10000091970 %%SYSTEM-SHNT Start smp server	
SNMP	Jan 1 00:15:47 1970: %%LINEPROTO-3-UPDOWN: Line protocol on Gi 0/2, changed state to up	
System Diagnostics	Jan 1001548 1970: %MLNEPROTO-3-UPPOWN: Line protocol on Gi 04, changed state to up Jan 1001548 1970: %MLNEPROTO-3-UPPOWN: Line protocol on Gi 06, changed state to up	
PSE System Management	Jan 1001:54 9179: 5%MLNEPROTO-3-UPDOWN: Line protocol on GL08, changed state to up Jan 1001:55 0179: 5%MLNEPROTO-3-UPDOWN: Line protocol on GL08, changed state to up Jan 1001:55 0179: 5%MLNEPROTO-3-UPDOWN: Line protocol on GL05, changed state to up Jan 1001:55 1179: 5%MLNEPROTO-3-UPDOWN: Line protocol on GL07, changed state to up Jan 1001:55 1179: 5%MLNEPROTO-3-UPDOWN: Line protocol on GL07, changed state to up Jan 1001:55 1179: 5%MLNEPROTO-3-UPDOWN: Line protocol on GL07, changed state to up Jan 1001:55 1179: 5%MLNEPROTO-3-UPDOWN: Line protocol on GL07, changed state to up Jan 1001:55 1179: 5%MLNEPROTO-3-UPDOWN: Line protocol on GL07, changed state to up Jan 1001:55 1179: 5%MLNEPROTO-3-UPDOWN: Line protocol on GL07, changed state to up	

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.

Figure 8-7 System Log Management

• To clear the log information, click "Clear".

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.

TRIPP·LITE	Current Useradmin
🛃 System Home	VLAN Management System Restart Change Password System Log Export ARP Table MAC Management
SQUICK Configuration	Description: This is a logupted to an external TFTP server.
Port Management	
VLAN Management	Log Export
▼ Fault / Safety	TFTP Server (IP):
Attack Prevention	File Name:
Path Detection	Export
Loop Detection	
Access Control	
IGMP Snooping	
 System Management 	
System Settings	
System Upgrade	
System Information	

Figure 8-8 LOG Export

8.1.6 ARP Table

Select "System Management \rightarrow System Settings \rightarrow ARP Table" to visit the ARP Table configuration page. This view displays the ARP Table contents.

System Home	VLAN Management System Restart Change Pas	ssword System Log Log Export ARP Table MAC Management	
Quick Configuration	Description: The table below contains the ARP entries. To clear the table, click t	the 'Clear ARP Table Entries' Icon.	
ort Management 'LAN Management	ARP Table		
ault / Safety	IP	MAC	Vian ID
Attack Prevention	10.0.0.1	00:1b:17:00:0a:12	1
Path Detection	10.22.0.33	94:39:e5:2e:7e:7b	1
Access Control	Clear ARP Table Entries	First Prev	ous [1] Next Last1 / 1Page
IGMP Snooping			
ystem Management			

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.

Manageme	nt VLAN System Restart	change password	System Log	og Export ARP Table	MAC Management
rotection Sta	itus			L	
truction: Ena	ble the function of protection MAC att	ack,To prevent malicious attacks	take up a lot of MAC table, ensu	re the normal communication of network	
rotection Set	ttings				
atic MAC: In c	order to ensure the security of importa	nt data,recommended that put the	e server and the important equipn	nent's MAC added to the static MAC tabl	ie.
MAC list: all	Manual binding MA	AC			
	User MAC	Port	Port type	VLAN	Operation
	0025.5689.1345	1	dynamic	1	0-0
	C860.00E0.2BCC	1	dynamic	1	00
	4016.7EB3.4063	1	dynamic	1	00
	3883.45EE.7332	1	dynamic	1	00
	C860.00E0.2B80	1	dynamic	Ť.	00
	4016.7EB3.40B7	1	dynamic	1	00
	7427.EA36.DD67	1	dynamic	1	00
	0088.9987.8163	1	dynamic	Ť	00
	BCEE.7B9A.D132	1	dynamic	1	00
	DOLL. IDJA.D IJZ				

Figure 8-10 Query Results of MAC Address

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 **O** 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.

TRIPPILITE	Current User:a	dmin							Log Out
🛃 System Home	VLAN Management	t System Restar	t Change Password	System Log	og Export	ARP Table	MAC Management		
R Quick Configuration	Protection Settings								
 Port Management VLAN Management 	Static MAC: To enhance the	e safety of important data	Configure MAC Binding			dd			
▼ Fault / Safety	MAC list: All 👻	Configure MAC Bin	User MAC	• (ormat.0000.0000.0	0000)			
Attack Prevention Path Detection		User MAC	Select a port bind to the MAC					Edit	
Loop Detection		100D.7FC0.21FD		17 19 21 23 11 11 11 12 11 11 11 12				60	
Access Control		0006.6705.0697		3 18 20 22 24 25				60	
IGMP Snooping		D039.720E.AE0B	COptional port Pixed port		on port 5-7 Trunk	Port		00	
System Management System Settings		28C6.8E34.1CD3						00	
System Upgrade		0006.6722.F7D8						00	
System Information		D05F.B880.696B	Save Exit					00	
Configuration Management		0025.6497.2724	26		Dynamic		1	00	
SNMP System Diagnostics		2405.0F68.033F	26		Dynamic		1	00	
PSE System Management		000E.7FF0.6251	26		Dynamic		1	00	
		0006.6723.DD32	26		Dynamic		1	90	
	Opnamic MAC to Sta	tic MAC 🤤 Delete Static	MAC				First Previous	[1][2][3][4][5] Next Last1 /	13Page

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 O-O

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

System Home	VLAN Managem	ent System Restart	Change Password	System Log	Log Export	ARP Table	MAC Management				
Quick Configuration	Protection Settings	Protection Settings									
rt Management AN Management	Static MAC: To enhan	ce the safety of important data, add the	e MAC addresses of the server a	and other important equip	ment to the static MAC	address table.					
ult / Safety	MAC list: All	Configure MAC Binding									
attack Prevention		User MAC			Туре		VLAN	Edit			
oop Detection	V	100D.7FC0.21FD	Sure	you want to bind as stati	MAC? amic		1	00			
ccess Control		0006.6705.0697			amic		1	00			
GMP Snooping		D039.720E.AE0B		OK Can	cel amic		1	00			
tem Management		28C6.8E34.1CD3	26		Dynamic		1	00			
ystem Upgrade		0006.6722.F7D8	26		Dynamic		1	00			
system Information		D05F.B880.696B	26		Dynamic		1	00			
Configuration Management		0025.6497.2724	26		Dynamic		1	00			
NMP vstem Diagnostics		2405.0F68.033F	26		Dynamic		1	00			
E System Management		000E.7FF0.6251	26		Dynamic		1	00			
		0006.6723.DD32	26		Dynamic		1	00			

Figure 8-12 Conduct Static MAC Address Configuration

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.

System Home	VLAN Manage	ment System Restart	Change Password	System Log Log Export	ARP Table MAC Management	
Quick Configuration	Protection Setting	s				
ort Management AN Management	Static MAC: To enha	ance the safety of important data, add th	e MAC addresses of the server ar	nd other important equipment to the static M	IAC address table.	
ult / Safety	MAC list: All	Configure MAC Binding				
Attack Prevention		User MAC	Port	Port Type	VLAN	Edit
Path Detection	V	ECA8.6BD8.C16D	26	Dynamic	1	00
Access Control		0006.6722.F7D8	26	Dynamic	1	00
IGMP Snooping		D05F.B880.696B	26	Dynamic	1	00
stem Management System Settings	1	0025.6497.2724	26	Dynamic	1	00
System Upgrade		D8EB.97D2.AE83	26	Dynamic	1	00
System Information		2405.0F68.033F	26	Dynamic	1	00
Configuration Management		000E.7FF0.6251	26	Dynamic	1	00
SNMP System Diagnostics		0006.6723.DD32	26	Dynamic	1	00
E System Management		001B.1700.0A12	26	Dynamic	1	00
		0006.6725.3810	26	Dynamic	1	00

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).

stem Home	VLAN Managemen	t System Restart	Change Password System	Log Log Export	ARP Table MAC Management	
ick Configuration	Protection Settings					
Management	Static MAC: To enhance the	he safety of important data, add the	MAC addresses of the server and other impo	rtant equipment to the static MAC a	address table.	
I Management / Safety ack Prevention	MAC list: Static 🗸	Configure MAC Binding				
h Detection		User MAC	Port	Port Type	VLAN	Edit
p Detection		D8EB.97D2.B332	26	Static	1	×
ess Control		3415.9E18.1A8E	26	Static	1	×
IP Snooping	V	28C6.8E34.1CD3	26	Static	1	×
m Management tem Settings		D039.720E.AE0B	26	Static	1	×
tem Upgrade		100D.7FC0.21FD	26	Static	i i	×
tem Information		F8F1.B6D6.C575	26	Static	1	×
figuration Management		0006.6705.0697	26	Static	i	×
IP tem Diagnostics	O Dynamic MAC to Sta	atic MAC 🤤 Delete Static MAC				First Previous [1] Next Last1 / 1Pa

Figure 8-14 Delete MAC Address(es)

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 \rightarrow System Information \rightarrow Memory Information" to visit the Memory Information page. This page displays the current system memory information.



Figure 8-16 Memory Information

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

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.

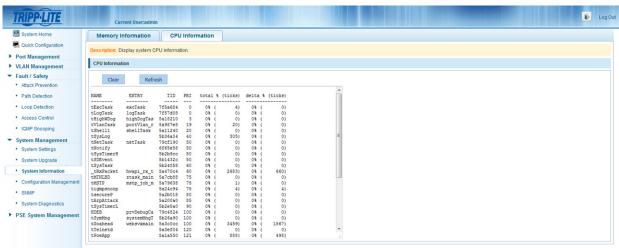


Figure 8-17 CPU Information

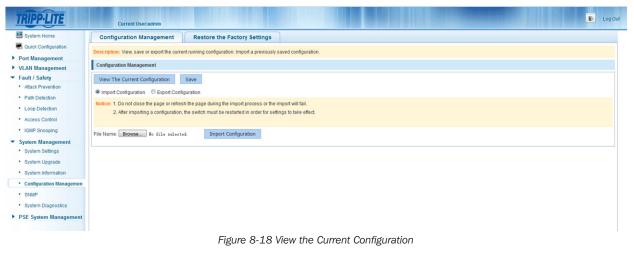
Notes:

- 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.



Save Configuration

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

TRIPP-LITE	Current Useradmin	Log Out
🛃 System Home	Configuration Management Restore the Factory Settings	
Cuick Configuration	Description: View, save or export the current running configuration. Import a previously saved configuration.	
Port Management		
VLAN Management	Configuration Management	
▼ Fault / Safety	View The Current Configuration Save	
Attack Prevention	Import Configuration Export Configuration	
Path Detection	Notice: 1. Do not clease the page or refresh the page during the import process or i Success	
Loop Detection	2. After importing a configuration, the switch must be restarted in order for	
Access Control		
IGMP Snooping	File Name: Browse	
▼ System Management		
System Settings		
System Upgrade		
System Information		
Configuration Managemen		
• SNMP		
System Diagnostics		
► PSE System Management		

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.

TRIPP·LITE	Current User:admin		🕑 Log Out
🛃 System Home	Configuration Management	Restore the Factory Settings	
Quick Configuration Port Management	Description: View, save or export the curren	t running configuration. Import a previously saved configuration.	
VLAN Management	Configuration Management		
 Fault / Safety Attack Prevention 	View The Current Configuration	Save	
Path Detection Loop Detection Access Control	Notice: 1. Do not close the page or refresh	The page during the import process of the import will fail. the switch must be restarted in order for settings to take effect.	
IGMP Snooping System Management	File Name: Browse No file selecte	4 Import Configuration	
System Settings System Upgrade			
System Information Configuration Management			
SNMP System Diagnostics			
PSE System Management			

Figure 8-20 Import Configuration

Export Configuration

Select "System Management \rightarrow Configuration Management \rightarrow Configuration Management". Click the "Export Configuration" radio button, then click the "Export configuration" button to export the current running configuration.

TRIPP·LITE	Current Useradmin	🕑 Log Out
🛃 System Home	Configuration Management Restore the Factory Settings	
Quick Configuration Port Management	Description: Wew, save or export the current running configuration. Import a previously saved configuration.	
VLAN Management	Configuration Management	
 Fault / Safety Attack Prevention 	View The Current Configuration Save	
Path Detection	Import Configuration Export Configuration Export Configuration	
Loop Detection Access Control		
IGMP Snooping		
System Management System Settings		
System Upgrade System Information		
Configuration Management		
• SNMP		
System Diagnostics		
PSE System Management		

Figure 8-21 Export Configuration

8.4.2 Restore the Factory Settings

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

TRIPP-LITE	Current User:admin				🕑 Log Out
🛃 System Home	Configuration Management	Restore the Factory Settings			
Cuick Configuration	Description: Click 'Restore' to reset the sw	itch to the factory default collinge			
Port Management		inch to the factory default settings.			
VLAN Management	Restore				
▼ Fault / Safety					
Attack Prevention					
Path Detection		Are you su	e you want to restore the factory configuration?		
Loop Detection		,,			
Access Control					
IGMP Snooping			OK Cancel		
▼ System Management					
System Settings					
System Upgrade					
System Information					
Configuration Managemen					
• SNMP					
System Diagnostics					
PSE System Management					

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.

🛃 System Home	SNMP
S Quick Configuration Port Management VLAN Management	Description: SNMP is used for remote monitoring and switch control. This feature can be enabled by togging the SNMP Service' switch. Notice: The SNMP monitor software must match the selected SNMP version, mismatched versions will cause communication failure.
Fault / Safety Attack Prevention Path Detection Loop Detection	SHMP Service: ON SHMP TRAP Service: ON Community Settings: Community Name Permissions @ RO RW OK SHMP Trap Host: Host: Trap Community Name SNMP Version V1 OK
Access Control IGMP Snooping System Management	
System Settings System Upgrade	
System Information Configuration Management	

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.

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:							
SNMP TRAP Service:							
Community Settings: Community Name	Permissions RO RW OK Cancel						
SNMP Trap Host: Host IP Trap	p Community Name SNMP Version V1 - OK Cancel						

Figure 8-24 Enable or Disable SNMP Service

Note: SNMP version supports V1 and V2C.

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:						
Community Settings: Community Name	Permissions RO	© RW OK Cancel				
SNMP Trap Host: Host IP	Trap Community Name	SNMP Version V1 -	OK Cancel			
	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.

TRIPPILITE	Current Useradmin		🕑 Log Ou
🛃 System Home	SNMP		
Real Quick Configuration	Description: SNMP is used for remote monitoring and switch control. This feature can be enabled by toggling the 'SNMF	Service' switch.	
Port Management	Notice: The SNMP monitor software must match the selected SNMP version, mismatched versions will cause communi		
VLAN Management Fault / Safety	SIMP Service: ON		
Attack Prevention	SNMP TRAP Service:		
Path Detection	Community Settings: Community Name Permissions RO RW	OK Cancel	
Loop Detection	SNMP Trap Host: Host IP Trap Community Name SN	MP Version V1 - OK Cancel	
Access Control	Community Name List		
IGMP Snooping	Community Name	Permissions	Remove
 System Management System Settings 	test	RO	×
System Upgrade		First Previ	ious [1] Next Last1 / 1Page
System Information			
Configuration Management			

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.

TRIPP-LITE	Current Useradmin		🕑 Log Out
🛃 System Home	SNMP		
Ouick Configuration Port Management VLAN Management Fault / Safety Attack Prevention Path Detection	Description: SNMP is used for remote monitoring and switch control. This feature can be enabled by toggling the 'SNMP Notice: The SNMP monitor software must match the selected SNMP version, mismatched versions will cause commun SNMP Service: ON SNMP TRAP Service: ON Community Settings: Community Name Permissions ® R0 RW	OK Cancel	
Loop Detection Access Control IGMP Snooping	SMMP Trap Host: Host IP Trap Community Name SN Community Name List Community Name	MP Version V1 OK Cancel Permissions	Remove
 System Management 		RO	
 System Settings 	test		×
 System Upgrade 		First Previ	ous [1] Next Last1 / 1Page
System Information			
Configuration Management			
SNMP			

Figure 8-27 Delete Community Name

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.

System Home Configuration System Home Configuration Configuration Configuration Control Contr	Current Useradmin SNMP Description: SNMP is used for remole monitoring and switch contin Notice: The SNMP monitor software must match the selected SNM SNMP Service: ON Community Settings: Community Name SNMP Trap Host: Host IP Tra	Persion, mismatched versions will cause communication failure.	DK Cancel				
Loop Detection	Loop Detection 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 Previ	ous [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 Previo	ous [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.

System Home	System Diagnostics
Quick Configuration	Description: System diagnostics can be used to export current system status.
Port Management	
/LAN Management	System Diagnostics
ault / Safety	
Attack Prevention	
Path Detection	
Loop Detection	
Access Control	
IGMP Snooping	
ystem Management	
System Settings	
System Upgrade	
System Information	
Configuration Management	
SNMP	
System Diagnostics	
SE System Management	

9.1 PSE System Configuration

9.1.1 View PSE System Configuration

Select "PSE System \rightarrow PSE System Configuration" to view the switch's PSE configuration.

TRIPP·LITE	Current User:admin		Deg Out
🛃 System Home	PSE System Configuration		
Quick Configuration Port Management	Notice: 1.Changing the Uninterrupted PoE P	ower setting will only take effect after saving the configu	ration. 2.The abnormal recovery time settings will only take effect when the power supply is set to automatic mode.
VLAN Management Fault / Safety Attack Prevention Path Detection Loop Detection Access Control IGNP Snooping	Uninterrupted PoE Power: Dis Non-standard PD compatible: Dis Power Supply Mode: En PoE Guard Band: 0 Abnormal Recovery Time Intervat: 10 Apply Settings PSE System Information	abled -	
 System Management 	Power supply port		
 PSE System Management PSE System Configuration 	Power management mode:	Energy saving mode	
POE Port Configuration	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 9-1 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.

TRIPPILITE	Current User:admin		De Dagoar
🛃 System Home	PSE System Configuration		
Quick Configuration Port Management VLAN Management Fault / Safety System Management PSE System Management · PSE System Configuration · POE Port Configuration	Uninterrupted PoE Power: Di Non-Standard PD Compatible: Do Power Supply Mode: En PoE Guard Band: 10 Abnormal Recovery Time Intervat: 10 Apply Settings Refresh	abled	rration. 2. The abnormal recovery time settings will only take effect when the power supply is set to automatic mode.
	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.

9.1.3 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.

System Home	PSE System Configuration		
Quick Configuration	Notice: 1.Changing the Uninterrupted PoE Po	ower setting will only take effect after saving the config	uration. 2.The abnormal recovery time settings will only take effect when the power supply is set to automatic mode.
/LAN Management Fault / Safety System Management PSE System Management	Uninterrupted PoE Power: Dis Non-Standard PD Compatible: Dis Power Supply Mode: Do PoE Guard Band: Dis Abnormal Recovery Time Intervat: 10	abled Not Modify bled	
PSE System Configuration POE Port Configuration	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 9-3 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.

TRIPP·LITE	Current User:admin		D Log Dat
System Home Culick Configuration Port Management VLAN Management Fault / Safety System Management PSE System Management PSE System Configuration	Uninterrupted PoE Power: Di Non-Standard PD Compatible: Di Power Supply Mode: Er PoE Guard Band: Dr Abnormal Recovery Time Intervai: En St	sabled - sabled -	uration. 2.The abnormal recovery time settings will only take effect when the power supply is set to automatic mode.
POE Port Configuration	Apply Settings Refresh PSE System Information Power Supply Port. Power Supply Port. Power Management Mode: Uninterrupted PoE Power. Non-Standard PD Compatible: Abnormal Recovery Time Internat: System Total Power. System Total Power. System Available Power.	Energy Saving Mode Disabled Disabled 10s 240 W 0 W 216 W (90%)	
	PoE Guard Band:	10%	

Figure 9-4 Modify Power Supply Mode

Note: The default "Power Supply Mode" is "Automatic Mode".

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.

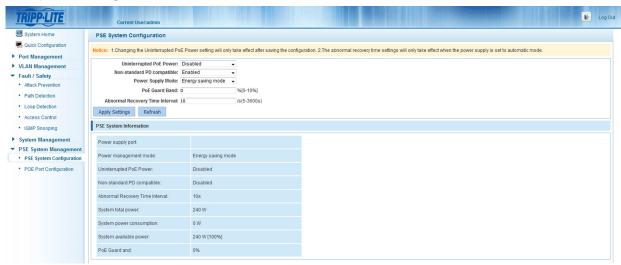


Figure 9-5 PoE Guard Band Configuration

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

9.1.6 Abnormal Recovery Time Interval Configuration

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

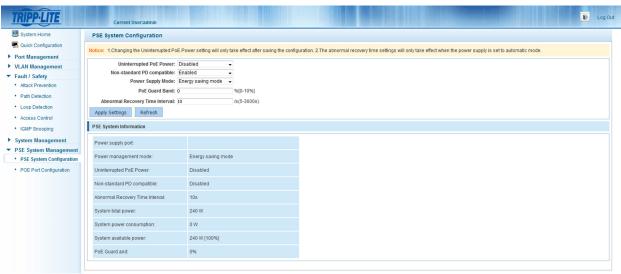


Figure 9-6 Abnormal Recovery Time Interval Configuration

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

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.

TRIPPILITE	Current User	radmin									Þ	Log Out
🛃 System Home	POE Port Settings											
SQUICK Configuration	Description: 1 When po	ort description is empty, there is r	o description for that r	ort 2 When max power	r and distribution of	power fields	are empty the po	ort is set to default settings				
Port Management		and description is empty, after the	o description for and p	on 2. mich max poner		ponernera	are empty, are pe	in is set to deladit settings.				
VLAN Management	Select a	port to configure:										
 Fault / Safety 	1 3 5 7	9 11 13 15 17 19 2	1 23									
Attack Prevention	122222	22222222	353									
Path Detection		10 12 14 16 18 20 2	2 24 25 26									
Loop Detection		Fixed port 🚔 Selected port 🖇										
Access Control	<u>S Copuonar port</u>	Leven hour Just selected hour 2	TC Aggregation port	select all Select all out	ers Gancer							
IGMP Snooping												
System Management	F	Port:		Dowor	Supply Enable: Do	Not Modify	•					
▼ PSE System Management		prity: Do Not Modify 🚽		r ou cr	Max Power:	rectinoutly	w[0-30W]					
PSE System Configuration	Recovery Me	lode: Do Not Modify 🗸		Distribu	tion of Power:		W[0-30W]					
POE Port Configuration	Apply Refresh	1										
	POE Port Information											
	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	

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.

System Home	POF	Port Settings												
R Quick Configuration														
Port Management	Descri	ption: 1. When po	rt description	is empty, there is no	description for that po	ort. 2. When max power	and distribution of	power fields	are empty, the po	rt is set to default settings.				
VLAN Management		Select a	port to confi	gure:										
Fault / Safety	1	3 5 7	9 11 13	15 17 19 21	23									
Attack Prevention	1				1 🗅									
Path Detection		ទេធ្នេះ		김김김김김	24 25 26									
Loop Detection	2			16 18 20 22										
Access Control		Optional port	Fixed port	Selected port 51	Aggregation port S	elect all Select all othe	rs Cancel							
IGMP Snooping														
System Management			Port:											
System Settings System Upgrade	Арр	Descrip Pric Recovery M	tion: prity: Do Not ode: Do Not				Max Power: Do Max Power: Do tion of Power: Ena Disa	Not Modify	[0-30W] [0-30W]					
System Settings System Upgrade System Information		Descrip Pric Recovery M	tion: prity: Do Not ode: Do Not				Max Power: Do I	Not Modify bled	[0-30W]					
System Settings System Upgrade System Information Configuration Management		Descrip Pric Recovery M ly Refresh	tion: prity: Do Not ode: Do Not		Current Power		Max Power: Do I	Not Modify bled	[0-30W]	Distribution of Power	Priority	Recovery Mode	Device Type	
System Settings System Upgrade System Information Configuration Management SNMP System Diagnostics	POE	Descrip Prio Recovery M ly Refresh Port Information	tion: prity: Do Not ode: Do Not	Modify -	Current Power	Distribu	Max Power: Do tion of Power: Dis	Not Modify bled abled	[0-30W] [0-30W]	Distribution of Power 30 W	Priority Low	Recovery Mode auto	Device Type NoPd	
System Settings System Upgrade System Information Configuration Management SNMP System Diagnostics SE System Management	POE I Port	Descrip Pric Recovery M ly Refresh Port Information Description	tion: Do Not ority: Do Not Do Not Status	Modify - Power Status		Distribu Average Power	Max Power: Do Ena tion of Power: Dis: Peak Power	Not Modify bled abled Voltage	[0-30W] [0-30W] Max Power			-		
System Settings System Upgrade System Information Configuration Management SNMP System Diagnostics SE System Management PSE System Configuration	POE Port	Descrip Pric Recovery M ly Refresh Port Information Description	tion: Do Not ode: Do Not Status Normal	Modify Power Status Detecting	0 W	Distribu Average Power 0 W	Max Power: Do tion of Power: Dis: Peak Power 0 W	Not Modify Ibled abled Voltage 0 V	[0-30W] [0-30W] Max Power 30 W	30 W	Low	auto	NoPd	
System Settings System Upgrade System Information Configuration Management SNMP System Diagnostics SE System Management PSE System Configuration	POE I Port 1 2	Descrip Pric Recovery M ly Refresh Port Information Description	tion: prity: Do Not ode: Do Not Status Normal Normal	Modify Power Status Detecting Detecting	0 W 0 W	Distribut	Max Power: Do tion of Power: Dis: Peak Power 0 W 0 W	Not Modify ibled abled Voltage 0 V 0 V	[0-30W] [0-30W] Max Power 30 W 30 W	30 W 30 W	Low	auto	NoPd NoPd	
System Settings System Upgrade System Information Configuration Management SNMP System Diagnostics System Diagnostics Set System Management PSE System Configuration	POE Port 1 2 3	Descrip Pric Recovery M ly Refresh Port Information Description	tion: prity: Do Not ode: Do Not Status Normal Normal	Modify - Power Status Detecting Detecting Detecting	0 W 0 W 0 W	Distribut Average Power 0 W 0 W	Max Power: Do Ena Disr Peak Power 0 W 0 W 0 W	Voltage O V O V O V O V	[0-30W] [0-30W] Max Power 30 W 30 W 30 W	30 W 30 W 30 W	Low Low Low	auto auto auto	NoPd NoPd NoPd	
9 yearn annungeneen 9 yearn Unprade 9 yearn Information • Configuration Management • Configuration Management • System Diagnostics PSE System Management • PSE System Configuration • POE Port Configuration	POE 1 Port 1 2 3 4	Descrip Pric Recovery M ly Refresh Port Information Description	tion: Do Not ode: Do Not Status Normal Normal Normal	Nodify Power Status Detecting Detecting Detecting Detecting	0 W 0 W 0 W 0 W	Distribut Average Power 0 W 0 W 0 W	Max Power: Do tion of Power: Disr Peak Power 0 W 0 W 0 W 0 W	Not Modify bibled abled 0 V 0 V 0 V 0 V 0 V	[0-30W] [0-30W] Max Power 30 W 30 W 30 W 30 W	30 W 30 W 30 W 30 W	Low Low Low	auto auto auto auto	NoPd NoPd NoPd NoPd	

Figure 9-8 Enable or Disable Power Supply

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

9.2.3 Modify Port Description

Select "PSE System \rightarrow 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.

TRIPP·LITE		Current Us	er:admin										•	Log Out
📑 System Home	POE	Port Settings												
Real Quick Configuration	Descri	ption: 1. When po	rt descriptior	n is empty, there is n	o description for that pe	ort. 2. When max power	and distribution of	power fields	are empty, the po	rt is set to default settings.				
 Port Management VLAN Management 		Select a	port to confi	gure:										
Fault / Safety	1	3 5 7	9 11 13	8 15 17 19 21	23									
System Management	1	2222	322	12222	12									
 PSE System Management 	2				24 25 26									
PSE System Configuration														
POE Port Configuration	12	Optional port j	(Fixed port)	Selected port 21	Aggregation port S	elect all Select all othe	ers Cancel							
	Арр	Descrip Pric Recovery M	ority: Do Not ode: Do Not High Interme	Modify			Supply Enable: Do Max Power: tion of Power:	Not Modify	• W[0-30W] W[0-30W]					
	POF	Port Information	Low											
												-		
	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

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

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.

🛃 System Home	POE	Port Settings												
Quick Configuration	Description			la analy there is a	d = = = = = = = = = = = = = = = = = = =		and distribution of							
Port Management	Descrip	don: 1. when po	n description	i is empty, there is no	description for that p	on. 2. when max power	and distribution of	power neids	are empty, the por	t is set to default settings.				
LAN Management		Select a	port to confi	gure:										
ult / Safety	1	3 5 7		15 17 19 21	23									
stem Management	123	2222	322		<u> </u>									
E System Management	2		10 12 14	16 18 20 22	24 25 26									
PSE System Configuration						elect all Select all othe	are Cancel							
POE Port Configuration	2	opuonai pont j	rived bour 1	Conected poin 11	C Aggregation por C	Select all Select all Out	era Ganter							
		Descrip Pric Recovery M	rity: Do Not				Supply Enable: Do Max Power: tion of Power:	Not Modify	• W[0-30W] W[0-30W]					
	Appl POE P	Pric Recovery M	ority: Do Not ode: Do Not High	Modify			Max Power:	Not Modify	W[0-30W]					
		Pric Recovery M / Refresh	ority: Do Not ode: Do Not High Interme	Modify	Current Power		Max Power:	Not Modify Voltage	W[0-30W]	Distribution of Power	Priority	Recovery Mode	Device Type	Ed
	POE P	Pric Recovery M Refresh	ority: Do Not ode: Do Not High Interme Low	Modify diate	Current Power 0 W	Distribu	Max Power: tion of Power:		W[0-30W] W[0-30W]	Distribution of Power 30 W	Priority	Recovery Mode auto	Device Type NoPd	
	POE P	Pric Recovery M Y Refresh ort Information Description	ority: Do Not Ode: Do Not High Interme Low	Modify diate Power Status		Distribu Average Power	Max Power: tion of Power: Peak Power	Voltage	W[0-30W] W[0-30W] Max Power					
	POE F Port	Pric Recovery M Y Refresh ort Information Description	ority: Do Not ode: Do Not High Interme Low Status Normal	Modify diate Power Status Detecting	0 W	Distribu Average Power 0 W	Max Power: tion of Power: Peak Power 0 W	Voltage 0 V	W[0-30W] W[0-30W] Max Power 30 W	30 W	Low	auto	NoPd	
	POE F Port 1	Pric Recovery M Y Refresh ort Information Description	ority: Do Not ode: Do Not High Interme Low Status Normal Normal	Modify diate Power Status Detecting Detecting	0 W 0 W	Distribu Average Power 0 W 0 W	Max Power: tion of Power: Peak Power 0 W 0 W	Voltage 0 V 0 V	W[0-30W] W[0-30W] Max Power 30 W 30 W	30 W 30 W	Low	auto	NoPd NoPd	
	POE F Port 1 2 3	Pric Recovery M Y Refresh ort Information Description	ority: Do Not ode: Do Not High Interme Low Status Normal Normal	Modify diate Power Status Detecting Detecting Detecting	0 W 0 W 0 W	Distribut Average Power 0 W 0 W	Max Power: tion of Power: Peak Power 0 W 0 W 0 W	Voltage 0 V 0 V 0 V	W[0-30W] W[0-30W] Max Power 30 W 30 W 30 W	30 W 30 W 30 W	Low	auto auto auto	NoPd NoPd NoPd	
	POE P Port 1 2 3 4	Pric Recovery M Y Refresh ort Information Description	Normal Normal Normal	Modify diate Power Status Detecting Detecting Detecting	0 W 0 W 0 W 0 W	Distribut Average Power 0 W 0 W 0 W	Max Power: tion of Power: Peak Power 0 W 0 W 0 W 0 W	Voltage 0 V 0 V 0 V 0 V 0 V	W[0-30W] W[0-30W] Max Power 30 W 30 W 30 W 30 W	30 W 30 W 30 W 30 W	Low Low Low Low	auto auto auto auto	NoPd NoPd NoPd NoPd	



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 \rightarrow 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.

TRIPP·LITE	Current Useradmin
📑 System Home	POE Port Settings
SQUICK Configuration	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.
Port Management	Description. F, thier por description is emply, une is no description for inaction 2. Then may power and dashouring other needs are emply, une ports set to description is settings.
VLAN Management	Select a port to configure:
 Fault / Safety 	1 3 5 7 9 11 13 15 17 19 21 23
Attack Prevention	
Path Detection	
Loop Detection	Coptional port 🚔 Fived port 🚔 Selected port Cl Apgregation port Select all Chers Cancel
Access Control	∑ obioiral boir ™ unsa hoir ™ unsa hoir 3 unsa na unsa suistra na
IGMP Snooping	
System Management	Port 1 Description: Power Supply Enable: Enabled
▼ PSE System Management	Priority: Low - Max Power: 30 W[0-30W]
PSE System Configuration	Recovery Mode: Auto Distribution of Power: 30 W[0-30W]
POE Port Configuration	Apply Refresh
	POE Port Information
	Port Description Status Power Status Current Power Average Power Voltage Max Power Distribution of Power Priority Recovery Mode Device Type Edit

Figure 9-11 Modify Max Power of a Port

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

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.

System Home	POE	Port Settings												
R Quick Configuration	FUE	Port Settings												
Port Management	Descrip	ption: 1. When po	rt description	is empty, there is no	description for that p	ort. 2. When max power	and distribution of	power fields	are empty, the po	t is set to default settings.				
VLAN Management		Select a	port to confi	aure:										
Fault / Safety		3 5 7	0 11 12	15 17 19 21	22									
Attack Prevention			àöč											
Path Detection			377		3 🖂 🔲 🔲									
 Loop Detection 	2			16 18 20 22										
Access Control		Optional port 🚞	Fixed port	Selected port 🚹	Aggregation port S	elect all Select all othe	rs Cancel							
IGMP Snooping														
System Settings System Upgrade	Appl	Descrip Pric Recovery M	Do Not Manual	Modify			Max Power: 30	ibled	• W[0-30W] W[0-30W]					
System Settings System Upgrade System Information		Descrip Pric Recovery M	tion: test rity: Low ode: Auto Do Not				Max Power: 30	ibled	W[0-30W]					
System Settings System Upgrade System Information Configuration Management		Descrip Pric Recovery M y Refresh	tion: test ority: Low ode: Auto Do Not Manual		Current Power		Max Power: 30	Voltage	W[0-30W]	Distribution of Power	Priority	Recovery Mode	Device Type	
System Settings System Upgrade System Information Configuration Management SNMP	POE F	Descrip Pric Recovery M y Refresh Port Information	tion: test ority: Low ode: Auto Do Not Manual Auto	Modify	Current Power	Distribu	Max Power: 30 tion of Power: 30		W[0-30W] W[0-30W]	Distribution of Power	Priority	Recovery Mode auto	Device Type	
System Settings System Upgrade System Information Configuration Management SNMP System Diagnostics 25E System Management	POE F Port	Description Price Recovery M Port Information	tion: test rity: Low ode: Auto Do Not Manual Auto Status Normal	Modify Power Status Detecting	0 W	Distribu Average Power 0 W	Max Power 30 tion of Power 30 Peak Power 0 W	Voltage 0 V	W[0-30W] W[0-30W] Max Power 30 W	30 W	Low	auto	NoPd	
System Settings System Upgrade System Information Configuration Management SNMP System Diagnostics SE System Management PSE System Configuration	POE F Port 1	Description Price Recovery M Port Information	tion: test irity: Low ode: Auto Do Not Manual Auto Status Normal	Modify Power Status Detecting Detecting	0 W 0 W	Distribut	Max Power: 30 tion of Power: 30 Peak Power 0 W 0 W	Voltage 0 V 0 V	W[0-30W] W[0-30W] Max Power 30 W 30 W	30 W 30 W	Low	auto	NoPd NoPd	
System Settings System Upgrade System Information Configuration Management SNMP System Diagnostics SE System Management PSE System Configuration	POE F Port	Description Price Recovery M Port Information	tion: test rity: Low ode: Auto Do Not Manual Auto Status Normal	Modify Power Status Detecting	0 W	Distribu Average Power 0 W	Max Power 30 tion of Power 30 Peak Power 0 W	Voltage 0 V	W[0-30W] W[0-30W] Max Power 30 W	30 W	Low	auto	NoPd	
System Settings System Upgrade System Information Configuration Management SNMP System Diagnostics SE System Management PSE System Configuration	POE F Port 1	Description Price Recovery M Port Information	tion: test irity: Low ode: Auto Do Not Manual Auto Status Normal	Modify Power Status Detecting Detecting	0 W 0 W	Distribut	Max Power: 30 tion of Power: 30 Peak Power 0 W 0 W	Voltage 0 V 0 V	W[0-30W] W[0-30W] Max Power 30 W 30 W	30 W 30 W	Low	auto	NoPd NoPd	
System Settings System Upgrade System Information Configuration Management SNMP System Diagnostics SE System Management PSE System Configuration	POE F Port 1 2 3	Description Price Recovery M Port Information	tion: test rity: Low ode: Auto Do Not Manual Auto Status Normal Normal	Modify Power Status Detecting Detecting Detecting	0 W 0 W 0 W	Distribut	Max Power: 30 ion of Power: 30 Peak Power 0 W 0 W 0 W	Voltage 0 ∨ 0 ∨ 0 ∨	W[0-30W] W[0-30W] Max Power 30 W 30 W 30 W	30 W 30 W 30 W	Low Low	auto auto auto	NoPd NoPd NoPd	
System Management System Settings System Lograde System Information Configuration Management SMMP System Diagnostics PSE System Configuration PSE System Configuration POE Port Configuration	POE F Port 1 2 3 4	Description Price Recovery M Port Information	Ition: test writy: Low de: Auto Do Not Manual Auto Status Normal Normal Normal	Power Status Detecting Detecting Detecting Detecting	0 W 0 W 0 W	Distribut Average Power 0 W 0 W 0 W	Max Power: 30 ion of Power: 30 Peak Power 0 W 0 W 0 W 0 W	Voltage 0 V 0 V 0 V 0 V	W[0-30W] W[0-30W] Max Power 30 W 30 W 30 W 30 W	30 W 30 W 30 W 30 W	Low Low Low Low	auto auto auto auto	NoPd NoPd NoPd 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 \rightarrow 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.

TRIPP·LITE		Current Use	er:admin										Ð	Log Out
🛃 System Home	POE Port Settings													
SQUICK Configuration	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.													
Port Management														
VLAN Management	Select a port to configure:													
 Fault / Safety 	1 3 5 7 9 11 13 15 17 19 21 23													
 Attack Prevention 														
Path Detection	2 4 6 8 10 12 14 16 18 20 22 24 25 26													
Loop Detection		Coptional port Presd port Selected port 12 Apprepation port Select all Others Cancel												
Access Control	Coheven how The section of the Contract how Contract and contract on contract on the contract of the Contract													
IGMP Snooping														
System Management		Descrip	Port: 1			Power	Supply Enable: En	abled	•					
▼ PSE System Management	Priority: Low Max Power: 30 M[0-30W]													
PSE System Configuration	Recovery Mode: Auto Distribution of Power: 30 W(0-30W)													
POE Port Configuration	App	ly Refrest	n											
	POE F	Port Information												
	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
	2		Normal	Detecting	0 W	0 W	0 W	0 V	30 W	30 W	Low	auto	NoPd	2
	3		Normal	Detecting	0 W	0 W	0 W	0 V	30 W	30 W	Low	auto	NoPd	1
					Figure 9-1	12 Madify	Distrikt in		-					

- 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 Cate	gory	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