

User Guide

Easy Managed Switch

1910013715 REV1.0.0

August 2024

CONTENTS

About This Guide

Intended Readers	. 1
Conventions	. 1
More Information	. 1

Introduction

Product Overview	.4
Logging Into the Switch	5

Managing System

System	8
overview	
Supported Features	8
System Summary	
Viewing the System Information	
Specifying the Device Name	
Configuring IP	
Configuring User Account	
Configuring LED	
Appendix: Default Parameters	

Switching

Switching1	7
Overview1	7
Supported Features	
Configuring Ports	9
Configuring IGMP Snooping	
Configuring LAG	2
Configuration Examples	3
Example for Configuring IGMP Snooping2	3
Network Requirements2	3
Configuration Scheme2	3
Configuration Steps2-	4
Example for Configuring LAG2	5

Network Requirements	25
Configuration Steps	
Appendix: Default Parameters	27

Configuring VLAN

Overview	29
Configuring MTU VLAN	;1
Configuring Port-Based VLAN	2
Configuring 802.1Q VLAN	3
Configuring the VLAN	33
Configuring the PVID	35
Configuring Management VLAN	
Configuration Example for 802.1Q VLAN	37
Network Requirements	37
Configuration Scheme	
Configuration Steps	}9
Appendix: Default Parameters	1

Configuring QoS

QoS	. 43
Overview	
Supported Features	43
Configuring Basic QoS	. 44
Configuring QoS in Port-Based Mode	45
Configuring QoS in 802.1p-Based Mode	47
Configuring QoS in DSCP-Based Mode	
Configuring Rate Limit	. 51
Configuring Storm Control	. 52
Configuration Example for Basic QoS	. 54
Network Requirements	
Configuration Scheme	54
Configuration Steps	55
Appendix: Default Parameters	. 57

Monitoring

Monitori	ing5	9
Ove	erview5	9

Supported Features	
Viewing Traffic Summary	
Configuring Mirroring	61
Testing Cables	
Configuring Loop Prevention	
Appendix: Default Parameters	65

System Tools

System Tools	67
Overview	67
Supported Features	67
Jpgrading the Firmware	68
Backing up and Restoring the Switch	70
Saving the Current Configuration	70
Restoring to the Previous Configuration	71
Resetting the Switch	73
Rebooting the Switch	74

Controller Settings

Controller Settings	76
Overview	76
Supported Features	76
Configuring Controller Settings	77
Appendix: Default Parameters	79

Configuring PoE (Only for Certain Devices)

PoE	81
Overview	81
Supported Features	81
Configuring PoE	. 82
Configuring PoE Auto Recovery	. 84
Configuring Extend Mode	. 86
Appendix: Default Parameters	. 87

About This Guide

This Configuration Guide provides information for configuring the Easy Managed Switch via the web interface. Read this guide carefully before operation.

You can also configure and manage the switch using the Omada Controller. For more information, refer to the **Omada SDN Controller User Guide**. Go to the website *https://www.tp-link.com/support/?type=smb*, search Omada SDN Controller, and you can find the guide on the product Support web page.

Intended Readers

This Guide is intended for network managers familiar with IT concepts and network terminologies.

Conventions

When using this guide, notice that features available in Easy Managed Switch may vary by model and software version. The availability of Easy Managed Switch may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual experience. Throughout the guide, we will take a specific model as the switch to be configured for example.

Some models featured in this guide may be unavailable in your country or region. For local sales information, visit *https://www.tp-link.com/business-networking/*.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute the warranty of any kind, express or implied. Users must take full responsibility for their application of any products.

In this Guide, the following conventions are used:

The symbol references that help you make better use of your device.

Menu Name > Submenu Name > Tab page indicates the menu structure. SYSTEM > System Info > System Summary means the System Summary page under the System Info menu option that is located under the SYSTEM menu.

Bold font indicates a button, toolbar icon, menu or menu item.

More Information

The latest software and documentations can be found at Download Center at https://www.tp-link.com/support/download/?type=smb.

- The Installation Guide (IG) can be found where you find this guide or inside the package of the switch.
- The authentication information can be found where you find this guide.
- Specifications can be found on the product page at *https://www.tp-link.com/business-networking/*.
- To ask questions, find answers, and communicate with TP-Link users or engineers, please visit *https://community.tp-link.com/business* to join TP-Link Community.
- Our Technical Support contact information can be found at the Contact Technical Support page at https://www.tp-link.com/support/?type=smb.

Part 1 Introduction

CHAPTERS

- 1. Product Overview
- 2. Logging Into the Switch

Product Overview

Easy Managed Switch is an ideal upgrade from Unmanaged Switch, designed for Small Office and Home Office networks. The switch supports the following features:

- Traffic monitoring: Traffic summary, port mirroring, loop prevention and cable test enable the administrator to monitor traffic of the network effectively.
- VLAN: MTU VLAN, Port-based VLAN and 802.1Q VLAN can restrict broadcast domain, enhance network security and help manage devices easily.
- QoS: Port-based QoS, 802.1P-based QoS and DSCP/802.1P based QoS optimize traffic on your business network, and keep latency-sensitive traffic moving smoothly. Rate limit helps distribute and utilize network bandwidth reasonably. Storm control helps avoid network broadcast storm.
- PoE: PoE (Power over Ethernet) is a remote power supply function. With this function, the switch can supply power to the connected devices over twisted-pair cables.



• The PoE Config is only available on Easy Managed Switches with PoE ports. For other non-PoE Easy Managed Switches, this feature is not supported.

_ . _ _ . _ _ . _ _ . _ _ . _ _ . _

2 Logging Into the Switch

To configure your switch through a web browser on your PC, follow these steps:

- 1) Connect your switch to the network and connect your PC to the switch.
- 2) Find out the IP address of the switch.
 - By default, the switch receives an IP address from a DHCP server (or a router that functions as a DHCP server) in your network. You can find out this IP address on the DHCP server.
 - If the switch cannot receive an IP address from a DHCP server, it uses the static IP address of 192.168.0.1, with a subnet mask of 255.255.255.0.
- 3) Configure IP address on your PC to make sure the switch and PC are in the same subnet.
 - If the switch uses an IP address assigned by a DHCP server, set your PC to obtain an IP address automatically from the DHCP server.
 - If the switch uses the static IP address of 192.168.0.1, configure your PC's IP address as 192.168.0.x ("x" ranges from 2 to 254), and subnet mask as 255.255.255.0.
- 4) Launch a web browser on your PC. The supported web browsers include, but are not limited to, the following types:
 - IE 8.0, 9.0, 10.0, 11.0
 - Firefox 26.0, 27.0
 - Chrome 32.0, 33.0
- 5) In the address bar of the web browser, enter the IP address of the switch. Here we suppose the switch uses the static IP address **192.168.0.1**.

Figure 2-1 Entering the IP Address of the Switch in the Browser

÷	÷	G	192.168.0.1	

6) Enter the username and password in the pop-up login window. Enter **admin** for both username and password in lower case letters.

Figure 2-2 Logging Into the Switch

Username	e		
8			
Passwort	1		
6			
Remen	nher Me		
	Login		

The first time you log in, you have to change the password to better protect your network and devices.

7) The typical web interface displays below. You can view the running status of the switch and configure the switch on this interface.

Figure 2-3 Launching the Web Interface

_ _ _ _ _ _ _ _ _

		δ tes el[test
ng en and (grant an integr - An item integr - Anni Anni - Anni Anni - Anni Anni - Anni	Sp. Interview Development Development Development Development	
After applying the configuration into		on the upper right of the page to put the

Part 2

Managing System

CHAPTERS

- 1. System
- 2. Configuring System Summary
- 3. Configuring IP
- 4. Configuring LED
- 5. Configuring User Account
- 6. Appendix: Default Parameters

1 System

1.1 Overview

In System Info module, you can view the system information and configure the system parameters and features of the switch.

1.2 Supported Features

System Summary

System Summary is mainly used to view the system information and configure the device name.

IP Settings

Each device in the network possesses a unique IP address. You can access the switch using IP address of the switch. You can set IP address of the switch manually or using DHCP.

User Account

User Account is mainly used to modify the administrator's username and password in order to refuse illegal users.

LED On/Off

LED On/Off config is used to turn on or off the LED on the switch.

2 System Summary

With System Summary, you can:

- View the system information
- Specify the device name

2.1 Viewing the System Information

Choose the menu **System Info > System Summary** to load the following page. You can view the basic system information of the switch.

Figure 2-1 Viewing the System Summary

Device Name.	F 82/16/1	
MACADORS	00.FF:00093.08.F1	
P Address:	192, 1983,0, 8	
SUDDET MASK:	201 201 201 10	
Defilin Galeway	192,168,0,1	
DNG Server	182 160 0 1	
Firmware Version	1.0 0 Dalid 20240420 Rel 70404	
Hardware Werston	E32056-1.0	
Serial Number.		
		Apply:
Notes		
The studies name long	in carmet accored 32 characters.	

• The Serial Number of the switch can be used to add the device to the Omada Cloud-Based Controller.

2.2 Specifying the Device Name

Choose the menu **System Info > System Summary** to load the following page. Specify a new device name for the switch, and click **Apply**.

Figure 2-2 Specifying the Device Name

Syste <mark>n Informat</mark>	n .	0	ł.
Design Name:	Sec 21-1		
NAC Address	00 PF.00 20 20 F1		
PAddices	112 198 2 3		
Leaved Doorse	TISSLIAGET		
CHOICE STRATE	190,161.1 1		
Dit Schemati	463 463 6 4		
Cintrate Version	1.0.0 Gener 200/03420 Part 73434		
Hadware Wiston	E5209G 1.0		
SCIM MURINA,			
		Sinty 1	
Neles. The device screenes	the assume responsed Wir sciences.		

3 Configuring IP

You can configure the system IP address in the following two ways:

- Configure the System IP Address Using DHCP
- Configure the System IP Address Manually

Configuring the System IP Address Using DHCP

Choose the menu **System Info > IP Settings** to load the following page.

Figure 3-1 Configuring System IP Address Using DHCP

" Setting pa		
er, Howeing V	Lingster	
(Leanway	102.100 X.I	
Intel Mark	20332 2030	
ени жана у	8.0.00	
IN LARK	Lindae V	
E CONTRACT	8.0.0 0	

Follow these steps to configure the system IP address using DHCP:

- 1) Select DHCP Settings as Enable from the drop-down list.
- 2) Configure Auto DNS.

a) Select Auto DNS as **Enable** from the drop-down list. The switch will obtain the DNS server's IP address from the DHCP Server.

b) Select Auto DNS as **Disable** from the drop-down list. You can specify the DNS server's IP address of the switch.

3) Click **Apply**. The switch will obtain IP settings from the DHCP server.

Configuring the System IP Address Manually

Choose the menu **System Info > IP Settings** to load the following page.

Figure 3-2 Configuring System IP Address Manually

DHCP Seturgs	Disabled v
HADRES:	192,156,0,1
Subnet Mask:	232 232 232 0
Detault Galescap	8.0.0.0
Auto DNS:	Disabled v
ENS Salva.	4.0.00

Follow these steps to configure the system IP address manually:

- 1) Select DHCP Settings as **Disable** from the drop-down list.
- 2) Specify the IP address, subnet mask, default gateway and DNS server.

IP Address	Specify the system IP of the switch. You can use this IP address to access the switch.
Subnet Mask	Specify the subnet mask of the switch.
Default Gateway	Specify the default gateway of the switch.
DNS Server	Specify the DNS server's IP address of the switch.

3) Click Apply.

4 Configuring User Account

With User Account, you can modify the administrator's username and password in order to refuse illegal users.

Choose the menu System Info > User Account to load the following page.

Figure 4-1 Configuring User Account

User Account Setti	a di seconda	
New Username:	admin	
Current Preseword.		
Mess Postsworth		
Confirm (Sassword)		
		 Apply
Money		
	den state de 20 alemania en la servicio e la servicio de la servicio de la servicio de la servicio de la servic	
	if contain 1-32 characters. No species are a loved. 5 contain 0-32 characters. No species are alloved.	

Follow these steps to configure the user account:

1) Specify the new username, enter the current password, specify a new password and confirm the new password.

New Username	Create a user name for login. Requirement for the user name varies among different devices. If your user name fails to meet the requirement, check the prompt information.
Current Password	Enter the current password of the switch. By default, the password is admin .
New Password	Specify a new password for login. Requirement for the password varies among different devices. If your password fails to meet the requirement, check the prompt information.
Confirm Password	Retype the new password.

2) Click **Apply**.

5 Configuring LED

With this function, you can turn on or turn off the LED with one click.

Choose the menu **System Info > LED On/Off** to load the following page. Choose the LED status and click **Apply**.

Figure 5-1 Configuring LED On/Off



6 Appendix: Default Parameters

Default setting of System Summary is listed in the following table.

Table 6-1Default Setting of System Summary

Parameter	Default Setting
Device Name	The model name of the switch.

Default settings of IP Settings are listed in the following table.

Table 6-2	Default Settings of IP Settings
-----------	---------------------------------

Parameter	Default Setting
DHCP Setting	Enable
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Auto DNS	Enable
DNS Server	0.0.0.0

Default setting of User Account is listed in the following table.

Table 6-3Default Setting of User Account

Parameter	Default Setting
New Username	admin

Part 3 Switching

CHAPTERS

- 1. Switching
- 2. Configuring Ports
- 3. Configuring IGMP Snooping
- 4. Configuring LAG
- 5. Configuration Examples
- 6. Appendix: Default Parameters

1 Switching

1.1 Overview

With the switching feature, you can configure Port Settings, IGMP Snooping and LAG.

1.2 Supported Features

The switch supports the following features about switching:

Port Settings

You can configure port state, speed, duplex mode and flow control for ports.

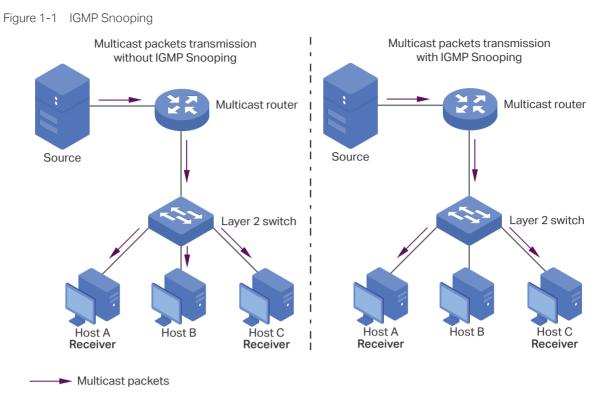
IGMP Snooping

In a point-to-multipoint network, packets can be sent in three ways: unicast, broadcast and multicast. With unicast, many copies of the same information will be sent to all the receivers, occupying a large bandwidth.

With broadcast, information will be sent to all users in the network no matter they need it or not, wasting network resources and impacting information security.

Multicast, however, solves all the problems caused by unicast and broadcast. With multicast, the source only needs to send one piece of information, and all and only the users who need the information will receive copies of the information. In a point-to-multipoint network, multicast technology not only transmits data with high efficiency, but also saves a large bandwidth and reduces network load.

When IGMP Snooping is disabled on the switch, multicast packets will be broadcast in the Layer 2 network; when IGMP Snooping is enabled on the switch, multicast data from a known multicast group will be transmitted to the designated receivers instead of being broadcast in the Layer2 network. The following figure shows how IGMP snooping works.



LAG

With LAG (Link Aggregation Group) function, you can aggregate multiple physical ports into a logical interface to increase link bandwidth and enhance the connection reliability.

2 Configuring Ports

Choose the menu **Switching > Port Settings** to load the following page.

Figure 2-1 Configuring Ports

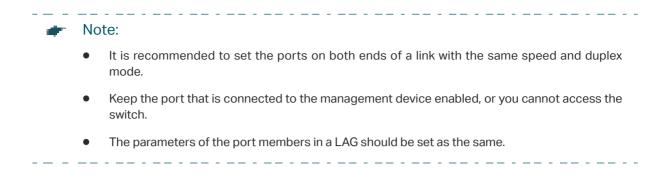
Pr	h	State	Spee	d	Dup	ies .	Flow Co	ottel
Por Por Por Por Por		v		÷		~		• Apply
Port	Six	k	Spe	Pal	ñ.c	iec.	Flow G	
900	Configuration	Aduat	Configuration	Actual	Configuration	Actual	Configuration	Actua
Port 1	Enabled	Disabled	AU0	Uns Down	Auto	Link Down	ा	or
Port 2	Frahled	Disabled	Auto	Hink Down	Arto	i ink Down	Cff	or
Pat 3	Crates	Disting	Auto	Uhk Down	Auto	Link Daven	OT	or
100.4	Enabled	Disabled	Auto	Link Down	Auto	Link Down	01	01
Port 6	Enabled	Enabled	AU0	1000M	Auto	F.01	ा	or

Follow these steps to configure the port parameters.

1) Select the desired ports and set basic parameters for the ports.

State	Enable or disable the port. When Enable is selected, the port can forward the packets normally.
Speed	Select the speed mode for the port. You can select Auto or manually specify the speed mode. When Auto is selected, the speed mode will be automatically determined by auto-negotiation. The device connected to the port should be in the same speed mode as the port.
Duplex	Select the duplex mode for the port. You can select Auto or manually specify the duplex mode. When Auto is selected, the duplex mode will be automatically determined by auto-negotiation. The device connected to the port should be in the same duplex mode as the port.
Flow Control	Select On or Off to enable or disable the Flow Control feature. When On is selected, the switch can synchronize the speed with its peer to avoid the packet loss caused by congestion.
Click Amply	

2) Click Apply.



3 Configuring IGMP Snooping

Choose the menu **Switching > IGMP Snooping** to load the following page.

Figure 3-1 Configuring IGMP Snooping

12	aritire se	MAR D	Port
новит токрот зарренниот.			Apply
ICMP Report Suppression:	O Enable 💄 Dicable		
ICAP Fash-lower	🗇 Enable - 🖶 Disable		
KSMP Secerclass	Tenable Cittable		
IGMP Sneeping			

Follow these steps to configure IGMP Snooping.

1) Enable IGMP Snooping. Enable or disable report message suppression according to your needs. Click **Apply**.

IGMP Snooping	Enable or disable IGMP Snooping globally.
IGMP Fast-leave	Enable or disable Fast Leave globally.
IGMP Report Suppression	Enable or disable Report Message Suppression function globally. If this function is enabled, the first Report Message from the listener will forward to the router ports while the subsequent Report Message will be suppressed to reduce the IGMP packets.

2) In the table below, you can view the current IGMP group information.

IP Address	Displays the IP address of the multicast group.
VLAN ID	Displays the VLAN ID of the multicast group. All port members of a multicast group should be included in the same VLAN.
Port	Displays the forwarding port list of the multicast group.

4 Configuring LAG

Choose the menu **Switching > LAG** to load the following page.

Figure 4-1 Configuring LAG

AG Cooliguration				
L	AS Grup		Forward Forl	
[TAST V		Port 3 Port 3 Port 3 Port 4	
				Addition
1.012.02.000		Francia Dat		Parton line
LUC Crop		Forward Port		Sciection
-				

Follow these steps to configure LAG:

- 1) Select the desired LAG group from the drop-down list.
- 2) Click the ports to add to the LAG group. Click **Apply**.
- 3) In the table below, you can verify the LAG configuration result. You can select the LAG and click **Delete** to delete ports from the LAG group.

LAG Group	Displays the group number of the LAG Group.
Forward Port	Displays the LAG Group member ports.
Selection	Select the LAG Group.

. . _ _ . _ _ . _ _ . _ _ . _ _ . _ _ . _ _ .

Note:

- It is recommended to configure the LAG function before configuring the other functions for the member ports.
- Ensure that devices on both ends of the aggregation link use the same number of physical ports with the same speed and duplex mode, flow control setting and QoS setting.
- Mirroring and mirrored ports cannot be added to an LAG group.
- The maximum of LAG groups varies among different devices. To check the maximum of LAG groups, refer to the actual web interface.
- Each LAG group has 1 port members at least and 4 port members at most.

5 Configuration Examples

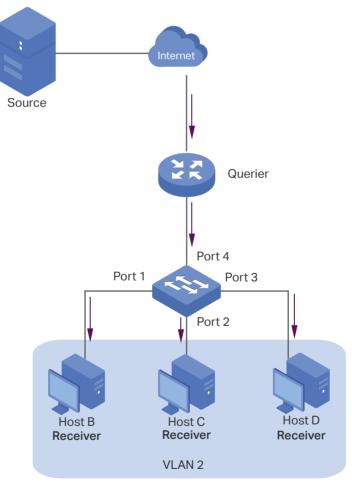
5.1 Example for Configuring IGMP Snooping

5.1.1 Network Requirements

Host B, Host C and Host D are in the same VLAN of the switch. All of them want to receive multicast streams sent to the same multicast group.

As shown in the following topology, Host B, Host C and Host D are connected to port 1, port 2 and port 3 respectively. Port 4 is the router port connected to the multicast querier.





5.1.2 Configuration Scheme

- Configure 802.1Q VLAN. Add the three member ports and the router port to the same VLAN.
- Enable IGMP Snooping.

Demonstrated with a specific model, the following section provides configuration steps.

5.1.3 Configuration Steps

 Choose the menu VLAN > 802.1Q VLAN > VLAN Config to load the following page. Select the 802.1Q VLAN Configuration as Enable. Click Apply. Specify the VLAN ID as
 Specify the VLAN name as VLAN2. Select port 1, port 2, port 3 as untagged ports. Select port 4 as a tagged port. Click Add/Edit.

TI NG VLAN GNADILOT	Creater Costere	C Poste (1)	1
VLAN (0) [(1-4894)	VLAN NAVE VLAN 2		
Pon	Untagged port	Teoper.port	Han-werder port
Scient All	Ω	Π.	
Poels		0	4
1002		0	.0
79H3		0	-0
110.4			12
Pech	6	6	

Figure 5-2 Configuring 802.1Q VLAN

 Choose the menu VLAN > 802.1Q VLAN > Port Config to load the following page. Select port 1, port 2, port 3 and port 4, and specify the PVID as 2 for the ports. Click Apply.

Figure 5-3	Configuring	802.1Q PVID
riuure o-o	Comuumu	

rt Conitg		
802.10 VLAN HOLDER.	O peace	Auto
10 Port Settings		
For	RVD	Taplesis Checking
Port 1 Rut 2 Port X Port 4	2	
Por	PVD	Highling Checking
14141.1	4	inotes
	24	Linksed
Part 2		
Port 2 Port 8	1	Embled
		Enabled

3) Choose the menu **Switching > IGMP Snooping** to load the following page. Enable IGMP snooping. Click **Apply**.

Figure 5-4 Configuring IGMP Snooping

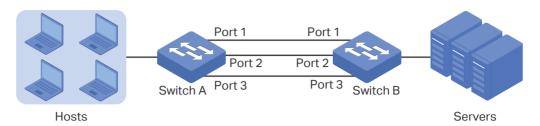
IGMP Sneeping				
KMP Drawing	Enable O Disable			
KARP Foot-known	🔿 Entrable 🔮 Distable			
KMP Report Suppression:	O Enable 🔹 Disable		Αρριγ	
IP a	eddresse	VLANID	Port	

5.2 Example for Configuring LAG

5.2.1 Network Requirements

As shown below, hosts and servers are connected to Switch A and Switch B, and heavy traffic is transmitted between the two switches. To achieve high speed and reliability of data transmission, you can bundle multiple physical ports into one logical interface. In this case, we bundle port 1, port 2 and port 3 of both switches into one logical interface.





Demonstrated with a specific model, the following section provides configuration steps. The configuration steps are similar for both switches, here we take Switch A for example.

5.2.2 Configuration Steps

Choose the menu **Switching > LAG** to load the following page. Add Port 1, Port 2 and Port 3 to LAG 1. Click **Add/Edit**.

U40 Ump	Forward	Forward Port	
LAGE			
LAG Drosp	Pressuet Parl.	Auger Sough	
LAS Seep	Prevent Port 1,2,3	South	

Figure 5-6 Configuring LAG

6 Appendix: Default Parameters

Default settings of Port are listed in the following table.

Table 6-1Default Settings of Port Configuration

Parameter	Default Setting
State	Enabled
Speed	Auto
Duplex	Auto
Flow Control	Off

Default settings of IGMP Snooping are listed in the following table.

Table 6-2	Default Settings of	FIGME Spooning	Configuration
Table 0-2	Delault Settings Of	I IOIVIE SHOOPING	Configuration

Parameter	Default Setting
IGMP Snooping	Enable
IGMP Fast-leave	Disable
IGMP Report Suppression	Disable

Default settings of LAG are listed in the following table.

Table 6-3Default Settings of LAG Configuration

Parameter	Default Setting
LAG Group	LAG 1

Part 4

Configuring VLAN

CHAPTERS

- 1. Overview
- 2. Configuring MTU VLAN
- 3. Configuring Port-Based VLAN
- 4. Configuring 802.1Q VLAN
- 5. Configuration Example for 802.1Q VLAN
- 6. Appendix: Default Parameters

1 Overview

VLAN (Virtual Local Area Network) is a network technique that solves broadcasting issues in local area networks. It is usually applied in the following occasions:

- To restrict broadcast domain: VLAN technique divides a big local area network into several VLANs, and all VLAN traffic remains within its VLAN. It reduces the influence of broadcast traffic in Layer 2 network to the whole network.
- To enhance network security: Devices from different VLANs cannot achieve Layer 2 communication, and thus users can group and isolate devices to enhance network security.
- To facilitate management: VLANs group devices logically instead of physically, so devices in the same VLAN need not be located in the same place. It eases the management of devices in the same work group but located in different places.

There are 3 types of VLAN modes supported on the switch:

MTU VLAN

MTU VLAN (Multi-Tenant Unit VLAN) defines an uplink port which will build up several VLANs with each of the other ports. Each VLAN contains two ports, the uplink port and one of the other ports in the switch, so the device connected to the uplink port can communicate with the device connected to any other port, but devices connected to other ports cannot communicate with each other.

Port-Based VLAN

VLANs are divided based on ports. In port based VLAN mode, each port can only be added to one VLAN.

802.1Q VLAN

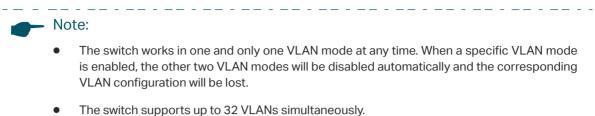
The IEEE 802.1Q protocol defines a new format of VLAN data frame (Tagged Frame). As the following figure shows, compared to the traditional Ethernet data frame (Untagged Frame), the VLAN data frame (Tagged Frame) adds a VLAN tag.

Figure 1-1 Untagged and Tagged Data Frame

Traditional Ethernet data frame (Untagged Frame)					
Destination Address	Source Address	Length/Type	Data	FCS	
VLAN data fram	e (Tagged Frame	e)			
Destination Address	Source Address	VLAN Tag	Length/Type	Data	FCS

On receiving a tagged frame, the switch checks the VID (VLAN ID) contained in the VLAN tag to determine which VLAN the frame belongs to. On receiving an untagged frame, the

switch will first insert a VLAN tag to the frame, using the PVID (Port VLAN ID) of the port as its VID, and then forward it as a tagged frame.



2 Configuring MTU VLAN

Choose the menu VLAN > MTU VLAN to load the following page.

Figure 2-1 Configuring MTU VLAN

NTU VLAN exames: Chame O Disable		Apply
Current Uplink Port	1	
Scied Upline Part	Pott 1 Pott 2 Pott 3 Pott 4	

Follow these steps to configure MTU VLAN:

1) Select MTU VLAN configuration as **Enable**. Click **Apply**.

MTU VLAN Check the box to enable/disable the MTU VLAN mode. enabled:

2) In the table below, change the uplink port from the list according to your needs. Click **Apply**.

Current Uplink Port	Current Uplink Port of the MTU VLAN.
Select Uplink Port	Select the desired uplink port(s) from the list. The uplink port will build up several VLANs with each of the other ports.

3 Configuring Port-Based VLAN

Choose the menu VLAN > Port-based VLAN to load the following page.

Figure 3-1 Configuring Port-based VLAN

off saser vitan ona	nea 🔅 Enadra	C LIBADIC			In the second
V.44	(† 1. maaint	in configurate a mbe	- 14		(
For	1	3	22	<u>83</u>	100
Realba	7			71.	17
				1004	Deek.
.v. Ab			Verson Pods		
V AN			Verse Boix		

Follow these step to configure port-based VLAN:

1) Select the port-based VLAN configuration as **Enable.** Click **Apply**.

Port-basedCheck the box to enable/disable the Port-based VLAN.VLAN enabled

2) Enter the VLAN ID and select ports to be added to the VLAN. Click **Apply**. To delete the VLAN created, enter the corresponding VLAN ID and click **Delete**.

	VLAN	Enter the ID number of VLAN. It ranges from 1 to 32.
	Port	Displays the port number.
	Member	Click the checkbox to choose one or multiple member ports of the current VLAN. If this field is checked, it indicates the port belongs to the current VLAN.
3)	In the table below	, you can verify the configuration result of the port-based VLAN.

 VLAN
 Displays the ID number of VLAN.

Member Ports Displays the member ports in the VLAN.

Note:

- By default, all the ports are added to VLAN 1.
- Once a port is added to another VLAN, it is deleted from the original VLAN automatically.
- Once a port is removed from all the other VLANs, it is added to VLAN 1 automatically.
- VLAN 1 includes at least one port and cannot be deleted.

4 Configuring 802.1Q VLAN

To complete the 802.1Q configuration, follow these steps:

- 1) Configure the VLAN, including creating a VLAN and adding the ports to the VLAN.
- 2) Configure the PVID.
- 3) Configure the management VLAN.

4.1 Configuring the VLAN

Choose the menu VLAN > 802.1Q VLAN > VLAN Config to load the following page.

Figure 4-1 Configuring 802.1Q VLAN

02 <mark>10</mark> VIAN 60	atalaat 🕴 🗮 Tandaka	Ottotes		Apely	
		Concernance.			
MANU	(1+1034))	CLAS Name	1	800-51-01	1 Delikit
ė	on .	Integrid and	-	Taggeri port	Non member part
See	i Al	E		E	Ξ
F:	8(0		¢.	0
- F-:	1.5	0		0	ă
F-:	÷ ř	0		6	8
E.	14	- 6		0 0 0	0 0 0
Te-4	848	0		0	0

Follow these steps to configure the VLAN:

1) Select the 802.1Q VLAN configuration as Enable. Click Apply.

802.1Q VLAN Check the box to enable/disable the 802.1Q VLAN. enabled

 Enter a VLAN ID and a VLAN name to identify the VLAN. Select the untagged port(s) and the tagged port(s) respectively to be added to the created VLAN based on the network topology. Click Add/Edit. To delete the VLAN created, enter the corresponding VLAN ID and click Delete.

VLAN ID Enter a VLAN ID, which ranges from 1 to 4094.

VLAN Name	Enter a VLAN name to identify the VLAN. The VLAN name only allows numbers, letters and underscores, and should not exceed 10 characters in length.
Untagged / Tagged / Non- member port	Set the port as an untagged port, a tagged port or a non-member port in the VLAN.
	Untagged port : Click the checkbox to configure the egress rule of the traffic on this port as untagged. The switch drops the tag header before sending the packet.
	Tagged port : Click the checkbox to configure the egress rule of the traffic on this port as tagged. The switch adds the tag header before sending the packet.
	Non-member port : Click the checkbox to exclude the port from the current VLAN.

3) In the table below, you can verify the configuration result of the 802.1Q VLAN.

VLAN ID	Displays the ID number of VLAN.
VLAN Name	Displays the user-defined description of the VLAN.
Member Ports	Displays the member ports in the VLAN.
Tagged Ports	Displays the tagged member ports in the VLAN.
Untagged Ports	Displays the untagged member ports in the VLAN.

Note:

- By default, all the ports are added to VLAN 1.
- The port can be removed from VLAN 1 only when the port is also a member of the other VLANs.
- Once a port is removed from all the current VLANs, it is added to VLAN 1 automatically.

• VLAN 1 cannot be deleted.

4.2 Configuring the PVID

Choose the menu VLAN > 802.1Q VLAN > Port Config to load the following page.

Figure 4-2 Configuring 802.1Q PVID

VIAN TRUTH	Comp I Knowperson WLAN	
Fort Comp		
Elžia visverster 🛛 🕇 Etate	Oberre	Alite
002.10 Port Settings		
Tex	1940	ingress checking
P011 P012 P013 P014		1
		(AGR) -
Fog	PWE	inters cacood
Potta	- M	Crobled
Pat 2		Craddel
1913	1	len stated
192.4	(<u>†</u>	E/rabied
Paris		Enabled

Follow these steps to configure the PVID:

1) Select the ports, set the PVID for the ports, and choose from the drop-down list to enable or disable Ingress Checking.

PVID	Enter the default VLAN ID for the port. It can be added to the untagged packets as VLAN ID, and then the port will forward the packets in the corresponding VLAN.
Ingress Checking	Enable or disable Ingress Checking. With this function enabled, the port will accept the packet of which the VLAN ID is in the port's VLAN list and discard others. With this function disabled, the port will forward the packet directly.
Click Apply.	

• You can specify a PVID only when the corresponding VLAN exists.

4.3 Configuring Management VLAN

Choose the menu VLAN > 802.1Q VLAN > Management VLAN to load the following page.

Figure 4-3 Configuring Management VLAN

VLAN Config] Port Config] Management VLAN	0
Management VI AN	
Management VLANI D: (1.4094) Apply	
Current lebragement VLAN ID	
1	

Follow these steps to configure the management VLAN:

1) Specify the management VLAN ID.

Management VLAN ID	Configure specific management VLANs, which should be within the range the configured 802.1Q VLANs. After configuration, only PCs with management VLAN tags can access to the management interface. Multiple management VLAN IDs can be configured.
2) Click Apply .	
Note:	
Only th	e computer in this VLAN can access the management interface of the switch.
 By defa 	ult, the management VLAN ID is 1.

5 Configuration Example for 802.1Q VLAN

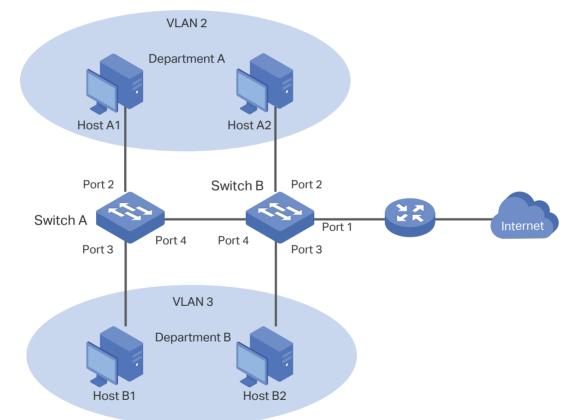
5.1 Network Requirements

As the following figure shows, a company has two departments. Hosts of the same department are located in different places and connected to different switches respectively.

Requirements:

- Hosts of both departments can access the internet.
- Hosts of the same department can communicate with each other, but hosts of different departments cannot.





5.2 Configuration Scheme

To implement the above requirements, configure 802.1Q VLAN on both switches.

 Create VLAN 2. On Switch A, add port 2 and port 4 to VLAN 2, while on Switch B, add port 1, port 2 and port 4 to VLAN 2.

- Create VLAN 3. On Switch A, add port 3 and port 4 of Switch A to VLAN 3, while on Switch B, add port 1, port 3 and port 4 to VLAN 3.
- Configure the default VLAN 1 to make sure the router can communicate with all ports of the two switches.

Table 5-1 and 5-2 show configurations of VLANs on each switch.

Table 5-1Relationships of Ports and VLANs on Switch A and Switch B.

Switch	Ports in VLAN 1	Ports in VLAN 2	Ports in VLAN 3
Switch A	2, 3, 4	2, 4	3, 4
Switch B	1, 2, 3, 4	1, 2 ,4	1, 3, 4

Table 5-2	Set	tings of Egress Rule and PVID or	n Switch A and Switch B	
Switch		Port	Egress Rule	PVID
Switch A		2	Untagged	2
		3	Untagged	3
		4	Tagged	1
Switch B		1	Untagged	1
		2	Untagged	2
		3	Untagged	3
		4	Tagged	1

- Note:

If a port is connected to terminal devices like computers, add the port to the corresponding VLANs as an untagged port, because terminal devices typically do not support VLAN tags.

5.3 Configuration Steps

Demonstrated with a specific model, the following section provides configuration steps. The configuration steps on both switches are similar. Here we take Switch A for example.

 Choose the menu VLAN > 802.1Q VLAN > VLAN Config to load the following page. Select 802.1Q VLAN configuration as Enable. Click Apply.

Figure 5-2 Configuring 802.1Q VLAN

0.10.9549 (1969)	t: Entry	0.00	uetoo	A ANT	
vional (241		terre 1		Detale
Pal		3	Hargest plat	Tagged parts	Non-member part.
Select A			0	0	Ð
,901.1			ö	0	0
Port 2			0	0	0
Pots			R	0.0	. e
Pert 4			0	0	0
*1414					

 Choose the menu VLAN > 802.1Q VLAN > VLAN Config to load the following page and create VLAN 2. Specify VLAN ID as 2, add port 2 to the VLAN as an untagged port, and add port 4 to the VLAN as a tagged port. Click Add/Edit.

Figure 5-3 Creating VLAN 2 and Adding Ports to the VLAN

милано (2000 стакано	V AN HARE MANY	700 50	Dates
Por.	Uninggod po 1	Tegolyal	Homens mixed and
Sec. All	0	Ξ	Ξ
Det 1	0	<	+
Prof 2	*	<	0
15 al 2.	2	6	+
1561.2	Э	*	0
Don F.	5	<	+

3) Choose the menu VLAN > 802.1Q VLAN > VLAN Config to load the following page and create VLAN 3. Specify VLAN ID as 3, add port 3 to the VLAN as an untagged port, and add port 4 to the VLAN as a tagged port. Click Add/Edit.

Figure 5-4 Creating VLAN 3 and Adding Ports to the VLAN

vi vali i k	V AK Barr MARK	ADD 0	Delice
HOP	an agreet part	Laggen pan	HOR THE YOR'S ACT.
Select All			
Poil 4	9	C.	*
Pol.2	9	C.	*
PML3	×	C.	
DW.4	0	×	
Pvt.5	0	<u> </u>	+

 Choose the menu VLAN > 802.1Q VLAN > Port Config to load the following page. Specify the PVID of port 2 as 2 and click Apply. Specify the PVID of port 3 as 3 and click Apply.

Figure 5-5 Configuring 802.1Q PVID

VLAN Central Dent	The state of the s	WINA	
Port Canfig			
NO 10 M AM ENSINE PHONE			10
02 1Q Port Sollings			
Put	PVD.		ingress childreng
Fot 1 Pot 1	4.000		Colorador and Color
[RESULT]	1.1		ENGEN V
			ACC/V
Pat	P/00		hymn Checking
Hod 1			
Port 2	2		Linkber
Peta	a		Enter
Po0 4	1		II/AD/00
Port 5	1		Ecober

6 Appendix: Default Parameters

Default settings of VLAN are listed in the following tables.

Table 6-1 Default Settings of MTU VLAN Configuration

Parameter	Default Setting
MTU VLAN Configuration	Disable

Table 6-2Default Settings of Port Based VLAN Configuration

Parameter	Default Setting
Port Based VLAN Configuration	Enable
VLAN ID	1
VLAN Member Port	1-5

Table 6-3 Default Settings of 802.1Q VLAN Configuration

Parameter	Default Setting
802.1Q VLAN Configuration	Disable

Table 6-4Default Settings of 802.1Q VLAN PVID Configuration

Parameter	Default Setting
PVID	1

 Table 6-5
 Default Settings of 802.1Q VLAN Management VLAN Configuration

Parameter	Default Setting
Management VLAN ID	1

Part 5

Configuring QoS

CHAPTERS

- 1. QoS
- 2. Configuring Basic QoS
- 3. Configuring Rate Limit
- 4. Configuring Storm Control
- 5. Configuration Example for Basic QoS
- 6. Appendix: Default Parameters

QoS

1.1 Overview

With network scale expanding and applications developing, internet traffic is dramatically increased, thus resulting in network congestion, packet drops and long transmission delay. Typically, networks treat all traffic equally on FIFO (First In First Out) delivery basis, but nowadays many special applications like VoD, video conferences, VoIP, etc. require more bandwidth or shorter transmission delay to guarantee the performance.

With QoS (Quality of Service) technology, you can classify and prioritize network traffic to provide differentiated services for certain types of traffic.

1.2 Supported Features

With the QoS feature, You can configure QoS Basic, Rate Limit and Storm Control on the switch to maximize the network performance and bandwidth utilization.

QoS Basic

QoS (Quality of Service) function is used to optimize the network performance. It provides you with network service experience of a better quality. The switch implements three priority modes based on port, 802.1p and DSCP.

Rate Limit

With a limited bandwidth, you can control the traffic rate on each port to ensure network in working order.

Storm Control

Storm Control function allows the switch to monitor broadcast packets, multicast packets and UL-frames (Unknown unicast frames) in the network. If the transmission rate of the packets exceeds the limit, the packets will be automatically discarded to avoid network broadcast storm.

2 Configuring Basic QoS

Configuration Guidelines

Select the QoS mode according to your network requirements. Three QoS modes are supported on the switch: Port-based, 802.1p-based and DSCP-based.

Port-Based

The Port Priority function can classify the packets based on the ports that the packets reach, then map them to different queues.

Based on 802.1p

802.1p gives the Priority field in 802.1Q tag a recommended definition. The tagged packets are mapped to different priority levels based on 802.1Q tag.

Based on DSCP

DSCP gives the IP DSCP field a recommended definition. The IP packets are mapped to different priority levels based on DSCP value.

2.1 Configuring QoS in Port-Based Mode

Choose the menu **QoS > QoS Basic** to load the following page.

```
Figure 2-1 Configuring Basic QoS in Port-Based Mode
```

Global Configuration			
OcS mode.	 Takōnisi 	0.0 met on 002, $\mu=0.0$ met on 0601	
			Avety -

Follow these steps to configure QoS in port-based mode:

1) In the Global Configuration section, select QoS mode as Port-Based. Click Apply.

QoS Mode Selec	t the QoS mode.
----------------	-----------------

2) In the **Based on Port Settings** section, specify the mapping from Port to Priority. Click **Apply**.

Figure 2-2 Configuring Based on Port Settings

Ohoka	Part	Priority
0		
- 11	POT 1	2
- 11	Por 5	2
- 11	HOP 1	2
- 11	POP 4	2
	Pref 2	-
		Apple
hoice	Select the desired port for port priority configuration.	
ort	Displays the physical port number of the switch.	
riority	Specify the priority for the port.	

3) In the **Priority Queue Mapping** section, specify the mapping from Priority to Queue. Click **Apply**.

Charai	enderry	CENN
		<u>01 v</u>
=		- 31
=	I	13
=	7	Q.
-	×	(Ø
-	-	C34
=		194
=	8	(3
-	() () () () () () () () () ()	Qf
		Anaki -

Figure 2-3 Configuring Priority Queue Mapping

Choice	Select the desired priority for queue configuration.
Priority	Displays the priority number.
Queue	Select the queue for the desired priority.

4) In the **Queue Weight Setting** section, specify the mapping from Queue to Weight. Click Apply.

Change -	General Contract of Contract o	Wagat
0		1
11	oc.	1
	or	1
	CC	1
	02	1
	01	1
	08	1
	00	1
11	07	1
		Apply
noice	Select the desired queue for weigl	nt configuration.

Specify the queue weight for the desired queue.

Figure 2-4 Configuring Queue Weight Setting

Weight

2.2 Configuring QoS in 802.1p-Based Mode

Choose the menu QoS > QoS Basic to load the following page.

```
Figure 2-5 Configuring Basic QoS in 802.1p-Based Mode
```

Gobal Conligue	al cas		0
Sione mitocher	Circa nova	Characteristics Characterics	
			Activ

Follow these steps to configure QoS based on 802.1p:

- 1) In the **Global Configuration** section, select QoS mode as **Based on 802.1p.** Click **Apply**.
- 2) In the **Priority Queue Mapping** section, specify the mapping from Priority to Queue. Click **Apply**.

Dance	Proces	Gara
		30 v
11	c	¢1
	4	0
11	:	C2
11	:	0
11	4	C1
11	:	05
11	¢	65
	,	07
		A44.9
noice	Select the desired priority for queue	configuration.
iority	Displays the priority number.	

Figure 2-6 Configuring Priority Queue Mapping

3) In the **Queue Weight Setting** section, specify the mapping from Queue to Weight. Click Apply.

Charles and	Galaxie -	Waght
0		
11	o:	4
	01	4
	02	4
	C2	4
	01	4
	05	4
	00	4
	œ	1
		Appl
noice	Select the desired queue for weight configuration	
leue	Displays the ID number of priority Queue.	

Specify the queue weight for the desired queue.

Figure 2-7 Configuring Queue Weight Setting

2.3 Configuring QoS in DSCP-Based Mode

Choose the menu QoS > QoS Basic to load the following page.

Figure 2-8 Configuring Basic QoS in DSCP-Based Mode

Weight



Follow these steps to configure QoS based on DSCP:

- 1) In the **Global Configuration** section, select QoS mode as **Based on DSCP.** Click **Apply**.
- 2) In the **Based on DSCP Settings** section, specify the mapping from DSCP to Priority. Click **Apply**.

Ohoka	0.907	Frierty
		1 v
11	t	0
11	1	Б
0	2	10
11	2	0
11	4	P.
0	E.	Ð
11	:	0
11	1	D.
0	9	I
11	:	1
11	10	1
		- App

Choice	Select the desired DSCP values for priority configuration.
DSCP	Displays the DSCP values.
Priority	Select the priority for the desired DSCP values.

3) In the **Priority Queue Mapping** section, specify the mapping from Priority to Queue. Click **Apply**.

Figure 2-10	Configuring Priority Queue Mapping

Charae	end my	CLEOP
		<u>01 v</u>
=		(31
=	1	13
-	9	19
-	x	19
-	-	634
=		(¥
-	×	(¥
Ξ	1	

Select the desired priority for queue configuration.

Priority	Displays the priority number.
Queue	Select the queue for the desired priority.

4) In the **Queue Weight Setting** section, specify the mapping from Queue to Weight. Click Apply.

Gaue	Galaxie -	Weight
0		
11	or.	4
	OI .	4
	<u>ac</u>	4
	02	4
	01	4
	08	4
	00	4
	œ	1
		Apply
oice	Select the desired queue for weig	nt configuration.
eue	Displays the ID number of priority	

Specify the queue weight for the desired queue.

Figure 2-11 Configuring Queue Weight Setting

Weight

3 Configuring Rate Limit

Choose the menu **QoS > Rate Limit** to load the following page.

Figure 3-1 Configuring Rate Limit

Fot	Ingress Eale (0-1000000)	Egunas Batin (0-1000000)	
Po11 Po12 Po13 Po14 Po16	[0] Kops	[a Kops	
		Apply	
Pat	ingress Rate	Egress Raie	
Port Port 1	ing tess Rate Disabled	Egress Rale Disabled	
Port 1	Disabled	Disabled	
Part 1 Part 2	Disabled Disabled	Disabled	

Follow these steps to configure rate limit:

1) Select the desired ports and configure the ingress rate and egress rate for the ports.

Ingress Rate (Kbps)	Configure the bandwidth for receiving packets on the port. If the rate for receiving packets on the port exceeds the ingress rate, the packets will be discarded.
Egress Rate (Kbps)	Configure the bandwidth for sending packets on the port. If the rate for sending packets on the port exceeds the egress rate, the packets will be discarded.

2) Click Apply.

Note:

- For a port, the ingress rate control feature and the storm control feature cannot be enabled at the same time. If you enable ingress rate control for a port, storm control will be disabled for that port automatically.
- When egress rate is set for one or more ports, it is recommended to disable the flow control on each port to ensure the switch works normally.
- For ports in the same LAG, rate limit should be configured the same to ensure a successful port aggregation.

4 Configuring Storm Control

Choose the menu **QoS > Storm Control** to load the following page.

Figure 4-1 Configuring Storm Control

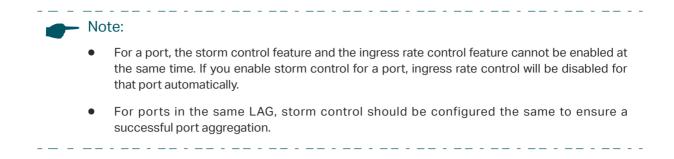
196 —	I héroszí hérest Padrabi		Well and Parsen		Dimensional Pointiels	
	38%6A	Speed Kops w	State .	Speed Knox w	Bitte	Speed Koos
Fot 1 Fot 2 Fot 1 Fot 4 Foto	Not Y		Not v		That v	
						A Aber
72/2	- Incore	un Jacks Facels	Her	vori Parlien	Times	Augy Caul Parkets
Port	disana trans	an Jacob Pacawa opera	iii ra Star	voet Packett	Fenno State	
		sproo		10000		and Parkets
	38726	opeen Ditase	Signe	speec	eure	and Factoria
State 1	sitte Einster	-speed 1 PAges J DRiggs	store Electric	speec Cidens	state Elected	card Partoers option Citigan
Port 1	ol72) Elentier Elentier	speed Skippe DELECT DELECT	SUT: Dirabled Dischal	Speec Status Sidese	State Destan	card Factors openin Didges

Follow these steps to configure storm control:

1) Select the desired ports and configure the upper rate limit for forwarding Unknown unicast packets, multicast packets and broadcast packets

State	Enable or disable storm control on the port.
Speed	Specify the speed for the broadcast threshold, multicast threshold and unknown unicast frames threshold on the desired port.
	kbps: The switch will limit the maximum speed of the specific kinds of traffic in kilo-bits per second.
	pps: The switch will limit the maximum speed of the specific kinds of traffic in packets per second.
Unknown Unicast Packets	Specify the upper rate limit for receiving unknown unicast frames. The traffic exceeding the limit will be processed according to the Action configurations.
Multicast Packets	Specify the upper rate limit for receiving multicast packets. The multicast traffic exceeding the limit will be processed according to the Action configurations.
Broadcast Packets	Specify the upper rate limit for receiving broadcast packets. The broadcast traffic exceeding the limit will be processed according to the Action configurations.

2) Click **Apply**.

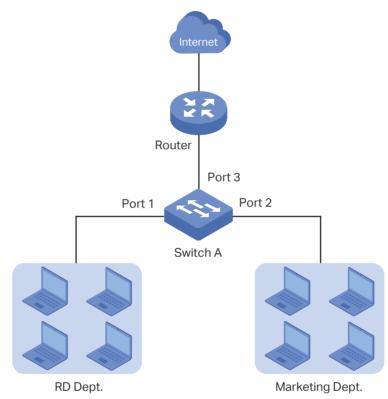


5 Configuration Example for Basic QoS

5.1 Network Requirements

As shown below, both RD department and Marketing department can access the internet. When congestion occurs, the traffic from two departments can both be forwarded and the traffic from the Marketing department should take precedence.

Figure 5-1 Basic QoS Application Topology



5.2 Configuration Scheme

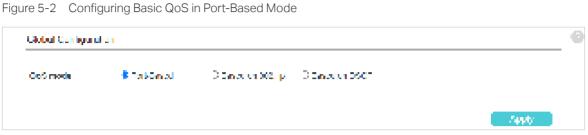
To implement this requirement, you can configure QoS in port-based mode to put the packets from the Marketing department into the queue with the higher weight than the packets from the RD department. Follow these procedures to configure QoS in port-based mode.

- 1) Enable port-based mode.
- 2) Map port 1 and port 2 to different weight.

Demonstrated with a specific model, the following section provides configuration steps.

Configuration Steps 5.3

1) Choose the menu **QoS > QoS Basic** to load the following page. In the **Global** Configuration section, select QoS mode as Port-based. Click Apply.



- 1) In the **Based on Port Settings** section, specify the Priority for Port 1 as 1 and the Priority for Port 2 as 2. Click **Apply**.

Choice	Part	Frienty
Ξ		н -
	POI 1	
	PC1 2	2
	921.0	9
	821.4	9
	82 T S	1

Figure 5-3 Configuring Based on Port Settings

2) In the **Priority Queue Mapping** table, specify the Queue for Priority 1 as Q0 and the Queue for Priority 2 as Q2. Click **Apply**.

Figure 5-4 Configuring Priority Queue Mapping

Character 1	Providy	Speciel 1
		00 ×
	1	21
	1	30
	2	22
	2	25
	1	2
		25
	2	36
	7	27

3) In the **Queue Weight Setting** table, specify the Weight for Queue Q0 as 1 and the Weight for Queue Q2 as 2. Click **Apply**.

Channel	Operation 2	Wight
=		
	30	4
	21	1
	22	1
	35	1
	3	1
	25	1
	36	1
	27	1

Figure 5-5 Configuring Queue Weight Setting

6 Appendix: Default Parameters

Default settings of QoS Basic configuration are listed in the following table.

Table 6-1Default Settings of QoS Basic Configuration

Parameter	Default Setting
QoS Mode	Port-Based

Default settings of Rate Limit configuration are listed in the following table.

 Table 6-2
 Default Settings of Rate Limit Configuration

Parameter	Default Setting
Ingress Rate (Kbps)	Unlimited
Egress Rate (Kbps)	Unlimited

Default settings of Storm Control configuration are listed in the following table.

Table 6-3	Default Settings of Storm C	ontrol Configuration
-----------	-----------------------------	----------------------

Parameter	Default Setting
Status	Disable
Speed	Unlimited

Part 6

Monitoring

CHAPTERS

- 1. Monitoring
- 2. Viewing Traffic Summary
- 3. Configuring Mirroring
- 4. Testing Cables
- 5. Configuring Loop Prevention
- 6. Appendix: Default Parameters

1 Monitoring

1.1 Overview

With the monitoring feature, you can monitor the traffic on the switch.

1.2 Supported Features

Traffic Summary

Traffic Summary displays the traffic information of each port, which facilitates you to monitor the traffic and analyze the network abnormity.

Mirroring

Mirroring refers to the process of forwarding copies of packets from one port to a mirroring port. Usually, the mirroring port is connected to a data diagnose device, which is used to analyze the mirrored packets for monitoring and troubleshooting the network.

Cable Test

Cable Test functions to test the cable connection status, length and error length when the cable is connected to the port of the switch, which facilitates you to locate and diagnose the trouble spot of the network.

Loop Detection

Loop Dectection is used to detect the loop created by a specific port.

2 Viewing Traffic Summary

Choose the menu **Monitoring > Traffic Summary** to load the following page.

Figure 2-1 Viewing Traffic Summary

alle Stemmery				
Auto Herrosti 🛛 🔿 🖬	naliske 💌 Dissatzka			
				Λφρίγ
				🖲 Refecto 🙆 Cle
Port	To bytes	Focioyies	TX prz.	Fectives
Port Port 1	Til bytes 0	Pocityres 0	Tx prz 0	Peoplets D
Port 1	0	0	0	D
Port 1 Port 2	0	0	n a	D

You can choose to enable or disable Auto Refresh and click Apply.

Auto Refresh	With this option enabled, the switch will automatically refresh the traffic summary
	every 10 seconds.

You can view the statistics of each port. You can click **Refresh** to refresh the data and click **Clear** to clear the data.

Port	Displays the port number of the switch.
Tx bytes	Displays the number of octets transmitted on the port. Error packets are counted.
Rx bytes	Displays the number of octets received on the port. Error packets are counted.
Tx pkts	Displays the number of packets transmitted on the port.
Rx pkts	Displays the number of packets received on the port.

– Note:

• Because of the supporting feature of jumbo frame, the frames with more than 15360 bytes can not be forwarded.

3 Configuring Mirroring

Choose the menu **Monitoring > Mirroring** to load the following page.

Figure 3-1 Configuring Mirroring

	ako	Minoring For.
[_nix	shie v	(
Dis	da v	¥
N Fored Port	ingress	Egress
Port 1 Port 2 Port 3 Port 3	Nohle v	Disable v
		Ap
le:	peak	Egreex
0 s	ablod	Disabled
UG	a0100	Disabled
_	abled	Disabled
0.5	aoleo	Liberto
	M Fored Fort Port 2 Port 3 Port 3 Port 4 Ins	Port 1 Port 2 Port 3 Port 3

Follow these steps to configure mirroring:

1) Enable the port mirror feature globally. Specify a mirroring port. Click **Apply**.

Session	Displays the session number.
Status	Select to enable/disable the port mirror feature.
Mirroring Port	Select a port from the drop-down list as the mirroring port.

2) Select one or more mirrored ports, enable or disable the ingress packets and egress packets to be mirrored for the ports. Click **Apply**.

Mirrored Port	Select one or multiple desired port(s) as the mirrored port(s).
Ingress	Select to enable/disable the Ingress feature. When the Ingress is enabled, the incoming packets received by the mirrored port will be copied to the mirroring port.
Egress	Select to enable/disable the Egress feature. When the Egress is enabled, the outgoing packets sent by the mirrored port will be copied to the mirroring port.

3) In the table below, you can verify the configuration result for port mirroring.

*	Note:
	The LAG member ports cannot be set as a mirroring port but a mirrored port.

User Guide

62

4 Testing Cables

Choose the menu **Monitoring > Cable Test** to load the following page.

Figure 4-1 Cable Test

		Twi
Natindas [4 v]		192
C4	(utiv Sialar	(uble Long Britt)
A		
D		
¢	-	
D		

Follow these steps to diagnose the cable:

1) Select a desired port for test. Click **Test** to test cables connected to the selected port.

Port Index Select the port for cable testing.

2) Check the test results in the table.

Pair	Displays the cable pairs.
Cable Status	Displays the cable test results.
Cable Length	If the connection status is Normal, here displays the length of the cable. If the connection status is Close (or Short), Open or Crosstalk, here displays the length from the port to the trouble spot.

Note:

Cable diagnostic is only supported for 1G speed.

5 Configuring Loop Prevention

Choose the menu **Monitoring > Loop Detection** to load the following page.

Figure 5-1 Configuring Loop Prevention

no Evention state [Disable	
Pret	Apply State
-m	Print .
1 2 42	turra.
r=i3	3001a
#±14	LC UT A
-Enti	600731

Follow these steps to configure loop prevention:

1) Enable or disable loop prevention. Click Apply.

Loop prevention Enable or disable the loop prevention feature. state

2) In the table below, you can check the state of each port.

Port	Displays the physical port number of the switch.
State	Displays the port status.

Note:

When a port detects loopback, the port will be automatically blocked.

6 Appendix: Default Parameters

Default settings of Traffic Summary are listed in the following table.

 Table 6-1
 Default Settings of Port Mirror Configuration

Parameter	Default Setting
Auto Refresh	Disable

Default settings of Mirroring are listed in the following table.

Table 6-2Default Settings of Port Mirror Configuration

Parameter	Default Setting
Mirroring Status	Disable
Ingress	Disable
Egress	Disable

Default settings of Cable Test are listed in the following table.

Table 6-3Default Settings of Port Mirror Configuration

Parameter	Default Setting
Port Index	1

Default settings of Loop Prevention are listed in the following table.

Table 6-4Default Settings of Loop Preventikon Configuration

Parameter	Default Setting
Loop prevention state	Disable

Part 7 System Tools

CHAPTERS

- 1. System Tools
- 2. Upgrading the Firmware
- 3. Backing up and Restoring the Switch
- 4. Resetting the Switch
- 5. Rebooting the Switch

1 System Tools

1.1 Overview

In System Tools module, you can upgrade the firmware, back up and restore configuration, reset and reboot the switch.

1.2 Supported Features

System Upgrade

The switch system can be upgraded to get more functions and better performance.

Backup Restore

The switch configuration can be backed up and saved as a file to your computer, and restored later.

System Reset

The switch can be reset to factory settings.

System Reboot

The switch can be manually rebooted.

2 Upgrading the Firmware

Choose the menu **System Tools > System Upgrade** to load the following page.

Figure 2-1 Being Ready to Upgrade the Firmware

System Upgrade		
You will get the new f	and on after uppending the firmware	
Firmware File	There is no life been valided Solitoti Filo	
Firmware Version:	1.0.0 Build 20240428 Ret73184	
Hardware Vaniko	E\$205G-1.0	
Notes		
1. Please wied the pro-	per linnware version multiling with your hardware to upgrade.	
$ 2\rangle$ to evold demograph	ease don't fum of the device while approxing.	
S. Alter opgrading, the	device will rebool automatically.	

Follow these steps to upgrade the firmware:

1) Click **Select File** to load the following page. Specify the firmware file path and select the firmware to upgrade.

Figure 2-2 Browsing the Firmware File

Con.					×
🔶 🚽 Y 🕈 📕 > TheRC	• Cocuments > timesre	v. 0			P
Organize + New Kride				詩: •	. 0
 Calific access CneDirve - Personal Taks PC Network 	ES2066 1.0, 1.0, 1 Baild 2024075 (R.d. 72920, ap. tin				
Rienanie		×	Allow Oues	1 0	-

2) Click Open and the following page will be displayed. Click Upgrade.

Figure 2-3 Upgrading the Firmware



- Note:

- It will take several minutes to upgrade the firmware. Wait without any operation.
- Select the proper software version matching with the hardware to upgrade.
- To avoid damage, do not power down the switch while upgrading the firmware.
- It is recommended to backup the configuration before upgrading.

3 Backing up and Restoring the Switch

With backup and restore, you can:

- Save the current configuration.
- Restore to the previous configuration.

3.1 Saving the Current Configuration

Choose the menu **System Tools > Backup Restore** to load the following page. In the **System Configuration Backup** section, click **Configuration Backup** to save the configuration file to your PC.

Figure 3-1 Backing Up the Configuration

System Configuration	n Beckup	
clics the computation	n backup oution to download the outrent computation.	
it is recommended to	save the current configuration before backing up.	
		Configuration Backup
System Configurati	n Restore	
Select a backup con	puration file and click the restore configuration button, then you	u can restore the switch to its previous configuration
Configuration File:	There is no file been weighter	
		Configuration Restore
Note:		
	everal minutes to save the configuration file.	

3.2 Restoring to the Previous Configuration

Choose the menu **System Tools > Backup Restore** to load the following page.

Figure 3-2 Restoring the Configuration

System Contigura	lion Beckup
crick the computa	tion backup butten to download the current computation.
It is recommended	to save the current configuration before backing up.
	Configuration Backup
System Configure	tion Restore
	tion Restore afgunation file and click the restore configuration button, then you can restore the switch to its previous configuration
	angunation file and click the regions configuration button, then you can restore the switch to its previous configuration

Follow these steps to restore the switch to the previous configuration:

1) In the **System Configuration Restore** section, click **Select File** to load the following page. Specify the configuration file path and select the configuration file.

Figure 3-3 Choosing the Configuration File

C Open				×
	· Documents · hedoay_comig	- <u>L</u>		р 0
Organize . New folger			田• 🖬	0
 Quict secons OneDrive - Perional Tria PC Retwork 	Hana ☐ sysCorrSgBochup dig	Type CRSFIe		
File rames		v Ka Files		2

_ _ _ _ _ _ _ _ _ .

 Click Open and the following page will be displayed. In the System Configuration Restore section, click Configuration Restore to restore the switch to the previous configuration. It will take effect after the switch automatically reboots.

System Configuration Backup	
Click the configuration backup button to download the current configuration	
It is recommended to save the current configuration before backing up.	
Contiguest on the dop	
System Computerion Restore	
Select a backup configuration file and click the restore configuration batters, then you can restore the switch to its provess configuration.	
Configuration File: TrysConfigBeckup.ctg	
Configuration Restore	
 Note:	
• It will take several minutes to restore the configuration. Wait without any operation.	
• To avoid any damage, do not power down the switch while being restored.	

__ . _ _ . _ _ . _ _ . _ _ . _ _ . _ _ . _ _ . _ _

Figure 3-4 Restoring to the Previous Configuration

• After being restored, the current configuration of the switch will be lost.

4 Resetting the Switch

Choose the menu **System Tools > System Reset** to load the following page.

Figure 4-1 Resetting the Switch

Savan Robertay		_
Responsible to taking user applicant responsible sectors.		
	lineer	
d a		

Follow these steps to reset the switch.

1) Click **Reset**, and the following page will pop up.

Figure 4-2 Confirming Reset Operation

ſ	All configurations will be cleared. Confirm submission?	0
	OK Cancel	

2) Click **OK** to reset the switch.

- Note:

- After the switch is reset, it will reboot automatically.
- It will take several minutes to reboot the switch. Wait without any operation while the switch reboots.
- To avoid any damage, do not power down the switch during the reset.

• After the switch is reset, all the settings will be restored to the default.

5 Rebooting the Switch

Choose the menu **System Tools > System Reboot** to load the following page. Click **Reboot**.

Figure 5-1 Rebooting the Switch



• To avoid any damage, do not power down the switch while the switch reboots.

Part 8

Controller Settings

CHAPTERS

- 1. Controller Settings
- 2. Configuring Controller Settings
- 3. Appendix: Default Parameters

1 Controller Settings

1.1 Overview

With the controller settings, you can enable the switch to be discovered and then be managed centrally by the Omada Controller.

1.2 Supported Features

Cloud-Based Controller Management

By enabling Cloud-Based Controller Management, you can configure your switch via the Omada Cloud-Based Controller and enjoy centralized management.

Controller Inform URL

By entering the Inform URL/IP Address of the controller, you can allow the switch to be discovered by the controller via this address.

Address

2 Configuring Controller Settings

Choose the menu **Controller Settings > Controller Settings** to load the following page.

Figure 2-1 Configuring Controller Settings

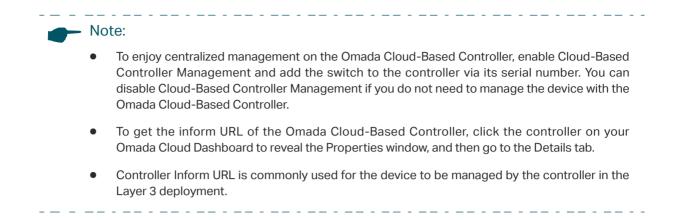
Connocitor: Status,	Disclosed			
Cloud-Based Controller P	Management.	C Eastle	🏶 Dixable	
Noter				
To a close control or a second				
resemble's restrictions arounds	yement en Cimada C	Joud-Rased Controlls	c, enable Cloud-Dased Controller Management and add the device to the controller	1
in social number	•			
ht social number	•		e, enable Cloud-David Controller Management and add the device to the controller with the Orizada Cloud David Controller	la I
in social number	ali yan da nat naadt			1a
Pa social number You can disable this feature	ali yan da nat naadt			la
he sortal number You can disable this feature Controller Inform URL	ali yan da nat naadt			ia
Prisonal number You can disable this feature Controller Inform URL Inform URL (IF Address Notes	Y you do not anot!	ta managorita device		ia

Follow these steps to configure controller settings:

discover the controller.

1) Select Cloud-Based Controller Management as Enable. Click Apply.

Connection Status	Displays the status of the connection between the switch and the Omada Cloud-Based Controller.
	Disabled: Cloud-Based Controller Management is disabled.
	Online : The switch is connected to the Omada Cloud and not managed by the Cloud-Based Controller yet.
	Offline: The switch is not connected to the Omada Cloud.
Cloud-Based Controller Management	Enable or disable Omada Cloud-Based Controller Management. With this feature enabled, the switch can communicate with the Omada Cloud Platform.
2) Specify the in	nform URL or IP address of the controller. Click Apply .
Inform URL/IP	Enter the inform URL or IP address of your controller to tell the switch where to



3 Appendix: Default Parameters

Default settings of Controller Settings are listed in the following table.

Table 3-1Default Settings of Controller Settings

Parameter	Default Setting
Cloud-Based Controller Management	Disable
Inform URL/IP Address	Null

Part 9

Configuring PoE

(Only for Certain Devices)

CHAPTERS

- 1. PoE
- 2. Configuring PoE
- 3. Configuring PoE Auto Recovery
- 4. Configuring Extend Mode
- 5. Appendix: Default Parameters

1.1 Overview

PoF

PoE (Power over Ethernet) is an implementation of power supply of PD (Powered Device) linked to the PoE switch through the RJ-45 port. It is a mechanism which implements power supply and data transmission synchronously.

In PoE module, you can configure basic settings, PoE auto recovery, and extend mode for the PoE ports of the switch.



•

The PoE Config is only available on Easy Managed Switches with PoE ports. For other non-PoE Easy Managed Switches, this feature is not supported.

1.2 Supported Features

ΡοΕ

You can configure the general PoE settings for the switch as well as the PoE parameters for each port.

PoE Auto Recovery

PoE Auto Recovery uses ping packets to detect the link status between PoE ports and connected PoE powered devices (PDs). The switch pings the IP addresses of PDs constantly. If a PD loses connection, the switch will reboot it automatically.

Extend Mode

Extend Mode can increase the transmission distance to support long-distance wiring. When enabled, it extends the maximum transmission distance from 100 m to 250 m but limits the maximum speed to 10 Mbps.

2 Configuring PoE

Choose the menu **PoE > PoE config** to load the following page.

Figure 2-1 Configuring PoE

System Power Limit				System	Power Const	mptio	n	System Power Remain			
	65	w(1.65)		[U V	•			Θ2	w	
											upply -
ort Canlig	J										
Belect Pr	art - DoE St	tatus	PoF Priority	PowerLimit	t (0 1w-30 0w)	Power(w)	Current(mA)	Voltage(v)	PD Class	Power Status
•		•	•								
E Po	d 1 Enab	lod .	1 mw	G	ass 4						OFF
E Po	d 2 Enab	lod	Low	ci	ass 4						OFF
E Po	d S Enab	led	Low.	C	ass 4						OFF
E Po	rt 4 Enab	lod	1 ow	c	ass 4						OFF

Follow these steps to configure PoE:

1) In the **Global Config** section, you can view the current PoE parameters. You can configure the System Power Limit. Click **Apply**.

System Power Limit	Configure the maximum power the PoE switch can supply.
System Power Consumption	Displays the real-time system power consumption of the PoE switch.
System Power Remain	Displays the real-time system remaining power of the PoE switch.

2) In the **Port Config** section, select the ports you want to configure and specify the parameters. Click **Apply**.

PoE Status	Enable or disable the PoE function on corresponding ports. A port can supply power to the PD when its status is enable.
PoE Priority	Select the priority level (High, Middle, Low) for the corresponding port. When the supply power exceeds the system power limit, the switch will power off PDs on low-priority ports to ensure stable running of other PDs.
Power Limit (0.1 w-30 w)	Specify the maximum power the corresponding port can supply. The following options are provided:
	Class 1 : The maximum power that the port can supply is 4 W.
	Class 2 : The maximum power that the port can supply is 7 W.
	Class 3 : The maximum power that the port can supply is 15.4 W.
	Class 4 : The maximum power that the port can supply is 30 W.
	Manual: You can enter a value manually.
Power (w)	Displays the real-time power supply of the port.
Current (mA)	Displays the real-time current of the port.
Voltage (v)	Displays the real-time voltage of the port.
PD Class	Displays the class which the linked PD belongs to.
Power Status	Displays the real-time power status of the port.

3 Configuring PoE Auto Recovery

Choose the menu **PoE > PoE Auto Recovery** to load the following page.

Figure 3-1 Configuring PoE Auto Recovery

Pol: 7	ulo Rec	overy. O i	Enable 🏽 🕷 D	Isable						Anniha
Defore Ping IP It is rec operfix	upgradir Addreso commente default \	g the connecter schoold match (d, some problems in d PoL powered devi the connected PD/s the switch and its o tis the PVID)	ice (PD), disable IP address: Othe	Pal. Auto Recov ancies, the awitch	ery on the corresp will continuely a	ponding por doort the Pf	t to avoid P D	U's dama	
orl Co										
al Go doct	Port	Ping IP Address	Startup Dolay (Seconds)	Interval (Seconds)	Falure Threshold	Broak Time (Seconds)	Failures	Reboots	Total Pings	Stahis
daat III	Port		(Seclands) ((30 600)	(Seconds) (10 120)	Threshold (1.10)	(Seconds) (0.120)			Pings	[
tale	-		(Seconds)	(Seconds)	Threshold	(Seconds)	Falluros 0	Reboots		Stahis
diast	Port 1		(Seconds) (30 600) 60	(Seconds) (10 120) 60	Threshold (1.10) 5	(Seconds) (0 120) 15	a	0	Pings 0	Status [Disabled
	Port 1 Port 2		(Seconds) (30 600) 60 60	(Seconds) (10 120) 60 60	Threshold (1.10) 5 5	(Seconds) (3 120) 15 15	0	0	Pings 0 0	Status Disabled

PoE Auto Recovery Enable or disable PoE Auto Recovery globally.

- Note:

When PoE Auto Recovery enabled, some problems may occur in case of specific application scenarios or improper configurations.

_ __ .

- Before upgrading the connected PoE powered device (PD), disable PoE Auto Recovery on the corresponding port to avoid PD's damage.
- It is recommended to configure the switch and its connected PDs to the same subnet, and when 802.1Q VLAN enabled, the connected PD should be in the port's default VLAN (whose ID is the PVID). For detailed configurations, refer to *Configuring 802.1Q VLAN*.

2) In the **Port Config** section, select the desired ports and specify the parameters. Click **Apply**.

Auto Refresh	When Auto Refresh is enabled, the switch refreshes the data every 5 seconds so you can get the real-time ping statistics.
Ping IP Address	Enter the IP address of the PD connected to the port.
	Ping IP Address should be the same as the connected PD's IP address. Otherwise, the switch will continually reboot the PD.
Startup Delay	Specify how long the switch waits for the connected PD's rebooting before the switch starts to ping the PD's IP address. It ranges from 30 to 600 seconds.
Interval	Specify the interval between two consecutive ping packets. It ranges from 10 to 120 seconds.
Failure Threshold	Specify the threshold for ping failures.
	If the switch fails to get the ping response from the PD on the port, the switch will retry until the number of ping failures reaches the threshold, and then the switch will reboot the PD. It ranges from 1 to 10.
Break Time	Specify how soon the switch reboots the PD after the number of ping failures reaches the threshold. It ranges from 3 to 120 seconds.
Failures	Display the number of ping failures since the latest reboot of the PD. It will be reset when the PD responds to the ping packet or is rebooted.
Reboots	Display the number of PD's reboots. It will be reset after reaching 9,999 or when the switch is rebooted.
Total Pings	Display the total number of ping packets that the switch sends to the connected PD. It will be reset after reaching 9,999 or when the switch is rebooted.
Status	Enable or disable PoE Auto Recovery on the desired ports. To make it enabled, enable PoE Auto Recovery both globally and on the port.

4 Configuring Extend Mode

Choose the menu **PoE > Extend Mode** to load the following page.

Figure 4-1 Configuring Extend Mode

	Port	Extend Mode
		v
11	Port 1	Disabled
11	Port 2	Disabled
11	Port 3	Disabled
1.1	Port 4	Disabled

Follow these steps to enable Extend Mode and configure the parameters:

1) In the **Extend Mode Config** section, select the desired ports and choose from the dropdown list to enable or disable **Extend Mode**.

Extend Mode Select to enable/disable Extend Mode on the desired port.

2) Click **Apply**.

5 Appendix: Default Parameters

Default settings of PoE are listed in the following table.

Table 5-1 Default Settings of PoE

Parameter	Default Setting
Global Config	
System Power Limit	65 W
Port Config	
PoE Status	Enabled
PoE Priority	Low
Power Limit	Class 4

Default settings of PoE Auto Recovery are listed in the following table.

Table 5-2Default Settings of PoE Auto Recovery

Parameter	Default Setting
Global Config	
PoE Auto Recovery	Disabled
Port Config	
Ping IP Address	Null
Startup Delay	60 seconds
Interval	60 seconds
Failure Threshold	5
Break Time	15 seconds
Status	Disabled

Default settings of Extend Mode are listed in the following table.

Table 5-3Default Settings of Extend Mode

Parameter	Default Setting
Extend Mode	Disabled

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. **P**tp-link is a registered trademark of TP-Link Technologies Co., Ltd. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2024 TP-Link Technologies Co., Ltd. All rights reserved.

https://www.tp-link.com