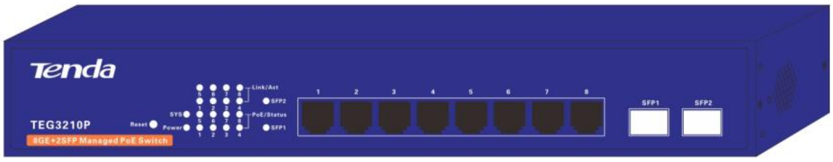
Tenda

User Guide



8GE+2SFP Managed PoE Switch

Model No.: TEG3210P

Copyright Statement

Tenda is the registered trademark of Shenzhen Tenda Technology Co., Ltd. All the products and product names mentioned herein are the trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Shenzhen Tenda Technology Co., Ltd. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of Shenzhen Tenda Technology Co., Ltd. If you would like to know more about our product information, please visit our website at http://www.tendacn.com.

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, Tenda reserves the right to make changes to the products without obligation to notify any person or organization of such revisions or changes. Tenda does not assume any liability that may occur due to the use or application of the product described herein. 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.

Preface

Thank you for choosing Tenda! Reading this manual will be helpful for you to configure this device.

Convention

If not specifically indicated, the switch, this product or this device mentioned in this Install Guide stands for Tenda 8GE+2SFP Managed PoE Switch TEG3210P.

Symbols in this Install Guide:

Symbol	Meaning
⚠ **Note**	Ignoring this type of note may result in a malfunction or damage to this device.
💡 **Tip**	This format is used to highlight a procedure that will save time or resources.

Overview of this Install Guide

Chapter	Description
Chapter I Product Overview	Introduction to this switch's package contents, physical appearance and features
Chapter II Installation	Introduction to this switch's installation considerations and installation procedures
Chapter III Device Management Introduction	Introduction to how to manage the switch via Web manager and fundamental operations about Web manager
Chapter IV Advanced Settings	Introduction to how to configure functions of the switch
Chapter V Appendix	Introduction to technical specifications, default settings and safety statement of the switch

Technical Support

Website: http://www.tendacn.com

Telephone: (86 755) 2765 7180

Email: support@tenda.com.cn

Contents

Contents

Chapter 1

Product Overview

Package Contents

Open the package and verify the following items:

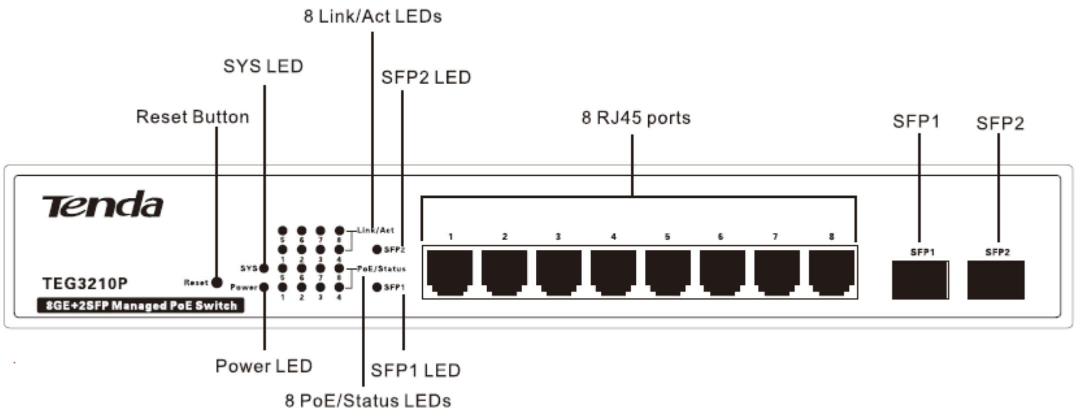
- Switch *1
- Power Cord *1
- L-shaped Bracket *2
- Screw *6
- Footpad *4
- Install Guide *1

If any item is missing or damaged, contact the place of purchase immediately.

Physical Appearance

1 Front Panel

The following parts are located on the front panel shown as below.



➘ Reset Button

With the switch powered on, pressing the Reset button for at least 5 seconds and then releasing it restore the switch to factory default settings. The switch will reboot automatically after reset and this process takes about 45 seconds.

While rebooting, following phenomena will occur: All LEDs light up→SYS LED is off→All LEDs are off except the Power LED→SYS is on and blinking.

➘ LEDs

The following table describes the LED designations：

LED	Status	Description
Power	Solid	Proper connection to power supply
	Off	Improper connection to power supply or malfunction occurs.
SYS	Blinking	The system is functioning properly.
	Solid	The system is functioning improperly.

	Off	The system is still rebooting.
Link/Act	Solid	A valid link is established on the corresponding RJ45 port.
	Blinking	Data transmission is occurring on the corresponding RJ45 port.
	Off	No link is established on the corresponding RJ45 port.
PoE/Status	Solid	The PoE powered device (PD) is connected on the corresponding RJ45 port and the port is supplying power successfully.
	Off	No PoE powered device (PD) connected.
SFP1&SFP2	Solid	A valid link is established or data transmission on the corresponding SFP port.
	Off	No link is established on the corresponding SFP port.

➘ RJ45 Ports

This switch comes with 8 10/100/1000Mbps auto-negotiation RJ45 ports. Each port has a corresponding Link/Act LED. Speeds and corresponding working modes of all RJ45 ports are described in the following table.

Speed	**Working Mode**
10Mbps (auto-negotiation)	Half/Full duplex auto-negotiation
100Mbps (auto-negotiation)	Half/Full duplex auto-negotiation
1000Mbps (auto-negotiation)	Full duplex auto-negotiation

All RJ45 ports are PoE-capable, and can connect up to 8 IEEE 802.3af-compliant PDs (15.4W for each) or 4 IEEE 802.3at-compliant PDs (30W for each).

Tip:

As pair 1, 2 and pair 3, 6 are applying PoE power supply, it is advisable to use cat 5 or higher UTP/STP cables. Note that Ethernet specifications limit the cable length between the switch and the attached device to 100 m (328 ft).

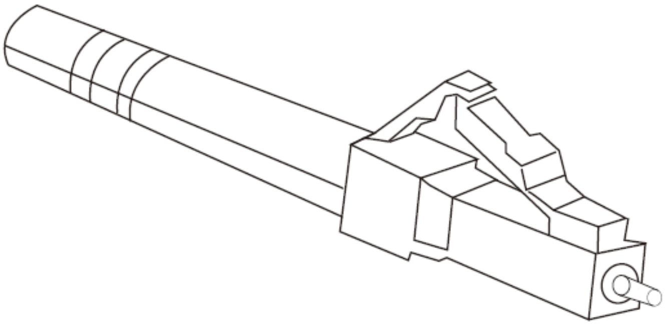
SFP Ports

This switch comes with 2 1000Mbps SFP fiber ports, accommodating a standard SFP fiber module.

SFP (Small Form-factor Pluggable）is a compact, hot-pluggable transceiver mainly used for implementing the switchover between fiber and electricity signals, including fiber rate control, modulation sending, signal detection, IV transformation and amplifier limiting judgment regeneration.

An optical fiber connector terminates the end of an optical fiber. The optical fiber connector (known as union), an indispensable passive device in optical fiber communication, is mainly used for detachable optical fiber connection, which is not only convenient for commissioning test and maintenance of the optical fiber system, but makes this system’s switch-over and scheduling more flexible.

TEG3210P only supports LC optical fiber connector as shown below:

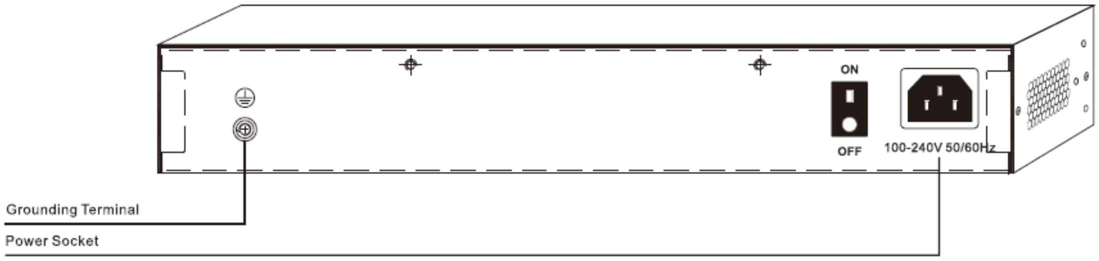


Tip:

The optical fiber module or photoelectric converter is not included in the package and you need to prepare it by yourself.

2 Back Panel

The following parts are located o[n the back panel as shown below:



➘ Power ON/OFF

Used for controlling power supply of this device.

➘ Grounding Terminal

Used for connecting the protective grounding cable for inductive lightning protection. As for the method of connecting protective grounding cable, please refer to Connect to Protective Grounding Cable.

➘ Power Socket

Used for connecting the included power cord for power supply.

Chapter II

Installation

1 Installation Considerations

To avoid any equipment damage or bodily injury caused by improper use, read the following safety recommendations before installing the switch. Note that the recommendations do not cover every possible hazardous condition.

➘ Safety Caution

- Do wear anti-static wrist straps and disable the power supply of this device while installing this device;
- Use the included power cord for power supply;
- Ensure operating power supply accords with rated input standard;
- Ensure ventilation holes of the switch are in good condition;
- Do not open or remove the housing of the switch;
- Do disconnect power supply while cleaning the switch and do not use any liquid to clean the switch;
- It's suggested to ground the switch to avoid strong inductive lightning. Keep the switch away from power lines, electric lights or strong power grid or anywhere the power grid with strong current is reachable, all for better performance.

Note:

There is a Tenda seal on one of the screws. You should keep the seal unbroken before the technical staff maintains your switch. You cannot open the housing of the device unless you get the local reseller’s permission, or you have to be responsible for the result that the device cannot be maintained because of unpermitted operation.

➘ Site Requirements

1. Temperature & Humidity

Environment	Temperature	Humidity
Operating	-10ºC ~ 45ºC	10% ~ 90%RH (non-condensing)
Storage	-40℃ ~ 70℃	5%~90% RH (non-condensing)

2. Cleanliness Requirements

In case that static electricity affects this device’s normal operation, please observe following guidelines:

- Keep indoor environment clean and dust the switch regularly;
- Keep the switch well-grounded for electrostatic transferring.

3．Inductive Lightning Protection

In case that strong current does damage to the switch due to inductive lightning, verify that:

- Power socket, rack, work bench and the grounding terminal of the switch are well-grounded;
- The switch is cabled properly. When the switch is cabled outdoors, it is advisable to use it together with the signal lightning arrester.

4. Installation Site Requirements

Whether install the switch in a rack or on a flat work bench, please verify:

- The rack or work bench is stable and sturdy enough;
- The switch should be clean and well ventilated. There is at least 10 centimeters free on all sides for cooling;
- No articles, especially heavy articles, are placed on the switch;
- There is more than 1.5 centimeters vertical distance free between devices that stack up.

2 Tools

Before installing the switch, prepare the following tools:

Antistatic Gloves	Phillips Screwdriver	Ethernet Cable

3 Installation

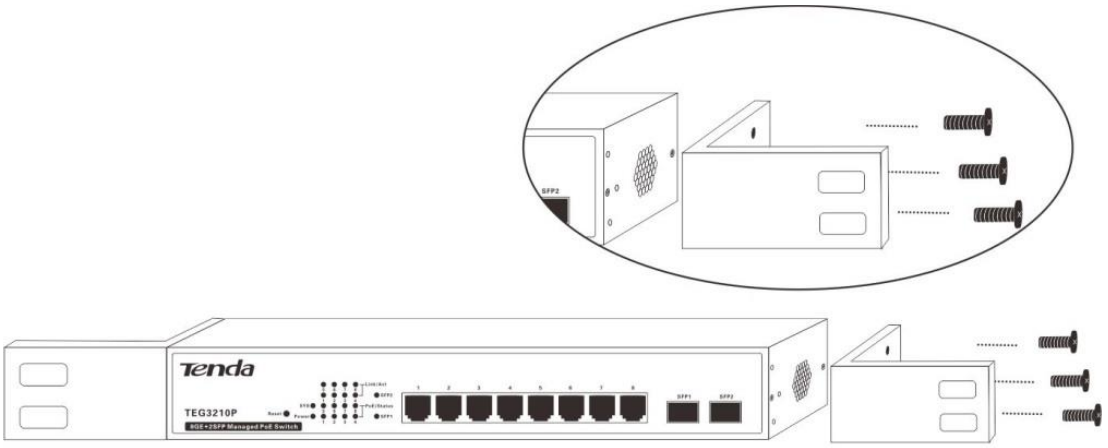
The switch can be installed either in a rack or on a desktop. You can choose the more suitable one as you need.

A. Mount the switch in a rack

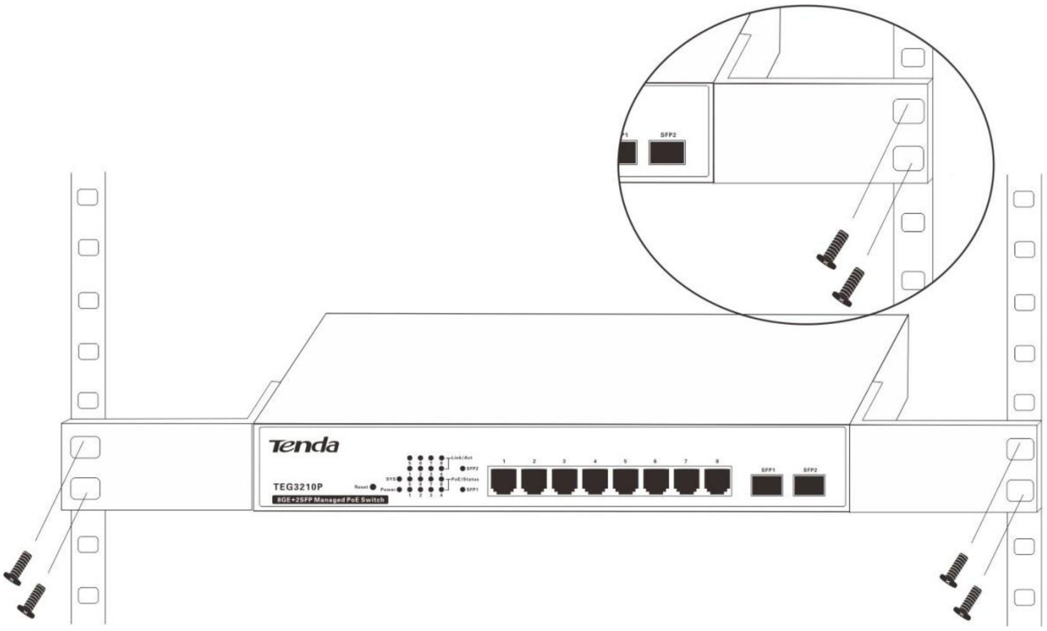
With the included L-shaped brackets and screws, you can install it in a 19-inch standard rack.

Step 1: Make sure the rack is well-earthed and stable;

Step 2: Attach the included mounting brackets to the two sides of the switch with the included screws;



Step 3: Insert screws (prepared by yourself) through each bracket and into the rack to securely fix the switch onto the rack.

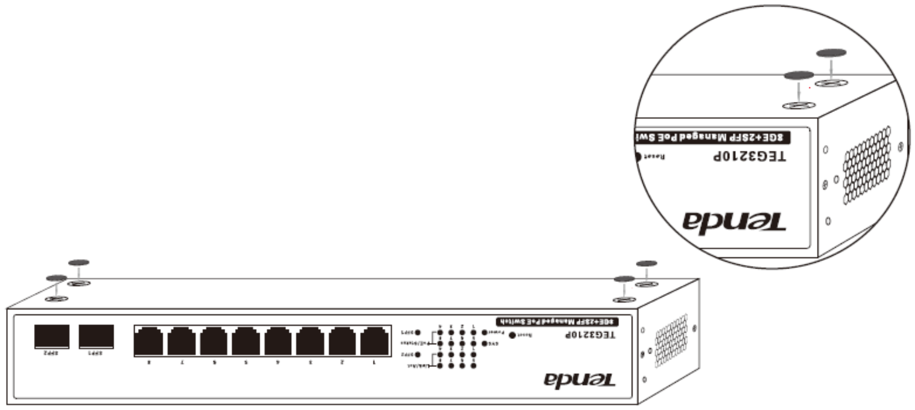


B. Mount the switch on a desktop

Without a 19-inch standard rack, you can install the switch on a desktop.

Step 1: Place the switch bottom up on a flat desktop;

Step 2: Attach four footpads to the corresponding circular grooves on the bottom of the switch;



Step 3: Place the switch face up on the desktop.

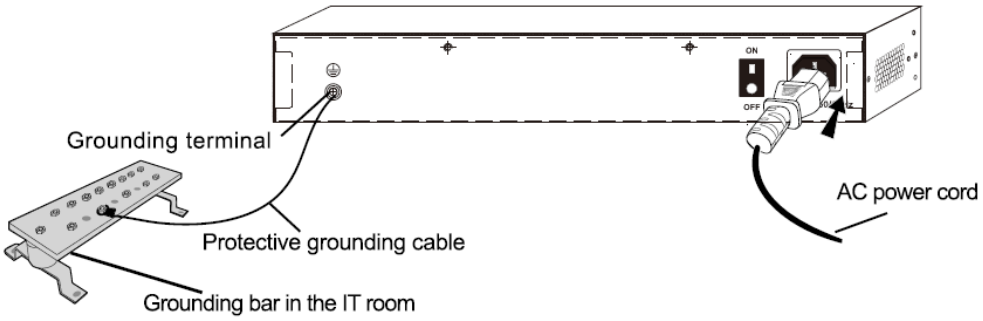
4 Connect to Protective Grounding Cable

Proper connection of protective grounding cable is not only important for inductive lightning protection and anti-interference, but for your own personal safety. Please select the most suitable method to connect protective grounding cable according to your installation environment.

A. With grounding bar

Step 1: Connect one end of the protective grounding cable to the binding post on the grounding bar.

Step 2: Connect the other end of the protective grounding cable to the grounding terminal and fix the screws.



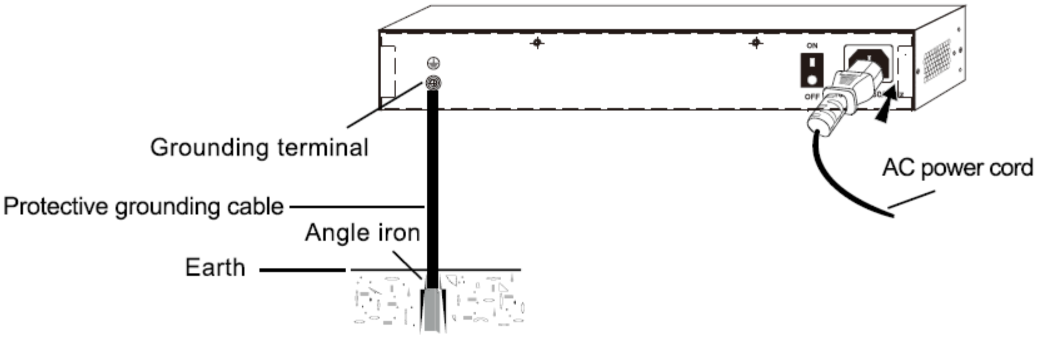
B. Without grounding bar

With mud land nearby and allowed to bury grounding bar, follow below steps:

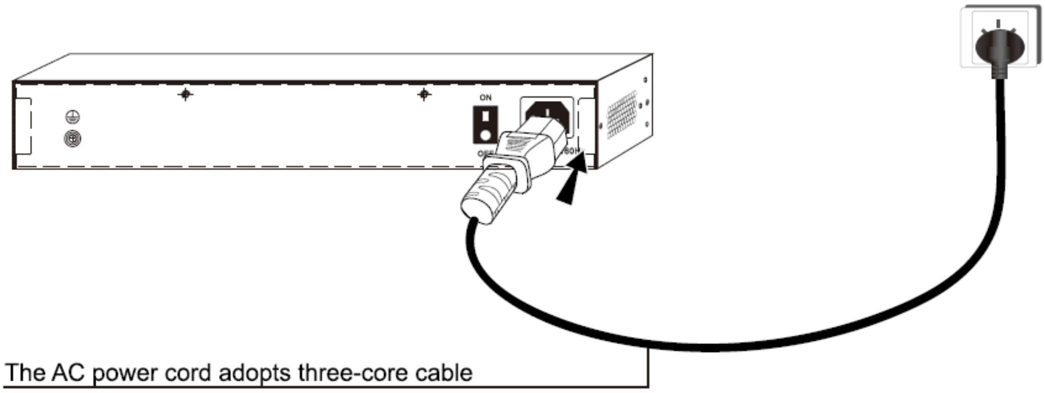
Step 1: Bury an angle iron or steel pipe (≥0.5m) into the mud land;

Step 2: Weld one end of the protective grounding cable to the angle iron or steel pipe and embalm the welding point;

Step 3: Connect the other end of the protective grounding cable to the grounding terminal.

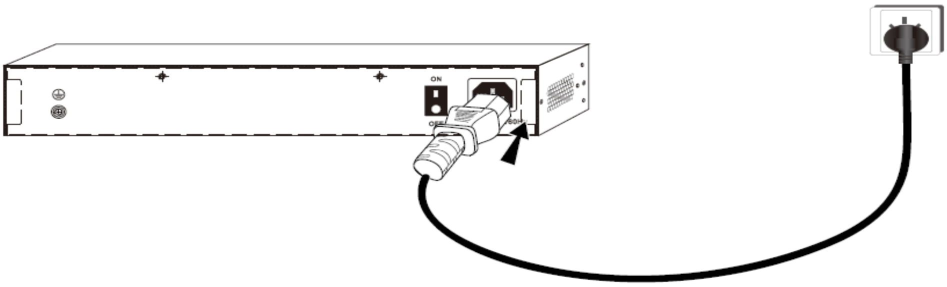


If not allowed to bury the grounding bar, you can connect it to ground through the three-core PE cable of the AC power socket on the precondition that the PE cable in the switchgear room or beside the AC power supply transformer is well-grounded.



5 Connect to Power Supply

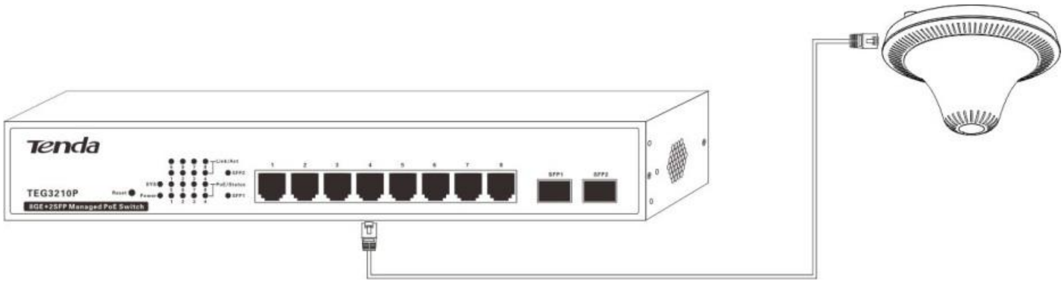
Please use the included power cord for power supply.



6 Cable Connection

➘ Connect to RJ45 Ports

Connect the switch to remote Ethernet devices with Ethernet cables.

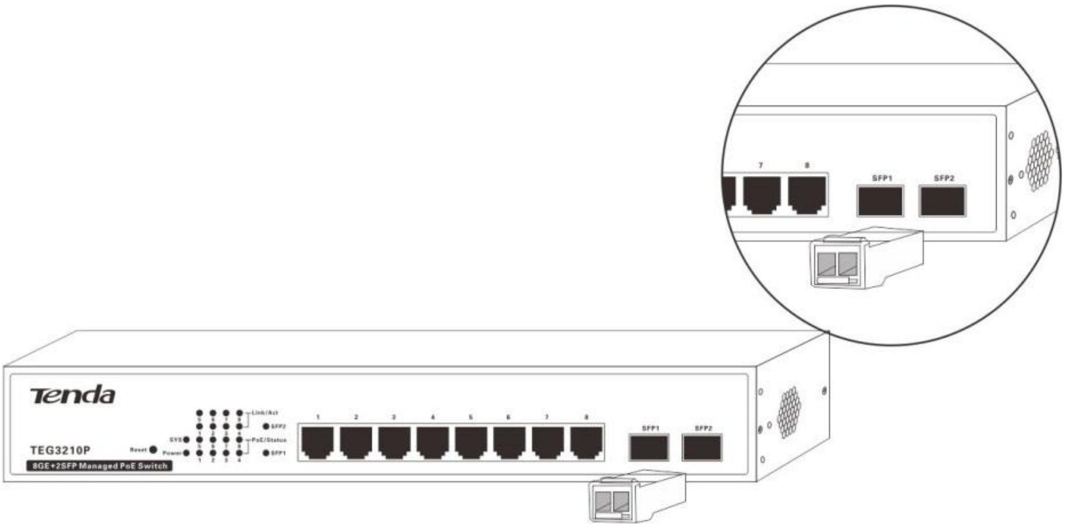


Tip:

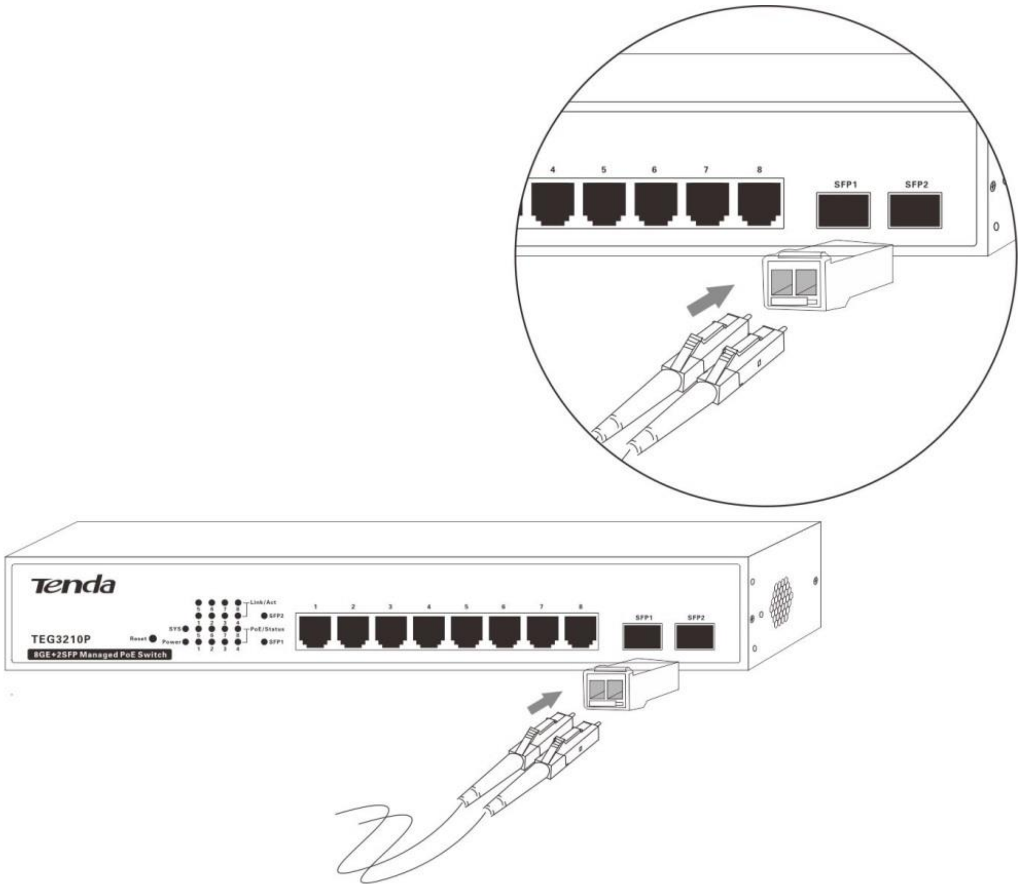
All RJ45 ports of the switch are Auto MDI/MDIX-capable, which allows you to attach devices using twisted pair category 5 or higher, either straight-through or crossover cables.

➘ Connect to SFP Fiber Ports

Step 1: Insert the SFP module into the SFP module bay.

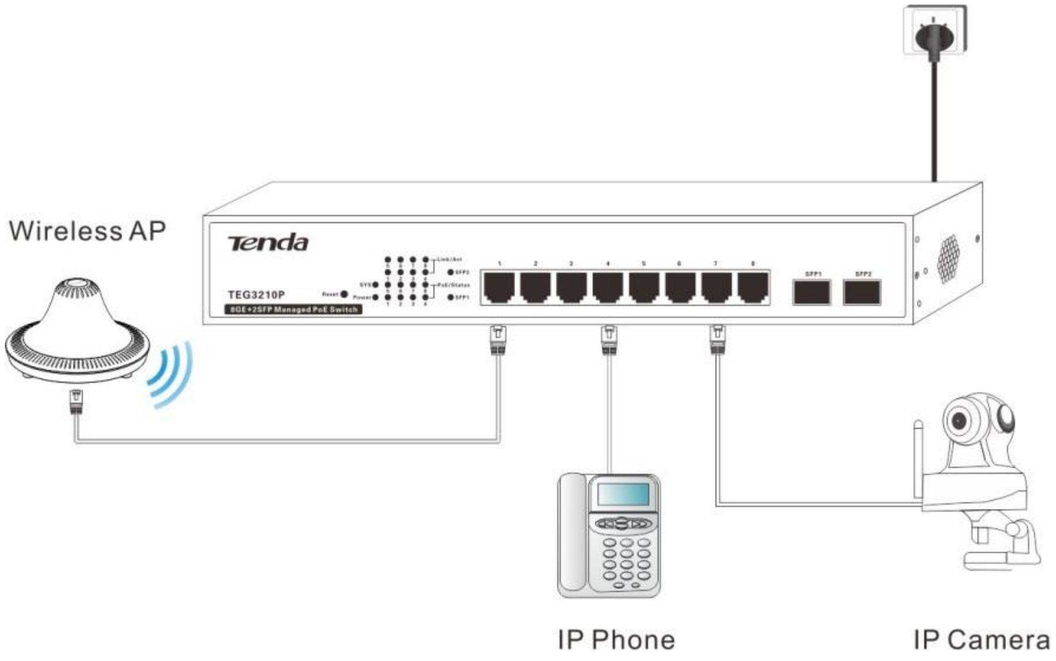


Step 2: Insert the LC optical fiber connector of the fiber into the SFP module.



➘ Connect to PDs

The PoE power supply feature on all RJ45 ports is enabled by default. You can connect IEEE 802.3at-/802.3af-compliant APs, IP telephones, IP cameras or other powered devices to the switch.



Tip:

The PoE power supply mode is dynamic, i.e. the switch accommodates power supply for powered devices automatically.

7 Power up the Device

Check the device thoroughly before powering up the device.

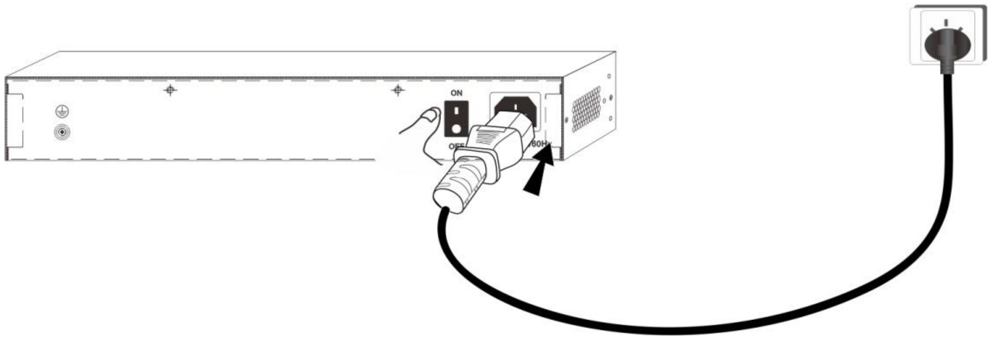
7.1 Check the Device

Before applying power supply, perform the following:

- The operating power supply should accord with rated input standard;
- The power cord and grounding cable is correctly connected;
- All cable connections (RJ45 ports, SFP ports) are correct.
- If cabling outside, ensure the Ethernet port lightning arrester and AC power source lightning arrester are connected.

7.2 Power up the Device

Step 1: Turn on the power switch (Power ON/OFF) on the back panel to power up the switch.



Step 2: After being powered on, the switch will be initialized automatically. Please ensure that following phenomena will occur to LEDs one by one:

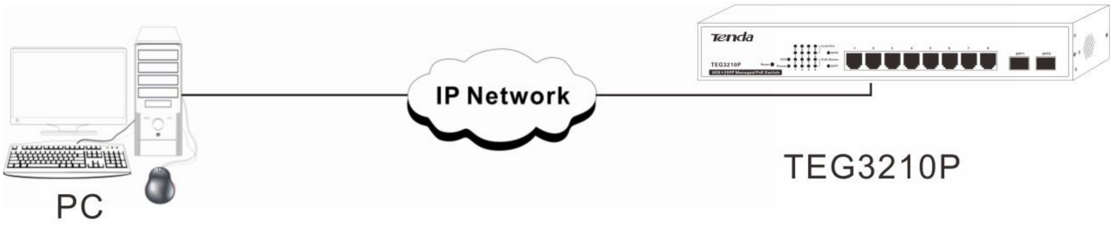
- All LEDs (Power, SYS, PoE/Status, Link/Act, SFP1, SFP2) will light up for self-checking.
- SYS LED is off.
- All LEDs are off except the Power LED.
- After restart, the Power LED lights up, SYS LED is blinking, corresponding Link/Act LED or SFP1/SFP2 LED is on or blinking and corresponding PoE/Status LED lights up.

Chapter III

Device Management Introduction

1 Web Administration

This switch comes with the web administration feature, which helps you manage and maintain this switch intuitively via its web browser-accessible administrator page. The network topology of application scenario is shown below:



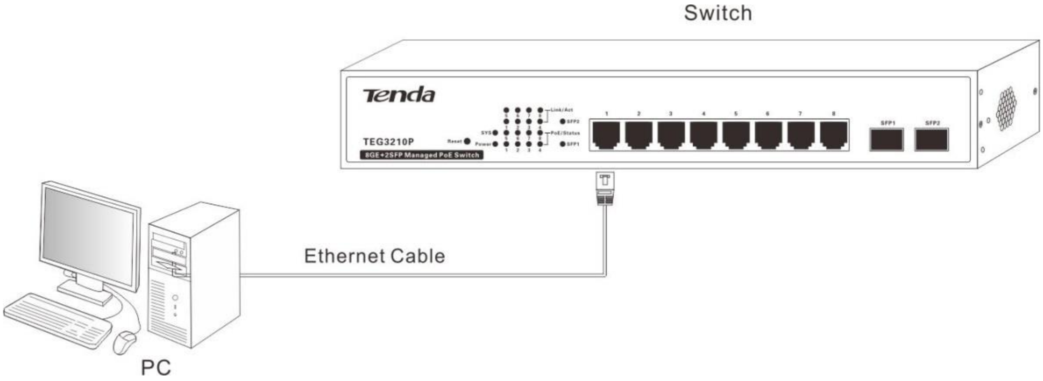
2 Web Login

The first time you use this device, you can log in to its web browser-accessible administrator page with following default login info.

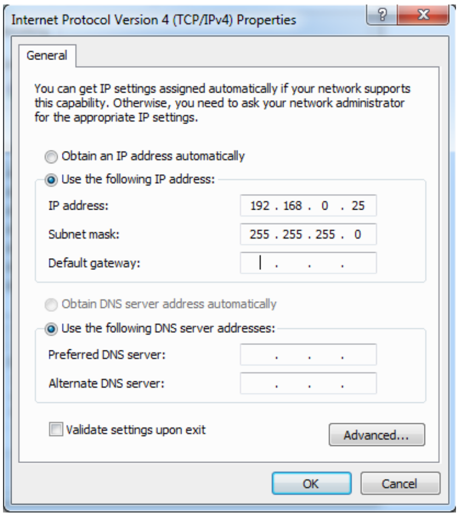
Login Info	Default Settings
User Name	admin
Password	admin
IP Address	192.168.0.1

Web Login:

1. Connect the PC to an RJ45 port of the switch using an Ethernet cable.



2. Configure your PC's IP, which should be in the same network segment but be different from the switch's management IP. The default management IP of the switch is 192.168.0.1, so you can set your PC's IP to **Use the following IP address**: IP address: 192.168.0.X (where X can be any number between 2 and 254); subnet mask: 255.255.255.0.



Internal Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 25

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

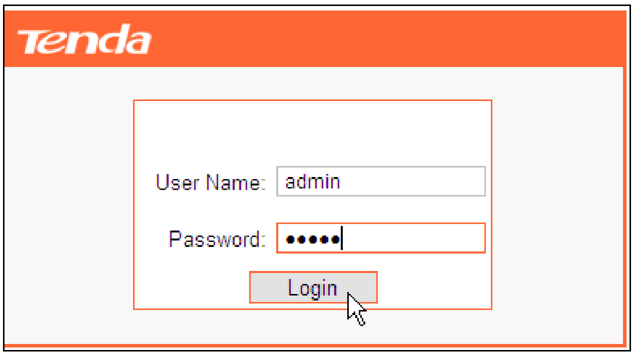
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

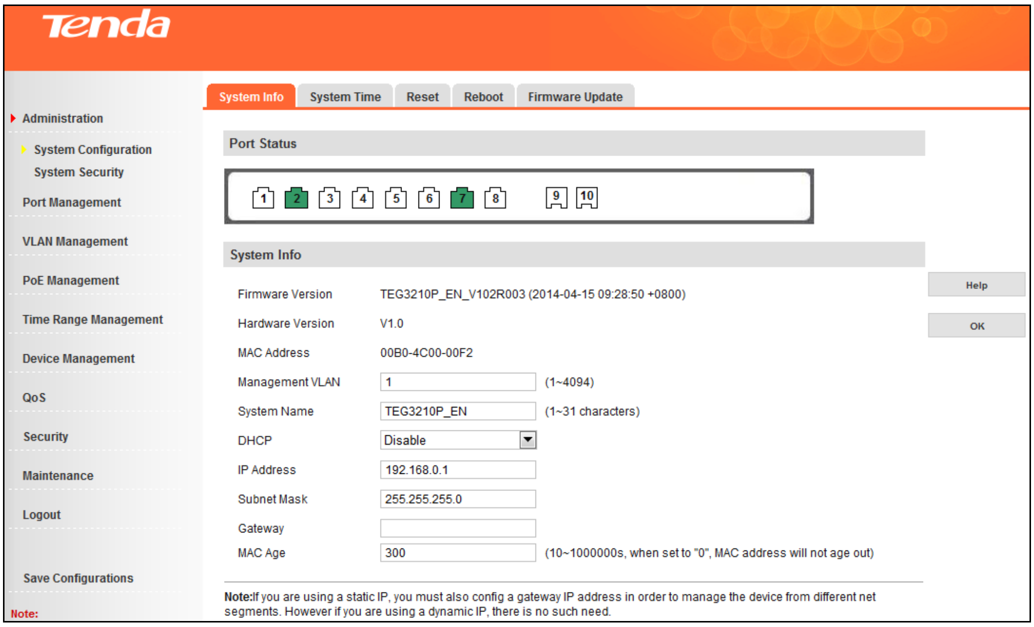
3. Launch a web browser, input 192.168.0.1 in the address bar and press **Enter**.
4. Enter the default user name admin and default password admin, and click **Login**.



User Name: admin

Password: •••••

5. Then you can go to the web browser-accessible administrator page to view or modify the switch's configuration info.



System Info

Firmware Version TEG3210P_EN_V102R003 (2014-04-15 09:28:50 +0800)

Hardware Version V1.0

MAC Address 00B0-4C00-00F2

Management VLAN 1 (1~4094)

System Name TEG3210P_EN (1~31 characters)

DHCP Disable

IP Address 192.168.0.1

Subnet Mask 255.255.255.0

Gateway

MAC Age 300 (10~1000000s, when set to "0", MAC address will not age out)

Note: If you are using a static IP, you must also config a gateway IP address in order to manage the device from different net segments. However if you are using a dynamic IP, there is no such need.

3 Web Logout

Directly closing your web browser or clicking **Logout** exits the web browser-accessible administrator page. Configurations won't be saved automatically while logging out. Thus it is advisable to save your configurations manually before logout.

Note:

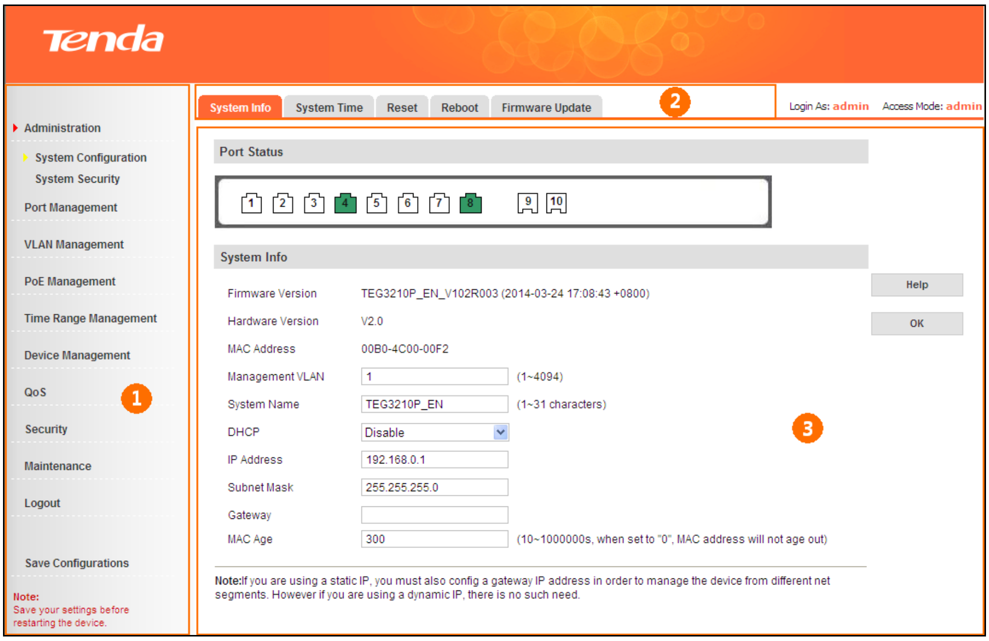
Closing the web browser tab won't log out automatically.

4 Layout of Web Browser-Accessible Administrator Page

The Web browser-accessible administrator page can be divided into two parts: navigation bar and the configuration section.

Note:

- Only web administration features that the switch supports will be displayed on navigation bars. Specifically, please refer to the actual software of your switch.
- If features or parameters on the web browser-accessible administration page display grey, they are not configurable.



Login As: admin Access Mode: admin

Firmware Version TEG3210P_EN_V102R003 (2014-03-24 17:08:43 +0800)
Hardware Version V2.0
MAC Address 00B0-4C00-00F2
Management VLAN 1 (1~4094)
System Name TEG3210P_EN (1~31 characters)
DHCP Disable
IP Address 192.168.0.1
Subnet Mask 255.255.255.0
Gateway
MAC Age 300 (10~1000000s, when set to "0", MAC address will not age out)

Note: If you are using a static IP, you must also config a gateway IP address in order to manage the device from different net segments. However if you are using a dynamic IP, there is no such need.

Note:
Save your settings before restarting the device.

Sequence Number	Name	Description
1	Primary & Secondary	The navigation bar presents web administration functions to you in the form of navigation tree. This

	Navigation Bar	section allows you to select function menus here.
②	Three-stage Navigation Bar	
③	Configuration Section	This section allows you to configure and view settings here.

5 Commonly Used Elements on Web Browser-Accessible Administrator Page

Port Graphical Status Overview:

Commonly Used Elements	Description
□	Indicates this is an RJ45 port.
□	Indicates this is an SFP port.
🟩 🟩	Indicates a link has been established on this port.
□ □	Indicates this port can be chosen and configured.
🟦 🟦	Indicates this port has been chosen.
▒ ▒	Indicates this port cannot be chosen and configured.

Commonly Used Buttons:

Commonly Used Elements	Description
Refresh	Used for refreshing displayed contents on the current page.
Add	Used for adding a new rule.
New	Used for adding a new rule.
Config	Used for batch configuring a certain function’s settings

Back	Used for cancel your settings on the current page and go back to the previous page.
Delete All	Used for deleting all rules on the page.
Batch Delete	Used for deleting selected rules on the page.
View	Used for looking up rules which match the search criteria.
Clear	Used for clearing all statistics on the current page.
Download	Used for exporting logging files for the switch.
Reset...	Used for restoring all configurations of the switch to factory default values.
Reboot...	Used for restarting the switch.
Help	Click it to acquire more help information.
OK	Used for saving configurations on the page. Once the switch reboots, configurations saved by merely clicking this button will be lost.
Save...	Used for saving all configurations for the switch. When the switch reboots, configurations saved by clicking this button won't be lost.
Backup...	Used for exporting configurations for the switch and saving these configurations to the local computer.
Restore...	Used for restoring configurations, which have been exported, to the switch.
Update	Used for upgrading the software version for the switch.
Browse...	Used for selecting the file while upgrading or restoring the switch.

Chapter Ⅳ

Advanced Settings

Administration

This section helps you view and configure basic info for the switch and instructs you how to use system maintenance tools. Specifically, the following two parts are included:

System Configuration: This section displays and allows you to configure switch system info/time, reboot the switch, reset the switch and upgrade software version for the switch..

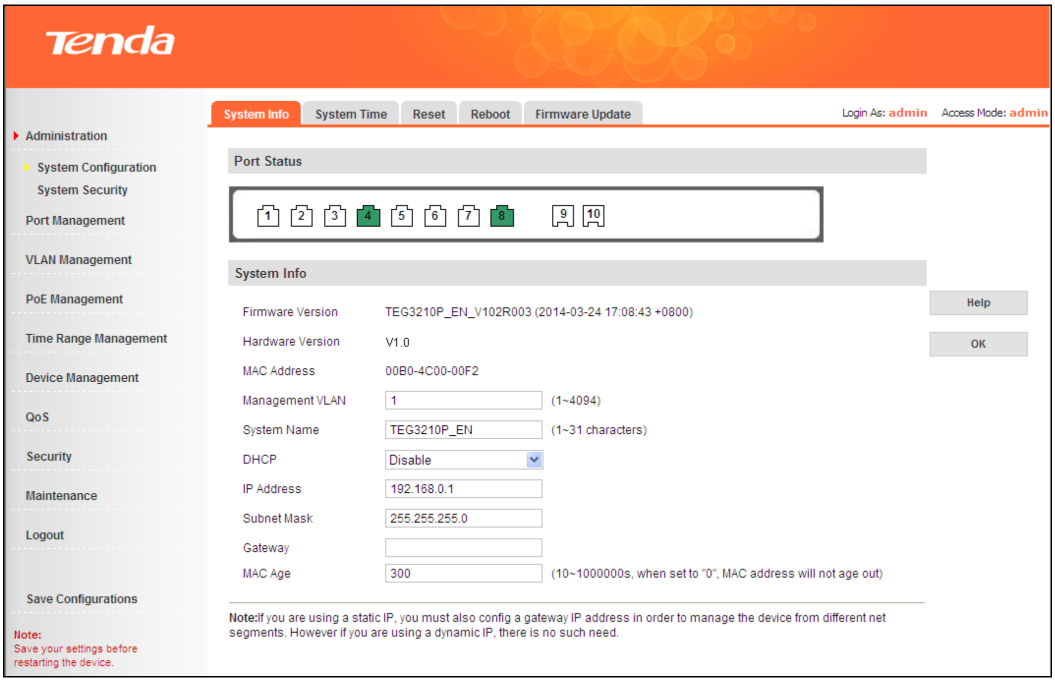
System Security: This section helps you prevent non-administrators from modifying configuration info, which ensures administration security for the switch.

1 System Configuration

System Configuration includes the following five parts: System Info, System Time, Reset, Reboot and Firmware Update.

1.1 System Info

Click **Administration** to enter page below and you can have a good knowledge of connection status of the currently connected port and the system info.



Note:
Save your settings before restarting the device.

Firmware Version	TEG3210P_EN_V102R003 (2014-03-24 17:08:43 +0800)	
Hardware Version	V1.0	
MAC Address	00B0-4C00-00F2	
Management VLAN	1	(1~4094)
System Name	TEG3210P_EN	(1~31 characters)
DHCP	Disable	
IP Address	192.168.0.1	
Subnet Mask	255.255.255.0	
Gateway		
MAC Age	300	(10~1000000s, when set to "0", MAC address will not age out)

Note:If you are using a static IP, you must also config a gateway IP address in order to manage the device from different net segments. However if you are using a dynamic IP, there is no such need.

Parameters on this page are described below:

Field	Description
Port Status	Displays all ports' connection status. When it is filled with the green color, a link has been established on this port. When it is filled with no color, no link is established on this port.

Firmware Version	Display the switch’s software version and release date.
Hardware Version	Display the switch’s hardware version.
MAC Address	Display the switch’s physical address.
Management VLAN	Management 802.1Q VLAN ID of the switch (default: 1). If you want to change the management VLAN, click **VLAN Management > VLAN Configuration** to create a management VLAN first. At this time, if you want to access the switch, you need to reconnect to a certain port in the new management VLAN (Note: Only this port’s PVID is the same with its management VLAN, can you have an access for the Internet.). **Tip:** Only in 802.1Q VLAN mode, can this parameter be configurable.
System Name	By default, the system name is TEG3210P_EN. It is suggested to configure a designated name for the switch so that you can locate it quickly when you manage it in your network.
DHCP	Enable/Disable the DHCP server on the switch. **Enable:** In this status, the switch will obtain an (management) IP address, subnet mask and gateway automatically and you can view the IP from DHCP clients list and use it to log in to the switch via Http or Telnet. **Disable:** In this status, you need to configure the switch’s IP address, subnet mask, and gateway manually.
IP Address	You can view and modify the switch’s IP address here when the DHCP server is disabled. The default value is 192.168.0.1. This IP address is also the management IP address of the switch. You can use it to log in to the switch via Http or Telnet.
Subnet Mask	You can view and modify the switch’s subnet mask here when the DHCP server is disabled. The default value is 255.255.255.0.
Gateway	You can view and modify the switch’s default gateway here when the DHCP server is disabled.

MAC Age	Aging time of the switch's dynamic MAC address (10~1000000s). The default value is 300s. When it is set to 0, MAC address won't be aged. **Tip:** This switch maintains an independent MAC address (forwarding) table for each VLAN.

1.2 System Time

This page displays and allows you to configure system time for the switch. Two methods are available here:

- **Acquire System Time via SNTP Server**

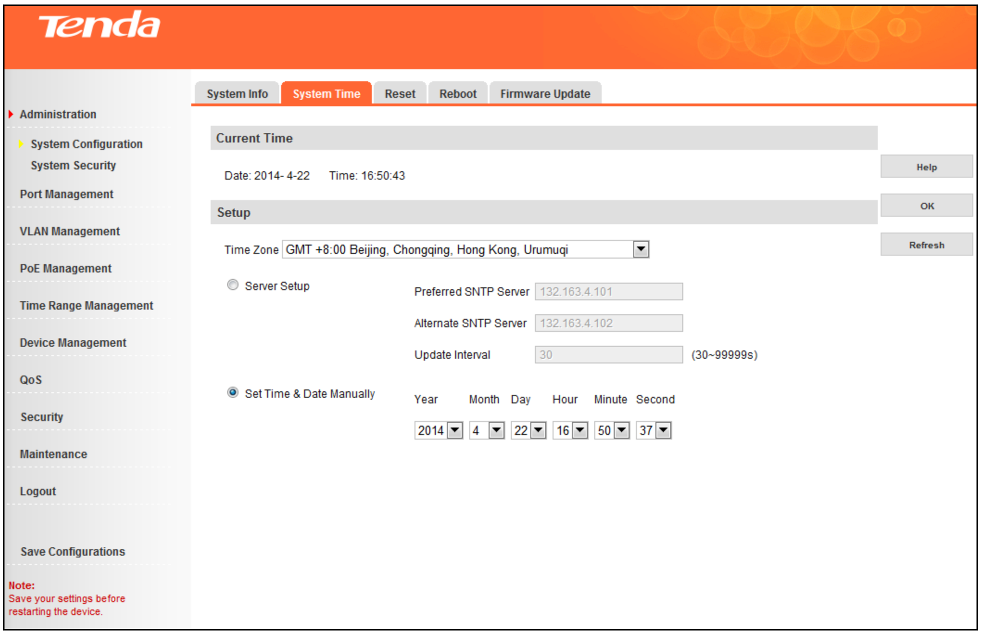
The Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. Simple Network Time Protocol (SNTP) is another less complex implementation of NTP. It synchronizes time between time servers and clients so that clock-dependent devices on the network can consistently provide diverse time based applications.

Note:

If you want to acquire system time via SNTP server, you need to have an access to the Internet. Method: click **Administration > System Configuration > System Info** to configure proper IP address, subnet mask and gateway for the switch.

- **Set Time & Date Manually**

Click **Administration > System Configuration > System Time** to enter page below and you can configure system time manually for the switch.



Current Time

Date: 2014- 4-22 Time: 16:50:43

Setup

Time Zone GMT +8:00 Beijing, Chongqing, Hong Kong, Urumuqi

○ Server Setup

Preferred SNTP Server 132.163.4.101

Alternate SNTP Server 132.163.4.102

Update Interval 30 (30~99999s)

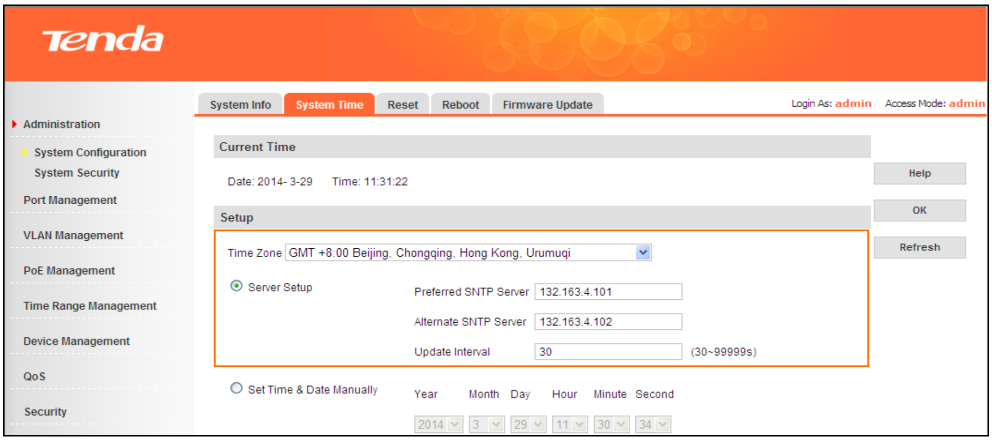
● Set Time & Date Manually

Year	Month	Day	Hour	Minute	Second
2014	4	22	16	50	37

Note:
Save your settings before restarting the device.

Configuration steps for acquiring system time via SNTP server:

1. Select a time zone from the **Time Zone** drop-down list;
2. Select **Server Setup**;
3. Enter proper SNTP server IP addresses in the **Preferred / Alternate SNTP Server** field;
4. Enter the automatic update interval in the **Update Interval** field within a valid range of 30 to 99999 seconds. The default value is 30s. Once configured, the switch will synchronize with the SNTP server accordingly;
5. Click **OK**.



Login As: admin Access Mode: admin

Current Time

Date: 2014- 3-29 Time: 11:31:22

Setup

Time Zone GMT +8:00 Beijing, Chongqing, Hong Kong, Urumuqi

● Server Setup

Preferred SNTP Server 132.163.4.101

Alternate SNTP Server 132.163.4.102

Update Interval 30 (30~99999s)

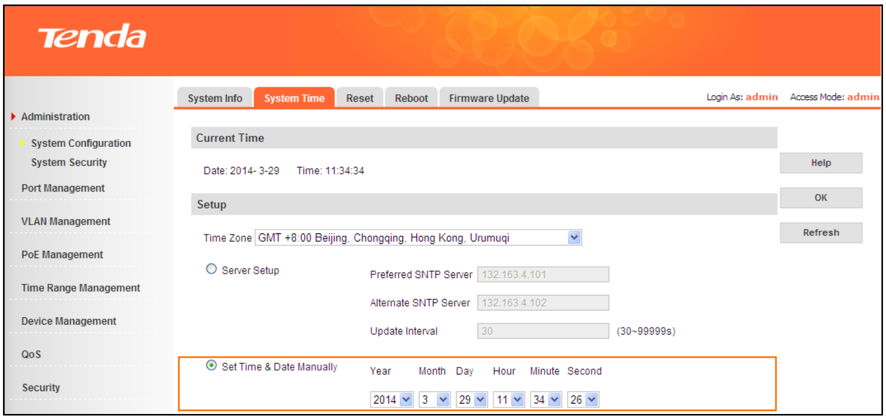
○ Set Time & Date Manually

Year	Month	Day	Hour	Minute	Second
2014	3	29	11	30	34

Configuration steps for setting system time manually:

1. Select a time zone from the **Time Zone** drop-down list;
2. Select **Set Time & Date Manually**;
3. Set proper date and time manually;

4. Click **OK**.



Login As: admin Access Mode: admin

Current Time

Date: 2014- 3-29 Time: 11:34:34

Setup

Time Zone GMT +8:00 Beijing, Chongqing, Hong Kong, Urumuqi

○ Server Setup

Preferred SNTP Server 132.163.4.101

Alternate SNTP Server 132.163.4.102

Update Interval 30 (30~99999s)

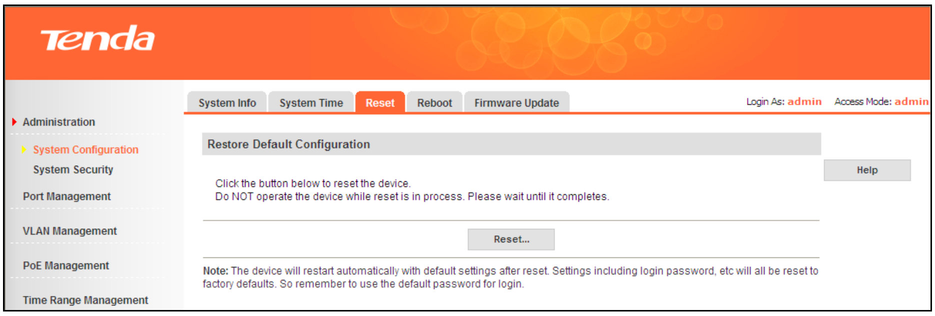
● Set Time & Date Manually

Year	Month	Day	Hour	Minute	Second
2014	3	29	11	34	26

When system time is configured successfully, you can view **Current Time** on this page to check whether your time settings are activated or not.

1.3 Reset

If you forgot your login info, like username/password or management VLAN, etc. or if you have a problem in surfing the Internet but cannot find out where the problem is, it is advisable to reset this device.



Login As: admin Access Mode: admin

Restore Default Configuration

Click the button below to reset the device.
Do NOT operate the device while reset is in process. Please wait until it completes.

Note: The device will restart automatically with default settings after reset. Settings including login password, etc will all be reset to factory defaults. So remember to use the default password for login.

Reset the device by the hardware button:

1. When the device is functioning properly, press the **Reset** button on the front panel of the device for at least 5 seconds and then release it;
2. Wait for 45 seconds until the device restarts.

Reset the device via web browser-accessible administrator page

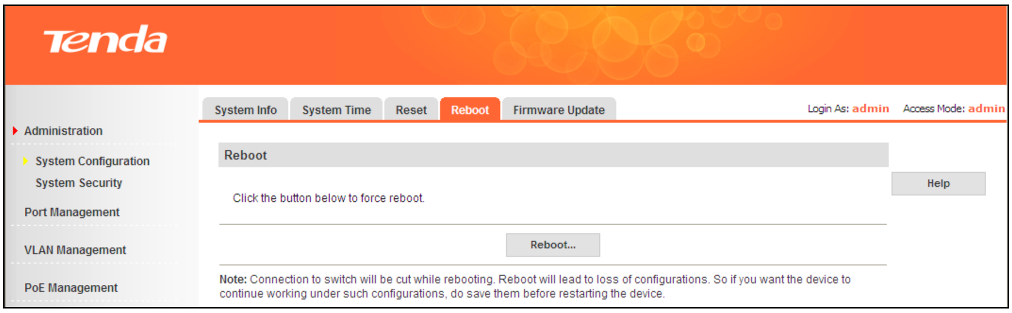
1. Log in to this device’s web browser-accessible administrator page;
2. Click **Administrator > System Configuration > Reset** to enter the **Reset** page;
3. Click **Reset…** and then follow onscreen instructions.

Tip:

After resetting this device, the management VLAN of the switch will be set to 1, the default login IP address is 192.168.0.1 and the default login username and password will be admin for both.

1.4 Reboot

Rebooting the switch can release some caches so that the switch can work with high performance. And in some cases, if system halt occurs or you are unable to log in to its web browser-accessible administrator page, rebooting the switch may help you out. Click **Administration > System Configuration > Reboot** to enter page below:



Reboot

Click the button below to force reboot.

Note: Connection to switch will be cut while rebooting. Reboot will lead to loss of configurations. So if you want the device to continue working under such configurations, do save them before restarting the device.

Note:

- After reboot, configurations saved by merely clicking **OK** will be lost. If you do not want to lose your configurations after reboot, please click **Save Configurations > Save** to save your configurations first.
- Operations like power up the switch after disconnecting its power supply, reset the switch, upgrade the switch, etc. will reboot this device.

1.5 Firmware Update

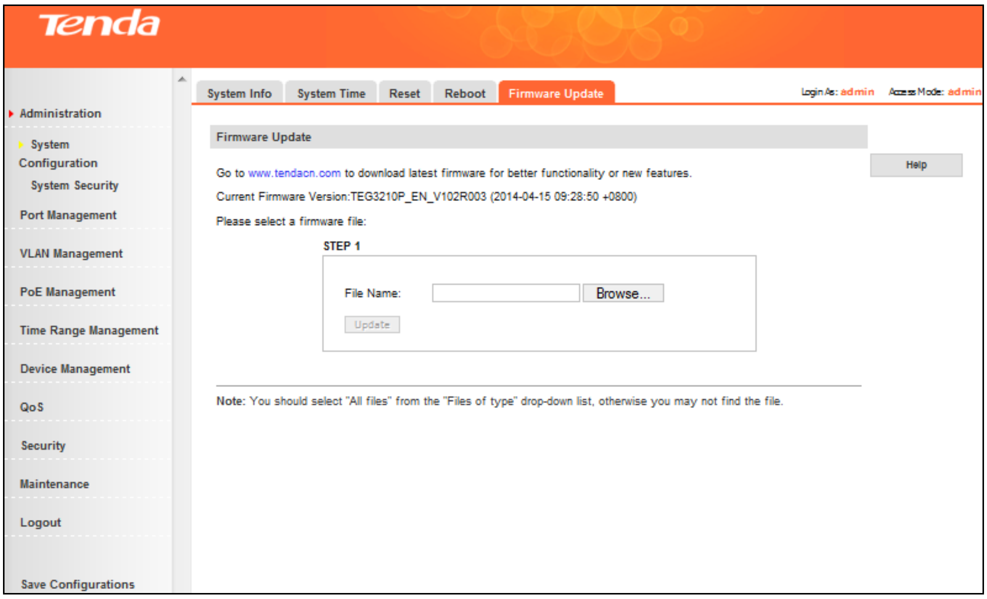
You can access our official website www.tendacn.com to download the latest software for upgrading, acquiring more value-added functions and better performance for your switch.

Note:

While upgrading, do not cut off power supply of the switch, otherwise you may do damage to the switch! If sudden power failure occurs, please re-upgrade it; if sudden power failure occurs and you are unable to access the web browser-accessible administrator page, please contact our maintenance stuff.

Upgrading Procedures:

1. Log in to our website www.tendacn.com to download the latest software to your local computer;
2. Click **Administration > System Configuration > Firmware Update** to enter page below:



Firmware Update

Go to www.tendacn.com to download latest firmware for better functionality or new features.

Current Firmware Version:TEG3210P_EN_V102R003 (2014-04-15 09:28:50 +0800)

Please select a firmware file:

STEP 1

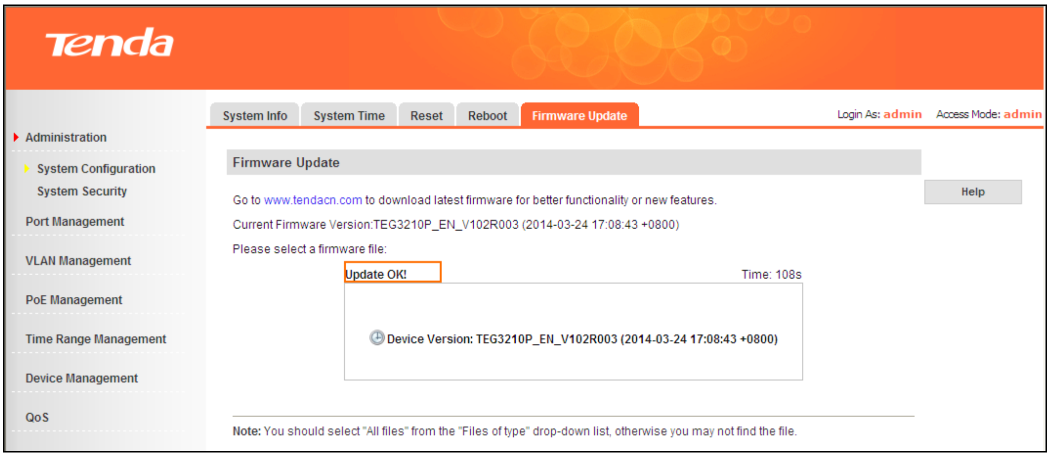
File Name:

Note: You should select "All files" from the "Files of type" drop-down list, otherwise you may not find the file.

3. Click **Browse** to select the software file you wish to upload from your local computer;

4. Click **Update** to confirm your upgrading;

5. Wait for about 1.5~2 minutes until the following page appears, which indicates the upgrading completes successfully.



Firmware Update

Go to www.tendacn.com to download latest firmware for better functionality or new features.

Current Firmware Version:TEG3210P_EN_V102R003 (2014-03-24 17:08:43 +0800)

Please select a firmware file:

Update OK!

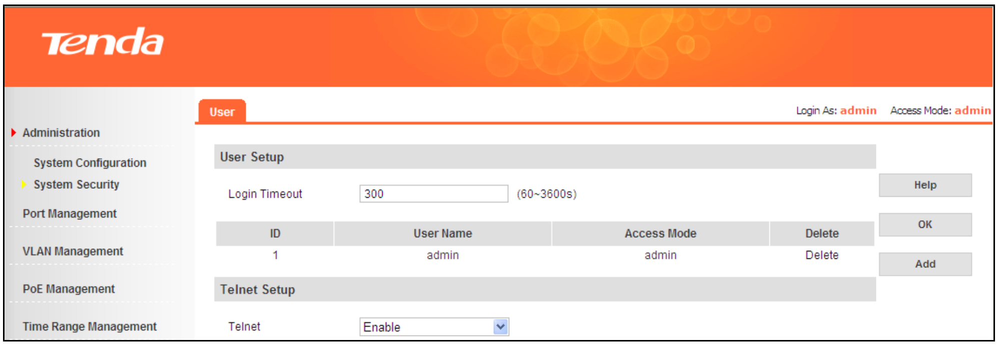
Time: 108s

Device Version: TEG3210P_EN_V102R003 (2014-03-24 17:08:43 +0800)

Note: You should select "All files" from the "Files of type" drop-down list, otherwise you may not find the file.

2 System Security

Click **Administration > System Security** to manage access control for the switch.



Login As: admin Access Mode: admin

User Setup

Login Timeout 300 (60~3600s)

ID	User Name	Access Mode	Delete
1	admin	admin	Delete

Telnet Setup

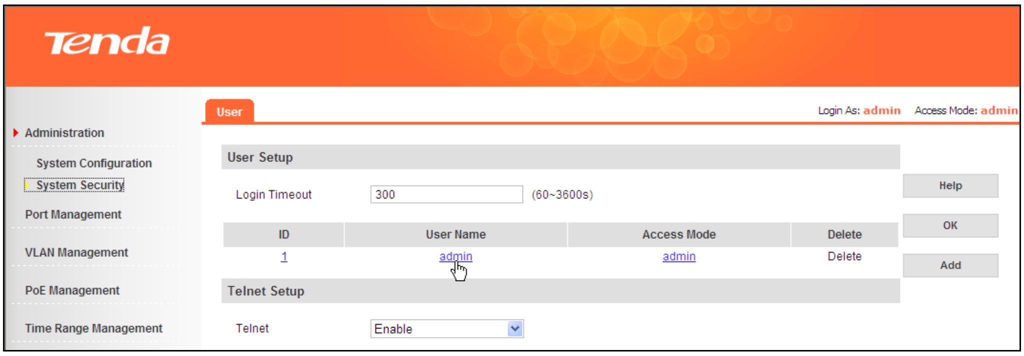
Telnet Enable

Parameters on this page are described below:

Field	Description
Login Timeout	This field specifies how long the web manager is allowed to remain idle. When reaching the set time, the web manager will return to login window. The Login Timeout can be set to any value between 30 and 3600 seconds. The default setting is 300 seconds.
User Name	User name used for logging in to the switch via http or telnet.
Access Mode	Specify an access right for a corresponding user: **Administrator:** Has absolute rights to view and configure switch's settings and system info. Only one administrator is allowed to be configured. By default, an administrator **admin** has already existed. You have no right to add an administrator and delete, modify the administrator **admin**, but you can modify its login password. **Technician:** Has the right to view and config switch's settings, except for “Firmware Update”, “User”, “Reset”, “Reboot” settings. Up to 5 technicians can be configured. **User:** Has the right to view switch's current settings but no right to manage/config them. Up to 10 users can be configured.
Telnet	Enable/Disable Telnet management. When enabled, you can manage the switch via Telnet. It is enabled by default.

Procedures for modifying password for the user name admin:

1. Click the user name **admin**;



Login As: admin Access Mode: admin

User Setup

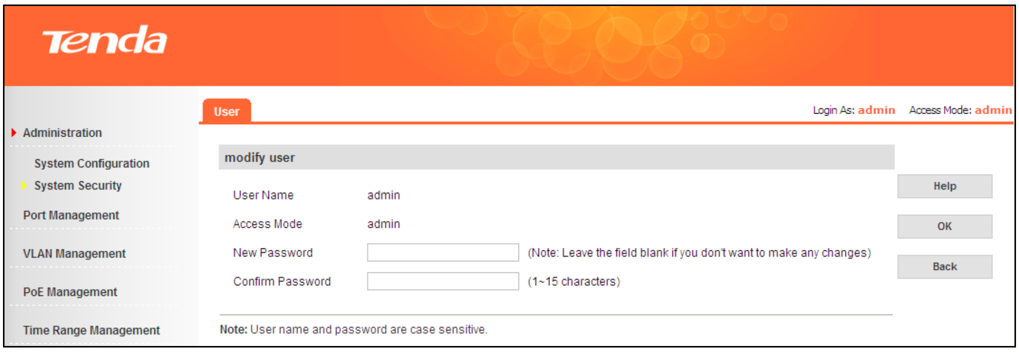
Login Timeout 300 (60~3600s)

ID	User Name	Access Mode	Delete
1	admin	admin	Delete

Telnet Setup

Telnet Enable

2. Enter the new password in the **New Password** field;
3. Enter your password again in the **Confirm Password** field to confirm your modification;
4. Click **OK**.



Login As: admin Access Mode: admin

modify user

User Name admin

Access Mode admin

New Password (Note: Leave the field blank if you don't want to make any changes)

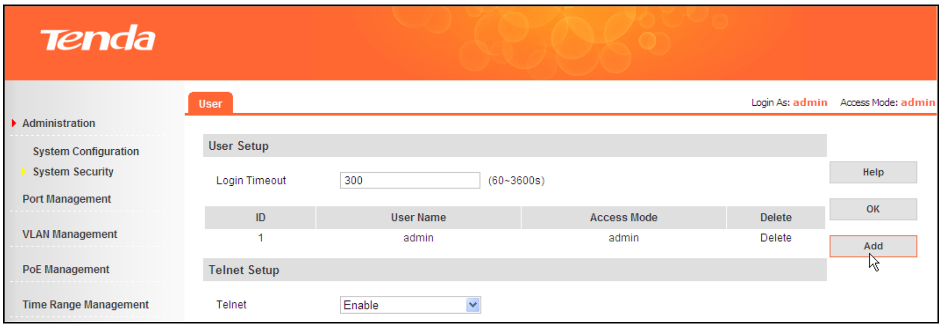
Confirm Password (1~15 characters)

Note: User name and password are case sensitive.

Once you've changed your password, next time you log in to the switch, do remember use the new password. If you forgot the password, pressing the **Reset** button for over 5 seconds and releasing it restore the device to factory default settings and your login password will be the default one **admin**.

Procedures for adding non-administrators:

1. Click **Add**;



Login As: admin Access Mode: admin

User Setup

Login Timeout 300 (60~3600s)

ID	User Name	Access Mode	Delete
1	admin	admin	Delete

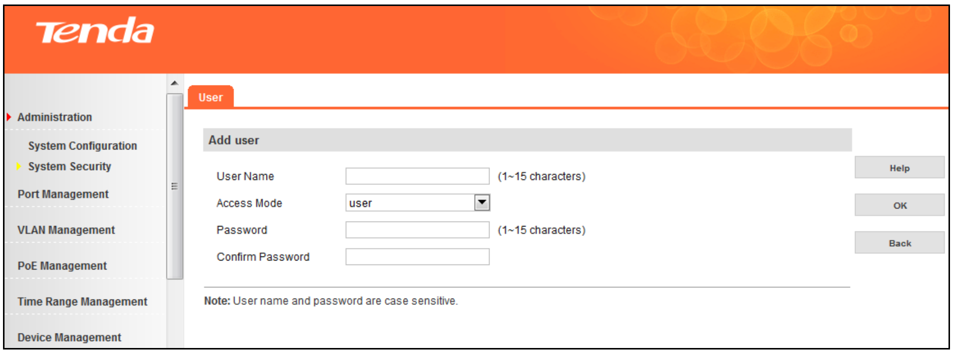
Telnet Setup

Telnet Enable

2. Customize a user name in the **User Name** filed;
3. Select **user** or **technician** from the **Access Mode** drop-down list;
4. Customize a password in the **Password** field;
5. Enter your password again in the **Confirm Password** field to confirm your

password;

6. Click **OK**.



Add user

User Name (1~15 characters)

Access Mode user

Password (1~15 characters)

Confirm Password

Note: User name and password are case sensitive.

Port Management

This section helps you have a good knowledge of packets forwarding on all ports. Following two parts are included:

Port Configuration: This section allows you to configure basic properties for all ports and port mirroring. And you can also view port statistics here.

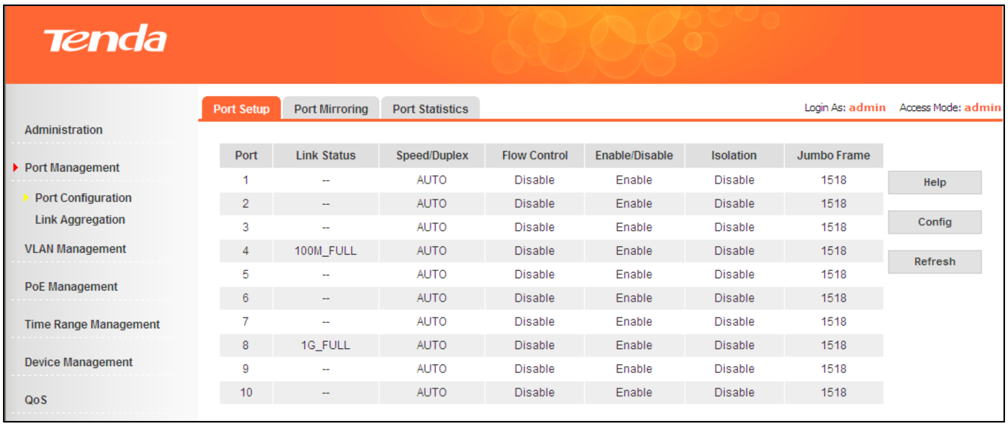
Link Aggregation: This section helps you increase link bandwidth and provides redundancy backup for the switch.

1 Port Configuration

Port Setup, Port Mirroring and Port Statistics are included in this section.

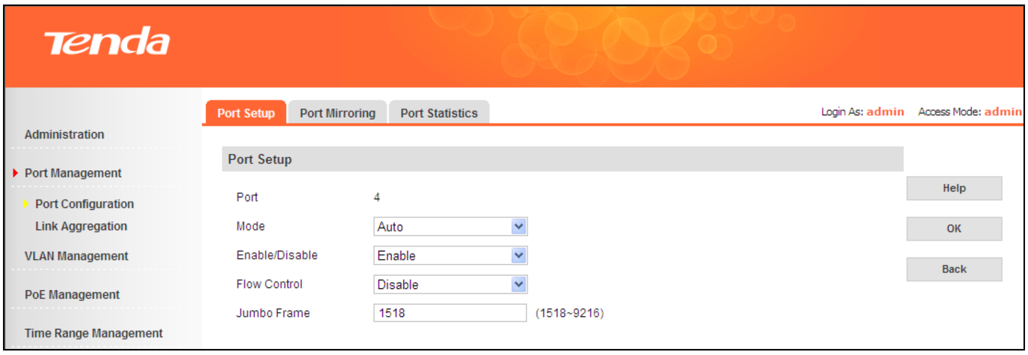
1.1 Port Setup

Click **Port Management > Port Configuration > Port Setup** to enter page below to configure properties for all ports.



Port	Link Status	Speed/Duplex	Flow Control	Enable/Disable	Isolation	Jumbo Frame
1	--	AUTO	Disable	Enable	Disable	1518
2	--	AUTO	Disable	Enable	Disable	1518
3	--	AUTO	Disable	Enable	Disable	1518
4	100M_FULL	AUTO	Disable	Enable	Disable	1518
5	--	AUTO	Disable	Enable	Disable	1518
6	--	AUTO	Disable	Enable	Disable	1518
7	--	AUTO	Disable	Enable	Disable	1518
8	1G_FULL	AUTO	Disable	Enable	Disable	1518
9	--	AUTO	Disable	Enable	Disable	1518
10	--	AUTO	Disable	Enable	Disable	1518

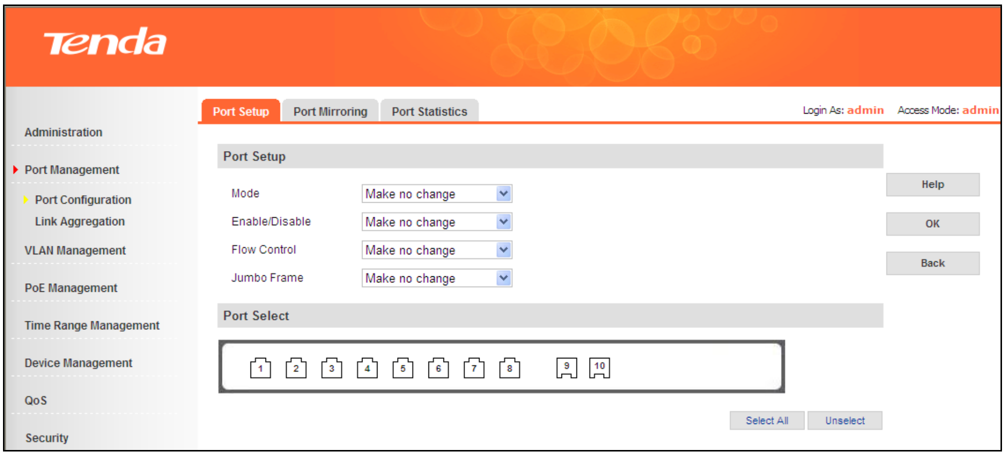
To configure properties for a certain port, click the corresponding port to enter the corresponding configuration page.



Port Setup

Port	4
Mode	Auto
Enable/Disable	Enable
Flow Control	Disable
Jumbo Frame	1518 (1518~9216)

To batch configure port properties, click **Config** to enter the configuration page.



Port Setup

Mode: Make no change

Enable/Disable: Make no change

Flow Control: Make no change

Jumbo Frame: Make no change

Port Select

Parameters on this page are described below:

Field	Description
Link Status	Display actual link rates and duplex modes on corresponding ports. "--" is displayed if a port is not linked or link failure occurs.
Speed/Duplex	Three types of duplex modes are available on RJ45 ports: 10M, 100M, 1000M. 10M/100M: half duplex (HDX) and full duplex (FDX); 1000M: full duplex (FDX). Only one duplex mode is available on SFP ports: 1000M full duplex. You can select different duplex modes as you need. • If you want the port to send and receive packets concurrently, you can set this port to work in full duplex mode. • If you want the port to either send or receive packets, you can set this port to work in half duplex mode. • When you set the port to work in auto mode, the duplex status of the port will be determined via auto-negotiation. By default, the speed/duplex mode for all ports is auto-negotiation.

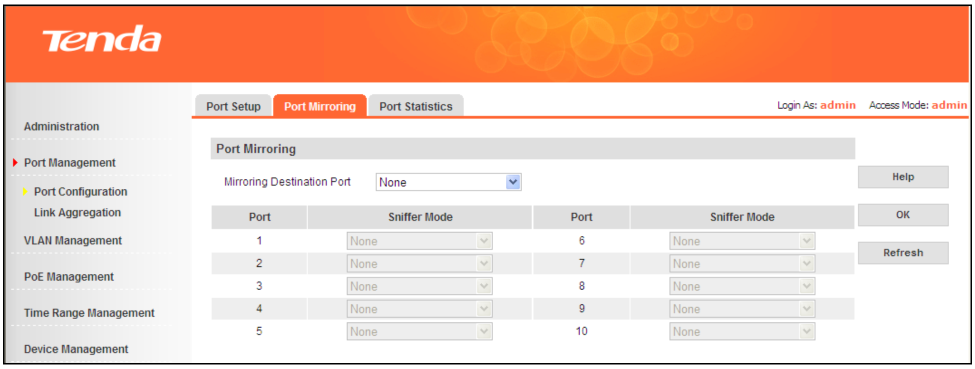
Flow Control	With flow control enabled on both the switch and its link partner, and full duplex mode enabled on the port, when encountering congestion, the port will send flow control frames to notify the link partner of such; upon receiving such frames, the link partner will temporarily stop sending packets to the switch, thus avoiding packets drop and ensuring a reliable network. Meanwhile, if a certain port receives Pause frame, it will also stop sending packets out. By default, the flow control feature is disabled. ⚠ **Note:** • This switch does not support half-duplex flow control; • Enabling full duplex mode can avoid data loss. However, this will affect communication between source ports and other devices. Thus, it is not advisable to use this feature on ports which have Internet access.
Enable/Disable	Enable/Disable selected port(s). Once a certain port is disabled, the port won’t forward packets.

Isolation	Enable/Disable port isolation. Only in 802.1Q VLAN mode, can this item be configured. By adding ports into isolation groups, data isolation among ports in isolation groups will be implemented. Port isolation not only ensures better security, but provides users with flexible networking solutions. By default, all ports are not isolated. ⚠ **Note:** • Only when ports in the same isolation group cannot intercommunicate, will intercommunication between ports within an isolation group and ports outside this group not be affected. • When a port in an aggregation group joins or leaves an isolation group, other ports in this aggregation group will join or leave the same isolation group automatically. • When a port in an aggregation group leaves an isolation group, other ports in this aggregation group will remain in the same isolation group, namely, isolation properties for ports in an aggregation will not be affected. • When a non-isolated port joins an isolated aggregation group, it will join the same isolation group automatically.
Jumbo Frame	Configure sizes of Jumbo frames the switch has received. The valid range is 1518~9216. The default value is 1518, which is the longest one in IEEE802.3 standard. Once Jumbo frame size is configured, the system will deal with data that ports have received within the size length.

1.2 Port Mirroring

Port Mirroring allows you to copy packets on one or more ports to a mirroring destination port. You can attach a monitoring device to the mirroring destination port to view details about the packets passing through the copied port(s). This is useful for network monitoring and troubleshooting purposes.

The switch provides local port mirroring function, namely, both mirrored ports and mirroring destination ports are located on the same device. Click **Port Management > Port Configuration > Port Mirroring** to enter page below:



Port Mirroring

Mirroring Destination Port: None

Port	Sniffer Mode	Port	Sniffer Mode
1	None	6	None
2	None	7	None
3	None	8	None
4	None	9	None
5	None	10	None

Parameters on this page are described below:

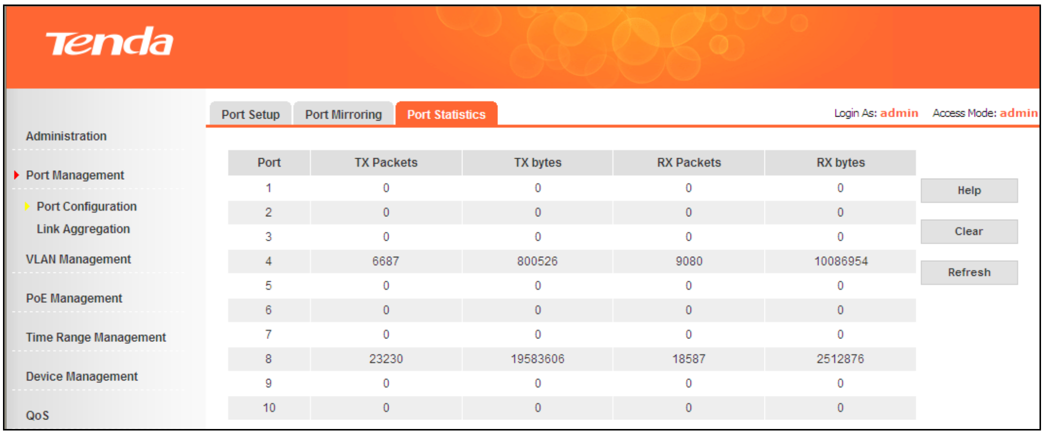
Field	Description
Mirroring Destination Port	Select the mirroring destination port. None indicates port mirroring feature is disabled. ⚠ **Note:** • A port cannot be set as the mirroring destination port and the mirroring source port simultaneously. • Only after a mirroring destination port is set, can you configure mirroring source port(s). • A port in an aggregation group cannot be configured as a mirroring destination port. • An STP-enabled and 802.1X authenticated port can't be configured as a mirroring destination port.
Sniffer Mode	Select the mirroring source port. None indicates the corresponding port won't be mirrored. **Ingress:** Only incoming packets on this port are copied to the mirroring destination port. **Egress:** Only outgoing packets on this port are copied to the mirroring destination port. **Egress & Ingress**: Both inbound and outbound packets on the corresponding port are copied to the mirroring destination port (monitor port). ⚠ **Note:** When total bandwidth of the mirrored port exceeds that of the mirroring port, packets loss will occur.

Tip:

- The mirroring destination port speed should be greater than that of total speed of all mirrored ports. So we recommend you configure the mirrored port as the routing port, namely, the port connected to the Internet, to monitor all packets.
- Only one copy is allowed for the same data flow. For example, if port 5 monitors ingress of port 1 and egress of port 2, as for packets forwarded from port 1 to port 2, only one copy is allowed on port 5.

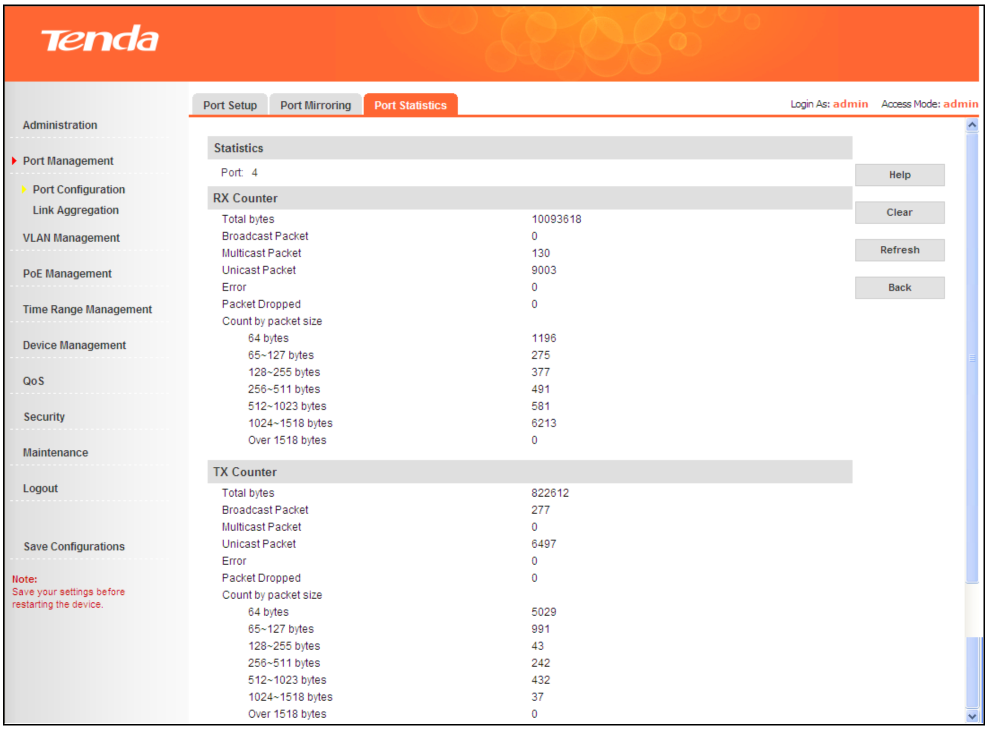
1.3 Port Statistics

Click **Port Management > Port Configuration > Port Statistics** to enter page below and it allows you to view and clear port statistics.



Port	TX Packets	TX bytes	RX Packets	RX bytes
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	6687	800526	9080	10086954
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	23230	19583606	18587	2512876
9	0	0	0	0
10	0	0	0	0

To view port statistics on a certain port, click the corresponding port number.



Note: Save your settings before restarting the device.

Statistics

Port: 4

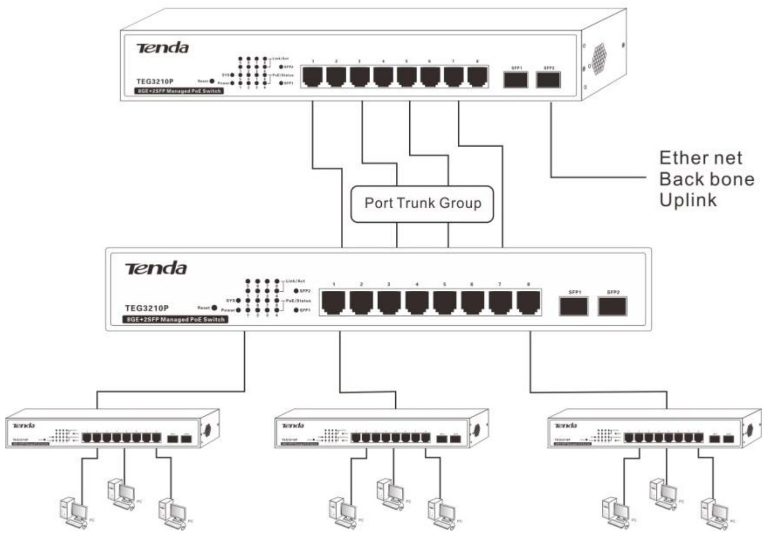
RX Counter	
Total bytes	10093618
Broadcast Packet	0
Multicast Packet	130
Unicast Packet	9003
Error	0
Packet Dropped	0
Count by packet size	
64 bytes	1196
65~127 bytes	275
128~255 bytes	377
256~511 bytes	491
512~1023 bytes	581
1024~1518 bytes	6213
Over 1518 bytes	0

TX Counter	
Total bytes	822612
Broadcast Packet	277
Multicast Packet	0
Unicast Packet	6497
Error	0
Packet Dropped	0
Count by packet size	
64 bytes	5029
65~127 bytes	991
128~255 bytes	43
256~511 bytes	242
512~1023 bytes	432
1024~1518 bytes	37
Over 1518 bytes	0

2 Link Aggregation

Link aggregation groups multiple Ethernet ports together in parallel to act as a single logical link. Aggregation-enabled devices treat all physical links (ports) in an aggregation group entirely as a single logical link (port). Member ports in an aggregation group share egress/ingress traffic load, delivering a bandwidth that is multiple of a single physical link. Link aggregation provides redundancy in case one of the links fails, thus reliability could be maintained. For network diagram of link aggregation, see below:

An Example of Link Aggregation



In the same aggregation group, all member ports must be set to the same configurations with respect to STP, port priority, VLAN configuration and port management. Following are illustrations in detail:

- Ports joining aggregation groups should share the following configurations: STP settings (STP status, P2P port, edge port, port priority and path cost included), port priority configurations, port VLAN configurations (port type, PVID, allowed VLAN, and Untagged/Tagged VLAN included), and port settings (Jumbo frame, flow control, isolation settings included).
- For ports having joined the aggregation group, following configurations are not allowed: adding static MAC address, configuring mirroring destination port, enabling voice VLAN function and enabling 802.1X authentication.
- The following ports cannot join the aggregation group: 802.1x-enabled port(s), mirroring destination port(s).

In terms of different link aggregation methods, there are two aggregation modes: static aggregation and LACP aggregation.

➘ Static Aggregation

For static aggregation, you must manually maintain the aggregation state of the member ports as system does not allow adding a new port or deleting any existing member port. LACP is disabled on member ports in static LACP mode.

Ports in static aggregation group must all be of the same port speed and will stay in forwarding state. If a certain port is set to a different speed, packets on it will be forwarded at the actual connection speed. The bandwidth of the aggregation group equals the total bandwidth of its member ports.

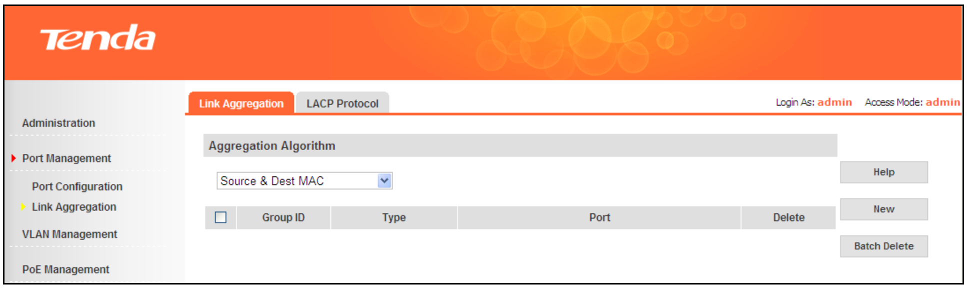
➘ LACP Aggregation

Based on IEEE 802.3ad, LACP (Link Aggregation Control Protocol) provides a method to implement link aggregation dynamically. Whether ports in LACP group are aggregation ports or not is determined by LLDPDU frame auto-negotiation. LACP is enabled on the member ports in LACP mode.

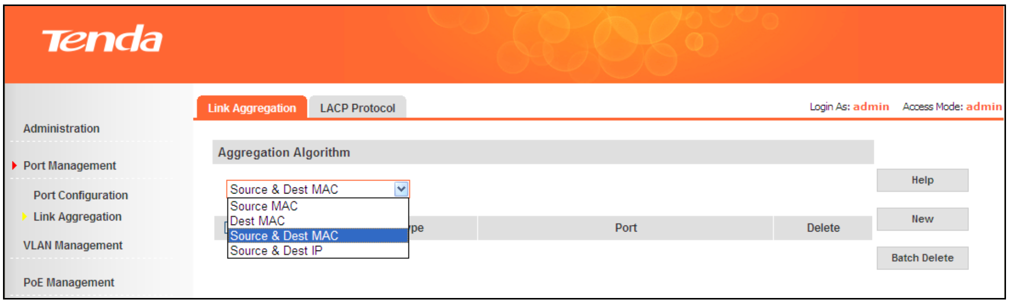
Ports in an LACP aggregation group may stay either in a forwarding status or a blocked status. Once LACP is shaped, ports will be in a forwarding status. If all ports in the aggregation group are not aggregated, only the first port will be in the forwarding status. Ports in forwarding status can send/receive both service packets and LACP frames; ports in blocked status can only send/receive LACP frames.

2.1 Link Aggregation

Click **Port Management > Link Aggregation** to enter page below:



Generally, there are four widely used aggregation algorithms. By default, the aggregation algorithm of the switch is Source & Destination MAC.

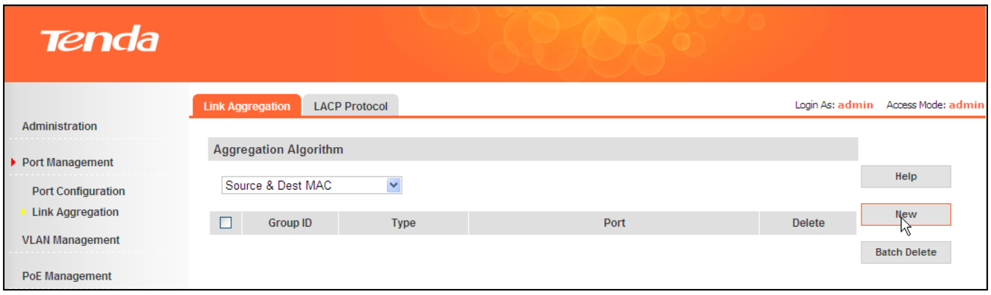


Parameters on the page are described below:

Algorithm	**Meaning**
Source MAC	Indicate member ports in a link aggregation group share traffic load according to source MAC addresses.
Dest MAC	Indicate member ports in a link aggregation group share traffic load according to destination MAC addresses.
Source & Dest MAC	Indicate member ports in a link aggregation group share traffic load according to source and destination MAC addresses.
Source & Dest IP	Indicate member ports in a link aggregation group share traffic load according to source and destination IP addresses.

Procedures for adding static aggregation:

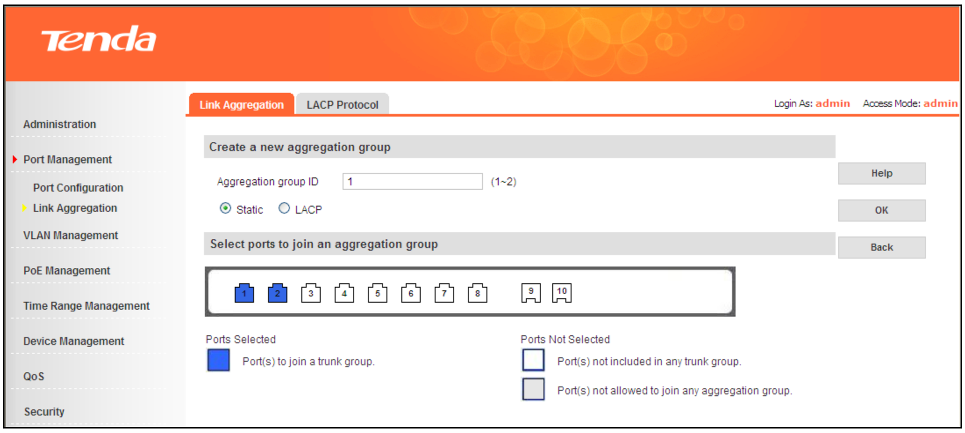
1. Click **New**;



2. On the appearing page type in a valid aggregation group number (1-2);

3. Select **Static**;

4. Select ports to join the aggregation group. Up to 8 ports and down to 2 ports can be added to each;
5. Click **OK**.



Create a new aggregation group

Aggregation group ID: 1 (1~2)

● Static ○ LACP

Select ports to join an aggregation group

Ports Selected

🟦 Port(s) to join a trunk group.

Ports Not Selected

□ Port(s) not included in any trunk group.

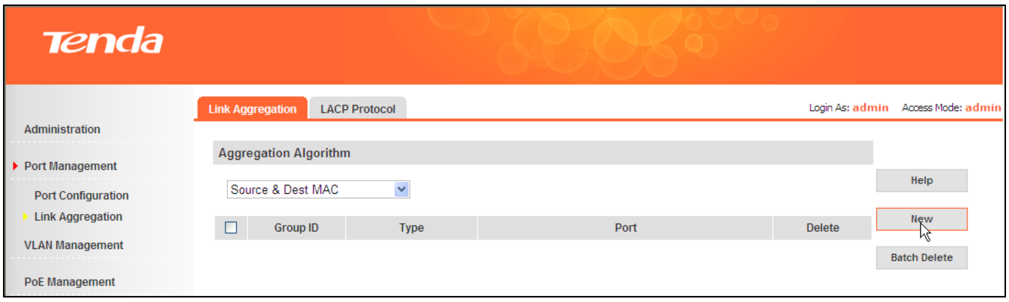
▨ Port(s) not allowed to join any aggregation group.

Tip:

Once ports in static aggregation group are linked successfully, they will be aggregated and won't be affected by port speed.

Procedures for adding LACP group:

1. Click **New** on the **Link Aggregation** page;

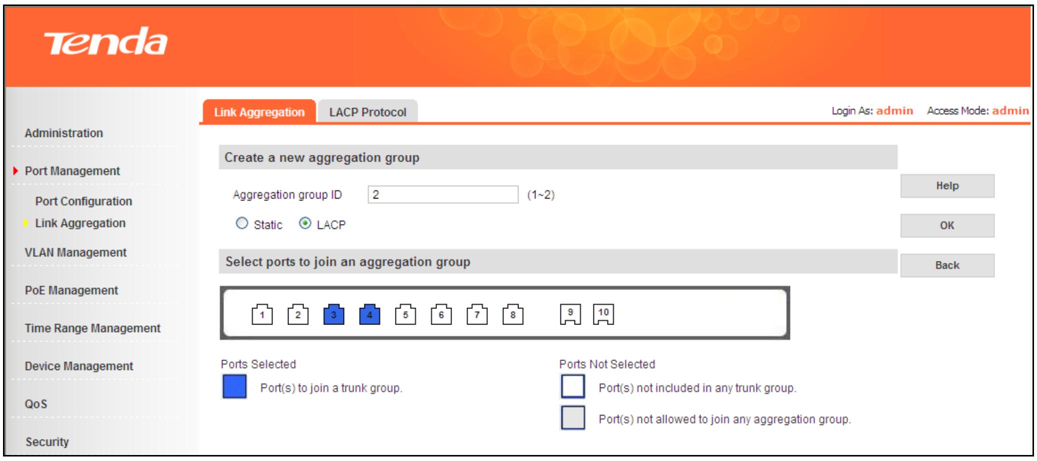


Aggregation Algorithm

Source & Dest MAC

□	Group ID	Type	Port	Delete

2. On the appearing page type in a valid aggregation group number (1-2);
3. Select **LACP**;
4. Select ports to join the aggregation group. Up to 8 ports and down to 2 ports can be added to each;
5. Click **OK**.



Login As: admin Access Mode: admin

Create a new aggregation group

Aggregation group ID: 2 (1~2)

○ Static ● LACP

Select ports to join an aggregation group

Ports Selected

🟦 Port(s) to join a trunk group.

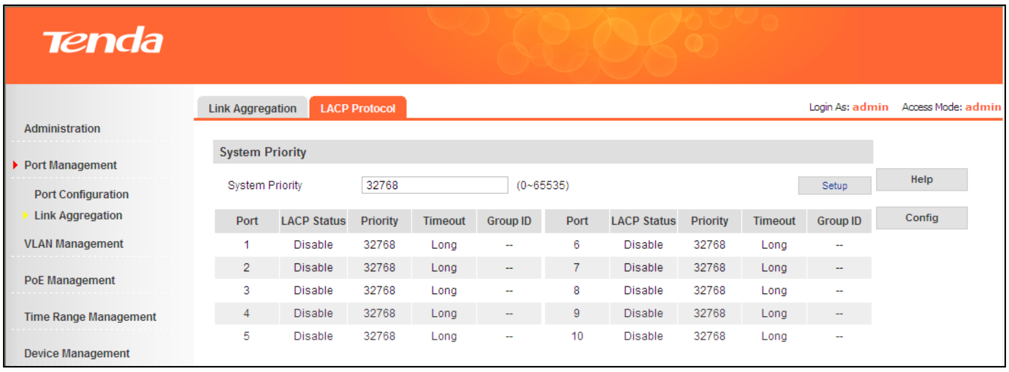
Ports Not Selected

□ Port(s) not included in any trunk group.

▨ Port(s) not allowed to join any aggregation group.

2.2 LACP Protocol

Click **Port Management > Link Aggregation > LACP Protocol** to enter page below to configure system LACP priority and port LACP priority.



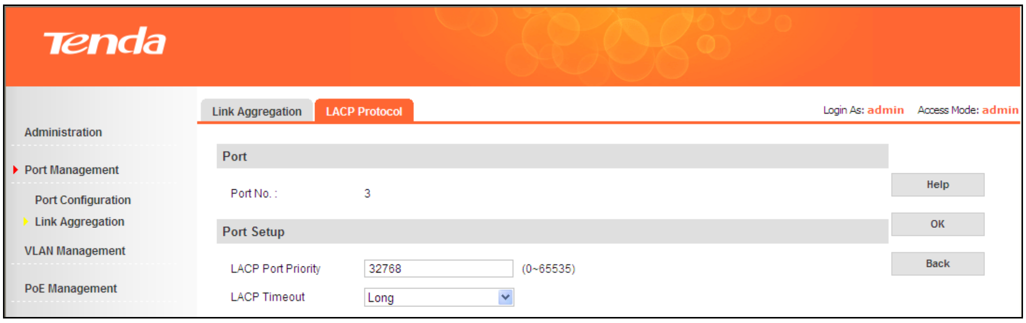
Login As: admin Access Mode: admin

System Priority

System Priority: 32768 (0~65535)

Port	LACP Status	Priority	Timeout	Group ID	Port	LACP Status	Priority	Timeout	Group ID
1	Disable	32768	Long	--	6	Disable	32768	Long	--
2	Disable	32768	Long	--	7	Disable	32768	Long	--
3	Disable	32768	Long	--	8	Disable	32768	Long	--
4	Disable	32768	Long	--	9	Disable	32768	Long	--
5	Disable	32768	Long	--	10	Disable	32768	Long	--

To configure LACP parameters on a single port, click the corresponding port number.



Login As: admin Access Mode: admin

Port

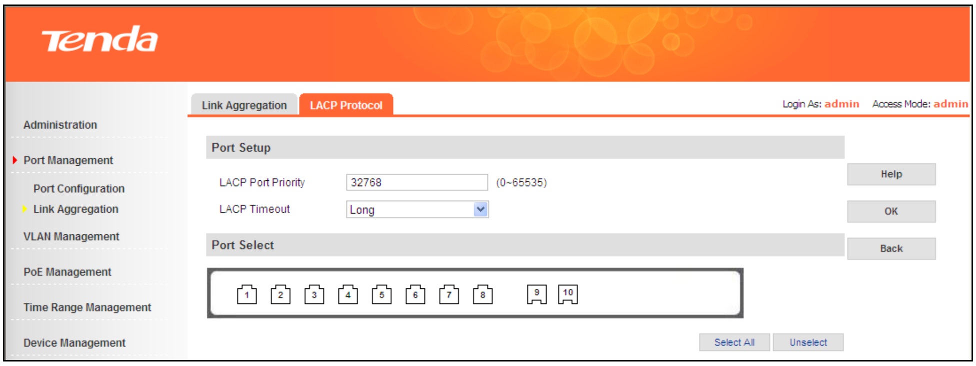
Port No. : 3

Port Setup

LACP Port Priority: 32768 (0~65535)

LACP Timeout: Long

To batch configure LACP parameters, click **Configure** to enter page below:



Port Setup

LACP Port Priority: 32768 (0~65535)

LACP Timeout: Long

Port Select

Parameters on the page are described below:

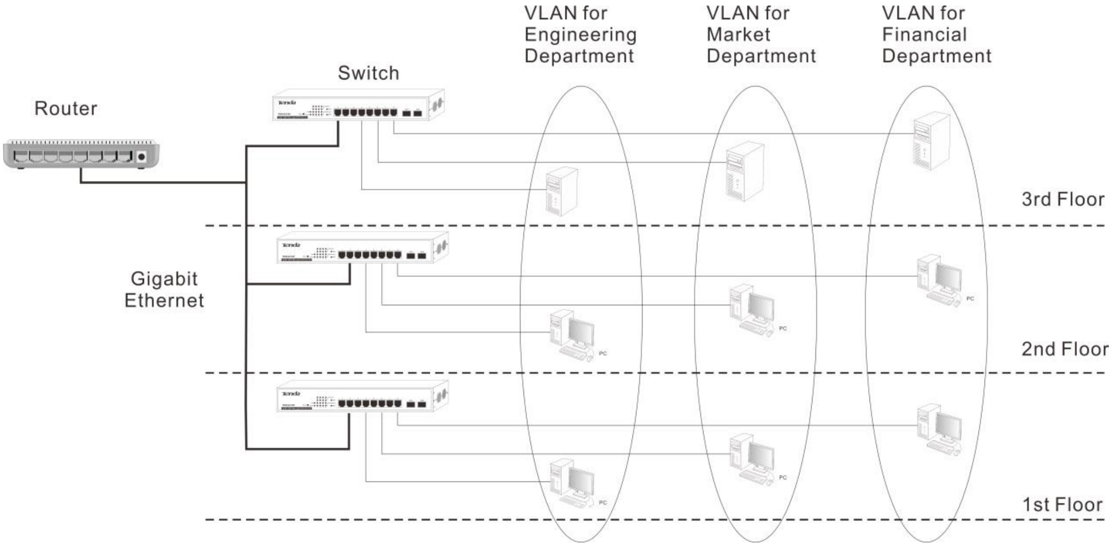
Field	Description
System Priority	Configure system priority (0-65535). The default is 32768. The smaller the value is, the higher the system priority is. When data transferring among different systems, the system with higher priority can determine to which aggregation link the link belongs; The system with lower priority will join a proper aggregation link according to its partner’s choice.
LACP Status	Display whether the port has joined the LACP aggregation group or not. **Enable:** The port has joined an LACP aggregation group. **Disable:** The port has joined a static aggregation group or has not joined any LACP aggregation group.
LACP Port Priority	LACP port priority is used for port selection in LACP aggregation group. The port with a smaller priority value will be a member of dynamic aggregation group. With the same port priority, the port with smaller port number will be a member of dynamic aggregation group. The default value is 32768.
Timeout	Configure LACP timeout. If the LACP aggregation group is not aggregated, LACPDU frames will be re-sent for auto-negotiation. The default setting is long.
Group ID	Display the LACP aggregation group ID.

VLAN Management

In traditional medium sharing Ethernet and switched Ethernet, all users are in a broadcast domain. With more and more PCs appearing in the networking, broadcast packets increase, which greatly increases data flow among devices in the networking. Thus, network performance becomes worse. With networking expands, broadcast storm may occur and the entire network may be paralyzed.

A Virtual Local Area Network (VLAN) is a network topology which allows to logically instead of physically segment a LAN into several net segments. A VLAN combines a group of hosts with a common set of requirements logically instead of physically relocating devices or connections.

VLANs allow a network to be logically segmented into different broadcast domains. All members in a VLAN are treated as in the same broadcast domain and communicate as if they were on the same net segment, regardless of their physical locations. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated. Different VLANs cannot intercommunicate directly. Inter-VLAN communication can only be achieved using a router or other layer 3 devices that are able to perform Layer 3 forwarding. VLAN network topology can be shown as below:


VLAN for Engineering Department
VLAN for Market Department
VLAN for Financial Department
Switch
Router
3rd Floor
Gigabit Ethernet
2nd Floor
1st Floor

Compared with the traditional Ethernet, VLAN enjoys the following advantages:

- Better network performance. By restricting all broadcast traffic to a VLAN, it saves network bandwidth and enhances network performance.
- Reduced cost. The use of VLANs to create broadcast domains eliminates the need for traditional routers to handle this function, permitting operation at lower latencies and cost compared to routers under heavy load and at high cost.
- Ease of network management. Members of a VLAN group can be geographically

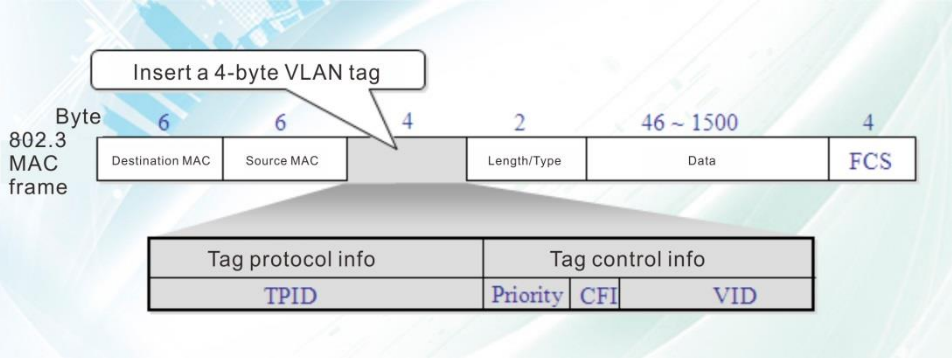
dispersed as they are logically related instead of physically on the same VLAN. Thus network administrators do not need to re-configure the network when a VLAN member changes its location.

- Better network security. PCs in different VLANs cannot intercommunicate directly. Inter-VLAN communication can only be achieved using a router or other layer 3 devices that are able to perform Layer 3 forwarding, which can ensure better security for different departments in enterprise networking.

This device supports 802.1Q VLAN, Port VLAN and voice VLAN. Next we will give explanations one by one.

1 802.1Q VLAN

Officially issued by IEEE in 1999, 802.1Q is used for regulating international VLAN standard and makes VLAN intercommunication among different vendors' devices possible. As defined in IEEE 802.1Q, a four-byte VLAN tag is inserted after the source MAC field to identify frames of different VLANs.



Explanations for 802.1Q tag are described below:

Field	Description
TPID	A 16-bit field set to a value of 0x8100 in order to identify the frame as an IEEE 802.1Q-tagged frame.
Priority	A 3-bit field with a valid range of 0~7 to identify packet frame priority. When blocking occurs, packets with higher priority will be sent out preferentially.
CFI	A 1-bit field for identifying whether the MAC address is encapsulated in the standard format. A value of 0 indicates that MAC addresses are encapsulated in the standard format. A value of 1 indicates that MAC addresses are encapsulated in a non-standard format. For Ethernet switches, it is set to 0 by default.

VID	VLAN ID, a 12-bit field specifying the VLAN to which the frame belongs. The VLAN ID range is 0 to 4095. Usually, 0 and 4095 are reserved, so a VLAN ID actually ranges from 1 to 4094.

➘ Three types of port link

When creating the 802.1Q VLAN, you should set the link type for the port according to its connected device. The link types of port include the following three types:

- Trunk: A trunk port can carry multiple VLANs to receive and send traffic for them. Usually, ports for switch cascade are configured as trunk ports.
- Hybrid: Like a trunk port, a hybrid port can carry multiple VLANs to receive and send traffic for them. It can be used for switch cascade or connecting to terminal devices.

➘ Processing relationship between PVID and VLAN packets

PVID (Port VLAN ID) is the default VLAN ID that a port belongs to. PVID indicates the ID of a default VLAN that a port belongs to. The PVID for an access port is the ID of the VLAN it belongs to; the default PVID for a trunk/hybrid port is "1" and this value is configurable.

This switch does not support ingress filter. When only 802.1Q VLAN is configured, Tag packets of ingress ports will be forwarded to ports in the corresponding VLAN in terms of VID; Untagged packets of ingress ports will be forwarded to ports in the corresponding VLAN in terms of these ports' PVID.

Different packets, tagged or untagged, will be processed in different ways, after being received by ports of different link types, which is illustrated in the following table:

Port Link Type	**Receiving Packets**		**Forwarding Packets**
	Receiving Tagged Packets	**Receiving Untagged Packets**	
Access	Packets will be forwarded to other ports in the corresponding VLAN according to the VID in the Tag.	Packets will be forwarded to other ports in the corresponding VLAN according to PVID on this port.	Packets will be forwarded after removing VLAN tags.
Trunk			If the VID of packet is the same as its PVID, the packet will be forwarded after removing its VLAN tag; If the VID of packet is not the same as its PVID, the packet will be directly forwarded.

Hybrid			If the VID value of the packet belongs to Tagged VLAN, the packet will be forwarded with Tag; If the VID value of the packet belongs to Untagged VLAN, the packet will be forwarded after removing its VLAN tag.

➘ 802.1Q VLAN configuration

This section includes the following four parts: VLAN Mode Toggle, 802.1Q VLAN, Trunk Port and Hybrid Port.

VLAN Mode Toggle: Used for toggling 802.1Q VLAN and Port VLAN.

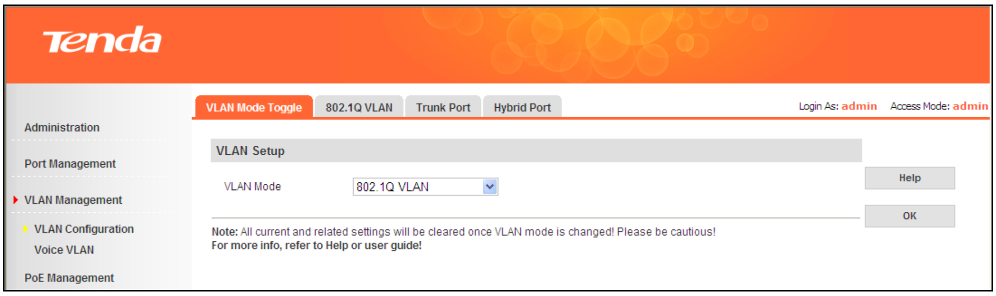
802.1Q VLAN: Used for configuring and displaying 802.1Q VLAN.

Trunk Port: Used for configuring Trunk ports.

Hybrid Port: Used for configuring Hybrid ports.

1.1 VLAN Mode Toggle

Click **VLAN Management > VLAN Configuration > VLAN Mode Toggle** to enter page below to set VLAN mode to 802.1Q VLAN.



VLAN Setup

VLAN Mode: 802.1Q VLAN

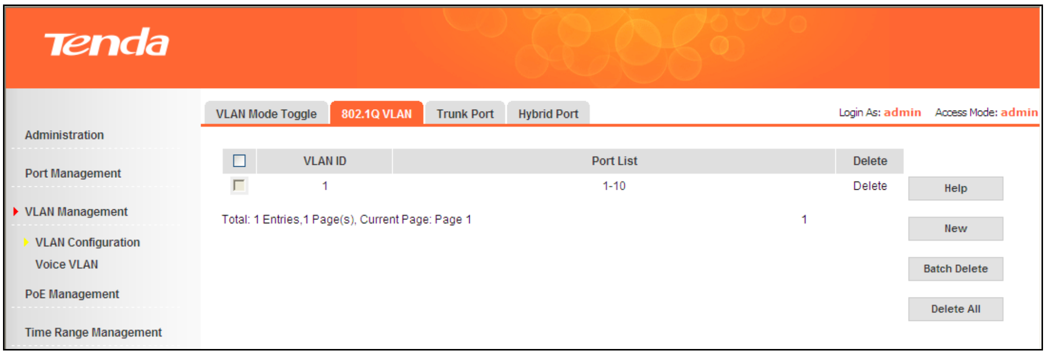
Note: All current and related settings will be cleared once VLAN mode is changed! Please be cautious!
For more info, refer to Help or user guide!

Note:

- Once VLAN mode is toggled from 802.1Q VLAN to Port VLAN, all configurations, including MAC filter, static MAC address and port isolation, related to 802.1Q VLAN will be cleared.
- If you want to enable Port VLAN, please ensure voice VLAN is disabled.

1.2 802.1Q VLAN

Click **VLAN Management > VLAN Configuration > 802.1Q VLAN** to enter page below to create 802.1Q VLAN.

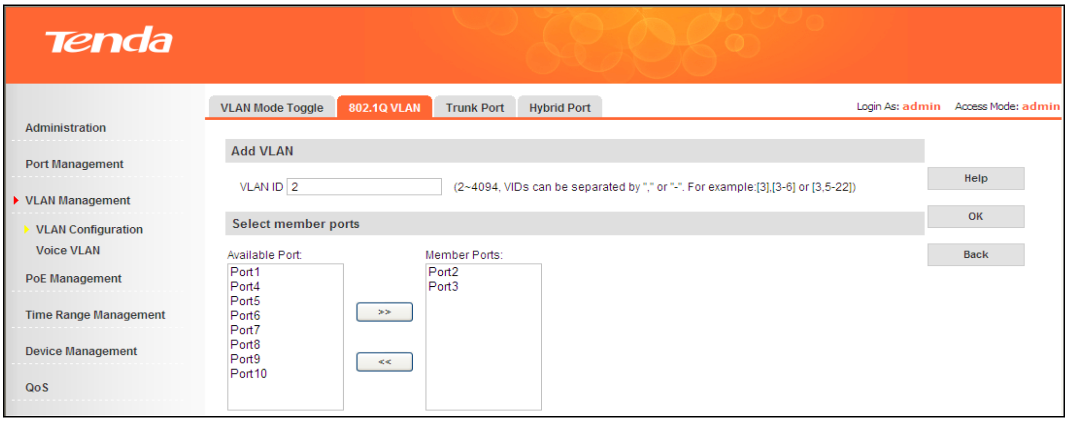


□	VLAN ID	Port List	Delete
□	1	1-10	Delete

Total: 1 Entries,1 Page(s), Current Page: Page 1 1

Add 802.1Q VLAN:

1. Click **New**;
2. Type in the VLAN ID;
3. Select ports which belong to the VLAN ID;



Add VLAN

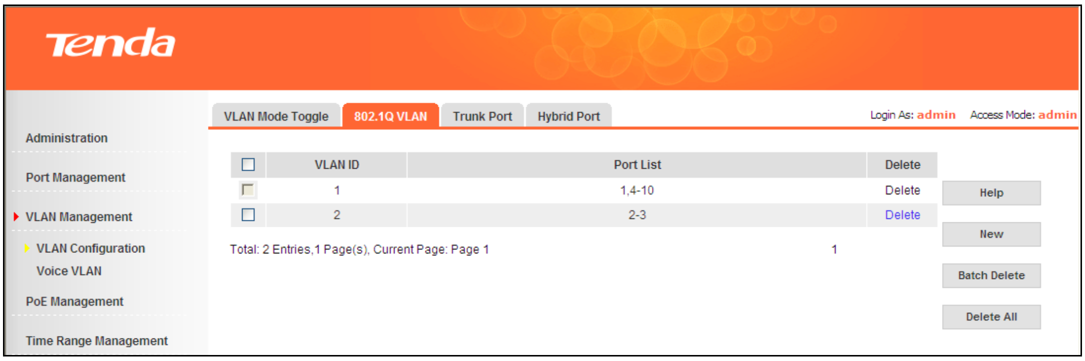
VLAN ID 2 (2~4094, VIDs can be separated by "," or "-". For example:[3],[3-6] or [3,5-22])

Select member ports

Available Port: Port1 Port4 Port5 Port6 Port7 Port8 Port9 Port10

Member Ports: Port2 Port3

4. Click **OK**.



□	VLAN ID	Port List	Delete
□	1	1,4-10	Delete
□	2	2-3	Delete

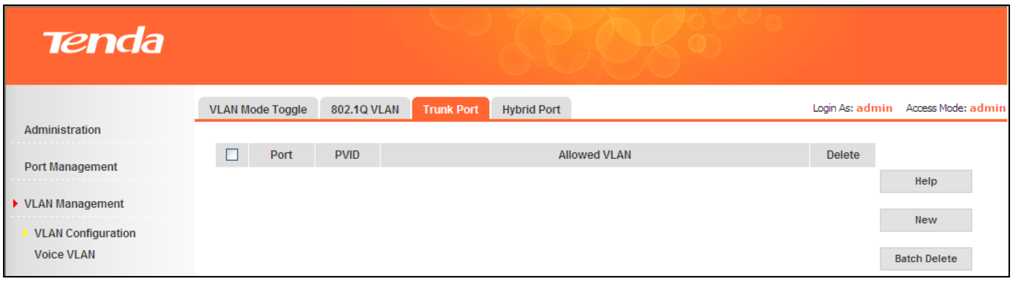
Total: 2 Entries,1 Page(s), Current Page: Page 1 1

Tip:

- Up to 20 characters are allowed for VLAN ID. When multiple values are entered, ports will be not selectable. And at this time, if you click **OK**, multiple empty VLANs will be created. For example, if you enter “2-10” in the VLAN ID field, 9 empty QVLANs will be configured; If you enter “2, 10” in the VLAN ID field, two empty QVLANs will be configured.
- By default, all ports belong to 802.1Q VLAN1. If a VLAN ID is deleted, ports included in this VLAN will belong to 802.1Q VLAN1 automatically.
- Up to 64 802.1Q VLANs can be configured.

1.3 Trunk Port

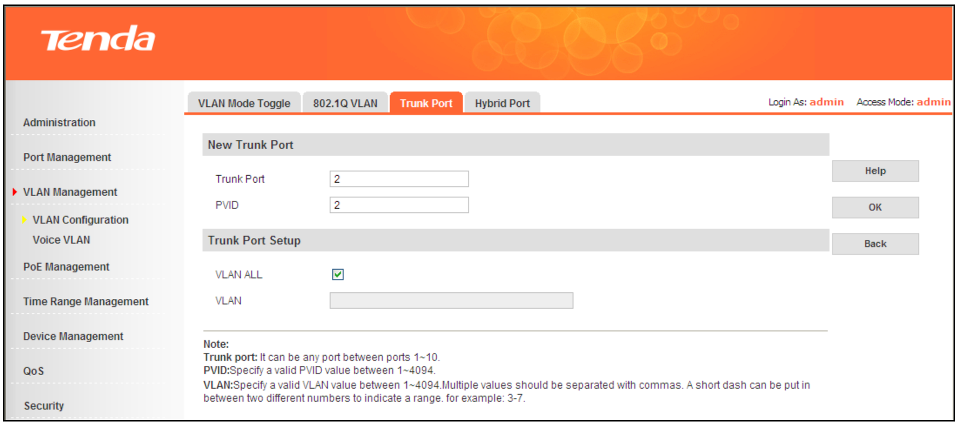
In 802.1Q VLAN mode, port link type is Access by default. If you want to change the port link type to Trunk, click **VLAN Management > VLAN Configuration > Trunk Port** to enter page below:



□	Port	PVID	Allowed VLAN	Delete

Add Trunk ports:

1. Click **New**;
2. Enter the trunk port number you wish to configure;
3. Enter the Trunk port’s PVID and the corresponding VLAN should already exist;
4. Configure VLANs the port belongs to. You can check **VLAN ALL** or enter specific VLAN numbers in the **VLAN** field;



New Trunk Port

Trunk Port: 2

PVID: 2

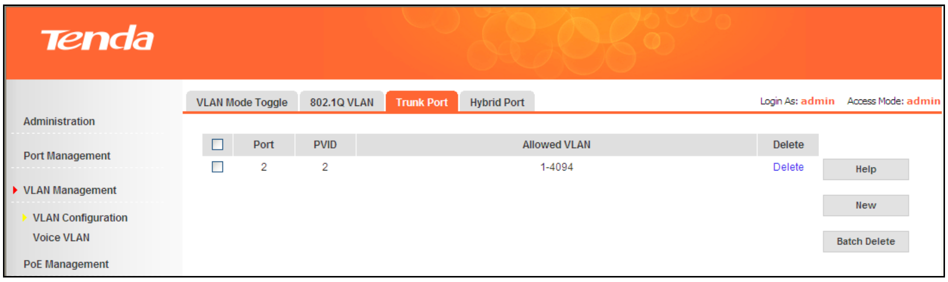
Trunk Port Setup

VLAN ALL ☑

VLAN

Note:
Trunk port: It can be any port between ports 1~10.
PVID:Specify a valid PVID value between 1~4094.
VLAN:Specify a valid VLAN value between 1~4094.Multiple values should be separated with commas. A short dash can be put in between two different numbers to indicate a range. for example: 3-7.

5. Click **OK**.

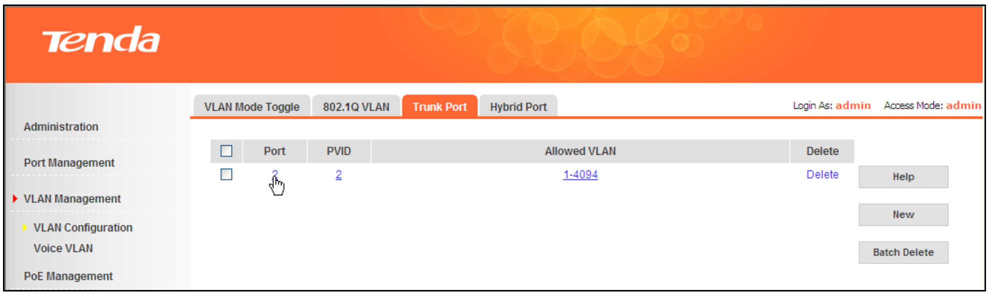


□	Port	PVID	Allowed VLAN	Delete
□	2	2	1-4094	Delete

Edit Trunk ports:

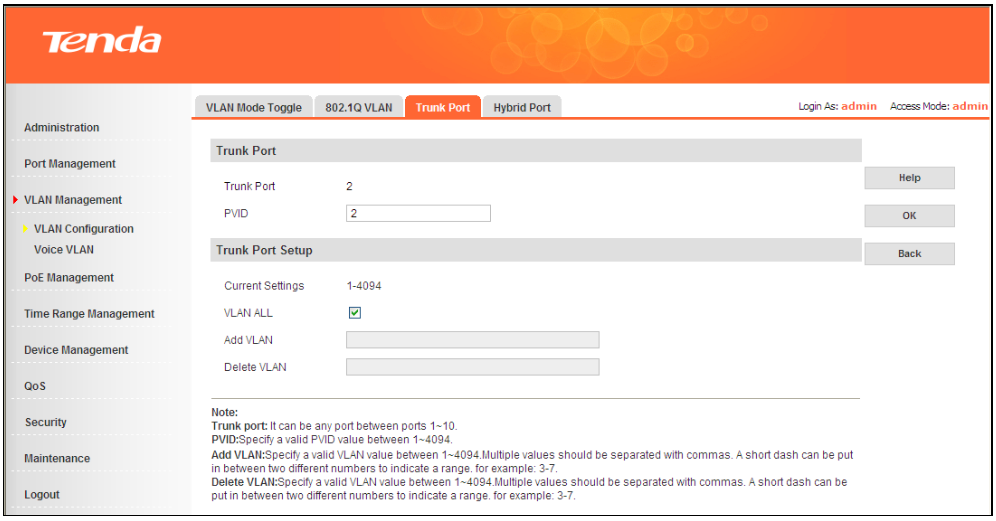
To modify some parameters of Trunk ports, such as PVID, VLAN, see steps below:

1. Click the corresponding Trunk port number on the **Trunk Port** page;



□	Port	PVID	Allowed VLAN	Delete
□	2	2	1-4094	Delete

2. Modify parameters on the appearing page;



Trunk Port

Trunk Port	2
PVID	2

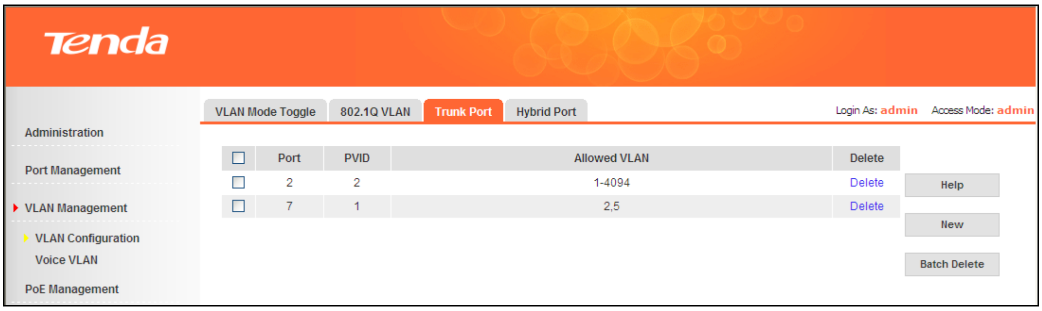
Trunk Port Setup

Current Settings	1-4094
VLAN ALL	☑
Add VLAN	
Delete VLAN	

Note:
Trunk port: It can be any port between ports 1~10.
PVID: Specify a valid PVID value between 1~4094.
Add VLAN: Specify a valid VLAN value between 1~4094.Multiple values should be separated with commas. A short dash can be put in between two different numbers to indicate a range. for example: 3-7.
Delete VLAN: Specify a valid VLAN value between 1~4094.Multiple values should be separated with commas. A short dash can be put in between two different numbers to indicate a range. for example: 3-7.

Delete Trunk ports:

Firstly, click **VLAN Management > VLAN Configuration > Trunk Port** to enter Trunk port display page.



□	Port	PVID	Allowed VLAN	Delete
□	2	2	1-4094	Delete
□	7	1	2,5	Delete

Click **Delete** behind the corresponding port number.

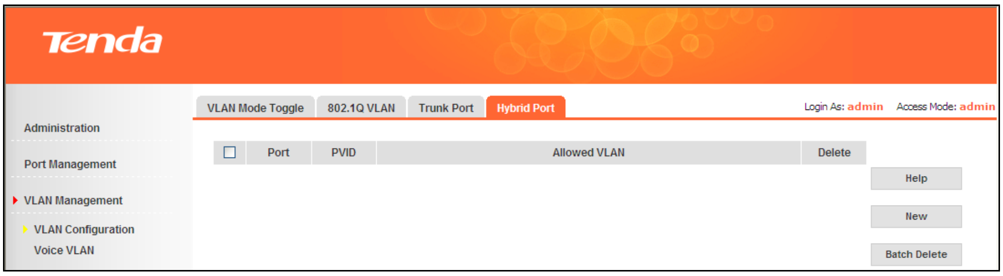
To batch delete Trunk ports, check ports you wish to delete and click **Batch Delete**.

Tip:

- A port cannot be configured to be the Hybrid port and Trunk port at the same time. If you want to set a Hybrid port to be a Trunk port, you need to delete Hybrid port settings for this port first.
- Deleted Trunk ports will be assigned to VLAN1 automatically and port link type will be changed to Access ports.

1.4 Hybrid Port

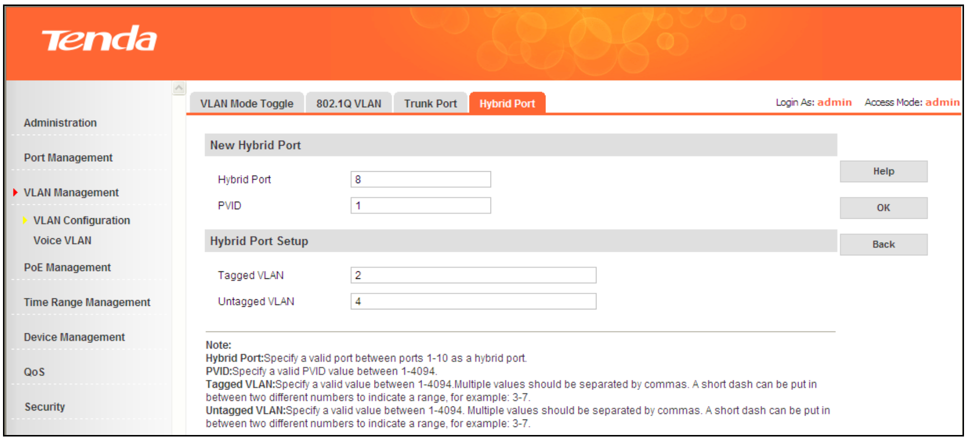
In 802.1Q VLAN mode, port link type is Access by default. If you want to change the port link type to Hybrid, click **VLAN Management > VLAN Configuration > Hybrid Port** to enter page below:



□	Port	PVID	Allowed VLAN	Delete

Add Hybrid ports:

1. Click **New**;
2. Enter the Hybrid port number you wish to within the valid range of 1~10;
3. Enter the Hybrid port’s PVID and verify that the corresponding VLAN has already existed;
4. Configure Tagged VLAN (range: 1~4094, null);
5. Configure Untagged VLAN (range: 1~4094, null);



New Hybrid Port

Hybrid Port: 8

PVID: 1

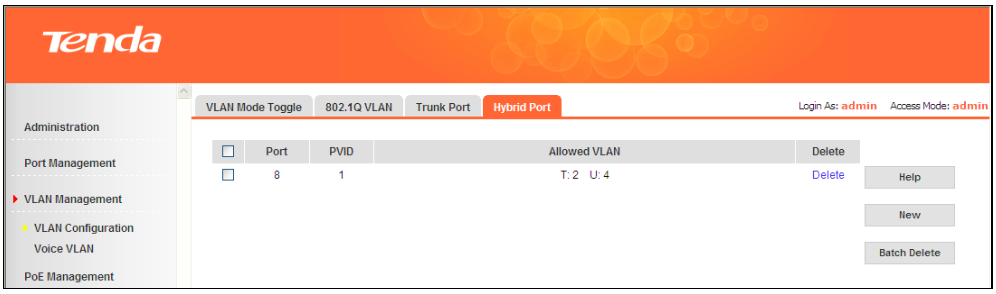
Hybrid Port Setup

Tagged VLAN: 2

Untagged VLAN: 4

Note:
Hybrid Port: Specify a valid port between ports 1-10 as a hybrid port.
PVID: Specify a valid PVID value between 1-4094.
Tagged VLAN: Specify a valid value between 1-4094.Multiple values should be separated by commas. A short dash can be put in between two different numbers to indicate a range, for example: 3-7.
Untagged VLAN: Specify a valid value between 1-4094. Multiple values should be separated by commas. A short dash can be put in between two different numbers to indicate a range, for example: 3-7.

6. Click **OK**.



□	Port	PVID	Allowed VLAN	Delete
□	8	1	T: 2 U: 4	Delete

2 Port VLAN

Port VLAN may be the easiest and most effective solution for partitioning VLAN. Users in the same VLAN can intercommunicate with each other and the same user can belong to multiple VLANs. For example, if port 1 and port 2 join a VLAN, and port 1 and port 3 join another VLAN, all data on port 2 and port 3 will only be forwarded to port 1. In this way, a link has been established between port 1 and port 2, 3 and no link is established between port 2 and port 3.

Tip:

Port VLAN and 802.1Q VLAN can be toggled randomly. If you toggle 802.1Q VLAN to port VLAN, related VLAN configurations, such as MAC filter, static MAC addresses and port isolation, will be cleared.

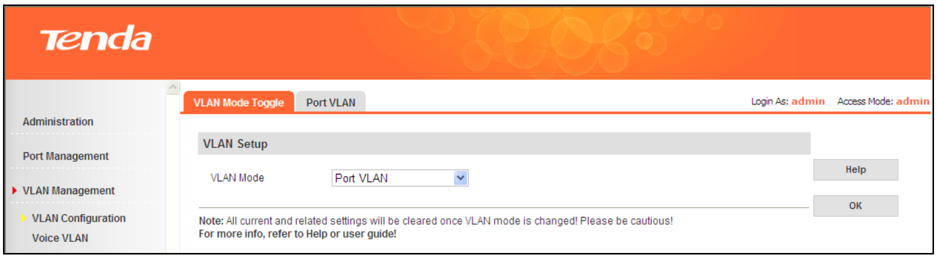
This section includes two parts: VLAN Mode Toggle and Port VLAN.

VLAN Mode Toggle: Used for toggling 802.1Q VLAN and Port VALN.

Port VLAN: Used for configuring and displaying Port VLAN.

2.1 VLAN Mode Toggle

To set VLAN mode to Port VLAN, click **VLAN Management > VLAN Configuration > VLAN Mode Toggle** to enter page below:



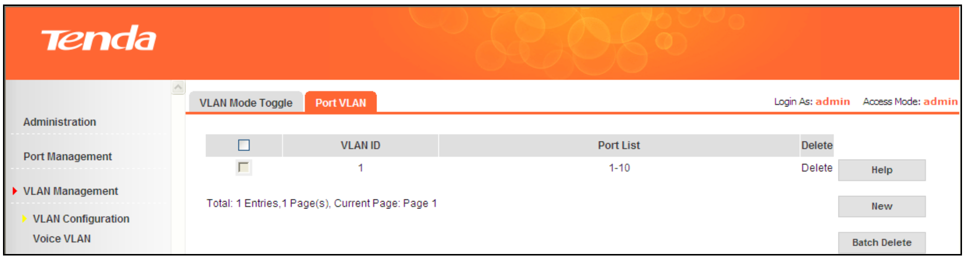
VLAN Setup

VLAN Mode: Port VLAN

Note: All current and related settings will be cleared once VLAN mode is changed! Please be cautious!
For more info, refer to Help or user guide!

2.2 Port VLAN

To create port VLANs, click **VLAN Management > VLAN Configuration > Port VLAN** to enter page below:

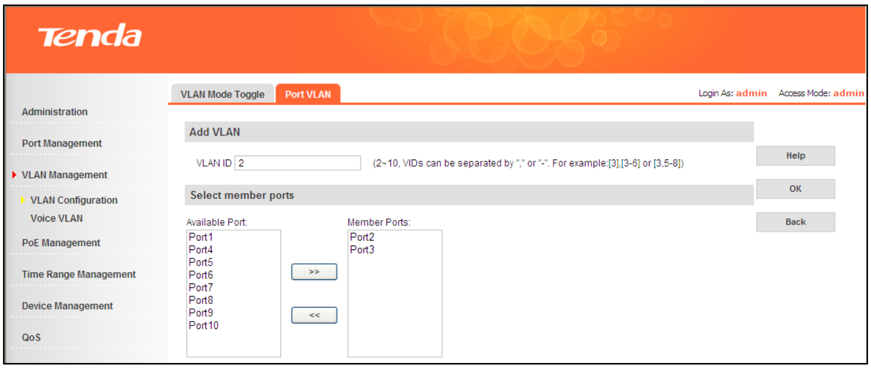


□	VLAN ID	Port List	Delete
□	1	1-10	Delete

Total: 1 Entries,1 Page(s), Current Page: Page 1

Add Port VLAN:

1. Click **New** to enter page below;
2. Follow onscreen rules to enter VLAN IDs;
3. Select ports from the **Available Port** list and click 》 to add them into **Member Ports** list;



Login As: admin Access Mode: admin

Add VLAN

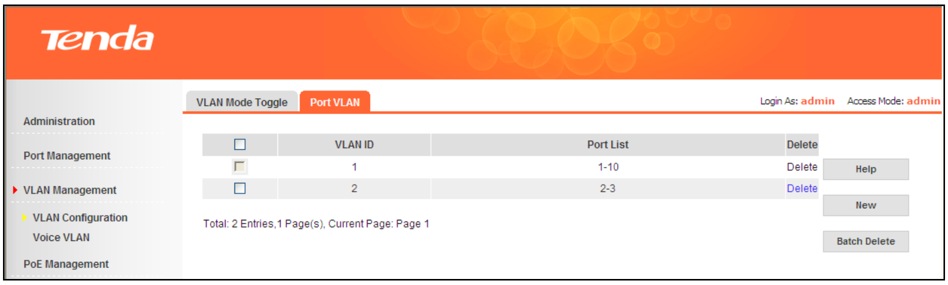
VLAN ID 2 (2~10, VIDs can be separated by "," or "-". For example:[3],[3-6] or [3,5-8])

Select member ports

Available Port: Port1 Port4 Port5 Port6 Port7 Port8 Port9 Port10

Member Ports: Port2 Port3

4. Click **OK**;



Login As: admin Access Mode: admin

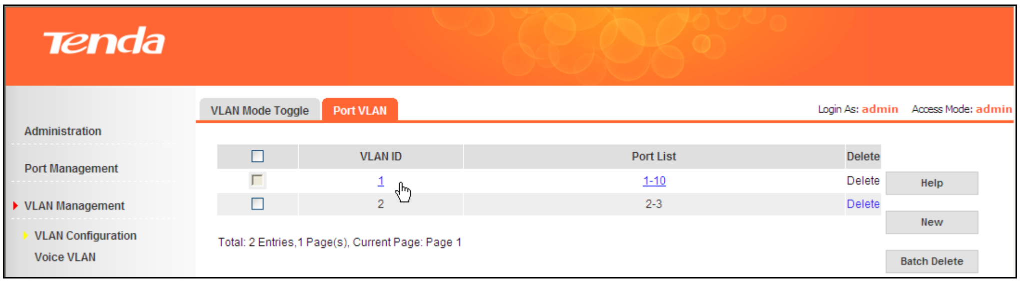
□	VLAN ID	Port List	Delete
□	1	1-10	Delete
□	2	2-3	Delete

Total: 2 Entries,1 Page(s), Current Page: Page 1

Edit port VLAN:

Click the corresponding port VLAN to enter the corresponding page to edit it. As mentioned above, Port 2 and port 3 are in VLAN1. If you want to isolate port 2, 3 from other ports, just delete port 2 and port 3 from VLAN1. Steps are as following:

1. Click VLAN1 on the **Port VLAN** page;

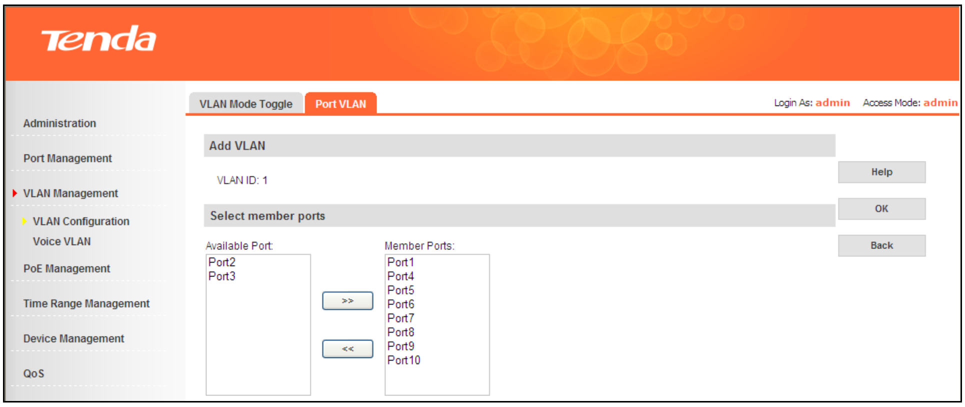


Login As: admin Access Mode: admin

□	VLAN ID	Port List	Delete
□	1	1-10	Delete
□	2	2-3	Delete

Total: 2 Entries,1 Page(s), Current Page: Page 1

2. Select ports you wish to delete from the **Member Ports** list and click << to add them into the **Available Port** list;



Login As: admin Access Mode: admin

Add VLAN

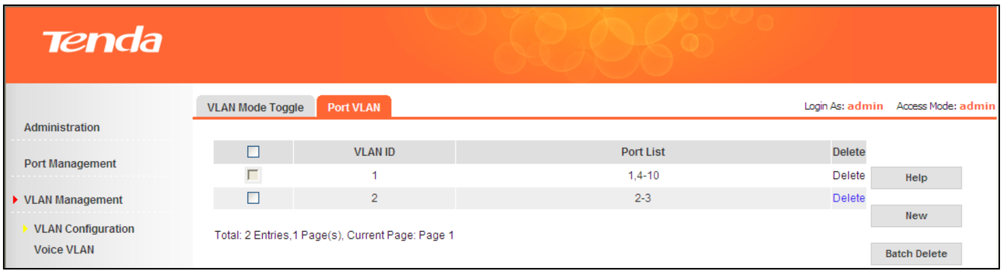
VLAN ID: 1

Select member ports

Available Port: Port2 Port3

Member Ports: Port1 Port4 Port5 Port6 Port7 Port8 Port9 Port10

3. Click **OK**.



□	VLAN ID	Port List	Delete
□	1	1,4-10	Delete
□	2	2-3	Delete

Total: 2 Entries,1 Page(s), Current Page: Page 1

Tip:

- Up to 10 port VLANs can be configured.
- Port VLAN cannot achieve inter-switch communication. Only ports that belong to the same VLAN on the same switch can intercommunicate.

3 Voice VLAN

With the development of voice technology, voice devices are becoming more and more widely used, especially in broadband resident districts. There are two kinds of traffic: voice traffic and business traffic. Usually, voice traffic boasts higher priority in transmission than business traffic to reduce delay and packets dropping.

Voice VLAN is a VLAN designed for voice data flow partition. By creating voice VLAN and adding ports connected to voice devices into the voice VLAN, you can centrally transmit data flow in the voice VLAN and it is very convenient to specifically configure QoS (Quality of Service), enhancing transmission priority of voice traffic and guaranteeing communication quality.

➘ Voice Stream Recognition

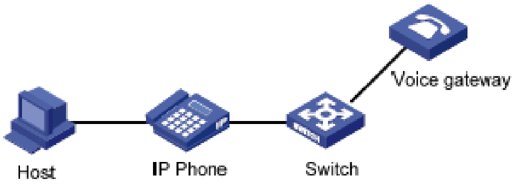
According to the source MAC fields of the ingress packets, this device can distinguish whether the data flow is voice data flow or not. If the source MAC address conforms to the voice device's OUI (Organizationally Unique Identifier) address, the packets will be regarded as voice data flow.

You can preset OUI address or use the default OUI address as the criteria. An Organizationally Unique Identifier (OUI) is a 24-bit number that uniquely identifies a vendor, manufacturer, or other organization globally or worldwide. This device supports OUI mask. You can adjust MAC address' matching depth by setting different masks.

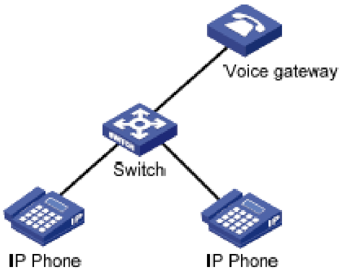
➘ Voice VLAN mode on different ports

Two voice VLAN modes are available on this device: auto and manual. Here auto or manual refers to how ports join voice VLAN.

Auto: In this mode, through untagged packets sent out by the IP telephone, the system can recognize source MACs of these packets to match OUI addresses. If matched successfully, the system will automatically add ingress ports into the voice VLAN and configure priority for these packets. Meanwhile, you can configure aging time of voice VLAN on this device. If within the aging time, the system does not receive any voice traffic from the ingress port, this port will be automatically removed from the voice VLAN. The whole add/remove process will be achieved automatically. The auto mode applies to PC-IP telephone serious connection, namely, voice traffic and business traffic are transmitted concurrently. See network topology below:



Manual: In this mode, you need to add the port connected to the IP telephone into voice VLAN manually. Then the system will try to match OUI addresses by recognizing source MACs of packets. If matched successfully, the system will issue ACL rules and configure priority for these packets. The whole add/remove process is implemented manually and the manual mode applies to IP telephone access alone, namely, only voice traffic is transmitted on this port in voice VLAN. This can make the port dedicated to voice traffic transmission, thus avoiding business traffic influence on voice traffic transmission.



➘ Voice VLAN supporting details on different link type ports

Voice VLAN supports transmitting voice data on Access, Trunk and Hybrid ports. Trunk and Hybrid ports of other VLANs on the switch can transmit voice and data traffic when voice VLAN feature is enabled. As IP phones vary, different ports need different supporting conditions. As for phones which obtain IP addresses and voice VLAN IDs automatically, supporting conditions on ports are described as below:

Voice VLAN Mode	Voice Traffic Type	Port Link Type
Auto	Tagged	Access: Not supported.
		Trunk: Supported, but the default VLAN of the

		access port must already exist and can't be voice VLAN. And the default VLAN is allowed on the access port.
		Hybrid: Supported, but the default VLAN of the access port must already exist and can't be voice VLAN. And the default VLAN should be in the allowed tagged VLAN list.
	Untagged	Access, Trunk, Hybrid: Not supported.
Manual	Tagged	Access: Not supported.
		Trunk: Supported, but the default VLAN of the access port must already exist and can't be voice VLAN. And the default VLAN is allowed on the access port.
		Hybrid: Supported, but the default VLAN of the access port must already exist and can't be voice VLAN. And the voice VLAN should be in the allowed tagged VLAN list.
	Untagged	Access: Supported, but the default VLAN of the access port must be voice VLAN.
		Trunk: Supported, but the default VLAN of the access port must be voice VLAN and voice VLAN is allowed on the access port.
		Hybrid: Supported, but the default VLAN of the access port must be voice VLAN and exist in allowed untagged VLAN list.

As for phones which require manually configured IP addresses and voice VLAN IDs, the matching relationship is relatively simple, for only tagged voice traffic can be sent.

Voice VLAN Mode	Port Link Type	Supporting Details
Auto	Access	Not supported.
	Trunk	Supported, but the default VLAN of the access port must already exist and can't be voice VLAN. And the default VLAN is allowed on the access port.

	Hybrid	Supported, but the default VLAN of the access port must already exist and can't be voice VLAN. And the default VLAN should be in the allowed tagged VLAN list.
Manual	Access	Not supported.
	Trunk	Supported, but the default VLAN of the access port must already exist and can't be voice VLAN. And the default VLAN is allowed on the access port.
	Hybrid	Supported, but the default VLAN of the access port must already exist and can't be voice VLAN. And voice VLAN should be in the allowed tagged VLAN list.

➘ Security Mode of Voice VLAN

Security Mode	Message Type	Process Mode
Disable	Untagged messages	No check for source MAC addresses of messages and all messages can be transmitted in voice VLAN.
	Voice-VLAN tagged messages	
	Other VLAN tagged messages	Messages' forwarding depends on their VIDs and won't be affected by voice VLAN security mode.
Enable	Untagged messages	When source MAC address of the message is a recognizable OUI address, this message can be transmitted in voice VLAN, otherwise it will be dropped.
	Voice-VLAN tagged messages	
	Other VLAN tagged messages	Messages' forwarding depends on their VIDs and won't be affected by voice VLAN security mode.

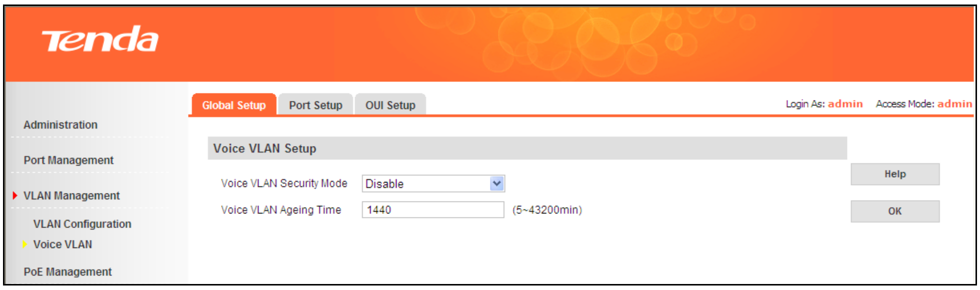
It is strongly not suggested to transmit both voice and business traffic in voice VLAN. If you have to, please disable Voice VLAN Mode.

3.1 Global Setup

Click **VLAN Management > Voice VLAN > Global Setup** to configure voice VLAN mode settings and voice VLAN aging time.

Note:

If you want to configure voice VLAN settings, please keep your VLAN mode in 802.1Q VLAN.



Voice VLAN Setup

Voice VLAN Security Mode: Disable

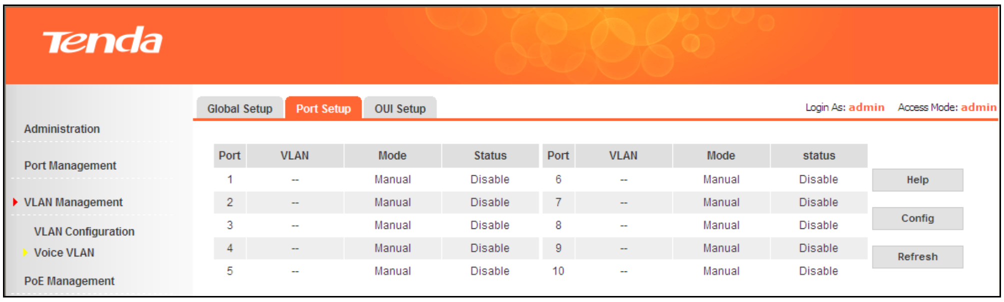
Voice VLAN Ageing Time: 1440 (5~43200min)

Parameters on the page are described below:

Field	Description
Voice VLAN Security Mode	Configure how ports forward messages. **Disable:** All messages will be forwarded. **Enable:** Only voice traffic will be forwarded.
Voice VLAN Aging Time	As for the port joining voice VLAN under auto mode, if the system doesn't receive any voice message after ageing time, this port will be removed from voice VLAN automatically. As for the port joining voice VLAN under manual mode, you need to delete it manually.

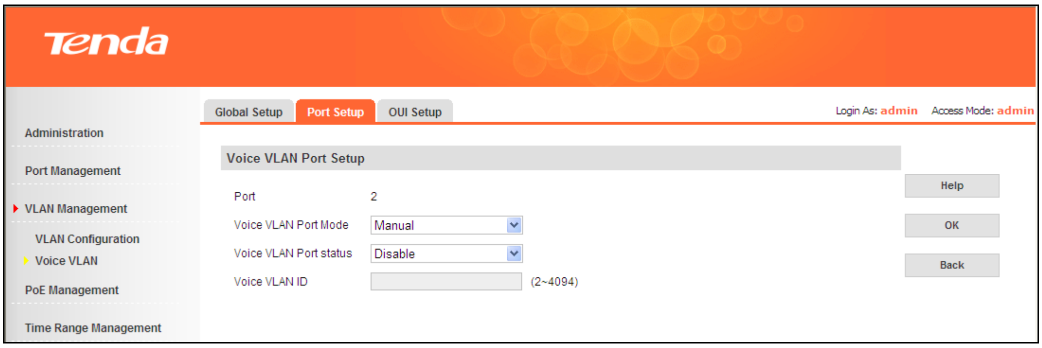
3.2 Port Setup

Click **VLAN Management > Voice VLAN > Port Setup** to enter VLAN port setup page.



Port	VLAN	Mode	Status	Port	VLAN	Mode	status
1	--	Manual	Disable	6	--	Manual	Disable
2	--	Manual	Disable	7	--	Manual	Disable
3	--	Manual	Disable	8	--	Manual	Disable
4	--	Manual	Disable	9	--	Manual	Disable
5	--	Manual	Disable	10	--	Manual	Disable

To configure voice VLAN settings on a single port, click the corresponding port number on the Port Setup page.



Voice VLAN Port Setup

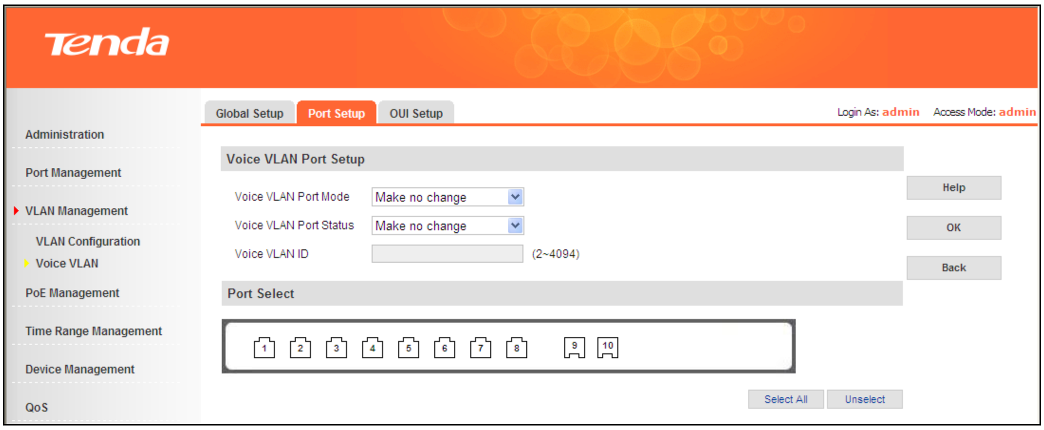
Port 2

Voice VLAN Port Mode: Manual

Voice VLAN Port status: Disable

Voice VLAN ID: (2~4094)

To batch configure voice VLAN settings, click **Config** on the Port Setup page.



Voice VLAN Port Setup

Voice VLAN Port Mode: Make no change

Voice VLAN Port Status: Make no change

Voice VLAN ID: (2~4094)

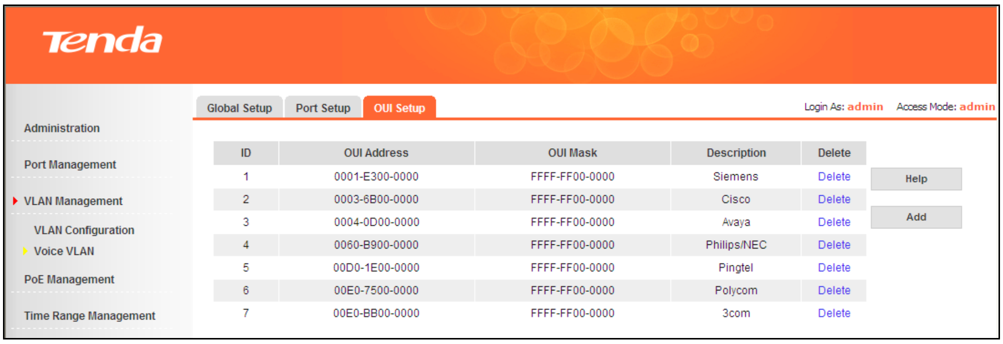
Port Select

Parameters on the page are described below:

Field	Description
Port	Display port number.
Voice VLAN Port Mode	Select voice VLAN working mode: Auto or Manual. If it is Manual, age time of voice VLAN becomes invalid.
Voice VLAN Port Status	Enable/Disable port voice VLAN feature
Voice VLAN ID	Configure port voice VLAN ID

3.3 OUI Setup

Click **VLAN Management > Voice VLAN > OUI Setup** to enter page below:

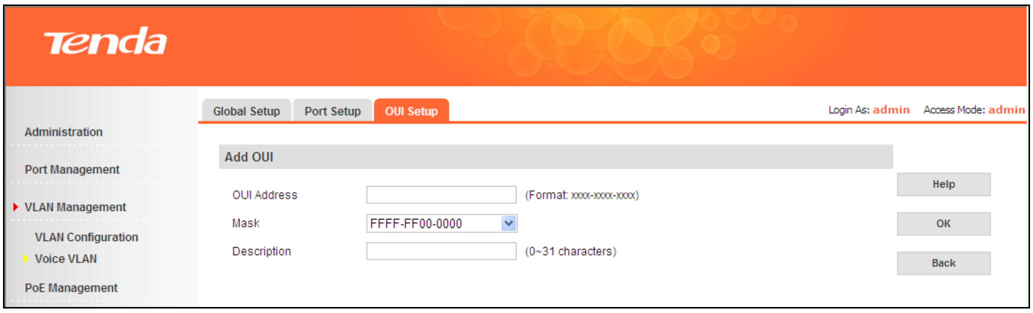


ID	OUI Address	OUI Mask	Description	Delete
1	0001-E300-0000	FFFF-FF00-0000	Siemens	Delete
2	0003-6B00-0000	FFFF-FF00-0000	Cisco	Delete
3	0004-0D00-0000	FFFF-FF00-0000	Avaya	Delete
4	0060-B900-0000	FFFF-FF00-0000	Philips/NEC	Delete
5	00D0-1E00-0000	FFFF-FF00-0000	Pingtel	Delete
6	00E0-7500-0000	FFFF-FF00-0000	Polycom	Delete
7	00E0-BB00-0000	FFFF-FF00-0000	3com	Delete

By default, recognizable OUI addresses of this switch are described as below:

ID	OUI Address	OUI Mask	Description
1	0001-E300-0000	FFFF-FF00-0000	Siemens
2	0003-6B00-0000	FFFF-FF00-0000	Cisco
3	0004-0D00-0000	FFFF-FF00-0000	Avaya
4	0060-B900-0000	FFFF-FF00-0000	Philips/NEC
5	00D0-1E00-0000	FFFF-FF00-0000	Pingtel
6	00E0-7500-0000	FFFF-FF00-0000	Polycom
7	00E0-BB00-0000	FFFF-FF00-0000	3com

You can also click **Add** on the OUI Setup page to add OUI addresses manually.



Login As: admin Access Mode: admin

Add OUI

OUI Address (Format: xxxx-xxxx-xxxx)

Mask FFFF-FF00-0000

Description (0~31 characters)

Parameters on the page are described below:

Field	Description
OUI Address	Used for recognizing source MAC addresses sent by voice devices.
Mask	Select the corresponding OUI mask from the drop-down list. The default is FFFF-FF00-0000, indicating only the top 24 bits must match the OUI address, can it be recognized as voice stream and the last 24 bits are arbitrary.
Description	Description of the corresponding manufacturer for a certain OUI address or other info.

PoE Management

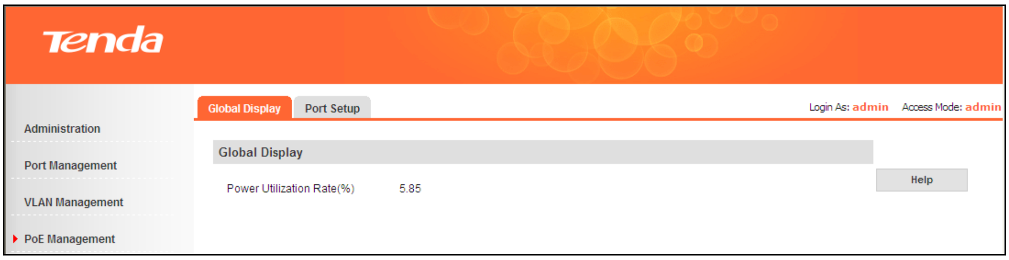
In traditional networking, all terminal devices are applying power supply directly via power lines, leading to high expenses and complicated cabling work.

Power over Ethernet or PoE describes any of several standardized or ad-hoc systems which pass electrical power along with data on Ethernet cabling. It not only ensures normal network operation, but greatly reduces expenses. PoE allows cable as long as 100m. This allows a single cable to provide both data connection and electrical power to devices such as network hubs, IP cameras, wireless APs and closed-circuit TV cameras, etc. The IEEE standard for PoE requires category 5 cable or higher for high power levels, but can operate with category 3 cable if less power is required.

8 10/100/1000M auto-negotiation RJ45 ports of this switch are IEEE 802.3af, IEEE 802.3at PoE capable, which allows it to connect to up to 8 IEEE 802.3 af PDs or 4 IEEE 802.3at PDs. The PoE power supply mode is dynamic, i.e. the switch accommodates power supply for powered devices automatically. Pair 1, 2 and pair 3, 6 are applying PoE power supply and Ethernet specifications limit the cable length between the switch and the attached device to 100 m (328 ft).

1 Global Display

If you want to have a glance of power utilization of this switch, click **PoE Management > Global Display** to enter page below:

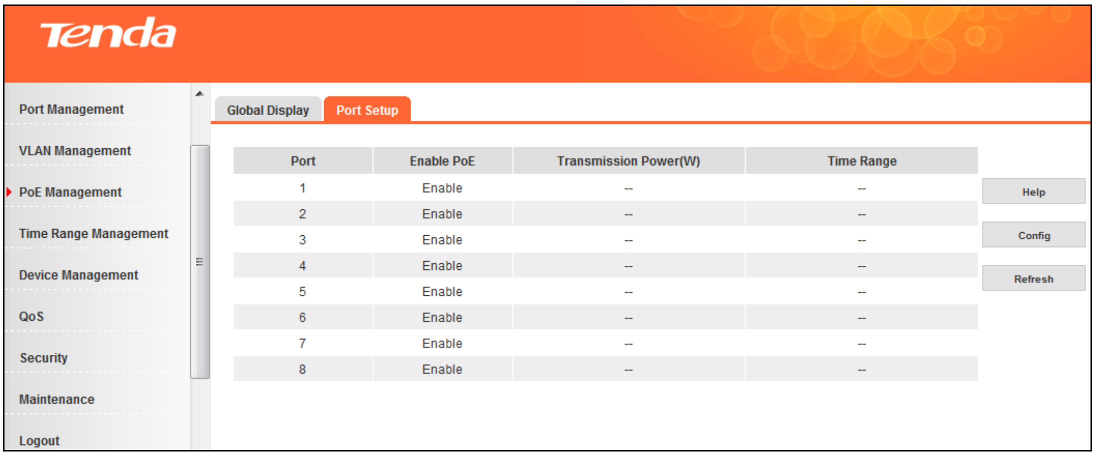


Global Display

Power Utilization Rate(%) 5.85

2 Port Setup

By default, all RJ45 ports of this switch are PoE-enabled. Click **PoE Management > Port Setup** to view power utilization of all RJ45 ports or modify port PoE properties.



Port	Enable PoE	Transmission Power(W)	Time Range
1	Enable	--	--
2	Enable	--	--
3	Enable	--	--
4	Enable	--	--
5	Enable	--	--
6	Enable	--	--
7	Enable	--	--
8	Enable	--	--

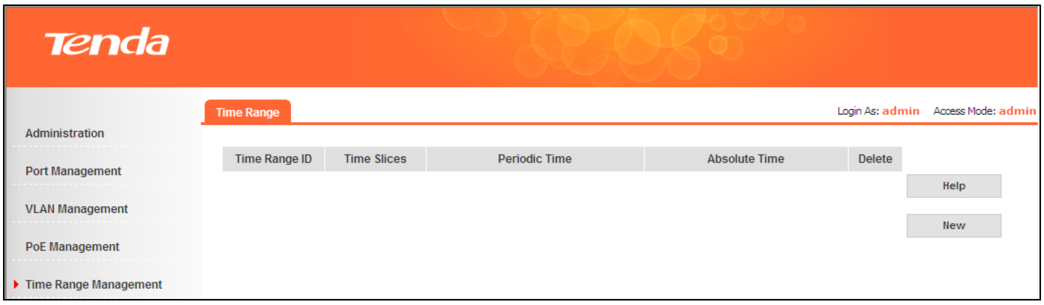
Parameters on this page are described below:

Field	Description
Enable PoE	Enable/Disable PoE feature. Only PoE feature is enabled on the port, can PoE function takes effect.
Transmission Power	Display PoE power on the corresponding port. The unit is W. Note that there may be errors on values displayed on the page.
Time Range	Configure the current port's specified time range ID (You need to configure time range on the **Time Range Management** page first). Unspecified means no time limit.

Time Range Management

Time range is used for describing a special time range, via which you can customize this switch’s PoE power supply time range, achieving smart power management and saving resources.

Click **Time Range Management** to enter page below:

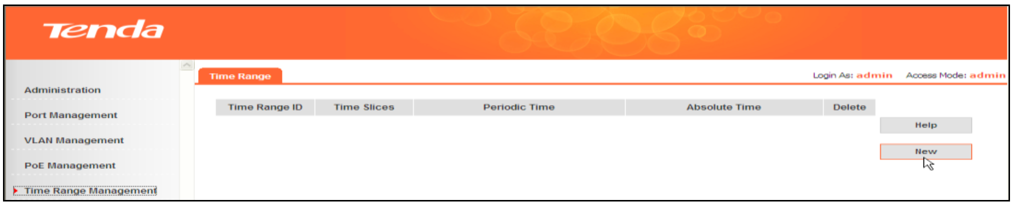


Parameters on this page are described below:

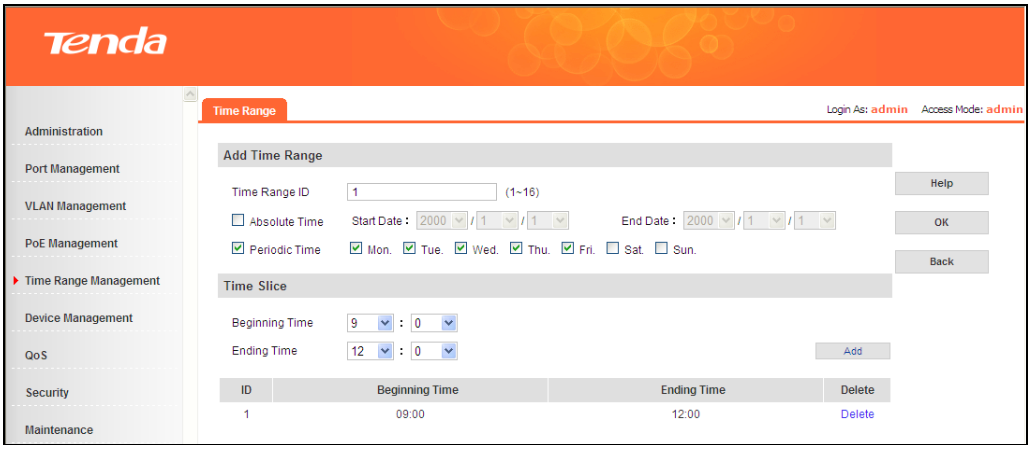
Field	Description
Time Range ID	The corresponding time range ID
Time Slices	Display total time slices of this time range. Up to 4 entries can be configured.
Periodic Time	Display this time range's periodic time (from Mon. to Sun.). If Absolute Time is selected, this option will display“--”.
Absolute Time	Display this time range's absolute time (from 2000, January 1st to 2035, December 31th). If Periodic Time is selected, this option will display “--”.

Create new time range:

1. Click **New**;



2. Specify the time range ID on the appearing page;
3. Check **Absolute Time** or **Periodic Time** and configure the corresponding date info;
4. Select the beginning time and ending time for **Time Slice**;
5. Click **Add** to add the configured time slice into the time slice list;



Add Time Range

Time Range ID 1 (1~16)

□ Absolute Time Start Date : 2000 / 1 / 1 End Date : 2000 / 1 / 1

☑ Periodic Time ☑ Mon. ☑ Tue. ☑ Wed. ☑ Thu. ☑ Fri. □ Sat. □ Sun.

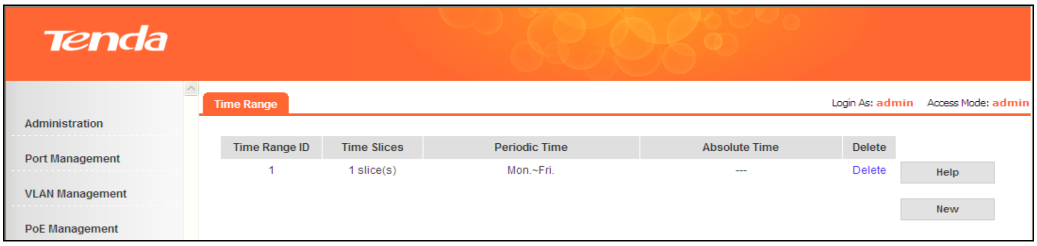
Time Slice

Beginning Time 9 : 0

Ending Time 12 : 0

ID	Beginning Time	Ending Time	Delete
1	09:00	12:00	Delete

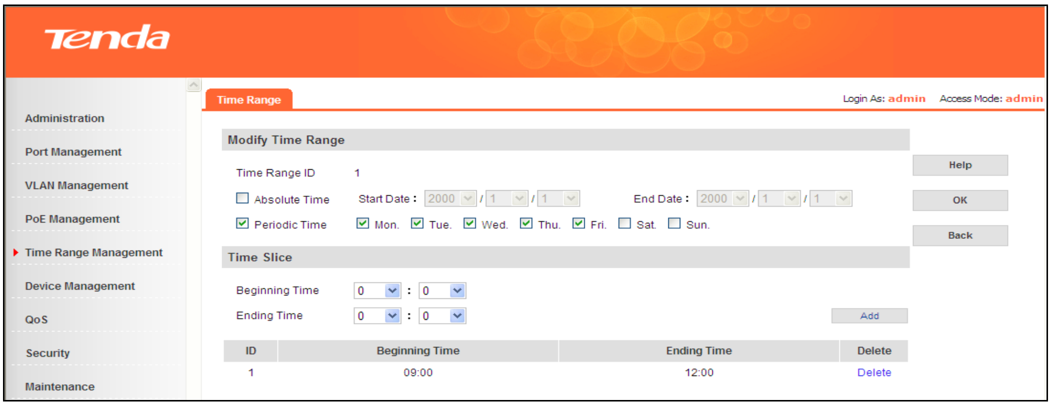
6. Click **OK** to save your settings.



Time Range ID	Time Slices	Periodic Time	Absolute Time	Delete
1	1 slice(s)	Mon.~Fri.	---	Delete

Edit time range:

If you want to modify a certain time range, click the corresponding time range ID to enter similar page below:



Modify Time Range

Time Range ID 1

□ Absolute Time Start Date : 2000 / 1 / 1 End Date : 2000 / 1 / 1

☑ Periodic Time ☑ Mon. ☑ Tue. ☑ Wed. ☑ Thu. ☑ Fri. □ Sat. □ Sun.

Time Slice

Beginning Time 0 : 0

Ending Time 0 : 0

ID	Beginning Time	Ending Time	Delete
1	09:00	12:00	Delete

Device Management

This section helps you enhance the switch's traffic forwarding capacity and manage the switch efficiently. The following five parts are included:

MAC: Manage this switch's MAC address forwarding table.

STP: Eliminate physical loop in data link layer, avoid broadcast storm and provide link backup redundancy.

IGSP: Manage and control multicast groups to save network bandwidth, to ensure better multicast security and to make each host's separate billing convenient.

SNMP: Manage the switch efficiently.

DHCP Snooping: Protect the DHCP server in local area network, prevent the DHCP server from being cheated and keep DHCP addresses from being used up.

1 MAC

The switch forwards frames in data link layer. In this process, by learning source MAC addresses of these frames, the switch will create the MAC address forwarding table, MAC address, VLAN ID (if there is), port number included.

When forwarding a frame, the device adopts the following forwarding modes based on the MAC address table:

- Unicast mode: If an entry is available for the destination MAC address, the device will forward the frame to the outgoing port indicated by the MAC address table entry.
- Broadcast mode: If the device receives a frame with the destination address whose lowest bit of the second byte is 1, or no entry is available for the destination MAC address, the device forwards the frame to all ports except the receiving port, i.e. broadcast packets, multicast packets and unknown unicast packets will be forwarded.

➘ MAC Forwarding Table Aging Scheme

To adapt to network changes and prevent inactive entries from occupying limited table space, an aging mechanism is adopted for dynamic MAC address entries. This aging mechanism ensures that the MAC address table can quickly update to accommodate the latest network changes.

Each time a dynamic MAC address entry is obtained or created, an aging timer starts (To configure MAC age, click **Administration > System Configuration > System info**). If the entry has not updated when the aging timer expires, the device deletes the entry.

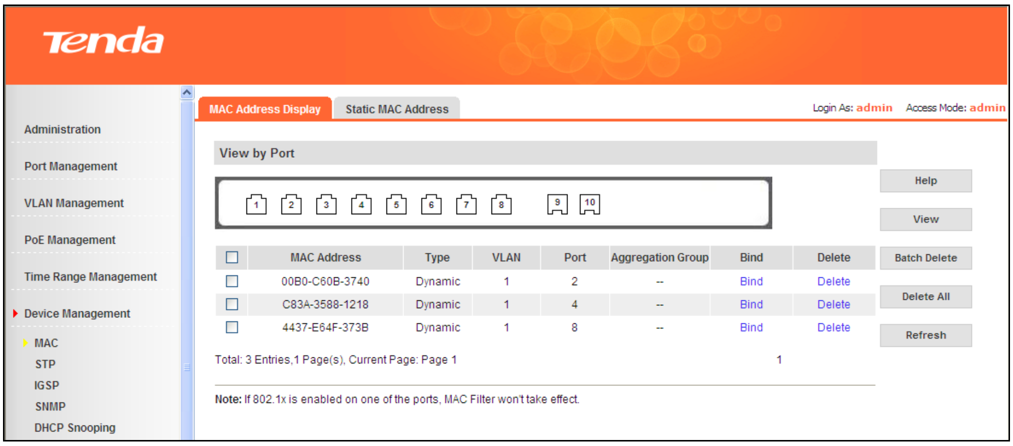
➘ Types of MAC address table entries

In terms of configuration method and respective features, MAC address table entries can be divided into two categories:

- Static MAC entries, also known as "Permanent Address", which are manually added and never age out. For a small network with little change, adding static MAC address entry manually may effectively reduce broadcast traffic.
- Dynamic MAC entries, which can be manually added or dynamically learned and might age out.

1.1 MAC Address Display

Click **Device Management > MAC > MAC Address Display** to view dynamic MAC address entries of this switch.



□	MAC Address	Type	VLAN	Port	Aggregation Group	Bind	Delete
□	00B0-C60B-3740	Dynamic	1	2	--	Bind	Delete
□	C83A-3588-1218	Dynamic	1	4	--	Bind	Delete
□	4437-E64F-373B	Dynamic	1	8	--	Bind	Delete

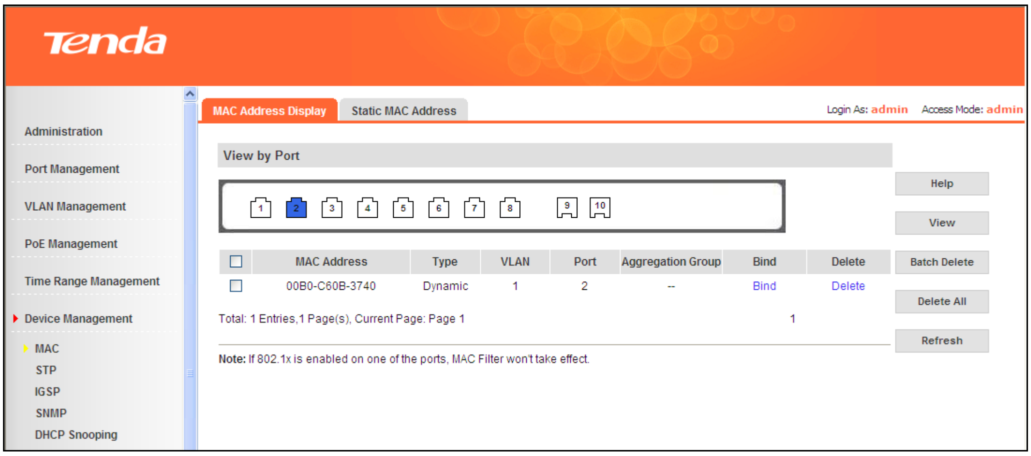
Total: 3 Entries,1 Page(s), Current Page: Page 1 1

Note: If 802.1x is enabled on one of the ports, MAC Filter won't take effect.

Tip:

- The MAC address length is 6 bytes. The format is XXXX-XXXX-XXXX and “X” is hexadecimal.
- The VLAN field displays "--" for port VLANs.

To display MAC address entries on a single port, click the corresponding port number.



□	MAC Address	Type	VLAN	Port	Aggregation Group	Bind	Delete
□	00B0-C60B-3740	Dynamic	1	2	--	Bind	Delete

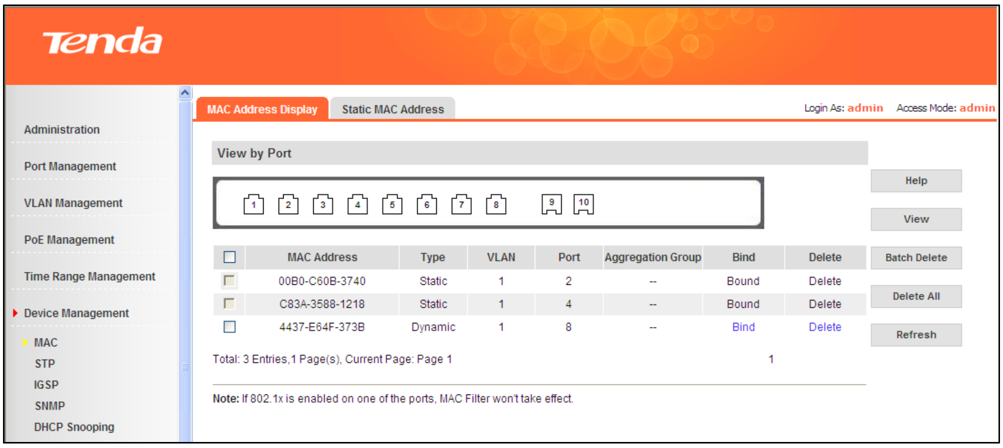
Total: 1 Entries,1 Page(s), Current Page: Page 1 1

Note: If 802.1x is enabled on one of the ports, MAC Filter won't take effect.

Bind

If you want a certain MAC address entry not to be aged, you can bind it and make it static.

Click this button to bind corresponding MAC address to a specific port. And the same button changes to **Bound** after being clicked.



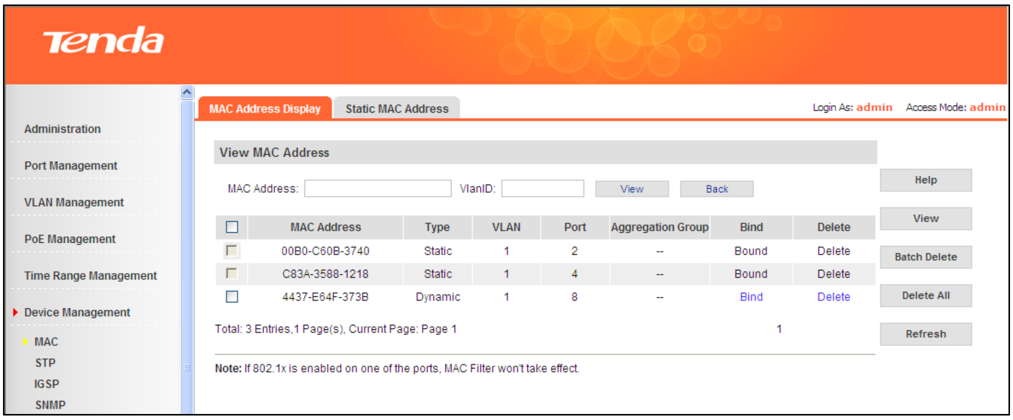
□	MAC Address	Type	VLAN	Port	Aggregation Group	Bind	Delete
□	00B0-C60B-3740	Static	1	2	--	Bound	Delete
□	C83A-3588-1218	Static	1	4	--	Bound	Delete
□	4437-E64F-373B	Dynamic	1	8	--	Bind	Delete

Total: 3 Entries,1 Page(s), Current Page: Page 1 1

Note: If 802.1x is enabled on one of the ports, MAC Filter won't take effect.

➘ View MAC address entry:

Click **View** and specify a MAC and a VLAN ID to view MAC address entries.



MAC Address: VlanID:

□	MAC Address	Type	VLAN	Port	Aggregation Group	Bind	Delete
□	00B0-C60B-3740	Static	1	2	--	Bound	Delete
□	C83A-3588-1218	Static	1	4	--	Bound	Delete
□	4437-E64F-373B	Dynamic	1	8	--	Bind	Delete

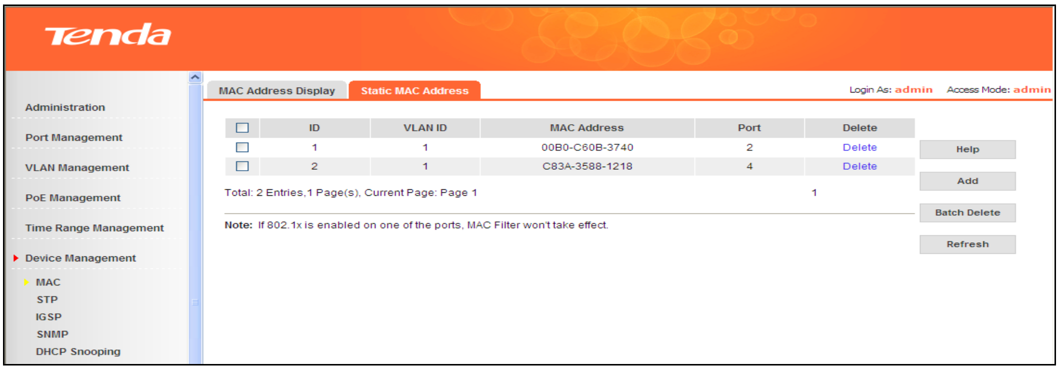
Total: 3 Entries,1 Page(s), Current Page: Page 1 1

Note: If 802.1x is enabled on one of the ports, MAC Filter won't take effect.

To view MAC address entry, you must enter the MAC address while the VLAN ID is optional. In port VLAN mode, only the MAC address should be entered.

1.2 Static MAC Address

Click **Device Management > MAC > Static MAC Address** to view and configure MAC address entries.



□	ID	VLAN ID	MAC Address	Port	Delete
□	1	1	00B0-C60B-3740	2	Delete
□	2	1	C83A-3588-1218	4	Delete

Total: 2 Entries,1 Page(s), Current Page: Page 1 1

Note: If 802.1x is enabled on one of the ports, MAC Filter won't take effect.

Tip:

- Each VLAN has a corresponding MAC address table. The same MAC address can be added into different VLANs.
- The MAC address entry in the Static Address Table cannot be added to the Filtering Address Table.
- Once VLAN mode is toggled, all current settings will be cleared.
- A certain port in the static MAC address table can receive packets whose source MAC address matches its corresponding VLAN ID; Packets whose destination MAC address matches the corresponding VID can only be forwarded to the corresponding port.

2 STP

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links.

Spanning Tree Protocol (STP) is standardized as IEEE 802.1D. As the name suggests, it creates a spanning tree within a network of connected layer-2 bridges (typically Ethernet switches), and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes.

➘ STP protocol packets

To implement spanning tree function, switches in the network transfer BPDUs between each other to exchange information. BPDUs carry the information that is needed for switches to figure out the spanning tree.

The network topology is determined by BPDU transmission among devices. There are two types of BPDUs in the original STP specification

- Configuration BPDU: Configuration BPDU (CBPDU), used for Spanning Tree computation and spanning tree topology maintenance.
- Topology Change Notification (TCN) BPDU, used to announce changes in the network topology

➘ Basic concepts of STP

1. Bridge ID

The bridge ID contains both numbers combined together - Bridge priority + MAC, in which the bridge priority is a configurable parameter. The smaller the bridge ID is, the higher the bridge priority is. The root bridge is the bridge with the lowest bridge ID.

2. Root Bridge

There is only one root bridge in the networking and it is changeable as the network topology changes. Initially, all devices regard themselves as the root bridge and generate their own configuration BPDUs and send them out periodically. When the network topology becomes stable, only the root bridge device will send configuration BPDUs out and other devices will forward these BPDUs.

3. Root Port

The root bridge port is the port that has the lowest path cost from this bridge to the Root Bridge and forwards packets to the root. There is only one root port on the non-root bridge device and no root port on the root bridge devices.

4. Designated Bridge and Designated Port

Designated bridge: As for a device, it is the device that connects to and forwards BPDUs the host. As for a LAN, it is the device that forwards BPDUs to the network segment.

Designated port: As for a device, it is the port that forwards BPDUs to the host. As for a LAN, it is the port that forwards BPDUs to the network segment.

5. Path Cost

The parameter for choosing the link path by STP. By calculating the path cost, STP chooses the better links and blocks the redundant links so as to disbranch the ring-network to form a tree-topological ring-free network.

➘ BPDU Priority in STP mode

Assuming two BPDUs: BPDU X and BPDU Y

If the root bridge ID of X is smaller than that of Y, X is superior to Y.

If the root bridge ID of X equals that of Y, but the root path cost of X is smaller than that of Y, X is superior to Y.

If the root bridge ID and the root path cost of X equal those of Y, but the designated bridge ID of X is smaller than that of Y, X is superior to Y.

If the root bridge ID, the root path cost and designated bridge ID of X equal those of Y, but the designated port ID of X is smaller than that of Y, X is superior to Y.

➘ STP Computing Process

- Initial Status

Initially, each switch regards itself as the root, and generates a configuration BPDU for each port on it as a root, with the root path cost being 0, the ID of the designated bridge being that of the switch, and the designated port being itself.

- BPDU Comparison

Each switch sends out configuration BPDUs and receives a configuration BPDU on one of its ports from another switch. The following table shows the comparing operations.

Step	Operation
1	If the priority of the BPDU received on the port is lower than that of the BPDU if of the port itself, the switch discards the BPDU and does not change the BPDU of the port. If the priority of the BPDU is higher than that of the BPDU of the port itself, the switch replaces the BPDU of the port with the received one and compares it with those of other ports on the switch to obtain the one with the highest priority.
2	The switch selects the best BPDU by comparing BPDUs on all ports.

- Select the root bridge

The root bridge is selected by BPDU comparing. The switch with the smallest root ID will be chosen as the root bridge.

- Select the root port and designated port

The operation is taken in the following way:

Step	Operation
1	For each switch (except the one chosen as the root bridge) in a network, the port that receives the BPDU with the highest priority is chosen as the root port of the switch.
2	Using the root port BPDU and the root path cost, the switch generates a designated port BPDU for each of its ports. • Root ID is replaced with that of the root port; • Root path is replaced with the sum of the root path cost of the root port and the path cost between this port and the root port; • The ID of the designated bridge is replaced with that of the switch; • The ID of the designated port is replaced with that of the port.
3	The switch compares the resulting BPDU with the BPDU of the desired port whose role you want to determine. • If the resulting BPDU takes the precedence over the BPDU of the port, the port is chosen as the designated port and the BPDU of this port is

	replaced with the resulting BPDU. The port regularly sends out the resulting BPDU; • If the BPDU of this port takes the precedence over the resulting BPDU, the BPDU of this port is not replaced and the port is blocked. The port only can receive BPDUs.

Tip:

In a STP with stable topology, only the root port and designated port can forward data, and the other ports are blocked. The blocked ports can only receive BPDUs.

➘ STP Timer

1. Hello Time

Hello Time ranges from 1 to 10 seconds. It specifies the interval to send BPDU packets. It is used to test the links.

2. Max Age

Max Age ranges from 6 to 40 seconds. It specifies the maximum time the switch can wait without receiving a BPDU before attempting to reconfigure.

3. Forward Delay

Forward Delay ranges from 4 to 30 seconds. It specifies the time for the port to transit its state after the network topology is changed.

When the STP regeneration caused by network malfunction occurs, the STP structure will get some corresponding change. However, as the new configuration BPDUs cannot be spread in the whole network at once, the temporal loop will occur if the port transits its state immediately. Therefore, STP adopts a state transit mechanism, that is, the new root port and the designated port begins to forward data after twice forward delay, which ensures the new configuration BPDUs are spread in the whole network.

➘ RSTP

RSTP (Rapid Spanning Tree Protocol), evolved from the 802.1D STP standard, enable Ethernet ports to transit their states rapidly (traditional STP: 50s; RSTP: 1s). The premises for the port in the RSTP to transit its state rapidly are as follows.

- The condition for the root port to transit its port state rapidly: The old root port of the switch stops forwarding data and the designated port of the upstream switch begins to forward data.
- The condition for the designated port to transit its port state rapidly: The designated port is an edge port or connecting to a point-to-point link. If the designated port is an

edge port, it can directly transit to forwarding state; if the designated port is connecting to a point-to-point link, it can transit to forwarding state after getting response from the downstream switch through handshake.

➘ RSTP Elements

1. Edge Port

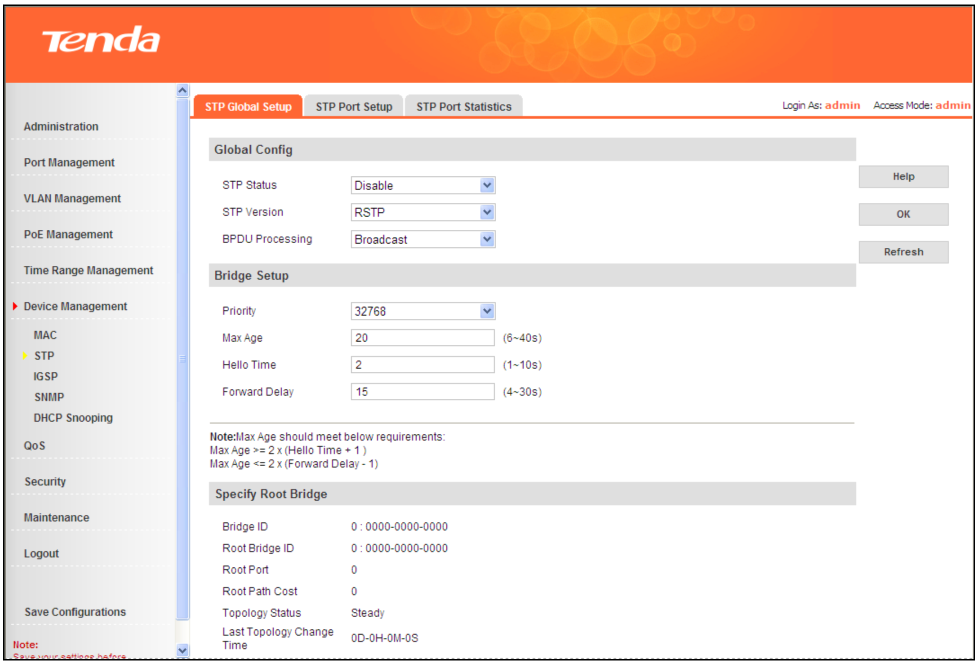
The edge port is a configurable designation port that is directly connected to a segment where a loop cannot be created. Usually it would be a port connected directly to terminals. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

2. P2P Port

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP/MSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

2.1 STP Global Setup

Click **Device Management > STP > STP Global Setup** to configure and view global properties of STP.



Login As: admin   Access Mode: admin

Global Config

STP Status	Disable
STP Version	RSTP
BPDU Processing	Broadcast

Bridge Setup

Priority	32768	
Max Age	20	(6~40s)
Hello Time	2	(1~10s)
Forward Delay	15	(4~30s)

Note: Max Age should meet below requirements:
Max Age >= 2 x (Hello Time + 1)
Max Age <= 2 x (Forward Delay - 1)

Specify Root Bridge

Bridge ID	0 : 0000-0000-0000
Root Bridge ID	0 : 0000-0000-0000
Root Port	0
Root Path Cost	0
Topology Status	Steady
Last Topology Change Time	0D-0H-0M-0S

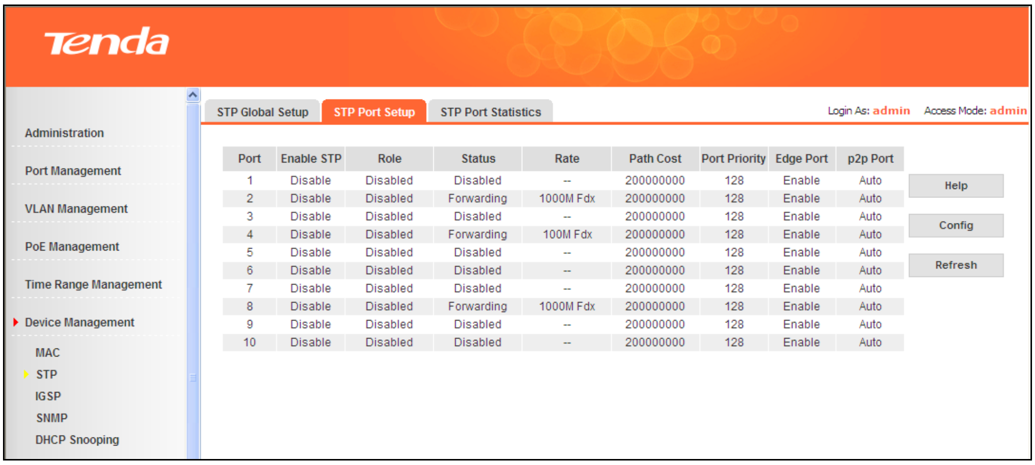
Parameters on this page are described below:

Field	**Description**

STP Status	Enable/Disable STP feature on this device. By default, the STP feature is disabled.
STP Version	Select the desired version of STP version. **STP:** Spanning-tree-compliant mode. **RSTP：** Rapid-spanning-tree-compliant mode.
BPDU Processing	Select a BPDU processing method when STP is disabled on this device. **Broadcast:** Broadcast BPDU packets. This is the default option. **Filter:** Filter BPDU packets.
Priority	Configure priority for this switch. Priority is an important factor for root bridge. Under the same conditions, the switch with the higher priority will be selected as the root bridge. The smaller the value is, the higher the priority is. The Bridge priority default is 32768 and can only be configured in multiples of 4096.
Max Age	Configure a max aging time for BPDU packets to live. The default value is 20s. Max Age should meet below requirements: Max Age >= 2 * (Hello Time + 1); Max Age <= 2 *(Forward Delay - 1).
Hello time	Configure the BPDU sending interval. The default value is 2s.
Forward Delay	Configure the delay time of port status transition when network topology changes. The default is 15s.
Specify Root Bridge	Display relevant info of STP feature.

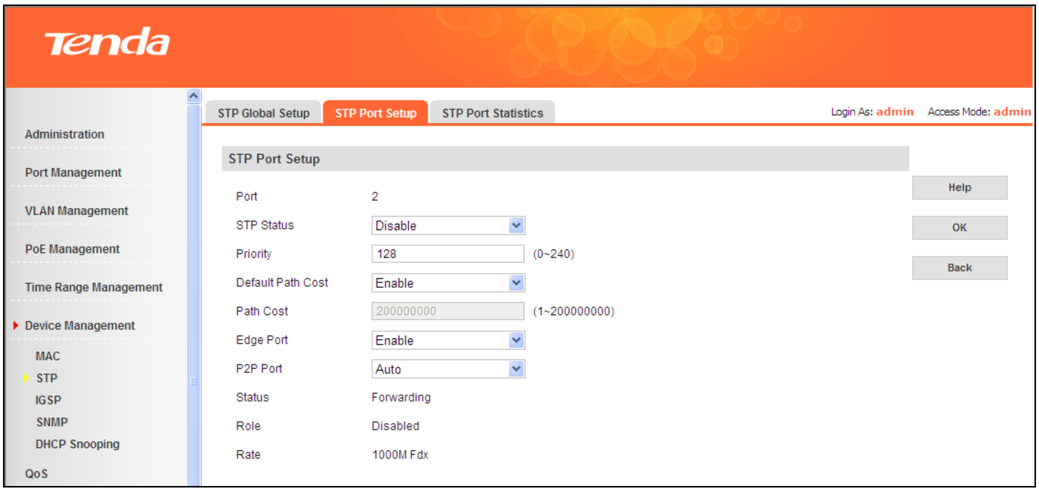
2.2 STP Port Setup

Click **Device Management > STP > STP Port Setup** to configure STP parameters on all ports.



Port	Enable STP	Role	Status	Rate	Path Cost	Port Priority	Edge Port	p2p Port
1	Disable	Disabled	Disabled	--	200000000	128	Enable	Auto
2	Disable	Disabled	Forwarding	1000M Fdx	200000000	128	Enable	Auto
3	Disable	Disabled	Disabled	--	200000000	128	Enable	Auto
4	Disable	Disabled	Forwarding	100M Fdx	200000000	128	Enable	Auto
5	Disable	Disabled	Disabled	--	200000000	128	Enable	Auto
6	Disable	Disabled	Disabled	--	200000000	128	Enable	Auto
7	Disable	Disabled	Disabled	--	200000000	128	Enable	Auto
8	Disable	Disabled	Forwarding	1000M Fdx	200000000	128	Enable	Auto
9	Disable	Disabled	Disabled	--	200000000	128	Enable	Auto
10	Disable	Disabled	Disabled	--	200000000	128	Enable	Auto

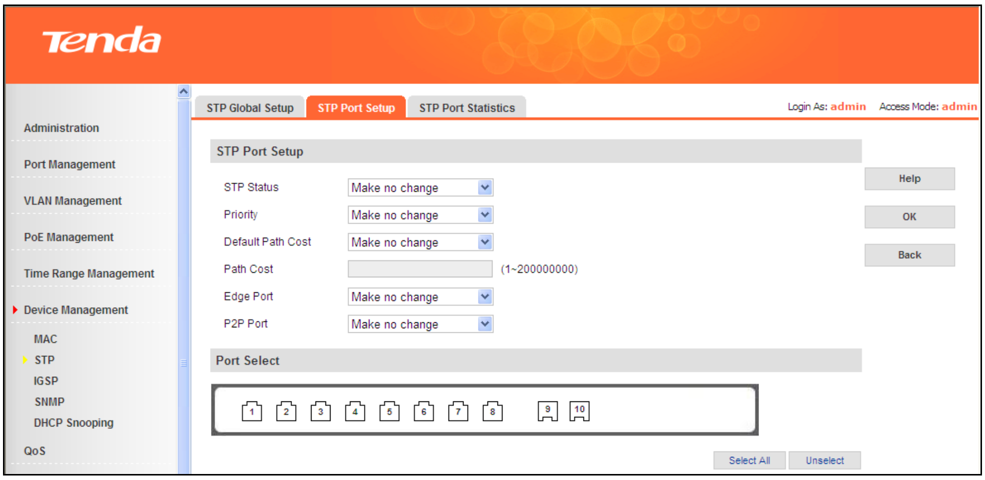
To configure STP parameters on a single port, click the corresponding port number.



STP Port Setup

Port	2	
STP Status	Disable	
Priority	128	(0~240)
Default Path Cost	Enable	
Path Cost	200000000	(1~200000000)
Edge Port	Enable	
P2P Port	Auto	
Status	Forwarding	
Role	Disabled	
Rate	1000M Fdx	

To batch configure STP parameters, click **Config**.



STP Port Setup

STP Status	Make no change	
Priority	Make no change	
Default Path Cost	Make no change	
Path Cost		(1~200000000)
Edge Port	Make no change	
P2P Port	Make no change	

Port Select

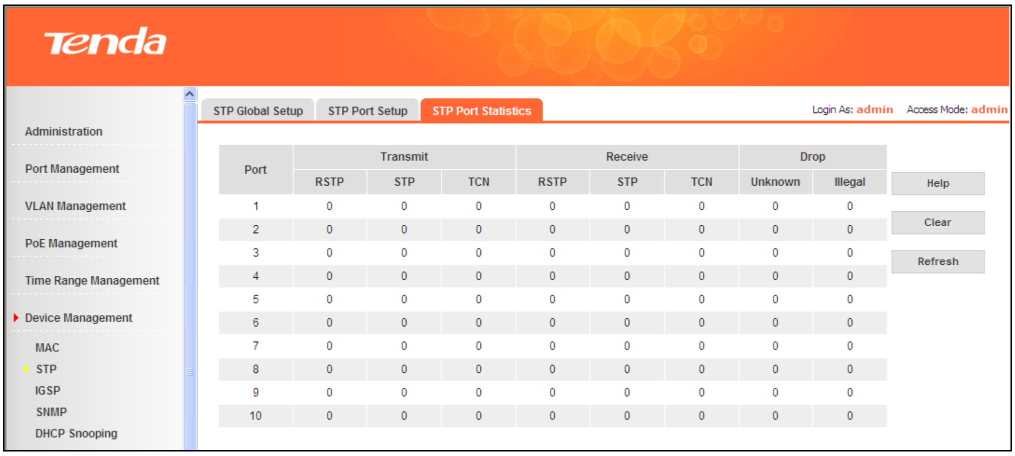
Parameters on this page are described below:

Field	Description

STP Status	Enable/Disable STP feature on ports. By default, the STP feature is disabled. Enabling global and port STP feature makes port STP feature effective.
Priority	Configure port priority, which is an important for selecting root port. Under the same conditions, the port with higher priority will be selected as the root port. The smaller the value is, the higher its priority is. The default value is 128 with a valid range of 0~240.
Default Path Cost	Enable/Disable port default path cost. You can customize the port path cost between 1 and 200,000,000 if you disable the default port path cost. When enabled, port path cost can be configured automatically and is 802.1t-compliant.
Path Cost	The default path cost is 200,000,000. **Tip:** Only if you disable the default path cost option, can path cost be configurable.
Edge Port	Select to enable or disable Edge Port. An edge port is a port that is connected to the terminal directly. Ports that are designated as edge ports transit rapidly from the blocked state to the forwarding state without delay. An edge port loses its status if it receives a BPDU packet, immediately becoming a non-edge port. By default, all ports are edge ports.
P2P Port	Select P2P link status for ports. If two ports are connected in P2P link, and they are root ports or designated ports, they can be rapidly transited to forwarding status, reducing unnecessary forwarding delay time. Under RSTP/MSTP, all ports operating in full-duplex mode are considered to be P2P ports. By default, port establishes a link automatically.

2.3 STP Port Statistics

Click **Device Management > STP > STP Port Statistics** to refresh and clear BPDU packets ports have received and sent.



Login As: admin Access Mode: admin

Port	Transmit			Receive			Drop	
	RSTP	STP	TCN	RSTP	STP	TCN	Unknown	Illegal
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0

3 IGSP

IGMP Snooping (Internet Group Management Protocol Snooping) is a multicast constraint mechanism on layer 2 switches for managing and controlling multicast groups.

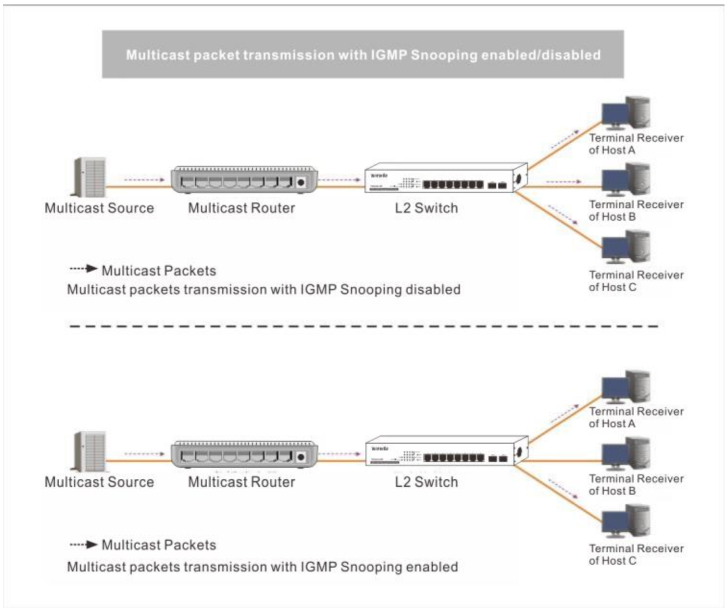
➘ Principle of IGMP snooping

By analyzing IGMP packets, the IGMP-Snooping-enabled layer-2 device will establish a map of links for ports and multicast MAC addresses, and forward multicast data.

An IGMP-Snooping-disabled layer-2 device will flood multicast traffic to all the ports in a broadcast domain (or the VLAN equivalent).

- With IGMP snooping disabled, known multicast traffic will be broadcast in layer 2.
- With IGMP snooping enabled, known multicast traffic won't be broadcast but multicast to a designated receiver in layer 2. Unknown multicast traffic will still be broadcast in layer 2.

Multicast packet transmission on this switch with IGMP Snooping enabled/disabled:


Multicast packet transmission with IGMP Snooping enabled/disabled
Multicast Source
Multicast Router
L2 Switch
Terminal Receiver of Host A
Terminal Receiver of Host B
Terminal Receiver of Host C
Multicast Packets
Multicast packets transmission with IGMP Snooping disabled
Multicast Source
Multicast Router
L2 Switch
Terminal Receiver of Host A
Terminal Receiver of Host B
Terminal Receiver of Host C
Multicast Packets
Multicast packets transmission with IGMP Snooping enabled

➘ How IGMP Snooping Works

A switch that runs IGMP snooping performs different actions when receiving different IGMP messages.

1．Group query

The IGMP querier periodically sends IGMP general queries to all hosts and routers on the local subnet to query which multicast group members exist on the subnet. After receiving an IGMP general query, the switch forwards it through all ports in the VLAN (except the port that receives the query) and performs corresponding actions on the receiving port (mainly resets/enables the age timer on this port).

2．Report membership

After receiving an IGMP query, a multicast group member host responds with an IGMP membership report. If the host wants to join a multicast group, it will send an IGMP membership report to the multicast router to announce that it wants to join the multicast group. After receiving an IGMP membership report, the switch forwards it through all the router ports in the VLAN, resolves the address of the reported multicast group and performs corresponding actions on the receiving port (mainly resets/enables the age timer). The switch does not forward an IGMP membership report through a non-router port.

➘ Leave the multicast group

When an IGMPv1 host leaves a multicast group, the host does not send an IGMP leaving message. However, as the aging timer on the corresponding member port expires, the switch immediately deletes its forwarding entry from the forwarding table.

When an IGMPv2 or IGMPv3 host leaves a multicast group, it sends an IGMP leaving message to the multicast router to inform of such leave.

When receiving an IGMP leaving message from the last member port, the switch forwards it through all router ports in the VLAN and resets the aging timer on the receiving port instead of immediately deleting its corresponding forwarding entry from the forwarding table as it cannot know whether there are still other members of that multicast group attached to such port.

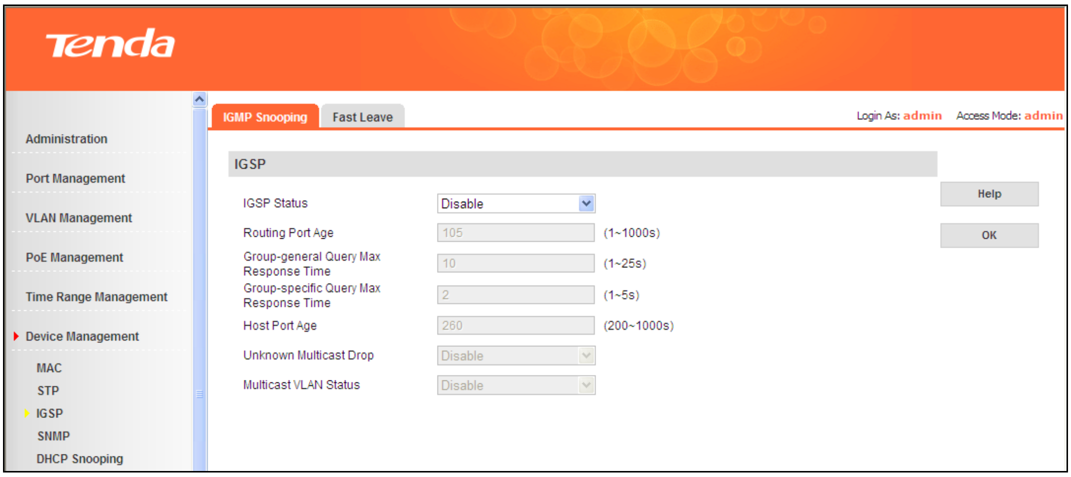
After receiving the IGMP leaving message from a host, the IGMP querier resolves the multicast group address in the message and sends an IGMP group-specific query to that multicast group through the receiving port. After receiving the IGMP group-specific query, the switch forwards it through all its router ports in the VLAN and all member ports in that multicast group.

The switch also performs the following actions on the port that receives the IGMP leaving message: If the port receives any IGMP membership report in response to the group-specific query before the aging timer expires, it indicates there are still multicast group members of this port and the switch will reset the aging timer on the port.

If the port receives no IGMP membership report in response to the group-specific query before its aging timer expires, it indicates there are no multicast group members of this port and the switch will remove the multicast forwarding entry that the port corresponds to from the forwarding table when the aging timer expires.

3.1 IGMP Snooping

Click **Device Management > IGSP > IGMP Snooping** to enter page below:



IGSP

IGSP Status: Disable

Routing Port Age: 105 (1~1000s)

Group-general Query Max Response Time: 10 (1~25s)

Group-specific Query Max Response Time: 2 (1~5s)

Host Port Age: 260 (200~1000s)

Unknown Multicast Drop: Disable

Multicast VLAN Status: Disable

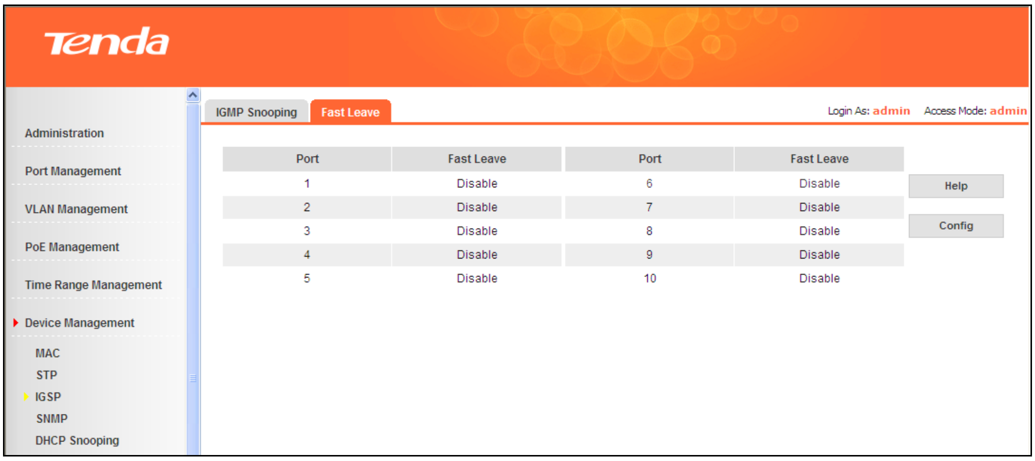
Parameters on this page are described below:

Field	Description
IGSP Status	Select to enable or disable IGMP Snooping feature on this device.
Routing Port Age	Within the set routing port age, if the switch does not receive any query packet from the routing port, this routing port will be invalid. The default is 105s. Range: 1~1000s.
Group-general Query Max Response Time	Configure max amount of time in response to group-general query messages (1-25 sec). The default is 10s.
Group-specific Query Max Response Time	Configure max amount of time in response to group-specific query messages (1-5 sec). The default is 2s.

Host Port Age	Within the set host port age, if the switch does not receive any report packet sent from the host port, the host port will be invalid. The default is 260s. Range: 200~1000s.
Unknown Multicast Drop	Enable/Disable the Unknown Multicast Drop feature. If enabled, the switch will drop unknown multicast packets it has received; If disabled, the switch will broadcast unknown multicast packets it has received. **Tip:** This feature is effective even if IGMP Snooping feature is disabled.
Multicast VLAN Status	Enable/Disable VLAN IGMP Snooping feature
Multicast VLAN ID	This option becomes visible when multicast VLAN is enabled. Typing the corresponding multicast VLAN ID makes multicast packets forwarded only in the corresponding VLAN.

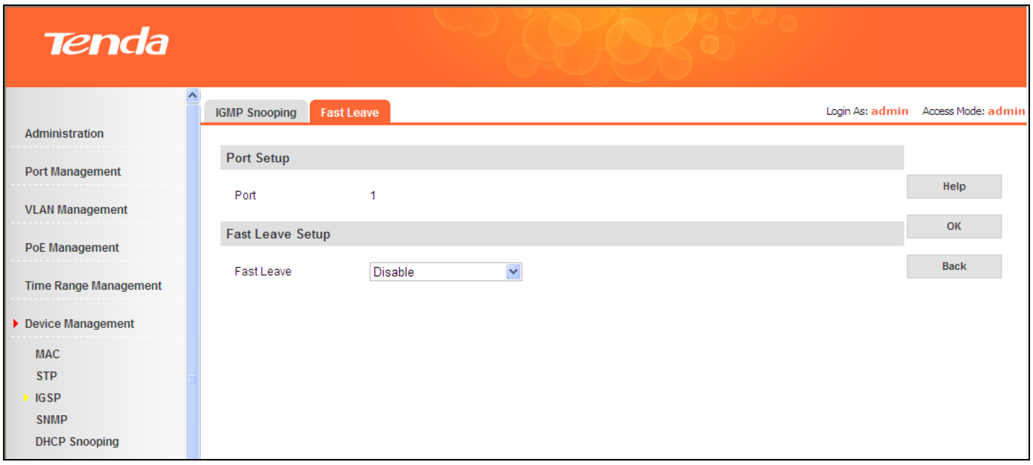
3.2 Fast Leave

Click **Device Management > IGSP > Fast Leave** to configure port fast leave settings in IGSP/V2.



Port	Fast Leave	Port	Fast Leave
1	Disable	6	Disable
2	Disable	7	Disable
3	Disable	8	Disable
4	Disable	9	Disable
5	Disable	10	Disable

To configure such settings on a single port, click the corresponding port you wish to.



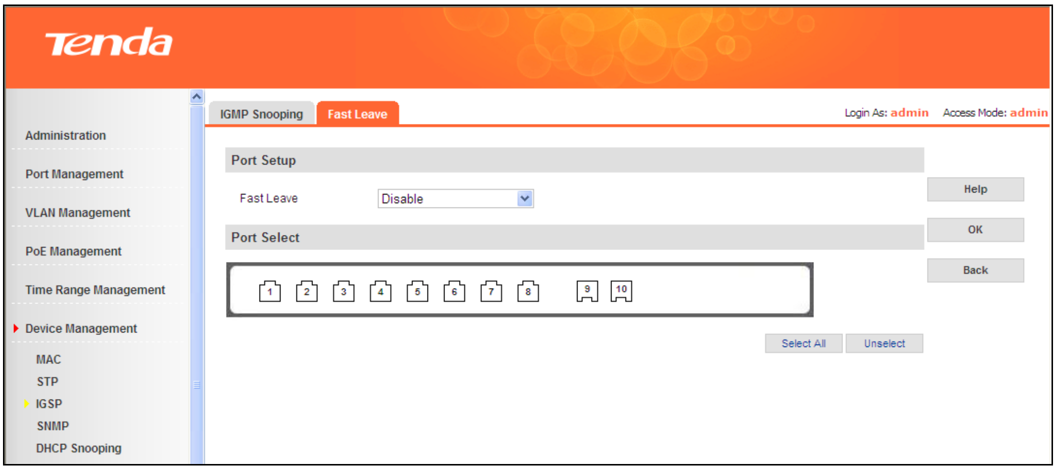
Port Setup

Port 1

Fast Leave Setup

Fast Leave Disable

To batch configure such settings, click **Config** to enter page below:



Port Setup

Fast Leave Disable

Port Select

4 SNMP

Simple Network Management Protocol (SNMP), the most widely used network management protocol in TCP/IP networking, is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network.

SNMP, using polling scheme, is suitable for use in small-sized network environment demanding high speed and low cost. SNMP, implemented through the connectionless UDP, can seamlessly interoperate with multiple devices.

➘ SNMP Framework

SNMP framework consists of three parts: SNMP manager, SNPM agent and MIB (Management Information Base).

- SNMP manager: A system used for controlling and monitoring network nodes via

SNMP protocol. The most commonly used is NMS (Network Management System), which can be a server specially used for network management or an application program for executing management function on a certain network device.

- SNMP agent: Software which runs on managed devices for maintaining management information base and reporting management data to a SNMP management system when it is needed.
- MIB: A management information base (MIB) is a database used for managing the entities in a communications network. It defines a series of properties for those managed entities: object name, access right, data type, etc. every SNMP has its corresponding MIB and the SNMP manager can perform read/write action accordingly.

SNMP agent is managed by SNMP manager and they two interact with each other via SNMP protocol.

➘ SNMP Actions

The following three basic actions are available on this switch to execute intercommunication between the SNMP manager and SNMP agent:

- Get request: A manager-to-agent request to retrieve the value of a variable or list of variables.
- Set request: A manager-to-agent request to change the value of a variable or list of variables in MIB.
- Trap: Asynchronous notification from agent to manager. SNMP traps enable an agent to notify the management station of significant events (such as reboot the managed device) by way of an unsolicited SNMP message.

➘ SNMP Protocol Versions

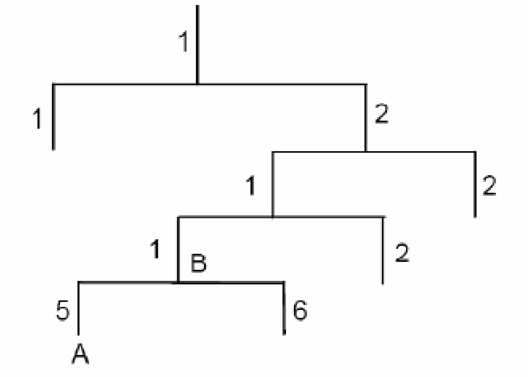
Only SNMP manager and SNMP agent share the same SNMP version configurations can they access each other successfully. So far, this switch supports SNMPv3 and is compatible with SNMPv1 and SNMPv2c.

- SNMPv1: The community name is used to define the relation between SNMP Manager and SNMP Agent. The SNMP packets failing to pass community name authentication are discarded. The community name can limit access to SNMP Agent from SNMP NMS, functioning as a password.
- SNMPv2c: SNMP v2c also adopts community name authentication. It is compatible with SNMP v1 while enlarges the function of SNMP v1: provide more action types (GetBulk and InformRequest); support more statistics types (like Count64); provide more error codes for distinguishing errors.
- SNMPv3: Based on SNMP v1 and SNMP v2c, SNMP v3 extremely enhances the

security and manageability. It adopts VACM (View-based Access Control Model) and USM (User-Based Security Model) authentication. The user can configure the authentication and the encryption functions. The authentication function is to limit the access of the illegal user by authenticating the senders of packets. Meanwhile, the encryption function is used to encrypt the packets transmitted between SNMP Manager and SNMP Agent so as to prevent any information being stolen. The multiple combinations of authentication function and encryption function can guarantee a more reliable communication between SNMP Management station and SNMP Agent.

➘ MIB Introduction

To uniquely identify the management objects of the device in SNMP messages, SNMP adopts the hierarchical architecture to identify the managed objects. It is like a tree, and each tree node represents a managed object, as shown in the following figure. Thus the object can be identified with the unique path starting from the root and indicated by a string of numbers. The number string is the Object Identifier of the managed object. In the following figure, the OID of the managed object B is {1.2.1.1}. While the OID of the managed object A is {1.2.1.1.5}.



Architecture of the MIB tree

➘ SNMP Configuration Outline

Configuration procedures for SNMPv3 are as following:

Step	Configuration Item	Note	Configuration Details
1	Enable SNMP agent	Required option	Click **Device Management > SNMP > Agent Setup** to enable SNMP function
2	Create MIB view	Required option	Click **Device Management > SNMP > View** to create view of the managed object.

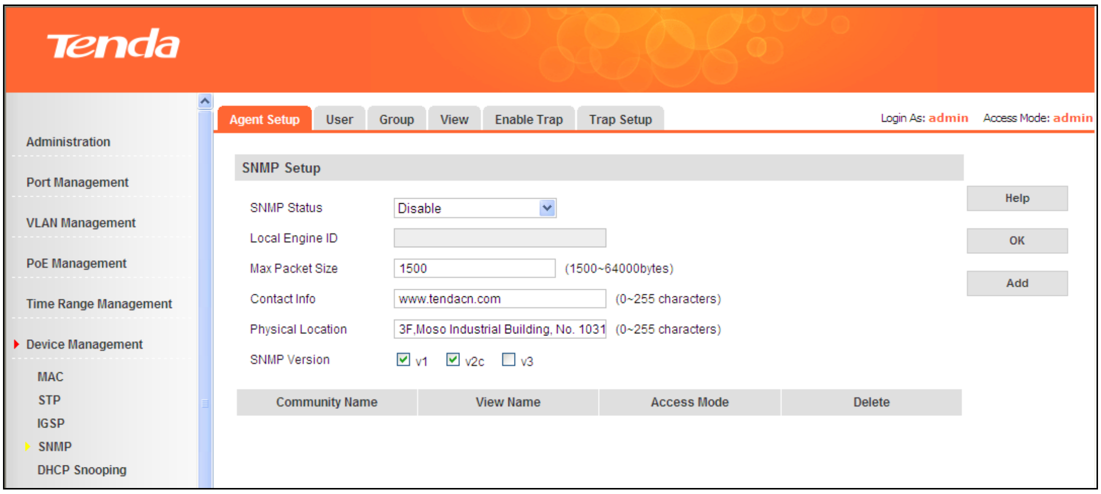
3	Create SNMP group	Required option	Click **Device Management > SNMP > Group** to create SNMPv3 group and configure views with different access rights for the group.
4	Create SNMP user	Required option	Click **Device Management > SNMP > User** to create SNMPv3 users, and configure authentication and encryption settings for users.
5	Configure SNMP Trap	Required option	Click **Device Management > SNMP > Enable Trap** to enable the Trap function, click **Device Management > SNMP > Trap Setup** to configure Trap types and the destination host.

Configuration procedures for SNMPv1/SNMPv2c are as following:

Step	Configuration Item	Note	Configuration Details
1	Enable SNMP agent	Required option	Click **Device Management > SNMP > Agent Setup** to enable SNMP function.
2	Create MIB view	Required option	Click **Device Management > SNMP > View** to create view for the managed object.
3	Create SNMP community	Required option	Click **Device Management > SNMP > Agent Setup** to configure community name for SNMPv1 and SNMPv2c.
4	Configure SNMP Trap	Required option	Click **Device Management > SNMP > Enable Trap** to enable the Trap function, click **Device Management > SNMP > Trap Setup** to configure Trap types and the destination host.

4.1 Agent Setup

Click **Device Management > SNMP > Agent Setup** to enter page below:



SNMP Setup

SNMP Status: Disable

Local Engine ID:

Max Packet Size: 1500 (1500~64000bytes)

Contact Info: www.tendacn.com (0~255 characters)

Physical Location: 3F,Moso Industrial Building, No. 1031 (0~255 characters)

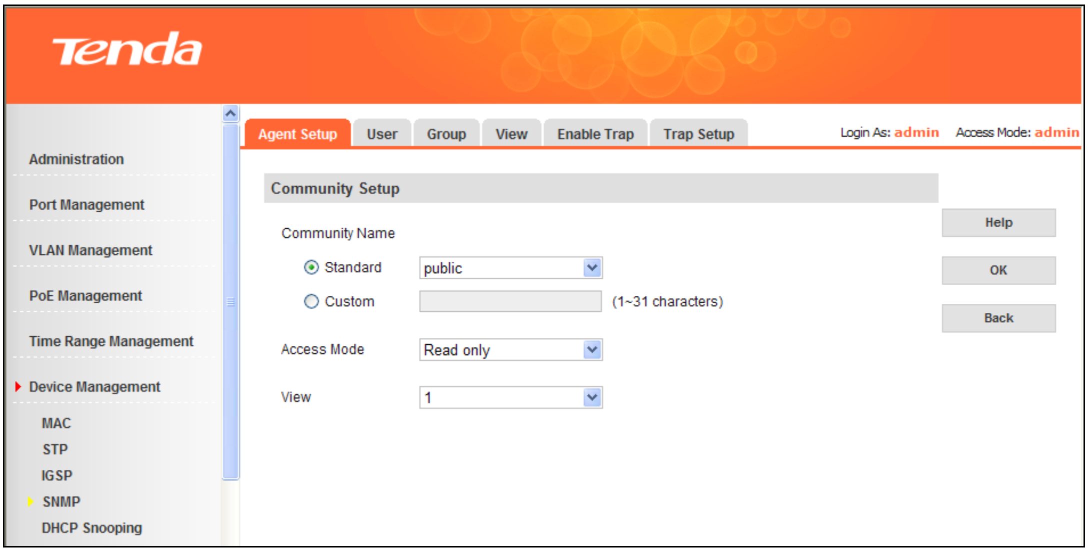
SNMP Version: ☑ v1 ☑ v2c □ v3

Community Name	View Name	Access Mode	Delete

Parameters on this page are described below:

Field	Description
SNMP Status	Enable/Disable the SNMP function.
Local Engine ID	Display the local SNMP engine ID. When SNMP Status is enabled, this field becomes unconfigurable.
Max Packet Size	Configure max packet size that the SNMP agent can receive/send. The default is 1500.
Contact Info	Configure contact info for the switch so that the SNMP manager can quickly locate the switch. Usually, it includes the domain name and IP address of the switch. The default contact info is www.tendacn.com.
Physical Location	Configure physical location info for the switch so that the SNMP manager can quickly locate the switch. The default physical location is 3F, Moso Industrial Building, No. 1031, Liming Road, Xili Town, Nanshan District, ShenZhen, P.R. CHINA.
SNMP Version	Configure SNMP versions for the SNMP agent. It supports SNMP v1, SNMP v2 and SNMP v3.

Click **Add** to enter the Community Setup page. Note that you should create a view first before creating a community.



Login As: admin Access Mode: admin

Community Setup

Community Name
● Standard public
○ Custom (1~31 characters)

Access Mode Read only

View 1

Parameters on this page are described below:

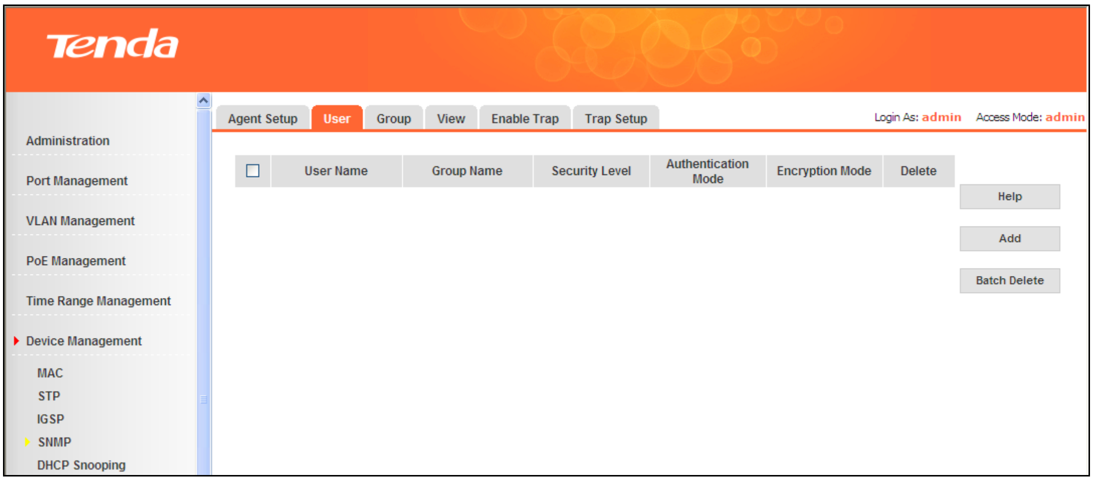
Field	Description
Community Name	Configure the community name here. You can select a standard community name or customize a community name. **Standard:** Select public or private. **Custom:** Customize the community name. The length of the community name should be within 31 characters.
Access Mode	Define the access rights of the community. **Read only:** Management right of the Community is restricted to read-only, and changes cannot be made to the corresponding View. **Read & write:** Management right of the Community is read-write and changes can be made to the corresponding View.
View	Select the MIB View for the community to access.

After creating a community, you can use the V1, or V2c community name to view or config node settings in the MIB.

4.2 User

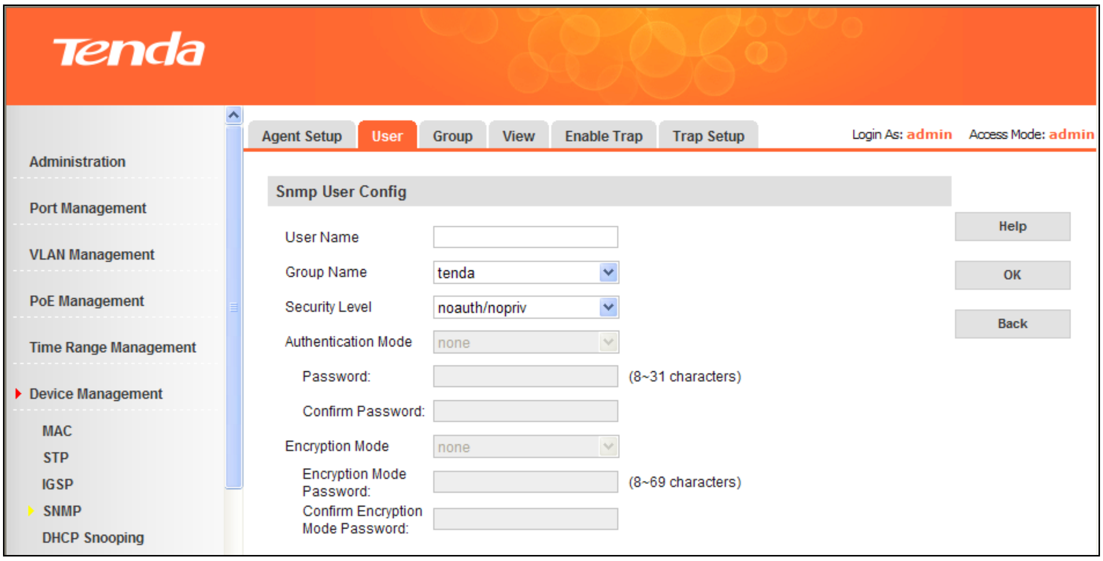
The User in a SNMP Group can manage the switch via the SNMP manager software. The User and its Group have the same security level and access right.

Click **Device Management > SNMP > User** to enter page below:



□	User Name	Group Name	Security Level	Authentication Mode	Encryption Mode	Delete

Click **Add** to enter page below. Note that you must create a group before you can add a user.



Snmp User Config

User Name
Group Name: tenda
Security Level: noauth/nopriv
Authentication Mode: none
Password: (8~31 characters)
Confirm Password:
Encryption Mode: none
Encryption Mode Password: (8~69 characters)
Confirm Encryption Mode Password:

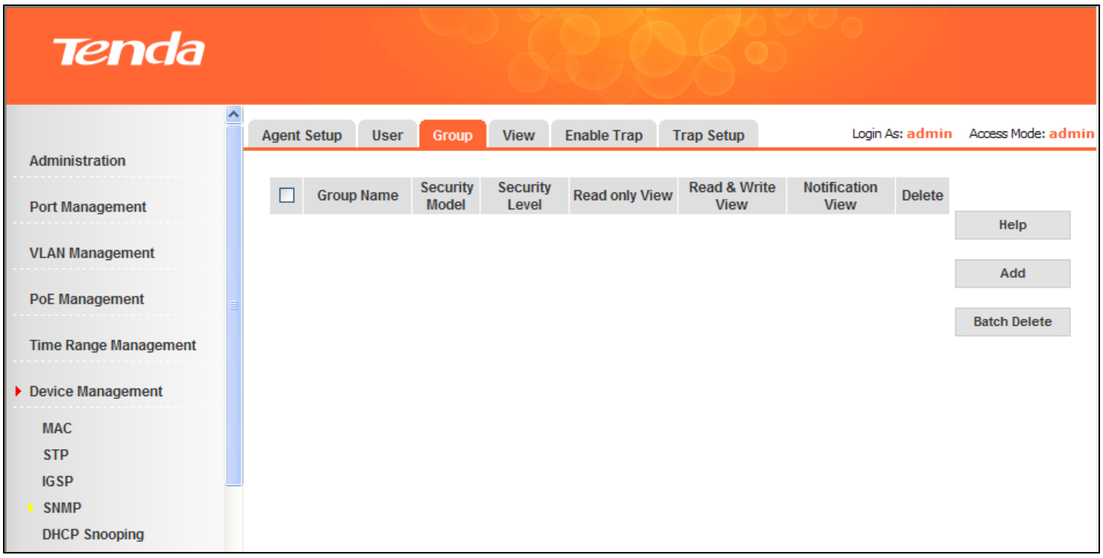
Parameters on this page are described below:

Field	**Description**
User Name	Enter the user name here.
Group Name	Select the group name here. You need to go to the **Device Management > SNMP > Group** page to configure group settings first. The user is classified to the corresponding Group according to its Group Name and Security Level.
Security Level	Select security level from the drop-down list.
Authentication Mode	Select the authentication mode for SNMP v3 users. Only when the security level is auth/priv or auth/nopriv, can this parameter be

	configurable. None: not authenticated. MD5: message digest 5. SHA: secure harsh algorithm.
Password	Enter the authentication password.
Confirm Password	Enter the authentication password again.
Encryption Mode	Select the encryption mode for SNMP v3 users. Only when the security level is auth/priv, can this parameter be configurable. None: not encrypted. DES: data encryption standard.
Encryption Password	Enter the encryption password.
Confirm Encryption Password	Enter the encryption password again.

4.3 Group

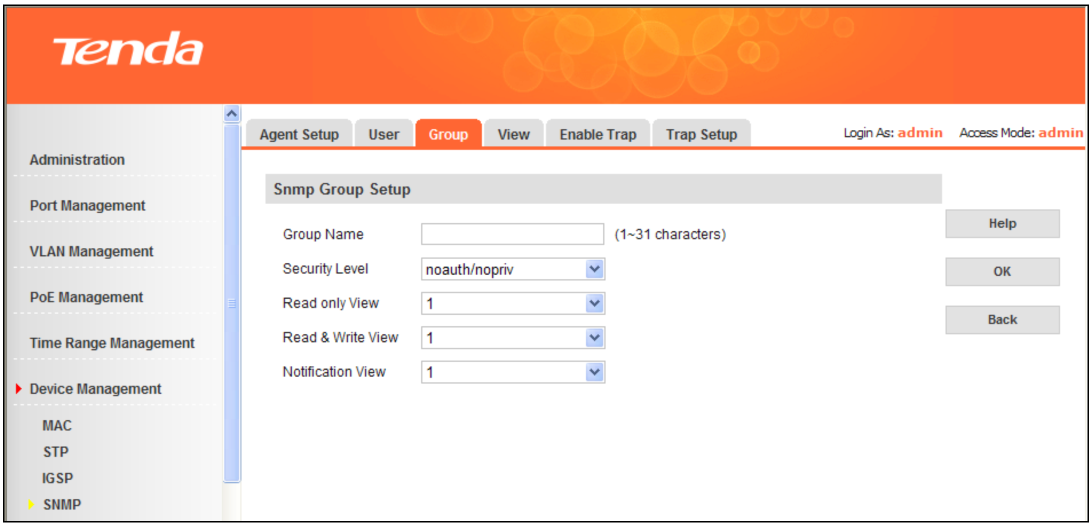
On this page, you can configure SNMP Group to control the network access by providing the users in various groups with different management rights via the Read View, Write View and Notify View. Click **Device Management > SNMP > Group** to enter page below:



Login As: admin Access Mode: admin

□	Group Name	Security Model	Security Level	Read only View	Read & Write View	Notification View	Delete

Click **Add** to enter page below. Note that you must create a view before you can add a group.



Snmp Group Setup

Group Name (1~31 characters)

Security Level: noauth/nopriv

Read only View: 1

Read & Write View: 1

Notification View: 1

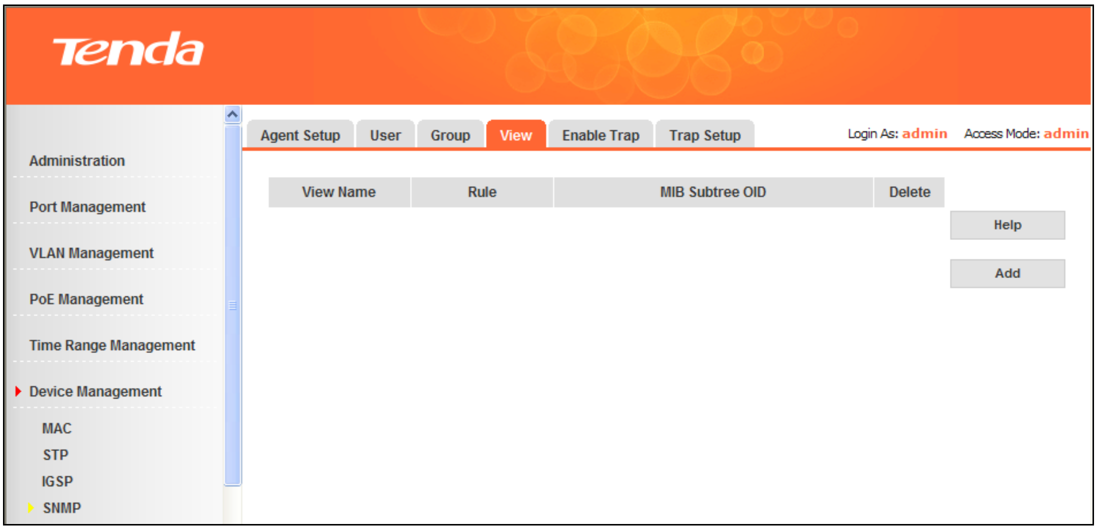
Parameters on this page are described below:

Field	Description
Group Name	Enter the SNMP Group name. The Group Name and Security Level compose the identifier of the SNMP Group. The Groups with these two items the same are considered to be the same.
Security Level	Select the security level for SNMP v3 group.
Read only View	Select the View to be the Read View. The management access is restricted to read-only.
Read & Write View	Select the View to be the Read & Write View. The View defined as the Read & Write View can be read and modified.
Notification View	Select the View to be the Notify View. The SNMP manager can receive trap messages of the assigned SNMP view generated by the switch's SNMP agent.

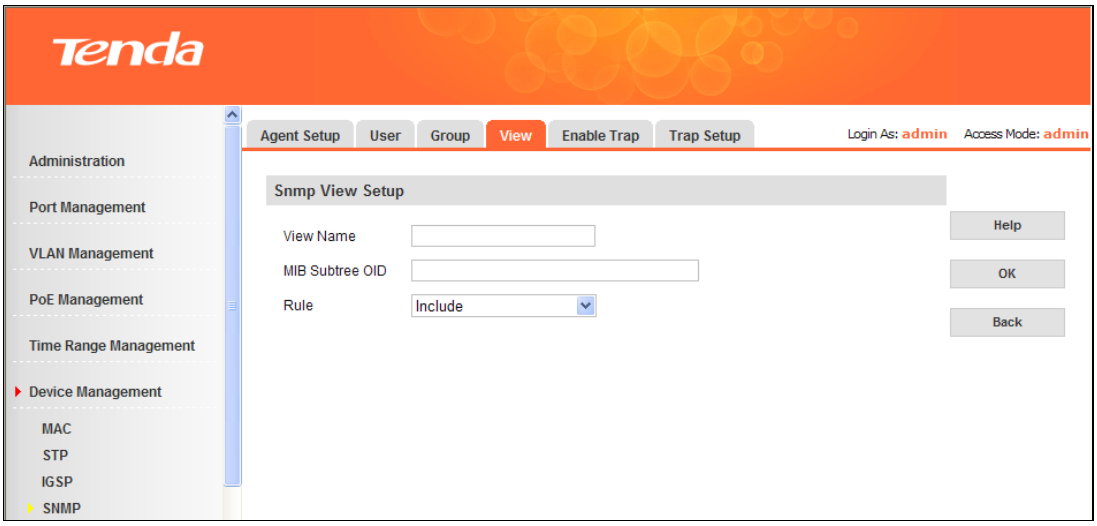
4.4 View

The OID (Object Identifier) of the SNMP packets is used to describe the managed objects of the switch, and the MIB (Management Information Base) is the set of the OIDs. The SNMP View is created for the SNMP manager to manage MIB objects.

Click **Device Management > SNMP > View** to enter page below:



Click **Add** to enter page below:



Snmp View Setup

View Name

MIB Subtree OID

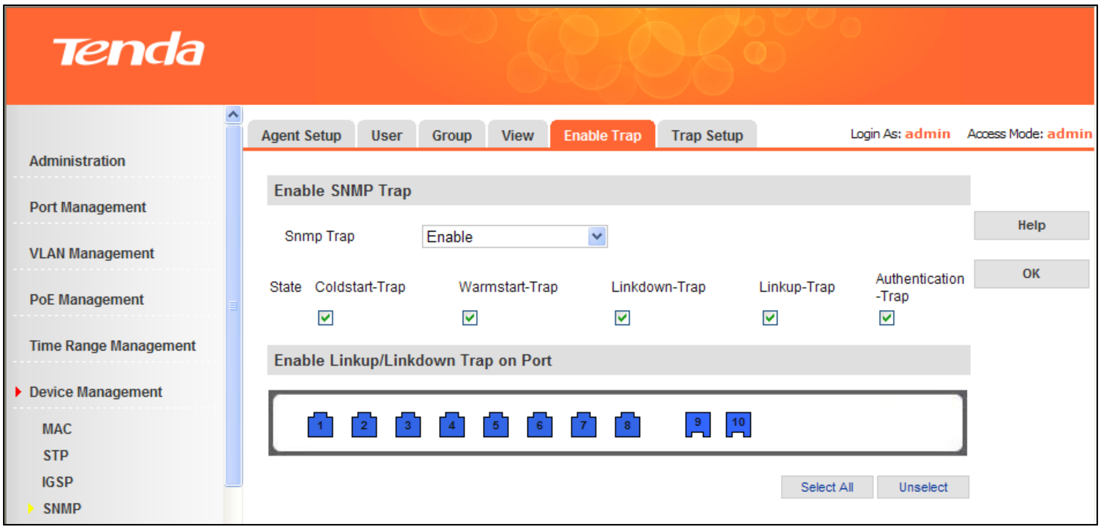
Rule: Include

Parameters on this page are described below:

Field	Description
View Name	Give a name to the View for identification.
MIB Subtree OID	Enter the Object Identifier (OID) for the entry of View.
Rule	Select the OID rule for the view entry. Include: The view entry can be managed by the SNMP manager. Exclude: The view entry cannot be managed by the SNMP manager.

4.5 Enable Trap

Trap function is used to inform the SNMP manager of critical events for the switch. Click **Device Management > SNMP > Enable Trap** to enter page below:



Enable SNMP Trap

Snmp Trap: Enable

State	Coldstart-Trap	Warmstart-Trap	Linkdown-Trap	Linkup-Trap	Authentication -Trap
	☑	☑	☑	☑	☑

Enable Linkup/Linkdown Trap on Port

By default, the SNMP Trap function is enabled on all ports. You can modify it as you need.

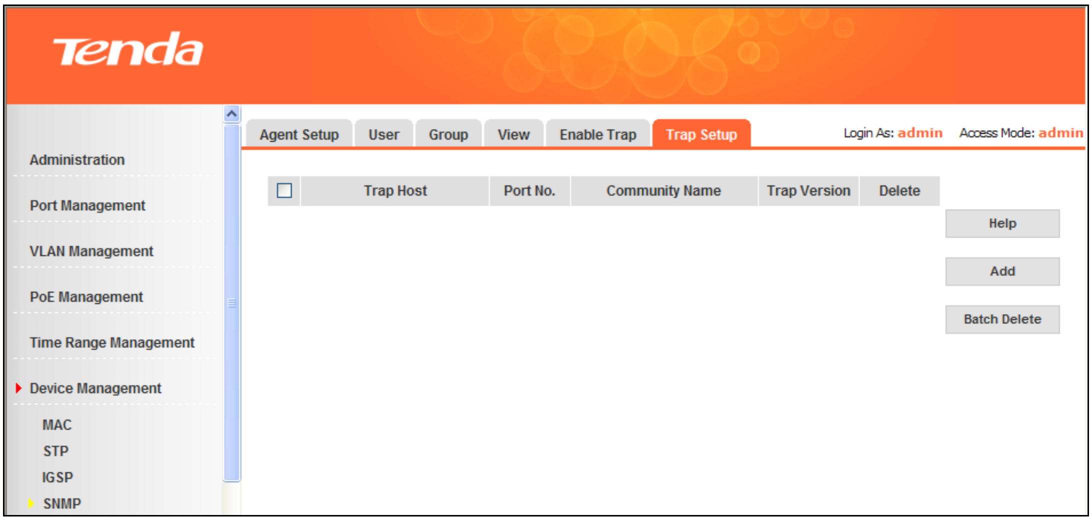
Parameters on this page are described below:

Field	Description
SNMP Trap	Enable/ Disable SNMP Trap function.
State	Select the Trap message type.
Coldstart-Trap	Send Coldstart Trap to designated host when device is undergoing a coldstart (power disconnection or reboot).
Warmstart-Trap	Send Warmstart Trap to designated host when the SNMP is disabled on the switch.
Linkdown-Trap	Send Linkdown Trap to designated host when an up link becomes down.
Linkup-Trap	Send Linkup Trap to designated host when a down link becomes up.
Authentication-Trap	Send Authentication failure Trap to designated host when SNMP module encounters an authentication failure.

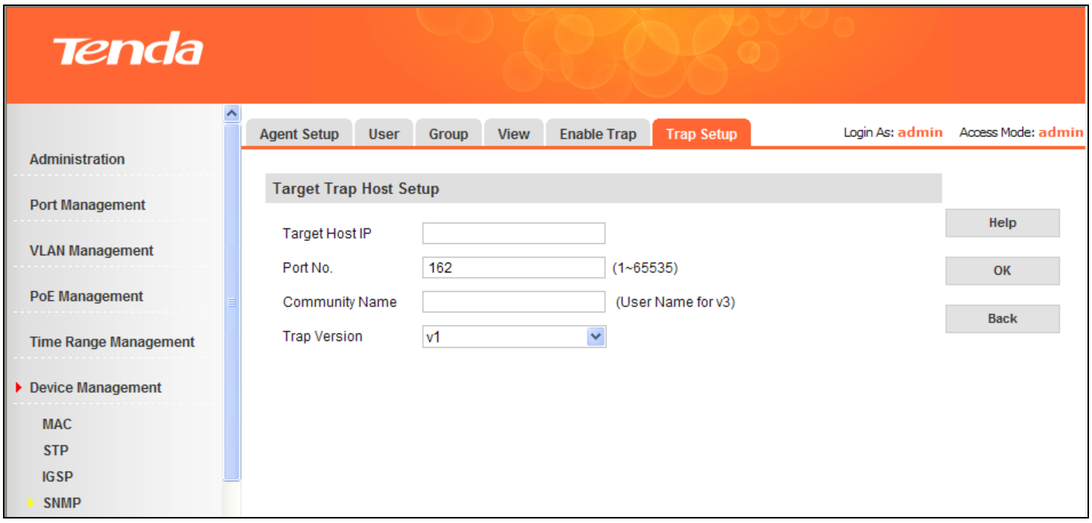
This page is only for enabling the SNMP Trap function. See the following for configuring the Trap Host to which Traps are to be sent.

4.6 Trap Setup

To enter the page for configuring the host to which Traps are to be sent, click **Device Management > SNMP > Trap Setup** as seen below.



Click **Add** to enter page below:



Target Trap Host Setup

Target Host IP

Port No. 162 (1~65535)

Community Name (User Name for v3)

Trap Version v1

Parameters on this page are described below:

Field	Description
Destination Host IP	Enter an IP address for the destination host. Note that the host IP should be on the same IP net segment as the management IP of the switch.
Port NO.	Enter a UDP port number to which Traps are to be sent. The default is 162.
Community Name	Enter a custom community name for the SNMP manager. As for SNMP v3, enter user name of the SNMP manager.
Trap Version	Select v1, v2c or V3. By default, the switch interacts with NMS using the SNMP v1.

5 DHCP Snooping

DHCP Snooping Functions

In computer networking DHCP snooping is a series of techniques applied to ensure the security of an existing DHCP infrastructure. When DHCP servers are allocating IP addresses to the clients on the LAN, DHCP snooping can be configured on LAN switches to harden the security on the LAN to allow only clients with specific IP/MAC addresses to have access to the network.

Ports which are connected to DHCP servers and other DHCP Snooping devices need to be configured as trusted ports and other ports need to be configured as untrusted ports, so that DHCP clients can only obtain IP addresses from legal DHCP clients.

- Untrusted Port: The port is used for connecting to terminal devices. Clients on this kind of ports can only send DHCP request packets.
- Trusted Port: Port or Trunk port connecting to legal DHCP servers.

The switch can establish a user binding list via DHCP snooping. Once a client connected to an untrusted port obtains a legal IP address, the switch will automatically display an entry (including client IP/ MAC address, port number/belonging VLAN, lease time, etc.) in the user binding list for MAC source defense and Ping test.

DHCP Option 82

As Option 82 records location info of DHCP clients, you can use it to locate DHCP clients, thus implementing security and accounting control for clients.

The DHCP Snooping function of this device supports Option 82 and two sub-options are available: circuit ID sub-option and remote ID sub-option. By default, the circuit ID sub-option is made up of port belonging VLAN ID of received DHCP client request packets and port number. The remote ID sub-option is made up of the MAC address of the DHCP Snooping device which receives DHCP client request packets.

When the switch receives DHCP request packets, it will process these packets according to whether Option 82 included, processing strategy of user configuration and user-defined option status, and then forward them to the DHCP server. Three strategies are available: replace, keep and drop.

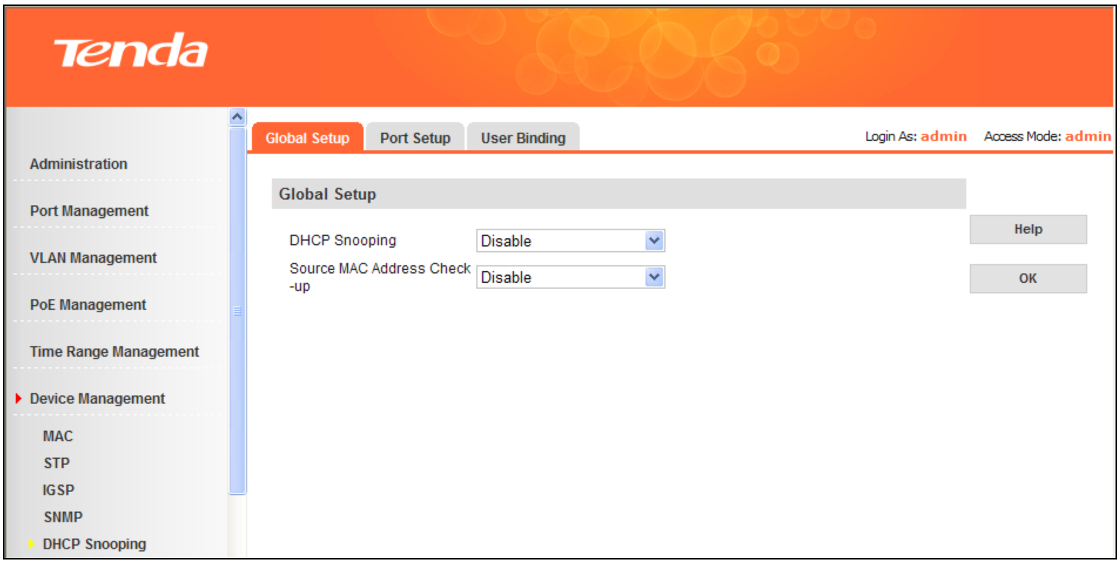
Option 82 included or not	Processing Strategy	User-defined Option Status	Description

Yes	Replace	Enable	Use user-defined circuit ID sub-option and remote ID sub-option to fill Option 82. Then the previous Option 82 information will be replaced and forwarded.
		Disable	Use the default circuit ID sub-option and remote ID sub-option on this switch to fill Option 82. Then the previous Option 82 information will be replaced and forwarded.
	Keep	Any	The previous Option 82 information will be kept and forwarded.
	Drop	Any	The previous Option 82 information will be discarded.
No	Any	Enable	Use the user-defined circuit ID sub-option and remote ID sub-option on this switch to fill Option 82 and forward it.
		Disable	Use the default circuit ID sub-option and remote ID sub-option on this switch to fill Option 82 and forward it.

When the switch receives response packets of the DHCP server, and if these packets contain Option 82, the switch will delete Option 82 and then forward these packets. If Option 82 not contained, packets will be forwarded directly.

5.1 Global Setup

Click **Device Management > DHCP Snooping > Global Setup** to enter page below:



Global Setup

DHCP Snooping: Disable

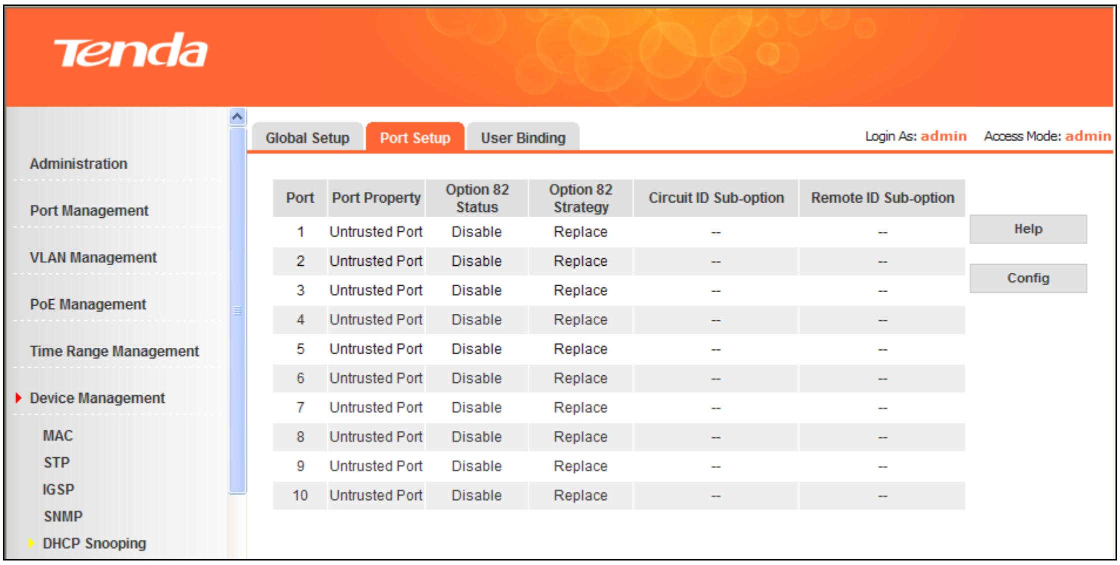
Source MAC Address Check-up: Disable

Parameters on this page are described below:

Field	Description
DHCP Snooping	Enable/Disable DHCP snooping function globally. By default, this function is disabled.
Source MAC Address Check-up	Enable/Disable source MAC address check-up function. There are two fields in DHCP packets for storing client MAC addresses. Once this function is enabled, the switch will make a comparison between these two fields. If these two fields are different, packets will be dropped.

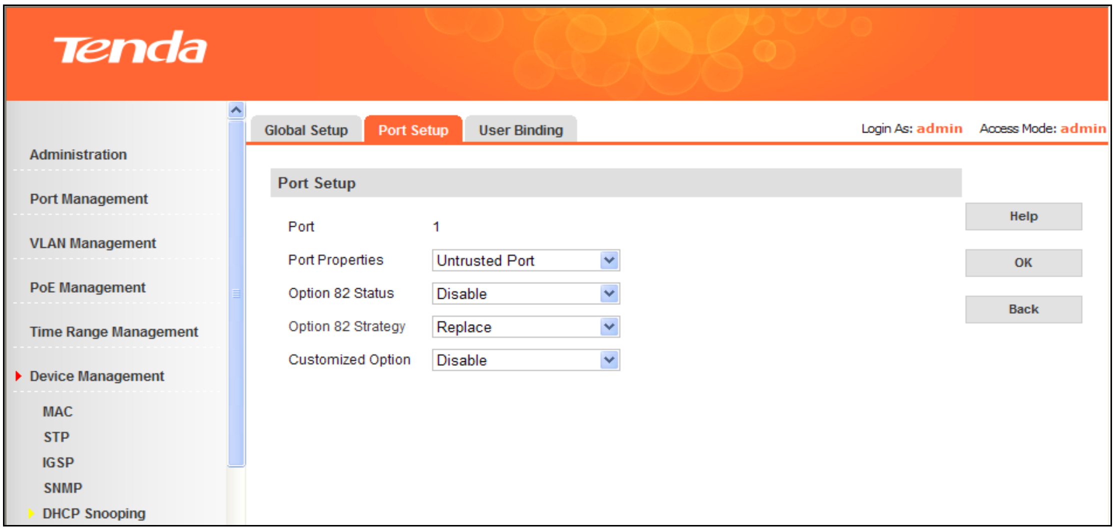
5.2 Port Setup

After finishing global DHCP snooping settings, you need to configure DHCP snooping port settings. Click **Device Management > DHCP Snooping > Port Setup** to enter page below:



Port	Port Property	Option 82 Status	Option 82 Strategy	Circuit ID Sub-option	Remote ID Sub-option
1	Untrusted Port	Disable	Replace	--	--
2	Untrusted Port	Disable	Replace	--	--
3	Untrusted Port	Disable	Replace	--	--
4	Untrusted Port	Disable	Replace	--	--
5	Untrusted Port	Disable	Replace	--	--
6	Untrusted Port	Disable	Replace	--	--
7	Untrusted Port	Disable	Replace	--	--
8	Untrusted Port	Disable	Replace	--	--
9	Untrusted Port	Disable	Replace	--	--
10	Untrusted Port	Disable	Replace	--	--

Click a certain port number to enter the corresponding port setup page.



Port Setup

Port 1

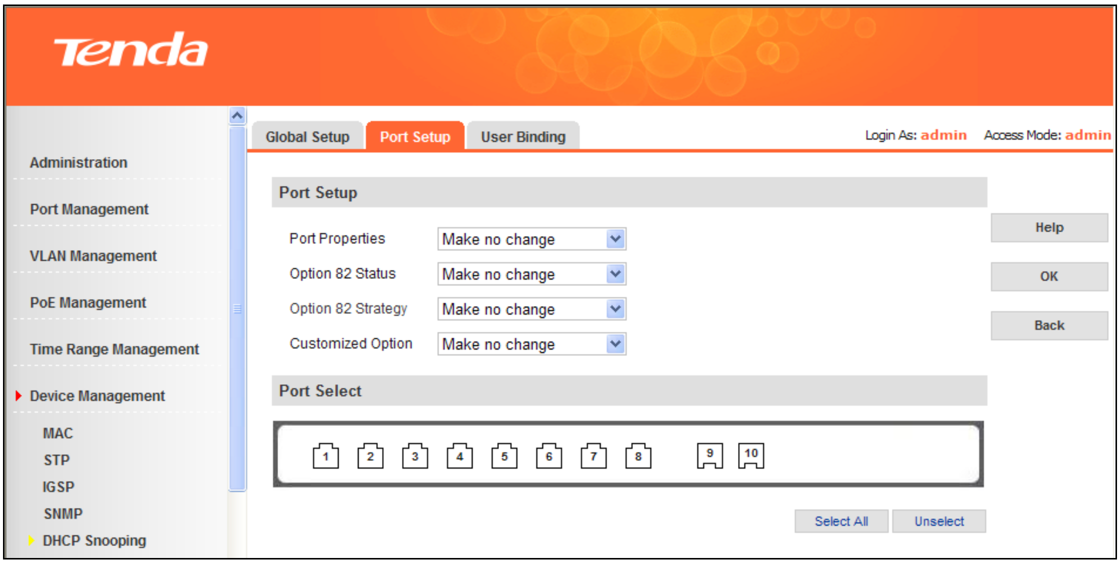
Port Properties: Untrusted Port

Option 82 Status: Disable

Option 82 Strategy: Replace

Customized Option: Disable

To batch configure port settings, click **Config**.



Port Setup

Port Properties: Make no change

Option 82 Status: Make no change

Option 82 Strategy: Make no change

Customized Option: Make no change

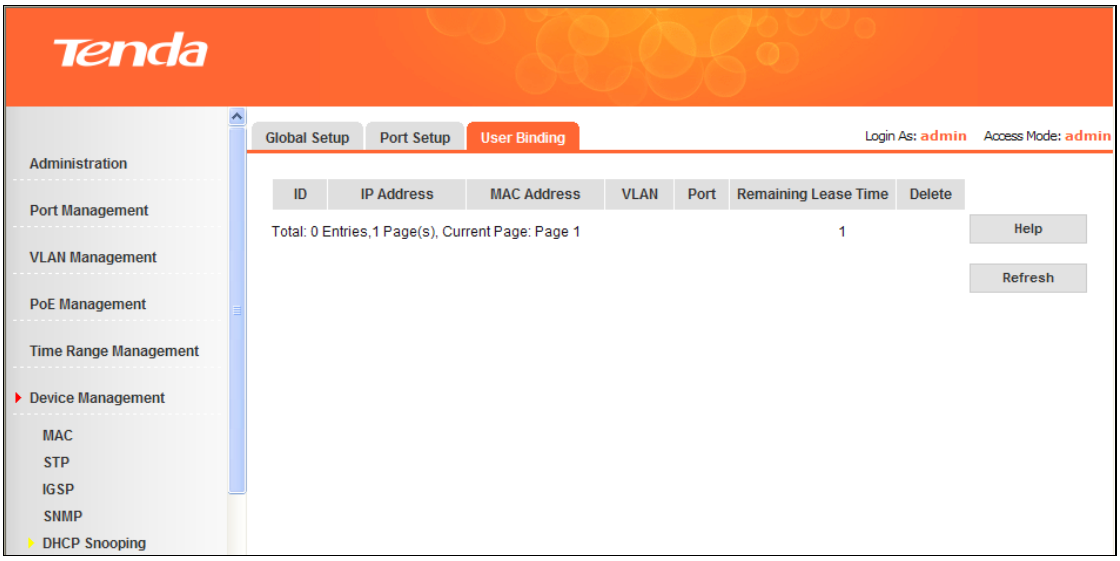
Port Select

Parameters on pages are described below:

Field	Description
Port	Display the corresponding port number.
Port Properties	Configure the current port's DHCP snooping property: trust or untrust.
Option 82 Status	Enable/Disable option 82. Option 82 records DHCP clients' location info. To make Option82 strategy valid, you need to enable Option82 first.
Option 82 Strategy	When there are option 82 fields in DHCP packets, three strategies are available: replace, keep and drop. **Replace:** Replace the previous option 82 info with default or user-defined option 82 info. **Keep:** Reserve option 82 fields in DHCP packets. **Drop:** Discard packets which include option 82 fields.
Customized Option	Enable/Disable customized circuit/remote ID sub-option function.
Circuit ID Sub-option	Specify the user-defined circuit ID sub-option.
Remote ID Sub-option	Specify the user-defined remote ID sub-option.

5.3 User Binding

Click **Device Management > DHCP Snooping > User Binding** to enter page below:



ID	IP Address	MAC Address	VLAN	Port	Remaining Lease Time	Delete

Total: 0 Entries,1 Page(s), Current Page: Page 1 1

Parameters on this page are described below:

Field	Description
ID	Display user binding digits in the list.
IP Address	Display the user binding's IP address.
MAC Address	Display user binding's MAC address.
VLAN	Display user binding's VLAN ID.
Port	Display user binding's port number.
Remaining Lease Time	Display user binding's remaining lease time.

QoS

QoS (Quality of Service) functions to provide different quality of service for various network applications and requirements and optimize the bandwidth resource distribution so as to provide a network service experience of a better quality. The following two parts are included:

QoS Configuration: Provide different network applications with different quality of service.

Traffic Control: Limit bandwidth and broadcast traffic for the switch to ensure normal network operation.

1 QoS Configuration

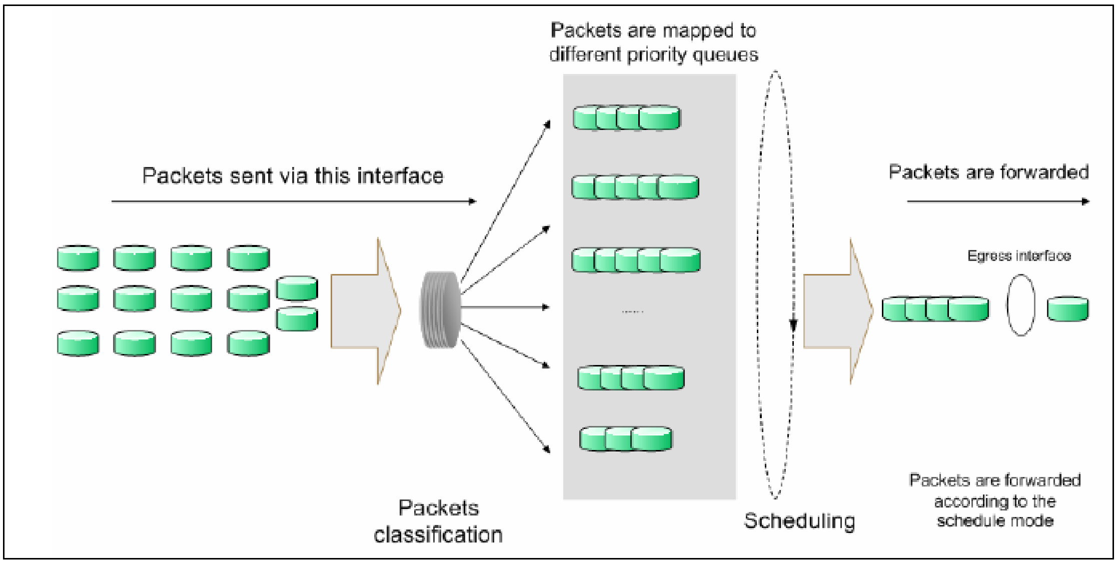
Traditional IP network mainly involves business, like www, FTP, E-mail, etc. It can deliver packets to the destination but ensures no guarantee of forwarding delay, jitter, packet loss rate and reliability.

As IP technology develops rapidly and all kinds of new business, such as distance education, teleconference, VOD, etc. emerge, IP network has turned into a multi-service bearer network from a pure data network. Thus, QoS appears.

Briefly speaking, QoS provides network applications with different quality of service, like provide dedicated bandwidth, decrease transmission delay and jitter, reduce packet loss rate, etc.

➘ How QoS works

This switch adopts DiffServ (Differentiated Service) QoS module. This switch classifies the ingress packets, maps the packets to different priority queues and then forwards the packets according to specified scheduling algorithms to implement QoS function. The schematic diagram is shown below:


Packets are mapped to different priority queues
Packets sent via this interface
Packets are forwarded
Egress interface
Packets classification
Scheduling
Packets are forwarded according to the schedule mode

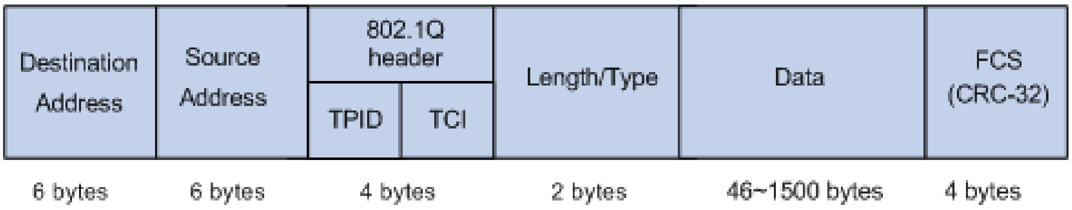
- Packets classification: Identifies packets conforming to certain characters according to certain rules.
- Map: The user can map the ingress packets to different priority queues based on the priority modes.
- Queue scheduling algorithm: When the network is congested, the problem that many packets compete for resources must be solved, usually in the way of queue scheduling.

Priority Mode

This switch implements three priority modes based on port, on 802.1P and on DSCP. For packets with CoS and DSCP enabled, DSCP takes effect. For packets with only CoS enabled, CoS takes effect. For packets without CoS and DSCP, port priority takes effect.

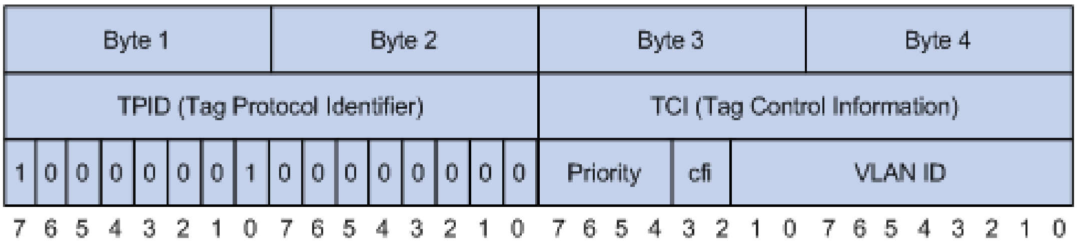
1．802.1p priority

The 802.1P priority, contained in the Ethernet header, is used by QoS disciplines to differentiate traffic on layer 2 where analyzing layer 3 IP header is not necessary. 802.1P priority is available only in an IEEE 802.1Q tagged frame. As seen below, the 4-byte 802.1Q tag contains a 2-byte TPID（Tag Protocol Identifier, value: 0x8100）and a 2-byte TCI（Tag Control Information).



Destination Address	Source Address	802.1Q header		Length/Type	Data	FCS (CRC-32)
		TPID	TCI			
6 bytes	6 bytes	4 bytes		2 bytes	46~1500 bytes	4 bytes

Below displays a detailed view of an 802.1Q tag. 802.1P priority, also known as class of service (CoS), is contained in the priority field of the TCI. It is made up of 3 bits and with available values ranging from 0 to 7.



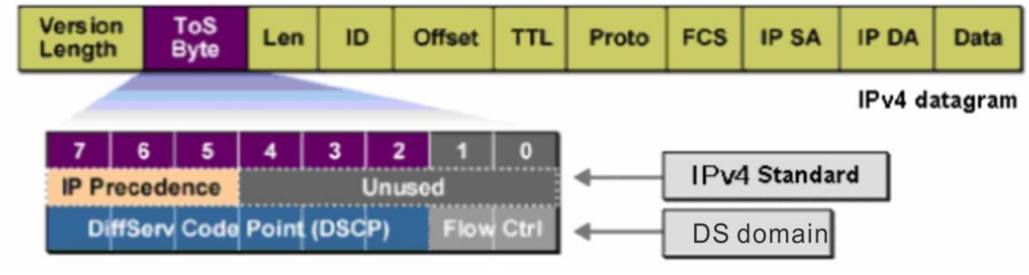
Byte 1								Byte 2								Byte 3								Byte 4							
TPID (Tag Protocol Identifier)																TCI (Tag Control Information)															
1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	Priority			cfi	VLAN ID											
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0

Here you can configure different CoS priority settings for different queues. Data-frames with 802.1Q tag are mapped to different priority levels based on priority mode of its tags but the untagged packets are mapped based on default ingress port priority mode (Click **QoS > QoS Configuration > Port Priority**).

By default, the 802.1P priority tags are mapped to the Switch's priority queues as follows:

802.1p Priority	Queue
1,2	1
0,3	2
4,5	3
6,7	4

2. DSCP Priority



IP datagram

As shown in the figure above, the ToS (Type of Service) in an IP header contains 8 bits. The first three bits indicate IP precedence in the range of 0 to 7. RFC2474 re-defines the ToS field in the IP packet header, which is called the DS field. The first six bits of the DS field indicate DSCP precedence in the range of 0 to 63. The last 2 bits are reserved.

On the Web management page, you can configure different DS field mapping to the corresponding priority levels. Non-IP datagram with 802.1Q tag are mapped to different priority levels based on 802.1P priority mode and on which data frames are tagged or not.

By default, the DSCP priority tags are mapped to the Switch's CoS priority queues as follows:

DSCP Priority	CoS Priority
0~15	1
16~31	3
32~47	5
48~63	7

3. Port Priority

The port priority is based on switch's physical ports in a range of 0 to 7. It is used to determine the forwarding sequence of packets which are not carrying priority identifiers.

Scheduling Mode Overview

When congestion occurs on the network, the problem that many packets compete for resources must be solved, usually in the way of queue scheduling. The switch provides two schedule modes: SP(Strict-Priority） and WRR (Weighted Round Robin).

1．Strict Priority Mode

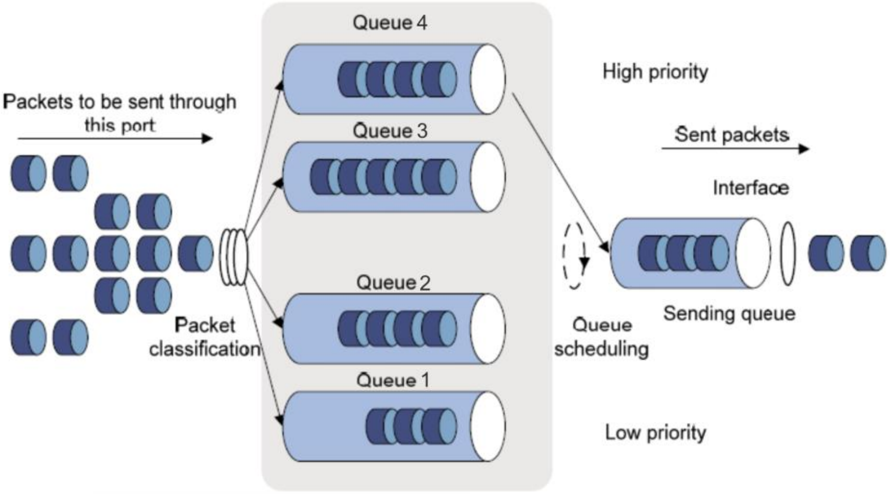


Diagram for SP queuing

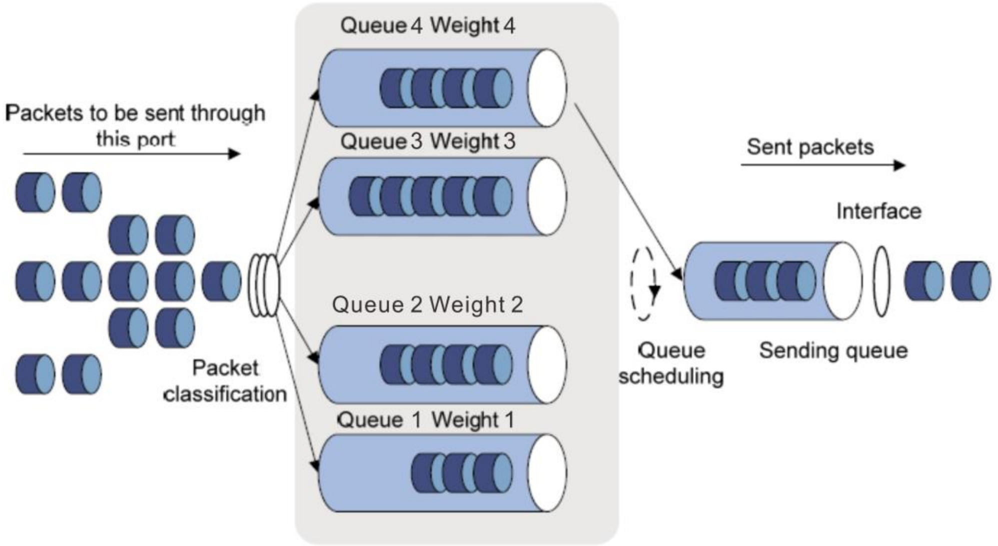
Strict Priority Queueing is specially designed to meet the demands of critical services or applications. When congestion occurs on the network, the system will ask for service preferentially to reduce response delay. For example, 4 egress queues 3, 2, 1 and 0 with descending priority are configured on a port.

Then under SP algorithm, the port strictly prioritizes packets from higher priority queue over those from lower priority queue. Namely, packets in the queue with lower priority are sent only when the queue with higher priority is empty. Thus High-priority packets are always processed before those of less priority. Medium-priority packets are always processed before low-priority packets. The lowest priority queue would be serviced only when highest priority queues had no packets buffered.

Disadvantages of SP: The SP queueing gives absolute priority to high-priority packets over low-priority traffic; it should be used with care. The moment a higher priority packet arrived in its queue, however, servicing of the lower priority packets would be interrupted in favor of the higher priority queue or packets will be dropped if the amount of high-priority traffic is too great to be emptied within a short time.

The disadvantage of SP queue is that: if there are packets in the queues with higher priority for a long time in congestion, the packets in the queues with lower priority will be "starved to death" because they are not served.

2．Weight Round Robin Mode (WRR)

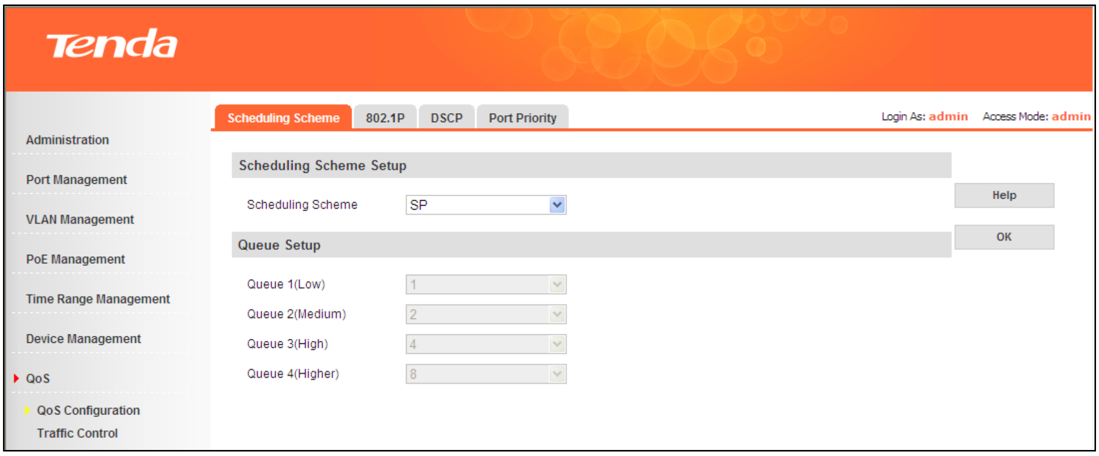


WRR-Mode: Weight Round Robin Mode. In this mode, packets in all the queues are sent in order based on the weight value for each queue and every queue can be assured of a certain service time. Assuming there are 4 egress queues on the port. The four weight values (namely, w4, w3, w2, and w1) indicate the proportion of resources assigned to the four queues respectively. On a 100M port, if you set the weight values of WRR queue-scheduling algorithm to 25, 15, 5 and 5(correspond to w4, w3, w2, and w1 respectively). Then the queue with the lowest priority can be ensured of, at least, 10 Mbps bandwidth, thus WRR queue overcomes the disadvantage of SP queue that the packets in the queues with lower priority cannot get service for a long time. In WRR mode, though the queues are scheduled in order, the service time for each queue is not fixed, that is to say, if a queue is empty, the next queue will be scheduled. In this way, the bandwidth resources are made full use of.

1.1 Scheduling Scheme

On this page you can select a schedule mode for the switch. When congestion occurs on the network, the problem that many packets compete for resources must be solved, usually in the way of queue scheduling.

Click **QoS > QoS Configuration > Scheduling Scheme** to enter page below:



Scheduling Scheme Setup

Scheduling Scheme: SP

Queue Setup

Queue 1(Low)	1
Queue 2(Medium)	2
Queue 3(High)	4
Queue 4(Higher)	8

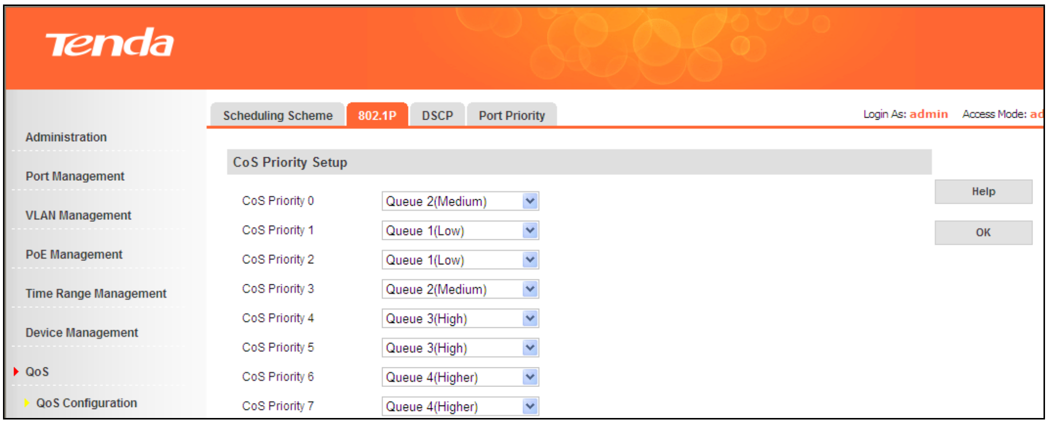
Parameters on this page are described below:

Field	Description
Scheduling Scheme	Select scheduling mode for the switch: SP or WRR. **SP:** Strict-Priority Mode. In this mode, the queue with higher priority will occupy the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty. **WRR:** Weight Round Robin Mode. In this mode, packets in all the queues are sent in order based on the weight value for each queue.
Queue Setup	Configure weight value for queues. Fields will be configurable in a range of 1 to 31 in WRR mode.

1.2 802.1P

Packets with 802.1Q tag are mapped to different priority levels based on 802.1P priority mode but the untagged packets are mapped based on port priority mode.

Click **QoS > QoS Configuration > 802.1P** to enter page below:



CoS Priority Setup

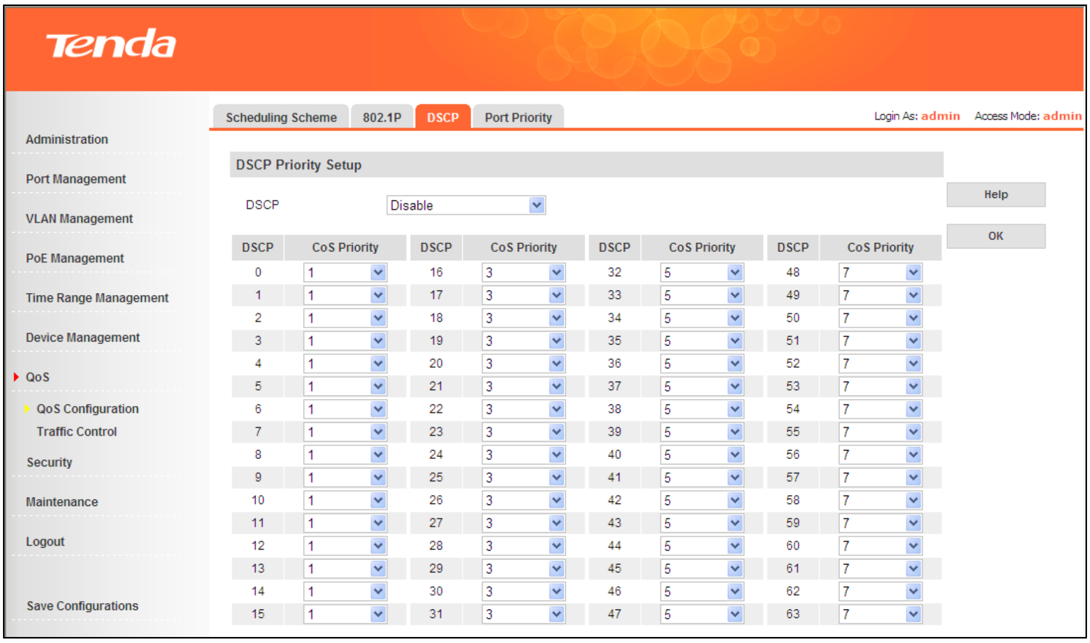
CoS Priority 0	Queue 2(Medium)
CoS Priority 1	Queue 1(Low)
CoS Priority 2	Queue 1(Low)
CoS Priority 3	Queue 2(Medium)
CoS Priority 4	Queue 3(High)
CoS Priority 5	Queue 3(High)
CoS Priority 6	Queue 4(Higher)
CoS Priority 7	Queue 4(Higher)

You can select CoS priorities for corresponding queues as you need. When congestion occurs on the port, the switch will assign packets with CoS priority to corresponding queues according to mapping relations you've set.

1.3 DSCP

On this page you can configure DSCP priority. DSCP (DiffServ Code Point) is a new definition to IP ToS field given by IEEE. This field is used to divide IP datagram into 64 priorities. When DSCP Priority is enabled, IP datagrams are mapped to different priority levels based on DSCP priority mode; non-IP datagrams with 802.1Q tag are mapped to different priority levels based on 802.1P priority mode；non-IP datagrams without 802.1Q tag are mapped to different priority levels based on port priority mode.

Click **QoS > QoS Configuration > DSCP** to enter page below:



DSCP Priority Setup

DSCP: Disable

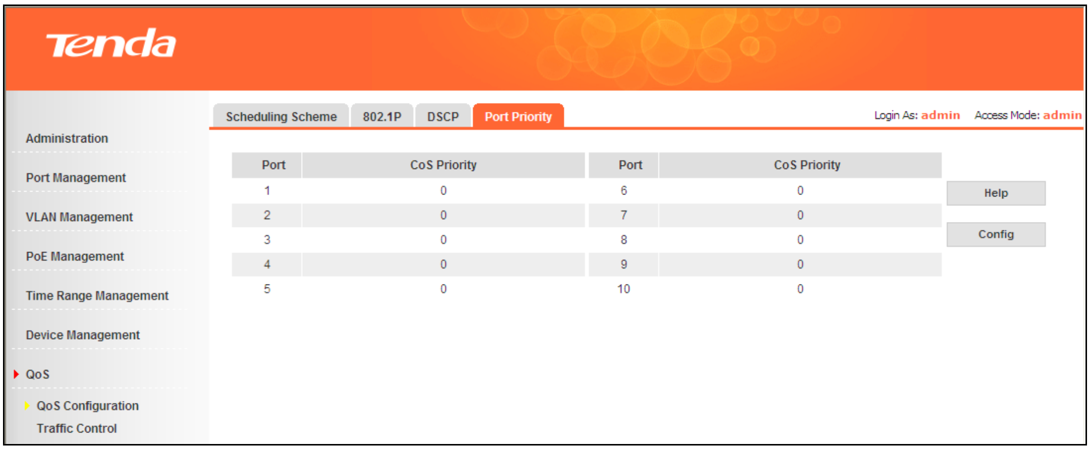
DSCP	CoS Priority	DSCP	CoS Priority	DSCP	CoS Priority	DSCP	CoS Priority
0	1	16	3	32	5	48	7
1	1	17	3	33	5	49	7
2	1	18	3	34	5	50	7
3	1	19	3	35	5	51	7
4	1	20	3	36	5	52	7
5	1	21	3	37	5	53	7
6	1	22	3	38	5	54	7
7	1	23	3	39	5	55	7
8	1	24	3	40	5	56	7
9	1	25	3	41	5	57	7
10	1	26	3	42	5	58	7
11	1	27	3	43	5	59	7
12	1	28	3	44	5	60	7
13	1	29	3	45	5	61	7
14	1	30	3	46	5	62	7
15	1	31	3	47	5	63	7

Parameters on this page are described below:

Field	**Description**
DSCP Priority Setup	Enable/Disable DSCP priority
DSCP	Indicate the priority is determined by the DS domain (range: 0~63) of IP datagram and CoS priority settings on the **QoS > QoS Configuration > 802.1P** page.

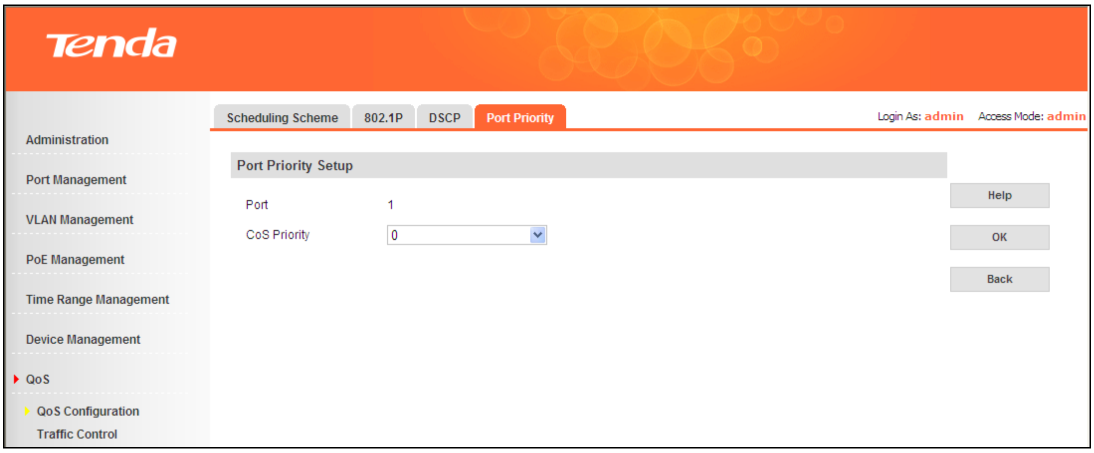
1.4 Port Priority

Click **QoS > QoS Configuration > Port Priority** to enter page below:



Port	CoS Priority	Port	CoS Priority
1	0	6	0
2	0	7	0
3	0	8	0
4	0	9	0
5	0	10	0

By default, CoS priority on all ports is 0 and you can modify it as you need.



Port Priority Setup

Port 1

CoS Priority 0

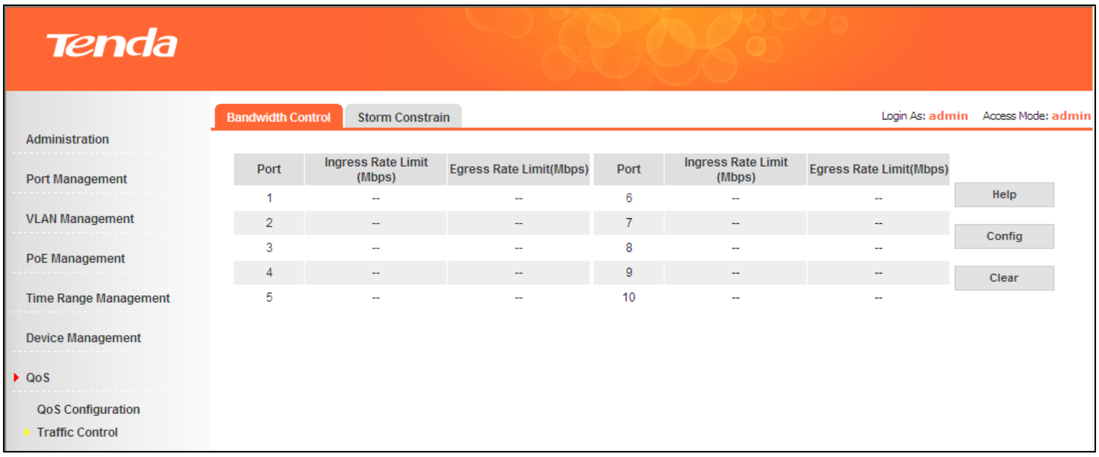
2 Traffic Control

The Traffic control function, limiting bandwidth and broadcast traffic on each port, is implemented on the **Bandwidth Control** and **Storm Constrain** pages.

2.1 Bandwidth Control

This switch adopts token bucket for flow control. If rate limit is configured on a certain port, all packets transmitted or received by this port will be processed first by token bucket. If there are enough tokens, packets can be received or transmitted, otherwise discarded.

Click **QoS > Traffic Control > Bandwidth Control** to enter page below:



Port	Ingress Rate Limit (Mbps)	Egress Rate Limit(Mbps)	Port	Ingress Rate Limit (Mbps)	Egress Rate Limit(Mbps)
1	--	--	6	--	--
2	--	--	7	--	--
3	--	--	8	--	--
4	--	--	9	--	--
5	--	--	10	--	--

By default, no bandwidth control settings are configured on all ports. You can click the corresponding port number or click **Config** on the **Bandwidth Control** page to configure bandwidth control settings.

Parameters on this page are described below:

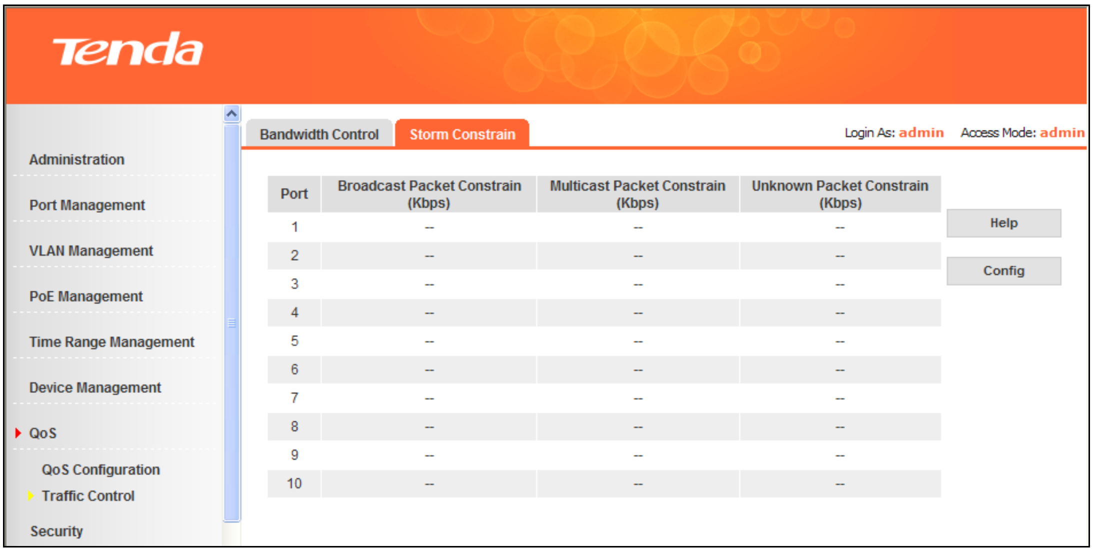
Field	Description
Ingress Rate Limit (Mbps)	Configure the bandwidth for receiving packets on the port with a range of 1 to 1000. The default is 1000 which indicates no limit.
Egress Rate Limit (Mbps)	Configure the bandwidth for sending packets on the port with a range of 1 to 1000. The default is 1000 which indicates no limit.

2.2 Storm Constrain

As a main method for discovering unknown devices, broadcast plays an important role in networking. With the increase of computers in networking, broadcast packets increase and the network is occupied by large numbers of broadcast packets. When the number of broadcast packets reaches 30%, the networking transmission capacity will be reduced greatly and P2Pcommunication will be influenced, leading to broadcast storm.

Storm Control function allows the switch to filter broadcast, multicast and unknown unicast frame in the network. If the transmission rate of the three kind packets exceeds the set bandwidth, the packets will be automatically discarded to avoid network broadcast storm.

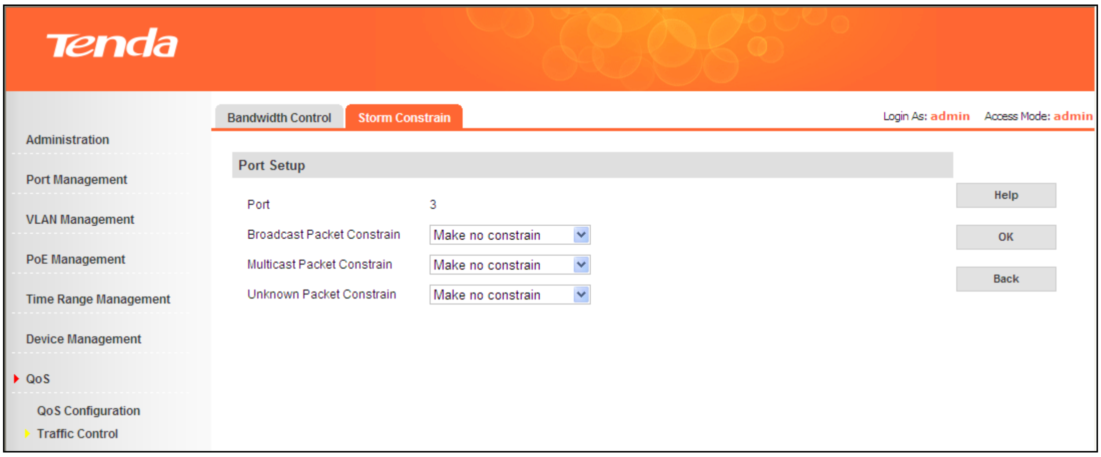
Click **QoS > Traffic Control > Storm Constrain** to enter page below:



Login As: admin Access Mode: admin

Port	Broadcast Packet Constrain (Kbps)	Multicast Packet Constrain (Kbps)	Unknown Packet Constrain (Kbps)
1	--	--	--
2	--	--	--
3	--	--	--
4	--	--	--
5	--	--	--
6	--	--	--
7	--	--	--
8	--	--	--
9	--	--	--
10	--	--	--

To configure storm constrain settings on a single port, click the corresponding port number.



Login As: admin Access Mode: admin

Port Setup

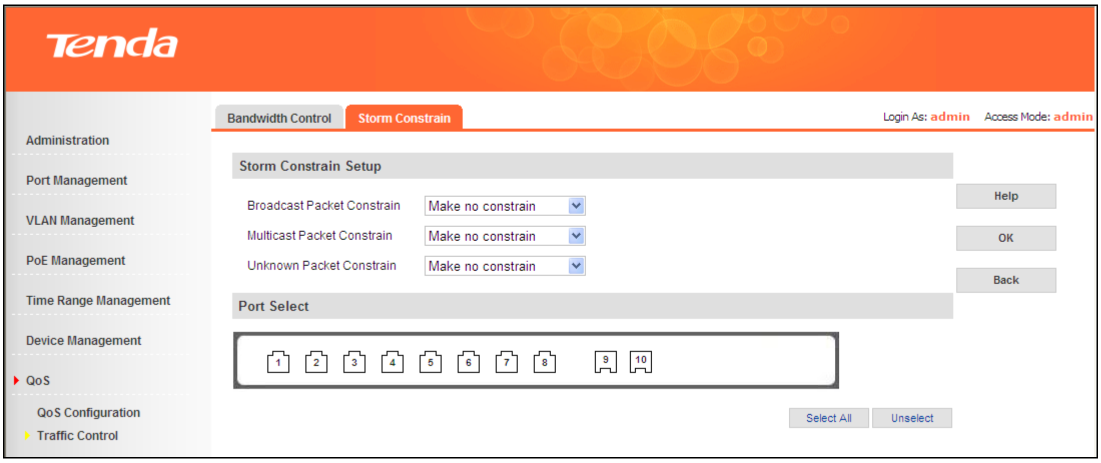
Port 3

Broadcast Packet Constrain: Make no constrain

Multicast Packet Constrain: Make no constrain

Unknown Packet Constrain: Make no constrain

To batch configure storm constrain settings, click **Config**.



Login As: admin Access Mode: admin

Storm Constrain Setup

Broadcast Packet Constrain: Make no constrain

Multicast Packet Constrain: Make no constrain

Unknown Packet Constrain: Make no constrain

Port Select

Parameters on this page are described below:

Field	Description
Broadcast Packet Constrain	Enable/Disable constrain function of the broadcast packet (its destination MAC is FF:FF:FF:FF:FF:FF) on the corresponding port. Once this function is enabled, you need to specify a broadcast constrain value within a range of 128~50000kbps.
Multicast Packet Constrain	Enable/Disable constrain function of the multicast packet (the 8th bit of its destination MAC is 1) on the corresponding port. Once this function is enabled, you need to specify a multicast constrain value within a range of 128~50000kbps.
Unknown Packet Constrain	Enable/Disable constrain function of the unknown packet (its destination MAC is not contained in the MAC table) on the corresponding port. Once this function is enabled, you need to specify an unknown constrain value within a range of 128~50000kbps.

Security

This section provides your local area network with security assurance. The following two parts are included:

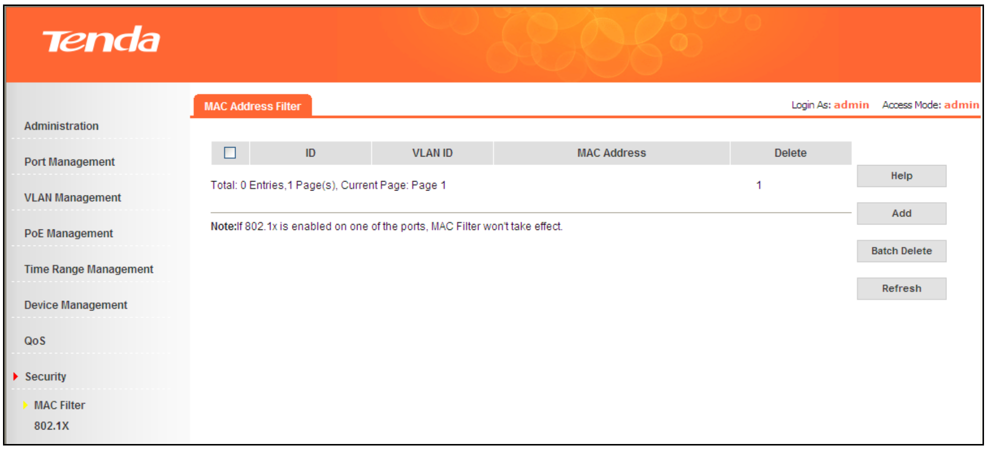
MAC Filter: Manage Internet access for computers in local area network.

802.1X: Authenticate access users in LAN and ensure security for LAN devices and resources.

1 MAC Filter

Once MAC filter settings are configured on this device, the device will check source and destination MAC addresses of ingress packets. If source and destination MAC addresses already exist in the MAC filter table, these packets will be discarded.

Click **Security > MAC Filter** to enter page below:



Login As: admin Access Mode: admin

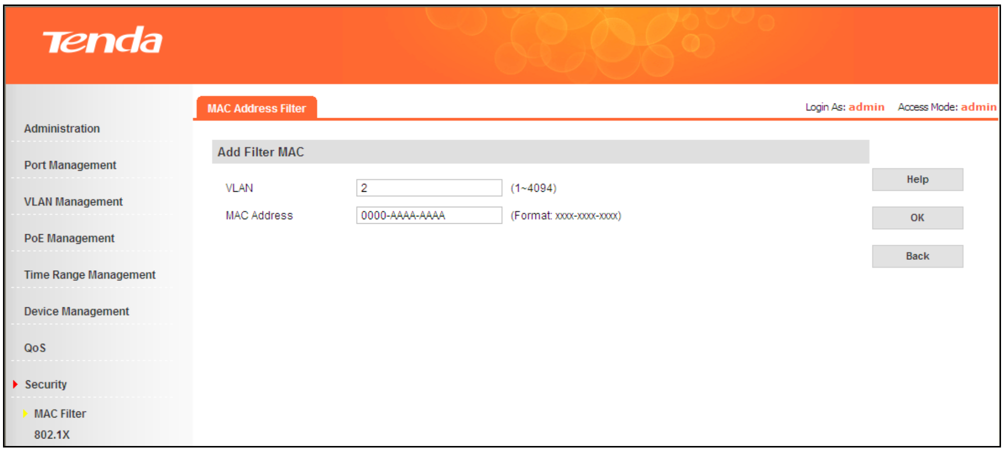
☐	ID	VLAN ID	MAC Address	Delete

Total: 0 Entries,1 Page(s), Current Page: Page 1 1

Note:If 802.1x is enabled on one of the ports, MAC Filter won't take effect.

Add MAC address filter entry:

1. Click **Add**;
2. Type in the VLAN ID (This step is omitted in port VLAN mode);
3. Follow onscreen instructions to type in the MAC address you wish to filter;



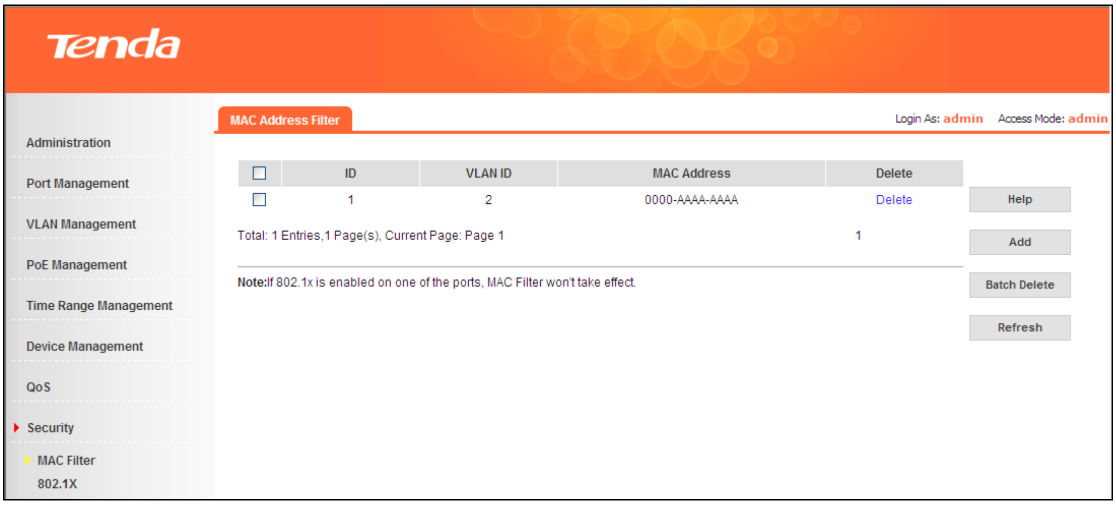
Login As: admin Access Mode: admin

Add Filter MAC

VLAN 2 (1~4094)

MAC Address 0000-AAAA-AAAA (Format: xxxx-xxxx-xxxx)

4. Click **OK**.



□	ID	VLAN ID	MAC Address	Delete
□	1	2	0000-AAAA-AAAA	Delete

Total: 1 Entries,1 Page(s), Current Page: Page 1 1

Note: If 802.1x is enabled on one of the ports, MAC Filter won't take effect.

Tip:

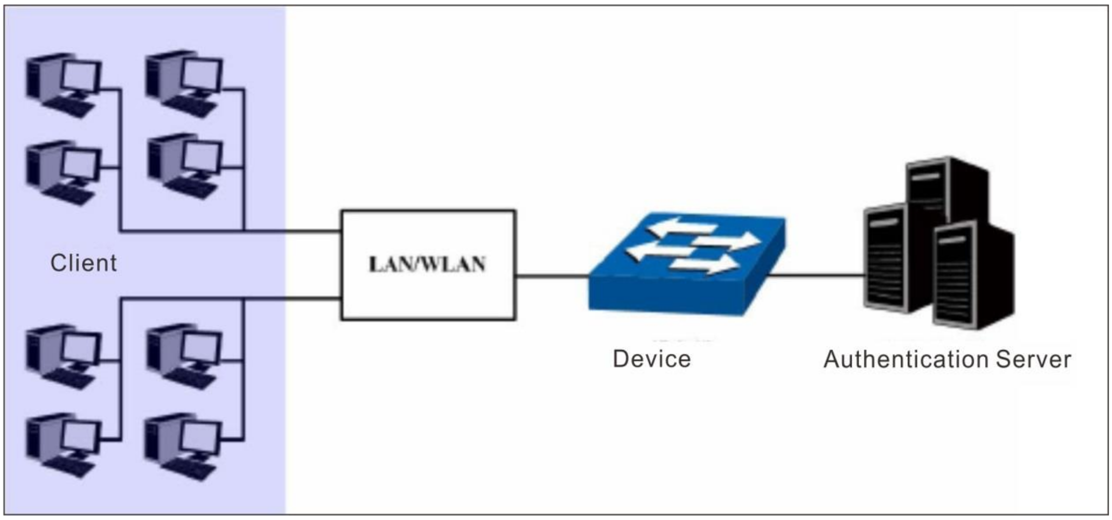
- The MAC address in the Static Address Table cannot be added to the Filtering Address Table.
- This MAC address filtering function is not available if the 802.1X feature is enabled.

2 802.1X

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism for devices wishing to attach to a LAN or WLAN. IEEE 802.1X defines the encapsulation of EAP over LAN" or EAPOL. With 802.1X port-based authentication, if the authentication server determines the credentials are valid, the client device will be allowed to access resources located on the protected side of the network.

➘ 802.1X system architecture

802.1X authentication involves three parties: Client, Device, and an authentication server.



- Client: A client device (such as a laptop) that wishes to attach to the LAN/WLAN for authentication should support EAPOL (Extensible Authentication Protocol over LAN）.
- Device: It is a network device, such as an Ethernet switch or wireless access point. Device acts as a physical/logical interface for LAN access and authenticates clients.
- Authentication server: An entity that provides authentication service for clients with authentication, authorization and billing. The commonly used one is the RADIUS (Remote Authentication Dial-In User Service) server.

➘ 802.1X Re-authentication

802.1X Re-authentication re-authenticates users that already pass authentication using timer or message trigger. With 802.1x Re-authentication enabled, the switch periodically checks users' connection status. If a user is detected not responding to re-authentication messages for a certain time length, then it will be disconnected. If it wishes to reconnect to the device, it must initiate an 802.1x authentication again via client software.

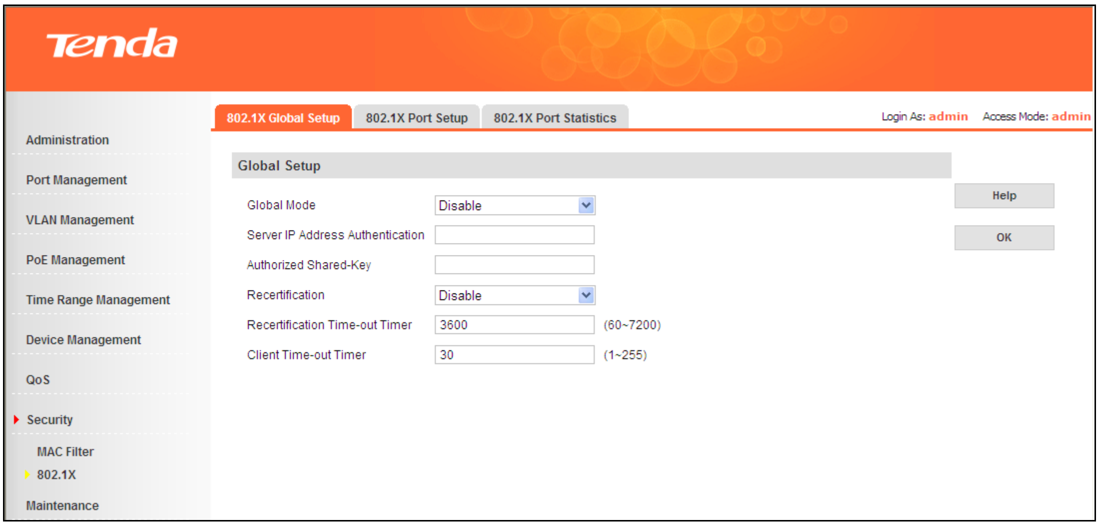
➘ 802.1X Access Control Method

This device supports port based access control method. When port based access control is adopted, as long as the first user connected to this port is authenticated successfully, other users accessed can use network resources without being authenticated. However, if the first user is disconnected, and when the re-authentication time is up, other users will be unable to access the Internet.

802.1X includes the following three parts: 802.1X Global Setup, 802.1X Port Setup, 802.1X Port Statistics.

2.1 802.1X Global Setup

Click **Security > 802.1X > 802.1X Global Setup** to enter the 802.1X Global Setup page.



Global Setup

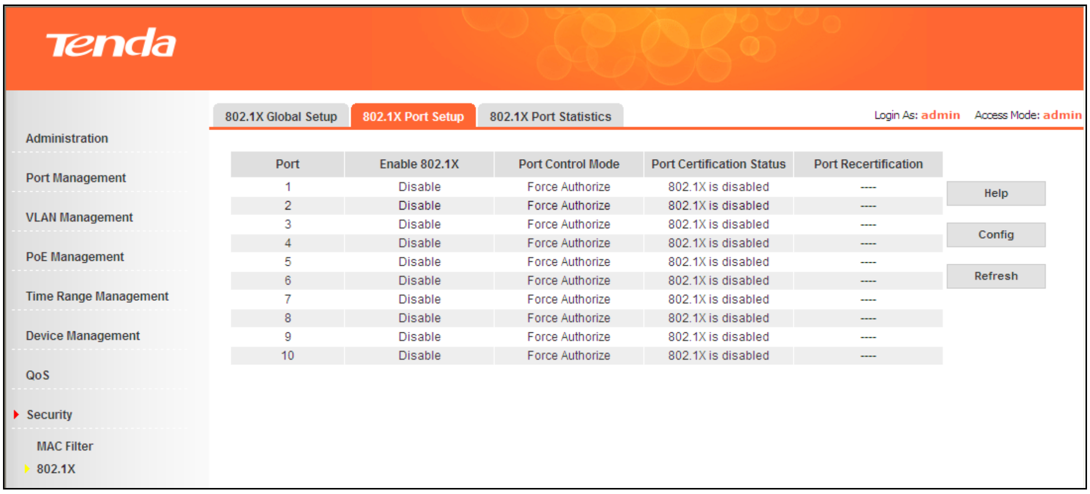
Global Mode	Disable	
Server IP Address Authentication		
Authorized Shared-Key		
Recertification	Disable	
Recertification Time-out Timer	3600	(60~7200)
Client Time-out Timer	30	(1~255)

Parameters on this page are described below:

Field	Description
Global Mode	Enable/Disable 802.1X feature globally. By default, the 802.1X feature is disabled globally on the device. **Tip:** 802.1X settings take effect only when the 802.1X feature is enabled on both the device and designated ports.
Authentication Server IP Address	Specify a valid Authentication Server IP that is on the same net segment as the switch's management IP address.
Authorized Shared-Key	Enter the authorized shared key as it is on the Radius authentication/authorization server.
Re-authentication	Enable or disable re-authentication on all ports.
Re-authentication Time-out Timer	Specify an interval for device to initiate an 802.1X re-authentication.
Client Time-out Timer	This timer is started while the switch sends EAP-Request/MD5 Challenge request to a targeted client. If no response is received from the client within the set time, switch will resend the request.

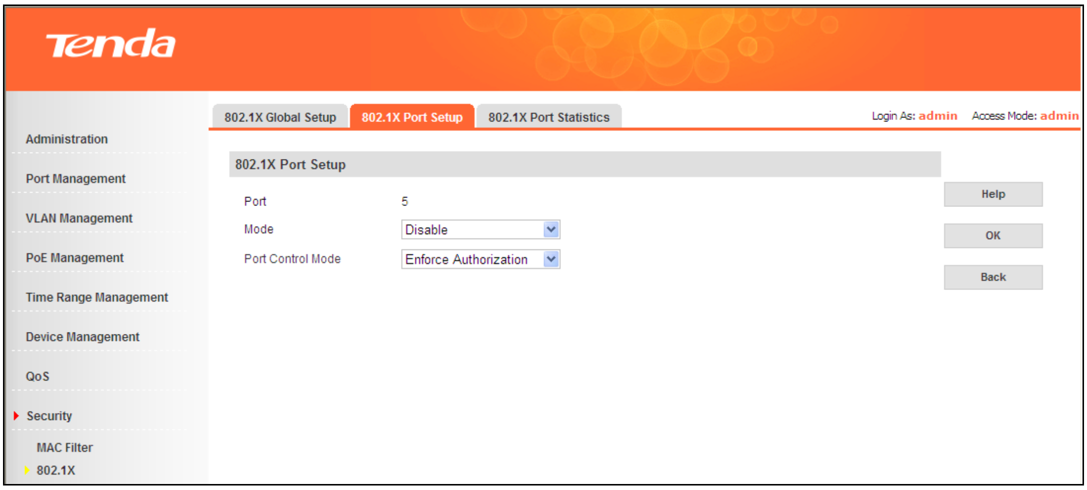
2.2 802.1X Port Setup

To configure 802.1X port settings, click **Security > 802.1X > 802.1X Port Setup**.



Port	Enable 802.1X	Port Control Mode	Port Certification Status	Port Recertification
1	Disable	Force Authorize	802.1X is disabled	----
2	Disable	Force Authorize	802.1X is disabled	----
3	Disable	Force Authorize	802.1X is disabled	----
4	Disable	Force Authorize	802.1X is disabled	----
5	Disable	Force Authorize	802.1X is disabled	----
6	Disable	Force Authorize	802.1X is disabled	----
7	Disable	Force Authorize	802.1X is disabled	----
8	Disable	Force Authorize	802.1X is disabled	----
9	Disable	Force Authorize	802.1X is disabled	----
10	Disable	Force Authorize	802.1X is disabled	----

To configure 802.1X port settings on a single port, click the corresponding port number.



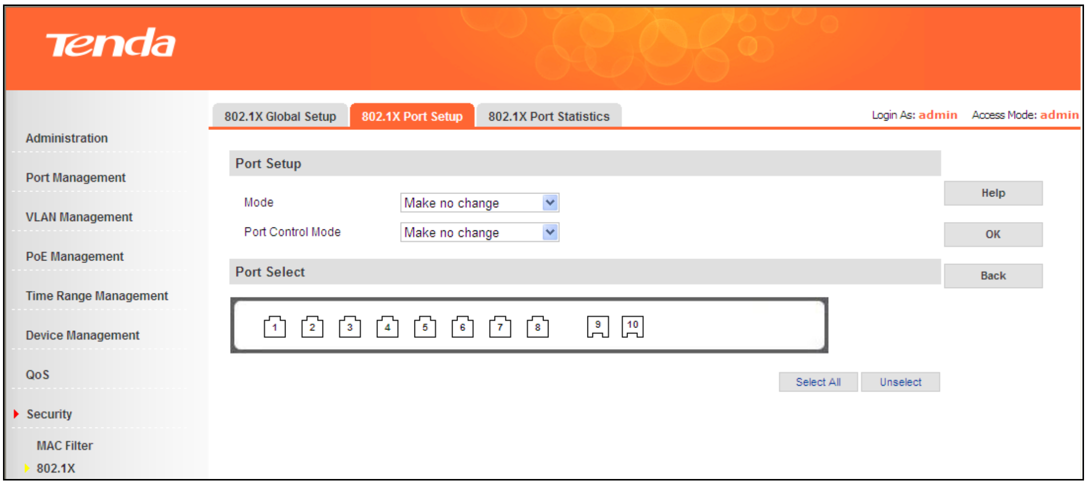
802.1X Port Setup

Port 5

Mode Disable

Port Control Mode Enforce Authorization

To batch configure 802.1X port settings, click **Config** to enter page below:



Port Setup

Mode Make no change

Port Control Mode Make no change

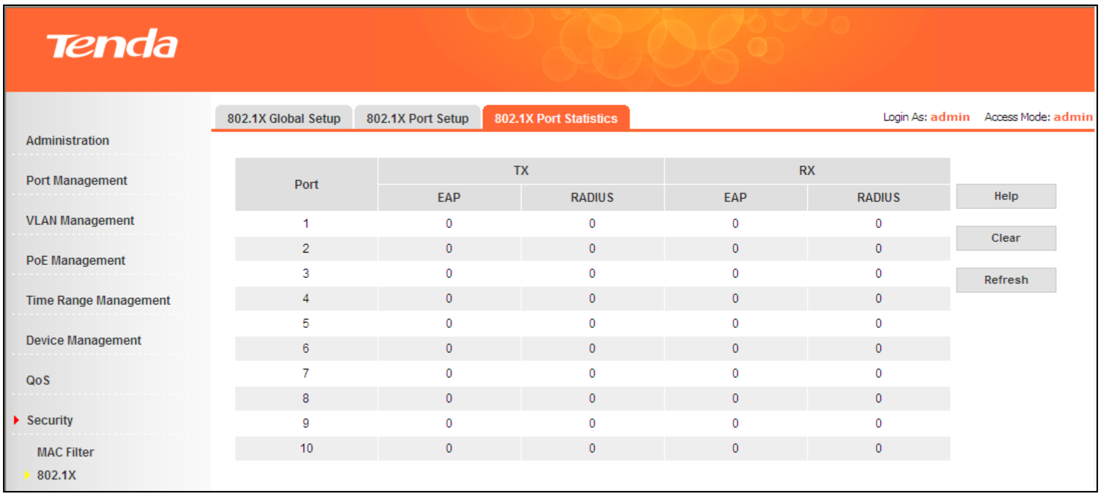
Port Select

Parameters on this page are described below:

Field	Description
Mode	Select to enable /disable 802.1X function.
Port Control Mode	Select the 802.1X port control mode from the drop-down list. **Auto:** Initially, the port is unauthorized. Only EAPoL packets can be transmitted and users are unable to access the Internet. If it is authenticated, the port will be authorized and users are able to access the Internet. **Enforce Authorization:** Ports are authorized and users are able to access the Internet without being authenticated. **Enforce Unauthorization:** Ports are unauthorized and users are unable to access the Internet. By default, the port control mode is Enforce Authorization.

2.3 802.1X Port Statistics

To view or clear 802.1X port statistics, click **Security > 802.1X > 802.1X Port Statistics** to enter page below:



Port	TX		RX	
	EAP	RADIUS	EAP	RADIUS
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

Maintenance

This section helps you know about operation status of this switch and provides you with methods of network diagnostics.

Syslog: View system logs, monitor network operation and troubleshoot network malfunction if necessary.

Network Diagnostics: When malfunction occurs, detect it via cable/Ping/tracert test.

1 Syslog

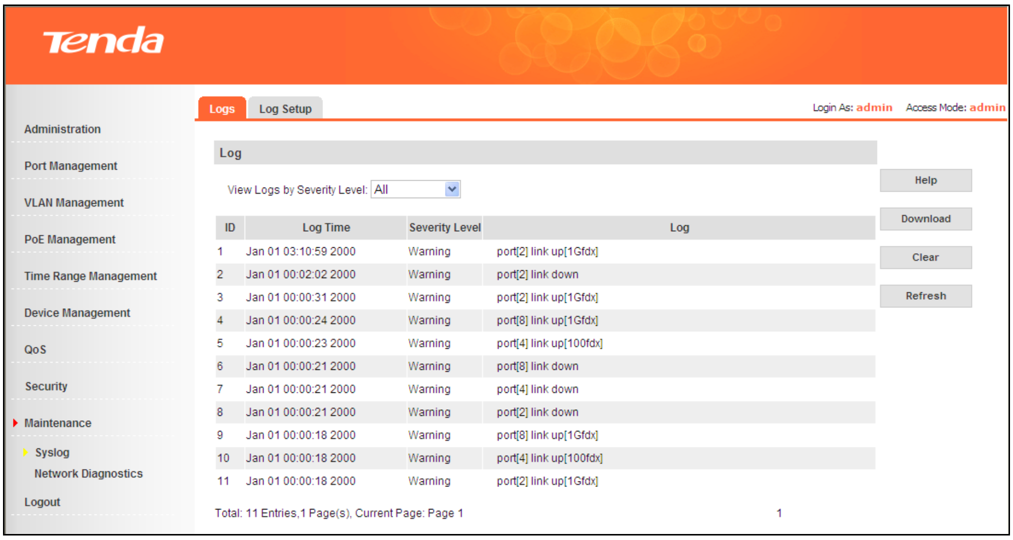
As the system information hub, system logs record, classify and manage system information, which offers a powerful support for network administrators to monitor network operation and diagnose malfunction.

The system logs of this switch are classified into the following eight levels by severity level. The smaller the value is, the higher the priority will be.

Secerity	Value	Description
Emergency	1	The system is unusable.
Alert	2	Actions must be taken immediately.
Critical	3	Critical conditions
Error	4	Error conditions
Warning	5	Warning conditions
Notice	6	Normal but significant conditions
informational	7	Informational messages which should be recorded
debug	8	Debug-level messages

1.1 Logs

To view and download system logs, click **Maintenance > Syslog > Logs** to enter page below:



Log

View Logs by Severity Level: All

ID	Log Time	Severity Level	Log
1	Jan 01 03:10:59 2000	Warning	port[2] link up[1Gfdx]
2	Jan 01 00:02:02 2000	Warning	port[2] link down
3	Jan 01 00:00:31 2000	Warning	port[2] link up[1Gfdx]
4	Jan 01 00:00:24 2000	Warning	port[8] link up[1Gfdx]
5	Jan 01 00:00:23 2000	Warning	port[4] link up[100fdx]
6	Jan 01 00:00:21 2000	Warning	port[8] link down
7	Jan 01 00:00:21 2000	Warning	port[4] link down
8	Jan 01 00:00:21 2000	Warning	port[2] link down
9	Jan 01 00:00:18 2000	Warning	port[8] link up[1Gfdx]
10	Jan 01 00:00:18 2000	Warning	port[4] link up[100fdx]
11	Jan 01 00:00:18 2000	Warning	port[2] link up[1Gfdx]

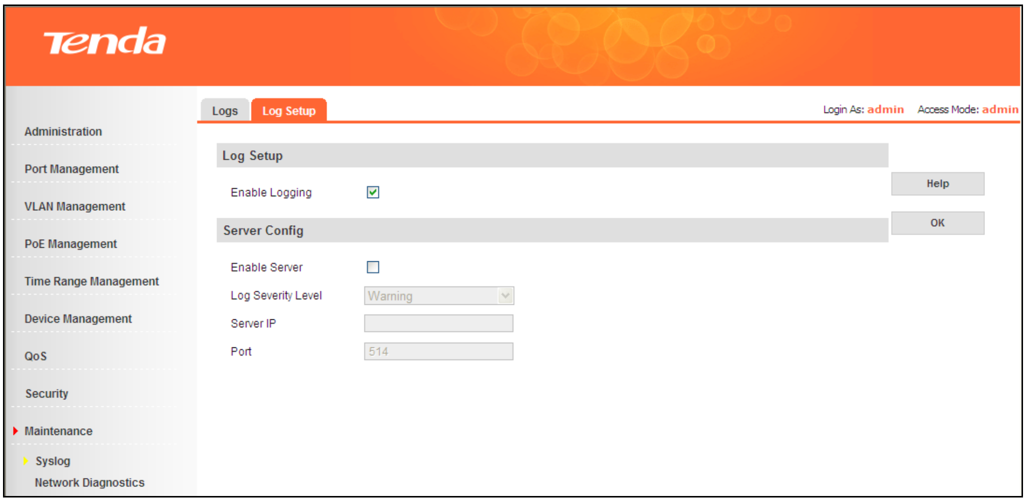
Total: 11 Entries,1 Page(s), Current Page: Page 1 1

For real-time network monitoring and network malfunction diagnosis, it is advisable to click **Administration > System Configuration > System Time** to configure system time for your switch so that the system can obtain correct system time.

1.2 Log Setup

This page allows you to configure remote logging, which can send system logs to the server of a designated IP. It is very convenient for network administrators to centrally monitor and manage log info of this switch.

Click **Maintenance > Syslog > Log Setup** to enter page below:



Log Setup

Enable Logging ☑

Server Config

Enable Server □

Log Severity Level Warning

Server IP

Port 514

Parameters on this page are described below:

Field	Description
Enable Logging	Check it to enable syslog feature. It is enabled by default.
Enable Server	Check it to enable the server for remote logging. It is disabled by default.

Log Severity Level	Configure severity level of logs which are sent to the log server. Only logs with severity level higher than the specified one can be sent to the log server.
Server IP	Enter the server IP address here.
Port	Display the UDP port number which is used for sending/receiving system logs. The default is 514 and cannot be modified.

Tip:

In order to verify that system logs can be sent to the remote log server, click **Administration > System Configuration > System Info** to configure IP address, subnet mask and gateway for this switch.

2 Network Diagnostics

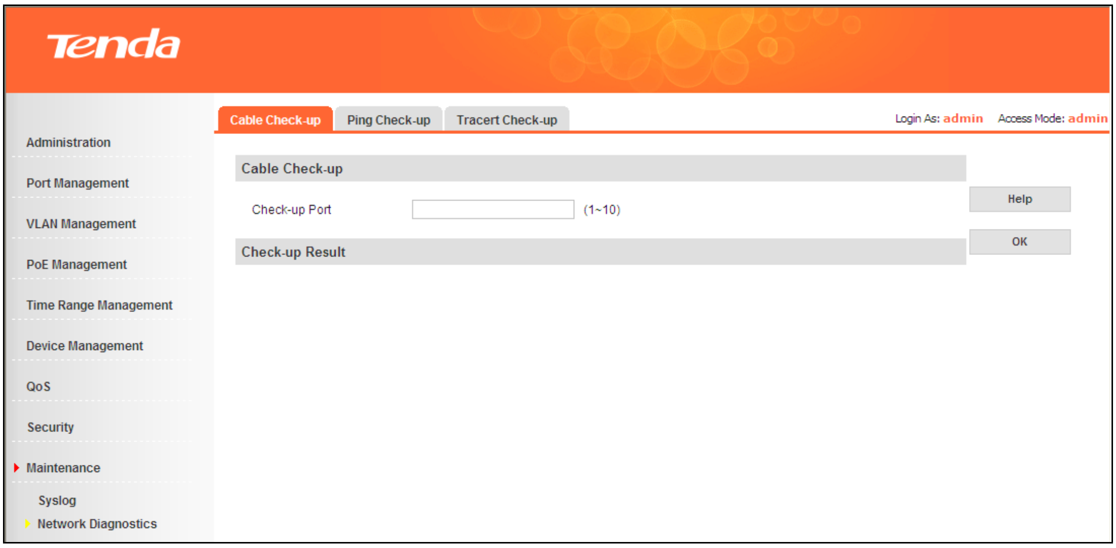
This section, Cable Check-up, Ping Check-up and Tracert Check-up included, is used for troubleshooting network malfunction.

2.1 Cable Check-up

On this device, you can test current cabling situations on all Ethernet interfaces, pair A, B, C, D connection status and pair length included. Click **Maintenance > Network Diagnostics > Cable Check-up** to enter page below:

Tip:

- The pair length is the total length of the twisted cable, not the length of its cable skin. There may be errors in the checking length.
- The test result is for reference only. In some special cases, test errors or failure may occur.

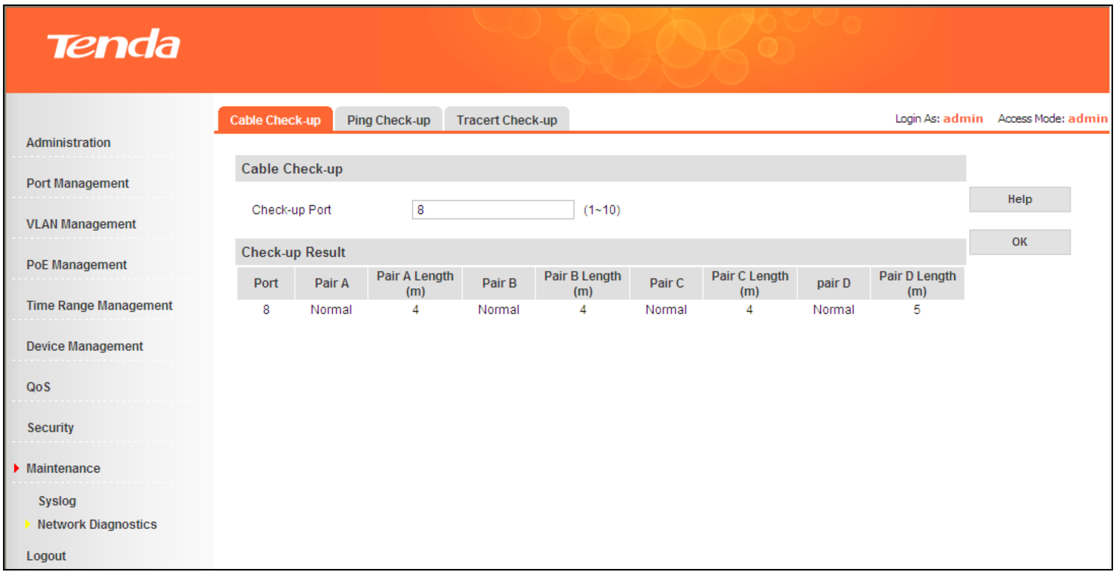


Cable Check-up

Check-up Port (1~10)

Check-up Result

Type in the port number you wish to test in the **Check-up Port** field, click **OK** and then you can view the test result in the **Check-up Result** bar.



Cable Check-up

Check-up Port 8 (1~10)

Check-up Result

Port	Pair A	Pair A Length (m)	Pair B	Pair B Length (m)	Pair C	Pair C Length (m)	pair D	Pair D Length (m)
8	Normal	4	Normal	4	Normal	4	Normal	5

2.2 Ping Check-up

Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.

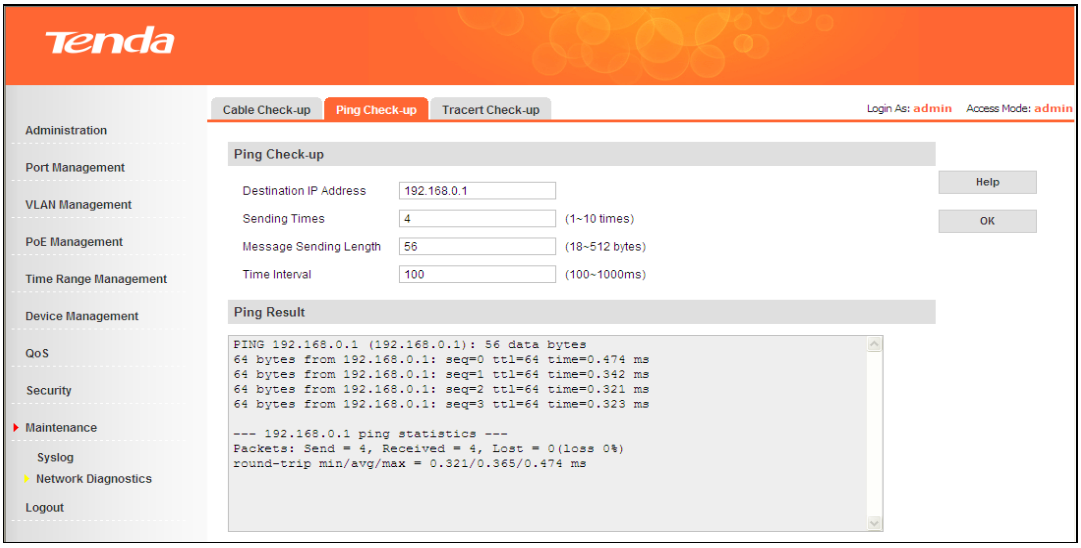
Ping test process and principles:

1. The switch sends Internet Control Message Protocol (ICMP) echo request packets to the target host and is waiting for an ICMP response
2. Then the system will tell you whether network operation is normal or not according to ECHO-REPLY packets it has received.

If network operates normally, the destination device will respond to the switch with ICMP request packets and relevant statistics will be displayed after the destination device receives ICMP request packets. If malfunction occurs, it will display “Unreachable Destination IP” or “Timeout”.

Ping Test:

1. Click **Maintenance > Network Diagnostics > Ping Check-up**;
2. Specify parameters in corresponding fields and click **OK**;



Ping Check-up

Destination IP Address: 192.168.0.1

Sending Times: 4 (1~10 times)

Message Sending Length: 56 (18~512 bytes)

Time Interval: 100 (100~1000ms)

Ping Result

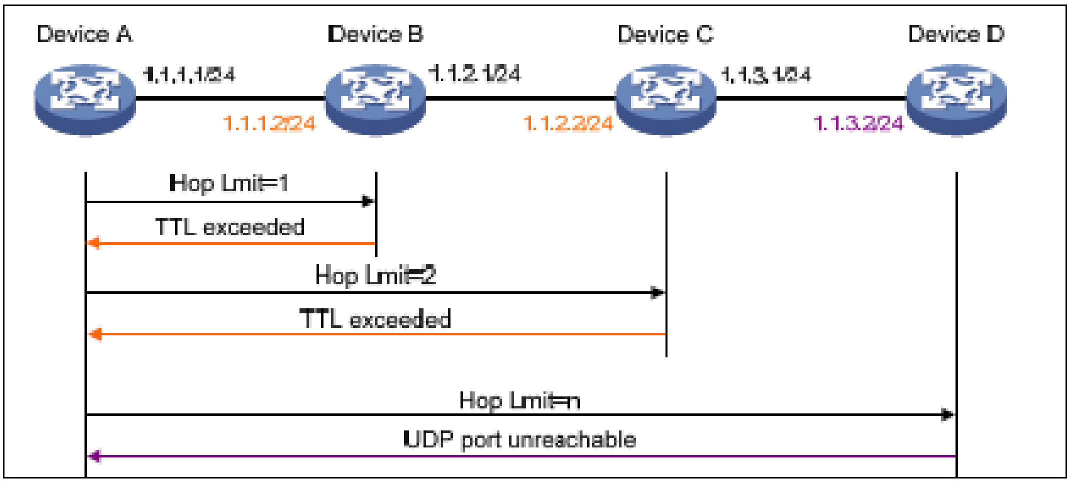
```
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: seq=0 ttl=64 time=0.474 ms
64 bytes from 192.168.0.1: seq=1 ttl=64 time=0.342 ms
64 bytes from 192.168.0.1: seq=2 ttl=64 time=0.321 ms
64 bytes from 192.168.0.1: seq=3 ttl=64 time=0.323 ms

--- 192.168.0.1 ping statistics ---
Packets: Send = 4, Received = 4, Lost = 0(loss 0%)
round-trip min/avg/max = 0.321/0.365/0.474 ms
```

Parameters on this page are described below:

Field	**Description**
Destination IP Address	Specify the destination host IP address.
Sending Times	Configure ICMP request sending packets (1~10). The default is 4.
Message Sending Length	Configure ICMP request packets length (18~512 bytes). By default it is 56 bytes.
Time Interval	Configure ICMP request packets time interval (100~1000ms). The default is 100ms.
Ping Result	Display the ping result.

2.3 Tracert Check-up

Tracert is a computer network diagnostic tool for displaying the route (path) and measuring whether network connection is available or not. When malfunctions occur to the network, you can locate trouble spot of the network with this tracert test. Tracert working diagram is shown below:

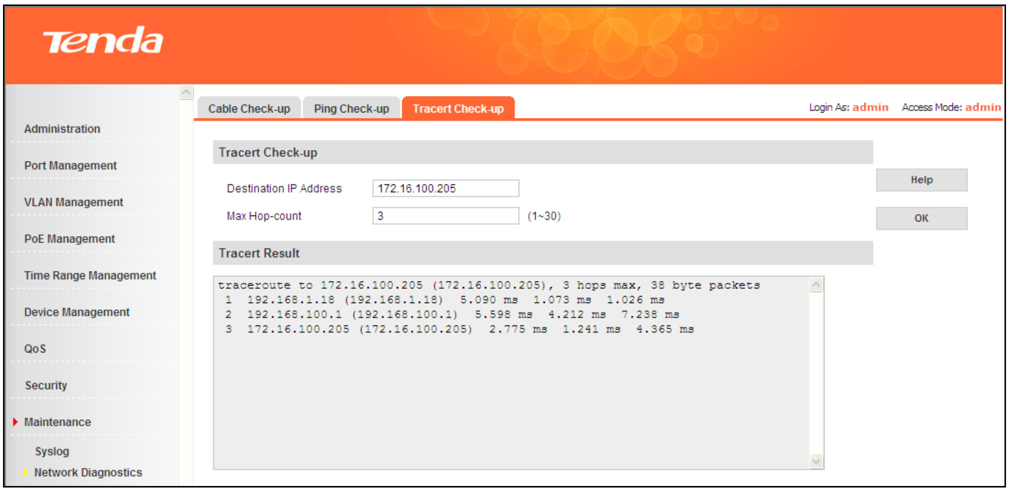


Tracert test process:

1. Device A transmits an IP packet with the TTL value 1 to Device D.
2. Device B (the first router that packets have reached) replies with an ICMP error of TTL timeout (Device B's IP 1.1.1.2 included), thus Device A obtains the first router's IP (1.1.1.2);
3. Device A re-transmits an IP packet to Device D and TTL value is 2;
4. Device C replies with an ICMP error of TTL timeout, thus Device A obtains the second router's IP (1.1.2.2);
5. The process mentioned above is performed repeatedly until packets reach Device D. In this way, Device A can obtain IP addresses of all routers that it has passed.

Tracert Test:

1. Click **Maintenance > Network Diagnostics > Tracert Check-up**;
2. Specify parameters in corresponding fields and click **OK**;



Tracert Check-up

Destination IP Address: 172.16.100.205

Max Hop-count: 3 (1~30)

Tracert Result

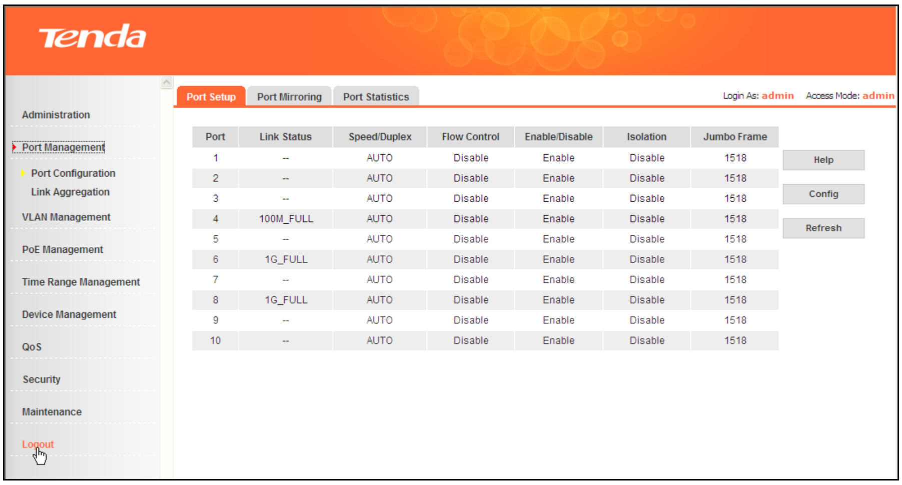
```
traceroute to 172.16.100.205 (172.16.100.205), 3 hops max, 38 byte packets
 1  192.168.1.18 (192.168.1.18)  5.090 ms  1.073 ms  1.026 ms
 2  192.168.100.1 (192.168.100.1)  5.598 ms  4.212 ms  7.238 ms
 3  172.16.100.205 (172.16.100.205)  2.775 ms  1.241 ms  4.365 ms
```

Parameters on this page are described below:

Field	Description
Destination IP Address	Specify the destination host IP address for tracert test.
Max Hop-count	Specify the maximum number of routers the test data can pass through. Valid range is 1-30 and the default is 3.
Tracert Result	Display Tracert result: ➢ When routes among devices are reachable, IP addresses of routers will be displayed. ➢ When routes among devices are unreachable, following info will be displayed: 1 * * * request timed out 2 * * * request timed out 3 * * * request timed out

Logout

If you want to exit the web page safely, click **Logout** in the left navigation bar of the page.



Port	Link Status	Speed/Duplex	Flow Control	Enable/Disable	Isolation	Jumbo Frame
1	--	AUTO	Disable	Enable	Disable	1518
2	--	AUTO	Disable	Enable	Disable	1518
3	--	AUTO	Disable	Enable	Disable	1518
4	100M_FULL	AUTO	Disable	Enable	Disable	1518
5	--	AUTO	Disable	Enable	Disable	1518
6	1G_FULL	AUTO	Disable	Enable	Disable	1518
7	--	AUTO	Disable	Enable	Disable	1518
8	1G_FULL	AUTO	Disable	Enable	Disable	1518
9	--	AUTO	Disable	Enable	Disable	1518
10	--	AUTO	Disable	Enable	Disable	1518

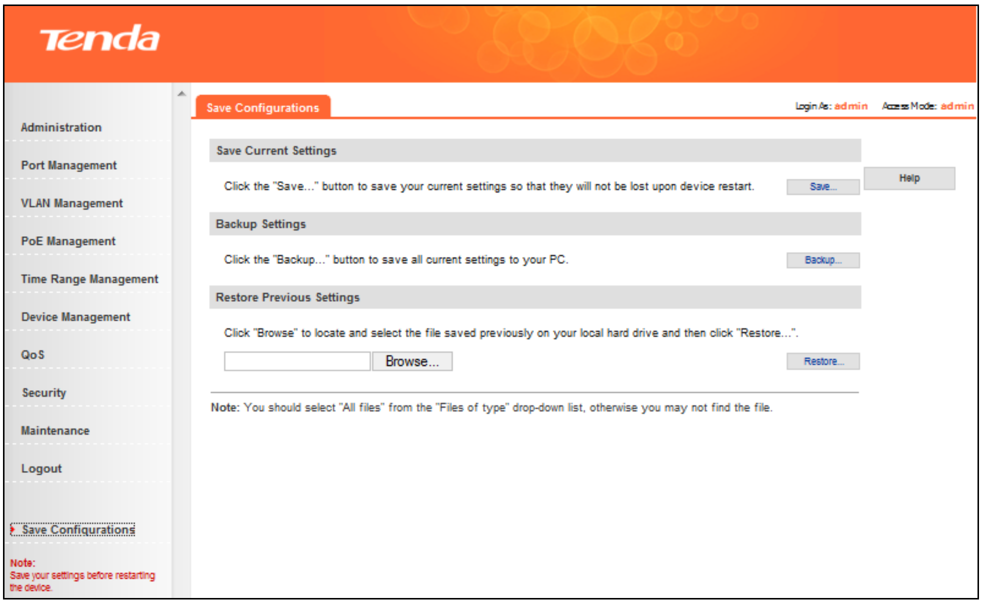
You can also close the web browser directly to log out safely.

Note:

Closing the web browser tab won't log out automatically.

Save Configurations

Click **Save Configurations** to enter page below to manage this switch's configuration info.



Note:
Save your settings before restarting the device.

Save Current Settings

Click the "Save..." button to save your current settings so that they will not be lost upon device restart.

Backup Settings

Click the "Backup..." button to save all current settings to your PC.

Restore Previous Settings

Click "Browse" to locate and select the file saved previously on your local hard drive and then click "Restore...".

Note: You should select "All files" from the "Files of type" drop-down list, otherwise you may not find the file.

➘ Save Current Settings

If you want to save your settings after reboot, click **Save** on this page.

⚠ **Note:**

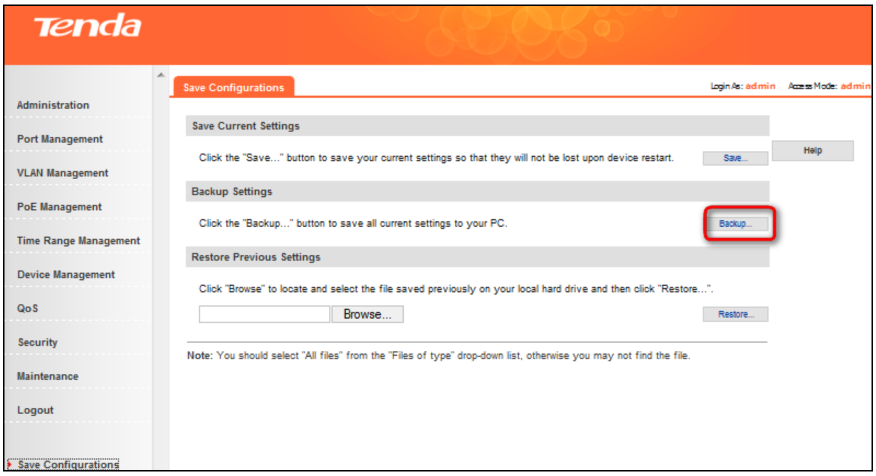
Operations, like power up the switch after disconnect its power supply, reset the switch, upgrade the switch, etc. will reboot this device.

➘ Backup Settings

If you configure settings on this switch, which will make this device work in good status and suitable environment, it is suggested to backup settings for this device, which will be convenient for troubleshooting and saving time for next time's configuration.

Procedures for backup settings

1. Click **Backup**;



Save Current Settings

Click the "Save..." button to save your current settings so that they will not be lost upon device restart.

Backup Settings

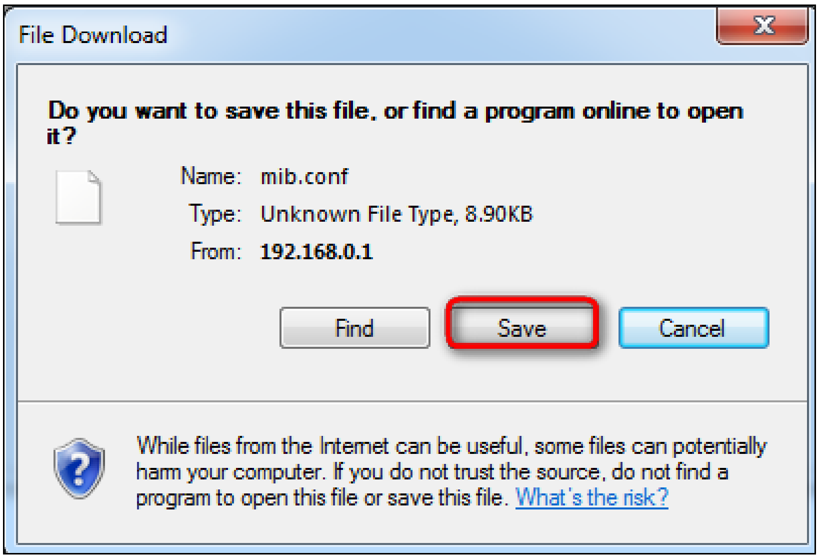
Click the "Backup..." button to save all current settings to your PC.

Restore Previous Settings

Click "Browse" to locate and select the file saved previously on your local hard drive and then click "Restore...".

Note: You should select "All files" from the "Files of type" drop-down list, otherwise you may not find the file.

2. Click **Save** on the pop-out dialog;



Do you want to save this file, or find a program online to open it?

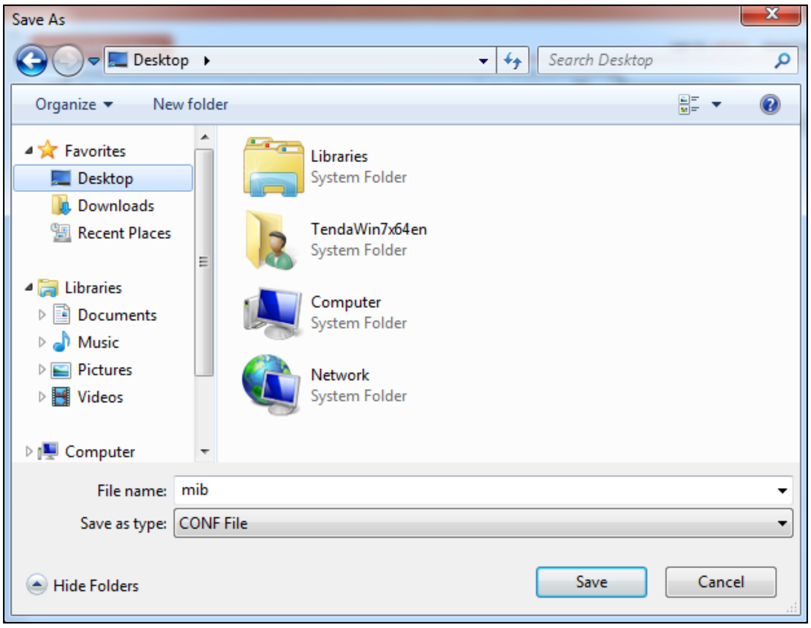
Name: mib.conf

Type: Unknown File Type, 8.90KB

From: 192.168.0.1

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

3. Select a path to save files to your local PC and click **Save**.



File name: mib

Save as type: CONF File

Tip:

By default, the file name is “mib.conf”. To make it remembered easily, you can modify the file name “mib”, but do not modify the file extension “.conf”.

➘ Restore Previous Settings

If you want to configure the same settings for multiple switches, or if you carelessly perform some actions, leading to performance degradation, you can use this function to restore previous settings for this switch.

Procedures for restoring previous settings:

Click **Browse** to load configuration files which you have stored on your hardware disk previously, click **Restore** and then follow onscreen instructions.

Chapter V

Appendix

Technical Specifications

1 Hardware Specifications

Item	Specification
Input Voltage	100-240V AC, 50/60Hz
Power Consumption	17W (no load) | 128W (full load)
PoE	8 10/100/1000Mbps auto-negotiation, PoE-capable RJ45 ports with up to 40W on each; Support dynamic power allocation and can connect up to 8 IEEE 802.3af-compliant PDs (15.4W) or up to 4 IEEE 802.3at-compliant PDs (30W)
Traffic Ports	8 10/100/1000Mbps auto-negotiation RJ45 ports, 2 1000Mbps SFP ports
Operating | Storage Temperature	-10℃ ~ 45℃ | -40℃ ~ 70℃
Operating | Storage Humidity	10% ~ 90% RH (non-condensing) | 5% ~ 90% RH (non-condensing)
Safety	UL 60950-1 CAN/CSAC22.2 No 60950-1 IEC 60950-1 EN 60950-1/A11 AS/NZS 60950-1
EMC	EN 55024;1998+A1:2001+A2:2003 EN 55022:2006 EN 61000-3-2:2000+A1:2001+A2:2005 EN 61000-3-3:1995+A1:2001+A2:2005 AS/NZS CISPR 22:2004 FCC PART 15:2005
MTBF	> 100, 000 hours
Dimension	294mm*178mm*44mm
Weight	< 2kg

2 Software Specifications

Item	Specification
Switching Capacity(full-duplex)	20Gbps
Packet Forwarding Rate (full load)	14.88Mpps
MAC Table	8K
VLAN	• Support port VLAN and up to 10 groups can be configured; • Support IEEE 802.1Q VLAN and up to 64 groups can be configured; • Support Voice VLAN
DHCP	• Support DHCP Snooping • Support DHCP Client
Multicast	• Support IGMP Snooping V1/V2 • Up to 200 multicast groups can be configured; • Support fast leave mode
Broadcast Storm Control	• Support port based broadcast storm control • Support port based multicast storm control • Support port based unknown unicast storm control
STP	• Support IEEE 802.1d STP • Support IEEE 802.1w rapid STP • Support edge port • Support P2P port • Support STP BPDU packets statistics
MAC Filter	• Support unicast MAC filter • Up to 64 entries can be configured.
QoS	• Support 802.1P port trust mode • Support IP DSCP port trust mode

	• Support bandwidth control • Up to 4-queue QoS mapping can be configured.
Certification	Support port based IEEE 802.1X certification
Loading and Upgrading	HTTP
Management	• Support SNMP (Simple Network Management Protocol) • Support Web management • Support Telnet management
Port Management	Port Setup: port speed rate setup and display, flow control setup, isolation setup, Jumbo frame setup (1518-9216) Port Mirroring: implement port ingress mirror image, egress mirror image and ingress & egress mirror image Port Statistics: display packets the port has received and sent Port Trunk: implement static trunk and LACP and up to 2 trunk groups can be configured with 2~8 ports in each group.
PoE	• Support IEEE 802.3at standard • Support IEEE 802.3af standard • Maximum power consumption: 115W
Time Range Management	Support absolute time, periodic time and superposition of time slices and applicable for PoE. Up to 16 time ranges can be configured and as for each time range, at most 4 time slices can be allowed.
Maintenance	Support Ping\Tracert\Cable test

Default Settings

Parameter			Default Settings
Login Info	Login method		HTTP (Web manager) Telnet
	Login IP		192.168.0.1
	Login Username/Password		admin/admin
System Info	Management VLAN		1
	System Name		TEG3210P_EN
	DHCP（Client）		Disable
	IP Address | Subnet Mask		192.168.0.1 | 255.255.255.0
	Gateway		None
	MAC Age		300s
	System Time		Date: 2000-1-1 Time: 0:00:00 Setup Mode: Set Time & Date Manually
	Web Login Timeout		300s
Port Management	Port Configuration	Speed/Duplex	Auto
		Flow Control	Disable
		Status	Enable
		Isolation Status	Disable
		Jumbo Frame	1518
		Port Mirroring	Disable
	Link Aggregation	Aggregation Feature	Disable
		Aggregation Algorithm	Source & Dest MAC
		Aggregation Mode	Static
		System Priority	32768
		LACP Status	Disable
		Timeout	Long
VLAN Management	VLAN Configuration	VLAN Mode	802.1Q VLAN
		VLAN ID	1 Member ports: 1-10

		Trunk Port	None
		Hybrid Port	None
	Voice VLAN	Security Mode	Disable
		Ageing Time	1440min
		Port Mode	Manual
		Port status	Disable
		OUI	See OUI Setup
PoE Management	PoE Status on RJ45 Ports		Enable
	Power Mode		Dynamic
	Time Range ID		Unspecified
Time Range Management			Not configured
Device Management	MAC Address Forwarding Table		Dynamic
	STP	Global Status	Disable
		Version	RSTP
		BPDU Processing	Broadcast
		Priority	32768
		Max Age	20s
		Hello Time	2s
		Forward Delay	15s
		Port Status	Disable
		Port Priority	128
		Default Path Cost	Enable
		Path Cost	200000000
		Edge Port	Enable
		P2P Port	Auto
	IGSP	IGSP Status	Disable
		Routing Port Age	105s
		Group-general Query Max Response Time	10s
		Group-specific Query Max Response Time	2s

		Host Port Age	260s
		Unknown Multicast Drop	Disable
		Multicast VLAN Status	Disable
		Fast Leave	Disable
	SNMP (Agent)	Status	Disable
		Max Packet Size	1500bytes
		Contact Info	www.tendacn.com
		Physical Location	3F, Moso Industrial Building, No. 1031, Liming Road, Xili Town, Nanshan District,ShenZhen, P.R. CHINA
		Version	v1, v2c
		Trap	Enable
		Trap State	Coldstart-Trap Warmstart-Trap Linkup-Trap Authentication-Trap Linkdown-Trap
	DHCP Snooping		Disable
QoS	QoS Configuration	Scheduling Scheme	SP
		802.1P	Enable
		DSCP	Disable
		Port Priority	CoS 0
	Traffic Control	Bandwidth Control	Not limited
		Storm Control	Not limited
Security	MAC Filter		Not filtered
	802.1X	Global Mode	Disable
		Recertification	Disable
		Recertification Time-out Timer	3600
		Client Time-out Timer	30

		Port 802.1X Mode	Disable
		Port Control Mode	Enforce Authorization
System Logs	Log Recording		Enable
	Log Server		Disable

Safety and Emission Statement

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.