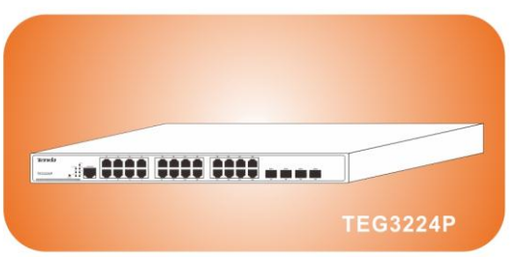
User Guide

Tenda



24-Port Gigabit PoE Managed Switch

Copyright Statement

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 described in this document 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 or circuit layout(s) 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.

Safety Guidelines

Observe the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage.

Basic Requirements

1. Keep the device strictly dry while storing, shipping and using;
2. Keep the device from fierce collision;
3. Follow the instructions provided in this manual to install the device;
4. Please contact the specified maintenance staff rather than remove the device on your own if any fault happens.

Environmental Requirements

1. Temperature - Install the switch in a dry area, with ambient temperature between 0 and 40ºC (32 and 104ºF). Keep the switch away from heat sources such as direct sunlight, warm air exhausts, hot-air vents, and heaters;
2. Operating humidity - The installation location should have a maximum relative humidity of 90%, non-condensing;
3. Ventilation - Do not restrict airflow by covering or obstructing air inlets on the sides of the switch. Keep it at least 10cm free on all sides for cooling. Be sure there is adequate airflow in the room or wiring closet where the switch is installed;
4. Operating conditions - Keep the switch away from nearest source of electromagnetic noise, such as photocopy machines, microwaves, cellphones, etc.

Use Notes

1. Use the provided accessories, such as the cable, mounting kit, etc;
2. Ensure the basic supply voltage standard must be met;
3. Keep the power plug clean and dry in case of electric shock or other dangers;
4. Keep your hands dry while plugging cables;
5. Shut down the device and power it off before plugging cables;
6. Disconnect the power supply and pull out all cables, such as the power cord, fiber, Ethernet cable, etc. in lightening days;
7. Disconnect the power supply and pull out the plug if the device is out of use for a long time;
8. Keep the device far from water or other liquids;
9. Contact the specified maintenance staff if any problem occurs;
10. Do not tread on, drag or excessively bend its cable;
11. Do not use worn or aged cables;
12. Do not look the fiber interface in your eyes in case of eye damage;
14. Prevent some matters, such as metals, from entering the device through the ventilation hole;
15. Do not scrape or fray the device’s housing shell in case of abnormal operation or human body allergic;
16. Keep the device out of children’s reaches.

Cleaning Notes

1. Shut down the device and pull out all cables before cleaning it;
2. Use soft cloth to clean the device’s housing shell.

Environmental Protection

1. Throw the discarded device or batteries into the specified recycling places;
2. Observe local relevant packages, wasted batteries and discarded device processing acts and support recycling action.

Contents

Chapter 1 Product Overview

1.1 Overview

Thank you for purchasing this product. This 24-port Smart Gigabit PoE Switch provides 24 10/100/1000Mbps auto-sensing RJ45 ports, 4 1000Mbps Combo (copper/fiber) ports and one Console port. All its RJ45 ports are PoE-capable and it can connect up to 24 IEEE 802.3af-compliant PDs (15.4W) or up to 12 IEEE 802.3at-compliant PDs (30W). In addition, it supports VLAN, QoS, DHCP, IGMP snooping, ACL, STP, RSTP, MSTP, port mirroring, link aggregation and other features. Aiming at solving the safety problems in LAN, it provides user management classification, management VLAN, ARP attack defense, worm attack defense, DoS attack defense, MAC attack defense, IP+MAC+PORT+VLAN Bind, MAC filter and other safety settings through visual WEB interface operations. With high performance and low cost, it is ideal for hotels and enterprises.

1.2 Physical Description

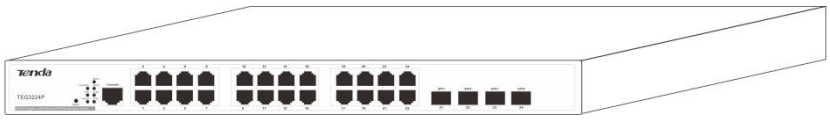


Figure 1-1 Outside View

1.2.1 Front Panel

The front panel contains the following:

- 24 10/100/1000Mbps RJ45 ports
- Four SFP ports
- One Console port
- Reset button
- Port LEDs
- System LEDs
- PoE-MAX LED

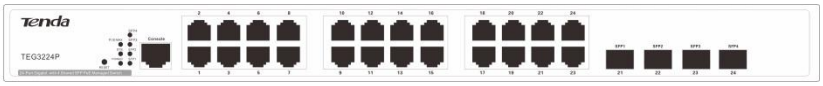


Figure 1-2 Front Panel

1.2.2 Back Panel

Figure 1-3 Back Panel

- A grounding stud for lightning protection;
- A 176-264VAC 50/60 Hz 6A power receptacle for accommodating the supplied power cord;
- A power switch for turning on/off power supply;

1.3 Specifications

1.3.1 Hardware Specifications

Item	Specification
Input Voltage	100 - 240VAC 50/60Hz 6A
Power Consumption	About 15W(no load); About 390W(full load);
PoE	24 10/100/1000Mbps auto-sensing, PoE-capable RJ45 ports with up to 30W on each; It supports static or dynamic power allocation and can connect up to 24 IEEE 802.3af-compliant PDs (15.4W) or up to 12 IEEE 802.3at-compliant PDs (30W);
Interface	24 RJ45 10/100/1000 auto-sensing Giga switching ports; 4 1000Mbps SFP ports;
Management Interface	One Console port
Operating Temperature	0℃ - 40℃
Storage Temperature	-40℃ - 70℃
Operating Humidity	10% - 90% RH, non-condensing
Storage Humidity	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 EN 60825-1 EN 60825-2
EMC	EN 55024;1998+A1:2001+A2:2003 EN 55022:2006 ICES-003:2004 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 ETSI EN 300 386 V1.3.3:2005
MTBF	> 100,000h
Dimension	440mm * 284mm * 44mm
Weight	< 7.5kg

1.3.2 Software Specifications

Features	Specification
Switch Volume (Full-duplex)	56Gbps
Packet Forwarding Rate(full load)	35.7Mpps

MAC Address Table	8K
VLAN	1. VLAN distribution based on ports. Up to 24 can be configured; 2. IEEE 802.1Q VLAN. Up to 128 can be configured; 3. Protocol VLAN. Up to 16 can be configured; 4. MAC VLAN. Up to 64 can be configured; 5. Voice VLAN;
DHCP	DHCP Snooping, DHCP Relay, and DHCP Client
Multicast	1. IGMP Snooping V1/V2; 2. Up to 128 can be configured; 3. Fast leave;
Broadcast Storm Constrain	1. Broadcast storm constrain based on ports; 2. Multicast storm constrain based on ports; 3. Unknown unicast storm constrain based on ports;
STP	1. IEEE 802.1d STP; 2. IEEE 802.1w FSTP; 3. IEEE 802.1s MSTP protocol. In MSTP mode, up to 16 STP instances can be configured; 4. Edge port; 5. P2P port; 6. STP BPDU packets statistics;
ACL	1. MAC ACL. Up to 100 entries can be configured; 2. IPv4 ACL. Up to 100 entries can be configured; 3. Time range limit;
Safety	1. ARP attack defense, worm attack defense, DoS attack defense and MAC attack defense; 2.User grading management and SSL certification; 3. Management VLAN; 4. IP+MAC+PORT+VLAN Bind. Up to 200 entries can be configured; 5. Interface isolation;
MAC Filter	1. Unicast MAC filter; 2. Up to 1000 entries can be configured;
QoS	1. 802.1P port trust mode; 2. IP DSCP port trust mode; 3. Bandwidth control; 4. Up to 4-queue QoS mapping;
Certification	1. IEEE 802.1X based on ports; 2. IEEE 802.1X based on MAC; 3. Up to 256 MAC can be certificated;
Upgrade	TFTP (Trivial File Transfer Protocol)
Management	1. Telnet configuration; 2. Console interface configuration; 3. SNMP (Simple Network Management Protocol); 4. WEB;

PoE	1. IEEE 802.3at and IEEE 802.3af; 2. Maximum power consumption: 385W;
Maintenance	Ping\Tracert\Cable check-up;

1.3.3 Package Contents

Please verify that the package contains the following items:

- Smart PoE Switch
- Power cord
- Install guide
- Console cable
- L-shaped Mounting Kit (2 brackets, screws)
- Four footpads

1.4 Device Hardware Interfaces

1.4.1 LEDs

The following table explains LED designations.

LED	Number	Color	Status	Description
POWER	1	Green	Off	Improper connection to power supply.
			Solid	Proper connection to power supply.
SYS	1	Green	Off	System is functioning improperly.
			Solid	System is functioning improperly.
			Blinking	System is functioning properly.
PoE-MAX	1	Green	Off	Power available for additional PDs.
			Solid	Reaching max power budget (354.2W) and no more power available for another new PD.
Link/Act 1-24	24	Orange	Off	An invalid link is established.
			Solid	A valid link is established.
			Blinking	Transmitting packets.
PoE 1-24	24	Green	Off	The PoE powered device (PD) is connected and the port is supplying power successfully.
			Solid	No PoE-powered device (PD) connected.
SFP1 - SFP4	4	Green	Solid	Packet transmission or a valid link is established on the port.
			Off	An invalid link is established on the port.

1.4.2 Interfaces

1.4.2.1 Console Port

This switch, with an RS232 asynchronous console port, can be used for connecting PCs to test, configure,

maintain and manage the system. The console cable is an 8-conductor cable. One end of the console cable, RJ45 plug, is connected to the Console port on the switch; while the other end, DB9 plug, is connected to 9-conductor console outlet.

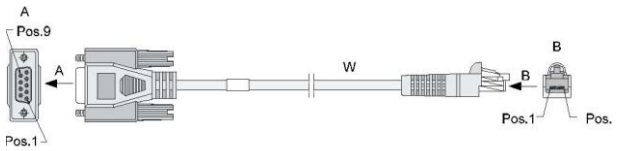


Figure 1-4 Console Port Connection

1.4.2.2 Ethernet Interface

(1) Ethernet interface overview

This device has 24 RJ45 10/100/1000M auto-negotiation Gigabit Ethernet switching ports and 4 1000M SFP fiber ports.

Speed rate and working mode in RJ45 port mode:

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

Note----------

SFP fiber ports can only work in full-duplex auto-negotiation mode.

---

(2) RJ45 Connector

The RJ45 physical connector, adopting CAT5 twisted-pair cable, is used for connecting 10/100/1000Mbps auto-negotiation RJ45 ports as shown below:

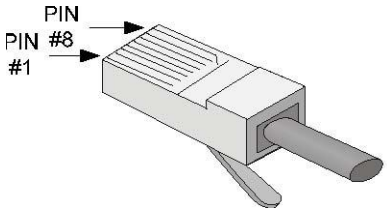


Figure 1-5 RJ45 Connector

(3) SFP Connector

SFP connector, mainly for detachable connection between optical channels, is very convenient for the test and maintenance of the optical system. This device, with its 1000Mbps Combo (copper/fiber) ports, supports gigabit SFP connector.

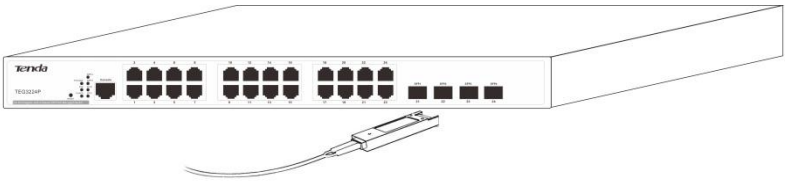


Figure 1-6 SFP Connector

1.4.2.3 RESET Button

To restore factory defaults, press and hold the button for more than 5 seconds when the switch functions correctly. When pressing it for a while, SYS LED will be off and POWER LED is solid. The device will restart and all LEDs will be on. When the rebooting finished, SYS LED will be blinking, indicating restoring to default factory settings.

1.4.3 Fan

This device has three fans for heat dissipation, one for mainboard and two for power supply to ensure stable power supply.

1.5 Interface Serial Number

- 1-24: 24 10/100/1000Mbps auto-negotiation RJ45 ports
- 21-24/SFP1-SFP4: 1000Mbps combo (copper/fiber)ports
- Console: RS232 asynchronous serial port

Chapter 2 Installation

The smart switch can be installed on a flat surface or in a standard 19-inch rack.

2.1 Installing the Switch in a Rack

To install the switch in a rack, observe the following procedures. To perform this procedure, you need the 19-inch rack-mount kit supplied with switch.

1. Keep the kit well-earthed and stable;
2. Insert the screws provided into the bracket mounting holes to fix brackets onto the switch as shown below.

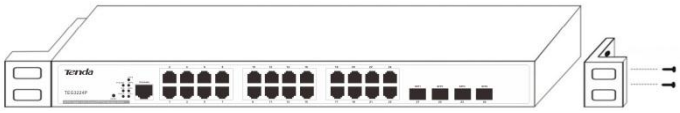


Figure 2-1 Attach L-shaped brackets to the switch

3. Tighten the screws with the Phillips screwdriver to secure the switch in the rack.

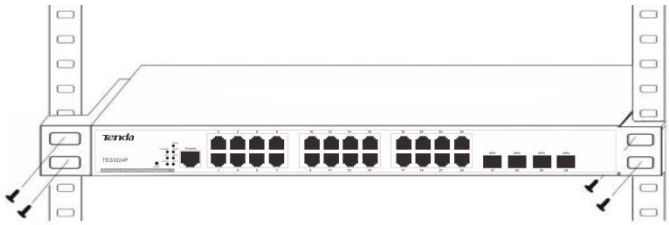


Figure 2-2 Install the switch in the rack

2.2 Installing the Switch on a Flat Workbench

If a standard 19-inch rack is not available, place the switch on a clean, flat workbench. Attach the 4 footpads to corresponding position of the switch bottom to avoid potential sliding and vibration, and ensure good ventilation and proper clearance around the switch for heat dissipation. See figure below:

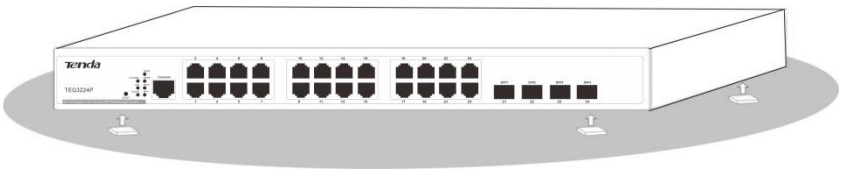


Figure 2-3 Paste footpads to the bottom of the switch

Note----------

1. Please keep the switch in a dry and well ventilated environment.
2. Keep the workbench stable and well-earthed.
3. Do not restrict airflow by covering or obstructing air inlets of the switch. Keep more than 10 centimeters free on all sides for cooling. Be sure there is adequate airflow in the room or wiring closet where the switch is installed.
4. Don’t put heavy articles on the Switch.
5. Make sure there is more than 1.5 centimeters vertical distance free between devices that stack each other.

2.3 Connecting to Protective Grounding Line

Proper connection of protective grounding line is important for lightning protection and anti-interference. Proper connection is as follows:

2.3.1 With Grounding Bar

Connect the yellow-green color protective grounding cable to binding post on the grounding bar and fix the screws.

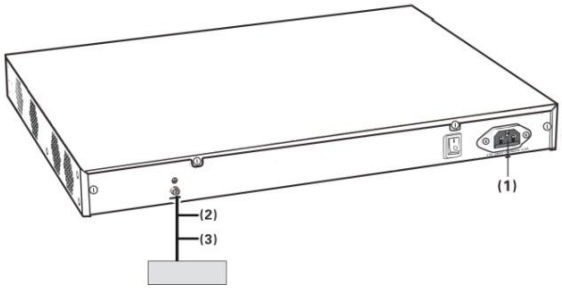


Figure 2-4 Installation with grounding bar

(1) AC power input
(2) Grounding terminal connection
(3) Grounding cable protection

Note----------

Firefighting hoses and building lightning rods are not proper options for grounding bar. The grounding cable on the switch should be connected to the grounding bar in the IT room.

2.3.2 Without Grounding Bar

A. With mud land nearby and allowed to bury grounding bar.

Bury an angle iron or steel pipe (≥0.5m) into the mud land. The yellow-green color protective grounding cable should be welded to the angle iron or steel pipe and the welding point should be embalmed.

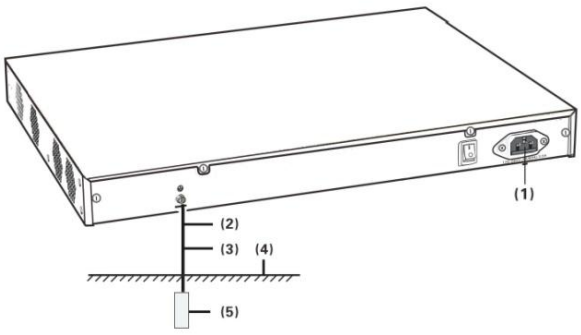


Figure 2-5 Installation with buried grounding bar

(1) AC power input
(2) Grounding terminal connection
(3) Grounding cable protection
(4) Earth
(5) Grounding bar

B. Not allowed to bury grounding bar.

If the device supports AC power supply, you can connect it to the grounding bar through the PE line of the AC power and ensure the PE line in the switchgear room or beside the AC power supply transformer is well-grounded.

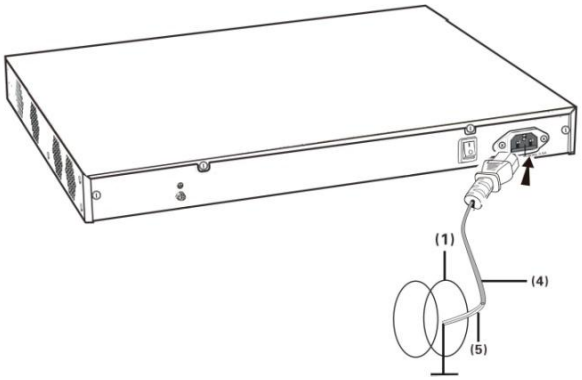


Figure 2-6 Connect to ground through the PE cable of the AC power socket

2.4 Connecting the power cord

Step1: Connecting one end of the included power cord to the switch and the other end to a nearby AC power outlet.

Step2: Verify the power LED on switch's front panel. An illuminated light indicates a proper power connection.

Note----------

As for the power cord, different countries have different standards. Please determine whether to install the card slot to fix the power cord according to the actual situation.

2.5 Connecting to Interface Cable

2.5.1 Connecting to Console Port

Follow below steps to connect the PC or terminal to the switch (The terminal can be the emulation program with RS232 console or a PC. Here take the PC for example):

1. Connect the DB9 plug on the console cable to the PC;
2. Connect the RJ45 connector to the console port on the switch.

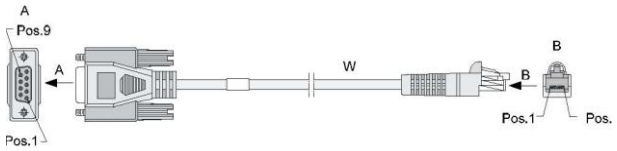


Figure 2-7 Console port connection

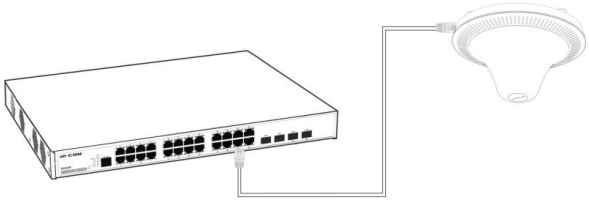
2.5.2 Connecting to RJ45 ports

The switch provides auto MDI/MDIX feature on each RJ45 port. PCs or other terminals can simply connect to any such ports of the switch via CAT.5, CAT.5e, UTP or STP cables.

1. Connect one end of the Ethernet cable to the Ethernet interface on the switch and the other end to

the remote device;

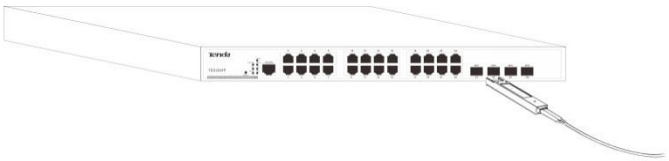
2. Check PoE LED status. For LED status, please refer to 1.4.1 LEDs.



2.5.3 Connecting to SFP fiber combo ports

The small form-factor pluggable (SFP) module is a compact, hot-pluggable transceiver used for optical signal transmission. The module bay is a combo port, sharing a connection with an RJ45 port. Being a combo port, only one type of connection can be active at any given time. For example, both copper and fiber port cannot be used at the same time. If both connectors are plugged in at the same time, the fiber port becomes active.

The SFP module accommodates a standard SFP module with an LC connector.



2.5.4 Connecting to PDs

Connect PDs (PoE powered devices, for example, 802.3at-/802.3af-compliant AP, IP telephone or IP camera) to switch. By default, the power supply mode is dynamic, PoE power supply is enabled and the power supply standard is 802.3at.

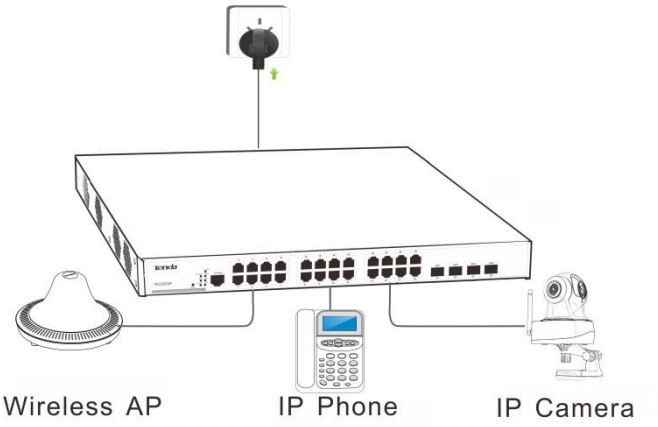


Figure 2-8 PD devices connection

2.6 Checking the Installation

Before applying power perform the following:

• Inspect the equipment thoroughly.

• Verify that all cables are installed correctly.

• Check cable routing to make sure cables are not damaged or creating a safety hazard.

• Ensure all equipment is mounted properly and securely.

Chapter 3 Login

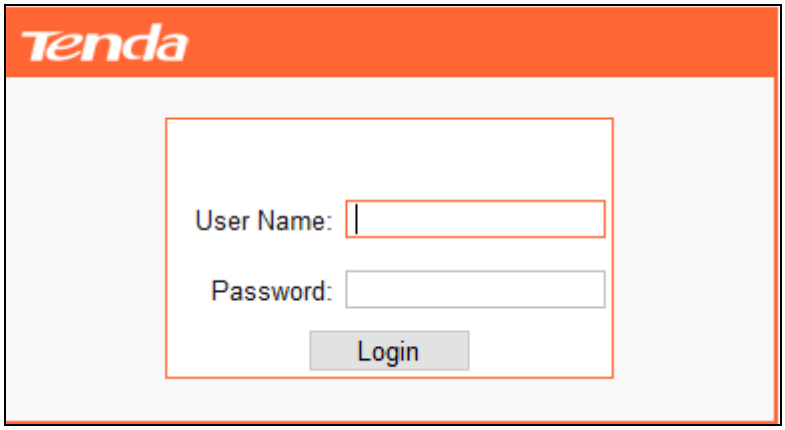
3.1 Web Login

3.1.1 Preparation

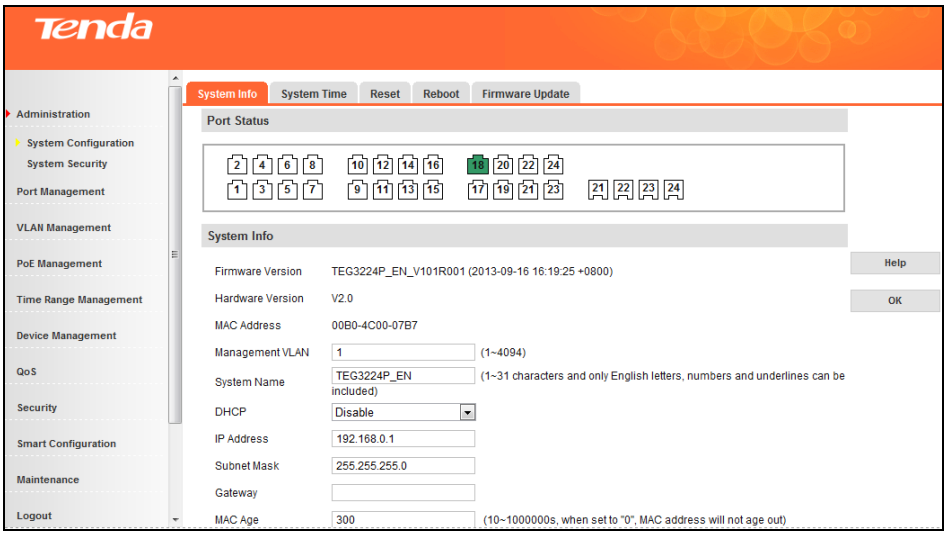
Item	Caption
PC	Network Interface Card installed
IP and Subnet Mask	PC's IP and the switch's IP should be in the same network segment (It can't be 192.168.0.1).
WEB Browser	Microsoft IE 8.0 or higher
Ethernet Cable	One CAT.5 RJ45 cable

3.1.2 Configuration Preparation

1) Launch the browser, such as IE8, enter http://192.168.0.1 and then press **Enter**. The login page of the switch would appear as shown below.



1) Enter the user name and password (the default values are admin), and then click **Login** to log in to the switch's configuration interface.



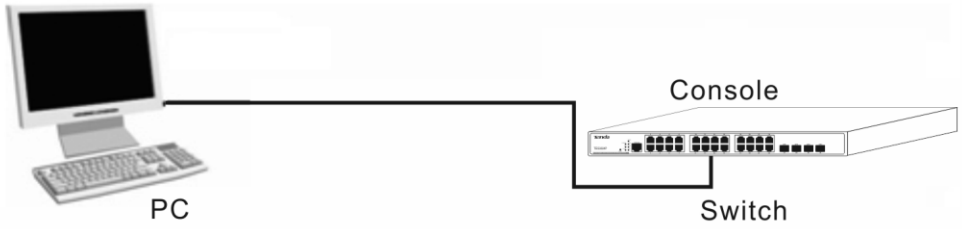
3.2 Login through Console Port

3.2.1 Preparation

Item	Caption
PC	With the Console port
Ethernet Cable	DB9-RJ45 Console Cable

3.2.2 Configuration Preparation

Step 1: Connect the console port from your PC (or other terminals) to the console port on the switch.



Step 2: Run terminal program (for example, terminal in Windows 3.X, Hyper Terminal in Windows 9X/Windows 2000/Windows XP, an example of Windows XP is described below) on PC and select the console port that is connected to the switch and configure as below (Note: For win7 and win8 OS, you need to download the Hyper Terminal programme first):

Bits per second: 115200; Data bits: 8; Parity: None; Stop bits: 1; Flow control: None.

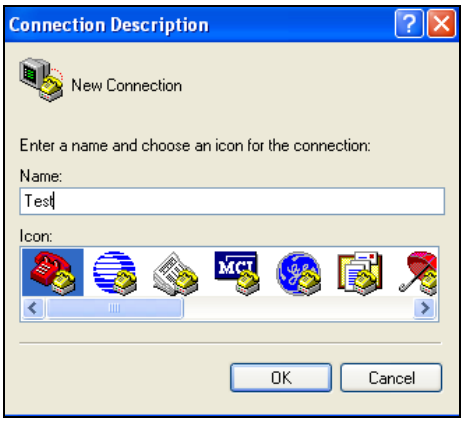


Figure 3-1: New Connection

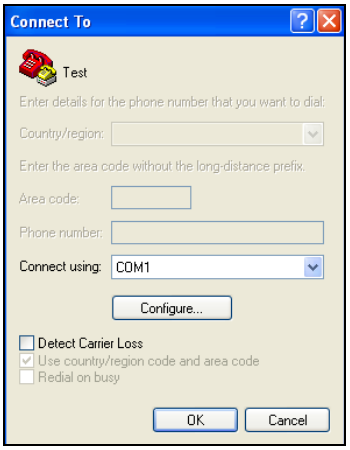


Figure 3-2: Connect To

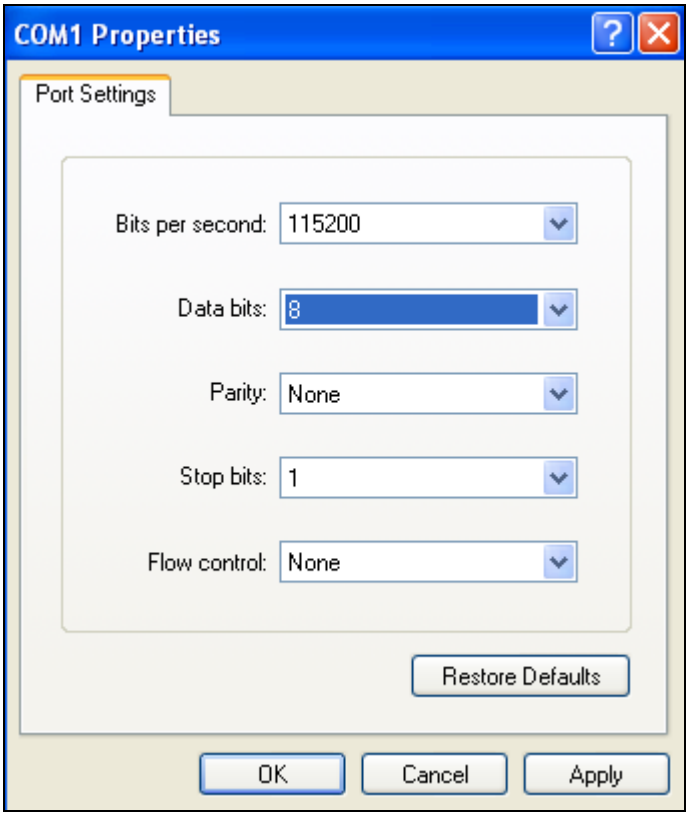
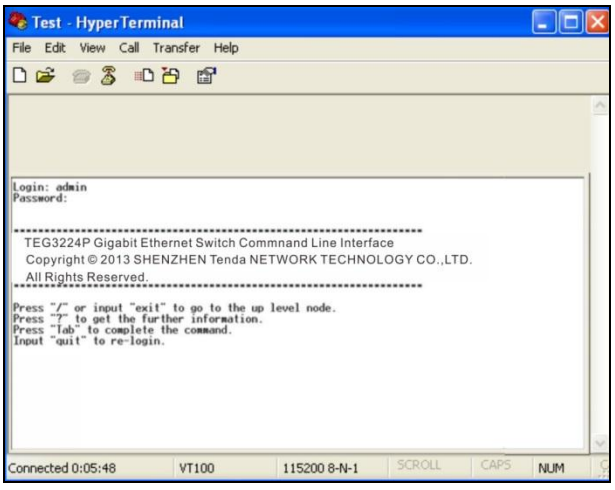


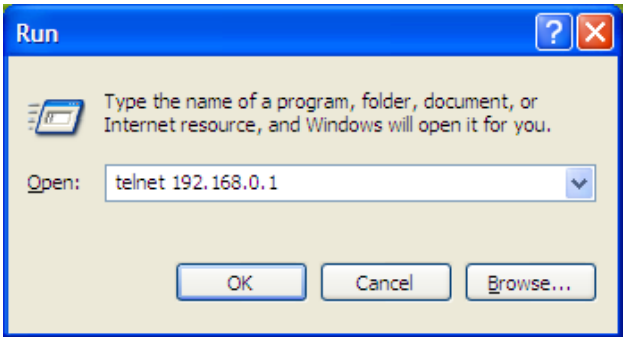
Figure 3-3: Port Settings

Step 3: Power the switch, press **Enter**, input user name and password (admin/admin by default) and then press **Enter** again. Below screen will appear.

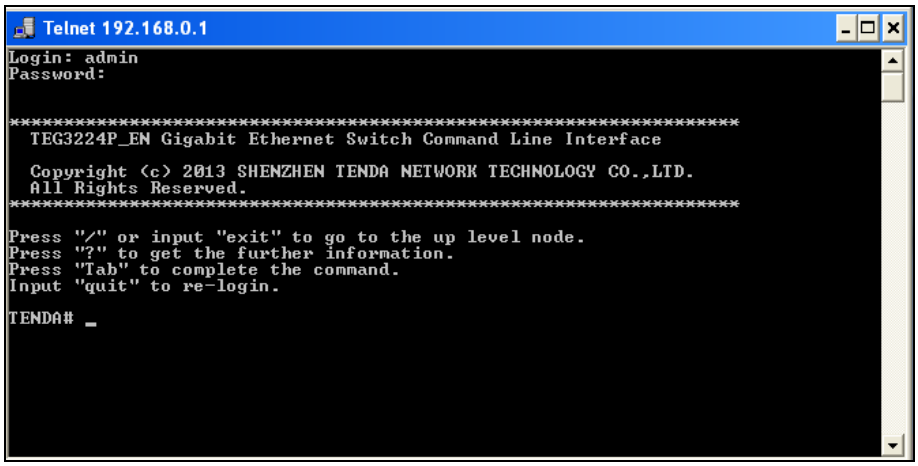


3.3 Telnet Login

Take Windows XP as an example, click **Start -> Run** and enter “telnet 192.168.0.1” as seen below:



Then press **OK**, input the username and password “admin/admin” and the following window will appear:



Chapter 4 Web Configuration

This chapter instructs how to configure switch's functionalities and features on the Web manager.
It includes below sections:

Menu	Submenu	Description
System Configuration	System Info	This section displays the device’s system parameters.
	System Time	This section allows you to configure system time either by synchronizing with SNTP server or specifying it manually.
	Reset	Resets all settings to factory defaults.
	Reboot	Reboots the device. Configurations will be lost if you don’t save them before rebooting.

	Firmware Update	Updates firmware.
	SSL Setup	Allows you to encrypt information.
	User	This section allows you to add new users and change old password.
Port Management	Port Setup	Displays and allows users to config port rate, flow control and jumbo size.
	Port Mirroring	Displays and allows users to config port mirroring settings.
	Port Statistics	Displays the number of packets transmitted and received on corresponding ports.
	Link Aggregation	Displays and allows users to config static and LACP link aggregation settings.
VLAN Management	VLAN	Allows users to config port VLAN and 802.1Q VLAN settings.
	MAC VLAN	Allows users to configure MAC VLAN. Up to 64 MAC VLANs can be configured.
	Protocol VLAN	Three forms: Ethernet, LLC, SNAP. Up to 16 protocol VLANs can be configured.

	Voice VLAN	Allows users to configure voice VLAN (manual or auto).
PoE Management	Global Setup	Static and dynamic allocations are supported. The default is dynamic allocation.
	Port Setup	Two power supply standards: 802.3at and 802.3af. By default, it is 802.3at.
Time Range Management	Time Range	Allows users to configure absolute time, periodic time, time slices, etc.
Device Management	MAC	Displays MAC table and allows users to manually add static MAC addresses and fast binding.
	STP	Allows users to configure STP, RSTP and MSTP settings. Up to 16 instances can be configured.
	LLDP	Allows users to configure LLDPBU settings and displays neighbor info.
	IGSP	Allows users to configure V1/V2 IGSP settings.
	SNMP	Allows users to configure V1/V2c/V3 SNMP settings.

	DHCP Relay	Allows users to implement DHCP among multiple VLANs.
	DHCP Snooping	Allows users to configure DHCP snooping settings, DHCP server trust settings and client access settings.
QoS	CoS	CoS priority 0-7 is supported. Default 0 and 3 correspond to queue 1; 1 and 2 correspond to 2; 4 and 5 correspond to queue 3; 6 and 7 correspond to queue 4.
	DSCP	DSCP priority 0-63 is supported.
	Scheduling Scheme	SP and WRR are supported. By default, it is SP.
	Port Priority	Port priority 0-7. The default is 0.
	Rate Limit	Allows users to configure ingress and egress rate limit.
	Storm Constrain	Allows users to configure broadcast, multicast, and unknown unicast constrain settings.
	ACL	Allows users to configure MAC/IP ACL settings. Up to 100 entries can be configured.
Security	ARP Attack Defense	Allows users to configure ARP attack defense settings.
	Worm Attack Defense	Allows users to configure TCP and UDP settings to filter packets.

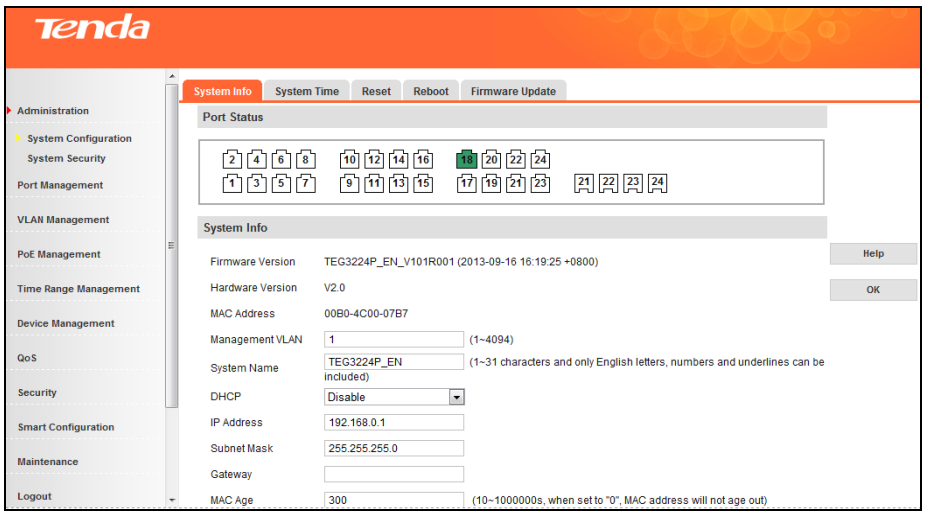
	DoS Attack Defense	Allows users to configure DoS attack defense settings.
	MAC Attack Defense	Allows users to configure MAC attack defense settings.
	IP Filter	Configure IP+MAC+Port+VLAN Binding, ARP filter and IP filter settings.
	802.1X	Displays and allows you to configure 802.1X settings.
Smart Configuration		Corporate and hotel network administrators can use this section to easily configure file server port and router port. For details, please refer to 4.9.
Maintenance		Allows users to configure syslog settings and network diagnose settings.
Save Configurations		Save/backup/restore settings.

4.1 Administration

4.1.1 System Configuration

System Info

Click **System Configuration -> System Info** to enter interface below:



Fields on the screen are described below:

Field	Description
Firmware Version	Displays switch's current firmware version and release date.
Hardware Version	Displays switch's current hardware version.
MAC Address	Displays switch's physical address.
Management VLAN	Displays switch's management VLAN ID. VLAN1 is preset to management VLAN by default.
System Name	Customize a system name for locating the device quickly.
DHCP	Enable/disable the DHCP feature. When enabled, the switch can obtain an IP address automatically (provided that there is an active DHCP server on the network and switch is successfully connected to the network); when disabled, you must config an IP address manually.
IP Address	Config a static IP address, which will be used to access the switch's web manager. The default is 192.168.0.1.
Subnet Mask	Config the corresponding subnet mask of the IP address specified above. The default is 255.255.255.0.
Gateway	Specify a gateway address for the switch.
MAC Age	This field specifies the length of time a learned dynamic MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). The MAC Address Aging Time can be set to any value between 10 and 1000000 seconds. The default setting is 300 seconds.

Note----------

To view the IP address obtained from a DHCP server on the network, access the DHCP server or type the "show ip" command on telnet interface.

System Time

1. Overview

The switch allows you to synchronize system time with SNTP server or config time and date settings manually.

➢ **Sync with SNTP Server**

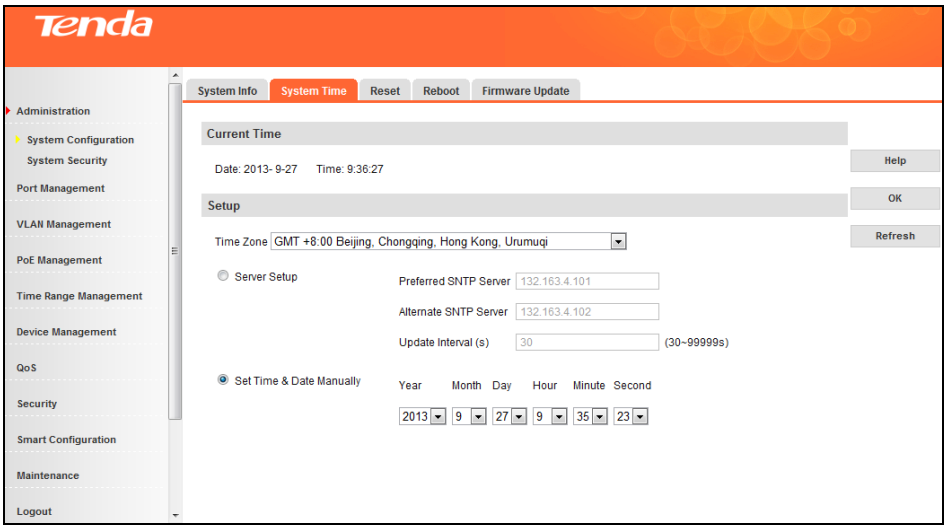
The Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. Simple Network Time Protocol (SNTP) is another less complex implementation of NTP. It synchronizes time between time servers and clients so that clock-dependent devices on the network can consistently provide diverse time based applications. Both SNTP server and client run over the User Datagram Protocol (UDP) on port number 123. When BLAT UDP attack defense is enabled, it won't be unable to acquire system time automatically.

➢ **Config time and date settings manually**

Manually configured time will not be updated or synchronized with other devices and will be restored to factory defaults after system reboot.

2. System Time -- Config

Click **System Configuration -> System Time** to enter interface below:



➢ **Steps to sync with SNTP server**

1. Select a proper time zone from the **Time Zone** pull down list;
2. Click **Server Setup** and enter SNTP server IP address;
3. Specify an Update Interval value between 30 and 99999 seconds. The default is 30 seconds;
4. Click **OK**.

Now the switch will update system time from SNTP.

➢ **Steps to config time and date settings manually**

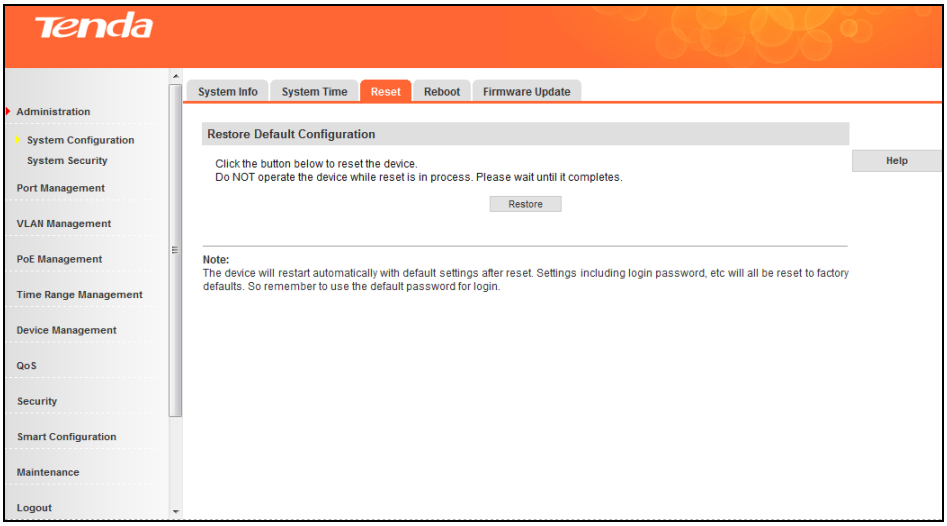
1. Select a proper time zone from the **Time Zone** pull down list;
2. Click **Set Time&Date Manually** to configure the time and date.
3. Click **OK**.

Now the switch will work with the configured time.

Reset

Click **System Configuration -> Reset** to enter below interface.

Clicking the **Restore** button restores Switch's configurations to the factory default settings.

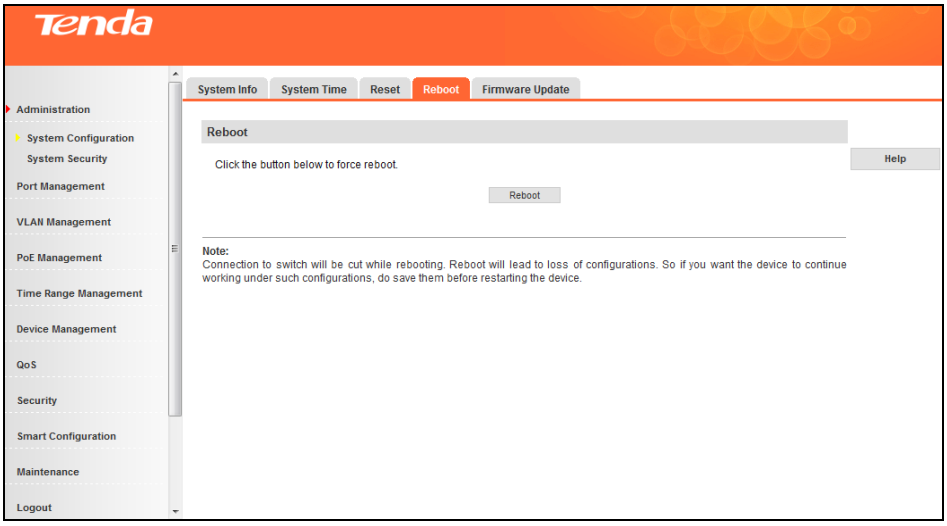


Note----------

1. Current settings will be lost after reset. So if you want to retain current settings, please click **Save Configurations**.
2. Do not operate the device while reset is in process. Otherwise it may be damaged.

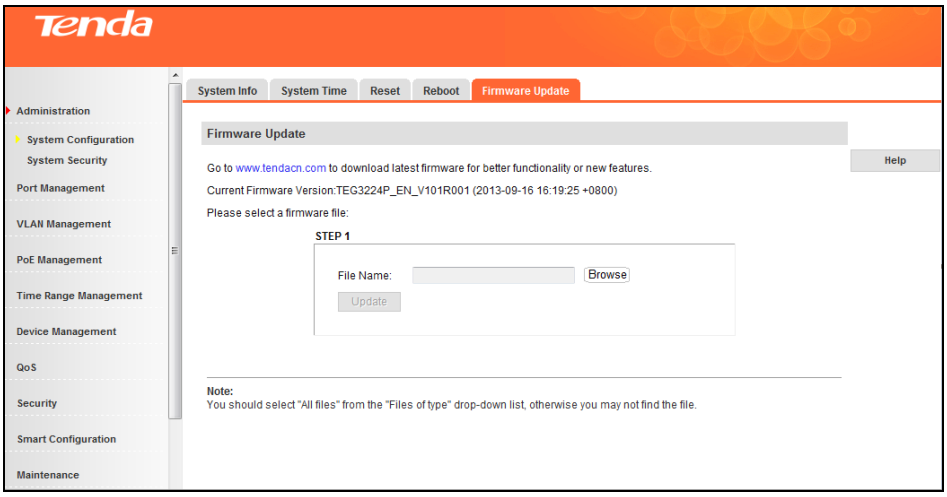
Reboot

Click **System Configuration -> Reboot** to enter the below screen and click the **Reboot** button here to restart the switch.



Firmware Update

Click **System Configuration -> Firmware Update** to enter interface below.



This section displays current firmware version. To update the switch's firmware, click **Browse** to locate and select the latest firmware and click **Update**. The process takes 1-2 minutes to finish.

Note----------

1. Do not disconnect power connection while upgrade is in process.
2. If power supply is disconnected, please upgrade it again; if unable to enter the management interface, contact maintenance personnel.

4.1.2 System Security

SSL Setup

Secure Sockets Layer (SSL) is a cryptographic protocol that is designed to provide communication security over the Internet. It is widely applied in E-commerce and Internet banking areas.

SSL Security

Privacy: Adopting asymmetrical encryption technology and RSA (Rivest Shamir and Adleman), SSL uses key pair to encrypt information.

Authentication: Authenticate the users and the servers based on the certificates to ensure the data are transmitted to the correct users and servers. SSL server and clients obtain CA certificates via PKI (Public Key Infrastructure).

Integrality: Maintain the integrality of the data based on Message Authentication Code (MAC) to prevent data being altered in the transmission. A MAC algorithm, sometimes called a keyed (cryptographic) hash function, accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a tag). The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

SSL Protocol Structure

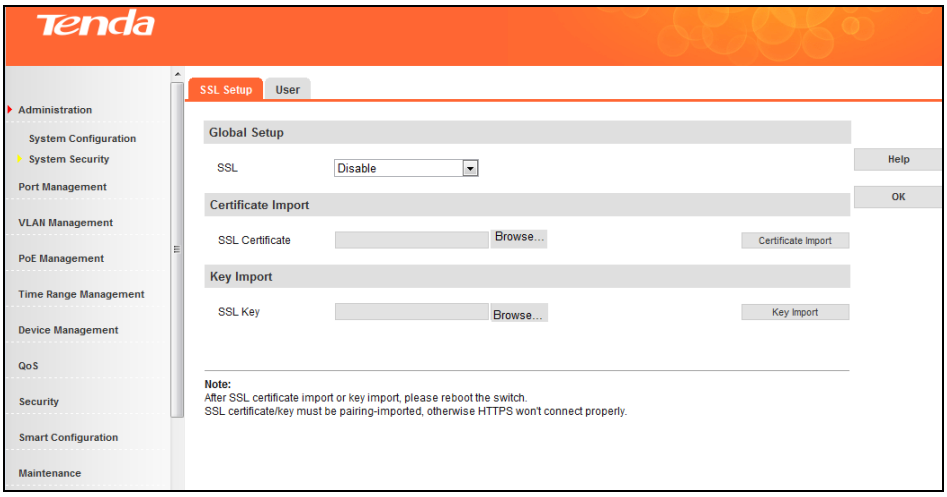
SSL protocol can be divided into 2 layers: The bottom layer is SSL record protocol; the top layer includes SSL handshake protocol, SSL change cipher spec protocol and SSL alert protocol.

SSL handshake protocol	**SSL change cipher spec protocol**	**SSL alert protocol**	**HTTP, FTP,…**
SSL record protocol			
TCP			
IP			

- SSL record protocol: Mainly applied for data partition, data calculation, MAC adding, encryption and record block transmission.
- SSL handshake protocol: It is a very important part of SSL protocol, mainly used for cryptography negotiation and authentication. A session will be established between clients and the server. Session ID, certificate of the other side, cryptography algorithm and primary security key are included in the session.
- SSL change cipher spec protocol: Clients and the server inform remote devices via SSL change cipher spec protocol and packets will adopt the newly negotiated cryptography algorithm and security key for protection and transmission.
- SSL alert protocol: mainly used for reporting alert info, and severity and description are included in messages.

SSL Setup

Click **Administration -> System Security -> SSL Setup** to enter interface below:



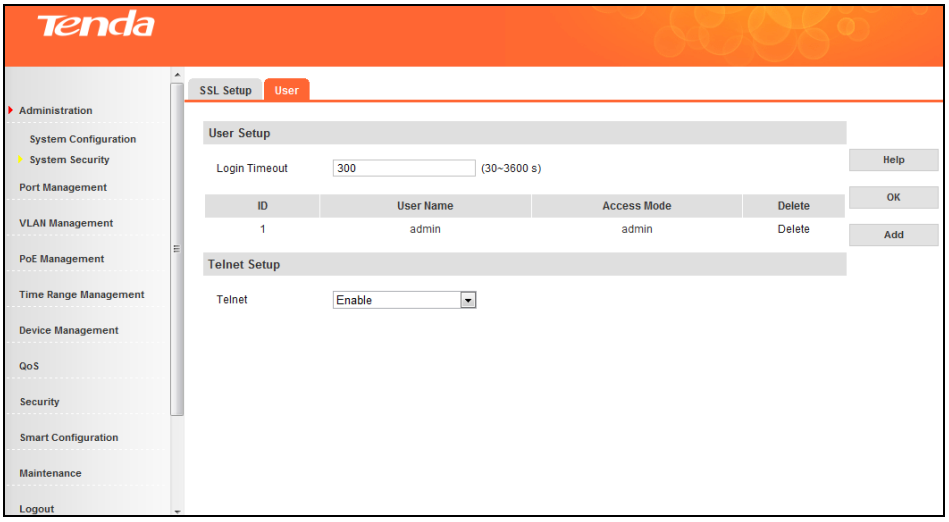
Fields on the screen are described below:

Field	Description

SSL	Enable/disable SSL
SSL Certificate	Select the desired certificate to download to the switch.
SSL Key	Select the desired SSL Key to download to the switch for encryption.
Certificate Import	Import the downloaded certificate
Key Import	Import the downloaded key

User

Click **Administration -> System Security -> User** to enter interface below:



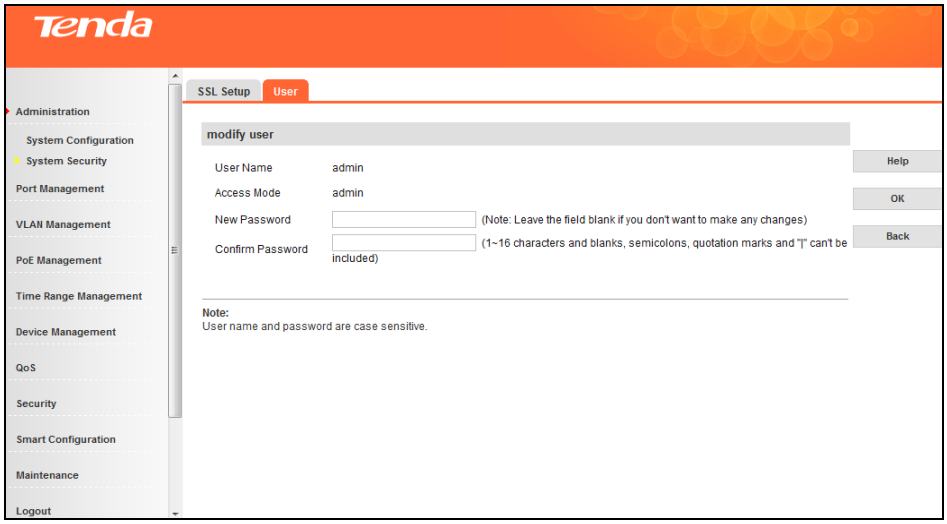
Fields on the screen are described below:

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	Specify a user name for login authentication.

Access Mode	Specify an access right for a corresponding user: Administrator: Has absolute rights to view and config switch's settings and system info. Technician: Has the right to view and config switch's settings, except for “Firmware Update”, “User”, “Reset”, “Reboot” settings. User: Has the right to view switch's current settings but no right to manage/config them.
Telnet	Enable/disable Telnet management. When enabled, you can manage the switch via Telnet.

➢ **To change password, do as follows:**

1. On the User Management screen, click **admin** to enter below interface:



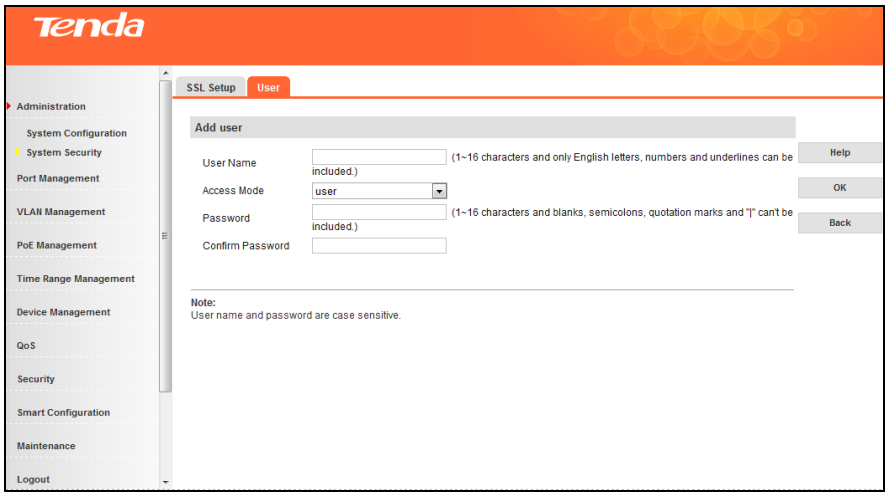
2. Enter the new password in the corresponding input box;
3. Enter the password again to confirm the new password;
4. Click **OK**.

Note----------

Use the new password to re-log into the switch once you change it. In case of losing passwords, press the hardware Reset button. And password will be reset to factory default.

➢ **To add user, do as follows:**

1. Click **Add** to enter interface below:



2. Enter the user name in the corresponding input box;
3. Select **User** or **Technician** from the **Access Mode** pull-down menu ;
4. Enter the password, for example, a12345+;
5. Retype the new password;
6. Click **OK**;
7. Exit from the management interface and use the new user name and password to re-access the switch.

Note----------

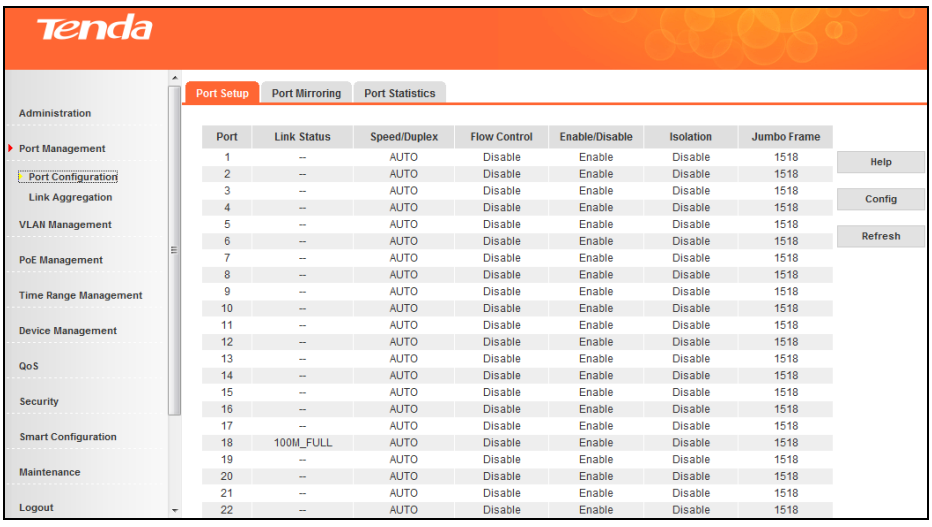
Apart from the default administrator, up to 5 technicians and 10 users can be added.

4.2 Port Management

4.2.1 Port Configuration

Port Setup

Click **Port Management -> Port Configuration -> Port Setup** to enter interface below:

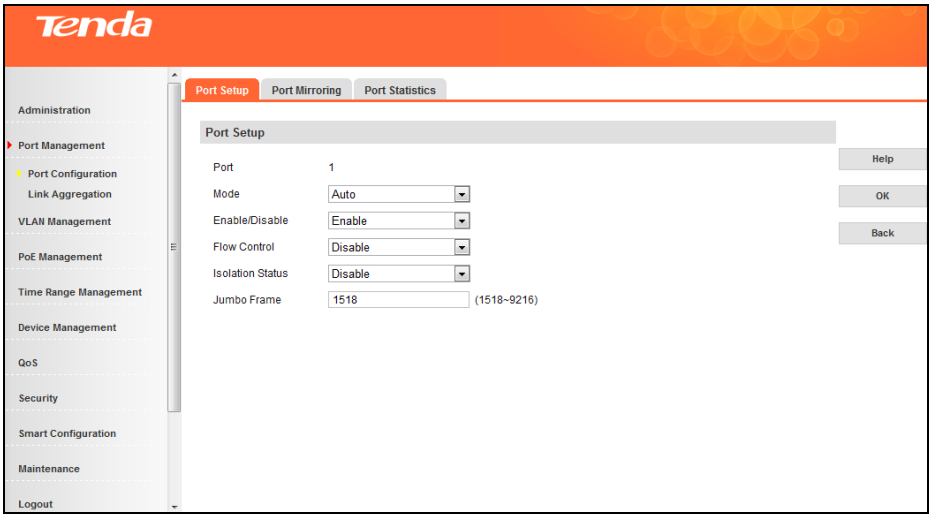


Fields on the screen are described below:

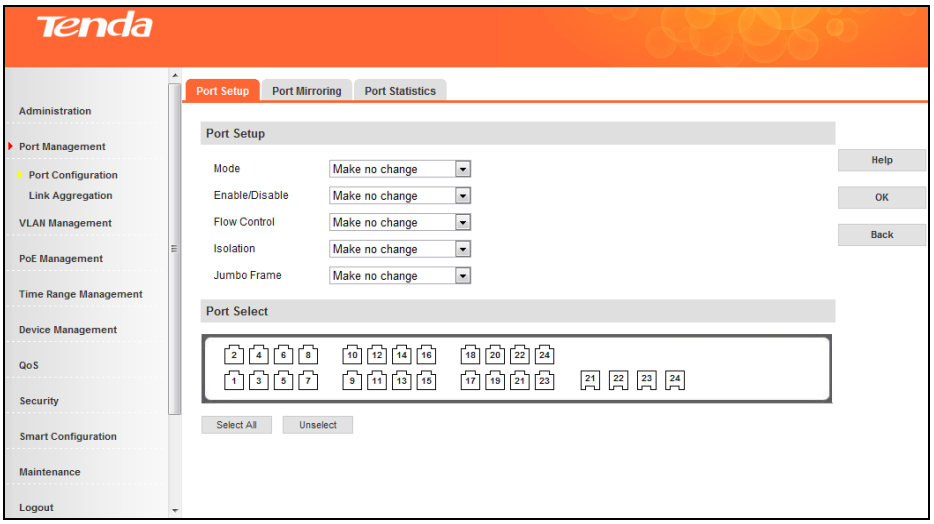
Field	Description
Link Status	Displays currently actual link rates and duplex modes on switch ports. "--" is displayed if a port is not linked.
Speed/Duplex	Three types of duplex modes are available on Ethernet ports: ➢ Full-duplex: Ports operating in Full-duplex mode can send and receive packets concurrently. ➢ Half-duplex: Ports operating in Half-duplex mode can either send or receive packets at a given time. ➢ Auto: Auto-negotiation, ports operating in Auto-negotiation mode determine their duplex mode through auto-negotiation with peer ports. By default, Auto (Auto-negotiation) is enabled for the Speed/Duplex option.
Flow Control	With flow control enabled on both the switch and its link partner, the switch, when encountering congestion, 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.
Enable/Disable	Enable/disable selected port(s). A disabled port cannot forward packets. By default, all ports are enabled.
Isolation	Use this option to group ports together to implement layer-2 data isolation among ports in an isolated group to, delivering better security and flexible networking solutions. Only in 802.1Q VLAN mode can it be configured. By default, ports are not isolated.

Jumbo Frame	Use this option to config the size of a jumbo frame (1518-9216) that the switch is to receive. The switch continues data processing within the jumbo frame range. The default jumbo frame size is 1518.

- To config a single port, click the corresponding port on the main screen and a screen for configuring the specific port will display.



- To config a group of ports as a batch task, click **Config** on the main screen and you will enter the intended screen.



Note----------

1. This device does not support half-duplex flow control. Enabling full duplex flow control can avoid packets loss, but will influence the communication speed between source interfaces and other devices. Thus, do not enable full duplex flow control on interfaces which connect to Internet unless necessary.

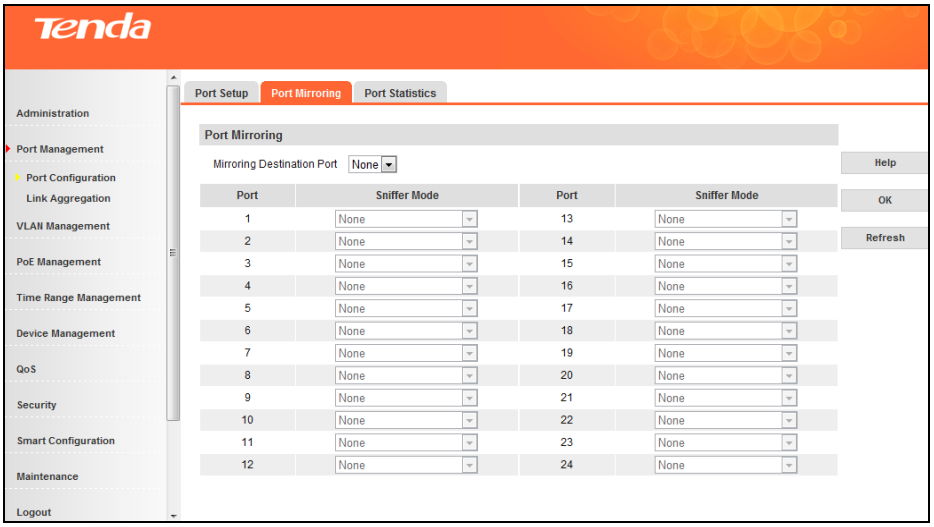
2. Only ports in the same isolation group cannot intercommunicate, will intercommunication between ports within an isolation group and ports outside such group not be affected.
3. When a port in an aggregation group joins or leaves an isolation group, other ports in such aggregation group will join or leave the same isolation group automatically.
4. When a port in an aggregation group leaves an isolation group, other ports in such aggregation group will remain in the same isolation group, namely, isolation properties for ports in an aggregation will not be affected.
5. When a non-isolated port joins an isolated aggregation group, it joins the same isolation group automatically.

Port Mirroring

Port Mirroring allows 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 functionality, namely, both mirrored ports and mirroring destination ports are located on the same device.

Click **Port Management -> Port Configuration -> Port Mirroring** to enter interface below:



Fields on the screen are described below:

Field	Description
Mirroring Destination Port	Select a mirroring destination port. "None" indicates disabling the mirroring feature. ➢ A port can not be set as the mirrored port and the mirroring destination port simultaneously. ➢ Only after a mirroring destination port is set, can you select mirroring source port(s). ➢ A port in an aggregation group cannot be configured as a mirroring destination port. ➢ A STP-enabled and 802.1X authenticated port can't be configured

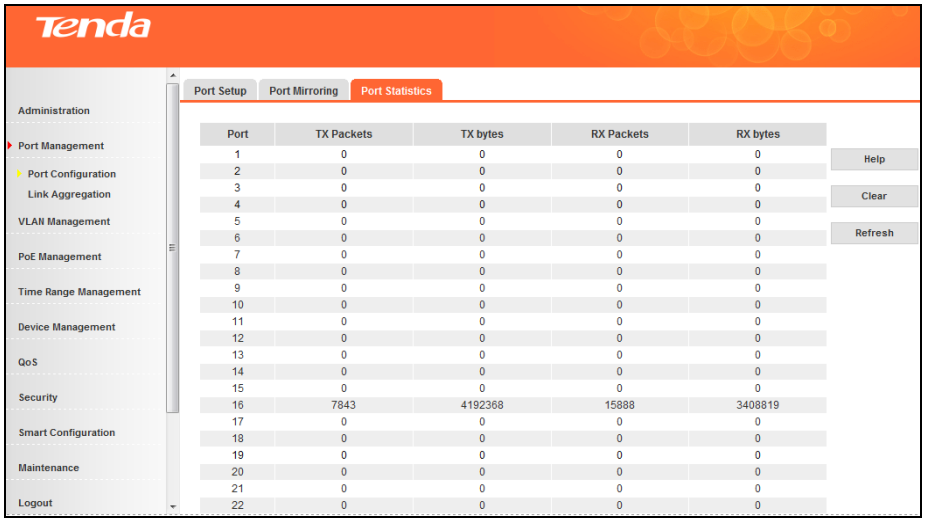
	as a mirroring destination port.
Sniffer Mode	Select a sniffer mode for a corresponding mirroring source port. "None" indicates the corresponding port is not mirrored. Mirroring can be implemented on packets of different directions (incoming/outgoing) on different ports concurrently. When total bandwidth of the mirrored port exceeds that of the mirroring port, packets loss will appear. ➢ Ingress：Only incoming packets are copied to the monitor port. ➢ Egress：Only outgoing packets are copied to the monitor port. ➢ Egress & Ingress: Both inbound and outbound packets on the corresponding port are copied to the monitor port (mirroring destination port).

Note----------

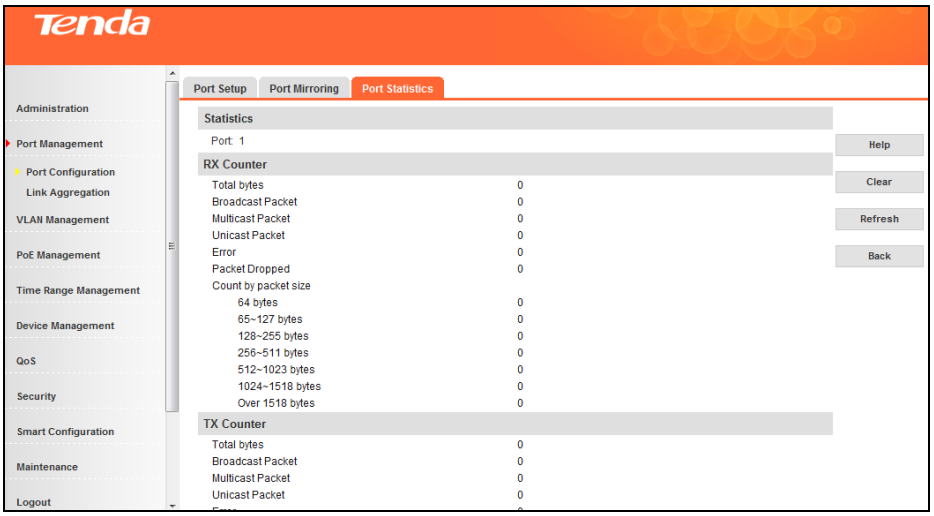
1. The mirroring destination port speed should be greater than that of total speed of all mirrored ports. So we recommend you configure the mirrored port as the routing port, namely, the port connected to Internet, to monitor all packets.
2. Only one copy is allowed for the same data flow.

Port Statistics

Click **Port Management -> Port Configuration -> Port Statistics** to enter the main interface below:



To display port-specific statistic info, click the corresponding port number:



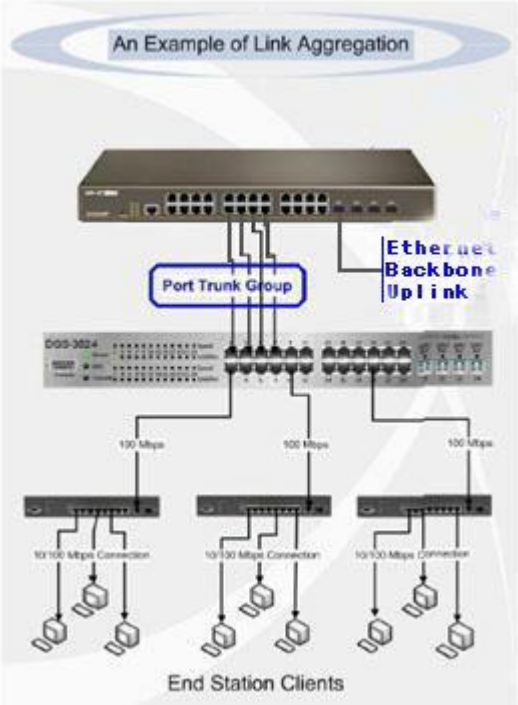
Buttons on the screen are described below:

Field	Description
Clear	Clicking it removes current statistic info.
Refresh	Clicking it updates current statistic info.
Back	Clicking it goes back to the interface which displays all ports' statistic info.

4.2.2 Link Aggregation

Link Aggregation Overview

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:



Benefits of Link Aggregation

1) Double bandwidth:

Aggregation-enabled devices treat all physical links (ports) in an aggregation group entirely as a single logical link (port). Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent. Link aggregation groups multiple Ethernet ports together in parallel to act as a single logical link. This gives a bandwidth that is a multiple of a single link's bandwidth.

2) Backup and redundancy:

Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group. The Spanning Tree Protocol will treat a link aggregation group as a single link, on the switch level. On the port level, the STP will use the port parameters of the Master Port in the calculation of port cost and in determining the state of the link aggregation group. If two redundant link aggregation groups are configured on the Switch, STP will block one entire group. In the same way, STP will block a single port that has a redundant link.

Link Aggregation Mode

1) 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. Down to 2 member ports must be included in a single aggregation group. LACP is disabled on the member ports in static LACP mode.

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

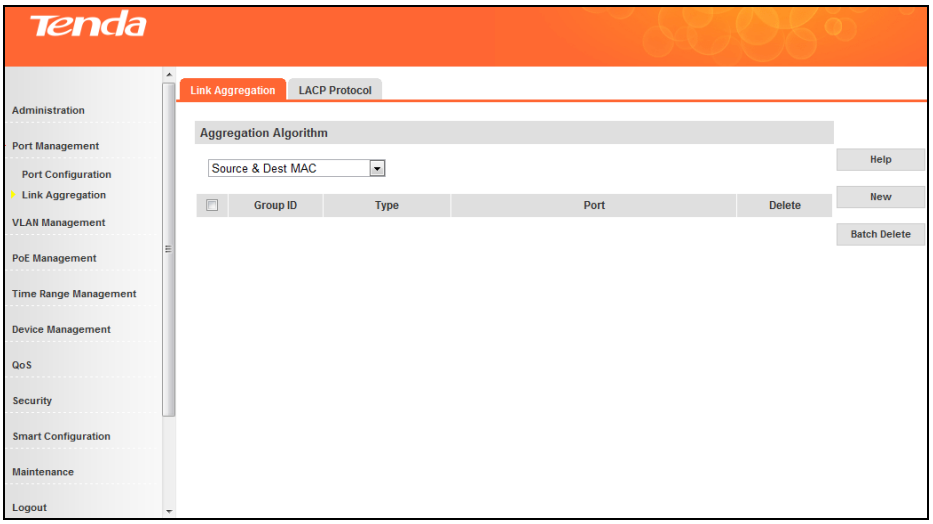
2) LACP

For LACP aggregation, you must manually maintain the aggregation state of the member ports. Whether ports in LACP group are aggregation ports or not is deterrmined by LLDPBU frame auto-negotiation. Down to 2 member ports must be included in a single aggregation group. 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. Ports in LACP aggregation group 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.

Link Aggregation--- View & Config

Click **Port Management -> Link Aggregation** to enter the main link aggregation interface:

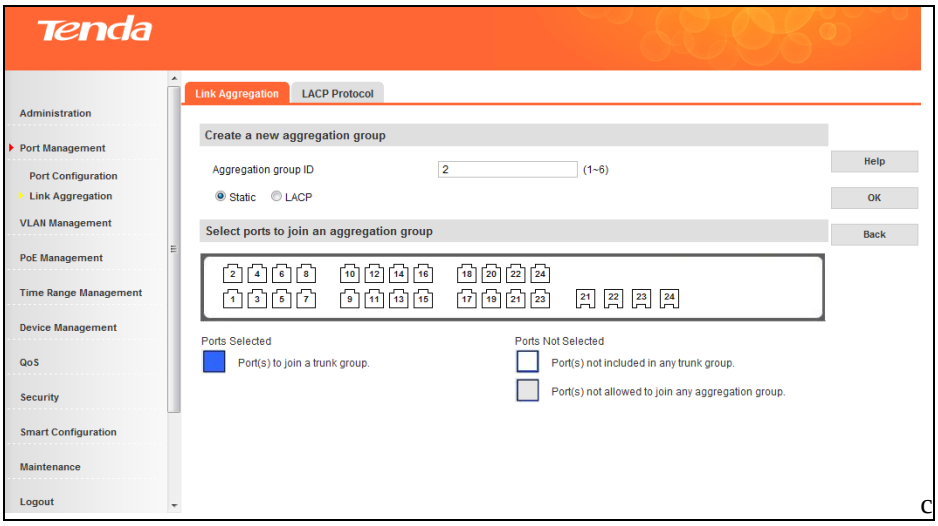


Four widely used aggregation algorithms are listed below:

Algorithm	Description
Source MAC	Member ports in a link aggregation group share traffic load according to source MAC addresses.
Dest MAC	Member ports in a link aggregation group share traffic load according to destination MAC addresses.
Source & Dest MAC	Member ports in a link aggregation group share traffic load according to source and destination MAC addresses.
Source & Dest IP	Member ports in a link aggregation group share traffic load according to source and destination IP addresses.

- **Static Aggregation—Config**

To enter the configuration screen as seen below, click **New**:



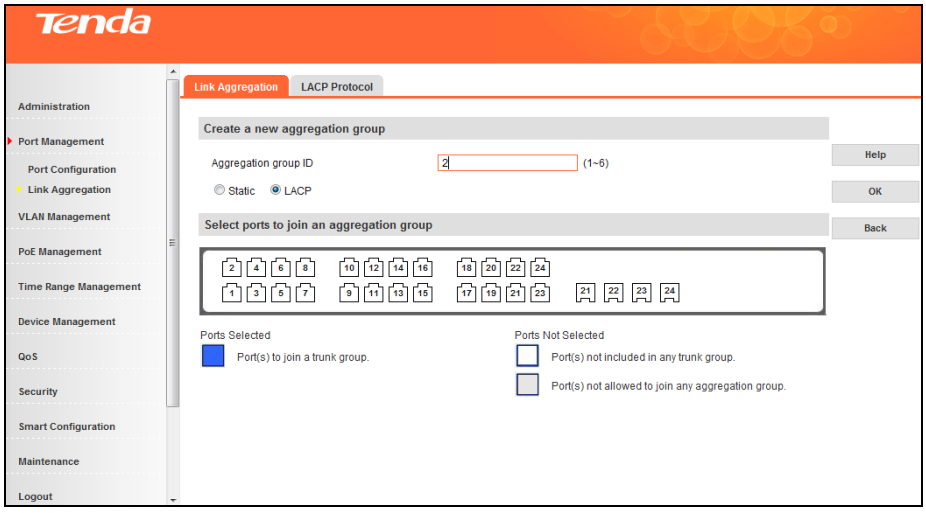
1. Enter a valid aggregation group number (1-6);
2. Select static aggregation;
3. Select ports to join the aggregation group. Up to 8 ports and down to 2 ports can be added to each.
4. Click **OK** and the group will be created.

Note----------

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

- **LACP Aggregation—Config**

To enter the configuration screen as seen below, click **New**:

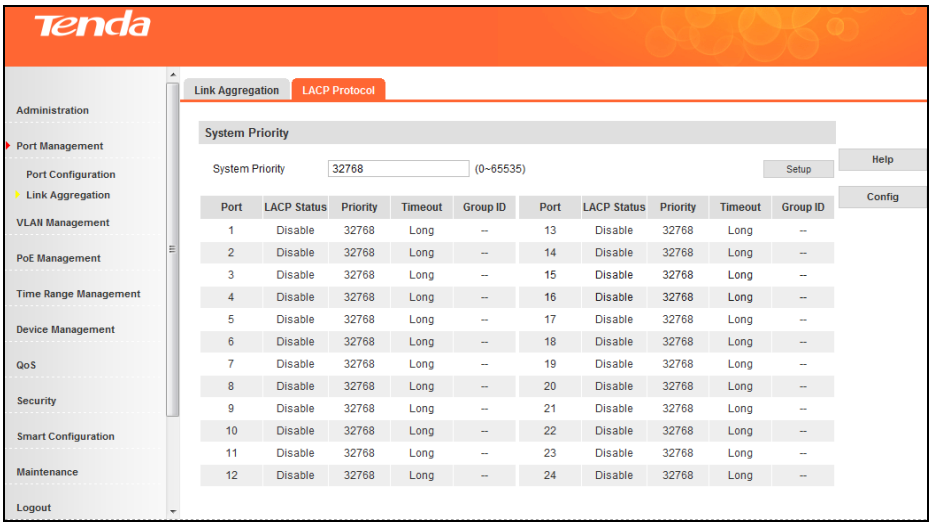


1. Enter a valid aggregation group number (1-6);
2. Select LACP aggregation;
3. Select ports to join the aggregation group. Up to 8 ports and down to 2 ports can be added to each.
4. Click **OK** and the group will be created.

LACP Parameters—Config

➢ **To config LACP parameters**

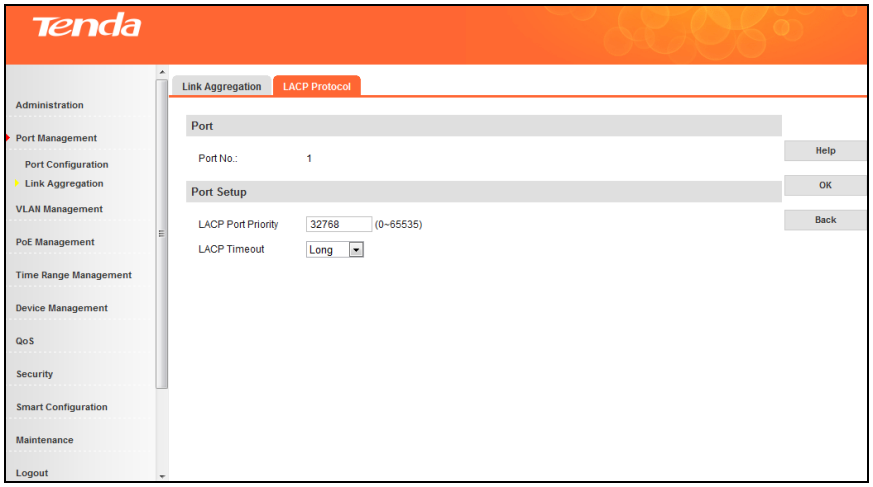
Click **Port Management -> Link Aggregation -> LACP Protocol** and below screen will be displayed:



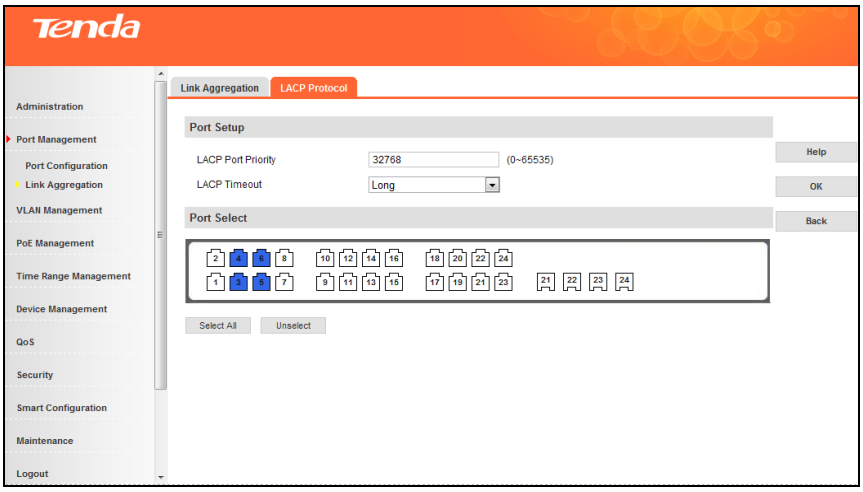
Fields on the screen are described below:

Field	Description
System Priority	Config system priority (0-65535). The default is 32768.
LACP Status	Displays Enable when corresponding port joins a LACP aggregation group and Disable when the port does not join any LACP aggregation group or joined a static aggregation group.
Priority	Config port priority (0-65535). The default is 32768.
Timeout	Select a LACP timeout: long or short. The default is long.
Group ID	Displays the LACP aggregation group ID.

To config LACP parameters on a single port: click the corresponding port as seen below:

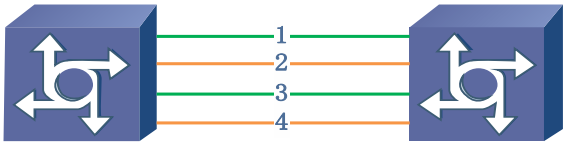


To config LACP parameters on a group of ports as a batch task: click **Config** as seen below:



Application Example of LACP

Configurable range of system priority is 0-65535 and the default is 32768. When system priority is set, ports in LACP aggregation group with higher priority will be selected. The primary device of LACP aggregation group is determined by priority+management MAC address. The primary port of LACP aggregation group is determined by port LACP priority+port number. Application example is interpretated as below:



Switch A Switch B

1) Create LACP aggregation group 5(ports 1-4 included) on switch A and switch B, and set port rate to 100M/FULL on port 1 and port 4.

2) By default, after negotiation, LACP aggregation group 5 contains port 1 and port 3. Then, on the **LACP protocol** interface, group ID 5 will be only displayed on port 1 and port 3.
3) Set Switch A's system priority (on the **LACP protocol** interface) to a value which is smaller than 32768 so that switch A's priority is higher than switch B's. At the same time, set port 2's LACP priority on switch A to a value which is smaller than 32768 so that port 2's priority is higher than port 1's. Then view the negotiation result of LACP aggregation group 5: Group ID on port 2 and port 4 displays 5, i.e. after negotiation, LACP aggregation group 5 will contain port 2 and port 4.
4) Set Switch A's system priority (on the **LACP protocol** interface) to a value which is greater than 32768 so that switch B's priority is higher than switch A's. At the same time, set port 1's LACP priority on switch B to a value which is smaller than 32768 so that port 1's priority is higher than port 2's. Then view the negotiation result of LACP aggregation group 5: Group ID on port 1 and port 3 displays 5, i.e. after negotiation, LACP aggregation group 5 will contain port 1 and port 3.

Port configuration considerations in link aggregation

To share egress/ingress traffic load, member ports in an aggregation group must be set to the same configurations with respect to STP, port priorities, VLAN, port management, ARP attack defense, etc.

- Consistent STP Configurations: Includes STP status, P2P port, edge port, port priority, path cost, etc.
- Consistent port priorities.
- Consistent VLAN Configurations: Includes interface type, PVID, allowed VLAN and Untag/Tag VLAN.
- Consistent port priorities: Includes Jumbo frame, flow control and isolation settings.
- Consistent ACL configurations: Includes Binding ACL lists
- Consistent ARP attack defense: Includes ARP rate limit and ARP receiving rate settings.

If parameters on any port are changed in the aggregation group, configurations on other member ports should be kept consistent.

For ports having joined in the aggregation group, following configurations are not allowed:

- Adding static MAC address
- Configuring MAC learning
- Enabling IP filter
- Configuring mirroring destination port
- Enabling voice VLAN feature
- Enabling 802.1X authentication

Below ports cannot join the aggregation group:

- 802.1x-enabled port(s)
- ACL Binding port(s)
- Mirroring destination port(s)
- Ports on which MAC address filter is enabled
- Ports on which IP address filter is enabled
- Ports on which MAC address learning limit is set

4.3 VLAN Management

4.3.1 VLAN

VLAN Overview

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. In 1999, IEEE released 802.1Q draft as a standardized VLAN implementation solution.

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.

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

(1) Better management and control of broadcast activity

VLANs conserve network resources by segmenting a large broadcast domain into several smaller broadcast domains or VLAN groups and restrict all broadcast traffic to the VLAN on which the broadcast was initiated.

(2) Reduced cost

The use of VLANs to create broadcast domains eliminates the need for routers to handle this function, permitting operation at lower latencies and cost compared to routers under heavy load and at high cost.

(3) Ease of network administration

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-config the network when a VLAN member changes its location. For example, in order to better collaborate with staffs from home or abroad on a special project a workgroup is indispensable. Using VLAN, all workstations and servers that a particular workgroup uses can be assigned to the same VLAN. For example, in order to better collaborate with staffs from home or abroad on a special project, a workgroup is indispensable. Using VLAN, all workstations and servers that a particular workgroup uses can be assigned to the same VLAN.

(4) Tighter network security

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 Mode

The switch provides 2 VLAN modes as below:

802.1Q VLAN Mode:

IEEE 802.1Q is the network standard that supports Virtual LANs (VLANs) on an Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames.

Port VLAN:

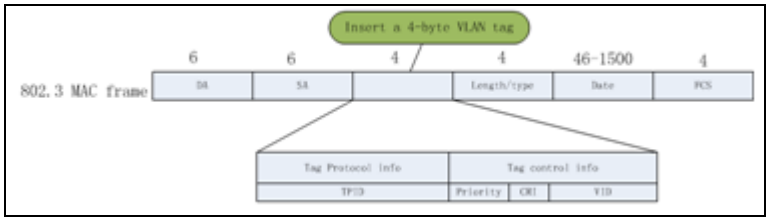
Port VLANs limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department. Members of the same VLAN can intercommunicate. A user can belong to multiple VLANs simultaneously. For example, if you want both user A and user B to communicate with user C while user A and user B cannot intercommunicate, simply put user A and user C to a VLAN and

user B and user C to the other VLAN.

802.1Q VLAN

VLAN Tag:

As defined in IEEE 802.1Q, a four-byte VLAN tag is inserted after the DA&SA field to identify frames of different VLANs.



(1) TPID: The 16-bit TPID field with a value of 0x8100 indicates that the frame is VLAN-tagged.

(2) Priority: The 3-bit priority field indicates the 802.1P priority of the frame (0-7).

(3) CFI: CFI is a 1-bit field, indicating whether the MAC address is encapsulated in the standard format in different transmission media. 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 advisable to set this value to 0.

(4) VID: The 12-bit VLAN ID field identifies the VLAN which the frame belongs to. The VLAN ID range is 0 to 4095. Because 0 and 4095 are reserved, a VLAN ID actually ranges from 1 to 4094.

802.1Q VLAN Port link type:

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 including the following three types:

(1) Access: An access port belongs to only one VLAN. It is usually used to connect a PC.

(2) Trunk: A trunk port can carry multiple VLANs to receive and send traffic for them. Usually, ports that connect switches are configured as trunk ports.

(3) Hybrid: Like a trunk port, a hybrid port can carry multiple VLANs to receive and send traffic for them. A port connected to a network device or user terminal can be configured as a hybrid port.

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 Type	Receiving Tagged Packets	Receiving Untagged Packets	Forwarding Packets
Access	The packet will be forwarded to other ports in the	The packet will be forwarded to other ports in	The packet will be forwarded after removing its VLAN tag.

Trunk	corresponding VLAN according to the VID in the Tag	the corresponding VLAN according to PVID on this port	If the VID of packet is the same as the PVID of the port, the packet will be forwarded after removing its VLAN tag; If the VID of packet is not the same as the PVID of the port, 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.

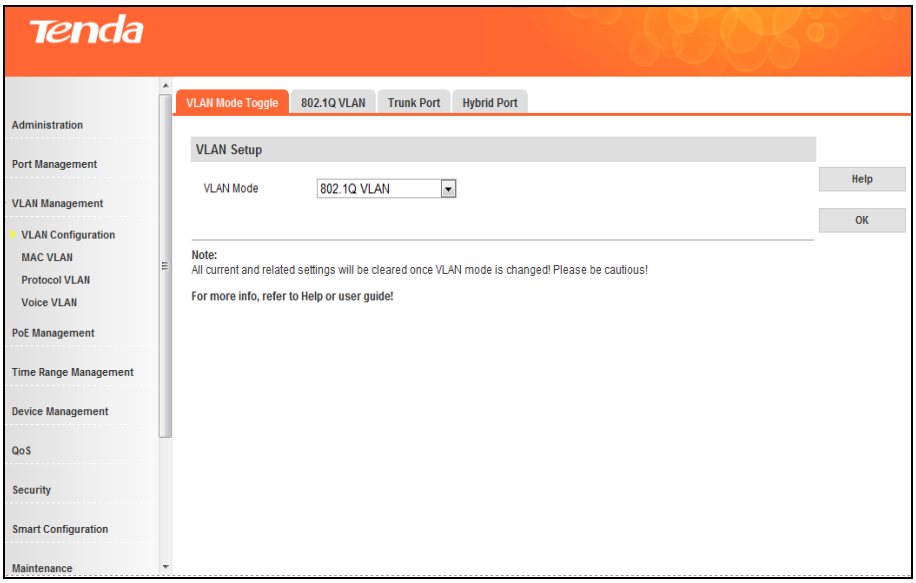
Note----------

1. 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.
2. This switch does not support ingress filter feature. Only in 802.1Q VLAN, ingress Tag packets will be forwarded according to the VID and ingress Untag packets will be forwarded according to the PVID.
3. If voice VLAN, protocol VLAN, MAC VLAN and 802.1Q VLAN are configured on this switch, ingress packets will be matched according to the VLAN sequence mentioned above.

VLAN Mode Toggle

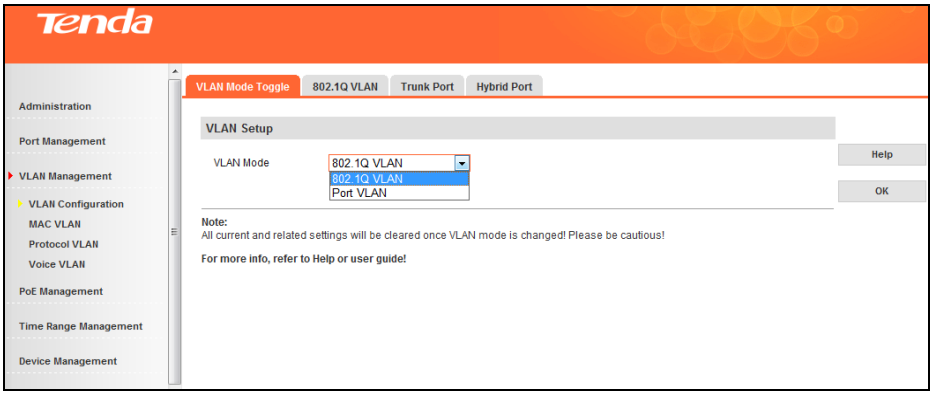
You can toggle between Port VLAN and 802.1Q VLAN. Note that related settings like static MAC binding, IP+MAC+Port+VLAN Binding settings will be cleared when you change the VLAN mode.

To enter the screen below, click **VLAN Management -> VLAN Configuration -> VLAN Mode Toggle**. The default is 802.1Q VLAN.



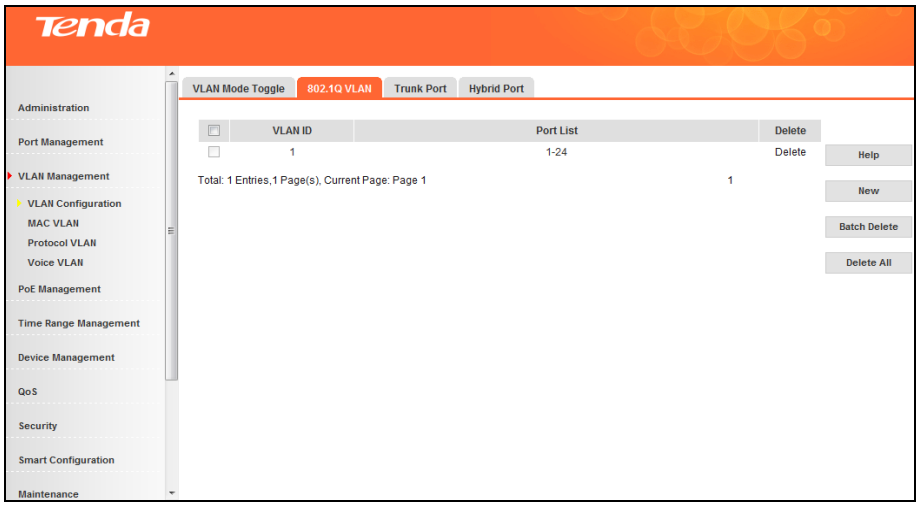
➢ To switch to Port VLAN:

Select Port VLAN and click **OK**.



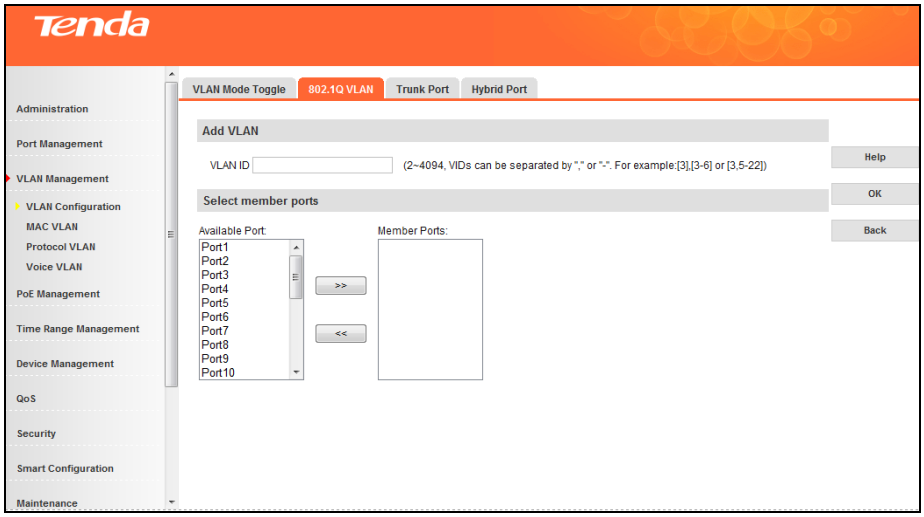
802.1Q VLAN--Config

To enter the screen below, click **VLAN Management -> 802.1Q VLAN**.



➢ To add QVLAN/Access port:

Click **New** to enter below screen:



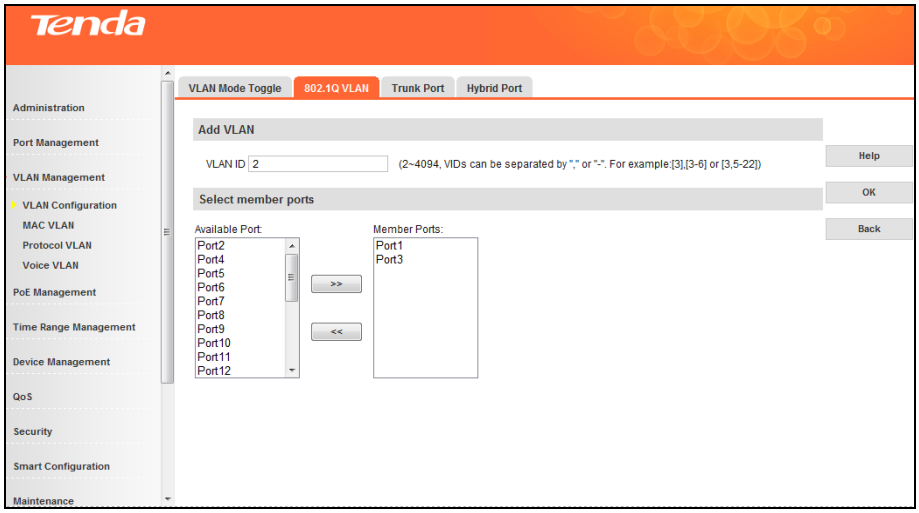
1. Enter 2 in VLAN ID field.
2. Select port1 and port2 from **Available Port** and click >> to move them to **Member Ports**.
3. Click **OK** and below screen will be displayed.

Note----------

1. Available values for VLAN ID range from 2 to 4029. You can config multiple VLANs by entering "x-x" in the VLAN ID field (where x represents any number between 2 and 4029). For example, "1-10" indicates 10 QVLANs while "1, 10" indicates 2 QVLANs.
2. Up to 128 QVLANs can be added.
3. By default, all ports belong to QVLAN1.
4. When a VLAN ID is deleted, ports of this VLAN ID will belong to 802.1Q VLAN1 automatically.

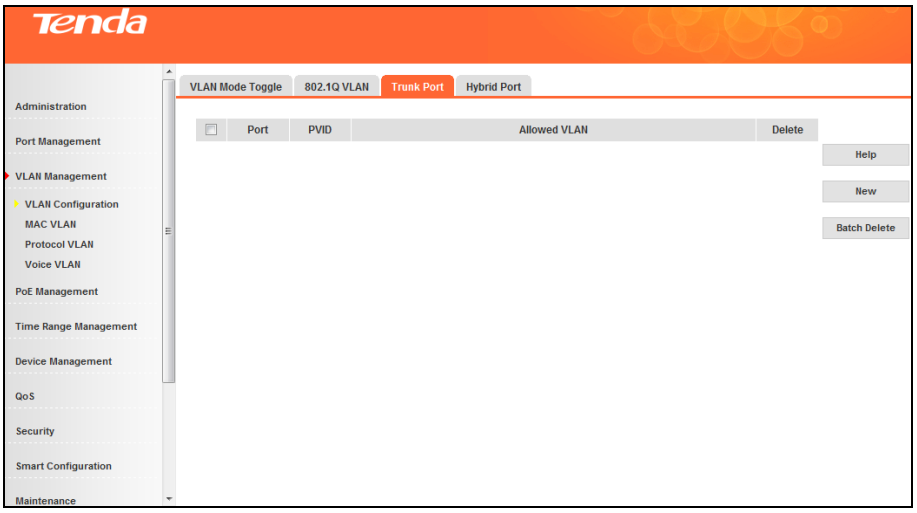
- Add/delete an access port
  1. Click the VLAN ID of 2.
  2. Select port3 from **Available Ports** and click >>.

3. Select port2 from **Member Ports** and click <<.
4. Click **OK**.

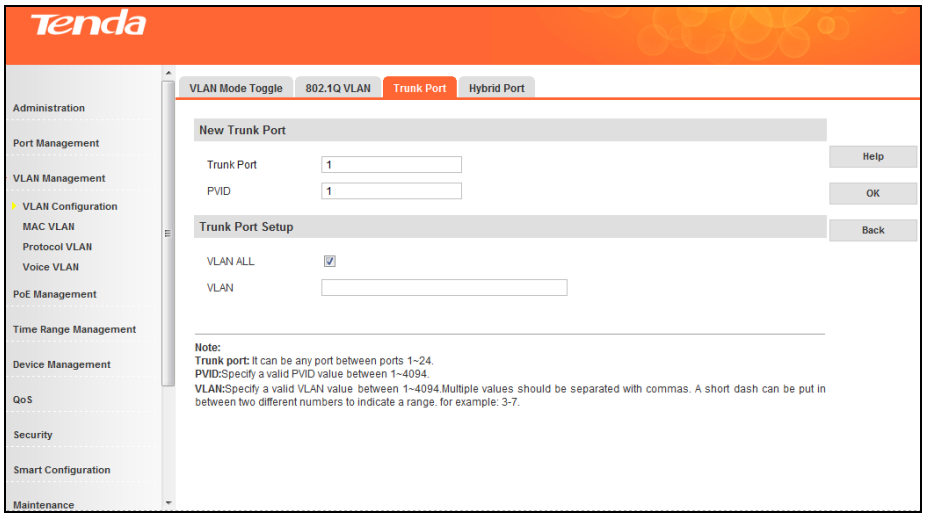


➢ Add trunk port

1. Click **Trunk Port** to enter the trunk port interface.



2. Click **New**.
3. Enter "1~24" in **Trunk Port** field.
4. Enter 1 or an existing VLAN ID in the PVID field.
5. Click **VLAN All** or enter "1-4094" in the VLAN field.
6. Click **OK**.

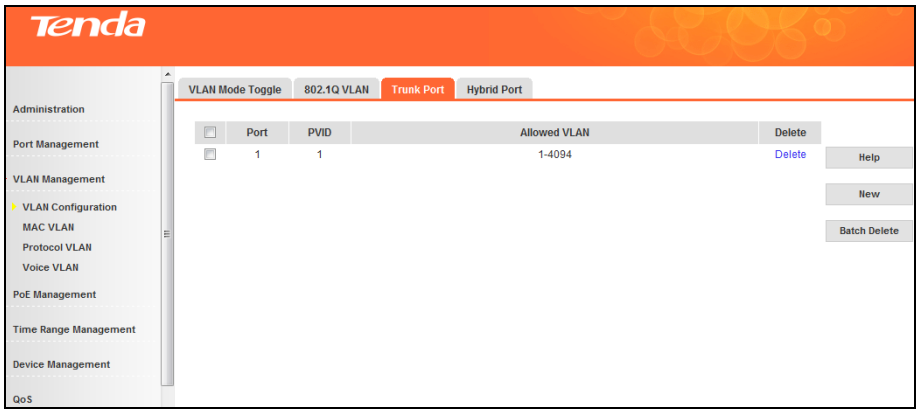


➢ Edit trunk port

1. Click trunk port 1.
2. The PVID is configurable and must be an existing VID and between 1 and 4094.
3. If you only want the trunk port to carry some VLANs, you can delete the unwanted VLANs or add desired VLANs.
4. Click **OK**.

➢ Delete a trunk port

You can delete a trunk port in the trunk port view.



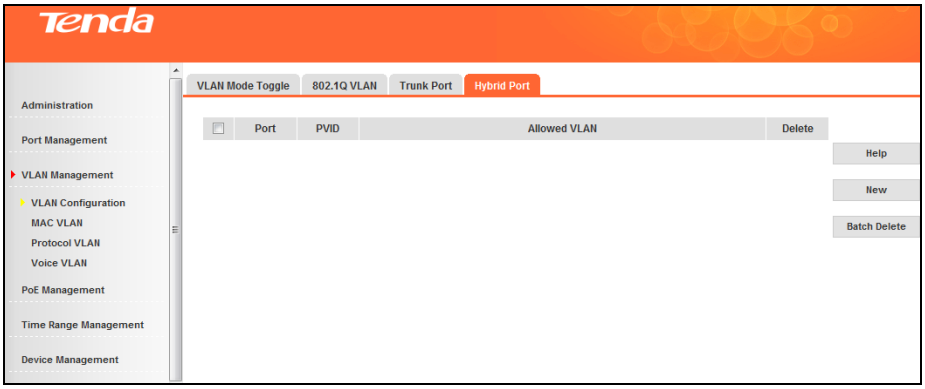
To delete a single trunk port, click the **Delete** button; to delete a batch of trunk ports, click  and then the **Batch Delete** button.

Note----------

1. An existing Hybrid port cannot be directly configured as a Trunk port. However, you can convert a Hybrid port into a Trunk port by first deleting it from hybrid ports and then setting it to a Trunk port.
2. Deleted trunk ports will join VLAN1 as access ports.
3. A trunk port can belong to multiple VLANs.

➢ Add a hybrid port

1. Click **Hybrid Port** to display below screen:



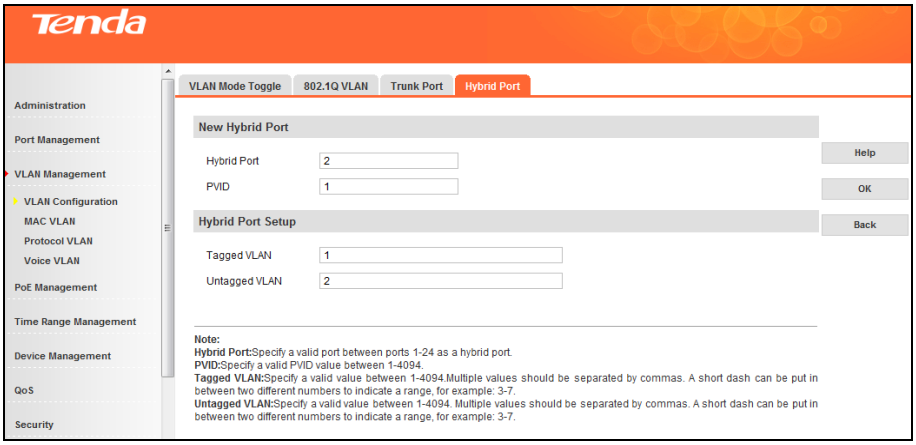
2. Click **New** and enter a port number in the Hybrid Port field. You can add multiple ports by entering "x-x" (where x represents any number between 1 and 24). For example, "1-24" denotes 24 ports while "1, 24" indicates 2 ports.

3. PVID: Enter an existing VLAN ID.

4. Tagged VLAN: Enter a value between 1 and 4094 or leave it empty.

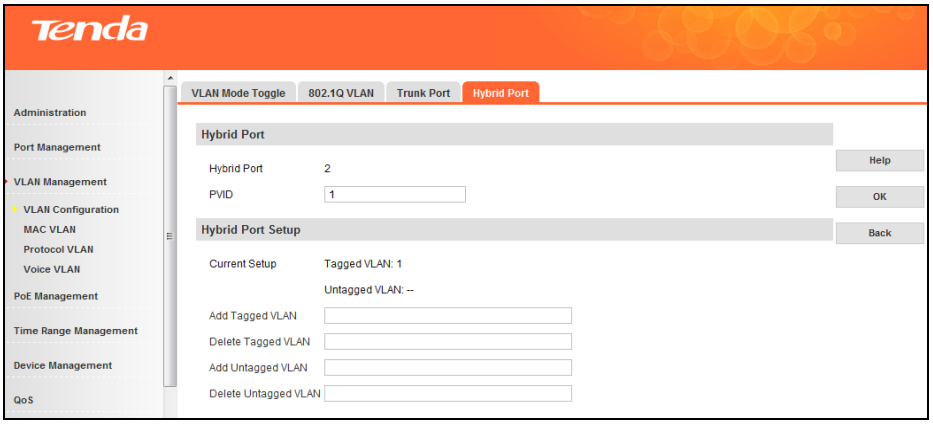
5. Untagged VLAN：Enter a value between 1 and 4094 or leave it empty.

6. Click **OK**.



➢ Edit a hybrid port

1. Click the corresponding hybrid port number as seen below:



2. The PVID is configurable and should be an existing VID and between 1 and 4094.
3. Add/delete currently configured Tagged VLAN and Untagged VLAN.
4. Click **OK**.

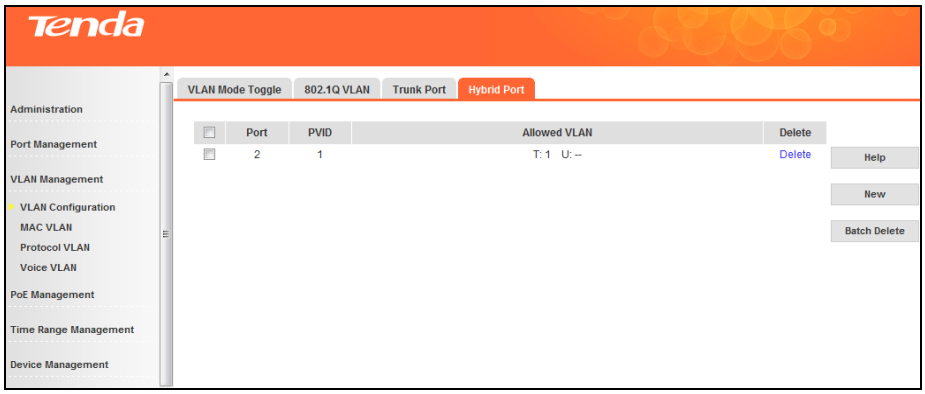
Note----------

1. Tagged VLAN and Untagged VLAN should not share the same VID.
2. Same settings should not be concurrently configured in both **Add Tagged VLAN** field and **Delete Untagged VLAN** field.
3. Settings configured in **Delete Untagged VLAN** field should not be concurrently the same as those in **Add Tagged VLAN** field.

➢ Delete a hybrid port

You can delete a hybrid port in the hybrid port view.

To delete a single hybrid port, click the **Delete** button; to delete a batch of hybrid ports, click  and then the **Batch Delete** button.



Note----------

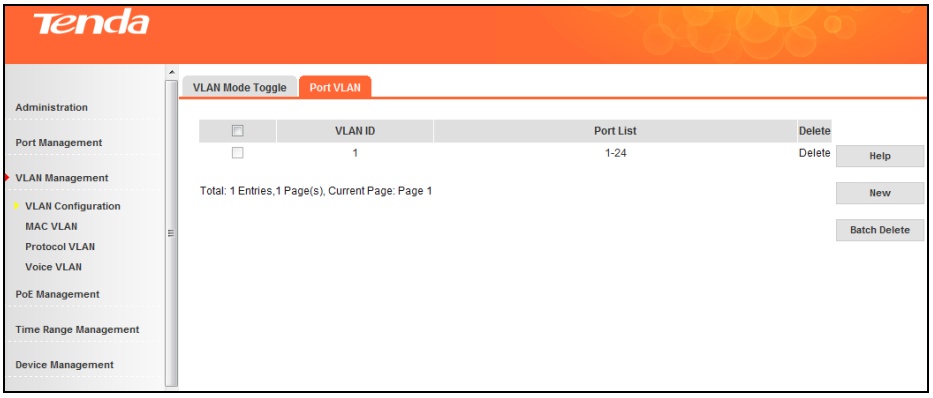
1. An existing Trunk port cannot be directly configured as a Hybrid port. However, you can convert a Trunk port into a Hybrid port by first deleting it from Trunk ports and then setting it to a Hybrid port.
2. Deleted hybrid ports will join VLAN1 as access ports.
3. A hybrid port can belong to multiple VLANs.

Port VLAN

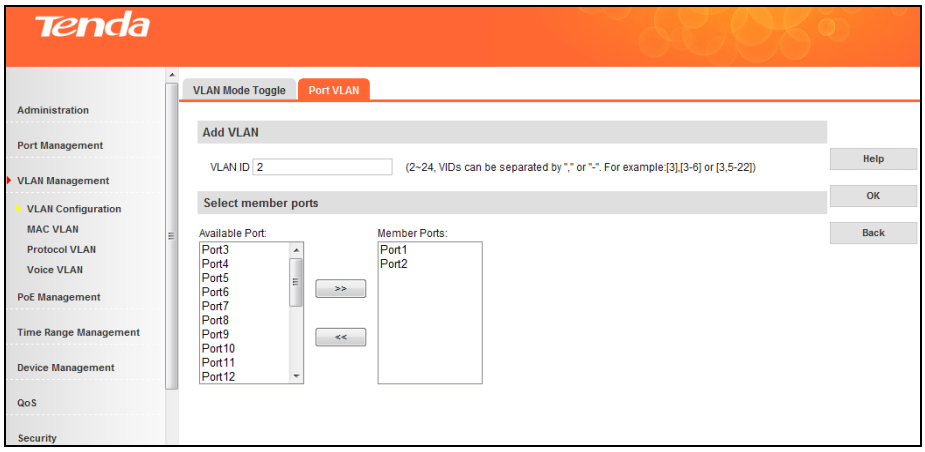
Port VLAN and 802.1Q VLAN can be toggled randomly. If you toggle 802.1Q VLAN to port VLAN, related VLAN configurations will be cleared.

➢ Create a port based VLAN

1. Toggle to the Port VLAN mode to enter the Port VLAN interface.
2. Click **Port VLAN** to enter below interface:



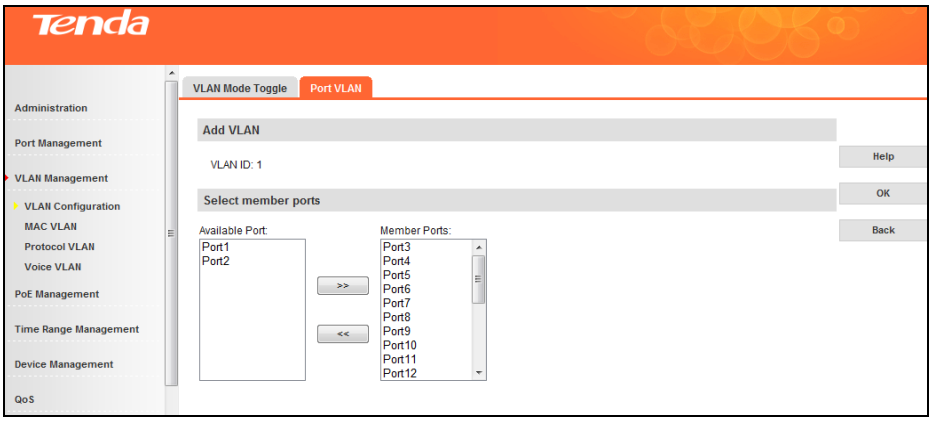
3. Click **New** as seen below:
4. Enter a VLAN ID: for example 2-24, which indicates 24 VLANs, or "1, 24", which indicates 2 VLANs.
5. Select port(s) from **Available Ports** and click >> to move them to **Member Ports**.
6. Click **OK** to finish.



➢ Delete members in a port VLAN

As seen above, ports 1-2 are still in VLAN1. To isolate them from other ports, do as follows:

1. Click VLAN1 as seen below.



2. Select port1 and port2 in **Member Ports** and click to move it back to **Available Ports**.
3. Click **OK**.

➢ Add members to a port VLAN

To add new ports to an existing port VLAN, click the corresponding VLAN ID to enter related interface for configuration.

Note----------

1. Up to 24 port VLANs can be configured.
2. Port based VLAN can not achieve inter-switch communication. Ports that belong to the same VLAN on the switch can intercommunicate.

4.3.2 MAC VLAN

Overview

MAC VLAN technology is the way to classify VLANs according to the MAC addresses of Hosts. MAC VLAN only takes effect on ingress untagged data. When the port receives an untagged packet, the device, with the matching key words of the packets' source MAC address, will search MAC VLAN entries to obtain the terminal's binding VLAN. In this way, packets of the designated terminal will be forwarded in the designated VLAN. Thus, the user terminal and VLAN will be bound accurately and flexibly.

Benefits of MAC VLAN

A MAC address corresponds to a single VLAN ID. For the device in a MAC VLAN, if its MAC address is bound to VLAN, the device can be connected to another member port in this VLAN and still takes its member role effect without changing the configuration of VLAN members.

Implementation of MAC VLAN

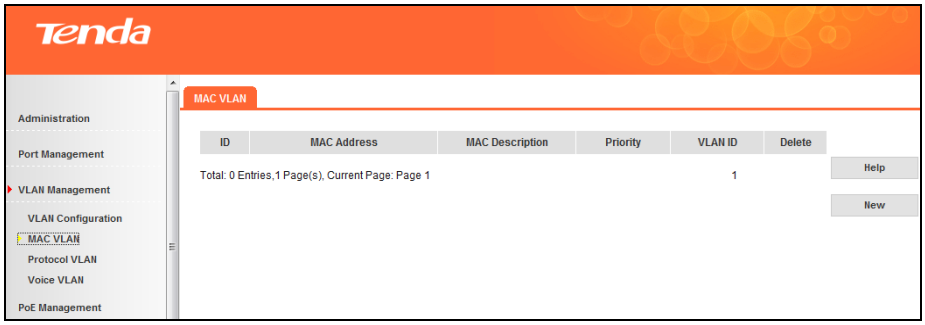
The packet in MAC VLAN is processed in the following way:

1. When receiving an untagged packet, the switch will check whether the corresponding MAC VLAN has been created. If the corresponding MAC VLAN has been created, the switch will add a corresponding MAC VLAN tag to it. If no MAC VLAN is matched, the switch will add a tag to the packet according to the PVID of the received port. Thus, the packet is assigned automatically to the corresponding VLAN for transmission.
2. When receiving tagged packet, the switch will process it based on the 802.1Q VLAN. If the received port is the member of the VLAN to which the tagged packet belongs, the packet will be forwarded normally. Otherwise, the packet will be discarded.

3. If the MAC address of a Host is classified into 802.1Q VLAN, please set its connected port of the switch to be a member of this 802.1Q VLAN so as to ensure the packets are forwarded normally.

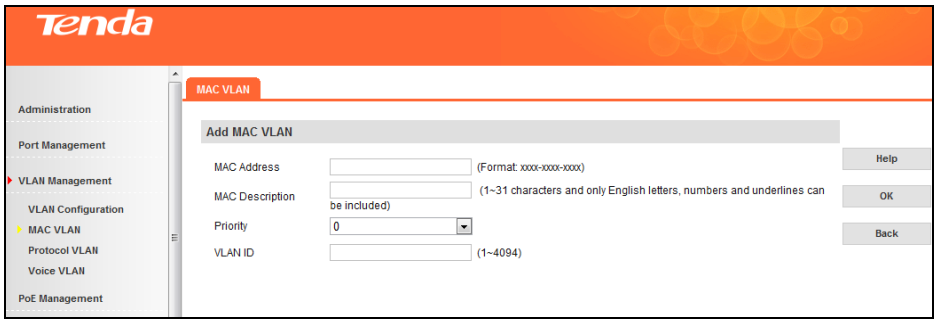
MAC VLAN---Config

MAC VLAN can only be valid in 802.1Q VLAN mode. Click **VLAN Management -> MAC VLAN** to enter interface below:

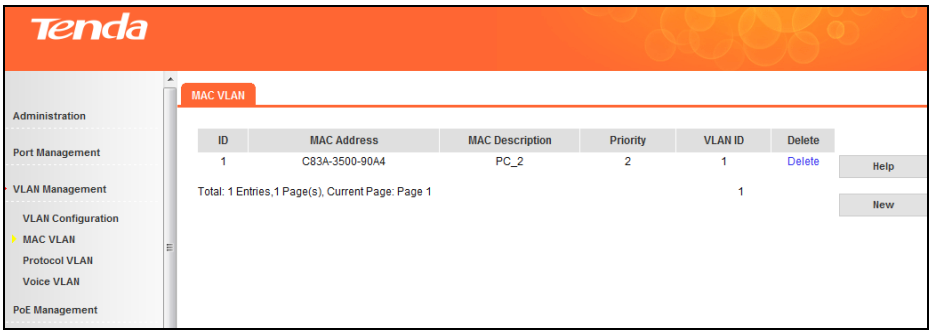


➢ Create MAC VLAN

1. Click **New** to enter interface below:



2. Enter the MAC address you wish to configure.
3. Enter the corresponding MAC address description.
4. Select this MAC VLAN's priority (0~7 available) from the drop-down list.
5. Configure the VLAN ID mapped from MAC address. This VLAN ID must already exist in 802.1Q VLAN.
6. Click **OK**.



➢ Delete MAC VLAN

As shown above, click the **Delete** button to delete the corresponding MAC VLAN. Up to 64 MAC VLANs can be supported on this device.

4.3.3 Protocol VLAN

Overview

Protocol VLAN, another way to classify VLANs based on network protocol, can bind ToS provided in the network to VLAN to realize the specific service. Through protocol VLAN, the switch can analyze the received untagged packets on the port and match the packets with the user-defined protocol template according to different encapsulation formats and the values of the special fields.

If a packet is matched, the switch will add a corresponding VLAN tag to it automatically and thus the data of specific protocol can be automatically assigned to the corresponding VLAN for transmission. The network administrator can manage network clients based on their specific applications and services through protocol VLAN.

Encapsulation Format of Ethernet Data

At present there are two encapsulation formats of Ethernet data, Ethernet II encapsulation and 802.2/802.3 encapsulation, shown as follows:

Ethernet II

Ethernet II framing (also known as DIX Ethernet, named after DEC, Intel and Xerox, the major participants in its design), defines the two-octet EtherType field in an Ethernet frame, preceded by destination and source MAC addresses, which identifies an upper layer protocol encapsulating the frame data. Once Frame type on this device is set to Ethernet II, Ether Type of this protocol VLAN will match 13-14th bytes of packets for VLAN mapping.

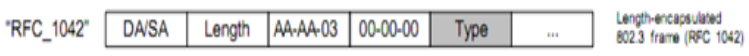
Destination MAC Address	Source MAC Address	Type	Data	CRC
6	6	2	46-1500	4

802.2/802.3

802.3, same as Ethernet II (above) except Type field is replaced by Length, and an 802.2 LLC header follows the 802.3 header. When Frame Type on this device is set to LLC, Ether Type of this protocol VLAN will match 16-18th bytes of the packet for VLAN mapping.

Ethernet SNAP

The biggest difference between Ethernet SNAP Frame and 802.3/802.2 Frame is the addition of 5-byte SNAP ID. The previous 3 bytes, manufacturer ID, are the same as those of the source MAC address and sometimes can be set to 0. The last 2 bytes are the same as Type Field of Ethernet II. When Frame Type on this device is set to SNAP, Ether Type of this protocol will match 23-24th bytes of the packet for VLAN mapping and 16-21th bytes: AA-AA-03-00-00-00.



The Procedure for the Switch to Process Protocol VLAN Packets

VLAN packets are processed in the following way:

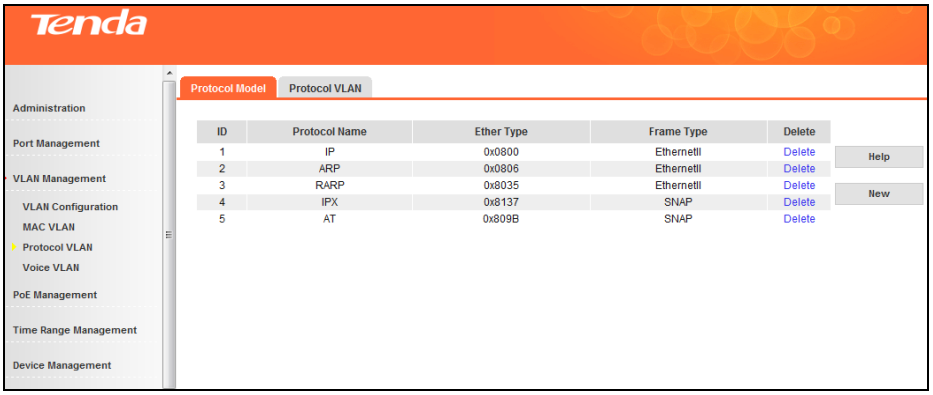
1. When receiving an untagged packet, the switch matches the packet with the current Protocol VLAN. If the packet is matched, the switch will add a corresponding Protocol VLAN tag to it. If no Protocol VLAN is

matched, the switch will add a tag to the packet according to the PVID of the received port and forward packets in the corresponding VLAN. Thus, the packet is assigned automatically to the corresponding VLAN for transmission.

2. When receiving a tagged packet, the switch will process it based on the 802.1Q VLAN. If the received port is the member of the VLAN to which the tagged packet belongs, the packet will be forwarded normally. Otherwise, the packet will be discarded.

Protocol Model---Config

Click **VLAN Management -> Protocol VLAN -> Protocol Model** to enter interface below:

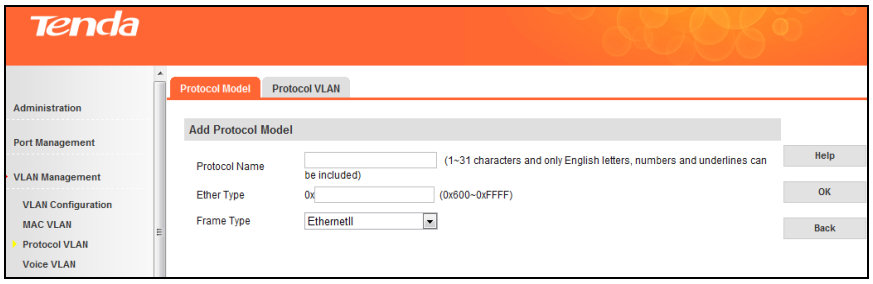


Fields on the screen are described below:

Field	Description
ID	Displays protocol model ID (1-16).
Protocol Name	Displays protocol name (case-sensitive).
Ether Type	Displays protocol model's Ether Type (0x600-0xffff) .
Frame Type	Displays protocol model's encapsulation Frame Type (Ethernet II, LLC or SNAP) .

➢ Add protocol model

1. Click **New** to enter interface below:



2. Configure protocol name in the **Protocol Name** Field. Up to 31 characters can be included and only

letters (case-sensitive), numbers and underlines can be configured here.

3. Enter the specific protocol Ether Type (0x600-0xFFFF). The corresponding relationship between Ether Type and protocol name is shown as below:

Ether Type	Corresponding Protocol Name
0x0806	ARP
0x0800	IP
0x8847/0x8848	MPLS
0x8137	IPX
0x8000	IS-IS
0x8809	LACP
0x888E	802.1x

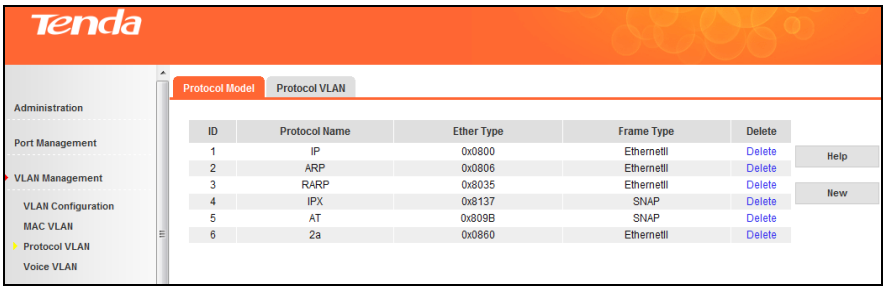
4. Configure protocol model's Frame Type. It can be configured as EthernetII, LLC and SNAP.
5. Click **OK**.

Note----------

1. It is not advisable to add special type into the protocol model, such as 0X8100 and 0x88a8.
2. EthernetII: Protocol VLAN matches with 13~14th bytes to map VLAN; LLC: Protocol VLAN matches with 17~18th bytes to map VLAN; SNAP: Protocol VLAN matches with 23~24th bytes to map VLAN and 16~21th bytes are AA-AA-03-00-00-00.

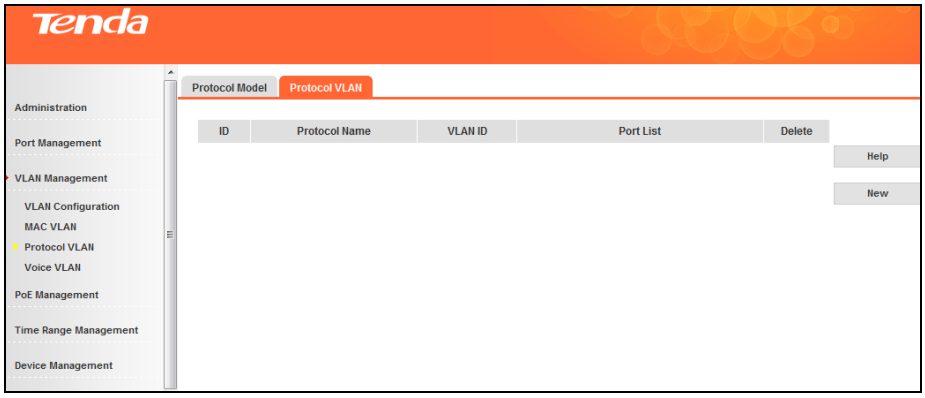
➢ Delete protocol model

Click the **Delete** button to delete the corresponding protocol model. If the protocol moel has been applied in protocol VLAN, this protocol model can't be deleted.



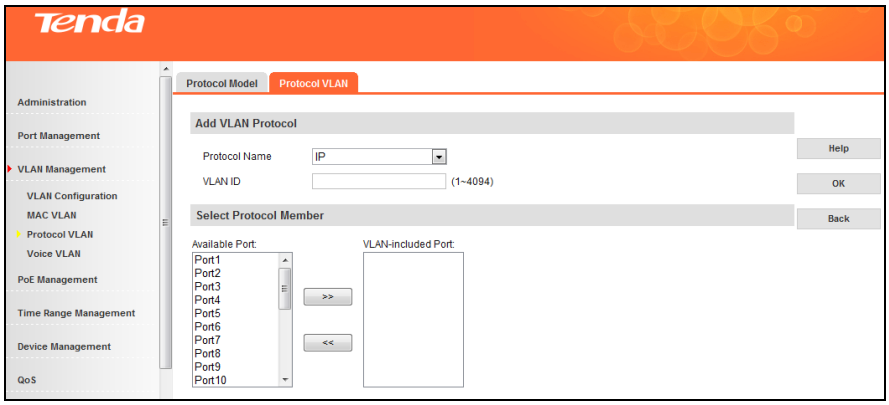
Protocol VLAN---Config

Click **VLAN Management -> Protocol VLAN ->Protocol VLAN** to enter interface below:



➢ Add protocol VLAN

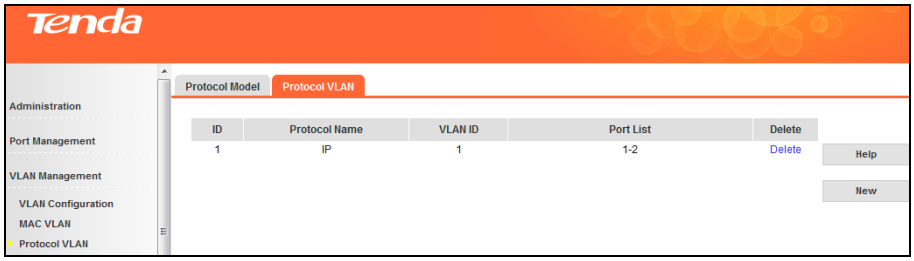
1. Click **New** to enter interface below:



2. Select protocol name from the pull-down list.
3. Enter VLAN ID. This VLAN ID must exist in 802.1Q VLAN already.
4. Click >> to move ports from **Available Port** to **VLAN-Included Port**.
5. Click **OK**.

➢ Delete protocol VLAN

Click **Delete** to delete corresponding protocol VLAN.



4.3.4 Voice VLAN

Voice VLAN Overview

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 and the port which has received the voice data flow will automatically join the voice VLAN. Thus, the voice-VLAN-tagged voice traffic of voice devices connected to this port can be transmitted and enjoys higher transmission priority. 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 Supporting Details on Different 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 phone varies, different ports need different supporting conditions. As for phones which can obtain IP address and voice VLAN ID automatically, supporting conditions on ports are described as below:

Voice VLAN Working Mode	Voice Traffic Type	Port Link Type
Auto	Tagged	Access: Not supported.
		Trunk: Supported, but the default VLAN of the connected port must already exist and can't be voice VLAN. And the default VLAN is allowed to pass on the connected port.
		Hybrid: Supported, but the default VLAN of the connected 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 connected port must already exist and can't be voice VLAN. And the default VLAN is allowed to pass on the connected port.
		Hybrid: Supported, but the default VLAN of the connected 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 connected port must be voice VLAN.
		Trunk: Supported, but the default VLAN of the

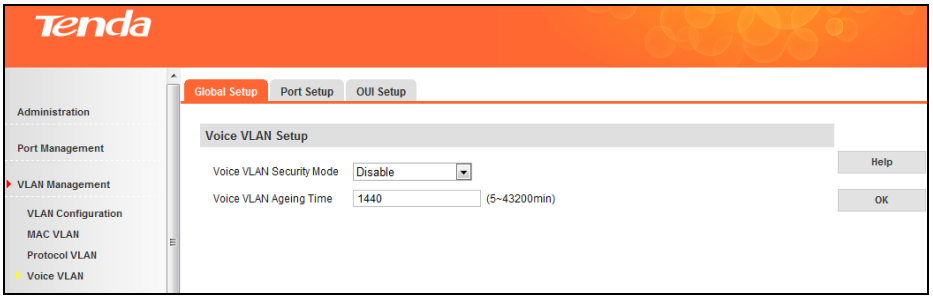
		connected port must be voice VLAN and voice VLAN is allowed to pass on the connected port.
		Hybrid: Supported, but the default VLAN of the connected port must be voice VLAN and exist in allowed untagged VLAN list.

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

Voice VLAN Mode	Port Type	Supporting Details
Auto	Access	Not supported.
	Trunk	Supported, but the default VLAN of the connected port must already exist and can't be voice VLAN. And the default VLAN is allowed to pass on the connected port.
	Hybrid	Supported, but the default VLAN of the connected 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 connected port must already exist and can't be voice VLAN. And the default VLAN is allowed to pass on the connected port.
	Hybrid	Supported, but the default VLAN of the connected port must already exist and can't be voice VLAN. And voice VLAN should be in the allowed tagged VLAN list.

Global Setup

Click **VLAN Management -> Voice VLAN -> Global Setup** to enter interface below:



➢ To configure voice VLAN setup:

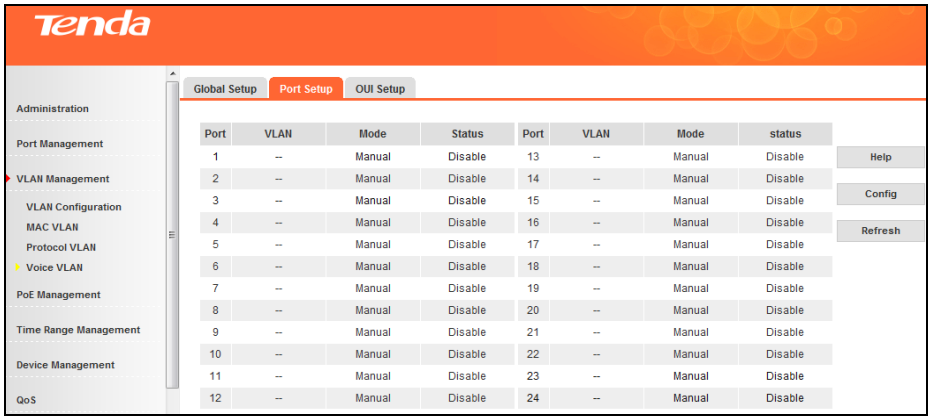
1. Select **Enable** or **Disable** from the pull-down list. Voice VLAN security mode is disabled by default.
2. From the **Voice VLAN Aging Time** field, specify the amount of time between 5 and 43200min. As for the port joining in voice VLAN under auto mode, if the system doesn't receive any voice message after ageing time, this port will be deleted from voice VLAN automatically. As for the port joining in voice VLAN under manual mode, you need to delete it manually.
3. Click **OK** to save your configurations.

Note----------

Only in 802.1Q VLAN mode, can you enable voice VLAN.

Port Setup

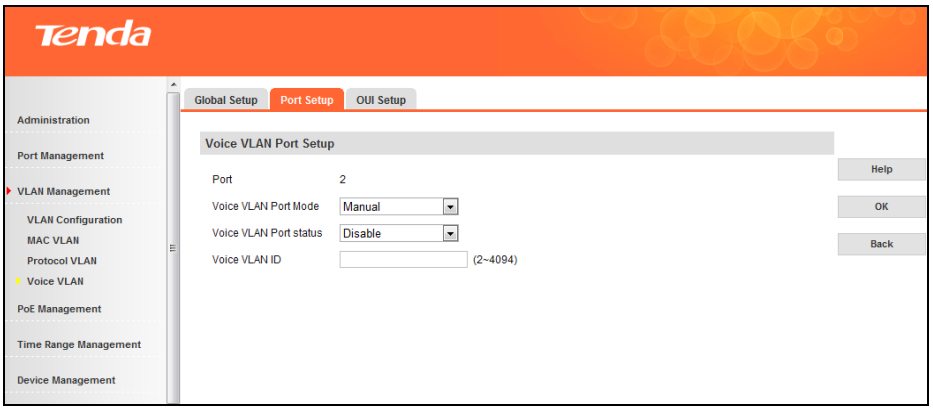
To display the Voice VLAN Port Setup page, click **VLAN Management ->Voice VLAN -> Port Setup**.



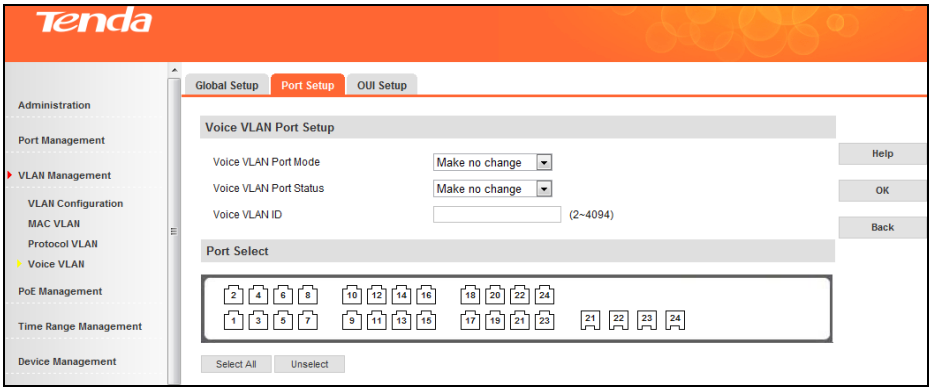
Fields on the screen are described below:

Field	Description
Port	Display port number.
VLAN	Display voice VLAN ID on corresponding port.
Mode	Display voice VLAN mode: auto or manual.
Status	Display voice VLAN status: Enable or Disable.

➢ To configure voice VLAN port setup on a single port, click the port you wish to on the port setup page:

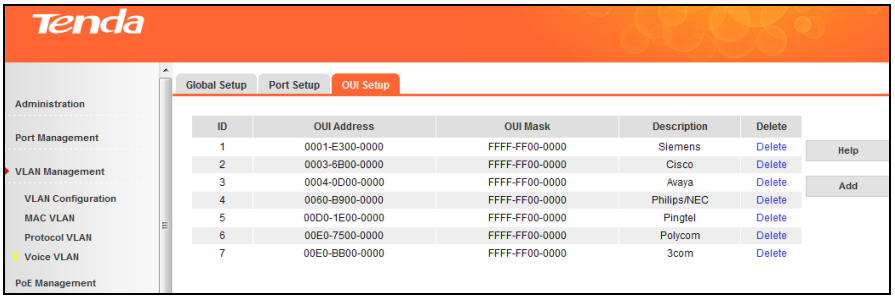


➢ To batch configure voice VLAN port setttings, click **Config** on the port setup page:



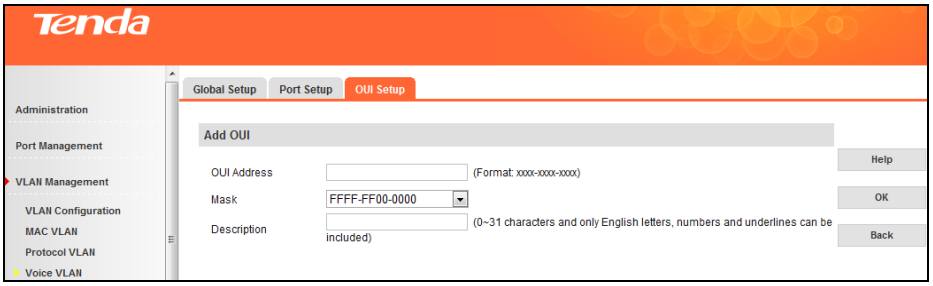
OUI Setup

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



➢ To configure OUI settings:

1. To add a new OUI address, click **Add** on the OUI Setup page.



Fields on the screen are described below:

Field	Description
OUI Address	Configures source MAC address (xxxx-xxxx-xxxx) sent by voice devices.
Mask	Click to select the prompted mask. The default is FFFF-FF00-0000, indicating the top 24 bits must match the OUI address and the last 24 bits are arbitrary.
Description	Description of OUI address, used for distinguishing different voice devices.

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

2. To delete an OUI address, click **Delete** on the OUI Setup page.

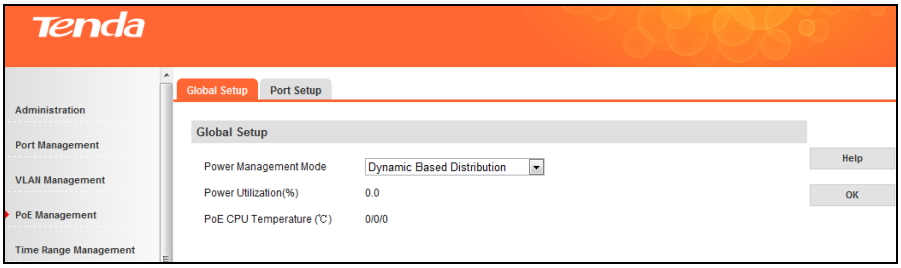
4.4 PoE Management

PoE Overview

Power over Ethernet or PoE describes any of several standardized or ad-hoc systems which pass electrical power along with data on Ethernet cabling. 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.

4.4.1 Global Setup

Click **PoE Management -> Global Setup** to enter interface below:

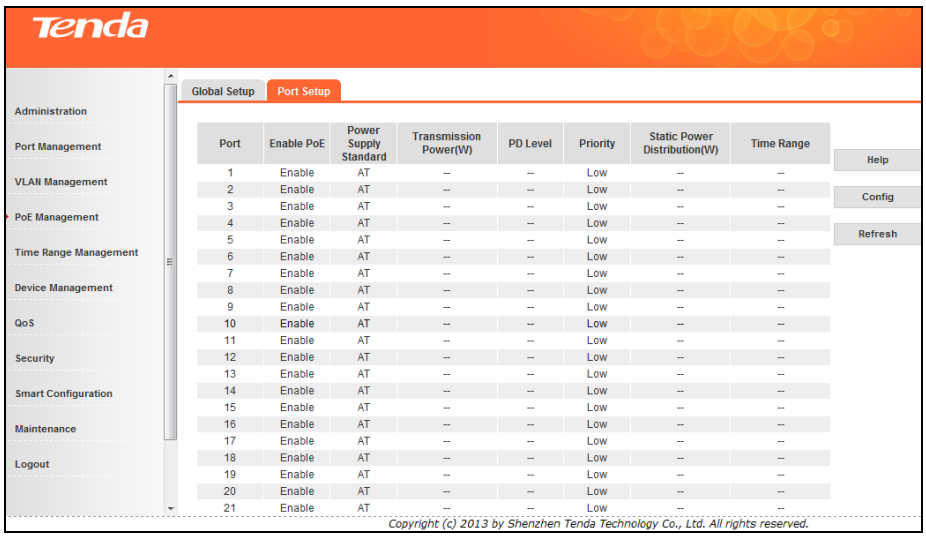


Fields on the screen are described below:

Field	Description
Power Management Mode	Configures PoE power management mode. When it is static, you can configure power allocation manually. When power supply is connected on the port, part of power will be enforced to be reserved for this port and can't be used by other ports. When it is dynamic, according to actual used power allocation, in full load, power will be allocated by port priority (priority + port number). If the priority is the same, the smaller the port number is, the higher the priority.
Power Utilization	Displays the current power utilization rate.
PoE CPU Temperature	Displays the three CPUs' temperature respectively.

4.4.2 Port Setup

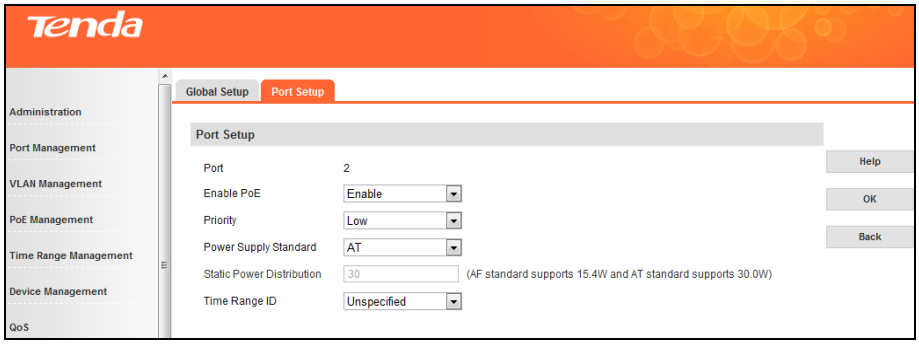
Click **PoE Management -> Port Setup** to enter interface below:



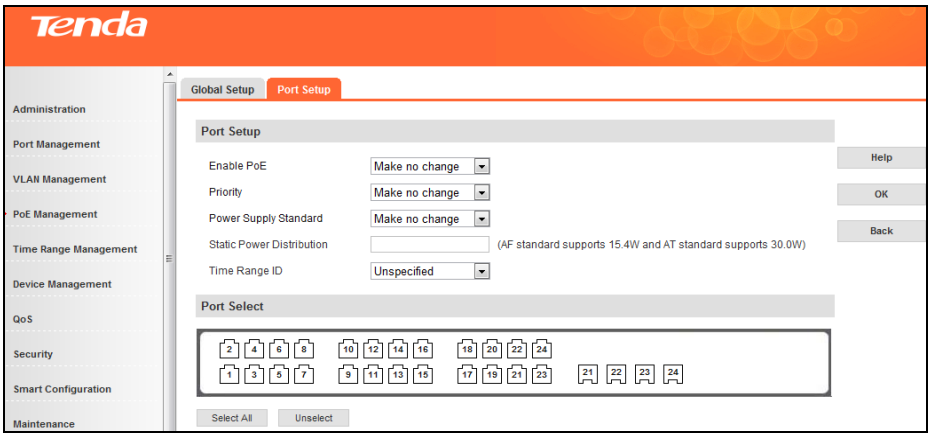
Fields on the screen are described below:

Field	Description
Enable PoE	Displays PoE is enabled or not.
Power Supply Standard	Displays the current PoE power standard (AT or AF).
Transmission Power	Displays PoE power.
PD Level	Displays PD level of the current connected port when power supply is normal. IEEE 802.3at: 0-4; IEEE 802.3af: 0-3.
Priority	This field is available only if dynamic allocation is selected. In static mode, it displays "--". Options available include High, Medium and Low. By default, this option is Low for all ports.
Static Power Distribution	This field is available for configuration if Static Power Distribution is selected from the power management mode pull-down list. In dynamic mode, it displays “--”. IEEE 802.3af: Enter a valid power value between 0-15.4w. If you enter a power value that is greater than 15.4w, 15.4w will be applied automatically. IEEE 802.3at: Enter a valid power value between 0-30w. If you enter a power value that is greater than 30, 30w will be applied automatically.
Time Range	Configures the current port's specified time range ID. Unspecified means no time limit.

➢ To configure PoE port setup on a single port, click the port you wish to on the PoE port setup page:



➢ To batch configure PoE port setup, click **Config** on the PoE port setup page to enter interface below:

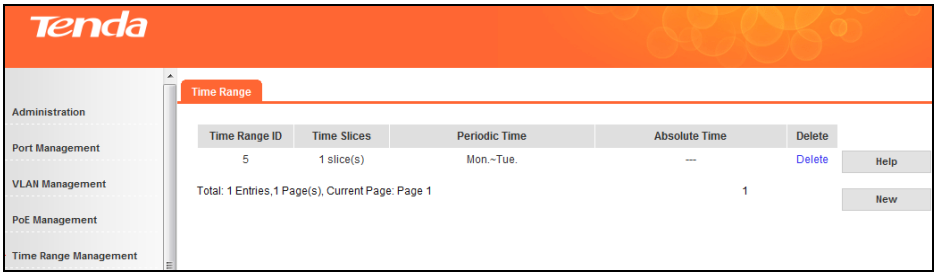


4.5 Time Range Management

If a configured ACL is needed to be effective in a specified time-range, a time-range should be firstly specified in the ACL. As the time-range based ACL takes effect only within the specified time-range, data packets can be filtered by differentiating the time-ranges. On this switch, absolute time and periodic time can be configured. Configure an absolute time section in the form of “beginning time to ending time” to make ACLs effective; configure a periodic time section to make ACLs effective on the fixed days of the week.

4.5.1 Time Range

Click **Time Range Management -> Time Range** to enter interface below:

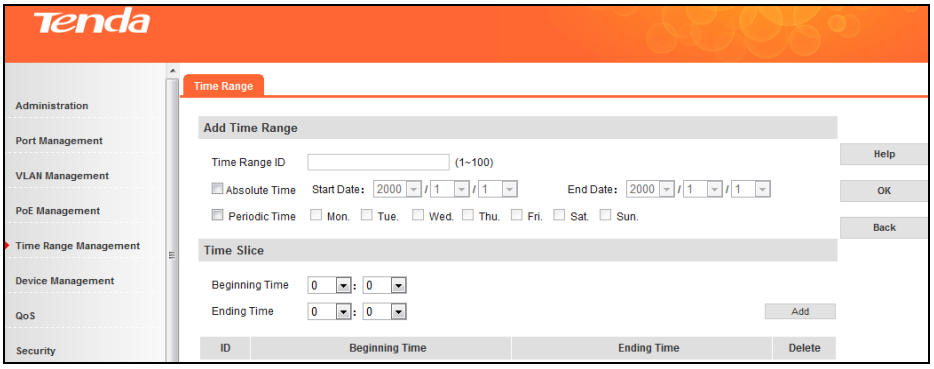


Fields on the screen are described below:

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

	display “--”.
Delete	Click to delete the corresponding time range.
New	Click to create a new time range.

➢ To create or modify time range, click **New** on the Time Range page to enter interface below:



Fields on the screen are described below:

Field	Description
Time Range ID	Displays corresponding time range ID.
Absolute Time	Configures this time range's absolute time (from 2000, January 1st to 2035, December 31th.).
Periodic Time	Configures this time range's periodic time (from Mon. to Sun.).
Add	Click to add a new time slice.
ID	Displays time slice ID (1~4).
Beginning Time	Displays time slice's starting time (00:00~23:59).
Ending Time	Displays time slice's ending time (00:00~23:59).
Delete	Click to delete the corresponding time slice.
Back	Click to go back to the Time Range page.

4.6 Device Management

4.6.1 MAC

MAC Forwarding Table Overview

An Ethernet device uses a MAC address table for forwarding frames through unicast instead of broadcast. This table describes from which port a MAC address (or host) can be reached. When forwarding a frame, the device first looks up the MAC address of the frame in the MAC address table for a match. If the switch does not find an entry, it broadcasts the frame. The MAC address table maintains a map of MAC addresses and corresponding forwarding ports for fast frame forwarding. A MAC address table entry includes the following information: destination MAC address, VLAN ID to which the port belongs and forwarding egress port number. MAC address length is 6 bytes. The format is XXXX-XXXX-XXXX and “X” is hexadecimal.

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

a) Unicast mode: If an entry is available for the destination MAC address, the device forwards the frame out of the outgoing port indicated by the MAC address table entry.

b) 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. Each time a dynamic MAC address entry is obtained or created, an aging timer starts. If the entry has not updated when the aging timer expires, the device deletes the entry. If the entry has updated before the aging timer expires, the aging timer restarts. This aging mechanism ensures that the MAC address table can quickly update to accommodate the latest network changes. (To config MAC age, click **Administration -> System Info -> MAC Age**).

Note----------

The MAC aging mechanism takes effect on dynamic MAC address entries only.

Types of MAC address table entries

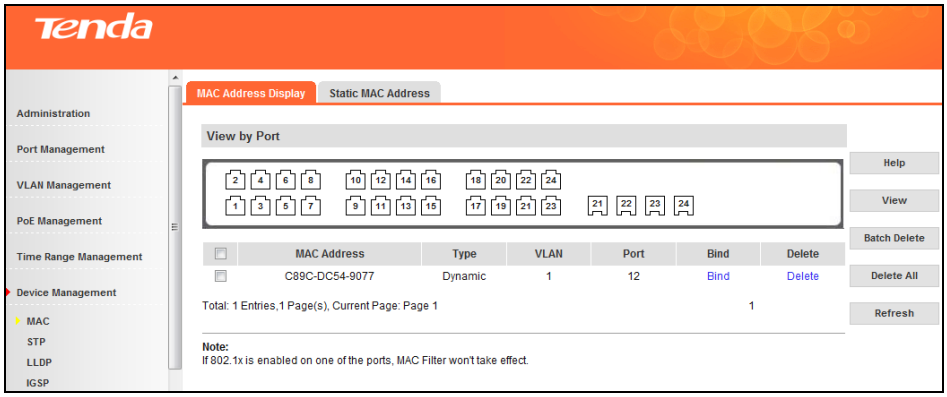
A MAC address table can contain the following types of MAC entries:

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

Configure MAC address table entries

To display MAC address entries globally

Click **Device Management -> MAC -> MAC Address Display** to enter interface below:

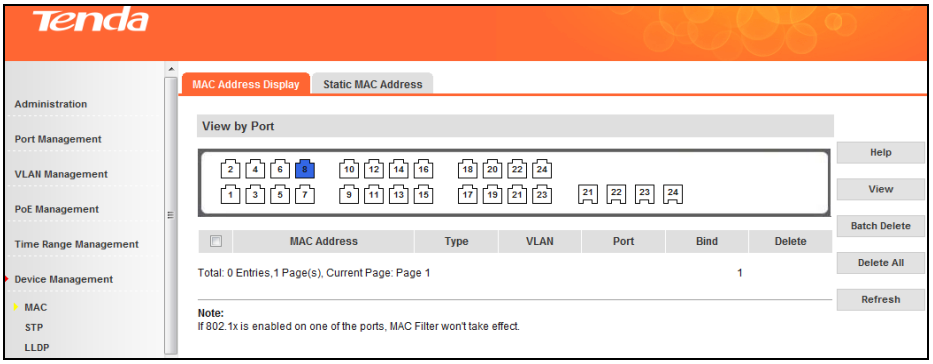


Note----------

The VLAN field displays "--" for port VLANs.

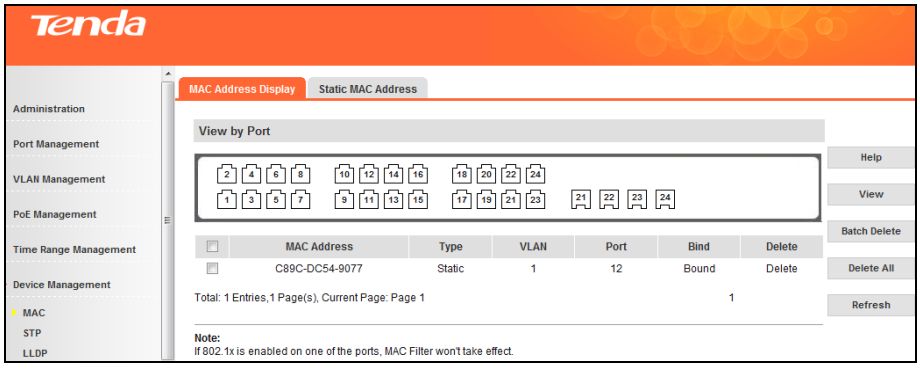
➢ **To display MAC address entries on a single port**

Click the corresponding port number, and all MAC address entries on it will be displayed.



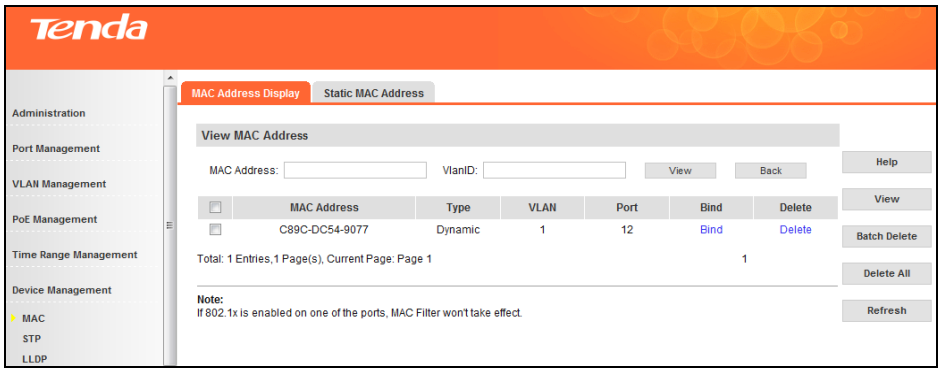
➢ Bind

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



➢ To view MAC address entry:

Click **View** and specify a MAC and a VLAN ID. (Note: To view MAC address entry, you must enter the MAC address while the VLAN ID is optional.)



➢ To delete a single MAC address

Click the **Delete** button next to the corresponding MAC address.

➢ To delete a batch of MAC address concurrently

Check corresponding check boxes and click **Batch Delete**.

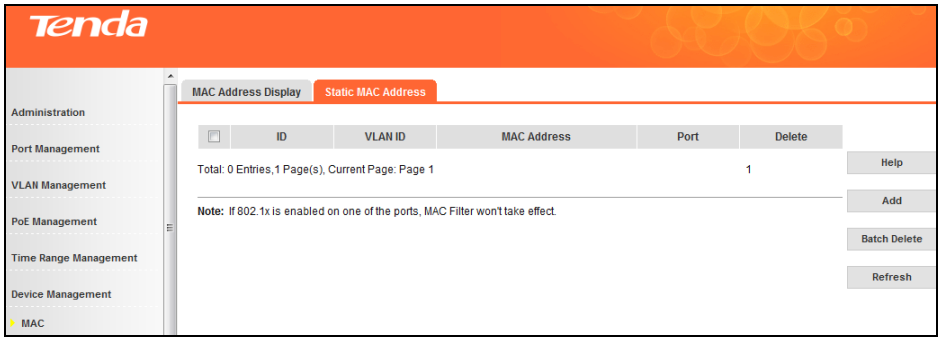
➢ To delete all MAC address entries, click **Delete All**.

Note----------

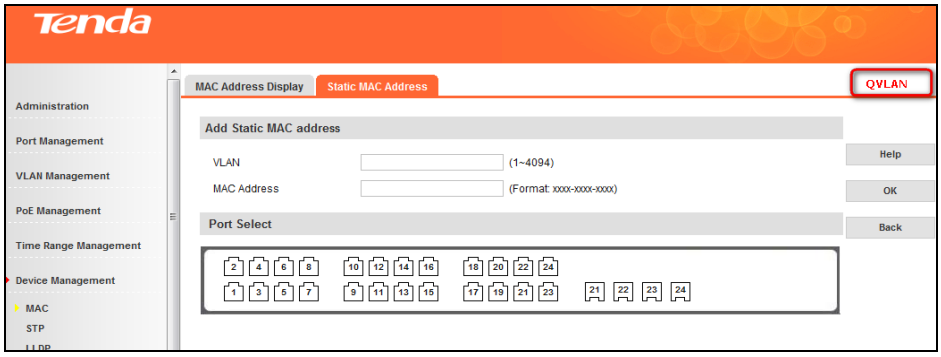
The **Delete All** and **Batch Delete** options do not take effect on bound MAC address entries.

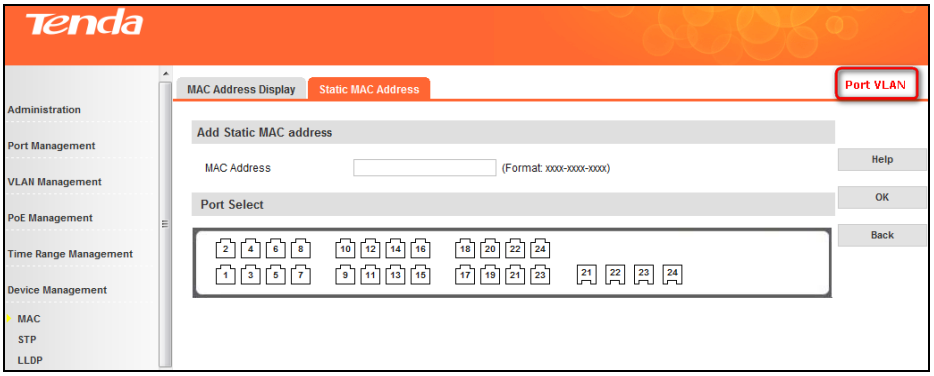
Static MAC Address

Click **Device Management -> MAC -> Static MAC Address** to enter interface below:



➢ To add a static MAC address entry, click **Add**, enter a MAC address and click **OK**. There is no VLAN field for you to specify in port VLAN mode.





- To delete a single MAC address, click the **Delete** button next to the corresponding MAC address.
- To delete a batch of MAC address concurrently, check corresponding check boxes and click **Batch Delete**.

Note----------

1. A certain interface's MAC address and VLAN ID can be bound to another interface.
2. The MAC address in the Static Address Table can not be added to the Filtering Address Table.
3. Once VLAN mode is toggled, all current settings will be cleared.
4. A certain interface in the static MAC address table can receive packets whose source MAC address matches its corresponding VID; Packets whose destination MAC address matches the corresponding VID can only be forwarded to the corresponding interface.

4.6.2 STP

STP Overview

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. On Ethernet, only a single active path at a time can be maintained between any two network nodes to avoid broadcast storm. However, spare (redundant) links are indispensable to ensure reliability. Spanning tree 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, and disable those that are not part of the spanning tree, leaving a single active path between any two network nodes. This is accomplished in the STP. A STP-enabled switch can perform the following tasks:

1. Discover and generate an optimum STP topology.
2. Discover and repair failures on the network; automatically update the network topology for future use. Local topology is generated by computing bridge configurations made by a network administrator. Thus, if configured properly, an optimum topology tree can be generated.

RSTP Overview

RSTP (Rapid Spanning Tree Protocol) provides significantly faster spanning tree convergence after a topology changes, introducing new convergence behaviors and bridge port roles to do this. RSTP is designed to be backwards-compatible with standard STP. RSTP is typically able to respond to changes within one second while STP can take 30 to 50 seconds to respond to a topology change.

RSTP delivers fast transition to forwarding status without relying on timer settings. A RSTP bridge is

responsive to other RSTP bridge's link status. The port does not need to wait for the topology to become stable. Edge port and P2P port are introduced to the protocol for faster transition. The explanation of an Edge port and a P2P port is shown below:

- 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 a single workstation. 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.

- 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. The three protocols are mutually compatible and no conflicts or network collapses will be caused in spanning tree application.

MSTP Overview

MSTP divides a network into several MST regions. The CST is generated between these MST regions, and multiple spanning trees can be generated in each MST region. Each spanning tree is called an instance. As well as STP, MSTP uses BPDUs to generate spanning tree. The only difference is that the BPDU for MSTP carries the MSTP configuration information on the switches. MSTP allows formation of MST regions that can run multiple MST instances (MSTI). Multiple regions and other STP bridges are interconnected using one single common spanning tree (CST). Unlike some proprietary per-VLAN spanning tree implementations, MSTP includes all of its spanning tree information in a single BPDU format. Not only does this reduce the number of BPDUs required on a LAN to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP. MSTP does this by encoding additional region information after the standard RSTP BPDU as well as a number of MSTI messages (from 0 to 64 instances, although in practice many bridges support fewer). Each of these MSTI configuration messages conveys the spanning tree information for each instance. Each instance can be assigned a number of configured VLANs and frames (packets) assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. In order to avoid conveying the entire VLAN to spanning tree mapping in each BPDU, bridges encode an MD5 digest of their VLAN to instance table in the MSTP BPDU. This digest is then used by other MSTP bridges, along with other administratively configured values, to determine if the neighboring bridge is in the same MST region as itself.

MSTP packets are as follow:

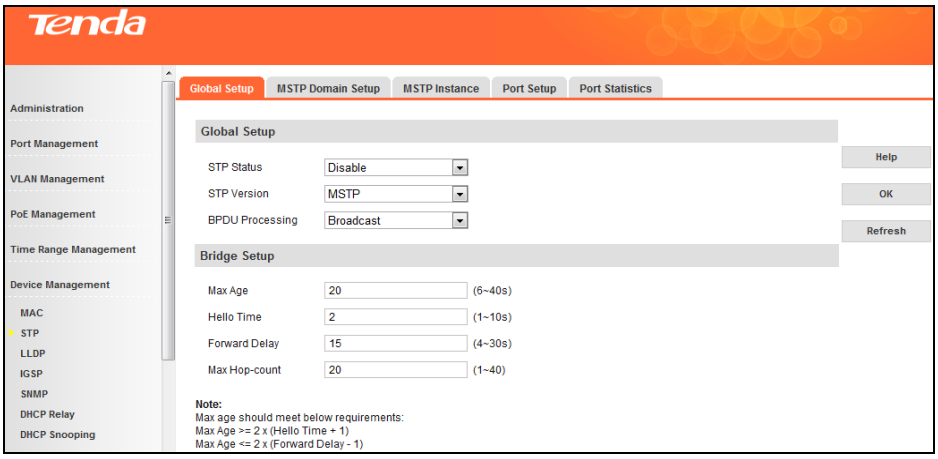
	Octet
Protocol Identifier	1–2
Protocol Version Identifier	3
BPDU Type	4
CIST Flags	5
CIST Root Identifier	6–13
CIST External Path Cost	14–17
CIST Regional Root Identifier	18–25
CIST Port Identifier	26–27
Message Age	28–29
Max Age	30–31
Hello Time	32–33
Forward Delay	34–35
Version 1 Length = 0	36
Version 3 Length	37–38
MST Configuration Identifier	39–89
CIST Internal Root Path Cost	90–93
CIST Bridge Identifier	94–101
CIST Remaining Hops	102
MSTI Configuration Messages (may be absent)	103–*39 + Version 3 Length*

Figure 14-1—MST BPDU parameters and format

Octet 39-89 for MST Configuration Identifier

Global Setup

Click **Device Management -> STP -> Global Setup** to enter interface below:



Fields on the screen are described below:

Field	Description
STP Status	Enable/Disable STP globally. By default, the STP feature is disabled.
STP Version	Select the desired version of STP version: MSTP/RSTP/STP compatible to eliminate loops on data link layer. The default is RSTP mode.

BPDU Processing	Select a BPDU processing method: Broadcast/Filter. This option takes effect only if STP is disabled globally. By default, BPDU packets are broadcasted.
Max Age	Config a max aging time for messages. You may choose a time between 6 and 40 seconds. The default value is 20s.
Hello Time	Config the Hello Time. You may choose a time between 1 and 10 seconds. The default value is 2s.
Forward Delay	The latency time for a bridge port to switch from a Listening state to a Learning state or from a Learning state to a Forwarding state. Valid values range from 4 to 30 seconds. The default is 15s.
Max Hop-count	Config max hop-count. In MSTP mode, it decreases by 1 upon every switch. If the received BPDU hop value is 1, this packet will be discarded.

Note----------

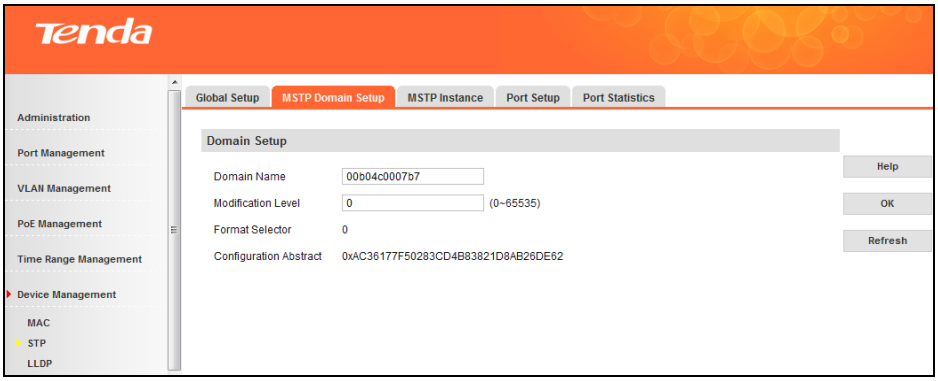
Max Age should meet below requirements:

Max Age >= 2 x (Hello Time + 1);

Max Age <= 2 x (Forward Delay - 1).

MSTP Domain Setup

Click **Device Management -> STP -> MSTP Domain Setup** to enter interface below:



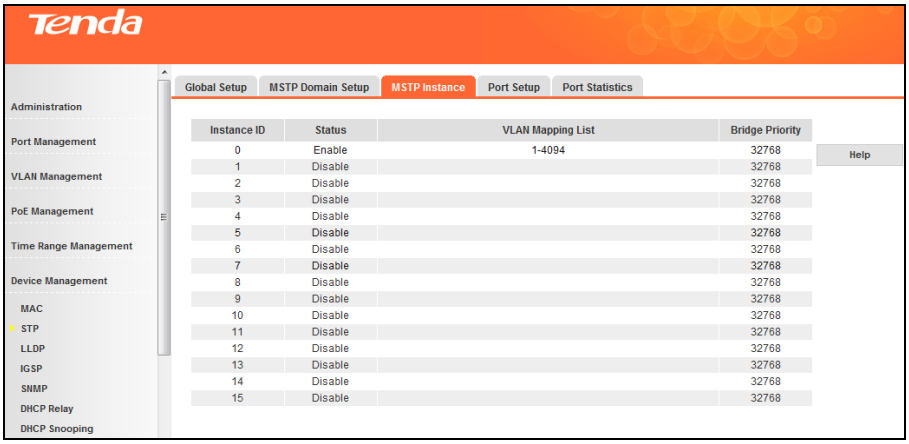
Fields on the screen are described below:

Field	Description
Domain Name	Config switch domain name (32 characters allowed). The default is the device's MAC address.

Modification Level	Config MSTP modification level. Valid range is 0-65535. The default is 0.
Format Selector	Display 0.
Configuration Abstract	A value worked out by VLAN mapping, belonging to an important parameter of the inter-domain calculation.

MSTP Instance

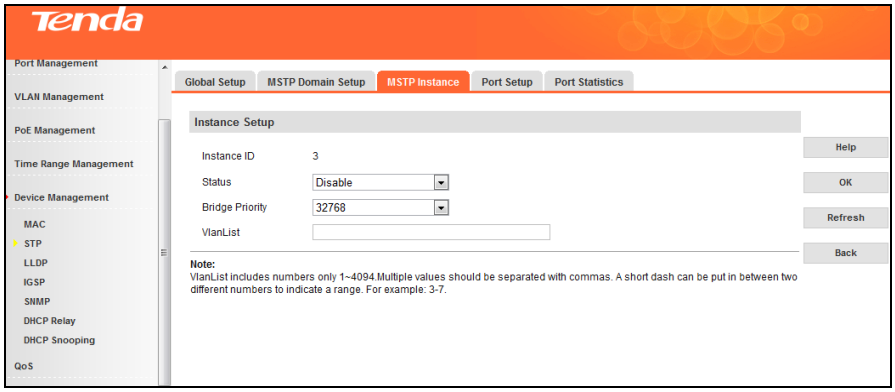
Click **Device Management -> STP -> MSTP Instance** to enter interface below:



Fields on the screen are described below:

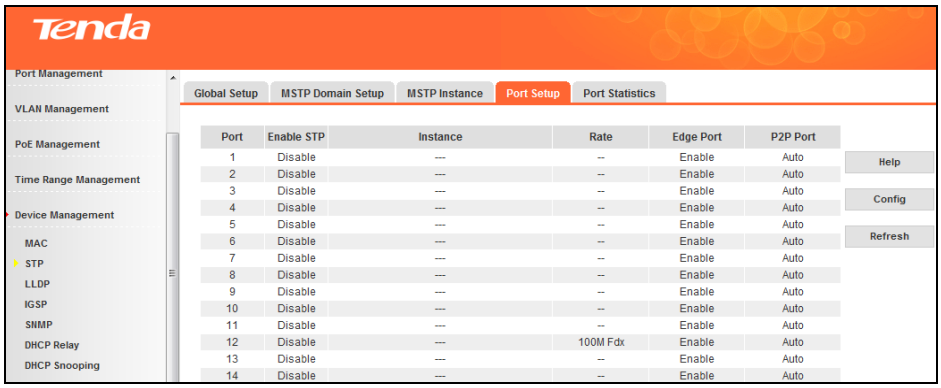
Field	Description
Instance ID	Instance ID: 0-15. 0: the inter-domain spanning tree.
Status	Enable/Disable the corresponding selected instance. Only instance 0 is enabled by default and can't be disabled.
VLAN Mapping List	Display instance's current mapping VLANs.
Bridge Priority	Display instance's current bridge priority.

To configure a single instance, click the corresponding instance to enter interface below:

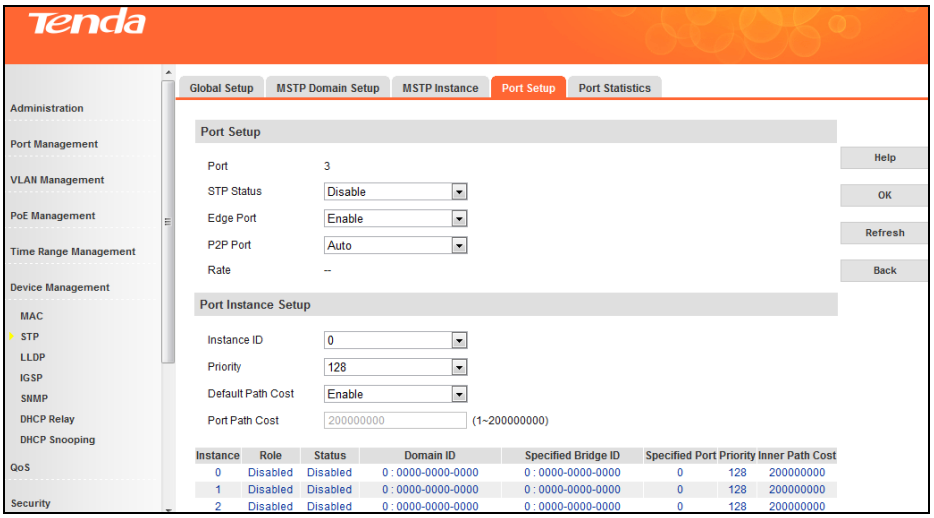


Port Setup

To configure STP port settings, click **Device Management -> STP -> Port Setup**.



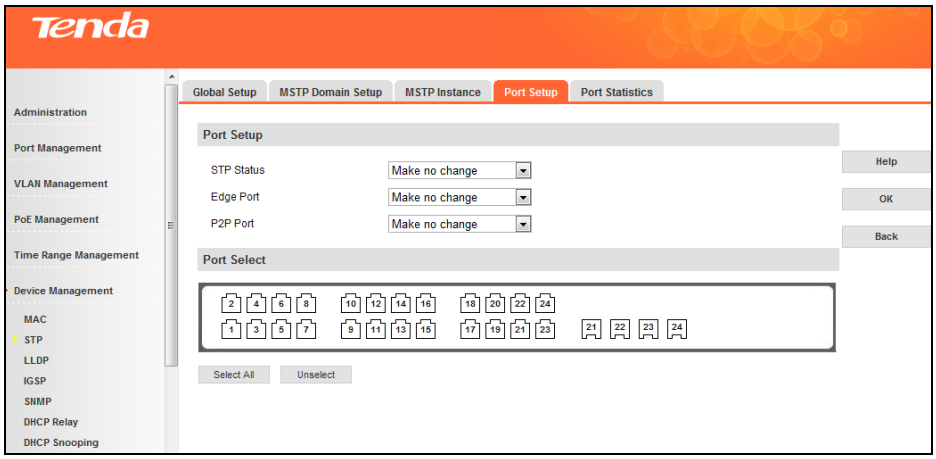
To config STP settings on a single port, click the corresponding port as seen below:



Fields on the screen are described below:

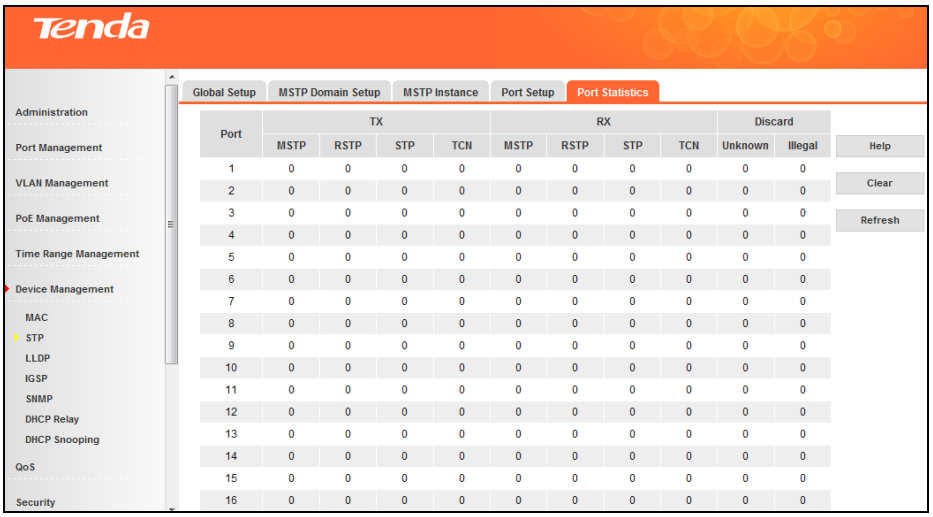
Field	Description
STP Status	Select to enable/disable the STP feature or make no change. By default, the STP feature is disabled. To activate the STP feature, you must enable STP both globally on the entire device and specifically on desired port(s).
Edge Port	An edge port is a port that is connected 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 normal spanning tree port. By default, all ports are edge ports.
P2P Port	A P2P port is also capable of rapid transition. Under RSTP/MSTP, all ports operating in full-duplex mode are considered to be P2P ports. By default, port establishes a link automatically.
Instance ID	Configure port parameters under different instances.
Priority	By default, the port priority is set to 128.
Default Path Cost	Enable/disable port default path cost. You can specify a custom 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 802.1at is supported.
Port Path Cost	The default path cost is 200,000,000. Only if you disable the default path cost option, can path cost be configurable.

To config STP settings on a batch of ports concurrently, click **Config** as seen below:



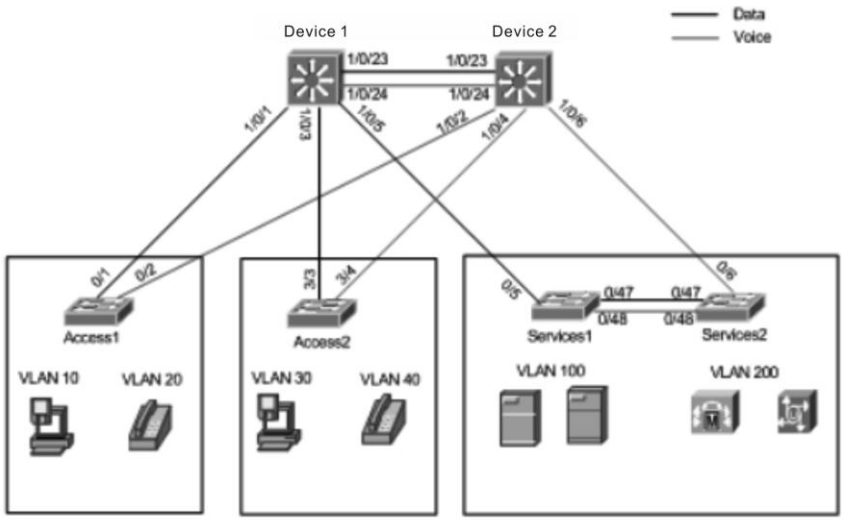
Port Statistics

To display STP port statistic info, click **Device Management -> STP -> Port Statistics**.



Application Example of MST

Typical application structure overview



As the topology shown above, Device 1 and Device 2 belong to the same domain (the same domain name, the same modification level and the same instance mapping). Set VLAN 10, 30, 100 to map instance 1 and set Device 1 as the root bridge of instance 1; Set VLAN 20, 40, 200 to map instance 2 and set Device 2 as the root bridge of instance 2. In this way, it is possible to make better use of the alternate paths available by using MSTP for different VLANs or groups of VLANs and realize the load balance.

Data Schema

Config Item	Data	Description
VLAN	Config switches according to allowed VLANs	Implemented by configuring VLAN and port VLAN

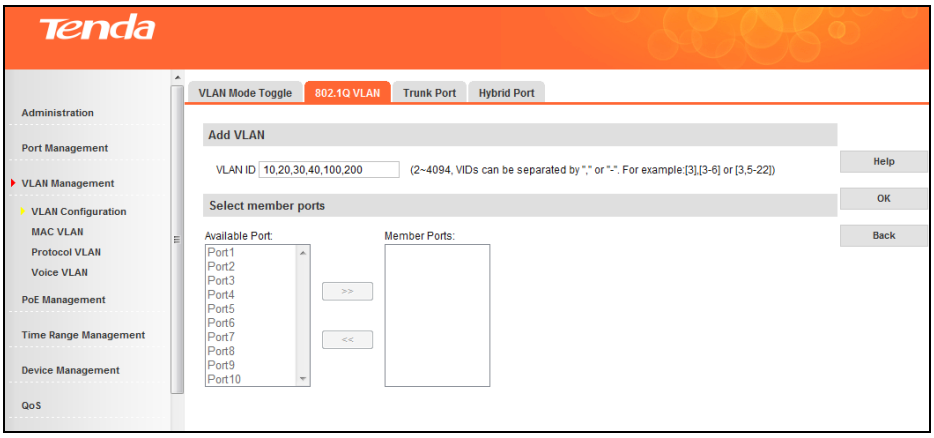
MSTP	Create instances 1-4, add instance mapping and configure instance priority	32 instances can be configured on this switch and instance ID range is 1-4094

Configuration Procedure

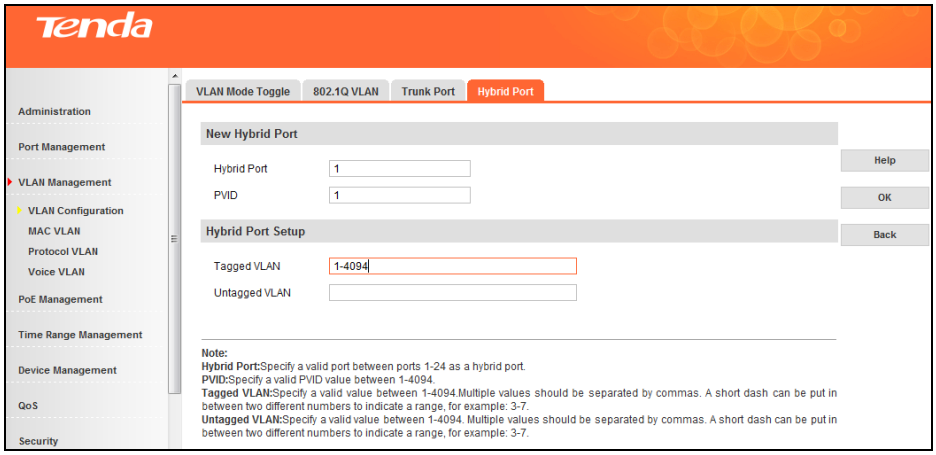
Start ⇨ VLAN Configuration ⇨ MSTP Configuration ⇨ Save configurations

Steps:

1. Add vlan10, 20, 30, 40, 100, 200;

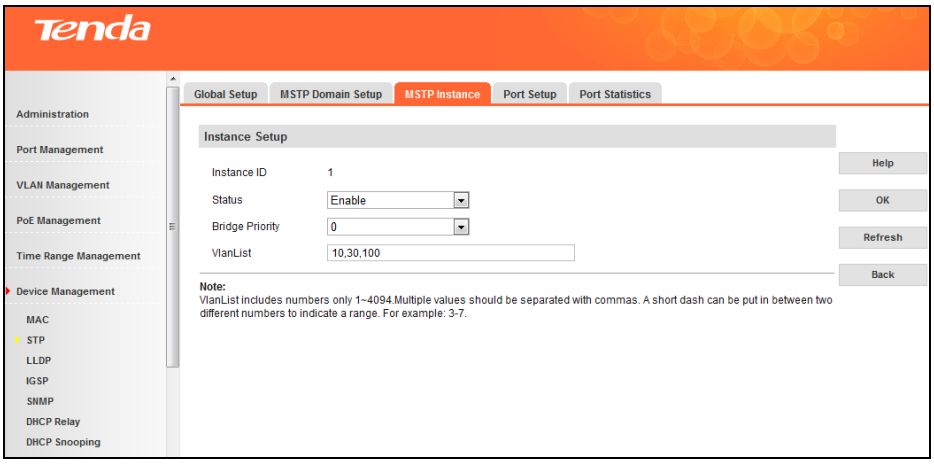


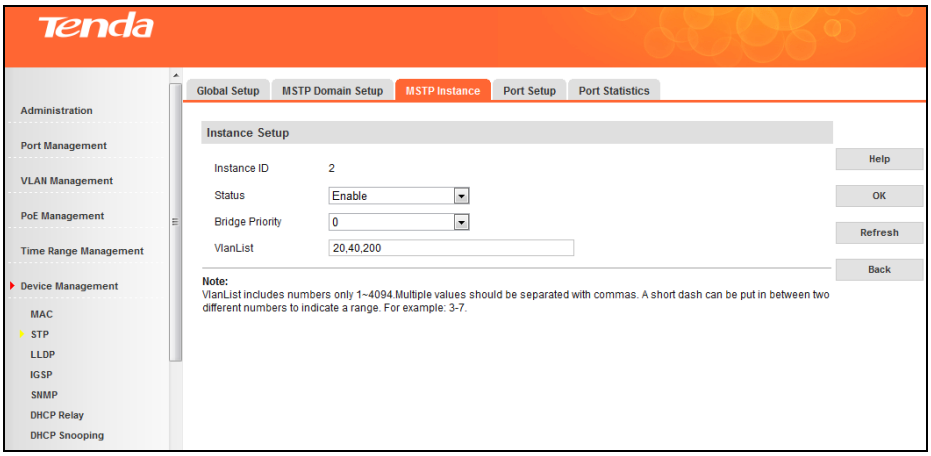
2. Set ports on Device 1 and Device 2 to Hybrid and Tagged;



3. Set Device 1 and Device 2's domain name to TEG3224P, set modification level to the default 0 and configure mapping between instances and VLANs: instance 1 maps VLAN 10, 30, 100; instance 2 maps VLAN 20, 40, 200;
4. Set Device 1's Bridge Priority to 0 and Device 2's Bridge Priority to 0, and then click **OK** to save

your configurations. In this way, packets of different VLANs can be forwarded via different instances.





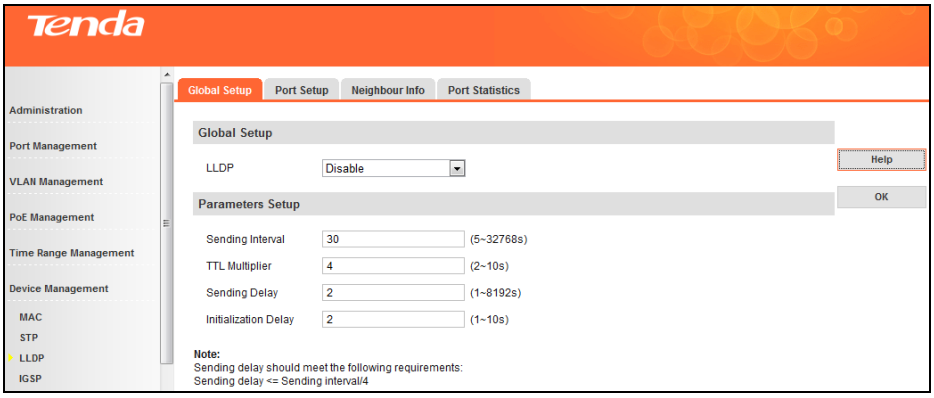
4.6.3 LLDP

LLDP Overview

LLDP (Link Layer Discovery Protocol) is a Layer 2 protocol that is used for network devices to advertise their own device information periodically to neighbors on the same IEEE 802 local area network. The advertised information, including details such as device identification, capabilities and configuration settings, is represented in TLV (Type/Length/Value) format according to the IEEE 802.1ab standard, and these TLVs are encapsulated in LLDPDU (Link Layer Discovery Protocol Data Unit). The LLDPDU distributed via LLDP is stored by its recipients in a standard MIB (Management Information Base), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

Global Setup

Click **Device Management -> LLDP -> Global Setup** to enter interface below:

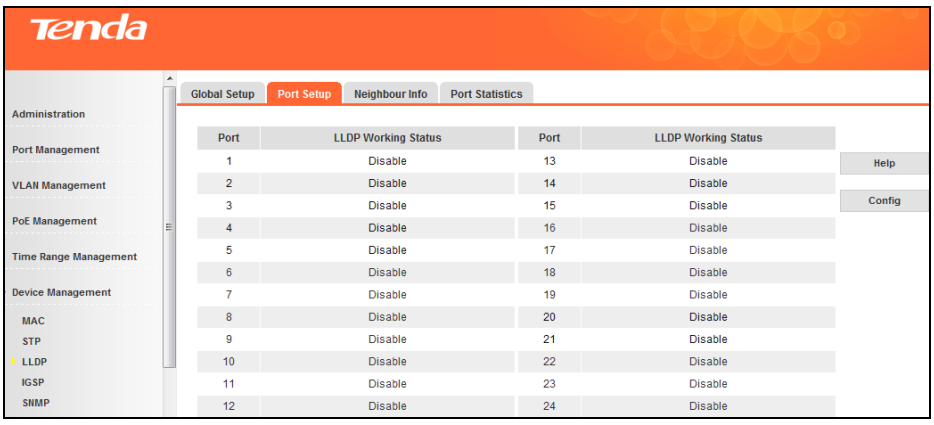


Fields on the screen are described below:

Field	Description
LLDP	Enable/ Disable LLDP feature.
Sending Interval	The interval among each LLDP message (5~32768s).
TTL Multiplier	TTL value is used to configure neighbor info's age time on local devices. TTL = Min (65535, (TTL multiplier × LLDP packet sending time interval)). Through adjusting TTL multiplier, you can control this device info's age time on the neighboring device (2~10s).
Sending Delay	When local configurations change, each LLDP packet will be sent after one sending delay time (1~8192s and <= sending time interval/4).
Initialization Delay	To avoid constant port initialization caused by frequent changes of working mode, you can configure port initialization delay time. When port's working mode changes, the initialization will be delayed for some time (1~10s).

Port Setup

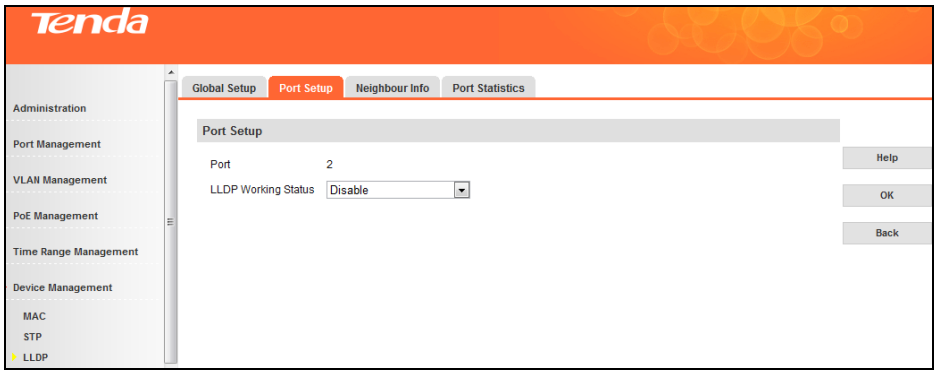
Click **Device Management -> LLDP -> Port Setup** to enter interface below:



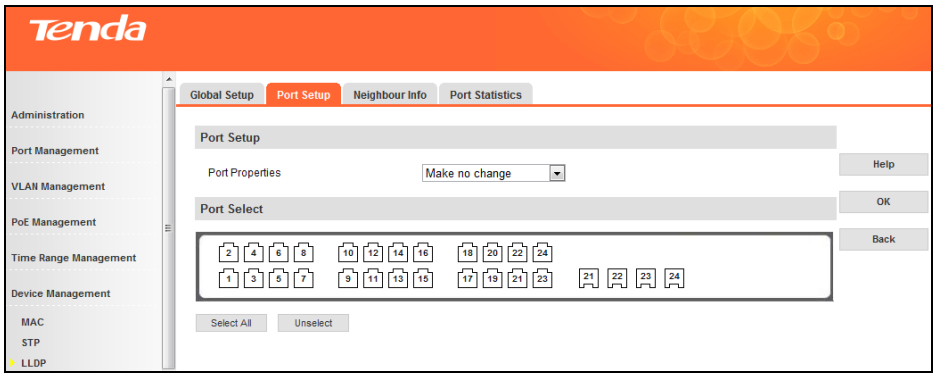
Fields on the screen are described below:

Field	Description
Port	Displays corresponding port numbers.
LLDP Working Status	Displays LLDP working status: Disable, TX, RX or TX & RX.
Config	Click **Config** to go to LLDP Batch Ports Setup page.

To config LLDP settings on a single port, click the corresponding port as seen below:



To config LLDP settings on a batch of ports concurrently, click **Config** as seen below:

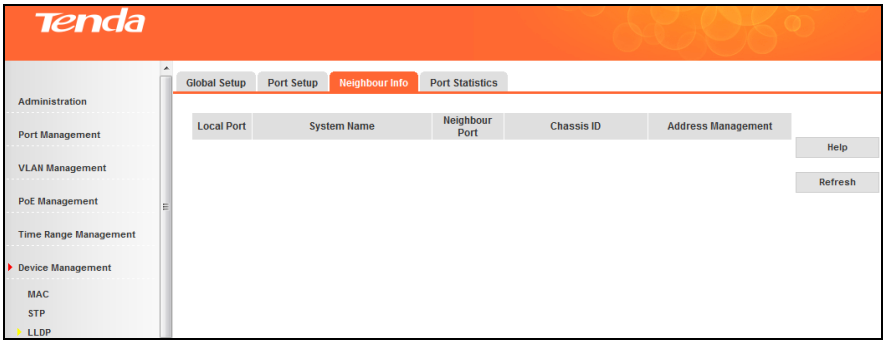


Fields on the screen are described below:

Field	Description
Port Properties	Select LLDP working status: Disable, Send Only, Receive Only, Transmit or make no change: Make no change: Make no change toward previous configurations. Disable: Disable LLDP feature. TX: Transmit LLDP packet only. RX: Receive LLDP packet only. TX & RX: Transmit and receive LLDP packet.
Port Select	Select the port you wish to configure on the panel.
Select All	Select all ports.
Unselect	Unselect all ports.

Neighbor Info

To display neighbor info, click **Device Management -> LLDP -> Neighbor Info**.

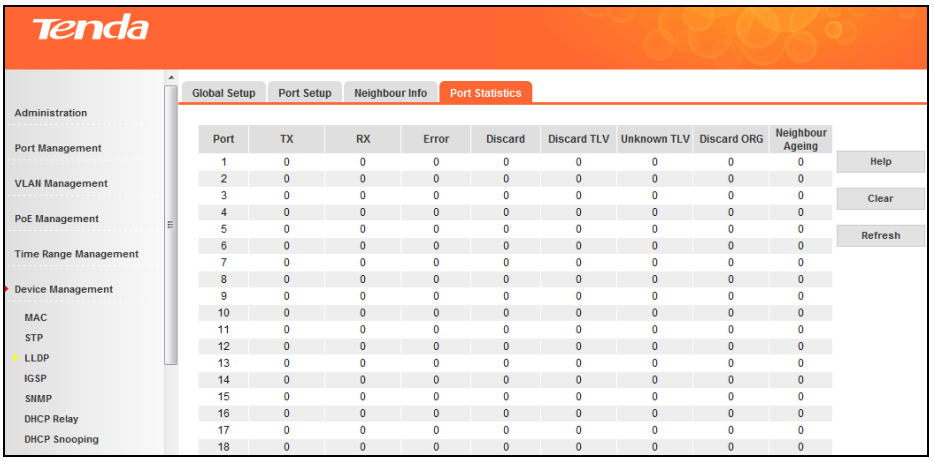


Fields on the screen are described below:

Field	Description
Local Port	Display the port which receives LLDP packet.
System Name	Display the neighboring device's system name.
Neighbor Port	Display the port which sends LLDP packets on the neighboring device.
Chassis ID	Display the MAC address of the neighboring device.
Address Management	Display the management IP address of the neighboring device.

Port Statistics

Click **Device Management -> LLDP -> Port Statistics** to enter interface below:



4.6.4 IGSP

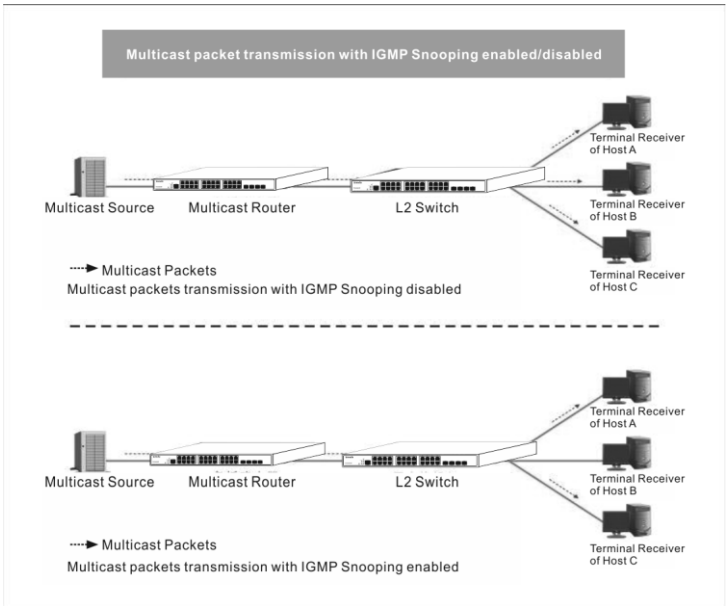
Overview

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. IGMP snooping, as implied by the name, is a feature that allows a network switch to listen to on the IGMP

conversation between hosts and routers.

Principle of IGMP snooping

By listening to the conversations between hosts and routers, the switch maintains a map of links which need IP multicast streams. Multicast streams may be filtered from the links which do not solicit them. 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 enabled, known multicast traffic will be forwarded to hosts that have explicitly joined the group. It provides switches with a mechanism to prune multicast traffic from links that do not contain a multicast listener (an IGMP client). Multicast packet transmission with IGMP Snooping enabled/disabled:



How IGMP Snooping Works

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

When receiving a general query

The IGMP querier periodically sends IGMP general queries to all hosts and routers on the local subnet to determine which active 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 (resets/enables the age timer).

When receiving a membership report

A host sends an IGMP membership report to the multicast router in the following circumstances:

After receiving an IGMP query, a multicast group member host responds with an IGMP membership report.

When intended to join a multicast group, a host sends 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 (resets/enables the age timer). A switch does not forward an IGMP membership report through a non-router port.

When receiving a leave message

When an IGMPv1 host leaves a multicast group, the host does not send an IGMP leave message, so the switch cannot know immediately that the host has left the multicast group. However, as the aging timer on

the member port that corresponds to the host 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 leave message to the multicast router to inform of such leave.

When receiving an IGMP leave 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 (the port that received the IGMP leave message) 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.

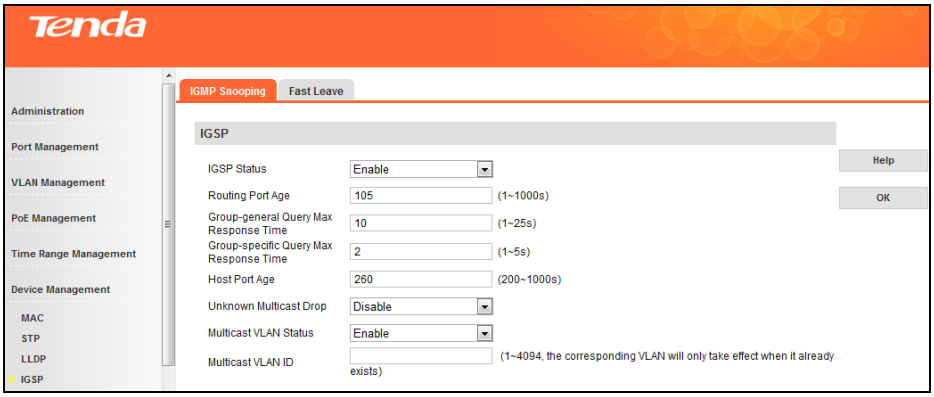
After receiving the IGMP leave message from a host, the IGMP querier resolves the multicast group address in the message and sends an IGMP group-specific query to that multicast group through the port that received the leave message. After receiving the IGMP group-specific query, the switch forwards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

The switch also performs the following actions on the port that received the IGMP leave message: If the port receives any IGMP membership report in response to the group-specific query before the aging timer expires, the switch considers that some host attached to the port is receiving or expecting to receive multicast data from that multicast group and 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, the switch considers that no hosts attached to the port are still members of that multicast group address and thus removes the multicast forwarding entry that the port corresponds to from the forwarding table when the aging timer expires.

IGMP Snooping

To config IGMP Snooping settings, click **Device Management -> IGSP -> IGMP Snooping**.



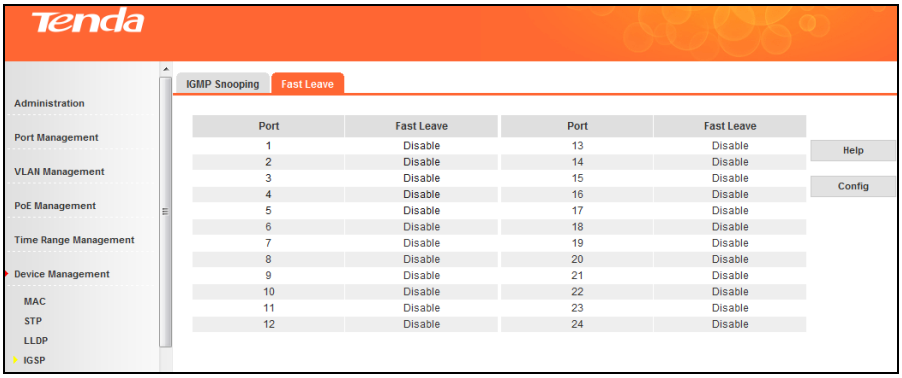
Fields on the screen are described below:

Field	Description
IGSP Status	Enable/disable the IGMP Snooping feature.
Routing Port Age	Config routing port aging time (1-1000 sec). The default is 105s.

Group-general Query Max Response Time	Config max amount of time in response to group-general query messages (1-25 sec). The default is 10s.
Group-specific Query Max Response Time	Config max amount of time in response to group-specific query messages (1-5 sec). The default is 2s.
Host Port Age	Config host port aging time (200-1000 sec). The default is 260s.
Unknown Multicast Drop	Enable/disable the unregistered multicast discard feature. This feature takes effect only if the IGSP feature has been enabled globally on the device.
Multicast VLAN Status	Enable/Disable multicast VLAN. When multicast VLAN is enabled, multicast VLAN ID becomes configurable and multicast packets can only be forwarded in this VLAN.
Multicast VLAN ID	This option becomes visible when multicast VLAN is enabled. This VLAN ID must already exist in 802.1Q VLAN and only ports in this VLAN can forward multicast packets. Valid range is 1-4094.

Fast Leave

To config Fast Leave settings, click **Device Management -> IGSP -> Fast Leave**.



- To config a single port: click it, select **Enable/Disable** and click **OK**.
- To config a batch of ports concurrently: click **Config**, specify required parameters and click **OK**.

4.6.5 SNMP

SNMP Overview

Simple Network Management Protocol (SNMP) 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 Work Mechanism

The SNMP framework comprises NMS and Agent:

NMS—Network Management Station NMS, is a station that runs the SNMP client software to monitor and manage the SNMP-capable devices in the network.

SNMP agent—Works on a managed network device (such a switch) to receive and handle requests from the NMS, and send traps to the NMS when some events occur.

Upon receiving GetRequest, GetNextRequest and SetRequest packets from NMS, the SNMP agent will perform Read or Write operation on managed objects depending on the type of packets received and generate Response packets to return to NMS.

SNMP Version

The device supports SNMPv3 and is compatible with SNMPv1 and SNMPv2c.

SNMPv3 adopts user name and password authentication mode.

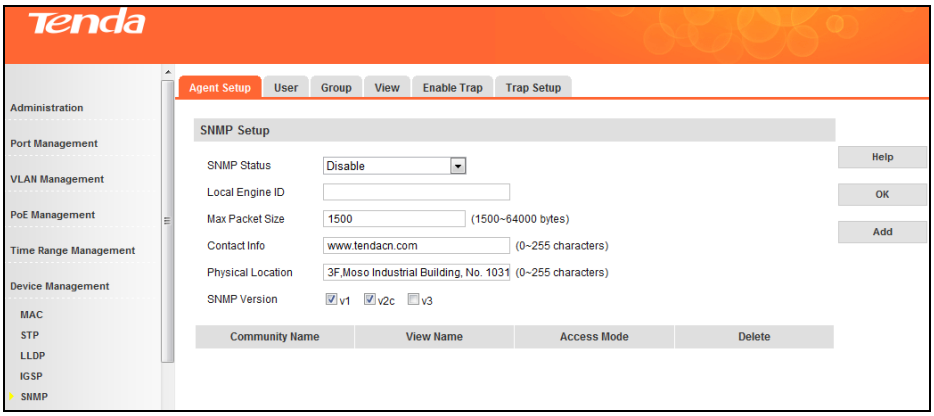
The switch supports SNMPv1 and SNMPv2c, both of which use community names for authentication. SNMP packets with community names that did not pass the authentication on the device will simply be discarded. The SNMP community name defines the relationship between an SNMP NMS and an SNMP Agent. A community name plays a similar role as a key/password and can be used to regulate access from NMS to Agent.

Trap

Traps are messages that alert network personnel of events that occur on the switch. The events can be as serious as a reboot (someone accidentally turns off the Switch), or less serious like a port status change. The switch generates traps and sends them to the trap recipient (or network manager).

Agent Setup

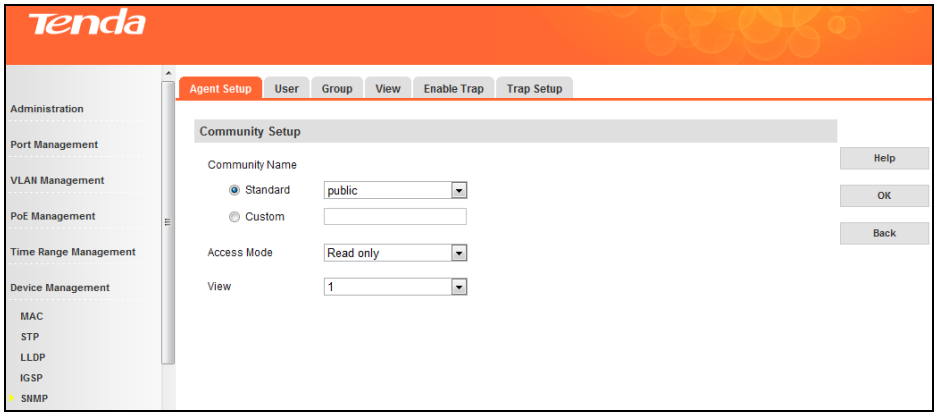
To enter below screen, click **Device Management -> SNMP -> Agent Setup**.



➢ To enable SNMP

1. Select **Enable** from the **SNMP Status** drop-down list.
2. You will see the Local Engine ID after enabling SNMP. This field is not configurable.

3. Specify a **Max Packet Size** value, the default is 1500.
4. Configure contact info. The default is www.Tendacn.com.
5. Here you can specify device's physical location.
6. SNMP Version: Select V1, V2c or V3.
7. Click **Add** to create a community name as seen below:



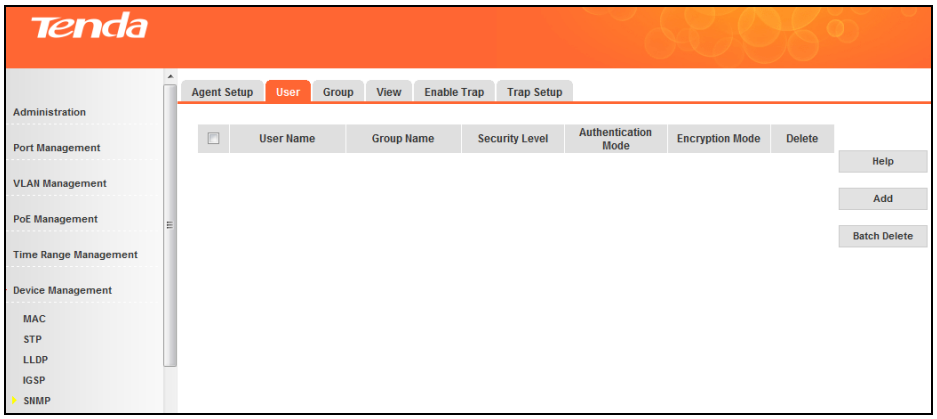
Note: You must create a view before you can create a community.

8. Community Name: Click **Standard** and select **public** or **private**; click **Custom** and enter a community name of up to 31 characters.
9. Access Right: Select **Read only** or **Read & Write**.
10. Click **OK**.

Now you can use the V1, or V2c community name to view or config settings of nodes in the MIB.

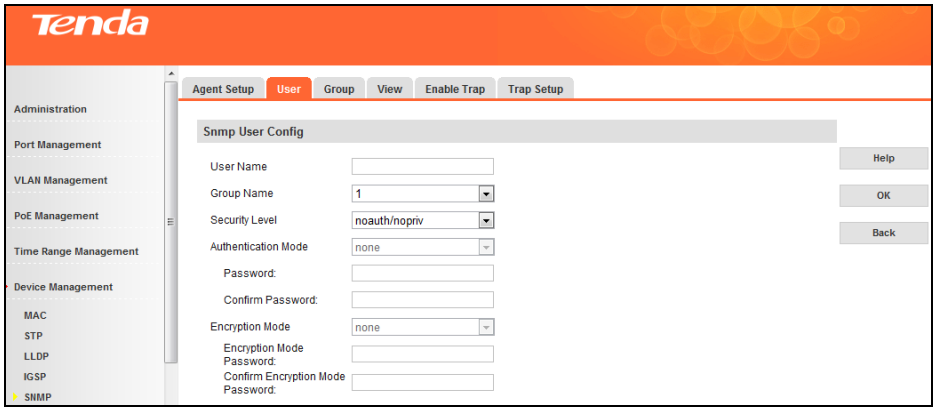
User

To enter the screen below, click **Device Management -> SNMP -> User**.



This section displays information of added user(s).

Click **Add** to enter interface below:



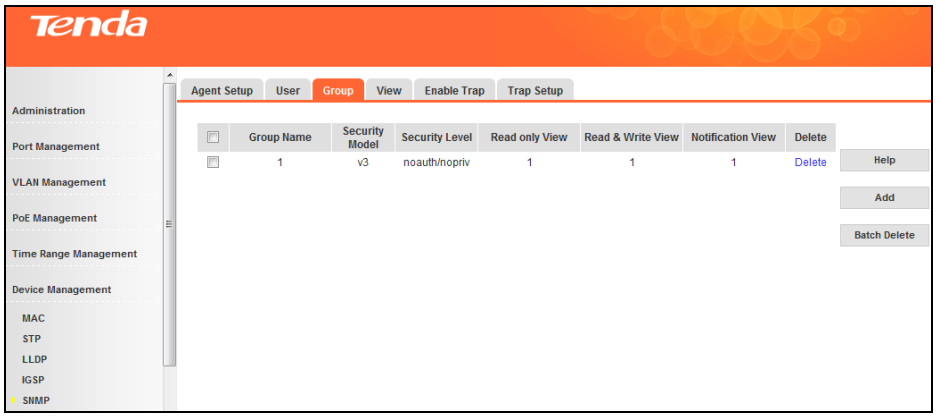
Note: You must create a group before you can add a user.

1. Specify a user name, say, zhangsan.
2. Specify a group name. All existing groups are displayed in the drop-down list.
3. Select a **Security Level** from the drop-down list.
4. Select an **Authentication Mode** from the drop-down list and enter a password and confirm the password (at least 8 characters). If **noauth/nopriv** is selected, this field will be greyed out.
5. Select an **Encryption Mode** from the drop-down list and enter a password and confirm password (at least 8 characters). If **noauth/nopriv or auth/noprivv** is selected, this field will be greyed out.

To edit users, click the corresponding user name to enter interface for modification.

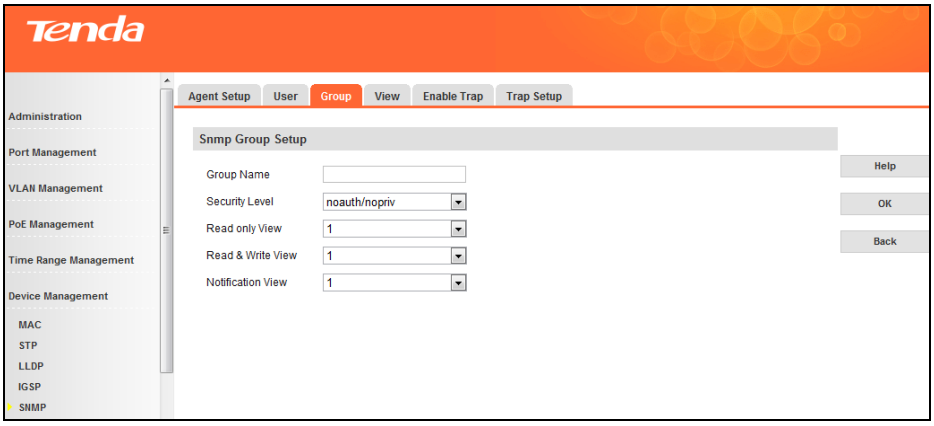
Group

To enter the screen below, click **Device Management -> SNMP -> Group**.



Here you can see at a glance all existing groups.

Click **Add** to enter below interface:



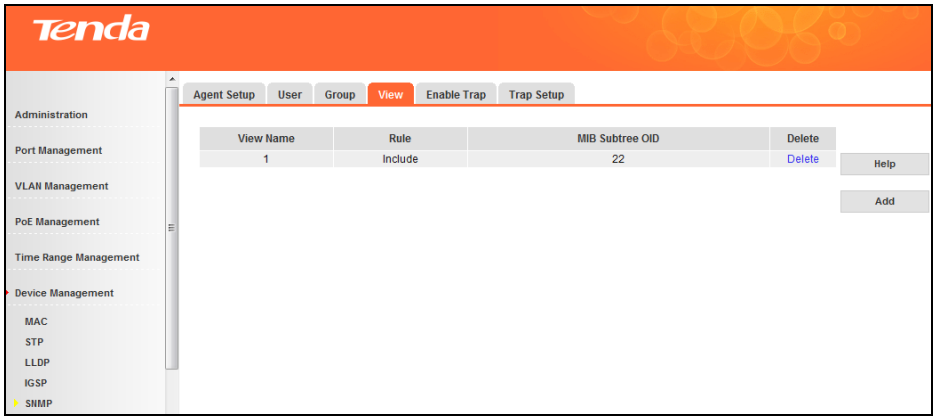
Note: You must create a view before you can create a group.

1. Specify a group name, say, Tenda.
2. Specify a security level, say, auth/nopriv.
3. Specify **Read only View, Read & Write View, Notification View** respectively from the corresponding drop-down list.

To edit groups, click the corresponding Group Name to enter the interface for modification.

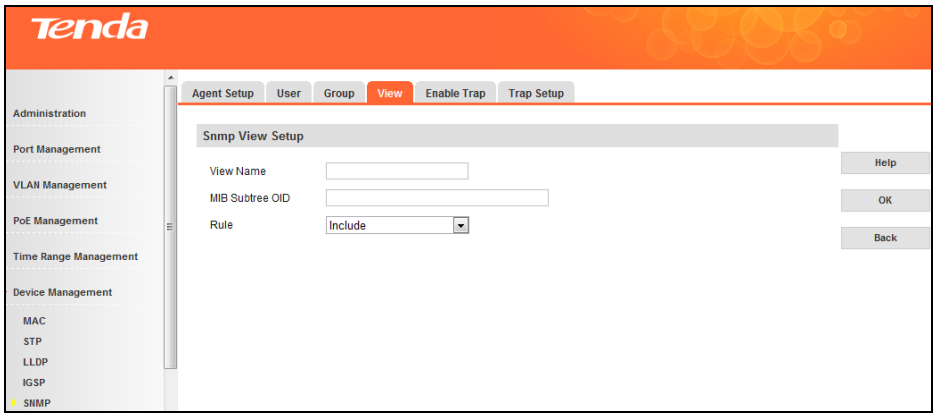
View

To enter the screen below, click **Device Management -> SNMP -> View**.



This section displays added view(s).

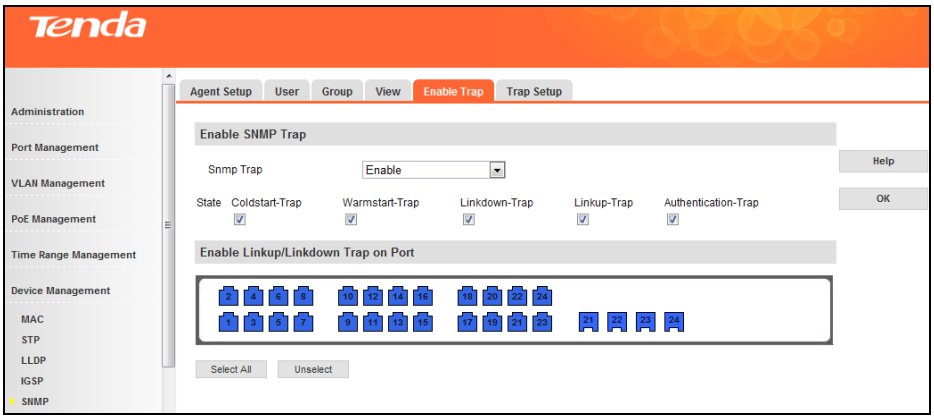
Click **Add** to enter below interface:



1. Specify a view name, say, qq.
2. Specify a MIB subtree OID, say, 1.2.1.
3. Specify a view rule from the drop-down list.

Enable Trap

To config SNMP Trap settings, click **Device Management -> SNMP -> Enable Trap** as below:



By default, the SNMP Trap feature is enabled on each port. Available generic Traps include:

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.

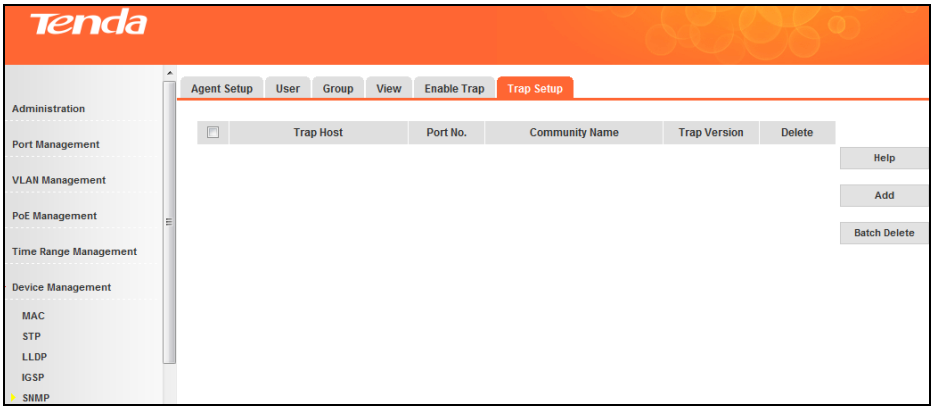
Linkup-Trap: Send Linkup Trap to designated host when a down link becomes up.

Authentication-Trap: Send Authentication failure Trap to designated host when SNMP module encounters an authentication failure.

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

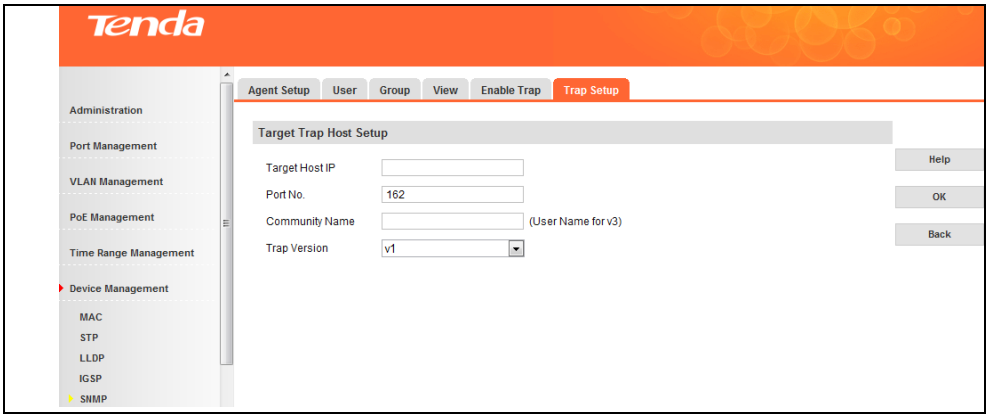
Trap Setup

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



To config the host, do as follows:

1. Click **Add** to enter the following screen:



2. Enter an IP address in the **Target Host IP** field. Note that the host IP must be a legal unicast address and should be on the same IP net segment as the switch, say "192.168.0.77".

3. Enter a UDP port number to which Traps are to be sent in the **Port NO.** field. The default is 162.

4. Enter a custom community name of up to 31 characters, such as "public" in the **Community Name** field. The community name is used to achieve successful interaction between NMS and SNMP Agent.

5. Trap Version: Select v1, v2c or V3. By default, the switch interacts with NMS using the SNMP v1.

6. Click **OK**.

With above settings applied successfully, NMS on the host can receive Traps sent by the SNMP agent on the switch.

4.6.6 DHCP Relay

DHCP Relay Agent Overview

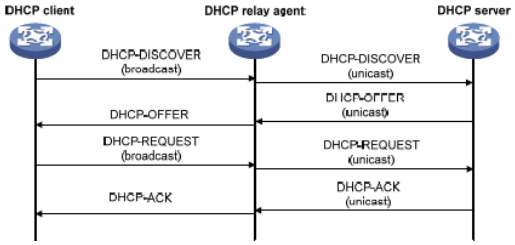
The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers that do not support forwarding of these types of messages. The DHCP Relay Agent is therefore the routing protocol that enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or which is not located on the local subnet. To enable clients to obtain IP addresses from a DHCP server on a remote subnet, you have to configure the DHCP Relay Agent on the subnet that contains the remote

clients, so that it can relay DHCP broadcast messages to your DHCP server.

Data forwarding of DHCP relay agent is different from general routing forwarding. General routing forwarding is relatively transparent and usually the transmitted IP packets won't be modified. However, if DHCP relay agent receives a DHCP packet, it will generate a new one and forward it out.

To the DHCP client, DHCP relay agent is DHCP server; to DHCP server, DHCP relay agent is the DHCP client.

DHCP relay forwarding process:



DHCP relay working process:

- When network devices with DHCP relay feature receive DHCP-DISCOVER or DHCP-REQUEST packets broadcast transmitted by DHCP clients, the giaddr field will be filled with DHCP relay IP and packets will be forwarded, using unicast, to the designated DHCP server according to configurations.
- According to the giaddr field, the DHCP server assigns IPs to clients and forwards configuration info to clients via DHCP relay, and thus clients are dynamically configured.

Option 82

Option 82 records the location of the DHCP Client. Administrator can be acquainted with the location of the DHCP Client via Option 82 so as to locate the DHCP Client for fulfilling the security control and account management of Client.

When the DHCP relay receives DHCP request packets, the device will process them according to process strategies of user configuration and whether option 82 is included or not.

This switch supports two sub-options: Circuit ID and Remote ID:

- Sub-option 1(Circuit ID): the number of the port which receives the DHCP Request packets and its VLAN number.
- Sub-option 2(Remote ID): the MAC address of DHCP Snooping device which receives the DHCP Request packets from DHCP Clients.

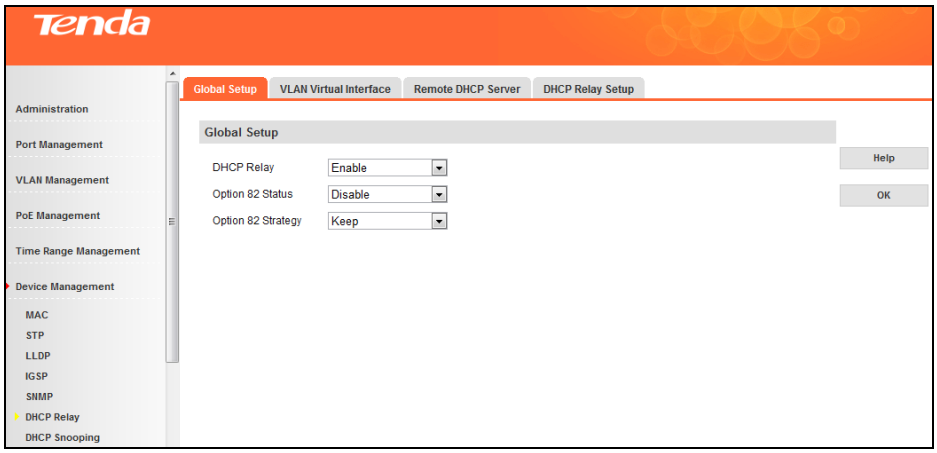
Operations supported for the Option 82:

Received DHCP Request Packets	Processing Strategy	DHCP Relay Processing
Packets with Option82	Replace	Replace the Option82 field of the packets with the switch-defined one and forward them.
	Keep	Keep the Option82 field of the packets and forward them.

	Drop	Discard the packets including the Option82 field.
Packets without Option82	Any	Add the switch-defined one into Option82 field.

DHCP Relay Global Setup

Click **Device Management -> DHCP Relay -> Global Setup** to enter interface below:

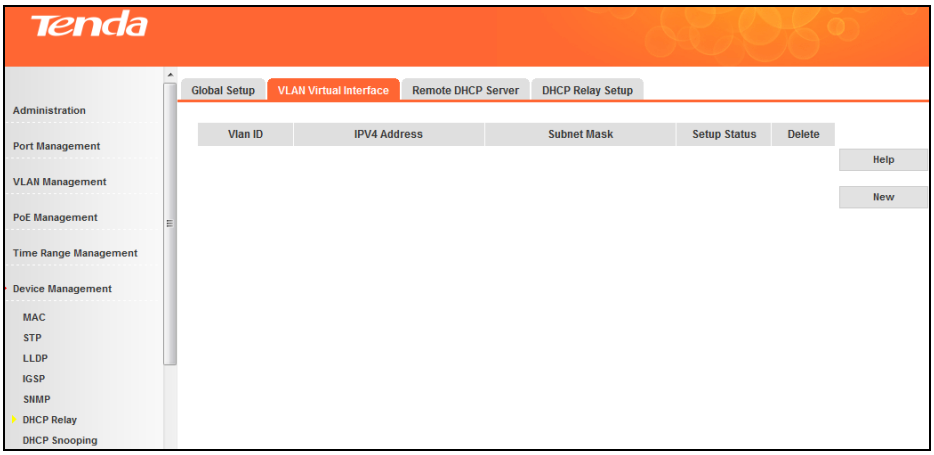


Fields on the screen are described below:

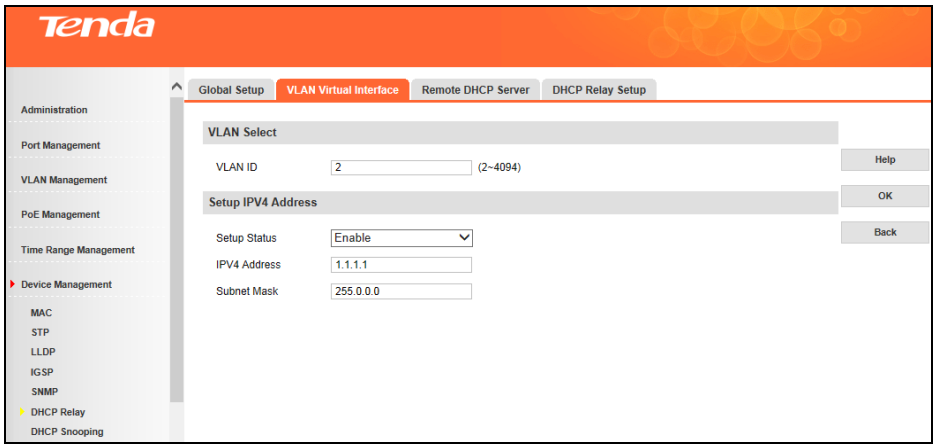
Field	Description
DHCP Relay	Enable/Disable DHCP relay feature. DHCP relay will only take effect when DHCP relay is enabled globally. By default, it is disabled.
Option82 Status	Enable/Disable Option82 feature. Option 82 strategy will only take effect when Option 82 is enabled.
Option82 Strategy	Three strategies are available: replace, keep, drop.

VLAN Virtual Interface

Click **Device Management -> DHCP Relay -> VLAN Virtual Interface** to enter interface below:

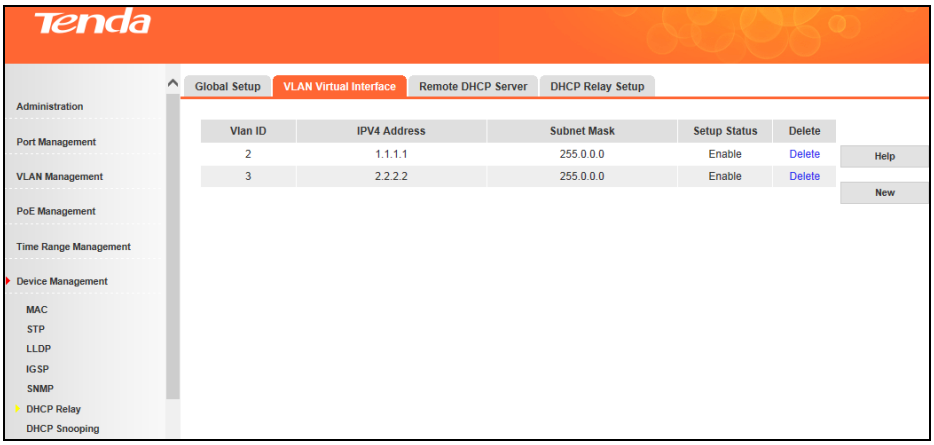


To create a new VLAN virtual interface, click **New** as below:

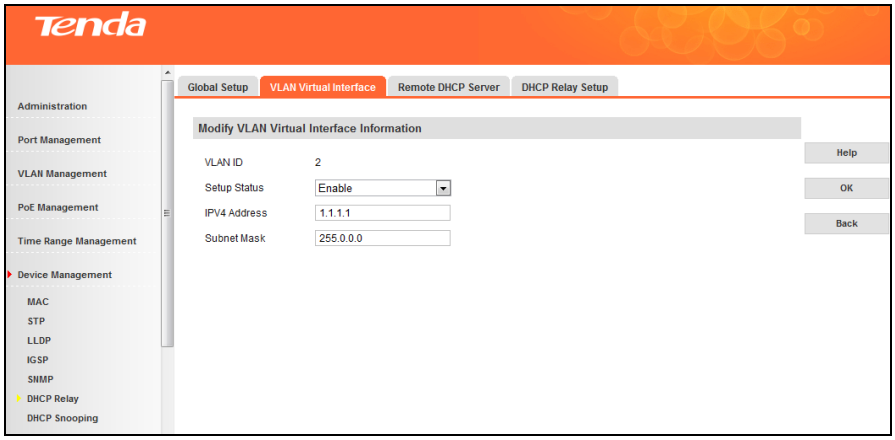


1. Specify the VLAN ID ranging from 2 to 4094 and the VLAN ID must be existing 802.1Q VLAN ID.
2. Enable the IPV4 setup status.
3. Enter the valid IPV4 address, say, 1.1.1.1.
4. Enter the valid subnet mask, say 255.0.0.0.
5. Click **OK**.

Then create VLAN virtual interface 3 as the same steps mentioned above.

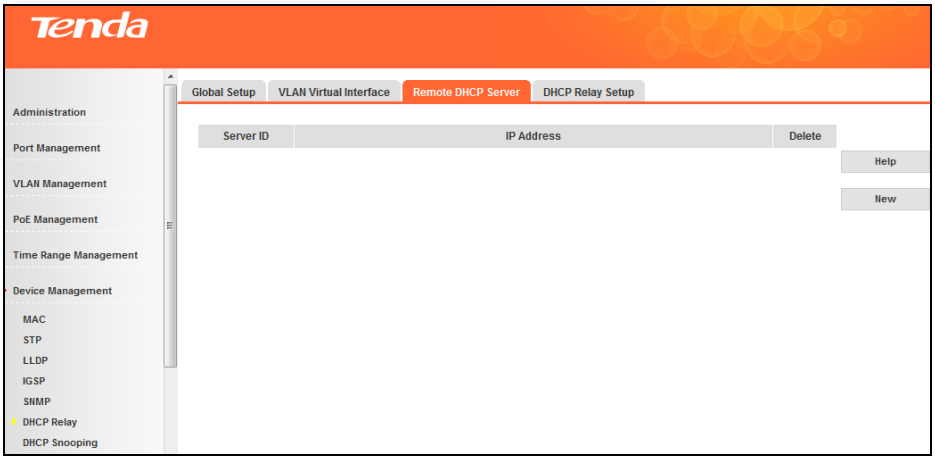


To modify the VLAN virtual interface, click the corresponding VLAN ID as below:

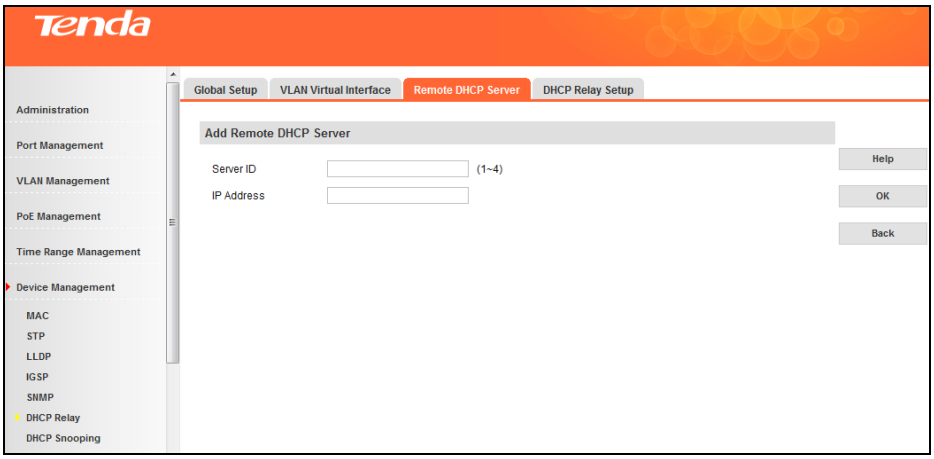


Remote DHCP Server

Click **Device Management -> DHCP Relay -> Remote DHCP Server** to enter interface below:

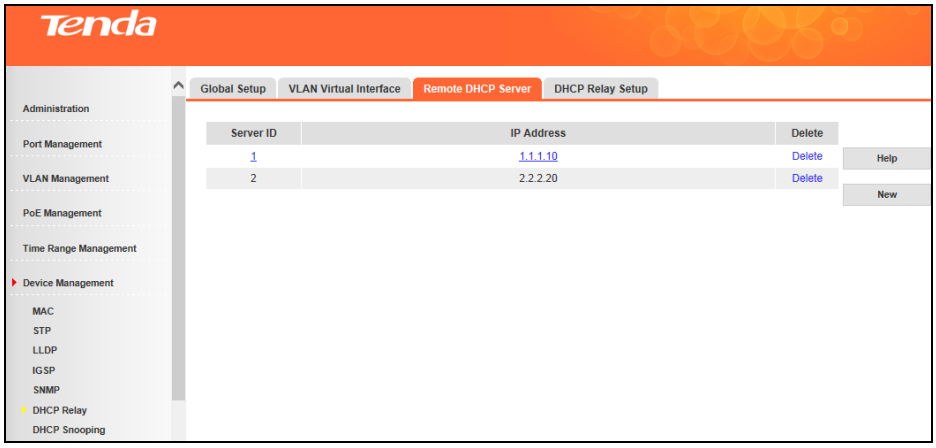


1. To create a remote DHCP server, click **New** as below:



2. Specify the server ID (1-4).
3. Specify the IP address, say 1.1.1.10.
4. Click **OK**.

Then continue to create remote DHCP server 2 as the same steps listed above.

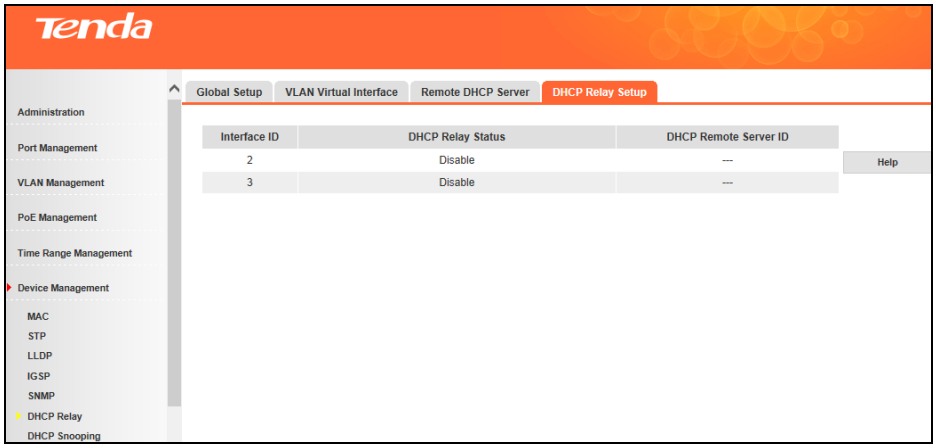


Note----------

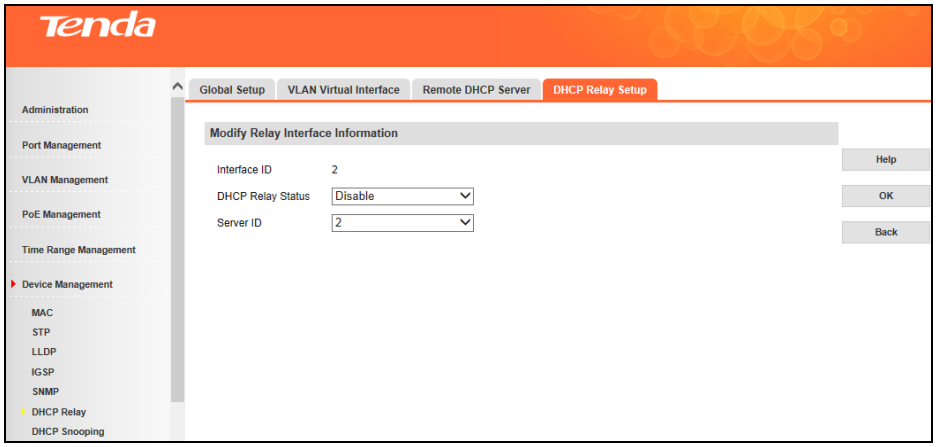
1. The remote server must be in the same network segment with one of the virtual interfaces.
2. Virtual interfaces on which DHCP relay has been enabled can't select remote servers which are in the same network segment with virtual interfaces themselves.
3. Remote servers applied for DHCP relay can't be deleted.

DHCP Relay Setup

1. Click **Device Management -> DHCP Relay -> DHCP Relay Setup** to enter interface below:



2. Click the corresponding interface ID, say 2, and the interface ID corresponds to the existing VLAN virtual interface ID.

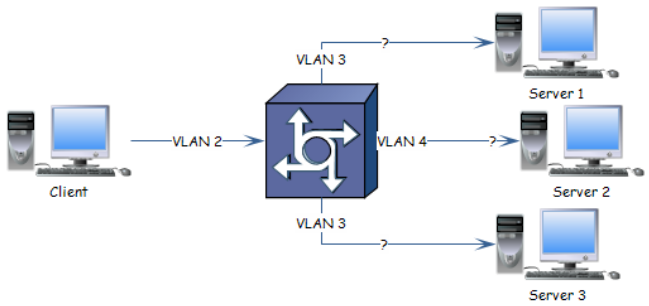


3. Select **Enable** from the **DHCP Relay Setup** drop-down list.

4. Select Server ID, say 2, and click **OK**. DHCP relay on VLAN virtual interface 2 is enabled.

When all DHCH relay settings are finished, clients connected to all servers in VLAN 2 can obtain IP from the DHCP IP pool in VLAN 3.

For more details, see below:



Each VLAN virtual interface has a corresponding VLAN ID. When Client sends out DHCP REQUEST packets, for switches without DHCP relay settings, these packets will be forwarded to other ports in VLAN 2.

When DHCP relay is enabled and Client sends out DHCP REQUEST packets, follow below steps to configure the switch:

1. View corresponding server ID of VLAN virtual interface 2 from the DHCP Relay Setup interface, say 2.
2. View corresponding IP of this server ID, say 2.2.2.20.
3. View the corresponding VLAN virtual interface which is in the same network segment as the IP in step 2, say VLAN virtual interface 3.
4. View corresponding VLAN ID of the VLAN virtual interface, say VLAN 3.
5. Packets will be forwarded to ports in VLAN 3 as step 4 describes.

Note----------

As for servers in VLAN 3, you need to set its DHCP server's DHCP relay IP to 1.1.1.1 so that clients in VLAN 2 can obtain IP automatically from the DHCP server in VLAN 3.

4.6.7 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. Its functions are as below:

- Ensure that clients only obtain IP addresses legal servers assign to them.

If illegal DHCP servers exist in computer networking, DHCP clients might obtain incorrect IP addresses and parameters, thus leading to abnormal communication. In order that DHCP clients obtain IP addresses via legal DHCP servers, trusted ports and untrusted ports are allowed:

Trusted ports can forward DHCP packets they've received.

After receiving DHCP-ACK and DHCP-OFFER packets, untrusted ports will discard these packets.

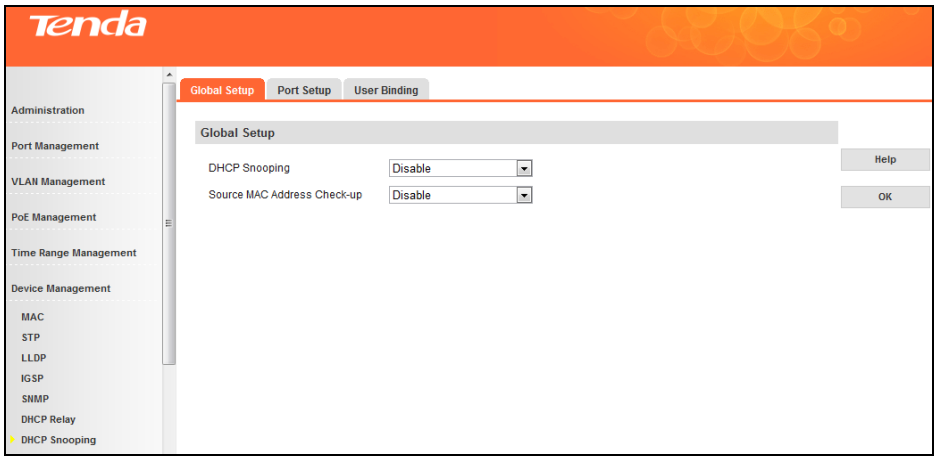
Ports which are connected to DHCP servers and other DHCP Snooping devices need to be configured as trusted ports and other ports need to be configured as untrusted ports, so that DHCP clients can only obtain IP addresses from legal DHCP clients.

- Record the corresponding relation between DHCP client's IP address and MAC address.

By snooping DHCP-REQUEST and DHCP-ACK broadcast packets trust ports have received, it records DHCP Snooping entries, including clients' MAC addresses, obtained IP addresses, ports connected to DHCP clients, ports' belonging VLAN info, etc.

Global Setup

To configure DHCP snooping global settings, click **Device Management -> DHCP Snooping -> Global Setup** as below:

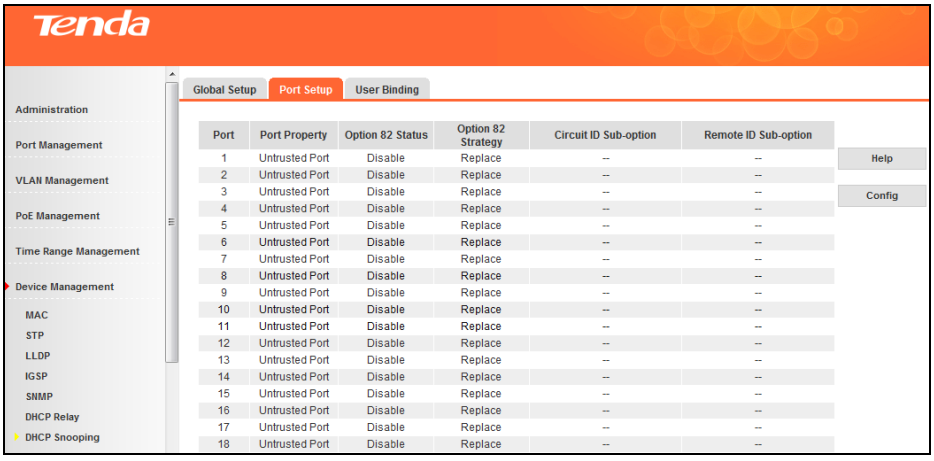


Fields on the screen are described below:

Field	Description
DHCP Snooping	Enable/Disable DHCP snooping feature globally. By default, it is disabled.
Source MAC Address Check-up	Config whether source MAC address check-up feature is enabled or not.

Port Setup

To configure DHCP snooping port settings, click **Device Management -> DHCP Snooping -> Port Setup** as below:



Fields on the screen are described below:

Field	Description
Port	The corresponding port number.
Port Property	Configure the current port's DHCP snooping property.

Option82 Status	Enable/Disable option 82. Option 82 records DHCP clients' location info.
Option82 Strategy	When DHCP snooping receives DHCP packets, it will process these packets according to whether Option 82 included, processing strategy of user configuration and fill pattern, and then forward them to DHCP server. Three strategies are available: replace, keep and drop.
Circuit ID Sub-option	Configure the current port's circuit ID sub-option.
Remote ID Sub-option	Configure the current port's remote ID sub-option.
Back	Click it to go back to port setup page.

Three strategies are available for this device:

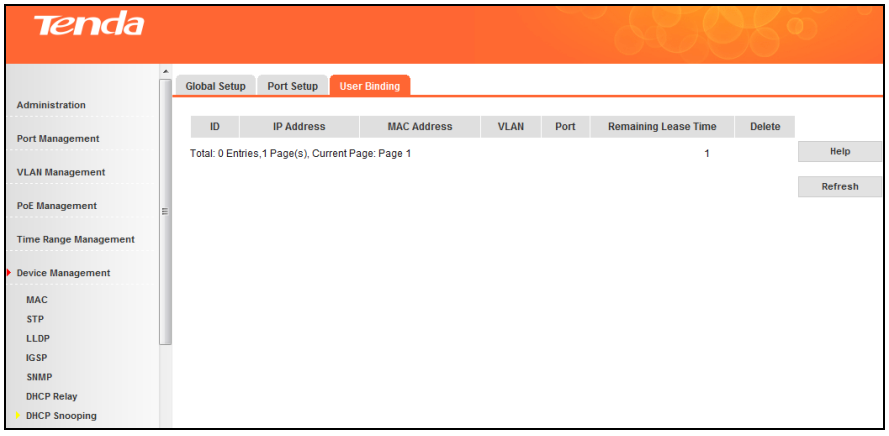
Replace: When DHCP relay receives DHCP packets with Option 82, the previous Option 82 information will be replaced by the default contents on this device and forwarded. When DHCP relay receives DHCP packets without Option 82, the default contents on this device will be added into Option 82.

Keep: When DHCP relay receives DHCP packets with Option 82, the previous Option 82 information will be kept and forwarded. When DHCP relay receives DHCP packets without Option 82, the default contents on this device will be added into Option 82.

Drop: When DHCP relay receives DHCP packets with Option 82, the previous Option 82 information will be discarded. When DHCP relay receives DHCP packets without Option 82, the default contents in this device will be added into Option 82.

User Binding

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



Fields on the screen are described below:

Field	Description
ID	Displays user binding digits in the list.

IP Address	Displays the user binding's IP address.
MAC Address	Displays user binding's MAC address.
VLAN	Displays user binding's VLAN ID.
Port	Displays user binding's port number.
Remaining Lease Time	Displays user binding's remaining lease time.
Delete	Click it to delete the user binding.

4.7 QoS

4.7.1 QoS Configuration

QoS Overview

Quality of service is the ability to provide different applications, users, or data flows with different priority, or to guarantee a certain level of performance to a data flow. For example, a required bit rate, delay, jitter, packet dropping probability and/or bit error rate may be guaranteed. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP, online games and IP-TV, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication.

QoS addresses network latency and congestion issues. Non-critical (elastic) applications like web browsing or emailing do not rely on QoS as they function however much or little bandwidth is available. However, for critical (inelastic) services or applications that require a certain minimum level of bandwidth and a certain maximum latency to function, QoS is indispensable. QoS can prevent critical traffic flow from being discarded or delayed on a congested and overloaded network, thus ensuring a mix of real-time/interoperative and non-real-time/non-interoperative traffic without meltdown.

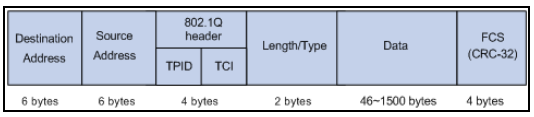
Widely used priority types

1） Port Priority

The port priority is based on switch's physical ports. To config it, click **QoS Configuration -> Port Priority**. Note that available values range from 0 to 7. It is used to determine the forwarding sequence of packets not carrying priority identifiers.

2） 802.1P Priority

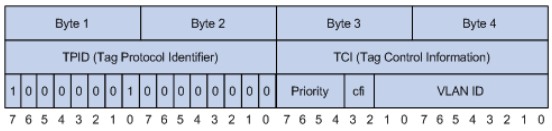
The 802.1P priority, contained in the Ethernet header, is used by QoS disciplines to differentiate traffic on layer 2 where analyzing IP header is not necessary. 802.1P priority is available only in an IEEE 802.1Q tagged frame. As seen below, the 4-byte 802.1Q tag contains a 2-byte TPID (Tag Protocol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



802.1Qtagged Ethernet frame

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.



802.1QTag

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

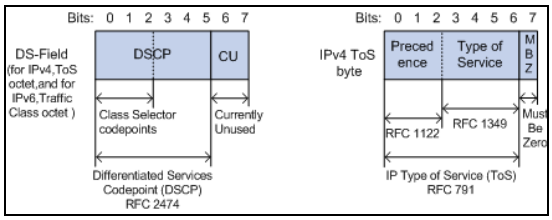
3）DSCP Priority

The DSCP priority resides in the IP header. The ToS field includes 8 bits, among which:

The first 3 bits denote the IP priority, with available values ranging from 0 to 7.

Bits 3-6 denote the ToS priority, with available values ranging from 0 to 15.

The RFC 2474 redefined the IPv4 ToS field as the DS field. The DSCP priority is denoted by the first 6 bits (bits 0～5), with available values ranging from 0 to 63, while the last 2 bits (bits 6-7) are reserved.



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

Scheduling Scheme Overview

QoS provides a queue scheduling policy to determine the packet forwarding sequence when congestion occurs. The switch provides two common scheduling techniques to achieve Quality-of-Service (QoS) while using shared resources: SP(Strict-Priority) and WRR (Weighted Round Robin).

1) Strict Priority Queueing

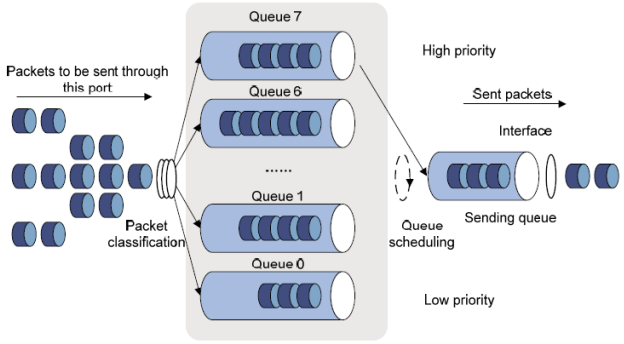


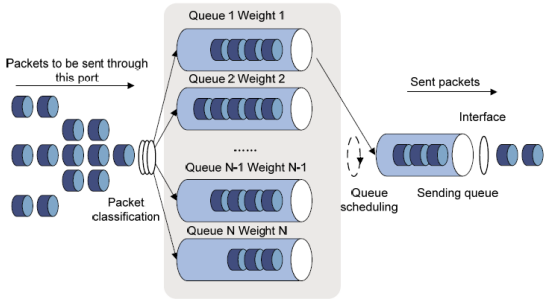
Diagram for SP queuing

Strict Priority Queueing is specially designed to meet the demands of critical services or applications. Critical services or applications such as voice are delay-sensitive and thus require to be dequeued and sent first before packets in other queues are dequeued on a congested network. 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, only after packets in highest priority queue are emptied, can packets in lower priority queue be forwarded. 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.

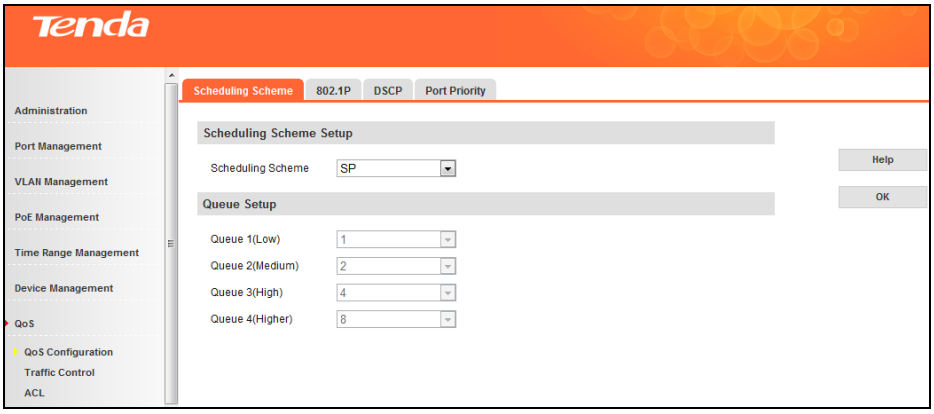
2）WRR



WRR queue scheduling algorithm ensures every queue a guaranteed service time by taking turns to schedule all queues. Assume there are 4 egress queues on the port. The four weight values (namely, w3, w2, w1, and w0) 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(corresponding to w3, w2, w1, and w0 respectively). Then the queue with the lowest priority can be ensured of, at least, 10 Mbps bandwidth, thus avoiding the disadvantage of SP queue-scheduling algorithm that packets in low-priority queues may not be served during a long time. Another advantage of WRR queue-scheduling algorithm is that though the queues are scheduled in turn, the service time for each queue is not fixed, that is to say, when a queue is emptied, the next queue will be scheduled immediately. Thus, bandwidth resources are fully utilized.

Scheduling Scheme

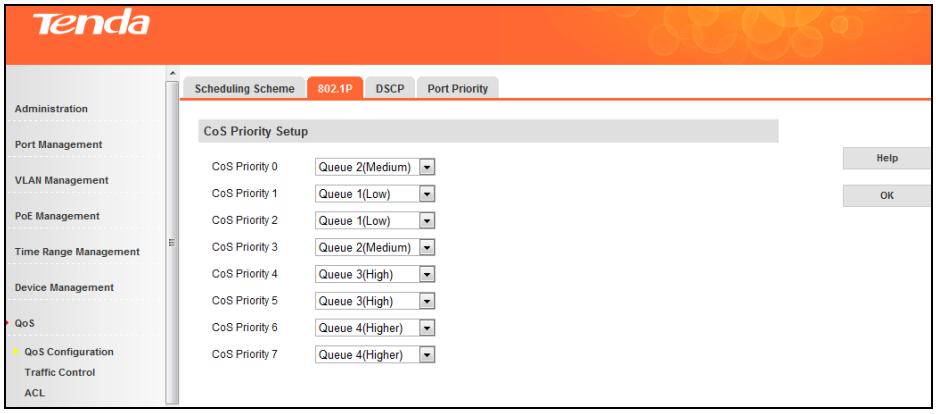
Click **QoS -> QoS Configuration -> Scheduling Scheme** to enter interface below:



- To configure scheduling scheme, select SP or WRR from the pull-down list and then click **OK**.
- To configure queue settings, select WRR scheduling scheme first, and then configure the queue weight values accordingly.

802.1P

To configure CoS priority settings, click **QoS -> QoS Configuration -> 802.1P** as below:



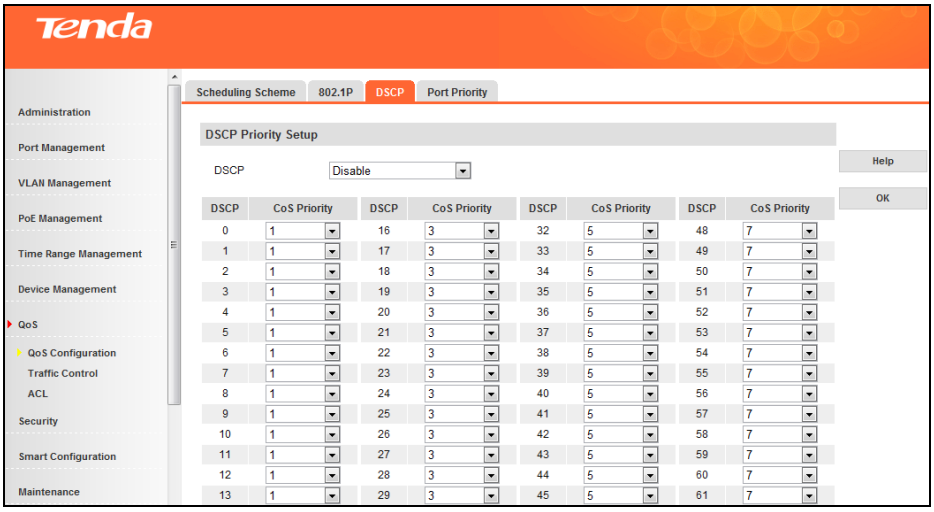
Then select the queue values for CoS priority 0-7 and click **OK**.

Note----------

When congestions occur, according to the mapping relationships you've configured, the device will assign packets with CoS priority to queues.

DSCP

To configure DSCP priority settings, click **QoS -> QoS Configuration-> DSCP** as below:

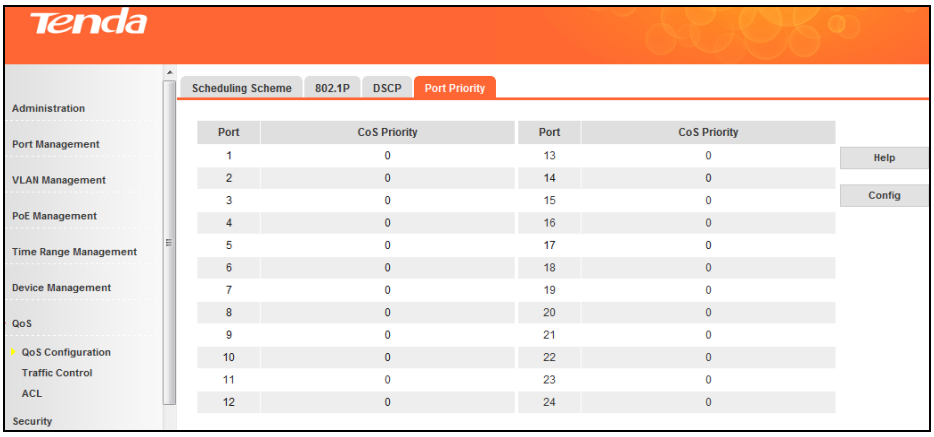


Note----------

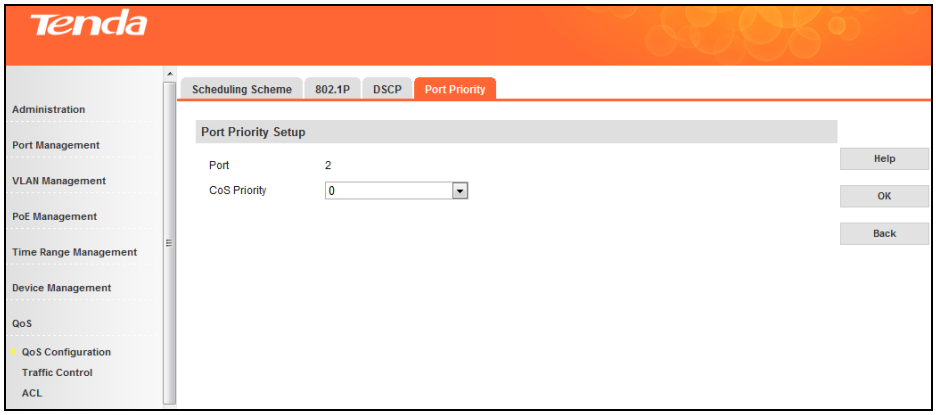
When congestions occur, the device will first map DSCP values to CoS values according to the configured mapping relationships. Then according to the CoS-queue mapping table, it assigns packets with DSCP priority to queues which CoS priority corresponds to.

Port Priority

To configure port priority settings, click **QoS -> QoS Configuration -> Port Priority** as below:



➢ To configure port priority settings on a single port, click the corresponding port, select CoS priority value and click **OK**.



➢ To configure port priority settings on multiple ports, click **Config**.

Note----------

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.

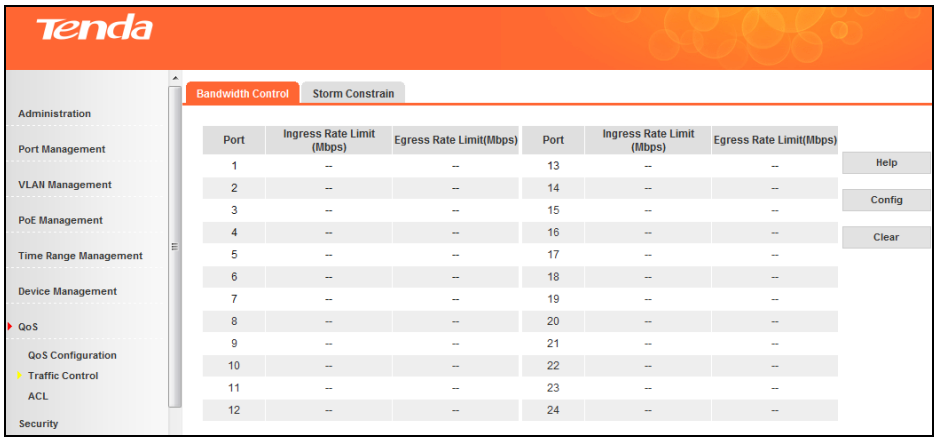
4.7.2 Traffic Control

Bandwidth Control

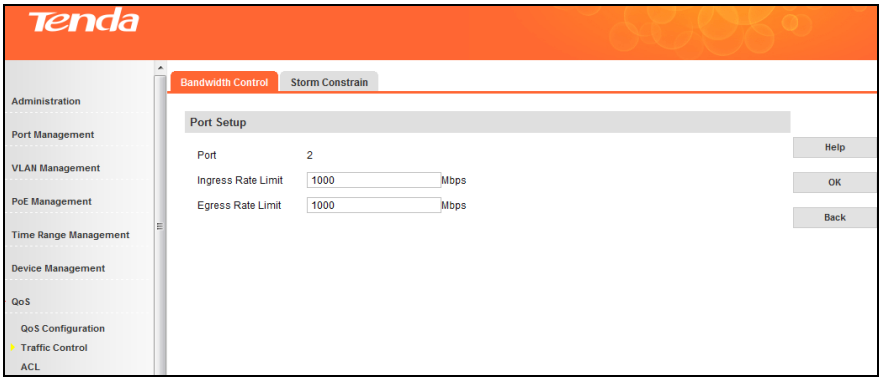
Rate limit functions to control the ingress/egress traffic rate on each port via configuring the available bandwidth of each port. In this way, the network bandwidth can be reasonably distributed and utilized.

Rate limit 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.

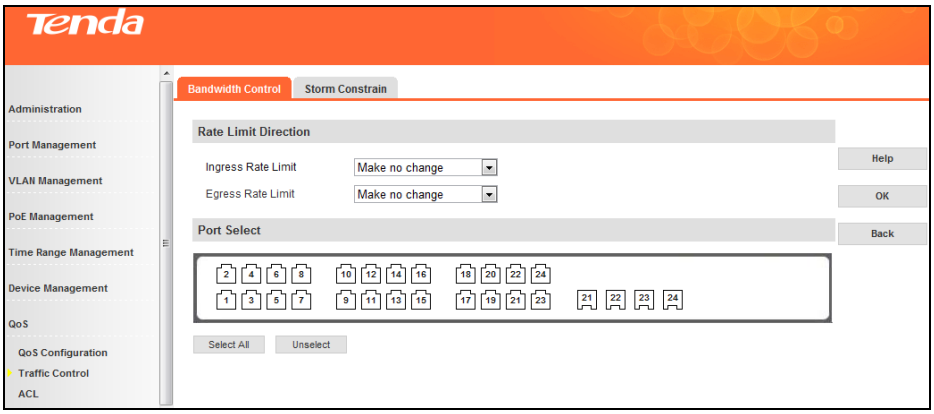
Click **QoS -> Traffic Control -> Bandwidth Control** to enter interface below ("--" means no limit.):



➢ To configure rate limit on a specified port, click the corresponding port.



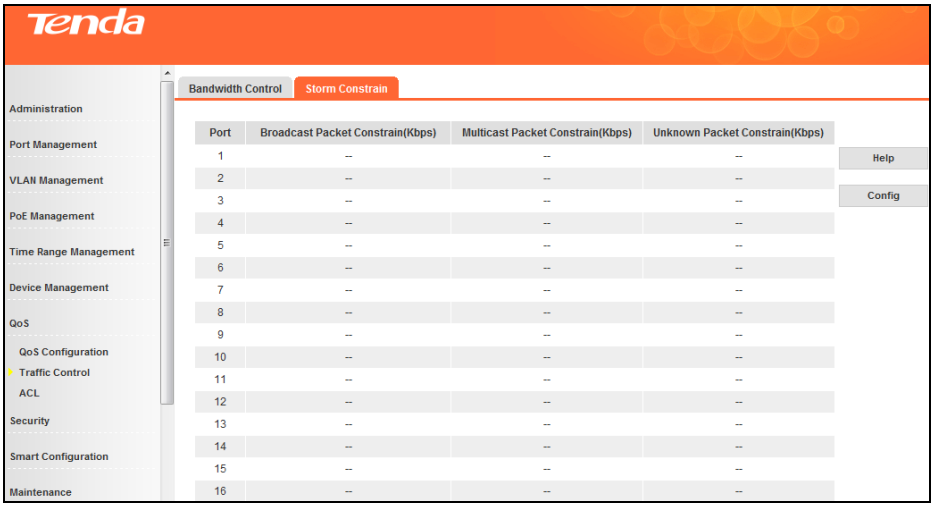
➢ To configure rate limit on multiple ports, click **Config**.



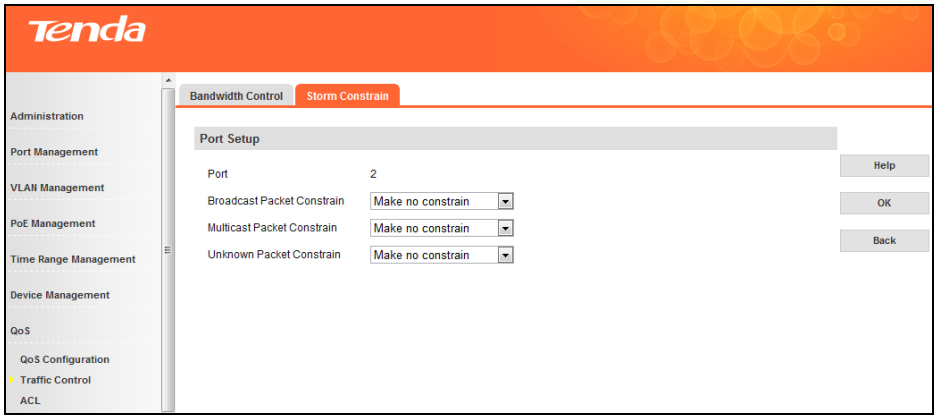
Storm Constrain

Storm Constrain function allows the switch to filter broadcast, multicast and unknown unicast frames 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.

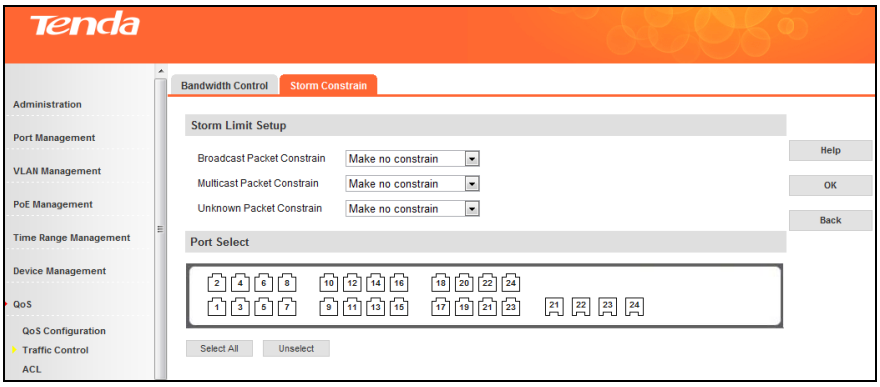
Click **QoS -> Traffic Control -> Storm Constrain** to enter interface below ("—"means no constrain is set to it.):



➢ To configure storm constrain settings on a specified port, click the corresponding port.



➢ To configure storm constrain settings on multiple ports, click **Config**.



4.7.3 ACL

ACL Overview

As traffic increases and network grows, network security appears more and more important. Pack filter can effectively block unauthorized users from accessing network and control traffic volume on the network for the purpose of conserving network resources. An access control list (ACL) implements packet filter via configured rules and operations attached to a packet.

When the switch receives a packet, it analyzes the packet using currently applied ACL rules and then handles the packet by preset operations (permit, prohibit or limit rate, mirroring, etc).

ACL Type

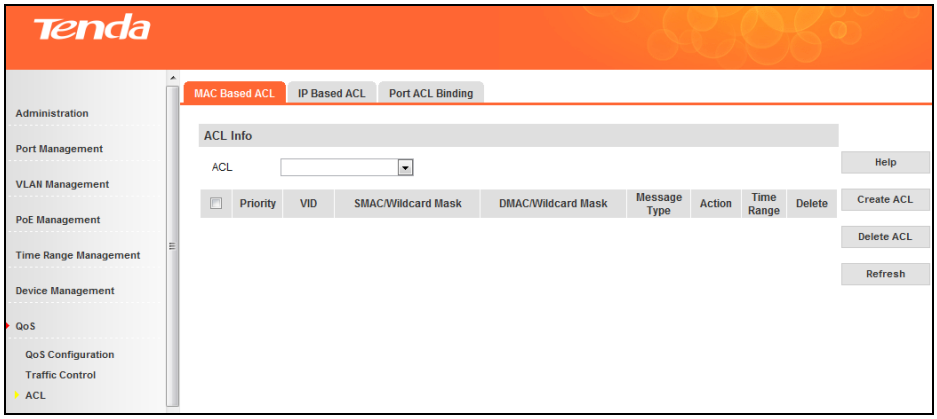
The following 2 ACLs are supported:

➢ MAC Based ACL: Specify operation rules based on source MAC, destination MAC, 802.1P priority, L2 protocol type and other L2 information of the packet.

➢ IP Based ACL: Specify operation rules based on protocol type, source IP, destination IP and protocol feature (source/destination TCP/UDP ports) of the packet.

MAC Based ACL

Click **QoS -> ACL -> MAC Based ACL** to enter interface below:

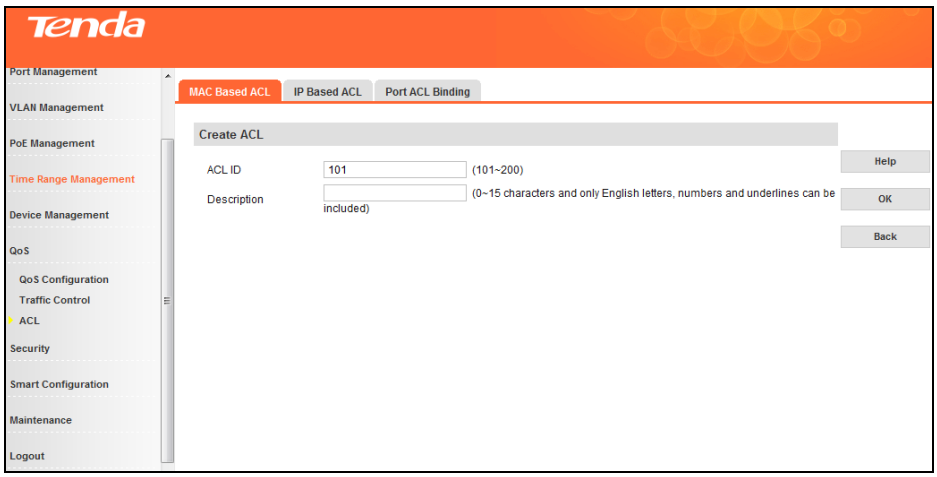


- This page displays all existing MAC based ACLs and rules thereof.
- To delete an existing MAC based ACL

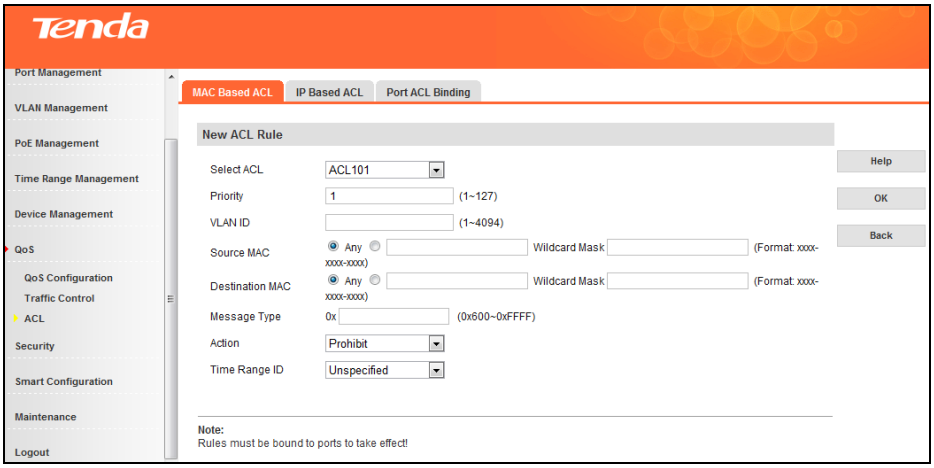
Select the ACL you wish to delete from the ACL drop-down list and click on the **Delete ACL** button.

- To create MAC based ACL

Click **Create ACL**, enter required settings and then click **OK**.



- To add rules to a specified ACL



1. Select an ACL
2. Click **Add Rule**. Configure required settings and click **OK**.

Fields on the screen are described below:

Field	Description
Select ACL	Select an existing ACL and specify rules for it.
Priority	Specify a priority for a given rule, which determines match scheduling order. If an ACL has multiple rules, the rule with smallest priority value will be first scheduled for match purpose.
VLAN ID	Specify the VLAN ID of the messages for ACL rules to apply.
Source/Destination MAC	Specify source MAC and destination MAC of packets for a rule to match. Note: If Any is selected, the rule will match and apply to all packets with whatever source MAC/destination MAC.
Message Type	Specify the message type in Hex.
Action	Permit: Allow messages that match existing rules to pass. Prohibit: Discard messages that match existing rules. Rate Limit: Limit forwarding rate of messages that match existing rules (64-1048576kbps). The default action is Prohibit.
Time Range ID	Select time range ID for rule application. Within the set time range, rules will take effect. By default, no time range is specified and ACL rules take effect at any time.

➢ To modify ACL rules

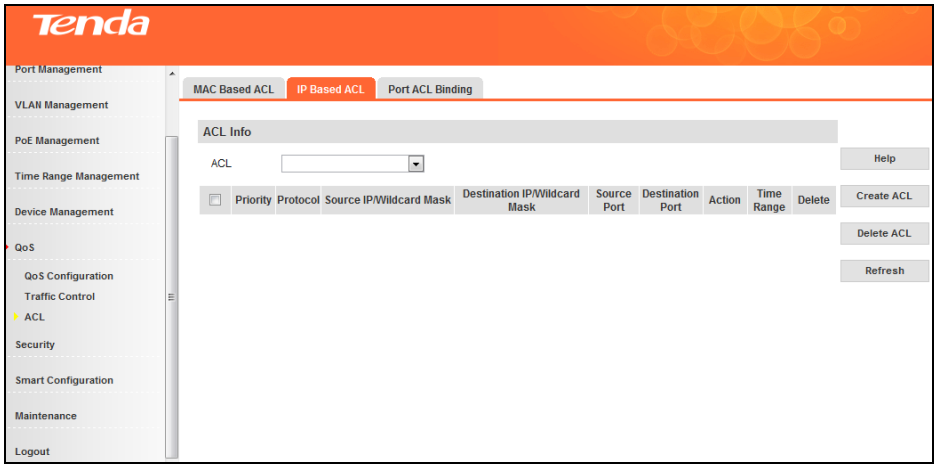
Click the corresponding rule you wish to modify, configure required modifications and click **OK**.

➢ To delete a rule

Check the rule you wish to remove and click **Delete Rule**.

IP Based ACL

Click **QoS -> ACL -> IP Based ACL** to enter interface below:



➢ This page displays all existing IP based ACLs and rules thereof.

➢ To delete an existing IP based ACL

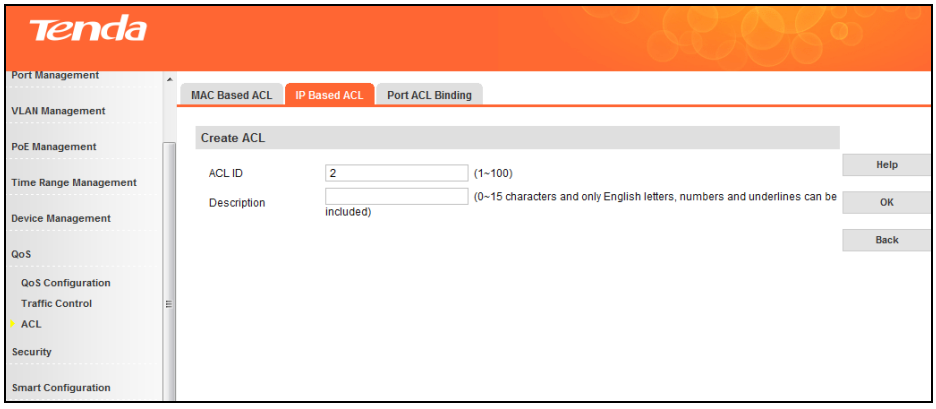
Select the ACL you wish to delete from the ACL drop-down list and click on the **Delete ACL** button.

➢ To batch delete rules in an ACL

Select the ACL and rules thereof you wish to delete, and click on the **Delete Rule** button.

➢ To create a new IP based ACL

Click **Create ACL** to enter corresponding page for configuration. Configure requied ACL settings and click **OK**.

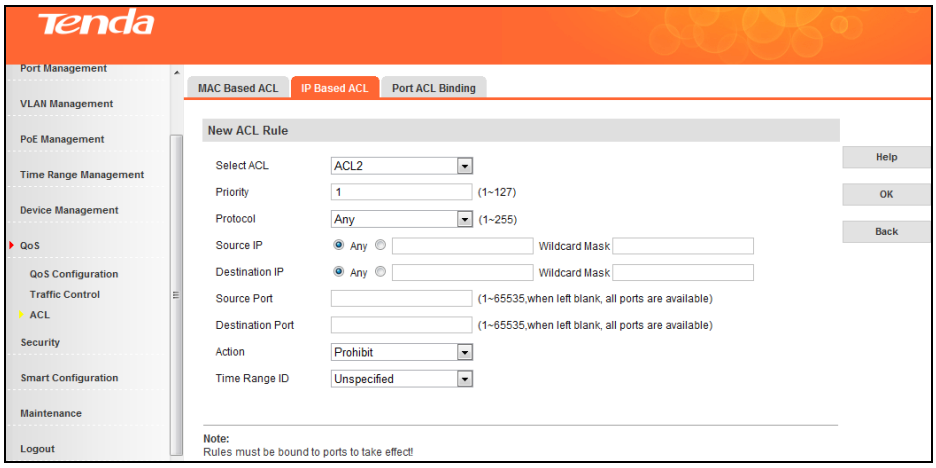


ACL ID: Specify an ACL ID between 1 and 100.

Description: Specify an ACL description.

➢ To add rules to a specified ACL

Select an ACL from the ACL drop-down list and click **Add Rule** to enter the corresponding interface. Specify a rule for the ACL and click **OK**.



Fields on the screen are described below:

Field	Description
Select ACL	Select an existing ACL and specify rules for it.
Priority	Specify a priority for a given rule, which determines match scheduling order. If an ACL has multiple rules, the rule with the smallest priority value will be first scheduled for match purpose.
Protocol	Select a protocol to match.
Source/Destination IP	Specify source IP and destination IP of packets for a rule to match. Note: If Any is selected, the rule will match and apply to all packets with whatever source IP/destination IP.
Source Port	Specify source port number to match TCP/UDP messages. Note: If Any is selected, the rule will match and apply to any source port. Source port is configurable only when TCP or UDP protocol is selected.
Destination Port	Specify destination port number to match TCP/UDP messages. Note: If Any is selected, the rule will match and apply to any destination port. Destination port is configurable only when TCP or UDP protocol is selected.
Action	Specify an action to handle messages: Permit: Allow messages that match existing rules to pass. Prohibit: Discard messages that match existing rules. Rate Limit: Limit forwarding rate of messages that

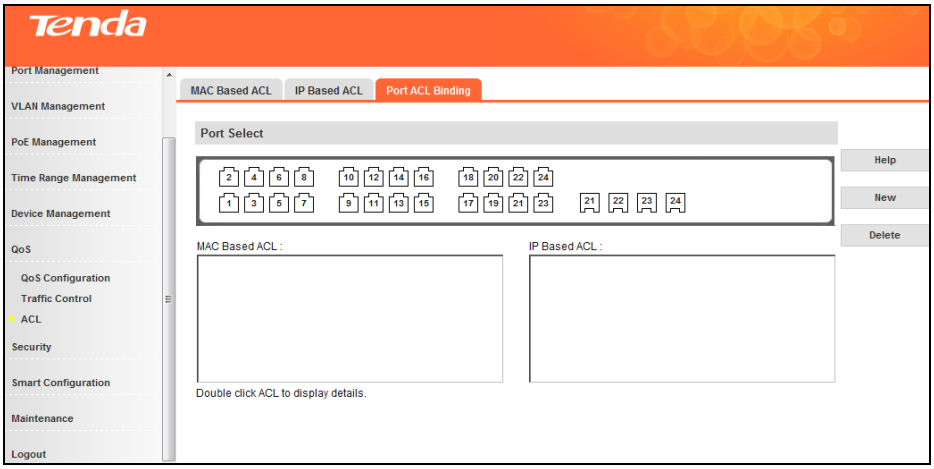
	match existing rules (64~1048576kbps). The default action is Prohibit.
Time Range ID	Select time range ID for rule application. Within the set time range, rules will take effect. By default, no time range is specified and ACL rules take effect at any time.

➢ To modify ACL rules

Click the corresponding rule you wish to modify, configure required modifications and click **OK**.

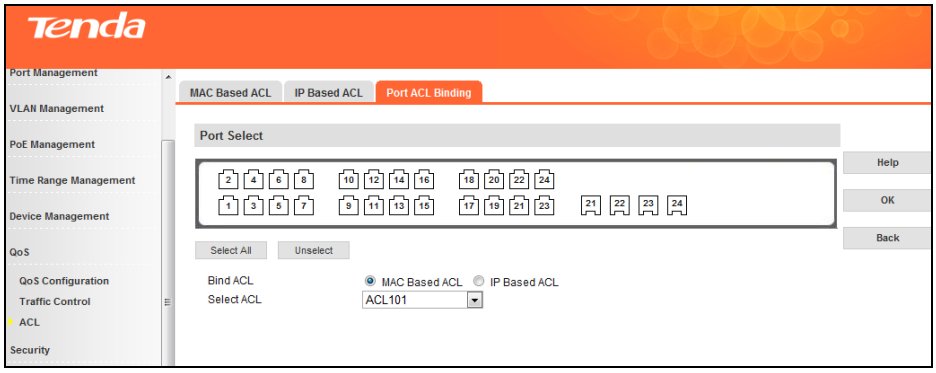
Port ACL Binding

Click **QoS -> ACL -> Port ACL Binding** to enter interface below:

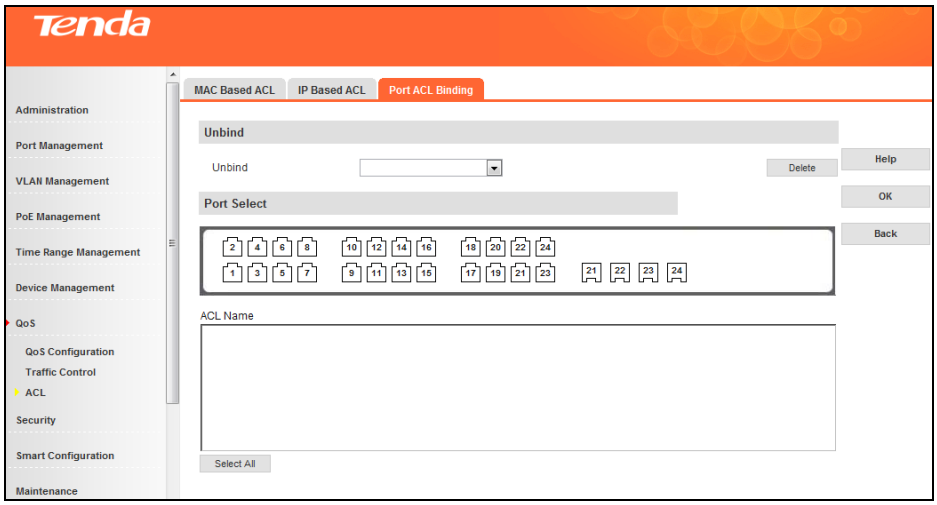


➢ To display port binding rules, select a port and MAC based ACL and IP based ACL (if any) will appear in corresponding lists.

➢ To create port ACL binding, click **New**, specify a port that you wish to apply a given ACL, configure required settings and click **OK**.



➢ To delete a specific Port ACL binding, click **Delete** on the port ACL binding page as below:



Select the port and the ACL you wish to unbind and then click **OK**.

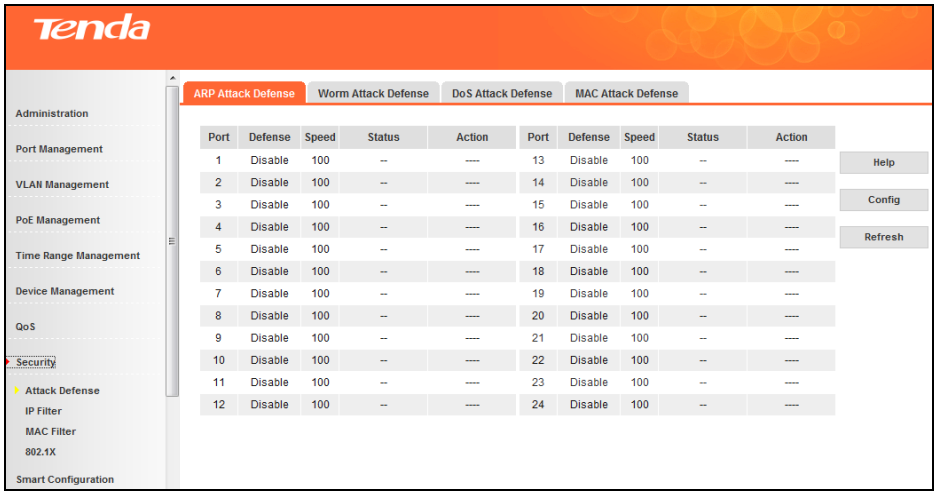
4.8 Security

4.8.1 Attack Defense

ARP Attack Defense

If a switch continuously receives an enormous number of ARP messages on a specific port, it will not function properly as CPU is overloaded and, worse still, may break up. ARP rate limit is just designed as a solution to these problems. ARP rate limit enabled ports will enter a protection status and discard all ARP messages received if they exceed the set threshold. When protection time ends, the ports will resume forwarding ARP messages. Thus the switch is protected against such attack.

Click **Security -> Attack Defense -> ARP Attack Defense** to enter interface below:



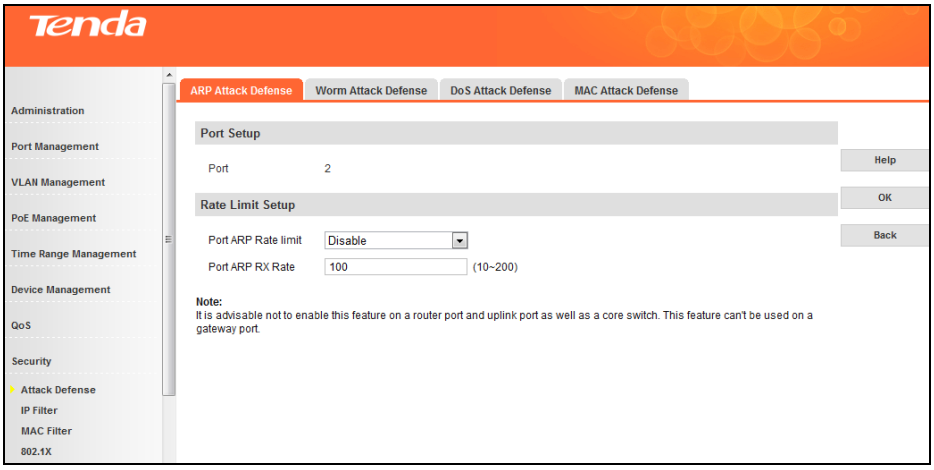
Fields on the screen are described below:

Field	Description
Port ARP Rate	By default, the Port ARP Rate limit feature is

Limit	disabled. Note: ARP rate limit enabled ports will check current ARP rate every 60s and discard ARP messages received if current ARP RX rate exceeds the set ARP RX rate threshold.
Port ARP RX Rate	The default is 100PPS. Note: PPS refers to the number of packets per second. It has nothing to do with the size of a packet.
Status	Displays the status how a corresponding port deals with received ARP messages. "--" means port ARP rate limit feature is not enabled. Normal: System does not detect ARP attacks and then forwards these ARP messages normally. Drop ARP: System detects ARP attacks and drops these malicious ARP messages.
Action	Displays ARP packets' receiving status. "--" means no ARP attack or ARP attack defense feature is not enabled. Normal: ARP packets are forwarded normally.

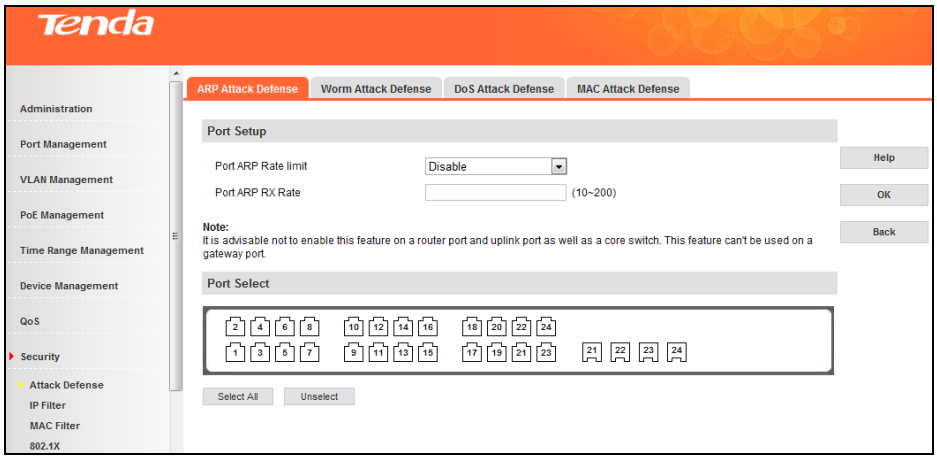
➢ To configure ARP rate limit status and ARP RX rate for a single port

Click the corresponding port to enter the configuration page.



➢ To configure ARP rate limit status and ARP RX rate for a batch of ports simultaneously

Click **Config** to enter corresponding page for configuration.

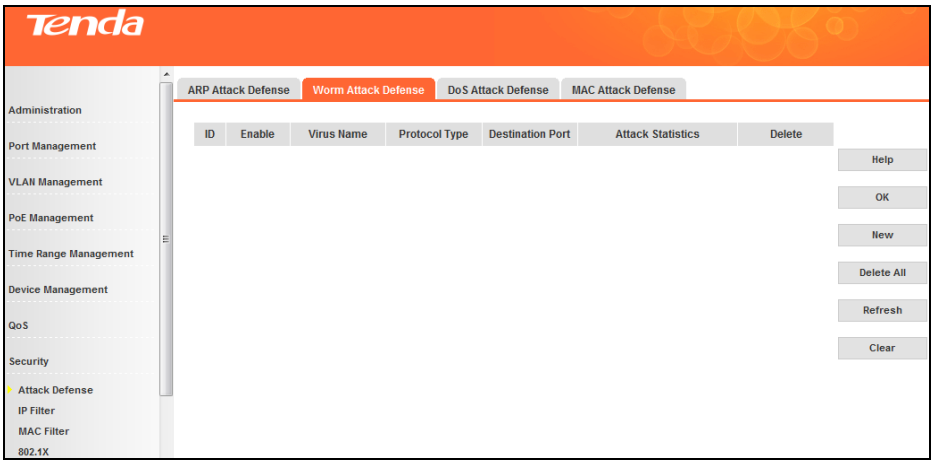


Worm Attack Defense

Worm Attack Defense prevents virus/worm infected PCs being spread to targeted healthy PCs and the whole network by scanning for security failures.

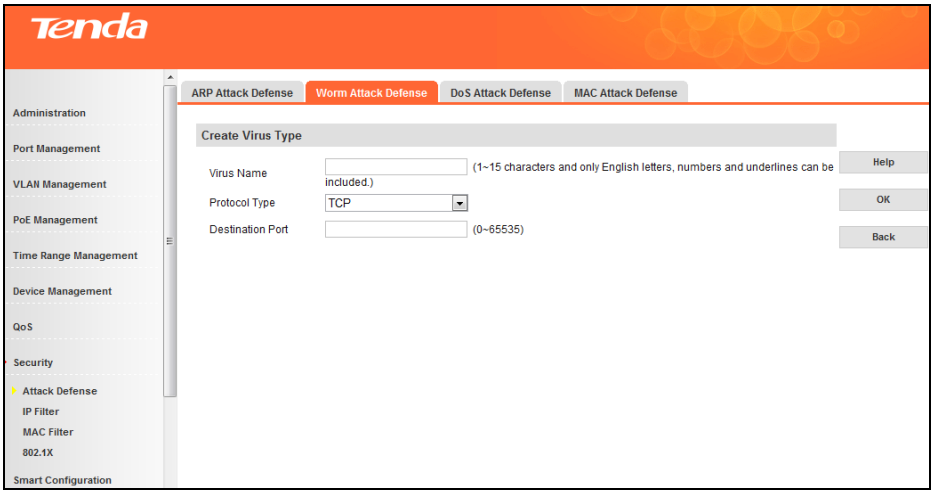
Once Worm Attack Defense feature is enabled, the switch directly discards messages that match features of predefined virus so that PC and other network devices will not be infected.

Click **Security -> Attack Defense -> Worm Attack Defense** to enter interface below:

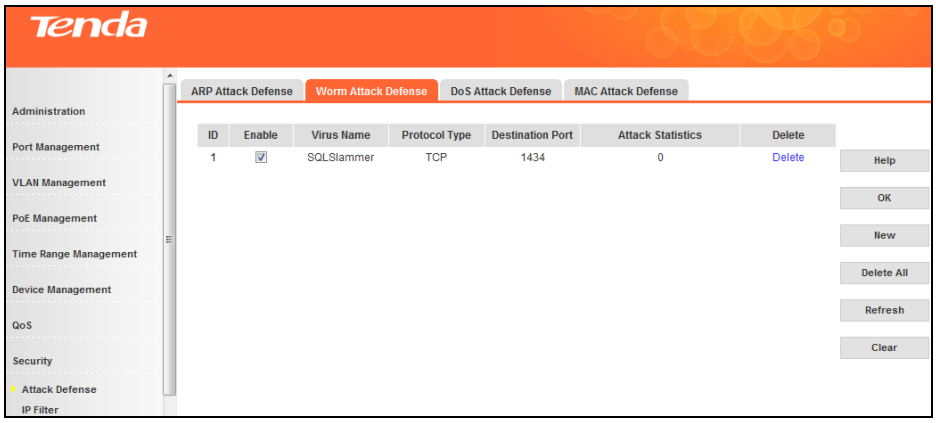


➢ To defend against known viruses, you need to add them to the device and enable the worm attack defense feature.

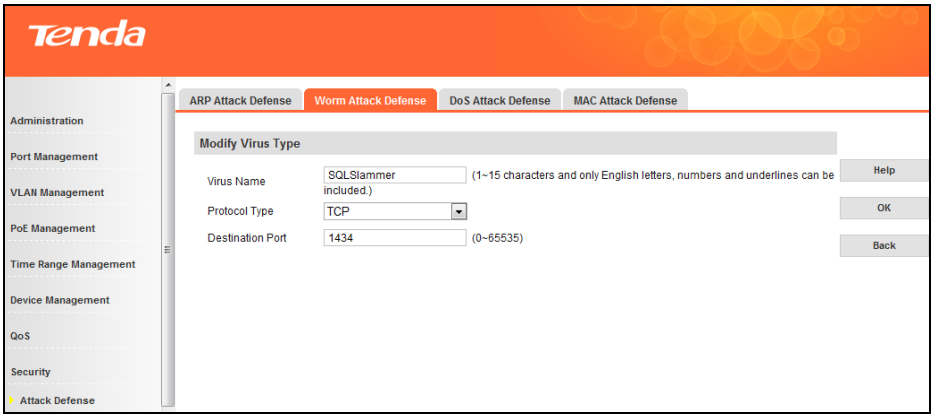
1. Click **New** to enter screen below



2. Enter the virus name, say, SQLSlammer.
3. Specify a protocol, say, TCP or UDP.
4. Specify the TCP destination port number, say, 1434.
5. Click **OK** and defense against this virus attack is automatically enabled. What you just added will appear on the page.



- To undo defense against this virus attack, simply uncheck it or directly click **Delete**. To delete a batch of items simultaneously, simply click **Delete All**.
- To edit an existing virus attack defense entry, simply click it to enter the corresponding interface. Re-configure it and then click **OK**.



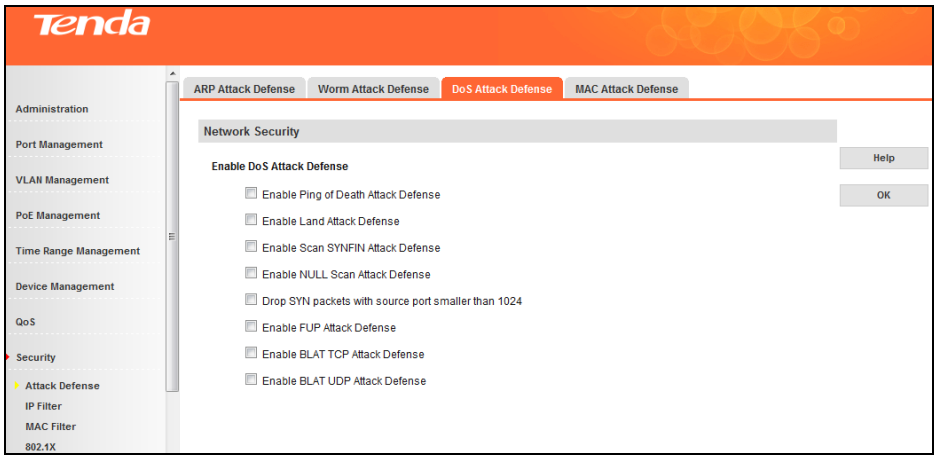
Note----------

The device supports up to 20 virus types.

DoS Attack Defense

DoS Attack Defense prevents potential attackers from making a machine or network resource unavailable to its intended users by saturating the target machine with large amount of malicious communication requests.

Click **Security -> Attack Defense -> DoS Attack Defense** to enter interface below:



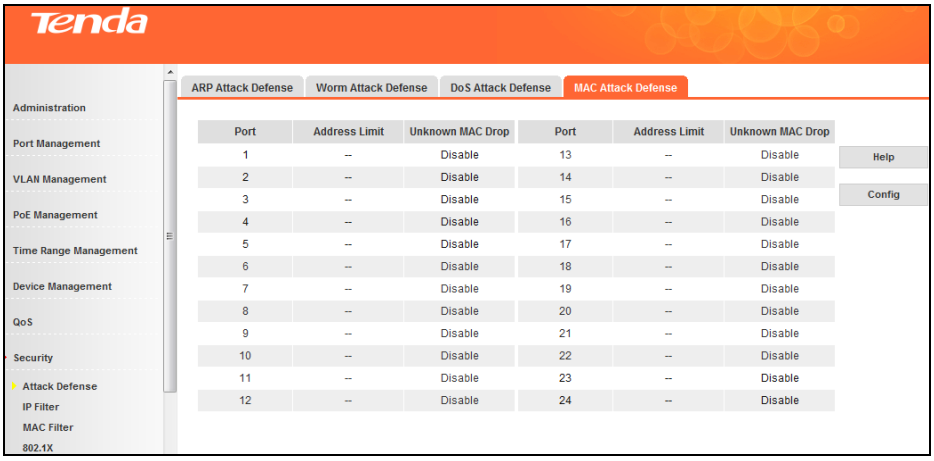
This section displays and allows you to config the DoS Attack Defense settings. By default all DoS Attacks are disabled. For detailed description of each DoS attack, click the **Help** button on the web page.

MAC Attack Defense

MAC Attack Defense prevents the device from learning large amount of unnecessary source MAC addresses so that forwarding capability will not be degraded due to an oversized MAC address table.

The MAC Attack Defense is implemented on the device by limiting the number of MAC addresses that can be learned on each port.

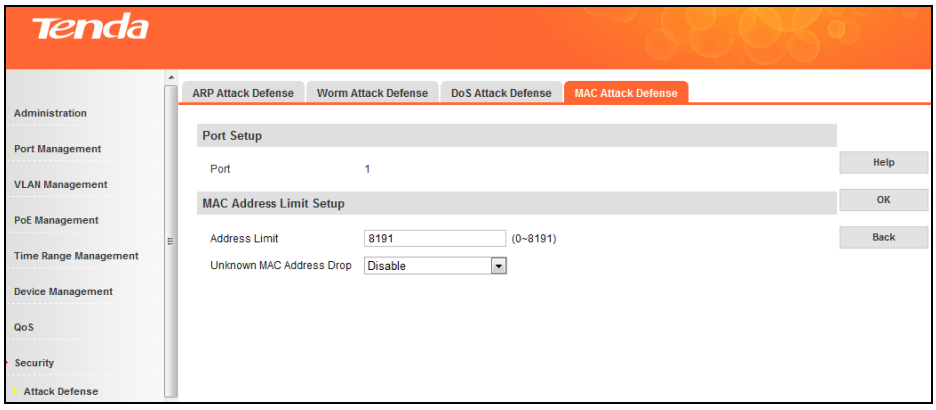
Click **Security -> Attack Defense -> MAC Attack Defense** to enter interface below:



This section displays the current number of MAC addresses that can be learned on corresponding ports and drop status of unknown MAC address. By default, the number of MAC addresses that a port can learn is not limited.

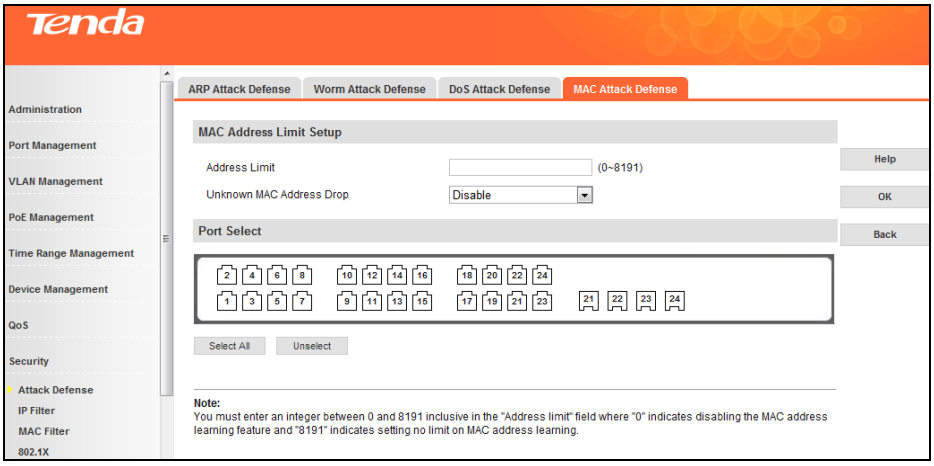
➢ To set a MAC address learning limit on a single port

Click the corresponding port to enter the configuration page.



➢ To set a MAC address learning limit on a batch of ports concurrently

Click **Config** to enter corresponding page for configuration.



Address Limit: Config it according to the actual network environment.
By default, the number of MAC addresses that each port can learn is not limited.
Unknown MAC Address Drop: If enabled, corresponding port(s) will discard packets where source MAC addresses are not in the MAC address table when reaching the set address limit, otherwise, continue forwarding. By default, this option is disabled on all ports.

Note----------

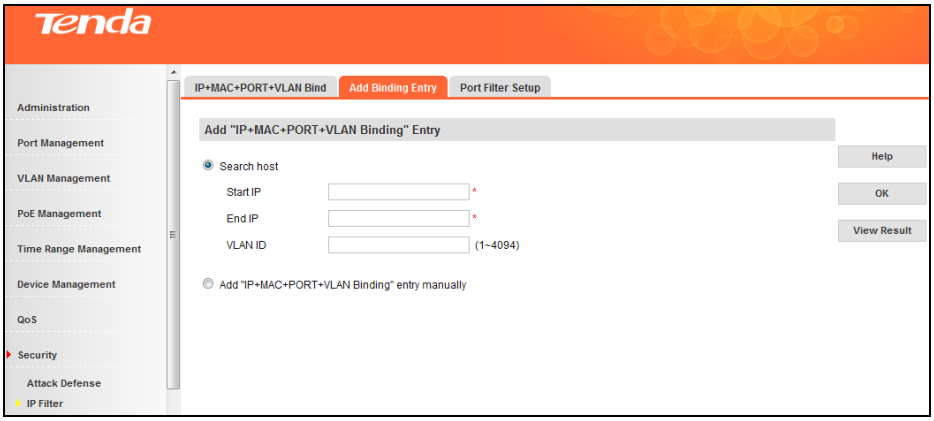
If MAC addresses the port learned are bound as static MAC addresses manually, this port will continue to learn MAC addresses until the maximum MAC number is reached.

4.8.2 IP Filter

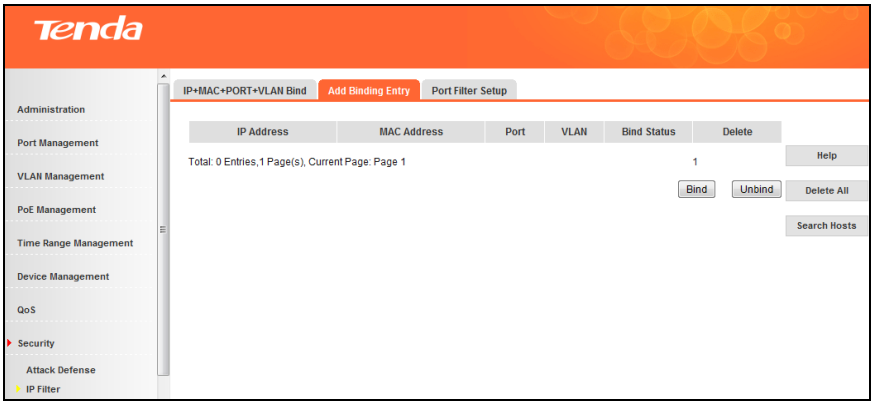
After you have configured and activated the IP+MAC+Port+VLAN Binding settings, the device will perform strict packet filter to further secure the network.

➢ **To search for IP+MAC+Port+VLAN Binding entries, smart binding.**

Click **Security -> IP Filter -> Add Binding Entry** to enter interface below:



1. Click **Search hosts**.
2. Enter an IP address in the Start IP field, for example "192.168.100.1".
3. Enter an IP address in the End IP field, for example "192.168.100.254".
4. Enter a number in VLAN ID field, for example "1", and this field is optional.
5. Click **OK** to start searching.
   Searched IP addresses will be displayed on pages after search.



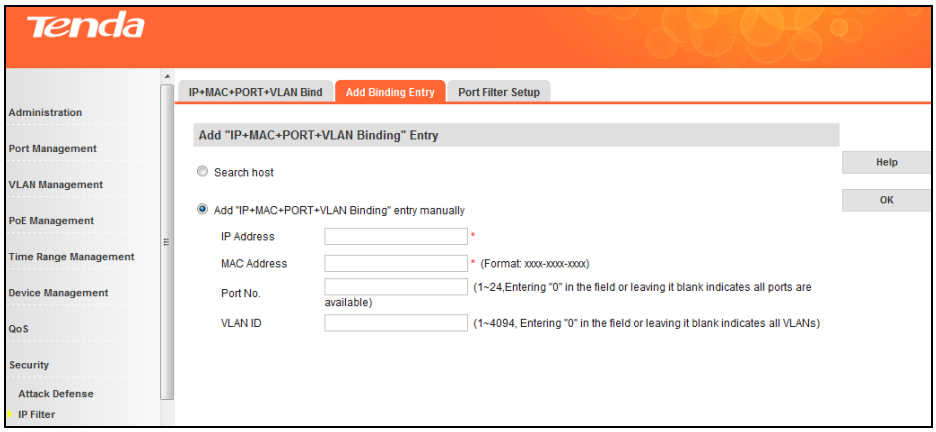
6. Click **Bind** and system will automatically bind the IP addresses on the current page, namely 10 items.

To re-search for host, click the **Search Hosts** button to return to the search page.

To delete a single host just searched, click the corresponding **Delete** button. To delete all searched host, click **Delete All**.

- **To add IP+MAC+Port+VLAN Binding entries manually**

1. Click **Security -> IP Filter -> Add Binding Entry** and on the appearing interface, select **Add IP+MAC+Port VLAN Binding entry manually**.

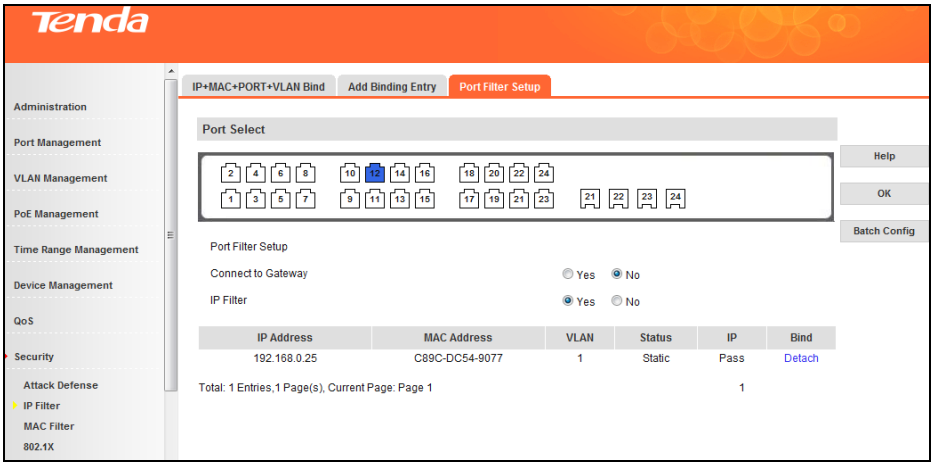


2. Enter an IP address, for example "192.168.10.1".
3. Enter a MAC address, for example "aaaa-bbbb-cccc".
4. Enter a port number, for example "24". This item is optional.
5. Enter a number in VLAN ID field, for example "1". This item is optional.
6. Click **OK**. The IP+MAC+Port+VLAN Binding screen will display added binding entries.

- **Port Filter Setup**

The IP+MAC+Port+VLAN Binding entries take effect only after the IP filter feature is enabled.

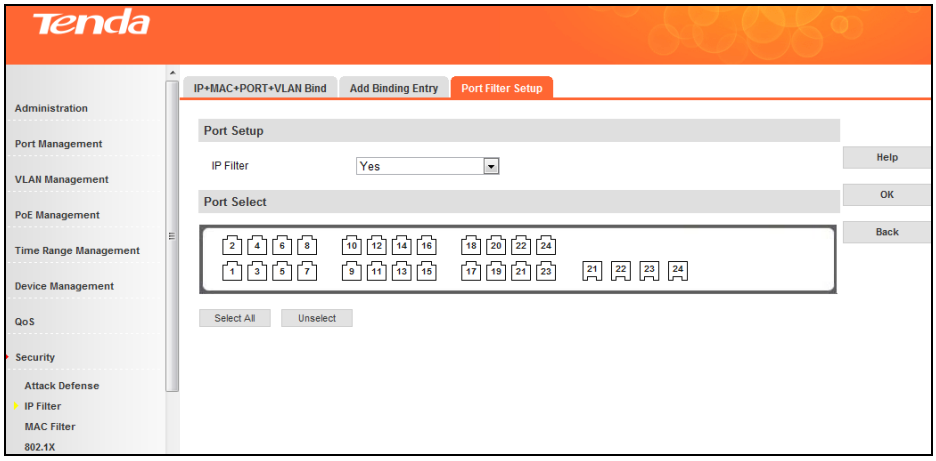
To config Port Filter settings on a single port: click **Security -> IP Filter -> Port Filter Setup**, select a port NO, select **Yes** from the IP Filter drop-down list and click **OK** to enable the IP filter feature.



Fields on the screen are described below:

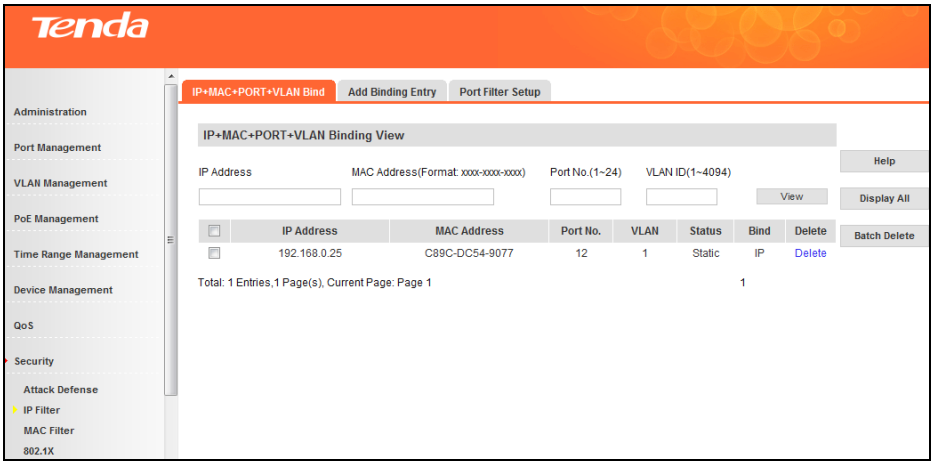
Field	Description
Connect to Gateway	Determine whether to connect selected port to gateway. Yes: Connect selected port to gateway and IP Filter is unavailable for configuration. No: Do not connect selected port to gateway and IP Filter is available for configuration. Note: It is advisable to connect application-specific ports such as a router port to the gateway.
IP Filter	Select whether to filter IP packets on specific port(s). Yes: Selecting **Yes** indicates corresponding port(s) are regarded as untrusted port(s); only IP packets that match the active IP+MAC+Port+VLAN Binding entries can pass such port(s), otherwise are dropped directly. No: Selecting **NO** sets corresponding port(s) as trusted port(s); namely, IP packets will not be examined when passing through such port(s). Note: Up to 126 IP+MAC+Port+VLAN Binding entries takes effect after the IP filter feature is enabled. For the "Bind" status, if "Pass" is displayed, it indicates the corresponding binding entry is activated; if "--" is displayed, it indicates IP filter is not enabled on the port.
Detach	When configuring IP filter settings, you can deactivate the corresponding binding entry by clicking the **Detach** button.

To config Port Filter settings concurrently on a batch of ports: click **Batch Config** to enter below screen; and then click **OK** after you have finished required settings.



➢ **Delete binding entry**

To delete a batch of binding entries concurrently, click the **Batch Delete** button on the IP+MAC+Port+VLAN Binding screen; to delete a single binding entry, on the IP+MAC+Port+VLAN Binding screen, click the **Delete** button at the end of the entry.



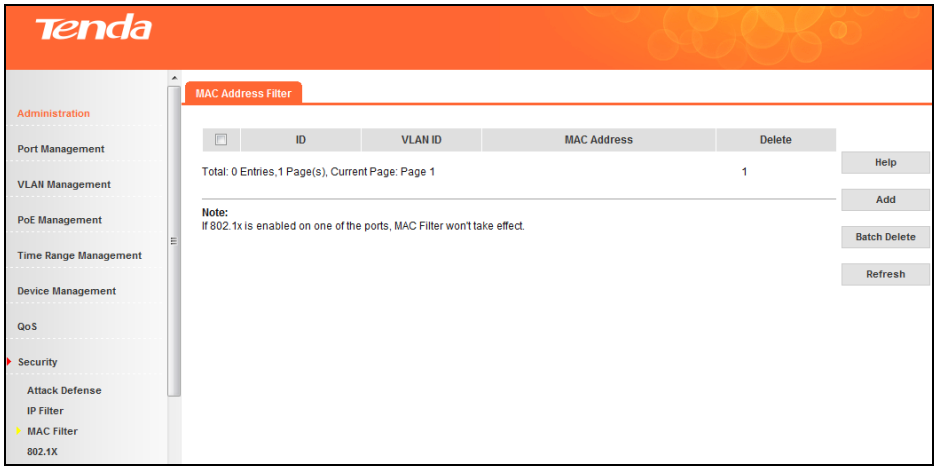
Note----------

After you delete a binding entry on a port, go to Port Filter Setup interface to check whether the IP filter is disabled, if not, such port will not be able to receive any IP packets. Thus, before you delete an IP+MAC+Port+VLAN Binding entry, ensure that the IP filter has been disabled.

4.8.3 MAC Filter

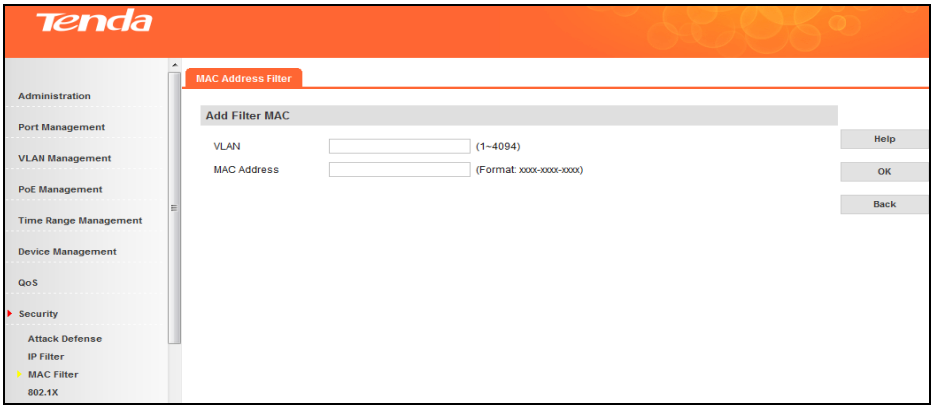
Once MAC filter settings are configured on this device, the device will check source and destination MAC addresses of ingress packets. If source and destination MAC addresses already exist in the MAC filter table, these packets will be discarded.

Click **Security -> MAC Filter -> MAC Address Filter** to enter interface below:



➢ To add MAC address filter

1. Click **Add** to enter interface below:



2. Specify the VLAN ID in the VLAN field. Valid range is 1-4094 and the VLAN ID must already exist.
3. Enter the MAC address you wish to filter, such as “0000-aaaa-aaaa”.
4. Click **OK**.

➢ To delete a single MAC address filter entry, click the corresponding **Delete** button.

➢ To batch delete MAC address filter entries, click **Batch Delete**.

Note----------

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

4.8.4 802.1X

➢ **802.1X Overview**

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 mechanismfor devices wishing to attach to a LAN or WLAN.IEEE 802.1X defines the encapsulation of EAP over LAN" or EAPOL. 802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The

supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term “supplicant” is also used interchangeably to refer to the software running on the client that provides credentials for the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols. The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant’s identity has been validated and authorized. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

- **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, it will then 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**

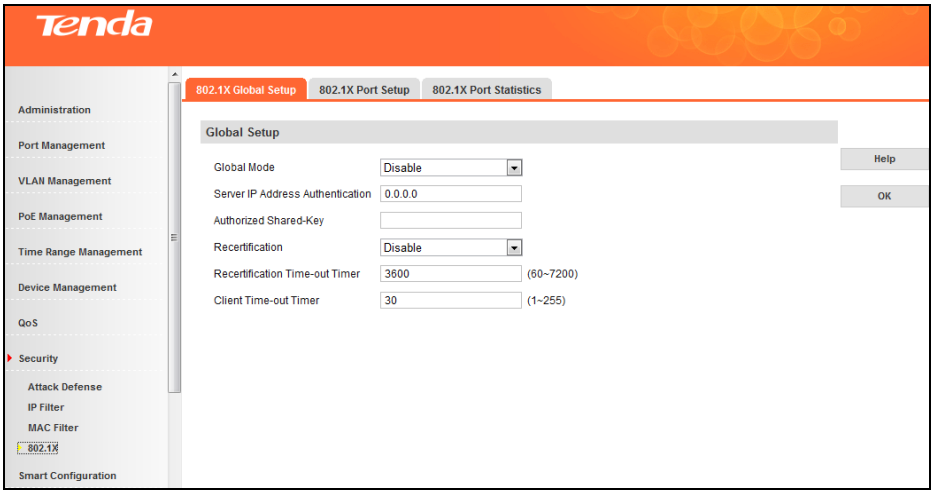
This device supports both port based access control method and MAC based access control method.
When port based access control is adopted, as long as the first user connected to this port is authenticated successfully, other users accessed can use network resources without being authenticated. However, if the first user is disconnected, other users will be unable to access Internet.
When MAC based access control is adopted, all users connected to this port need to be authenticated respectively. If some user is disconnected, only this user is unable to access Internet.

- **802.1X Port Control Mode**

Auto: Port is initially in an "unauthorized" status; in this status, it can only transfer/receive EAPoL messages but cannot access network resources. Once authenticated, the port control mode will toggle to be authorized and users can access Internet.
Enforce Authorization: The port is always in an "authorized" status and can implement communication without being authenticated.
Enforce Unauthorization: The port is always in an "unauthorized" status and can only be used to access device's management interface but cannot implement communication.

802.1X Global Setup

To configure 802.1X settings globally, click **Security -> 802.1X -> 802.1X Global Setup**.

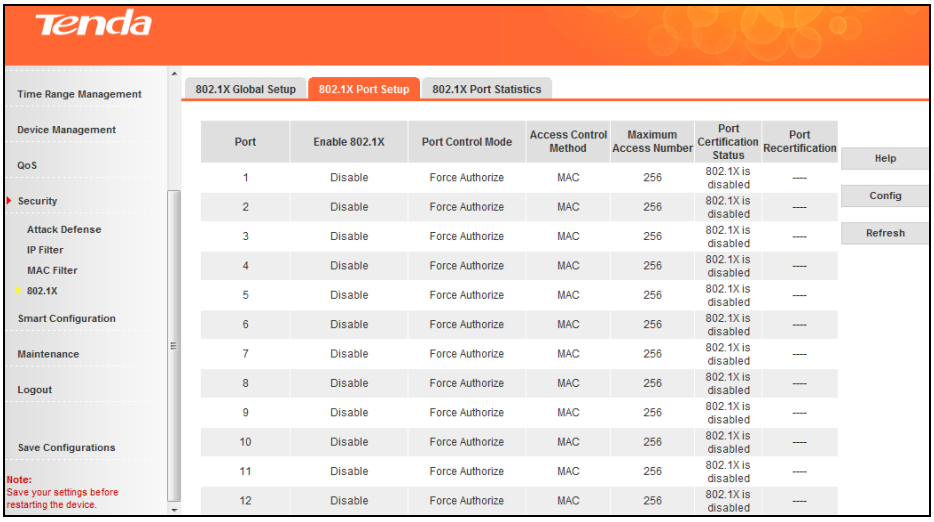


Fields on the screen are described below:

Field	Description
Global Mode	Configure global 802.1X status Enable: Enable 802.1X feature globally. Disable: Disable 802.1X feature globally. By default, the 802.1X feature is disabled globally on the device. Note: 802.1X settings take effect only when the 802.1X feature is enabled on both the device and specific ports.
Server IP Address Authentication	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.
Recertification	Enable or disable re-authentication on all ports.
Recertification 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 Request/Challenge request to a targeted client. If no response is received from the client within the set time length, switch will resend the request.

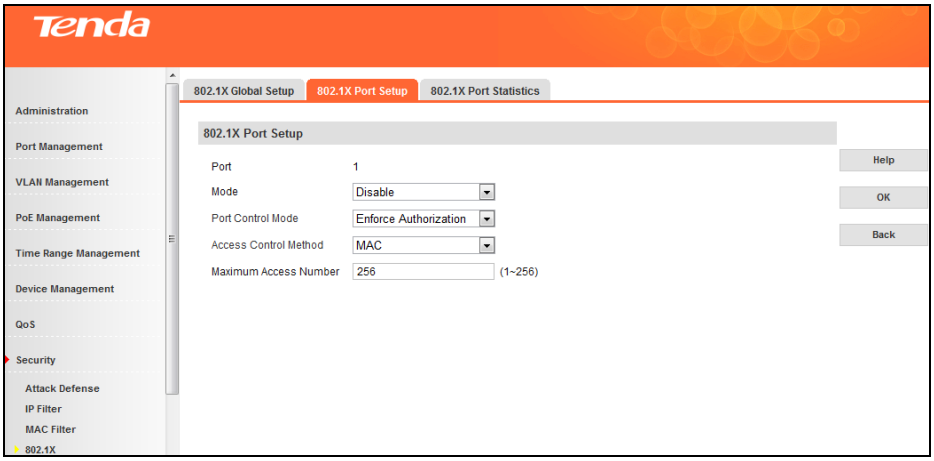
802.1X Port Setup

Click **Security -> 802.1X -> 802.1X Port Setup** to enter interface below:



➢ To configure MAC based 802.1X settings on a single port

1. Click the corresponding port.



2. Select **Enable** from **Mode** drop-down list and **Auto** from **Port Control Mode** drop-down list.
3. Select **MAC** from **Access Control Method** drop-down list.
4. Specify the **Maximum Access Number** field. The default is 256.
5. Click **OK** and the 802.1X feature will be enabled. Then users connected to this port need authenticating first to communicate with other devices.

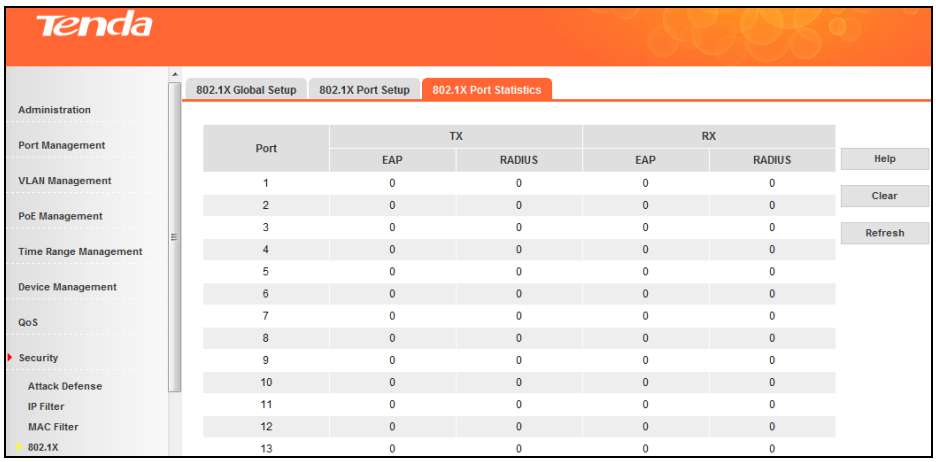
Note----------

If **PORT** is select from Access Control Method drop-down list, the default maximum access number is 1. But this does not indicate only one user can be connected to this port. It indicates as long as one user connected to this port is authenticated, other users can also communicate with other devices via this port.

➢ To configure MAC based 802.1X settings on multiple ports, click **Config**, finish required settings and click **OK**.

802.1X Port Statistics

To display 802.1X port statistics, click **Security -> 802.1X -> 802.1X Port Statistics** as below:



Fields on the screen are described below:

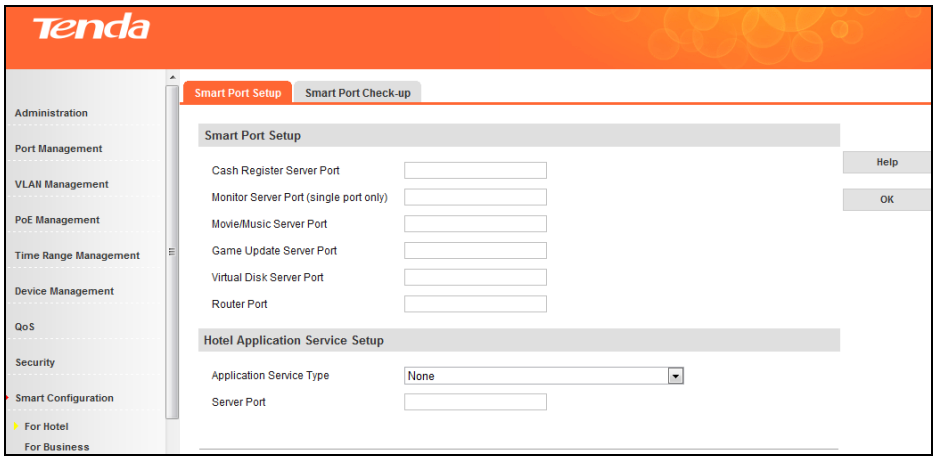
Field	Description
Port	Corresponding Port Number
TX	EAP: EAP packets sent from ports to 802.1x clients. RADIUS : RADIUS packets sent from ports to 802.1x server.
RX	EAP: EAP packets received from 802.1x clients to ports. RADIUS: RADIUS packets sent from ports to 802.1x server.
Clear	Clear all statistics.
Refresh	Refresh the statistics.

4.9 Smart Configuration

4.9.1 For Hotel

Smart Port Setup

Click **Smart Configuration -> For Hotel -> Smart Port Setup** to enter interface below:



Fields on the screen are described below:

Field	Description
Cash Register Server Port	The priority of a Cash Register Server Port will be automatically set to 7 and 2 cash register server ports can be configured.
Monitor Server Port (single port only)	If a port is set as a monitor server port, flow control and monitoring port will be automatically enabled on it.
Movie/Music Server Port	If a group of ports are set to connect movie/music servers, flow control will be automatically enabled on them and port priority will be automatically set to 5 respectively.
Game Update Server Port	If a group of ports are set to connect game update servers, flow control will be automatically enabled on them and port priority will be automatically set to 5 respectively.
Virtual Disk Server Port	If a group of ports are set to connect virtual disk servers, flow control will be automatically enabled on them and port priority will be automatically set to 5 respectively.
Router Port	Ports connect to routers (router port) will be automatically enabled as mirrored ports and apply port priority of 5.

Hotel Application Service Setup

The device supports 3 application/service types:

- **Diskless Service:** Diskless service enables a diskless node (or diskless workstation) without

installed physical hard drives to employ network booting to load its operating system from a server. It lowers hotel production/maintenance cost and delievers unified management at ease for IT admininstrators.

- **GHOST Service:** GHOST (General Hardware-Oriented System Transfer) is a disk cloning program that supports unicast, multicast (by default) and broadcast transfers. Hotel administrators can use it to copy OS straight from a single PC to a batch of PCs all at once.
- **Intel® Platform Administration Technology service:** Intel® Platform Administration Technology Agent software actively broadcasts requests to join server's management domain and server determines whether to accept the client. When accepting such client, the Intel® Platform Administration Technology system will remotely control and manage assets thereof, including hard drive image and update package.

By default, no service type is enabled.

Server Port: Specify port(s) to be connected to server.

If the port is used for diskless service, system will automatically enable flow control on it and set its port priority to 3.

If the port is used for GHOST service, system will automatically disable flow control and enable IGMP-Snooping on it.

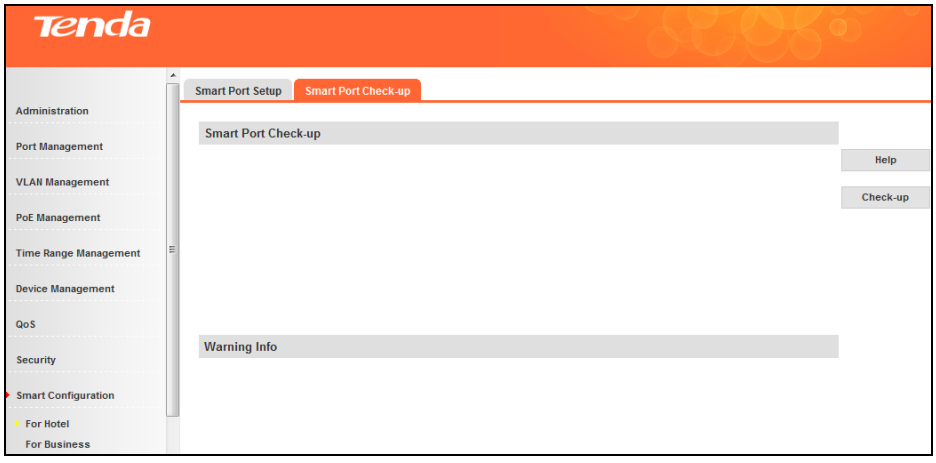
If the port is used for Intel® Platform Administration Technology service, system will automatically enable IGMP-Snooping on it.

Note----------

Cashier register service and monitor service can share a single port; movie/music service, game update service and virtual disk service can be implemented on a single port. Except the above mentioned, any two services cannot share one port.

Smart Port Check-up

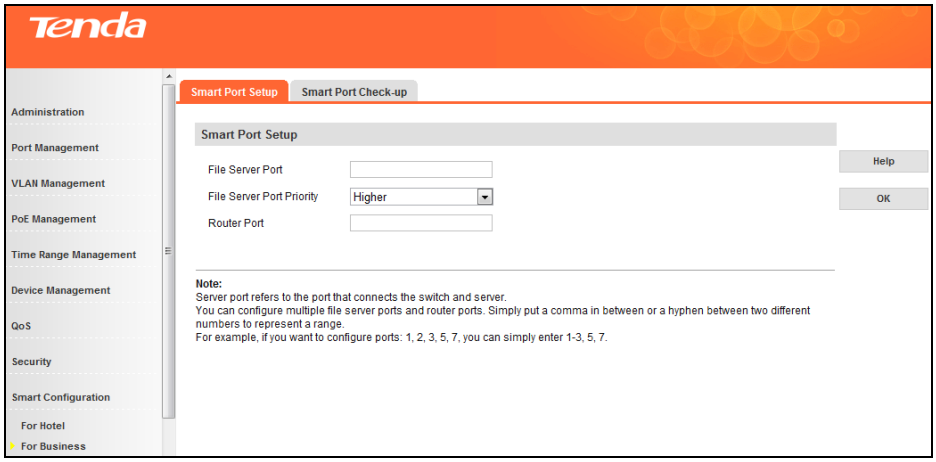
Click **Security -> For Hotel -> Smart Port Check-up**, on the appearing interface you can check hotel smart port settings. Click **Check-up** to check smart port settings and it will prompt you with tips if detecting changes in the settings.



4.9.2 For Business

Smart Port Setup

Click **Smart Configuration -> For Business -> Smart Port Setup** to enter interface below (Specify file server port and router port according to your practical needs.):



Fields on the screen are described below:

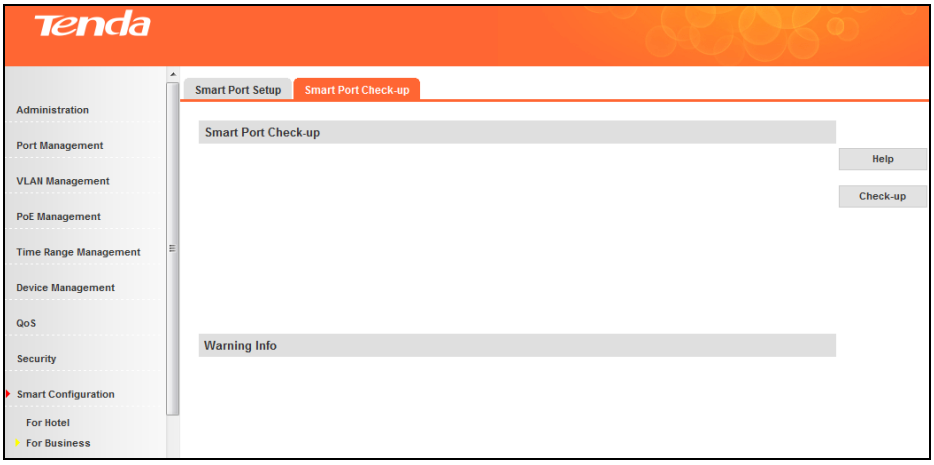
Field	Description
File Server Port	Specify a port to connect to a file server.
File Server Port Priority	Specify priority for the file serve port, say, Higher, High, Standard or Low, which represents 7, 5, 3, 1 respectively. For example: If you select High, priority of the file serve port will be set to 5.
Router Port	Specify a port to connect to a router. The priority of a Router Port for this switch will be automatically set to 5.

Note----------

File server port and router port cannot be the same.

Smart Port Check-up

Click **Security -> For Business -> Smart Port Check-up**, on the appearing interface you can check hotel smart port settings. Click **Check-up** to check smart port settings and it will prompt you with tips if detecting changes in the settings.



4.10 Maintenance

4.10.1 Syslog

Syslog Overview

As the system information hub, system logs classify and manage system information. Together with the debugging command, system logs offer a powerful support for network administrators and developers to monitor network operation and diagnose malfunction.

The system logs have the following features:

1) Classification of Syslog

Log: log info

Trap: warning info

Debug: debugging info

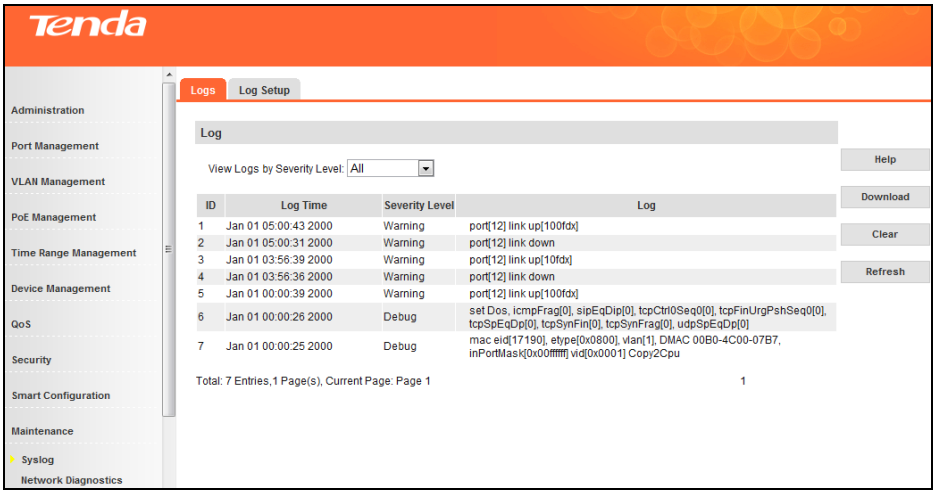
2) Eight Levels of Syslog

The Logs of switch are classified into the following eight levels. The smaller value has the higher priority.

Severity	Level	Description
Emergency	1	The system is unusable
Alert	2	Action 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
Debug	8	Debug-level messages

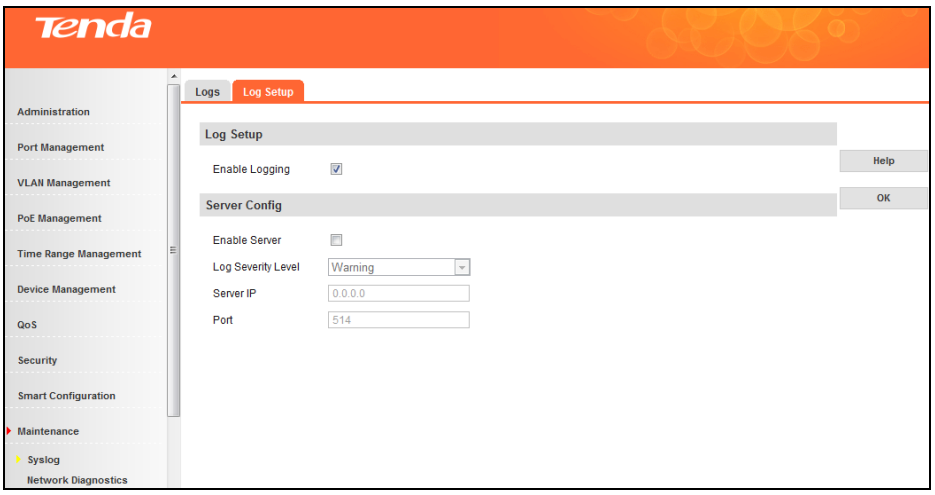
Logs

To view syslogs, click **Maintenance -> Syslog -> Logs** as below:



Log Setup

To configure log settings, click **Maintenance -> Syslog -> Log Setup** as below:



Fields on the screen are described below:

Field	Description
Enable Logging	Enable/disable Log feature. By default, it is enabled.
Enable Server	Check to enable log server.
Log Severity Level	Only logs of severity level equal to or lower than the specified one can be sent to the log host.
Server IP	Config log server IP address.
Port	By default, it is 514 and can't be configurable.

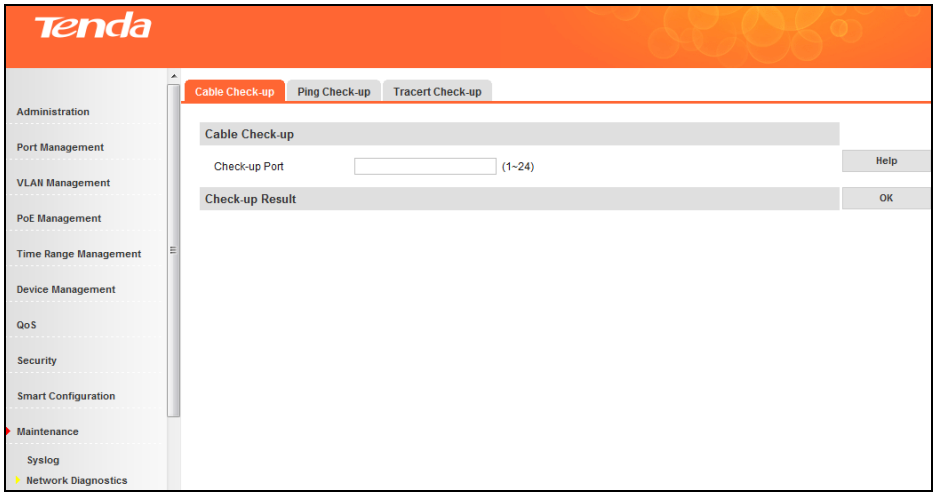
4.10.2 Network Diagnostics

This device provides Cable check-up, Ping check-up and Tracert check-up functions for network diagnose.

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 interface below:



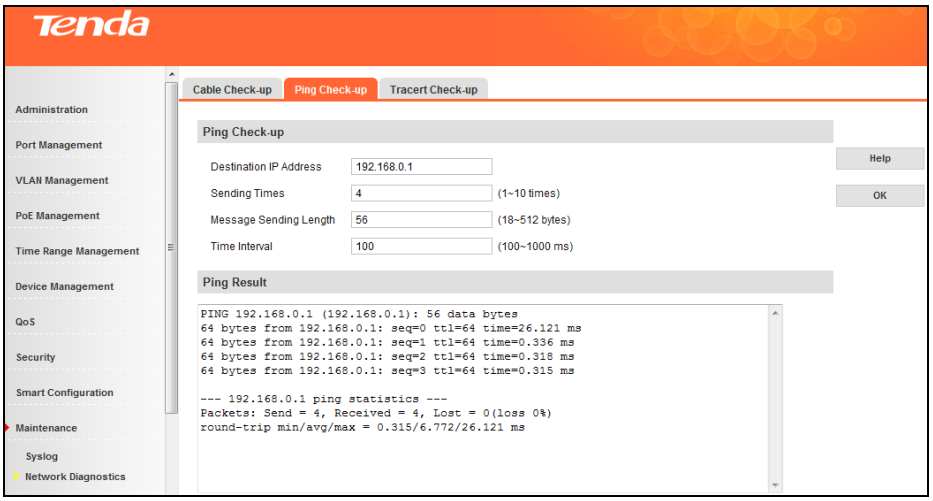
Specify the check-up port field as you wish and click **OK**. Then the corresponding check-up result will be displayed.

Ping Check-up

Ping Overview

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 operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response. In the process it measures the time from transmission to reception (round-trip time) and records any packet loss. The results of the test are printed in the form of a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times, and sometimes the standard deviation of the mean. Ping does not evaluate or compute the time to establish the connection; it only gives the mean round-trip times of an established connection with an open session.

To implement ping check-up, click **Maintenance -> Network Diagnostics -> Ping Check-up**, finish required settings and click OK. Then Ping check-up begins and the ping info will be displayed in the ping result box.



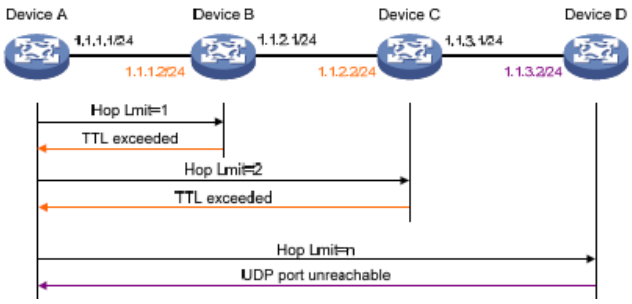
Fields on the screen are described below:

Field	Description
Destination IP Address	Specify the destination host IP which should be in the same network segment as this device. This field is blank by default.
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.

Tracert Check-up

Tracert Overview

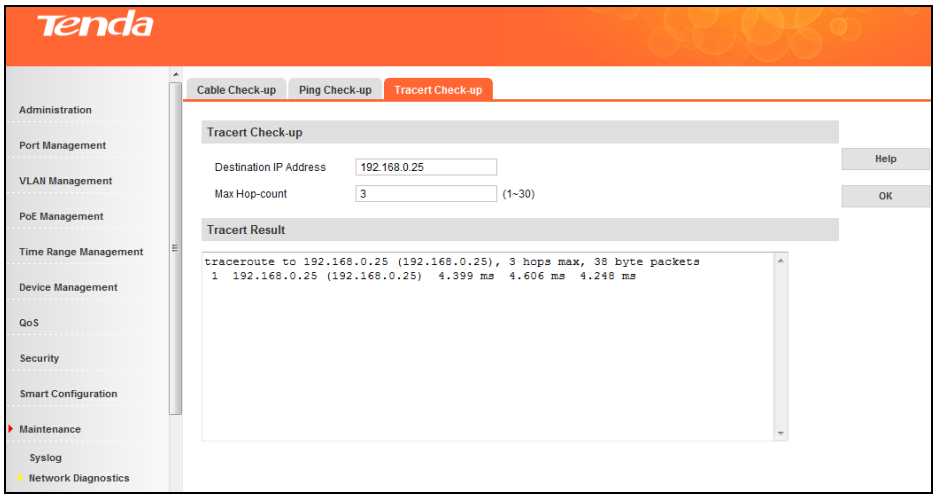
Tracert is a computer network diagnostic tool for displaying the route (path) and measuring whether network connection is available or not. When malfunctions occur to the network, you can locate trouble spot of the network with this tracert test. Tracert working diagram is shown below:



Tracert is also implemented on the basis of ICMP. The tracert working principle figure is shown above:

(1) Device A transmits an IP packet to Device D, and TTL value is 1. And the UDP port number can't be used by any application program on Device D.

(2) Device B (the first L3 device 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 L3 device'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 L3 device's IP (1.1.2.2);
(5) The process mentioned above is performed continually until packets reach Device D. As no application program on Device D uses this UDP port, Device D replies with an unreachable ICMP error (Device D's IP 1.1.3.2 included).
(6) When Device A receives this unreachable ICMP error, it knows packets have reached Device D and the route packets have passed from Device A to Device D is obtained (1.1.1.2; 1.1.2.2; 1.1.3.2).
To implement tracert check-up, click **Maintenance -> Network Diagnostics -> Tracert Check-up**, finish required settings and click **OK**. Then tracert check-up begins and the tracert info will be displayed in the tracert result box.

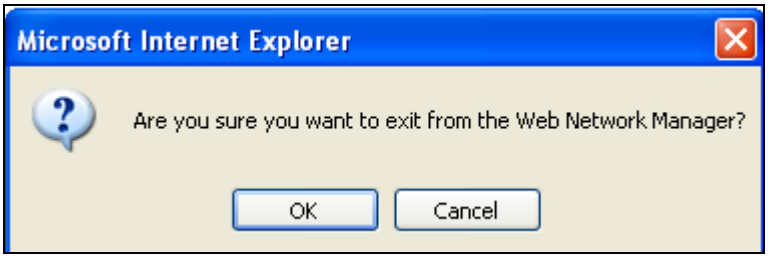


Fields on the screen are described below:

Field	Description
Destination IP Address	Enter the IP address of the destination device.
Max Hop-count	Specify the maximum number of the L3 devices the test data can pass through. Valid range is 1-30 and the default is 3.
Tracert Result	Display the tracert info.

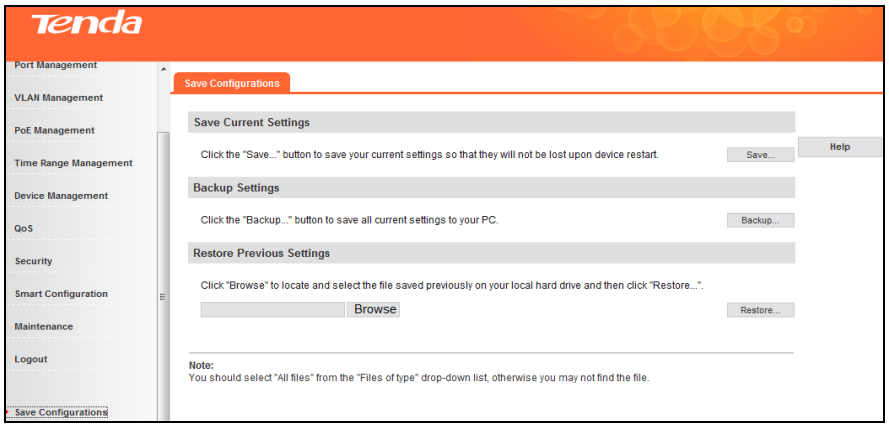
4.11 Logout

This section allows you to exit from the switch's web manager safely.



4.12 Save Configurations

Configurations on switch will be lost if they are not saved before switch reboots. So do save them on this screen before you reboot the switch.



1. Save Current Settings

Use this feature to save device current configurations to ensure you will still have them on the switch even after the device restarts.

Note: It takes about 10 seconds to save device current configurations. Do not operate or interrupt the switch during this period. Otherwise parts of the configurations may be lost. When the page refreshes, the action of saving configurations is completed.

2. Backup Settings

Once you have configured the device the way you want, you can save all settings to your local hard drive, which can later be imported to the device in case that it is restored to factory default settings.

To back up current settings, click the **Backup** button.

Note: To backup current settings, you must first click **Save** to save them. Do not disconnect the device from power supply and the management PC during this process.

3. Restore Previous Settings

To restore settings that are previously saved on your local hard drive, click the **Browse** button to locate and select the file and then click the **Restore** button.

Chapter 5 CLI Configuration

5.1 Login

For login method, please see sections 3.2-3.3, which describe available Telnet commands that can be used to config and manage the switch as well as how to manage the switch via the console port.

5.2 Features of Command Interface

Below lists and explains available commands for your references. The command line interface has the following features:

- Entering a question mark "?" displays online help.
- The **Tab** key on your keyboard serves as a functional key to supplement a command. For example, you can only enter a command string of "con" and press the **Tab** key to populate the rest automatically: if multiple matches are found, they will all be displayed for your selection; if only one match is found, then it will be populated to the "con" field automatically.
- To go back to previous directory, press the "/" key. "/" is invalid in "Tenda #".
- To activate a command, press **Enter** after you finish entering it.

Three access rights are available for the command line interface:

- admin—The administrator has absolute rights to manage the switch except debugging.
- operator— The operator has all the same rights as administrator except rights to "Firmware Update", "User", "Reset" and "Reboot' features.
- user —The user has only the right to read/view switch's current settings but no right to manage/config the switch.

5.3 Command Line Configuration Guide

5.3.1 Commands for entering common views

TENDA# configure terminal
TENDA (config)#
Note: Enter configuration view

TENDA (config)# interface gigabitethernet 0/1
TENDA (config-if)#
Note: Enter single-port view

TENDA (config)# interface range gigabitethernet 0/1-24
TENDA (config-if)#
Note: Enter multiple-port view

5.3.2 Config system info

TENDA (config)# snmp-server chassis-id TEG3224P
Note: Config device name as TEG3224P

TENDA (config)# snmp-server contact Tenda

Note: Config contact as Tenda

TENDA (config)# snmp-server location Shenzhen
Note: Config location as Shenzhen

5.3.3 Config IP address manually

TENDA (config)# ip address 192.168.111.217 255.255.255.0
Note: Config a static IP address
TENDA (config)#ip route 192.168.111.1
Note: Config a gateway IP address

TENDA # show ip
Note: View configured IP address (es)

5.3.4 Enable DHCP client to obtain an IP address

TENDA(config)# ip dhcp
Note: Enable DHCP client and switch will obtain an IP address automatically from a DHCP server on the network

TENDA(config)# show ip
Note: View the IP address obtained automatically

5.3.5 User configuration

TENDA(config)# local-user 123456 admin admin
Note: Change default password to 123456

TENDA(config)# local-user abc abc admin
Note: Add a user name of "abc" with the password of "abc" and access mode of "Administrator"

TENDA(config)# local-user admin admin user
Note: Change the access mode of "Administrator" to "User"

TENDA(config)# local-user 1a 1a user
Note: Add a user name of "la" with the password of "la" and access mode of "User"

TENDA(config)# local-user 123 123 opt
Note: Add a user name of "123" with the password of "123" and access mode of "Operator"

TENDA(config)# no local-user user
Note: Delete the user

TENDA# service telnet start
Note: Start Telnet service

TENDA# no service telnet
Note: Disable Telnet service

5.3.6 System Time Configuration

TENDA# clock set 14:09:30 4 11 2012

Note: Manually set system date and time to Apr 11 2012 and 14：09：30 respectively

TENDA(config)# sntp enable
Note: Enable SNTP server

TENDA(config)# no sntp
Note: Disable SNTP server

TENDA(config)# sntp preferred-server 192.168.111.79
Note: Set Primary SNTP Server IP address to 192.168.111.79
TENDA(config)# sntp alternate-server 192.168.111.78
Note: Set Secondary SNTP Server IP address to 192.168.111.78

TENDA(config)# sntp broadcastdelay 100
Note: Set Sync Interval to 100s

TENDA(config)# clock timezone GMT-0800
Note: Set Time Zone to (GMT-0800)Beijing

5.3.7 Reset and reboot

TENDA# erase startup-config
Note: Delete all current settings and restore device to factory default settings

TENDA# reload
Note: Reboot switch (To restore factory defaults, system first deletes current settings and then restarts)

5.3.8 Firmware Update

TENDA# archive download-sw 192.168.111.79：G3224_V100R004.bin

Note: Load firmware from a TFTP server for upgrade

TENDA#archive startup-config 192.168.111.79：mib.conf

Note: Save firmware to local hard drive via a TFTP server

5.3.9 Web login timeout configuration

TENDA(config)# http redirect timeout 300

Note: Config web login timeout interval as 300 seconds

TENDA# show http redirect timeout

Note: View web login timeout settings

5.3.10 Config port settings

TENDA(config)# interface gigabitethernet 0/3

Note: Enter the interface for configuring port 3

TENDA(config)# interface range gigabitethernet 0/3-8,12,15

Note: Enter the interface for configuring a batch of ports concurrently

TENDA(config-if)# speed 100

Note: Set port speed to 100

TENDA(config-if)# speed auto

Note: Set port speed to auto (auto-negotiation)

TENDA(config-if)# duplex full

Note: Set duplex to full duplex

TENDA(config-if)#cos 7

Note: Set port priority to 7

TENDA(config-if)# flow-control on

Note: Enable flow control

TENDA(config-if)# no shutdown

Note: Enable port

TENDA(config-if)# storm-control broadcast level 20%

Note: Set storm constrain ratio to 20%

TENDA(config-if)# port-isolated

Note: Enable port isolation

TENDA(config-if)# mtu 9600

Note: Set max jumbo frame size to 9600B on the port

5.3.11 Port mirroring configuration

TENDA(config)# monitor destination interface gigabitethernet 0/8

Note: Config port 8 as the mirroring destination port

TENDA(config)# monitor source interface range gigabitethernet 0/1-3 rx
Note: Config ports 1-3 as mirroring source ports and sniffer mode as Ingress.

TENDA(config)# monitor source interface range gigabitethernet 0/4-5 tx
Note: Config ports 4-5 as mirroring source ports and sniffer mode as Egress.

TENDA(config)# monitor source interface gigabitethernet 0/6 both
Note: Config port 6 as mirroring source port and sniffer mode as Egress & Ingress.
TENDA(config)# no monitor
Note: Clear mirroring settings

5.3.12 View RX/TX packet statistics

TENDA# show interface gigabitethernet 0/2 counter
Note: View RX packet statistics on port 2
TENDA# show interfaces counter
Note: View statistics on all ports

5.3.13 Config Port Rate Limit

TENDA(config)# interface range gigabitethernet 0/1
TENDA(config-if)# rate-limit input 100
Note: Set ingress rate limit to 100M on port 1

TENDA(config-if)# rate-limit output 10
Note: Set egress rate limit to 10M on port 1
TENDA(config-if)# no rate-limit input
Note: Clear ingress rate limit on the port

TENDA(config-if)# no rate-limit output
Note: Clear egress rate limit on the port

5.3.14 Config Link Aggregation

- **Create aggregation group**

TENDA(config)# interface range gigabitethernet 0/1-4
Note: Set ports 1-4 as link aggregation member ports
TENDA(config-if)# trunk-group 1 type static
Note: Set aggregation group ID to 1 and type to static

TENDA(config-if)# trunk-group 2 type lacp
Note: Create a LACP static aggregation group: 2

- **Delete aggregation group**

TENDA(config)# interface range gigabitethernet 0/1-2
TENDA(config-if)# no trunk-group
Note: Delete member ports 1-2 from the aggregation group

- **Config LACP settings**

TENDA(config-if)# lacp priority 65535
Note: Set LACP port priority to 65535

TENDA(config-if)# lacp timeout long
Note: Set timeout to long

TENDA(config-if)# lacp timeout short
Note: Set timeout to short

TENDA(config)# lacp system-priority 65535
Note: Config LACP system priority
TENDA(config)# port-channel load-balance dst-mac
Note: Config destination MAC algorithm

TENDA(config)#port-channel load-balance src-dst-mac
Note: Config source and destination MAC algorithm

TENDA(config)# port-channel load-balance src-mac
Note: Config source MAC algorithm

TENDA(config)# port-channel load-balance src-dst-ip
Note: Config source and destination IP algorithm

- **View aggregation info**

TENDA# show aggregate-port
Note: View aggregation group

TENDA# show lacp all counters
Note: View LACP packet statistics

TENDA# show lacp all internal
Note: View peer LACP port info
TENDA# show lacp all neighbor
Note: View remote LACP port info

TENDA# show lacp sys-id
Note: View local LACP system priority and MAC address

5.3.15 VLAN configuration

- **Add 802.1Q VLAN**

  TENDA# configure terminal
  TENDA(config)# vlan 2
  Note: Create a new QVLAN

  TENDA(config)# vlan 3-5
  Note: Create multiple QVLANs

- **Add QVLAN member ports**

  TENDA(config)# interface range gigabitethernet 0/1-10
  Note: Enter the directory of ports 1-10
  TENDA(config-if)# switchport access vlan 2
  Note: Add ports 1-10 to VLAN2

- **Delete QVLAN member ports**

  TENDA(config)# interface range gigabitethernet 0/2,5,6
  Note: Enter the directory of port 2, port 5 and port 6
  TENDA(config-if)# switchport access vlan 1

  Note: Delete port 2 , port 5 and port 6 from QVLAN2(A port must belong to a single VLAN and belong to VLAN1 by default)

- **Delete QVLAN**

  TENDA(config)# no vlan 2
  Note: Delete QVLAN2

  TENDA(config)# no vlan 10-15
  Note: Delete multiple VLANs 10-15

- **Create trunk port**

  TENDA# configure terminal
  TENDA(config)# interface gigabitethernet 0/2
  Note: Enter the directory of port 2
  TENDA(config-if)# switchport mode trunk
  Note: Set port 2 to a Trunk port

  TENDA(config-if)# switchport trunk native vlan 1
  Note: Set the PVID of Trunk port 2 to 1

  TENDA(config-if)# switchport trunk allowed vlan all
  Note: VLAN Set Trunk port to carry all VLANs

TENDA(config)# interface gigabitethernet 0/24
TENDA(config-if)# switchport mode trunk
Note: Set port 24 to a Trunk port
TENDA(config-if)# switchport trunk native vlan 2
Note: Set the PVID of Trunk port 24 to 2
TENDA(config-if)# switchport trunk allowed vlan add 1,2 or 1-2
Note: Set Trunk port to carry VLANs 1-2

TENDA(config-if)# switchport trunk allowed vlan except 2
Note: VLAN Set Trunk port to carry all VLANs except VLAN2

TENDA(config-if)# switchport trunk allowed vlan remove 3
Note: Delete VLAN3 from VLANs allowed to be carried

- **Delete trunk port**

TENDA(config)# interface gigabitethernet 0/24
TENDA(config-if)# switchport mode access
Note: Change port 24 to access port; trunk port 24 becomes nonexistent

TENDA(config)# interface range gigabitethernet 0/1-10
TENDA(config-if)# switchport mode access
Note: Change ports 1-10 to access ports; trunk ports 1-10 become nonexistent

- **Create hybrid port**

TENDA# configure terminal
Note: Enter configuration directory

TENDA(config)# vlan 10，20，30，4094

Note: Create VLAN10，VLAN20，VLAN30，VLAN4094

TENDA(config)# interface gigabitethernet 0/10
Note: Enter the directory of port 10

TENDA(config-if)# switchport mode hybrid
Note: Set port 10 to Hybrid Port

TENDA(config-if)# switchport hybrid native vlan 20
Note: Set the PVID of Hybrid Port 10 to 20

TENDA(config-if)# switchport hybrid allowed vlan tagged add 10-20
Note: Set port 10 to carry tagged VLANs 10-20
TENDA(config-if)# switchport hybrid allowed vlan untagged add 4094

Note: Set port 10 to carry untagged VLAN4094

TENDA(config-if)# switchport hybrid allowed vlan untagged except 30
Note: Set port 10 to carry all untagged VLANs except VLAN30

TENDA(config-if)# switchport hybrid allowed vlan untagged remove 4094
Note: Delete VLAN4094 from untagged VLANs; VLAN4094 then cannot be carried on the port

- **Delete hybrid port**
  TENDA(config)# interface gigabitethernet 0/10
  TENDA(config-if)# switchport mode access
  Note: Delete existing Hybrid port 10

  TENDA(config)# interface range gigabitethernet 0/1-24
  TENDA(config-if)# switchport mode access
  Note: Delete all hybrid ports

- **VLAN mode toggle**
  TENDA(config)# private-vlan on
  Note: Switch VLAN mode from QVLAN to Port VLAN

  TENDA(config)# private-vlan off
  Note: Switch VLAN mode from Port VLAN to QVLAN

- **Create port based VLAN**
  TENDA(config)# private-vlan on
  TENDA(config)# private-vlan VID 24
  Note: Create port VLAN24
  TENDA(config-pvlan)# add 1-20
  Note: Add ports 1-20 to VLAN24

  TENDA(config-pvlan)# remove 10-20
  Note: Delete ports 10-20 from VLAN24

  TENDA(config-pvlan)# add 22,23
  Note: Add port 22 and port 23 to VLAN24

  TENDA(config-pvlan)# remove 8
  Note: Remove port 8 from VLAN24

- **Delete port based VLAN**
  TENDA(config)# no private-vlan 24
  Note: Delete port VLAN 24

- **View VLAN settings**

TENDA(config)# show vlan 2-3

Note: View settings of VLANs 2-3

TENDA(config)# show vlan summry

Note: View settings of all VLANs

5.3.16 MAC VLAN

TENDA# configure terminal

TENDA(config)# vlan 2

Note: Create QVLAN2

TENDA(config)# mac-vlan 0000.0000.0001 vl1 vlan 2 cos 0

Note: Add MAC VLANs whose MAC address is 0000.0000.0001. It is described as v11 and corresponds to vlan2 with cos 0.

TENDA# configure terminal

TENDA(config)# no mac-vlan 0000.0000.0001

Note: Delete the corresponding MAC VLAN whose MAC address is 0000.0000.0001

TENDA# show mac-vlan

Note: View MAC VLAN configurations

5.3.17 Protocol VLAN

TENDA# configure terminal

TENDA(config)# protocol-vlan marble eth-type 0x800 frame-type snap

Note: Create a protocol VLAN with the name “marble”, ethtype “0x800” and frametype “snap”

TENDA(config)# no protocol-vlan marble

Note: Delete the protocol VLAN named marnle

TENDA(config)# interface range gigabitethernet 0/3-5

TENDA(config-if)# protocol-vlan IP vlan 5

Note: Add protocol VLAN named IP on ports 3-5

TENDA(config)# interface range gigabitethernet 0/4

TENDA(config-if)# no protocol-vlan IP

Note: Remove protocol VLANs named IP on all ports

TENDA# show protocol-vlan

Note: Check protocol VLAN info

5.3.18 Voice VLAN

- **Voice VLAN global settings**

TENDA(config)# voice vlan secmode

Note: Enable voice VLAN global security mode

TENDA(config)# no voice vlan secmode
Note: Disable voice VLAN global security mode
TENDA(config)# voice vlan agetime 3600
Note: Set voice VLAN agetime to 3600min

TENDA# show voice vlan global
Note: View voice VLAN global info

- **Voice VLAN port settings**

TENDA# configure terminal
TENDA(config)# interface gigabitethernet 0/6
Note: Enter port settings interface
TENDA(config-if)# switchport voice vlan mode auto
Note: Set voice VLAN mode of port 6 to auto
TENDA(config-if)# switchport voice vlan mode manual
Note: Set voice VLAN mode of port 6 to manual

TENDA(config-if)# switchport voice vlan
Note: Enable voice VLAN on port 6

TENDA(config-if)# no switchport voice vlan
Note: Disable voice VLAN on port 6

TENDA# show voice vlan global
Note: View all ports info in voice VLAN

TENDA# show voice vlan interface gigabitethernet 0/6
Note: View single port info in voice VLAN

- **Voice VLAN OUI settings**

TENDA(config-if)# voice vlan mac-address c234-1200-0000 mask ffff-ff00-0000 description m23
Note: Configure voice VLAN OUI settings

TENDA(config-if)# voice vlan vvid 2
Note: Configure Voice Vlan ID

TENDA# show voice vlan oui
Note: View voice VLAN OUI info

5.3.19 MAC Configuration

- **Config MAC age**

TENDA(config)# mac-address-table aging-time 0

Note: Set MAC address never to age out

TENDA(config)# mac-address-table aging-time 100
Note: Config MAC age time
TENDA(config)# no mac-address-table aging-time
Note: Restore default MAC age settings
TENDA# show mac-address-table age-time
Note: Display MAC age time

- **Config static MAC address**

TENDA(config)# mac-address-table static 0000.0000.0002 interface gigabitethernet 0/1 vlan 1
Note: Add static MAC address of 0000.0000.0002 to port 1 of VLAN1

TENDA(config)# no mac-address-table static
Note: Delete all static MAC addresses
TENDA(config)# no mac-address-table static 0000.0000.0002 interface gigabitethernet 0/1 vlan 1
Note: Delete a single static MAC address

- **Display MAC address**

TENDA# show mac-address-table
Note: Display all MAC addresses

TENDA# show mac-address-table address 0000.0000.0002
Note: Display a single MAC address (similar to View)

TENDA# show mac-address-table dynamic
Note: Display all dynamic MAC addresses

TENDA# show mac-address-table static
Note: Display all static MAC addresses

TENDA# show mac-address-table vlan 1
Note: Display all MAC addresses in VLAN1

TENDA# show mac-address-table interface gigabitethernet 0/5
Note: Display MAC address (es) on a certain port

- **Clear MAC address table**

TENDA# clear mac-address-table
Note: Delete all dynamic MAC addresses

5.3.20 QoS Configuration

- **QoS Priority type select**

TENDA(config)# QoS trust cos
Note: Set Priority Type to CoS

TENDA(config)# QoS trust dscp
Note: Set Priority Type to DSCP

- **QoS Scheduling scheme select**

TENDA(config)# QoS scheduler sp
Note: Set Scheduling Scheme to SP

TENDA(config)# QoS scheduler wrr
Note: Set Scheduling Scheme to WRR
TENDA(config)# wrr-queue bind-width 1 6 10 31

Note: Assign QoS weights: 1，6，10 and 31 to queues: 1，2，3 and 4 respectively

5.3.21 STP Configuration

- **Enable/disable STP**

TENDA(config)# spanning-tree
Note: Enable STP

TENDA(config)# no spanning-tree
Note: Disable STP

- **Config STP system settings**

TENDA(config)# spanning-tree mode stp
Note: Set STP version to stp

TENDA(config)# spanning-tree mode rstp
Note: Set STP version to rstp

TENDA(config)# spanning-tree mode mstp
Note: Set STP version to mstp

TENDA(config)# spanning-tree bpdu-forward broadcast
Note: Broadcast BPDU packets
TENDA(config)# spanning-tree bpdu-forward filter
Note: Filter BPDU packets

TENDA(config)# spanning-tree max-age 6
Note: Set max age to 6s

TENDA(config)# spanning-tree hello-time 1
Note: Set Hello Time to 1s

TENDA(config)# spanning-tree forward-time 4
Note: Set Forward Delay to 4s

TENDA(config)# spanning-tree mstp max-hops 30
Note: Set max hops to 30

TENDA(config)# spanning-tree mstp 0 priority 32768
Note: Set instance priority

Note----------

BPDU message broadcast and filter take effect when STP is disabled.

- **Reset STP system settings**

TENDA(config)# no spanning-tree mode
Note: Delete current STP version setting and restore it to the default mstp

TENDA(config)# no spanning-tree max-age
Note: Delete current max age setting and restore it to the default 20

TENDA(config)# no spanning-tree hello-time
Note: Delete current Hello Time setting and restore it to the default 2

TENDA(config)# no spanning-tree forward-time
Note: Delete current forward delay setting and restore it to the default 15
TENDA(config)# no spanning-tree mstp max-hops
Note: Delete max hop setting and restore it to the default 20

TENDA(config)# no spanning-tree mstp 0 priority
Note: Delete instance bridge priority setting and restore it to the default 30768

- **Configure MSTP domain**

TENDA(config)# spanning-tree mstp configuration
Note: Enter MSTP configuration interface

TENDA(config-mst)# name 2222
Note: Configure domain name

TENDA(config-mst)# revision 52
Note: Configure revision level

TENDA(config-mst)# instance 2 vlan 52
Note: Configure vlan mapping and enable this instance
TENDA(config-mst)# no name

Note: Delete domain name settings and restore to default factory settings (MAC address of the device)

TENDA(config-mst)# revision 52

Note: Delete revision level settings and restore it to the default 0.

TENDA(config-mst)# no instance 3

Note: Delete this instance's vlan mapping and disable this instance

- **STP Port configuration**

TENDA(config)# interface range gigabitethernet 0/1-4

Note: Enter the directory of ports 1-4

TENDA(config-if)# spanning-tree

Note: Enable STP

TENDA(config-if)# no spanning-tree

Note: Disable STP

TENDA(config-if)# spanning-tree autoedge

Note: Set corresponding port(s) to edge port(s).

TENDA(config-if)# no spanning-tree autoedge

Note: Set corresponding port(s) to non-edge port(s).

TENDA(config-if)# spanning-tree link-type point-to-point auto

Note: spanning-tree link-type point-to-point auto

TENDA(config-if)# spanning-tree link-type point-to-point force-false

Note: Set port as non-p2p port

TENDA(config-if)# spanning-tree link-type point-to-point force-true

Note: Set port as p2p port

TENDA(config-if)# no spanning-tree link-type point-to-point

Note: Delete current p2p port setting and restore it to factory default

TENDA(config-if)# spanning-tree mstp 10（0-15） cost default

Note: Set path cost to 802.1t auto mode in the instance

TENDA(config-if)# spanning-tree mstp 0 cost 2000

Note: Set port path cost to 2000

TENDA(config-if)# spanning-tree mstp 2 port-priority 96

Note: Set port priority to 96

TENDA(config-if)# no spanning-tree mstp 0 cost
Note: Delete current port path cost setting and restore it to factory default

TENDA(config-if)# no spanning-tree mstp 2 port-priority
Note: Delete current instance priority setting and restore it to factory default

- **Display STP status**

TENDA# show spanning-tree summary
Note: Display STP status, current version, forwarding rules, max age, forward delay, hello time and max-hop settings

TENDA# show spanning-tree interface gigabitethernet 0/5
Note: Display STP status, port cost, port priority, edge port setting, P2P port setting, port role, port status, STP statistics on port 5

TENDA# show spanning-tree detail
Note: Display all STP info

TENDA# show spanning-tree enable-instance
Note: Display all enable-instances and linkup port info

TENDA# show spanning-tree region-configuration
Note: Display switch's domain info

5.3.22 IGMP configuration

Enter configuration directory:Tenda # configure terminal

- **Enable/disable IGMP**

TENDA(config)# ip igmp snooping ivgl
Note: Enable IGMP
TENDA(config)# no ip igmp snooping
Note: Disable IGMP

- **Config processing scheme of unknown IGMP pakets**

TENDA(config)# ip igmp unknown-multicast deny
Note: Allow unknown IGMP multicast
TENDA(config)# ip igmp unknown-multicast permit
Note: Deny unknown IGMP multicast

- **Config IGMP settings**

TENDA(config)# ip igmp snooping dyn-mr-aging-time 105
Note: Config Max age of IGMP routing port
TENDA(config)# ip igmp snooping host-aging-time 200
Note: Config Max age of IGMP host port

TENDA(config)# ip igmp snooping last-member-query-interval 4
Note: Config group-specific query max response time
TENDA(config)# ip igmp snooping querier max-response-time
Note: Config group-general query max response time

- **Delete IGMP settings (Restore IGMP factory defaults)**
  TENDA(config)# no ip igmp snooping dyn-mr-aging-time
  Note: Reset Max age of IGMP routing port to factory default

  TENDA(config)# no ip igmp snooping host-aging-time
  Note: Reset Max age of IGMP host port to factory default

- **Enable/disable IGMP port fast leave**
  TENDA(config)# interface range gigabitethernet 0/1-4
  Note: Enter port configuration directory

  TENDA(config-if)# fast-leave on
  Note: Enable IGMP port fast leave

  TENDA(config-if)# fast-leave off
  Note: Disable IGMP port fast leave

5.3.23 Time Range Management

- **Configure time range**
  TENDA(config)# timerange 99 absolute start time 11 23 2010 end time 08 16 2013
  Note: Configure absolute time
  TENDA(config)# timerange 67 weekday 8
  Note: Configure periodic time
  TENDA(config)# timerange 12 periodic start time 03:40 end time 05:35
  Note: Configure time slices

- **Delete time range**
  TENDA(config)# no timerange 67
  Note: Delete time range

  TENDA(config)# no timerange 12 periodic start time 03:40 end time 05:35
  Note: Delete time slices

- **View time range**
  TENDA# show timerange
  Note: View time range

5.3.24 POE management

- **Global Settings**

  TENDA(config)# power inline static|auto

  Note: Configure PoE management mode

- **Port configuration**

  TENDA(config)# interface range gigabitethernet 0/9

  TENDA(config-if)# power inline disable|enable

  Note: Enable/disable PoE

  TENDA(config)# interface range gigabitethernet 0/9

  TENDA(config-if)# power inline standard af|at

  Note: Configure interface power supply standard

  TENDA(config)# interface range gigabitethernet 0/6

  TENDA(config-if)# power inline consumption default <0-300>

  Note: Configure PoE power

  TENDA(config-if)# power inline priority high|low|medium

  Note: Configure current port priority setting and it only takes effect in static mode

  TENDA(config-if)#power timerange <1-100>

  Note: Configure current specified time range ID and not specified means no time limit

- **View PoE settings**

  TENDA# show power

  Note: View PoE settings, including global settings, port settings, actual transmission power and remote PD level

5.3.25 ACL Configuration

- **Add ACL**

  TENDA# configure terminal

  TENDA (config)# access-list 125

  Note: Create MAC based ACL: 125

  TENDA(config)# access-list 1

  Note: Create IP based ACL: 1

- **Add MAC based ACL rule**

  TENDA (config)# access-list 125

  TENDA(config)# mac access-list 125

  Note: Enter ACL 125

  TENDA(config-mac-nacl)# rule 1 deny vlan 2 eth-type any src-mac any dst-mac any

  Note: Add rule 1 and deny all packets to pass

TENDA(config-mac-nacl)#rule 2 deny vlan 1 eth-type any src-mac aaaa.aaaa.aaaa src-mac-mask any dst-mac any dst-mac-mask any

Note: Add rule 3 and deny all packets at the source MAC address of "aaaa.aaaa.aaa" to pass.

Note----------

Deny: Deny packets matching rule to pass; vlan: Specify VID; eth-type: Specify protocol type; src-mac: Specify source MAC address; dst-mac: Specify destination MAC address

If source MAC and destination MAC are set to Any, corresponding fields, such as mask field, will not be configurable.

TENDA(config-mac-nacl)#rule <101-200> bind-with timerange <1-100>

Note: Configure MAC ACL rule and time range binding

- **Add IP based ACL rule**

TENDA(config)# ip access-list extended 1

Note: Enter ACL 1

TENDA(config-ip-nacl)# rule 1 deny tcp src-ip any eq any dst-ip any eq any

Note: Add rule 1 and deny all TCP packets to pass

TENDA(config-ip-nacl)# rule 2 rate-limit 64 ip src-ip 192.168.10.1 src-ip-mask any dst-ip any

Note: Add rule 2 and set RX rate of packets with the source IP address of 192.168.10.1 to 64kbps

Note----------

Deny: Deny packets matching rule to pass; IP: Specify protocol type; src-ip: Specify source IP address; dst-ip: Specify destination IP address.

Source port and destination port are configurable only when you specify TCP and UDP as the protocol type.

TENDA(config-mac-nacl)#rule <1-100> bind-with timerange <1-100>

Note: Configure IP ACL rule and time range binding

- **Delete ACL**

TENDA(config)# no access-list 125

Note: Delete MAC based ACL: 125

TENDA(config)# no access-list 1

Note: Delete IP based ACL: 1

- **Delete an ACL rule**

TENDA(config)# mac access-list 125

TENDA(config-mac-nacl)# no rule 1

Note: Delete rule 1 of ACL 125

TENDA(config)# mac access-list 1
TENDA(config-ip-nacl)#no rule 2
Note: Delete rule 2 of ACL 1

- **Add port binding**

TENDA(config)# mac access-list 125
TENDA(config-mac-nacl)# bind-to interface range gigabitethernet 0/1
Note: Enter ACL 125 and bind it with port 1

TENDA(config)# ip access-list extended 1
TENDA(config-ip-nacl)# bind-to interface range gigabitethernet 0/1-24
Note: Enter ACL 1 and bind it with ports 1-24

- **Delete port binding**

TENDA(config)# mac access-list 125
Note: Enter ACL 125
TENDA(config-mac-nacl)# no bind-to interface range gigabitethernet 0/1
Note: Delete binding between ACL 125 and port 1

TENDA(config)# ip access-list extended 1
TENDA(config-ip-nacl)#no bind-to interface range gigabitethernet 0/1-4
Note: Enter ACL 1 and unbind ACL 125 with ports 1-4

- **Display ACL settings**

TENDA# show access-lists
Note: Display all ACLs and bound ports

TENDA# show access-lists 1
Note: Display ACL 1 and the bound port(s)

5.3.26 DoS Attack Defense Configuration

TENDA(config)# ip deny ping-of-death
Note: Enable Ping of Death Attack Defense

TENDA(config)# no ip deny ping-of-death
Note: Disable Ping of Death Attack Defense

TENDA(config)# ip deny land
Note: Enable Land Attack Defense

TENDA(config)# no ip deny land
Note: Disable Land Attack Defense

TENDA(config)# ip deny null-scan
Note: Enable NULL Scan Attack Defense

TENDA(config)# no ip deny null-scan
Note: Disable NULL Scan Attack Defense

TENDA(config)# ip deny syn-port-less-1024
Note: Enable Drop SYN packets with source port smaller than 1024
TENDA(config)# no ip deny syn-port-less-1024
Note: Disable Drop SYN packets with source port smaller than 1024

TENDA(config)# ip deny fup
Note: Enable FUP Attack Defense

TENDA(config)# no ip deny fup
Note: Disable FUP Attack Defense

TENDA(config)# ip deny blat-tcp
Note: Enable BLAT TCP Attack Defense

TENDA(config)# no ip deny blat-tcp
Note: Disable BLAT TCP Attack Defense

TENDA(config)# ip deny blat-udp
Note: Enable BLAT UDP Attack Defense

TENDA(config)# no ip deny blat-udp
Note: Disable BLAT UDP Attack Defense

5.3.27 Worm Attack Defense Configuration

TENDA(config)# filter aaa tcp 10 on
Note: Enable filter of TCP virus packets with destination port number of 10

TENDA(config)# filter aaa tcp 10 off
Note: Disable filter of TCP virus packets with destination port number of 10
TENDA(config)# filter ccc udp 65535 on
Note: Enable filter of UDP virus packets with destination port number of 65535

TENDA(config)# filter ccc udp 65535 off
Note: Disable filter of UDP virus packets with destination port number of 65535
TENDA(config)# no filter udp 65535
Note: Delete configurations of UDP virus with destination port of 65535

TENDA(config)# no filter tcp 10

Note: Delete configurations of TCP virus with destination port of 10

5.3.28 ARP Attack Defense Configuration

- **Enable ARP Attack Defense**

  TENDA(config)# interface gigabitethernet 0/10
  TENDA(config-if)# ip arp inspection trust
  TENDA(config-if)# ip arp inspection limit rate 200
  Note: Enable ARP attack defense on port 10 and ARP RX rate to 200PPS

  TENDA(config)# interface rang gigabitethernet 0/11-20
  TENDA(config-if)# ip arp inspection trust
  TENDA(config-if)# ip arp inspection limit rate 150
  Note: Enable ARP attack defense on ports 11-20 and ARP RX rate to 150PPS

- **Disable ARP Attack Defense**

  TENDA(config)# interface gigabitethernet 0/10
  TENDA(config-if)# no ip arp inspection trust
  Note: Disable ARP Attack Defense on port 10

  TENDA(config)# interface rang gigabitethernet 0/11-20
  TENDA(config-if)# no ip arp inspection trust
  Note: Disable ARP Attack Defense on ports11-20

5.3.29 Config MAC Attack Defense

TENDA(config)# interface gigabitethernet 0/1
TENDA(config-if)# mac-address learning-limit 8191
Note: Set no limit of MAC address learning on port 1

TENDA(config-if)# mac-address learning-limit 0
Note: Disable MAC address learning on port 1

TENDA(config-if)# mac-address learning-limit 200
Note: Set MAC Address learning Limit on port 1 to 200

TENDA(config)# interface rang gigabitethernet 0/1-24
TENDA(config-if)# mac-address learning-limit 2000
Note: Set MAC Address learning Limit on ports 1-24 to 2000

TENDA(config-if)# mac-address unknown-discard
Note: Enable to drop excessive MAC address learning packets (beyond address limit)

TENDA(config-if)#no mac-address unknown-discard
Note: Disable to drop excessive MAC address learning packets (beyond address limit)

5.3.30 IP Filter Configuration

- **Add IP+MAC+Port+VLAN binding entry**

  TENDA(config)# ipmacbind 192.168.0.1 0000.0000.0001

  Note: Add IP+MAC+Port+VLAN binding entry: bind the IP address of 192.168.0.1 and MAC address of 0000.0000.0001 to all ports and all VLANs

  TENDA(config)# ipmacbind 192.168.0.5 0000.0000.0002 4094

  Note: Add IP+MAC+Port+VLAN binding entry: bind the IP address of 192.168.0.5 and MAC address of 0000.0000.0002 to all ports in VLAN4094

  TENDA(config)#ipmacbind 192.168.0.5 0000.0000.0006 interface gigabitethernet 0/1

  Note: Add IP+MAC+Port+VLAN binding entry: bind the IP address of 192.168.0.5 and MAC address of 0000.0000.0006 to port 1

  TENDA(config)# ipmacbind 192.168.0.5 0000.0000.0002 4094 interface gigabitethernet 0/5

  Note: Add IP+MAC+Port+VLAN binding entry: bind the IP address of 192.168.0.5 and MAC address of 0000.0000.0002 to port 5 in VLAN4094

- **Port binding and unbinding**

  TENDA(config)# interface range gigabitethernet 0/1-4

  TENDA(config-if)# ipmacbind 192.168.0.5

  Note: Bind the IP+MAC+Port+VLAN binding entry containing the IP address of 192.168.0.5 to ports 1-4

  TENDA(config-if)# no ipmacbind 192.168.0.5

  Note: Unbind the IP-MAC-Port-VLAN binding entry containing the IP address of 192.168.0.5 to ports 1-4

- **Delete binding entry**

  TENDA(config)# no ipmacbind 192.168.0.1

  Note: Delete the IP-MAC-Port-VLAN binding entry containing the IP address of 192.168.0.1

- **Port Filter Setup**

  TENDA(config-if)# filter arp

  Note: Enable ARP filter on port

  TENDA(config-if)# no filter arp

  Note: Disable ARP filter on port

  TENDA(config-if)# filter ip

  Note: Enable IP filter on port

  TENDA(config-if)# no filter ip

  Note: Disable IP filter on port

  TENDA(config-if)# filter gateway

  Note: Enable gateway filter on port

TENDA(config-if)# no filter gateway
Note: Disable gateway filter on port

- **Display IP+MAC+Port+VLAN binding entry**
  TENDA# show ipmacbind
  Note: Display all IP-MAC-Port-VLAN binding entries

  TENDA# show ipmacbind interface gigabitethernet 0/1
  Note: Display port filter settings and IP+MAC+Port+VLAN binding entries on a single port

  TENDA# show ipmacbind interfaces
  Note: Display all port filter settings and IP+MAC+Port+VLAN binding entries

5.3.31 DHCP Relay

- **DHCP relay global settings**
  TENDA(config)# service dhcp
  Note: Enable DHCP feature globally

  TENDA(config)# no service dhcp
  Note: Disable DHCP feature globally

  TENDA(config)# service information option82
  Note: Enable Option82
  TENDA(config)# service information policy replace
  Note: Set Option82 strategy to replace

  TENDA(config)# service information policy keep
  Note: Set Option82 strategy to keep
  TENDA(config)# service information policy drop
  Note: Set Option82 strategy to drop

  TENDA(config)# no service information option82
  Note: Disable Option82

- **Display DHCP global settings**
  TENDA# show dhcp service

- **VLAN virtual interface configuration**
  TENDA(config)# interface vlan-interface 2
  Note: Enter VLAN virtual interface 2

  TENDA(vlan-if)# ip address 2.2.2.2 255.0.0.0

Note: Configure IP address and subnet mask of virtual interface 2

TENDA(vlan-if)# enable
Note: Enable virtual interface 2

TENDA(vlan-if)# no enable
Note: Disable virtual interface 2

- **Display virtual interface settings**

TENDA# show interface vlan-interface all
Note: Display all virtual interfaces which have been created

TENDA# show interface vlan-interface 2
Note: Display settings on VLAN virtual interface 2

- **Remote server configuration**

TENDA(config)# ip helper-address 4　192.168.10.1

Note: Set remote server ID4, IP：192.168.10.1

TENDA(config)# no ip helper-address 4
Note: Delete remote server ID4

- **DHCP relay configuration**

TENDA(config)# interface vlan-interface 2
Note: Enter VLAN virtual interface 2

TENDA(vlan-if)# dhcp relay
Note: Enable DHCP relay on VLAN virtual interface 2

TENDA(vlan-if)# helper-address 1
Note: Select remote server ID1

TENDA(vlan-if)# no dhcp relay
Note: Disable DHCP relay on VLAN virtual interface 2
TENDA# show dhcp remoteserver
Note: Display remote server

- **Display relay configuration**

TENDA# show dhcp relay
Note: Display all relay configurations

5.3.32 DHCP Snooping

- **Global settings**

TENDA(config)# ip dhcp snooping
Note: Enable DHCP snooping globally
TENDA(config)# no ip dhcp snooping
Note: Disable DHCP snooping globally

TENDA(config)# ip dhcp snooping verify mac-address
Note: Enable MAC checking
TENDA(config)# no ip dhcp snooping verify mac-address
Note: Disable MAC checking

- **Port settings**
  TENDA(config)# interface range gigabitethernet 0/7
  TENDA(config-if)# ip dhcp snooping trust
  Note: Set port property to trust
  TENDA(config-if)# no ip dhcp snooping trust
  Note: Set port property to untrust
  TENDA(config-if)# ip dhcp snooping information policy drop
  Note: Set option strategy to drop
  TENDA(config-if)# ip dhcp snooping information policy keep
  Note: Set option strategy to keep
  TENDA(config-if)# ip dhcp snooping information policy replace
  Note: Set option strategy to replace

  TENDA(config-if)# ip dhcp snooping information option
  Note: Enable option82
  TENDA(config-if)# no ip dhcp snooping information option
  Note: Disable option82

  TENDA(config-if)# ip dhcp snooping option user-option
  Note: Enable user-defined option
  TENDA(config-if)# no ip dhcp snooping option user-option
  Note: Disable user-defined option

  TENDA(config-if)# ip dhcp snooping information option circuit-id 123 remote-id 345
  Note: Configure current port's circuit ID sub-option and remote ID sub-option

- **View DHCP SNOOPING global info**
  TENDA# show dhcp snooping

5.3.33 SNMP Agent Configuration

- **Enable SNMP Agent**
  TENDA(config)# snmp-server community public rw
  Note: Set community name to public, access right to read & write, and enable SNMP in the

meantime (Adding the first community name enables the SNMP agent feature and the SNMP will stay enabled thereafter unless disabled intentionally); note that you must create a view before you can create a community

TENDA(config)# snmp-server community private ro
Note: Set community name to private, access right to read only

TENDA(config)# snmp-server community TENDA rw
Note: Specify community name as Tenda and access right as read & write

TENDA(config)# snmp-server packetsize 1500
Note: Set SNMP packet size to 1500
TENDA(config)# snmp-server version 1&2c
Note: Specify SNMP version as V1 and V2c

TENDA(config)# snmp-server version 1
Note: Set SNMP version to V1

TENDA(config)# snmp-server version V2c
Note: Set SNMP version to V2c

TENDA(config)# no snmp-server community TENDA
Note: Delete community name

- **Disable SNMP agent**
  TENDA(config)# no snmp-server
  Note: Disable SNMP agent globally

- **View SNMP agent settings**
  TENDA# show snmp-server

- **Enable Trap**
  TENDA(config)# snmp-server trap on
  Note: Enable Trap

  TENDA(config)# snmp-server trap type 1
  Note: Enable cold trap on the switch

  TENDA(config)# snmp-server trap type 2
  Note: Enable warmstart trap on the switch

  TENDA(config)# snmp-server trap type 4
  Note: Enable Linkdown Trap on the switch

TENDA(config)# snmp-server trap type 8
Note: Enable Linkup Trap on the switch

TENDA(config)# snmp-server trap type 16
Note: Enable Authentication Trap on the switch
TENDA(config)# snmp-server trap type 31
Note: Enable all Trap features the switch supports

TENDA(config)# snmp-server trap interface range fastethernet 0/1-24
Note: Enable trap features mentioned above on all ports

- **View Trap settings**
  TENDA# show snmp-server traps

- **Disable trap**
  TENDA(config)# snmp-server trap off

- **Create the destination host**
  TENDA(config)# snmp-server host 192.168.0.2 traps version 2c public udp-port 162
  Note: Set destination host IP to 192.168.0.1, Trap version to V2c, UDP port number to 162 and community name to public
  TENDA(config)# snmp-server host 172.16.100.20 traps version 1 555 udp-port 200
  Note: Set destination host IP to 172.16.100.20, Trap version to V1, UDP port number to 200 and community name to 555

- **Delete the destination host**
  TENDA(config)# no snmp-server host 192.168.0.2 public
  Note: Delete destination host IP 192.168.0.2

5.3.34 Log configuration

- **Enable/disable logging**
  TENDA(config)# logging on
  Note: Enable log
  TENDA(config)# logging off
  Note: Disable log

- **Enable/disable log server**
  TENDA(config)# logging host 192.168.100.78 level warning on
  Note: Enable log server
  TENDA(config)# logging host 192.168.100.78 level warning off
  Note: Disable log server

- **Display logs and log settings**

TENDA# show logging-server
Note: Display log server

TENDA# show logging all
Note: Display all system logs

TENDA# show logging alert / critical / debug / emergency / error / informational / notice / warning
Note: Display logs by 9 severity levels

- **Clear logs**
  TENDA# clear logging
  Note: Clear logs

5.3.35 802.1X Configuration

- **802.1X Global Setup**
  TENDA(config)# aaa dot1x enable
  Note: Enable 802.1X
  TENDA(config)# no aaa dot1x enable
  Note: Disable 802.1X
  TENDA(config)# radius-server host 192.168.0.78
  Note: Specify the IP address of 802.1X server. Note that it must be on the same net segment as device
  TENDA(config)# radius-server key WinRadius
  Note: Specify a key for the 802.1X server

  TENDA(config)# dot1x re-authentication
  Note: Enable 802.1X re-authentication
  TENDA(config)# no dot1x re-authentication
  Note: Disable 802.1X re-authentication

  TENDA(config)# dot1x timeout re-authperiod 1
  Note: Specify 802.1X re-authentication timeout as 1s
  TENDA(config)# dot1x timeout tx-period 255
  Note: Specify 802.1X client timeout as 255s

- **802.1X Port Setup**
  TENDA(config)# interface range gigabitethernet 0/1-4
  Note: Enter ports 1-4
  TENDA(config-if)# dot1x
  Note: Enable 802.1X on port(s)
  TENDA(config-if)# dot1x port-control-mode mac-based 200
  Note: Set control mode to MAC and access numbers to 200
  TENDA(config-if)# dot1x port-control-mode port-based

Note: Set control mode to PORT

TENDA(config-if)# dot1x port-control auto
Note: Specify port control mode as auto
TENDA(config-if)# dot1x port-control force-authorized
Note: Specify port control mode as force authorized
TENDA(config-if)# dot1x port-control force-unauthorized
Note: Specify port control mode as force unauthorized

TENDA(config-if)# dot1x port-reauthentication
Note: When the port control mode is PORT, you can enable port re-authentication manually

TENDA(config-if)# no dot1x
Note: Disable 802.1X

- **802.1X status**

TENDA# show dot1x all
Note: Display 802.1X global settings and port status

TENDA# show dot1x statistics
Note: Display all ports' status

TENDA# show dot1x interface gigabitethernet 0/1
Note: Display a single port's status

5.3.36 Save Configurations

TENDA# copy running-config startup-config
Note: Save current settings

TENDA# copy running-config 192.168.111.79：mib.conf

Note: Save current settings to local hard drive via TFTP server

TENDA# copy startup-config 192.168.111.79:mib.conf
Note: Save settings to local hard drive via TFTP server

- **Delete settings on port**

TENDA(config-if)#no cos
Note: Delete priority settings on port; the default is 0

TENDA(config-if)# flow-control off
Note: Disable flow control
TENDA(config-if)# shutdown
Note: Disable port

TENDA(config-if)# no port-isolated

Note: Disable port isolation

- **Display settings on port**

  TENDA# show interface gigabitethernet 0/3

  Note: Display basic settings on port 3

  TENDA# show interface status

  Note: Display basic settings on all ports

Chapter 6 Appendix

6.1 Glossary

SNTP

Simple Network Time Protocol (SNTP), using UDP datagram packets at the transport layer, is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

HTTP

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, which defines information format, transmission mode, WEB server and browser actions. HTTP functions as a request-response protocol in the client-server computing model. A web browser, for example, may be the client and an application running on a computer hosting. A web site may be the server. The client submits an HTTP request message to the server. The server, which provides resources, such as HTML files and other content, or performs other functions on behalf of the client, returns a response message to the client. Another primary standard of controlling how World Wide Web works is HTML, which defines how web pages are formed and displayed. Any web server includes a HTTP daemon background program in addition to web files. This program is designed to expect and process HTTP requests. A web browser, as an HTTP client, is used for sending requests to the server. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a server (typically port 80). An HTTP server listening on that port waits for a client's request message. Upon receiving the request, the server sends back a status line, and a message of its own.

Auto-negotiation

Auto negotiation is an Ethernet procedure by which two connected devices choose common transmission parameters, such as speed, duplex mode, and flow control. In this process, the connected devices first share their capabilities regarding these parameters and then choose the highest performance transmission mode they both support.

IEEE 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 to devices wishing to attach to a LAN or WLAN. IEEE 802.1X defines the encapsulation of EAP over LAN or EAPOL. 802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN, though the term “supplicant” is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.The authenticator acts as a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant’s identity has been validated and authorized. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device)

is allowed to access resources located on the protected side of the network.

Port Mirroring

Network Engineers or Administrators use port mirroring to copy traffic from multiple ports to the mirroring destination port for analyzing and debugging data or diagnosing errors on a network. It helps the administrator keep a close eye on network performance and will alert him when problems occur. (Mirroring traffic here is equivalent to copying traffic.) It can be used to mirror either inbound or outbound traffic on single or multiple interfaces.

LACP

Within the IEEE specification the Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. In this way, link bandwidth is increased, available redundancy is raised and transmission quality is also enhanced.

ACL

An ACL (Access Control List) contains entries that specify individual user or group rights to specific system objects such as programs or processes. These entries are known as access control entries (ACEs). Each accessible object contains an identifier to its ACL. The privileges or permissions determine specific access rights. On some types of proprietary computer hardware (in particular routers and switches), an Access Control List refers to rules that are applied to port numbers or IP Addresses that are available on a host or other layer 3, each with a list of hosts and/or networks permitted to use the service. Both individual servers as well as routers can have network ACLs. Access control lists can generally be configured to control both inbound and outbound traffic, and in this context they are similar to firewalls.

DHCP

The Dynamic Host Configuration Protocol (DHCP) is a network protocol that is used to configure network devices so that they can communicate on an IP network. A DHCP client uses the DHCP protocol to acquire configuration information, such as an IP address, a default route and one or more DNS server addresses from a DHCP server. The DHCP client then uses this information to configure its host. Once the configuration process is complete, the host is able to communicate on the Internet. The DHCP server maintains a database of available IP addresses and configuration information, ensuring each IP address assigned is unique on the network. A valid IP address (lease time has not expired) will never be allocated to a second client. The IP pool is maintained by the DHCP server itself instead of a network administrator.

ARP

Address Resolution Protocol (ARP) is a protocol used for resolution of network layer addresses into link layer addresses, such as Ethernet addresses. In order to communicate with a neighboring host, the host needs to first know its neighbor's IP address. It also needs to know its neighbor's MAC address by sending a broadcast ARP message requesting an answer for the neighbor's IP address.

DoS

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment

gateways, and even root name servers. One common method of attack involves saturating the target machine with external communication requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable.

IGMP

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. IGMP can be used for online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications.

IP

The Internet Protocol (IP) is the principal communications protocol used for relaying datagrams (also known as network packets) across an internetwork using the Internet Protocol Suite. Responsible for routing packets across network boundaries, it is the primary protocol that establishes the Internet. The Internet Protocol only provides best effort delivery and its service is characterized as unreliable. Each network device attached to LAN or WAN is assigned with an IP address. This IP address is used for unique identifier of a network device on the network.

The dominant internet working protocol in the Internet Layer in use today is IPv4; IPv4 uses 32-bit addresses, which indicates 4 billion, or 4.3×109, available addresses. Thus IPv6 is brought into use for addressing rapid exhaustion of IP addresses. The IPv6 uses 128-bit addresses, which indicates 340 undecillion, or 3.4×1038 available addresses. Yet, IPv4 is still the dominant protocol of the internet. Its successor of IPv6 is increasing in use though slow.

MAC Table

An Ethernet device uses a MAC address table for forwarding frames. When forwarding a frame, the device first looks up the MAC address of the frame in the MAC address table for a match. A switch maintains a MAC address table for frame forwarding. Each entry in this table maps the MAC address to associated interface. It tells the switch from which port a MAC address (or host) can be reached. A MAC address table consists of two types of entries: static and dynamic. Static entries are manually configured by administrators and never age out.

A frame also carries a source MAC address which indicates the sender. The device can automatically populate its MAC address table by obtaining the source MAC addresses (known as “MAC address learning”) of incoming frames on each port. If a dynamic entry has not updated when the aging timer expires, the device deletes the entry.

PING

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 operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response. In the process it measures the time from transmission to reception (round-trip time) and records any packet loss. The results of the test are printed in the form of a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times, and sometimes the standard deviation of the mean.

Port VLAN

Port-based VLANs are created by assigning ports to a VLAN.

QoS

QoS(Quality of Service) is the ability to provide different priority for different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. Delay sensitive applications such as real-time HD streaming multimedia, voice over IP, online games and IP-TV, are often transfered on networks where the capacity is a limited resource. Thus, a network should be able to provide a real time lag-free Internet experience. Providing guaranteed quality of service now becomes the secret of success in end-to-end business network solution. When configured properly, the QoS can help effectively manage network resources.

STP/RSTP/MSTP

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. In 1998, the IEEE 802.1w introduced Rapid Spanning Tree Protocol (RSTP). RSTP provides significantly faster spanning tree convergence after a topology changes, introducing new convergence behaviors and bridge port roles to do this. RSTP was designed to be backwards-compatible with standard STP.

SNMP

SNMP Simple Network Management Protocol (SNMP) is a component of the Internet Protocol Suite for managing devices on IP networks. The SNMP allows reverse network objects to join the network management architecture. It monitors networks by analyzing Traps or notifications received on network management systems.

Tag Priority

Tag Priority is a 3-byte field in 802.1Q frame, which indicates priority level.

TCP

The Transmission Control Protocol (TCP) is one of the two original components of the suite, complementing the Internet Protocol (IP), and therefore the entire suite is commonly referred to as TCP/IP. TCP provides a communication service at an intermediate level between an application program and the Internet Protocol (IP).

TELNET

Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communications facility between Telnet server and client using a virtual terminal connection. It uses the TCP protocol.

TFTP

(TFTP)Trivial File Transfer Protocol is a file transfer protocol notable for its simplicity. It is generally used for automated transfer of configuration or boot files between machines in a local environment. Different from FTP, It has been implemented on top of the User Datagram Protocol (UDP) using port number 69 and thus can penetrate multiple firewalls. Compared to FTP, TFTP is extremely limited, providing no user authentication, and is rarely used interactively by a user due to unreliability. Yet, it is suitable for transferring trivial files on private networks.

ToS

The modern redefinition of the TOS field is a six-bit Differentiated Services Field (DS field) field and a two-bit Explicit Congestion Notification (ECN) field. While Differentiated Services is somewhat backwards compatible with TOS, ECN is not. The TOS field could specify a datagram's priority and request a route for low-delay, high-throughput, or highly-reliable service.

UDP

The User Datagram Protocol (UDP) is one of the core members of the Internet protocol suite, the set of network protocols used for the Internet. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths.

VLAN

A virtual local area network, virtual LAN or VLAN, is a group of hosts with a common set of requirements, which communicate as if they were attached to the same broadcast domain, regardless of their physical location.

VLAN ID

VLAN Identifier (VID): a 12-byte field specifying the VLAN to which the frame belongs.

6.2 Technical Support

If any problem occurs while in use, please feel free to go to www.tendacn.com to find a solution or email your problems to: support@tenda.com.cn or support02@tenda.com.cn. We will be more than happy to help you out as soon as possible.

Manufacturer: Shenzhen Tenda Technology Co., Ltd
Website: http://www.tendacn.com
Email: support02@tenda.com.cn
Skype: tendasz

YouTube: Tendasz1999
Hotline:
1-800-570-5892 (USA) (061) 1300787922 (Australia)
(0852)36120883 (HongKong) (064) 800787922 (New Zealand)

Appendix 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.