Tenda

User Guide

TEG2 Series Gigabit Switch

www.tendacn.com

Copyright statement

Disclaimer

Pictures, images and product specifications herein are for reference only. To improve internal design, operational function, and/or reliability, Tenda reserves the right to make changes to the products without obligation to notify any person or organization of such revisions or changes. Tenda does not assume any liability that may occur due to the use or application of the product described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute a warranty of any kind, express or implied.

Preface

Thank you for choosing Tenda! This user guide helps you configure, manage and maintain switches.

This user guide applies to: TEG2205D, TEG2208D, TEG2216D, TEG2224D, TEG2226F, TEG2220P-16-250W, TEG2228P-25-410W. TEG2220P-16-250W is used for illustration unless otherwise specified.

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and firmware version. Please refer to the actual product.

The UI screenshots, IP addresses and other data are for illustrative purposes only and do not affect your configuration.

Conventions

The typographical elements that may be found in this document are defined as follows.

Item	Presentation	Example
Cascading menus	>	**System** > **Live Users**
Parameter and value	Bold	Set **User Name** to **Tom**.
Variable	Italic	Format: *XX*:*XX*:*XX*:*XX*:*XX*:*XX*
UI control	Bold	On the **Policy** page, click the **OK** button.
Message	""	The "Success" message appears.

The symbols that may be found in this document are defined as follows.

Symbol	Meaning
NOTE	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
TIP	This format is used to highlight a procedure that will save time or resources.

For more documents

If you want to get more documents of the switch, visit www.tendacn.com and search for the corresponding product model.

Technical support

Contact us if you need more help. We will be glad to assist you as soon as possible.

Email address: support@tenda.cn

Website: www.tendacn.com

Revision history

Tenda is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the switch was introduced.

Version	Description	Date
V2.0	1. Added the description of PoE, cloud management, cloud backup, loop guard and cable testing 2. Modified content structure	2024-9-18
V1.0	Historical version	2024-07-19

Contents

1 Log in to web UI

TIP

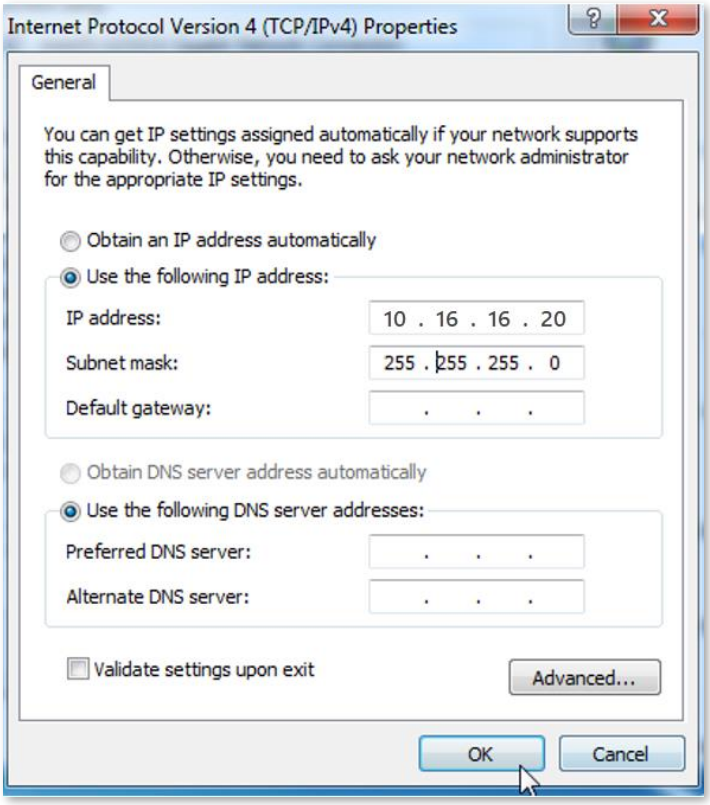
This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and firmware version. Please refer to the actual product.

1.1 Login

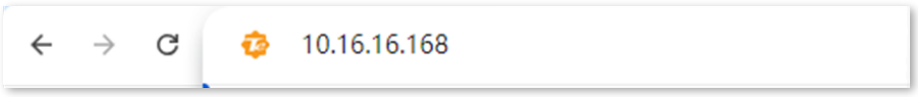
Step 1 Connect the computer to any RJ45 port of the switch using an Ethernet cable.

Step 2 Set a unique IP address for the computer that belongs to the same subnet as the switch.

The default IP address of the switch is **10.16.16.168**, you can set the IP address of the computer to 10.16.16.*X* (*X* ranges from 2 to 254 excluding 168, and is unused), and subnet mask to **255.255.255.0**.



Step 3 Start a browser (such as Chrome) and enter the management IP address of the switch (default: **10.16.16.168**) in the address bar to access the login page.



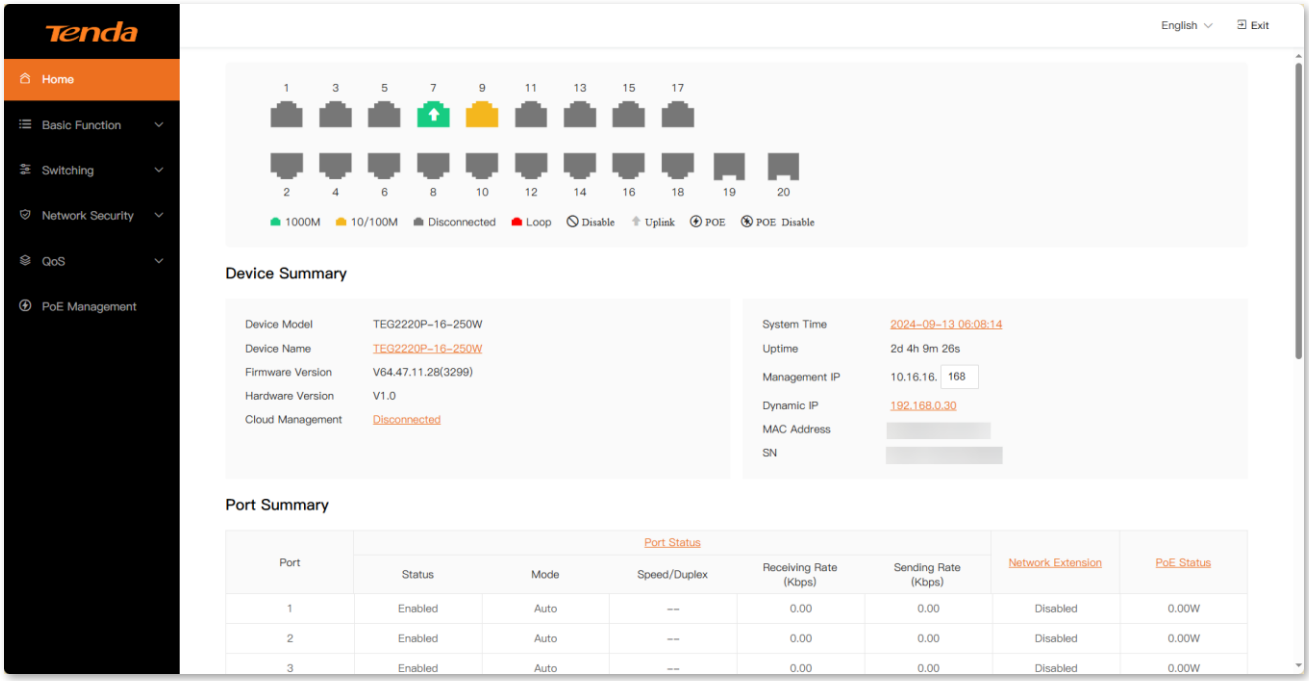
Step 4 Follow the onscreen instructions and finish logging in.

TIP

- When logging in for the first time, use the default password on the label of the switch if a login password is required. For network security, be sure to change the password after login.
- If the web UI does not appear, try the following solutions:
  - Ensure that the switch is powered on.
  - Ensure that the computer is connected to the switch properly.
  - Ensure that the Ethernet cable is not damaged and meets the specification requirements (generally, ≤100 meters).
  - Ensure that the computer and the switch are in the same subnet. For example, if the switch's IP address is 10.16.16.168, the computer's IP address can be set to 10.16.16.*X* (*X* ranges from 2-254 excluding 168, and is unused)
  - Ensure that the switch's IP address is unique in the local network.
  - Clear the cache of the web browser or try another web browser.
  - If the problem persists, reset the switch and try again.

---End

After logging in to the web UI, you can start to configure the switch.



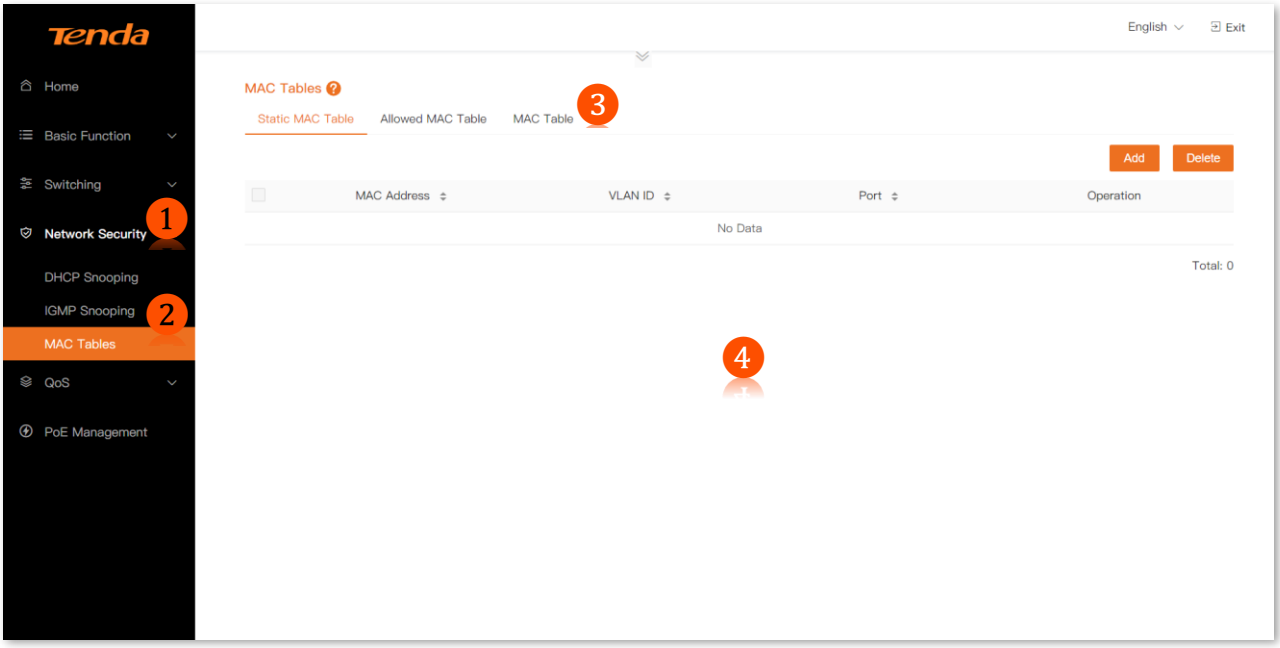
1.2 Logout

After you log in to the switch's web UI, the system will automatically log you out if there is no operation within 5 minutes. Alternatively, you can directly click **Exit** in the top right corner to exit the web UI.

1.3 Web UI

1.3.1 Web layout

The web UI can be divided into four parts: level-1 navigation bar, level-2 navigation bar, tab, and the configuration area.



No.	Name	Description
1	Level-1 navigation bar	Used to display menu items in the form of a navigation tree that allows you to access functions of the switch.
2	Level-2 navigation bar	
3	Tab	
4	Configuration area	Used to enable you to view and modify configuration.

1.3.2 Common buttons

The following table describes the common buttons on the switch's web UI.

Button	Description
Save OK	Used to save and apply the current configuration.
Cancel	Used to restore the original configuration without saving the configuration on the current page.
	Used to view help information for the function on the current page.
Add	Used to add rules.
Delete / Delete	Used to delete rules.
Clear / Clear	Used to clear rule configuration or data on the current page.
Edit / Edit	Used to modify rules on the current page.
	Used to expand or collapse the port status bar. TIP Generally, the button is located at the top of the port configuration page.
Port number	Enter the port number to select the port. Example: 1-10,12,14. – To select continuous ports, such as port 1 to port 10, enter 1-10 or drag the mouse to select ports 1-10. – To select discontinuous ports, such as ports 12 and 14, enter 12 and 14 or click ports 12 and 14. – To select both continuous and discontinuous ports, such as port 1 to port 10, ports 12 and 14, enter 1-10, 12, 14, or drag the mouse to select ports 1-10 and then click ports 12 and 14.
All Ports	Used to select all ports.

2 Get device infomation

TIP

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and firmware version. Please refer to the actual product.

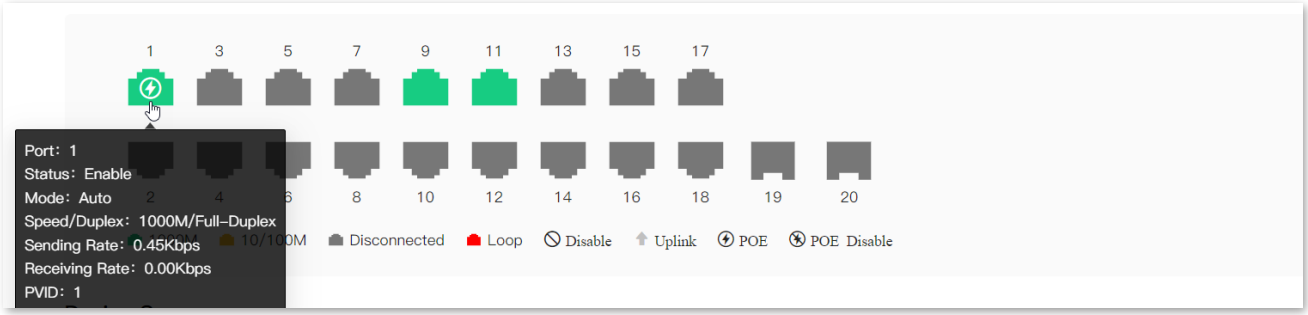
To access the page:

Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **Home**.

2.1 Port status

On the top of the **Home** page, you can view the connection status, port status and mode, connection speed and duplex, sending and receiving rates and PVID just by hovering your mouse over a port.



Parameter description

Button	Description
Port	Specifies the ID of the port.
Status	Specifies whether the port is enabled.
Mode	Specifies the configured connection rate and duplex mode of the port.
Speed/Duplex	Specifies the actual connection rate and duplex mode of the port.
Sending Rate	Specifies the sending rate of the port.
Receiving Rate	Specifies the receiving rate of the port.
PVID	Specifies the VLAN ID to which the port belongs by default. When a port receives untagged packets, they are forwarded to a specific VLAN based on the PVID.

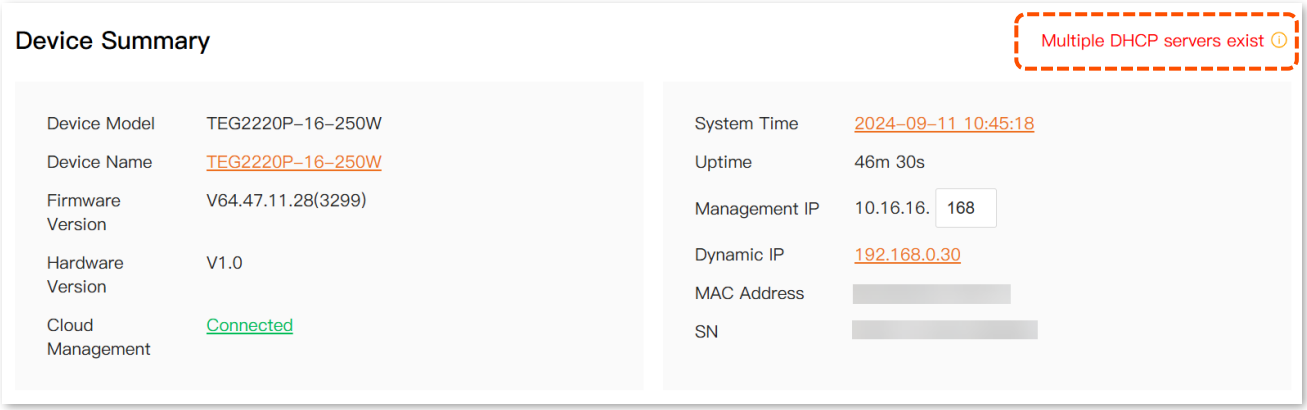
2.2 Device summary

On the **Device Summary** module of the **Home** page, you can view a summary of information of the switch.

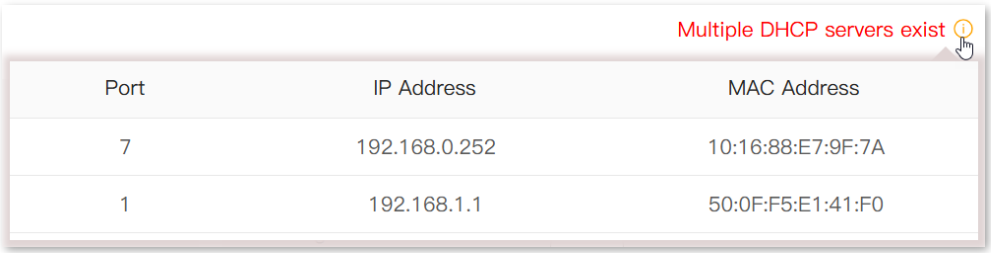
When multiple DHCP servers are detected in the LAN, an alarm will be displayed in the upper right corner of the **Device Summary** module.

TIP

If DHCP Client is disabled on the switch, the DHCP alarm function will not take effect.



By clicking the icon, you can view more details about the alarm, including the VLAN ID, port, DHCP server IP address and MAC address.



Parameter description

Name	Description
Device Model	Specifies the model of the switch.
Device Name	Specifies the name of the switch. By default, it displays as the device model. Click the device name to change it on the Device Info page.
Firmware Version	Specifies the firmware version of the switch.
Hardware Version	Specifies the hardware version of the switch.

Management VLAN	Specifies the management VLAN of the switch. When 802.1Q VLAN is enabled, the management VLAN defaults to VLAN 1. Change the value as required.
Cloud Management	Specifies whether the switch is connected to Tenda CloudFi Cloud platform. Click the connection status to configure cloud management on the Device Info page.
System Time	Specifies the current system time of the switch. Click the system time to change the setting on the Maintenance page.
Uptime	Specifies how long the switch has been running since its last launch.
Management IP	Specifies the management IP address of the switch. Default: 10.16.16.168. Change the setting as required. Computers in the LAN connected to the management VLAN member port can use this IP address to log in to the switch's web UI.
Dynamic IP	Specifies the dynamic IP address of the switch. By default, it is obtained from the LAN DHCP server. Computers in the LAN connected to the management VLAN member port can use this IP address to log in to the switch's web UI. Click the dynamic IP address to change the setting on the Device Info page.
MAC Address	Specifies the physical address of the switch.
SN	Specifies the serial number of the switch.

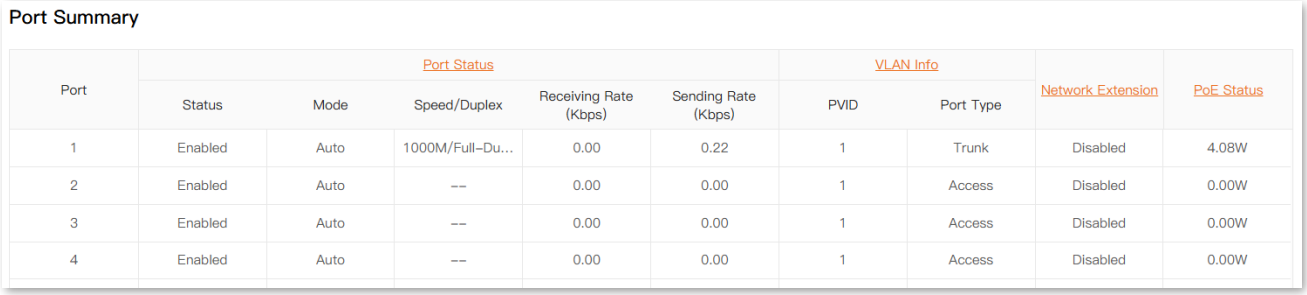
2.3 Port summary

On the **Port Summary** module of the **Home** page, you can view a summary of the status, VLAN, PoE comsumption and network extension of all ports on the switch.

To view specific details about port configuration, VLAN, or PoE comsumption, click **Port Status**, **VLAN Info**, **Network Extention**, or **PoE Status** when necessary.

TIP

Only when 802.1Q VLAN is enabled, VLAN information can be viewed.


Port Summary

Port	Port Status					VLAN Info		Network Extension	PoE Status
	Status	Mode	Speed/Duplex	Receiving Rate (Kbps)	Sending Rate (Kbps)	PVID	Port Type		
1	Enabled	Auto	1000M/Full-Du...	0.00	0.22	1	Trunk	Disabled	4.08W
2	Enabled	Auto	--	0.00	0.00	1	Access	Disabled	0.00W
3	Enabled	Auto	--	0.00	0.00	1	Access	Disabled	0.00W
4	Enabled	Auto	--	0.00	0.00	1	Access	Disabled	0.00W

Parameter description

Name		Description
Port		Specifies the ID of the port.
Port Status	Status	Specifies whether the port is enabled.
	Mode	Specifies the configured connection rate and duplex mode of the port.
	Speed/Duplex	Specifies the actual connection rate and duplex mode of the port. TIP "--" indicates that the port is not connected or the negotiation failed.
	Receiving Rate	Specifies the receiving rate of the port.
	Sending Rate	Specifies the sending rate of the port.
VLAN Info	PVID	Specifies the VLAN ID to which the port belongs by default. When a port receives untagged packets, they are forwarded to a specific VLAN based on the PVID.
	Port Type	Specifies the type of the port. – **Access**: An access port can join only one VLAN and send untagged packets. This type of port is used to connect client devices (such as computers). – **Trunk**: A trunk port can allow multiple VLANs to pass, and receive or send packets from multiple VLANs. This type of port is used for cascading ports between switches.
Network Extension		Specifies whether network extension is enabled.
PoE Status		(Only available on PoE switches) Specifies the PoE output status of the port.

3 Connect to the internet

TIP

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and firmware version. Please refer to the actual product.

By default, the switch will automatically obtain an IP address to connect to the internet. To change the switch's IP address and DNS acquisition method, take the following steps:

Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar

Step 2 Navigate to **Basic Function** > **Device Info**.

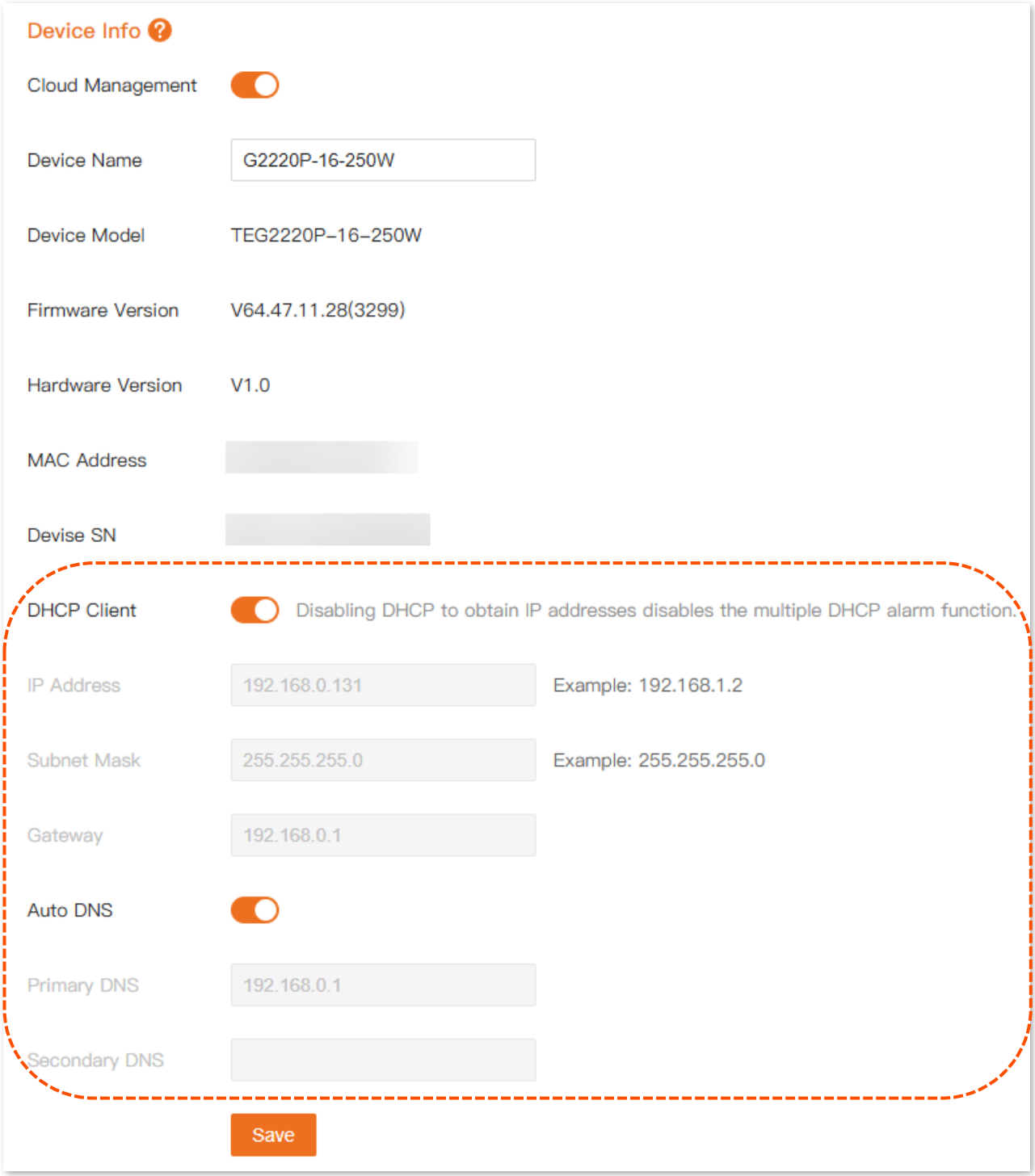
Step 3 Enable or diable **DHCP Client**.

Step 4 When **DHCP Client** is diabled, enter an IP address, subnet mask and gatway for the switch.

Step 5 Enable or disable **Auto DNS**.

Step 6 When **Auto DNS** is diabled, enter a primary and secondary DNS server address for the switch.

Step 7 Click **Save**.



*The figure shows an example of configuring the switch to automatically obtain an IP address and DNS server address.

---End

Parameter description

Name	Description
DHCP Client	Used to enable or disable the switch to automatically obtain network parameters from the DHCP server. – When enabled, the switch automatically obtains network parameters from the DHCP server. – When disabled, you need to manually configure network parameters for the switch. • **IP Address**: IP address of the switch. • **Subnet Mask**: Subnet mask corresponding to the switch's IP address. • **Gateway**: Gateway address of the switch. TIP When this function is disabled, the DHCP alarm function will be disabled simultaneously.
Auto DNS	Used to enable or disable the switch to automatically obtain a DNS server address. It is enabled by default. – When enabled, the switch automatically obtains a DNS server address from the DHCP server. – When disabled, you need to manually configure a primary and secondary DNS server address for the switch. • **Primary DNS**: Primary DNS server address of the switch. • **Secondary DNS**: (Optional) Secondary DNS server address of the switch.

4 Manage switches on cloud

TIP

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and firmware version. Please refer to the actual product.

Tenda CloudFi is a Tenda company-owned cloud platform where you can manage Tenda devices with cloud management support. Tenda CloudFi is available in mobile app and web versions (https://cloudfi.tendacn.com), and the data is interoperable.

4.1 Enable cloud management

By default, cloud management is enabled. To disable this function, take the following steps:

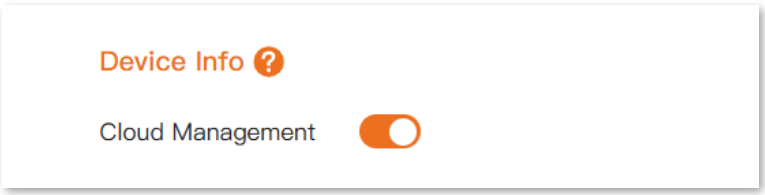
Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **Basic Function** > **Device Info**.

Step 3 Disable **Cloud Management**.

Step 4 Click **Save**.

---End



4.2 Add the switch to Tenda CloudFi

After cloud management is enabled, you can add a switch to Tenda CloudFi through either of two methods below.

Once the switch is added, configuration changes can be made either on the Tenda CloudFi cloud platform or the switch's local web UI. The configuration last modified will come into effect.

TIP

Before managing the switch on the Tenda CloudFi cloud platform, ensure that the switch is connected to the internet.

Or

GET IT ON Google Play

Download on the App Store

4.2.1 Add the switch in LAN

Step 1 Download the Tenda CloudFi App to your mobile device by scanning the QR code or searching for **Tenda CloudFi** in **Google Play** or **App Store**.

Step 2 Connect your mobile device to the switch's LAN network.

Step 3 Open your Tenda CloudFi App, and tap the project (or create one if no projects exist) to which you want to add the switch.

Step 4 Tap the pop-up window that shows the switch is detected, and add the switch to the project.

TIP

If the pop-up window does not appear, tap + and follow the instructions on your screen.

4.2.2 Add the switch with QR code

Step 1 Download the Tenda CloudFi App to your mobile device by scanning the QR code or searching for **Tenda CloudFi** in **Google Play** or **App Store**.

Step 2 Open your Tenda CloudFi App, and tap the project (or create one if no projects exist) to which you want to add the switch.

Step 3 Scan the QR code on the switch and remotely add the switch to the project.

---End

5 Assign VLANs

TIP

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and firmware version. Please refer to the actual product.

5.1 Overview

Virtual Local Area Network (VLAN) is a technology that divides devices in LAN into different logical, instead of physical, network segments to realize virtual working groups. VLANs allow a network station constituted by switches to be logically segmented into different domains for broadcast separation. All members in a VLAN are treated as in the same broadcast domain and communicate as if they were on the same network segment, regardless of their physical locations. 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.

This switch supports 802.1Q VLAN and can communicate with devices that support 802.1Q VLAN in VLAN as well. 802.1Q VLAN is defined by IEEE 802.1q protocol. With 802.1Q VLAN, the switch can process packets by identifying the tags in packets.

This switch supports two 802.1Q VLAN port types:

- Access: An access port can join only one VLAN. This type of port is used for connecting the computer.
- Trunk: A trunk port can receive and send packets belonging to multiple VLANs. This type of port is used for connection between switches.

Methods of each port type to process packets are shown as follows.

Port type	Receiving tagged data	Receiving untagged data	Sending data
Access port	Forward data to the ports with VLANs assigned based on the VLAN ID	Forward data to the ports with VLANs assigned based on the PVID	Strip the tag from the packet and then forward it
Trunk port			VLAN ID = PVID of the port, strip the tag from the packet and then forward it VLAN ID ≠ PVID of the port, retain the tag in the packet and then forward it

5.2 VLAN configuration

Enable 802.1Q VLAN

Navigate to **Basic Function** > **VLAN**. Here you can enable or disable 802.1Q VLAN on the switch.

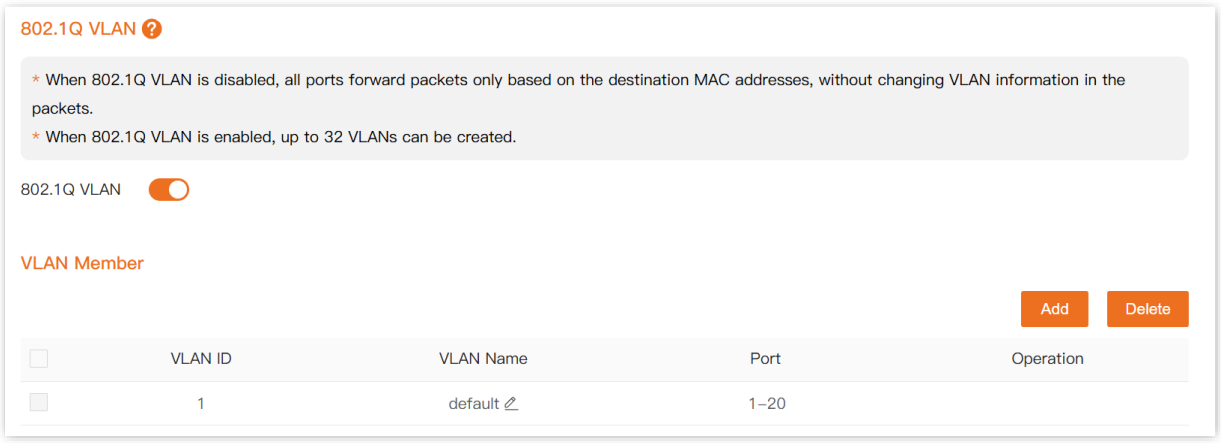
The 802.1Q VLAN function is disabled by default. When it is disabled, the switch is in VLAN transparent transmission mode and can forward all VLAN data. After it is enabled, you can create and configure a VLAN, as shown below.

> NOTE
>
> Enabling 802.1Q VLAN will remove all dynamic MAC addresses in the MAC table. Once it is enabled, disabling this function will remove the current VLAN configuration on the switch and all MAC addresses in the MAC table. Operate when necessary.

Create VLANs

When 802.1Q VLAN is enabled, you can view, create or delete a VLAN in the **VLAN Member** module.

To ensure that the switch in factory condition can communicate normally, the system creates 1 VLAN by default. All ports belong to this VLAN by default, the VLAN ID is 1, and the IP address defaults to 10.16.16.168. This VLAN cannot be deleted.

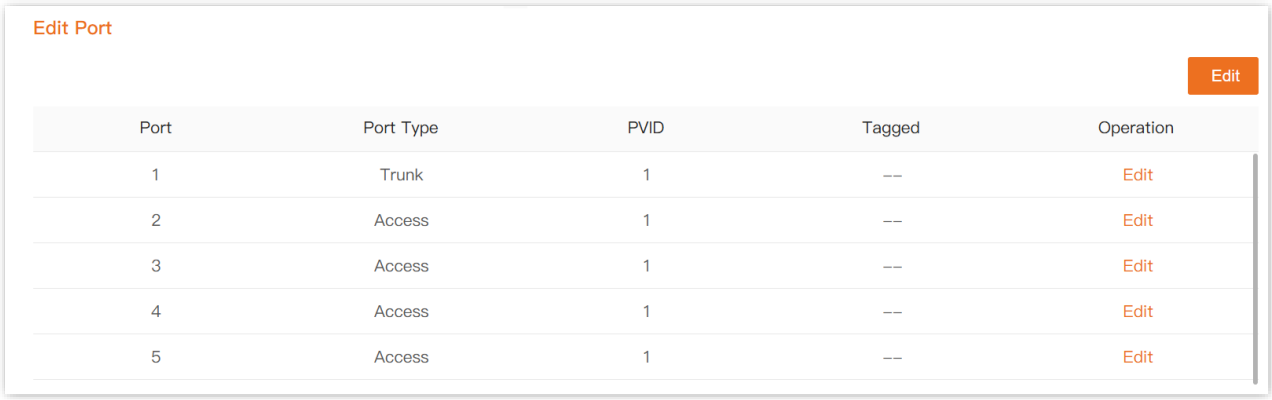


Parameter description

Name	Description
VLAN ID	Specifies the ID of the VLAN. By default, VLAN 1 is considered as the management VLAN.
VLAN Name	Specifies the name of the VLAN. If it is not set, the default name is "VLAN and four-digit VLAN ID". For example, when the VLAN ID is 3, the VLAN name is VLAN0003.
Port	Specifies the port that allows the corresponding VLAN to pass.

Configure VLANs

When 802.1Q VLAN is enabled, you can achieve VLAN isolation by configuring the port type, PVID, and allowed VLANs of each port on the switch in the **Edit Port** module.



Parameter description

Name	Description
Port	Specifies the ID of the port.
Port Type	Supported port types: Access and Trunk. – **Access**: An access port can join only one VLAN and send untagged packets. This type of port is used to connect to client devices, such as computers. – **Trunk**: A trunk port can receive and send packets belonging to multiple VLANs. This type of port is used as a cascade-connected port between switches.
PVID	Specifies the VLAN ID to which the port belongs by default. The PVID of each port defaults to 1. When a port receives untagged packets, they are forwarded to a specific VLAN based on the PVID.
Tagged	Specifies the VLAN that the port allows to pass. If the VLAN ID of the tagged packets received by the port is the same as the tagged VLAN, the port retains the tags of the packets and transmit them.

5.3 Example of configuing 802.1Q VLAN

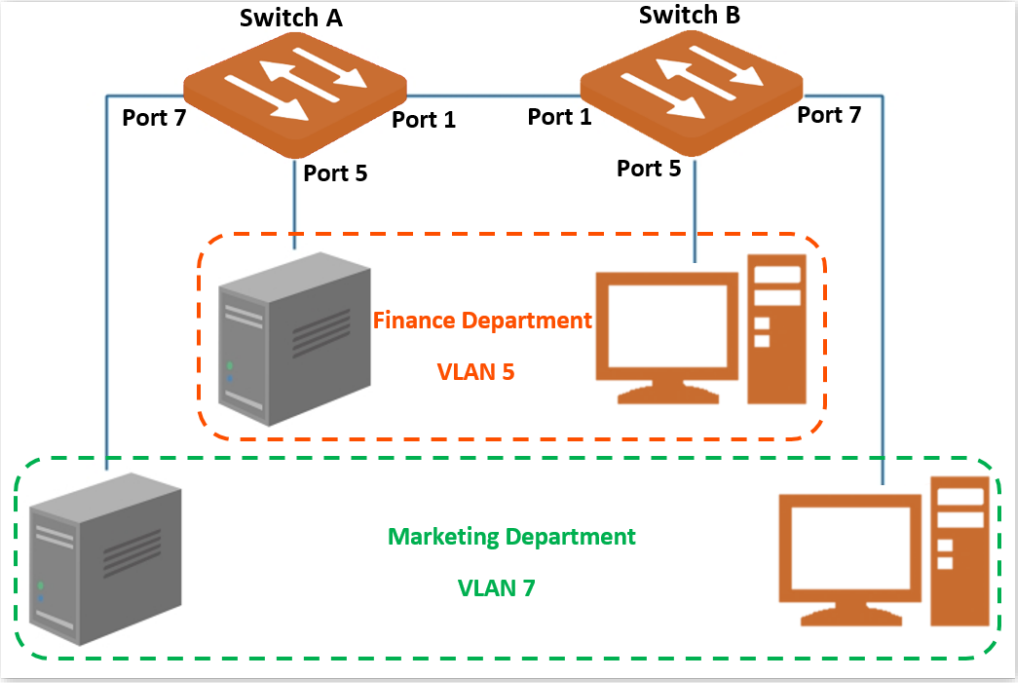
Network requirement

The staff in the Finance department and Marketing departments of a company work on the second floor, while the servers for these two departments are on the third floor. Now it is required that internal communication and server access is available within the departments, but the departments cannot communicate with each other.

Solution

Configure an 802.1Q VLAN for two switches:

- Create two VLANs for the switches. Assign the ports connected to the Finance department's devices to VLAN 5, and the ports to the Marketing department's devices to VLAN 7.
- Add the ports that connect two switches to both VLAN 5 and VLAN 7.



Configuration procedure

I. Configure Switch A

Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

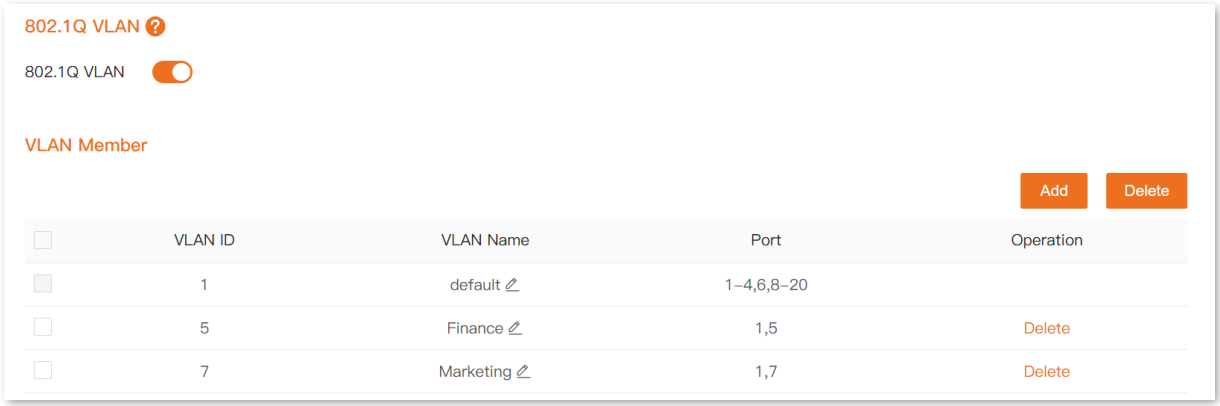
Step 2 Navigate to **Basci Function** > **VLAN**.

Step 3 Enable **802.1Q VLAN**.

Step 4 In the **VLAN Member** module, click **Add** and enter the following parameters on the pop-up window, and then click **OK**.

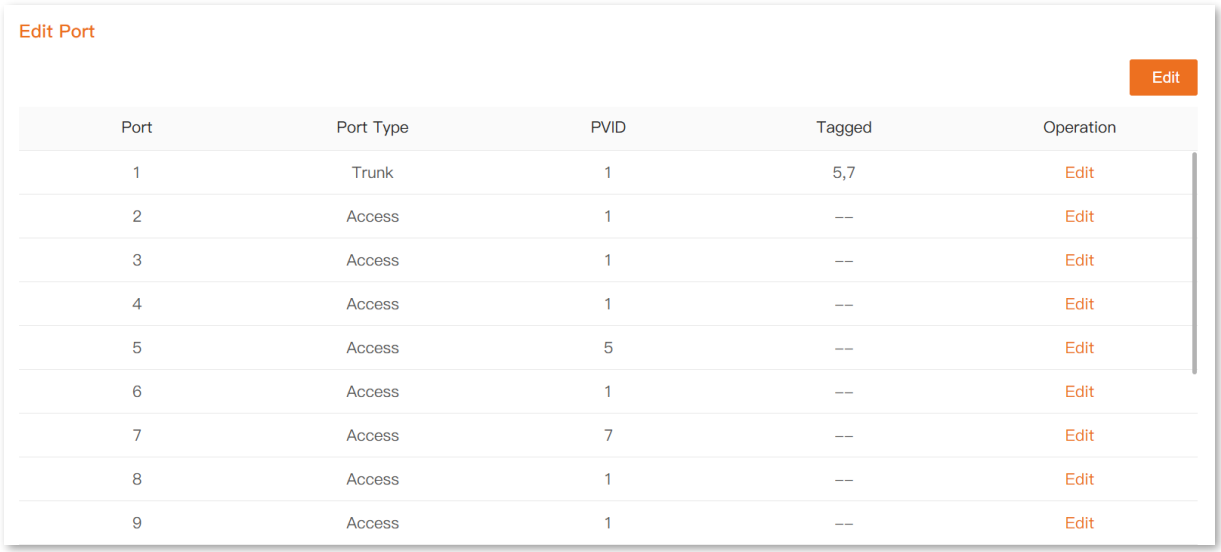
- Set **VLAN ID** to **5**.
- Set **VLAN Name** to **Finance**.

Step 5 Repeat step 4 and add another VLAN with the **VLAN ID** of **7** and **VLAN Name** of **Marketing**.



Step 6 In the **Edit Port** module, configure the VLANs.

1. Locate the port 5 and click **Edit**. Set **PVID** to **5**.
2. Locate the port 7 and click **Edit**. Set **PVID** to **7**.
3. Locate the port 1 and click **Edit**. Set **Type** to **Trunk**, and **Tagged** to **5,7**.



II. Configure Switch B

Refer to the steps of configuring Switch A.

---End

Verification

The staff can access the server of their department, but cannot access the server of the other department. The staff in the same department can communicate with each other but cannot communicate to the staff of other departments.

6 Change management IP/VLAN

TIP

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and firmware version. Please refer to the actual product.

The default management IP address is 10.16.16.168, and there is no management VLAN by default unless VLAN configured. When VLAN is enabled on the switch, management VLAN defaults to 1. Users in the LAN can access the switch web interface through the management IP address.

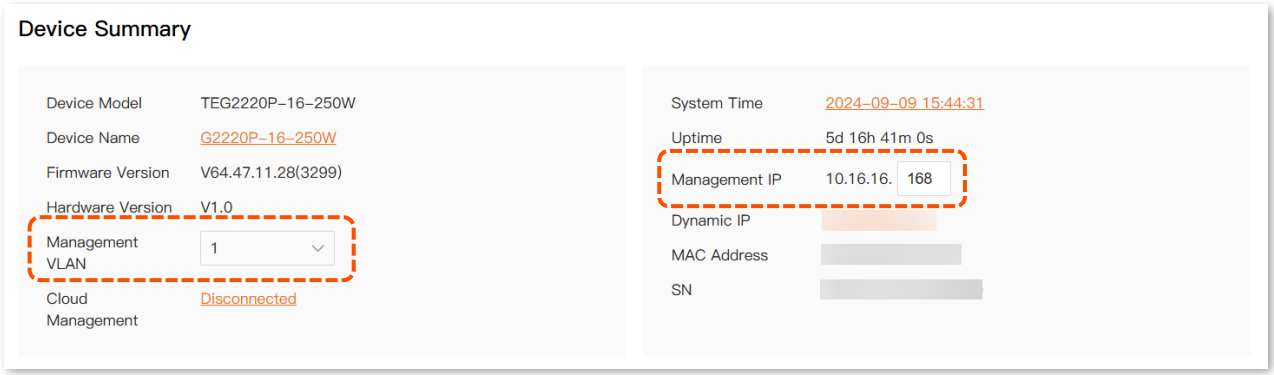
To change the management VLAN or IP address, take the following steps:

Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **Basic Function** > **Home**.

Step 3 On the **Device Summary** module, enter a new management VLAN and IP address as required.

Step 4 Wait for your configuration to take effect.



---End

After changing the management IP address and VLAN, you need to connect to the new management VLAN and access the new management IP address for login.

7 Change management account

TIP

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and firmware version. Please refer to the actual product.

To safeguard your network, periodically change the switch management password as follows:

Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

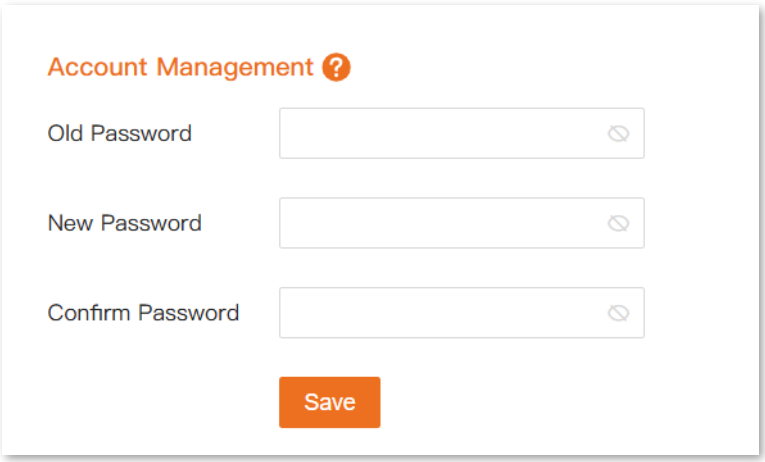
Step 2 Navigate to **Basic Function** > **Account Management**.

Step 3 For **Old Password**, enter your current management password.

Step 4 For **New Password**, enter a new password.

Step 5 For **Confirm Password**, enter your new password again.

Step 6 Click **Save**.



---End

After changing the password, you will be redirected to the login page. Enter the password you just set to log in to the switch's web interface.

8 Handle maintenance tasks

TIP

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and firmware version. Please refer to the actual product.

8.1 Upgrade firmware

After the firmware is upgraded on the switch, your data and settings remain unchanged.

NOTE

To avoid damage to the switch, ensure stable power supply to the switch during the upgrade.

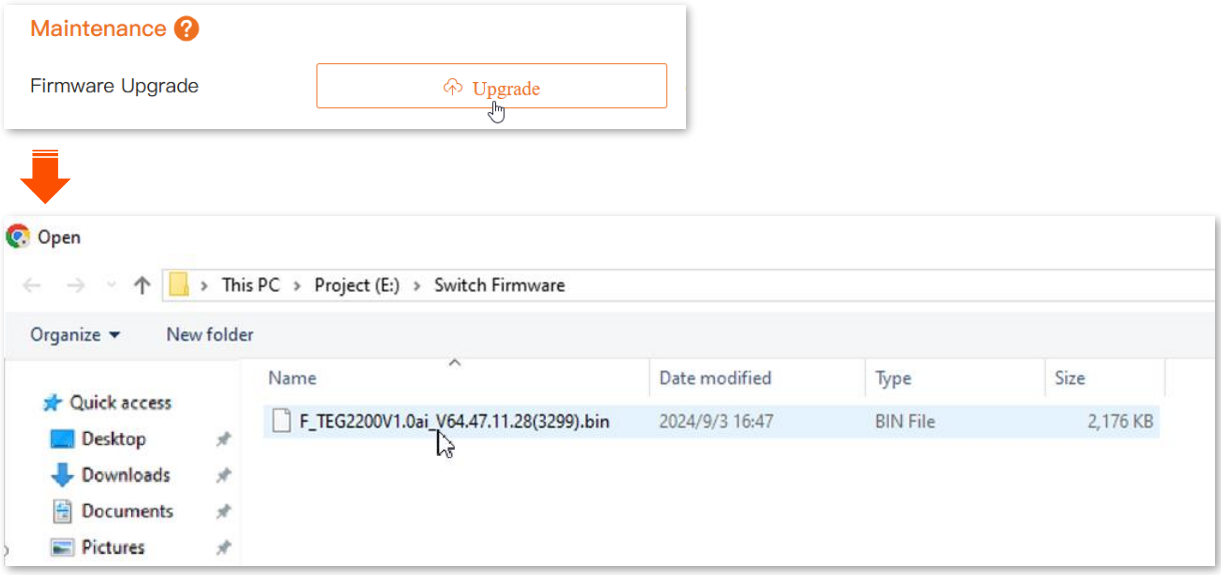
Procedure:

Step 1 Download the proper firmware from https://tendacn.com/default.html. Generally, the unzipped upgrade file is suffixed with **.bin**.

Step 2 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 3 Navigate to **Basic Function** > **Maintenance**.

Step 4 Click **Upgrade** to upload the firmware file you downloaded.



Step 5 Click **OK**.

---End

The firmware upload and update progress bars show in turn until they finish.

8.2 Back up configuration

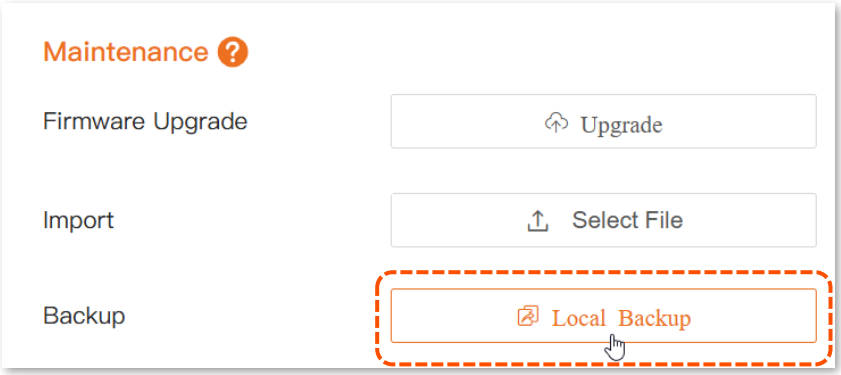
You can back up the switch configuration on the Tenda CloudFi cloud web UI or local computer.

8.2.1 Perform backup on the local computer

Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **Basic Function** > **Maintenance**.

Step 3 Click **Local Backup**.



Step 4 Click **OK**.

---End

The configuration file suffixed with.**cfg** will be download to the local computer.

TIP

If an "insecure donwload" reminder pops up, select "Keep" to download the file.

8.2.2 Perform backup on the Tenda CloudFi cloud web UI

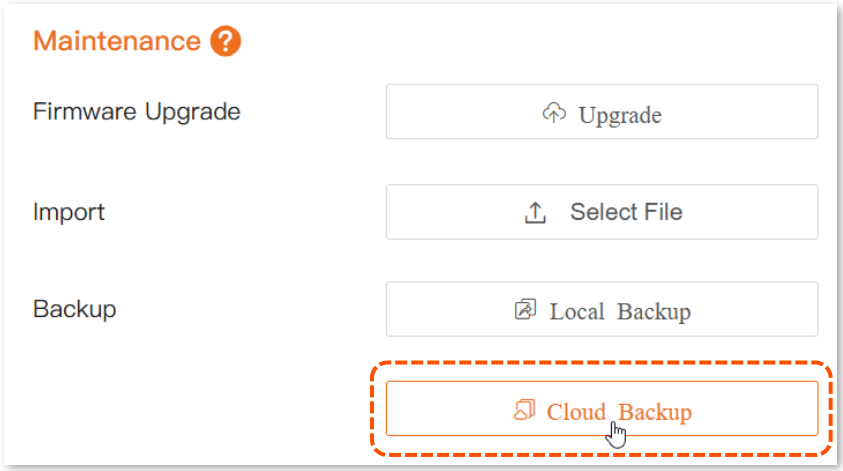
The switch must be managed by the Tenda CloudFi cloud platform before backup.

Procedure:

Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **Basic Function** > **Maintenance**.

Step 3 Click **Cloud Backup**.



Step 4 Click **OK**.

---End

Wait until cloud backup is successful, and back up the switch configuration to the Tenda CloudFi cloud platform.

8.3 Restore configuration

You can import the previously backed-up configuration file into the switch to restore the switch to the configuration status at that time.

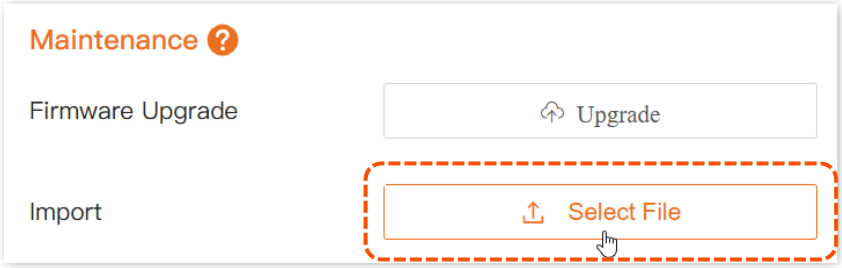
NOTE

The switch does not verify the contents of the configuration file. Please make sure that the configuration file is correct before importing it. The suffix of the configuration file is .cfg.

Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **Basic Function** > **Maintenance**.

Step 3 Click **Select File** and import the configuration backup into the switch.



---End

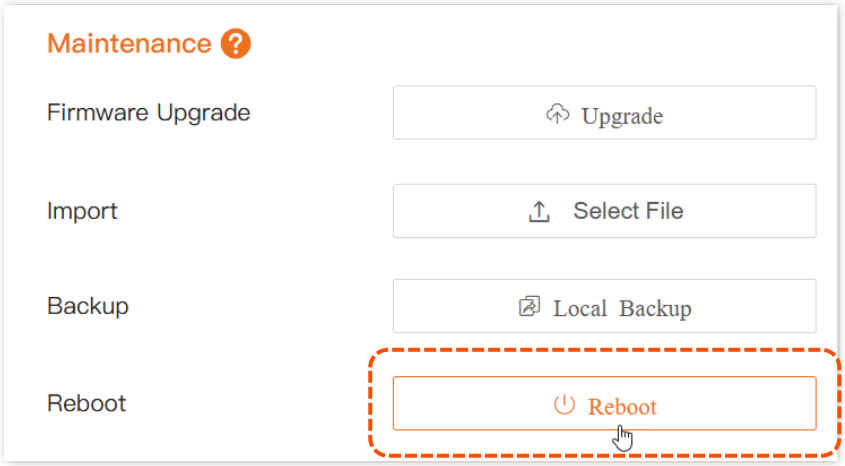
The switch will reboot to make the configuration take effect when the progress bar is filled.

8.4 Reboot the switch

Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **Basic Function** > **Maintenance**.

Step 3 Click **Reboot**.



Step 4 Click **OK**.

---End

The switch will reboot when the progress bar is filled.

8.5 Reset the switch

If you fail to locate a fault, or forget your username or password when you log in the web UI of the switch, you can restore the switch to factory settings. Once the switch is reset, the management IP address of the switch defaults to 10.16.16.168. If a management password is required for login, use the password on the label on the bottom of the switch.

Both firmware reset and hardware reset are supported.

NOTE

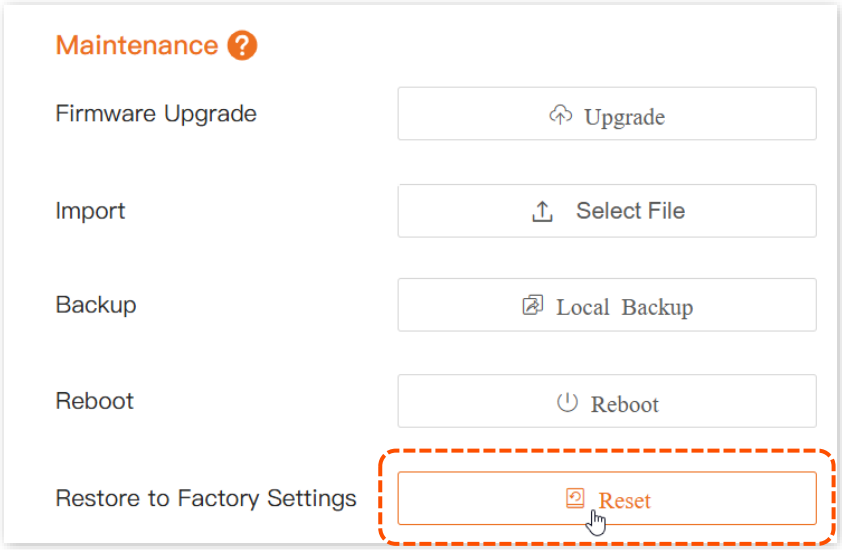
- To avoid damage to the switch, ensure stable power supply to the switch during factory reset.
- Resetting the switch will remove all user configuration. Operate when necessary.

Firmware reset

Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **Basic Function** > **Maintenance**.

Step 3 Click **Reset**.



Step 4 Click **OK**.

---End

The switch will be restored to factory settings and rebooted when the progress bar is filled.

Hardware reset

When the system indicator (**SYS**) is blinking, press and hold the reset button (**RST**, **Reset**, **RESET**) with a needle-like object for about 7 seconds, and then release it when all indicators are solid on. When the system indicator blinks again, the switch is restored to factory settings.

9 Change date and time

TIP

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and firmware version. Please refer to the actual product.

By default, the switch is in local time mode. After connecting to the Tenda CloudFi cloud platform, the switch automatically synchronizes the time to the project that it added to.

TIP

To ensure that time-based functions of the switch (such as PoE schedule) operate normally, connect the switch to the Tenda CloudFi cloud platform or synchronize the switch time with the internet.

To synchronize the switch system time with the internet:

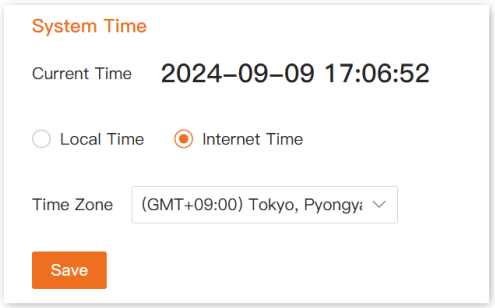
Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **Basic Function** > **Maintenance**.

Step 3 Select **Internet Time**.

Step 4 Select the time zone where the switch locates.

Step 5 Click **Save**. The following figure is for reference only.



---End

The switch will be synchronized to the network time at the selected time zone.

Parameter description

Name	Description
Sync Local Time	Used to synchronize the time of the computer where you manage the switch to the switch.

10 Diagnose the network

TIP

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and firmware version. Please refer to the actual product.

By running Ping tests, you can test the network connectivity and quality.

Procedure:

Assume you want to test the network connectivity between the switch and Google website.

Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

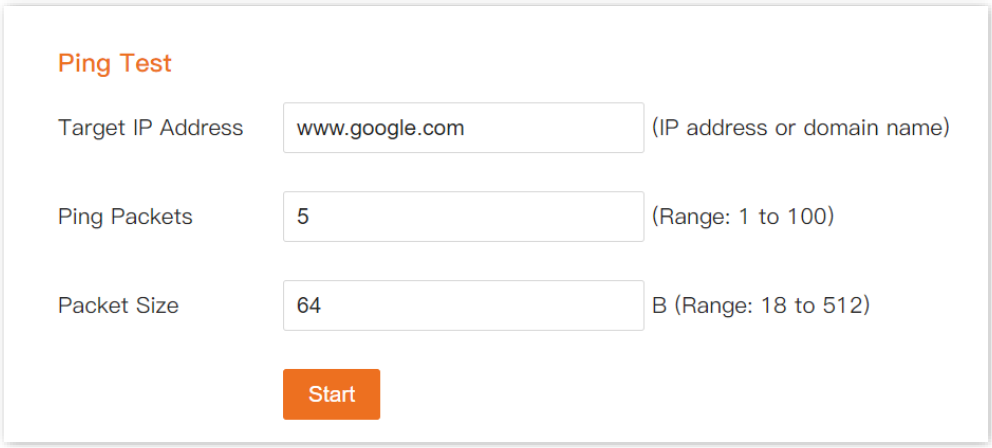
Step 2 Navigate to **Basic Function** > **Diagnostics**.

Step 3 For **Target IP Address**, enter the IP address domain name of the target device.

Step 4 (Optional) For **Ping Packets**, set the number of echo request packets. Default value is retained in this example.

Step 5 (Optional) For **Packet Size**, set the size of the echo request packets. Default value is retained in this example.

Step 6 Click **Start**.



---End

You can see the Ping test result information in the test result area.

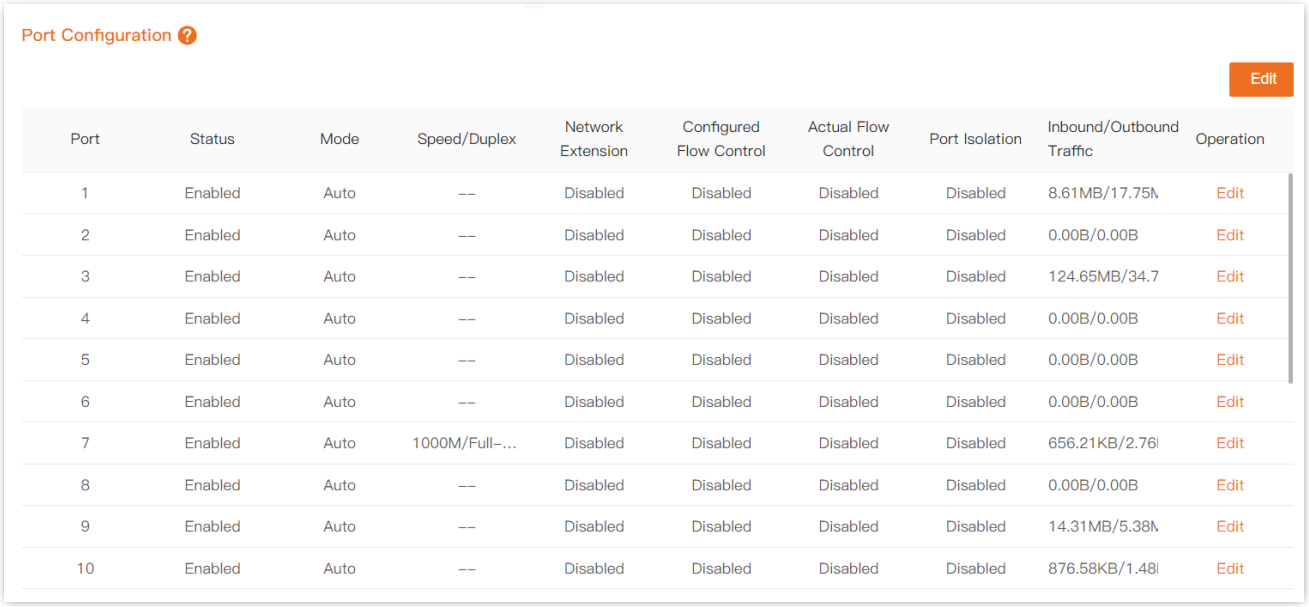
11 Configure switching

TIP

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and firmware version. Please refer to the actual product.

11.1 Port configuration

On the **Switching** > **Ports** page, you can view and configure port parameters.



Parameter description

Name	Description
Port	Specifies the ID of the port.
Status	Enabled by default. Click **Edit** to enable or disable the port. TIP **No Change** indicates that the port status remains unchanged.

Name	Description
Mode	Configured connection speed and duplex mode of the port. Click **Edit** to change. – **Auto**: Auto-configure the port's connection rate and duplex mode. – **10M/HDX**: Configure the port to 10 Mbps connection rate and half-duplex mode. – **10M/FDX**: Configure the port to 10 Mbps connection rate and full-duplex mode. – **100M/HDX**: Configure the port to 100 Mbps connection rate and half-duplex mode. – **100M/FDX**: Configure the port to 100 Mbps connection rate and full-duplex mode. – **1000M/FDX**: Configure the port to 1000 Mbps connection rate and full-duplex mode. – **No Change**: The port's connection rate and duplex mode remain unchanged.
Speed/Duplex	Used to display the actual connection speed and duplex mode of the port. TIP "--" indicates that the port is not connected or the negotiation failed.
Network Extension	Disabled by default. Click **Edit** to enable or disable network extension. After enabling this function, the data transmission distance of the switch port can be extended, which brings great convenience to network deployment. When this function is enabled on the port, it only supports 10Mbps full and half-duplex communication, but the port data transmission distance can exceed 100 meters, up to 250 meters. When the switch needs to be connected to client devices at a long distance (>100 meters), it is recommended to enable this function. TIP – **No Change** indicates that the function status remains unchaged. – To ensure the network extension effect, use CAT5e or above Ethernet cables, and set the speed and duplex mode of the peer device port to **Auto**. If the peer device is a network camera, adjust its code stream to below 8 Mbps to ensure the timeliness of video data transmission.

Name	Description
Configured Flow Control	Configured flow control mode of the port. It is disabled by default. **No Change** indicates that the function status remains unchanged. When flow control is enabled on both the switch and the peer device, if congestion occurs on a port of the switch, the port will send a flow control (Pause) frame to the peer device. After receiving the flow control frame, the peer device will pause sending data to the port of the switch. Similarly, when a port of this switch receives a flow control frame, the port will also stop sending data to the outside. NOTE Enabling flow control can avoid packet loss caused by inconsistent sending and receiving rates, but the communication rate between the data source port and other devices will be affected. Use this function with caution on ports connected to the internet.
Actual Flow Control	Used to display the actual flow control of the port.
Port Isolation	Disabled by default. Click **Edit** to enable or disable port isolation. When port isolation is enabled, isolated ports are isolated from each other and can only communicate with non-isolated ports. TIP **No Change** indicates that the function status remains unchanged.
Ingress Flow	Used to display data traffic received by the port.
Egress Flow	Used to display data traffic sent by the port.

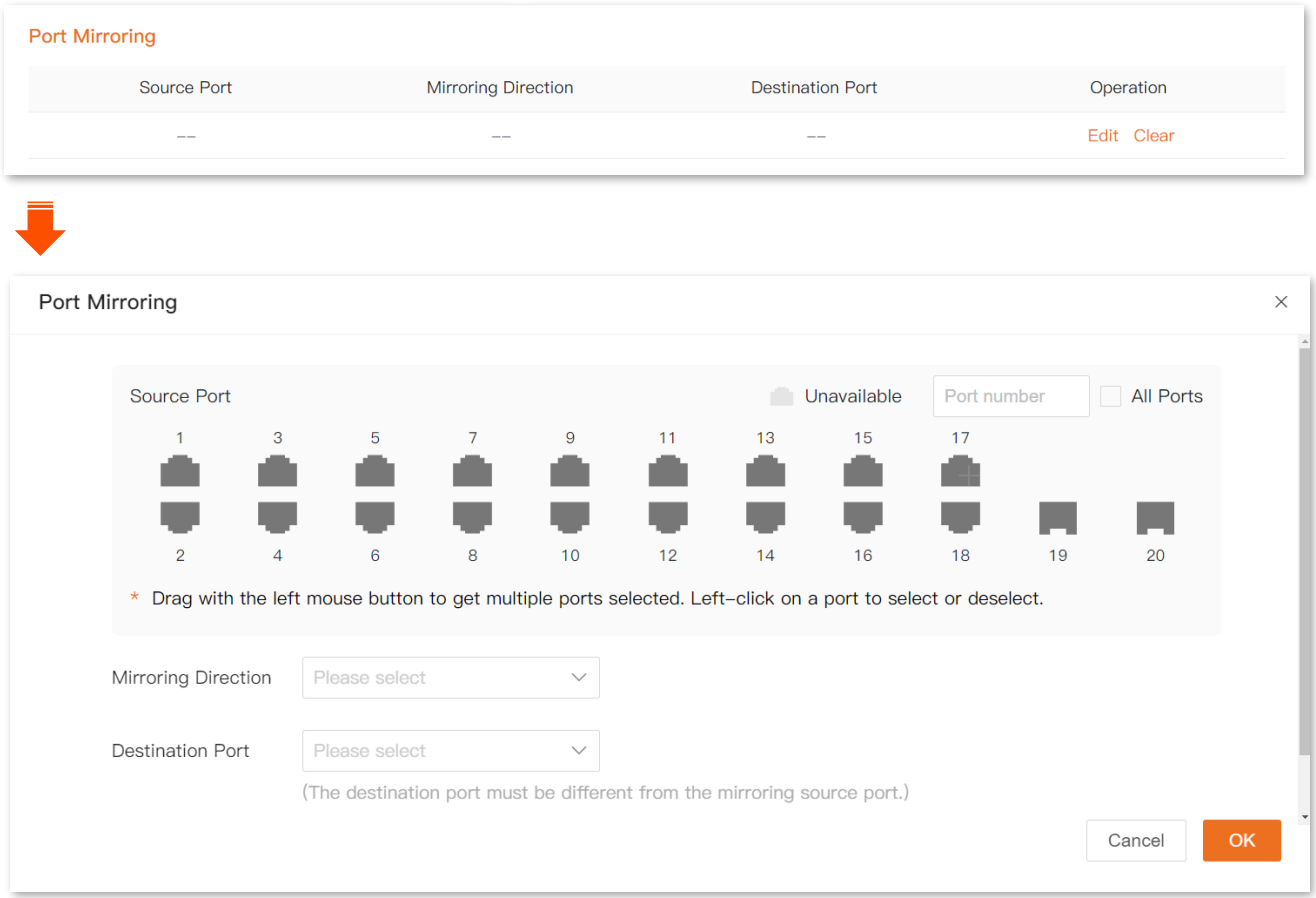
11.2 Port mirroring

Port mirroring is a method of copying and sending network packets from a port or multiple ports (source ports) to a specified port (destination port) of the switch. The destination port is commonly connected to a data monitoring device, enabling you to monitor data traffic, analyze performance, and diagnose faults.

On the **Switching** > **Port Mirroring** page, you can click **Edit** and configure port mirroring rules.

TIP

You can configure only one port mirroring rule.



Parameter description

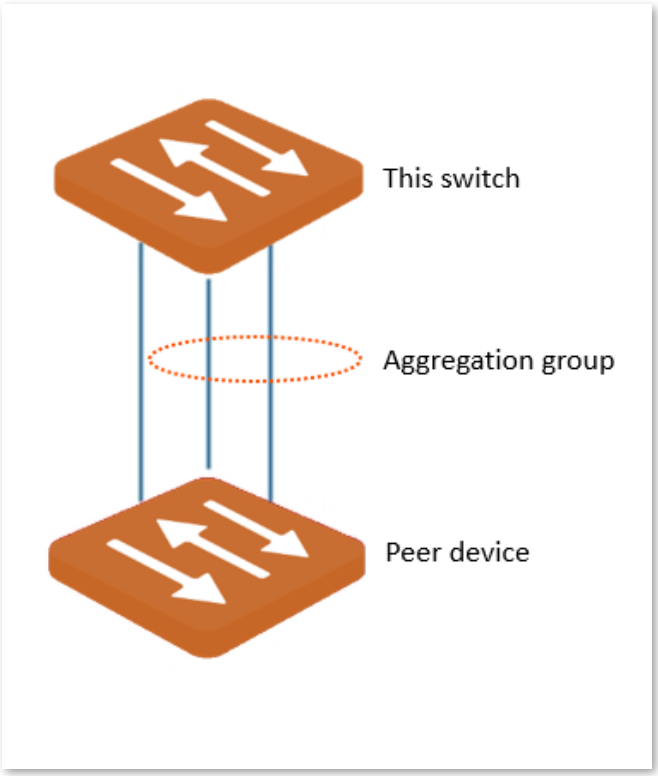
Name	Description
Source Port	Specifies the port to be mirrored. Multiple ports can be selected.
Mirroring Direction	Specifies the packet type. – **Ingress**: Packets received by source ports will be copied to the destination port. – **Egress**: Packets transmitted by source ports will be copied to the destination port. – **Two-way**: Packets transmitted and received by source ports will be copied to the destination port.
Destination Port	Packets of source ports will be copied to this port. A mirroring group can contain only one destination port.

11.3 Port aggregation

Port aggregation is used to converge multiple physical ports into a logical aggregation group, and multiple physical links in one aggregation group are regarded as one logical link. The port aggregation function binds multiple physical links into one logic link and enables them to share

traffic load for each other, thus increasing the bandwidth between the switch and peer device. Meanwhile, each member in an aggregation group backs up each other's data dynamically, improving connection reliability.

The network topology of port aggregation is shown as follows.

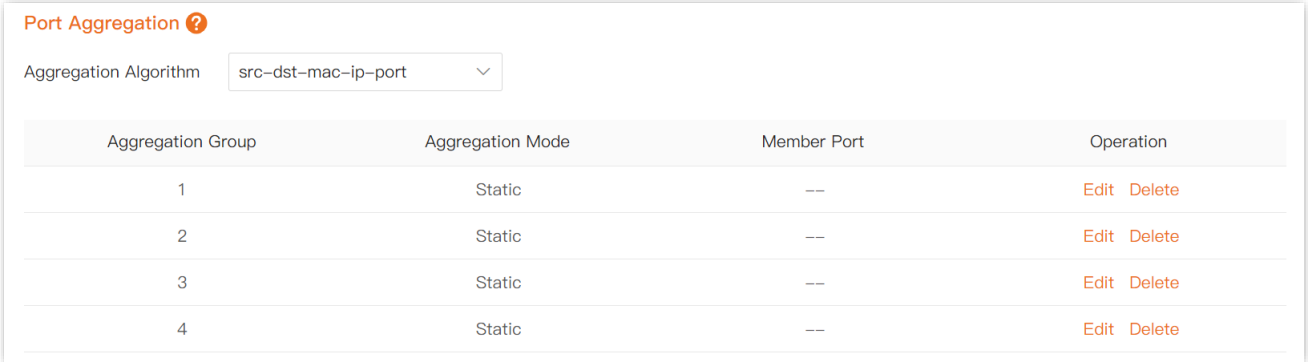


NOTE

- In the same aggregation group, all member ports must be set to the same configurations with respect to QoS, VLAN and port configuration.
- Mirrored ports cannot be added to aggregation groups.

On the **Switching** > **Port Aggregation** page, there are four default static port aggregation groups. To configure the aggregation group, click **Edit**. To delete its configuration, click **Delete**. Port aggregation groups cannot be added or deleted.

Here you can find four preset port aggregation groups.



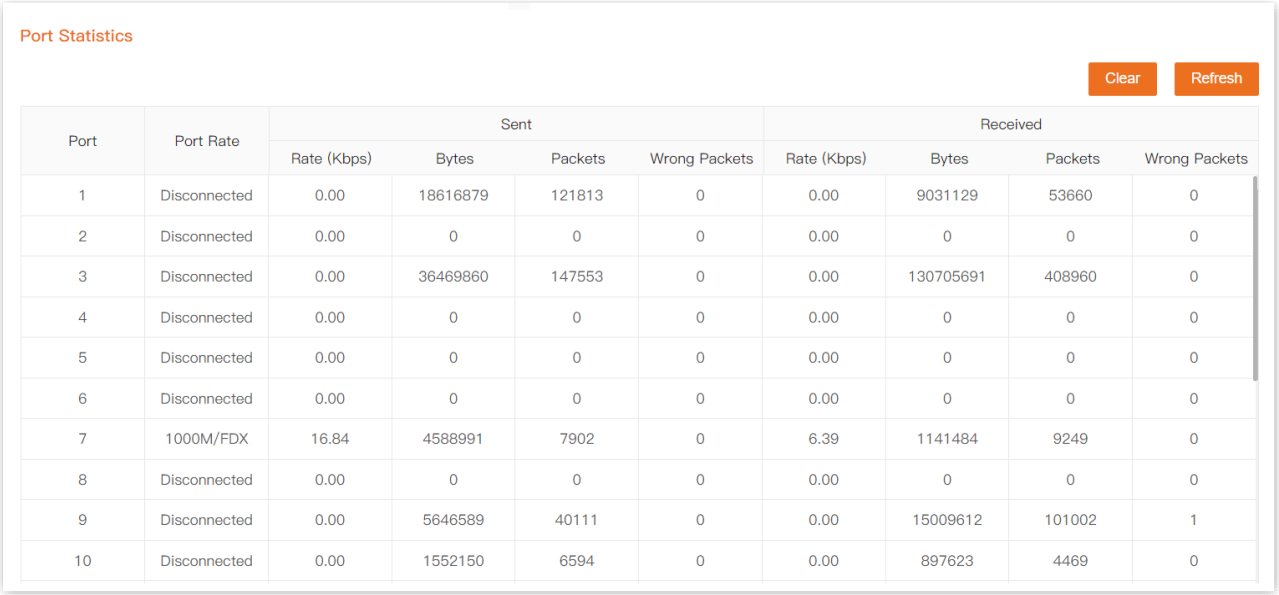
Parameter description

Name	Description
Aggregation Algorithm	Specifies the routing algorithm for the four static aggregation groups: – **src-dst-mac-ip-port**: Member ports in the aggregation group share the load based on the source MAC address, destination MAC address, source IP address, destination IP address, TCP or UDP source port number and destination port number in the received packet. – **src-dst-mac**: Member ports in the aggregation group share the load based on the source MAC address and destination MAC address in the received packet. – **src-dst-ip**: Member ports in the aggregation group share the load based on the source IP address and destination IP address in the received packet.
Aggregation Group	Specifies the ID of aggregation groups. Editing is not allowed.
Aggregation Mode	Specifies the aggregation mode of the aggregation group. Only static aggregation mode is supported, that is, all member ports in the aggregation group converge into one logical port. NOTE The aggregation mode of the switch needs to be the same as that of the peer device. Otherwise, the data cannot be forwarded properly or a loop occurs.
Member Port	Specifies the member ports of the aggregation group.

11.4 Port statistics

On the **Switching** > **Port Statistics** page, you can view the status, connection speed and duplex mode and packet statistics of each port, or clear the packet statistics of each port.

To clear the packet statistics of each port, click **Clear**. To refresh the packet statistice of each port, click **Refresh**.



Port	Port Rate	Sent				Received			
		Rate (Kbps)	Bytes	Packets	Wrong Packets	Rate (Kbps)	Bytes	Packets	Wrong Packets
1	Disconnected	0.00	18616879	121813	0	0.00	9031129	53660	0
2	Disconnected	0.00	0	0	0	0.00	0	0	0
3	Disconnected	0.00	36469860	147553	0	0.00	130705691	408960	0
4	Disconnected	0.00	0	0	0	0.00	0	0	0
5	Disconnected	0.00	0	0	0	0.00	0	0	0
6	Disconnected	0.00	0	0	0	0.00	0	0	0
7	1000M/FDX	16.84	4588991	7902	0	6.39	1141484	9249	0
8	Disconnected	0.00	0	0	0	0.00	0	0	0
9	Disconnected	0.00	5646589	40111	0	0.00	15009612	101002	1
10	Disconnected	0.00	1552150	6594	0	0.00	897623	4469	0

Parameter description

Name		Description
Port		Specifies the ID of the port.
Port Rate		Specifies the connection rate and duplex mode of the port.
Sent	Rate	Specifies the sending rate of the port.
	Bytes	Specifies the total number of bytes sent by the port.
	Packets	Specifies the total number of packets sent by the port.
	Wrong Packets	Specifies the total number of wrong packets sent by the port.
Received	Rate	Specifies the receiving rate of the port.
	Bytes	Specifies the total number of bytes received by the port.
	Packets	Specifies the total number of packets received by the port.
	Wrong Packets	Specifies the total number of wrong packets received by the port.

11.5 Loop guard

After loop guard is enabled, the port where the loop occurs will be blocked and no packets will be forwarded if a loop exists on the switch. After the loop is eliminated, the port will automatically return to the forwarding state.

On the **Switching** > **Loop Guard** page, you can enable or disable loop guard on the switch. This function is disabled by default. When it is enabled, the page is displayed as follows.

11.6 Cable testing

Using cable tseting, you can get a picture of the cable status of each port on the switch (such as whether the cable is disconnected or damaged). This helps you further locate and diagnose network failures.

Procedure:

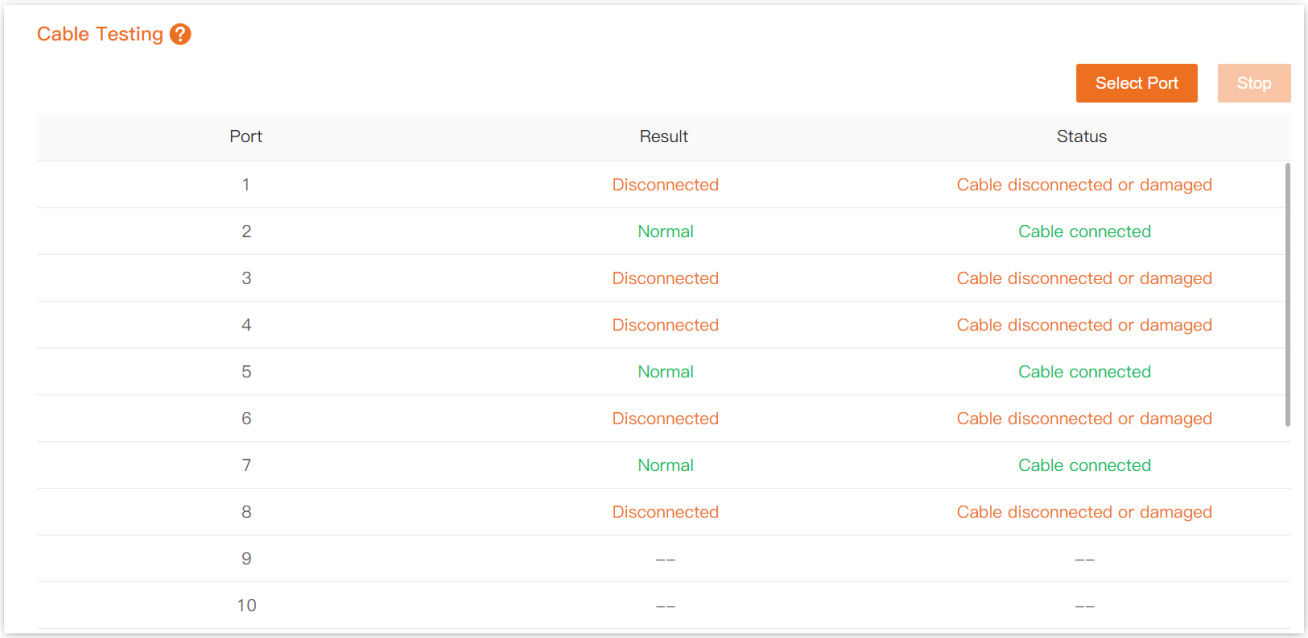
Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **Switching** > **Cable Testing**.

Step 3 Click **Select Port,** select ports to be detected, and then click **Start**.

---End

Wait until the testing results appear.



11.7 Jumbo frames

Through the jumbo frame function, the data transmission capacity of the port can be increased, thereby improving link utilization and obtaining better network performance.

On the **Switching** > **Jumbo Frames** page, you can enable or disable jumbo frames on the switch. This function is disabled by default. When it is enabled, the size of packets sent or received by each port of the switch can be increased to 3072 bytes.

12 Network security

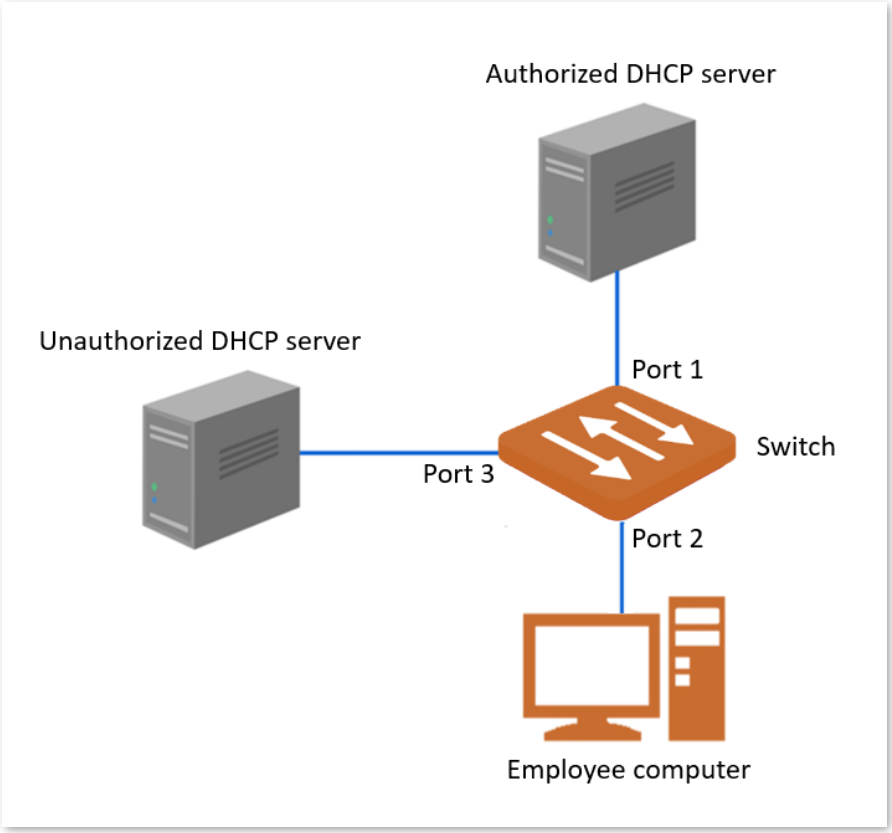
TIP

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and firmware version. Please refer to the actual product.

12.1 DHCP snooping

After DHCP snooping is enabled on the switch, users can only obtain IP addresses through DHCP servers connected to trusted ports and unauthorized DHCP servers will be blocked.

As shown in the figure below, a company has deployed switches on the office floor. Switch port 2 is connected to employee computers, which use DHCP to obtain IP addresses. An authorized DHCP server is deployed on the network, and switch port 1 is connected to the authorized DHCP server.



At present, unauthorized DHCP server access often occurs on office floors, causing employee computers to obtain wrong addresses and being unable to access the internet, or causing employee computers to obtain conflicting addresses.

Procedure:

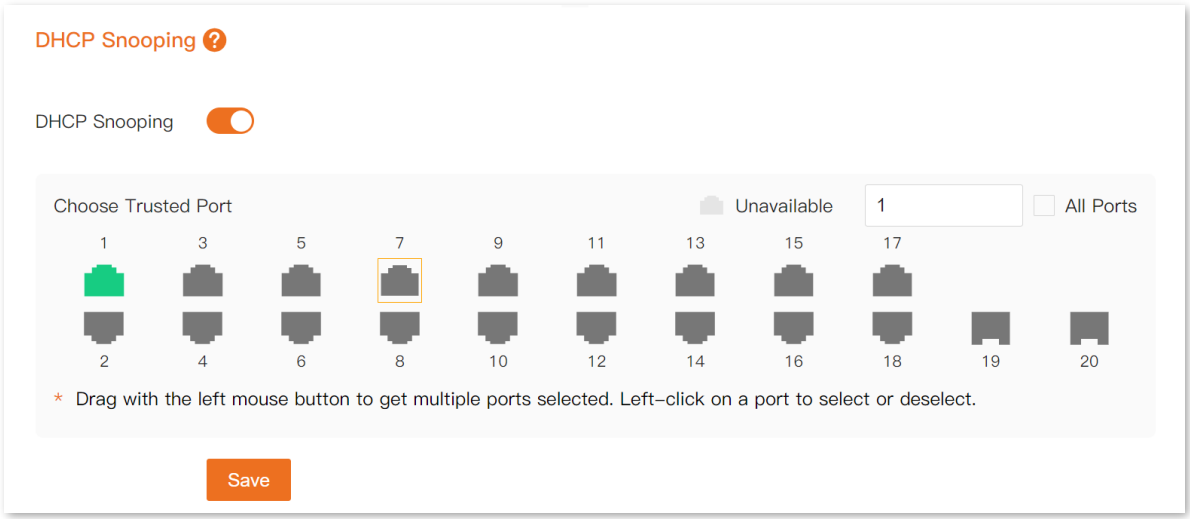
Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **Network Security** > **DHCP Snooping**.

Step 3 Enable **DHCP Snooping**.

Step 4 Select port 1.

Step 5 Click **Save**.



---End

After completing the above configuration, employee computers can only obtain IP address information from authorized DHCP servers, and unauthorized DHCP servers cannot assign IP address information to employee computers.

Parameter description

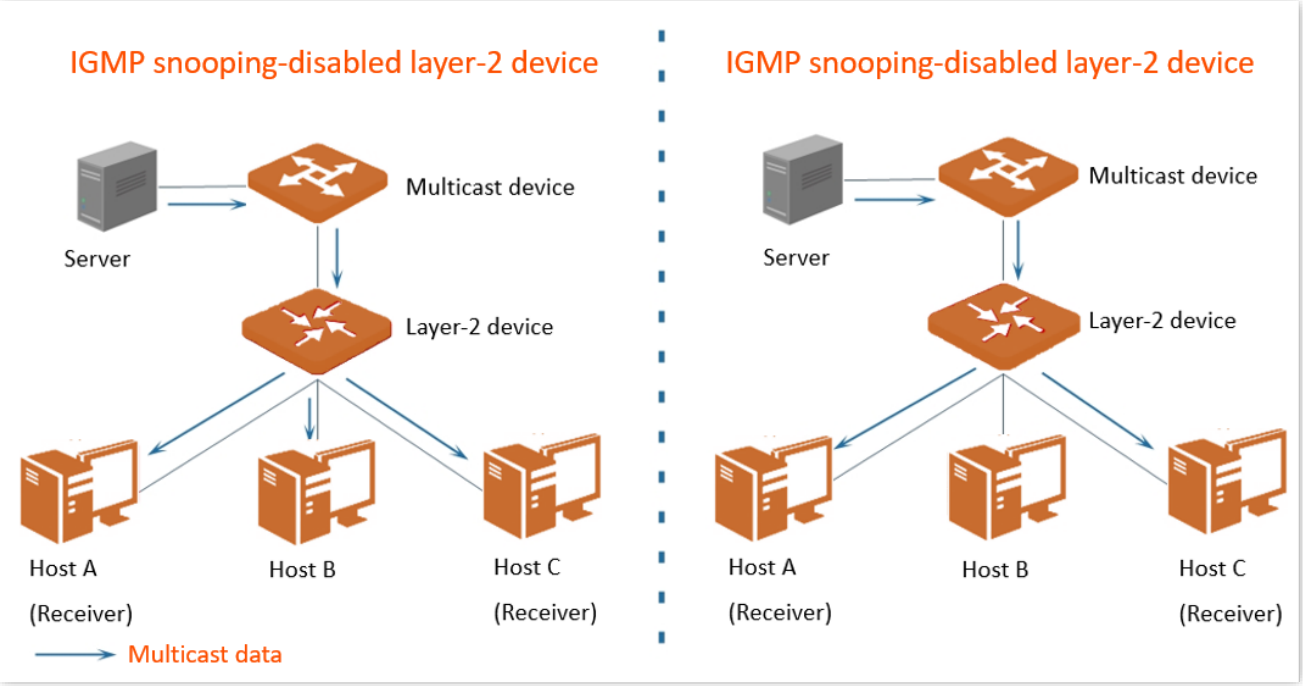
Name	Description
Choose Trusted Port	A trusted port can forward the received DHCP packets and is used to connect to the authorized DHCP server. TIP When DHCP snooping is enabled, the following situations occur by default: – If the switch obtains an IP address from the DHCP server in the LAN and can ping any website (such as www.google.com), and the port connected to the DHCP server is the same as the port connected to the upstream gateway, this port is marked in green and set as trusted by default. If the port connected to the DHCP server is different from the port connected to the upstream gateway, these two ports are marked with a rectangle symbol and recommended as trusted ports. – If the switch obtains an IP address from the DHCP server in the LAN but cannot ping any website, the port connected to the DHCP server is marked with a rectangular symbol and recommended as trusted port. – If the switch does not obtain an IP address from the DHCP server but can ping any website, the port connected to the upstream gateway is marked with a rectangular symbol and recommended as trusted port. – If the switch does not obtain an IP address from the DHCP server and cannot ping any website, set all ports as trusted and they will be marked in green.

12.2 IGMP snooping

12.2.1 Overview

Internet Group Management Protocol Snooping (IGMP snooping) is a multicast restriction mechanism that runs on layer-2 Ethernet switches and is used to manage and control multicast groups.

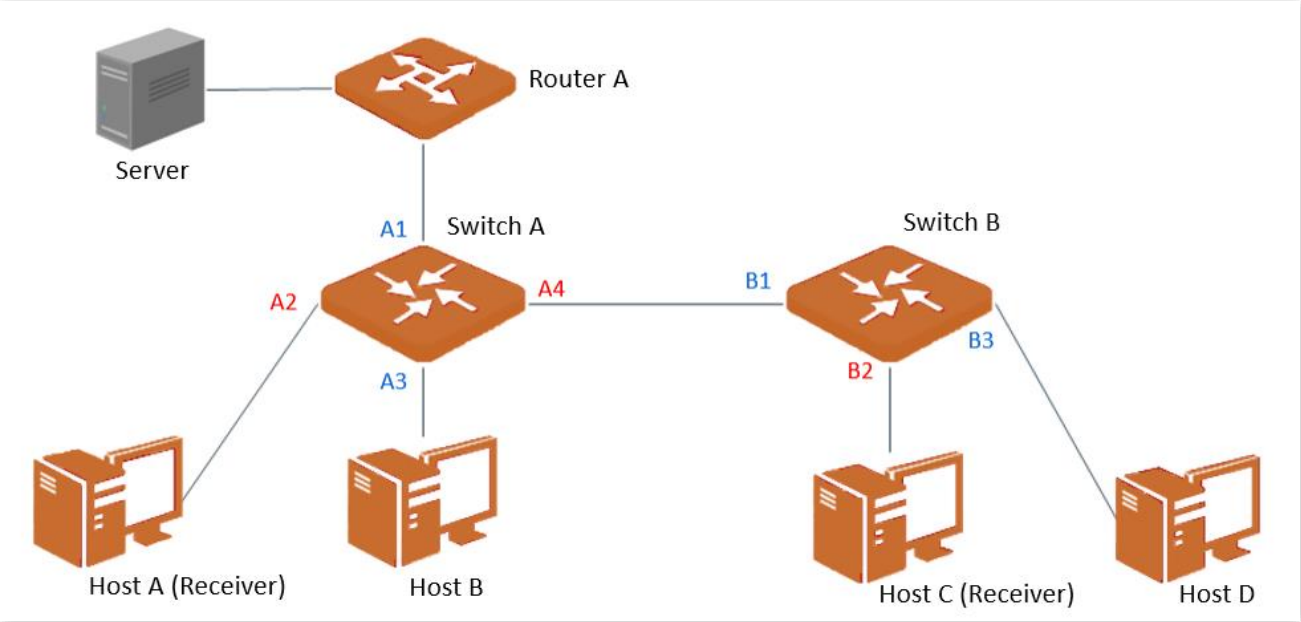
As shown in the figure below, multicast data is broadcasted from the IGMP snooping-disabled layer-2 device; But with IGMP snooping enabled, the layer-2 device will establish a mapping table for ports and multicast MAC addresses by analyzing IGMP packets, and forward multicast data to the specific receiver.



IGMP snooping only forwards data to the specific receivers through the layer-2 multicast, providing the following advantages:

- Reduce broadcast in layer-2 network and saves network bandwidth.
- Enhance the security of multicast data.
- Provide convenience for charging management to each host.

As shown in the following figure, router A is connected to the multicast source, IGMP snooping is enabled on switch A and switch B, while host A and host C are the receivers of the multicast data.



- **Router port**

  On an IGMP-snooping-enabled layer 2 device, the ports toward upstream layer 3 multicast devices are called router ports (Ports A1 and B1 in the above figure).

- **Member port**

  On an IGMP-snooping-enabled layer 2 device, the ports toward downstream receiver hosts are called host ports (Ports A2, A4 and B2 in the above figure).

- **General query**

  The IGMP querier (router A in the above figure) periodically sends IGMP general queries to all hosts and devices in the local network segment to check the multicast group members.

  After receiving an IGMP general query, the layer 2 device (switches A and B in the above figure) forwards the query, and performs the following treatment to the receiving ports:

  - If the receiving port is included in the mapping table, the layer 2 device restarts the aging timer for the port.
  - If the receiving port is excluded in the mapping table, the layer 2 device adds the port to the mapping table and starts an aging timer for the port.

- **Specific query**

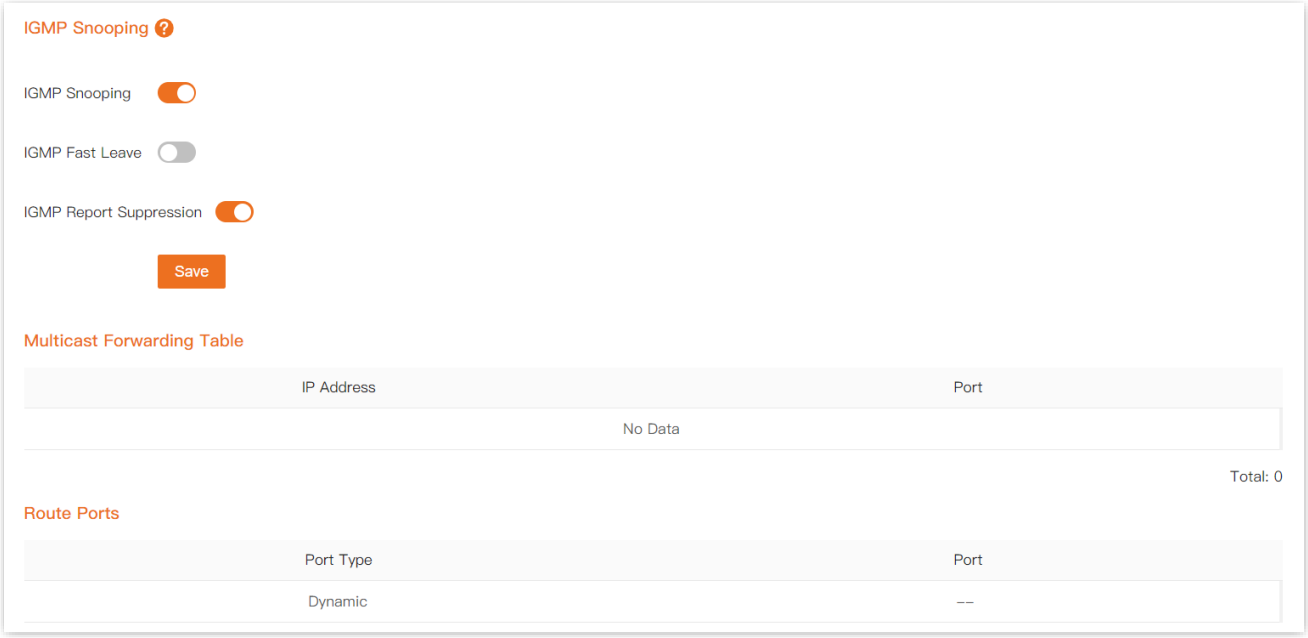
  When a host with enabled IGMPv2 or IGMPv3 leaves the multicast group, it sends IGMP leave group packets. When the ports of the layer-2 devices (switches A and B in the above figure) receive the IGMP leave group message, the following actions will be done based on the mapping table:

  - If no forwarding entry of the multicast group is found or the matching forwarding entry does not contain the receiving port, the layer 2 device discards the IGMP leave group message directly instead of forwarding it to other ports.
  - If the forwarding entry of the multicast group is found, and the matching forwarding entry contains other host ports, the layer 2 device discards the IGMP leave group message directly instead of forwarding it to other ports, and sends an IGMP specific query message to the leaving host.
  - If the forwarding entry of the multicast group is found, and the matching forwarding entry does not contain other host ports, the layer 2 device forwards the message through the router port and also sends an IGMP specific query message to the host.

12.2.2 Configure IGMP snooping

On the **Network Security** > **IGMP Snooping** page, you can configure IGMP snooping on the switch.

This function is disabled by default. When it is enabled, the page is displayed as follows.

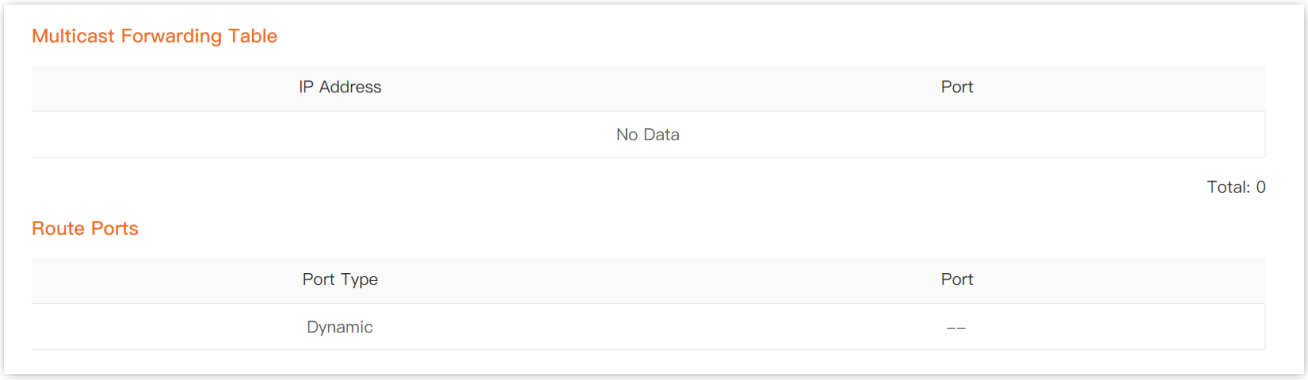


Parameter description

Name	Description
IGMP Snooping	Used to enable or disable IGMP snooping.
IGMP Fast Leave	Used to enable or disable IGMP fast leave. When it is enabled, when the switch receives an IGMP leave group message from a host to leave a multicast group, it directly deletes the port from the corresponding IGMP snooping multicast forwarding table without waiting for the host port aging time to expire.
IGMP Report Suppression	Used to enable or disable IGMP report suppression. When it is enabled, the switch forwards only the first IGMP report message for each multicast group to the IGMP querier within a query interval, and suppresses subsequent IGMP report packets for the same multicast group. This function prevents duplicate report packets from being sent to IGMP queriers.

12.2.3 View multicast forwarding table and route table

On the **Network Security** > **IGMP Snooping** page, you can view the current multicast forwarding table in the **Multicast Forwarding Table** module and and route ports for multicast in the **Route Ports** module.



Parameter description

Name		Description
Multicast Forwarding Table	IP Address	Specifies the IP address of the multicast group.
	VLAN ID	Specifies the VLAN ID of the multicast group.
	Port	Specifies the member port of the multicast group.
Route Ports	Port Type	Specifies the type of the routing port of the multicast group. Only dynamic routing ports are displayed currently.
	Port	Specifies the routing port of the multicast group.

12.3 MAC tables

12.3.1 Overview

A MAC address table is used by the switch to record the correspondence between MAC addresses, ports, and the VLANs that the ports belong to. The switch automatically generates dynamic MAC address entries by learning source MAC addresses. Administrators can manually add static MAC address tables. Only dynamic MAC address table entries are subject to aging time limits.

The switch forwards messages according to the MAC address table, improving network communication efficiency.

12.3.2 Quickly bind static/allowed MAC addresses

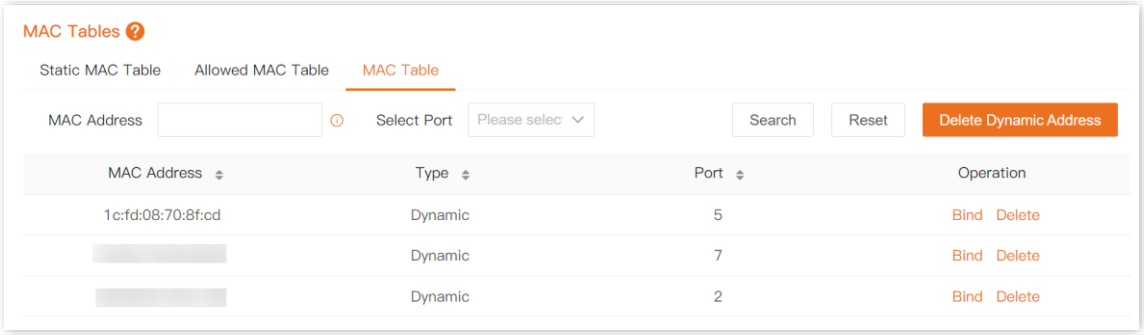
NOTE

This function may be unavailable for some models. The actual web user interface prevails.

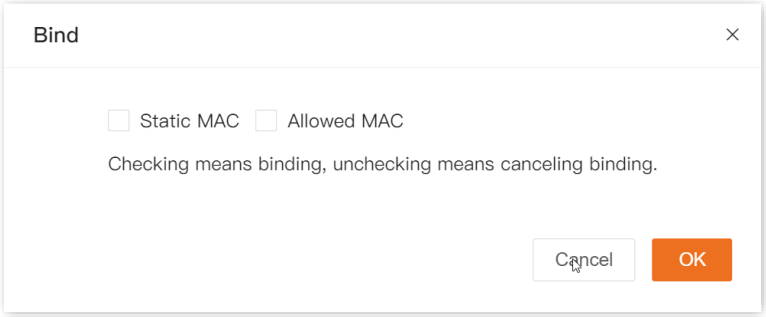
Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **Network Security** > **MAC Tables**, and select the **MAC Table** tab.

Step 3 Locate the taget device and click **Bind**. The following figure is for reference only.



Step 4 Select **Static MAC** or **Allowed MAC** as required, and click **OK**.



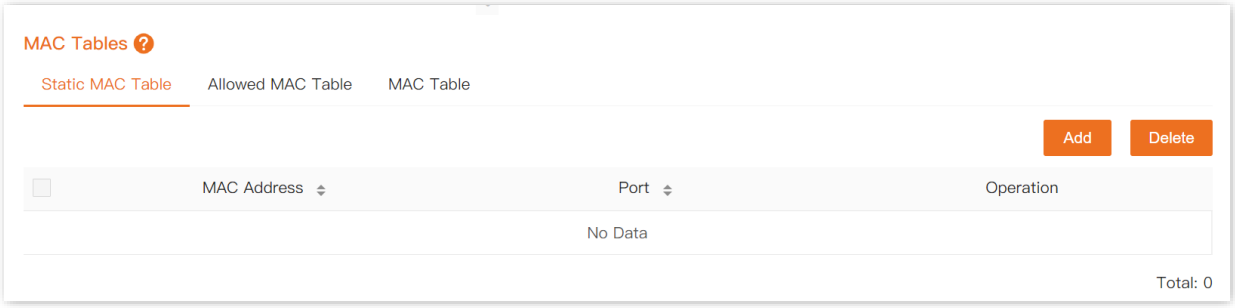
---End

12.3.3 Manually add static MAC addresses

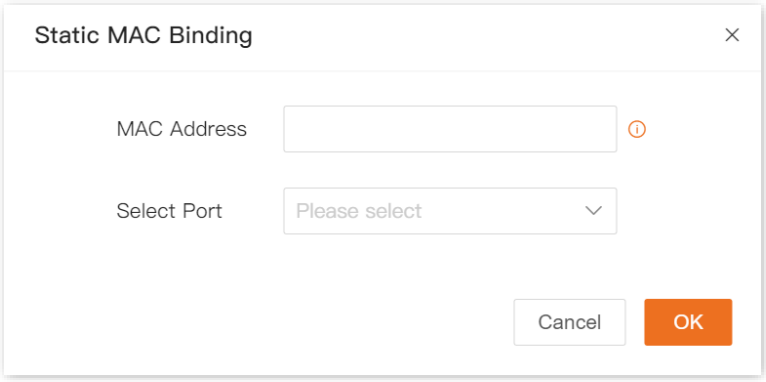
Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **Network Security** > **MAC Tables**, and select the **Static MAC Table** tab.

Step 3 Click **Add**.



Step 4 Configure the static MAC table, and click **OK**.



---End

After configuration, you can view the static MAC address entries in the MAC table.

Parameter description

Name	Description
MAC Address	Specifies the MAC address. Format: XX:XX:XX:XX:XX:XX, XXXX-XXXX-XXXX or XXXXXXXXXXXX.
VLAN ID	Specifies the VLAN to which the MAC address belongs.
Port	Specifies the physical port of the switch where the MAC address resides.

12.3.4 Manually add allowed MAC addresses

After a MAC address is bound to a switch port, the switch port only allows the specific client to access.

NOTE

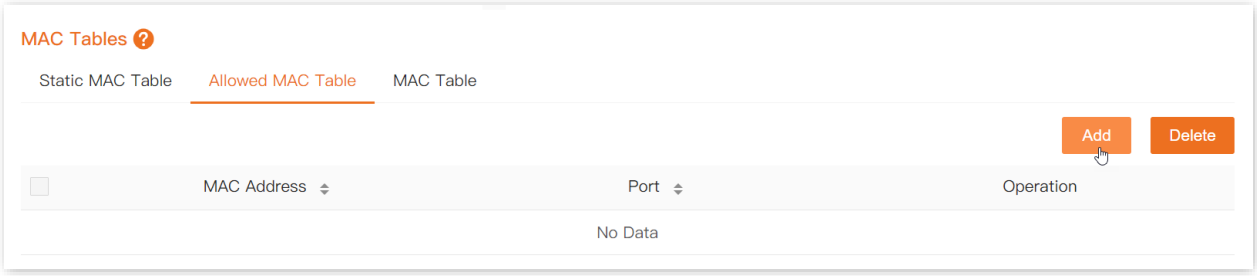
Configuration errors may cause the switch or its clients to be disconnected from the network. Operate with caution.

Procedure:

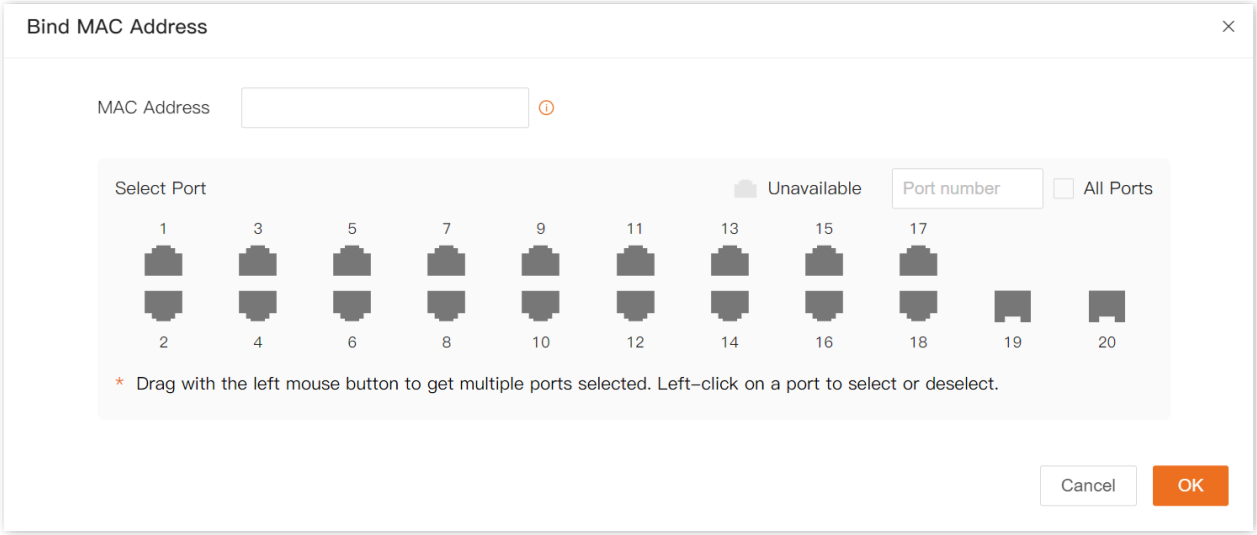
Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **Network Security** > **MAC Tables**, and select the **Allowed MAC Table** tab.

Step 3 Click **Add**.



Step 4 Enter the target MAC address, select ports, and click **OK**.



---End

Parameter description

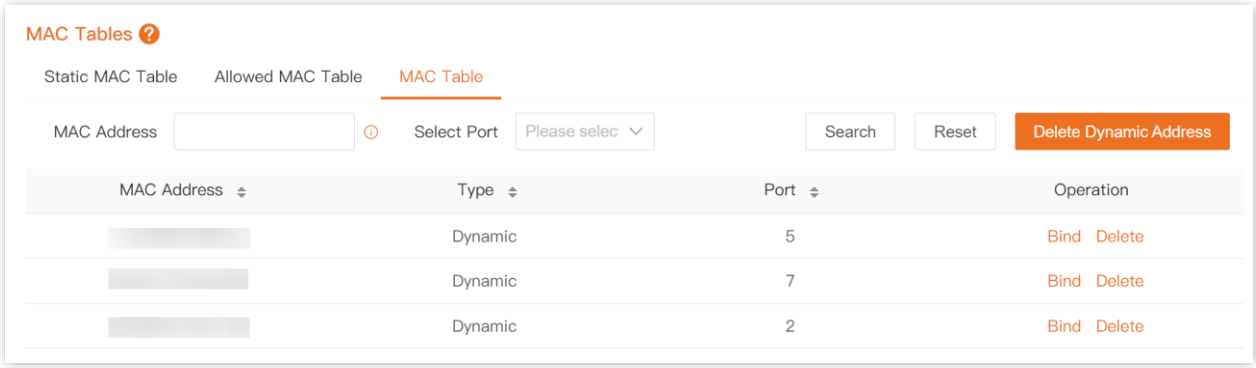
Name	Description
MAC Address	Specifies the MAC address of the client bound to the switch port. Format: XX:XX:XX:XX:XX:XX, XXXX-XXXX-XXXX or XXXXXXXXXXXX.
Port	Specifies the physical port of the switch where the MAC address resides.

12.3.5 View and delete MAC address entries

To access the page:

Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **Network Security** > **MAC Tables**, and select the **MAC Table** tab.



Query parameters and buttons description

Name	Description
MAC Address	Enter the MAC address to be queried. TIP You can fuzzy query for MAC address with at least 2 consecutive bytes. Format: XX-XX, XX: XX or XXXX.
VLAN ID	Enter the VLAN ID that the MAC address to be queried belongs to.
Select Port	Enter the physical port of the switch where the MAC address to be queried is located.
Search	Enter keywords in the MAC address, VLAN ID, and port selection input boxes, and click this button to query the MAC address entry in a fuzzy or exact manner.

Parameters and other buttons description

Name	Description
MAC Address	Specifies the MAC address in the format XX:XX:XX:XX:XX:XX.
VLAN ID	Specifies the VLAN ID that the MAC address belongs to.
Type	Specifies the type of the MAC address. – **Static**: MAC address entry manually configured by the administrator. – **Dynamic**: MAC address entry automatically generated by the switch. TIP The dynamic MAC address starts timing when it is added to the MAC table. If each port does not receive data with the source address of the MAC address within the aging time of 300 seconds, the address will be deleted from the MAC table.
Port	Specifies the physical port of the switch where the MAC address resides.

Name	Description
Reset	Used to delete all MAC address entries on the current page.
Delete Dynamic Address	Used to delete all dynamic MAC address entries on the current page.
Bind	Used to quickly bind the MAC address to the static MAC table or allowed MAC table. TIP This function may be unavailable for some models.

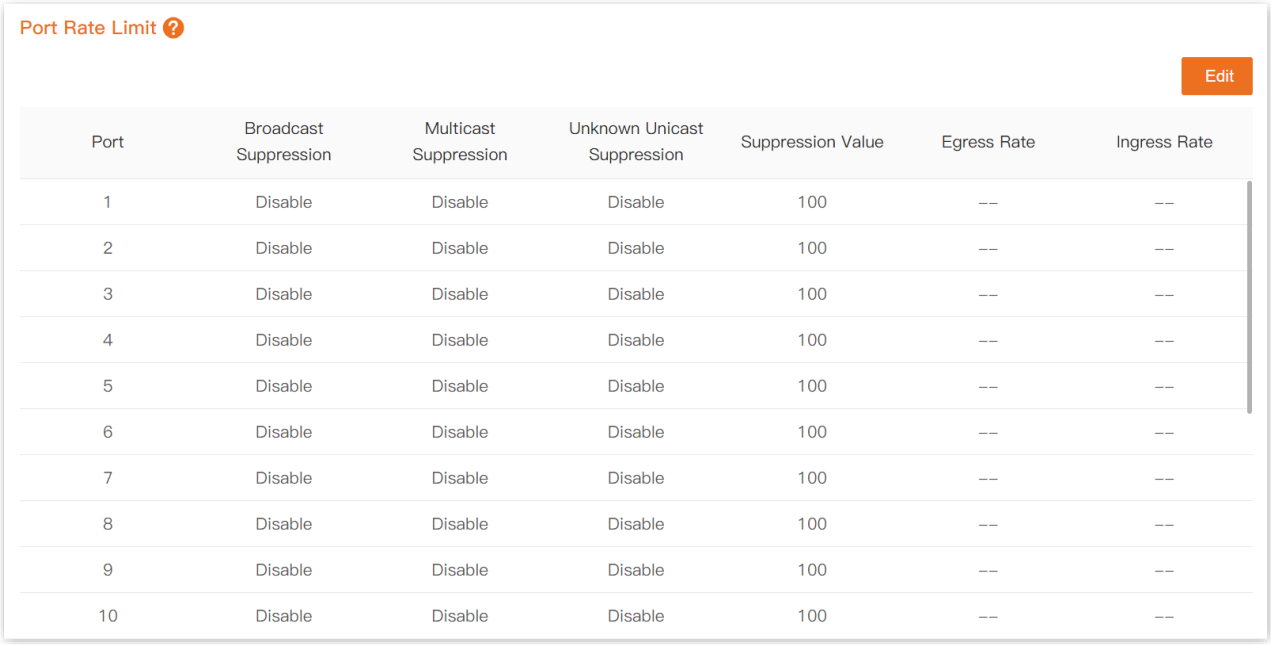
13 QoS

TIP

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and firmware version. Please refer to the actual product.

13.1 Port rate limit

On the **QoS** > **Port Rate Limit** page, you can set the suppression value of each port for receiving broadcast, multicast and unknown unicast packets, and configure the ingress and egress rates of the port.



Parameter description

Name	Description
Port	Specifies the ID of the port.
Broadcast Suppression	Used to enable or disab broadcast suppression. It is disabled by default. **No Change** indicates that the function status remains unchanged.
Multicast Suppression	Used to enable or disable multicast packet suppression. It is disabled by default. **No Change** indicates that the function status remains unchanged.

Name	Description
Unknown Unicast Suppression	Used to enable or disable unknown unicast suppression. It is disabled by default. **No Change** indicates that the function status remains unchanged.
Suppression Value	Used to set the maximum broadcast, multicast or unknown unicast packet allowed to pass through the port per second. When broadcast, multicast or unknown unicast packets exceeds the suppression value, these extra packets will be discarded, thereby reducing the proportion of broadcast, multicast or unknown unicast traffic on the port to a limited range, and ensuring network service. For example, if broadcast suppression and multicast suppression are enabled on a port and the suppression value is set to 100, then the broadcast and multicast packet traffic allowed to pass through the port per second will be 100 Mbps, and the exceeding packets will be discarded.
Egress Rate	Specifies the maximum sending rate of the port. -- indicates no rate limit.
Ingress Rate	Specifies the maximum receiving rate of the port. -- indicates no rate limit.

13.2 QoS policies

13.2.1 Overview

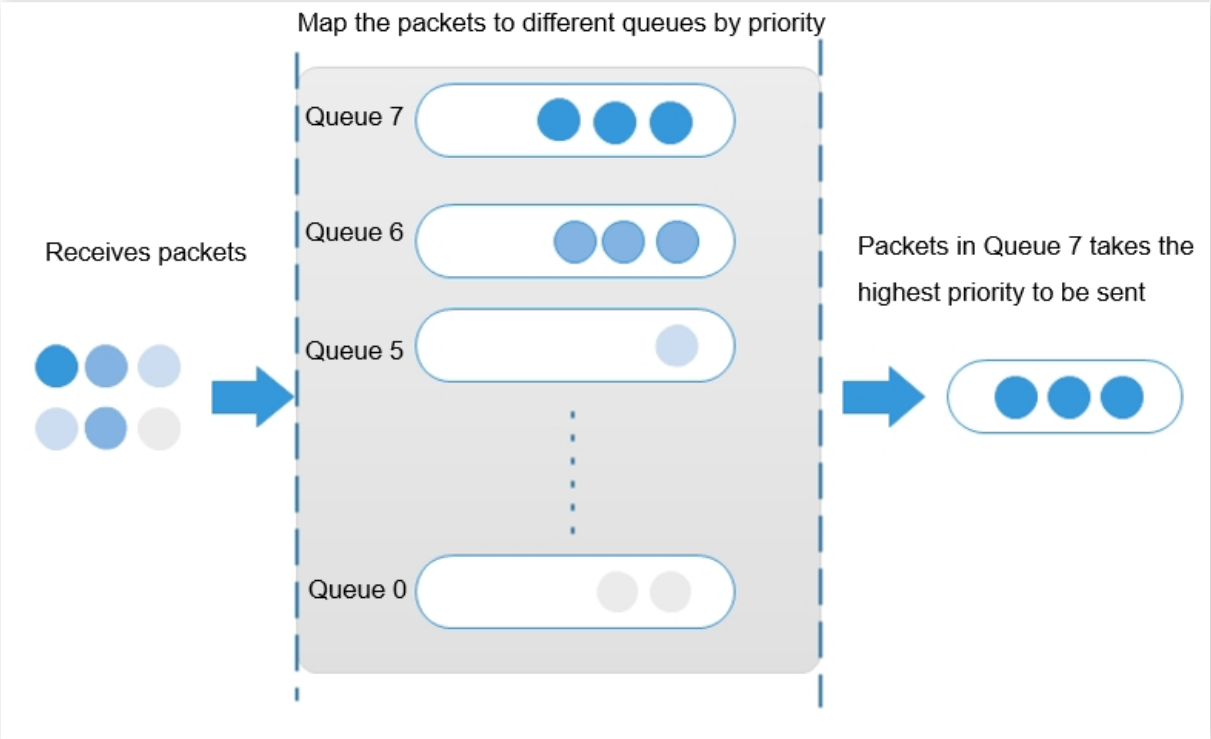
In traditional IP network, packets are treated equally. This network service policy is known as Best-effort, which delivers the packets to their destination with the best effort, with no assurance and guarantee for delivery delay, reliability, and so on. Nowadays, in addition to traditional applications such as www, FTP and E-mail, new services occur, such as video conference, remote education, Video-on-Demand (VoD) and video telephone, which need higher requirements of bandwidth, delay and jitter. Quality of Service (QoS) policy can meet the above demands and improve the quality of service in the network.

This switch classifies the packets based on priority at the ingress stage, then maps them to different queues at the egress stage, and finally forwards these packets by queues based on the scheduling mode, so as to guarantee the quality of network service.

Scheduling mode

Queue scheduling is used to solve the problem of resource preemption by multiple packets when the network is congested. This switch supports three scheduling modes: strict priority, simple weighted priority and weighted priority. Each scheduling mode has eight queues to determine the data forwarding priority.

- **Strict priority**



Strict priority scheduling algorithm is specially designed for critical service applications. An important feature of critical services is that they demand preferential service in congestion in order to reduce the response delay.

In queue scheduling, the packets are sent in queues strictly following the priority order from high to low (Queue 7 > Queue 6 > … > Queue 0). When the queue with higher priority is empty, packets in the queue with lower priority are sent. You can put critical service packets into the queues with higher priority and put non-critical service packets (such as E-mail) into the queues with lower priority. In this way, critical service packets are sent preferentially, and non-critical service packets are sent when the critical service packets are not sent.

But there is a downside to this scheduling algorithm. If there are packets in the queues with higher priority for a long time during congestion, the packets in the queues with lower priority will keep stuck because they are not served.

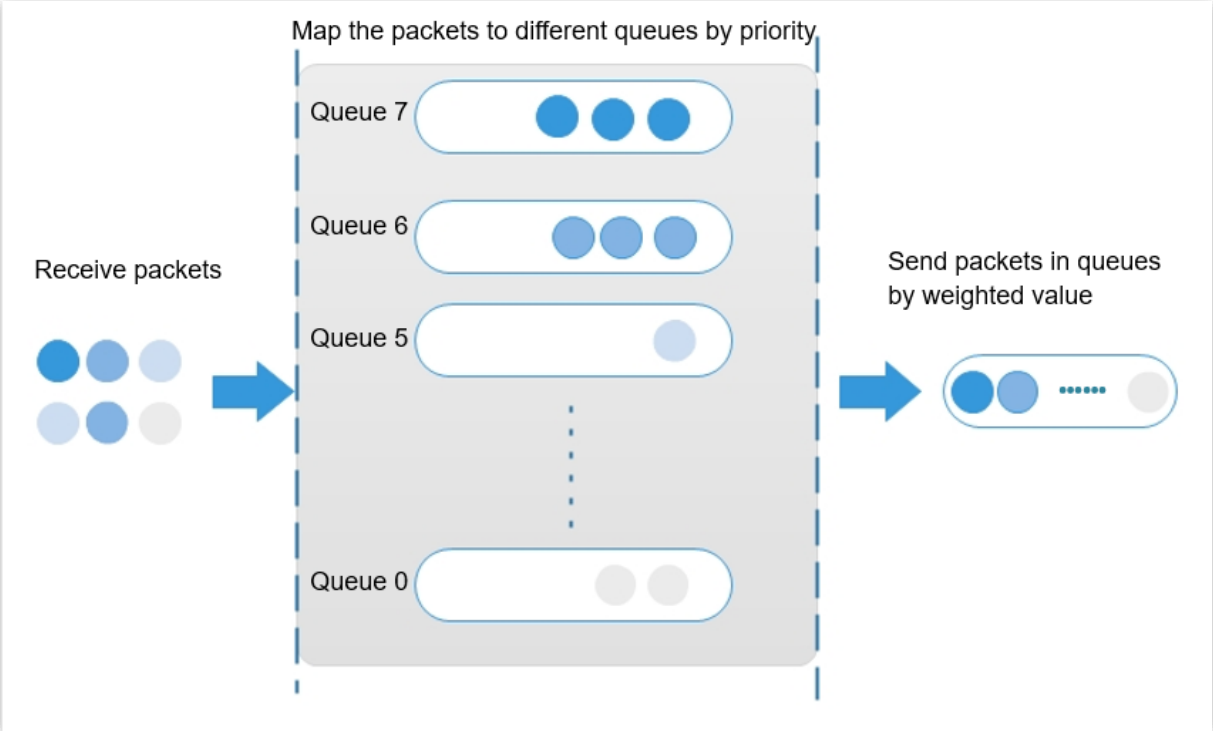
- **Simple weighted priority**

In this mode, there is no priority and all queues equally share the bandwidth.

- **Weighted priority**

This scheduling algorithm schedules all the queues in turn to ensure that every queue can be assigned a certain service time. The weighted value stands for the proportion of assigned resource. Assuming there are eight output queues for a port, and each queue is assigned with a weighted value. For instance, you can configure the eight weighted values of a 100 Mbps port to 25, 20, 15, 15, 10, 5, 5 and 5 respectively. In this way, the queue with the lowest priority can be assured of 5 Mbps of bandwidth at least, thus avoiding the disadvantage of Simple Priority queue-scheduling algorithm that packets in low-priority queues are possibly not to be served for a long time. Another advantage of Weighted Priority queue-scheduling

algorithm is that though the queues are scheduled in turn, the service time for each queue is not fixed, which means if a queue is empty, the next queue will be scheduled immediately. In this way, the bandwidth resources can be fully utilized.

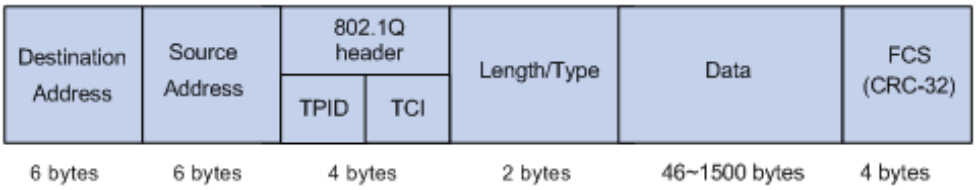


Priority

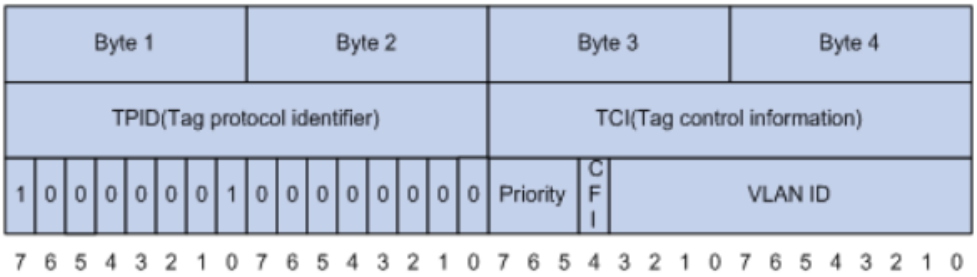
This switch supports three priority modes: 802.1P priority, DSCP priority, and port priority.

- **802.1P priority**

  802.1P priority lies in Layer 2 packet headers and applies to occasions where the Layer 3 packet header does not need analysis but QoS must be assured at Layer 2. 802.1P priority is available only in an 802.1Q tagged packet. As seen below, the 4-byte 802.1Q tag contains a 2-byte Tag Protocol Identifier (TPID, value: 0x8100) and a 2-byte Tag Control Information (TCI).



  The figure below displays a detailed view of an 802.1Q tag. The field **Priority** under TCL is the 802.1P priority, which consists of 3 bits ranging from 0 to 7.

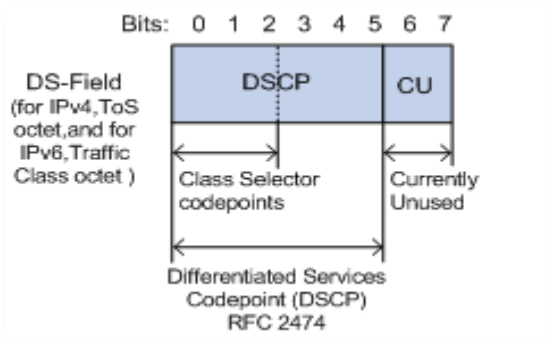


By default, the 802.1P priority, queues, and key words of this switch are mapped as follows.

802.1P priority	Queue	Key word
0	0	best-effort
1	1	background
2	2	spare
3	3	excellent-effort
4	4	controlled-load
5	5	video
6	6	voice
7	7	network-management

- **DSCP priority**

RFC2474 re-defines the Type of Service (ToS) field in the IP message header, which is called the Differentiated Services (DS) field. The first six bits (bits 0 to 5) of the DS field indicate Differentiated Services Codepoint (DSCP) priority ranging from 0 to 63. The last 2 bits (bits 6 and 7) are reserved.



The mapping between the DSCP priority and key words are as follows.

DSCP priority (decimal)	DSCP priority (binary)	Key word
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
18	010010	af21

DSCP priority (decimal)	DSCP priority (binary)	Key word
20	010100	af22
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be (default)

By default, the DSCP priority and queues of this switch are mapped as follows.

DSCP priority	Queue
0 - 7	0
8 - 15	1
16 - 23	2
24 - 31	3
32 - 39	4
40 - 47	5

DSCP priority	Queue
48 - 55	6
56 - 63	7

- **Port priority**

  You can manually configure the Class of Service (CoS) priority of physical ports to map the physical ports with queues. The port maps packets to the corresponding queues based on the configured mapping relationship when the following two situations occur:

  - The packets received by the port do not carry the priority tags trusted by the port. Example: For a port with 802.1P priority mode enabled, the received packets do not carry the 802.1Q tag.
  - The port does not trust the 802.1P priority mode and DSCP priority mode.

  The CoS priority of the ports and queues are mapped as follows.

CoS priority	Queue
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

13.2.2 Configuration wizard

Based on 802.P priority

Step	Task	Description
1	QoS scheduling	**Required.** Select the scheduling mode of the switch based on actual demands.
2	802.1P	**Required.** Configure the mapping relation between 802.1P priority and queues.

Step	Task	Description
3	QoS ports	**Required.** Set the priority mode of corresponding ports to **802.1P Trust** and configure the CoS priority for all ports.

Based on DSCP priority

Step	Task	Description
1	QoS scheduling	**Required.** Select the scheduling mode of the switch based on actual demands.
2	DSCP	**Required.** Configure the mapping relation between DSCP priority and queues.
3	QoS ports	**Required.** Set the priority mode of corresponding ports to **DSCP Trust** and configure the CoS priority for all ports.

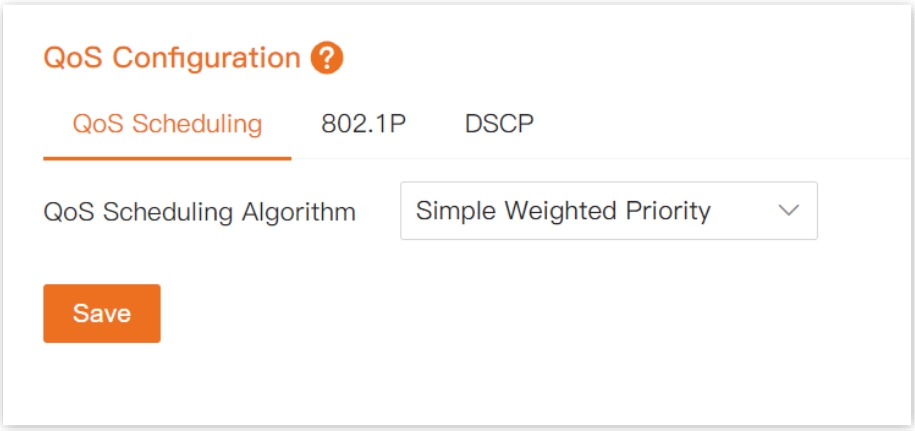
Based on CoS priority

Step	Task	Description
1	QoS scheduling	**Required.** Select the scheduling mode of the switch based on actual demands.
2	QoS ports	**Required.** Set the priority mode of corresponding ports to **No Trust** and configure the CoS priority for all ports.

13.2.3 Configure QoS settings

QoS scheduling

On the **QoS** > **QoS Configuration** > **QoS Scheduling** page, you can configure the QoS scheduling mode.

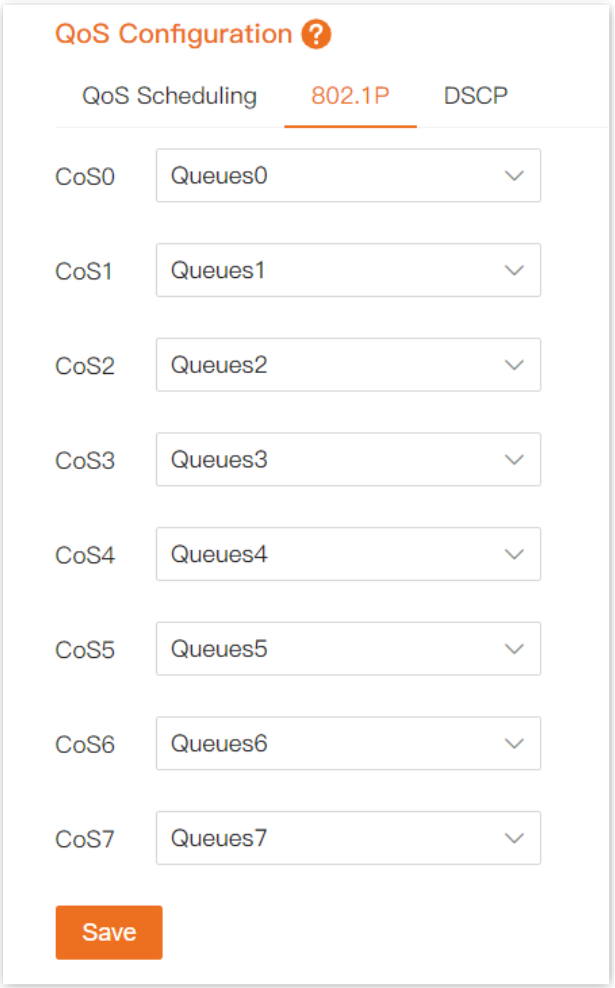


Parameter description

Name	Description
QoS Scheduling Algorithm	Specifies the QoS scheduling algorithm for the port traffic. – **Strict Priority**: The switch forwards the packets strictly based on the priority from high to low. The queue packets with the lower priority are forwarded only when the queue with higher priority is empty. – **Simple Weighted Priority**: 8 queues equally share the bandwidth. – **Weighted Priority**: You need to configure a weighted value for each queue. The weighted value indicates the weight of obtaining resources. If congestion occurs on the port, the bandwidths are assigned based on the weight of each queue.
Queues	If the **QoS Scheduling Algorithm** is set to **Weighted Priority**, you need to configure the weighted value for each queue.

802.1P

On the **QoS** > **QoS Configuration** > **802.1P** page, you can configure the mapping relationship between the 802.1P priority and queues.

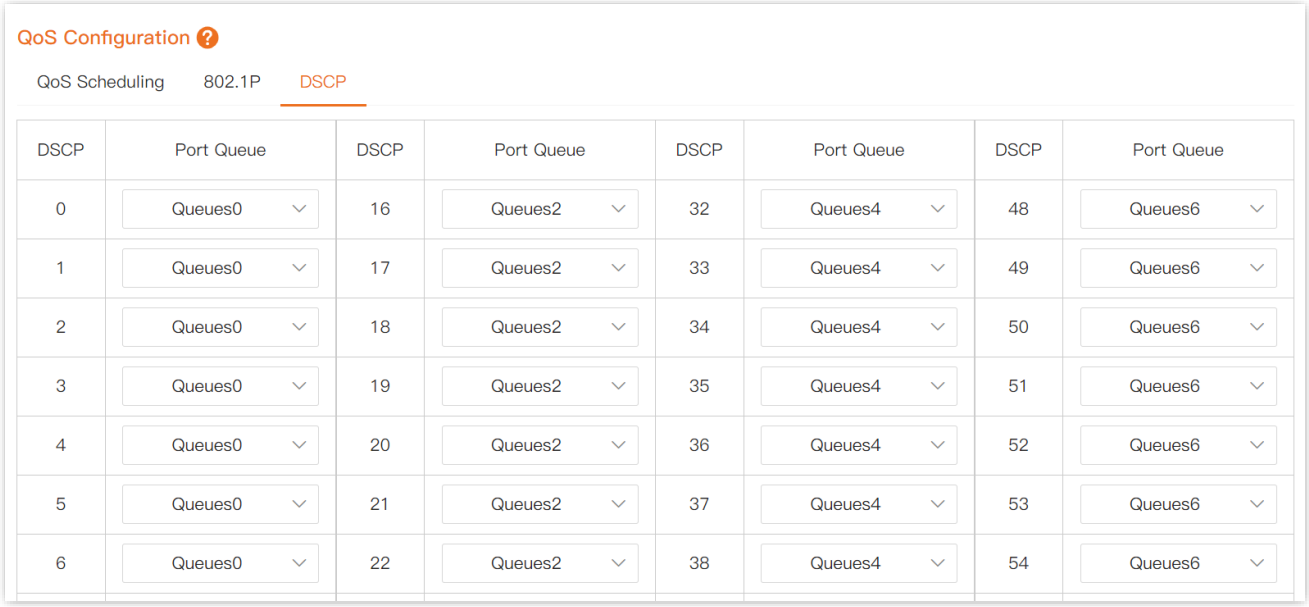


Parameter description

Name	Description
Q0	Specifies the queue in which the VLAN packets' priority is 0.
Q1	Specifies the queue in which the VLAN packets' priority is 1.
Q2	Specifies the queue in which the VLAN packets' priority is 2.
Q3	Specifies the queue in which the VLAN packets' priority is 3.
Q4	Specifies the queue in which the VLAN packets' priority is 4.
Q5	Specifies the queue in which the VLAN packets' priority is 5.
Q6	Specifies the queue in which the VLAN packets' priority is 6.
Q7	Specifies the queue in which the VLAN packets' priority is 7.

DSCP

On the **QoS** > **QoS Configuration** > **DSCP** page, you can configure the mapping relationship between the DSCP priority and queues.

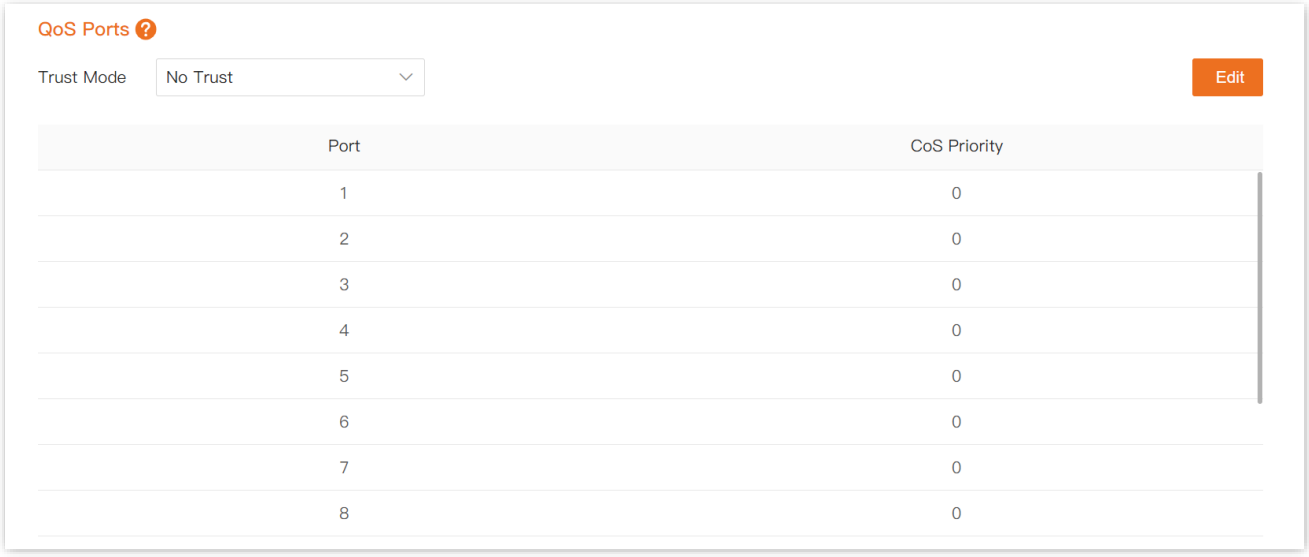


Parameter description

Name	Description
DSCP	Specifies the priority level defined by DS field of the IP packet heads. Range: 0-63.
Port Queue	Specifies the DSCP priority of the queue.

13.2.4 Configure QoS ports

On the **QoS** > **QoS Ports** page, you can configure the priority mode and the CoS priority of each physical port on the switch.



Parameter description

Name	Description
Trust Mode	Specifies the method which the port uses to process the received packets. – **No Trust**: All packets received by the port rejoin queues based on the correspondence of the configured CoS priority. – **802.1P Trust**: When the port receives VLAN packets, the packets rejoin queues based on the correspondence of the 802.1P. When the port receives other packets, the packets rejoin queues based on the correspondence of the CoS priority. – **DSCP Trust**: When the port receives IP packets, the packets rejoin queues based on the correspondence of the DSCP. When the port receives other packets, the packets rejoin queues based on the correspondence of the CoS priority.
Port	Specifies the ID of the port.
CoS Priority	Specifies the CoS priority of the physical ports. When the switch receives packets not in accordance with the trust mode rules or the port is in **No Trust** mode, the packets rejoin queues based on the CoS priority.

14 Manage PoE

TIP

- This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and firmware version. Please refer to the actual product.
- This function is only available for product models with "P". TEG2220P-16-250W is used for illustration.

PoE (Power over Ethernet, also known as remote power supply) means that the device delivers power to powered devices such as IP phones, wireless APs and IP cameras through Ethernet cables.

PoE ports on the switch can automatically detect powered devices and supplies PoE power to the powered devices that comply with the IEEE 802.3af and IEEE 802.3at standards.

By default, the PoE function is enabled on PoE ports.

14.1 View PoE budget and comsumption

To access the page:

Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **PoE Management** and select the **PoE Configuration** tab.

14.2 Enable PoE schedule

TIP

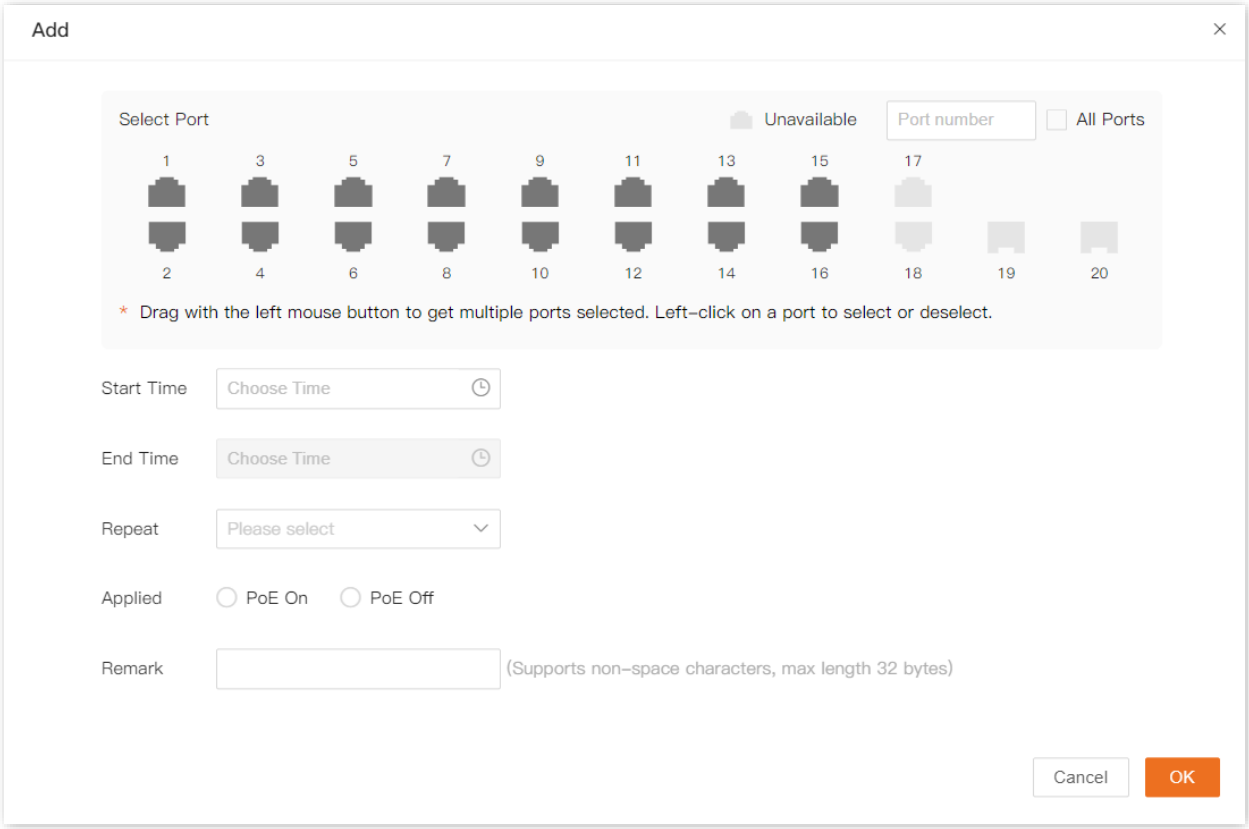
To ensure that this function works properly, connect the switch to the Tenda CloudFi to ensure that the switch system time is correctly synchronized.

Step 3 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 4 Navigate to **PoE Management**, select the **Period Setting** tab, and click **Add** to add PoE schedules.

- **Select Port**: Select ports that you apply the PoE schedule to.
- **Start/End Time**: Select the time period for the PoE schedule to take effect.
- **Repeat**: Select dates for the PoE schedule to repeat.

- **Applied**: Select the PoE schedule to apply.



---End

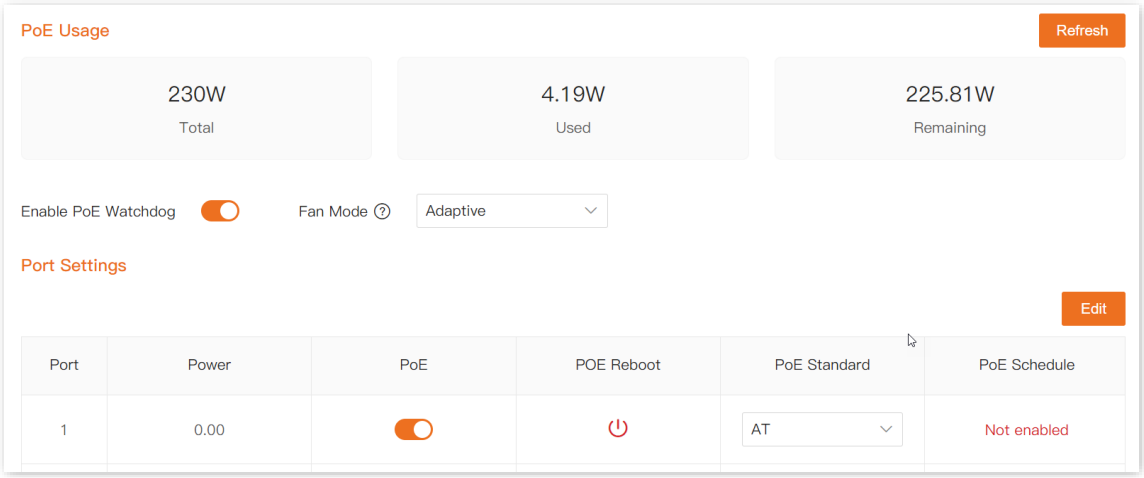
If other ports need to apply this PoE schedule policy, make changes on this page or click **Edit** in **Port Settings** of the **PoE Management** > **Port Configuration** page.

14.3 Change PoE port settings

Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **PoE Management**, and select the **Port Configuration** tab.

Step 3 Click **Edit** to batch change, or change settings of a single port in **Port Settings**. The following figure is for reference only.



---End

Parameter description

Name	Description
Enable PoE Watchdog	When enabled, PoE reboot is performed on th port if no data is transmitted within 5 minutes after the port is connected to a powered device.

14.4 Change fan mode

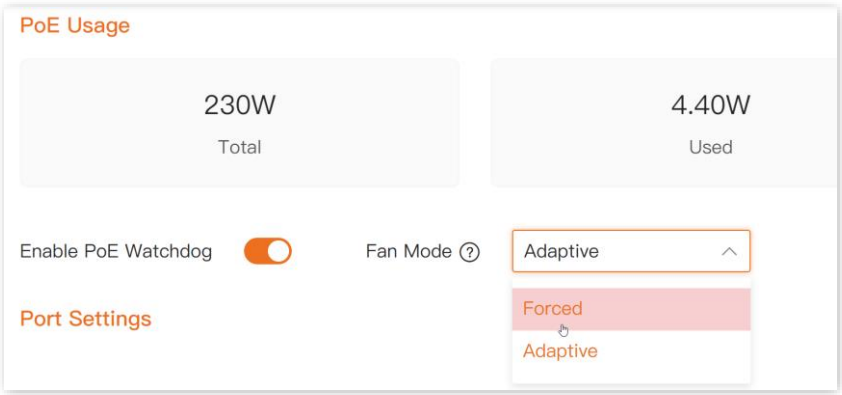
Some high-power PoE switches dissipate heat through built-in fans. Adaptive is the default fan mode. To change the fan mode, take the following steps:

Step 1 On a computer connected to the switch port belonging to the management VLAN, open a browser and enter the switch management IP address in the address bar.

Step 2 Navigate to **PoE Management**, and select the **PoE Configuration** tab.

Step 3 Select the fan mode. The following figure shows an example of setting Forced mode.

- **Adaptive**: When the PoE output exceeds a certain power, the fan automatically runs to dissipate heat from the switch. When the output drops, the fan automatically stops.
- **Forced**: The fan constantly runs to dissipate heat from the switch.



---End

Appendix

Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
CoS	Class of Service
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSCP	Differentiated Services Code Point
ID	Identity Document
IGMP	Internet Group Management Protocol
IP	Internet Protocol
MAC	Medium Access Control
PoE	Power over Ethernet
PVID	Port-base VLAN ID
QoS	Quality of Service
RMON	Remoter Monitoring
RSTP	Rapid Spanning Tree Protocol
SNMP	Simple Network Management Protocol
TCI	Tag Control Information
TCP	Transmission Control Protocol
ToS	Type of ServiceS
TPID	Tag Protocol Identifier

Acronym or Abbreviation	Full Spelling
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network