

H3C S1600V2 Switch Series Web Configuration Guide

New H3C Technologies Co., Ltd.
<http://www.h3c.com>

Software version: Release 8806 and later
Document version: 6W100-20240307

Copyright © 2024, New H3C Technologies Co., Ltd. and its licensors

All rights reserved

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of New H3C Technologies Co., Ltd.

Trademarks

Except for the trademarks of New H3C Technologies Co., Ltd., any trademarks that may be mentioned in this document are the property of their respective owners.

Notice

The information in this document is subject to change without notice. All contents in this document, including statements, information, and recommendations, are believed to be accurate, but they are presented without warranty of any kind, express or implied. H3C shall not be liable for technical or editorial errors or omissions contained herein.

Preface

This configuration guide describes the software features available on the Web interface. It guides you through the feature configuration procedures and provides configuration examples to help you apply the software features to different network scenarios.

This preface includes the following topics about the documentation:

- [Audience](#).
- [Conventions](#).
- [Documentation feedback](#).

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators working with the S6805, S6850, or S9850 switch series.

Conventions

The following information describes the conventions used in the documentation.

Command conventions





Convention	Description
Boldface	Bold text represents commands and keywords that you enter literally as shown.
<i>Italic</i>	<i>Italic</i> text represents arguments that you replace with actual values.
[]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x y ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x y ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x y ... }*	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x y ...]*	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions













Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the New User window opens; click OK .
>	Multi-level menus are separated by angle brackets. For example, File > Create >

Convention	Description
	Folder.

Symbols

Convention	Description
 WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
 CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
 IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
 TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

Logging in to the device	1
Using the web interface	2
Overview	2
Webpage layout	2
Top-level menu items and features.....	3
Home.....	3
System menu	3
Monitoring menu	3
Switch Settings menu.....	4
VLAN Settings menu.....	4
QoS Settings.....	5
Home.....	6
Overview	6
Port Statistics	6
System	7
IP Settings.....	7
Configuring IP settings	7
Configuring DNS settings.....	8
Account.....	8
System Restart.....	8
System Upgrade	9
Restore to Factory.....	10
Monitoring.....	12
Port Statistics	12
Cable Detection.....	12
Overview	12
Restrictions and guidelines	12
Procedure.....	13
Loop Prevention	13
Overview	13
Procedure.....	14
Configuration examples	16
Example: Configuring basic loop detection functions.....	16
Switch Settings	19
Port Settings.....	19
Overview	19
Configuring port settings	19
Port Info.....	20
Port Mirroring	20
Overview	20
Concepts.....	20
Configuring port mirroring	21
Displaying and clearing port mirroring information.....	21
Port Isolation	21
Overview	21
Configuring port isolation settings	21
Displaying port isolation information	22
Static MAC	22
Overview	22
Configuring static MAC address settings	23
Displaying static MAC addresses.....	24
Filtering MAC addresses.....	24

MAC List.....	25
DHCP Snooping.....	26
Overview	26
DHCP snooping benefits.....	26
Configuring DHCP snooping.....	26
Displaying DHCP snooping information	28
PoE Settings	28
Overview	28
Procedure.....	29
Configuration examples	30
Example: Configuring port mirroring	30
Example: Configuring port isolation	32
MAC address configuration example	34
Example: Enabling DHCP snooping globally	36
VLAN Settings	38
Overview	38
VLAN features.....	38
Overview	38
Procedure.....	38
VLAN Members.....	38
Creating VLANs	38
Deleting VLANs.....	39
VLAN Settings.....	39
Overview	39
Configuring port VLAN settings.....	40
Displaying port VLAN information	41
Configuration example	42
Network configuration	42
Procedure.....	42
QoS Settings	46
Port Rate Limit	46
Overview	46
Configuring port bandwidth settings.....	46
Displaying port bandwidth information	46
Storm Control.....	47
Overview	47
Configuring storm control	47
Displaying storm control information	47
Troubleshooting	48
A fiber port fails to come up	48
Symptom	48
Troubleshooting flowchart.....	48
Solution	48
A copper port fails to come up	49
Symptom	49
Troubleshooting flowchart.....	50
Solution	50
PoE power supply anomaly.....	51
Symptom	51
Troubleshooting flowchart.....	51
Solution	51
Error packets on a port.....	52
Symptom	52
Troubleshooting flowchart.....	52
Solution	52

Logging in to the device

NOTE:

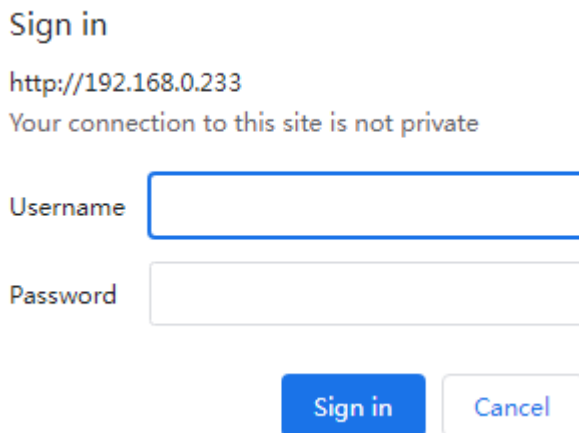
As a best practice, use the following Web browsers:

- Google Chrome 109.0.5414.120 or higher.
- Mozilla Firefox 110.0 or higher.
- Microsoft Edge 89.0.774.68 or higher.

Internet Explorer Web browsers are not supported in the current software version.

1. Connect the PC to the LAN port on the device.
2. Assign an IP address in the 192.168.0.233/24 network for the PC.
3. Check whether the PC is enabled with the proxy service. If the PC uses a proxy server to access the Internet, disable the proxy service.
4. Open the browser, enter <http://192.168.0.233> in the address bar, and then press Enter. 192.168.0.233 is the default management IP address of the device, and you can edit the address after login.
5. On the login page, enter the default username (**admin**) and password (**admin**), and then click **Log In**. As a best practice, change the login password immediately after the first successful login for security purposes. For configuration procedures, see "[Account](#)."

Figure 1 Web login page



Sign in

http://192.168.0.233

Your connection to this site is not private


Username

Password

Using the web interface

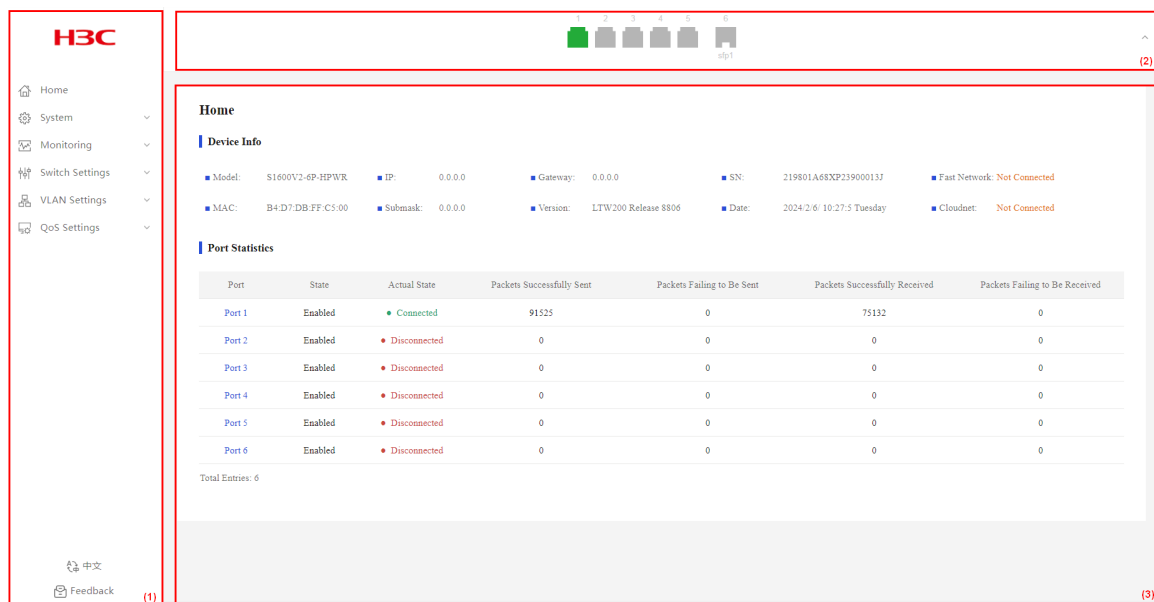
Overview

The top-level menus on the webpage navigation pane include **Home**, **System**, **Monitoring**, **Switch Settings**, **VLAN Settings**, and **QoS Settings**. Clicking on a top-level menu expands its submenu, displaying the feature names. Clicking on a feature name opens the webpage for configuring that feature.

Clicking the  **Feedback** icon on the bottom of the navigation pane opens the feedback page. The feedback page is an important channel for communication with users, and we highly appreciate your opinions. You can fill out the form with your functional suggestions, views on the product interface, discovered bugs, and requirements for new features. We will read every piece of feedback carefully and continuously optimize our product based on your opinions. Thank you for your support and understanding.

Webpage layout

Figure 2 Webpage layout






1) Navigation pane

2) Port state pane









3) Content pane

As shown in the figure above, the webpage has the following functional areas:

- **Navigation pane**—Provides the Web menu for device functions in a tree structure. You can easily select function menus in the navigation pane. The content pane displays the selection result. You can click the H3C logo on the top of the navigation pane to access the H3C official website, and click the feedback icon  **Feedback** on the bottom of the navigation pane to open the feedback page.
- **Port state pane**—Displays port quantity and port state information.
 - Click the  or  icon on the right of the port state pane to hide or display the port state pane.

- When the port state pane is displayed, the pane displays the port quantity and port physical state, and the information is refreshed every 10 seconds.
- [Table 1](#) provides the port state description.
- **Content pane**—Allows users to perform configuration tasks, and view information and the operation result.

Table 1 Port state description

Port type	Icon	Description
Copper port		The port is disconnected.
		The port is connected.
		A loop was detected on the port, and loop protection was triggered.
		A loop was detected on the port.
Fiber port		The port is disconnected.
		The port is connected.
		A loop was detected on the port, and loop protection was triggered.
		A loop was detected on the port.

Top-level menu items and features

Home

The homepage displays basic device information and port information.

System menu

Use [Table 2](#) to navigate to the tasks you can perform from the **System** menu.

Table 2 System menu navigator

Menus	Tasks
IP Settings	Configure device management IP.
Account	Manage account and password.
System Restart	Reboot the device
System Upgrade	Update system software.
Restore to Factory	Restore factory default settings.

Monitoring menu

Use [Table 3](#) to navigate to the tasks you can perform from the **Monitoring** menu.

Table 3 Monitoring menu navigator

Menus	Tasks
Port Statistics	Display port statistics information.
Cable Detection	Perform cable diagnosis and analysis.
Loop Prevention	<ul style="list-style-type: none">• Loop protection• Loop detection

Switch Settings menu

Use [Table 4](#) to navigate to the tasks you can perform from the **Switch Settings** menu.

Table 4 Switch Settings menu navigator

Menus	Tasks
Port Settings	<ul style="list-style-type: none">• Edit port state.• Configure port rate and duplex mode.• Configure traffic control.• Display port information.
Port Mirroring	<ul style="list-style-type: none">• Enable/disable port mirroring.• Configure source and destination ports.• Display port mirroring information.
Port Isolation	<ul style="list-style-type: none">• Enable/disable port isolation.• Display port isolation information.
Static MAC	<ul style="list-style-type: none">• Add and delete static MAC address entries.• Configure source MAC blocking.• Display MAC address information.
MAC Search	Filter MAC address entries.
MAC List	<ul style="list-style-type: none">• Display existing MAC address entries.• Clear dynamic MAC address entries.
DHCP Snooping	<ul style="list-style-type: none">• Enable/disable DHCP snooping.• Configure trusted and untrusted ports.• Display DHCP snooping information.
PoE Settings	<ul style="list-style-type: none">• Enable/disable PoE for interfaces.• Display PoE information.

VLAN Settings menu

Use [Table 5](#) to navigate to the tasks you can perform from the **VLAN Settings** menu.

Table 5 VLAN Settings menu navigator

Menus	Tasks
VLAN Members	<ul style="list-style-type: none">• Enable/disable VLAN.• Create and delete VLANs.• Display static VLAN information.
VLAN Settings	<ul style="list-style-type: none">• Enable/disable VLAN.

Menus	Tasks
	<ul style="list-style-type: none"> • Divide VLANs based on ports. • Display port VLAN information.

QoS Settings

Use [Table 6](#) to navigate to the tasks you can perform from the **QoS Settings** menu.

Table 6 QoS Settings menu navigator

Menus	Tasks
Port Rate Limit	<ul style="list-style-type: none"> • Enable/disable port rate limiting. • Display port bandwidth information.
Storm Control	<ul style="list-style-type: none"> • Enable/disable storm control. • Display storm control information.

Home

Overview

The homepage displays device information and port information.

Port Statistics

1. From the navigation pane, select **Home**.
2. In the port statistics area, you can view port statistics information, including port physical state, packets sent successfully, and packets failed to be sent.

Figure 3 Homepage

The screenshot displays the H3C device homepage. On the left is a navigation pane with the H3C logo and menu items: Home, System, Monitoring, Switch Settings, VLAN Settings, and QoS Settings. The main content area is titled 'Home' and contains two sections: 'Device Info' and 'Port Statistics'. The 'Device Info' section lists various system parameters. The 'Port Statistics' section features a table with columns for Port, State, Actual State, Packets Successfully Sent, Packets Failing to Be Sent, Packets Successfully Received, and Packets Failing to Be Received. The table shows that Port 1 is connected, while Ports 2 through 6 are disconnected. At the bottom of the page, there are links for '中文' (Chinese) and 'Feedback'.

Port	State	Actual State	Packets Successfully Sent	Packets Failing to Be Sent	Packets Successfully Received	Packets Failing to Be Received
Port 1	Enabled	Connected	91525	0	75132	0
Port 2	Enabled	Disconnected	0	0	0	0
Port 3	Enabled	Disconnected	0	0	0	0
Port 4	Enabled	Disconnected	0	0	0	0
Port 5	Enabled	Disconnected	0	0	0	0
Port 6	Enabled	Disconnected	0	0	0	0

System

IP Settings

Configuring IP settings

1. From the navigation pane, select **System > IP Settings**.
2. Configure the DHCP enabling state.
By default, DHCP is enabled.
3. Select the management VLAN.
4. Enter the management IP address, subnet mask, and gateway address.
5. Click **Submit**.
6. In the dialog box that opens, click **OK**.

Figure 4 IP settings page

The screenshot shows the H3C IP Settings page. On the left is a navigation pane with 'IP Settings' selected. The main area contains two sections: 'IP Settings' and 'DNS Settings'. The 'IP Settings' section has fields for DHCP (set to 'Enable'), Management VLAN (set to '1'), IP Address (0.0.0.0), Subnet Mask (0.0.0.0), and Gateway Address (0.0.0.0). Each field has a 'Submit' button below it. The 'DNS Settings' section has a field for DNS Address (0.8.8.8) with a 'Submit' button below it. The top right of the page shows a status bar with six indicators, the first of which is green and labeled 'stp1'.

Figure 5 Confirming operation

192.168.0.233 says

Changing the IP address will cause disconnection. Continue anyway?

OK Cancel

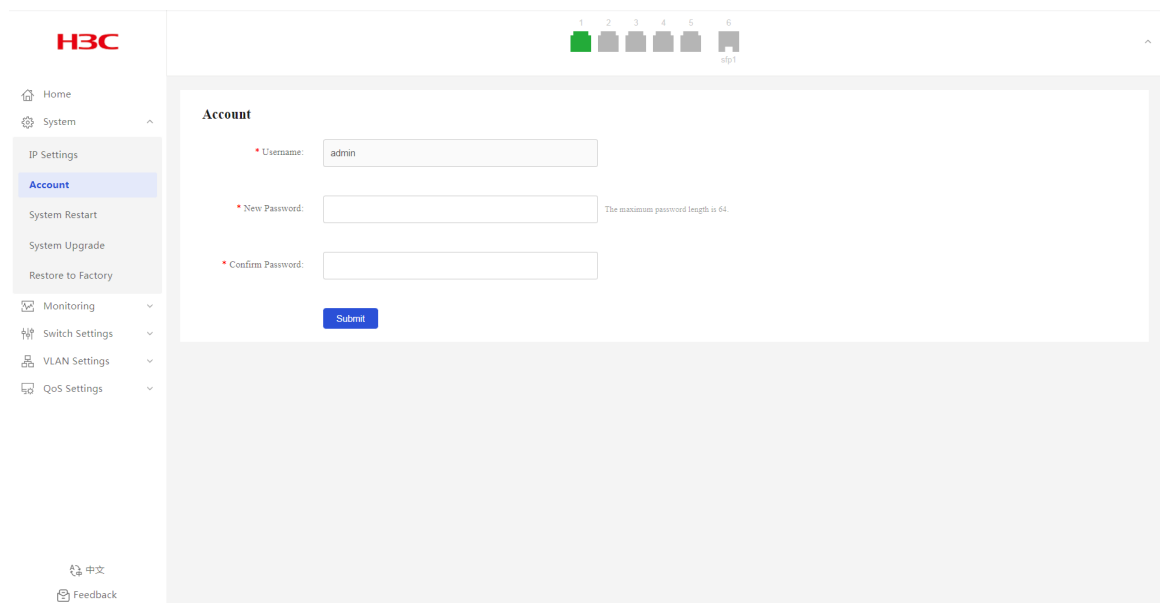
Configuring DNS settings

1. From the navigation pane, select **System > IP Settings**.
2. Enter the DNS address.
3. Click **Submit**.

Account

1. From the navigation pane, select **System > Account**.
2. In the **New Password** field, enter a new password.
The default password is **admin**.
3. Enter the new password again in the **Confirm Password** field.
4. Click **Submit**.

Figure 6 Configuring account information



The screenshot shows the H3C web management interface. On the left is a navigation pane with the following menu items: Home, System (expanded), IP Settings, Account (highlighted), System Restart, System Upgrade, Restore to Factory, Monitoring, Switch Settings, VLAN Settings, and QoS Settings. At the bottom of the navigation pane are links for 中文 and Feedback. The main content area is titled 'Account' and contains three input fields with red asterisks indicating required fields: 'Username' (containing 'admin'), 'New Password', and 'Confirm Password'. A blue 'Submit' button is located below the 'Confirm Password' field. A note next to the 'New Password' field states 'The maximum password length is 64'. At the top right of the interface, there are six status indicators labeled 1 through 6, with indicator 1 being green and the others grey.

System Restart

1. From the navigation pane, select **System > System Restart**.
2. Click **Restart**. Refresh the webpage later to re-enter the system.

Figure 7 System restart page

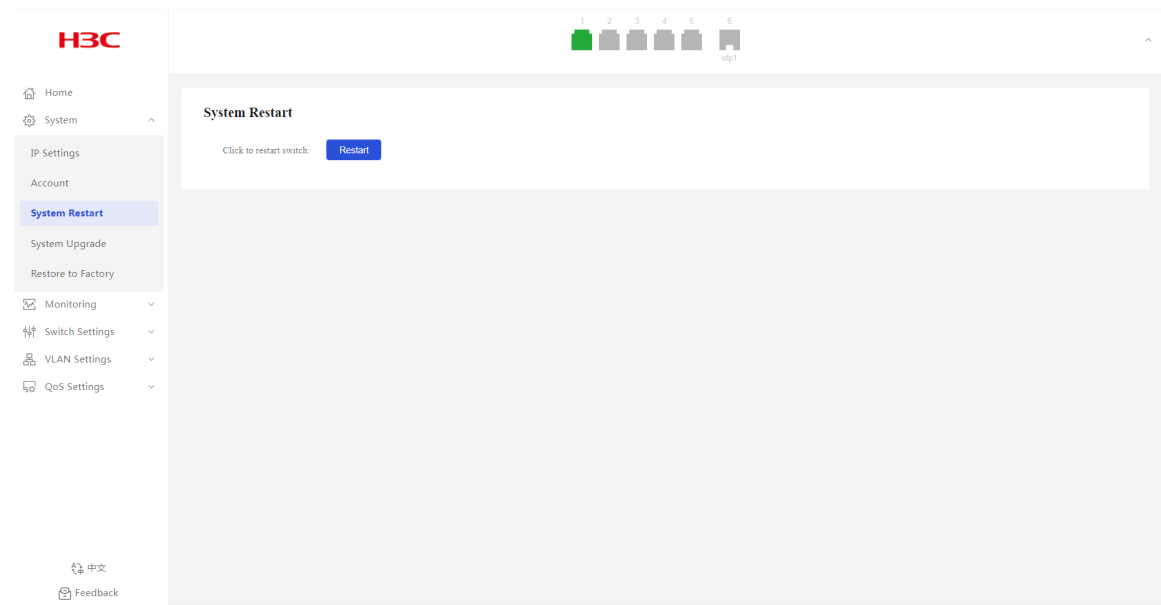
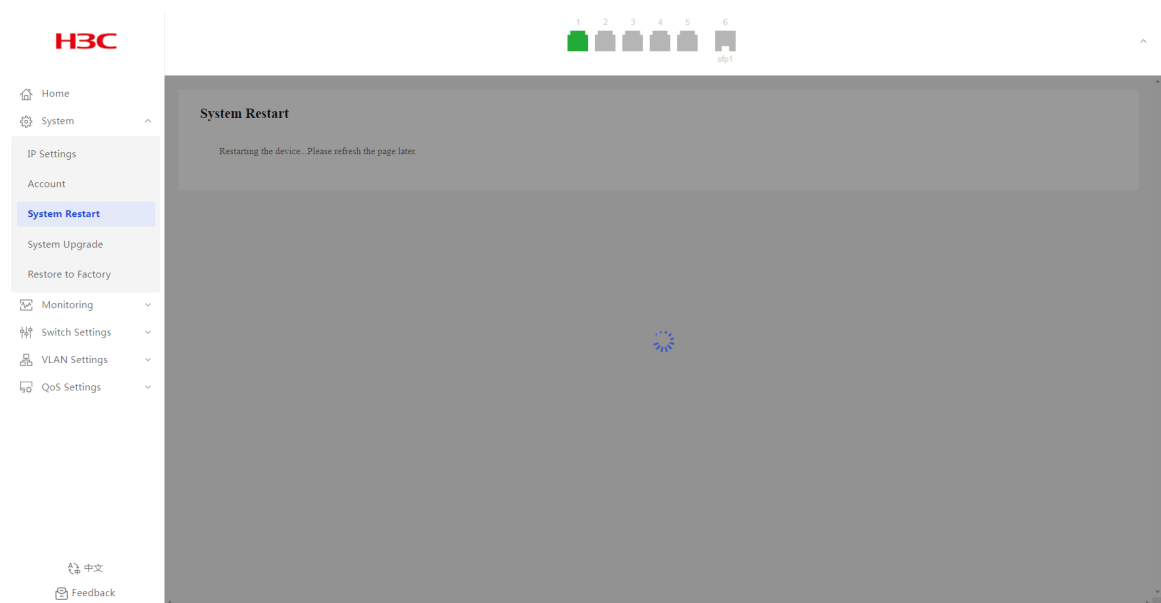


Figure 8 Prompt page



System Upgrade

1. From the navigation pane, select **System > System Upgrade**.
2. Click **Select File**, and then select the target local file.
3. Click **Upgrade**.
4. In the dialog box that opens, click **OK**. Refresh the webpage after the file is uploaded successfully to re-enter the system.

Figure 9 System upgrade page

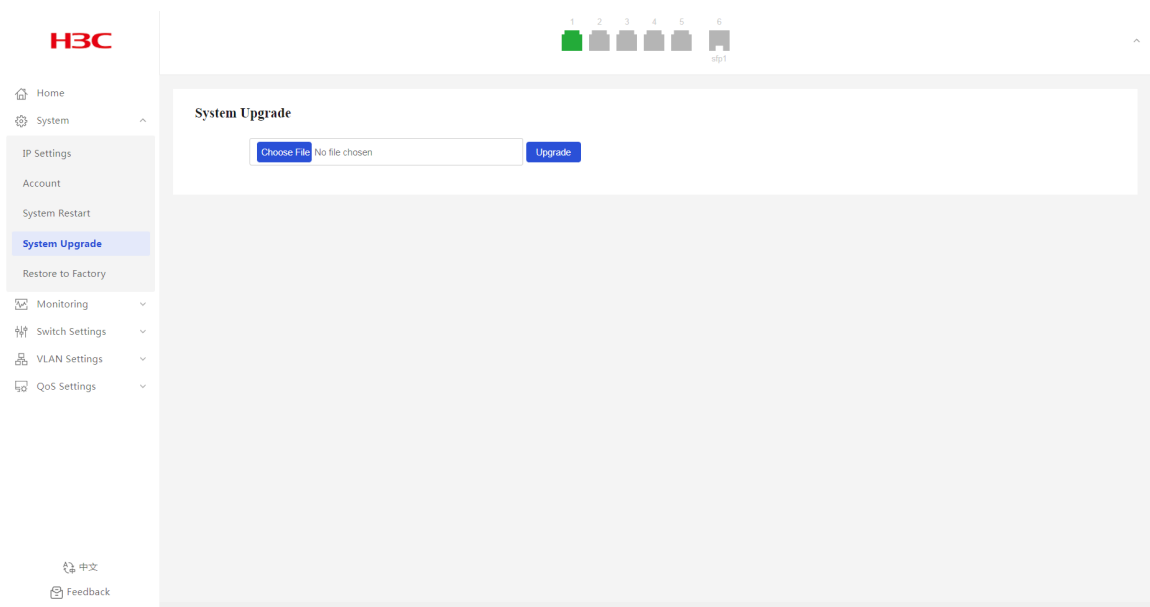


Figure 10 Confirming operation

192.168.0.233 says

It must restart your device for the upgrade to take effect. Continue anyway?



Restore to Factory

1. From the navigation pane, select **System > Restore to Factory**.
2. Click **Restore to Factory**. Wait for the restoration to complete.

Figure 11 Restoring factory default settings

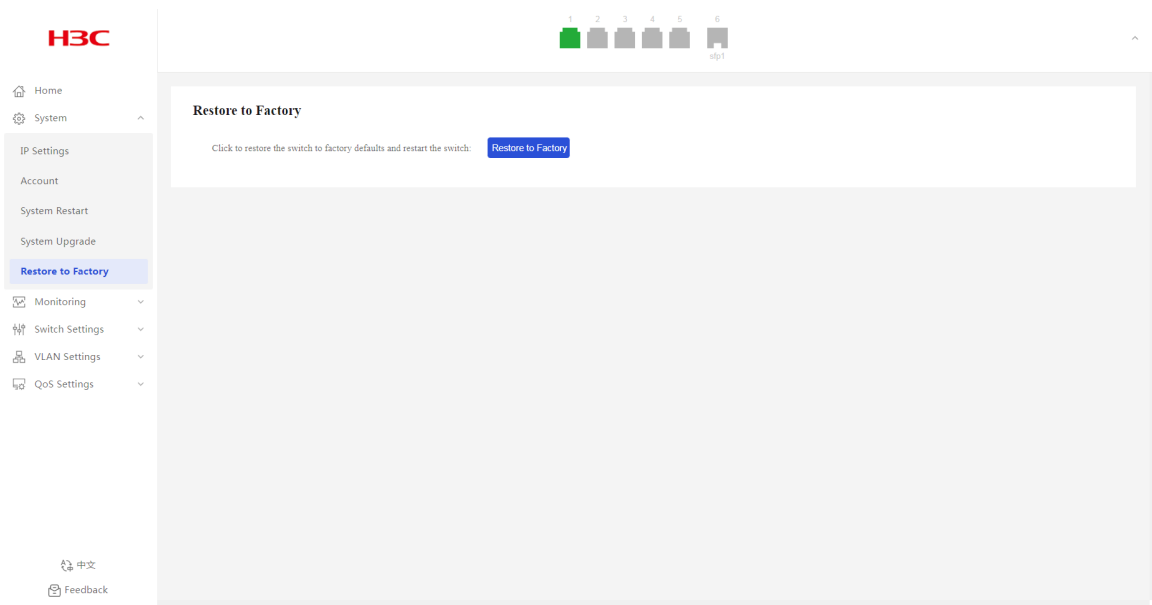
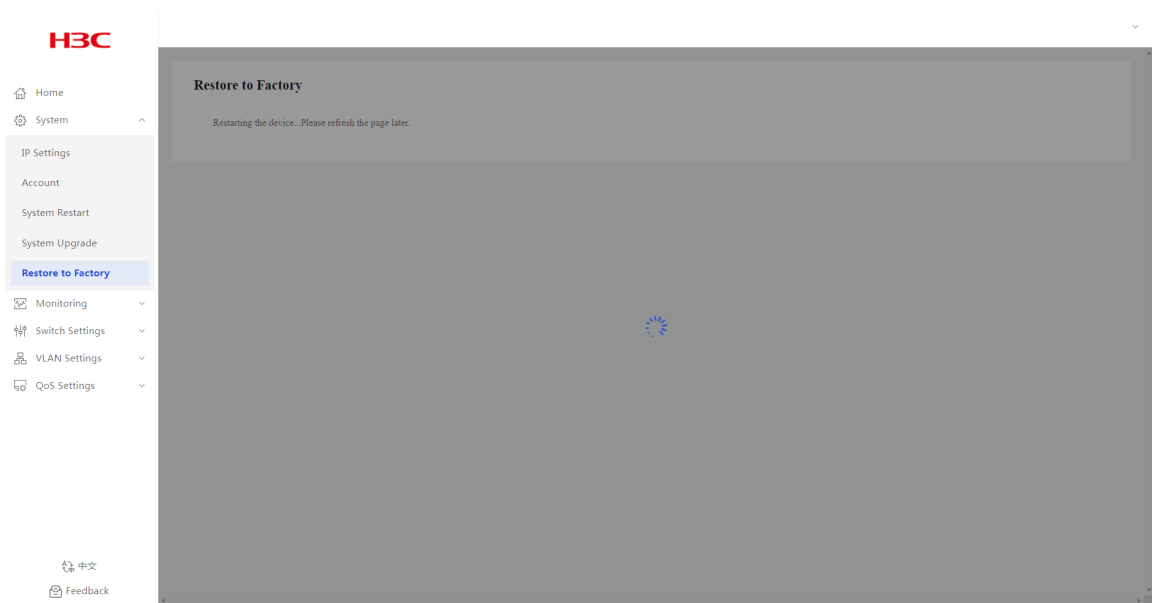


Figure 12 Prompt page

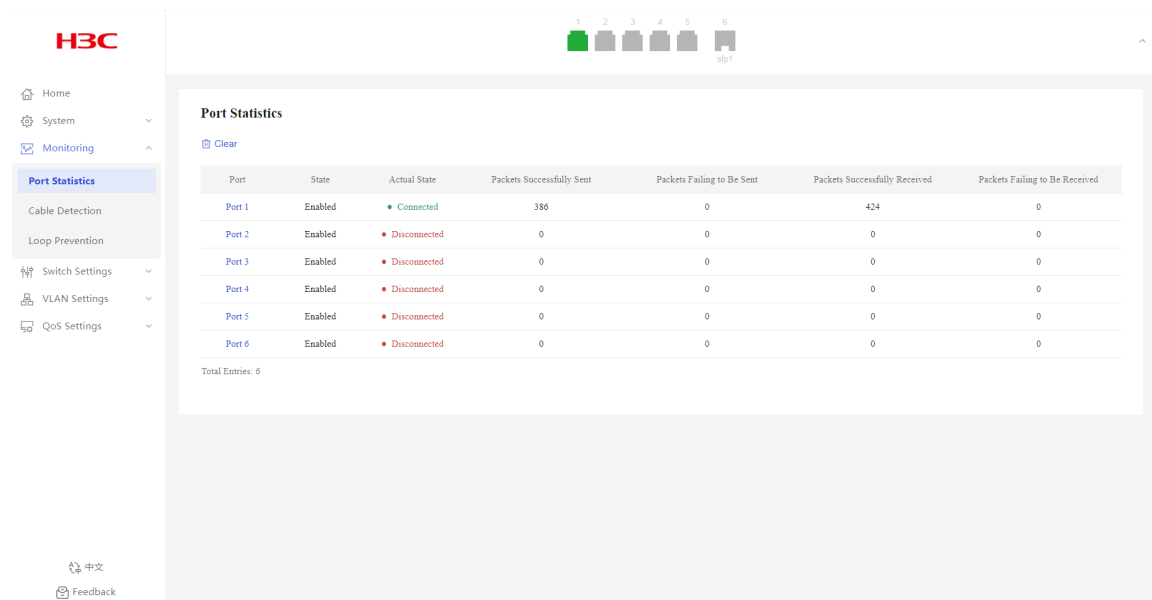


Monitoring

Port Statistics

1. From the navigation pane, select **Monitoring > Port Statistics**.
2. You can view port statistics information, including port physical state, packets sent successfully, and packets failed to be sent.

Figure 13 Port statistics page



Cable Detection

Overview

Table 7 Cable detection results

Detection result	Description
Error	Failed to obtain data.
Short Circuit	Verify whether a loop exists or change the cable.
Disconnected	Verify whether a loop exists or change the cable.
Mismatch	Verify whether a loop exists or change the cable.
Connected	The cable is in good condition.

Restrictions and guidelines

Administratively shut down ports do not support cable detection.

Procedure


1. From the navigation pane, select **Monitoring > Cable Detection**.
2. Select the target ports.
3. Click the detect icon  .

Figure 14 Cable detection page

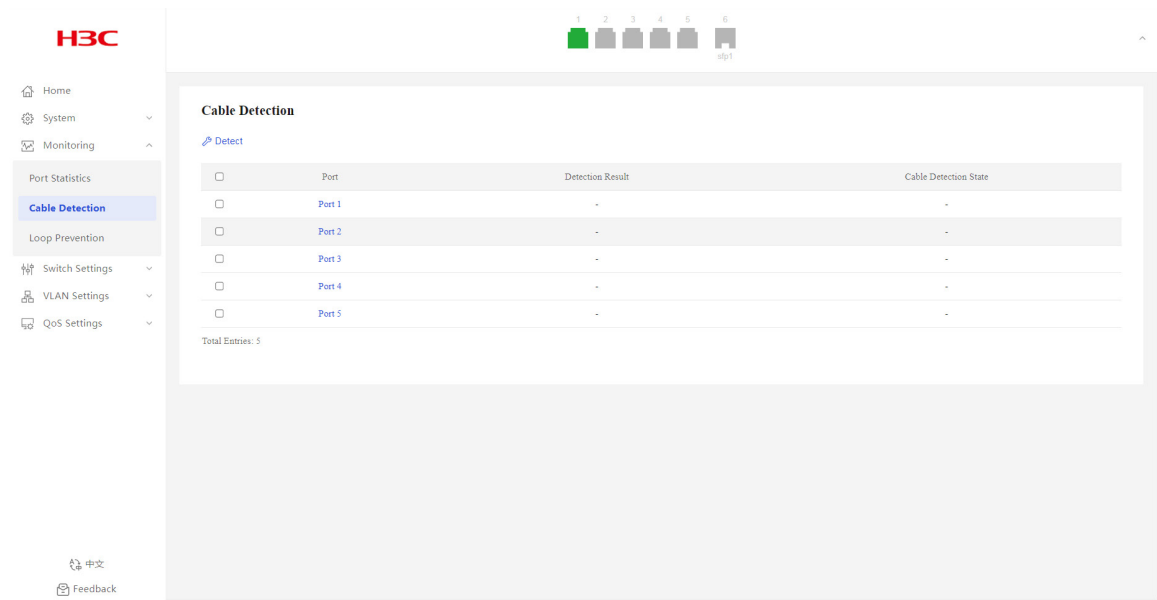


Figure 15 Cable detection results

<input type="checkbox"/>	Port	Detection Result	Cable Detection State
<input type="checkbox"/>	Port 1	-	-
<input checked="" type="checkbox"/>	Port 2	Disconnected	Please check the cable for loops or replace the network
<input type="checkbox"/>	Port 3	-	-
<input type="checkbox"/>	Port 4	-	-
<input type="checkbox"/>	Port 5	-	-

Total Entries: 5

Loop Prevention

Overview

Background

The loop detection mechanism performs periodic checks for Layer 2 loops. The mechanism immediately generates a log message when a loop occurs so that you are promptly notified to adjust network connections and configurations.

- **Loop detection**—When the system detects a loop on a port, it does not take any actions on the port, but it will display a red icon for the port on the port state pane.

- **Loop protection**—When the system detects a loop on a port, it automatically blocks that port to avoid packet flooding. The system also displays the port as blocked in the Port Loop Info list and the port state pane (yellow icon).

Loop prevention interval

Loop detection is a continuous process as the network changes. Loop detection frames are sent at the loop detection intervals to determine whether loops occur on ports and whether loops are removed.

Port state auto recovery

When the device detects a loop on a port and does not receive any loop detection packets within the recovery interval, it assumes that the loop has been eliminated. The port is then automatically restored to normal forwarding state. This process is the automatic port state recovery process.

Procedure

Configure Loop Prevention

1. From the navigation pane, select **Monitoring > Loop Prevention**.
2. To configure loop protection:
 - Select **Loop Protection** from the **Loop Feature** list.
 - Configure the detection interval. The default interval is two seconds.
 - Configure the recovery interval. The default interval is 10 seconds.
3. To configure loop detection:
 - Select **Loop Detection** from the **Loop Feature** list.
 - Configure the detection interval. The default interval is two seconds.
 - Configure the recovery interval. The default interval is 10 seconds.
4. Click **Submit**.

Displaying port loop information

After enabling loop prevention, you can view the port state information:

- As shown in [Figure 17](#), port 3 is blocked because a loop is detected on it.
- As shown in [Figure 18](#), port 2 and port 3 are displayed with a red icon on the port state pane because a loop is detected.

Figure 16 Loop prevention page

H3C

Home
System
Monitoring
Port Statistics
Cable Detection
Loop Prevention
Switch Settings
VLAN Settings
QoS Settings

中文
Feedback

1 2 3 4 5 6
sfp1

Loop Prevention

Loop Prevention Settings

* Loop Feature: Loop Protection

* Detection Interval: 2 Range: 1 to 32767 (in seconds)

* Recovery Interval: 10 Range: 0 or 4 to 1000000 (in seconds)

Submit

Port Loop Info

Port	Loop Settings	Loop State
Port 1	Enabled	Normal
Port 2	Enabled	Normal
Port 3	Enabled	Normal
Port 4	Enabled	Normal
Port 5	Enabled	Normal
Port 6	Enabled	Normal

Total Entries: 6

Figure 17 Loop protection

H3C

Home
System
Monitoring
Port Statistics
Cable Detection
Loop Prevention
Switch Settings
VLAN Settings
QoS Settings

中文
Feedback

1 2 3 4 5 6
sfp1

Loop Prevention

Loop Prevention Settings

* Loop Feature: Loop Protection

* Detection Interval: 2 Range: 1 to 32767 (in seconds)

* Recovery Interval: 10 Range: 0 or 4 to 1000000 (in seconds)

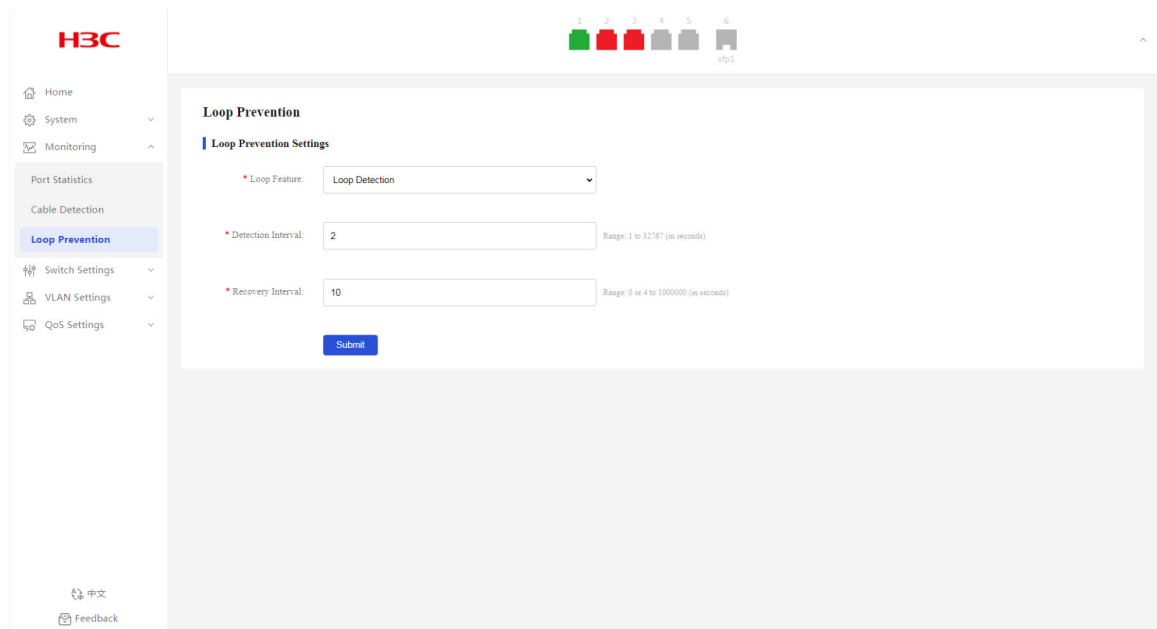
Submit

Port Loop Info

Port	Loop Settings	Loop State
Port 1	Enabled	Normal
Port 2	Enabled	Normal
Port 3	Enabled	Blocked
Port 4	Enabled	Normal
Port 5	Enabled	Normal
Port 6	Enabled	Normal

Total Entries: 6

Figure 18 Loop detection



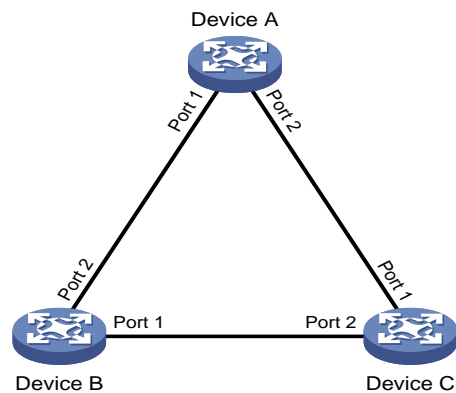
Configuration examples

Example: Configuring basic loop detection functions

Network configuration

As shown in Figure 19, configure loop detection on Device A to automatically shut down the interface on which a loop is detected.

Figure 19 Network diagram



Procedure

1. From the navigation pane, select **Monitoring > Loop Prevention**.
2. Select **Loop Protection** from the **Loop Feature** list.
3. Set the detection interval to 100 milliseconds.
4. Set the recovery interval to 10000 milliseconds.
5. Click Submit.

Figure 20 Loop prevention page

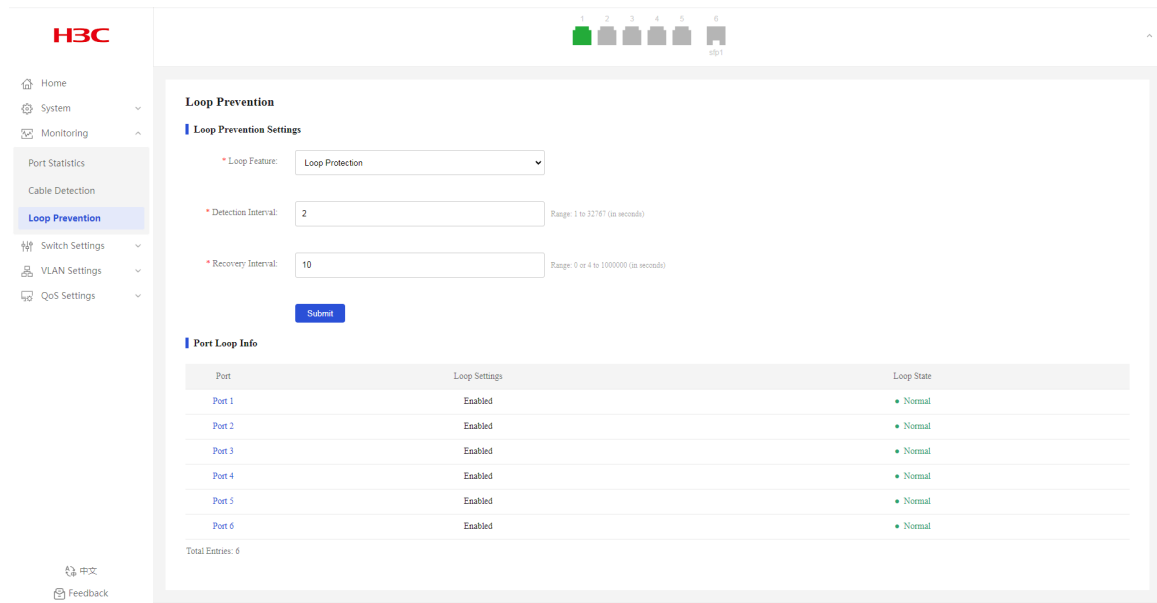


Figure 21 Loop protection

Loop Prevention

Loop Prevention Settings

* Loop Feature:

* Detection Interval: Range: 1 to 32767 (in seconds)

* Recovery Interval: Range: 0 or 4 to 1000000 (in seconds)

Verifying the configuration

As shown in [Figure 22](#), when a loop is detected on port 3, you can view that port 2 is blocked and its icon is displayed in yellow.

Figure 22 Port loop information

The screenshot displays the H3C web management interface for Loop Prevention. The left sidebar contains navigation options: Home, System, Monitoring, Port Statistics, Cable Detection, Loop Prevention (highlighted), Switch Settings, VLAN Settings, and QoS Settings. At the bottom of the sidebar are links for 中文 and Feedback.

The main content area is titled "Loop Prevention" and includes a status bar with six colored indicators (1-6) and an "H3C" logo. Below the title is the "Loop Prevention Settings" section, which contains:

- Loop Feature: Loop Protection (dropdown menu)
- Detection Interval: 2 (input field, Range: 1 to 32767 (in seconds))
- Recovery Interval: 10 (input field, Range: 0 or 4 to 100000 (in seconds))
- Submit button

Below the settings is the "Port Loop Info" section, which contains a table with the following data:

Port	Loop Settings	Loop State
Port 1	Enabled	Normal
Port 2	Enabled	Normal
Port 3	Enabled	Blocked
Port 4	Enabled	Normal
Port 5	Enabled	Normal
Port 6	Enabled	Normal

Total Entries: 6

Switch Settings

Port Settings

Overview

This feature allows you to view the physical state, operating mode, rate, and traffic control information about each port and edit port settings.

Interface rate

Generally, a device automatically negotiates the rate of an Ethernet interface with the peer device. The negotiated rate can be any rate within the rate capability range. To allow the interface to use only specific rates, you can configure auto negotiation rate settings.

Operating mode

You can configure an Ethernet interface to operate in one of the following duplex modes:

- **Full duplex mode**—The interface can send and receive packets simultaneously.
- **Half duplex mode**—The interface can only send or receive packets at a given time.
- **Auto negotiation mode**—The interface negotiates a duplex mode with its peer.

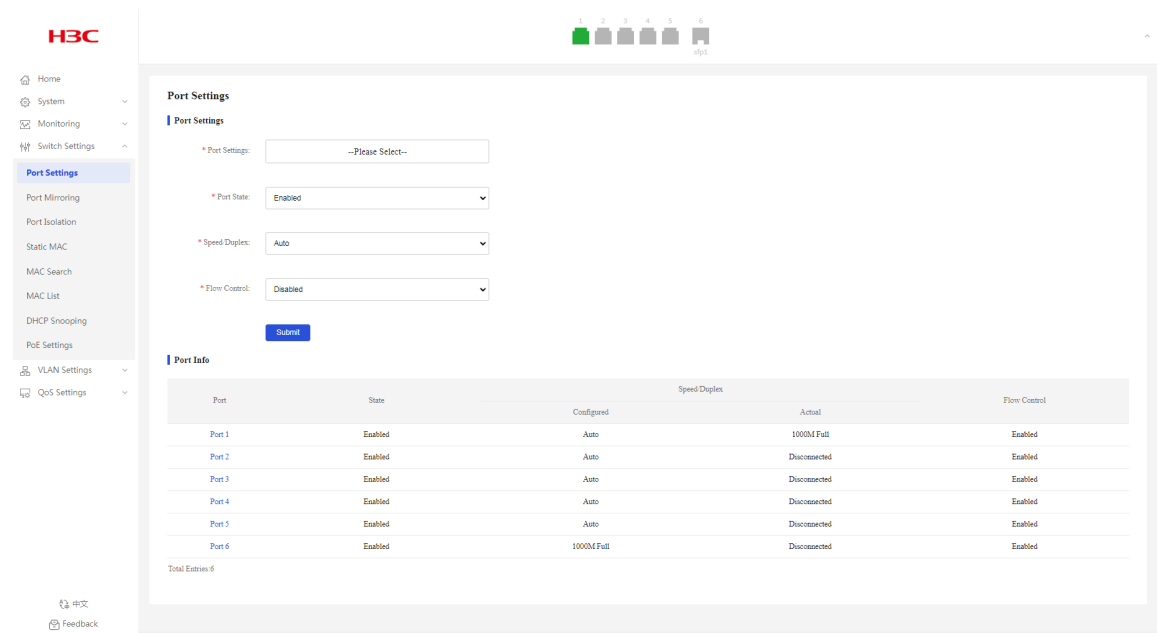
Flow control

With flow control enabled, when traffic congestion occurs at the receiving end, the receiving end sends a flow control (Pause) frame to ask the sending end to suspend sending packets.

Configuring port settings

1. From the navigation pane, select **Switch Settings > Port Settings**.
2. From the **Port Settings** list, select the ports to configure.
3. Bring up or shut down the ports. By default, a port is up.
4. Select a rate and duplex mode. By default, the auto mode is used.
5. Enable or disable flow control. By default, flow control is disabled.
6. Click **Submit**.

Figure 23 Configuring port settings



Port Info

1. From the navigation pane, select **Switch Settings > Port Settings**.
2. You can view port information in the **Port Info** area.

Port Mirroring

Overview

Port mirroring copies the packets passing through a port to the destination port that connects to a data monitoring device for packet analysis.

Concepts

Mirroring source

Monitored port on the device. Packets of the monitored port will be copied and sent to the destination port.

Mirroring destination

Port that connects to the data monitoring device. Packets of the source port will be copied and sent to the destination port.

Mirroring direction

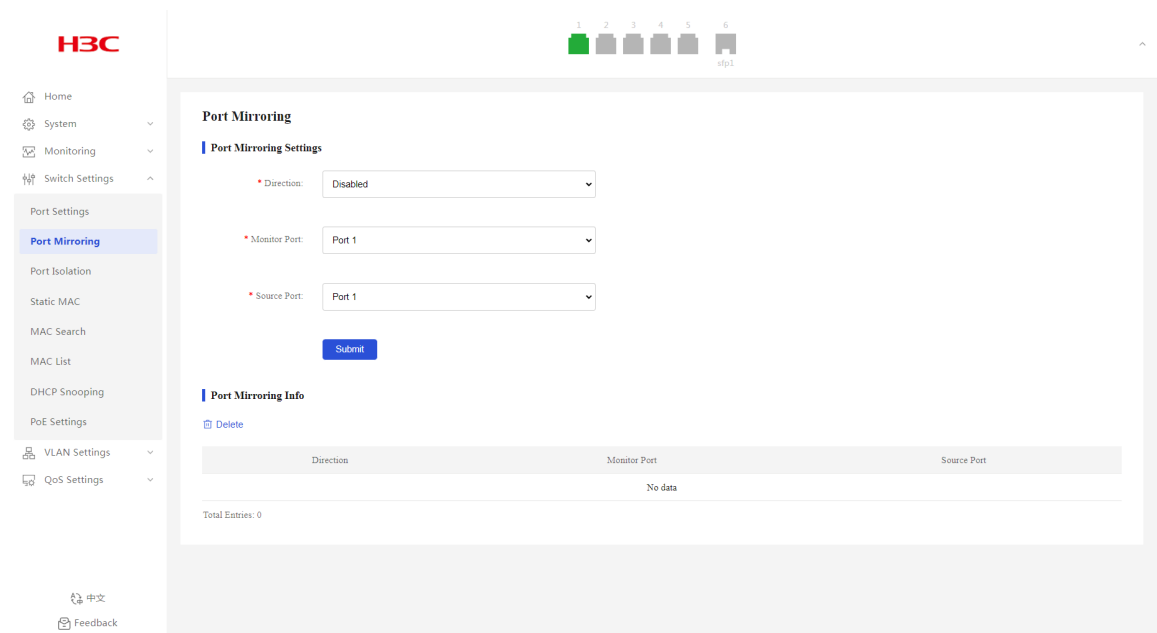
Direction of packets copied on a mirroring source.

- **Rx**—Copies only packets received by the source port.
- **Tx**—Copies only packets sent by the source port.
- **Both**—Copies packets sent and received by the source port.

Configuring port mirroring

1. From the navigation pane, select **Switch Settings > Port Mirroring**.
2. Select a mirroring direction. By default, port mirroring is disabled.
3. Select the monitor and source ports.
4. Click **Submit**.

Figure 24 Configuring port mirroring



Displaying and clearing port mirroring information

1. From the navigation pane, select **Switch Settings > Port Mirroring**.
2. You can view port mirroring information in the **Port Mirroring Info** area.
3. To clear port mirroring information, click the delete icon [Delete](#).

Port Isolation

Overview

The port isolation feature isolates Layer 2 traffic for data privacy and security without using VLANs.

Configuring port isolation settings

1. From the navigation pane, select **Switch Settings > Port Isolation**.
2. Enable or disable port isolation. By default, port isolation is disabled.
3. In the dialog box that opens, click **OK**.

Figure 25 Configuring port isolation settings

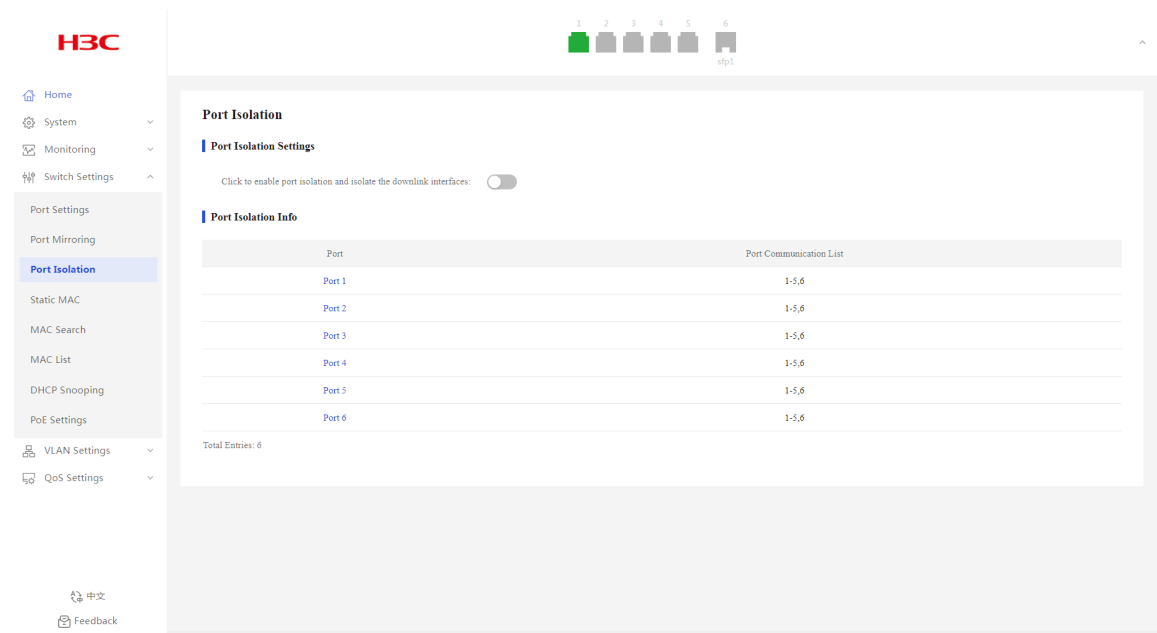


Figure 26 Confirming operation

192.168.0.233 says

Are you sure you want to change the port isolation state?



Displaying port isolation information

1. From the navigation pane, select **Switch Settings > Port Isolation**.
2. You can view port isolation information in the **Port Isolation Info** area.

Static MAC

Overview

An Ethernet device uses a MAC address table to forward frames. A MAC address entry includes a destination MAC address, an outgoing interface, and a VLAN ID. When the device receives a frame, it uses the destination MAC address of the frame to look for a match in the MAC address table.

- The device forwards the frame out of the outgoing interface in the matching entry if a match is found.
- The device floods the frame in the VLAN of the frame if no match is found.

MAC address entry generation

The entries in the MAC address table include entries automatically learned by the device and entries manually added.

MAC address learning

The device can automatically populate its MAC address table by learning the source MAC addresses of incoming frames on each interface.

The device performs the following operations to learn the source MAC address of incoming packets:

1. Checks the source MAC address (for example, MAC-SOURCE) of the frame.
2. Looks up the source MAC address in the MAC address table.
 - The device updates the entry if an entry is found.
 - The device adds an entry for MAC-SOURCE and the incoming port if no entry is found.

For security and efficient use of table space, the MAC address table uses an aging timer for each dynamic MAC address entry. If a dynamic MAC address entry is not updated before the aging timer expires, the device deletes the entry. This aging mechanism ensures that the MAC address table can promptly update to accommodate latest network topology changes.

Manually configuring MAC address entries

Dynamic MAC address learning does not distinguish between illegitimate and legitimate frames, which can invite security hazards. When Host A is connected to Port A, a MAC address entry will be learned for the MAC address of Host A (for example, MAC A). When an illegal user sends frames with MAC A as the source MAC address to Port B, the device performs the following operations:

- Learns a new MAC address entry with Port B as the outgoing interface and overwrites the old entry for MAC A.
- Forwards frames destined for MAC A out of Port B to the illegal user.

As a result, the illegal user obtains the data of Host A. To improve the security for Host A, manually configure a static entry to bind Host A to Port A. Then, the frames destined for Host A are always sent out of Port A. Other hosts using the forged MAC address of Host A cannot obtain the frames destined for Host A.

Types of MAC address entries

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

- **Static entries**—A static entry is manually added to forward frames with a specific destination MAC address out of the associated interface, and it never ages out.
- **Dynamic entries**—A dynamic entry is dynamically learned to forward frames with a specific destination MAC address out of the associated interface. A dynamic entry might age out.

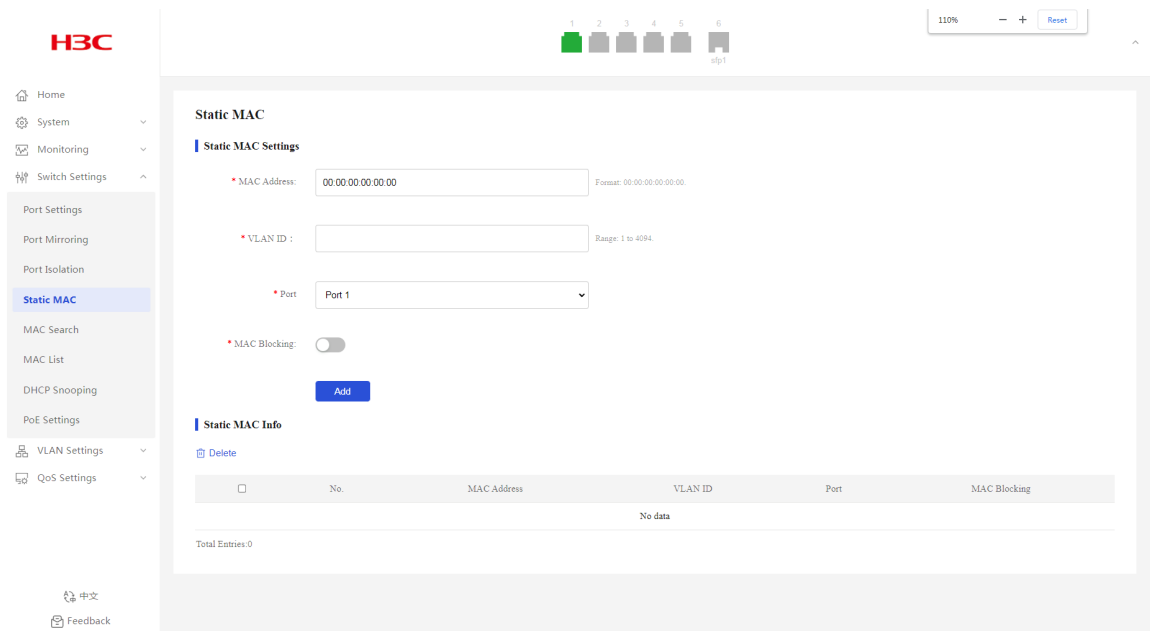
Blackhole entries

A blackhole entry is manually configured and never ages out. A blackhole entry is configured for filtering out frames with a specific source or destination MAC address. For example, to block all frames destined for or sourced from a user, you can configure the MAC address of the user as a blackhole MAC address entry.

Configuring static MAC address settings

1. From the navigation pane, select **Switch Settings > Static MAC**.
2. Enter the target MAC address.
3. Enter the ID of the VLAN to which the interface belongs.
4. Select the outgoing interface from the port list.
5. Enable MAC blocking as needed. By default, MAC blocking is disabled.
6. Click **Add**.

Figure 27 Configuring static MAC address settings



Displaying static MAC addresses

1. From the navigation pane, select **Switch Settings > Static MAC**.
2. You can view the static MAC addresses in the **Static MAC Info** area.

Filtering MAC addresses

1. From the navigation pane, select **Switch Settings > MAC Search**.
2. Enter the target MAC address and its VLAN ID, and then click **Search**.
The page will display the filtering result.

Figure 28 MAC address filtering

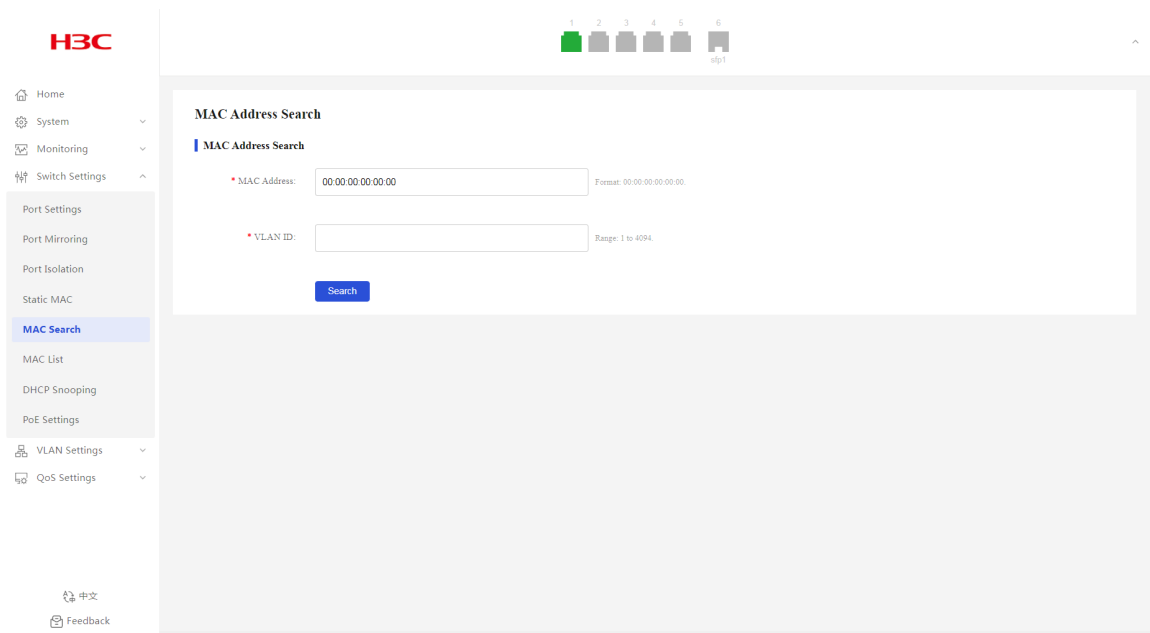
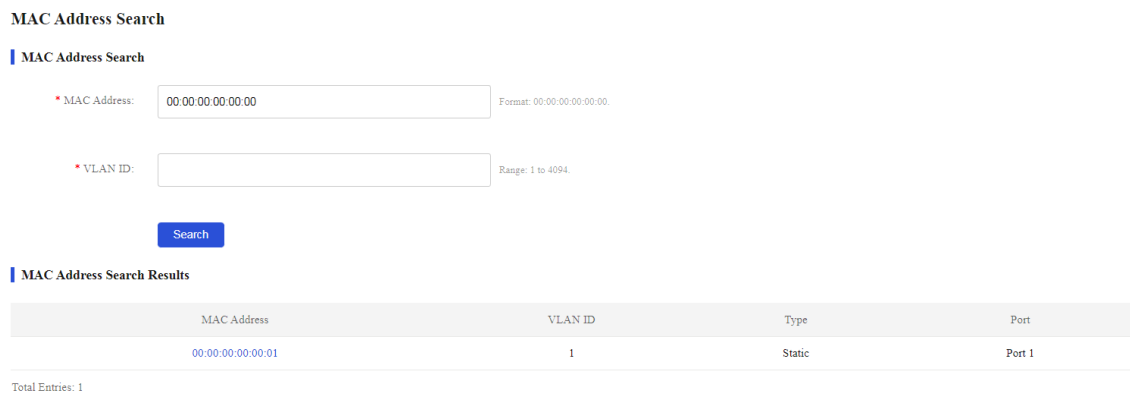


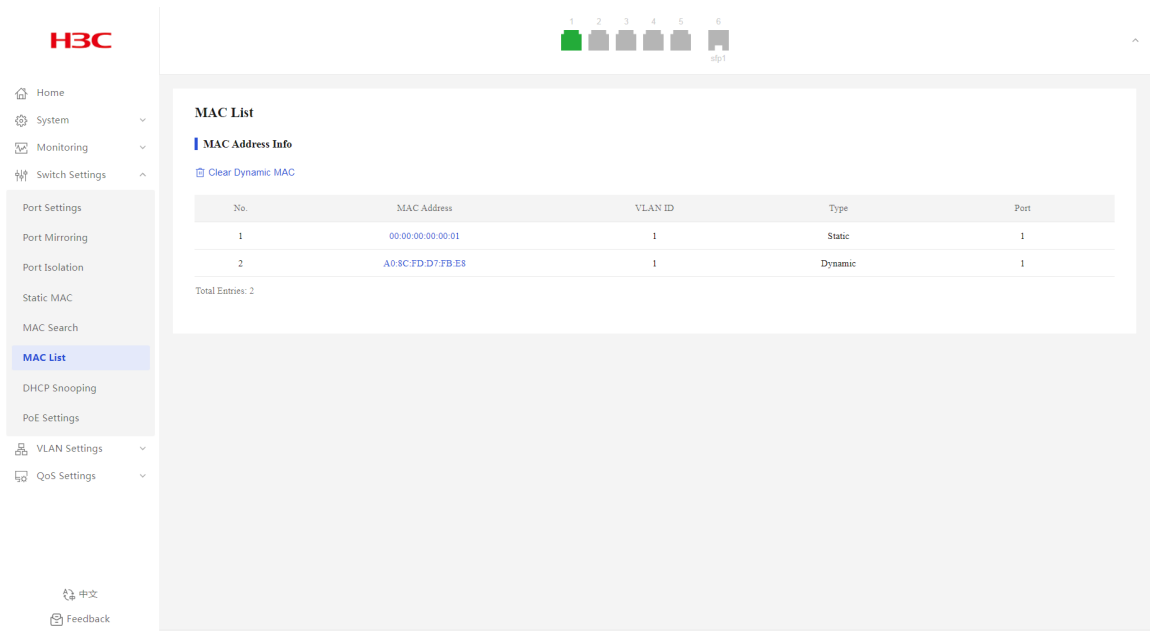
Figure 29 MAC address filtering result



MAC List

1. From the navigation pane, select **Switch Settings > MAC List**.
2. You can view the MAC address information.

Figure 30 MAC address list



DHCP Snooping

Overview

DHCP snooping is a security feature for DHCP.

DHCP snooping works between the DHCP client and server, or between the DHCP client and DHCP relay agent. When a DHCP snooping device is located between a DHCP server and a DHCP relay agent, the DHCP snooping feature does not take effect.

DHCP snooping benefits

DHCP snooping guarantees that DHCP clients obtain IP addresses from authorized DHCP servers. DHCP snooping defines trusted and untrusted ports to make sure clients obtain IP addresses only from authorized DHCP servers.

- **Trusted**—A trusted port can forward DHCP messages correctly to make sure the clients get IP addresses from authorized DHCP servers.
- **Untrusted**—An untrusted port discards received DHCP-ACK and DHCP-OFFER messages to prevent unauthorized servers from assigning IP addresses.

Configure the DHCP snooping device's ports facing the DHCP server as trusted ports, and configure other ports as untrusted ports. The trusted port forwards response messages from the DHCP server to the client. The untrusted port connected to the unauthorized DHCP server discards incoming DHCP response messages.

Configuring DHCP snooping

1. From the navigation pane, select **Switch Settings > DHCP Snooping**.
2. Configure the DHCP snooping feature state, and then click **OK** in the dialog box that opens. By default, DHCP snooping is disabled.

3. Configure DHCP snooping settings:
 - a. Select the trusted or untrusted port state. By default, all ports on the device are trusted ports after DHCP snooping is enabled.
 - b. Select the target ports from the port list.
 - c. Click **Submit**.

Figure 31 DHCP snooping page

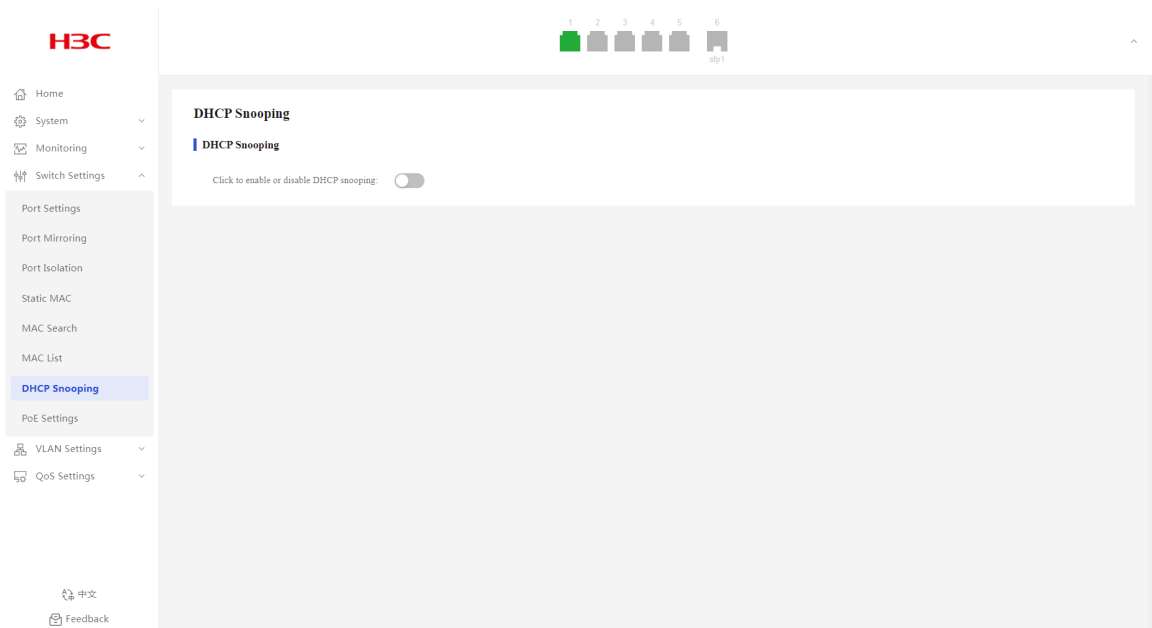


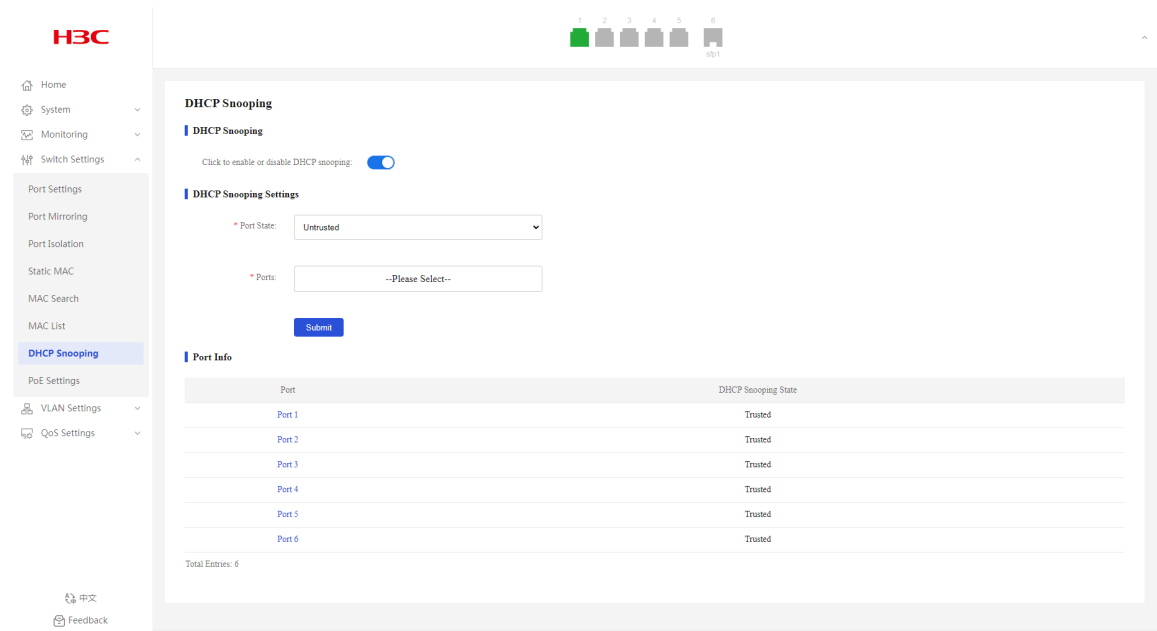
Figure 32 Confirming operation

192.168.0.233 says

Are you sure you want to enable or disable DHCP snooping?



Figure 33 DHCP snooping page



Displaying DHCP snooping information

1. From the navigation pane, select **Switch Settings > DHCP Snooping**.
2. You can view DHCP snooping information in the **Port Info** area.

PoE Settings

Overview

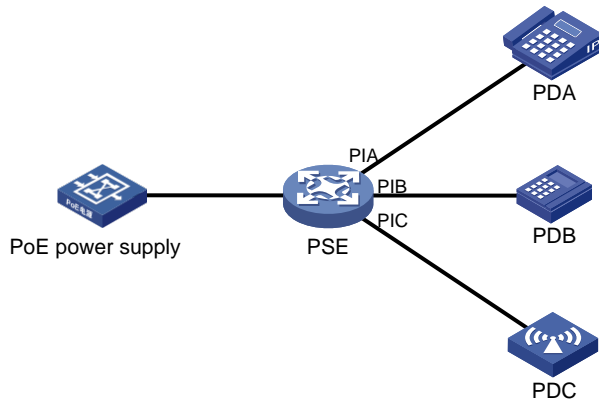
Power over Ethernet (PoE) enables a device to supply power for powered devices (PDs) over twisted pair cables.

PoE system

As shown in [Figure 34](#), a PoE system includes the following elements:

- **PoE power supply**—A PoE power supply provides power for the entire PoE system.
- **PSE**—A power sourcing equipment (PSE) supplies power to PDs.
- **PI**—A power interface (PI) is a PoE-capable Ethernet interface on a PSE.
- **PD**—A powered device (PD) receives power from a PSE. PDs include IP telephones, APs, portable chargers, POS terminals, and Web cameras. You can also connect a PD to a redundant power source for reliability.

Figure 34 PoE system diagram



Procedure

1. From the navigation pane, select **Switch Settings** > PoE Settings.
2. In the PoE Info area, configure the PoE state for the target port. By default, PoE is enabled for a port.
3. In the dialog box that opens, click **OK**.

Figure 35 PoE settings page

H3C

Home
System
Monitoring
Switch Settings
Port Settings
Port Mirroring
Port Isolation
Static MAC
MAC Search
MAC List
DHCP Snooping
PoE Settings
VLAN Settings
QoS Settings

中文
Feedback

PoE Settings

PoE Info

Total Power: 73.0 W Used Power: 0.0 W Available Power: 73.0 W Operating State: OK

PoE Info

Refresh

PoE State	Port	Power(mW)	Electric Current(mA)	Voltage(mV)	Power Supply State
<input checked="" type="checkbox"/>	Port 1	0	0	0	Not Supplying Power
<input checked="" type="checkbox"/>	Port 2	0	0	0	Not Supplying Power
<input checked="" type="checkbox"/>	Port 3	0	0	0	Not Supplying Power
<input checked="" type="checkbox"/>	Port 4	0	0	0	Not Supplying Power

Total Entries: 4

Figure 36 Confirming operation

192.168.0.233 says

Are you sure you want to change the port state?



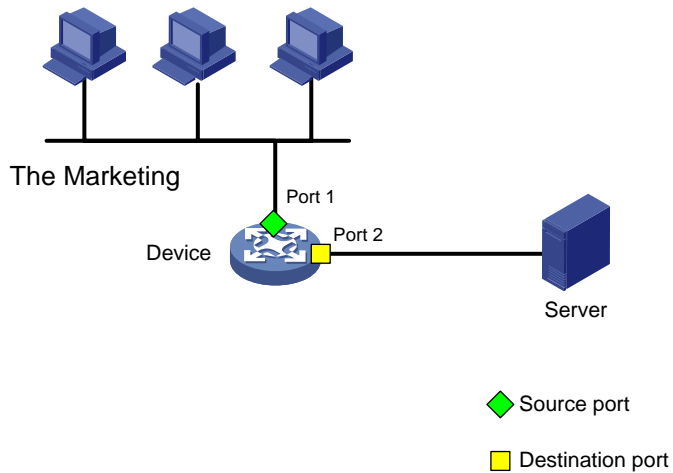
Configuration examples

Example: Configuring port mirroring

Network configuration

As shown in [Figure 37](#), the device connects to the marketing departments through port 1 and to the server through port 2. Configure local port mirroring in source port mode to enable the server to monitor the bidirectional traffic of the two departments.

Figure 37 Network diagram



Procedure

1. From the navigation pane, select **Switch Settings > Port Mirroring**.
2. Select **Both** in the direction list.
3. Select port 2 as the monitor port, and select port 1 as the source port.
4. Click **Submit**.

Figure 38 Port mirroring page

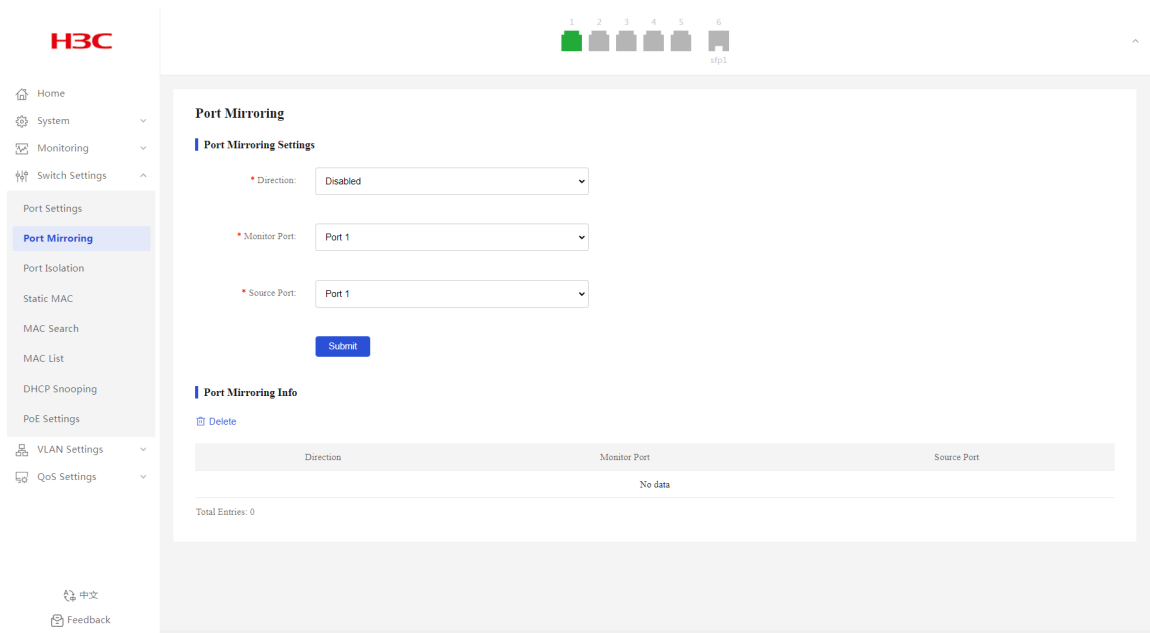


Figure 39 Configuring port mirroring

Port Mirroring

Port Mirroring Settings

* Direction:

* Monitor Port:

* Source Port:

Verifying the configuration

As shown in Figure 40, the port mirroring direction is both, the monitor port is port 2, and the source port is port 1. Verify that you can monitor the incoming packets and outgoing packets of the marketing and technology departments on the server.

Figure 40 Port mirroring information

Port Mirroring Info

[Delete](#)

Direction	Monitor Port	Source Port
Both	2	1

Total Entries: 1

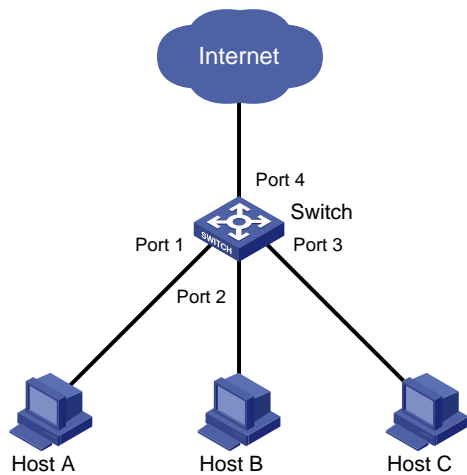
Example: Configuring port isolation

Network configuration

As shown in [Figure 41](#), LAN users Host A, Host B, and Host C are connected to Port 1, Port 2, and Port 3 on the device, respectively. The device connects to the Internet through Port 4.

Configure the device to provide Internet access for all the hosts, and isolate them from one another.

Figure 41 Network diagram



Procedure

1. From the navigation pane, select **Switch Settings > Port Isolation**.
2. Configure the port isolation state, and then click **OK** in the dialog box that opens. By default, port isolation is disabled.

Figure 42 Port isolation page

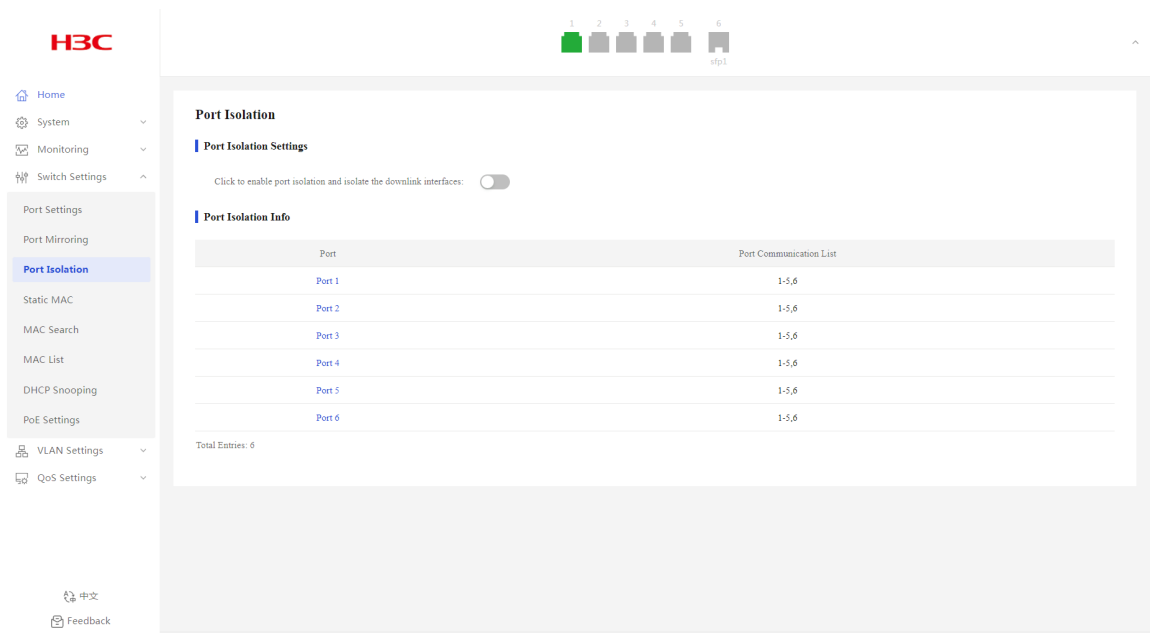


Figure 43 Confirming operation

192.168.0.233 says

Are you sure you want to change the port isolation state?



Verifying the configuration

1. From the navigation pane, select **Switch Settings > Port Isolation**.
2. Verify that Port 1, Port 2, and Port 3 are isolated from one another at Layer 2, and Host A, Host B, and Host C cannot communicate with each other at Layer 2.

Figure 44 Port isolation information



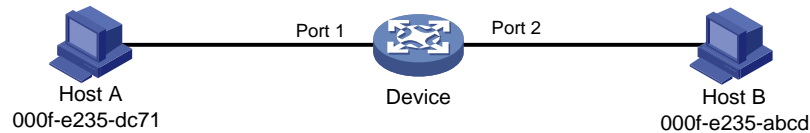
MAC address configuration example

Network configuration

Host A at MAC address 00:0f:e2:35:dc:71 is connected to Port 1 of Device and belongs to VLAN 1. Host B at MAC address 00:0f:e2:35:ab:cd, which behaved suspiciously on the network, also belongs to VLAN 1. Configure the MAC address table as follows:

- To prevent MAC address spoofing, add a static entry for Host A in the MAC address table of Device.
- To drop all frames destined for Host B, add a blackhole MAC address entry for Host B.

Figure 45 Network diagram



Procedure

Add a static MAC address entry with destination address 00:0f:e2:35:dc:71, outgoing interface Port 1, and VLAN ID 1.

1. From the navigation pane, select **Switch Settings > Static MAC**.
2. Enter MAC address 00:0f:e2:35:dc:71 and VLAN ID 1, select port 1 as the outgoing interface, and then click **Add**.

Add a static MAC address entry with destination address 00:0f:e2:35:ab:cd, outgoing interface Port 1, and VLAN ID 1, and block the MAC address.

1. From the navigation pane, select **Switch Settings > Static MAC**.
2. Enter MAC address 00:0f:e2:35:ab:cd and VLAN ID 1, select port 1 as the outgoing interface, enable MAC blocking, and then click **Add**.

Figure 46 Static MAC address entries

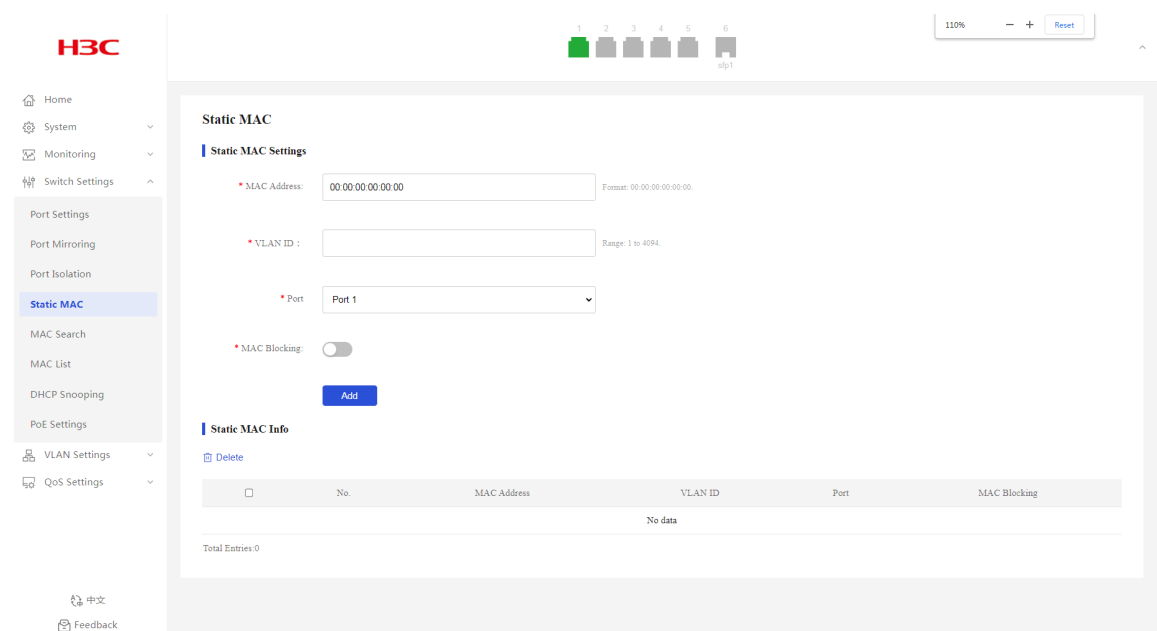


Figure 47 Adding a static MAC address entry

Static MAC

Static MAC Settings

* MAC Address: Format: 00:00:00:00:00:00.

* VLAN ID : Range: 1 to 4094.

* Port ▼

* MAC Blocking:

Figure 48 Adding a static MAC address entry and blocking it

Static MAC

Static MAC Settings

* MAC Address: Format: 00:00:00:00:00:00.

* VLAN ID : Range: 1 to 4094.

* Port ▼

* MAC Blocking:

Verifying the configuration

Verify that the MAC address entries are displayed in the list.

Figure 49 Static MAC address entries

Static MAC Info

[Delete](#)

<input type="checkbox"/>	No.	MAC Address	VLAN ID	Port	MAC Blocking
<input type="checkbox"/>	1	00:0F:E2:35:AB:CD	1	2	-
<input type="checkbox"/>	2	00:0F:E2:35:DC:71	1	1	-

Total Entries:2

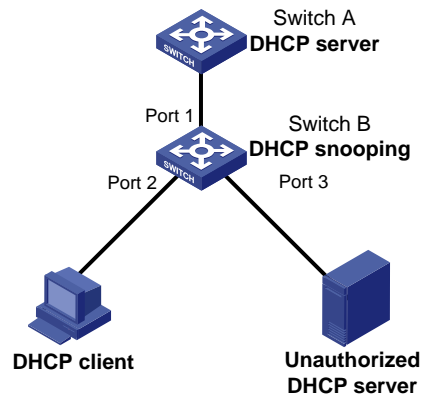
Example: Enabling DHCP snooping globally

Network configuration

Switch B is connected to the authorized DHCP server through Ethernet port 1, to the unauthorized DHCP server through Ethernet port 3, and to the DHCP client through Ethernet port 2.

Configure only the port connected to the authorized DHCP server to forward the responses from the DHCP server.

Figure 50 Network diagram

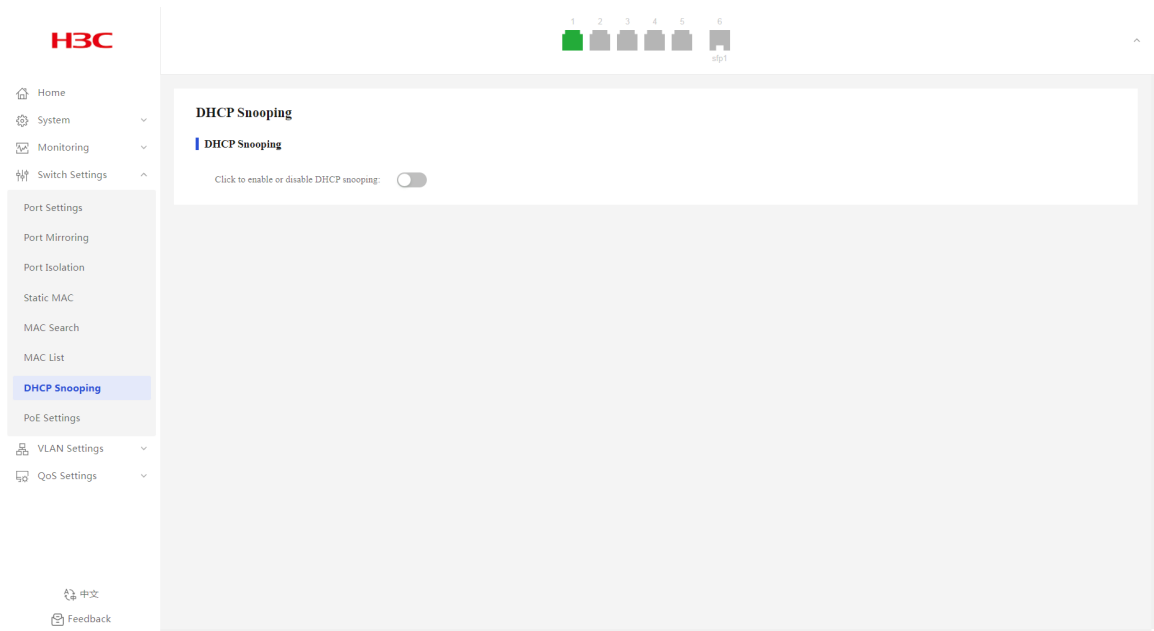


Procedure

Enable DHCP snooping globally:

1. From the navigation pane, select **Switch Settings > DHCP Snooping**.
2. Enable DHCP snooping.

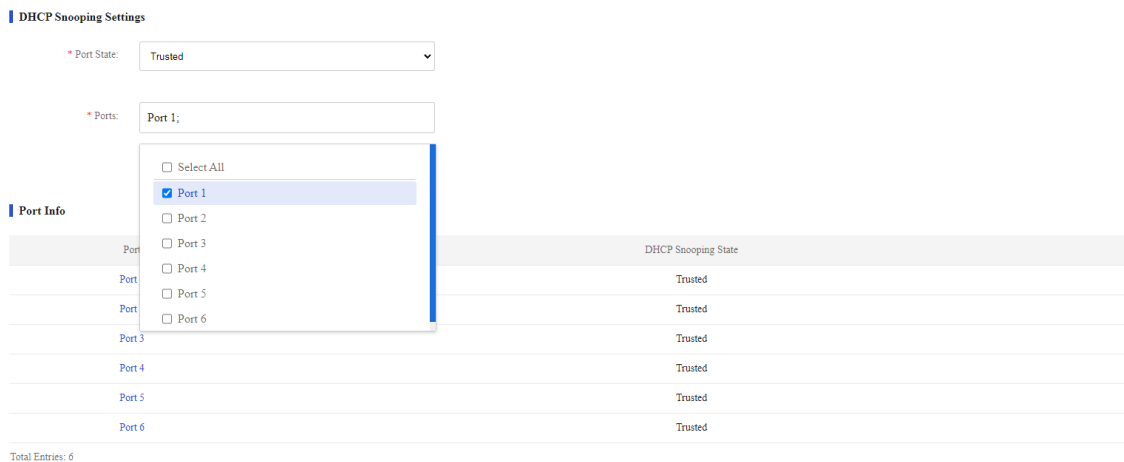
Figure 51 DHCP snooping page



Configure port 1 as a trusted port:

1. From the navigation pane, select **Switch Settings > DHCP Snooping**.
2. Select the port state to trusted.
3. Select port 1 from the port list.
4. Click **Submit**.

Figure 52 Configuring DHCP snooping settings



Verifying the configuration

Verify that the DHCP client can obtain an IP address and other configuration parameters only from the authorized DHCP server.

VLAN Settings

Overview

The Virtual Local Area Network (VLAN) technology divides a physical LAN into multiple logical LANs. Each VLAN is a broadcast domain. Hosts in the same VLAN can communicate with one another at Layer 2, but they are isolated from hosts in other VLANs at Layer 2.

VLAN features

Overview

If you disable the VLAN feature, the device forwards received packets without processing VLAN tags.

Procedure

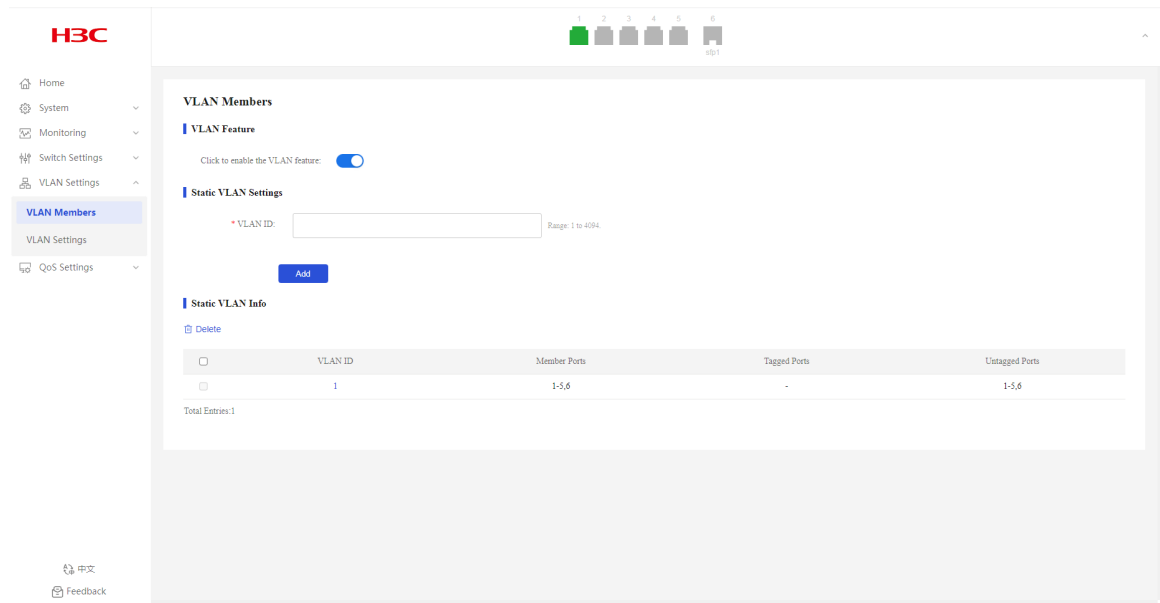
1. Access the VLAN members or VLAN settings page.
2. Enable or disable the VLAN feature, and then click **OK** in the dialog box that opens.
By default, VLAN is enabled.

VLAN Members

Creating VLANs

1. From the navigation pane, select **VLAN Settings > VLAN Members**.
2. Enter the target VLAN ID, and then click **Add**.
By default, only system-defined VLAN 1 exists.

Figure 53 Creating a VLAN



Deleting VLANs

1. From the navigation pane, select **VLAN Settings > VLAN Members**.
2. Select the VLANs to be deleted, and then click **Delete**. VLAN 1 cannot be deleted.

VLAN Settings

Overview

Port-based VLANs group VLAN members by port. A port forwards packets from a VLAN only after it is assigned to the VLAN.

Port link type

You can set the link type of a port to access or trunk. The port link type determines whether the port can be assigned to multiple VLANs. The link types use the following VLAN tag handling methods:

- **Access**—An access port can forward packets only from one VLAN and send these packets untagged. An access port is typically used in the following conditions:
 - Connecting to a terminal device that does not support VLAN packets.
 - In scenarios that do not distinguish VLANs.
- **Trunk**—A trunk port can forward packets from multiple VLANs. Except packets from the port VLAN ID (PVID), packets sent out of a trunk port are VLAN-tagged. Ports connecting network devices are typically configured as trunk ports.

PVID

The PVID (native VLAN) identifies the default VLAN of a port. Untagged packets received on a port are considered as the packets from the port PVID.

An access port can join only one VLAN. The VLAN to which the access port belongs is the PVID of the port. A trunk port supports multiple VLANs and the PVID configuration.

How ports of different link types handle frames

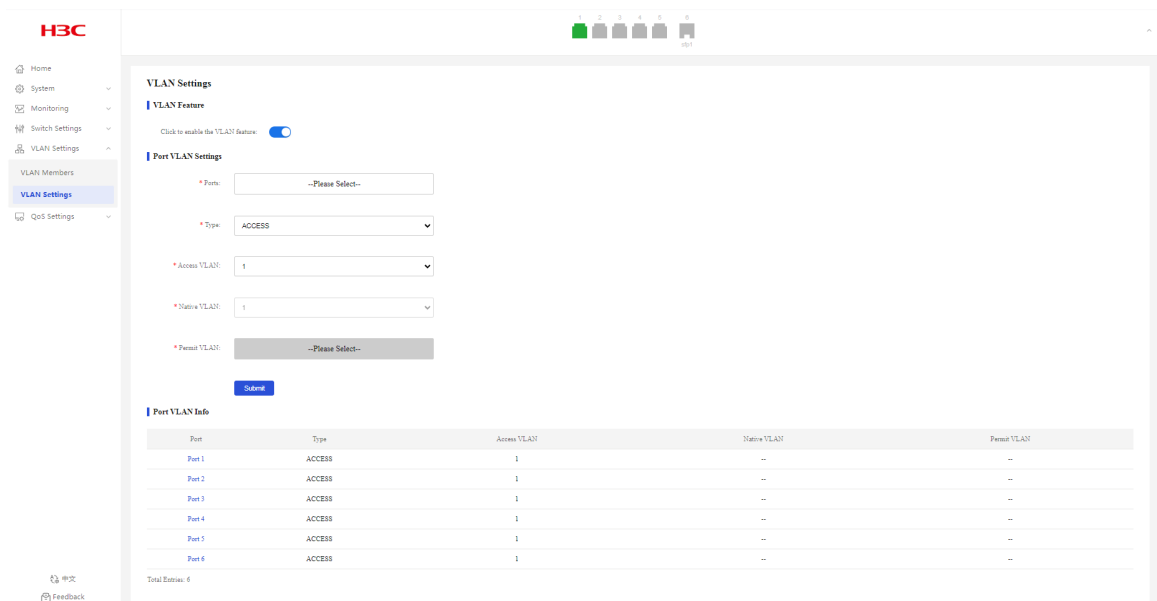
Actions	Access	Trunk
In the inbound direction for an untagged frame	Tags the frame with the PVID tag.	<ul style="list-style-type: none"> If the PVID is permitted on the port, tags the frame with the PVID tag. If not, drops the frame.
In the inbound direction for a tagged frame	<ul style="list-style-type: none"> Receives the frame if its VLAN ID is the same as the PVID. Drops the frame if its VLAN ID is different from the PVID. 	<ul style="list-style-type: none"> Receives the frame if its VLAN is permitted on the port. Drops the frame if its VLAN is not permitted on the port.
In the outbound direction	Removes the VLAN tag and sends the frame.	<ul style="list-style-type: none"> Removes the tag and sends the frame if the frame carries the PVID tag and the port belongs to the PVID. Sends the frame without removing the tag if its VLAN is carried on the port but is different from the PVID.

Configuring port VLAN settings

Configuring access ports and specifying an access VLAN

1. From the navigation pane, select **VLAN Settings > VLAN Settings**.
2. Select the target ports from the port list.
3. Select the access link type. The default link type is access.
4. Select an access VLAN. By default, all access ports belong to VLAN 1.
5. Click **Submit**.

Figure 54 Configuring access ports and specifying an access VLAN



Configuring trunk ports and specifying PVID and permit VLAN

1. From the navigation pane, select **VLAN Settings > VLAN Settings**.
2. Select the target ports from the port list.

3. Select the trunk link type. The default link type is access.
4. Select native and permit VLANs.
5. Click **Submit**.

Displaying port VLAN information

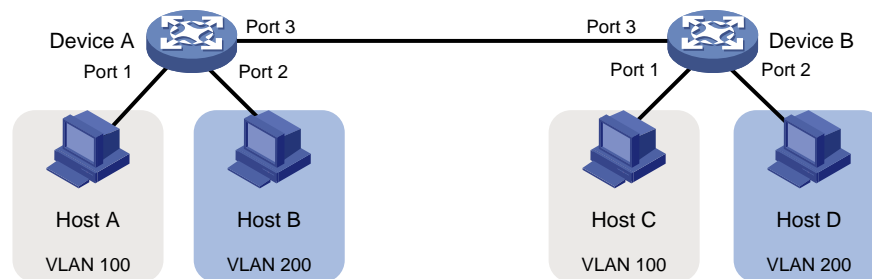
1. From the navigation pane, select **VLAN Settings > VLAN Settings**.
2. You can view port VLAN information in the **Port VLAN Info** area.

Configuration example

Network configuration

- Host A and Host C belong to Department A but access the company network through different devices. Host B and Host D belong to Department B and access the company network through different devices.
- To ensure communication security and avoid flooding broadcast packets, use VLANs to isolate Layer 2 traffic of different departments. Configure department A to use VLAN 100, and configure department B to use VLAN 200.

Figure 55 Network diagram



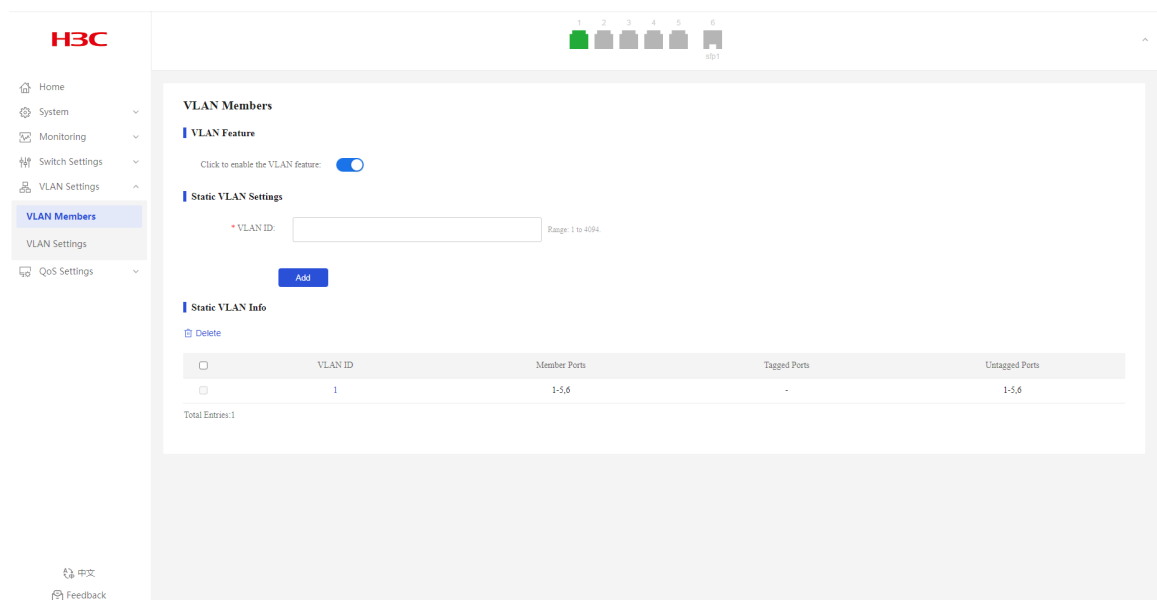
Procedure

Configuring Device A

Create VLAN 100 and VLAN 200:

1. From the navigation pane, select **VLAN Settings > VLAN Members**.
2. Enter VLAN ID 100, and then click **Add**.
3. Enter VLAN ID 200, and then click **Add**.

Figure 56 Adding VLAN IDs



Configure port VLANs:

1. From the navigation pane, select **VLAN Settings > VLAN Settings**.
2. Assign port 1 to VLAN 100:
 - a. Select port 1 from the port list.
 - b. Select the access link type.
 - c. Select VLAN 100 from the access VLAN list.
 - d. Click **Submit**.

Figure 57 Configuring VLAN settings for port 1

Port VLAN Settings

* Ports:

* Type:

* Access VLAN:

* Native VLAN:

* Permit VLAN:

3. Assign port 2 to VLAN 200:
 - a. Select port 2 from the port list.
 - b. Select the access link type.
 - c. Select VLAN 200 from the access VLAN list.
 - d. Click **Submit**.

Figure 58 Configuring VLAN settings for port 2

Port VLAN Settings

* Ports:

* Type:

* Access VLAN:

* Native VLAN:

* Permit VLAN:

4. Configure port 3 as a trunk port and assign it to VLANs 100 and 200, so that Device A can send packets from VLAN 100 and VLAN 200 to Device B.
 - a. Select port 3 from the port list.
 - b. Select the trunk link type.
 - c. Select VLAN 1 from the native VLAN list.
 - d. Select VLANs 100 and 200 from the permit VLAN list.
 - e. Click **Submit**.

Figure 59 Configuring VLAN settings for port 3

Port VLAN Settings

* Ports:

* Type:

* Access VLAN:

* Native VLAN:

* Permit VLAN:

Configuring Device B

Configure Device B in the same way you configure Device A.

Configuring the hosts

Assign Host A and Host C to the same subnet, for example, 192.168.100.0/24. Assign Host B and Host D to the same subnet, for example, 192.168.200.0/24.

Verifying the configuration

Verify that Host A and Host C can successfully ping each other, and they cannot ping Host B or Host D. Verify that Host B and Host D can successfully ping each other, and they cannot ping Host A or Host C.

QoS Settings

Port Rate Limit

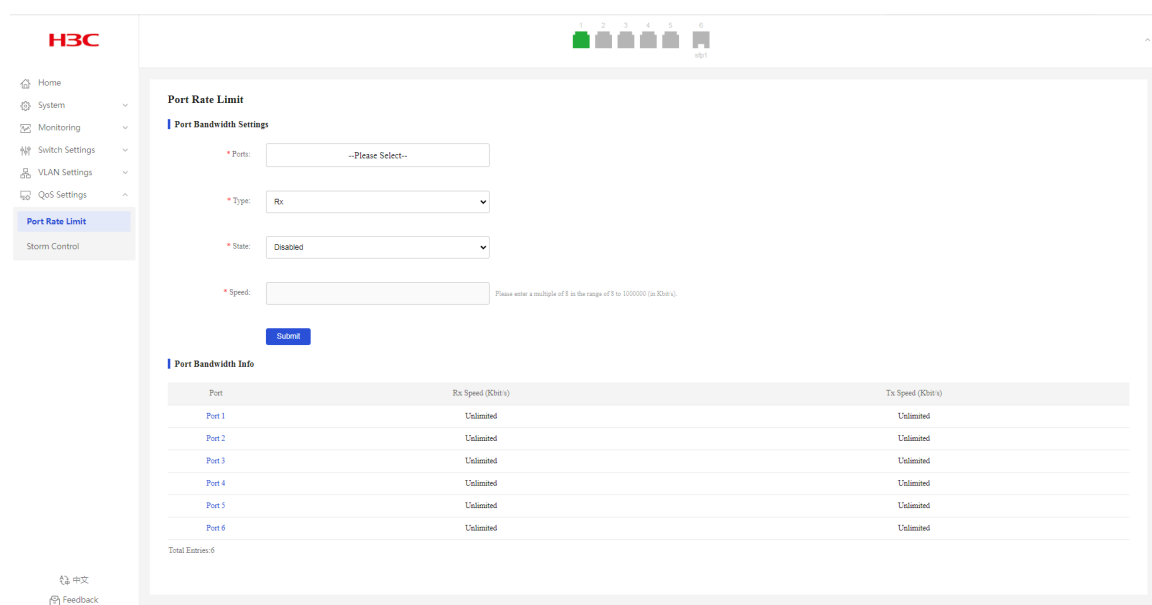
Overview

This feature allows you to limit the total packet rate.

Configuring port bandwidth settings

1. From the navigation pane, select **QoS Settings > Port Rate Limit**.
2. Select the target ports from the port list.
3. Select Tx or Rx from the type list.
4. Select a port rate limit state.
By default, port rate limit is disabled.
5. If you enable port rate limit, enter the rate limit.
6. Click **Submit**.

Figure 60 Configuring port bandwidth settings



Displaying port bandwidth information

1. From the navigation pane, select **QoS Settings > Port Rate Limit**.
2. You can view port bandwidth information in the **Port Bandwidth Info** area.

Storm Control

Overview

After you configure broadcast/unknown unicast/unknown multicast storm control on an interface, if the broadcast/unknown unicast/unknown multicast traffic exceeds the specified threshold, the system discards the excessive traffic.

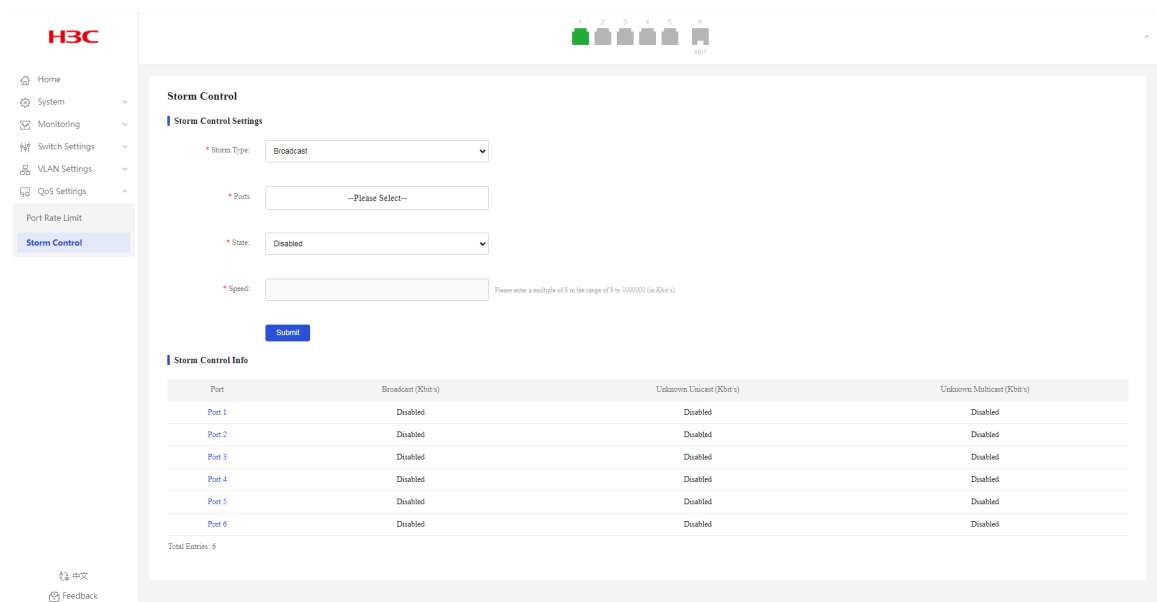
On a Layer 2 Ethernet interface, you can also configure traffic thresholds to suppress traffic storms. Traffic threshold control suppresses traffic through software, which might affect device performance. Storm control uses the chip to suppress traffic and has less impact on the device performance than traffic threshold control.

After packets of a protocol are added to the storm suppression and storm control allowlist, storm suppression and storm control do not take effect on packets of the protocol.

Configuring storm control

1. From the navigation pane, select **QoS Settings > Storm Control**.
2. Select a traffic type from the **Storm Type** list.
3. Select the target ports.
4. Enable or disable storm control. By default, storm control is disabled.
5. Set the suppression threshold in the Speed field.
6. Click **Submit**.

Figure 61 Configuring storm control



Displaying storm control information

1. From the navigation pane, select **QoS Settings > Storm Control**.
2. You can view storm control information in the **Storm Control Info** area.

Troubleshooting

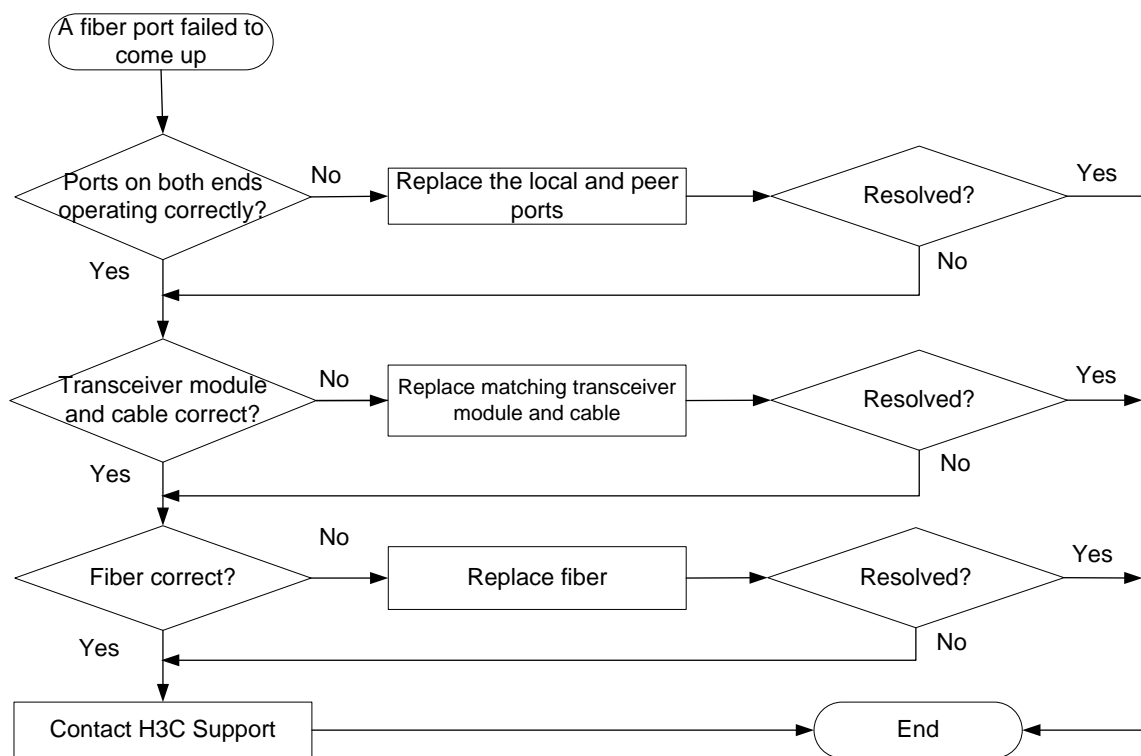
A fiber port fails to come up

Symptom

A fiber port fails to come up.

Troubleshooting flowchart

Figure 62 Troubleshooting link up failure on a fiber port



Solution

Verifying that the ports at both ends are operating correctly

Use a transceiver module and a fiber to connect the port to another port on the local end. Identify whether the port can come up:

- If the port can come up, you can determine that the peer port fails. Replace the peer port with a new port operating correctly.
- If the port cannot come up, you can determine that the local port fails. Replace the local port with a new port operating correctly.

Verifying that the transceiver module and cable are operating correctly

If the transceiver module is not operating correctly, replace it with a H3C transceiver module that matches the fiber port. Perform the following tasks to troubleshoot the transceiver module:

1. Verify that the wavelength and transmission distance of the local transceiver module are consistent with the wavelength and transmission distance of the peer transceiver module.
2. Use an optical power meter to verify that the Tx power and Rx power of the transceiver module are stable and are within the correct range.

For more information about transceiver modules and cables, see the installation guide.

Verifying that the fiber is operating correctly

Verify that the fiber matches the transceiver module. If they do not match, replace the fiber with a new one that matches the transceiver module. For more information about fibers, see the installation guide.

Contacting H3C Support

If the issue persists after the above procedures, collect the fault information, and contact H3C Support.

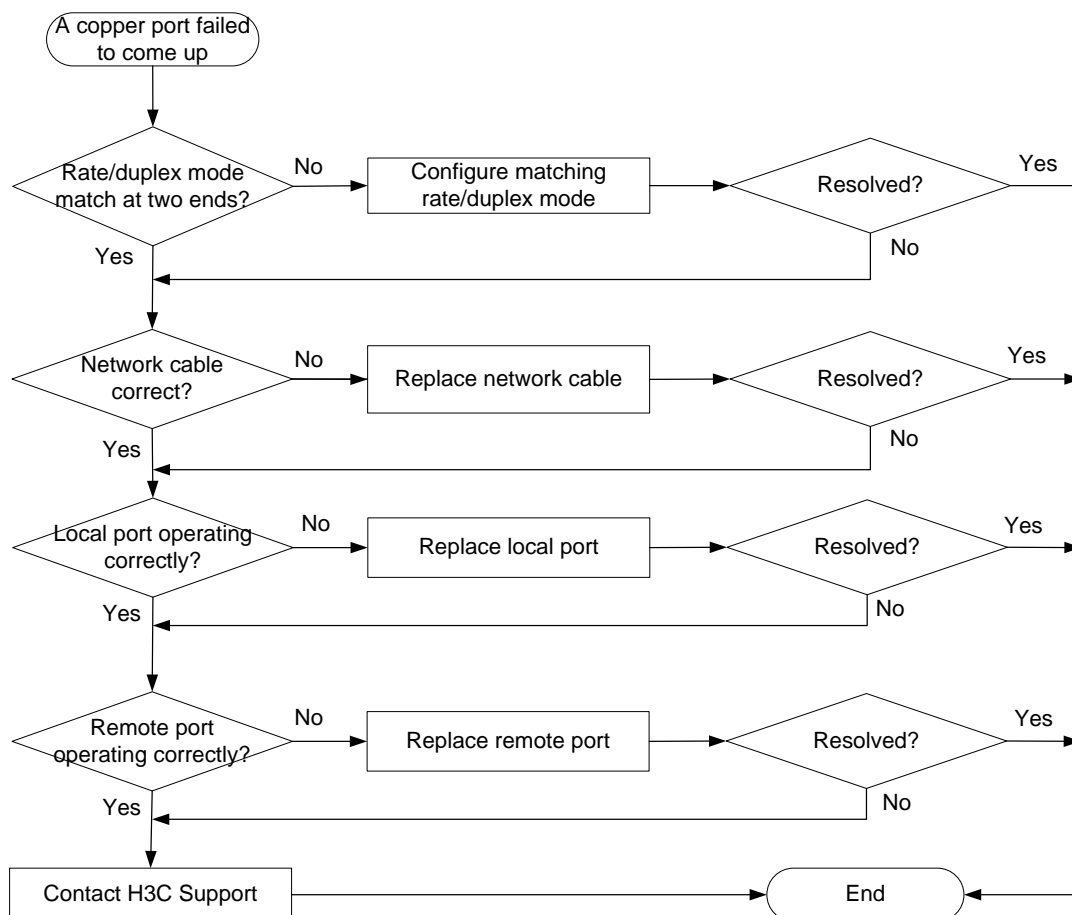
A copper port fails to come up

Symptom

A copper port fails to come up.

Troubleshooting flowchart

Figure 63 Troubleshooting link up failure on a copper port



Solution

Verifying that the local and remote ports are consistent in rate and duplex mode

To view port rate and duplex mode information, see "[Port Info](#)." If the local and remote ports are inconsistent in rate and duplex mode, edit the settings. For procedures, see "[Configuring port settings](#)."

Verifying that the network cable is in good condition

Replace the network cable with a new one to verify that the network cable is in good condition.

Verifying that the local port is operating correctly

Replace the local port with a new one to verify that the local port is operating correctly.

Verifying that the peer port is operating correctly

Replace the peer port with a new one to verify that the peer port is operating correctly.

Contacting H3C Support

If the issue persists after the above procedures, contact H3C Support.

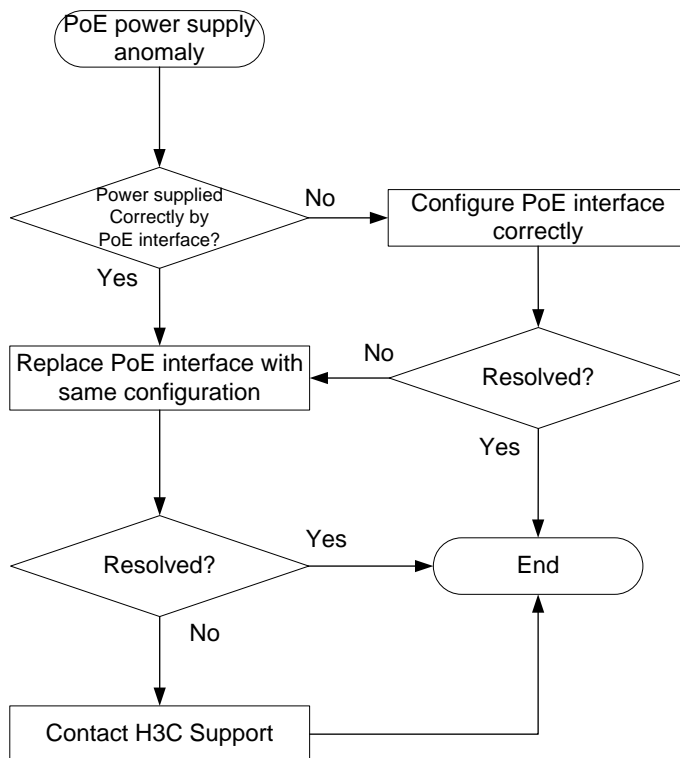
PoE power supply anomaly

Symptom

The PoE device cannot supply power correctly.

Troubleshooting flowchart

Figure 64 Troubleshooting PoE power supply anomaly



Solution

1. Verify that the PoE settings are correct. For more information, see "[PoE](#)."
If the PoE power is close to or reach the maximum power, disable unnecessary PoE port features or use PoE power with higher-wattage supply.
2. Verify that the PoE port is operating correctly.
Replace the PoE port with a new one to verify that the PoE port is operating correctly. If the PoE port is not operating correctly, replace and port and send the fault information to Technical Support.
3. If the issue persists after the above procedures, collect the fault information, and contact H3C Support.

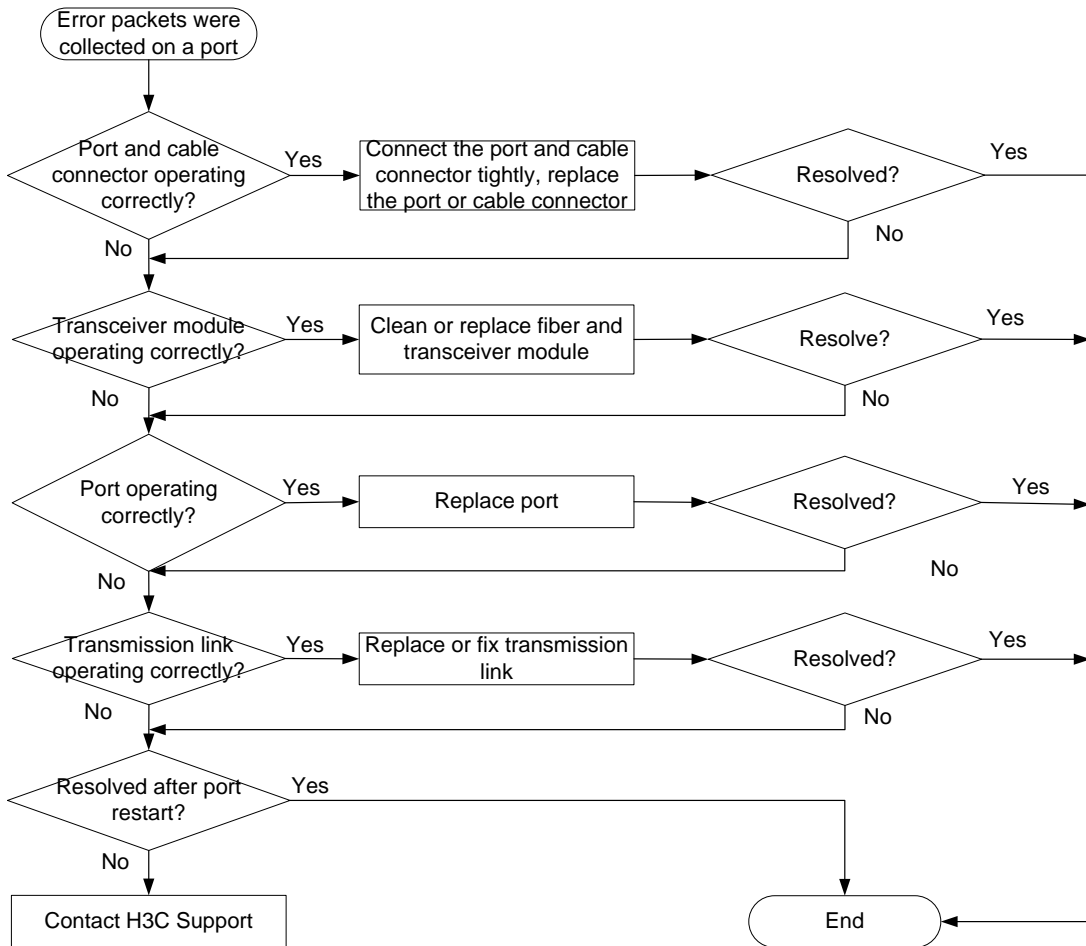
Error packets on a port

Symptom

Error packets were collected on a port.

Troubleshooting flowchart

Figure 65 Troubleshooting error packets on a port



Solution

1. Verify that the port and cable connector are operating correctly.
 - o Verify that the port and cable connector are connected tightly.
 - o Inspect the port for any abnormalities, such as foreign objects inside the port, bent pins, or malformation. If abnormalities are found, replace the port or transceiver module.
 - o Verify that the cable connector is not damaged. In case of any damages, replace it.
2. Verify that the transceiver module is operating correctly.

Use a fiber to connect the Tx and Rx ends of the port's transceiver module, and then refresh the traffic statistics page to see if the number of error packets increase. If the number increases, the transceiver module is not operating correctly.

- 3.** Replace the port with a new one to verify that the port is operating correctly.
Replace the port with a new one to verify that the port is operating correctly. If the port is not operating correctly, replace the port and send the fault information to H3C Support.
- 4.** Verify that the transmission link is operating correctly.
 - Use a tester to test the transmission link. Poor link quality or excessive optical signal attenuation can lead to packet errors during transmission.
 - Verify that the devices on the transmission link (including the fiber converter, adapter cable, and transmission device) are operating correctly. In case of any failures, replace the devices or link.
- 5.** Access the details page of the failed port, restart the link, and verify whether the port recovers.
- 6.** If the issue persists after the above procedures, collect the fault information, and contact H3C Support.