



Wireless AC & AP

FAQ

TABLE OF CONTENTS

Chapter 1 Device Management	1
1.1 How to log in to the device via PC when logging in for the first time?.....	1
1.2 What are the initial login user name and password of the device?	1
1.3 How to change the password of the device's web page?.....	1
1.4 How to reset the login password if I forget it?	1
1.5 Unable to log in to the WEB management interface of a new device, how to troubleshoot?	2
1.6 Difference Between Port Mirroring and Packet Capture Diagnosis	3
Chapter 2 Network Issue	4
2.1 WAN port sometimes fails to obtain an IP address?.....	4
2.2 No Internet access via WAN port?	4
2.3 If the static routing or policy-based routing configuration of multi-WAN is not effective, how to troubleshoot?	6
2.4 How to troubleshoot when the PC or other devices cannot get IP address via direct connection?	6
2.5 If the device can get an IP address from the gateway of the LAN but cannot access the Internet, check if the gateway is connected to the Internet.....	8
2.6 What should I do if my Internet speed is slow and games are lagging?.....	9
2.7 How to troubleshoot the issue of IPTV not playing normally?	10
2.8 Setting PPPOE dial-up for the device failed?	12
2.9 How to troubleshoot the issue of invalid PPPoE account package or actual effect not conforming to rules? ...	14
Chapter 3 AP Networking Issue	16
3.1 The AP is linked to the gateway device, but the APs are not displayed in the list. How can I check this?	16
Chapter 4 Wi-Fi Issue	19
4.1 Gateway devices cannot be found after adding WIFI. How to troubleshoot?.....	19
4.2 If you can see the Wi-Fi network but cannot connect to it, perform the following checks:.....	21
Chapter 5 Virtual Private Network	22
5.1 If the L2TP client on PC cannot dial up VPN, follow these steps to check:	22
5.2 How can I reconnect to the IPsec VPN after disconnection?	23
5.3 The VPN tunnel display exception with message indicating network exception caused connection failure.	24
Chapter 6 Internet Behavior Management.....	26
6.1 The device is connected to the gateway, but the IP address of the gateway is not displayed on the terminal. How can I troubleshoot?.....	26
6.2 How to troubleshoot when the phone does not pop up the portal page after enabling authentication?.....	26
6.3 How to troubleshoot when the web page shows that network is not secure?	27
6.4 The device can still access the Internet even if local cloud authentication is configured. How to troubleshoot?	27
6.5 The application control is not taking effect after it is enabled. How can I troubleshoot?.....	28
6.6 The custom flow control is not effective. How to check?	28
6.7 The access control rule is not effective.	29
6.8 Accessing the device is not allowed even if the firewall is not enabled because the network above the device is disconnected.	31

Chapter 7 Other Function Disabled	33
7.1 How to troubleshoot the issue that the Hik-Connect cloud service is offline?.....	33
7.2 The device already has an online upgrade package but cannot prompt for online upgrade. How to troubleshoot?	33
7.3 Error Occurred When SADP Modified Network Parameters	33
7.4 No devices displayed when all devices are migrated to Hik-Connect for Teams. How to troubleshoot?	34
7.5 The message "online upgrade" is displayed on the gateway page, but the online upgrade fails. How to troubleshoot?.....	35
7.6 How to troubleshoot when the gateway fails to issue an AP upgrade?.....	35

Chapter 1 Device Management

1.1 How to log in to the device via PC when logging in for the first time?

To log in to the device for the first time, connect your PC to the LAN interface of the device, and enter <http://192.168.188.1> or <https://192.168.188.1>.

1.2 What are the initial login user name and password of the device?

The device has no user name and password at the initial status. After activation, the login password is the one configured when activating the device.

1.3 How to change the password of the device's web page?

Click the small lock in the upper-right corner to edit the management PIN of the gateway device.



1.4 How to reset the login password if I forget it?

Press the Reset button on the front panel of the device to reset it.

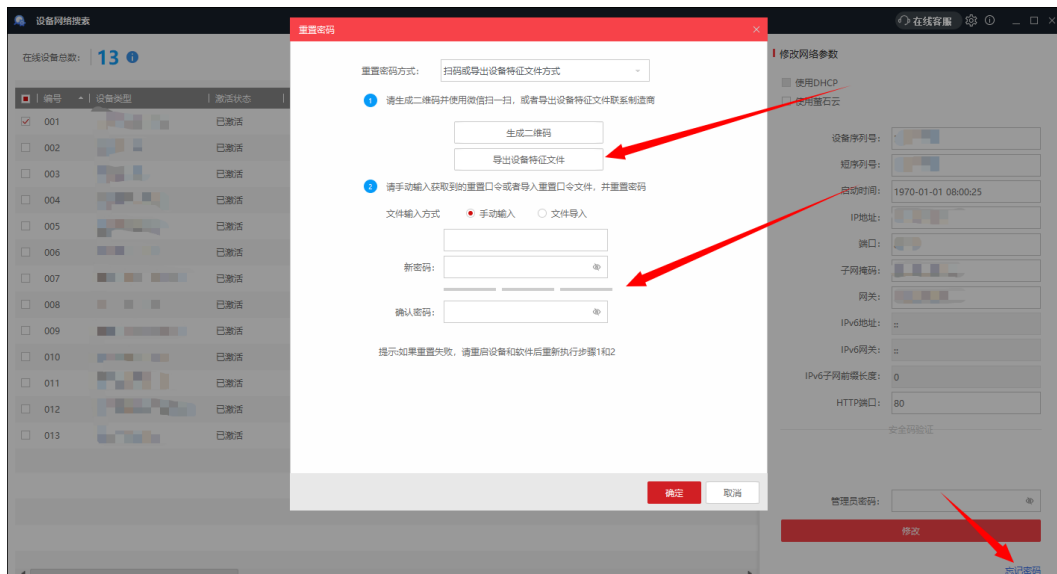
- Method 1: Restore Web Unactivated Status

Press and hold the Reset button for 5 to 10 seconds. When the status indicator flashes green rapidly, release the reset button. The device will be restored to unactivated status, and you can set the admin password again.

- Method 2: Change the password via SADP.

- 1) Check the box next to each device, tap Forget Password in the lower-right corner of the Parameters page, tap Export Device Feature File in the pop-up window, and select the storage location for the file. The manufacturer can then use the file to reset the device password.

- 2) The manufacturer will generate a reset PIN file according to this file. Users can import the reset PIN file into the pop-up window and enter the new password and confirm the new password. Tap OK. A message "Password reset successfully" will be displayed.



1.5 Unable to log in to the WEB management interface of a new device, how to troubleshoot?

Step 1 Check if the wiring method is correct.

Connect the PC's network interface to the device's LAN interface.

Step 2 Confirm the NIC settings of PC are correct.

When logging in to the Devices for the first time, the PC's nic can be set to "automatically get notified about IP address" or manually configure the IP address to 192.168.188.2 (any address within the range [192.168.188.2, 192.168.188.254] is acceptable), with the subnet mask set to 255.255.255.0.

Step 3 Check if the browser version is the recommended version.

It is recommended to use Internet Explorer 10 or later versions, Chrome 57 or later versions, and Firefox 35 or later versions to access the Web client.

Step 4 Check if the initial login address of the device is correct.

The initial login address of the device is <http://192.168.188.1> or <https://192.168.188.1>.

Step 5 Confirm that you entered the correct user name and PIN.

The device is in initial inactive status and has no user name or password.

1.6 Difference Between Port Mirroring and Packet Capture Diagnosis

Fault Diagnosis > Packet Capture Diagnosis: Capture network data packets to analyze the network communication process and diagnose network connection issues, data packet loss, etc. Common packet capture tools include Wireshark, tcpdump, etc.

[Fault Diagnosis >> Port Mirroring]: Refers to copying the packets passing through a specified port (source port or mirror port) to another specified port (destination port or monitoring port), enabling network data stream monitoring of the mirrored port. It is generally used to duplicate packets from a specified port to another port, allowing for centralized video monitoring of packets from multiple ports on a single port.

Chapter 2 Network Issue

2.1 WAN port sometimes fails to obtain an IP address?

- Dynamic IP Address

Step 1 Check if the network cable is connected correctly.

Check if the network cable is connected to the correct interface and the indicator of the interface lights up.

Step 2 Check if VLAN is configured for WAN.

Enter [Network Management>>WAN Configuration], view the advanced settings, and check if the 801.Q TAG is open.

Step 3 Check Upper Level If Condition Allowed

Check if the corresponding service is enabled and if there are any restrictions.

Step 4 Packet Capture and Protocol Analysis

Go to Fault Diagnosis > Packet Capture Diagnosis, capture packets on the WAN port, and check whether normal DHCP interaction exists.

- Broadband Dial-up

Step 1 Check if the network cable is connected correctly.

Check if the network cable is connected to the correct interface and the indicator of the interface lights up.

Step 2 Check the Dial-Up Status of the Broadband Dial-up Interface

Step 3 If it is a dial-up timeout, capture and analyze the interaction through [Fault Diagnosis >> Port Image].

2.2 No Internet access via WAN port?

Firstly, perform 3-ping test: PC pings the LAN address of the device, PC pings the WAN address of the device, and PC pings the WAN gateway address. Check where the ping fails.

- When the PC cannot ping the device's LAN address

Step 1 Check if the network cable is connected correctly.

Check if the network cable is connected to the correct interface and the indicator of the interface lights up.

Step 2 Computer settings issue:

Is the computer's gateway or mask configured correctly?

Step 3 Gateway API configuration issue.

Set the LAN IP address, subnet mask of the gateway correctly.

Step 4 Two NICs on the computer.

If the wireless NIC is enabled on your computer, disable it and test again.

Step 5 Hardware issue:

Change the LAN interface and network cable to test if you can access the Internet.

- PC cannot ping the WAN interface address of the device.

Step 1 Gateway API configuration issue:

Check if the WAN IP address, subnet mask, and gateway of the gateway are set correctly. For dial-up lines, check if the entered account and password are correct.

Step 2 Hardware issue:

Change the WAN interface and network cable to test if you can access the Internet.

Step 3 Is routing configured in the Layer-3 environment?

If the user's gateway is on the switch and whether a back-to-back route is configured on the switch.

Step 4 Center device filtering:

If not connected to the PC via the gateway directly, bypass the center device and test again.

- PC cannot ping WAN gateway address

Step 1 Check the network status to see if there is any problem.

Go to Test > Network Self-Test > Gateway Test to check the reason for the network disconnection and take corresponding actions.

Step 2 View line detection results.

Check If WAN Interface Is Online via Line Detection

Step 3 Check if the WAN network cable is connected properly.

Plug the external line directly into the computer to check if the internet is working, and test the dial-up line for any overdue fees.

Step 4 Hardware issue:

Change the WAN interface and network cable to test if you can access the Internet.

Step 5 Behavior Management Control

If you enabled ARP protection, MAC filtering and access control, or forced PPPoE dial-up?

- If All Three Are Pingable

Check if DNS is not configured or configured incorrectly.

2.3 If the static routing or policy-based routing configuration of multi-WAN is not effective, how to troubleshoot?

- Static Route

Step 1 Check the static route reachability status to see if the route is effective.

If it is unreachable, check if the current routing's outgoing interface can ping the next hop address.

Step 2 Check if the WAN interface gets network information.

Step 3 Check if policy-based routing is configured: The priority of policy-based routing is higher than that of static routing.

Step 4 Check if VPN Is Configured: The VPN Routing Priority Is Higher than Static Routing

- Policy-Based Routing

Step 1 Check if the destination address is for LAN test.

Step 2 Check WAN configuration to see if the WAN API can get IP address normally.

2.4 How to troubleshoot when the PC or other devices cannot get IP address via direct connection?

- Check if there is any wiring issue.

Handle Method: Gently shake the network cable to check if any device and gateway indicator turns green. If not, try another network cable or another network interface.

- The device connection port is IPTV port.

Handle it by first connecting to other network interfaces to get the IP address and log in to the gateway management page. Go to Network Management > IPTV Configuration to check if the port that cannot get the IP address is the IPTV port. If yes, please disable the IPTV service or connect to other network interfaces for use.

- The DHCP service of the device LAN port is disabled or the DHCP address pool is full.

Method 1: If other network interfaces can obtain an IP address, connect to another port. Tap "Network & Internet -> Network settings -> Change device adapter selection" on the device. Tap the connected NIC, then tap "Details" to view the IPv4 DHCP server. Enter the IPv4 DHCP server address in a browser to access the gateway management page. Go to "Network Management -> LAN Configuration" and confirm that the DHCP service for each VLAN is in the Open state.

Method 2: If you cannot get the IP address via any network interface, connect to the gateway LAN1 port, and set the device's static IP address as 192.168.188.1, and subnet mask as 255.255.255.0. In the browser, enter the IPv4 DHCP server address 192.168.188.1 to access the gateway's Network Management > LAN Configuration page, and confirm that the DHCP service is enabled for each VLAN.

Method 3: Check if the number of available IP addresses is 0. If yes, it means that the VLAN address pool is insufficient and you can increase the network segment size.

Method 4: Go to Network Management > LAN Configuration > DHCP Fixed Address Allocation, and check whether there are many static binding IP addresses. The existing fixed address will preempt the normal address pool. You can delete some of them.

VLAN ID	IP地址	子网掩码	DHCP服务	开始地址	可分配IP数	地址租期 (分)	VLAN隔离	备注	操作
默认VLAN	192.168.188.1	255.255.255.0	☒	192.168.188.1	253	30	☐	--	
访客VLAN	192.168.253.1	255.255.255.0	☒	192.168.253.1	254	30	☒	访客VLAN默认与...	

- The LAN port connected to the device is configured as closed WAN port or aggregation port.

The device is connected to a LAN interface that is configured as closed. Connect the device to other interfaces to get an IP address and log in to the gateway management page. Enter Device Network Management > Port Configuration to check if the port status is closed. If yes, configure it as open.

The LAN port connected to the device is configured as a WAN port. First, connect to another network interface to obtain an IP address and log in to the gateway management page. Go to the device's [Network Management >> WAN Configuration] page and check if the port status is set as WAN port. If so, please use another port.

The device is connected to the port of LAN aggregation. Connect other network interfaces to get IP address and log in to the gateway management page. Enter Device Network Management > Port Aggregation to check if the port status is aggregation. If yes, please use other ports.

- Other devices exist between the device and the network, which may cause the device to fail in accessing the network.

If the PC device and the AC device are connected to the same switch, the devices cannot get IP address. Make sure that the port VLAN of the AC device is configured correctly with the switch port VLAN. Make sure that the VLAN message is transparently transmitted by the intermediate node devices.

- Wireless Device Failed to Get IP Address

See Issue 4.1.

2.5 If the device can get an IP address from the gateway of the LAN but cannot access the Internet, check if the gateway is connected to the Internet.

- Check WAN Port Connection

How to handle: Refer to Issue 2.1.

- Check If The Port Configuration Is Correct

How to handle: Replug the port or switch to another port. Refer to Issue 2.4 (4).

- Set Proxy DNS Server

Handle by: Go to Network Management > LAN Configuration > DNS Proxy to check if DNS proxy is enabled. You can disable the DNS proxy or switch to a DNS address that can resolve domain names, such as 8.8.8.8 and 114.114.114.114.

- Check If Security Management Is Enabled on Gateway Device

Handling Method

Go to Device Management > ARP Protection > ARP Binding to check if the ARP binding is enabled on the gateway device. If it is enabled, disable it and set static MAC-IP binding for your device.

Go to Security Management > MAC Filtering, tap "Open" / "Close" to enable or disable MAC filtering, and tap "Add" / "Delete" to add or delete devices' MAC addresses.

Go to the Gateway page and check if there is any rule that restricts the access of the terminal device(s) to the Internet. If so, disable the rule or delete it.

- Check If Forced PPPoE Dial-up Is Enabled

Handling Method: Go to Advanced Management > PPPoE, and check if the Forced PPPoE Dial-Up is enabled. If it is, disable it, or add the device IP address in Exclusion IP Management.

- Check if Parental Control Rules Exist

Handling Method

Use the Hikvision Cloud Network Mobile Client to bind devices and check if the Parental Control rules limit the devices from going online during this period. If yes, delete or edit the rules to allow the devices to go online.

- Check if Portal Authentication Rule Exists

Handling Method

Go to Security Management > MAC Filtering, and check if there is any related configuration in Portal Authentication. If yes, delete the rule or allow access after authentication.

● Wireless Issue

How to handle: Refer to the answer of Issue 4.1.

2.6 What should I do if my Internet speed is slow and games are lagging?

● Check If Connection Limit Is Enabled

Handling Method:

Go to Advanced Management > Connection Limit to check if the rule is configured to limit the number of user's internet access connections.

● Port Configuration Issue

Handle it by checking if the speed of the port is negotiated to 10M in the Network Management > Port Configuration page.

配置设备直连端口，点击保存后需要刷新页面

端口配置

点击可选中端口，再次点击将取消选择

LAN1

LAN2

LAN3

LAN4

LAN5

LAN6

LAN7

LAN8

WAN2

WAN1

连接 聚合组编号

端口配置

已选端口 + 所有端口 清空

未选择端口，请先至左侧面板添加端口

启用端口 ☒

速率 自动

双工 自动

启用流控 ☐

保存

端口状态

刷新

端口	端口连接状态	端口开关	配置双工/速率(M)	实际双工/速率(M)	流控配置状态	流控实际状态
LAN1	连接	开启	自动/自动	全双工/1000M	关闭	关闭
LAN2	断开	开启	自动/自动	--	关闭	关闭
LAN3	断开	开启	自动/自动	--	关闭	关闭
LAN4	断开	开启	自动/自动	--	关闭	关闭
LAN5	断开	开启	自动/自动	--	关闭	关闭
LAN6	断开	开启	自动/自动	--	关闭	关闭
LAN7	断开	开启	自动/自动	--	关闭	关闭
LAN8	断开	开启	自动/自动	--	关闭	关闭
WAN2	断开	开启	自动/自动	--	关闭	关闭
WAN1	连接	开启	自动/自动	全双工/1000M	关闭	关闭

● Enable Flow Control Settings

Handle Method: Go to Behavior Management > Traffic Settings > Traffic Control, and check if the user is not allowed to access Internet or if WAN port speed limit is enabled. Or go to Behavior Management > Traffic Settings > Custom Policy, and check if some IP addresses are limited.

● The device is connected via PPPOE and the account package is configured.

Handle Method: Go to Advanced Management > PPPoE Server Configuration > Online Users to check if the user is offline. Check if the account in Advanced Management > PPPoE Server Configuration > Account Management has activated a data plan and if the network data is insignificant.

2.7 How to troubleshoot the issue of IPTV not playing normally?

- Check if the VLAN of the configured IPTV upstream/downstream port (check the downstream port in single-line mode and check both upstream and downstream ports in dual-line mode) is modified.

Method 1: Delete IPTV configuration and reconfigure it in Network Configuration > IPTV.

- Check if the upstream/downstream port (downstream port in single-line mode; upstream and downstream ports in dual-line mode) is changed to WAN port – multiple WANs are configured in WAN configuration.

Method 1: Delete IPTV configuration and reconfigure it in Network Configuration > IPTV.

- Check if the AP bound to IPTV is offline by comparing the online APs in Wireless Management > AP List with those in Network Management > IPTV.

Method 1: Connect to the AP that is bound with IPTV service and log in again.

Method 2: Go to Network Configuration > IPTV and reconfigure the IPTV service and select online APs.

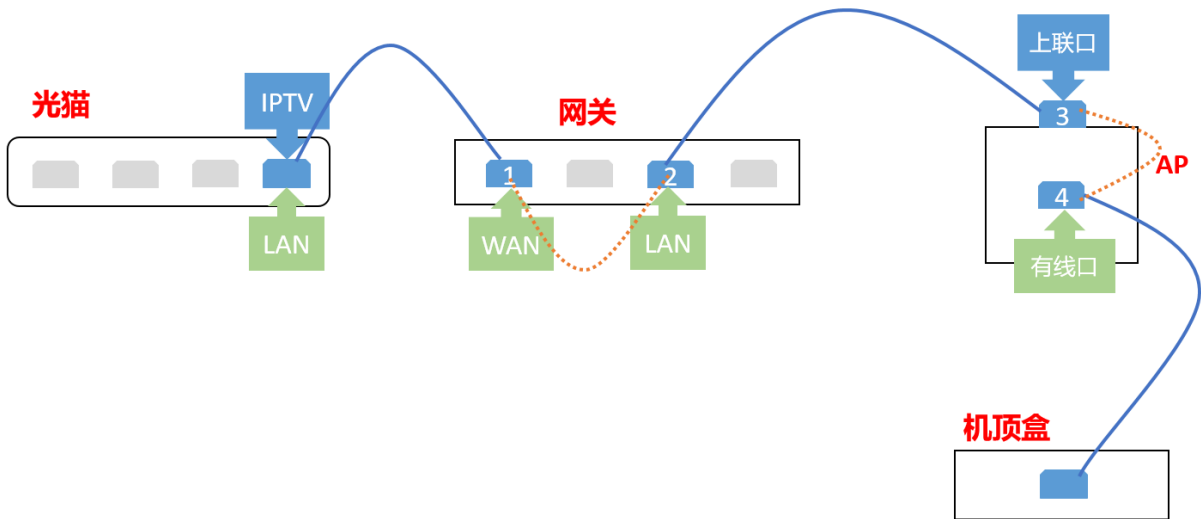
- Check if the VLAN of the wired port of the bound AP is modified.

Method: Go to Network Configuration > IPTV, delete the IPTV configuration, and then reconfigure it.

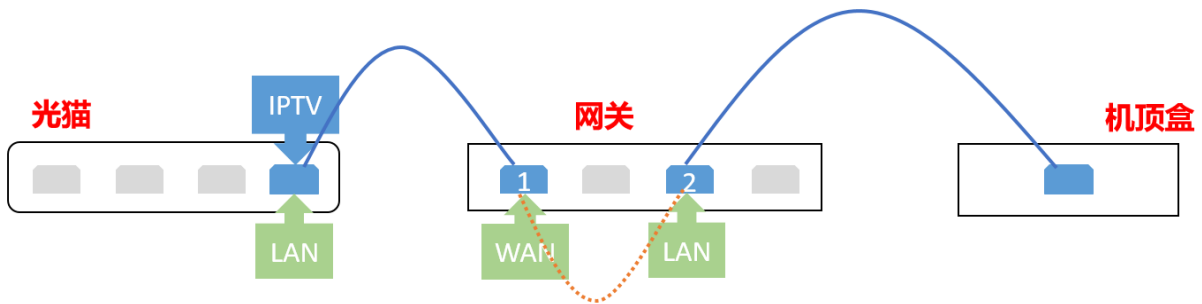
Method 2: In Wireless Configuration > AP Wired Port, change the VLAN of the wired port of the AP bound to IPTV to be the same as that of IPTV.

- Check If Wiring Matches the Diagram

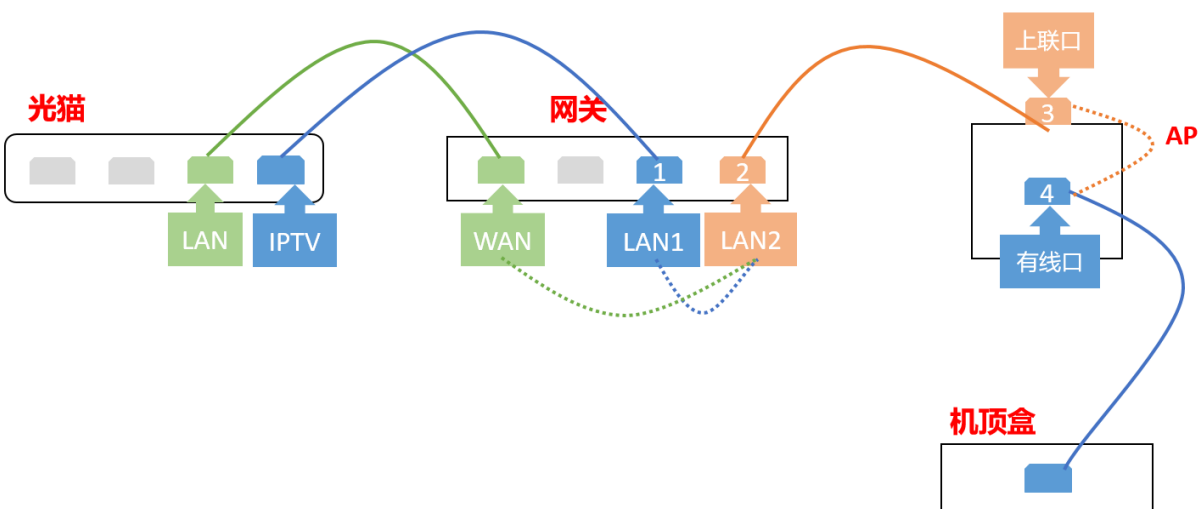
When you select single-line mode and choose AP (single-line mode/cable box connected to AP), the wiring order is: optical modem — gateway WAN — gateway LAN — AP — cable box.



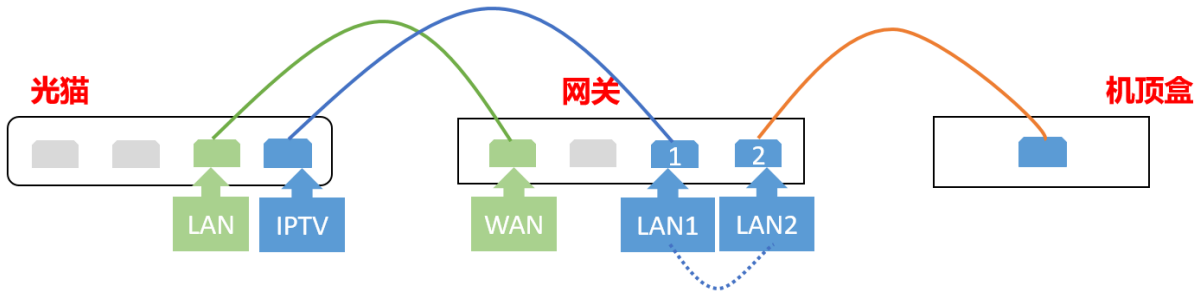
If you select Single Line Mode (AP/STB Directly Connected to AC), the wiring order is: optical modem — WAN port of the gateway — LAN port of the gateway — STB.



When you select the dual-line mode and choose AP (dual-line mode/top box connected to AP), follow this wiring order: optical modem — LANa of the gateway — LANb of the gateway — AP — top box.



If you select dual-line mode and do not select AP (dual-line mode / set-top box connected to AC router directly), the wiring order is: optical modem — LANa of the gateway — LANb of the gateway — set-top box.



2.8 Setting PPPOE dial-up for the device failed?

- The VLAN of the bound PPPOE server and that of the port mismatch.

Go to Advanced Management > PPPOE Server Configuration > Global Configuration, and check:

Enable PPPOE Server?

If the VLAN bound to PPPOE is consistent with the VLAN where the customer is located? If not, you can enter the WEB [Network Management >> Port VLAN Configuration] to check the port VLAN configuration, and switch the VLAN where the customer is located to the VLAN bound to the PPPOE server;

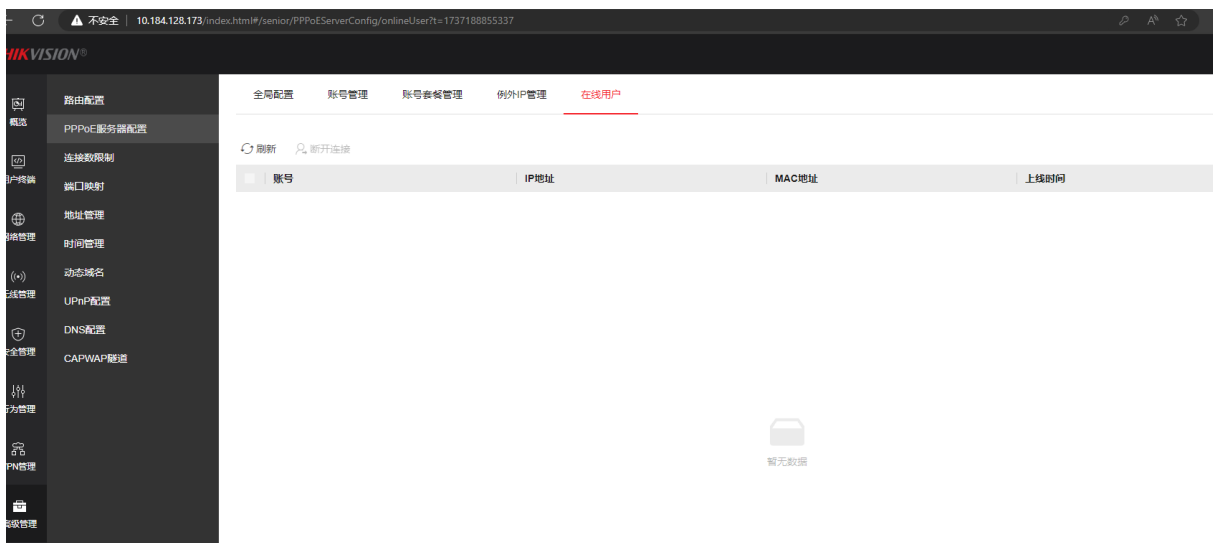
The screenshot shows the 'PPPoE服务器配置' (PPPoE Server Configuration) page. The '全局配置' (Global Configuration) tab is active. The '启用' (Enable) toggle is turned on. The '强制PPPoE拨号' (Force PPPoE dialing) toggle is turned off. The '本地地址' (Local Address) is set to 11.22.33.99. The '地址池IP范围' (Address Pool IP Range) is set to 11.22.33.100 - 11.22.33.250. The 'VLAN' dropdown is set to 'VLAN22'. The 'DNS服务器' (DNS Server) and '备选DNS服务器' (Backup DNS Server) fields are empty. The '最大未应答LCP包数' (Maximum number of unanswered LCP packets) is set to 10. The '认证方式' (Authentication Method) section shows PAP, CHAP, MSCHAP, and MSCHAP2 all checked. A '保存' (Save) button is at the bottom.



- Check if the PPPoE account is available. If the account status is closed, you cannot pass the authentication with this account.



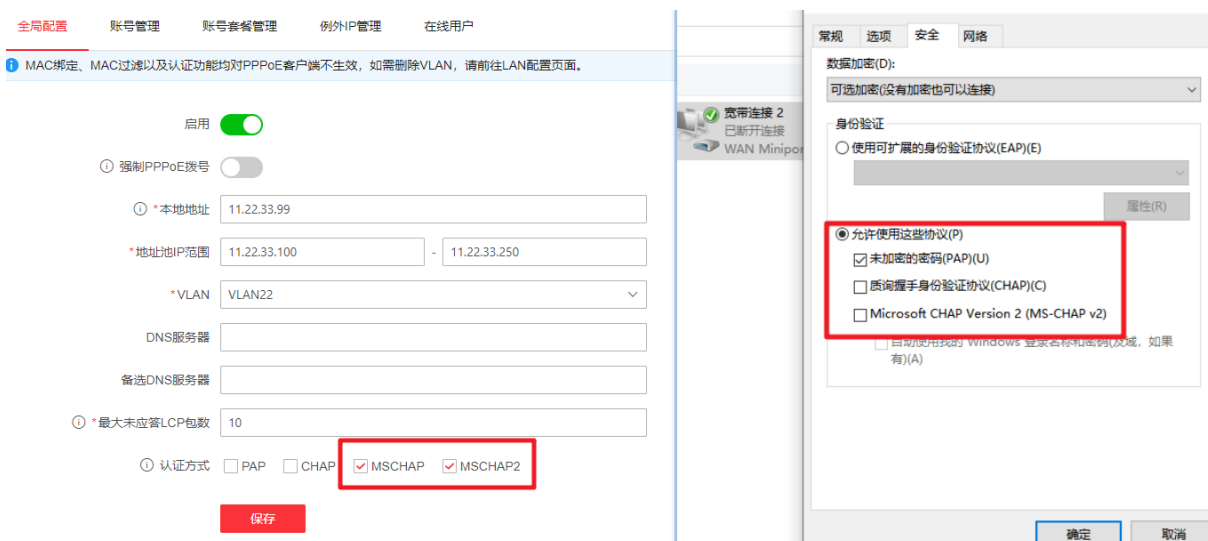
- Check the PPPoE client list to see if other devices are using the same account. One account of PPPoE server on the gateway is only allowed to log in one client. If another client has logged in with this account, try again with another account.



- Check the maximum number of concurrent PPPoE clients supported by the current device model. When the concurrent connections have reached the limit, no more clients can be connected.



- Check if the supported authentication methods of NIC configuration match with that configured on PPPoE server. If not, edit the NIC configuration and try again.
- Please check if portal authentication rules are configured on the PPPoE VLAN [Security Management -> Portal Authentication], and if so, delete the portal authentication rules.



2.9 How to troubleshoot the issue of invalid PPPoE account package or actual effect not conforming to rules?

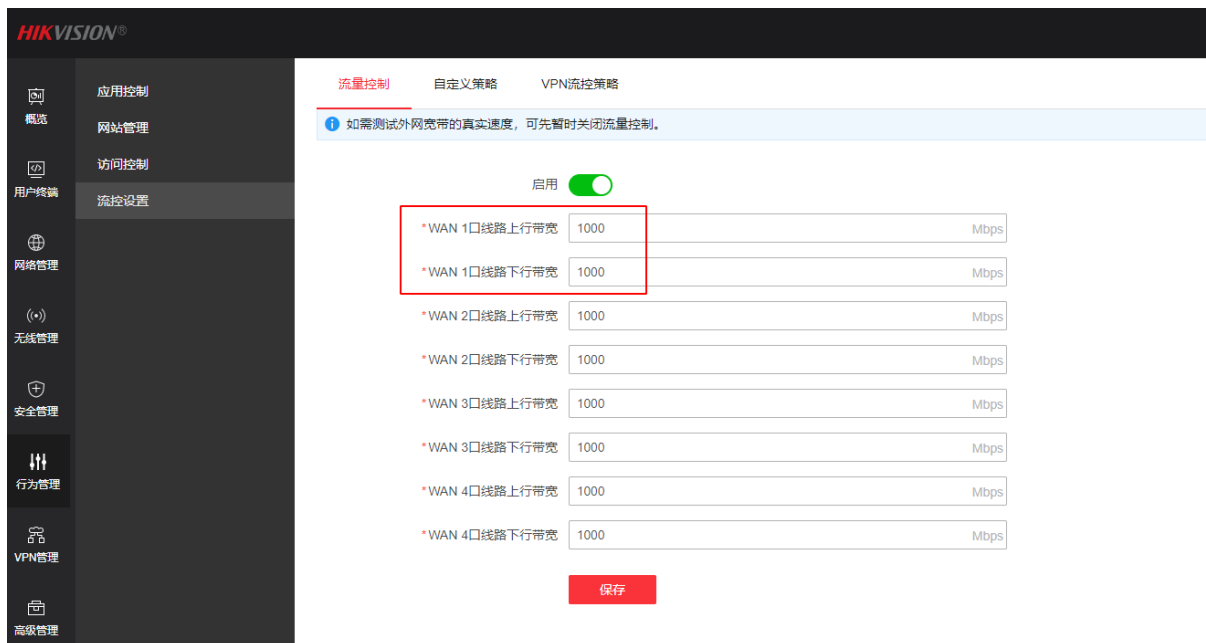
- Check if the WAN Outbound Interface of Actual Device is the Same as the Current Set API Interface in the Package.

Go to Advanced Management > PPPoE Server Configuration > Account & Package Management to check if the WAN interface of the applied package is consistent with that of the device. If not, edit the WAN interface of the applied package to be the same as that of the device. If you are not sure which WAN interface the device's traffic goes out from, you can set the WAN interface to All WAN Interfaces.



● Check If WAN Port Downstream and Upstream Bandwidth Limit Is Configured on the Traffic Control Page

Enter the gateway device page [Behavior Management >> Network Data Control], check if the WAN port upstream and downstream bandwidth limits are configured on the Network Data Control page. The account set and intelligent flow control have no priority; when configured simultaneously, all rules are issued and take effect according to the insignificant configuration. You can adjust the upstream and downstream bandwidth of intelligent flow control or the account set based on the requirement.



Chapter 3 AP Networking Issue

3.1 The AP is linked to the gateway device, but the APs are not displayed in the list. How can I check this?

- The PoE power supply of the port is not enabled.

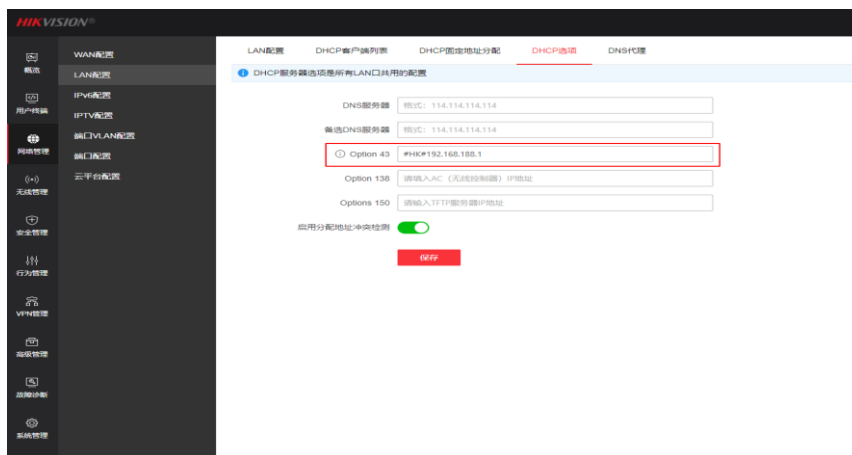
Handle method: Enter the gateway overview page to view the port information and check if the PoE power status of the port is powered off. If the icon of the port is in gray, it means that the port is not powered. Tap Advanced Management >> PoE Power to open the PoE switch button.

- The AP cannot get an IP address.

How to handle: Refer to Issue 2.4.

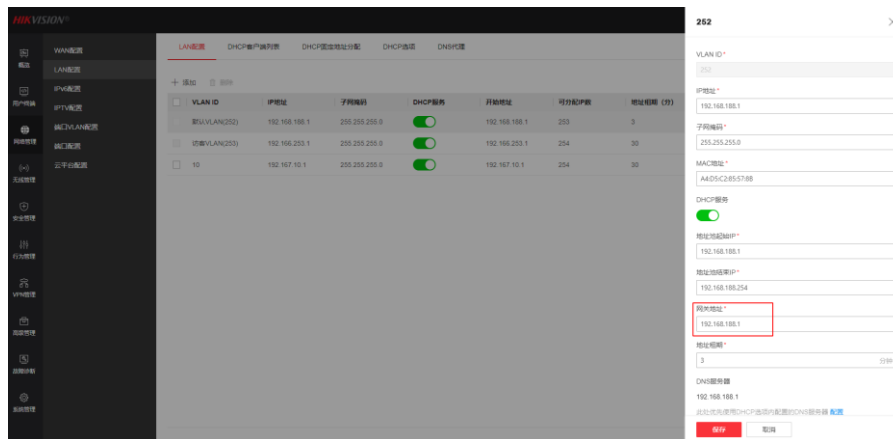
- Configure Gateway via Option 43

Handling method: On the gateway management page, navigate to [Network Management >> LAN Configuration >> DHCP option], check if option43 has been configured. If configured, Delete the option43 Configuration and Save, then restart the AP Devices. View the option43 Configuration page as follows:



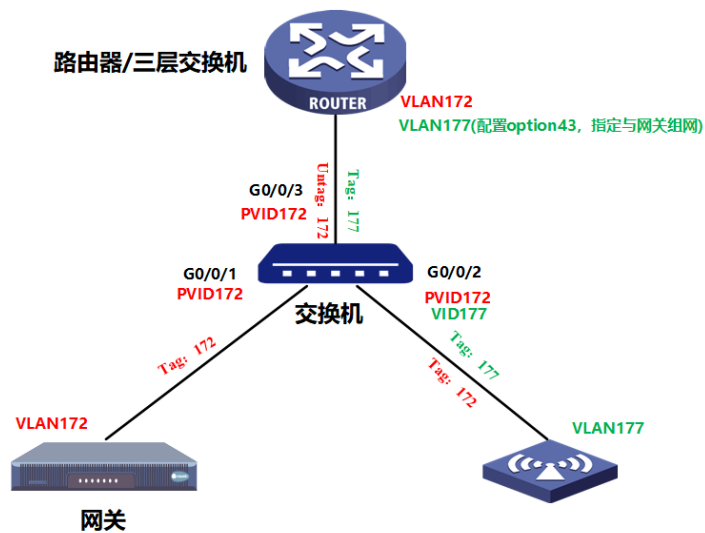
- Gateway Address Unreachable

Handling Method: Go to Gateway Management page, and enter Network Management > LAN Configuration to check if the gateway address of VLAN configuration is reachable. If not, go to Fault Diagnosis > Network Tools > Ping Communication to use the Ping tool to ping the gateway address and view the Ping result. If the address is unreachable, change it to a reachable gateway address. The gateway address configuration page is as follows:

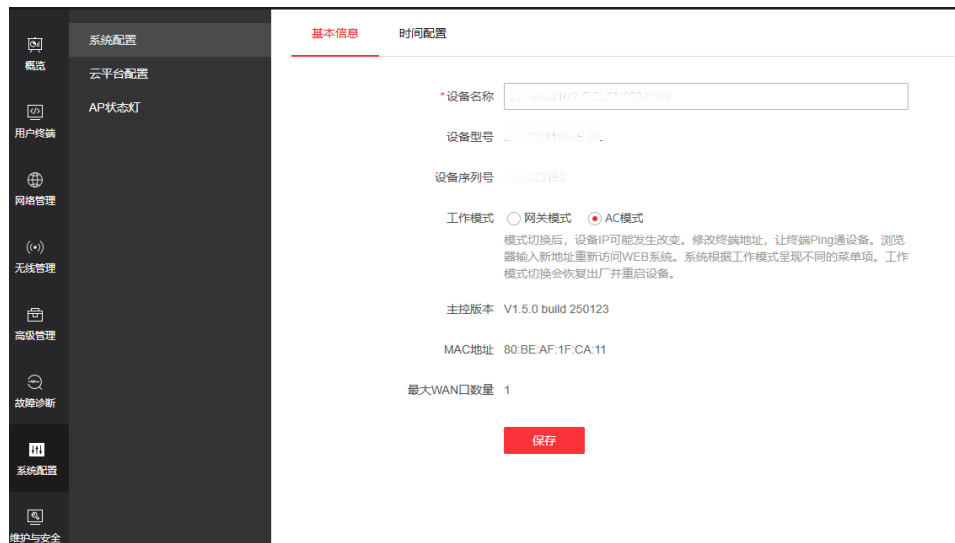


● The Work Mode of Gateway Does Not Match the Actual Scene

Handling method: When the gateway and AP are in the same LAN, go to Gateway Management > System Configuration > System Management to check if the work mode is AC mode. If not, switch to AC mode, and then restart the device. The following diagram shows the network topology.



Pattern View Mode



● Gateway Model and AP Model Not Match

Handle by checking the labels of the gateway device and AP device to confirm that both the gateway and AP are of special model (ZD) or from the same series (DS-3).

The AP configured with static IP address cannot access the gateway network.

Handle by pressing and holding the reset button on the AP to restore it to factory settings.

● The AP Connection Port is the IPTV Port.

Handle: Connect to other network interfaces to get the IP address and log in to the gateway management page. Go to Network Management > IPTV Configuration to check if the port that cannot get the IP address is the IPTV port. If yes, please disable the IPTV service or connect to other network interfaces.

● The network cable between the gateway and AP is abnormal.

Handle the problem by testing the network cable with a line tester or replacing the cable to check if it is caused by a line issue.

Chapter 4 Wi-Fi Issue

4.1 Gateway devices cannot be found after adding WIFI. How to troubleshoot?

- Check the AP list to ensure that there is an AP connected to the gateway and successfully added to the system.

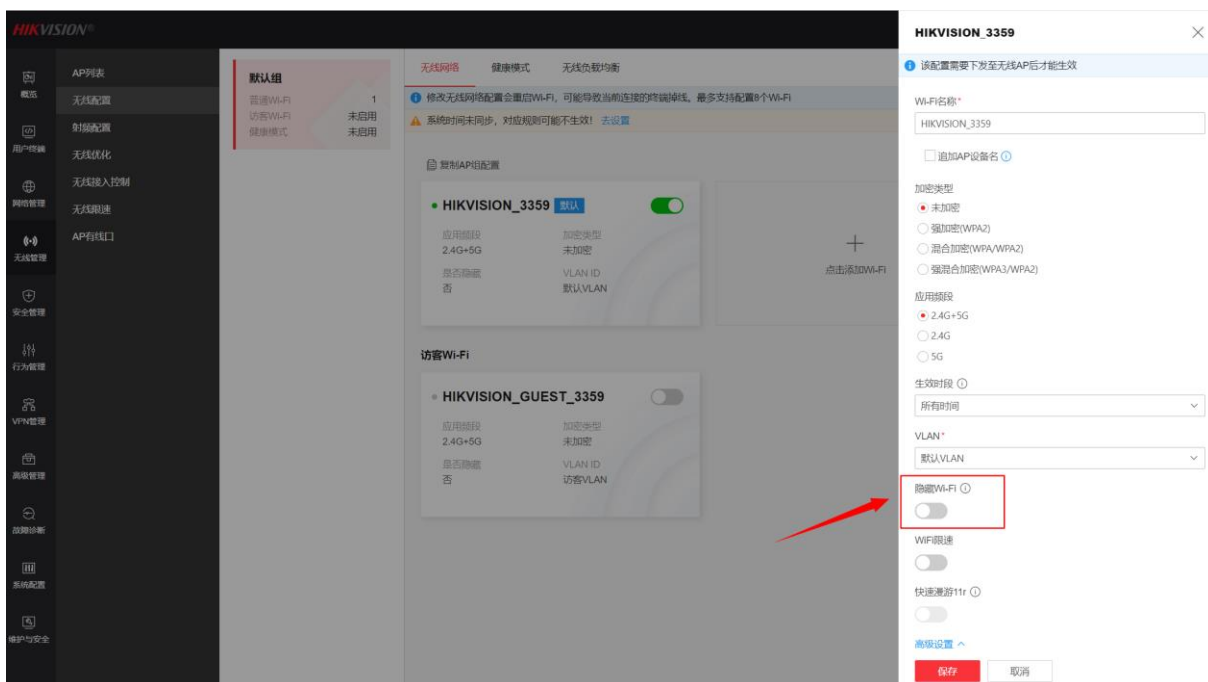
Handle it as follows: Refer to 3.1 .

- Make sure the terminal device is within the Wi-Fi coverage of the AP.

Handling Method: Approach the AP device and check if the WIFI can be found.

- Check If Corresponding Wi-Fi Hides Wi-Fi

Go to Wireless Management > Wireless Configuration, and tap WIFI to check if the Hide Wi-Fi button is enabled. If it is enabled, you can manually search for and add devices, or disable this function.



- Check If Current Health Monitoring Mode Is Enabled

Go to Wireless Management > Wireless Configuration > Health Mode, and disable the health mode.



● Check If AP Is in the Corresponding Wi-Fi Configuration AP Group of Gateway Device

If not, move the AP to the Wi-Fi configuration group manually. Check the AP devices in the AP List page under Wireless Management > AP List and make sure that the Wi-Fi of the same group is consistent with that in the Wireless Configuration page.

● Check If Independent Wi-Fi Configuration Is Enabled on AP

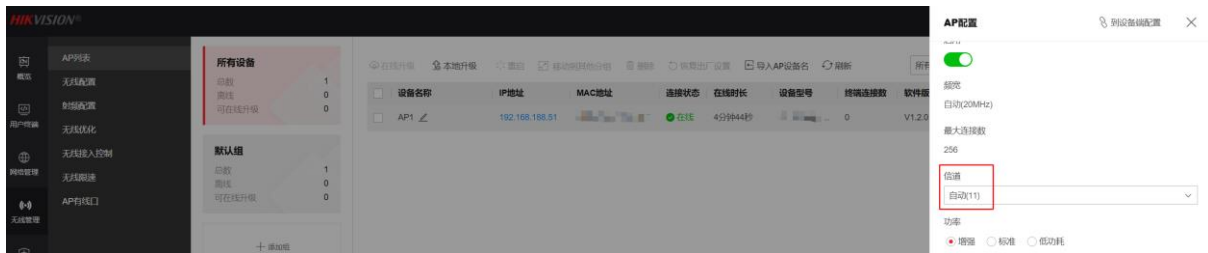
Go to Wireless Management > AP List, tap Configure in the operation column, and tap Wireless Configuration to check if independent Wi-Fi configuration is enabled.



● Check If RF Switch of AP Is Enabled Normally



● If there are too many wireless devices in the network and the interference is strong, you can change the RF channel to an available one, and then select Manual Verification on the terminal to add Wi-Fi.



4.2 If you can see the Wi-Fi network but cannot connect to it, perform the following checks:

- Make sure the Wi-Fi password is correct.

Go to Wireless Management > Wireless Configuration, tap WIFI to open it, and confirm that the password is correct.

- Check the DHCP function of the gateway to ensure that the wireless terminal can get an IP address.

Refer to Issue 2.4 (3).

- Check the wireless VLAN ID in Wireless Configuration and make sure the gateway provides DHCP service in this VLAN.

Confirm that the port VLAN ID, WLAN VLAN ID, and Wi-Fi VLAN ID are correct in the switch configuration.

- Check the switch configuration between the gateway and AP to ensure that the switch can forward VLAN data of the corresponding Wi-Fi.
- Make sure that the middle device is configured correctly, and the AP and AC are directly connected to the switch. Wireless devices should get IP address normally. Make sure that the port VLAN of AC and switch are configured correctly. Make sure that the VLAN message can be transmitted transparently on the middle node device.
- Go to Wireless Management > Wireless Control Access to check if the MAC address of your phone is in the blocklist. If yes, you can delete the device from the blocklist or allowlist. If the page shows Allowlist, you can add the MAC address of your phone to the allowlist so that it can access the Internet.

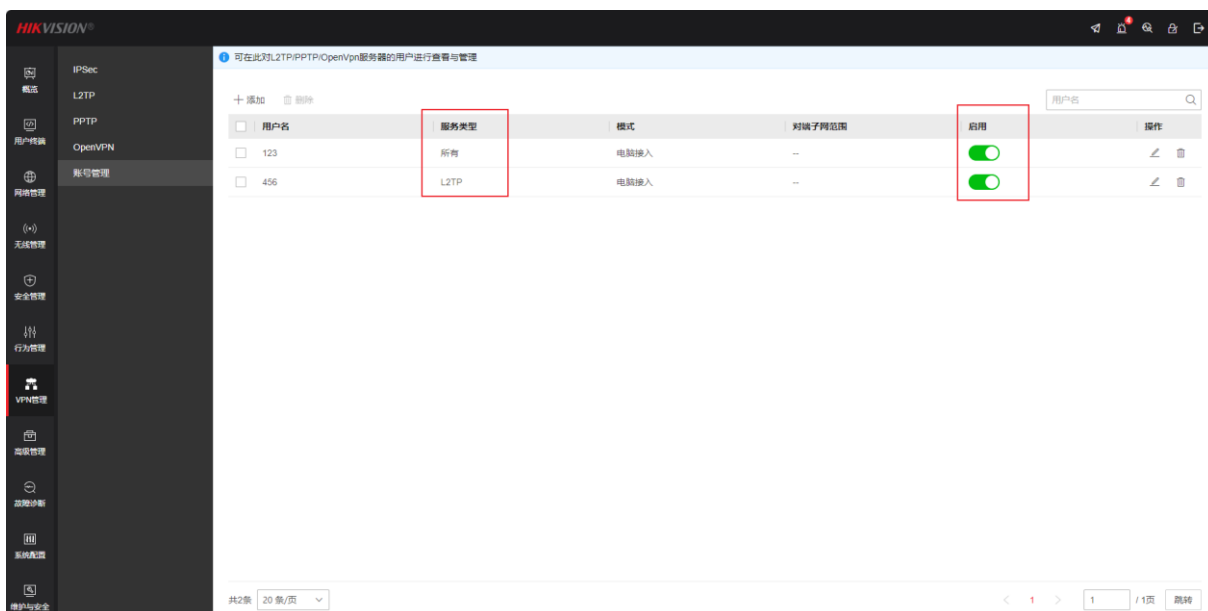
Chapter 5 Virtual Private Network

5.1 If the L2TP client on PC cannot dial up VPN, follow these steps to check:

- Check if the L2TP server has enabled the VPN account provided for you.

Go to VPN Management > Account Management, enter the account name filter field, and check the Enable status.

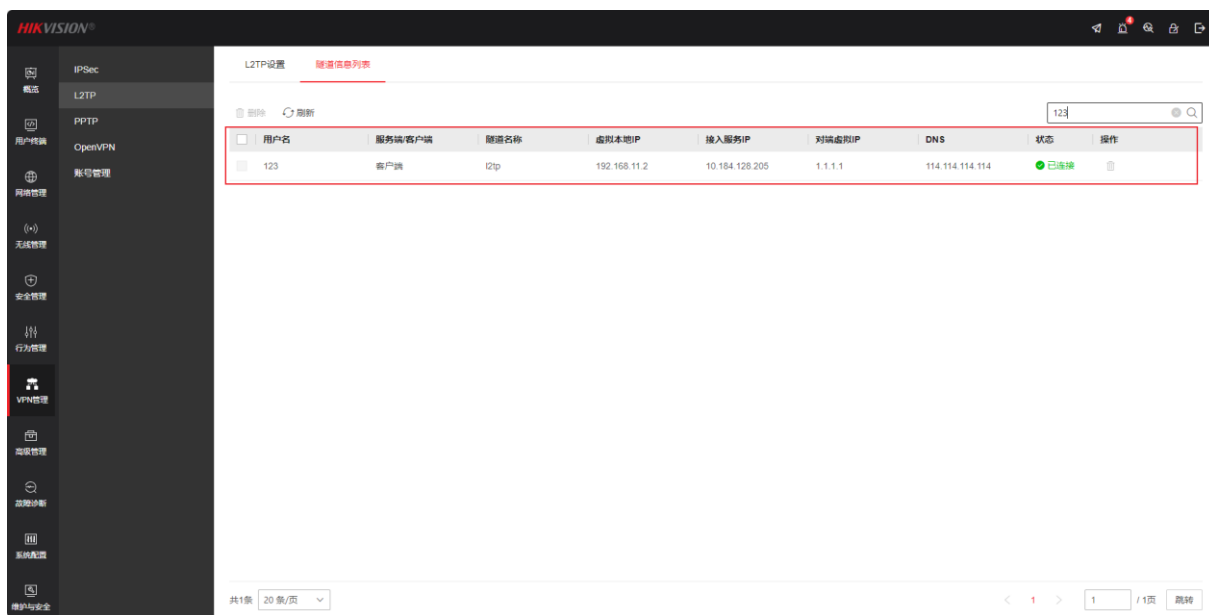
Check If Service Type Supports L2TP Client



- Check if the VPN account provided by L2TP server has been used by client access.

Go to VPN Management > L2TP > Tunnel Information List, filter the account name, and check if the account is in use.

The single L2TP account provided by the server is only for use by one client.



● Check If the Entered VPN Account Name and PIN for PC Dial-Up Are Correct

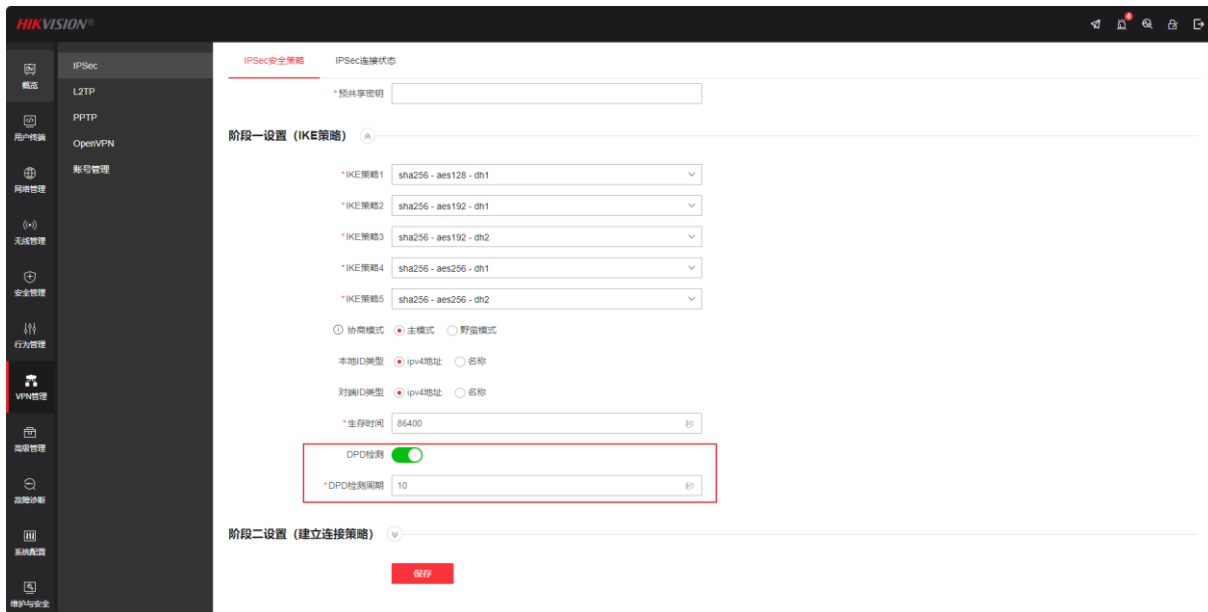
Enter the account name and PIN of the VPN again. The steps are as follows:

Tap the network icon in the lower-right corner of your PC desktop (i.e., the taskbar), right-click on the L2TP client name, and select Connect in the pop-up menu. In the window that pops up, enter the user name and password provided by the L2TP server, and then tap Connect.

5.2 How can I reconnect to the IPsec VPN after disconnection?

The common cause is that the DPD function in the IPsec policy is not enabled. To enable it, follow these steps:

- In the web page of the device, go to VPN Management > IPsec > IPsec Security Policy.
- Tap the edit icon in the Operation column of the corresponding IPsec policy to enter the page for editing IPsec policy.
- Tap <Phase 1 Settings (IKE Policy)> to show the Phase 1 Settings Configuration items.
- Tap Enable in the DPD Test Configuration item to enable DPD test and enter the DPD test cycle.
- Tap Save to complete the configuration.



5.3 The VPN tunnel display exception with message indicating network exception caused connection failure.

- Check the tunnel information list and hover the mouse over the abnormal status to view the cause of the issue.



Common Exception Statuses

Connecting in progress: At this time, the VPN client has just started and is connecting.

WAN port disconnected: The WAN port bound to the VPN client has no network information. Check the physical status and DHCP service status of the upstream link.

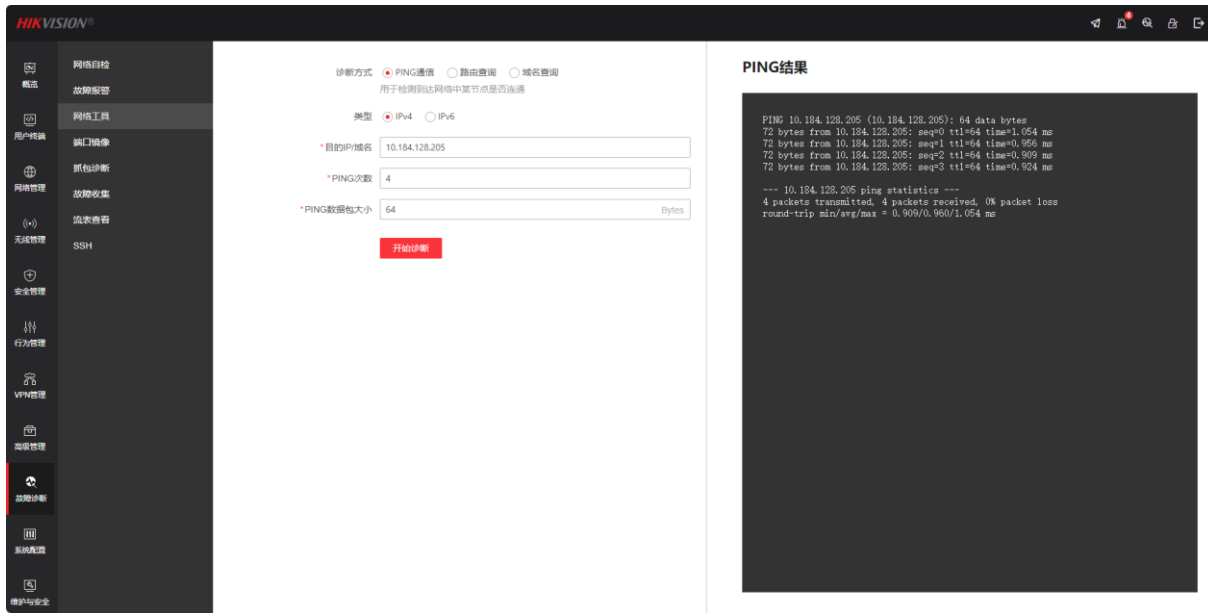
Network exception: The VPN client cannot access the server normally. Check if the server address is reachable and check the server address pool as well as whether the number of access clients has reached the limit.

Configuration exception: Check if there is any critical configuration inconsistency between the client and server, such as different encryption algorithms.

Not Synced: Device Time Not Synced

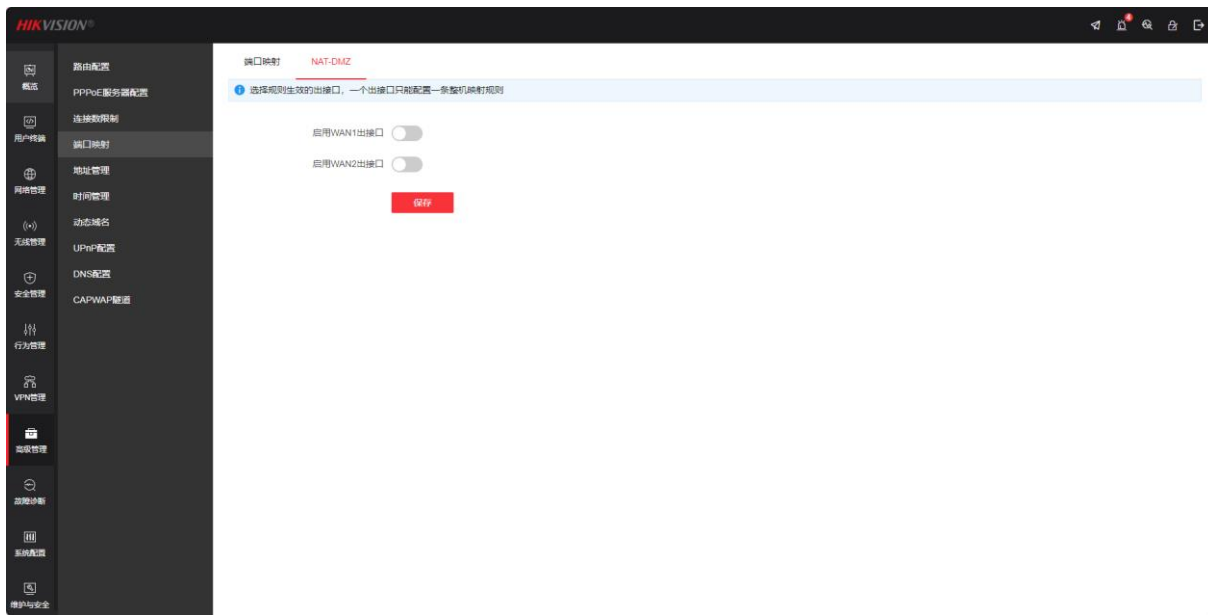
- Check if the server address in VPN configuration is reachable.

Go to Fault Diagnosis -> Network Tools -> PING Communication to check if the server IP address in VPN configuration is reachable. If not, please confirm the server network connectivity.



● Check Whether Enabling Port Mapping/DMZ Function on VPN Server/Client Affects Negotiation

Go to Advanced Management -> Port Mapping and check if the port mapping or NAT-DMZ function is enabled. If the port mapping is enabled, the negotiation message of VPN will be tampered with and redirected, which may cause negotiation failure.



Chapter 6 Internet Behavior Management

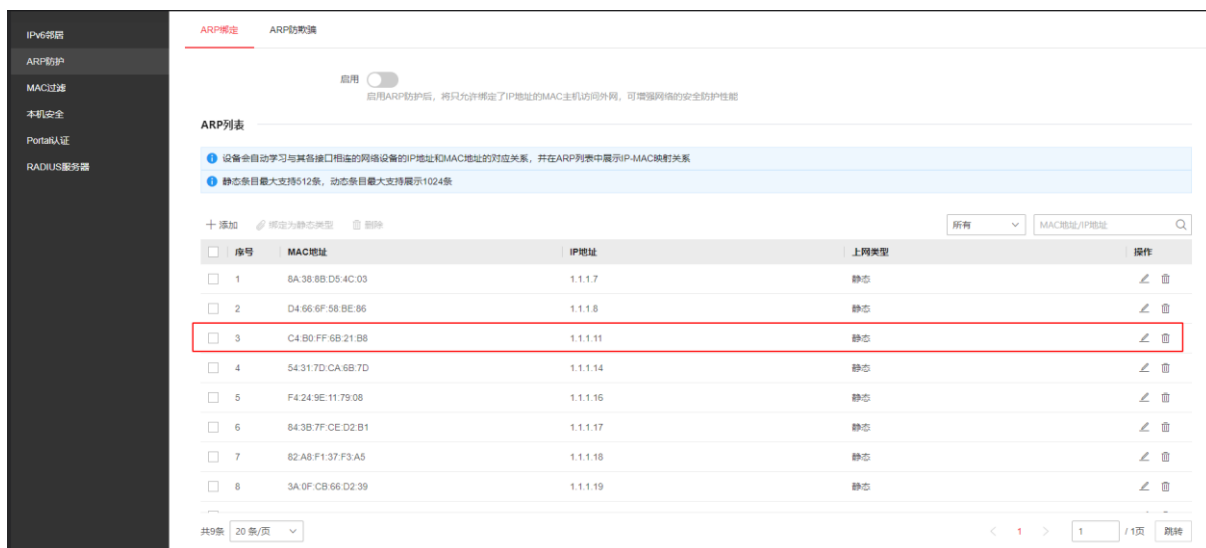
6.1 The device is connected to the gateway, but the IP address of the gateway is not displayed on the terminal. How can I troubleshoot?

- Check if the IP address of the terminal device is in the same network segment as that of the gateway device.

If the terminal's IP address and the gateway device are not in the same network segment, communication between them will fail, and the gateway cannot get the terminal's IP address. In this case, you need to change the terminal's access mode to Dynamic or set its network segment to be the same as that of the gateway.

- The terminal IP address is statically bound to another device.

If the IP address is bound to other MAC addresses and the terminal uses the bound IP address, the terminal cannot access the Internet or communicate with the gateway. On the web page, go to Security Management > ARP Protection > ARP Binding, and check whether the terminal IP address is bound to other MAC addresses. If it is, unbind the IP address from the MAC address or switch the terminal IP address.



6.2 How to troubleshoot when the phone does not pop up the portal page after enabling authentication?

Check the following one by one.

Step 1 The pop-up window cannot be automatically displayed on your phone due to the model of your phone.

Solution: Manually visit the http/https tab, reconnect to Wi-Fi, or forget Wi-Fi and reconnect.

Step 2 The Gateway Is Not Connected to WAN

Handling Method: Go to the Gateway Management page, click Fault Diagnosis -> Network Self-Test -> Test Now, and check if the network connection status is normal. If it shows that WAN port public network connection exception occurs, please check the WAN network.

Step 3 Incorrect terminal DNS or gateway configuration.

Handle method: Check the default gateway and IPv4 address on your phone or computer. If you are not sure whether they are correct, set them to automatically obtained.

Step 4 The terminal is not in the VLAN or IP address range that requires authentication.

Handle by: Go to the Gateway Management page > Security > Portal Authentication, and check if the IP address or VLAN of the terminal is in the list of authenticated IP addresses or VLANs. If not, the terminal does not need to be authenticated and can access the Internet directly.

Step 5 The gateway enabled other functions which limit this terminal.

Handle by checking if there is any rule that limits the access of the terminal in ARP protection, MAC filtering, access control, and wireless access control functions, and delete such rules if found.

Step 6 Other Function Conflicts With Authentication

Handle by: Check if the IP address range in IPsec, L2TP, PPTP, OpenVPN, and PPPoE functions of VPN Management conflicts with that of Portal Authentication. If yes, configure other Portal Authentication IP address range / VLAN.

6.3 How to troubleshoot when the web page shows that network is not secure?

Accessing HTTPS tab causes

How to handle: Tap Continue to access the web page or go to http://... .

6.4 The device can still access the Internet even if local cloud authentication is configured. How to troubleshoot?

The cloud network, easy debugging, and unified network management platform are not configured with cloud authentication.

How to handle: Log in to the above-mentioned platform and configure the Portal Authentication Template. (Only for devices with debugging function.)

6.5 The application control is not taking effect after it is enabled.

How can I troubleshoot?

Check If the Terminal IP Address Is in the Range Specified by the Rule

The application control rule only takes effect for terminals with IP addresses in the set range. If the terminal's IP address is not in the range, you can edit the rule to change the IP address range, or create a new application control rule for the terminal's IP address.

Confirm if the current time is the effective time.

The application control will only be effective within the set time period. If the current time is not in the effective time period, you can edit the managed time period to include the current time period.

Check if Application Control Rules Are Enabled

Applying control rules will take effect only after you enable them.

Is the Application in Disabled List

The application control only takes effect on the specified applications and does not affect other applications. You can edit the range of disabled applications. If the preset applications do not meet your requirements, you can set custom applications based on the five-tuple information of network data, and then select them in the application control rule.

地址组/IP地址范围	受管理的时间段	禁用应用/禁用应用组	备注	启用	操作
188	所有时间 >	斗鱼 虎牙 哔哩哔哩 爱奇艺 腾讯视频 抖音 快手 西瓜视频 优酷 搜狐视频	test	☒	
1.1.1.1-2.2.2.2	工作日 >	微信 Soul 陌陌 知乎 探探 最右 书旗小说 快看漫画 YY 微博	--	☒	

6.6 The custom flow control is not effective. How to check?

Check If Terminal IP Is Within Speed Limit Rule

The flow control rule only takes effect for terminals with IP addresses in the specified range. If the terminal's IP address is not in the range, you can edit the rule to change the IP address range, or create a new flow control rule for the terminal.

Check If Flow Control Rule Is Effective

Check if the flow control rule is in inactive status. If yes, check if the network cable of the application interface is loose or if the upper-level network is normal.

Confirm If The Application Interface Of The Rule Is The WAN Port Of The Gateway Device

The flow control rule only takes effect on the traffic forwarded from the specified API. If you are not sure which API forwards the traffic, set the API of the flow control rule to All APIs.

流量控制 自定义策略 VPN流控策略									
+ 添加 - 删除									
☐	策略名称	地址组	带宽模式	上行带宽 (Mbps)	下行带宽 (Mbps)	应用接口	启用	生效状态	操作
☐	A	192.168.188.1 - 192.168.188.25	共享	10	20	所有WAN口	☒	已生效	编辑 删除
☐	B	192.168.188.1 - 192.168.188.25	共享	10	20	所有WAN口	☒	已生效	编辑 删除

6.7 The access control rule is not effective.

Check the following:

- If the network is not connected, first check if other internet blocking functions in the network security area are enabled.

Access Control is a sub-function of the Security Subsystem. Its priority is lower than that of ARP Protection, MAC Filtering, and Mandatory PPPoE Dial-up, but higher than that of Access Control, Parental Control, and Portal Authentication.

Go to the ARP Protection page of the gateway device and check if ARP protection is enabled. If it is, check if the device in the ARP list is dynamic or static. If it is dynamic, you can bind it to static.

ARP防护 启用 ☒

启用状态下，只允许指定了IP地址的MAC主机访问外网（内网不作限制）

出接口 默认VLAN, 访客VLAN [编辑](#)

ARP列表

设备会自动学习与其各接口相连的网络设备的IP地址和MAC地址的对应关系，并在ARP列表中展示IP-MAC映射关系

静态条目最大支持256条，动态条目最大支持展示512条

ID	MAC地址	IP地址	上网类型	操作
1	6c:b1:58:ba:a8:8b	192.168.188.182	动态	编辑

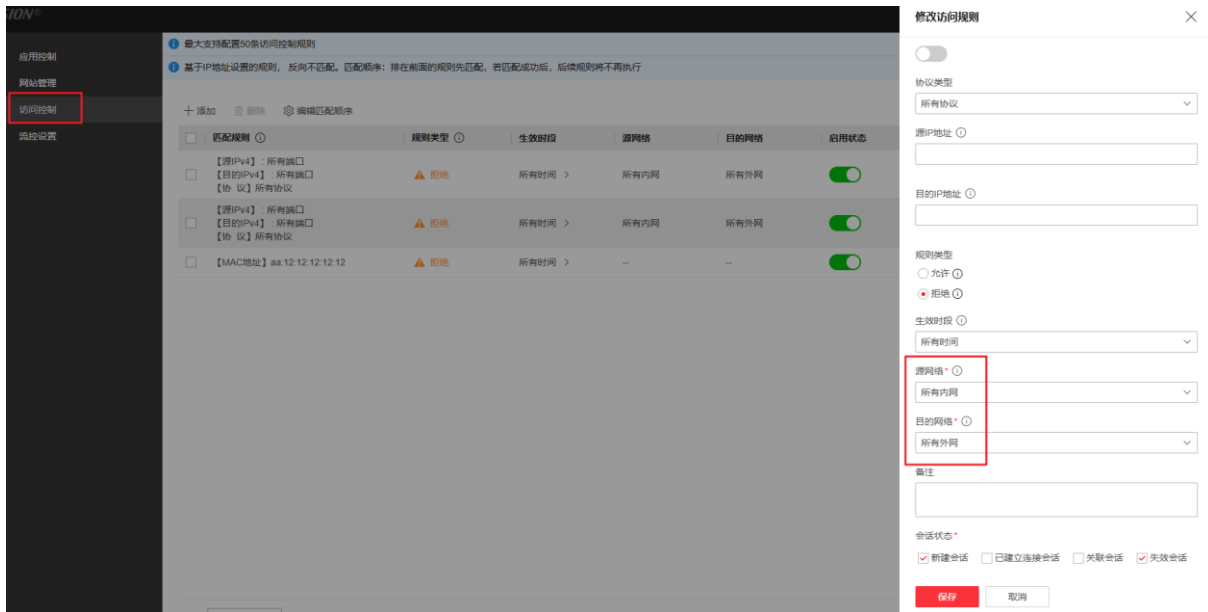
b. After step an is completed, check if the network is connected. If not, go to Security Management > MAC Filtering, and check if MAC filtering is enabled. If so, disable it and check if the network is connected.



c. If the connection is still not established after step b, go to Security Management > Authentication Configuration to check if the authentication is enabled. Disable it and try again.



- Go to Behavior Management > Access Control to view the rule configuration and check if it is consistent with the actual network topology. Pay special attention to whether the source network domain and destination network domain are consistent with the topology. In addition, note that when source IP address, address group, source network, or destination network is configured, these configurations will take effect together.

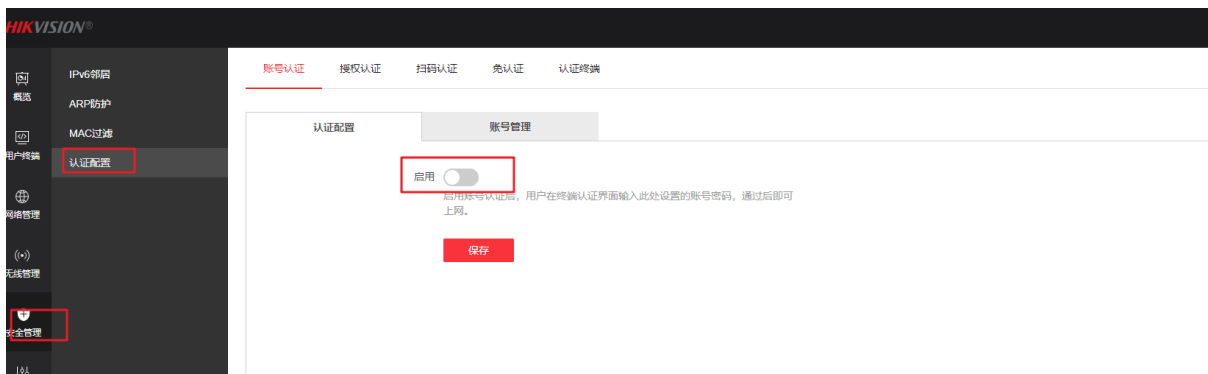


Device Cannot Access the Internet

According to step 2.5, check if the network itself is normal;

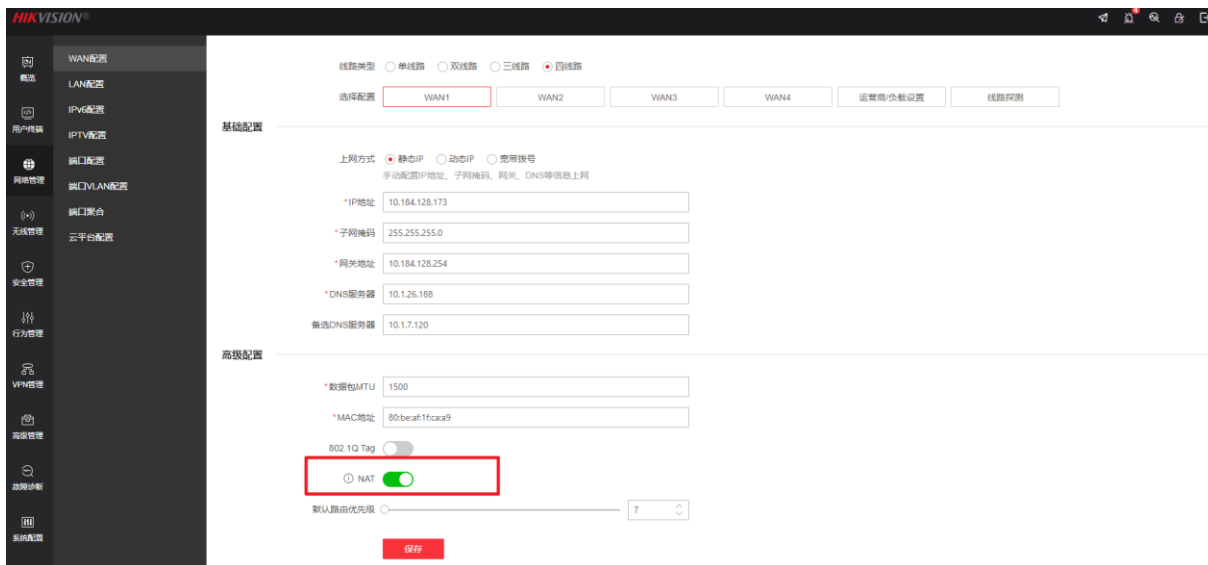
6.8 Accessing the device is not allowed even if the firewall is not enabled because the network above the device is disconnected.

Step 1 Firewall function (such as ARP protection, MAC filtering, access control, and parental management) is not enabled, but you cannot access the upper-level network. Check if cloud authentication configuration exists first.



Go to Security Management > Authentication Configuration, and disable cloud authentication.

Step 2 If the device is still unreachable after Step 1, you can check if WAN port NAT is enabled. It is usually enabled by default but may be disabled. If it is not enabled, the device will be unreachable.

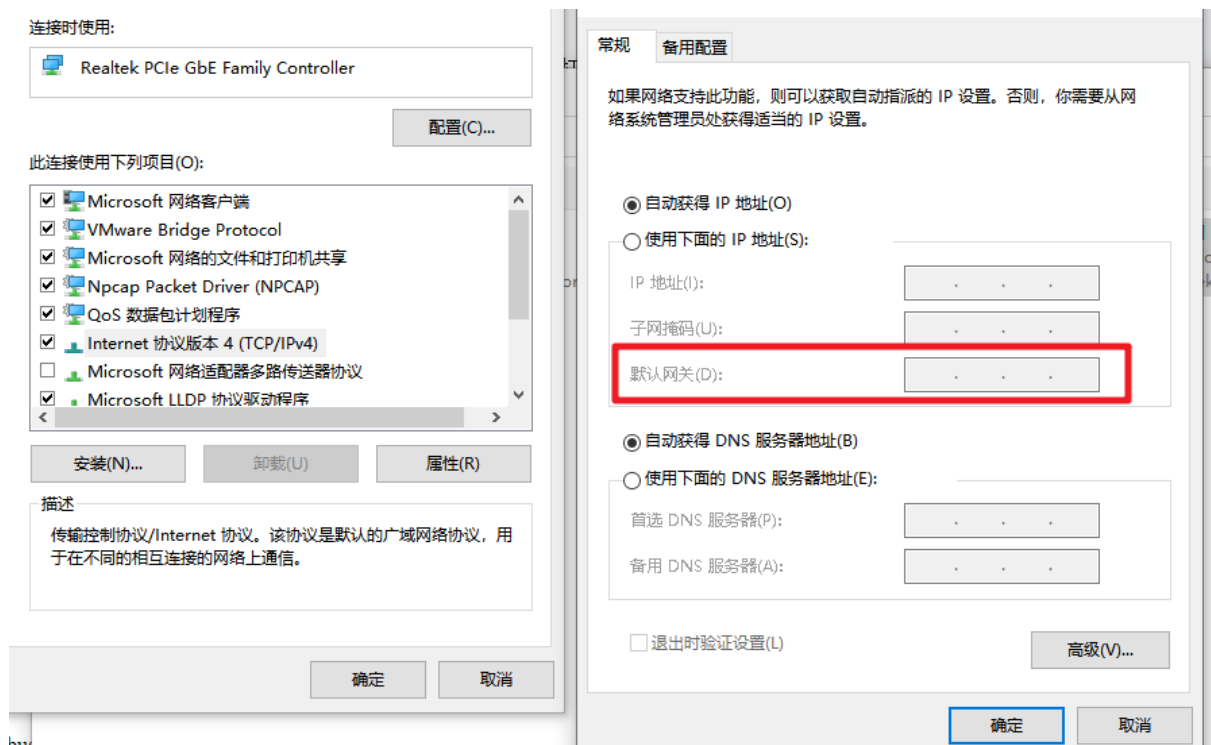


Step 3 Check if Parental Control is enabled on the device.

Log in to the Cloud Network or Easy Debug APP from your mobile phone to check if the device is restricted outside of the allowed internet access period. If it is indeed restricted, you can remove the corresponding terminal from the rules.

Step 4 Check if the device connected to the gateway is configured with the gateway and got IP address.

Set the NIC IP address acquisition mode to Dynamic. Refer to Issue 2.4/2.5 for details.

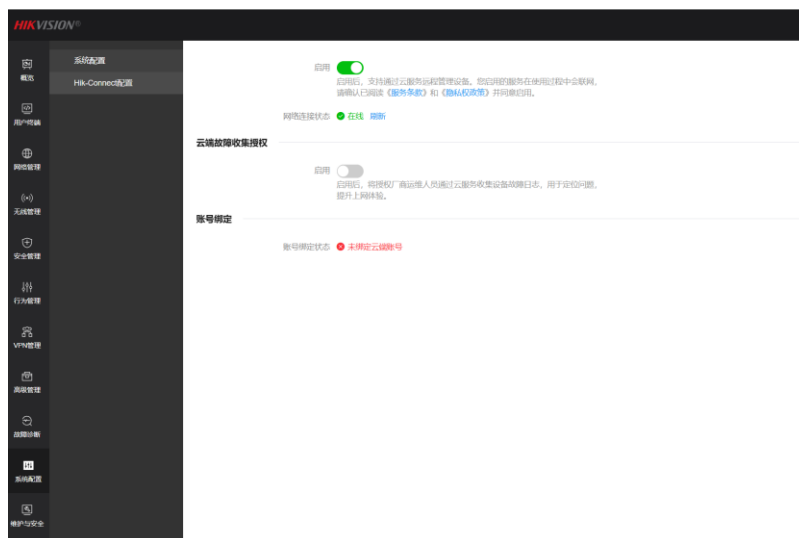


Chapter 7 Other Function Disabled

7.1 How to troubleshoot the issue that the Hik-Connect cloud service is offline?

- Check if the cloud service is enabled.

Go to System Configuration > Hik-Connect Configuration to check if the switch is enabled. If it is disabled, please enable it.



- Check if there is any issue with the WAN cable connection.

Gently shake the network cable to check if any green light is on for the gateway connected to the optical modem or upstream device. If not, try another network cable or WAN port.

- Check if WAN upstream is connected to Hik-Connect server.

Go to Web Client > Tools > Network Diagnosis > Network Tool, and ping litedev.hik-connect.com to check if the server IP address is reachable.

7.2 The device already has an online upgrade package but cannot prompt for online upgrade. How to troubleshoot?

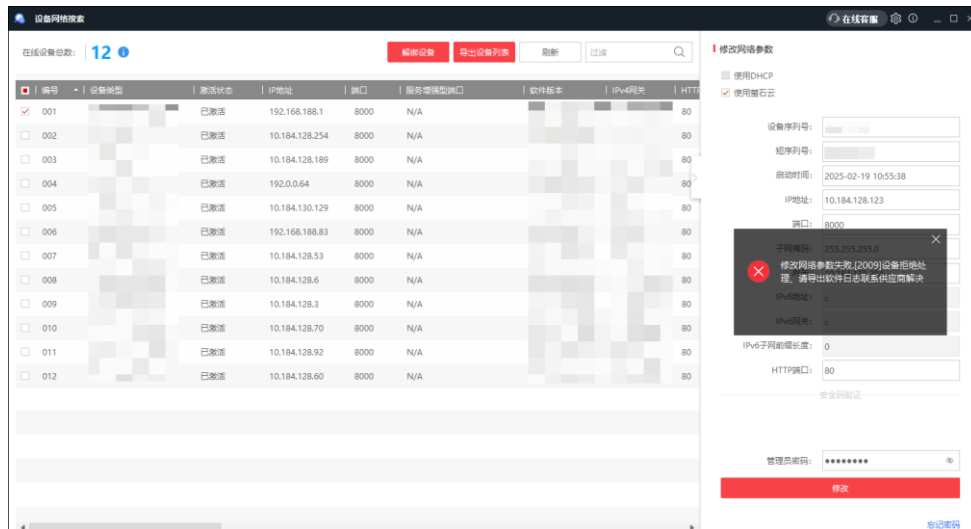
Check if the Hik-ProConnect account is online.

Refer to 7.1 Issue for details. After the gateway cloud service switches from offline to online, wait for 5 to 30 minutes.

7.3 Error Occurred When SADP Modified Network Parameters

- Check If Parameter Is Valid

For example, the IP address and gateway address should be in the same network segment; whether the IP address conflicts with the WAN port IP address or the server IP address and address pool. The error message is as follows:



- Check if the Admin Password Entered Is Correct.
- Check if the network cable is properly connected.

7.4 No devices displayed when all devices are migrated to Hik-Connect for Teams. How to troubleshoot?

- Check if the network cable of the connected device is properly connected.

Whether the network cables for directly connected devices such as AP, IPC, and switch are loose, or whether the network cables for the switch group connected under AC are loose;

- Whether the device is added by other accounts of other APPs.

Log in to the WEB page corresponding to different devices [Wireless Management >> Cloud platform Configuration]. Check if it is bound. If it is bound, you can unlink it using the SADP Tools and then Add it again. If it is not bound, Please contact customer service or Reset the device to resolve the issue.

- Check if the sub device supports cloud access.

You can log in to the web page corresponding to different devices [wireless management >> Cloud platform Configuration] to check if there is a Cloud tube plane function. If none, it does not support Cloud. 7.6 Local upgrade Message upgrade failure, how to troubleshoot.

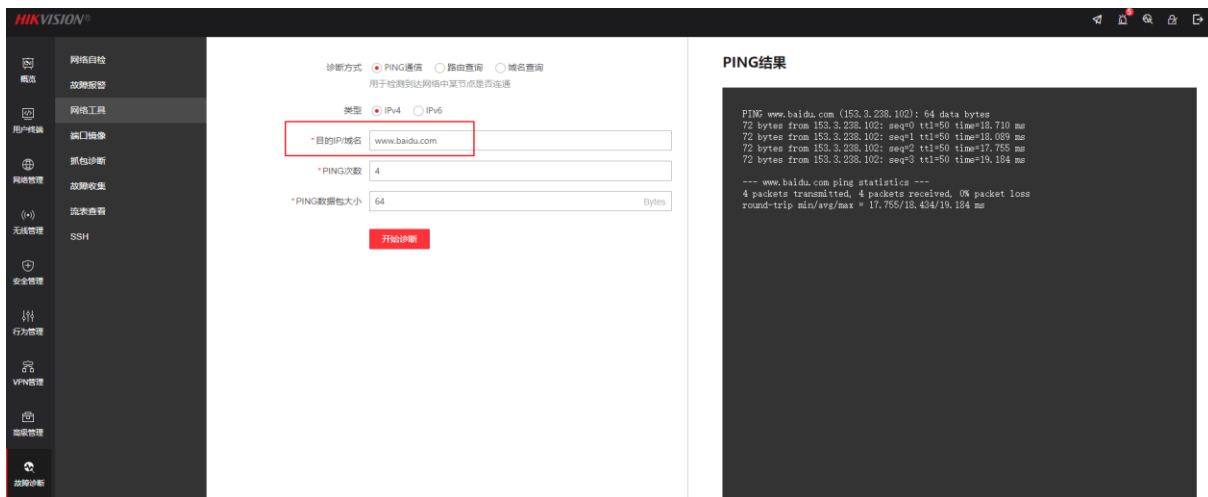
- Check if the upgrade package is correct and suitable for this model.
- Check If There Is Enough Memory for Upgrade (About 20 MB)
- Check if the network cable is disconnected.

7.5 The message "online upgrade" is displayed on the gateway page, but the online upgrade fails. How to troubleshoot?

- Go to Network Management > WAN Configuration to check if the WAN port IP address is normal.



- If the WAN port IP address is normal, go to Fault Diagnosis > Network Tools, enter www.baidu.com as the destination domain name, tap Start Diagnosis, and check if the WAN port of the current gateway device can access the Internet normally.



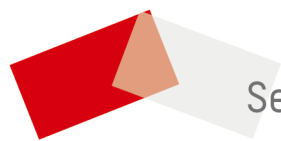
7.6 How to troubleshoot when the gateway fails to issue an AP upgrade?

Go to Wireless Management > AP List, and tap the Retry button in the pop-up window of upgrading failure. You can see the specific reason for upgrade failure on the right side.



The following reasons may cause the upgrade to fail:

- The server is disconnected from the AC. Check if the network connection between the AC and AP is normal. If it is the online upgrade of AP, check if the WAN port is connected to the Internet normally. After excluding the exception environment problem, try again.
- If the device is disconnected during device upgrade and an AP goes offline when the AC router issues the upgrade command to the AP, check the connection between the AC router and the AP.
- Repeated upgrade: Before the AP is remotely upgraded by the AC, it has triggered an upgrade and the upgrade is ongoing.



See Far, Go Further