Smart Managed Router

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (*https://www.hikvision.com*). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY

RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Applicable Models

This manual is applicable to the Smart Managed Router.

Symbol Conventions

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

Symbol	Description
Note	Provides additional information to emphasize or supplement important points of the main text.
Caution	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
Danger	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

TABLE OF CONTENTS

Chapter 1 First Use Device

To activate the access controller gateway (hereinafter referred to as "gateway" or "device") and complete configuration on the management page, please follow the steps below.

1.1 Connect Device

Note

- The appearance of devices of different models may vary. The picture here is for reference only.
- Make sure the gateway is connected to ground and powered on. For details, refer to the Quick Start Guide.

Step 1 Use a network cable to connect the WAN port of the gateway to the upstream network (e.g., the LAN port of the modem).

Step 2 Use a network cable to connect the AP to the LAN port of the gateway.

1.2 Activate Device

1.2.1 Wired Connection

Step 1 Connect PC to the LAN port of the gateway via a network cable.

Step 2 Set the PC to automatically get an IP address (recommended) or manually configure its IP address in the same network segment as 192.168.9.1 so that it can access the gateway's management page.

Step 3 Check the proxy service settings on your PC. If your PC is using a proxy server to access the Internet, you should disable the proxy service first.

Step 4 Run a web browser on your PC, and enter the management IP address of the gateway (192.168.9.1) in the address bar to access the web page.

Step 5 Set the management PIN of the gateway device and confirm it. Click Activate.

1.2.2 Wireless Connection

Step 1 Check the gateway bottom label, get notified about the last 4 digits of the device serial No. XXXX, and the device Wi-Fi network name is HIKVISION_XXXX.

Step 2 Connect your mobile device or PC to the same Wi-Fi network as the device (e.g., HIKVISION_XXXX).

Step 3 After the connection is successfully established, you will be redirected to the gateway management page automatically.

Note

If the redirection fails, go to the browser and enter the management IP address (192.168.9.1) of the gateway in the address bar.

Step 4 Set the management PIN of the gateway device and confirm it. Click Activate.

1.3 Configuration Guide

After the device activation is completed, the page will automatically jump to the configuration guide page. After configuration is completed, you can use the wireless network.

Step 1 Go to Online Device page to confirm the online device(s), and then click Configure.

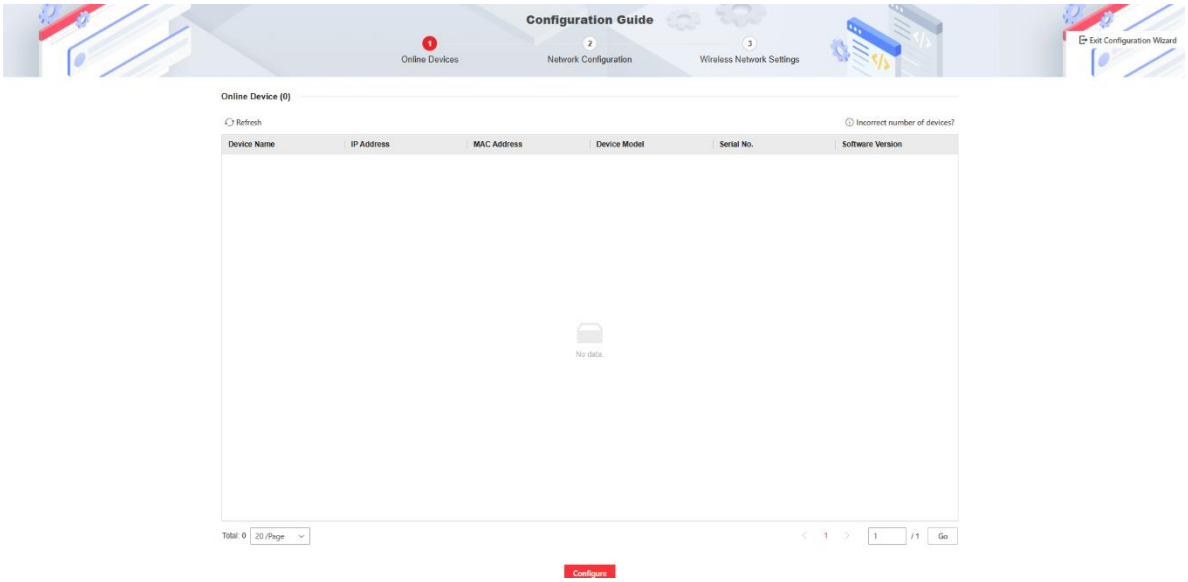

Figure 1-1 Start Configuration

Step 2 Set the Internet access mode, enable cloud fault log collection, and configure the cloud platform. Click Next after the settings are completed.

- Dynamic IP address (Recommended): Select this mode to automatically assign a dynamic IP address. No additional configuration is required.
- Broadband Dial-up: Manually enter the broadband account and password provided by your broadband service provider.
- Static IP Address: Enter the IP address, subnet mask, gateway, and DNS provided by your broadband service provider manually.

Step 3 Configuring the information about the wireless network on the Configuration page.

- Wi-Fi Name: Customizable.
- Encryption Type: Choose the type as needed..
- Wi-Fi Password: Length should be no less than 8 bytes.

Step 4 Now that the device activation and configuration are completed, the terminal device can search for Wi-Fi networks and enter the PIN to connect to the Internet.

Chapter 2 General Function

After you finish the configuration guide or log in to the gateway management page, the general toolbar of the platform will be displayed on the upper-right corner of the page. The functions are described as follows:

- Click  to enter the configuration guide page, where you can configure the Internet access mode, cloud platform switch, and Wi-Fi parameters.
- Click  to enter the alarm page and view alarm information.
- Click  to enter the network test page. When the device has network issues, you can perform quick network test and configure the device according to the test result.
- Click  to log out.
- Click  to enter the page for changing login password, and then enter the old and new passwords to change the platform login password.

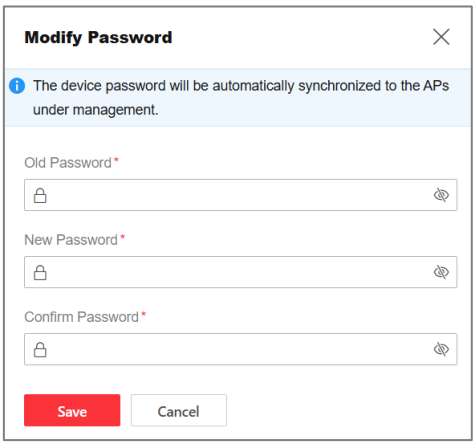

Figure 2-1 Change Platform Password

Note

- After you change the device password, you need to log in again to access the web page.
- After you change the device password, it will be synchronized to the AP devices managed by gateway.

Chapter 3 Overview

After completing the configuration guide or logging in to the gateway management page, you can view device information and access common functions on the Overview page.

Note

The available functions may vary for different models. Refer to the actual interface.

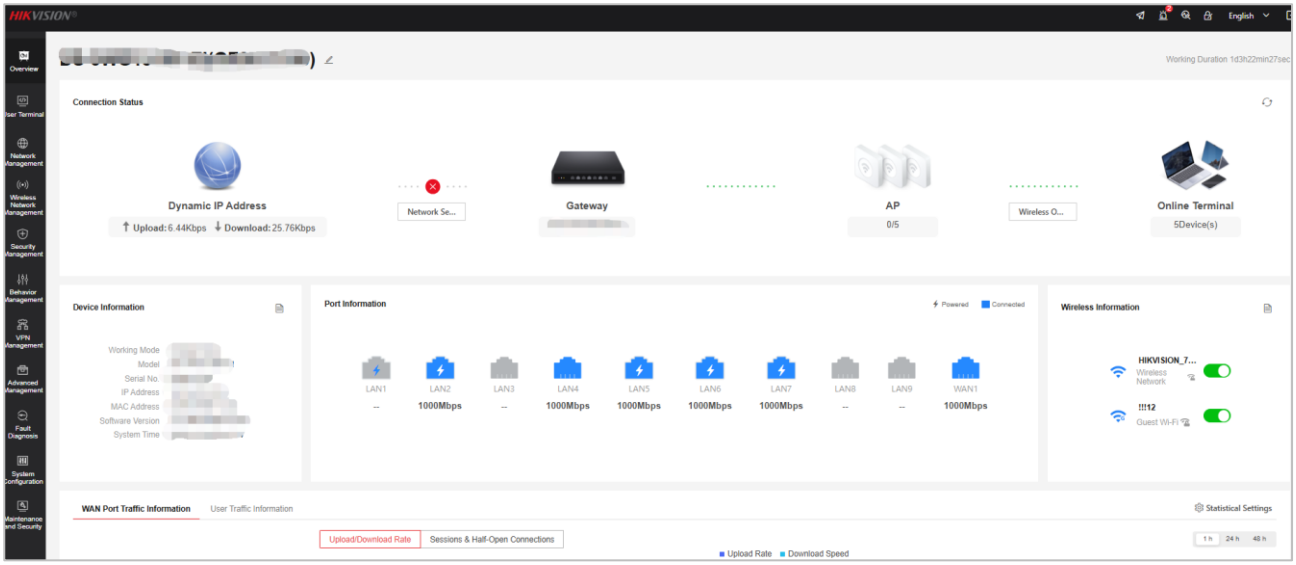

Figure 3-1 Overview

3.1 Modify Gateway Name

Click next to the name of the gateway device in the upper-left corner to quickly edit the gateway name.

3.2 View Overview Information

Overview of each section on the page is as follows:

Note

The following lists all the functions of the series. However, different series may support different functions. For details, see the device manual.

Table 3-1 Partition Information Description on Overview Page

Partition	Note
Connection Status	Click  to view the current network connection mode and network information.
	Click to view the AP information and set AP parameters.
	Click  to view the information of the terminal and set its permission.
	Click Network Self-Test to perform network test when the device has network issues and configure the device according to the test result.
	Click Wireless Optimization to optimize the user network for better Wi-Fi performance.
Device Information	Click to view the gateway information and go to system configuration.
Port Information	Check the connection status and speed of each port of the gateway.
Wireless Information	Drag the slider to enable or disable the wireless network. Tap Enable Wireless Network to go to the configuration page.
WAN Port Traffice Information	View the upload/download speed, number of sessions, and half-opened connections of the gateway or selected WAN port in the last 48 hours.
User Traffic Information	View the network data information of users in the past 7 days, including IP address, online duration, sessions, current upload/download speed, and total upload/download data. • Click  to turn the function on/off and set the unit for statistical parameters. • Click  to refresh the user's network data. • Click  to expand and view the details of user traffic data, and search for specific users in the upper-right corner.
Hardware Resource	View the memory usage and CPU usage of devices. **Note** Not all devices support this function. The actual interface may vary.

Chapter 4 Common Configuration

By configuring the following items, users in the LAN can access WAN via Wi-Fi of AP.

Note

The supported configuration functions may vary for different device models/versions. Refer to the actual interface.

4.1 WAN Configuration

WAN (Wide Area Network) configuration covers multiple aspects, including network interface settings, protocol configuration, IP address management, and MTU adjustment.

4.1.1 Select Line Type

The device supports multiple WAN access types.

Step 1 Enter Network Management > WAN Configuration.

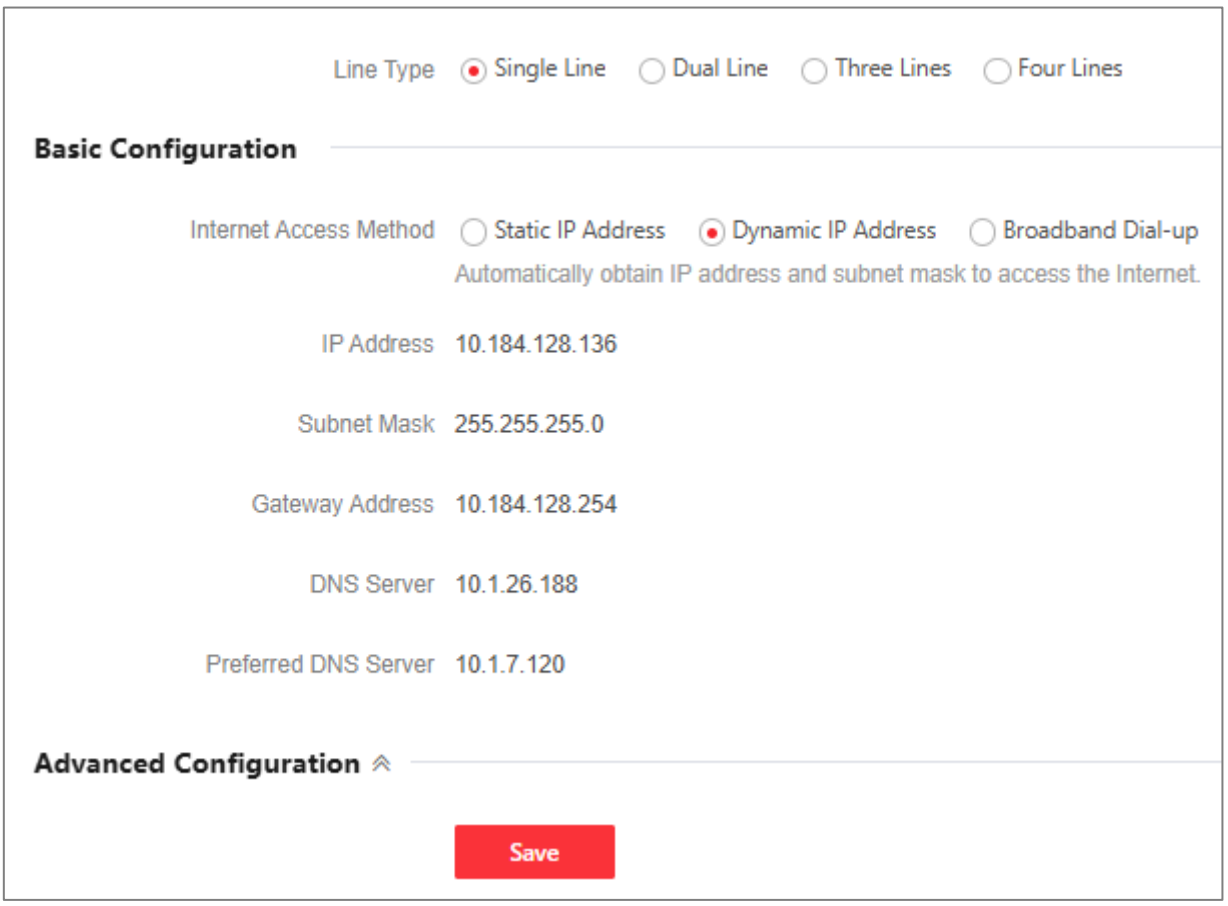

Figure 4-1 Example of WAN Port Parameter Configuration Page

Step 2 Select the line type.

- If the user only rents one operator network, select Single Line.
- If you rent multiple carriers' networks, select Multi-Domain. In this case, the LAN/WAN ports of devices will be switched to WAN ports.

Note

- The configuration methods of the two types are the same.
- The number of WAN ports on different device models is different, and so is the supported line type. Please refer to your actual device.

4.1.2 Set Internet Access Method

After you select the line type, you can configure the Internet access method.

Step 1 (Optional) If you select other than Single Line, select the WAN port for configuration.

Step 2 Enter Network Management > WAN Configuration > Basic Configuration

Step 3 Select Internet Access Method

- Dynamic IP address (Recommended): Select this mode to automatically assign a dynamic IP address. No additional configuration is required.
- For broadband dial-up: Manually enter the broadband account and password provided by your broadband service provider.
- Static IP: Enter the IP address, subnet mask, gateway, and DNS provided by your broadband service provider manually.

4.1.3 Advanced Settings

Keep the parameters in Advanced Settings as default. If you have special requirements for your Internet access, you can configure them according to your needs.

Step 1 Go to Network Management > WAN Configuration > Advanced Settings.

Step 2 Set the maximum length of the TCP segment in the Data Packet MTU. The default value is 1500 for static IP and dynamic IP, and 1480 for broadband dial-up.

Step 3 Set the MAC Address. By default, it is the factory MAC address of the API interface. When you access the WAN via the public IP address assigned by your carrier, enter the MAC address bound to your carrier here.

Step 4 (Optional) Enable 802.1Q Tag and set VLAN ID for the WAN port.

Step 5 (Optional) If you enable NAT, the device will convert the address of network data, which is applicable to scenes that need WAN access.

Step 6 (Optional) Set the Default Routing Priority. The smaller the value, the higher the priority.

Step 7 Click Save.

4.1.4 Set Carrier/Load Pattern

If you select other than Single Line as the type, you can set the Carrier and Load Pattern.

Step 1 Go to Network Management > WAN Configuration > Operator/Load Settings.

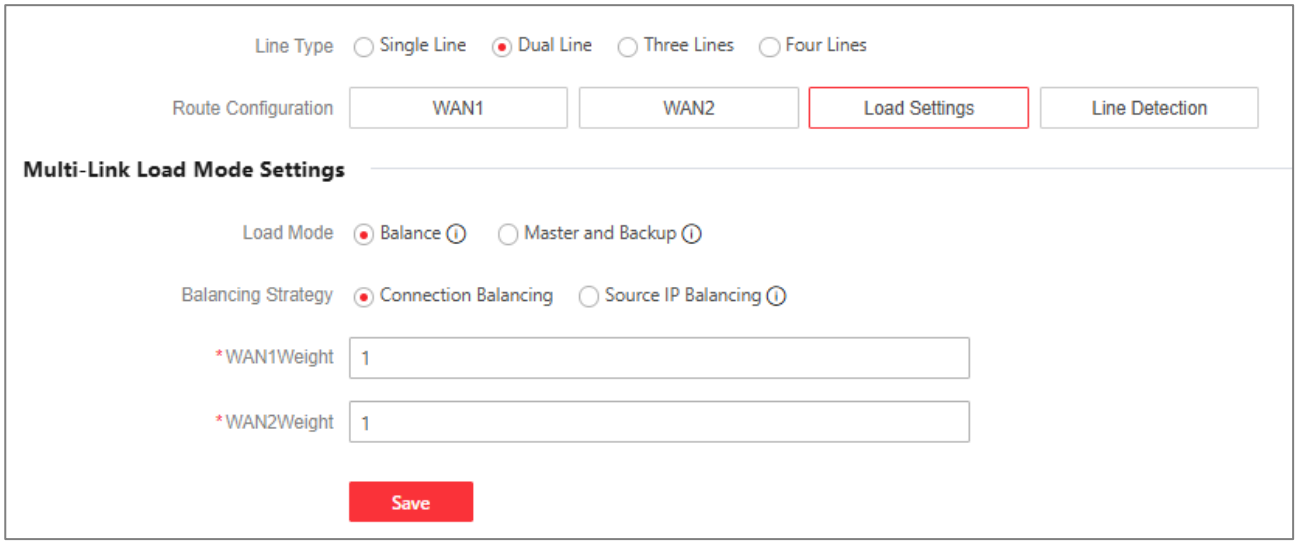

Figure 4-2 Set Carrier/Load Page Example

Step 2 Click Enable Address Library Routing and select the carrier for the WAN port.

Note

- Set the correct exit carrier according to actual situation. If multiple exits belong to the same carrier, it is not recommended to enable address library routing.
- After enabled, the data stream will automatically select path according to operator address library and avoid cross-operator access for faster network access.

Step 3 Set the Load Balance Mode of multiple links to Balanced or Active and Standby.

- Round Robin: Network data is allocated to WAN ports according to the weights of the WAN ports.
  - Set Load Balancing Strategy to Connection-Based or Source IP-Based.
  - Set the weights for WAN ports. The weight range is from 1 to 1000, and the default value is 1.
- Main and Standby: When the main interface is working normally, all traffic will go through the main interface; when the main interface fails, all traffic will automatically switch to the standby interface. For multiple main/standby interfaces, set weights for them.

4.1.5 Set Line Crossing Detection

If you select other than "Single Line", you can configure and display IPv4 line probing settings, including sending probe messages at the interval time to check whether the corresponding address is pingable.

Step 1 Go to Network Management > WAN Configuration > Line Detection.

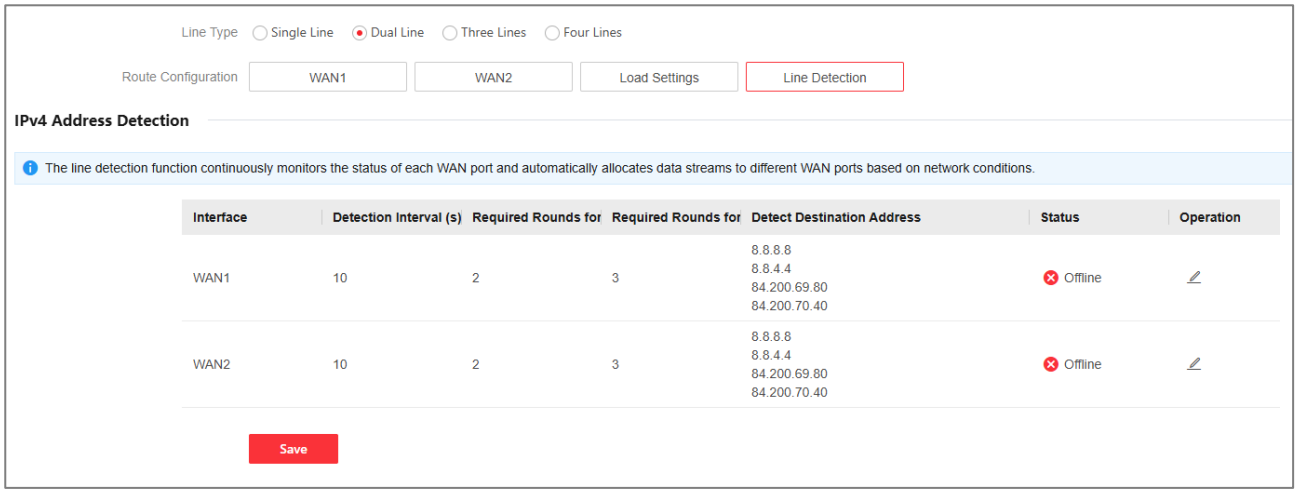

Figure 4-3 Line Crossing (Different Models Have Slight Differences)

Step 2 Click the operation icon of an API in the list (you can edit the set line crossing rule).

Step 3 Set the probe interval, required online/offline rounds, and add destination IP address/domain name.

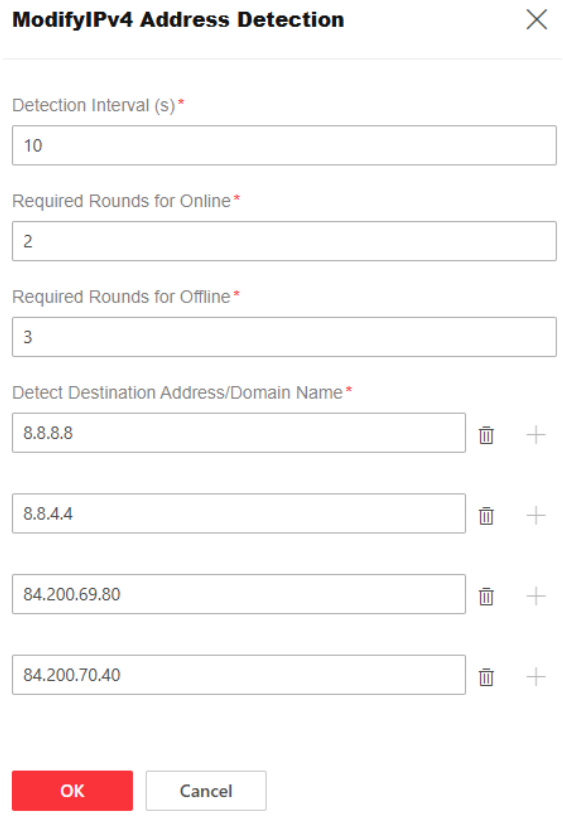

Figure 4-4 Set Line Crossing Detection

- probe interval: The time interval between two consecutive probes to the destination address or domain name of a line.

- times to ping successfully for WAN online status: If the line detection can be pinged and the number of consecutive pings that are successful reaches the set times to ping successfully for WAN online status, the WAN is in online status.
- times to be offline: If the WAN is not pinged back and the number of consecutive failed pings reaches the set times to be offline, the WAN will be marked as offline.
- destination address/domain name: The destination address or domain name to which the system sends Ping requests.

Step 4 Click Save.

4.2 LAN Configuration

4.2.1 Add VLAN

Step 1 Enter Network Management > LAN Configuration > LAN Configuration.

Step 2 Click Add.

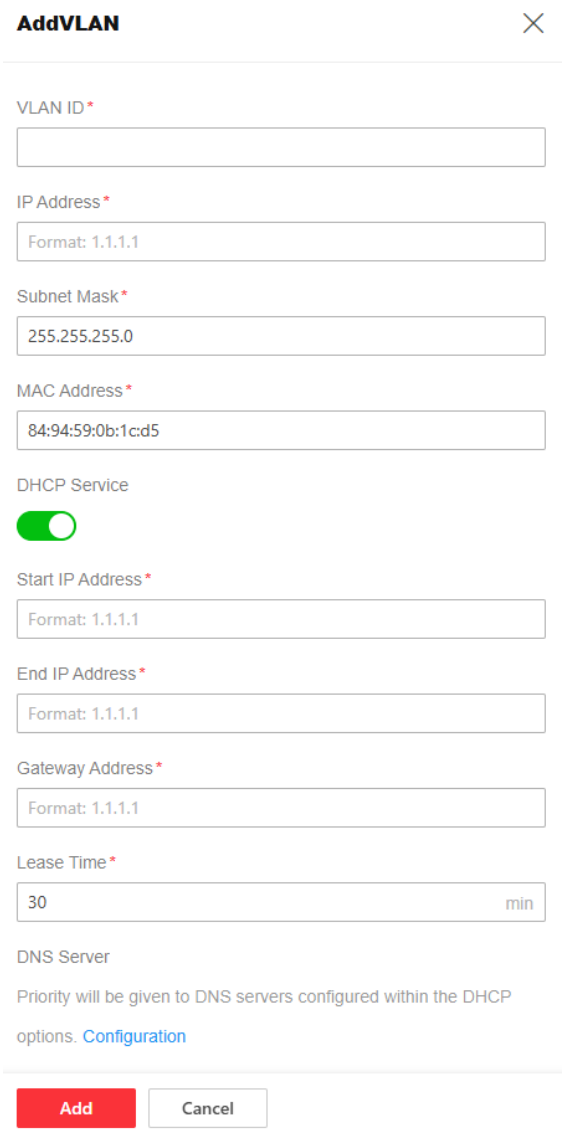

Figure 4-5 Add VLAN

Step 3 Configure VLAN parameters.

Step 4 Click Add.

4.2.2 Edit/Delete VLAN

Step 1 Enter Network Management > LAN Configuration > LAN Configuration.

Step 2 Click on the right side of the VLAN list to edit the VLAN parameters.

Step 3 Click on the right of the VLAN list to delete the VLAN parameter.

Note

- Editing VLAN ID is not supported.
- Default VLAN and visitor VLAN cannot be deleted.

4.2.3 Multi-VLAN Segmentation

Step 1 Enter Network Management > Port VLAN.

Note

Not all models support port VLAN configuration. Refer to actual interface.

Step 2 Select the relation between VLAN and LAN port.

- Untag: Set the VLAN as the only PVID of this LAN port.
- TAG: VLAN is assigned to LAN port.
- Not added: The VLAN is not allowed to be assigned to this LAN port.

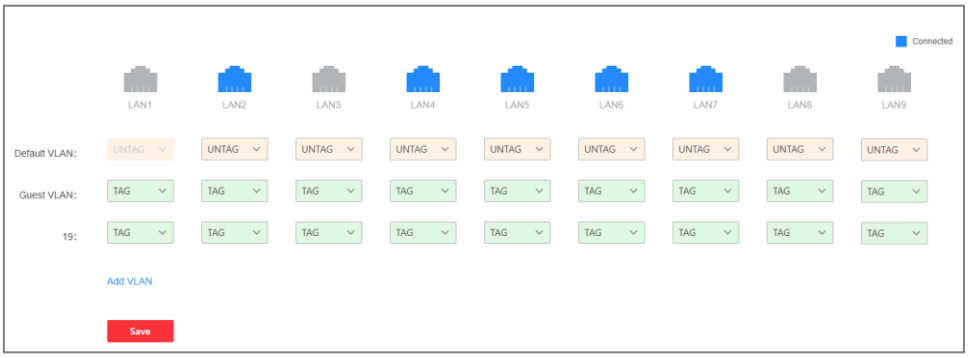

Figure 4-6 Multi-VLAN Segmentation

Step 3 (Optional) Click Add VLAN to add a VLAN. For details, please refer to the previous section Adding VLAN.

Step 4 Click Save.

4.3 AP Management and Configuration

4.3.1 Manage AP

View AP Status

Note

Not all devices support this function. For details, see the device interface.

Step 1 Enter Wireless Management > AP List.

Step 2 Click to view the selected AP.

Step 3 You can view the basic information or statistics of devices as needed.

Step 4 (Optional) Click Go to Device End for Configuration to go to the AP management platform and configure devices.

Note

- Make sure that your PC and AP are connected to the same LAN.
- If your PC and AP are not on the same LAN, you can add port mapping rules to access the AP remotely.

Change AP Name

- Single Modification

Supports customizing AP device names for easy identification and management.

Step 1 Enter Wireless Management > AP List.

Step 2 Click to the right of the device name to edit the AP name.

Step 3 Click Save.

- Batch Edit

Step 4 Enter Wireless Management > AP List.

Step 5 Click Import AP Name above the list to import APs via their MAC addresses and device names, and then batch change and apply AP names to the imported APs.

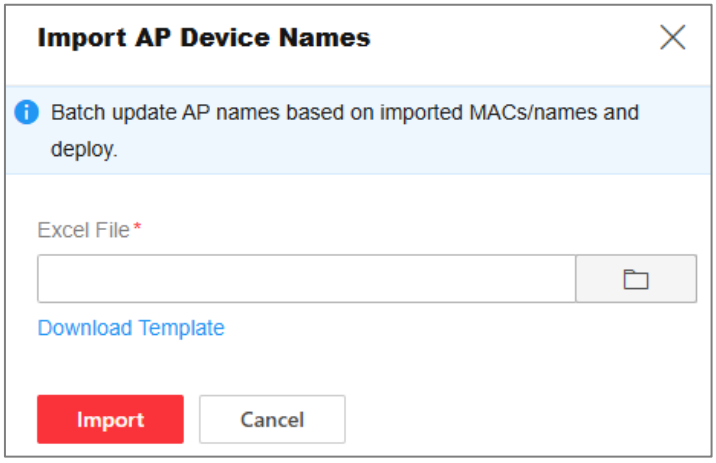

Figure 4-7 Import AP Name

Step 6 Click Download Template to save the template to your local computer and complete the filling.

Step 7 Click to import the completed file.

Step 8 Click Add after checking the imported list.

Set AP Group

You can add multiple APs to the same group and set the same Wi-Fi settings for these APs. In this way, you can configure different SSIDs for different APs.

Step 1 Enter Wireless Management > AP List.

Step 2 Click Add Group, set Group Name, and then click Add.

Step 3 Select the APs to be added to the group.

Step 4 Click Move to Other Group, select a group, and then click Move.

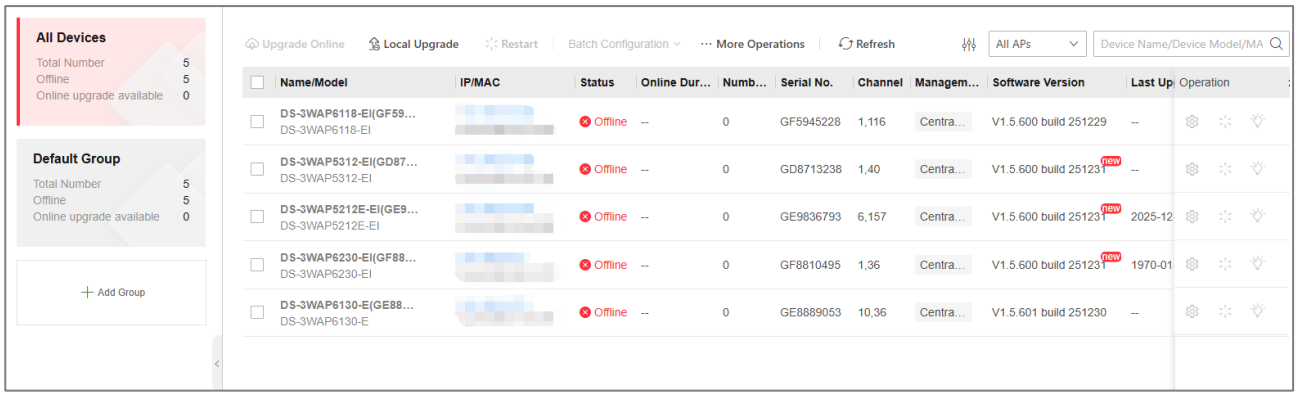

Figure 4-8 Set AP Group

Step 5 (Optional) When you move the mouse to the group area, the edit and delete icons will be displayed. Click them to perform relevant operations.

Note

By Default, two groups, All Devices and Default Group, are preset and cannot be edited or deleted.

Upgrade AP

- Online Upgrade AP via Gateway

Note

New version available for Hik-Connect Cloud service.

Go to Wireless Management > AP List, check the boxes of the APs to be upgraded, and click Online Upgrade. The gateway will upgrade the APs automatically.

Note

If the selected AP is already at the latest version, offline, upgrading, or in cloud management mode, a message will pop up to indicate that no upgrade is needed.

- Local Upgrade of AP via Gateway

Step 1 Go to Wireless Management > AP List, and check the boxes of the APs to be upgraded.

Step 2 Click Local Upgrade.

Step 3 Select Existing Firmware Version to select an existing version, or click Upload Firmware Version and select the upgrade package on your local computer.

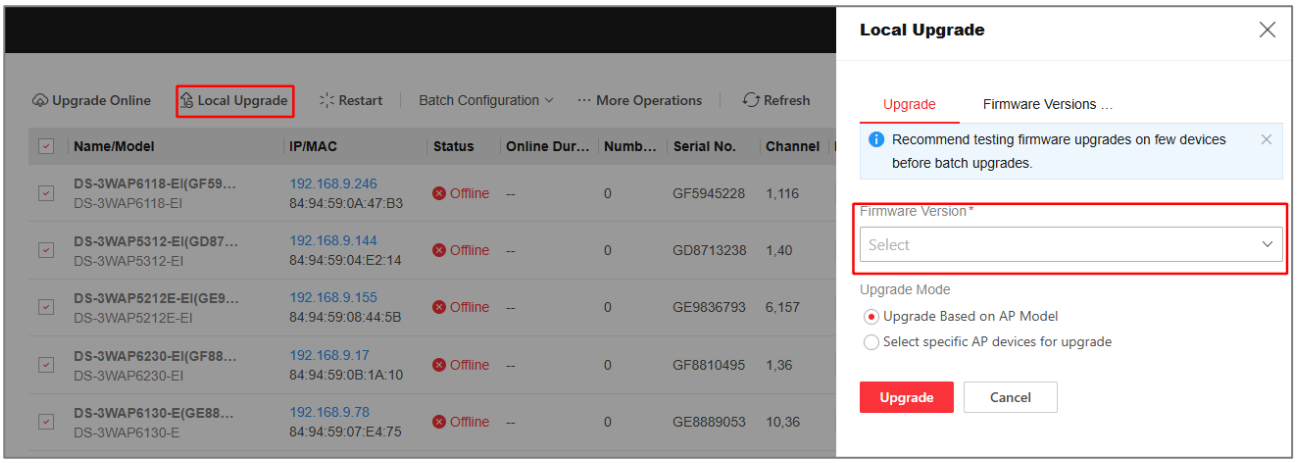

Figure 4-9 Firmware Version Uploading

Step 4 (Optional) Select Upgrade Based on AP Device Model or Select Specified AP Device for Upgrade.

- Based on AP device model: Upgrade the selected APs of the specified model in the AP list.
- Select Specified AP Device Upgrade: You can search for specified AP devices by device name or serial No..

Step 5 Click Upgrade to upgrade the AP firmware. After the upgrade is completed, the AP will restart automatically.

Step 6 (Optional) Click Firmware Version Management ***to*** upload the firmware version file and perform other operations such as adding description. The uploaded firmware versions can be selected directly in Step 3.

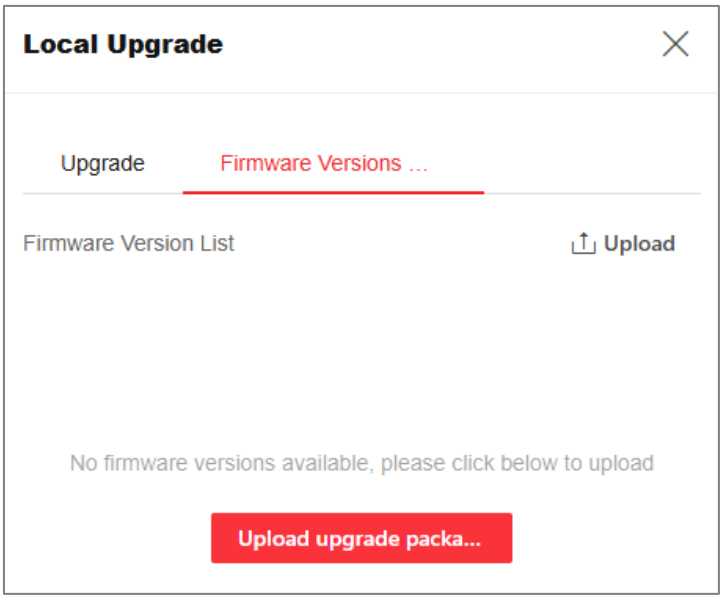

Figure 4-10 Firmware Version Management

- Upgrade via Portal

Go to Wireless Management > AP List. Click the IP address of the AP to be upgraded to enter the AP management page.

Figure 4-11 Go To AP Management Page

Note

- Make sure that your PC and AP are on the same LAN.
- If your PC and AP are not on the same LAN, you can add port mapping rules to access the AP remotely.

Step 1 Log in to the AP management page. The login password is the same as the gateway management password.

Step 2 Go to the Upgrade page of an AP and select Online Upgrade or Local Upgrade. Refer to the above two sections for details.

Reboot/Restore AP

In the Wireless Management > AP List page, you can select one or more APs to perform the following settings:

- Click to reboot the selected APs.
- Click to delete the selected offline APs.

- Click to restore the selected AP to factory settings.
- Click . The selected AP indicator light will flash for easy locating.
- Click to configure the uplink port and radio frequency of the selected APs.

Note

For offline devices, only deletion is supported, and other configuration items are not supported.

Configure AP Uplink Port

Step 1 Go to Wireless Management > AP List, select the target AP, and click .

Step 2 In the Network Configuration module, select Internet Access Mode.

- Dynamic IP address (Recommended): Select this mode to automatically assign a dynamic IP address. No additional configuration is required.
- Static: Enter the IP address, subnet mask, gateway, and DNS provided by your broadband service provider manually.

Step 3 Set the MAC Address. By default, it is the factory MAC address of the API interface. When you access the WAN via the public IP address assigned by your carrier, enter the MAC address bound to your carrier here.

Step 4 (Optional) Enable 802.1Q Tag and set VLAN ID for the uplink port.

Note

Some versions of devices support batch enabling this function by selecting AP devices in bulk and then clicking "Batch Configuration to Manage VLAN Configuration" above the list.

Step 5 Click Save.

Configure AP RF

Step 1 Go to Wireless Management > AP List, select the target AP, and click .

Note

In some versions, you can select multiple APs and then click Batch Configure > RF Configuration to batch configure this function.

Step 2 Go to RF Configuration > Module, and select whether to enable 2.4G or 5G wireless network.

Step 3 Configure the following parameters：

- Set Channel: A channel is a data transmission path that uses wireless signals as the transmission medium. If you select Auto, the AP will automatically select an optimal channel based on its

environment.

- Set Power: Power affects the wireless signal strength. For large area or more partitions, set power to Advanced.
- Enable Access Control for Low Signal Strength: By setting the signal strength threshold and refusal times, you can prevent terminals with low signal strength from accessing the network, reduce the occupation of wireless channels, and improve the overall performance and user experience of the wireless network.
- Set Threshold for Forcing Offline: When the Wi-Fi signal strength of end users is lower than the set threshold, they will be forced to go offline.
- Set Roaming Sensitivity: Increasing the roaming sensitivity can improve the link quality of terminals during roaming and keep them in a good signal state. If the sensitivity is too high, the terminal may frequently switch Wi-Fi networks, which will affect its internet access.

Note

Note: Only part of device models support the functions of weak signal access control, offline threshold, and roaming sensitivity. For other models, please refer to their actual interfaces.

Configure AP Wireless Function

Note

Not all devices support this function. For details, see the device interface.

Step 1 Go to Wireless Management > AP List, select the target AP, and click .

Step 2 Go to Wireless Configuration / Advanced Settings to configure the AP device with the wireless network synchronization status of the gateway device / whether to enable the directional antenna.

Note

After enabling the targeted antenna function, the device's wireless signal will be transmitted directionally, allowing the signal to penetrate further with greater concentration, making it suitable for long-distance scenarios such as corridors and outdoor areas.

Maintain AP

Note

Not all devices support this function. For details, see the device interface.

Step 1 Enter Wireless Management > AP List.

Step 2 (Optional) Select the devices to be collected, and click Batch Configuration > Collect Faults in One Click above the list. The system will collect faults automatically. After the collection is completed, you can view the results.

Step 3 (Optional) For devices under cloud management mode, check the boxes of devices to be switched to centralized management, and click Batch Configuration Switch Management Mode above the list to complete the mode switching.

4.3.2 Configure AP Wired Port

Configure the AP with LAN port.

Step 1 Enter Wireless Management > AP Wired Port.

Step 2 Enter the VLAN ID of the Ethernet port, and then click Save to set the default VLAN of the Ethernet port of the AP.

Step 3 Add AP Wired Port Configuration.

1. Click + in the AP Wired Port Configuration List.
2. Select the VLAN ID of the Ethernet port and apply it to the AP device.
3. Click Add.

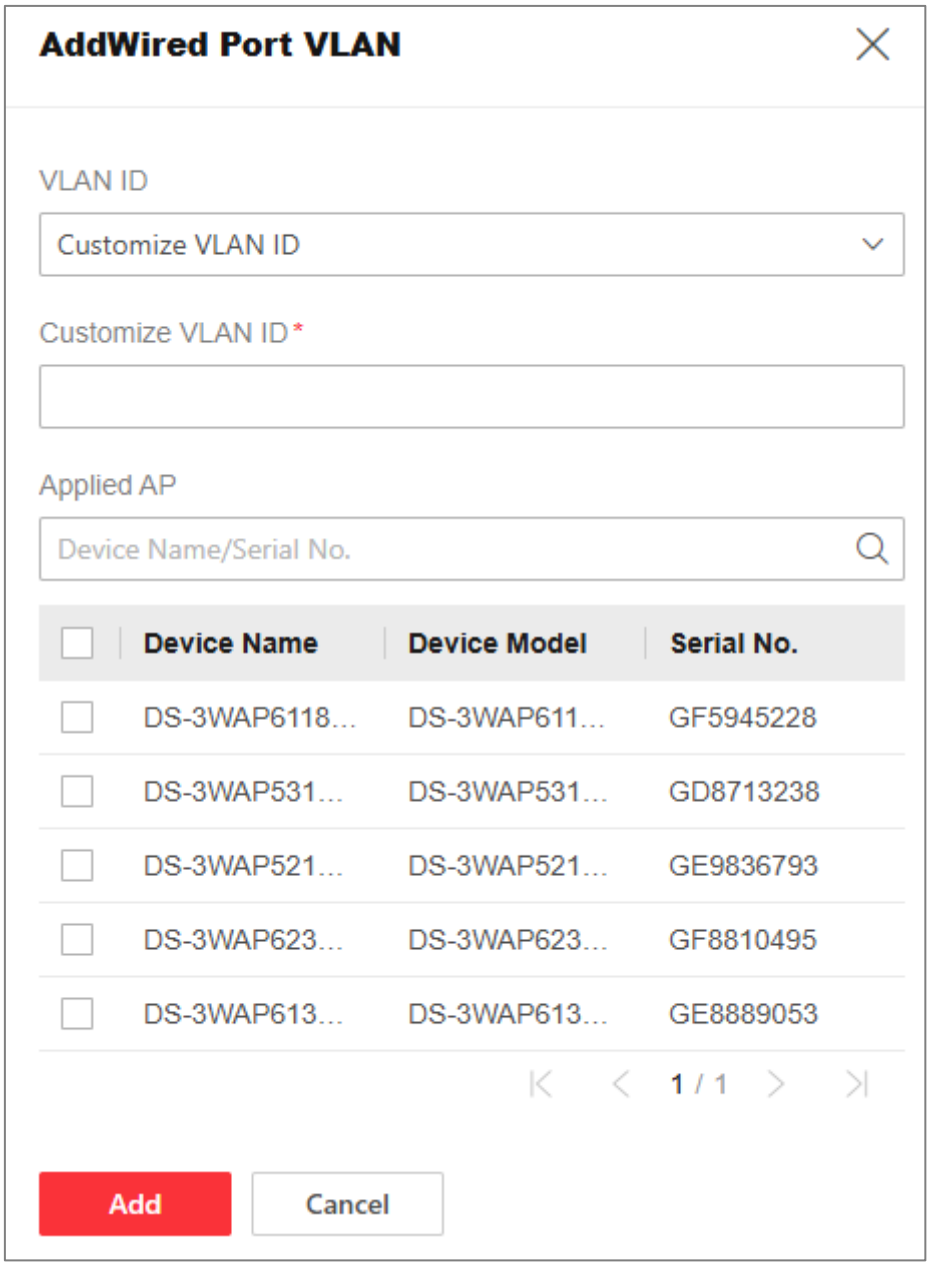

Figure 4-12 Add AP Wired Port Configuration

Note

Priority is given to the configurations applied to the AP in the "AP Wired Port Configuration List". APs in the network that have not had configurations applied will take effect from the "AP Wired Port Default Configuration".

4.3.3 Enable AP Status Indicator

Go to Wireless Management > AP Status Indicator, and enable the Global Switch for AP Status Indicator to enable the status indicator of all APs connected to the gateway device. If you need to adjust the status indicator of a specific AP, go to Device > AP to configure it.

4.3.4 Link Access Point to Terminal

Go to Wireless Management > Terminal Linking to configure terminal linking. After the terminals are linked to specific APs, they can only connect to the linked APs and cannot connect to other APs in this network environment. Function priority: Wireless Access Control > Terminal Linking.

- Quickly add links: Click to select the AP and check the online terminals to be linked.
- Manual Link: Click to select the AP and enter the MAC address of the terminal to be linked manually. No more than 5 terminals can be linked at one time.
- Edit terminal linking: Click the operation bar behind the linked terminal to edit its linked AP device and note information.
- Delete linked terminal: Click the operation bar behind the linked terminal to delete its linkage.

4.4 Wireless Management

Two Wi-Fi Networks Predefined on Device:

- Main Wi-Fi: HIKVISION_XXXX. It is enabled by default and the password is the Wi-Fi password set when activating the device.
- Guest Wi-Fi: HIKVISION_GUEST_XXXX. It is disabled by default and has no password by default. The guest Wi-Fi is isolated from other VLANs by default.

4.4.1 Add Wi-Fi

Step 1 Enter Wireless Management > Wireless Configuration > Wireless Network.

Step 2 Select a group to add the Wi-Fi network, and click . (Refer to Settings for setting AP group.)

Step 3 Configure Wi-Fi Parameters

Note

The available parameters vary with the device model. Refer to the actual device for details.

1. Select Wi-Fi Mode as needed.
2. Enter Custom to set the Wi-Fi name, select Encryption Type and Application Band, and set the Wi-Fi password.
3. Click Advanced Settings to set effective time period, VLAN, whether to hide Wi-Fi, Wi-Fi speed limit, and fast roaming 11r.

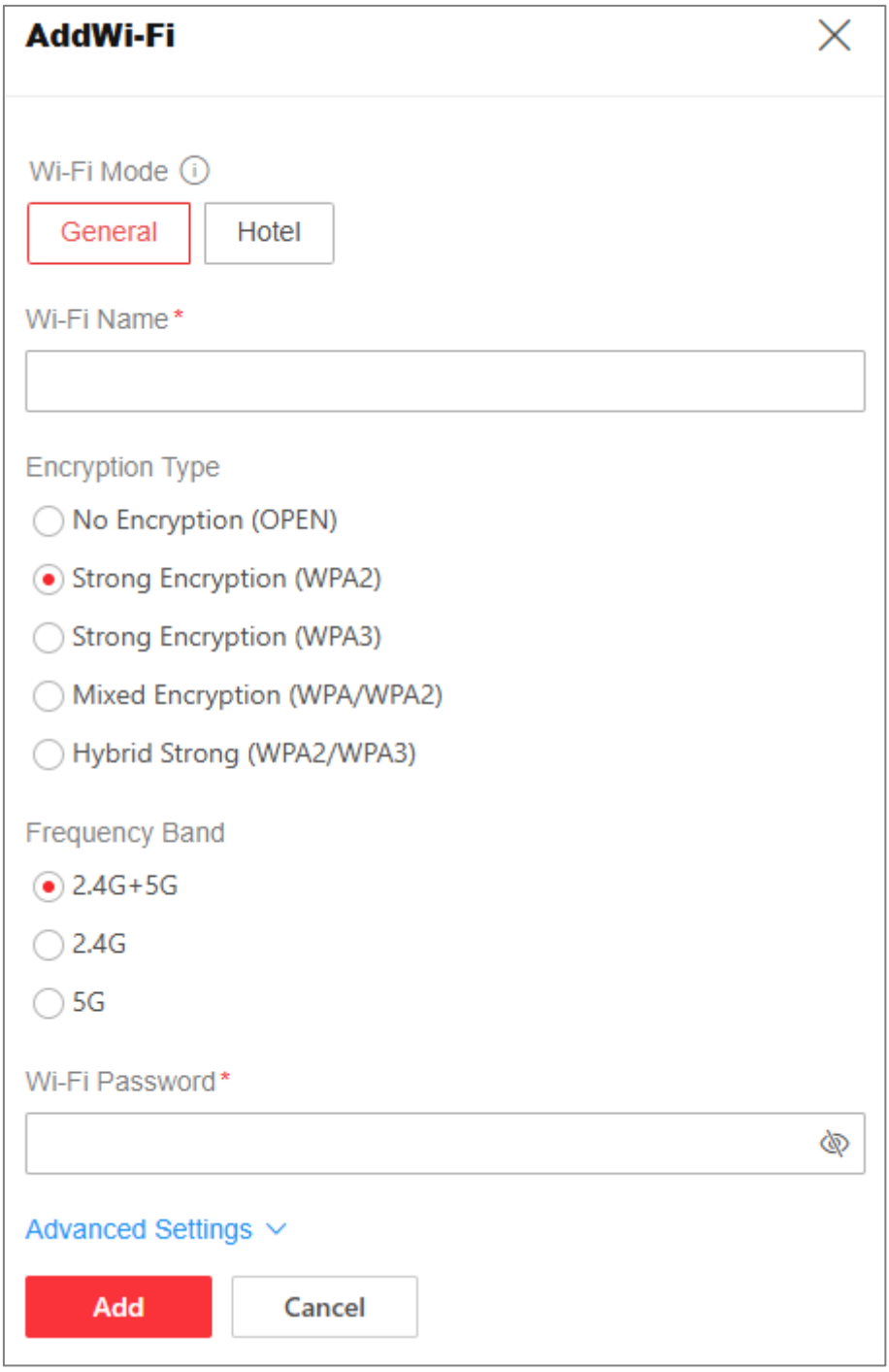

Figure 4-13 Add Wi-Fi

Step 4 Click Add.

Step 5 (Optional) Click the Current Wi-Fi Group page.

4.4.2 Change Wi-Fi

Enter Wireless Management > Wireless Configuration > Wireless Network.

- Click the slider to the right of the Wi-Fi name to enable or disable Wi-Fi quickly.

- Move the mouse to the Wi-Fi area and tap to edit Wi-Fi password and other information.
- Move the mouse to the Wi-Fi area and tap to delete the Wi-Fi.

Note

Main Wi-Fi and Guest Wi-Fi cannot be deleted.

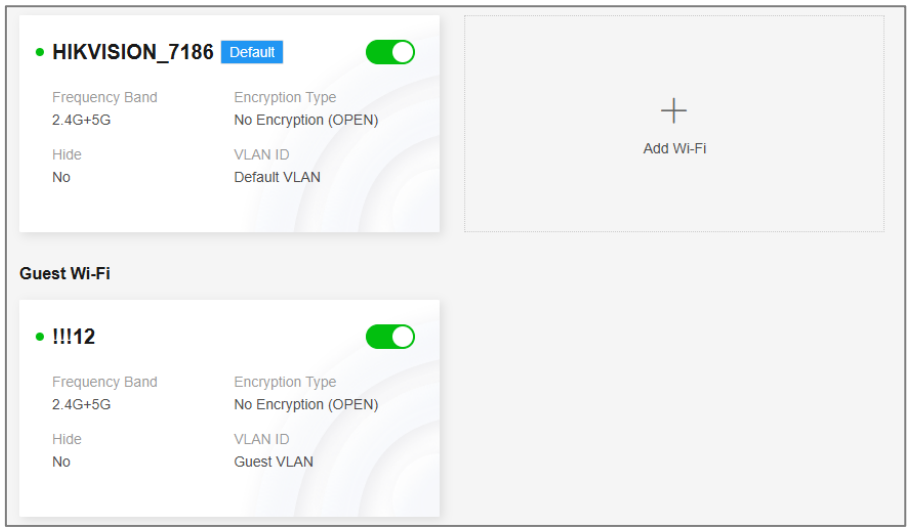

Figure 4-14 Change Wi-Fi

4.4.3 Wireless RF Configuration

You can configure Wi-Fi RF parameters for a group of devices.

Step 1 Go to Wireless Management > RF Configuration.

Step 2 Select a group to configure.

Step 3 Set the bandwidth and max. terminal connections for different frequency bands.

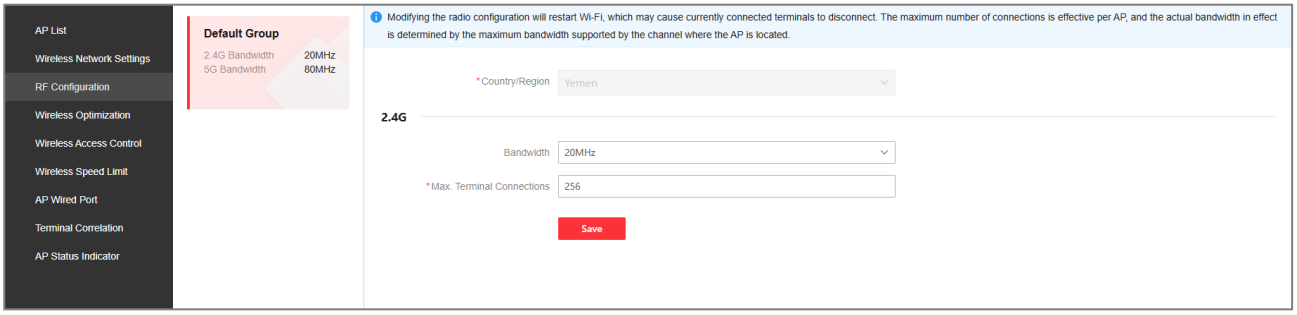

Figure 4-15 RF Configuration

Step 4 Click Save.

Note

- Modifying RF configuration will restart Wi-Fi and may cause the connected terminals to be disconnected. The actual effective bandwidth is determined by the maximum bandwidth supported by the channel of the AP.
- To configure the AP channel, go to the AP's Web page.

4.4.4 Set Health Check Mode

After you enable the health mode of the wireless network, devices will reduce the RF output power to minimize radiation during the effective period.

Step 1 Enter Wireless Management > Wireless Configuration > Health Mode.

Step 2 Enable the function.

Step 3 Set Effective Time Period.

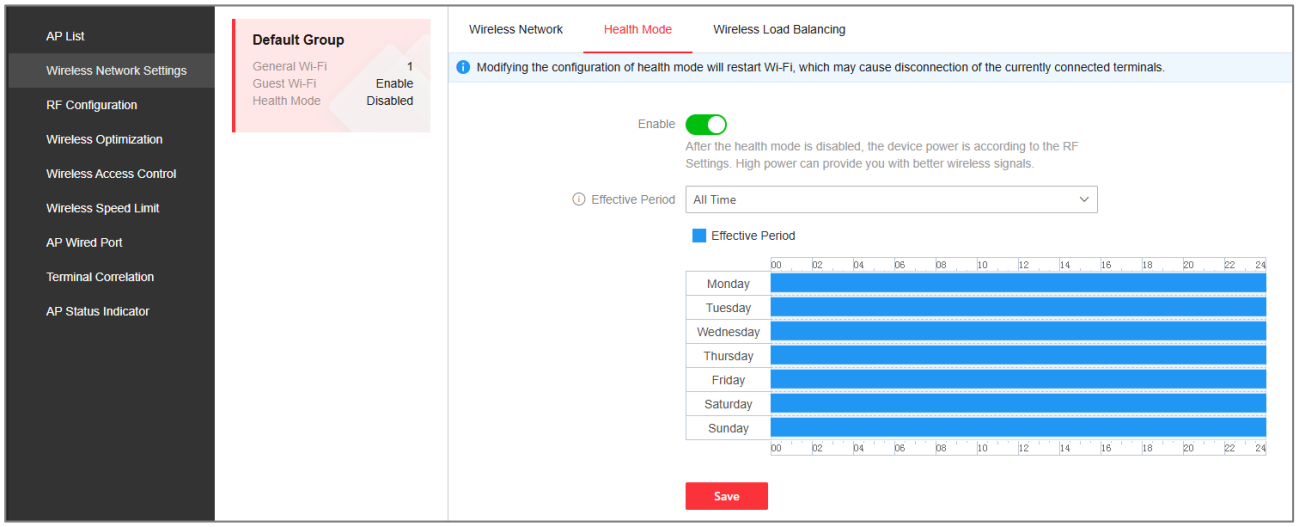

Figure 4-16 Set Effective Time Period

Step 4 (Optional) Click Add in the Effective Time Period drop-down list to customize the time period.

Step 5 Click Save.

Note

Rebooting Wi-Fi is required to change the health check settings, which may cause the connected terminals to be disconnected.

4.4.5 Wireless Load Balancing Configuration

Wireless Load Balancing Strategy can be added.

Step 1 Go to Wireless Management > Wireless Configuration > Wireless Load Balancing.

Step 2 Click Add.

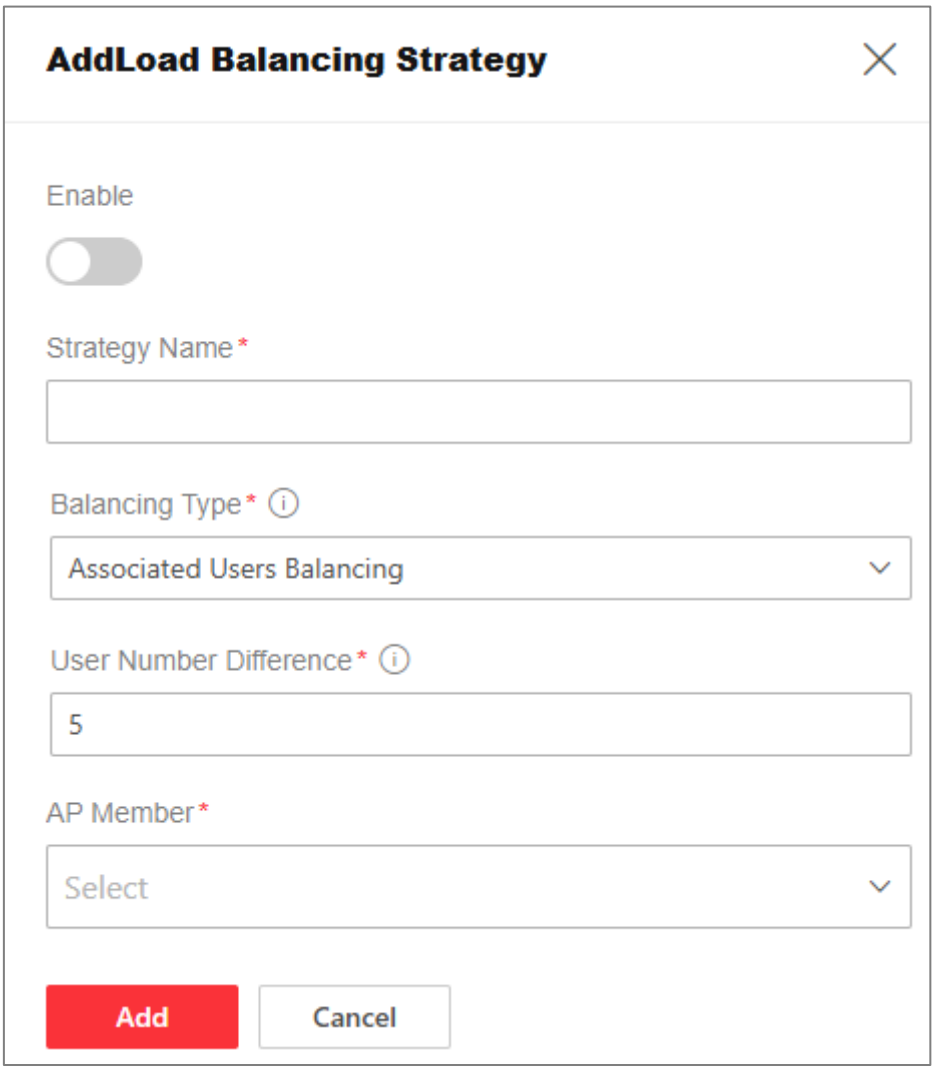

Figure 4-17 Wireless Load Balancing Configuration

Step 3 Enable/Disable the strategy.

Step 4 Configure the Following Parameters:

- Load Balancing Group Name: The name of the load balancing group.
- Load Balancing Mode: based on the number of linked users.
- User Count Difference: Load balancing is triggered when the linked user count difference reaches the set value, with a range of [1, 8] and a default of 2.
- AP Member: Select AP devices under the gateway device to perform load balancing among APs in the same group.

Step 5 Click Add.

Note

The functions of different device models may vary. Refer to the actual interface on your device.

4.4.6 Optimize Wireless Network

Three ways to optimize your Wi-Fi network performance:

- ***One-Click Optimization:***

  Enter Wireless Management > Wireless Optimization > Quick Optimization, and click Quick Optimization.

- ***Auto Optimize:***

  Go to Wireless Management > Wireless Optimization > Scheduled Optimization and enable Auto Optimization.

- ***Scheduled Optimization:***

  Enter Wireless Management > Wireless Optimization > Scheduled Optimization, enable Scheduled Optimization, and set the time.

Go to Optimization Record page to view the details.

4.4.7 Control Wireless Access

This function supports filtering MAC addresses via the set filtering type to control their access to Wi-Fi network.

Set Blocklist

Step 1 Go to Wireless Management > Wireless Access Control > Block List.

Step 2 Add or import blocklist.

- Click "Add Blocklist" / "Manual Add", and enter the MAC address manually.
- Click Quick Add to add the current online terminals quickly.
- Click Import Blocklist to import the pre-filled Excel file. If you have enabled Auto Replace Duplicated MAC Address List, the system will automatically replace the information of the existing MAC address with that of the imported MAC address. Otherwise, the system will keep the information of the existing MAC address.

Step 3 (Optional) Click Label Management to add labels for subsequent terminal classification management.

Step 4 Click Add or Import.

Step 5 (Optional) Click  to delete the MAC address from the list.

Set Authorization List

Step 1 Enter Wireless Management > Wireless Access Control > Authorization List.

Note

When switching to this mode, all terminals can access the Internet if the list is empty; otherwise, terminals not in the list cannot access the Internet.

Step 2 (Optional) Check the box of the current online terminal to add it to the allowlist.

Step 3 Add or import an authorization list.

- Click Manual Verification / Add Authorization List to enter the MAC address manually.
- Click Quick Add to add the current online terminals quickly.
- Click Import Authorized List to import the pre-filled Excel file. If you have enabled Auto Replace Duplicated MAC Address List, the system will automatically replace the information of the existing MAC address with that of the imported MAC address. Otherwise, the system will keep the information of the existing MAC address.

Step 4 (Optional) Click Label Management to add labels for subsequent terminal classification management.

Step 5 Click Add or Import.

Step 6 (Optional) Click to delete the MAC address from the list.

4.4.8 Wireless Speed Limit

Enter "Wireless Management > Wireless Speed Limiting" to limit the wireless network speed through the following 4 methods.

- Intelligent Speed Limit: Supports one-touch speed limit. Enabling speed limit will affect the speed testing performance. If you need to test speed, please disable intelligent speed limit first.
- Terminal-based speed limit: Select terminals from the user terminal or manually add terminal MAC addresses, and set upstream and downstream speed limits.
- Based on SSID speed limiting: Select 1 Wi-Fi network, choose upstream and downstream speed limiting methods respectively, and set the upstream and downstream speed limiting rates.
- Based on RF rate limiting: You can separately set the uplink and downlink rate limiting methods and rates for the 2.4 G and 5 G RF.

Note

When multiple speed limit configurations of different types exist simultaneously, the following rules determine which speed limit rule takes effect: terminal-based speed limit > SSID-based speed limit > RF-based speed limit > intelligent speed limit.

4.5 Terminal Management

Go to User Terminal to view the details of terminals.

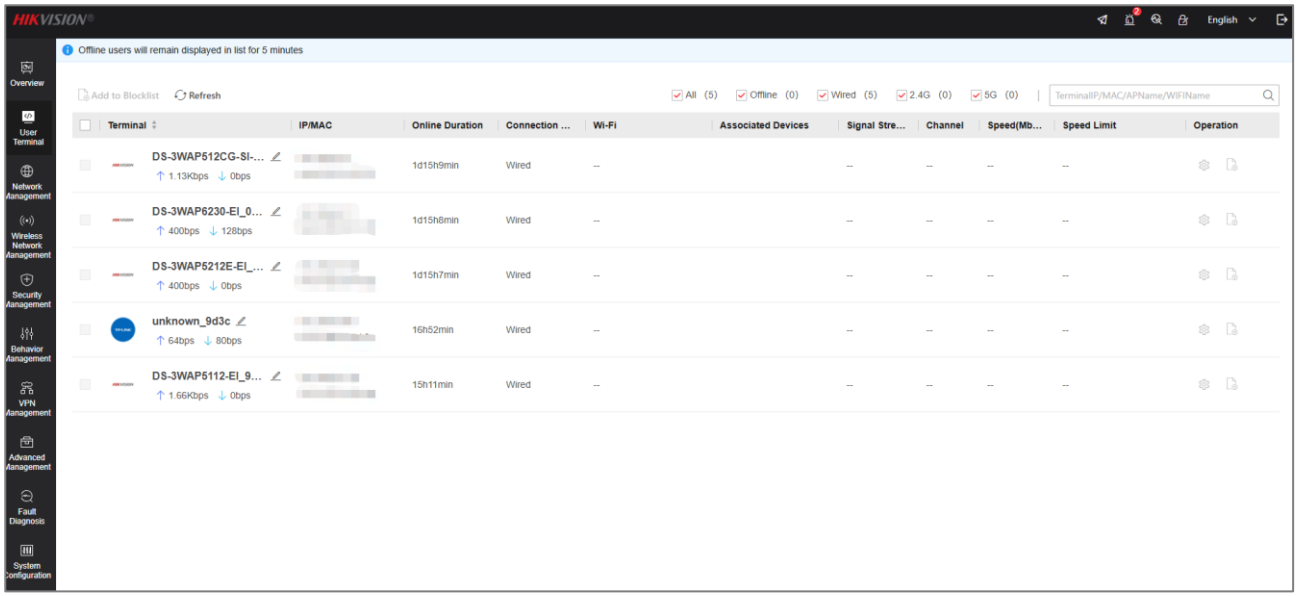

Figure 4-18 User Terminal

The following operations are supported:

- Click the picture on the right of the terminal name to edit the user terminal name.
- Click in the operation list of the single terminal to add the user terminal to the blocklist and disable its network access.
- Select terminals to disable and click Add to Block List in the upper-left corner of the list.

Note

- To withdraw the operation, go to Wireless Management > Wireless Access Control > Block List to delete the device.
- This function is only available when the access control mode of the wireless network is set to block list. For details, please refer to Local Security Settings.
- Not all devices support this function. For details, see the actual interface.

4.5.2 Set Security Zone

Security Zone is primarily used to manage multiple APIs on firewall Devices that share the same security requirement. By dividing APIs into different security domains, unified management of security control policies can be achieved.

Add Security Zone

You can add security domains according to the overall planning.

Step 1 Enter "Security Management > Local Security > Security Zone".

Step 2 In the Security Zone Configuration module, click Add.

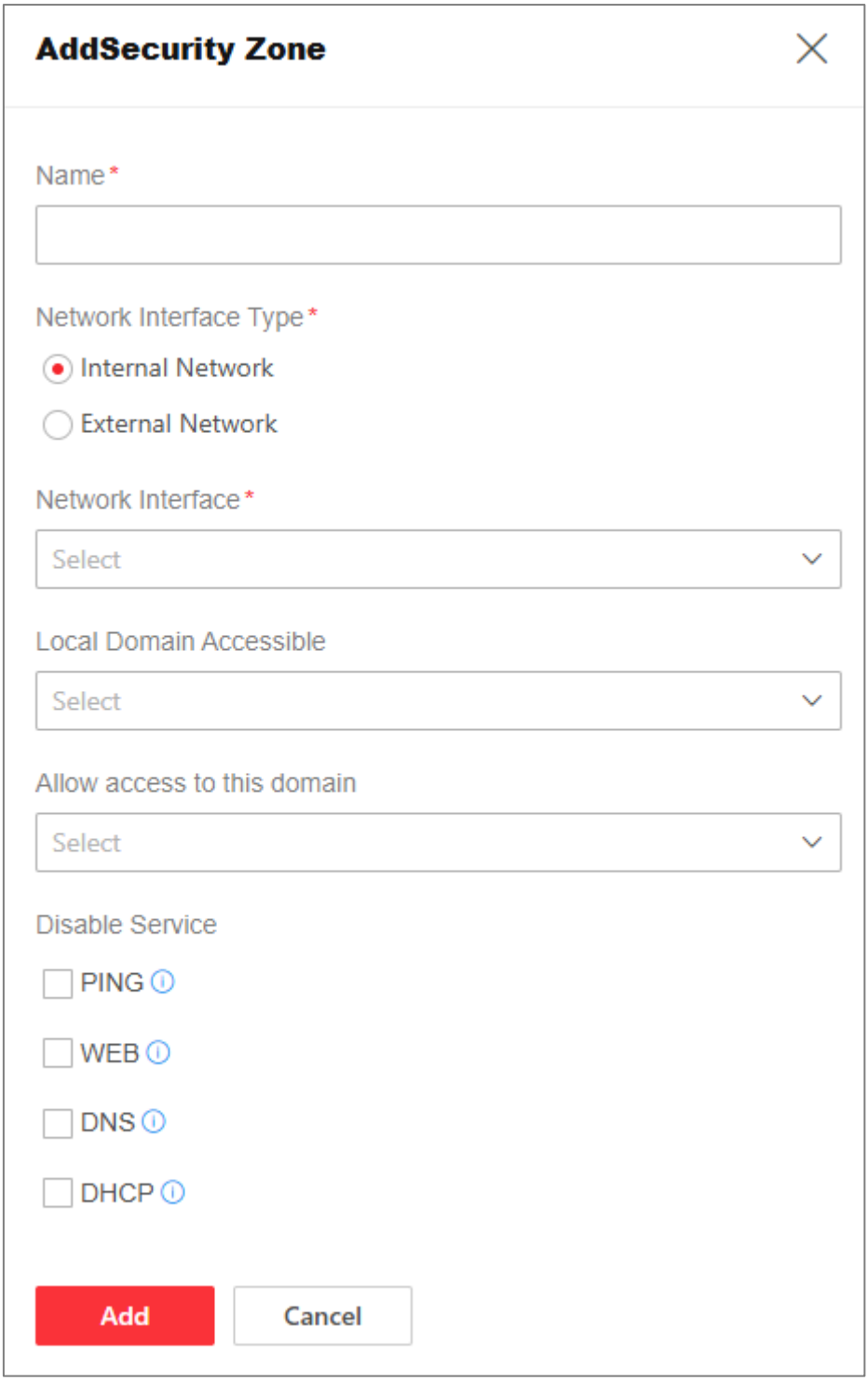

Figure 4-19 Add Security Zone

Step 3 Enter the domain name, configure the domain API, accessible domain, and disable service.

Note

Description of Disabled Service Options:

- Ping: If selected, terminals in this domain cannot ping the device.
- If you select this, terminals in the domain cannot access the device's Web page.
- DNS: If selected, terminals in the security zone will not be able to access web pages if they use the local address as their DNS server.
- DHCP: If selected, terminals in this security zone cannot access the DHCP service of the device.

Step 4 Click Add.

Step 5 (Optional) Click the operation column at the back to modify the current configuration entry.

Step 6 (Optional) Click the picture in the operation bar above the list to delete the current entry.

Add Allowlist

You can add allowlist to further refine the resource access permission.

Step 1 Enter "Security Management > Local Security > Security Zone".

Step 2 In the Allowlist Configuration module, click Add.

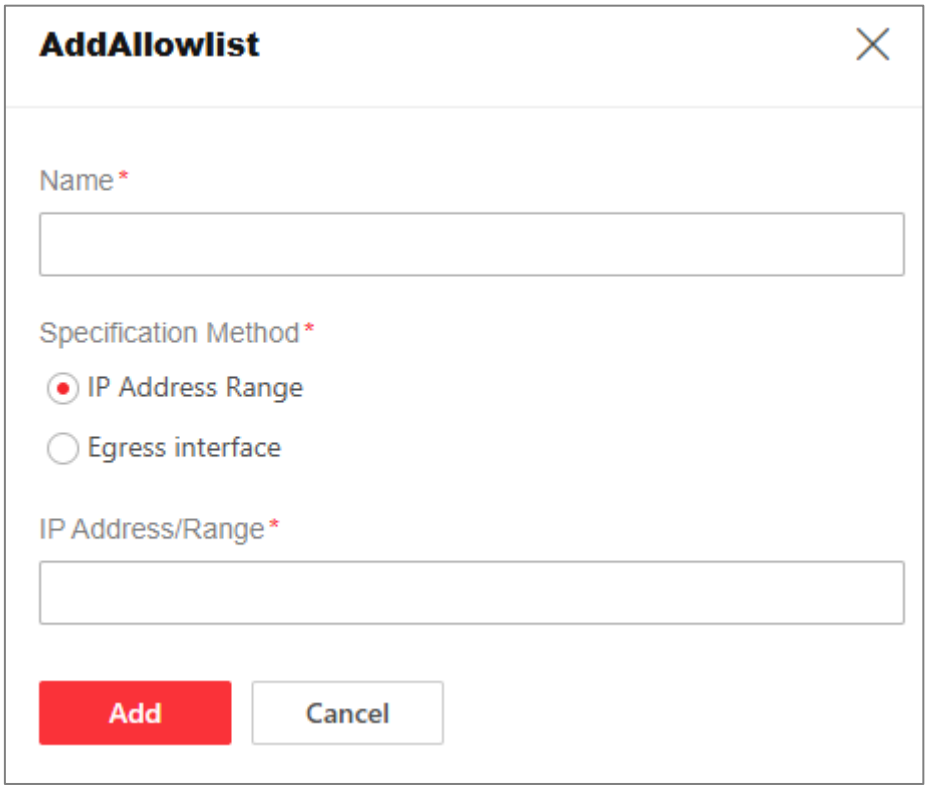

Figure 4-20 Add Allowlist

Step 3 Enter the name and configure other parameters.

Step 4 Click Add.

Step 5 (Optional) Click the Edit button in the operation bar at the lower part of the page to edit the current configuration item.

Step 6 (Optional) Click the picture in the operation bar above the list to delete the current entry.

4.5.3 Anti-Attack Configuration

Step 1 Go to Security Management > Local Security > Anti-Attack.

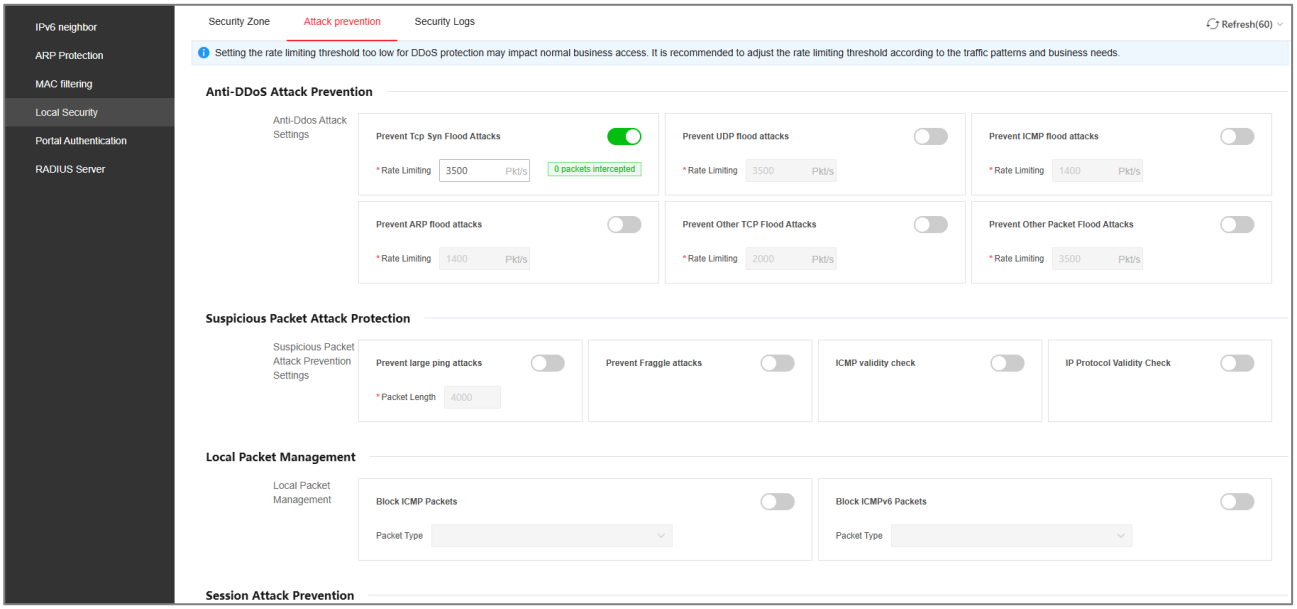

Figure 4-21 Anti-Attack Configuration

Step 2 Enable and configure the anti-attack function if needed.

- DDoS protection: By identifying, interrupting, or mitigating malicious traffic, this service ensures the normal operation of your business. Please enable it and set the limit rate reasonably. If the limit rate is too low, it may affect the access of your normal business.
- Anti-Suspicious Packet Attack: By identifying and blocking network data packets that do not conform to protocol specifications or have malicious features, this function can prevent attackers from using malformed packets or forged packets to attack the system.
- Local Packet Management: Control, monitor, and optimize the network data packets sent by the device to prevent malicious or abnormal packet sending behaviors.
- Anti-Session Attack: Identifying and blocking malicious operations on user sessions to ensure the legality and security of sessions within their lifecycles.

Step 3 Click Save.

Step 4 (Optional) Click Restore Default to reset all settings to the factory settings.

Step 5 (Optional) Enter Device Management > Security Management > Security Log, and filter security logs by time period and keyword.

4.6 Portal Authentication

Supports forcing terminals to go through authentication before accessing Internet.

Note

- Not all models support this function. For details, see the actual interface.
- The functions supported and the way they are presented may differ among devices of different models/versions. Refer to actual device interface for details.

4.6.1 Local Authentication

Account Authentication

Step 1 Enable the function.

1. Enter Security Management > Authentication Mode > Local Authentication > Account Authentication.
2. In the function editing page, set parameters for authentication and click Save. The terminals in this IP address or VLAN need to pass the authentication before they can access the Internet.
3. Enable.

Step 2 Manage account.

1. Enter Security Management > Authentication Portal > Authentication Mode > Local Authentication > Account Authentication.
2. In the function editing page, click "Add".
3. Set the account name, PIN, and max. number of persons allowed to log in simultaneously.
4. Click Add. Now the terminals in the IP address or VLAN need to enter account password for authentication to access the Internet.

Authentication and Authorization

After you enable the Authorization Authentication, when an authorized IP user scans the QR code on the pop-up window of the IP camera terminal, he/she can access to Internet.

Go to Security Management > Authentication > Authentication Mode > Local Authentication > Authorization Authentication, and then configure parameters such as the prompt information for scanning code, authentication IP/VLAN, and online duration in the Function Editing page.

Scan QR Code Authentication

After you enable this, authenticated users can scan the specified QR code to access the Internet.

Enter Security Management > Authentication Portal > Authentication Mode > Local Authentication > QR Code Authentication, and configure parameters such as QR code information, authenticated IP address/VLAN, and online duration in the Function Edit page.

Authentication-Free Zone

Set terminals for exempting from authentication, WAN IPs for exempting from authentication, and domain names for exempting from authentication.

Enter Security Management > Authentication Server > Authentication Mode > Local Authentication > No Authentication, select the group, and click Add. Follow the prompts to enter the information about the device.

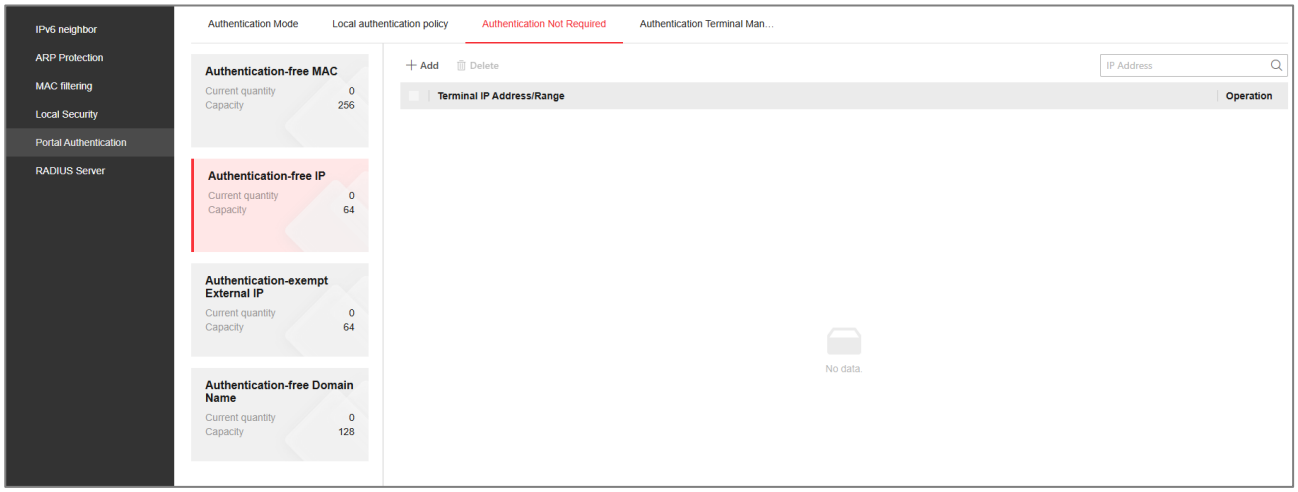

Figure 4-22 Authentication-Free Zone

Authentication Terminal

Enter Security Management > Authentication Configuration > Account Authentication > Authentication Terminal or Security Management > Portal Authentication > Authentication Mode > Local Authentication > Authentication Terminal.

View authenticated terminal information and set offline detection mode. Terminals will be forced offline if no network data is detected in the configured time period.

4.6.2 Cloud Authentication

Note

Not all devices support this function. For details, see the actual interface.

Supports Hik-Partner Pro for cloud-based authentication.

Cloud Authentication Configuration

Step 1 Enter Security Management > Authentication Mode > Cloud Authentication.

Step 2 Click Enable Cloud Authentication.

Step 3 Select the cloud server type and configure its parameters.

Note

If you select CMCC2.0 Third-Party Server, you can configure the server in Security Management > Authentication > Authentication Mode > Cloud Authentication > Portal Server.

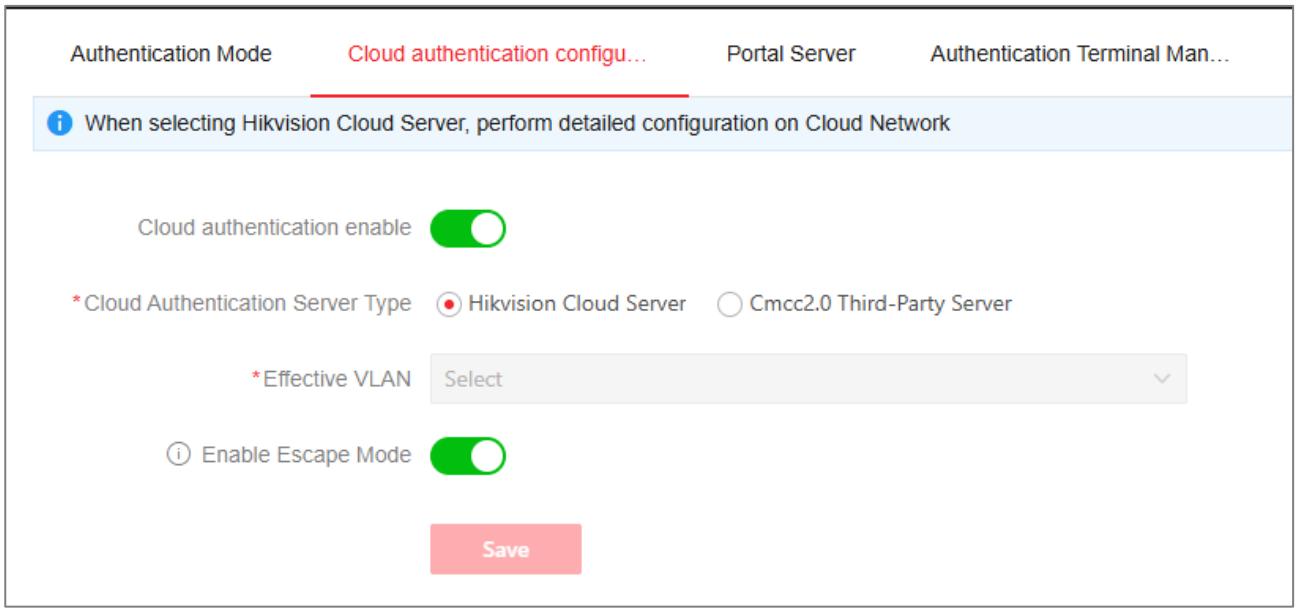

Figure 4-23 Set Cloud Authentication

Step 4 (Optional) Enable escape mode to bypass authentication when server is abnormal.

Step 5 Click Save.

iVMS Portal Server

Step 1 Enter Security Management > Authentication Mode > Cloud Authentication > Portal Server.

Step 2 Click Add.

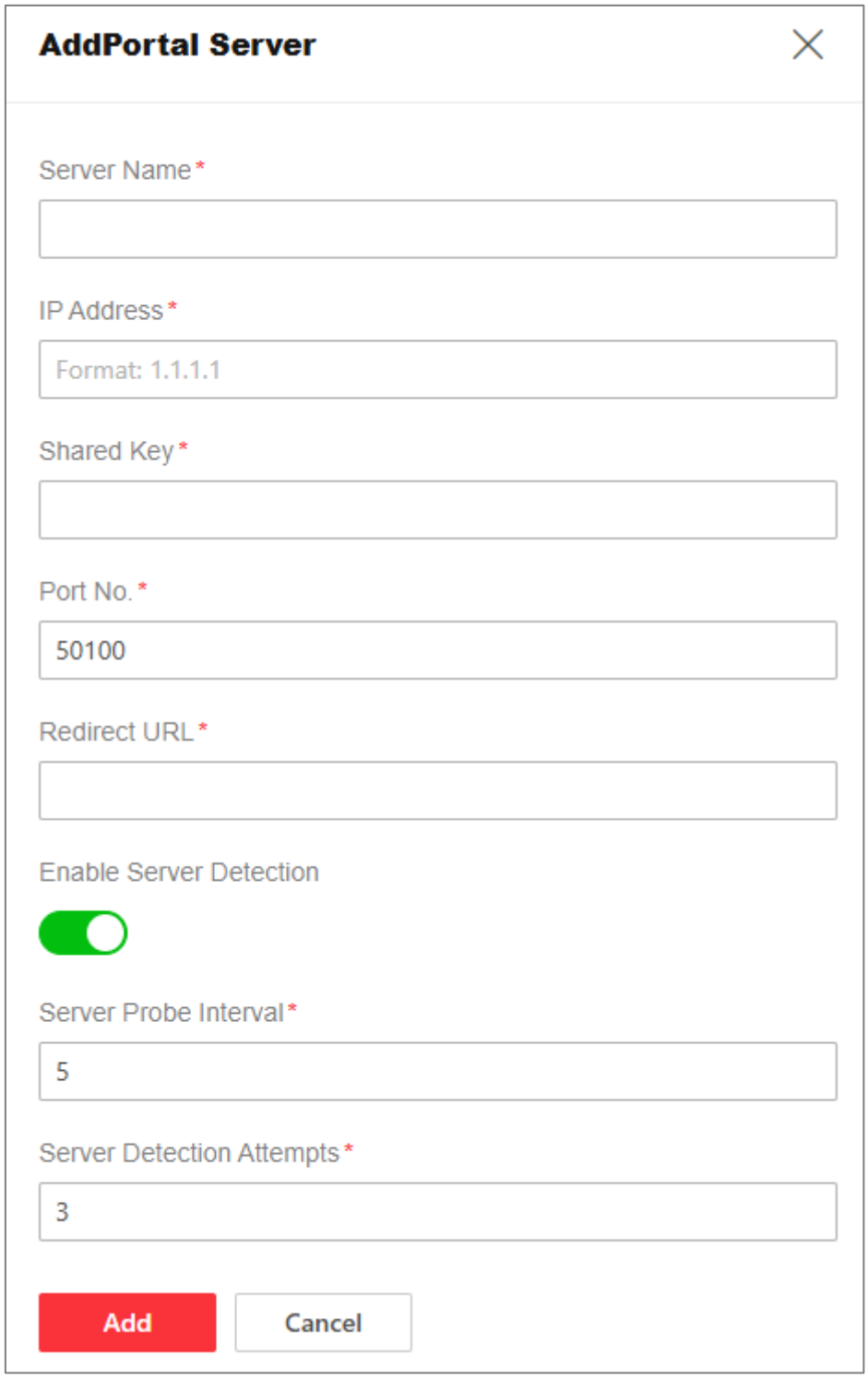

Figure 4-24 Add Portal Server

Step 3 Configure server parameters.

Step 4 Click Add.

Step 5 (Optional) You can click to edit the added server(s) later.

Step 6 (Optional) You can click to delete the added server(s) if needed.

Authentication Terminal Management

Go to Security Management > Authentication > Authentication Mode > Cloud Authentication > Authentication Terminal Management to view the information of the authentication terminals, including user name, IP address, and MAC address.

4.7 RADIUS Server

Note

Not all devices support this function. For details, see the actual interface.

Supports configuration and maintenance of Radius server for remote user authentication, authorization, and billing to ensure network access security.

4.7.1 Global Configuration

Enter Security Management > RADIUS Server > Global Configuration to configure the global parameters of the server.

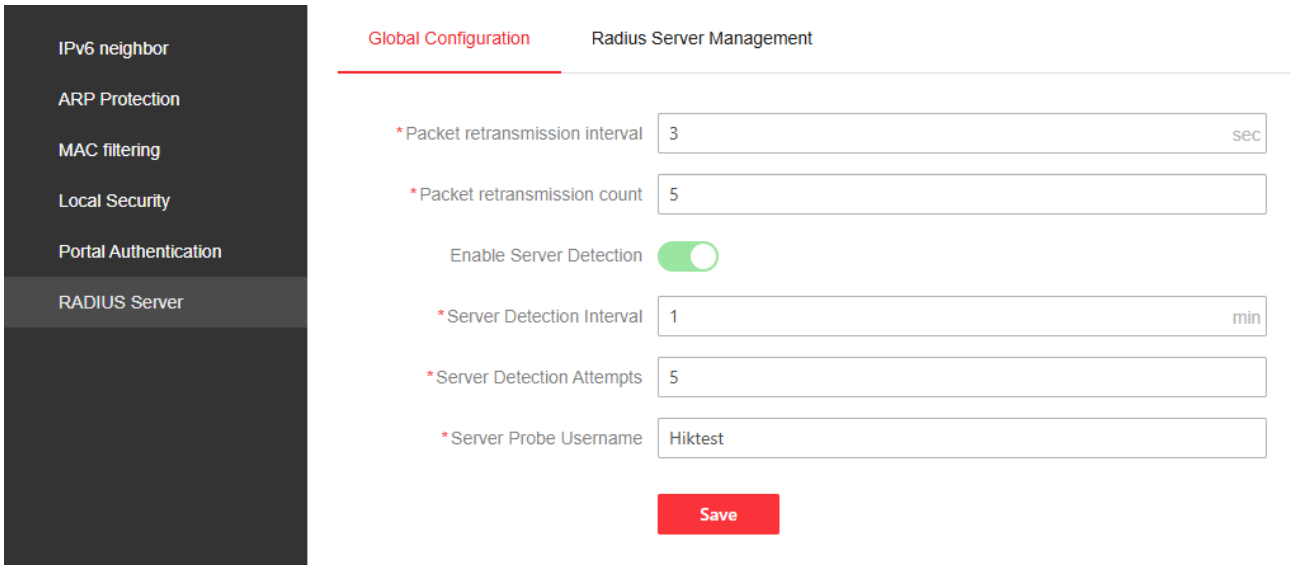

Figure 4-25 Global RADIUS Server Configuration

4.7.2 Server Management

Support group management of RADIUS servers to improve business reliability, load balancing, and flexibility.

Step 1 Enter Security Management > RADIUS Server > RADIUS Server Management.

Step 2 Tap Add / Tap to add server group, enter the server name, and add the server group.

Step 3 Click the upper-left corner of the server group card to add a server, and enter relevant parameters to add server members to the current server group.

Step 4 Click Add.

Step 5 (Optionally) Click the "Drag and drop to sort" button in the upper-left corner of the server group card to sort the existing servers within the group. In each server group, servers are matched from top to bottom.

Step 6 (Optional) You can click the upper-right corner Delete of the server group card to delete the server group. Click  in the Operation list to limit the terminal's downstream rate and upstream rate.

Chapter 5 Network Configuration

Note

The configuration functions supported by different device models/versions may vary. For details, see the actual interface.

5.1 DHCP Configuration

After enabling the DHCP server, you can automatically assign IP address to terminal devices. For details about basic DHCP configuration, please refer to 4.2.1 Adding VLAN.

5.1.1 Configure DHCP Option

The DHCP Server option is shared by all LAN ports.

Step 1 Go to Network Management > LAN Configuration > DHCP Option.

Step 2 Configure the Following Parameters:

- DNS Server and Alternate DNS Server: The DNS server address provided by the carrier.
- Option 43: When the gateway and AP are not in the same LAN, or when there are multiple gateways in the network environment, you can configure Option 43 to let AP discover the gateway.

  Caution

  - Enter #HK# at the beginning of the IP address, such as #HK#192.168.188.1.
  - To let the AP get IP address and join the network quickly, it is recommended that you select the APs to restart in Wireless Management > AP List.
- Option 138: Gateway IP address. When the gateway and AP are not in the same LAN, or when there are multiple gateway devices in the network environment, you can set Option 138 to let AP get the IPv4 address of the gateway.
- Option 150: TFTP Server Address. Specify the TFTP server address for clients.
- Enable address conflict detection: If enabled, when the DHCP server allocates an IP address, it will first check whether the target IP address is occupied and then decide whether to allocate the address to reduce network faults caused by conflicts.

5.1.2 Assign Static Address

You can reserve an IP address for a specified MAC address. When the host requests an IP address from the DHCP server, the server will assign the reserved IP address to it.

Step 1 Go to Network Management > LAN Configuration > Static Address Allocation.

Step 2 Click Add.

Step 3 Enter ***the*** spec***ifie***d MAC address and reserved IP address.

Step 4 Click Add.

Step 5 (Optional) In the list page, you can search for devices by MAC address or IP address, and select No. to delete the assigned device(s).

5.1.3 View Client List

Go to Network Management > LAN Configuration > Client List to view the information about the client.

- Search by host name, MAC address, or IP address.
- Click Bind as Fixed Address after a single host entry, or select multiple host entries and click Bind as Fixed Address in the upper-left corner of the list, and then confirm to quickly bind MAC address and IP address.

5.1.4 Set DNS Proxy

The DNS server proxy is optional. The device will get the DNS server address from its parent device by default.

Note

Not all device models or versions support port DNS configuration. Refer to actual interface.

Step 1 Go to Network Management > LAN Configuration > DNS Proxy.

Step 2 Enable DNS Server Proxy and enter the server IP address.

Step 3 Click Save.

5.2 IPv6 Configuration

Enter "Network Management > IPv6 Configuration". Enabling it can resolve the issue of insufficient network address resources in IPv4.

After the WAN and LAN port IPv6 information is configured, the device can act as a DHCPv6 server to assign IPv6 address to terminals. Go to DHCPv6 Dynamic Address Allocation to view client information.

5.2.1 Configure WAN IPv6 Address

Basic Configuration

Go to Network Management > IPv6 Configuration > WAN Configuration, and make sure that the IPv6 function is enabled.

- Select Configuration: Select the WAN port to configure.

- Internet access method: Select one of the following options.
- Dynamic IP: When the device is set as a DHCPv6 client, it can apply for an IPv6 address/prefix from the upstream device and no manual configuration is required.
- Static IP: manual verification of IPv6 address/length, gateway address, and DNS server is required.
- None: The IPv6 function is not enabled on the WAN port.
- NAT66: When enabled, the IPv6 address of the terminal can be accessed via the WAN if it is also a private IPv6 address. Default is disabled.
- Default Routing Priority: Set the priority of the default routing for the current route. The smaller the value, the higher the priority. When choosing the optimal route for a destination address, the system will select the route with the highest priority.

Set IPv6 Load Pattern

Please make sure that IPv6 is enabled.

Note

- Not all devices support this function. The actual interface may vary.
- In non-Line pattern, IPv6 Load is disabled by default.

Step 1 Go to Network Management > IPv6 Configuration > WAN Configuration > Load Settings.

Step 2 Enable and select multi-link load balancing mode.

- Round Robin: Network data is allocated to WAN ports according to the weights of the WAN ports.

1. Set Load Balancing Strategy to Connection-Based or Source IP-Based.
2. Set the weights for WAN ports. The weight range is from 1 to 1000, and the default value is 1.

- Main and Standby: When the main interface is working normally, all traffic will go through the main interface; when the main interface fails, traffic will automatically switch to the standby interface. For multiple standby interfaces, the priority of interface 1 is higher than that of interface 2.

Configure IPv6 Link Layer Detection

Please make sure that IPv6 is enabled.

When the gateway is not in single-line mode, you can configure and display IPv6 line detection, which sends detection messages at regular intervals to check whether the gateway can ping the corresponding address.

Step 1 Go to Network Management > IPv6 Configuration > WAN Configuration > Line Detection.

Step 2 Enable IPv6 address line probing.

Step 3 Click the operation icon of an API in the list (you can edit the set line crossing rule).

Step 4 Set the probe interval, required online/offline rounds, and add destination IP address/domain name.

- probe interval: The time interval between two consecutive probes to the destination address or domain name of a line.
- times to ping successfully for WAN online status: If the line detection can be pinged and the number of consecutive pings that are successful reaches the set times to ping successfully for WAN online status, the WAN is in online status.
- times to be offline: If the WAN is not pinged back and the number of consecutive failed pings reaches the set times to be offline, the WAN will be marked as offline.
- destination address/domain name: The destination address or domain name to which the system sends Ping packets.

Step 5 Click Save.

5.2.2 Set LAN Port IPv6 Address

Step 1 Go to Network Management > IPv6 Configuration > LAN Configuration to ensure that the IPv6 function is enabled.

Step 2 Click Add in the VLAN ID list to add a VLAN, or click  to edit a VLAN.

- VLAN ID: Select an existing VLAN or add a new VLAN ID.
- Address Allocation Method
  - Auto (Recommended): Use DHCPv6 and SLAAC to assign IPv6 address to terminals.
  - DHCPv6: To assign an IPv6 address to the terminal via DHCPv6 protocol.
  - SLAAC: Stateless Address Auto configuration (SLAAC) is an IPv6 mechanism for automatically assigning IP addresses without DHCP servers.
  - Not Assigned: No address is assigned to the device.
- IPv6 address/length: Enter a local address with a length not exceeding 64 bits, and the length of this address.
- Subnet Prefix Name: Select IPv6 address as the default.
- Subnet Prefix Length: The range of the subnet prefix length is from 48 to 64.
- Subnet ID: The value should be in hexadecimal format. 0 means auto-increment.
- Address Lease Time: The unit is minute(s).
- IPv6 DNS server address: The address of the DNS server.
- Alternate DNS Server: Configure the alternate IPv6 DNS server address.

5.2.3 Configure DHCPv6 Address

DHCPv6 (Dynamic Host Configuration Protocol for IPv6, IPv6 dynamic host configuration protocol) is a protocol that allows a DHCPv6 server to pass configuration information (such as parameters like IPv6 network addresses, DNS, NIS, and SNTP server addresses) to IPv6 nodes. By configuring the DHCPv6 function, gateway devices can provide LAN users with IPv6 addresses.

Optional Operation:

- Dynamic Address
  - View Dynamic Address Allocation Information: Enter Network Management > IPv6 Configuration > DHCPv6 Dynamic Address Allocation.
  - Bind dynamic address to static address: Select an item in the list and click the icon, or select multiple items and click Batch Bind as Static Type.
  - Search: Enter the DUID or IPv6 address in the search box to find the entry.
- Static Address
  - View static address binding information: Go to Network Management > IPv6 Configuration > Static DHCPv6.
  - Manually bind static address: Click Add, enter IPv6 address and DUID, and then click Save.
  - Search: Enter the DUID or IPv6 address in the search box to find the entry.

5.3 IPTV Configuration

By enabling IPTV service, you can enjoy multimedia services via IPTV TV while surfing the Internet.

Step 1 Enter Network Management > IPTV Configuration, and click Start Configuration.

Step 2 Select the type of modem and connect the device.

- If the optical modem does not have an IPTV port, select Single-Line Type.

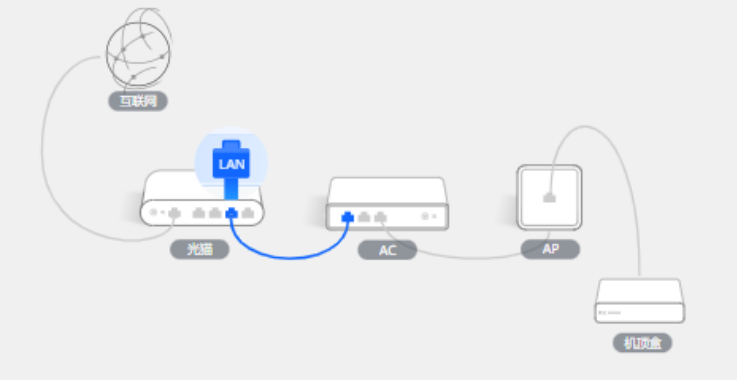

Figure 5-1 Single Line Type Connection

- If the optical modem has an IPTV port, you can select dual-line type.

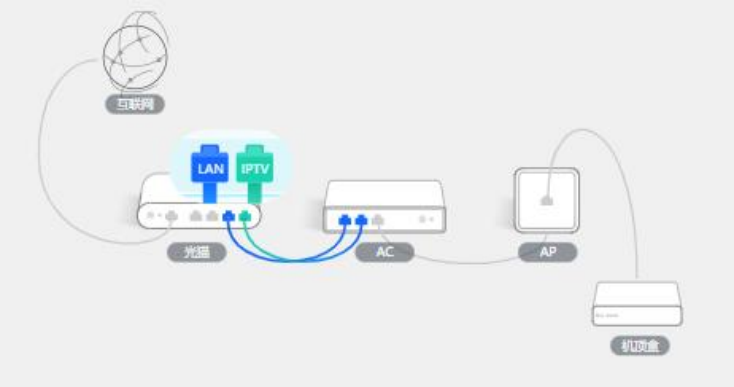

Figure 5-2 Double Line Type Connection

Step 3 Select the uplink port, i.e., the LAN port of the gateway device connected to IPTV.

Note

For dual-line type, you need to select the uplink port.

Step 4 Select the downstream port, i.e., the LAN port of the gateway device connected to the AP.

Note

The uplink port and downlink port cannot be set as the same LAN port in dual-line mode.

Step 5 Select the AP and VLAN ID connected to TV. The VLAN ID should be the same as that provided by the IPTV operator.

Step 6 Click Finish.

5.4 Port Configuration

If you need to define the description, status, etc., of the port, configure the port attributes.

Step 1 Enter Network Management > Port Configuration.

Step 2 Select the ports to configure, or click + in Port Configuration to select all ports.

Step 3 Configure the relevant port attribute parameters according to your actual needs.

- Enable port: Select to enable or disable the port. If disabled, no data will be transmitted via the port.
- Rate: The data transmission rate of the port. Supports configuration of 10M/100M/1000M, and the default is auto.
- Duplex: Select the port working mode.
  - Half-Duplex: Supports bidirectional data transmission but cannot transmit data simultaneously.
  - Full-Duplex: Supports bidirectional data transmission and can send and receive data simultaneously.

– Auto: Default to auto.

- Enable flow control: After you enable port flow control, you can prevent packet loss. The function is disabled by default.

Step 4 Click Save.

Step 5 Optional Operation:

- View the basic information of port status, including port switch, port speed, work mode, flow control, etc. Click Refresh to view the latest status information of device ports.
- View the port traffic data, including port rate, input/output rate, received/sent bytes, received/sent data packets, CRC/FCS error packets, incomplete/oversize data packets, and collision times. The port data is refreshed every 5 minutes and supports manual refresh and clear all.

5.5 Port Aggregation

Note

Not all devices support this function. The actual interface may vary.

Port aggregation is to combine multiple physical ports into one logical port for load balancing and increasing bandwidth. When a member port's link fails, you can select another available port as the sending port to ensure reliable transmission.

Step 1 Enter Network Management > Port Aggregation.

Step 2 Click the port in the Port Aggregation panel to select it.

Step 3 Select aggregation group number.

Step 4 Click Save.

Step 5 (Optional) You can delete an aggregation group or edit member ports.

Note

- Only Layer 2 aggregation of the LAN port is supported.
- Aggregation is not supported when the number of aggregation groups is more than 3, the number of participants is less than 2, or the number of LAN interfaces on devices is less than 2.
- The port type, rate, duplex mode, and aggregation type of the ports to be added to an aggregation port must be identical; otherwise, the aggregation will fail. After configuring

an aggregation port, the port attributes will be modified to the default state of full-duplex, 1000M, and flow control disabled.

- The configuration of the port in use will affect the separate sending and receiving of packets after it is added to an aggregation group.
- Ports with port security and MAC address authentication enabled cannot be added to LAGs.
- After aggregation, the aggregated port supports port settings information. The configuration will be kept after rebooting.

Chapter 6 Security Management

Note

The configuration functions supported by different device models/versions may vary. For details, see the actual interface of your device.

6.1 IPv6 Neighbor

IPv6 Neighbor Discovery Protocol is a basic protocol for IPv6. It utilizes five types of ICMPv6 messages—NA, NS, RA, RS, and Redirect—to determine the relation and address information between neighbor nodes, enabling functions such as address resolution, verifying if neighbors are reachable, duplicate address test, router discovery/prefix discovery, address automatic configuration, and Redirect. IPv6 neighbors can be manually configured as needed.

Step 1 Go to Security Management > IPv6 Neighbor Discovery.

Step 2 Add Dynamic IPv6 Neighbor

1. Click Add.
2. Configure IPv6 neighbor parameters.
   - specified output interface: the specified physical output interface for message forwarding.
   - Destination MAC address / Device MAC address: The specified MAC address corresponding to the destination IPv6 address.
   - Destination IPv6 Address/IPv6 Address: Specifies the IPv6 address of the neighbor.
3. Click Add.

Note

- The same MAC address can be bound to multiple IPv6 addresses.
- The same IPv6 and MAC address can be bound to different ports.
- Two devices with the same IPv6 address and different MAC addresses cannot be bound to the same port.

Step 3 Select the dynamic entry in the list, and click Bind / in the operation bar to bind a static IPv6 address.

Step 4 (Optional) You can also perform the following operations as needed:

- Select multiple dynamic entries, and then click Batch Link to Static Address above the list to link them to static addresses in batches.
- Select multiple dynamic entries and click Batch Delete/Delete above the list to batch delete dynamic entries.

- Click Refresh to refresh the list of entries.
- You can search for relevant items by IP address or MAC address in the search box.

Note

If the static entry is online, deleting it will make it dynamic; if the static entry is offline, deleting it will delete the static entry.

6.2 ARP Protection

6.2.1 ARP Binding

Enable the Gateway ARP Protection function on devices that are not connected to the gateway via interfaces. After the function is enabled, when an interface receives an ARP message, it will check whether the source IP address in the ARP message is the same as the IP address of the protected gateway. If yes, the message is considered illegal and will be discarded; if no, the message is considered legal and will be handled normally.

Step 1 Enter Security Management > ARP Protection.

Step 2 Enable the function.

Step 3 Click Add.

Step 4 Enter the IP address and MAC address of the AP to be bound.

Note

- The IP address cannot be the same as that configured in an ARP entry.
- The MAC address in static entries cannot be the same as that in existing entries. The MAC address in static and dynamic entries can be the same.

Step 5 Click Add.

Step 6 Select the binding relations, and then click Bind as Static Type above the list to batch bind them, or directly click the operation bar behind each item for individual binding.

Note

- After binding as static type, only devices linked can access the device network, which can effectively reduce ARP attacks and IP address conflicts, and improve network stability.
- Static type is recommended for small-scale network deployment with less than 100 devices.
- The maximum number of static and dynamic entries may vary for different models. Please refer to the actual interface.

Step 7 (Optionally) Some Devices support clicking "Edit" below the outbound API to force link ARP (Address Resolution Protocol) table entries with a specified outbound interface, ensuring that network data is forwarded from the specified interface.

6.2.2 ARP Spoofing

The ARP spoofing protection can prevent the LAN/WAN side server from being attacked and deceived by ARP.

Step 1 Go to Security Management > ARP Protection > ARP Anti-Spoofing.

Step 2 Enable the function.

If enabled, when the device detects that there is an ARP spoofing device in the network, it will delete the device from the network.

6.3 MAC Filtering

After enabling MAC filtering, you can control the terminals' access to Internet via the set filtering type.

Set Blocklist

Step 1 Go to Security Management > MAC Filtering > Blocklist.

Step 2 Add or import blocklist.

- Click Add to Blocklist and select MAC address in ARP table or click Manual Verification to enter MAC address manually.
- Click Import Blocklist to import the pre-filled Excel file.

Step 3 (Optional) Click Tag Management to add labels for subsequent terminal classification and management.

Step 4 Click Add.

Set Authorization List

Step 1 Enter Security Management > MAC Filtering > Authorization List.

Step 2 Add or import an authorization list.

- Click Add Authorization List, and then select MAC address from the ARP list or manually add MAC address.
- Click Import Authorization List to import the pre-filled Excel file.

Step 3 (Optional) Click Label Management to add labels for subsequent terminal classification management.

Step 4 Click Add.

Step 5 (Optional) Click Add Online Terminal to quickly add MAC addresses of terminals for the authorized user.

Enable MAC Filtering

Step 1 Enter Security Management > MAC Filtering > MAC Filtering.

Step 2 Enable the function and select filtering type.

- Allowlist: Only terminals in allowlist can access WAN.
- Blocklist: The terminals in the blocklist are not allowed to access WAN.

Step 3 Click Save.

6.4 Local Security

Note

Not all devices support this function. For details, see the actual interface.

6.4.1 Set Security Zone

Security Zone is primarily used to manage multiple APIs on firewall Devices that share the same security requirement. By dividing APIs into different security domains, unified management of security control policies can be achieved.

Add Security Zone

You can add security domains according to the overall planning.

Step 1 Enter "Security Management > Local Security > Security Zone".

Step 2 In the Security Zone Configuration module, click Add.

Step 3 Enter the domain name, configure the domain API, allow access to the domain, and disable services.

Note

Description of Disabled Service Options:

- ***Ping***: If selected, terminals in this domain cannot ping the device.
- ***Web:*** If you select this, terminals in the domain cannot access the device's Web page.
- ***DNS***: If selected, terminals in the security zone will not be able to access web pages if they use the local address as their DNS server.
- ***DHCP***: If selected, terminals in this security zone cannot access the DHCP service of the device.

Step 4 Click Add.

Step 5 (Optional) Click the Edit button in the operation bar at the lower part of the page to edit the current configuration item.

Step 6 (Optional) Click the picture in the operation bar above the list to delete the current entry.

Add Allowlist

You can add allowlist to further refine the resource access permission.

Step 1 Enter "Security Management > Local Security > Security Domain".

Step 2 In the Allowlist Configuration module, click Add.

Step 3 Enter the name and configure other parameters.

Step 4 Click Add.

Step 5 (Optional) Click the Edit button in the operation bar at the lower part of the page to edit the current configuration item.

Step 6 (Optional) Click the picture in the operation bar above the list to delete the current entry.

6.4.2 Anti-Attack Configuration

Step 1 Go to Security Management > Local Security > Anti-Attack.

Step 2 Enable and configure the anti-attack function if needed.

- DDoS protection: By identifying, blocking, or mitigating malicious traffic, this service ensures the normal operation of your business. Please enable it and set the limit rate reasonably. If the limit rate is too low, it may affect the access of your normal business.
- Anti-Suspicious Packet Attack: By identifying and blocking network data packets that do not conform to protocol specifications or have malicious features, this function can prevent attackers from using malformed packets or forged packets to attack the system.
- Local Packet Management: Control, monitor, and optimize the network data packets sent by the device to prevent malicious or abnormal packet sending behaviors.
- Anti-Session Attack: Identifying and blocking malicious operations against user sessions to ensure

the legality and security of sessions within their lifecycles.

Step 3 Click Save.

Step 4 (Optional) Click Restore Default to reset all settings to the factory settings.

Step 5 (Optional) Enter Device Management > Security Management > Security Log, and filter security logs by time period and keyword.

6.5 Portal Authentication

Supports forcing terminals to go through authentication before accessing Internet.

Note

- Not all models support this function. For details, see the actual interface.
- The functions supported and the way they are presented may differ among devices of different models/versions. Refer to actual device interface for details.

6.5.1 Local Authentication

Account Authentication

Step 1 Enable the function.

1. Enter Security Management > Authentication Mode > Local Authentication > Account Authentication.
2. In the function editing page, set parameters and click Save. The terminals in this IP address or VLAN need to be authenticated before they can access the Internet.
3. Enable.

Step 2 management account.

1. Enter Security Management > Authentication Portal > Authentication Mode > Local Authentication > Account Authentication.
2. In the function editing page, click "Add".
3. Set the account name, PIN, and max. number of persons allowed to log in simultaneously.
4. Click Add. Now the terminals in the IP address or VLAN need to enter account password for authentication to access the Internet.

Authentication and Authorization

After you enable the Authorization Authentication, when an authorized IP user scans the QR code on the pop-up window of the IP camera terminal, he/she can access to Internet.

Go to Security Management > Authentication > Authentication Mode > Local Authentication > Authorization Authentication, and then configure parameters such as the prompt information for scanning code, authentication IP/VLAN, and online duration in the Function Editing page.

Scan QR Code Authentication

After you enable this, authenticated users can scan the specified QR code to access the Internet.

Enter Security Management > Authentication Portal > Authentication Mode > Local Authentication > QR Code Authentication, and configure parameters such as QR code information, authenticated IP address/VLAN, and online duration in the Function Edit page.

Authentication-Free Zone

Set terminals for exempting from authentication, WAN IPs for exempting from authentication, and domain names for exempting from authentication.

Enter Security Management > Authentication Server > Authentication Mode > Local Authentication > No Authentication, select the group, and click Add. Follow the prompts to enter the information about the device.

Authentication Terminal

Enter Security Management > Authentication Configuration > Account Authentication > Authentication Terminal or Security Management > Portal Authentication > Authentication Mode > Local Authentication > Authentication Terminal.

View authenticated terminal information and set offline detection mode. Terminals will be forced offline if no network data is detected in the configured time period.

6.5.2 Cloud Authentication

Note

Not all devices support this function. For details, see the actual interface.

Supports cloud-based authentication via Hikvision Cloud Market/Hikvision Cloud Network Mobile Client.

Cloud Authentication Configuration

Step 1 Enter Security Management > Authentication Mode > Cloud Authentication.

Step 2 Click Enable Cloud Authentication.

Step 3 Select the cloud server type and configure its parameters.

Note

If you select CMCC2.0 Third-Party Server, you can configure the server in Security Management > Authentication > Authentication Mode > Cloud Authentication > Portal Server.

Step 4 (Optional) Enable escape mode to bypass authentication when server is abnormal.

Step 5 Click Save.

iVMS Portal Server

Step 1 Enter Security Management > Authentication Mode > Cloud Authentication > Portal Server.

Step 2 Click Add.

Step 3 Configure server parameters.

Step 4 Click Add.

Step 5 (Optional) You can click to edit the added server(s) later.

Step 6 (Optional) You can click to delete the added server(s) if needed.

Authentication Terminal Management

Go to Security Management > Authentication > Authentication Mode > Cloud Authentication > Authentication Terminal Management to view the information of the authentication terminals, including user name, IP address, and MAC address.

6.6 RADIUS Server

Note

Not all devices support this function. For details, see the actual interface.

Supports configuration and maintenance of Radius server for remote user authentication, authorization, and billing to ensure network access security.

6.6.1 Global Configuration

Enter Security Management > RADIUS Server > Global Configuration to configure the global parameters of the server.

- message retransmission interval: The time interval between two consecutive RADIUS request messages when the system fails to receive the response from the RADIUS server.
- message retransmission times: The maximum number of message retransmissions allowed by the client before it gives up.
- Enable Health Check: Enable/Disable Active Health Check (detect whether the server is alive).

- Server Check Cycle: The interval between two consecutive server checks.
- server detection failure limit: The system will mark the server as unavailable and stop detecting if it fails to detect the server for consecutive times.
- server probe user name: A dedicated user name for health check.

6.6.2 Server Management

Group Management: Support for grouping RADIUS servers to improve business reliability, load balancing, and flexibility.

Step 1 Enter Security Management > RADIUS Server > RADIUS Server Management.

Step 2 Tap Add / Tap to add server group, enter the server name, and add the server group.

Step 3 Click the upper-left corner of the server group card to add a server, and enter relevant parameters to add server members to the current server group.

Step 4 Click Add.

Step 5 (Optional) Click the "Drag and drop to sort" button in the upper-left corner of the server group card to sort the existing servers within the group.

In each server group, servers are matched from top to bottom.

Step 6 (Optional) You can click the upper-right corner Delete of the server group card to delete the server group.

Chapter 7 Internet Behavior Management

Note

The supported configuration functions may vary for different device models/versions. Refer to the actual interface.

7.1 Application Control

Set application control rules to limit specific users from using applications during certain time periods.

7.1.1 Custom Application

Add other applications except the default application.

Step 1 Go to Behavior Management > Application Control, and click Custom Application.

Step 2 Click Add.

Step 3 Set the new application name, protocol type, and rule type, and enter the corresponding IP address according to the rule type.

Step 4 Click Add.

7.1.2 Custom Application Group

You can add applications to custom groups for convenient application control rule settings.

Step 1 Go to Behavior Management > Application Control > Custom Application Group.

Step 2 Click Add.

Step 3 Set Application Group Name and select applications from the list. You can select all applications by category, or select individual applications manually.

Step 4 Click Add.

7.1.3 Set Application Control Rules

Step 1 Go to Behavior Management > Application Control > Application Control.

Step 2 Click Add.

Step 3 Set Application Rules:

- Address Type: Address of users who are not allowed to use the application.
  - If you select address group, you need to select an address group or create a new one. Address group supports adding multiple IP address segments.

– If you select Custom, you need to set the IP address range and add multiple IP address ranges.

- Managed Time Period: Select an existing time period or create a new one for this application control rule to take effect.
- Disabled Application Type: Select applications from the application list, or select a custom application group.

Step 4 Click Add.

7.2 Website Management

You can set website filtering rules to limit specific users' access to certain websites during specific time periods.

7.2.1 Website Group

Go to Behavior Management > Website Control > Website Group or Behavior Management > Website Management > Website Group.

- Click to view all the sites contained in each group.
- Click  to edit the name of an existing group and the websites in it.
- Click Add to create a custom group for the website.
- Click  to delete the existing group.

7.2.2 Set Website Filtering Rule

Step 1 Go to Behavior Management > Website Control > Website Filtering or Behavior Management > Website Management > Website Filtering.

Step 2 Click Add.

Step 3 Select managed IP address group, managed time period, and disabled website type.

Step 4 Click Add.

7.3 Access Control

Set access rules to control whether LAN users can access WAN.

Step 1 Enter Behavior Management > Access Control.

Step 2 Click Add.

Step 3 Set Access Rule

- Access rule based on MAC address: Control the access of specific MAC address terminals to WAN in the effective period, allowing or denying access.
- Access Rule Based on IP Address: The data stream will be matched with the source IP address, destination IP address, protocol, etc. of the rule, and then the system will block or allow the data stream according to the settings in the effective period.

Step 4 Click Add.

Step 5 (Optional) When multiple rules match, click Edit Matching Order above the list, and drag to sort the rules.

Note

- The rule based on IP address settings is not matched reversely.
- If multiple rules match with the same target, the system will execute them in the specified order and stop when one of them is triggered successfully.
- No more than 64 access control rules can be configured.
- Access Control rules do not apply to devices in the same VLAN.

7.4 Flow Control Settings

Supports classifying network data according to certain rules and handling the data in different ways based on their categories.

7.4.1 Flow Control

Enter Behavior Management > Flow Control Settings > Intelligent Flow Control or Behavior Management > Flow Control Settings > Traffic Control, and enable this function to set the upstream and downstream bandwidth for different WAN ports when the bandwidth is insufficient or you need to reasonably allocate network data.

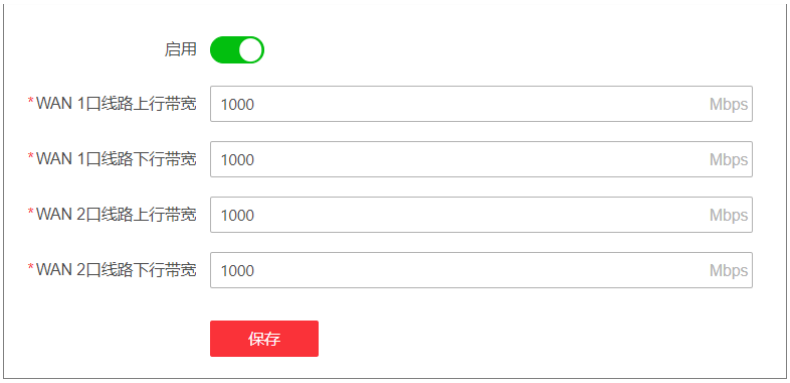

Figure 7-1 Intelligent Flow Control

7.4.2 Custom Policy

Supports rate limiting for specific IP address segments.

Step 1 Go to Behavior Management > Flow Control Settings > Custom Policy.

Step 2 Click Add.

Step 3 Set the name of the access level.

Step 4 Set IP addresses to be speed limited via address group or custom mode.

Step 5 Select the bandwidth mode and application API, and set the maximum upstream and downstream bandwidth.

Step 6 Click Add.

7.4.3 VPN Flow Control Policy

Manage and optimize the network data in VPN network to ensure proper allocation of network resources.

Note

Not all devices support this function. Refer to the actual interface of your device.

Step 1 Go to Behavior Management > Flow Control Settings > VPN Flow Control Policy.

Step 2 Click + to add a strategy.

Step 3 Set the name of the access level.

Step 4 Set IP addresses to be speed limited via address group or custom mode.

Step 5 Set upstream and downstream bandwidths and API.

Step 6 Click Add.

Step 7 (Optional) Enable, disable, edit, or delete the added access levels.

Step 8 (Optional) Click Drag and Drop to sort the current strategy by dragging ≡.

Chapter 8 VPN Management

A VPN (virtual private network) is a technology that establishes an encrypted connection via a public network (such as the Internet) to transmit data securely in an insecure network environment.

Note

- Not all models support this function. For details, see the actual interface.
- The configuration functions supported by different device models/versions may vary. For details, see the actual interface.

8.1 IPSec

IPSec (IP Security, IP security) is a three-layer tunneling encryption protocol developed by the Internet Engineering Task Force (IETF) to provide end-to-end encryption and authentication services for networks, offering high-quality, interoperable, and cryptographically secure protection for data transmitted over the network.

IPSec protocol is widely used for networking interconnection between headquarters and branches of organizations. Currently, the device supports deploying IPSec server or client. Based on IPSec protocol, a secure tunnel can be built between headquarters and each branch, which can ensure the confidentiality of transmitted data and improve network security.

In the IPsec configuration process, you can use the Internet Key Exchange (IKE) protocol to establish Security Associations (SA). The IKE protocol provides services of automatic negotiation, exchanging keys, establishing, and maintaining SAs for IPsec, which simplifies the usage and management of IPsec.

The IPSec Security Policy is designed to set up matching security policies on both ends of communication so that an IPSec security tunnel can be established between the IPSec client and server for protecting the communication data.

Before adding an IPsec VPN policy, you need to complete the basic configuration of LAN and WAN on both devices. (For details, refer to Chapter 4 Common Configuration.)

8.1.1 Set IPSec Server

Basic Settings

Step 1 Go to VPN Management > IPsec > IPsec Security Policy.

Step 2 Enable the function.

Step 3 Set Strategy Type to Server or Server Cluster.

Step 4 Enter Related Parameters

Note

The available parameters may differ among devices of different models/versions. Refer to the actual device interface for details.

- Strategy Name: You can customize the name.
- Bind Interface: Set the WAN port for local use in the API binding. If you have multiple WAN lines, it is recommended to set it as "Auto".
- IKE: Internet Key Exchange Protocol. Select the protocol to establish Security Associations (SAs) for IPSec VPN.
- Local Subnet Range: The LAN port subnet range of the server.
- Pre-Shared Key: Each IPSec server and client pair should be configured with the same unique pre-shared key.

Step 5 Click Save.

Phase I Settings (IKE Policy)

Keep the default configuration if no special requirements exist.

- IKE Policy: The IKE protocol consists of a combination of three parameters: "hash algorithm - parameter encryption algorithm - Diffie-Hellman group identifier". Support for setting up 5 IKE policies is available, and both parties involved in the IKE negotiation must have at least one consistent IKE policy.
- Negotiation Mode
  - Main Mode: In this mode, the authentication is conducted after key exchange, and more steps are required for negotiation. It is applicable to scenarios with strict requirements on identity protection.
  - Rapid Mode: Authentication and key exchange are conducted simultaneously with fewer negotiation steps, which is applicable to scenarios with less stringent requirements for identity protection.
- Local ID type: The local device identity type and identity used for IKE authentication. Should be consistent with the peer ID type.
- Remote ID Type: The type of the remote device identity for IKE authentication. It should be consistent with Local ID Type.
- Time To Live: The time interval for IKE re-negotiation. When the time interval is exceeded, the system will trigger re-negotiation of the related IKE parameters.
- DPD test: Peer Detection, used for IPsec neighbor status detection. When the link is unstable, it is recommended to configure DPD function.
- DPD detection cycle: Set the cycle of DPD detection for specified peer, i.e., the interval time for triggering DPD query.

Phase 2 Settings (Connection Strategy)

Keep the default configuration if no special requirements exist.

- Transformation Set: A combination of "Security Protocol - Encryption Algorithm". During the IPSec Security Association negotiation, both sides use the same specific transformation set to protect certain data streams. The transformation set configurations on the IPSec server and client should be consistent.
- PFS (perfect forward secrecy): PFS is a security feature that ensures the compromise of one key does not affect other keys, as these keys have no derivation relationship. When using a security policy to initiate an IKE SA negotiation, IKE can perform a PFS exchange. If this end sets the PFS feature, the remote end should also set the PFS feature, and the specified DH group of this end and the remote end should be the same, or the negotiation will fail.
- Time To Live: The time interval for re-negotiation of the conversion set. If the time interval exceeds the value configured in the parameter, the conversion set will be re-negotiated.

8.1.2 Set IPSec Client

Step 1 Go to VPN Management > IPsec > IPsec Security Policy.

Step 2 Enable the function.

Step 3 Select Client as the strategy type.

Step 4 Enter Related Parameters

Note

The available parameters may differ among devices of different models/versions. Refer to the actual device interface for details.

- Strategy Name: You can customize the name.
- Remote Gateway: The IP address or domain name of the remote gateway.
- Alternate Gateway: The alternative IP address or domain name of the peer gateway.
- Bind Interface: Set the WAN port for local use in the API binding. If you have multiple WAN lines, it is recommended to set it as "Auto".
- IKE: Internet Key Exchange Protocol. Select the protocol to establish Security Association (SA) for IPSec VPN.
- Local Subnet Range: The LAN port network segment of the customer's device.
- Terminal Network Range: The LAN port network segment of the server.
- Pre-Shared Key: Each IPSec server and client pair should be configured with the same unique pre-shared key.

Step 5 (Optional) For advanced settings, refer to Phase 1 settings (IKE policy) and Phase 2 settings (connection establishment policy). If there are no special requirements, keep the default configuration.

Step 6 Click Save.

Step 7 (Optional) After you complete the configuration on both ends, go to VPN Management > IPsec > IPsec Connection Status to view the connected status.

8.2 L2TP

L2TP (Layer Two Tunneling Protocol) is a virtual tunnel protocol that is commonly used in virtual private networks.

The L2TP protocol itself does not provide functions of encryption and reliability verification, but it can be used in combination with security protocols to realize encrypted data transmission. The L2TP protocol is often used in combination with the IPsec protocol, i.e., the message is encapsulated by L2TP first and then encapsulated by IPsec, where L2TP is used to realize user authentication and address allocation, and IPsec is used to ensure the security of communication.

L2TP VPN can be used to build secure tunnels between branch offices and headquarters, as well as for roaming employees to access the headquarters. The current device supports L2TP server or client deployment.

8.2.1 Set L2TP Server

Step 1 Enter VPN Management > L2TP > L2TP Settings.

Step 2 Enable the function.

Step 3 Set Strategy Type to Server or Server Cluster.

Step 4 Enter Related Parameters

Note

The available parameters may differ among devices of different models/versions. Refer to the actual device interface for details.

- Local Tunnel Address: The local virtual IP address of the VPN tunnel server. After dialing in, the client can access the server via this address.
- Address Pool IP Range: The range of IP addresses in the address pool that is used by the L2TP server to assign IP addresses to clients.
- DNS Server: The DNS address sent from the L2TP server to the client.
- Tunnel Authentication: The tunnel authentication request can be initiated by the client side. As long as one end has enabled tunnel authentication, it will only build a tunnel with the other end if tunnel authentication is also enabled on the other end, and the keys on both ends are completely consistent and not empty. Otherwise, the tunnel connection will be automatically disconnected at this end. If tunnel authentication is disabled on both ends, no authentication key is required when building the tunnel.
- Tunnel Authentication Key: Set this if you enable tunnel authentication.
- IPSec Encryption: Whether to encrypt the tunnel. If encryption is enabled, IPSec is used to encrypt the L2TP tunnel. If the current device has already enabled the IPSec security policy, IPSec encryption for the L2TP tunnel is not supported. The IPSec encryption configuration on the L2TP server and client should be consistent. (For IPSec-related parameters, please refer to 8.1.1 Settings IPSec Server) [MERGEFORMAT]
- Authentication Methods: PAP, CHAP, MS-CHAP, and MS-CHAPv2.

- Link Maintenance Interval: The interval of sending PPP link maintenance test messages after L2TP VPN is connected. It is recommended to keep the default value.

Step 5 Click Save.

8.2.2 Set L2TP Client

Step 1 Enter VPN Management > L2TP > L2TP Settings.

Step 2 Enable the function.

Step 3 Select Client as the strategy type.

Step 4 Enter Related Parameters.

Note

The available parameters may differ among devices of different models/versions. Refer to the actual device interface for details.

- User name and password: The user name and password for L2TP tunnel user identity verification. They should be the same as the server's settings for L2TP user.
- Binding Interface: WAN port used by the client.
- Local tunnel IP: The client virtual IP address of the VPN tunnel. Selecting "Dynamic" means the IP address is obtained from the server address pool. Selecting "Static" means manually configuring a static address within the range of the server address pool that does not cause conflicts as the local tunnel IP address.
- Server IP Address: Enter the WAN IP address or domain name of the server. The server's WAN IP address should be a public IP address.
- Target terminal network range: Enter the LAN network segment of the server you want to access. It cannot overlap with the LAN network segment of the client.
- Tunnel Authentication: If you enable tunnel authentication, enter the same tunnel authentication key as that on the server.
- IPSec Encryption: Match With Server
- Work Mode:
  - NAT: Perform NAT conversion on data packets passing through this L2TP tunnel (replace the source IP address of the data packet with the local virtual IP address of the L2TP tunnel). In NAT mode, the server cannot access the LAN of the client.
  - Routing: The server can access the client's LAN and only route and forward data packets that pass through this L2TP tunnel.
- Link Maintenance Interval: The interval of sending PPP link maintenance test messages after L2TP VPN is connected. It is recommended to keep the default value.
- Authentication methods: PAP, CHAP, MS-CHAP, and MS-CHAPv2.
- Redirect all network data via VPN: When enabled, the client will force all IPv4 traffic generated by the client to go through the VPN tunnel.

Step 5 Click Save.

Step 6 (Optional) After you complete the configuration on both ends, go to VPN Management > L2TP > Tunnel Information List to view the connected tunnels.

8.3 PPTP

PPTP (Point-to-Point Tunneling Protocol) is an enhanced security protocol developed on the basis of PPP (Point-to-Point Protocol). It allows enterprises to extend their private networks over public networks via "tunnels". PPTP VPN relies on PPP protocol for security functions such as encryption and authentication.

8.3.1 Set PPTP Server

Step 1 Enter VPN Management > PPTP > PPTP Settings.

Step 2 Enable the function.

Step 3 Set Strategy Type to Server or Server Cluster.

Step 4 Enter Related Parameters

Note

The available parameters may differ among devices of different models/versions. Refer to the actual device interface for details.

- Local Tunnel Address: The local virtual IP address of the VPN tunnel server. After dialing in, the client can access the server via this address.
- Address Pool IP Range: The range of IP addresses in the address pool that the PPTP server allocates to clients.
- DNS Server: The DNS address sent from the PPTP server to the client.
- MPPE Encryption: If enabled, the PPTP tunnel will be encrypted by MPPE. By default, no encryption is enabled on the server. Enabling MPPE encryption will lower the bandwidth performance. If there is no special security requirement, it is recommended to keep this function disabled.
- Authentication Methods: PAP, CHAP, MS-CHAP, and MS-CHAPv2.
- PPP Link Maintenance Interval: The time interval between two PPP link maintenance tests after PPTP VPN is connected.

Step 5 Click Save.

8.3.2 Set PPTP Client

Step 1 Enter VPN Management > PPTP > PPTP Settings.

Step 2 Enable the function.

Step 3 Select Client as the strategy type.

Step 4 Enter Related Parameters

Note

The available parameters may differ among devices of different models/versions. Refer to the actual device interface for details.

- User name and password: The user name and password for PPTP tunnel user identity verification. Note that they should be the same as the server settings.
- Binding Interface: WAN port used by the client.
- Local Tunnel IP: The virtual IP address of the client in the VPN tunnel.
- Server IP Address: The WAN port IP address or domain name of the server. The exit IP address of the server must be a public IP address.
- Target terminal network range: Enter the LAN network segment of the server you want to access. It cannot overlap with the LAN network segment of the client.
- MPPE encryption: should be consistent with the server configuration.
- Work Mode:
  - NAT: Only allow the client to access the server network and not allow the server to access the client network.
  - Routing: Allow server to access client network.
- Link Maintenance Interval: The interval between two PPP link maintenance tests. PPTP tunneling is enabled after the two ends successfully establish a PPP link. We recommend you to keep the default value.
- Authentication methods: PAP, CHAP, MS-CHAP, and MS-CHAPv2.
- Redirect all network data via VPN: When enabled, the client will force all IPv4 traffic generated by it to go through the VPN tunnel.

Step 5 Click Save.

Step 6 (Optional) After you complete the configuration on both ends, you can go to VPN Management > PPTP > Tunnel Information List to view the connected tunnels.

8.4 OpenVPN

OpenVPN is a VPN that realizes two/three-layer tunnels via virtual NICs. OpenVPN supports flexible client authorization methods, including certificate, user name, and password. It allows users to connect to the virtual interface of VPN via firewall, which is more simple and user-friendly than other types of VPN.

OpenVPN can pass through most proxy servers and work well in NAT environment. The server can push certain network configuration information to the client, including IP address, routing settings, DNS configuration, etc.

Note

Make sure the server time is synchronized with the client time. Otherwise, the OpenVPN certificate will not take effect.

8.4.1 Set OpenVPN Server

Basic Settings

Step 1 Enter VPN Management > OpenVPN > OpenVPN Settings.

Step 2 Enable the function.

Step 3 Set Strategy Type to Server or Server Cluster.

Step 4 Enter Related Parameters

Note

The available parameters may differ among devices of different models/versions. Refer to the actual device interface for details.

- Device Mode: Select the type of virtual network devices.
  - TUN mode: Network layer (Layer 3) device that only handles IP data packets.
  - TAP mode: Data Link Layer (Layer 2) device that handles Ethernet frames.
- Server Mode: The device supports authenticating via account and password, certificate, or account and password + certificate.
- All communications of OpenVPN are based on a single IP port and use the UDP or TCP protocol. It is recommended to use the UDP protocol.
- Server IP address: The IP address of the server for client access. Domain name is also supported.
- Server Port: The port used by the OpenVPN service process.
- IP address range of address pool: OpenVPN address pool network segment. The first available IP address in the address pool is assigned to the server, and the rest are assigned to clients.
- Set router configuration: When the client accesses the server's LAN, it should go through the VPN dial-up line. To allow the client to access the server's LAN, you need to set this parameter to inform the client of the router information. No more than 3 routes can be configured.
- Client Configuration: Click "Export" to export the parameter configuration tar package for the client connected to this server. After decompression, use it to configure the OpenVPN client.

Step 5 Click Save.

Advanced Settings

- TLS Authentication: The TLS key is used to enhance OpenVPN security by requiring both sides to have a shared key before the TLS handshake. After enabling TLS authentication, the client should import the TLS key.
- Data Encryption: The data packets are encrypted before transmission to ensure that the

information cannot be read even if the data packets are intercepted.

- Digest Algorithm: The Digest Algorithm used by the server will be informed to the client. Default is SHA256.
- Allow Data Compression: If enabled, the data can be compressed by LZO algorithm to save bandwidth at the cost of certain CPU resource occupation. Note that this configuration should be consistent between the client and server for connection success.
- All Network Data through VPN: When enabled, this will force all IPv4 traffic generated by clients to pass through the VPN tunnel. Applicable only to SSL/TLS mode (certificate parity check) for tunnel networks with subnets greater than /30.
- Push DNS Configuration: The server sends the DNS address to the client. Currently, only Windows system clients can receive the DNS address.

8.4.2 Set OpenVPN Client

Step 1 Enter VPN Management > OpenVPN > OpenVPN Settings.

Step 2 Enable the function.

Step 3 Select Client as the strategy type.

Step 4 Select Manual Verification or Interface Configuration for Client Configuration.

Step 5 Enter Related Parameters

Note

The available parameters may differ among devices of different models/versions. Refer to the actual device interface for details.

- Device Mode: Select the type of virtual network devices.
  - TUN mode: Network layer (Layer 3) device that only handles IP data packets.
  - TAP mode: Data Link Layer (Layer 2) device that handles Ethernet frames.
- Server Mode: The device supports three authentication modes: account and password, certificate, and account and password + certificate.
- User Name and Password: Enter the user name and password configured on the server.
- Client Configuration: Select the client configuration file exported from the server side for upload.
- Device Mode: The configuration should be consistent with that of the server.
- Configuration: The configuration should be consistent with that on the server.
- Server Address: The IP address or domain name of the server to be connected to.
- Server Port No.: The port number of the server to be connected.
- CA certificate: Tap Browse to select a CA certificate file with .ca extension and upload it.

Step 6 (Optionally) When the Client Configuration is set to Interface Configuration, refer to Advanced Settings for details about the related settings.

Note

- If the server certificate is not used to display signature, you need to disable "Server Uses Certificate to Display Signature" for the connection to be established.
- If you want to accept the server's route and network segment push so that your devices can access these segments via this VPN route, enable Server Route Push.

Step 7 Click Save.

Step 8 (Optional) After you finish the configuration on both ends, go to VPN Management > OpenVPN > Tunnel Information List to view the connected tunnels.

8.5 Account Management

Go to VPN Management > Account Management to view and manage L2TP/PPTP/OpenVPN server users.

- Add User: Click "Add" to set username, password, server type, and access mode.
- Enable / disable: Click the slider in the user name list to enable or disable the user account quickly.
- Change PIN: Click in the user name list to change the PIN.
- Modify Access Mode: Click in the user name list to change the access mode.
- Delete account: Click in the user name list to delete the account.

Chapter 9 Advanced Management

Note

The supported configuration functions may vary for different device models/versions. Refer to the actual interface.

9.1 Route Configuration

Supports configuring multiple routing strategies, including policy-based routing, static routing, and address library selection. When multiple strategies exist, the priority is: policy-based routing > static routing > address library selection.

9.1.1 Policy-Based Routing

Policy routing is a mechanism that forwards packets based on user-defined policies. It can perform specified actions (such as setting the next hop or egress interface) for packets meeting certain conditions (such as source and destination addresses).

In multi-WAN mode, the system will select WAN links for data streams in an equalized way by default, which may cause data flow direction error when accessing internal or external networks. Therefore, you need to configure policy-based routing to control data forwarding between internal and external networks.

Note

Not all models support this function. For details, see the actual interface.

Step 1 Go to Advanced Management > Route Configuration > Policy-Based Routing or Advanced Management > Route Configuration > IPv6 Policy-Based Routing.

Step 2 Click Add.

Step 3 Configure the Following Parameters:

- Rule name: Rule name cannot be the same with that of an existing rule.
- Specific Protocol: the specific protocol that the policy routing is applicable to.
- Source IP address/range and destination IP address/range: the matching item of policy-based routing rule.
- Outlet: the interface for forwarding data packets.

Step 4 Click Add.

9.1.2 Static Route

Static routing is the manually set fixed routing entries in routers. When your network structure is simple and stable, you can configure static routing to realize network intercommunication.

Step 1 Go to Advanced Management > Route Configuration > Static Route or Advanced Management > Route Configuration > IPv6 Static Route.

Step 2 Click Add.

Step 3 Configure the Following Parameters:

Note

The configuration parameters of IPv4 and IPv6 are different. Please refer to the actual interface.

- Destination IP address: Only IPv4 static routing configuration is supported. Enter the destination network's IP address that the device will access.
- IPv6 address/length: Only for IPv6 static routing configuration. Enter the IPv6 address and length of the destination network that the input device will access.
- Subnet Mask: The subnet mask of the destination IP address.
- Outlet: the interface for forwarding data packets.
- Next Hop: Set the outgoing interface and next hop IP address for forwarding packets to the destination network.

Step 4 Click Add.

9.1.3 RIP Configuration

RIP (Routing Information Protocol) is a simple interior gateway protocol that is mainly used in small-scale networks to allow routers to exchange routing information via IPv4-based networks.

Step 1 Go to Advanced Management > Routing Configuration > RIP > RIP Configuration.

Step 2 Click Add.

Step 3 Select the type of RIP to add and configure it.

Step 4 Click Add.

Step 5 (Optional) Click RIP Advanced Settings to configure the advanced parameters.

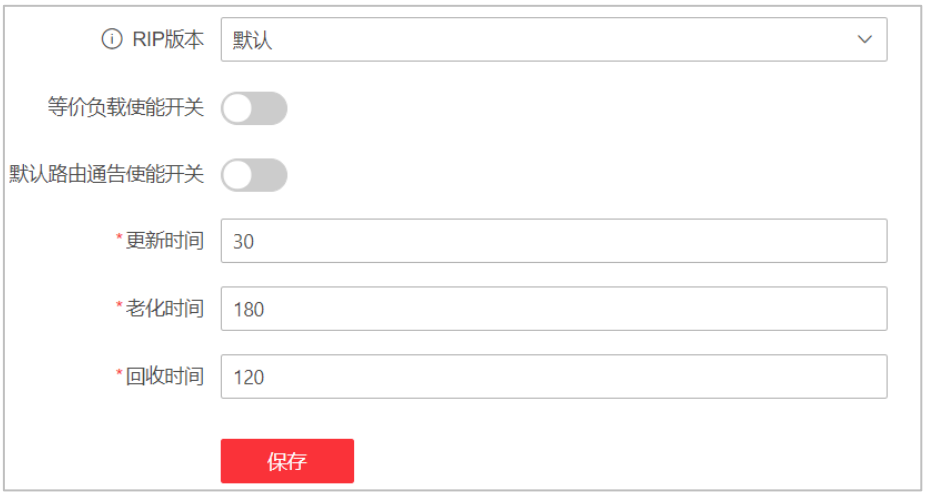

Figure 9-1 Set Advanced RIP Parameters

- RIP version: The version of the RIP protocol to be used.
  - ***RIPv1***: Supports only broadcast updates.
  - ***RIPv2***: Supports multicast updates, CIDR, VLSM, route aggregation, and plain text or MD5 authentication.
- Enable Equivalent Load: After this function is enabled, the traffic can be shunted to multiple equivalent RIP routes, which can improve the bandwidth utilization.
- Enable Default Route Advertisement: Forces RIP to advertise a default route to its neighbors. It is often used in router devices.
- Update Time: Controls the frequency with which the RIP routing device sends routing updates.
- Aging Time: Set the time for routing information to be considered invalid. If no update is received for a route within this period, it will be marked as unreachable.
- Expiration time: The time when the route will be deleted from the routing table.

Step 6 (Optional) Enter Advanced Management > Routing Configuration > RIP > Neighbor Information to view other RIP devices that are directly connected to the current device and exchange routing information with it.

9.1.4 OSPFv2

OSPFv2 (Open Shortest Path First version 2) is an interior gateway protocol based on link state that distributes routing information within a single autonomous system.

Step 1 Set basic parameters.

1. Go to Advanced Management > Routing Configuration > OSPFv2 > Basic Configuration.
2. Tap "Add" / "Click to add process" to add a process.
   - Process ID: A locally significant OSPF instance identifier used to distinguish multiple OSPF processes on the same Device, with a range of [1, 16].
   - Router ID: A 32-bit unique identifier used to identify a router within an OSPF domain, range [0.0.0.1, 255.255.255.255].
   - Enable default route advertisement: When enabled, it forces ABR/ASBR to advertise a default route into the OSPF domain.
   - Distance Management: Set the priority of route confidence. The smaller value means higher priority. It is recommended to keep the default settings.
   - LSA: To prevent frequent LSA updates, you can set the time for generating/receiving LSA.
   - SPF calculation: Set the time interval for SPF calculation to prevent frequent calculation.
   - GR function: Enable graceful restart helper (assist neighbors in completing graceful restart), LSA check, and maximum waiting time as needed.
3. Click Add.
4. Tap "Add Area" / "Tap to Add Area", set the area name and type, and tap "Add".

5. (Optional) Edit or delete the added process/area.
6. (Optional) Click Advanced Settings in the upper-right corner of the process to add routing reference for the current process.

Step 2 Set the API parameters.

1. Go to Advanced Management > Routing Configuration > OSPFv2 > Interface Configuration.
2. Click Add to add API configuration.
3. Select Application API, Application Process, and Area.
4. (Optional) Set parameters such as priority, network type, and HELLO message.
5. Click Add.
6. (Optional) Edit or delete the added API.

Step 3 Go to Advanced Management > Routing Configuration > OSPFv2 > Neighbor Information to view the OSPF neighbor information.

9.1.5 Route Table Information

Go to Advanced Management > Routing Configuration > Routing Table Information to view IPv4/IPv6 routing table information, or filter and display the current existing routing information by routing type.

9.2 PoE Power Supply

Note

Not all models support this function. For details, see the actual interface.

Go to Advanced Management > PoE Supply to view the total power and port power supply information.

Supports configuring PoE switch and powering on the connected AP devices.

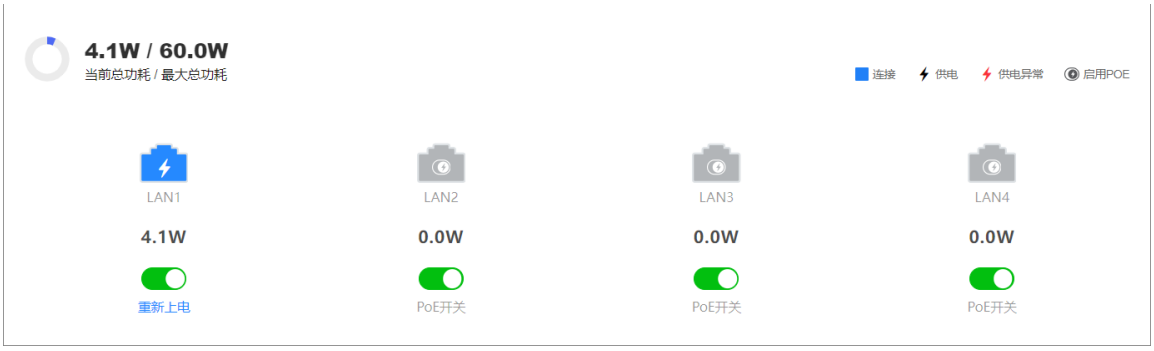

Figure 9-2 PoE Power Supply

9.3 PPPoE Server Configuration

The gateway can act as the PPPoE server to provide dial-up Internet access and IP address allocation for connected devices.

Note

Not all models support this function. For details, see the actual interface.

Step 1 Enable Global Configuration:

1. Go to Advanced Management > PPPoE Server Configuration > Global Configuration.
2. Enable Global Configuration and Configure the Following Parameters:
   - Enforce PPPoE Dial-up: When enabled, users can access the Internet via IP addresses in the exception list but not via other IP addresses.
   - Local Address: The point-to-point address of the PPPoE server.
   - Address Pool IP Range: The range of IP addresses allocated by the PPPoE server to clients.
   - VLAN: Current VLAN of the PPPoE server.
   - Alternate DNS server: The alternate DNS server address that is applied to the client.
   - Max. Unresponded LCP Packets: If the number of unresponded LCP packets exceeds this value, the PPPoE server will automatically disconnect this connection.
   - Authentication Method: PAP, CHAP, MSCHAP, or MSCHAPv2.
3. Click Save.

Step 2 Add account, user needs to approve account PIN to get online:

1. Go to Advanced Management > PPPoE Server Configuration > Account Management.
2. Click Add.
3. Set the account and password for the device. You can also set expiration time for the account.
4. (Optional) Enable account rate limit and select the binding set.
5. Click Add.

Note

- After the account is deleted or its status is changed to closed, all users who log in with this account will be logged out and need to log in again with a new account and password.
- Editing account password and notes will not affect the devices using this account to dial-up and go online.

Step 3 Exception IP: The user can access the Internet via PPPoE dial-up mode with this IP address.

1. Go to Advanced Management > PPPoE Server Configuration > Exceptional IP Management.

2. Click Add.
3. Set the range of exception IP addresses.
4. Click Add.

Step 4 Optional Operation:

- Manage Online Users: Enter Advanced Management > PPPoE Server Configuration > Online Users to view the information of up to 32 online devices. You can also force disconnect users from one or more devices in batches.
- Set Account Bandwidth: Go to Advanced > PPPoE S***erver Conf***iguration > Account Set Management, and click Add to set the downstream and upstream bandwidths of the account and other parameters.

Note

- If the intelligent flow control is disabled, you cannot configure the limit speed status of the account. Before configuring the PPPoE account limit speed, make sure that the intelligent flow control is enabled.
- After the intelligent flow control is disabled, the speed limit status of accounts that are bound to sets will be changed to Disabled, and the binding relationship between accounts and sets will be automatically unbound.

9.4 IP Address Connection Limit Exceeded

Step 1 Enter Advanced Management > Connection Limit.

Step 2 Click Add.

Step 3 Set the rule name, IP address range, and maximum connections (range [50, 20000]).

Step 4 Click Add.

9.5 Port Mapping

9.5.1 Configuration port mapping

Map the specified port of the LAN server to a WAN IP address and port, facilitating access from the WAN to services provided by the LAN server on the specified port.

Enter Advanced Management > Port Mapping > Port Mapping, click Add, and configure the following parameters:

- rule name: A description of the port mapping rule for identification.
- Common Server: Select the service type to be mapped, and the system will automatically fill in the common internal port number of the service. You can also enter a custom port number.
- Protocol Type: Select the protocol class for the selected service between TCP and UDP, or select

Both to enable both protocols. The selected protocol class should conform to the client configuration of the selected service.

- External Server IP: The IP address of the main server for WAN access.
  - Select All WAN Ports or Select Specified WAN Port.
  - External IPv4 address: Enter the WAN IP address.
- **Externa**l Port / Range: The port number that WAN clients use to access the device.
- **Interna**l Server IP: The address of the server that sets up service in the LAN.
- **Interna**l Port Range: The service port of the LAN host.

9.5.2 Enable NAT-DMZ

When the data packet from WAN does not match any port mapping rule, it will be redirected to the LAN server according to the DMZ rule, which means all data packets sent from Internet to device will be forwarded to the specified DMZ server, and then the LAN server can provide services for WAN users. At the same time, other hosts in LAN are protected.

Enter Advanced Management > Port Mapping > NAT-DMZ, enable this function, and enter the server address.

9.6 Address Group Management

Go to Advanced Management > Address Group to add, edit, or delete address groups.

Predefined address group for quick selection in configuration process such as Internet access management.

9.7 Time Period Management

Enter Advanced Management > Time Management to add, edit, or delete time periods.

Predefined time periods are convenient for you to select applications quickly in the process of configuring Internet behavior management and other functions.

9.8 Dynamic Domain Name System

Setting a dynamic domain name system binds a dynamically changing WAN IP address to a fixed domain name, facilitating remote access.

Note

Different models/versions of devices support different types of dynamic domain name system settings, including PeanutHull, NO-IP, DynDns, 3322.org, cloudfare, Alibaba Cloud, and Comexe. The following two domain name settings are provided as examples for illustration; please refer to the actual interface for specific details.

9.8.1 PeanutHull Dynamic Domain Name System

By binding the WAN IP address of devices with the domain name of PeanutHull, you can access devices via domain names when terminals and devices communicate over the Internet.

Step 1 Go to "Advanced Management > Dynamic Domain Name System > PeanutHull Dynamic Domain Name" or "Advanced Management > Dynamic Domain Name > tap to Add Dynamic Domain Name".

Step 2 Enable the function.

Step 3 (Optional) Fo**r som**e devices, you need to select the service provider as "PeanutHull" manually.

Step 4 Select Service Interface, enter Domain Name, etc.

Step 5 Click Save or Add.

9.8.2 Dynamic Domain Name System

Map the dynamic WAN-side public IP address to a fixed domain name so that users can access the IP address of the WAN side via the domain name.

Step 1 Go to Advanced Management > Dynamic Domain Name System > No-IP Dynamic Domain Name or Advanced Management > Dynamic Domain Name System > Tap to Add Dynamic Domain Name.

Step 2 Enable the function.

Step 3 (Optional) Fo**r som**e devices, you need to manually select the service provider as NO-IP.

Step 4 Select Service Interface, enter Domain Name, etc.

Step 5 Click Save or Add.

9.9 UPnP Configuration

Go to Advanced Settings > UPnP Configuration or Advanced Management > UPnP Configuration to enable or disable this function. Some devices support setting External API.

UPnP (Universal Plug and Play, Universal Plug and Play) is a set of protocols for devices to communicate with each other. As an UPnP gateway, the main function of the device is to complete automatic port mapping. To realize automatic port mapping via UPnP, three conditions should be met:

- The UPnP function of the device should be enabled.
- The operating system of the LAN server should support and enable UPnP.
- The application should support and enable UPnP function. For example, Thunder, BitComet, eMule, and MSN support UPnP function.

When Devices enable UPnP function, it can automatically add port mapping for applications that support this function, speed up peer-to-peer transmission, and resolve issues where traditional services (such as MSN) cannot traverse NAT. However, enabling UPnP function can also establish mappings for illegal applications that support this function, creating safety hazards.

9.10 DNS Management

Note

The supported configuration functions may vary for different device models/versions. Refer to the actual interface.

9.10.1 Local DNS

The local DNS server is not required to be configured. If it is not configured, the device will get the DNS server address from the upstream device. When configured, the local DNS server 1 and 2 have no priority.

Step 1 Go to Advanced Settings > Local DNS or Advanced Management > DNS Configuration > Local DNS.

Step 2 Enter the IP address of local DNS server 1 and local DNS server 2.

Step 3 Click Save.

9.10.2 DNS Policy

DNS policy is a set of rules that control the handling mode of DNS queries.

Step 1 Go to Advanced Management > DNS Configuration > DNS Policy.

Step 2 Select the type of access level to add and configure its parameters.

- Static DNS resolution: Directly bind the domain name with IP address via local file to bypass the DNS query process. The priority is higher than that of DNS server resolution.
- Specify DNS server for domain name resolution: Configure devices to use specific DNS servers for domain name resolution, which depends on network communication to complete the query.

Step 3 Click Add.

9.10.3 DNS Proxy

The DNS proxy is an optional configuration item. If not configured, the device will get the DNS server address from the upstream device. The DNS proxy receives DNS requests from clients and forwards or modifies the responses according to rules. It does not usually participate in recursive queries.

Step 1 Go to Advanced Management > DNS Configuration > DNS Proxy.

Step 2 Enable DNS server proxy.

Step 3 Enter the DNS server IP address.

Step 4 Click Save.

Chapter 10 Fault Diagnosis

10.1 Network Self-test

Perform network self-test when your device has network problem.

Step 1 Go to Fault Diagnosis > Network Self-Test.

Step 2 Click Start Test.

Step 3 Configure your devices according to the test results.

10.2 Fault Alarm

Enter Fault Diagnosis > Fault Alarm to view the list of fault alarms. More operations are as follows:

- Handle the alarm according to the details in the suggestion.
- Click Acknowledge Alarm to delete the alarm record.
- Click Alarm Type Settings to select whether to accept the alarm. If you disable receiving, the system will not report this type of alarm information.

10.3 Network Tools

The following network tools support communication check or query for IPv4 and IPv6 addresses.

10.3.1 PING Communication

The PING command is used to test the network connection to a certain node in the network.

Step 1 Go to Diagnostics > Network Tools > Ping Communication.

Step 2 (Optional) For some devices, you can select the device type.

Step 3 Set Destination IP/DNS Name, Ping Times, and Data Packet Size.

Step 4 Click Start Diagnosis. If the result is "PING Communication Failed", it indicates that the device is not connected to this IP address or domain name.

10.3.2 Route Query

The Routing Query function is used to detect the number of nodes that a data packet passes through and the address of these nodes. By using this function, you can determine the route of data transmission.

Step 1 Go to Diagnosis > Network Tools > Route Query.

Step 2 (Optional) For some devices, you can select the device type.

Step 3 Set the maximum TTL for destination IP address/domain name and routing query.

Step 4 Click Start Diagnosis.

10.3.3 Domain Name Query

Domain Name Query is used to check the information of network domain names or diagnose DNS server issues. When the terminal can ping an IP address on the WAN but cannot access a web page via browser, you can check the domain name to see if the domain name resolution is normal.

Step 1 Go to Diagnosis & Tools > Network Tools > Domain Name Query.

Step 2 Set destination IP address or domain name.

Step 3 Click Start Diagnosis.

10.4 IP Address Conflict Detection

Note

Not all devices support this function. For details, see the actual interface.

IP address conflict detection is used to check if two or more devices in the same LAN have the same IPv4 address.

Step 1 Go to Fault Diagnosis > IP Conflict Detection.

Step 2 Select the VLAN on LAN side.

Step 3 Set the detection range.

Note

By default, the system automatically calculates the test range based on the IP address and subnet mask of the VLAN host. You can also manually narrow down the range.

Step 4 Click Start Test.

10.5 Port Mirroring

Mirroring refers to copying the packets that pass through a specified port (source port or mirror port) to another specified port (destination port or monitor port) for monitoring the network data flow of the mirror port.

Step 1 Enter Fault Diagnosis > Port Mirroring.

Step 2 Click the port in the Port Mirroring Area as the source port. The source port is the port that you want to monitor, also called the mirror source or mirror port. The device where the source port locates is called the source device.

Step 3 Select direction and destination port.

- Direction: Select the directions of packets that can be copied on the source port.
  - Inbound: Copy Only Messages Received by Source Port
  - Outbound: Copy only the messages sent from the source port.
  - Both directions: copy received and sent packets of the source port.
- Destination port: The destination port of mirrored packets is called the destination port or monitoring port. The device where the destination port locates is called the destination device.

Note

- The destination port can only be one port excluding the source port.
- Only one port mirroring can be configured per-session. The configured item can be edited or deleted in the list.
- The configuration will not be saved if you restart the device.

Step 4 Click Save.

10.6 Capture Packet Diagnosis

When a device fails, you can analyze the captured packets to locate and troubleshoot the issue.

Step 1 Go to Fault Diagnosis > Packet Capture Diagnosis.

Step 2 Select the API or File, enter the host IP address, and set the maximum file size and number of messages.

Note

The host IP address supports IPv4 or IPv6 address.

Step 3 Click Start Capturing.

Step 4 (Optional) You can click Stop Packet Capture to stop packet capture at any time.

Step 5 Click Download in the captured packet result area to download the captured packet file and parse it locally.

10.7 Fault Collection

Pack the device configuration file into a compressed file and decrypt and decompress it to provide the information for locating faults to developers.

Step 1 Enter Fault Diagnosis > Fault Collection.

Step 2 Click Collect All.

Step 3 Save the configuration file to local storage.

10.8 Flow Table View

Note

Not all devices support this function. For details, see the actual interface.

A flow table is composed of multiple flow table items. After a data packet enters the switch, it matches with the flow table item according to priority and performs the corresponding action.

Go to Fault Diagnosis > Flow Table to view the current device flow table items. Click in the upper-right corner of the list to customize columns.

10.9 SSH

Enter Fault Diagnosis > SSH to enable or disable the function of remote device management via SSH. For security reasons, it is recommended that you disable the SSH service. This function is for professional users to debug devices.

Chapter 11 System Tools

11.1 System Configuration

11.1.1 Person Information

Go to System Configuration > Basic Information to do the following:

- View the basic information of the gateway device.
- Change the name of the gateway device.
- Select the Work Mode of Gateway Device
- In gateway mode, AP devices are directly connected to the LAN side of the gateway.
- In AC mode, the WAN port of the gateway device and the uplink port of the AP device are connected to the same core switch.
- Enable AP Management (available for some devices only).
- CAPWAP tunnel encryption (supported by some devices only). The CAPWAP control messages are encrypted by DTLS (Datagram Transport Layer Security) to prevent the configuration parameters in CAPWAP tunnel messages from leaking.

11.1.2 Time Configuration

Enter System Configuration > Time Configuration to select the time zone, and then select one of the following methods to calibrate time.

- Set NTP Server: Enter the server IP address and set the time calibration interval.
- Manual Verification: You can set the time manually or click Sync With Computer Time.

11.2 Cloud Platform Configuration

After adding devices to the cloud platform, you can manage them on the cloud platform.

Step 1 Enter System Configuration > Cloud Platform Configuration.

Step 2 Enable the Cloud Platform function on the Hik-Connect for Teams Mobile Client.

Step 3 (Optional) Customize the access server address.

Step 4 Click OK.

Step 5 Scan the QR code of the device via Hikvision Market or Hikvision Cloud Mobile Client to link the device to your Hikvision Cloud account.

Note

- The device should be online to link with the Hik-Connect account.
- After linking your Hik-ProConnect account, if you need to unlink your AP from the Hik-ProConnect account, go to the Hik-ProConnect Mobile Client and perform the unbinding operation. You can also restore the AP to factory settings to automatically unlink it from the Hik-ProConnect account.

11.3 Maintenance

11.3.1 Upgrade Gateway

Go to Maintenance & Security > System Maintenance > Upgrade to upgrade the gateway device in the following two ways:

- Local Upgrade: Click , select the local upgrade package, and then click Upgrade.
- Online Upgrade: After the device is connected to the network, it will automatically detect for the latest version. Click Check for Updates now to upgrade. The device will restart automatically after upgrading is completed.

11.3.2 Reboot Gateway/AP

Go to Maintenance & Security > System Maintenance > Reboot to manually reboot the gateway/AP device or set scheduled reboot.

- Manual Verification: Select the gateway or AP device and click Restart.
- Scheduled Restart: Enable this to set the scheduled date and time. Click Save to restart the gateway and all APs at the scheduled time.

11.3.3 Backup And Reset Gateway

Go to Maintenance & Security > System Maintenance > Backup & Reset.

- Export: Click Export to generate the backup configuration file and download it to your local computer.
- Restore: Click Restore to restore the device to its factory settings.
- Backup Import: Click , select the local backup configuration file, and then click Import.

11.3.4 Log Management

Security Audit Log is used to monitor and detect security events and behaviors of devices, as well as conduct security event investigations and tracebacks.

Step 1 Go to Maintenance & Security > System Maintenance > Security Audit Log.

Step 2 Select the grading, module, keyword, or time, and then click Search.

Step 3 Click Export to export the selected log(s) to your local computer.

Step 4 (Optional) Configure the log server by entering the server IP address and port, with the port number range [1, 65535].

11.3.5 Login Management

Go to System Configuration > System Configuration > Login Management or Maintenance and Security > System Maintenance > Login Management" to set the "login timeout threshold. After exceeding this time, you need to log in to the management page again.

11.3.6 Remote Web Access

Note

Not all devices support this function. For details, see the actual interface.

Go to Maintenance and Security > Remote Web Access, click Enable to check Remote Web Access, and set the duration. After you enable remote web access, users can access the web page of the gateway via its WAN IP address.

Chapter 12 Frequently Asked Questions

Scan the QR code below or tap the link to view the FAQ collection.

https://pinfodata.hikvision.com/analysisQR/showQR/4de0b9c3

UD45463B